

## Legal Notice

Neither the documents nor the programs that you may access may be copied, reproduced, translated, or transferred to any electronic or readable media without prior written permission from Cytomic (Business Unit of Panda Security, S.L.U.), Santiago de Compostela, 12, 48003 Bilbao (Bizkaia), SPAIN.

## Registered Trademarks

Windows Vista and the Windows logo are trademarks or registered trademarks of Microsoft Corporation in the United States and/or other countries. All other product names may be registered trademarks of their respective owners.

© Cytomic 2024 (Business Unit of Panda Security, S.L.U.). All rights reserved.

## Contact Information

Corporate Headquarters:

Cytomic (Business Unit of Panda Security, S.L.U.)

Calle Santiago de Compostela 12

Bilbao (Bizkaia) 48003 Spain.

<https://www.pandasecurity.com/spain/about/contact/>

**Version:** 2.34.22

**Author:** Cytomic

**Date:** 12/2/2024

## **Cytomic Orion Technical Documentation**

To get the latest version of this User Guide, go to:

<https://info.cytomicmodel.com/resources/guides/Orion/en/ORION-guide-EN.pdf>

For more information about a specific topic, see the product online help at:

<https://info.cytomicmodel.com/resources/help/ORION/en/index.htm>

For more information about the specific functions of the Threat Hunting library, see the online help at:

<https://info.cytomicmodel.com/resources/help/ORION/en/threathuntingAPI/index.htm>

For more information about the specific functions of the Notebooks library, see the online help at:

<https://info.cytomicmodel.com/resources/help/ORION/es/Notebooklib/index.htm>

## **Technical Information about Modules and Services Compatible with Cytomic Orion**

To see the ServiceNow integration guide, go to:

<https://info.cytomicmodel.com/resources/guides/Orion/en/ORION-snowguide-EN.pdf>

To see the MISP integration guide, go to:

<https://www.vanimpe.eu/2020/03/10/integrating-misp-and-cytomic-orion/>

## **Cytomic Orion User Guide Survey**

Rate this guide and send us suggestions and requests for future versions of our documentation at:

<https://es.surveymonkey.com/r/feedbackOrionGuideEN>

# Table of Contents

---

<b>Table of Contents</b> .....	<b>4</b>
<b>Preface</b> .....	<b>10</b>
Target Audience .....	10
What is Cytomic Orion? .....	11
Icons .....	11
<b>Basic Information about Cytomic Orion</b> .....	<b>12</b>
Threat Hunting Aims .....	12
Cytomic Orion Benefits .....	14
Cytomic Orion Architecture .....	16
Cytomic Orion Features .....	22
Product User Profile .....	24
Supported Operating Systems, Browsers, and Languages .....	25
Response Tool Requirements .....	27
<b>Analysis Console</b> .....	<b>28</b>
Benefits of the Analysis Console .....	28
Analysis Console Requirements .....	29
Analysis Console General Structure .....	30
Top Menu (1) .....	30
Left-side Panel (2) .....	34
Right-side Panel (3) .....	35
Central Panel (4) .....	35
Basic Components of the Analysis Console .....	35
<b>Access, Control, and Monitor the Analysis Console</b> .....	<b>44</b>
General Concepts .....	45
Manage User Accounts .....	45
Create the First User Account .....	46
Create Subsequent User Accounts .....	47
Edit the Personal Details for a User Account .....	48
Edit the Email Address or Password for a User Account .....	48
Delete User Accounts .....	49

Enable Two-factor Authentication .....	50
Client Visibility Settings .....	51
Manage Roles and Permissions .....	53
Basic Concepts .....	53
Create and Configure Roles .....	54
Understanding Permissions .....	56
User Account Activity Log .....	60
<b>Indicators and Hunting Rules .....</b>	<b>64</b>
Basic Concepts of the Indicator System .....	64
Access the Indicators Area .....	66
Indicators List .....	66
Filter and Group Indicators .....	69
Delete Indicators Manually .....	70
Delete Indicators Automatically .....	71
Manage Deletion Rules .....	73
Restore Indicators and Manage the Recycle Bin .....	75
Indicator Management Best Practices .....	76
<b>Manage Hunting Rules .....</b>	<b>78</b>
List of Hunting Rules .....	79
List of Hunting Rules .....	79
Manage Hunting Rules .....	80
Manage Hunting Rules .....	81
Create a Hunting Rule .....	82
Validate a Hunting Rule .....	85
Edit a Hunting Rule .....	86
Delete a Hunting Rule .....	86
Email Notification Rules .....	87
Create a Notification Rule .....	87
Edit a Notification Rule .....	88
List of Notification Rules .....	88
Manage the List of Notification Rules .....	88
Notifications Related to Changes in the MITRE Framework .....	90
<b>Manage Investigations .....</b>	<b>92</b>
Investigations List .....	93
Investigations List .....	93
Search for, Sort, and Filter Investigations .....	95
Create an Investigation .....	95

---

Manually Assign and Remove Indicators from Investigations .....	96
Automatically Assign and Remove Indicators from Investigations .....	98
Create an Assignment Rule .....	98
Edit an Assignment Rule .....	99
Run an Assignment Rule Manually .....	99
Assignment Rules List .....	99
Manage the Assignment Rules List .....	100
Structure of an Investigation .....	100
The Investigation Page .....	101
Entities of Interest Panel .....	107
Manage Entities .....	109
Activity Log Associated with an Investigation .....	117
Remote Operation Log .....	121
<b>Activity Visibility in Cytomic Orion .....</b>	<b>122</b>
Investigations and Indicators Dashboard .....	123
MITRE Dashboard .....	128
Data Usage .....	129
Amount of Data Assigned and Usage Monitoring Resources .....	130
Notebook Data consumed in advanced queries .....	130
Data Usage Dashboard .....	132
Data Usage by User Dashboard .....	133
Data Usage by Query Dashboard .....	135
Data Usage by Client Dashboard .....	137
Assigned Data Dashboard .....	139
Usage Notification Email .....	141
<b>Investigate the Event Flow .....</b>	<b>144</b>
Advanced SQL Query Module .....	145
Queries Side Panel (1) .....	145
Advanced SQL Query Panel .....	153
SQL Statement Optimization .....	155
Wizard-guided Queries Module .....	155
Condition Block Structure .....	157
Results Panel .....	158
<b>Assisted Investigations .....</b>	<b>160</b>
Create Assisted Investigations and Investigation Context .....	160
Create an Assisted Investigation from a Computer Entity of Interest .....	161
Create an Assisted Investigation from an Indicator .....	161

Create an Assisted Investigation from an Event .....	162
Structure of an Assisted Investigation .....	162
Types of Searches in Assisted Investigations .....	164
<b>Indicator Analysis Using the Investigation Console .....</b>	<b>172</b>
Access the Investigation Console .....	172
From a Newly Created or Ongoing Investigation .....	173
From an Indicator .....	175
From the Investigation Console .....	176
From the Cytomic Orion API .....	176
Investigation Console Structure .....	177
Filters Side Panel .....	179
Central Panel .....	180
<b>Graphs .....</b>	<b>188</b>
Access Graphs .....	188
Information Shown on Graphs .....	189
Graph Structure .....	190
Graph Settings .....	191
Information Contained in Graphs .....	198
Process Tree Template .....	198
New Users in a Client Template .....	202
<b>Investigations with Notebooks .....</b>	<b>204</b>
Concepts and Definitions .....	205
Main Benefits of Notebooks .....	208
Access and Create Notebooks .....	208
List of Notebooks Created in an Investigation .....	209
Notebook Structure .....	209
Run a Notebook .....	211
Use Notebook Templates .....	212
Template Management Access .....	212
Template Management .....	213
Use Quick Answers with Notebooks .....	215
Quick Answer Overview .....	215
Quick Answer Management .....	216
Use Parameters in Templates and Quick Answers .....	218
Notebook Management Quick Guide .....	220
Working Method with Notebooks .....	220
Libraries Available in Notebooks .....	223

---

<b>IT Infrastructure Investigation with OSQuery</b> .....	<b>230</b>
Introduction to OSQuery .....	230
Use Cases for Analysts .....	231
Access OSQuery .....	232
Send OSQuery Queries .....	233
OSQuery Statement Results .....	233
<b>Response Tools</b> .....	<b>236</b>
Requirements .....	236
Access the Response Tools .....	237
Description of Response Tools .....	239
Isolate Computer .....	239
Restart Computer .....	241
Process Manager .....	242
Service Manager .....	243
File Transfer .....	244
Remote Command Line .....	245
Command Line Tools .....	245
<b>Advanced Query Module SQL Syntax</b> .....	<b>252</b>
Supported Data Types .....	252
Regular Expressions .....	256
Select Clause Syntax .....	256
Regular Functions .....	262
Aggregate Functions .....	289
<b>Cytomic Orion Integration with SOC Tools</b> .....	<b>292</b>
Test the Functionality of APIs in Cytomic Orion .....	293
Postman Project .....	293
Sample Code in Python .....	294
SOC Integration Architecture .....	294
Types of APIs Available in Cytomic Orion .....	295
Requirements and Access to the Cytomic Orion APIs .....	296
General Requirements .....	296
Enable Access to the API from External Programs .....	296
Cytomic Orion and OAuth Authentication .....	298
Basic Concepts .....	298
OAuth Data Flow .....	299
Cytomic Orion API Specification .....	307



---

IOC API .....	308
Knowledge API .....	318
Indicator API .....	325
Response API .....	328
OSQuery Access API .....	331
Data/Advanced Query Access API .....	338
Investigation Management API .....	339
<b>Format of the Events Used in Cytomic Orion .....</b>	<b>374</b>
Fields in the Events Received by Cytomic Orion .....	375
<b>Glossary .....</b>	<b>422</b>

# Chapter 1

## Preface

This User Guide contains basic information and procedures for making the most out of Cytomic Orion.

### CHAPTER CONTENTS

---

<b>Target Audience</b> .....	<b>10</b>
<b>What is Cytomic Orion?</b> .....	<b>11</b>
<b>Icons</b> .....	<b>11</b>

## Target Audience

This documentation is intended for analysts and threat hunters who search for indicators of dangerous activities within an organization IT infrastructure. These activities are usually part of attacks targeted at a company IT infrastructure through very recent malware, or attacks that use legitimate tools that are part of computer operating systems. In both cases, these attacks are not identified as such by cybersecurity vendors; consequently, they are not detected by traditional security tools.

Cytomic Orion is intended for both MSSPs (Managed Security Service Providers) and MDR (Managed Detection and Response) security vendors who offer threat investigation services to a large number of clients. It is also intended for companies that have decided to provide this service within the organization through an internal SOC (Security Operations Center).

To correctly interpret the information the product provides and to draw conclusions that help strengthen a company's security, you must know the tactics and techniques hackers use to navigate an organization's IT systems. You must also have thorough knowledge of the most frequently attacked platforms at process, file system, and registry levels, as well as understanding the network protocols commonly used in corporate networks.

## What is Cytomic Orion?

Cytomic Orion is a cloud service that makes threat hunting tasks easier. Its goal is to detect, at an early stage, cyberattacks designed to go undetected by traditional protection systems (perimeter protection and local protection for workstations and servers). With the set of tools and the knowledge gathered by Cytomic, analysts can detect suspicious execution patterns that exploit operating system legitimate tools to take advantage of flaws and access companies' information systems.

After a threat is detected, Cytomic Orion also makes remediation tasks easier by providing the information necessary for designing a correct response plan.

## Icons

These icons are used in this guide:



*Explanations and additional information, such as an alternate method for performing a certain task.*



*Suggestions and recommendations.*



*See another chapter or section in the User Guide.*

# Chapter 2

## Basic Information about Cytomic Orion

Cytomic Orion is a tool that makes it easier to seek out attacks that use advanced tactics to evade detection by the protection installed on workstations and servers.

The general architecture of Cytomic Orion and the functionality provided in each of its modules have been designed to adapt to the roles in SOCs of medium-sized and large companies or those in an MSSP/MDR vendor.

### CHAPTER CONTENTS

---

<b>Threat Hunting Aims</b> .....	<b>12</b>
<b>Cytomic Orion Benefits</b> .....	<b>14</b>
<b>Cytomic Orion Architecture</b> .....	<b>16</b>
<b>Cytomic Orion Features</b> .....	<b>22</b>
<b>Product User Profile</b> .....	<b>24</b>
<b>Supported Operating Systems, Browsers, and Languages</b> .....	<b>25</b>
<b>Response Tool Requirements</b> .....	<b>27</b>

## Threat Hunting Aims

Digitization of commercial and governmental activities has become a major source of wealth, and a key factor that differentiates organizations from their competitors. Hackers therefore, with new economic, political, and strategic goals, have developed increasingly sophisticated techniques to illegally access confidential intellectual property. .

### New Techniques and Tactics Used in Cyberattacks

As companies and governments continue to expand into the digital world, there are more incentives to develop new, sophisticated strategies to bypass perimeter security solutions (firewalls, UTMs, SCMs,

NGFWs, etc.) and local ones (antivirus, EDR, NGAV, etc.) without being detected. New tactics used in cyberattacks include:

- Recruitment of company employees (insiders) who make it easier to access IT systems.
- Exploiting legitimate tools already installed on IT systems and which therefore go undetected by security solutions. These are known as 'living off the land' techniques.
- Use of social engineering to deceive company users and clients (phishing) and create an environment that provides access to its IT systems.
- Use of multiple infection vectors to bypass organization defenses and then move laterally to obtain a position from which high-value objectives can be targeted.

The spread of these advanced techniques and tactics has seen the rise of a new category of malware: APTs, or Advanced Persistent Threats. These are targeted attacks with very specific goals and which delay the inclusion of digital signatures into the signature files used by security providers in their traditional protection solutions. These sort of advanced attacks thereby maximize the window of opportunity for reaching their targets.

For this reason, the 'sit and wait' approach used by conventional security tools in dealing with APTs and similar threats means the exposure time will extend **on average to 175 days from the beginning of an attack until it is visible and detectable**. It is therefore often down to law enforcement agencies or credit card companies to pick up the pieces, and by then companies' reputations can be severely affected.

## The Response: Threat Hunting

Governments and corporations have identified this risk and have allocated larger budgets for creating specialized resources: a new group of professionals focused on detecting and repelling this type of cyberattack. Generally known as 'threat hunters', this figure has the knowledge necessary to detect new cyberattack techniques and tactics, and leverage a new set of advanced tools to bolster the traditional security products already implemented by companies.

Threat hunting tools enable SOCs within organizations to face their main challenges:

- Difficulty finding qualified staff to perform experienced security analyst tasks.
- Larger number of potentially dangerous situations that companies face. This can exceed the capacity of the SOC, and increase the chances of real alerts not being investigated due to lack of time or resources.
- The growing number of sophisticated tools required and the absence of a single, centralized solution that meets all the needs of SOCs underlines the need for highly integrated tools to deliver a cohesive and flexible software solution.

For this reason, companies and nations are forced to contemplate far larger budgets if they want to face these new attacks and protect their intellectual property and credibility.

## Cytomic Orion Benefits

Cytomic Orion is a service for specialized security analysts. Its key benefits are:

- Proactive and automated search for advanced threats and cyberattacks that do not use malware to achieve their goals, thereby making their detection through conventional security tools more difficult.
- Search for TTPs (tactics, techniques, and procedures) used by hackers.
- Early detection of attacks before they can achieve their goals.
- Ability to establish response measures against detected threats, including containment of security breaches, rollback of changes made by attackers to computers on the network, and collection of evidence to perform forensic analysis tasks.
- Seamless integration with the other tools used by SOCs.

### Proactive Search for Advanced Threats

Cytomic Orion continuously monitors networks and searches for indicators under the premise that there is a permanent threat of attackers successfully ‘installing’ themselves on an organization network. It automatically creates hypotheses in the form of indicators that show the new evasion techniques and lateral movements detected, providing analysts with a starting point for more in-depth investigation to validate these hypotheses.

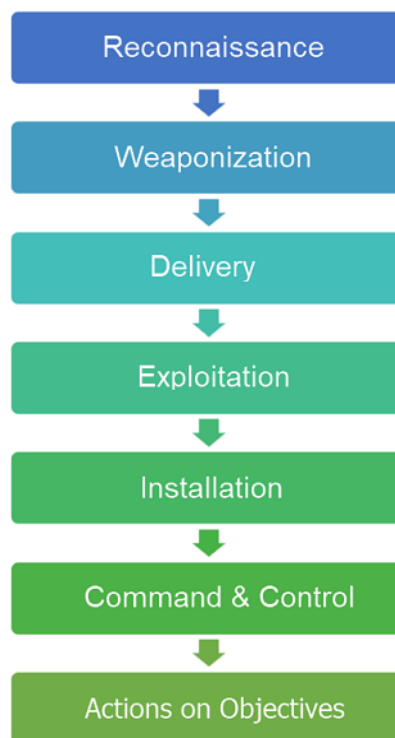


Figure 2.1: CKC chain phases

## Early Detection of Attacks

Early detection of the attacker makes it possible to reduce the risk, accelerate containment capabilities, and reduce operational costs. Cytomic Orion can stop attacks in any of the phases defined in the cyber kill chain (CKC).

## Search for TTPs

The ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge) framework, developed by the MITRE Corporation, was created in 2015 as a living and growing document of the tactics and techniques used by hackers, resulting from researching millions of attacks on networks.

The MITRE Corporation's goal is to coherently and clearly divide and classify attacks, facilitating their identification and detection. Most attackers use a combination of tactics and techniques to hide their lateral movements, discover and exploit system weaknesses, evade protection, and take advantage of weaknesses and non-secure settings on networks and computers.

Finding each one of these techniques during an ongoing attack is crucial in identifying which phase of the CKC the attacker is in. This streamlines the analysis and increases efficiency in collecting evidence that helps to identify a hacker's goals and enables a company to develop a detailed response plan.

For this reason, the Cytomic Orion threat hunting rules match the techniques described in the ATT&CK framework, thereby facilitating their interpretation and accelerating the implementation of response mechanisms.

## Response Measures

Incident response is a process made up of a series of sequential steps led and taken by the CSIRT (Computer Security Incident Response Team), many of which are assisted by the remote remediation tool provided by Cytomic Orion:

### Damage Containment and Risk Mitigation

Quick action can reduce the effects and severity of an attack. The aim of the containment phase is to protect an organization confidential information during the course of the attack without interfering with the tasks carried out by the incident response team. This includes protecting system files against loss or tampering that can result in prolonged service outage.

### Identification of the Type and Severity of an Attack

For an organization to recover effectively from an attack, it must be able to determine the severity of the risk that the computers on its network have been exposed to. To do that, organizations must be able to establish the nature, source, start date, and purpose of the attack, and identify which computers have been compromised and which files have been accessed by attackers.

### Collection of Evidence

In many cases, if an organization suffers a targeted attack, it may be necessary to report it to the relevant law enforcement agencies. To do that, you must collect evidence of the attack: files tampered with, network traces, executed processes, as well as other information from compromised computers.

## Recovery of Computers

How services are restored generally depends on the scope of the security incident. Any method must include action plans for dealing with deletion of files and processes, recovery of backups made prior to the start of the incident, etc.

## Integration with SOC Tools

Cytomic Orion incorporates multiple APIs to facilitate integration with the other tools deployed at the SOC. This way, organizations can build a set of tools that provide these benefits:

- Enable the SOC to provide a homogeneous response to the various types of incidents and situations it will face.
- Minimize manual data exchange among the different tools implemented.
- Automate repetitive tasks, enabling technicians to save time and effort that they can devote to more productive tasks.

# Cytomic Orion Architecture

Cytomic Orion is an advanced threat hunting service that integrates with the different tools used by corporate SOCs to perform these tasks:

- Triage/filter indicators.
- Investigate threats.
- Set containment and response policies.
- Report detected malicious activity and the actions performed to mitigate its effects.

To do that, Cytomic Orion analyzes all the information collected by Cytomic EDR: the events and actions carried out by the processes run on workstations and servers are sent to the cloud and enriched with context and security information to generate telemetry. This telemetry is interpreted by Cytomic Orion to generate indicators that SOC technicians investigate, searching for malicious activity.

Below is a diagram of the different modules that make up Cytomic Orion, as well as the actors and data sources that interact with the environment. Additionally, there is an introduction to the concepts most frequently used in this User Guide.

The Cytomic Orion architecture is divided into three large groups:

- SOC/MSSP/MDR staff.
- Platform processes and technologies.
- Intelligence, integration, and external data sources.



## SOC/MSSP/MDR Staff



Figure 2.2: SOC/MSSP/MDR staff

In mid-to-large-sized SOC, technical staff are specialized and organized into tiers according to their skill sets:

- **Tier 1:** Analysts performing indicator triage. They check and catalog the hypotheses generated by Cytomic Orion and create investigations that group similar indicators to assign them to Tier 2 and Tier 3 technicians, who analyze them in more depth. Additionally, Tier 1 technicians rule out false hypotheses that correspond to normal process operations. As such, they act as a filter that prevents overloading higher tiers.
- **Tier 2:** Analysts who receive the investigations generated by Tier 1 which are likely to pose a threat to the organization. This tier is responsible for investigating indicators to identify genuine intrusion attempts, assessing the resulting damages, and setting relevant remediation and containment methods.
- **Tier 3:** Top-level security analysts who develop new hypotheses using different investigation methods based on external information, such as third-party security bulletins, CVEs (Common Vulnerabilities & Exposures), portals and web pages specialized in security, etc. They do not require the indicator triage performed in Tier 1 in order to perform their tasks,
- **SOC Manager:** Responsible for coordinating analyst activity, reassigning investigations, allocating resources and time to priority clients, and assessing the performance and results of completed investigations.

## Platform Processes and Technologies

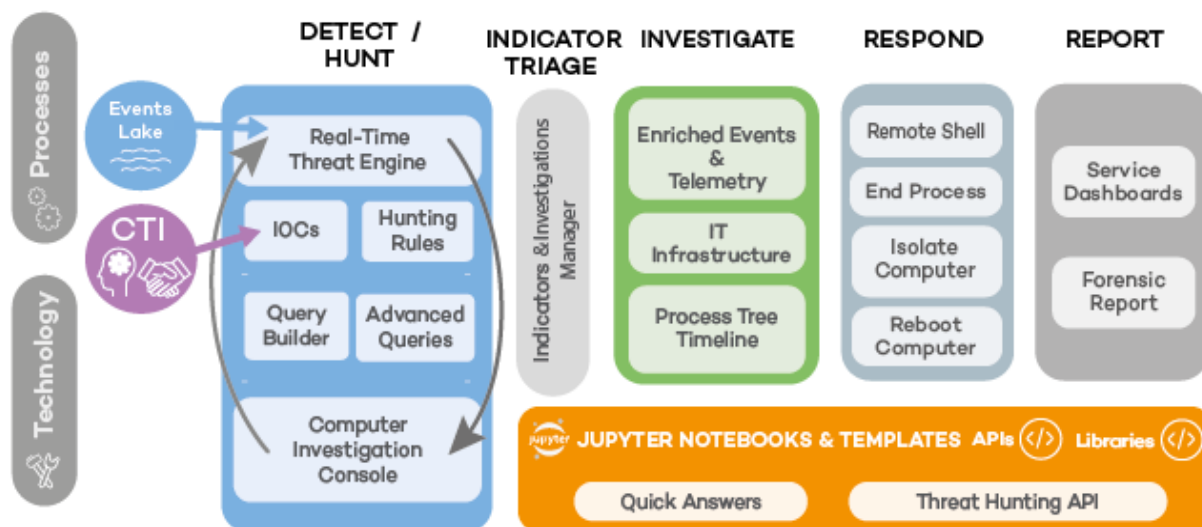


Figure 2.3: Platform processes and technologies

Process	Technology	Description
Detection and searches	CTI (Cyber Threat Intelligence)	Open-source platform that centralizes and stores security intelligence about recent malware. It supports investigations into cyber crime and cyber espionage.
	Data lake	Data source used by Cytomic Orion to execute hunting processes and retrospective analyses. It contains all telemetry collected from computers in the organization as a result of monitoring the processes run on all workstations and servers on the company network. The retention time for the telemetry stored in the data lake is one year.
	Real-time cyberattack radar	Checks the data lake automatically and in real time, searching for suspicious event patterns that could indicate a cyberattack.
	Hunting rules	Describe the behavior patterns that the cyberattack radar looks for in the telemetry data flow generated by the processes executed on the client’s computers. See <a href="#">Indicators and Hunting Rules</a> on page 64 and <a href="#">Manage Hunting Rules</a> on page 78.
	IOCs	Industry standard for describing conditions that can

Process	Technology	Description
		compromise the security of organizations. Despite being a similar concept to the signature file used by malware protection tools, IOCs use an open format that enables sharing and exchange. The cyberattack radar supports IOCs to search for patterns in real time.
	<b>Wizard-guided queries</b>	Build queries in a simple, guided way to retrieve tabulated information from the data lake. See <a href="#">Advanced SQL Query Module</a> on page 145.
	<b>Advanced queries</b>	Create complex SQL queries. See <a href="#">Advanced SQL Query Module</a> on page 145.
	<b>Investigation console</b>	Enables a retrospective analysis of the processes run on workstations and servers to get more in-depth data about the conditions that triggered the indicator generated by the real-time cyberattack radar. See <a href="#">Indicator Analysis Using the Investigation Console</a> on page 172.
<b>Indicator triage</b>	<b>Manual filtering by Tier 1 analysts of the indicators generated by the cyberattack radar. Its purpose is to distinguish indicators corresponding to real attacks from false positives. This prevents task overload at Tier 2, directing analysts' attention to the cases that pose an actual threat to the organization.</b>	
<b>Analysis</b>	<b>This includes all the features of the investigation console, the graphs, and the resources implemented in the agent installed on the company IT devices.</b>	
	<b>Process tree</b>	Shows the parent-child relationships of the processes run on the computers on the IT network. See <a href="#">Graphs</a> on page 188.
	<b>Timeline</b>	Shows all occurred events, sorted by time stamp to help analysts view the progression of attacks.
	<b>Enriched event list</b>	Shows the complete list of all events occurred and enriched with Cytomic security intelligence. See <a href="#">Indicator Analysis Using the Investigation Console</a> on page 172.

Process	Technology	Description
	IT infrastructure	Complete access to the status of resources and processes on the computers within the company IT infrastructure. See <a href="#">IT Infrastructure Investigation with OSQuery</a> on page 230.
Incident response		Tools for remotely resolving security breaches and retrieving information to be used in the forensic analysis of compromised computers. See <a href="#">Response Tools</a> on page 236.
Jupyter Notebooks		They automate retrospective analyses, generate reports, and enable analysts to share hunting techniques. See <a href="#">Investigations with Notebooks</a> on page 204.
	Quick answers	Small reusable code snippets that function independently and resolve specific issues arising frequently in analysts' daily routines. See <a href="#">Response Tools</a> on page 236.
	Templates	Predefined notebooks published by Cytomic or by clients to be shared and used as a base by analysts in the automation of hunting tasks. See <a href="#">Template Management</a> on page 213.

Table 2.1: Cytomic Orion platform processes and technologies

### Intelligence and Data Sources

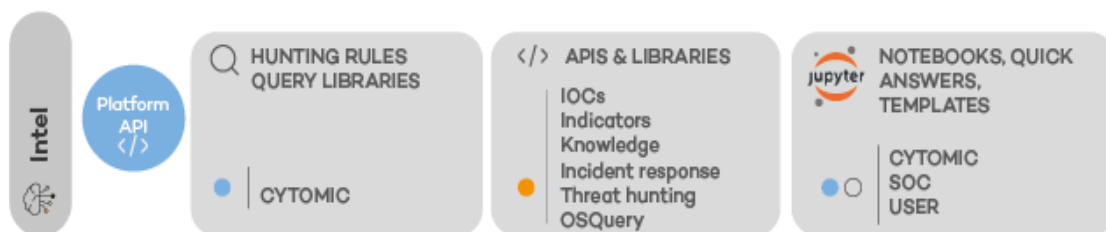


Figure 2.4: Intelligence and data sources

Data source	Description
Query library	Speeds up and facilitates analysts' hunting tasks. It is built and maintained by the Cytomic team of threat hunters and SOC analysts using Cytomic Orion. See <a href="#">Investigate the Event Flow</a> on page 144.

Data source	Description
<b>Threat hunting library</b>	Access the data lake from notebooks and speed up analysis procedures. For more information about this library, go to <a href="https://info.cytomicmodel.com/resources/help/ORION/es/threathuntingAPI/index.htm">https://info.cytomicmodel.com/resources/help/ORION/es/threathuntingAPI/index.htm</a> .
<b>IOC API</b>	Enables the use of external sources of security intelligence to import new indicators of compromise, thereby extending the analysis capabilities of hunting rules. See <a href="#">IOC API</a> on page 308.
<b>Indicator API</b>	Provides integration with ticketing platforms to automate and improve the monitoring of the incidents detected by Cytomic Orion. See <a href="#">Indicator API</a> on page 325.
<b>Knowledge API</b>	Share, with third parties, extended information about the files seen on the client's IT network and the computers that store them. See <a href="#">Knowledge API</a> on page 318.
<b>Incident response API</b>	Allows third-party applications or applications developed by the SOC to isolate, deisolate, and restart computers from the client's network that are at risk of a cyberattack. See <a href="#">Response API</a> on page 328.
<b>OSQuery access API</b>	Gets detailed information about the status of resources and processes executed on a user's computer. See <a href="#">OSQuery Access API</a> on page 331
<b>Notebook templates</b>	The Cytomic team of threat hunters develops and maintains a library of notebook templates that automate the most complex retrospective analyses and are used as a base by SOC analysts for their own developments.
<b>Quick answers</b>	The Cytomic team of threat hunters develops and maintains a library of reusable code snippets for resolving very specific problems. These snippets can be used as a base by SOC analysts to develop more complex notebooks.

Table 2.2: Data sources available in Cytomic Orion

## Data Lake and Process Monitoring

Cytomic Orion relies on the probes installed on workstations and servers to continually monitor the running of all processes loaded into computers' RAM, regardless of whether these have been previously classified as goodware, system processes, non-classified (unknown) processes, malware, or PUPs. Any process classified as goodware which has been compromised (for example, through exploits that use a vulnerability detected in the process) is monitored and its telemetry is sent to the data lake. This way, analysts can

investigate and check the sequence that led to the exploitation of that vulnerability and its effects on the compromised process to organize the response tasks considered necessary.

Likewise, programs classified as suspicious by the heuristic engines of the security solution are also monitored, and their telemetry is sent to an analyst to determine whether their behavior is legitimate or whether they show a sequence of actions that can be interpreted as dangerous and harmful to an organization.

## Cytomic Orion Features

Cytomic Orion incorporates all elements necessary to centralize the threat hunting tools required by analysts in SOCs, whether in-house or part of an MSSP/MDR vendor dedicated to providing security services to clients.



Figure 2.5: Cytomic Orion feature diagram

Cytomic Orion key features:

### Automatic Hypothesis Creation

Indicators are the most frequent point of entry when initiating an investigation. These are warnings generated by the real-time cyberattack radar showing an anomalous execution pattern. Analysts should review them in a process known as 'indicator triage' or 'indicator validation'.

### Indicator Generation Adapted to Each Client

Cytomic analysts carry out transversal inspection of the telemetry data generated by clients' computers. As a result of this investigation, hunting rules are generated which the cyberattack radar uses to detect patterns and sequences of actions that could be part of an attack. To adapt the detection of behavior patterns to the specific circumstance of each client, SOC analysts are also able to develop their own hunting rules that will generate indicators to be investigated.

## Shared Investigation Environment

Cytomic Orion gives analysts a resource to store all the information they generate over time, produced during the investigation processes on one or more specific indicators. This resource is called 'Investigation' in Cytomic Orion, and can be used by and shared among several analysts.

## Flexible Filtering of Monitored Events

To facilitate cross-searching in the data lake created with all the monitored activity of workstations and servers, Cytomic Orion provides an SQL engine with which analysts can create advanced queries and search suspicious activities to support their investigations.

## Query Wizard

Additionally, for analysts not used to working with the SQL language, Cytomic Orion provides a query wizard that enables you to create simple searches quickly and easily.

## In-Depth Computer Activity Investigation

This provides the analyst with a computer investigation console that includes all the necessary tools to view and check each event occurred on workstations and servers. This enables investigations to be better focused. The computer investigation console enables you to view the flow of events in two ways:

- **Process tree:** Shows the parent-child relationship between processes.
- **Timeline:** Shows the event chronology to assess the progression of an attack.

## Detailed Investigation into Computer Status

Access to the OSQuery library provides a highly detailed view of the status of all the computers on the client's IT infrastructure. This information is used by SOC analysts to extend the depth of open investigations as well as to confirm and complete indicators detected by checking monitored events.

## Automation and Sharing of Analyses and Searches

Cytomic Orion supports Jupyter Notebooks, where analysts can encode algorithms in Python language to help in investigations, sharing them among the rest of the team, and automating and accelerating investigation processes and searches.

Additionally, Cytomic Orion enables you to reuse and share the code generated in automations through templates and quick answers.

## Investigation Status Charts

The notebooks available in Cytomic Orion visually show the analysts' findings through widely-used libraries such as `matplotlib` and others. See [Libraries Available in Notebooks](#) on page 223.

Graph-type notebooks provide a graphical representation of the telemetry flow using nodes and relationships to help analysts interpret the operations performed by the software installed on the client's computers. See [Graphs](#) on page 188.

## Dashboard

Statistics display for the SOC manager to confirm, at a glance, the computers with a higher potential risk within the organization as well as the status of analysts' investigations.

## Incident Response Tools

Cytomic Orion provides tools for containing attacks in progress and mitigating their effects. These tools enable the incident response team to isolate compromised computers, monitor and control running processes and services, and send and collect files from computers. They can also be used to run command lines remotely with specialized tools to further investigate cases and apply specific incident resolution procedures.

## Integration with Third-Party Tools

Cytomic Orion incorporates a REST API for integration with the tools most frequently used by SOCs (ticketing tools, security intelligence exchange platforms, etc.). The features accessible to third-party applications are divided into five groups: IOCs, Indicators, OSQuery, Knowledge, and Response. Establish the permissions required from the Cytomic Orion console to restrict access from third-party applications. Additionally, you can establish the scope of the information returned by Cytomic Orion by indicating the clients that will be part of the response to the API calls.

Cytomic Orion implements secure API access: The HTTPS protocol is used to communicate with the third-party application. Also, the authentication/authorization phase must be completed in compliance with the OAuth standard.

## Product User Profile

Cytomic Orion is a product aimed at threat hunters, security professionals working in managed service providers (MSSPs/MDR vendors), and in-house SOCs. These threat hunters and cybersecurity analysts proactively use manual or assisted techniques to detect security incidents designed to bypass protection systems on workstations and servers. Threat hunters try to detect incidents that remain hidden to organizations, providing an additional line of defense against advanced persistent threats (APT).

To detect security incidents, analysts use their critical thinking skills and intuition developed through experience to observe normal execution patterns and identify anomalies in process behavior. A threat hunter must have significant understanding of a business and its daily operations. This way, they will be able to distinguish unusual events that could belong to an attack from normal events to reduce false positives. Additionally, they must have good communication skills to share investigation results. It is especially important for security analysts to be up to date with the latest security trends.

Instead of concentrating on preventing attackers from infiltrating the system from the outside, as is common during penetration tests, security analysts work on the assumption that the enemy has already entered the system. They carefully analyze the entire system and use behavior analysis and a hypothesis-based approach to find unusual conditions that could signal malicious activity.



## Security Analyst Responsibilities

Threat hunters have the goal of detecting advanced IT threats. Their job is to track and neutralize adversaries that cannot be detected through traditional methods. The threats they search for can be launched by insiders, such as an organization employee, as well as by external attackers, such as organized crime groups.

After the potential threats have been identified, security analysts gather as much information as possible about hackers' behavior, targets, and methods. They also sort and analyze collected data to determine trends in the organization security strategy, make predictions about the future, and remove present vulnerabilities.

## Required Skills and Knowledge

- **Experience in IT security:** Threat hunters must have experience in information security, cybersecurity, or network engineering. They must also have hands-on experience in forensic analysis, data analysis, reverse engineering techniques applicable to malware, network security, workstations and servers security, adversary tracking, and other tasks related to IT security.
- **Understanding IT security:** In addition to hands-on experience, threat hunters must also have in-depth knowledge of methods used by present and past malware, attacking methodologies, and TTP (tactics, techniques, and procedures). TTPs evolve rapidly over time, so updated knowledge is crucial for a successful IT threat investigation.
- **Operating system and network protocol knowledge:** Wide knowledge of operating system internal operation and details of different network protocols used by companies (TCP/IP stack, more common application-level protocols, etc.) is essential.
- **Programming skills:** Hunters must know at least one scripting language. Nowadays, for its versatility, the most-widely used scripting language in security environments is Python. You must also know how to analyze and handle records, automate tasks, and perform complex data analysis.
- **Report writing and data graphical representation skills:** Creating security reports and different technical documents is an essential part of cyberthreat hunting, so analysts must also have excellent technical writing and reporting skills.
- **Other skills:** Analytical, research, and problem-solving skills. Security analysts tend to work independently, with minimal administration. However, they must also have interpersonal and collaborative skills, as they usually work with professionals in other IT security fields.

## Supported Operating Systems, Browsers, and Languages

### Compatibility with Probes Installed on Workstations and Servers

To analyze and store the telemetry generated from the monitoring of the processes run on the network, Cytomic Orion requires the installation and execution of one of these security products:

- Cytomic EPDR
- Cytomic EDR

## Compatibility with Operating Systems

Cytomic Orion monitors events caused by running processes on these operating systems:

- **Windows**
  - **Workstations:** Windows XP SP3, Windows Vista, Windows 7, Windows 8, Windows 10, and Windows 11.
  - **Servers:** Windows 2003 SP2, Windows 2008, Windows Server Core 2008, Windows Small Business Server 2011, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, and Windows Server 2022.
  - **Versions with ARM processor:** Windows 10 Home and Pro. Windows 11 Home and Pro.
  - **Exchange servers:** 2003 to 2019.
- **macOS**
  - **Operating systems:** macOS 10.10 Yosemite and higher.
- **Linux**
  - **64-bit operating systems:** Ubuntu 14.04 LTS and higher, Fedora 23 and higher, Debian 8 and higher, Red Hat 6.0 and higher, CentOS 6.0 and higher, Linux Mint 18 and higher, SUSE Linux Enterprise 11.2 and higher, Oracle Linux 6 and higher. It does not require a graphical user interface.
  - **32-bit operating systems:** Red Hat 6.0 to Red Hat 6.10 and CentOS 6.0 to CentOS 6.10.



To check the latest version of the Linux kernel supported by Cytomic Orion, see <https://www.pandasecurity.com/support/card?id=700009>.



For a more detailed list of the Cytomic EPDR and Cytomic EDR requirements, see <https://info.cytomicmodel.com/resources/guides/EDR/latest/en/EDR-guide-EN.pdf> and <https://info.cytomicmodel.com/resources/guides/EPDR/latest/en/EPDR-guide-EN.pdf>.

## Supported Web Browsers

The management console supports the latest versions of these web browsers:

- Chrome
- Microsoft Edge

- Firefox

## Languages Supported in the Web Console

- English
- Spanish

## Response Tool Requirements

To use the remote access and command line tools, the user computer and the perimeter firewall must permit traffic to and from these URLs:

- dir.rc.pandasecurity.com through port 443.
- eu01.rc.pandasecurity.com through ports 8080 and 443.
- eu02.rc.pandasecurity.com through ports 8080 and 443.
- eu03.rc.pandasecurity.com through ports 8080 and 443.
- eu04.rc.pandasecurity.com through ports 8080 and 443.
- eu05.rc.pandasecurity.com through ports 8080 and 443.
- eu06.rc.pandasecurity.com through ports 8080 and 443.
- ams01.rc.pandasecurity.com through ports 8080 and 443.
- ams02.rc.pandasecurity.com through ports 8080 and 443.

## Analysis Console

Cytomic Orion uses the latest technologies to provide an analysis console in the cloud, allowing simple and agile interactions with the security service. Its main features include:

- **Adaptability:** Responsive design that adapts to the screen size of the device used to manage the service.
- **User friendly:** Interface developed with Ajax technology, which avoids reloading entire pages.
- **Flexibility:** Adaptable interface that saves settings for future access.
- **Homogeneity:** Well-defined usability patterns to minimize the learning curve for analysts.

### CHAPTER CONTENTS

---

<b>Benefits of the Analysis Console</b> .....	<b>28</b>
<b>Analysis Console Requirements</b> .....	<b>29</b>
<b>Analysis Console General Structure</b> .....	<b>30</b>
Top Menu (1) .....	30
Left-side Panel (2) .....	34
Right-side Panel (3) .....	35
Central Panel (4) .....	35
<b>Basic Components of the Analysis Console</b> .....	<b>35</b>

## Benefits of the Analysis Console

The web console, also known as 'analysis console' or just 'console', is the analyst's main tool for incident triage and investigation processes. As it is a web service, it delivers features that make the work of the SOC easier.

### Single Tool for the Hunting Process

No matter what tier they belong to, all SOC analysts have all the necessary functionality available for investigation processes without the need for other third-party tools.

The entire functionality is provided from a single web console, which integrates the various tools and minimizes the complexity of using several products from different vendors.

### Centralized Processes for Remote SOCs and Roaming Devices

The web console is hosted in the Cytomic cloud, so VPN settings or corporate router port redirections are not necessary to access it from outside the office. Any analyst can access the service at any time and place and start an incident triage or investigation about any workstation or server, no matter what network they are connected to, or whether they are roaming or at home.

Neither MSSPs/MDR vendors nor companies that subcontract the security services need to invest in IT infrastructure such as servers, OS licenses, or databases; maintenance or hardware warranty management is not necessary to ensure service operation.

### Security Management from Any Device

The web console is responsive and adaptable; this means it adjusts to the screen size of the device used by the analyst. This way, you can manage security from any place and at any time with a laptop or desktop..

## Analysis Console Requirements

To access the web console, use this URL:

<https://orion.cytomicmodel.com>

You must meet these requirements to access the web console:

- You must have valid login credentials (user name and password).




*For more information about how to create a Cytomic account to access the web console, see [Access, Control, and Monitor the Analysis Console on page 44](#).*

- You must use a supported browser. The solution supports the most recent version of these web browsers:
  - Chrome
  - Microsoft Edge
  - Firefox
- You must have an Internet connection and be able to communicate through port 443.

## Federation with IdP

Cytomic Orion delegates credential management to an identity provider (IdP) in a centralized app responsible for managing the web console user identities.

With a single Cytomic account, the network administrator can access all the products contracted with Cytomic simply and securely.



*For more information about the IdP and how to create Cytomic accounts, see [Access, Control, and Monitor the Analysis Console](#) on page 44.*

## Analysis Console General Structure

The web console resources provide a coherent and homogeneous working environment across SOC tiers, not only for indicator triage, but also for completing investigations.

The aim of the console is to give analysts a simple but flexible and powerful tool that enables them to complete investigations productively and as fast as possible.

Below is a description of the console basic features and how to use them.

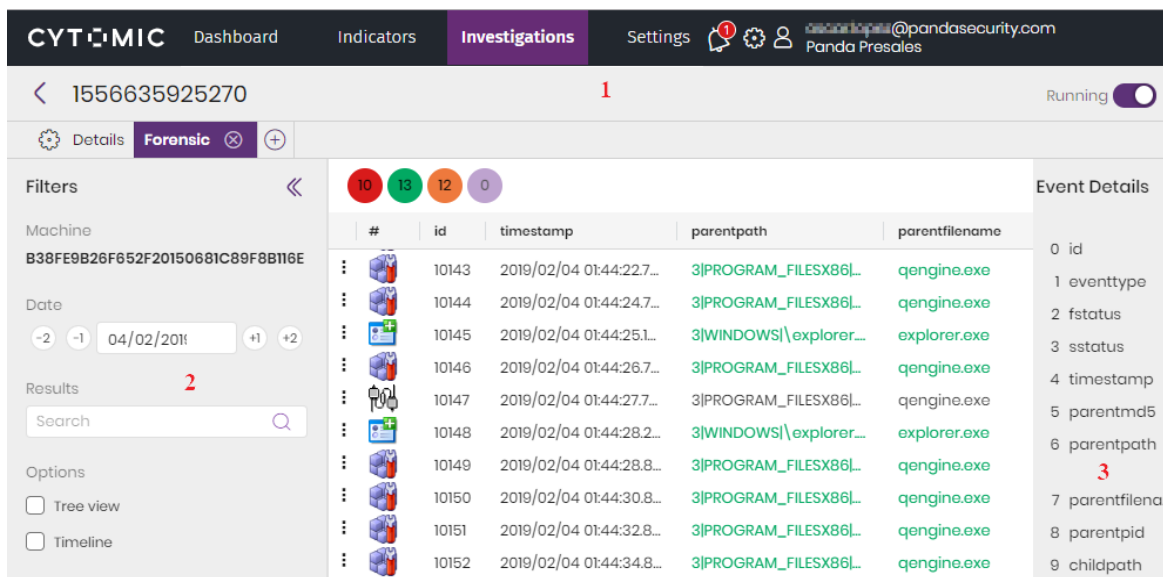


Figure 3.1: Analysis console overview

## Top Menu (1)

The console features are distributed in different areas or zones accessible from the top menu:

- Dashboard
- Indicators

- Investigations
- Settings
- Product management
- User account

## Dashboard Area

The Dashboard area shows the console control panel from which analysts and SOC administrators can see all the information about completed investigations and indicators. The dashboard widgets are interactive: When you click the different areas of a graph, the console changes zones to show the data Cytomic Orion used when generating the graph.



## Indicators Area

The Indicators area shows the list of hypotheses generated by the real-time cyberattack radar for Tier 1 analysts to complete the triage and create the investigations to be carried out by Tier 2 technicians. The indicator module provides all the necessary tools for managing indicators (status change, filter, basic information about the computer that triggered the indicator, etc.).




## Investigations Area

This area contains a list of investigations created, basic tools for managing investigations, and information that describes investigations which Tier 2 analysts use.



## Notifications Area

To access the general notifications that Cytomic provides to all console users, click the  icon.

Notifications are sorted by date and can include information about:

- Scheduled maintenance.
- Critical vulnerability warnings.
- Security advice.

Each notification has a priority level:

-  Important
-  Warning
-  Information

The icon number indicates the number of unread notifications. When you open the notifications panel, all content is considered read and the notifications icon is set back to zero and is no longer visible.

### Archive Notifications

To archive a web notification, click the cross icon . Archived notifications are no longer shown in the drop-down menu.

To access archived notifications, click the **View all notifications** link.

Notifications older than one month are considered expired and are deleted from the notifications area.

### Persistent Notifications

These are important notifications that do not have a cross icon. You cannot archive them manually.

### Always Visible Notifications

Some notifications are considered mandatory and are shown just below the top menu. These notifications are listed if there are more than one, and they take up the entire width of the page. The importance of the notification is indicated by the same color scheme as for normal notifications.

If an analyst closes an always visible notification by clicking the cross icon, it is automatically shown again whenever a user opens the analysis console.

Always visible notifications also appear in the notifications panel. You cannot archive them manually.

## Settings Area

The left panel enables you to set parameters to regulate access to the console and the service as well as to configure the presentation of data:

- **Users:** Manage the user accounts that access the console, along with their permissions and the visibility they have of SOC clients' computers. See [Access, Control, and Monitor the Analysis Console](#) on page 44.
- **Authorized applications:** Establish permissions for accessing the various APIs from third-party applications. See [Cytomic Orion Integration with SOC Tools](#) on page 292.
- **Clients:** Manage and organize the clients the SOC can access into groups. See [Client Visibility Settings](#) on page 51.
- **IOCs:** Shows a list of the indicators of compromise loaded using the Cytomic Orion API. See [IOC API](#) on page 308.
- **Hunting rules:** Manage the rules that analyze the telemetry sent from monitored computers for patterns of events that could belong to the Cyber Kill Chain (CKC) of a cyberattack. See [Manage](#)



### Hunting Rules on page 78

- **Deletion rules:** Manage rules that automatically delete indicators considered not useful for the analyst. See [Delete Indicators Automatically](#) on page 71.
- **Automated investigations:** Create and publish notebooks that SOC analysts can then use to perform investigations. See [Use Notebook Templates](#) on page 212.
- **Quick answers:** Create and publish small, reusable code snippets that SOC analysts can combine to speed up investigations. See [Use Quick Answers with Notebooks](#) on page 215.
- **Graph templates:** Create and publish graphs that SOC analysts can then use to perform investigations. See [Use Notebook Templates](#) on page 212.
- **My preferences:**
  - **Notify me each time an investigation is assigned to me:** Cytomic Orion sends an email message to the console user who has been assigned an investigation. This option is disabled by default.
  - **Email me notifications about new versions, Cytomic communications, etc.**
  - **Email me when the data used in queries approaches the maximum quota.:** See [Assigned Data Dashboard](#) on page 139.
  - **Theme:** Personalize the console appearance.
  - **Default time zone:** Set the time zone for the events shown in the console. Internally, all events monitored and managed in Cytomic Orion are timestamped in UTC+0. Because it is possible for a SOC to investigate computers in other time zones, analysts can set a different default time zone for the whole console. After you select it, the date data shown in the console is set for the chosen time zone, and the date data entered by analysts is translated internally to UTC+0 according to the time zone established. In addition, throughout the console you can select different time zones in each list or date-type text box to work with different time zones simultaneously.
- **Activity log:** Stores the operations performed by the SOC user accounts. See [User Account Activity Log](#) on page 60.

## Product Management Area

This area shows a drop-down menu with these options:

Option	Description
Online help	Access to the product help file.
User guide	Access to the user guide.
License agreement	EULA (End User License Agreement).

Option	Description
Language	Change the language of the console.
About Cytomic Orion	Shows version information.

Table 3.1: Product management menu

## User Account Area


This area shows a drop-down menu with these options:

Option	Description
Set up my profile	Change the information of the account you are using.
Change organization	List of the accounts that can be accessed by the administrator. Select an account to operate the console.
Log out	Logs you out of the console and takes you back to the IdP page.

Table 3.2: User account menu

## Left-side Panel (2)

The left-side panel contains filter tools that help you find information in the central panel. The left panel varies according to the area you select in the top menu.

In cases where the central panel contains lots of information and more space is desired, you can collapse the left panel by clicking the  icon.

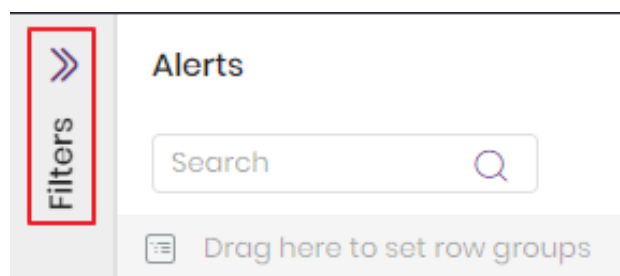





Figure 3.2: Collapsed panel


A collapsed panel looks like the one shown in figure [Collapsed panel](#). To expand it, click .

## Right-side Panel (3)

The right-side panel provides extended information about the items you select in the central panel. Like the left panel, you can collapse and expand the right panel by clicking  and .

## Central Panel (4)

The central panel shows all the relevant information about the area or zone selected by the analyst. In figure [Analysis console overview](#), you can see the computer investigation console. For more information about this resource, see [Indicator Analysis Using the Investigation Console](#) on page 172.

In panels that contain a large number of fields, you can expand the information shown by default by selecting an entry. When you do this, a sliding sub-panel opens that shows full information and an  icon in the upper-right corner to close it.

# Basic Components of the Analysis Console

The web console uses several common resources to enable the interaction between the analyst and the service. Below is a description of the console controls and how to use them.

## Tab Menu

The tab menu is a menu bar that enables you to select the content shown in the central panel and shows the different modules.

Depending on the selected zone, you can configure the tab menu and these settings are then maintained to enable analysts to continue the task where they left off.

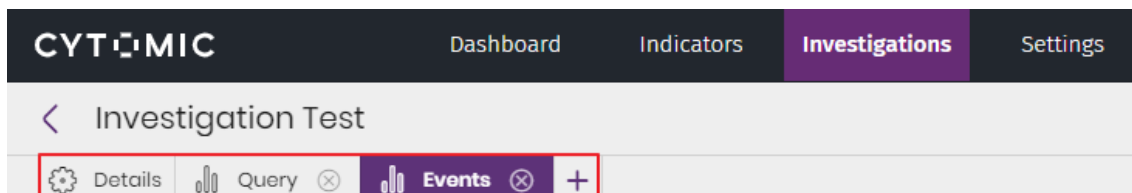




Figure 3.3: Configurable tab menu

- To select one of the available modules, click its name.
- To create a new entry in the tab menu, click the  icon
- To delete an entry from the tab menu, place your cursor over the entry you want to delete. Click the  icon. The module and all its information are deleted

Other tab menus are not configurable and look like the menu shown in figure [Fixed tab menu](#)

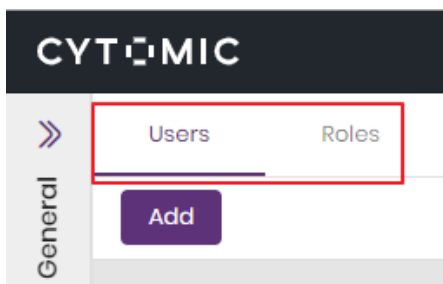


Figure 3.4: Fixed tab menu

## Sub-panels

When the central panel has different types of information, the page divides into sub-panels.

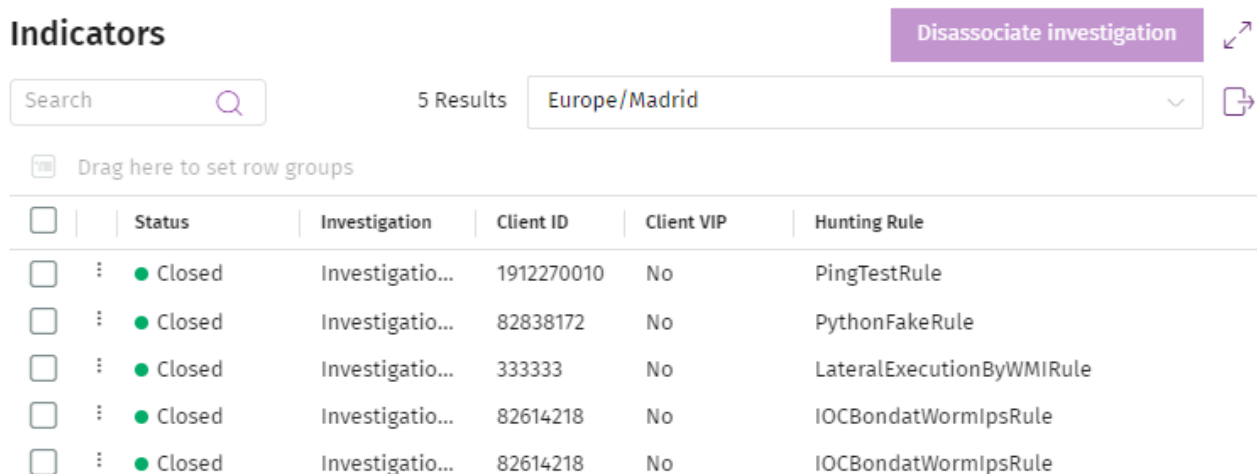





Figure 3.5: Indicators sub-panel in an investigation

You can maximize sub-panels to take up the whole page if there is a large amount of data shown.

- To maximize a sub-panel, click .
- To minimize a sub-panel, click .

Some sub-panels have their own tools for searching and filtering, which affect only data in the sub-panel. See [Search Tools](#).

## Tools for Configuring Lists

Lists in Cytomic Orion are totally configurable to make reading the presented data easier for analysts. The tools available for configuring lists are described below. You can access the majority of the configuration tools through the context menu  that appears when you place your cursor over the column header.

### Select All the Items in a List

Select the  checkbox in the header of the list to select the visible and non-visible items.

The checkboxes allow several status types:

Icon	Description
<input type="checkbox"/>	Unselected item
<input checked="" type="checkbox"/>	Selected item
<input checked="" type="checkbox"/>	All the items in the list or group are selected.
<input type="checkbox"/>	Some (not all) the items in the list or group are selected.

Table 3.3: Checkbox status

### Sort Columns


To change the order of a column in a list, click the name of the column and drag and drop it to its new position.

### Add or Remove Columns

To show or hide columns in a list, follow these steps::




- Click the context menu icon ☰ for a column. A drop-down menu with several tabs appears.
- Select the **||||** tab. Select the columns you want to show in the list.
- To quickly find a column within the drop-down menu, use the **Filter** text box. The list of available columns updates automatically.
- After you have selected the columns, click anywhere on the page. The list updates automatically with the new column settings.

### Group Entries by Columns

At the top of the list, the group bar is shown  (1). This is a recipient control where analysts can drag the columns that make up the grouping criteria.

#### Indicators

Search

 **MUID**  > **Hunting Rule**  **1**

Group **2**  Investigation Indicator date ▾

DD12FCBF-4801-4696-A4D7-B8B536C80F59 (5)




FileHashloc Found in Event Stream (4)

**4**  2020/23/03 08:23:...




2020/23/03 08:22:...

Figure 3.6: List grouped by the MUID and Hunting rule columns

To group the list results by one column, drag the column name to the grouping control **(1)**, or follow these steps:

- Click the context menu icon  for a column. A drop-down menu with several tabs appears.
- Select the  tab. Select the **Group by (name of the column)** option. 

After you have created the new group, the list updates with these changes:

- A column is created on the left side of the list with the “**group**” name. This column show the content of the groups **(2)**.
- The columns selected as grouping criteria appear on the group bar in the order in which they were added **(3)**.
- The icons  and  are added to expand or collapse a group of results.
- To delete a group, click the  icon of the group you want to delete from the group bar.
- If the grouping criteria is made up of more than one column, the order selected is respected: The list is grouped by the column chosen first and, within each group of resulting rows, it is grouped again by the second column, and so on.
- To change the order in which a group appears, click its name and drag it to the left or right in the group bar.
- To change the order of the groups in accordance with the number of items they contain, click the name of the **Group** column.

### Select All the Items in a Group







To select all the items that belong to a group, select the checkbox **(4)** associated with the group.




*You cannot select multiple groups of the same level at the same time. When you select a group, the console cancels the rest of the selections.*

### Pin Columns

In lists where there is a large number of columns, you must use the horizontal scrolling bar in to see the columns that do not fit on the page. To pin a column, select the **Pin column** option.



- Click the context menu icon  for a column. A drop-down menu with several tabs appears.
- From the context menu, select the  tab.
- Select **Pin column** . Choose where to place the column: to the left  or to the right. 
- To restore a previously pinned column, select the **No pin**  option.

## Resize Columns

To change a column width, click the separating icon  between the names of the columns. Drag it to the right or to the left



## Resize Columns according to Their Content

To adapt a column width to its content, follow these steps:

- Click the context menu icon  for a column. A drop-down menu with several tabs appears.
- Select the  tab. Select the **Autosize this column** option.
- To adjust the width of all columns, select **Autosize all columns**.

## Filter Information at Column Level



To filter the list rows according to the content of a specific cell, follow these steps:

- Click the context menu icon  for a column. A drop-down menu with several tabs appears.
- Select the  tab. Select a filter criteria.

Depending on the type of data stored in the column, different filter criteria are available:

- **For date-type columns:** Enter two dates to show the range of entries within the set interval, or enter a single date to show the entries that correspond to that date.
- **For text-type columns:** Enter the text that will serve as the filter and the filter logic: **Equals - Not equal** for exact matches, **Contains - Does not contain** for partial matches at any point of the character string, and **Starts with - Ends with** for matches at the beginning or at the end of the character string.
- **For number-type columns:** Select the enumeration items that will serve as the filter.

## Restore Column Settings

- Click the context menu icon  for a column. A drop-down menu with several tabs appears.
- Select the  tab. Select the **Reset columns** option.

## Show and Hide Columns and Filters

Lists incorporate a sidebar with two shortcuts that enable you to:

- Quickly show and hide columns and filters in the list.
- Quickly sort columns in the list.
- Show columns in the event that they were all previously hidden by mistake.


Search  23 Results Europe/Madrid ↻ 🔍 ℹ️

📄 Drag here to set row groups

<input type="checkbox"/>	Indicator date ▾	Computer	Risk	MUID	
<input type="checkbox"/>	2022/17/08 00:01:31.000	UA-61-W10X86-20	Unknown	44416C18-5BD3-435...	Columns Filters
<input type="checkbox"/>	2022/17/08 00:08:31.000	QAW10X64ESP	Unknown	3721B191-5D75-47ED...	
<input type="checkbox"/>	2022/17/08 00:23:43.000	MEMW2012X64	Unknown	7B15A67C-C805-47E...	
<input type="checkbox"/>	2022/17/08 01:23:44.000	MEMW2012X64	Unknown	7B15A67C-C805-47E...	
<input type="checkbox"/>	2022/17/08 01:55:05.000	ADFS1	Unknown	76BBA76E-DEB6-471...	
<input type="checkbox"/>	2022/17/08 02:23:49.000	MEMW2012X64	Unknown	7B15A67C-C805-47E...	
<input type="checkbox"/>	2022/17/08 02:55:22.000	ADFS1	Unknown	76BBA76E-DEB6-471...	

Figure 3.7: Bar with shortcuts to columns and filters in a list

## Search Tools

Search tools show the most relevant data for analysts. To perform a global search on a list, enter the text strings you want to search for in the text box. Click the  icon.

Unlike **Tools for Configuring Lists**, where filters were applied to certain columns, this section describes the search tools that apply to all the columns in the corresponding list.

These features are common to the search tools:

- Partial searches are permitted, with the beginning, middle, or end of a text string.
- The search covers all the columns in the list.
- The search applies to the list in the corresponding panel or sub-panel. Figure **Search controls associated with a panel list** shows three search controls (1, 2, and 3) associated with their respective panels (1, 2, and 3).

**Indicators** 0 Results Europe/Madrid 1  ✕ 🔍 ℹ️ ↗️

📄 Drag here to set row groups

<input type="checkbox"/>	Status	Investigation	Indicator date	Last event	MUID
<input type="checkbox"/>	In Progress	De Fernando	2019/13/05 15:45:37	<span>1</span>	FCC165B5-76B7-0330-642D-67A1BAD95012
<input type="checkbox"/>	In Progress	De Fernando	2019/13/05 15:45:34		40D23992-E156-5085-4EA7-9A54249970CF

**Entities of interest** + 🔍 📄 ↗️ 2

<input type="checkbox"/>	573BA93E-8343-1AC8-0E0D-9CAB063568D9 (BIOOSALICIO)	<span>⋮</span>	
<input type="checkbox"/>	7326B611-BE10-C0D6-0B56-6B33005E1F38	<span>2</span>	<span>⋮</span>

**Files** + 🔍 📄 ↗️ 3

Name	Created
New Document 1645	<span>3</span> Jun 1

Figure 3.8: Search controls associated with a panel list



## Filter Tools

These are controls that enable you to select values that are applied as a filter to a list. They appear in the left panel in some console areas. The filters displayed depend on the console area and its lists.

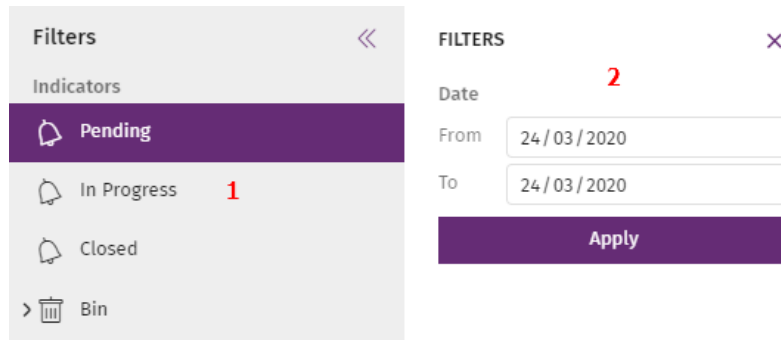



Figure 3.9: Filter controls

Frequent filter tools are:

- **Status filters (1):** They filter entries by a certain status.
- **Date filters (2):** They filter entries by a time range.

## Context Menus

These shows groups of options to aid the work of analysts. Some context menus are represented by the  icon, but others are shown only when you right-click a console item. For example, when you right-click an indicator from the list in an investigation, you have the option to open the investigation console with the computer identifier and the date of the indicator.

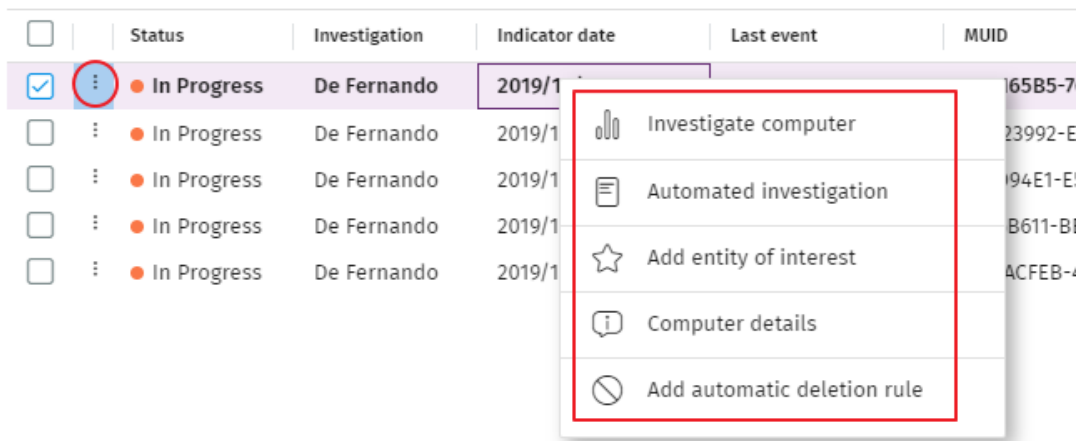



Figure 3.10: Investigations area context menu and icon

## Tool for Converting a Computer Name to an MUID

Cytomic Orion uniquely identifies clients' computers by using a character string comprising groups of letters and numbers separated by a hyphen. This makes it possible to reference computers unambiguously, bearing in mind that a specific computer name can be used by multiple clients managed by the same SOC. To simplify management of devices and avoid memorizing MUIDs, Cytomic Orion provides a conversion tool

that translates a computer name (easier to remember for analysts) to its corresponding MUID. This tool is invoked through the  icon in text boxes where you must enter an MUID. The tool works as follows:

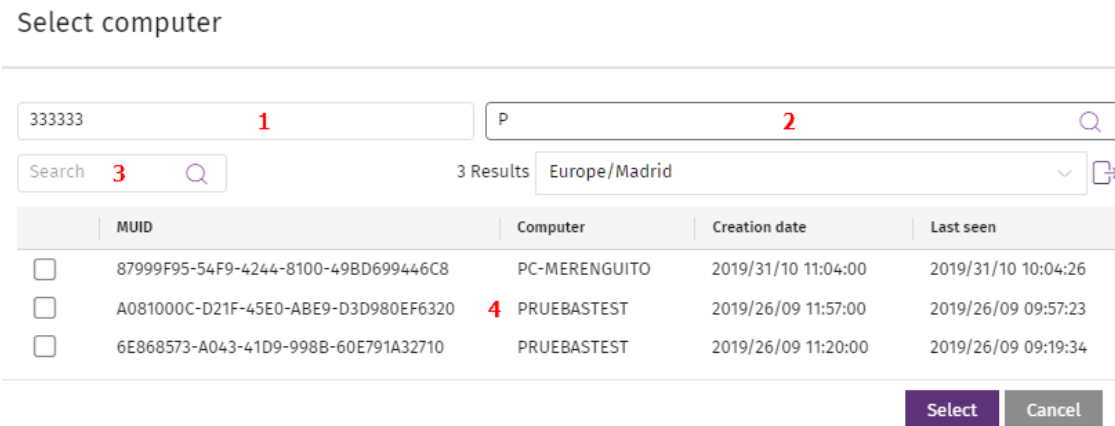



Figure 3.11: Tool for converting computer names to MUIDs




- In the **Client** text box (1), enter the SOC client to which the computer belongs.
- Enter a character from the computer name in the **Search computer** (2) text box. The text box (4) automatically shows the names of the computers with those characters.
- To filter the results, use the search text box (3).
- Select the computer and click **Select**. The MUID of the computer is copied to the text box from which you invoked the name conversion tool.

### Multi-value Text Boxes

Some text boxes enable analysts to enter lists of values they can enter manually or by pasting them from the clipboard:

- **From the clipboard:** Press `control + v` to paste the contents of the clipboard. Separate the values in the list by the character “,” so that the console can interpret them as independent items.
- **With the  icon associated with the text box:** Click this icon. A dialog box opens where you can select the items you want to include.

### Other Controls

Icon	Description
	Adds an item.
	Deletes an item.
	Changes the status (enabled or disabled) of an item.



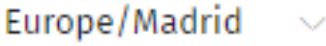
Icon	Description
	Refreshes the content of the associated panel.
	Exports the results shown in the associated panel to CSV format.
	<p>Specifies the time zone associated with the selected country and city.</p> <p>In a list of items, it adjusts dates based on the selected time zone. In text boxes, it enables you to set a time zone for searches.</p>

Table 3.4: Other controls used in the analysis console

# Chapter 4

## Access, Control, and Monitor the Analysis Console

Cytomic EDR implements multiple resources for limiting, controlling, and monitoring access to its web console and the actions that analysts can take through it:

- User account.
- Roles assigned to user accounts.
- User account activity log.

### CHAPTER CONTENTS

---

<b>General Concepts</b> .....	<b>45</b>
<b>Manage User Accounts</b> .....	<b>45</b>
Create the First User Account .....	46
Create Subsequent User Accounts .....	47
Edit the Personal Details for a User Account .....	48
Edit the Email Address or Password for a User Account .....	48
Delete User Accounts .....	49
Enable Two-factor Authentication .....	50
<b>Client Visibility Settings</b> .....	<b>51</b>
<b>Manage Roles and Permissions</b> .....	<b>53</b>
Basic Concepts .....	53
Create and Configure Roles .....	54
Understanding Permissions .....	56
<b>User Account Activity Log</b> .....	<b>60</b>

# General Concepts

## User Account

A user account is a resource consisting of a set of data that Cytomic Orion uses to allow analysts to access the web console and set the actions they can take on user computers.

User accounts are used only by the SOC analysts who access the Cytomic Orion web console. Each analyst can have one or more user accounts assigned.

The main characteristics of user accounts are:

- They are accounts managed by analysts. Analysts can create or delete accounts, change their passwords, add or remove permissions, or enable two-factor authentication.
- A user account provides access to all products purchased from Cytomic through Cytomic Central.
- A user account can provide access to multiple clients. The analyst can choose the product they want to access in Cytomic Central, and then select the console they want to access on the **Select account** page.

## Cytomic Central

This is a portal that centralizes access to all the products included in the Cytomic portfolio. A user account created in a Cytomic product provides access to the portal, from which the analyst can access the various consoles of the purchased products.



For more information, see <http://nexus-documents.cytomic.ai/AdvancedGuide/NEXUS-Manual-EN.pdf>

## SOC/MSSP Client Account

This is a resource consisting of confidential data associated with the SOC/MSSP that has purchased a Cytomic product. The fiscal address, full name, tax identification number, and other data are part of the SOC/MSSP account.

# Manage User Accounts

A user account consists of multiple pieces of information that are generated when you create the account:

- **Account login email address:** Identifies the user who accesses the console.
- **Account password:** Allows or prevents access to the analysis console.
- **Assigned role:** Determines which computers the account user can manage and the actions they can take.
- **Client:** Determines the analyst visibility of the workstations and servers managed by the MSSP/SOC.

## Create the First User Account

The procedure to create the first user account is different from the steps to create subsequent accounts. The first user account always has the Full Control role assigned. This role enables the analyst to perform any action through the console. You cannot delete or modify this account.

### Receive the Welcome Email

- After you purchase Cytomic Orion, you receive an email message from Cytomic.
- Click the **Click here** link in the message to access the website from which you can create the first user account.

### Complete the Create Your Cytomic Account Form

- Enter your email address and click **Create**. You will receive a new email message at the email address you specified in the form to activate the account you created.

### Activate the User Account

- Click the activation button in the message you received to verify the email address you provided when you created the user account. If the button does not work, copy and paste the link included in the message into your browser. The **Cytomic Account** page opens.
- Enter the password for the account. The password length must be at least 8 characters. The password must contain at least one number and at least one letter.
- Choose the country. Click **Activate account**. The **One second and you are done** page opens.
- Enter your first and last name, date of birth, phone number, and address. Click **Save**. You can skip this step by clicking **Not now**. The Cytomic Central end-user license agreement opens.
- Click **Accept and continue**. The Cytomic Central page opens, from which you can access all services purchased from Cytomic.

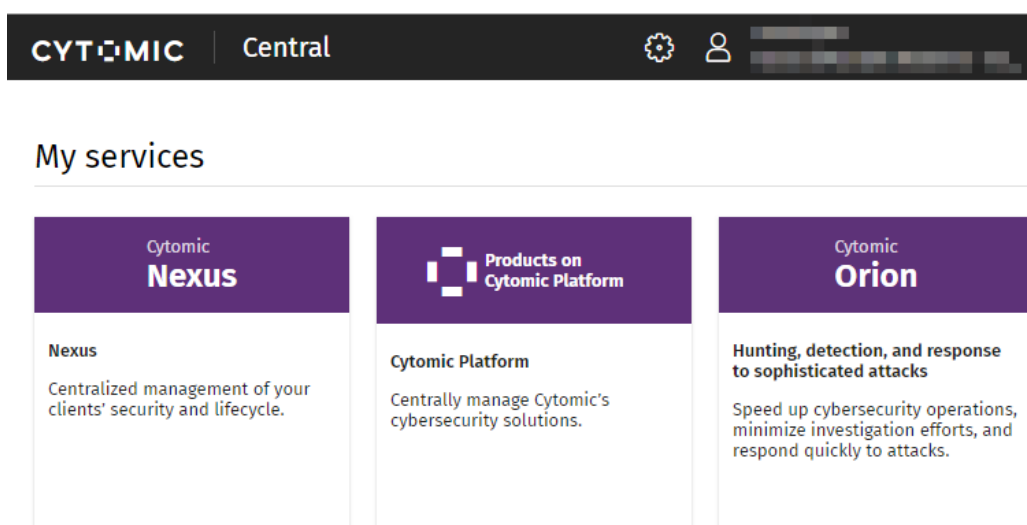


Figure 4.1: Cytomic Central page


- To access the Cytomic Orion console, click the Cytomic Orion tile in **My services**. The first time you access the console, a wizard opens that prompts you to accept the license and data processing agreements.
  - On the **License agreement** page, click the **Accept and continue** button.
  - On the **Data processing agreement** page, click **Go to data processing agreement**.
  - On the **Data processing agreement** page, click **Accept**. The Cytomic Orion console opens.

## Create Subsequent User Accounts

	Email	Role	Client Groups
<input type="checkbox"/>	asthe@pandasecurity.com	Administrators	SRFPRe
<input type="checkbox"/>	asthe@pandasecurity.com	Administrators	SRFPRe
<input type="checkbox"/>	angela.elrosa@watchguard.com	Administrators	All Clients
<input type="checkbox"/>	david.perez@pandasecurity.com	Administrators	SRFPRe
<input type="checkbox"/>	jordan@panda.concepts.com	Control Total	All Clients
<input type="checkbox"/>	kenneth@panda.com	Administrators	SRFPRe
<input type="checkbox"/>	proble@panda.com	Administrators	dfhh
<input type="checkbox"/>	raul.deltav@watchguard.com	Administrators	All Clients
<input type="checkbox"/>	thomas@webconsole@panda.com	Administrators	All Clients
<input type="checkbox"/>	thomas@webconsole2@panda.com	Control Total	All Clients
<input type="checkbox"/>	thomas@webconsole3@panda.com	Administrators	All Clients

Figure 4.2: User list

After you create the first user account, you can access the Cytomic Orion console, from which you can create all other user accounts you might need.

- Make sure you have the **Manage users, permissions, and clients** permission assigned. See [Understanding Permissions](#).
- From the top menu, select **Settings**. From the side menu, select **Users**.
- Select the **Users** tab. A page opens that shows a list of all users created in the management console.
- Click **Add user (1)**. The **Add user** page opens.
- In the **Email** field, enter the console user email address. Enter a description if needed.
- Choose a role for the user account. See [Understanding Permissions](#).
- To specify the clients that are visible to the user account:
  - Under **Clients the user has permission on**, click the  icon. The **Choose client groups** dialog box opens.

- Select the checkboxes next to the client groups the analyst will have access to.
- Click **OK**.




For more information about visibility for a user account, see [Client Visibility Settings](#).

- Click **Save**. Cytomic Orion sends an email to the specified email address so that the user can create an access password and accept the terms of the license and data processing agreements.



For MSSPs/SOCs with multiple Cytomic products, if the email account already exists in the Cytomic systems, the activation email is not sent. The account can access Cytomic Orion with the credentials used for other products.


## Edit the Personal Details for a User Account

- In the management console, click the  icon in the upper-right corner of the page. A drop-down menu appears.
- Select **Set up my profile**.

### Cytomic Central

- The **Cytomic Account** page opens.
- In the left menu, select **Profile**. Fill the form with the personal details for the account.
- Click **Save**. The changes are stored on the Cytomic server.

## Edit the Email Address or Password for a User Account

- In the management console, click the  icon in the upper-right corner of the page. A drop-down menu appears.
- Select **Set up my profile**.

### Cytomic Central

- The **Cytomic Account** page opens.
- In the left menu, select **Login**. Click the **Change email address** or **Change password** links. A page opens that prompts you to validate the old data and enter the new one.
- Click **Change**.




## Access the Users List

- From the top menu, select **Settings**. From the side menu, select **Users**.
- Select the **Users** tab. A list appears that shows all user accounts created in Cytomic Orion, along with this information:

Field	Description
<b>Email</b>	The email address associated with the user.
<b>Role</b>	Set of permissions associated with the user account.
<b>Client groups</b>	Client groups to which the account has visibility.

Table 4.1: Fields in the Users list


## Delete User Accounts

- Make sure you have the **Manage users, permissions, and clients** permission assigned. See [Understanding Permissions](#).
- From the top menu, select **Settings**. From the side menu, select **Users**.
- Select the **Users** tab. A page opens that shows a list of all users created in the analysis console.
- Select the checkboxes **(3)** next to the users you want to delete.
- In the toolbar, click the  icon. A confirmation dialog box opens.
- Click **OK**. Deleted users cannot access the web console or the threat hunting library, nor do they receive email notifications. However, investigations, notebooks, and audit information generated by deleted users remain on the system. You can continue using deleted users in investigation search filters provided they have created an investigation or have investigations assigned.

## Reactivate Users

You can register a deleted user again by following the normal process for creating a new user. In that case, all the information previously generated by the user is reassigned to the account.

## Export the Users List

To download the Users list as an Excel file, click the  icon **(4)** in the upper-right corner of the page.

## Search for Users

Type a search term in the text box **(5)** to search in any of the list fields. You can type only a partial string.


## Enable Two-factor Authentication

Cytomic Orion supports the two-factor authentication (2FA) standard to add an additional layer of security beyond that provided by the 'user-password' basic pair. This way, when you try to access the web console, you are prompted to enter an additional authentication item: a code that only the account owner has. This is a random code that is generated on a specific device, typically the Cytomic Orion administrator personal smartphone or tablet.

### Requirements for Enabling 2FA

- Access to a personal smartphone or tablet with a built-in camera.
- Download the WatchGuard AuthPoint free app (or similar) from:
  - **iOS:** <https://apps.apple.com/app/watchguard-authpoint/id1335115425>
  - **Android:** <https://play.google.com/store/apps/details?id=com.watchguard.authpoint>

### Enable 2FA

- In the analysis console, click the  icon in the upper-right corner of the page. A drop-down menu appears.
- Select **Set up my profile**.

### Cytomic Central

- The **Cytomic Account** page opens.
- From the side menu, select **Login**. In section **Two-step verification**, click the **Enable** link. The **Synchronization using an authentication app** dialog box opens.
- The first time that you use the WatchGuard AuthPoint app on your mobile device, tap **Activate**. If you have used it before, tap the QR code icon in the upper-right corner of the page. The mobile device camera opens.



Figure 4.3: Scan the QR code with WatchGuard AuthPoint

- Point the camera at the QR code in the Cytomic Orion console. A new entry is added to WatchGuard AuthPoint and a token is generated every 30 seconds.
- Enter the code generated by WatchGuard AuthPoint in the Cytomic Orion console to link the device to the user account. Click **Verify**. A dialog box opens that shows the message **Two-factor authentication is enabled**.
- Click **OK**.

## Access the Web Console from Cytomic Central Using an Account with 2FA Enabled

- Go to <https://central.cytomic.ai/Login>. Enter your user name and password. Click **Log in**.
- Enter the verification code generated by WatchGuard AuthPoint on your mobile device. Click **Verify**. The **Cytomic Central** page opens.

### Force all Console Users to Use 2FA

The user account with which you enforce the use of 2FA must have the **Manage users, permissions, and clients** permission assigned and full visibility into the IT network. See [Understanding Permissions](#).

- From the top menu, select **Settings**. From the side menu, select **Users**. Select the **Security** tab.
- Select the option **Require users to have two-factor authentication enabled to access this account**.
- If the user account with which you force all console users to use 2FA does not have two-factor authentication enabled, a warning message is shown prompting you to access your **Cytomic Account** and enable the feature. See [Enable 2FA](#).

## Client Visibility Settings

To share the workload by priority or volume within the SOC, you can restrict access to certain clients from user accounts, thereby segmenting and assigning investigations to certain groups of threat hunters. An analyst without access to a client cannot perform any analysis tasks for that client.

### Access to the Client Visibility Settings

In the top menu, select **Settings**. In the left panel, select **Clients**.

### Create a New Group and Assign Clients

You configure the visibility settings by client groups. The SOC administrator must create as many client groups as access combinations are necessary for analysts. If a team of analysts needs to access clients 1, 2, and 4, and another team needs to access clients 2, 3, and 4, you must create two different access groups and assign the corresponding groups to each analyst's user account.




*A user account can have multiple client groups assigned. The accessible clients will be all clients belonging to groups assigned to the user account.*

#### To view groups and their assigned clients:

- In the top menu, select **Settings**. In the left panel, select **Clients**.
- The **Groups** panel shows a list of all created groups and the number of clients in them.

- The **All clients** special group is also shown. This group is used for managing groups as specified further on in this section.
- To see the clients that belong to a group, click the group name. The client panel shows the names of the clients in the group, the unique identifier for each client, and the groups each client belongs to.

#### To create a new group and assign clients:

- At the top of the page, click the  icon in the **Groups** panel.
- Enter a name for the group. click **OK**.

#### To delete a group:

- Point the mouse to the name of the group you want to delete. A context menu opens.
- Select **Delete group**.




*If the group has already been assigned to a user account, the system shows an error message.*

#### To rename a group:

- Point the mouse to the group you want to rename. In the context menu, select **Rename**. A dialog box opens for you to enter the new name.
- Enter the new name for the group. Click **OK**.

#### To assign new clients to an existing group:


- In the **Groups** panel, select the **All clients** special group.
- Click the  icon to open the **Search** text box and find clients quickly.
- Select the checkboxes next to the clients that you want to add to the group. In the toolbar, click **Assign to group**. The selected clients are added to the group.

#### To delete clients from a group:


- In the **Groups** panel, select the group whose clients you want to delete. Select the clients.
- In the toolbar, click **Remove from group**. A confirmation dialog box opens. Click **OK**. From that moment on, the user accounts with this group assigned cannot access the deleted client, except if the client belongs to another group also assigned to the user account.

#### To assign a client group to a user account:

- In the top menu, select **Settings**. In the left panel, select **Users**. Select the **Users** tab. A list opens that shows all users created in Cytomic Orion.

- Select a user. In the **Clients the user has permission on** section, click the  icon. A dialog box opens that shows all created groups.
- Select the checkboxes next to the groups the user account will have access to. Click **OK**. From that moment on, the user account has access to the data Cytomic Orion stores about the clients in the selected groups.

#### To assign all clients managed by the SOC to a user account:

- In the top menu, select **Settings**. In the left panel, select **Users**. Select the **Users** tab. A list opens that shows all users created in Cytomic Orion.
- Select a user. In the **Clients the user has permission on** section, click the  icon. A dialog box opens that shows all created groups.
- Choose the **All clients** special group, which contains all clients managed by the SOC. From that moment on, the user account has access to the data Cytomic Orion stores about all the clients managed by the SOC.

## Manage Roles and Permissions

### Basic Concepts

#### Roles

A role is a specific configuration of permissions that you apply to one or more user accounts. A user account is authorized to view or modify certain resources in the console depending on the role you assign to it.

A user account can have only one role assigned. However, you can assign a role to more than one user account.

A role consists of these elements:

- **Role name:** This is purely for identification. You assign the role name when you create the role.
- **Visibility:** Restricts access to certain computers on the network.
- **Permission set:** Determines the specific actions that the user account can take on computers belonging to groups defined as accessible.

#### Why are Roles Necessary?

In a small SOC, all technicians typically access the console with the Full Control role without any restriction. However, in mid-sized or large MSSPs/MDR vendors with large networks and a multitude of clients to manage, it is highly likely that it is necessary to organize or segment access to computers, under two criteria:

##### The Number of Computers to Manage

MSSPs/MDR vendors with a large computer infrastructure to scan might need to sort it by client and assign computers to analysts to share the workload and improve response time. In that case, each analyst

researches only the computers belonging to a specific group of clients.

Another option is taking client priority into account, grouping them by importance and assigning them to teams of different sizes or skill sets.

### The Knowledge or Expertise of the Technician

MSSPs/MDR vendors are usually divided into three tiers, which facilitates the analysis workload distribution to prevent bottlenecks. Depending on each analyst skills, they belong to one tier or another, and have access to certain console resources and not others, according to their tasks and responsibilities.

These two criteria can overlap, giving rise to a combination of settings profiles that are highly flexible and easy to set up and maintain. This also makes it easy to define the functions of the console for each analyst, depending on the user account with which they access the system.

## Full Control Role

All Cytomic Orion licenses come with the **Full Control** role assigned. The default account also has this role assigned. This account enables you to take every action available in the console.

You cannot edit or delete the **Full Control** role. You can assign this role to any user account through the analysis console.

## Permission

A permission controls access to a specific section of the management console. There are different types of permissions that provide access to many features included in the Cytomic Orion console. A specific configuration of all available permissions makes up a role, which you can assign to one or more user accounts.

## Visibility

Each user account enables you to configure the security of a subset of computers from all the computers added to the Cytomic Orion console. This is determined by the account visibility.

## Create and Configure Roles

In the top menu, select **Settings**. In the left panel, select **Users**. Select the **Roles** tab to perform all necessary actions to create and edit a role:

### Create a Role

- In the top menu, select **Settings**. In the left panel, select **Users**. Select the **Roles** tab. A page opens that shows a list of all created roles.
- Click **Add**. The **Add role** page opens.
- In the **Name** text box, type a name for the role. In the **Description** text box, type a description of the role (optional).


- Enable or disable the relevant permissions.
- Click **Add**.

### Limitations When you Create Users and Roles


To prevent privilege escalation problems, users with the **Manage users , permissions , and clients** permission assigned have these limitations when it comes to creating new roles or assigning roles to existing users:

- A user account can create only new roles with the same or lower permissions than its own.
- A user account can edit only the same permissions as its own in existing roles. All other permissions remain disabled.
- A user account can assign only roles with the same or lower permissions than its own.
- A user account can copy only roles with the same or lower permissions than its own.

### Delete a Role

- In the top menu, select **Settings**. In the left panel, select **Users**.
- Select the **Roles** tab. A list appears that shows all created roles.
- Click the  icon of a role to delete it. If the role you are trying to delete has user accounts assigned, the delete operation is canceled.

### Copy a Role

- In the top menu, select **Settings**. In the left panel, select **Users**.
- Select the **Roles** tab. A list appears that shows all created roles.
- Click the  icon of a role to copy it. The **Copy role** page opens. This page shows the settings of the copied role.
- Edit the role settings. Click **Save**.

### Edit a Role

- In the top menu, select **Settings**. In the left panel, select **Users**.
- Select the **Roles** tab. A list appears that shows all created roles.
- Click the role you want to edit. The **Edit role** page opens.
- Edit the role settings. Click **Save**.

## Understanding Permissions

### Access to advanced queries

- **Enabled:** The account user has access to the **Investigations** area and can select the **Advanced SQL query** tab to create SQL statements and search the data lake collected by Cytomic Orion for suspicious operations.
- **Disabled:** The account user has access to the **Investigations** area but cannot select the **Advanced SQL query** tab

### Access to OSQuery

- **Enabled:** The account user has access to the **Investigations** area and can select the **OSQuery query** tab to create a notebook used in the analysis of the SOC clients' IT infrastructure.
- **Disabled:** The account user has access to the **Investigations** area but cannot select the **OSQuery query** tab.

### Access to the query wizard

- **Enabled:** The account user has access to the **Investigations** area and can select the **Wizard-guided queries** tab to create simple searches to explore the data lake collected by Cytomic Orion for suspicious operations.
- **Disabled:** The account user has access to the **Investigations** area but cannot select the **Wizard-guided queries** tab.

### Isolate/deisolate computers

- **Enabled:** The account user can restrict communications from SOC clients' computers to isolate them if they are compromised or to contain the effects of an attack.
- **Disabled:** The account user cannot restrict communications from SOC clients' computers to isolate them if they are compromised or to contain the effects of an attack.

### Delete IOCs for all clients

- **Enabled:** The account user can execute calls to the Cytomic Orion API to delete IOCs previously loaded on the platform.
- **Disabled:** The account user cannot execute calls to the Cytomic Orion API to delete IOCs previously loaded on the platform.



## Search for IOCs

- **Enabled:** The account user can execute calls to the Cytomic Orion API to search clients' computers for IOCs previously loaded on the platform.
- **Disabled:** The account user cannot execute calls to the Cytomic Orion API to search clients' computers for IOCs previously loaded on the platform.

## Create hunting rules and notification rules for all clients

- **Enabled:** The account user can create hunting rules and notification rules that affect all clients regardless of the client visibility settings associated with the account.
- **Disabled:** The account user cannot create hunting rules or notification rules that affect all clients.

## Create notebooks for manual investigation

- **Enabled:** The account user can create, edit, and delete notebooks to automate investigations.
- **Disabled:** The account user cannot create, edit or delete notebooks.

## Create notebooks from automated investigation templates

- **Enabled:** The account user has access to the **Automated investigation** option in the tab bar of an investigation to create a notebook using a template previously created in Cytomic Orion.
- **Disabled:** The account user does not have access to the **Automated investigation** option and cannot create notebooks using templates.

## Create quick answers

- **Enabled:** The account user can create and delete small code snippets (quick answers) to speed up investigations.
- **Disabled:** The account user cannot create or delete small code snippets (quick answers) to speed up investigations.

## Create indicator notification rules

- **Enabled:** The account user can create, edit, and delete notification rules for indicators generated by hunting rules for all clients the account user has visibility to.
- **Disabled:** The account user cannot create, edit, or delete notification rules for indicators generated by hunting rules.

## Delete indicators and manage automatic indicator deletion rules

- **Enabled:** The account user can delete indicators and create, edit, and delete rules for deleting indicators.
- **Disabled:** The account user cannot delete indicators nor create, edit, or delete rules for deleting indicators, although they can see the existing rules and the indicators deleted by each rule.

## Manage investigation notebook templates

- **Enabled:** The account user can access the **Automated investigations** side panel in the **Settings** section to create, edit, publish, and delete notebook templates.
- **Disabled:** The account user cannot access the **Automated investigations** side panel in the **Settings** section.

## Managing hunting rules

- **Enabled:** The account user can create, delete, edit, enable, and disable hunting rules.
- **Disabled:** The account user cannot create, edit, delete, enable, or disable hunting rules although they can see the existing rules and their definitions if they were created by a SOC account.

## Manage automatic indicator assignment rules

- **Enabled:** The account user can create, delete, edit, and see new rules to automatically assign indicators to investigations.
- **Disabled:** The account user cannot access the **Assignment rules** side panel in the **Settings** section.

## Manage users, permissions, and clients

- **Enabled:** The account user can create new users and roles, assign permissions based on the analyst profile and the service level assigned to them within the SOC, and configure client visibility. This permission is commonly assigned to SOC managers.
- **Disabled:** The account user cannot access the **Users** or **Clients** side panels in the **Settings** section.

## Import IOCs for all clients

- **Enabled:** The account user can execute calls to the Cytomic Orion API to load new IOCs on the platform.
- **Disabled:** The account user cannot execute calls to the Cytomic Orion API to load new IOCs on the platform.

## Restart computers

- **Disabled:** The account user can invoke the reboot sequence on the SOC clients' computers.
- **Disabled:** The account user cannot invoke the reboot sequence on the SOC clients' computers.

## Remote shell and view executed commands

- **Enabled:** The account user can remotely open a command line on the SOC clients' computers.
- **Disabled:** The account user cannot remotely open a command line on the SOC clients' computers.

## View the data usage dashboard

- **Enabled:** The account user can open the data usage dashboard by selecting **Data usage** in the side panel.
- **Disabled:** The account user cannot open the data usage dashboard.

## View client names

- **Enabled:** The console shows the names of clients that computers belong to, and not just ID numbers.
- **Disabled:** The console does not show the names of clients, just ID numbers. This way, analysts cannot link the data shown in Cytomic Orion to specific clients, thereby respecting any confidentiality agreements signed and data protection regulations (GDPR and other laws).

## View computer names

- **Enabled:** The console shows the names of computers, not just ID numbers.
- **Disabled:** The console does not show the names of computers, just ID numbers. This way, analysts cannot link the data shown in Cytomic Orion to specific computers, thereby respecting any confidentiality agreements signed and data protection regulations (GDPR and other laws).

## View the organization activity log

- **Enabled:** The account user can access the **Activity log** section from the top menu **Settings** to view a list of the actions performed by user accounts outside the context of an investigation.
- **Disabled:** The account user cannot access the **Activity log** section.

## View graphs

- **Enabled:** The account user can access the **Graphs** option, accessible from an investigation or from an event shown in the investigation console, to view graph-type notebooks.
- **Disabled:** The account user cannot access the **Graphs** option.

# User Account Activity Log

Cytomic Orion logs the actions taken by SOC analysts in the console outside of an investigation. For more information about the actions logged within the context of an investigation, see [Activity Log Associated with an Investigation](#) on page 117.

## Access the User Activity Log

In the top menu, select **Settings**. In the side panel, select **Activity log**. The **User activity log** list opens.

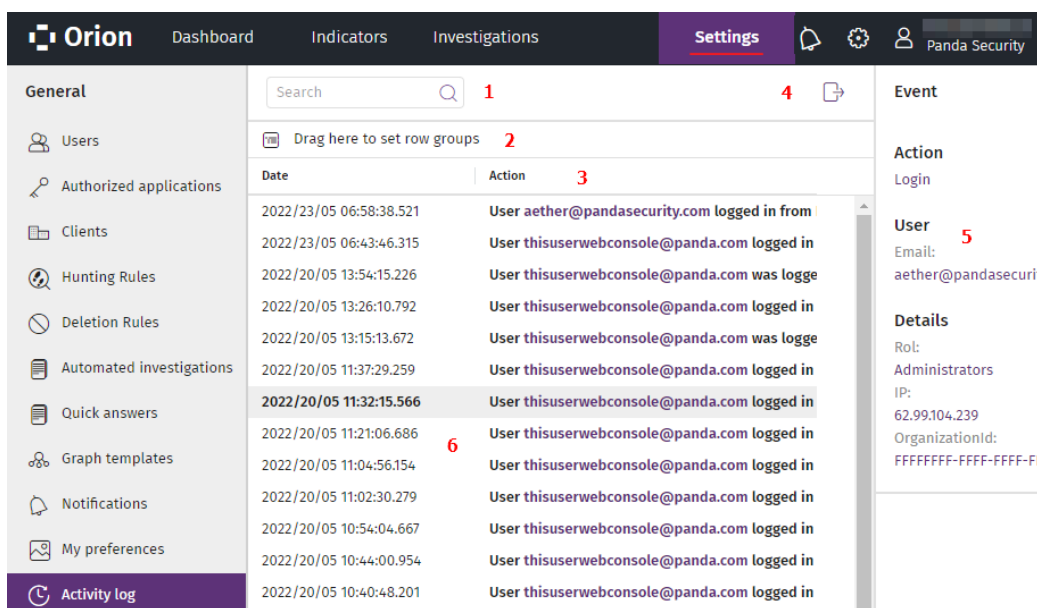


Figure 4.4: User Activity Log list

- **Search tool (1):** Searches the contents of the **Action**, **User**, and **Action type** fields. You can type only a partial string. See [Search Tools](#) on page 40.
- **Grouping tool (2):** Groups items in the list by the column you choose. For more information about the grouping tool, see [Group Entries by Columns](#) on page 37.
- **Sort list (3):** To sort the list by a particular column, click the column header. Click the same header a second time to switch between ascending and descending order. See [Sort Columns](#) on page 37.
- **Export (4):** Exports the contents of the list to a CSV file.
- **Side panel (5):** Shows extended information about the items you select in the list. See [Additional Information about Logged Events](#).
- **Center panel (6):** Shows a list of actions that match the search criteria you entered. This table describes the columns included in the list:

Field	Description
Date	Date of the logged action.

Field	Description
<b>Action</b>	Logged action along with the user account that started it and additional information. See <a href="#">Actions Logged in Cytomic Orion</a> .
<b>User</b>	Name of the account that started the action. This column is not shown by default.
<b>Action type</b>	Type of logged action. This column is not shown by default.

Table 4.2: Fields in the Activity Log list

## Actions Logged in Cytomic Orion

Action type	Description
<b>Login</b>	The user logged in to the console.
<b>Logout due to inactivity</b>	The console user did not take any action in two hours and was logged out of Cytomic Orion automatically for security reasons.
<b>Logout</b>	The user logged out of the console.
<b>Create quick answer template/automatic investigation template/graph template</b>	The user created the specified quick answer template, investigation template, or graph template.
<b>Modify quick answer template/automatic investigation template/graph template</b>	The user edited the specified quick answer template, investigation template, or graph template.
<b>Delete quick answer template/automatic investigation template/graph template</b>	The user deleted the specified quick answer template, investigation template, or graph template.
<b>Update the description or category of a quick answer template/automatic investigation template/graph template</b>	The user updated the description or the category of the specified quick answer template, investigation template, or graph template.
<b>Rename quick answer template/automatic investigation template/graph template</b>	The user renamed the specified quick answer template, investigation template, or graph template.
<b>Copy quick answer template/automatic investigation template/graph template</b>	The user copied the specified quick answer template or graph template.

Action type	Description
Disable two-factor authentication	The user disabled two-factor authentication for their account.
Enable two-factor authentication	The user enabled two-factor authentication for their account.
Create hunting rule	The user created a hunting rule.
Modify hunting rule	The user modified a hunting rule.
Delete hunting rule	The user deleted a hunting rule.

Table 4.3: Types of logged actions

### Additional Information about Logged Events

Field	Description
Action	Logged action. See <a href="#">Actions Logged in Cytomic Orion</a> .
Email	Email address of the user account that performed the logged action.
Role	Role of the user account that performed the logged action.
IP	Public IP address of the last network device the analyst used to log in to the console.
OrganizationID	ID of the SOC/MSSP that the user account belongs to.
NotebookId	ID of the document on which the operation was performed.
OldNotebookDescription	Notebook description before it was edited.
NewNotebookDescription	New description associated with the notebook.
NotebookName	Name of the notebook on which the operation was performed.
DocumentName	Name of the document on which the operation was performed.

Field	Description
<b>OldNotebookName</b>	Notebook name before it was edited.
<b>NewNotebookName</b>	New notebook name.
<b>ImageId</b>	ID of the Jupyter image that was used as the basis for the notebook.
<b>DocumentId</b>	ID of the document on which the operation was performed.
<b>DocumentVersionId</b>	ID of the document internal version number.
<b>DocumentIsManualSave</b>	<ul style="list-style-type: none"> <li>• <b>True:</b> The document was saved manually.</li> <li>• <b>False:</b> The document was saved automatically.</li> </ul>
<b>OldCategoryId</b>	Notebook category before it was edited.
<b>NewCategoryId</b>	New notebook category.
<b>Discriminator</b>	<p>Type of document on which the operation was performed.</p> <ul style="list-style-type: none"> <li>• <b>0:</b> Not set</li> <li>• <b>1:</b> Document</li> <li>• <b>2:</b> Template</li> <li>• <b>3:</b> Quick answer</li> <li>• <b>4:</b> Graph</li> <li>• <b>5:</b> OSQuery</li> </ul>
<b>SourceNotebookId</b>	ID of the notebook that was copied.
<b>TargetNotebookId</b>	ID of the new, copied notebook.

Table 4.4: Fields in the right panel

# Indicators and Hunting Rules

In most cases, SOC analysts begin the hunting process after a new indicator or hypothesis has appeared. Cytomic Orion generates an indicator when it detects a behavior that could belong to the Cyber Kill Chain (CKC) of a cyberattack in the telemetry collected from a client's computers. This hypothesis is analyzed by Tier 1 technicians to determine whether it is a false positive or a possible threat to be investigated. The filtering process is known as 'indicator triage' and aims to deliver to Tier 2 technicians hypotheses that correspond to anomalous situations that should be investigated in greater depth.

## CHAPTER CONTENTS

---

<b>Basic Concepts of the Indicator System</b> .....	<b>64</b>
<b>Access the Indicators Area</b> .....	<b>66</b>
<b>Indicators List</b> .....	<b>66</b>
<b>Filter and Group Indicators</b> .....	<b>69</b>
<b>Delete Indicators Manually</b> .....	<b>70</b>
<b>Delete Indicators Automatically</b> .....	<b>71</b>
Manage Deletion Rules .....	73
<b>Restore Indicators and Manage the Recycle Bin</b> .....	<b>75</b>
<b>Indicator Management Best Practices</b> .....	<b>76</b>

## Basic Concepts of the Indicator System

### Hunting Rules

Hunting rules are descriptions of patterns of events suspicious of belonging to the Cyber Kill Chain (CKC) of a cyberattack. Hunting rules are created by two different groups of analysts:



- Cytomic analysts who, with the aid of automated machine learning systems transversally analyze the flow of events generated by Cytomic Orion clients to create and test new hunting rules.
- SOC analysts who want to adapt the generated indicators to the real environments of their clients, enabling and disabling existing rules and creating new ones in accordance with the events that occur.



See *Manage Hunting Rules* on page 78

## Indicator Characteristics

When the monitoring of processes detects a sequence of events that matches a hunting rule, Cytomic Orion generates an indicator. This indicator is associated with the hunting rule that generated it and the computer it was found on.

The key attributes that analysts must consider are these:

- **The moment when Cytomic Orion logged the last event that generated the indicator:** This determines when the situation suspicious of belonging to the Cyber Kill Chain (CKC) of a cyberattack occurred, so analysts can thoroughly investigate the status of the computer at that moment.
- **Name and identifier of the affected computer.** An indicator refers only to one computer. If the same sequence of suspicious events occurs on multiple computers, a separate indicator is generated for each computer.
- **Number of times the indicator occurs:** If the same indicator pattern is detected continuously on one computer, Cytomic Orion generates only one indicator, specifying the number of occurrences. See [Indicator Grouping](#)
- **Indicator status:** Indicates whether the indicator is pending investigation, has already been investigated, or the investigation is ongoing.
- **Indicator severity:** Indicates whether the indicator corresponds to an attack which, because of the way it operates, can have a major impact on the normal operation of a company IT systems. Such an impact could result in serious financial losses for organizations, and therefore analysts should use this to prioritize investigations.
- **Associated hunting rule:** An indicator is associated with a single hunting rule that Cytomic Orion used to detect the suspicious event pattern. The name of a hunting rule is descriptive and provides a guideline for the investigation.

## Basic Structure of the Indicator Generation Process

This diagram summarizes the main steps in the indicator generation process.

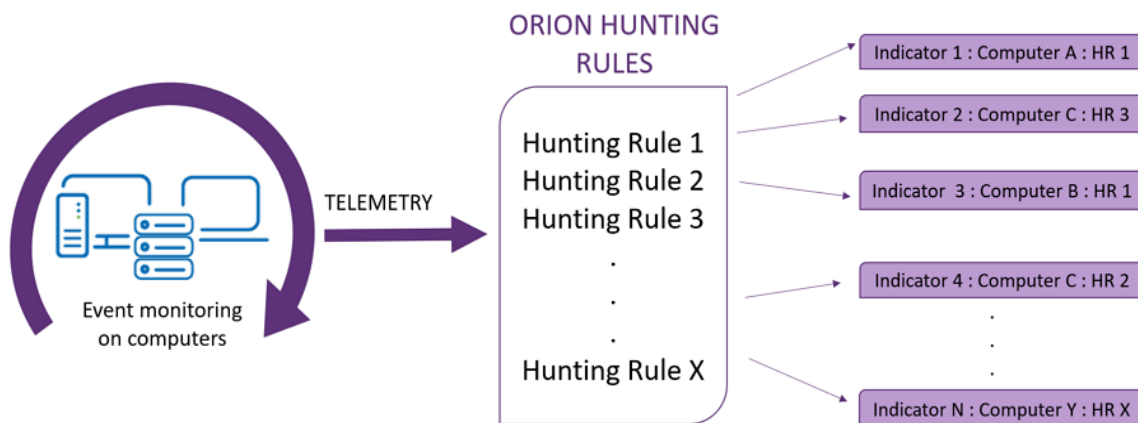


Figure 5.1: Indicator generation process based on hunting rules

## Access the Indicators Area

In the top menu, select **Indicators**. A page opens that is divided into these sections:

- **Filtering panel (1):** The left panel provides indicator filtering tools that make it easier for analysts to assign indicators to investigations and delete indicators that are of no use.
- **Search panel (2):** Enables analysts to search for indicators by their content.
- **Indicators panel (3):** Lists all the indicators generated on the computers of the MSSP/MDR vendor clients, and provides tools for Tier 1 SOC analysts to manage indicators and generate investigations.

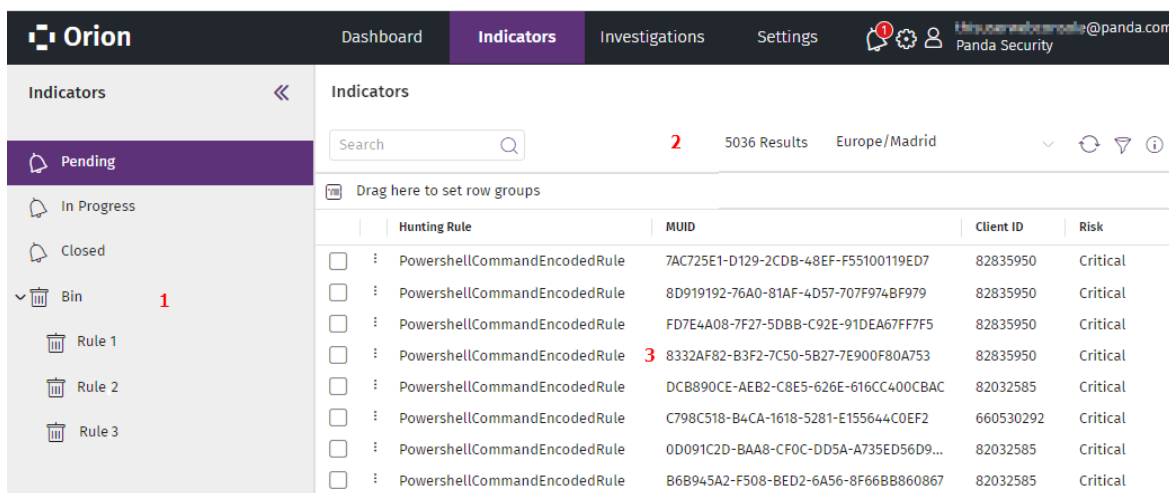


Figure 5.2: Indicators area overview

## Indicators List

The Indicators panel shows the indicators generated by the hunting rules and a number of columns that describe each indicator.

Field	Description
<b>Hunting rule</b>	Name of the hunting rule that generated the indicator and description of the artifacts monitored on the client's computer.
<b>Status</b>	<p>Indicates whether the indicator has been assigned to an investigation and the indicator status.</p> <ul style="list-style-type: none"> <li>• <b>In progress:</b> The indicator is assigned to an investigation and a Tier 2 analyst is investigating it.</li> <li>• <b>Pending:</b> The indicator has still not been assigned to an investigation.</li> <li>• <b>Closed:</b> The indicator was assigned to an investigation and has been resolved.</li> </ul>
<b>Investigation</b>	Name of the investigation associated with indicators with the status <b>In progress</b> or <b>Closed</b> .
<b>Indicator date</b>	Date the indicator was generated.
<b>Last event</b>	Date of the last event that led to the generation of the indicator. This date might not be the same as the <b>Indicator date</b> if there was a delay in generating the indicator, for example because of an interruption of the communication between the Cytomic Orion server and the client's computer.
<b>Computer</b>	Name of the client's computer where the indicator was detected.
<b>Group</b>	Group in the Cytomic EPDR console the computer belongs to.
<b>Date deleted</b>	Date a deletion rule was applied to the indicator and the indicator was moved to the bin.
<b>Deleted by</b>	Name of the deletion rule that moved the indicator to the bin.
<b>MUID</b>	Unique identifier of the client's computer where the indicator was detected.
<b>Client ID</b>	Unique identifier of the client the computer where the indicator was detected belongs to.
<b>Risk</b>	Severity of the indicator impact: <b>Critical, High risk, Medium risk, Low risk</b> .
<b>MITRE</b>	Tactic, technique, and sub-technique associated with the hunting rule according to the MITRE specification. If there is more than one tactic and technique pair,

Field	Description
	they are separated by the character '#'. For more information, see <a href="#">Details Panel</a> .
<b>Occurrences</b>	Number of times Cytomic Orion detected the same type of indicator repeatedly on the same computer. See <a href="#">Indicator Grouping</a>
<b>Details</b>	Description of the indicator and name of the associated hunting rule. This specifies the type of suspicious event logged so that the Tier 1 team can triage the incident.
<b>Operating systems</b>	Operating systems searched by the hunting rule that detected the suspicious event.

Table 5.1: Fields in the Indicators list

The Indicators panel provides this additional information:

- **Number of indicators the solution found based on the configured selection criteria:** This appears at the top of the list (2).
- **Time zone:** Change the time zone configured by default for the entire console. Set it using the control at the top of the list (2). This setting affects both the **Indicator date** column in the lists and the date format entered in the filter panel. See [Settings Area](#) on page 32.

## Indicator Grouping

With the aim to not hinder analysts' investigation activities with too long lists that show repeated indicators, Cytomic Orion groups indicators depending on where they were detected.

### Indicators Detected on the Server

If hunting rules classify as a potential threat an event pattern that appears repeatedly in the telemetry that a computer sends to the server, Cytomic Orion generates these indicators:


- A first indicator with the **Occurrences** field set to 1 when it detects the first pattern on the computer.
- An indicator every hour. This indicator groups all detections made in that interval of time on the computer. The **Occurrences** field shows the number of detected occurrences.

### Indicators Detected on a Computer

If the protection software installed on a computer classifies an event pattern that appears repeatedly on the computer as a potential threat, Cytomic Orion generates these indicators:

- A first indicator with the **Occurrences** field set to 1 when it detects the first pattern on the computer.
- An indicator every 6 hours. This indicator groups all detections made in that interval of time. The **Occurrences** field shows the number of detected occurrences.

## Details Panel

Click the  icon in the upper-right corner to open the **Details** panel. Two tabs appear:

- **Details:** Shows fields with information about the selected indicator. See [Indicators List](#)
- **MITRE:** Shows details of the MITRE tactic and technique associated with the hunting rule that generated the indicator. If the hunting rule is associated with more than one technique, the MITRE panel groups the information in drop-down tabs, one for each technique. The information shown on the MITRE tab is gathered from the official source, at <https://attack.mitre.org/matrices/enterprise/>


Field	Description
<b>Tactic</b>	Name of the MITRE matrix tactic related to the hunting rule that generated the indicator. Tactics are identified by a character string in the TXXXX format.
<b>Technique</b>	Name of the MITRE matrix technique related to the hunting rule that generated the indicator. Techniques are identified by a character string in the TXXXX format.
<b>Sub-technique</b>	Name of the MITRE matrix sub-technique related to the hunting rule that generated the indicator. Sub-techniques are identified by a character string in the TXXXX.YYY format.
<b>Platform</b>	Operating systems affected by the tactic and technique.
<b>Required permissions</b>	Permissions required by the adversary to perform the attack described in the tactic and technique.
<b>Description</b>	Tactic and technique description according to the data published by MITRE.

Table 5.2: Fields on the MITRE tab

## Filter and Group Indicators

Cytomic Orion provides multiple tools for filtering indicators that enable analysts to rapidly and flexibly find the information they need.

### Filter by Indicator Status

The left panel (1) provides a tool for filtering indicators by status. Select a status with the  icon to update the list:

- **In progress:** The indicator is assigned to an investigation and a Tier 2 analyst is investigating it.
- **Pending:** The indicator has still not been assigned to an investigation.
- **Closed:** The indicator was assigned to an investigation and has been resolved.

## Filter by Indicator Features


The Indicators list provides tools for filtering the entries shown based on the content of the columns. These tools enable you to sort and configure the list according to your needs. For more information about the Cytomic Orion tools common to all lists, see [Tools for Configuring Lists](#) on page 36.

## Search for Indicators by Content

At the top of the list, you can find a tool that supports partial searches and extends the search to the content of all the fields in the list. For more information, see [Search Tools](#) on page 40.

## Filter Indicators by Time Period

The filter you set applies to the creation date of the last event associated with the indicator (**Last event** field of the event).

- Click the  icon (2). A filter panel appears on the side.
- In the **Date** field, select a filter:
  - **Last 24 hours**
  - **Last 7 days**
  - **Custom:** Set the dates and times for the interval.
- Select a time zone to filter indicators.
- Click **Apply**. The indicator list (3) updates.

## Sort and Group Indicators in the List

To change the order of results and the way indicators are shown in the list, see [Tools for Configuring Lists](#) on page 36.


# Delete Indicators Manually

Ambiguous hunting rules can generate a large number of indicators that can be false positives. This excessive noise can overload Tier 1 analysts when triaging. To avoid this situation, Cytomic Orion enables you to move indicators manually to the recycle bin.

## Required Permissions

To delete indicators and manage indicator deletion rules, the analyst account must have the **Delete indicators and manage automatic indicator deletion rules** permission assigned to the account role. For more information about roles and permissions, see [Understanding Permissions](#) on page 56.

## Move One or More Indicators to the Recycle Bin

- Select the checkboxes for the indicators you want to delete. You can delete only indicators that have the **Pending** status.
- In the toolbar, select **Delete** . The indicators are automatically moved to the **Deleted manually** section of the bin.



Indicators marked as **Deleted** are held in the recycle bin for seven days. After that time, they are permanently removed from Cytomic Orion.

## Delete Indicators Automatically

Analysts can create deletion rules to define filtering criteria for the flow of indicators generated by Cytomic Orion. When an indicator that matches the criteria defined for a deletion rule is detected, it is assigned the status **Deleted** and removed from the list of indicators. Indicators marked as **Deleted** are temporarily moved to the recycle bin, although if an indicator was previously assigned to an investigation, it is not removed from it.



Indicators marked as **Deleted** are held in the recycle bin for seven days. After that time, they are permanently removed from Cytomic Orion.




## Add a Deletion Rule

You create deletion rules from a single indicator. Before you begin the process to create a rule, make sure that only one indicator is selected in the list.

- In the top menu, select **Indicators**. Select an indicator by using the relevant checkbox.
- In the toolbar, select **Add automatic deletion rule (4)**. A dialog box opens that shows information about the indicator you want to delete.

Or

- Click the context menu **(2)** next to the checkbox or right-click any of the indicator's fields to open the drop-down menu. Select **Add automatic deletion rule**.
- Fill in the fields for the deletion rule:
  - **Name:** Name of the deletion rule.
  - **Description:** Text field where the analyst can specify the reasons for deleting indicators.
- Fill in the fields that describe the indicators you want to delete:

- **Client ID:** Specify the client IDs associated with the indicators you want to delete. All deletion rules must have at least one associated client. Click the  icon to select the clients, or copy and paste a list of client IDs separated by commas.
- **Hunting Rule:** This is the name of the hunting rule that generated the indicators you want to delete. This is an optional field.
- **MUID:** Specify the computer IDs associated with the indicators you want to delete. Click the  icon to select the MUIDs, or copy and paste a list of MUIDs separated by commas. This is an optional field.
- **Computer:** Specify the names of the computers where the indicators you want to delete originated. Click the  icon to select the computers, or copy and paste a list of computer names separated by commas. This is an optional field.
- **Details:** Specify the **Details** field for the indicators you want to delete. You can determine the exact content of the field with the **Equals** option, or flexibly with a regular expression by using the **RegEx** option. For more information, see [Manage Deletion Rules](#).

By default, deletion rules are created as restrictively as possible, and it is up to analysts to disable the optional fields they deem unnecessary in order to make the rule more flexible.

If you define multiple criteria for a deletion rule, the logical operator AND is used. This way, only those indicators that meet all the criteria set out in the deletion rule are filtered.

## Regular Expressions



*For more information about the syntax allowed in regular expressions, see <https://docs.microsoft.com/en-us/dotnet/standard/base-types/regular-expression-language-quick-reference>.*

*To validate the regular expressions created, see <http://regexstorm.net/tester>.*

Cytomic Orion supports RegEx C to describe flexible patterns in the **Details** field of indicators. As with most languages used to describe character patterns, you must escape those characters considered special or belonging to the language itself. To this end, the “\” character is used in RegEx C.

To help with the development of regular expressions, there is a preview panel which enables you to check whether the patterns you want to search for match the regular expression as you write it.

To generate a regular expression, select the **RegEx** option from the drop-down menu in the **Details** field. The content of the field updates with a regular expression that meets the content of the preview panel. All the special characters are escaped automatically by the console to make it easier for the analyst to edit the regular expression.



## Example of Exclusion Created by Using Regular Expressions in the Details Field

You want to remove from the Indicators panel all executions of the `net.exe` tool when it tries to add the `"gcch\GG_SEC_IBM_PC_Admins"` user to the administrators group, because it is a frequent action but risk free.

The indicator generated by Cytomic Orion in this situation is this:

```
{
  "contents":
  [
    {
      "ChildPath": "SYSTEM|net.exe",
      "CommandLine": "net localgroup administrators "gcch\GG_SEC_
IBM_PC_Admins" /add",
      "ParentPath": "SYSTEM|cmd.exe",
      "extendedInfo": "",
      "loggedUser": "NT AUTHORITY\SYSTEM"
    }
  ]
}
```

The indicator is shown in a compact format in the Details field of the Cytomic Orion console:

```
{"contents": [{"ChildPath":"SYSTEM|net.exe","CommandLine":"net localgroup administrators "gcch\GG_SEC_IBM_PC_Admins /add","ParentPath":"SYSTEM|cmd.exe","extendedInfo":"","loggedUser": "NT AUTHORITY\SYSTEM"}]}
```

The regular expression that filters indicators by the content of the Details field according to the criteria established by the analyst would be:

```
{"ChildPath":"SYSTEM|net.exe".+gcch\GG_SEC_IBM_PC_Admins
```

The preview panel enables you to verify that the regular expression defined generates the character pattern that matches the content of the indicator's Details field.

## Manage Deletion Rules

To manage deletion rules centrally, select **Settings** in the top menu. In the side panel, select **Deletion rules**. A list opens that shows all the deletion rules created so far.

### Deletion Rules List

Field	Description
<b>Name</b>	Deletion rule name assigned by the analyst.
<b>Creation date</b>	Date the deletion rule was created.

Field	Description
<b>Modification date</b>	Date the deletion rule was last modified.
<b>Description</b>	Description assigned by the analyst.
<b>Hunting rule</b>	Name of the hunting rule that generated the indicator and description of the artifacts monitored on the client's computer.
<b>Indicators deleted in the last 30 days</b>	Number of indicators deleted by the rule in the last 30 days. Analysts can use this field to determine the usefulness of the deletion rule.
<b>Last deletion date</b>	Date and time the rule last deleted an indicator. Analysts can use this field to determine the usefulness of the deletion rule.

Table 5.3: Fields in the Deletion Rules list

## Edit a Deletion Rule

If an analyst finds that a rule is deleting useful indicators, they can edit it. Follow these steps:

- In the side panel, select **Bin** to show the deletion rules created.
- Click the context menu icon for the deletion rule you want to edit. A drop-down menu appears.
- Select **Edit automatic deletion rule**. Set the new criteria for deleting indicators:
  - **Name**: Name of the deletion rule.
  - **Description**: Text field where the analyst can specify the reasons for deleting indicators.
  - **Client ID**: Specify the IDs of the clients that the computers where the indicators you want to delete were detected belong to.
  - **Hunting rule**: Name of the hunting rule associated with the deletion rule.
  - **MUID**: Specify the IDs of the computers where the indicators you want to delete were detected.
  - **Computer name**: Name of the computers where the indicators you want to delete were detected.
  - **Details**: Specify the **Details** field for the indicators you want to delete. You can determine the exact content of the field with the **Equals** option, or flexibly with a regular expression by using the **RegEx** option. For more information, see [Regular Expressions](#) on page 256.


Indicators already affected by the deletion rule do not undergo any changes and are not shown in the main list, although they are shown when you click the edited rule.

## Delete a Deletion Rule

If an analyst finds that a rule is deleting useful indicators, they can delete it.

- In the side panel, select **Bin** to show the deletion rules created.
- Click the context menu icon for the deletion rule you want to delete. A drop-down menu appears.
- Select **Delete**. Recent indicators affected by the deletion rule reappear in the Indicators list with the status **Pending**. Indicators from more than seven days ago are not retrieved.


## Export the List

Click the  icon to download a CSV file with the content of the **Deletion rules** list.

# Restore Indicators and Manage the Recycle Bin

## Sort and Group the Deletion Rules Defined

To make it easier to find deleted indicators, the recycle bin groups indicators automatically based on the deletion rule that was used to delete them. Because there might be many deletion rules defined, Cytomic Orion provides tools to sort and group them in different ways:

- In the top menu, select **Indicators**. In the left menu, click the  icon. A page opens that show all deletion rules defined, without any particular sorting or grouping criterion applied.
- Click the bin context menu. The **Sort by** option appears, along with these criteria:
  - **Modification date**: Sorts the deletion rules by the date they were last modified.
  - **Hunting rule**: Groups the deletion rules by the associated hunting rule. There will be as many groups as hunting rules have been used by Cytomic Orion to generate the indicators deleted by the analyst.
  - **Name**: Sorts the deletion rules by name.
  - **Ascending**: Means the smallest, or first, or earliest in the order will appear at the top of the list.
  - **Descending**: Means the smallest, or first, or earliest in the order will appear at the bottom of the list.

## Restore Indicators from the Recycle Bin

- In the top menu, select **Indicators**. In the left menu, click the bin icon. Deletion rules are shown as a tree depending on the sorting and grouping criteria you selected for the recycle bin.
- Select the deletion rule associated with the indicators you want to restore to filter the indicator list shown in the right panel.

- Select the checkboxes next to the indicators you want to restore. In the toolbar, select the **Move to pending** option. The status of the indicators changes to **Pending** and they are removed from the recycle bin.

## Restore All Indicators Deleted by a Deletion Rule

If, by mistake, a deletion rule moves indicators useful to SOC analysts to the recycle bin, follow these steps to restore them:

- In the top menu, select **Indicators**. In the left menu, click the bin icon. Deletion rules are shown as a tree depending on the sorting and grouping criteria you selected for the recycle bin.
- In the recycle bin, select the deletion rule associated with the indicators you want to restore. In the rule context menu, select **Move all indicators that meet this rule**. A drop-down list appears with the available statuses for the indicators deleted by the rule.
- Select **Pending**. All indicators contained in the deletion rule are reincorporated into the Indicators list with the chosen status.

## Show all Indicators Stored in the Recycle Bin

In the side panel, select **Bin**. The central panel shows all indicators marked as Deleted in the last seven days.

## Show Indicators Deleted by a Rule

In the left panel, select **Bin** to show the deletion rules created by the analyst. Select a deletion rule to show all deleted indicators that matched the criteria set in that particular rule.

# Indicator Management Best Practices

For Tier 1 SOC analysts to manage the indicators generated by Cytomic Orion according to their severity, follow these tips. For more information about how to use the grouping and filtering tools, see [Tools for Configuring Lists](#) on page 36.

- Order indicators by created date. You can do this by double-clicking the **Last event** column name to show the most recent indicators first.
- Filter indicators by status to easily find indicators with the status **Pending**.
- Add a grouping by the **Risk** column. The **Critical** group contains the most dangerous indicators for the organization and those most likely to need to be added to an investigation.
- To review all the indicators generated by a hunting rule, group them by dragging the **Hunting Rule** column to the grouping bar. It is quite probable that one hunting rule generates several related indicators
- To review situations where a hunting rule continuously generates a very high number of indicators, sort entries by the **Occurrences in the last hour** column.

- Check the **Details** column for indicators because it contains a description of the hunting rule that generated the indicator. Using the name and the **Details** column, an analyst can determine the starting point for triage or for the investigation. If this column is not shown in the Indicators list, follow the steps listed in [Add or Remove Columns](#) on page 37.
- Group rules according to their tactic and technique to assign them to technicians specialized in specific attack strategies.

## Manage Hunting Rules

Cytomic Orion analyzes the telemetry data flow sent by computers on the network, looking for suspicious event patterns that could belong to the Cyber Kill Chain (CKC) of a cyberattack. Each of these patterns is stored in a hunting rule, and the cyberattack radar compares them against the telemetry data to generate indicators when a positive match occurs.

In Cytomic Orion, there are two possible sources for hunting rules:

- Cytomic analysts and automatic machine learning (ML) systems. They continuously analyze the flow of events received to create and test new hunting rules. These rules are visible to all Cytomic Orion clients.
- Each SOC analysts, who can generate their own hunting rules. These rules are visible only to the analysts' organization.

### CHAPTER CONTENTS

---

<b>List of Hunting Rules</b> .....	<b>79</b>
List of Hunting Rules .....	79
Manage Hunting Rules .....	80
<b>Manage Hunting Rules</b> .....	<b>81</b>
Create a Hunting Rule .....	82
Validate a Hunting Rule .....	85
Edit a Hunting Rule .....	86
Delete a Hunting Rule .....	86
<b>Email Notification Rules</b> .....	<b>87</b>
Create a Notification Rule .....	87
Edit a Notification Rule .....	88
List of Notification Rules .....	88
Manage the List of Notification Rules .....	88
Notifications Related to Changes in the MITRE Framework .....	90

# List of Hunting Rules

## Access the List of Hunting Rules

In the top menu, select **Settings**. In the side panel, select **Hunting rules**. Select the **Hunting rules** tab. A list opens that shows all the hunting rules created so far.

## Required Permissions

No special permissions are required to access the list of hunting rules.

## List of Hunting Rules

This list shows the hunting rules created so far, both by Cytomic and by the SOC analysts. Hunting rules created by analysts are only applied within the SOC and are visible only to user accounts that belong to the SOC.

Field	Description
<b>Name</b>	The name of the hunting rule. The indicators generated by a hunting rule show the hunting rule name in the <b>Hunting rule</b> column in the <b>Indicators</b> list. See <a href="#">Indicators List</a> on page 66
<b>Risk</b>	The severity of the impact of the indicators generated by the hunting rule: <b>Critical</b> , <b>High risk</b> , <b>Medium risk</b> , <b>Low risk</b> , <b>Unknown</b> .
<b>Created by</b>	SOC user account that created the hunting rule. If it is an internal Cytomic Orion rule, the Cytomic logo appears.
<b>Owner</b>	Name of the organization to which the user account that created the rule belongs. If it is an internal Cytomic Orion rule, the Cytomic logo appears.
<b>Status</b>	<ul style="list-style-type: none"> <li>• <b>Disabled</b>: The rule has been manually disabled by the analyst. It does not generate new indicators until it is re-enabled.</li> <li>• <b>Enabled</b>: The cyberattack radar analyzes the event flow collected from the client's computers and compares it to the hunting rule to generate indicators.</li> <li>• <b>Automatically disabled</b>: The cyberattack radar detected that the hunting rule generated too many indicators and disabled it automatically to avoid affecting performance. See <a href="#">Change the Status of a Hunting Rule</a>.</li> </ul>
<b>MITRE</b>	Tactic, technique, and sub-technique associated with the hunting rule according to the MITRE specification. If there is more than one tactic and technique pair, they are separated by the character '#'. For more information, see <a href="#">Details Panel</a> on

Field	Description
	page 69.
<b>Creation date</b>	Date the hunting rule was created.
<b>Modification date</b>	Date the hunting rule was last modified.
<b>Status change</b>	Date of latest change of status.
<b>Operating systems</b>	Operating systems on which the hunting rule searches for indicators.


Table 6.1: Fields in the Hunting Rules list.

## Manage Hunting Rules

### View a Hunting Rule Settings

Click the name of a hunting rule to show the rule creation wizard. If the analyst has sufficient permissions, they can edit the rule parameters; otherwise, all options are disabled. See [Manage Hunting Rules](#)

### Export the List of Hunting Rules

To download the list of hunting rules to an Excel file, click the  icon in the upper-right corner of the page. For more information about the meaning of the fields in the Excel file, see [List of Hunting Rules](#).


### Search For a Hunting Rule

To search the **Name** field, use the **Search** text box in the upper-right corner of the list of hunting rules. Partial searches are valid.

### Sort Hunting Rules

To sort and group the content of the columns in the list, use the resources described in [Tools for Configuring Lists](#) on page 36.

### Refresh the List of Hunting Rules

To show the changes made to the hunting rules in the list, as well as new entries or deletions, click the  icon in the upper-right corner of the page.



## Change the Status of a Hunting Rule



The user account you used to access the analysis console must have the **Manage hunting rules** permission assigned. For more information about roles and permissions, see [Understanding Permissions](#) on page 56.

- Select the checkboxes next to the rules whose status you want to change.
- In the top tool bar, select **Enable** or **Disable**. The status of the selected rules changes as indicated in the **Status** column in the list.

## Disable a Hunting Rule Automatically

For Cytomic Orion to automatically disable a hunting rule, the rule must meet one of these two conditions:

- The hunting rule has a significant impact on the performance of the cyberattack radar.
- The hunting rule generates a large number of indicators.

If a hunting rule uses too many resources, Cytomic Orion disables it automatically. In that case, these actions are performed:

- A warning message appears at the top of the page that indicates that some rules have been automatically disabled.
- The status of the disabled rules changes to **Automatically disabled**.
- Every Monday, Cytomic Orion sends an email message with a list of the hunting rules it stopped the previous week. This message is sent to the SOC accounts that have one of these permissions:
  - Manage hunting rules.
  - Create hunting rules and notification rules for all clients.
  - Create indicator notification rules.

Click the **See stopped hunting rules** link in the warning message to see only those rules that have been automatically stopped by Cytomic Orion.

# Manage Hunting Rules

## Access the List of Hunting Rules


In the top menu, select **Setting**. In the side panel, select **Hunting rules**. Select the **Hunting rules** tab. A list opens that shows all the hunting rules created so far.



## Required Permissions

The user account used to access the analysis console must have the **Manage hunting rules** permission assigned. For more information, see [Manage Hunting Rules](#).

Analysts can create hunting rules only for events generated by the computers of clients for which they have visibility. To simplify the management of roles, Cytomic Orion includes the **Create hunting rules and notification rules for all clients** permission to enable you to create hunting rules regardless of the visibility settings of the account you use. For more information about roles and permissions, see [Understanding Permissions](#) on page 56.

## Create a Hunting Rule

- Click the **Add hunting rule** link or the  icon in the upper-right corner of the page. The wizard for creating hunting rules opens.
- Enter this data:

Field	Description
<b>Name</b>	The name of the hunting rule. The indicators generated by a hunting rule show the hunting rule name in the <b>Hunting rule</b> column in the <b>Indicators list</b> . See <a href="#">Indicators List</a> on page 66
<b>Description</b>	The analyst’s notes associated with the hunting rule.
<b>Status</b>	<ul style="list-style-type: none"> <li>• <b>Disabled:</b> The rule has been manually disabled by the analyst. It does not generate new indicators until it is re-enabled.</li> <li>• <b>Enabled:</b> The cyberattack radar analyzes the event flow collected from the client’s computers and compares it to the hunting rule to generate indicators.</li> </ul>
<b>Risk</b>	The severity of the impact of the indicators generated by the hunting rule: <b>Critical, High risk, Medium risk, Low risk, Unknown.</b>
<b>MITRE</b>	Tactic, technique, and sub-technique associated with the hunting rule according to the MITRE specification. A hunting rule can have multiple associated tactics, techniques, and sub-techniques. Click the  and  icons to add or remove tactics. A tactic must always have a technique associated with it. However, a technique does not necessarily have to have a sub-technique associated with it. For more information, see <a href="#">Details Panel</a> on page 69.
<b>Clients</b>	Specify the clients whose event flow is inspected by the hunting rule. <ul style="list-style-type: none"> <li>• <b>All clients:</b> This option appears only if the analyst account has the <b>Create</b></li> </ul>



Field	Description
	<p><b>hunting rules for all clients</b> permission assigned.</p> <ul style="list-style-type: none"> <li>• <b>The following clients:</b> Add clients by copying and pasting a comma-separated list, or through the <b>Add clients</b> dialog box that opens after you click the  icon.</li> <li>• <b>All clients except these:</b> This option appears only if the analyst account has the <b>Create hunting rules for all clients</b> permission assigned. Add the clients you want to exclude by copying and pasting a comma-separated list, or through the <b>Add clients</b> dialog box that opens after you click the  icon.</li> </ul>
<b>Operating systems</b>	Restrict the search performed by the hunting rule to the specified operating systems.

Table 6.2: Fields in a hunting rule

- Define the hunting rule with the wizard.
- Run the validation process to verify the hunting rule does not impact the performance of the cyberattack radar. See [Validate a Hunting Rule](#).

After you create a rule, the cyberattack radar immediately begins to compare the telemetry data received against the new hunting rule.

## General Structure of the Wizard

To build a hunting rule with the wizard, you must configure these parameter blocks:

- **Type (1):** The type of event that the hunting rule looks for in the telemetry data. It is equivalent to the `FROM [table]` clause in SQL. The drop-down menu lists the tables shown in [Tables \(1\)](#) on page [146](#).
- **Condition (2):** Equivalent to the `WHERE` clause in SQL. See below for a detailed description of this clause.
- **Indicator information (3):** Specify the content of the fields that are added to the indicator when it is generated by the hunting rule.

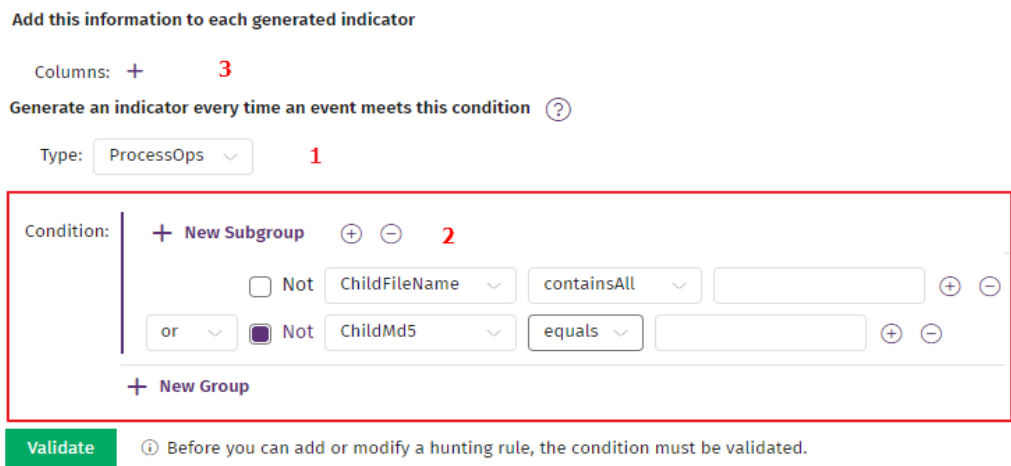


Figure 6.1: Main parameter blocks in the wizard

### Condition Block Structure

The **Condition** block is equivalent to the `WHERE` clause in SQL and allows a high degree of flexibility to specify the search conditions.

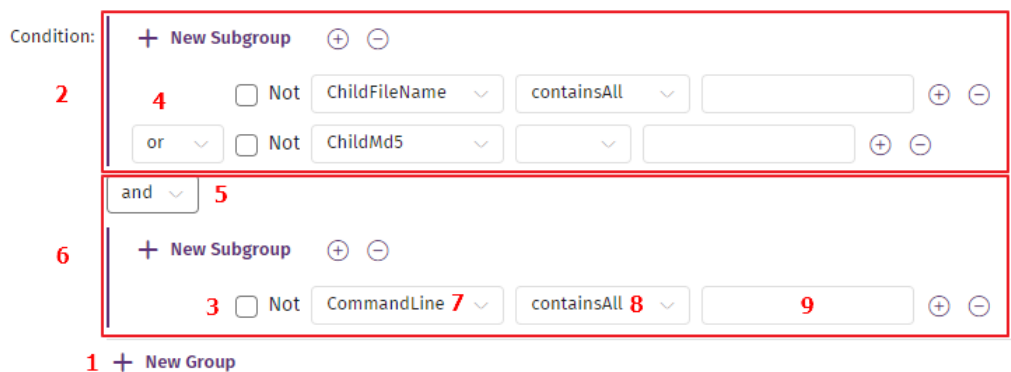


Figure 6.2: Condition block structure with two groups related by the logical operator AND.

The **Condition** block is divided into condition groups. Within a condition group, there can be a single condition (block (6)) or multiple conditions (block (2)).

#### Conditions

A simple condition (6) consists of a column name (7), a comparison operator (8) (see **Comparison Operators**), and the value to be compared against (9). Additionally, it can have an associated Boolean negation operator (3).

A compound condition (2) consists of multiple simple conditions related to each other through the AND and OR operators (4).

#### Groups

Each new group you create is equivalent to entering a simple or compound condition in parentheses in the `WHERE` clause of the corresponding SQL statement.

You can create multiple groups with the **New group** (1) button and relate them by the logical operator AND/OR (5).

Additionally, you can create one or more groups of simple or compound conditions within a group using the second-level **New group (10)** button.

## Comparison Operators

- **containsAny**: This operator is equivalent to the “Like” operator in SQL. It searches for a character substring.
- **equals**:: This operator searches for an exact character string.
- **endsWithAny**: This operator searches for a character substring at the end of a string.
- **startsWithAny**: This operator searches for a character substring at the beginning of a string.
- **containsInOrder**: This operator searches for three character substrings in the specified order. Specifying a single string is equivalent to using the **containsAny** operator. The operator will show results that contain all the strings you indicate (logical operator AND) in the order you specify.
- **Boolean operators**: The basic logical operators are supported ('<', '>', '>=', '<=', '==').
- **matches**: This operator enables you to write a regular expression in Java format. For more information about the format of regular expressions, escape characters, and other details about RegEx implementation in Java, see <https://docs.oracle.com/javase/8/docs/api/java/util/regex/Pattern.html>.

## Case-sensitive Searches

By default, all character string-type conditions are case insensitive, although analysts can change this through the associated drop-down menu.



Figure 6.3: Drop-down menu to set the comparison type for character string-type fields

The **ParentFilename** and **ChildFilename** fields are stored in the data lake in lowercase because they are taken from the **ParentPath** and **ChildPath** fields respectively. After they are extracted, a normalization process is automatically run in which all uppercase letters are changed to lowercase. Any hunting rule where you specify ‘case sensitive’ and uses uppercase letters to search in the **ParentFilename** or **ChildFilename** fields will not return any results. However, the **ParentPath** or **ChildPath** fields are not subject to this normalization process and are stored in the data lake as they are. In this case, it makes sense to use the ‘case sensitive’ or ‘case insensitive’ options according to the analyst’s requirements.

## Validate a Hunting Rule

To prevent situations in which Cytomic Orion must disable analyst-defined hunting rules because of an overload in the cyberattack radar, you must test each rule you create before you store it on the platform. The validation process runs the hunting rule on the SOC clients’ data lake from the last seven days and checks the number of indicators generated. The process generates a color code based on the number of indicators and allows or prevents you from storing the hunting rule on the platform.

You must run the validation process each time you create a hunting rule or edit an existing one.

- After you create or edit a hunting rule, click **Validate**. An internal test is run that checks the number of indicators generated by the rule every day.
- If the hunting rule generates too many indicators, the **Save** button is disabled.
- Edit the hunting rule until it passes the test. Then, click **Save**.

## Color Codes and Ranges of Indicators Found

- **Red**: More than 100 indicators generated at least one day of the week. You must edit the hunting rule and repeat the validation test until the color is orange or green.
- **Orange**: Between 80 and 100 indicators generated at least one day of the week. A warning message appears that indicates that the cyberattack radar could disable the hunting rule over time because it is close to the limit of 100 indicators. Click **Accept and continue** to enable the **Save** button.
- **Green**: Fewer than 80 indicators generated every day of the week. The chances of the cyberattack radar disabling the rule over time are very low. The **Save** button is enabled automatically.


## Edit a Hunting Rule

- To open the wizard, click the name of a hunting rule. You can edit only rules created by SOC technicians. You cannot edit rules created by Cytomic.
- To assign new values to a hunting rule, see [Create a Hunting Rule](#).
- After you finish editing the hunting rule, you must validate it before you save it. See [Validate a Hunting Rule](#).
- Click **Save**. The changes are applied immediately, and the cyberattack radar updates the patterns it searches for in the telemetry data received from devices.



*You cannot save an edited hunting rule that references deprecated tactics, techniques, or sub-techniques. If a MITRE tactic, technique, or sub-technique associated to the hunting rule that you are editing is deprecated, the console highlights it in red. However, you can enable or disable hunting rules that reference deprecated tactics, techniques, or sub-techniques.*

## Delete a Hunting Rule

- Select the checkboxes next to the hunting rules you want to delete.
- Right-click and select **Delete**. Or, in the action bar, select **Delete** .

# Email Notification Rules

A notification rule sends the indicators detected on clients' computers to one or more email accounts. This saves analysts from having to repeatedly access the analysis console to check the status of clients' IT resources.

## Access the Email Notifications List

In the top menu, select **Settings**. In the side panel, select **Hunting rules**. Select the **Email notifications** tab. A list opens that shows all the hunting rules created so far.


## Required Permissions

The user account must have the **Create indicator notification rules** permission assigned and have visibility of the clients that generate the notifications.

To simplify role management, Cytomic Orion includes the **Create hunting rules and notification rules for all clients** permission that enables you to create notification rules regardless of the visibility settings of the account you use. For more information about roles and permissions, see [Understanding Permissions](#) on page 56.

## Create a Notification Rule

Analysts can create notification rules for hunting rules created in the corresponding SOC/MSSP as well as for hunting rules published by Cytomic.

- In the top menu, select **Settings**. In the side panel, select **Hunting rules**. Select the **Email notifications** tab. A page opens that shows all the notification rules created by the analyst.
- Click the **Add notification** button in the upper-right corner of the page. The **Add notification** page opens.
- Complete these fields on the page:
  - **Name**: Name of the notification rule.
  - **Description**: Explanatory text associated with the rule.
  - **Notify indicators detected on the following clients' computers**: Specify the clients that will be affected by the new notification rule:
    - Select **All clients** if the analyst account has the **Create hunting rules and notification rules for all clients** permission assigned (see [Understanding Permissions](#) on page 56).
    - Select **The following clients** and add clients using the  icon if the notification rule affects indicators generated by specific clients. The analyst account must have visibility of these clients (see [Client Visibility Settings](#) on page 51). This field enables you to paste a list of clients separated by a comma “,”.

- **Notify indicators generated by the following hunting rules:** Specify which hunting rules will be monitored.
- Select **All hunting rules** to monitor all the hunting rules created in the SOC.
- Select **All hunting rules with the following risk levels** to monitor hunting rules with a specific risk level.
- Select **The following hunting rules** to monitor specific hunting rules.
- **Notify at the following email addresses:** Specify the email addresses that must receive the email messages with the indicators generated by the hunting rules you want to monitor.
- **Notification limit:** Specify the maximum number of email messages sent in a given period of time.

## Edit a Notification Rule

To edit a notification rule, the analyst must have visibility of all the clients associated with the rule.

Click the notification rule you want to edit. The **Edit notification** page opens. For a description of the fields in a notification rule, see [Create a Notification Rule](#).

## List of Notification Rules

In the top menu, select **Settings**. In the side panel, select **Hunting rules**. Select the **Email notifications** tab. A page opens that shows all the notification rules created by the analyst and their details:


- **Name:** The name of the notification rule.
- **Recipients:** The number of email addresses that receive the notification.
- **Notification limit:** The maximum number of email messages that can be sent in the specified period of time.

## Manage the List of Notification Rules

### Search for, Filter, and Sort Notification Rules

To sort, search for, filter, or group notification rules, see [Tools for Configuring Lists](#) on page 36.

### Delete a Notification Rule

Select the checkbox for each notification rule you want to delete. In the toolbar, click the  icon.

### Information Emailed to Notification Recipients

Field	Description
From	Sender of the email message.



Field	Description
<b>Sent</b>	Date and time the email message was sent.
<b>Subject</b>	“Name of the hunting rule associated with the notification” indicator in client “client name”.
<b>Hunting rule</b>	Name of the hunting rule that generated the indicator and description of the artifacts it monitors on the client’s computer.
<b>Operating system</b>	List of operating systems that generated the indicator. The operating systems are separated by commas.
<b>Indicator date</b>	Date the indicator was generated.
<b>Last event</b>	Date of the last event that led to the generation of the indicator. This date might not be the same as the <b>Indicator date</b> if there was a delay in generating the indicator, for example because of an interruption of the communication between the Cytomic Orion server and the client’s computer.
<b>Occurrences in the last hour</b>	Number of times that Cytomic Orion generated the same indicator in the last hour.
<b>Client ID</b>	Unique identifier of the client the computer where the indicator was detected belongs to.
<b>Computer</b>	Name of the client’s computer where the indicator was detected.
<b>MUID</b>	Unique identifier of the client’s computer where the indicator was detected.
<b>Risk</b>	Severity of the indicator impact: <b>Critical, High risk, Medium risk, Low risk.</b>
<b>MITRE</b>	Category of the technique and tactic associated with the hunting rule, mapped to the MITRE matrix.
<b>Details</b>	Contents of the relevant fields in the event that generated the indicator.

Table 6.3: Description of the fields in the email message sent by the notification rule

## Notifications Related to Changes in the MITRE Framework

Cytomic Orion downloads the MITRE tactic, technique, and sub-technique knowledge base twice a day. If a change is detected in the knowledge base that involves deleting tactics or techniques, Cytomic Orion checks all the hunting rules created so far to make sure that all associated tactics and techniques are valid.

Every Monday, Cytomic Orion users receive an email notification with the hunting rules they need to update if these conditions are met:

- The user account has at least one of these permissions assigned:
  - Manage hunting rules.
  - Create hunting rules and notification rules for all clients.
  - Create indicator notification rules.
- At least one MITRE tactic, technique, or sub-technique associated with a hunting rule is deprecated.



*For more information about the permissions associated with a user account, see [Manage Roles and Permissions](#) on page 53.*

Additionally, when Cytomic Orion downloads an updated MITRE knowledge base and detects a deprecated tactic or technique associated with a hunting rule, it shows a notification with the name of the affected hunting rule at the top of the console for 12 hours.



# Chapter 7

## Manage Investigations

Cytomic Orion implements a repository where it logs and stores everything discovered by SOC technicians during an analysis. This resource is called 'investigation'.

In most cases, investigations are created by Tier 1 analysts who triage indicators. If there is enough evidence to suspect a cyberattack, the analyst creates a new investigation that compiles the indicators related to that attack. This provides Tier 2 technicians with a well-defined study framework and an environment where they can share all the information generated.

All actions carried out by the SOC technicians within the framework of an investigation are stored for future consultation. This enables you to keep track of the use of data derived from investigation-related activities, and monitor access to SOC clients' computers by analysts, along with other actions.

### CHAPTER CONTENTS

---

<b>Investigations List</b> .....	<b>93</b>
Investigations List .....	93
Search for, Sort, and Filter Investigations .....	95
Create an Investigation .....	95
<b>Manually Assign and Remove Indicators from Investigations</b> .....	<b>96</b>
<b>Automatically Assign and Remove Indicators from Investigations</b> .....	<b>98</b>
Create an Assignment Rule .....	98
Edit an Assignment Rule .....	99
Run an Assignment Rule Manually .....	99
Assignment Rules List .....	99
Manage the Assignment Rules List .....	100
<b>Structure of an Investigation</b> .....	<b>100</b>
The Investigation Page .....	101
<b>Entities of Interest Panel</b> .....	<b>107</b>
Manage Entities .....	109
<b>Activity Log Associated with an Investigation</b> .....	<b>117</b>
<b>Remote Operation Log</b> .....	<b>121</b>

# Investigations List

## Access the Investigations List

In the top menu, select **Investigations**. A page opens that shows all investigations created so far, as well as information about them and search and management tools.

For an investigation to appear in the list, the user account used by the analyst to access the web console must have visibility of all the clients that are part of the investigation. Otherwise, the investigation is not visible to the analyst.

## Investigations List

The **Investigations** list page is divided into multiple sections:

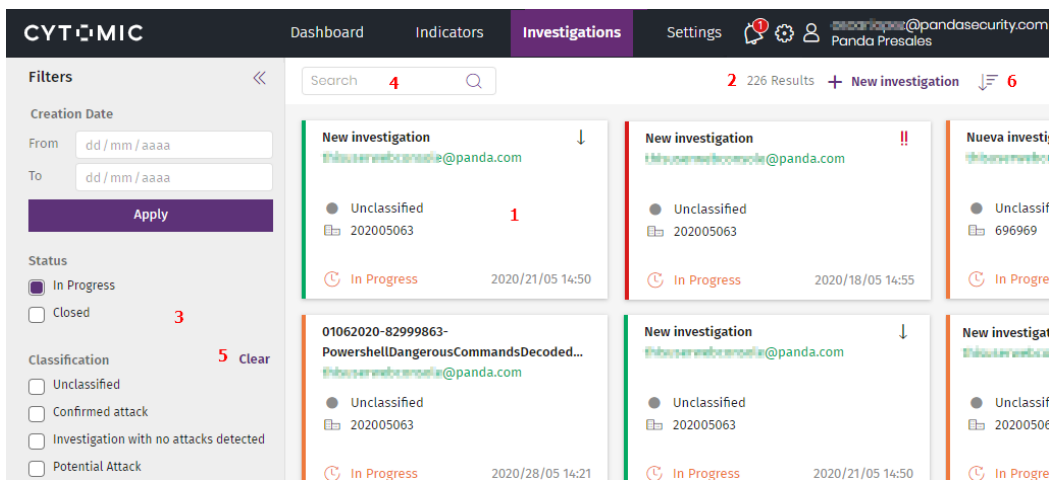


Figure 7.1: Investigations list overview

- **Investigations panel (1)**: Contains a number of tiles, each corresponding to a previously created investigation. For more information about the details shown in each tile, see [Format of an Investigation Tile](#).
- **Filter panel (3)**: Helps analysts find investigations. See [Filter Investigations](#).
- **Search (4)**: Find investigations by their name. See [Search for Investigations](#).
- **Sort list (6)**: Shows the list of investigations according to the sort order you select.
- **New investigation (2)**: Shows the wizard for creating a new investigation. See [Create an Investigation](#)

## Format of an Investigation Tile

For each investigation, a tile is shown with this information:

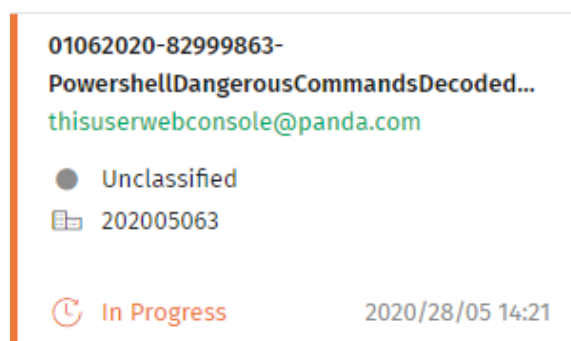


Figure 7.2: Format of an investigation tile

- **Name (1):** Cytomic Orion sets the default name 'New investigation'.
- **User (2):** User account assigned to the investigation. This name appears in green if it matches the user account with which you accessed the console. Otherwise, it appears in gray.
- **Classification (3):** Indicates the investigation classification:
  - **Unclassified** ●: The investigation is pending analysis.
  - **Confirmed attack** ●: The indicator investigation resulted in the detection of an attack.
  - **Investigation without detected attacks** ●: The indicator investigation did not find any attacks.
  - **Potential attack** ●: The indicator investigation is inconclusive, but the indicators have a high probability of being an attack.
- **Clients (4):** Names of the clients assigned to the investigation. If the account with which you accessed the web console does not have sufficient permissions, only the identifiers are shown.
- **Status (5):**
  - **In progress:** The investigation remains open.
  - **Closed:** The investigation has been closed. The tile is grayed out.
- **Start date (6):** Date and time the investigation was created
- **Priority:** The investigation priority is indicated with a color in the border of the tile and an icon in the upper-right corner.
  - **Critical** !!: The risk level of the investigated indicators is very high. The color is red.
  - **High** !: The risk level of the investigated indicators is high. The color is orange.
  - **Medium**: The risk level of the investigated indicators is medium. The color is green.
  - **Low** ↓: The risk level of the investigated indicators is low. The color is gray.

## Search for, Sort, and Filter Investigations

### Search for Investigations

Use the text box (4) at the top of the **Investigations** page to perform searches on the **Name** attribute. Partial searches are valid.


### Filter Investigations

The left panel (3) provides multiple filtering tools:

- **Creation date:** Shows the investigations created within the range you specify with the **From** and **To** controls. Enter the dates and click **Apply** to refresh the list.
- **Status:** Shows investigations according to their status: **In progress** (open) or **Closed** (completed).
- **Classification:** Filters the list according to how the investigation is cataloged (**Unclassified**, **Confirmed attack**, Investigation without detected attacks, **Potential attack**). For more information about an investigation classification, see [Description Sub-panel \(3\)](#).
- **Priority:** Filters the list according to the potential impact the investigated attack could have on the company assets (**Not set**, **Critical**, **High**, **Medium**, **Low**). For more information about an investigation priority, see [Description Sub-panel \(3\)](#).
- **Assigned to:** Shows the investigations assigned to one or more analysts. When you select this filter, you first see the investigations that are assigned to you, then the investigations that are not assigned to any users and, finally, the investigations assigned to other user accounts ordered alphabetically.
- **Created by:** Shows the investigations created by one or more analysts.
- **Clients:** Shows investigations associated with specific clients of the MSSP/MDR vendor.

To reset the filter criteria, click **Clear**.

### Sort Investigations

Click the  icon (6) to open a panel that shows the investigation attributes you can use to sort the list. You can also select whether the order is ascending or descending.

## Create an Investigation

#### To create a new investigation without indicators assigned:

- Click the **New investigation** button in the upper-right corner of the page (2). A dialog box opens that shows a list of the clients that are accessible to the user account that is creating the investigation.
- Select the clients that you want to be a part of the investigation. Click **OK**. A new investigation is created with the clients you selected assigned to it and without indicators.

#### To create an investigation and assign one or more indicators to it:

- See [Manually Assign and Remove Indicators from Investigations](#).

# Manually Assign and Remove Indicators from Investigations

You can assign an indicator only to one investigation. Therefore, you cannot assign an indicator that already has an investigation assigned to another investigation unless you move it or remove it from the first investigation.

You can assign indicators to investigations only if the indicators have not been excluded previously with a deletion rule. See [Delete Indicators Manually](#) on page 70.

## Create a New Investigation That Contains One or More Indicators

- In the top menu, select **Indicators**. Select the check boxes for the indicators with the status **Pending** that you want to assign to the new investigation.
- In the toolbar, select **Investigate indicator**, or right-click the indicator to open its context menu and select the **Investigate indicator** option. A new investigation is created to which the selected indicators are assigned along with an automatically generated name.

Or

- Select the check boxes for the indicators with the status **Pending** that you want to assign to the new investigation.
- Click the context menu icon next to the check box, or right-click the indicator to open a drop-down menu. Select **Investigate indicator**.

## Add Indicators to an Existing Investigation

- In the top menu, select **Indicators**. Select the check boxes for the indicators with the status **Pending** that you want to assign to the new investigation.
- In the toolbar, select **Add to existing investigation**, or right-click the indicator to open its context menu and select the **Add to existing investigation** option.
- A dialog box opens that shows a list of all investigations created and a search box you can use to find investigations according to the content of the columns in the list:
  - **ID**: Internal identifier of the investigation.
  - **Name**: Name of the investigation assigned by the analyst.
  - **Status**: Status of the investigation. See [Format of an Investigation Tile](#).
  - **Classification**: Classification of the investigation. See [Format of an Investigation Tile](#).
  - **Assigned to**: Analysis console user account to which the investigation is assigned.
- Select the check box for the investigation to which you want to assign the indicator. Click **OK**.

Or



- Select the check boxes for the indicators with the status **Pending** that you want to assign to the investigation.
- Click the context menu icon next to the check box, or right-click the indicator to open a drop-down menu. Select **Add to existing investigation**.

After you assign a **Pending** indicator to an investigation, the indicator status changes to **In progress** until it is closed, when the status changes to **Closed**.

## Unassign Indicators from an Investigation

An analyst can unassign indicators from the list of indicators or from the investigation to which the indicator is assigned.

In the **Indicators** panel, select the check boxes for the indicators you want to remove. Click **Remove from this investigation**. You can also select this option by right-clicking an indicator to show its context menu.

## Move Indicators Between Investigations

When you move an indicator, you unassign it from an investigation and assign it to another one. This process is done in a single step:

- In the top menu, select **Investigations**. Select the investigation whose indicator you want to move.
- In the **Indicators** panel, select the checkboxes next to the indicators you want to move. In the toolbar, select **Move to another investigation**. You can also select this option by right-clicking an indicator to show its context menu.
- A dialog box opens that shows a list of all investigations created and a search box you can use to find investigations according to the content of the columns in the list:
  - **ID**: Internal identifier of the investigation.
  - **Name**: Name of the investigation assigned by the analyst.
  - **Status**: Status of the investigation. See [Format of an Investigation Tile](#).
  - **Assigned to**: Analysis console user account to which the investigation is assigned.
- Select the target investigation. Click **OK**.

## Move Indicators from an Existing Investigation to a New Investigation

If an analyst does not want to unassign an indicator before assigning it to a new investigation, they can create a new investigation and move the indicator in one step:

- In the top menu, select **Investigations**. Select the investigation that contains the indicator you want to assign. Alternatively, in the top menu, select **Indicators**. In the side panel, select **In progress**. A page opens that shows all indicators that are assigned to investigations.
- In the **Indicators** panel, select the check boxes for the indicators that you want to add to a new investigation. In the toolbar, select **Add to new investigation**. You can also select this option by right-

clicking an indicator to show its context menu. A new investigation is created and all selected indicators are automatically assigned to it.

## Automatically Assign and Remove Indicators from Investigations

Cytomic Orion enables you to automatically assign indicators to investigations using assignment rules.

### Access the Assignment Rules List

In the top menu, select **Settings**. In the left panel, select **Assignment rules**. A page opens that shows all the assignment rules created so far.


### Required Permissions

To access the assignment rules list, the user account you use must have the **Manage automatic indicator assignment rules** permission assigned to it.

### Create an Assignment Rule

You can create assignment rules to speed up the first stages of the indicator triage process. This way, depending on the characteristics of the indicators generated by the cyberattack radar, the indicators are assigned automatically to the investigations chosen by you.

To create an assignment rule:

- In the top menu, select **Indicators**. In the side panel, select **Pending**. A page opens that shows all the indicators generated by the cyberattack radar that are yet to be assigned to an investigation.
- Select an indicator. In the toolbar, select **Add automatic assignment rule**. You can also right-click the indicator and select **Add automatic assignment rule** in the context menu shown. A dialog box opens. Enter the conditions the indicator must meet for the assignment rule to apply:
  - **Investigation**: Select the investigation that will receive the indicators that satisfy the conditions set in the rule. Click the  icon. A dialog box opens that shows all the investigations created so far. Select an investigation. Click **OK**.
  - **Rule name**: The name of the assignment rule.
  - **Description**: Explanatory text associated with the assignment rule.
  - **Client ID**: The rule will apply to the indicators detected on the networks of the clients in the list. Your account must have visibility of the clients you add. See [Manage Roles and Permissions](#) on page 53.
  - **Hunting rule**: The rule will apply to the indicators generated by the cyberattack radar that were detected with the hunting rule you specify.

- **MUID:** The rule will apply to the indicators detected on the user computers whose IDs you specify.
- **Machine name:** The rule will apply to the indicators detected on the user computers whose names you specify.
- **Details:** Specify the content of the **Details** field for the indicators you want to assign. You can determine the exact content of the field with the **Equals** option, or flexibly with a regular expression by using the **RegEx** option. For more information, see [Regular Expressions](#) on page 256.
- **Run this rule automatically:** The rule you create will apply not only to the new indicators generated in the future, but also to old indicators generated seven days before the rule was created.

## Edit an Assignment Rule

To edit an assignment rule, your account must have visibility of all the clients that are affected by the rule you want to edit. See [Manage Roles and Permissions](#) on page 53.

- In the top menu, select **Settings**. In the side panel, select **Assignment rules**. A page opens that shows all the assignment rules created so far.
- Click an assignment rule. A page opens that shows the rule properties.
- Edit the assignment rule properties. Click **Save**.

After the assignment rule has been edited, it begins to apply to all new indicators that are generated. The edited assignment rule will not apply to old indicators. To apply an edited assignment rule to old indicators, see [Run an Assignment Rule Manually](#).

## Run an Assignment Rule Manually

To apply an assignment rule to indicators generated in the last seven days:

- In the top menu, select **Settings**. In the side panel, select **Assignment rules**. A page opens that shows all the assignment rules created so far.
- Select the checkboxes for the assignment rules you want to run. A toolbar appears.
- Select **Run rule**. The selected rules apply to the indicators generated in the last seven days. The indicators move to the relevant investigations.

## Assignment Rules List

This list contains the assignment rules created so far.

To access the assignment rules list, select **Settings** in the top menu. In the side panel, select **Assignment rules**. The list shows these fields:

Field	Description
<b>Name</b>	Name of the assignment rule.
<b>Creation date</b>	Date the assignment rule was created.
<b>Modification date</b>	Date the assignment rule was last modified.
<b>Description</b>	Description of the assignment rule.
<b>Hunting rule</b>	Hunting rule associated with the assignment rule.
<b>Investigation</b>	Name of the investigation to which the indicators that meet the conditions set in the assignment rule will move.


Table 7.1: Fields in the Assignment Rules list

## Manage the Assignment Rules List

### Search for, Filter, and Sort Assignment Rules

To sort, search for, filter, or group assignment rules, see [Tools for Configuring Lists](#) on page 36.

### Delete an Assignment Rule

Select the checkboxes for the assignment rules you want to delete. In the toolbar, click the  icon.

## Structure of an Investigation

### Access an Investigation

- In the top menu, select **Investigations**. A page opens that shows all investigations created so far.
- Use the filtering and search tools to find a specific investigation
- Select an investigation. A page opens that shows the investigation information.

### Access the Investigation Associated with an Indicator

To quickly find the investigation assigned to a specific indicator, follow these steps:

- In the top menu, select **Indicators**. Select an indicator that has the status **In Progress** or **Closed**
- Click the context menu icon to the right of the indicator checkbox, or right-click the indicator. A context menu opens.
- Select **Go to investigation**. The **Investigation** page opens filtered to show the investigation associated with the selected indicator.

## The Investigation Page

In the top menu, select **Investigations**. A page opens and shows all investigations created so far. In the list, select an investigation. The **Investigation** page opens. This page shows a number of sub-panels and a toolbar.

### Investigation Name (1)

To edit the name of an investigation, click it.

### Tab Bar (2)

Add a persistent analysis tool to the investigation. These tools are kept even if you close the investigation page. Click the **+** icon to open a drop-down menu with the available tools:

- **Advanced SQL query**: Create searches using the SQL language on the data lake stored in Cytomic Orion and collected through the monitoring of the processes run on clients' computers. For more information about advanced queries and the query wizard, see **Investigate the Event Flow** on page 144.

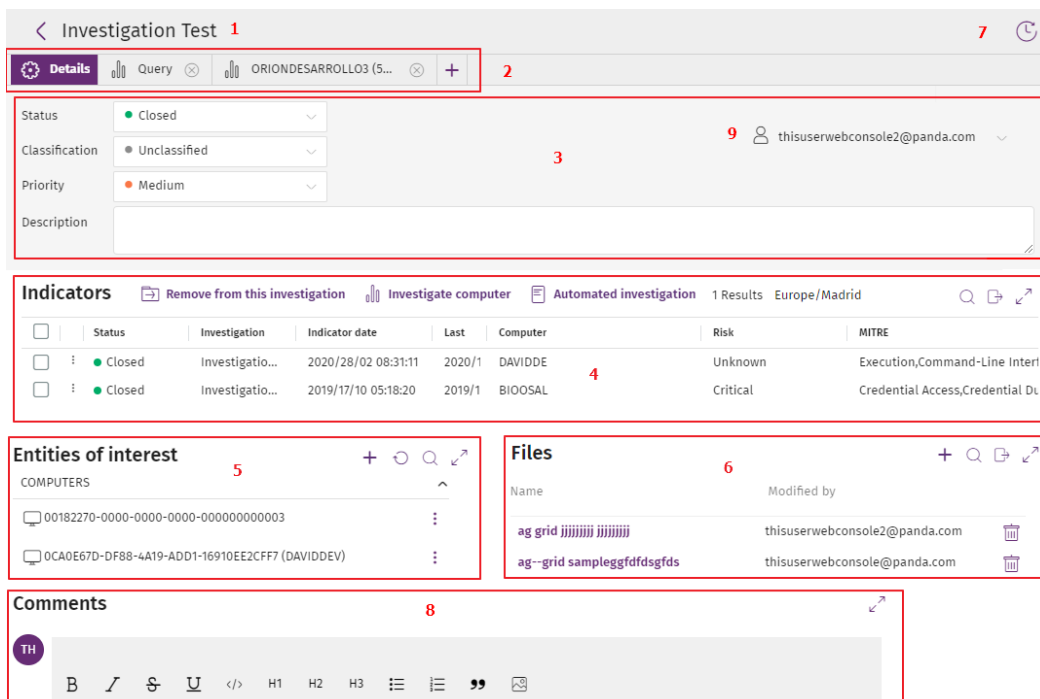


Figure 7.3: Investigation overview

- **Wizard-guided queries:** Create searches on the data lake stored in Cytomic Orion using a wizard. You do not need knowledge of the SQL language. For more information about advanced queries and the query wizard, see [Investigate the Event Flow](#) on page 144.
- **OSQuery query:** Build SQL statements to get information about the hardware, software, running processes, file system, registry, etc. of computers. Analysts can use this information in their investigations or to respond to incidents. See [IT Infrastructure Investigation with OSQuery](#) on page 230.
- **Computer investigation:** Open the investigation console for an in-depth analysis of the events generated on a specific computer on a specific day. The console shows all events gathered from all the processes run on the specified computer on the specified day, along with their parent-child relationships. For more information about the investigation console, see [Indicator Analysis Using the Investigation Console](#) on page 172.
- **Manual investigation:** Add a new blank notebook to the investigation notebooks panel (4). The notebook editor opens with the Quick Answers module. For more information about notebooks in Cytomic Orion, see [Investigations with Notebooks](#) on page 204.
- **Automated investigation:** Opens a list that shows the templates available to the analyst to create a new notebook. For more information about notebooks in Cytomic Orion, see [Investigations with Notebooks](#) on page 204.
- **Graphs:** View the execution flow of the processes run in the client's IT infrastructure. Graphs use nodes and arrows to provide a graphical representation of the entities involved in the events stored in the data lake and their relationships. See [Graphs](#) on page 188.

## Sort and Group Tabs in Panels

If an analyst needs to view two tabs/tools simultaneously, they can split the investigation page into two and group and arrange the tabs they need on each side of the page:

- Add all tabs you need to an ongoing investigation. See [Tab Bar \(2\)](#).
- To sort the tabs, click one of them. Drag it to the right or left and drop it.
- To create a new panel and split the investigation page into two, click a tab and move it to the right side of the page. The area of the page where the new panel is to be created is highlighted. Drop the tab. A new panel is created that contains the tab you dragged.
- You can move tabs from one panel to another and create new tabs in each panel independently.
- To change the size of the panels, click the vertical bar that separates them and move it to the right or left.
- If you close all tabs in a panel, the panel disappears from the **Investigations** page.

## Description Sub-panel (3)

Set the investigation status through a series of attributes:

Attribute	Values
<b>Status</b>	<p>Indicates whether the indicators are being investigated by technicians or have already been analyzed.</p> <ul style="list-style-type: none"> <li>• <b>Closed:</b> The investigation has been completed. The status of the assigned indicators is <b>Closed</b>.</li> <li>• <b>In progress:</b> The investigation remains open. The status of the assigned indicators is <b>In progress</b>.</li> </ul>
<b>Classification</b>	<p>Indicates the investigation classification:</p> <ul style="list-style-type: none"> <li>• <b>Unclassified:</b> The investigation is pending analysis.</li> <li>• <b>Confirmed attack:</b> The indicator investigation resulted in the detection of an attack.</li> <li>• <b>Investigation without detected attacks:</b> The indicator investigation did not find any attacks.</li> <li>• <b>Potential attack:</b> The indicator investigation is inconclusive, but the indicators have a high probability of being an attack.</li> </ul>
<b>Priority</b>	<p>Indicates the impact that the potential attack investigated could have on the company assets:</p> <ul style="list-style-type: none"> <li>• <b>Not set:</b> The impact has not yet been determined.</li> <li>• <b>Critical:</b> The risk level of the investigated indicators is very high. The color code is red.</li> <li>• <b>High:</b> The risk level of the investigated indicators is high. The color code is orange.</li> <li>• <b>Medium:</b> The risk level of the investigated indicators is medium. The color code is green.</li> <li>• <b>Low:</b> The risk level of the investigated indicators is low. The color code is gray.</li> </ul>
<b>Description</b>	<p>A text box in which you can enter a detailed description of the investigation status.</p>




Table 7.2: Attributes for the description sub-panel

## Indicators Sub-panel (4)

This panel shows a list of the indicators assigned to the investigation. For more information about how to sort, filter, and group the indicators assigned to an investigation, see [Tools for Configuring Lists](#) on page 36

. For more information about the meaning of the fields in the **Indicators** area, see [Indicators List](#) on page 66

The **Indicators** sub-panel provides these tools:

- **Results:** Specifies the number of indicators assigned to the investigation.
- **Time zone:** Enables you to set the time zone for the **Indicator date** and **Last** event fields. The time zone you set also affects the content of searches.
- **Search** : Click the icon to show a text box where you can enter the search terms. You can type only a partial string. Searches are performed on the content of all of the indicator fields.
- **Export** : Save the content of the sub-panel to a CSV file. The columns in the file correspond to the columns in the list.
- **Indicator information:** Maximize the sub-panel and open the **Details** right panel. This panel has two tabs:
  - **Details:** Shows fields with information about the selected indicator.
  - **MITRE:** Shows details of the MITRE tactic and technique associated with the hunting rule that generated the indicator.
- **Maximize** : Expands the sub-panel to full screen.

Select an indicator to show a toolbar with these options:

Option	Description
<b>Remove from this investigation</b>	Removes the indicator from the investigation. The indicator status changes to <b>Pending</b> .
<b>Investigate computer</b>	Opens the investigation console for the computer associated with the indicator to show the events logged on the specified date. See <a href="#">Indicator Analysis Using the Investigation Console</a> on page 172.
<b>Automated investigation</b>	Shows a lists of all notebook templates created. When the analyst opens a template, Cytomic Orion automatically populates all compatible parameters in the template with the selected indicator fields. See <a href="#">Investigations with Notebooks</a> on page 204.
<b>Add entity of interest</b>	Select an entity to show in the <b>Entities of interest</b> sub-panel in the associated investigation to rapidly access the information. See <a href="#">Entities of Interest Panel</a> .
<b>Computer details</b>	Shows information about the computer. See <a href="#">Computer Details</a> .



Option	Description
<b>Add automatic deletion rule</b>	<p>This option appears only when you select a single indicator.</p> <p>For more information about indicator filtering, see <a href="#">Delete Indicators Manually</a> on page 70.</p>

Table 7.3: Indicator toolbar

You can also access these options through the context menu that appears when you right-click an indicator.


## Entities of Interest Sub-panel (5)

This panel shows a list of items selected by the analyst as important during the course of an investigation.


For more information, see [Entities of Interest Panel](#).

## Files Sub-panel (6)




This panel shows a list of the notebooks that Tier 1 and Tier 2 analysts generated using the **Automated investigation** and **Manual investigation** tools. For each notebook, this information appears:

- **Name:** The notebook name.
- **Created:** The date the notebook was created.
- **Modified:** The date the notebook was last modified.
- **Modified by:** Console user account that last modified the notebook.
- **Delete** : Deletes the associated notebook.

Additionally, the **Files** sub-panel has a toolbar with these options:

- **Create notebook** : Opens a drop-down menu from which you can select the notebook you want to create:
  - **OSQuery query:** Adds a new notebook to generate an SQL statement to get information about the hardware, software, running processes, file system, registry, etc. of computers. See [IT Infrastructure Investigation with OSQuery](#) on page 230.
  - **Manual investigation:** Adds a new blank notebook to the investigation **Files** panel (6). The left panel shows the notebook editor with the Quick Answers module. For more information about notebooks in Cytomic Orion, see [Investigations with Notebooks](#) on page 204.
  - **Automated investigation:** Shows a list of templates available to the analyst to create a new notebook. For more information about notebooks in Cytomic Orion, see [Investigations with Notebooks](#) on page 204.
  - **Graphs:** Adds a notebook that provides a graphical representation of the telemetry flow generated by the client's IT infrastructure and stored in the data lake. See [Graphs](#) on page 188.





- **Search** : Click the icon to show a text box where you can enter the search terms. Searches are performed on the content of all the fields in the notebook list. You can type only a partial string.
- **Export** : Save the content of the sub-panel to a CSV file. The columns in the file correspond to the columns in the list.
- **Maximize** : Expands the sub-panel to full screen.

## Activity Log (7)

This section logs the actions taken by the analyst, specifying the user account used, the type of action, and the item that received the action. See [Activity Log Associated with an Investigation](#).

## Comments (8)

Analysts can enter comments and additional information about the status of an investigation to share with other SOC analysts. You can enter rich text and images by using the toolbar below the panel. You can also edit and delete comments with the  and  icons that appear in the upper-right corner of the panel when you point to a previously saved comment.

## Assign an Investigation to an Analyst (9)

When an analyst creates an investigation, it is assigned to the analyst. Any analyst with access to the investigation can assign it to another technician, provided the technician has visibility of all the clients associated with the investigation.

When you click the name of the analyst assigned to an investigation, a drop-down menu opens that shows a list of all user accounts that have visibility of the clients associated with the investigation. When you select a new analyst, these actions are performed:

- The new owner of the investigation receives an email message that contains the information described in table [Attributes for the description sub-panel](#), provided the option **Notify me each time an investigation is assigned to me** is selected (top menu **Settings**, side panel **My preferences**).
- The change of ownership is logged in the **Activity log**. See [Activity Log Associated with an Investigation](#).

To leave the investigation unassigned, click the name of the analyst and press the delete key in the keyboard. The investigation is unassigned and an entry is created in the **Activity log**.

## Persistence of Changes Made and Collaboration

Option	Description
<b>Investigate computer</b>	Opens the investigation console for the computer associated with the indicator to show the events logged on the specified date. See <a href="#">Indicator Analysis Using the Investigation Console</a> on page 172.
<b>Automated investigation</b>	Shows a lists of all notebook templates created. When the analyst opens a template, Cytomic Orion automatically populates all compatible parameters in the template with the selected indicator fields. See <a href="#">Investigations with Notebooks</a> on page 204.
<b>Add entity of interest</b>	Select an entity to show in the <b>Entities of interest</b> sub-panel in the associated investigation to rapidly access the information. See <a href="#">Entities of Interest Panel</a> .
<b>Computer details</b>	Shows information about the computer. See <a href="#">Computer Details</a> .
<b>Add automatic deletion rule</b>	This option appears only when you select a single indicator. For more information about indicator filtering, see <a href="#">Delete Indicators Manually</a> on page 70.

Table 7.4: Context menu for an indicator

An investigation is a container that stores all the evidence studied and collected by analysts. All changes you make to an investigation (edit or add notebooks, add analysis tools, configure the list of indicators, etc.) are kept between sessions without the need to explicitly save the investigation status.

## Entities of Interest Panel

The **Entities of interest** sub-panel of an investigation stores the entities that the analyst has observed and considered important, or relevant to annotate for future consultation. That is why this resource is used as a repository for items that can be accessed quickly, which also acts as a history showing the direction that the investigation is taking.

### Access the Entities of Interest Panel

In the top menu, select **Investigations**. Select an investigation. Select the **Details** tab. Find the **Entities of interest** sub-panel at the bottom left of the page.

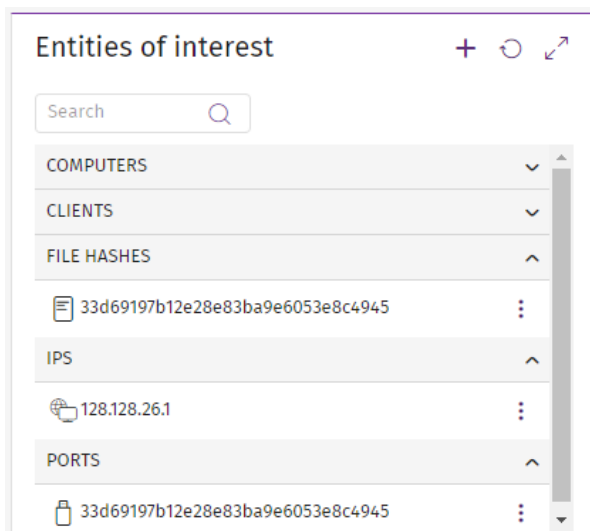


Figure 7.4: Entities of interest panel

The entities in the panel are grouped by type. Click a group title to show or hide the group entities.

### Types of Entities of Interest

Each entity of interest has a type associated with it, which you select when you mark an entity as an entity of interest:

Name	Description
<b>Computer</b>	MUID of the investigated computer.
<b>Client</b>	Name and identifier of the client to which the investigated computer belongs. If the account with which you are accessing the web console does not have sufficient permissions, only the identifier is shown.
<b>User</b>	User account that ran the program on the investigated computer.
<b>File hash</b>	Hash of the file stored on the investigated computer.
<b>IP</b>	IP address of the investigated computer.
<b>Port</b>	Port used by the process run on the investigated computer.
<b>Domain</b>	Domain belonging to the communication established from/to the investigated computer.
<b>URL</b>	Web address accessed from the investigated computer.

Name	Description
File path	Path to the file in the investigated computer file system.
File name	Hash of the file stored on the investigated computer.


Table 7.5: Types of entities of interest

The data type you assign to an entity determines the actions that Cytomic Orion can take on the entity. Therefore, it is very important that analysts assign the entity type correctly.

## Manage Entities

An entity of interest must be associated with a specific investigation. In most cases, the person responsible for making this association is the technicians when, in the course of an investigation, they find items they want to save for later consultation. Moreover, Cytomic Orion can also automatically add entities of interest during an investigation.

The **Entities of interest** sub-panel enables you to take action on entities, or delete them. To take action on an entity, follow these steps:


- In the **Entities of interest** panel, expand the group to which the entity belongs.
- Click the  icon associated with the entity to open the entity context menu. Select an action. The actions shown vary depending on the type of entity. Some actions are related to incident remediation tasks.

## Add Entities Automatically


Cytomic Orion automatically adds entities that are being analyzed to the **Entities of interest** panel. The situations in which an entity is automatically added to an investigation are these:

- **When an analyst adds an indicator to an investigation:** Computer ID (MUID) and client ID.
- **When an analyst opens an investigation console:** File hash (MD5) and/or computer ID (MUID).

## Add Entities in a Guided Way

Analysts can add entities to the **Entities of interest** sub-panel through the option  **Add entity of interest**.


This option is available for these elements in the analysis console, when you right-click the element to open its context menu:

- The indicators assigned to an investigation.
- Click the  icon associated with an indicator. For more information, see chapter [Indicators and Hunting Rules](#) on page 64.
- The results of an SQL advanced query. For more information, see chapter [Investigate the Event Flow](#) on page 144.


- The computer events shown in the investigation console. For more information, see chapter [Indicator Analysis Using the Investigation Console](#) on page 172.

Cytomic Orion determines the type of entity of interest that is added depending on the field where the analysts clicks to show the context menu. If, for example, the analyst right-clicks the **Computer** field of an indicator, Cytomic Orion adds the entity with the type **Computer** automatically assigned to it, although the analyst can later change it by choosing a new type from the relevant drop-down menu.

To add an entity to the **Entities of interest** sub-panel, follow these steps:


- Find the piece of data you want to add. Right-click it to open its context menu.
- Select  **Add entity of interest**. A dialog box opens where you can select the entity type.
- Click **OK**. The entity is immediately added to the **Entities of interest** sub-panel and Cytomic Orion enables you to take action on it.

## Add Entities in a Non-Guided Way

To add any type of entity, click the  icon in the **Entities of interest** sub-panel. A dialog box opens where you can select the type of entity you want to add. In the **Entity** text box, enter the entity value. The console analyzes the data you have entered to verify that it conforms to the expected format according to the type of entity selected.

To speed up the entity configuration process, the **Entity** text box filters from all available entities. Enter the entity name letter by letter. A drop-down menu is shown that displays the entities that match the characters you entered.

## Deleting an Entity of Interest

- In the top menu, select **Investigations**. Select the investigation that contains the entity of interest that you want to delete. In the tab bar, select **Details**. All panels associated with the ongoing investigation are shown.
- In the **Entities of interest** panel, click the context menu icon for the entity of interest that you want to delete. In the context menu, select  **Delete from the list of entities of interest**.
- Click **OK**. The entity is immediately deleted.

## Actions Available for Entities of Interest

The entities of interest you have added to the console have a context menu associated that makes it easier to take action on them or navigate the web console.





Action	Description	Available for these types of entities
<b>Copy to clipboard</b>	Copies the entity information to the computer clipboard so that you can use it somewhere else in the analysis console.	All

Action	Description	Available for these types of entities
<b>Delete from the list of entities of interest</b>	Deletes the entity from the list of entities of interest associated with the investigation.	All
<b>Investigate computer</b>	Opens a panel that shows the investigation console for the computer MUID to display the events occurred on the computer on the selected date. For more information see <a href="#">Indicator Analysis Using the Investigation Console</a> on page 172.	Computer
<b>Investigation notebook</b>	Opens a list of all notebook templates to generate a new notebook taking the computer MUID as parameter. For more information, see <a href="#">Investigations with Notebooks</a> on page 204.	Computer
<b>Isolate computer</b>	Isolates the computer, preventing it from communicating with the network. For more information, see <a href="#">Response Tools</a> on page 236.	Computer
<b>Stop isolating computer</b>	Restores communications on previously isolated computer. For more information, see <a href="#">Manage Investigations</a> .	Computer
<b>Remote access to computer</b>	Provides remote access to a computer management resources. For more information, see <a href="#">Response Tools</a> on page 236.	Computer
<b>Restart computer</b>	Starts the computer reboot sequence. For more information, see <a href="#">Response Tools</a> on page 236.	Computer
<b>Computer details</b>	Opens a dialog box that shows detailed information about the device. For more information about the meaning of the fields, see <a href="#">Computer Details</a> .	Computer

Table 7.6: Available actions based on the entity

## Tools in the Entities of Interest Panel

The **Entities of interest** panel provides these tools at the top:

- **Add entity of interest** : See [Add Entities in a Non-Guided Way](#).
- **Refresh panel** : Requests the list of entities of interest from the server and loads it in the sub-panel.
- **Search** : Click the icon to show a text box where you can enter the search terms. You can type only a partial string. Searches are performed on the content of all the fields in the entity of Interest.
- **Maximize** : Expands the sub-panel to full screen.

## Computer Details

Section	Field	Description
<b>General</b>		
	IP addresses	List of all the IP addresses (primary addresses and aliases) of the computer.
	Active directory path	Path to the computer in the company's Active Directory.
	Group	Group in the Cytomic EDR or Cytomic EPDR group tree to which the computer belongs. To change the computer group, click <b>Change</b> .
	Operating system	Name of the operating system installed on the computer.
<b>Client info</b>		
	Client ID	Identifier of the client to which the computer belongs in the Cytomic Orion systems.
	Client name	Name of the client.
	Creation date	Date the client was created in the Cytomic systems.
<b>Computer</b>		
	Name	Name of the computer on the client's network.
	Type	Computer type:



Section	Field	Description
		<ul style="list-style-type: none"> <li>• Desktop</li> <li>• Server</li> <li>• Laptop</li> <li>• Mobile device (smartphone, tablet, etc.)</li> </ul>
	Platform ID	<p>Type of operating system installed on the computer.</p> <ul style="list-style-type: none"> <li>• Windows</li> <li>• Linux</li> <li>• macOS</li> <li>• Undefined</li> </ul>
	MUID	Unique identifier of the computer in Cytomic Orion.
	IP addresses	List of all the IP addresses (primary addresses and aliases) of the computer.
	Physical addresses (MAC)	Physical address of the network cards installed on the computer.
	Domain	Windows domain the computer belongs to. This is empty if it does not belong to a domain.
	Active directory path	Path to the computer in the organizational unit hierarchy.
	Group	Group in the Cytomic EDR or Cytomic EPDR group tree to which the computer belongs. To change the computer group, click <b>Change</b> .
	Operating system	Name of the operating system installed on the computer.
	Virtual machine	Indicates whether the computer is physical or virtual.
	Is a non-persistent	Indicates whether the operating system of the virtual machine resides on a storage device that persists between restarts, or

Section	Field	Description
		reverts to its original state instead.
	Licenses	Cytomic product licenses installed on the computer.
	License status	<ul style="list-style-type: none"> <li>Assigned</li> <li>Not assigned</li> </ul>
	Agent version	Internal version of the Cytomic agent installed on the computer.
	Agent language	Language in which Cytomic EDR or Cytomic EPDR shows the local console and pop-up messages.
	Isolation	Shows the isolation status of the computer: <ul style="list-style-type: none"> <li>Isolated</li> <li>Isolating</li> <li>Stop isolating</li> <li>Not isolated</li> </ul>
	Reboot requested	The computer is pending restart.
	Creation date	Date the agent was installed on the user computer and the computer was registered in the Cytomic cloud.
	Last connection	Date when the client software last connected to the Cytomic cloud. The communications agent connects to the cloud at least every four hours.
	Last boot time	Date when the computer was last booted.
<b>Security</b>		
	Advanced protection	Indicates whether the Cytomic EDR or Cytomic EPDR advanced protection module is enabled on the user computer and the mode it is configured in (Audit, Hardening, or Lock).
	File antivirus	Indicates whether the Cytomic EDR or Cytomic EPDR file protection module is enabled on the user computer.

Section	Field	Description
	Mail antivirus	Indicates whether the protection for the protocols used to send and receive email is enabled on the user computer.
	Web browsing antivirus	Indicates whether the protection against malware downloaded from web pages is enabled on the user computer.
	Firewall	Indicates whether the module for protecting against network traffic generated by applications on the user computer is enabled.
	Device control	Indicates whether the module is enabled for protecting against infections through external storage devices or devices that allow users computers to connect to the Internet bypassing the organization communications infrastructure (USB modems and others devices).
	Exchange server antivirus	Indicates whether the module for protecting against viruses received at Microsoft Exchange servers is enabled.
	Exchange server antispam	Indicates whether the module for protecting against spam received at Microsoft Exchange servers is enabled.
	Exchange server content filter	Indicates whether the protection is enabled for email messages received at Microsoft Exchange servers that could have attachments with dangerous extensions.
	Web access control	Indicates whether the module is enabled that protects against users accessing web content not permitted by the administrator.
	Patch management	Indicates whether the patch and update module for Windows operating systems and third-party applications is enabled on the user computer.
	Data control	Indicates whether the module for tracking personal data is enabled.
	Antitheft	Indicates whether the module is enabled that mitigates the exposure of data in the event of theft of an Android device.

Section	Field	Description
	Encryption	Indicates whether the file encryption module is enabled on the user computer.
	Data search control status	Indicates whether the computer has a Cytomic Data Watch settings profile assigned that allows it to receive file searches and report their results.
<b>Protection</b>		
	Protection update status	Indicates whether the protection module installed on the computer is the latest version released by Cytomic. <ul style="list-style-type: none"> <li>• Updated</li> <li>• Not updated (seven days without updating since last release)</li> <li>• Pending restart.</li> </ul>
	Protection version	Version of the Cytomic EDR or Cytomic EPDR protection module installed on the user computer.
	Knowledge update status	Indicates whether the signature file installed on the user computer is the latest version released by Cytomic. <ul style="list-style-type: none"> <li>• Updated</li> <li>• Not updated (three days without updating since last release)</li> </ul>
	Knowledge update date	Date when the signature file was last downloaded to the user computer.
<b>Data protection</b>		
	Personal data monitoring	Indicates whether you can see files on storage devices on the client's computer to generate a database on the computer to speed up content retrieval.
	Personal data monitoring	Indicates whether extensions for accessing Microsoft Office suite files are installed on the client's computer.
	Index status	Indicates the status of the Cytomic Data Watch indexing engine. <ul style="list-style-type: none"> <li>• Not indexed</li> </ul>


Section	Field	Description
		<ul style="list-style-type: none"> <li>Indexed</li> <li>Indexed (text only)</li> <li>Indexed (all content)</li> <li>Indexing</li> </ul>

Table 7.7: Computer details fields

## Activity Log Associated with an Investigation

Every action taken by SOC technicians in the context of an investigation is logged along with additional information that helps to determine its type and source. This information enables you to identify the security impact the actions performed by analysts on clients' computers and infrastructure can have.

### Access the Activity Log Associated with an Investigation

In the top menu, select **Investigations**. Select an investigation from the list. Click the  icon (**Activity log**) in the upper-right corner of the page. A page opens that shows the list of actions that SOC technicians took as part of the investigation, along with multiple tools that enable you to search and filter information.

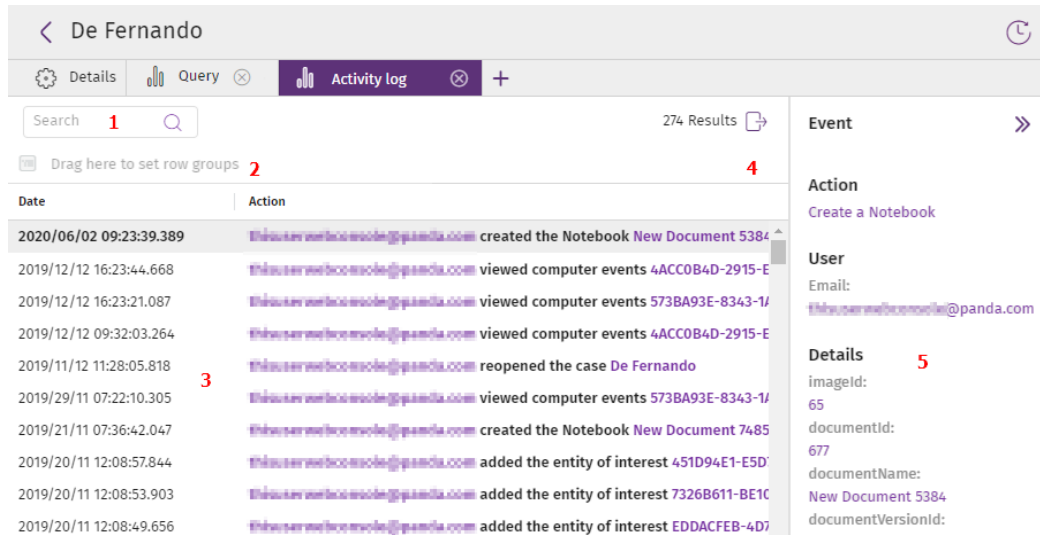


Figure 7.5: Activity log associated with an investigation

- **Search tool (1):** Searches the contents of all columns in the list to filter information. You can type only a partial string.
- **Grouping tool (2):** Groups items in the list by the column you choose. For more information about the grouping tool, see [Filter Tools](#) on page 41.
- **Export (4):** Exports the contents of the list to a CSV file.

- **Side panel (5):** Shows extended information about the items you select in the list.
- **Central panel (3):** Shows a list of actions that match the search criteria you entered. The following table describes the columns included in the list:

Field	Description
<b>Date</b>	Date of the logged action.
<b>Action</b>	Logged action along with the user account that took it and additional information. For more information, see <a href="#">Activity Log Associated with an Investigation</a> .
<b>User</b>	Name of the account that took the action. This column is not shown by default.
<b>Action type</b>	Type of logged action. This column is not shown by default.

Table 7.8: Fields in the Activity Log list

## Actions Logged in Cytomic Orion

Action	Description
<b>Create an investigation</b>	The console user assigned one or more indicators to a new investigation.
<b>Rename an investigation</b>	The console user changed the name of an investigation.
<b>Change an investigation classification</b>	The console user changed the classification of an investigation.
<b>Change an investigation priority</b>	The console user changed the priority of an investigation.
<b>Add or delete clients from an investigation</b>	The console user changed the client-type entities of interest assigned to an investigation.
<b>Close an investigation</b>	The console user closed an investigation.

Action	Description
<b>Reopen an investigation</b>	The console user reassigned the status <b>In progress</b> or <b>Pending</b> to an indicator assigned to an investigation.
<b>Add indicators to an investigation</b>	The console user assigned an indicator to an existing investigation.
<b>Remove indicators from an investigation</b>	The console user unassigned an indicator from an investigation.
<b>Assign an investigation to a user</b>	The console user changed the user assigned to an investigation.
<b>Unassign an investigation</b>	The console user removed the user assigned to an investigation.
<b>Run a query</b>	The console user ran an SQL query.
<b>Cancel a query</b>	The console user stopped the execution of an SQL query.
<b>Query result</b>	An SQL query finished executing.
<b>Query statistics</b>	Shows data about the executed SQL query (full SQL statement, number of bytes read, etc.). You can use this field to determine the Cytomic Orion data usage.
<b>Query error</b>	Execution of an SQL query completed with errors.
<b>Investigate computer</b>	The console user opened an investigation from the MUID of a client's computer.
<b>Investigate file</b>	The console user opened an investigation from the MD5 of a file.
<b>Investigate computer</b>	The console user opened an investigation from the name of a client's computer.
<b>Create a notebook</b>	The console user started an analysis by creating a notebook.

Action	Description
<b>Update a notebook</b>	The console user worked on an analysis by editing a notebook.
<b>View a notebook</b>	The console user opened a notebook to view it.
<b>Rename a notebook</b>	The console user changed the name of a notebook.
<b>Delete a notebook</b>	The console user deleted a notebook.
<b>Convert notebook to PDF</b>	The console user generated a PDF report from a notebook results.
<b>Run a notebook</b>	The console user obtained the results of an investigation by running a notebook.
<b>Start remote access to a computer</b>	Cytomic Orion retrieved, from the platform, the credentials required for the analyst who requested remote access to the investigated computer to be able to access it and use the remediation tools. To view the commands run by the analyst, see <a href="#">Remote Operation Log</a> .
<b>Attempt to start remote access to a computer</b>	Cytomic Orion tried to retrieve, from the platform, the credentials required to remotely access the investigated computer, but the process failed.
<b>Request to restart computers</b>	The console user started the process to remotely restart a computer.
<b>Request to isolate computers</b>	The console user started the process to isolate a computer.
<b>Request to stop isolating computers</b>	The console user started the process to deisolate a computer.
<b>Add entities of interest</b>	The console user added an entity of interest to an investigation.




Action	Description
Delete entities of interest	The console user removed an entity of interest from an investigation.

Table 7.9: Fields in the Activity Log list

## Remote Operation Log

Commands run by analysts when they access a computer remotely are logged separately and in a more detailed way.

### Access the Remote Operation Log

- In the top menu, select **Investigations**. Select an investigation from the list. Click the  icon (**Activity log**) in the upper-right corner of the page. A page opens that shows the list of actions that SOC technicians took as part of the investigation.
- In the central panel (3), select a **Start remote access to a computer**-type item. A side panel opens that shows details of the selected item (5).
- In the side panel (5), find the **sessionId** attribute. Click its content. The **Remote session details** page opens.

Field	Description
Session ID	Session ID assigned by Cytomic Orion.
Date	Date the remote access started.
IP address	IP address of the accessed computer.
Category	<ul style="list-style-type: none"> <li><b>Files:</b> File-related operation.</li> <li><b>Processes:</b> Process-related operation.</li> <li><b>Services:</b> Service-related operation.</li> <li><b>Terminal:</b> Remote command line.</li> <li><b>Connection:</b> Remote connection status.</li> </ul>
Action	Action taken on the remote computer and logged by Cytomic Orion.

Table 7.10: Fields in the Remote Session Details list

# Chapter 8

## Activity Visibility in Cytomic Orion

Cytomic Orion shows a summary of the main activity logged in the console through graphical resources (tiles). A dashboard groups all tiles that provide information about a specific area. Analysts and SOC managers use the dashboards to see, at a glance, the security status of clients' networks and the progress of planned analyses.

The available dashboards are:

- **Investigations and indicators:** See [Investigations and Indicators Dashboard](#).
- **MITRE:** See [MITRE Dashboard](#).
- **Data usage:** see [Data Usage](#).

### CHAPTER CONTENTS

---

<b>Investigations and Indicators Dashboard</b> .....	<b>123</b>
<b>MITRE Dashboard</b> .....	<b>128</b>
<b>Data Usage</b> .....	<b>129</b>
Amount of Data Assigned and Usage Monitoring Resources .....	130
Notebook Data consumed in advanced queries .....	130
Data Usage Dashboard .....	132
Data Usage by User Dashboard .....	133
Data Usage by Query Dashboard .....	135
Data Usage by Client Dashboard .....	137
Assigned Data Dashboard .....	139
Usage Notification Email .....	141

## Investigations and Indicators Dashboard

This dashboard shows information about the detected indicators, the status of the created investigations, the computers and clients most likely to suffer a cyberattack, and the hunting rules that generated most indicators on the platform.

To access the dashboard:

- In the top menu, select **Dashboard**. In the side panel, select **Investigations and indicators**. A page opens that shows the dashboard tiles.
- Select a time period for the data shown in the tiles:
  - Last 24 hours
  - Last 7 days
  - Last month
  - Last year

### Open Investigations

This tile shows all the investigations that have the status **In Progress**. These investigations are divided into two groups: investigations opened by the user account that accessed the dashboard and investigations opened by other user accounts.

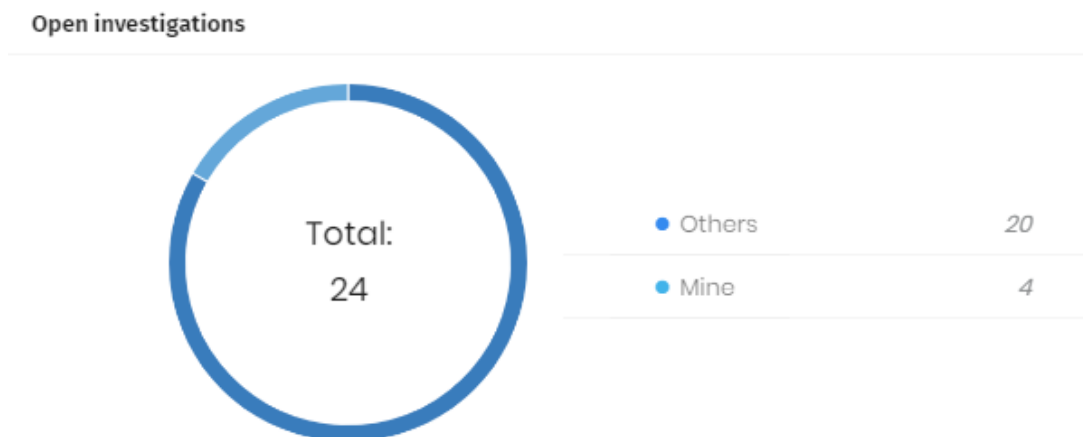


Figure 8.1: Open Investigations tile

### Meaning of the Data Displayed

Data	Description
Others	Investigations with status <b>In Progress</b> that have been opened by user accounts other than the one you used to access the analysis console.

Data	Description
Mine	Investigations with status <b>In Progress</b> opened by the user account you used to access the analysis console.

Table 8.1: Meaning of the data displayed in the Open Investigations tile

### Indicators Pending Investigation

This tile shows all indicators that have not yet been assigned to an investigation and therefore have not been investigated, and the indicators which, although assigned to an investigation, have not been closed and therefore the investigation has not been concluded.

#### Indicators pending investigation

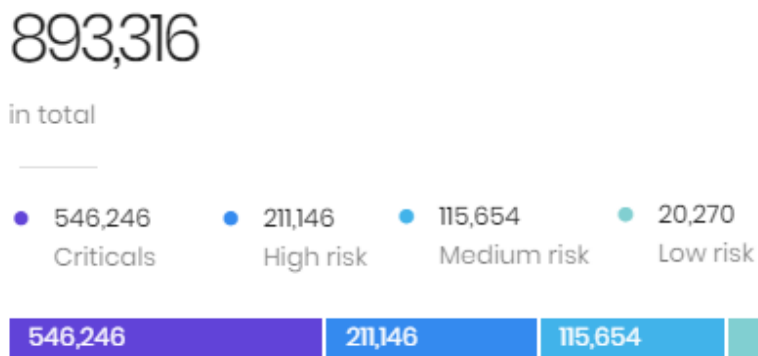


Figure 8.2: Indicators Pending Investigation tile

### Meaning of the Data Displayed

Data	Description
<b>Total</b>	Total number of indicators with status In Progress and Pending
<b>Critical</b>	Indicators whose Severity level is 1 (Critical)
<b>High risk</b>	Indicators whose Severity level is 2 (High risk)
<b>Medium risk</b>	Indicators whose Severity level is 3 (Medium risk)
<b>Low risk</b>	Indicators whose Severity level is 4 (Low risk)

Table 8.2: Meaning of the data displayed in the Indicators Pending Investigation tile

## Top Risk Computers

This tile shows the computers where Cytomic Orion has detected greatest risk, with the number of indicators assigned and their severity level. The list is sorted so that it first shows the computers where most critical indicators were detected, then those with most high-risk indicators, then medium-risk ones, and finally low-risk ones.

**Top risk computers**


























Name	Client	Alerts			
 2BD2B276E6AC92083CDE78E2...	(82899249)	 55	 57	 40	 25
 E7BF7480C0A324B77E4B62530...	(82899249)	 49	 21	 20	 11
 081F4BBBEA85DE6DCAE866DE...	(763053259)	 45	 22	 15	 13
 F4656BEA41C6FACC60D577E8...	(82856221)	 44	 29	 11	 11
 411589434C5BA13C03AD2A0B2...	(82856221)	 43	 29	 12	 11

Figure 8.3: Top Risk Computers tile

### Meaning of the Data Displayed





Field	Description
<b>Name</b>	ID of the computer.
<b>Client</b>	ID of the client.
<b>Indicators</b>	Number of indicators found, grouped by severity level. <ul style="list-style-type: none"> <li> Critical indicators.</li> <li> High risk indicators.</li> <li> Medium risk indicators.</li> <li> Low risk indicators.</li> </ul>

Table 8.3: Meaning of the data displayed in the Top Risk Computers tile

## Top Risk Hunting Rules

This tile shows the hunting rules that have generated most indicators, sorted by severity level, along with the number of computers affected and the number of indicators the rules generated. The list is sorted so that it first shows the hunting rules that generated most critical indicators, then those with most high-risk indicators, then medium-risk ones, and finally low-risk ones. Within each severity level, the rules are sorted by the number of indicators generated.

Top risk hunting rules			
Name	Severity	Computers	Indicators
NetworkOpsDSLRule	Critical	7	577
ProcessOpsDSLRule	Critical	7	25
DownloadDSLRule	Critical	3	15
PythonFakeRule	Critical	1	4
IPloc Found in Event Stream	High risk	1	3614


Figure 8.4: Top Risk Hunting Rules tile

### Meaning of the Data Displayed

Field	Description
<b>Name</b>	ID of the hunting rule.
<b>Severity</b>	Severity level associated with the hunting rule.
<b>Computers</b>	Number of different computers where an indicator was generated.
<b>Indicators</b>	Number of indicators generated by the hunting rule.

Table 8.4: Meaning of the data displayed in the Top Risk Hunting Rules tile

### Top Risk Clients



*This tile appears only for MSSPs/MDR vendors who manage multiple clients.*

This tile shows the clients whose computers have most Pending or In Progress indicators assigned. The list is sorted by severity level, so that it shows the clients with the greatest amount of critical indicators first, then the ones with high-risk indicators, followed by the medium-risk ones, and finally the low-risk ones.

Top risk clients				
Name	Indicators			
(82856221)	6029	5304	3669	2290
(763088626)	508	551	420	241
(82831186)	468	376	289	162
(82751722)	430	375	255	183
(763031783)	409	551	423	239

Figure 8.5: Top Risk Clients tile

### Meaning of the Data Displayed

Field	Description
Name	ID of the client. <ul style="list-style-type: none"> <li>● Critical indicators.</li> <li>● High risk indicators.</li> <li>● Medium risk indicators.</li> <li>● Low risk indicators.</li> </ul>

Table 8.5: Meaning of the data displayed in the Top Risk Hunting Rules tile

### Indicators

This tile contains a line graph that shows the number of indicators generated over time, based on their severity level. The graph includes four data series: one for each severity level supported in Cytomic Orion.



Figure 8.6: Indicators tile

### Meaning of the Data Displayed

Data	Description
●	Critical indicators
●	High risk indicators.
●	Medium risk indicators.
●	Low risk indicators.

Table 8.6: Meaning of the data displayed in the Indicators tile

# MITRE Dashboard

This dashboard provides information about the detected indicators, arranged by the tactics and techniques classified in the MITRE ATT&CK matrix.

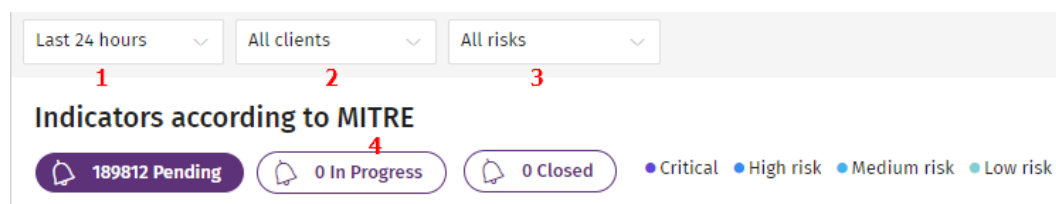


Figure 8.7: Indicators according to MITRE panel

To access the dashboard:

- In the top menu, select **Dashboard**. In the side panel, select **MITRE**. A page opens that shows the dashboard tiles.
- Select a time period for the data shown in the tiles **(1)**:
  - Last 24 hours
  - Last 7 days
  - Last month
- Select the client for which indicators are shown **(2)**:
  - **Select client**: Shows indicators for all clients.
  - **Client ID**: Shows indicators for the selected client.
- Select the risk level for the techniques and tactics shown on the page **(3)**:
  - All risks
  - Critical
  - High risk
  - Medium risk
  - Low risk
- Select the status of the indicators shown on the page **(4)**:
  - **Pending**: Indicators that are yet to be assigned to an investigation.
  - **In progress**: Indicators assigned to an open investigation.
  - **Closed**: Indicators assigned to a closed investigation.



## Meaning of the Data Displayed

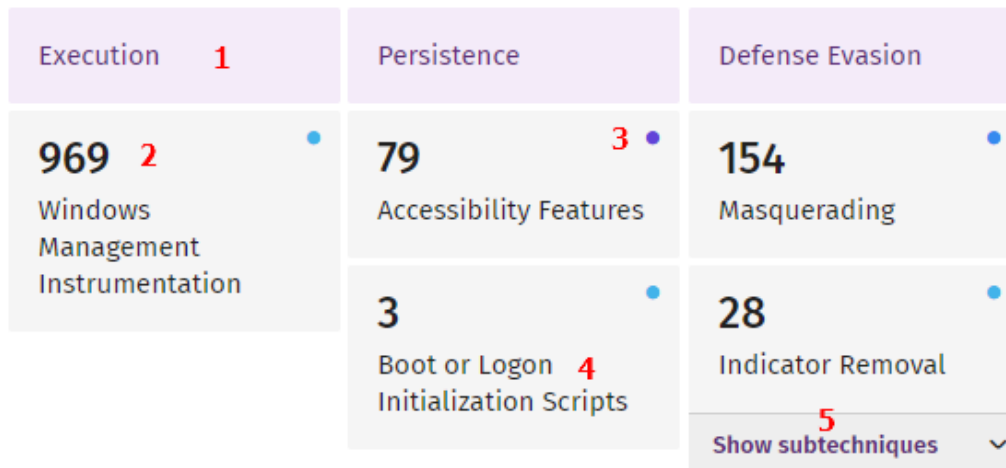


Figure 8.8: Indicators according to MITRE panel

Data	Description
(1)	MITRE technique
(2)	Number of indicators found with the specified tactic and technique.
(3)	Risk associated with the tactic and technique used for the grouped indicators.
(4)	MITRE tactic
(5)	Drop-down list showing the sub-techniques used. For each sub-technique, the number of indicators that have that sub-technique assigned is shown. Not all indicators have a sub-technique assigned.

Table 8.7: Meaning of the data displayed in the Indicators according to MITRE panel

## View the Indicators Mapped to a Tactic and Technique

Click the box for the relevant technique (2) or sub-technique (5). The **Indicators** page opens, with the list of indicators associated with the selected technique or sub-technique.

## Data Usage

Cytomic Orion provides analysts with a set of tools that enables them to run searches on the data lake corresponding to the computers they are investigating. There are no limits on the storage of data in the data lake for console users, although the retrieval of this information is monitored to determine the amount of data used by each MSSP.

Cytomic Orion sets out some limits as guidelines, although they do not affect the maximum amount of data that can be stored in the data lake nor the bandwidth used when retrieving this data. The information is only provided as a guide to compare the bandwidth usage of each MSSP/SOC with the amount recommended by Cytomic.

## Amount of Data Assigned and Usage Monitoring Resources

### Amount of Data Assigned

Each MSSP has an annual allocation of 5 GB of data usage for each managed computer. Analysts who access the data lake use the amount allocated to the SOC at their own discretion. For example, one user can use all the data assigned annually on a single day to investigate a single computer belonging to a specific client of the MSSP or, alternatively, all analysts could use the assigned amount of data to investigate some or all of the MSSP's clients' computers.

### Data Usage Monitoring Resources



To monitor data usage for each MSSP, Cytomic Orion provides console users with multiple complementary resources:

- **Data used in advanced queries:** A notebook that shows the amount of data used by each user account. See [Notebook Data consumed in advanced queries](#).
- **Data usage by user dashboard:** A set of panels that provide both a consolidated view and breakdown of the data used by the MSSP user accounts. See [Data Usage by User Dashboard](#).
- **Data usage by query dashboard:** A set of panels that provide both a consolidated view and breakdown of the MSSP actions involving access to the data lake. See [Data Usage by Query Dashboard](#).
- **Data usage by client dashboard:** A set of panels that provide both a consolidated view and breakdown of the data used by each client managed by the MSSP. See [Data Usage by Client Dashboard](#).
- **Assigned data dashboard:** A history of changes to the amount of data assigned to the MSSP. See [Assigned Data Dashboard](#).
- **Notification email:** Notifies console users when data usage exceeds certain configured thresholds. See [Usage Notification Email](#).

### Notebook Data consumed in advanced queries

To see the volume of data that each console user account has used, create and run a notebook from the [Data used in advanced queries](#) template.

## Access the Notebook

- In the top menu, select **Investigations**. Select an open investigation or create a new one:
  - Click the **New investigation** icon  in the upper-right corner of the page.
  - Select the MSSP clients on which you want to run the investigation. In this case, that data is not relevant because the aim is to run a notebook from a template.
- In the **Files** panel, click the  icon. A drop-down menu appears.
- In the menu, select **Automated investigation**. Select the **Data used in advanced queries** template. The parameters dialog box opens.
- In `date_from` and `date_to` enter the time limits for the data usage information you require. Click **OK**.



*The maximum period is six months. If you select a greater period, an error message appears.*

## Content of the Data Used in Advanced Queries Notebook

The **Data used in advanced queries** notebook contains a series of fields that show the amount of data used, measured in GB and corresponding to the specified period:

Field	Description
<b>Total usage</b>	The accumulated total from all user accounts managed by the MSSP.
<b>Average usage per day</b>	Daily average from all user accounts managed by the MSSP.

Table 8.8: Data usage section

Field	Description
<b>Email</b>	User account email address.
<b>Total notebook (GB)</b>	Amount of data requested from the data lake from notebooks.
<b>Total exploration (GB)</b>	Amount of data requested from the data lake from SQL queries.

Field	Description
<b>Total (GB)</b>	Amount of data requested from the data lake by each user account. This is the sum of all the previous categories.
<b>Average (GB)</b>	Daily average of data usage for the specified period.

Table 8.9: Data usage per user section

Field	Description
<b>Email</b>	User account email address.
<b>Clients</b>	Clients visible to the user account. See <a href="#">Client Visibility Settings</a> on page 51.
<b>Total (GB)</b>	Amount of data requested from the data lake by each user account.

Table 8.10: Usage per user and clients that users have access to section

## Data Usage Dashboard

This dashboard shows annual data usage for the current year and the amount of data assigned to the MSSP.

### Required Permissions

No special permissions are required to view the panel. **Data usage** is always visible.

### Access the Dashboard

In the top menu, select **Dashboards**. **Data usage** appears in the side panel.

### Data Usage

This panel shows the accumulated data usage of all the SOC accounts for the current year.

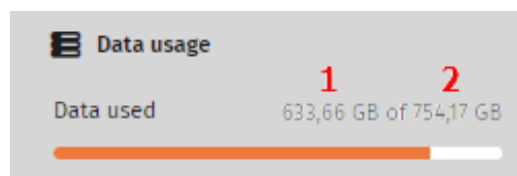


Figure 8.9: Data usage panel

## Meaning of the Data Displayed

Data	Description
(1)	Total data used by the MSSP in the current year.
(2)	Total data assigned to the MSSP.
Bar	Percentage of data used in the current year: <ul style="list-style-type: none"> <li>• <b>Green:</b> Less than 80%.</li> <li>• <b>Yellow:</b> Between 80% and 90%.</li> <li>• <b>Orange:</b> Between 90% and 100%.</li> <li>• <b>Red:</b> Over 100%.</li> </ul>

Table 8.11: Description of the data displayed in the Data Usage panel

## Data Usage by User Dashboard

This dashboard shows the MSSP data usage broken down by user accounts.

### Required Permissions

The user account requires the **View the data usage dashboard** permission to access the dashboard content.

### Access the Dashboard

- In the top menu, select **Dashboard**. In the side panel, select **Data usage**.
- Select the **Users** tab.

### Data Usage by User

The dashboard contains these items:

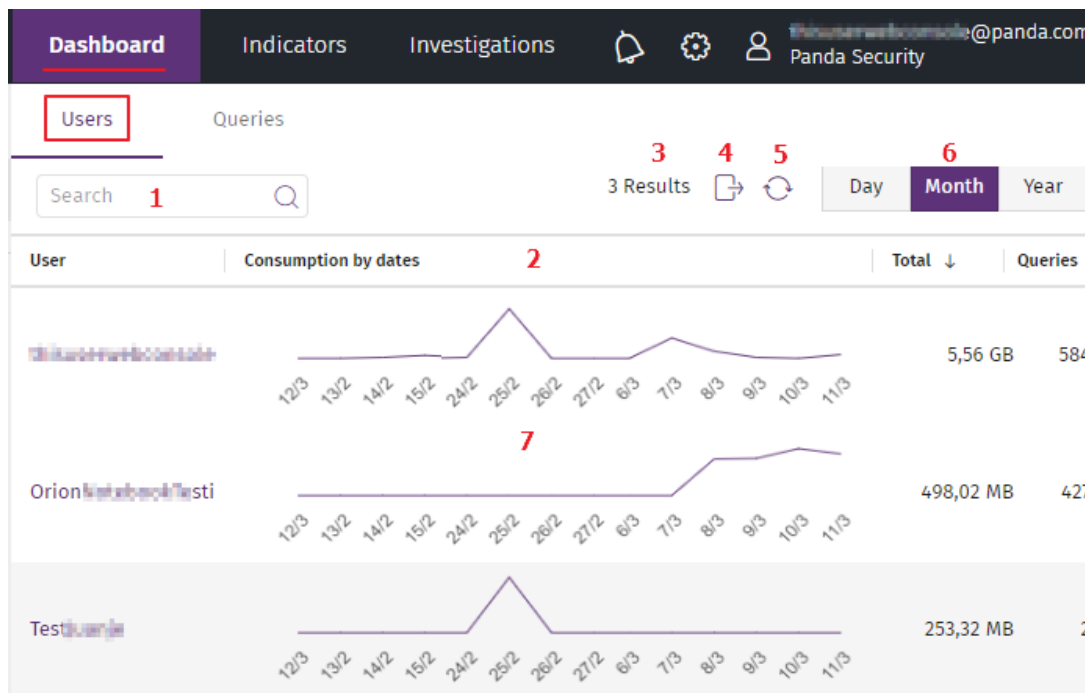


Figure 8.10: Data usage by user dashboard

- **Search (1):** Filters the results by the content of the **User** column. You can enter substrings.
- **Sort columns (2):** See [Tools for Configuring Lists](#) on page 36.
- **Results (3):** The number of user accounts for which usage data is shown in the dashboard.
- **Export (4):** Downloads an Excel file with the dashboard content to the analyst computer.
- **Refresh (5):** Refreshes the dashboard content to update the data.
- **Date range (6):**
  - **Day:** Accumulated data for the last 24 hours.
  - **Month:** Accumulated data for the last 30 days.
  - **Year:** Accumulated data for the last 12 months.
- **Data Usage by User graphs (7):** Shows the trend of data usage for each of the MSSP user accounts for the selected period (6):

Column	Description
User	MSSP user account name.
Usage by dates	Line graph showing the trend of data usage.
Total	The amount of data used by each user account.

Column	Description
Queries	Number of read queries on the data lake.

Table 8.12: Description of the data displayed in the Data Usage by User graph

## Data Usage by Query Dashboard

This dashboard shows the data usage of an MSSP user account according to the queries made to the data lake.

### Required Permissions

The user account requires the **View the data usage dashboard** permission to access the dashboard content.

### Access the Dashboard

- In the top menu, select **Dashboard**. In the side panel, select **Data usage**.
- Select the **Users** tab.
- Configure a time period, then select a user account. The **Data usage by query** dashboard appears for the corresponding user account.

### Data Usage by Query

The dashboard contains these items:

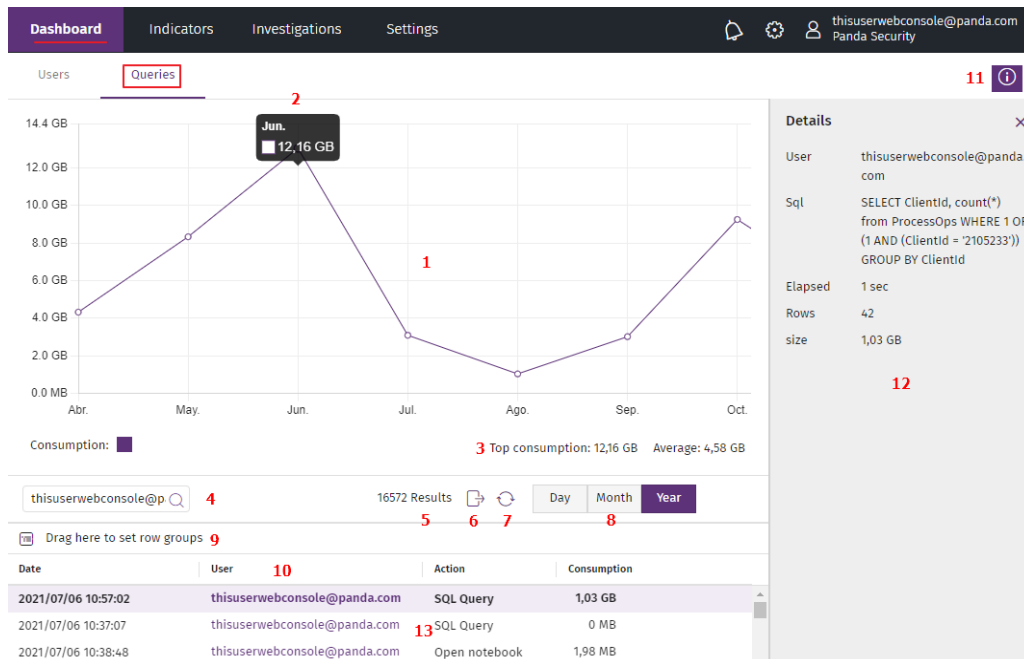


Figure 8.11: Data usage by query dashboard

- **Line graph (1):** Shows the trend of data usage for the selected user account.
- **Tooltip (2):** Point the mouse to the points in the line graph. A tooltip appears that shows the content of the corresponding X and Y coordinates.
- **Usage statistics (3):** Shows peak usage and the maximum volume of data recommended by Cytomic for the selected period.
- **Search (4):** Filters the list of logged operations by the content of the **Date**, **User**, and **Action** columns.
- **Results (5):** Number of queries to the data lake in the time period defined in (8).
- **Export:** Downloads an Excel file with the content of the list (13).
- **Refresh (7):** Updates the content of the list (13).
- **Date range (8):**
  - **Day:** Accumulated data for the last 24 hours.
  - **Month:** Accumulated data for the last 30 days.
  - **Year:** Accumulated data for the last 12 months.
- **Group columns (9):** See **Group Entries by Columns** on page 37.
- **Sort columns (10):** See **Sort Columns** on page 37.
- **Details button:** Shows or hides the **Details** panel (12).
- **Details (12):** Panel containing information about the query selected in (13):

Column	Description
User	MSSP user account name.
SQL	Logged SQL statement that retrieved information from the data lake.
Elapsed	Time the SQL statement took to run.
Rows	The number of rows retrieved from the data lake.
Size	The amount of data retrieved from the data lake.

Table 8.13: Description of the Details panel

- **List (13):** Queries to the data lake corresponding to the user account for the time period specified in (8).



Attribute	Description
<b>Date</b>	Date on which the query was run.
<b>User</b>	MSSP user account that ran the query.
<b>Action</b>	<p>Module or tool used to retrieve the information from the data lake:</p> <ul style="list-style-type: none"> <li>• <b>SQL query:</b> Includes the queries generated through the Advanced SQL Query and Wizard-guided Queries modules. See <a href="#">Investigate the Event Flow</a> on page 144.</li> <li>• <b>Open notebook:</b> Includes queries generated from a notebook. See <a href="#">Investigations with Notebooks</a> on page 204.</li> <li>• <b>Query from application:</b> Includes the information retrieved from calls to the Cytomic API. See <a href="#">Cytomic Orion Integration with SOC Tools</a> on page 292.</li> </ul>
<b>Usage</b>	The number of rows retrieved from the data lake.

Table 8.14: Description of the Details panel

## Data Usage by Client Dashboard

This dashboard shows the data used in the investigations performed on clients managed by the MSSP.

### Required Permissions

The user account requires the **View the data usage dashboard** permission to access the dashboard content.

### Access the Dashboard

- In the top menu, select **Dashboard**. In the side panel, select **Data usage**.
- Select the **Clients** tab.
- Select a time period. The **Data usage by client** dashboard shows the relevant data.

### Calculate Usage for Data Shared among Clients

Because one query or investigation can affect multiple clients simultaneously, you must divide data usage for each client proportionally.

To divide usage among multiple clients, we establish a weight or percentage of usage based on the number of licenses that each client has. Here is an example of how we calculate the percentage of data used:

The SOC analyst launches a query on the computers of three clients. The query uses a total of 250 MB. Each client has the following number of licenses:

- Client 1: 57 licenses
- Client 2: 3 licenses
- Client 3: 7 licenses

The total number of licenses for the three clients is  $57 + 3 + 7 = 67$  licenses.

The percentage of licenses that each user has is:

- Client 1:  $57 / 67 = 0.85$  (85% of the traffic used by the query corresponds to client 1).
- Client 2:  $3 / 67 = 0.04$  (4% of the traffic used by the query corresponds to client 2).
- Client 3:  $7 / 67 = 0.10$  (10% of the traffic used by the query corresponds to client 3).

The amount of data used by each client is:

- Client 1:  $250 * 0.85 = 212$  MB
- Client 2:  $250 * 0,04 = 10$  MB
- Client 3:  $250 * 0,10 = 25$  MB

### Data Usage by Client

The dashboard contains these items:

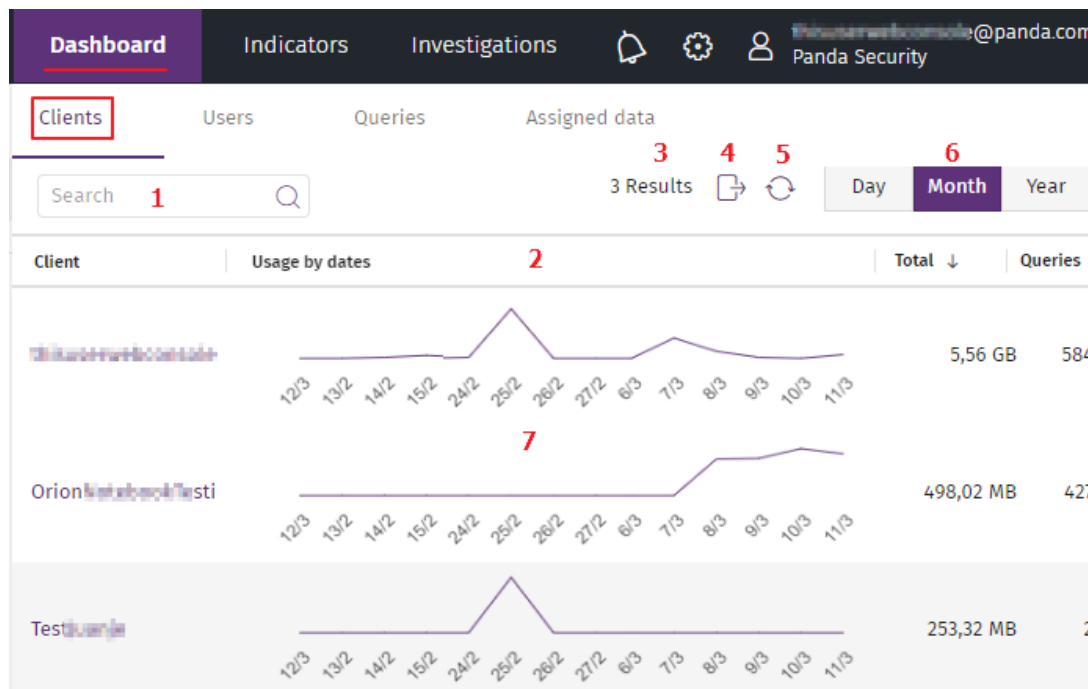


Figure 8.12: Data usage by client dashboard

- **Search (1):** Filters the results by the content of the **Client** column. You can enter substrings.
- **Sort columns (2):** See **Tools for Configuring Lists** on page 36.
- **Results (3):** The number of clients for which usage data is shown in the dashboard.

- **Export (4):** Downloads an Excel file with the dashboard content to the analyst's computer.
- **Refresh (5):** Refreshes the dashboard content to update the data.
- **Date range (6):**
  - **Day:** Accumulated data for the last 24 hours.
  - **Month:** Accumulated data for the last 30 days.
  - **Year:** Accumulated data for the last 12 months.
- **Data usage by client graphs (7):** Show the trend of data usage for each client of the MSSP for the selected period (6):

Column	Description
Client	Name of the MSSP's client.
Usage by dates	Line graph showing the trend of data usage.
Total	The amount of data used by the client.
Queries	Number of read queries on the data lake.

Table 8.15: Description of the data displayed in the Data Usage by Client graph

## Assigned Data Dashboard

This dashboard shows a history of changes to the amount of data assigned to the MSSP in the last year.

Because Cytomic Orion assigns MSSPs 5 GB of data for each managed computer, if there is a change in the number of managed computers, the total amount of data is adjusted accordingly.

### Required Permissions

The user account requires the **View the data usage dashboard** permission to access the dashboard content.

### Access the Dashboard

- In the top menu, select **Dashboard**. In the side panel, select **Data usage**.
- Select the **Assigned data** tab.

### Assigned Data History

The dashboard contains these items:

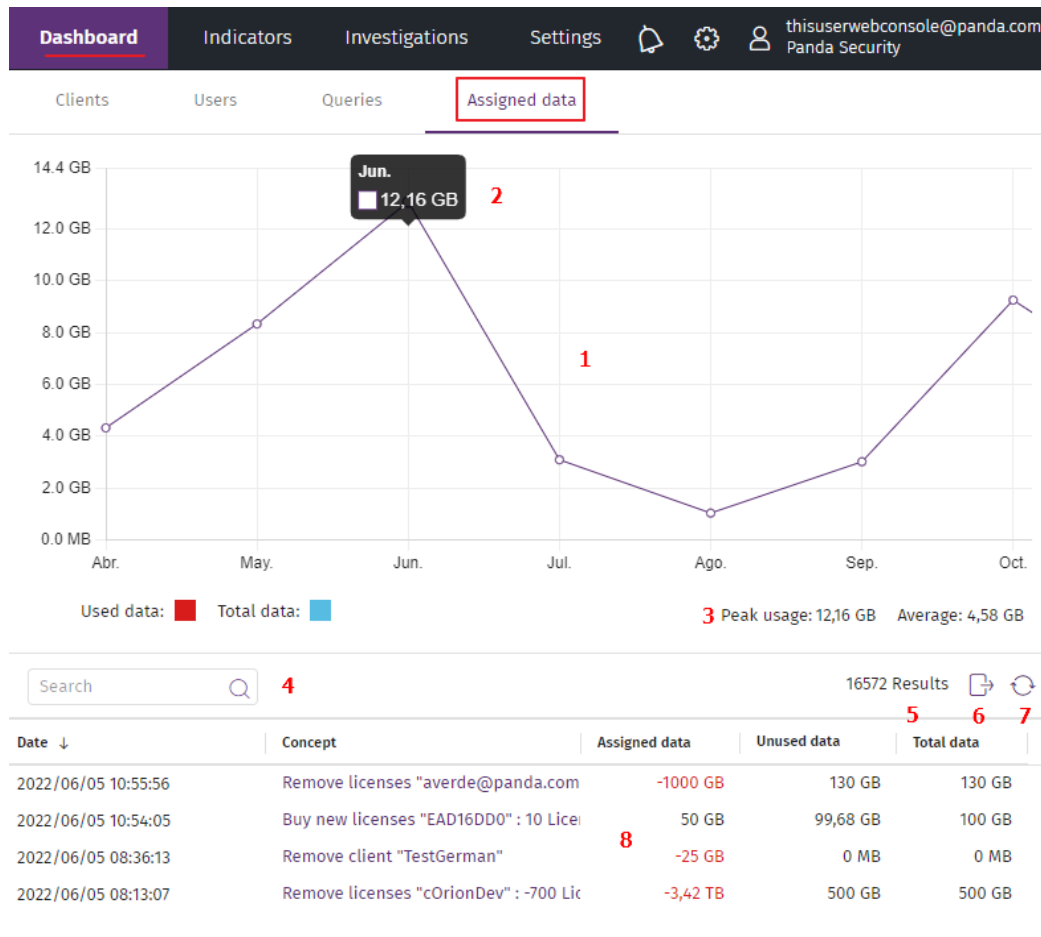


Figure 8.13: Assigned Data dashboard

- **Line graph (1):** Shows the trend of data assigned to the MSSP and data used.
- **Tooltip (2):** Point the mouse to the points in the line graph. A tooltip appears that shows the content of the corresponding X and Y coordinates.
- **Usage statistics (3):** Shows peak usage and the maximum volume of data recommended by Cytomic for the selected period.
- **Search (4):** Filters the list of logged operations by the content of the **Concept** column.
- **Results (5):** Number of changes to the assigned data.
- **Export:** Downloads an Excel file with the content of the list **(8)**.
- **Refresh (7):** Updates the content of the list **(8)**.
- **List (8):** Logs the changes made to the amount of assigned data in the last year.

Attribute	Description
<b>Date</b>	Date of the change in the amount of assigned data.
<b>Concept</b>	Type of logged change:

Attribute	Description
	<ul style="list-style-type: none"> <li>• <b>License reduction:</b> The amount of data assigned to the MSSP is reduced by 5 GB for each computer that is no longer managed.</li> <li>• <b>License purchase:</b> The amount of data assigned to the MSSP is increased by 5 GB for each new managed computer.</li> <li>• <b>Client deletion:</b> The amount of data assigned to the MSSP is reduced based on the total number of computers that belonged to the deleted client.</li> <li>• <b>New client:</b> The amount of data assigned to the MSSP is increased based on the total number of computers that belong to the new client.</li> </ul>
<b>Assigned data</b>	Increase or decrease in the amount of data assigned to the MSSP, based on the logged change.
<b>Unused data</b>	The amount of data assigned minus the amount of data used at the time the change in the amount of data was logged.
<b>Total data</b>	Total data assigned to the MSSP after the logged operation.

Table 8.16: List description

## Usage Notification Email

Analysts receive an email notification when one of the user accounts that access the Cytomic Orion console uses more data than assigned to the SOC/MSSP. See [Amount of Data Assigned](#).

### Notification Recipients

To receive the email notification, these requirements must be met:

- The user account must have the **View the data usage dashboard** permission assigned. See [Understanding Permissions](#) on page 56.
- The user account must have the **Email me when the data used in queries approaches the maximum quota** option enabled. To see this option, select **Settings** in the top menu. In the side menu, select **My preferences**.

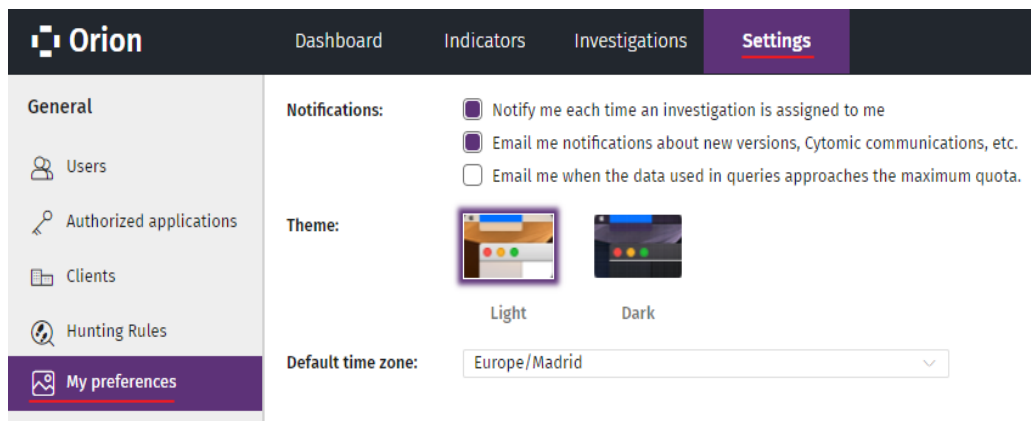


Figure 8.14: Page for enabling data usage notifications

When Cytomic Orion detects that a user account exceeds the total amount of data assigned to the SOC/MSSP, it sends a notification to all users that meet the aforementioned requirements.

### Number of Notifications Sent

Cytomic Orion establishes three thresholds regarding data usage: 80%, 90%, and 100%. When a console user exceeds any of the configured thresholds, a notification email is sent. To keep the number of emails sent to the minimum, the solution sends only one email for each threshold that is exceeded.

If the amount of data assigned to the SOC/MSSP changes, an email message is sent again when any of the set thresholds are exceeded.

### Information Included in the Email

Field	Description
Email subject	Indicates the exceeded threshold, with this color: <ul style="list-style-type: none"> <li>80% and 90%: Orange.</li> <li>100%: Red.</li> </ul>
Date	Date the excessive usage was detected.
Used data	Amount of data used when the notification was sent.
Allowed quota	Total amount of data assigned to the SOC/MSSP.

Table 8.17: Notification email description



# Chapter 9

## Investigate the Event Flow

Cytomic Orion provides two very flexible yet powerful modules to selectively retrieve information stored in the Cytomic data lake: **Advanced SQL Queries** and **Wizard-guided Queries**. Both modules give analysts the possibility to create their own queries or use the queries designed by Cytomic to retrieve the information obtained from the monitoring of each process run on clients' computers. This information is used in indicator triage and to perform thorough investigations.

Cytomic Orion organizes all the information it collects by type into tables and keeps it available to analysts on the platform for one year.



*The retention period for the telemetry stored in the data lake is one year.*

### CHAPTER CONTENTS

---

<b>Advanced SQL Query Module</b> .....	<b>145</b>
Queries Side Panel (1) .....	145
Advanced SQL Query Panel .....	153
SQL Statement Optimization .....	155
<b>Wizard-guided Queries Module</b> .....	<b>155</b>
Condition Block Structure .....	157
Results Panel .....	158



# Advanced SQL Query Module

## Access the Advanced SQL Query Module

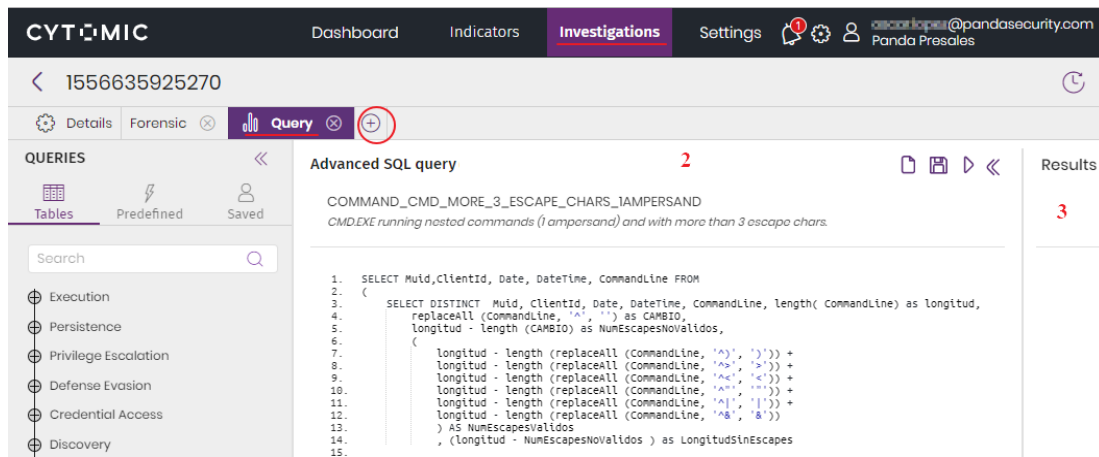


Figure 9.1: Process explorer tab

- In the top menu, select **Investigations**. Select the investigation that contains the indicator generated by the hunting rules, or create a new investigation by clicking the **New investigation** button in the upper-right corner of the page. For more information, see [Create an Investigation](#) on page 95.
- In the tab menu, click the **+** icon to open the context menu. Select **Advanced SQL query**. The query editor page opens. This page is divided into these sections:
  - **Queries side panel (1)**: Enables you to access previously saved queries and the data model.
  - **Advanced SQL query panel (2)**: Enables you to create new queries or edit previously created ones.
  - **Results panel (3)**: Shows the results of the queries.

## Required Permissions

The user account requires the **Access to advanced queries** permission to run SQL statements. The results that analysts get are restricted to those clients visible to their user account. See [Access, Control, and Monitor the Analysis Console](#) on page 44.

## Queries Side Panel (1)

This panel provides access to the queries previously saved by analysts or created by Cytomic. It contains these elements:

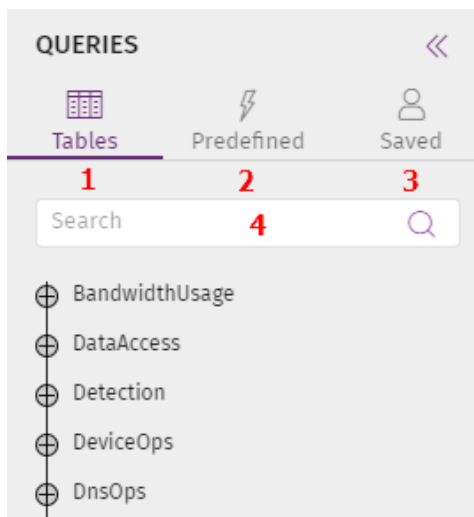


Figure 9.2: Queries side panel

- **Tables (1):** Contains the data model used by Cytomic Orion to organize the information collected from the monitoring of processes.
- **Saved (3):** Contains SQL statements designed by the analyst and saved for frequent use sentences library organized in a tree structure and designed by Cytomic.
- **Predefined (2):** Contains a tree of SQL statements created by Cytomic.
- **Search (4):** Text box to quickly find queries.

## Tables (1)

*For more information about the meaning of the fields in the data model, see chapter [Format of the Events Used in Cytomic Orion](#) on page 374.*

This tab shows the tables and fields available to the analyst to create their own queries. To speed up the process, click a field to automatically copy it to the **Advanced SQL query** panel in the position indicated by the cursor.

The **Tables** tab includes all the information collected from the client's IT infrastructure, organized into a number of tables that represent multiple techniques and actions frequently run by the processes in a cyberattack.

Table	Description
<b>BandwidthUsage</b>	Volume of information handled in each data transfer operation performed by the process.
<b>DataAccess</b>	Contains an entry for each operation in which the process accessed data files

Table	Description
	hosted on internal mass-storage devices.
<b>Detection</b>	Contains an entry for each detection made by the Cytomic EDR active protections.
<b>DeviceOps</b>	Contains an entry for each operation in which the process accessed an external device.
<b>DnsOps</b>	Contains an entry for each operation in which the process accessed the DNS name server..
<b>Download</b>	Contains an entry for each operation in which the process downloaded data.
<b>Evidence</b>	Contains an entry for each ungrouped indicator detected.
<b>Indicators</b>	<p>Contains an entry with grouped indicators. For more information about how Cytomic Orion groups indicators, see <a href="#">Indicator Grouping</a> on page 68.</p> <p>The <b>Indicators</b> table matches the indicator list that appears in the Cytomic Orion console. See <a href="#">Indicators List</a> on page 66</p>
<b>LoginOutOps</b>	Contains an entry for each login or logout operation performed by the user.
<b>NetworkOps</b>	Contains an entry for each network operation performed by the process.
<b>ProcessOps</b>	Contains events for processes that performed operations on the computer hard disk.
<b>RegistryOps</b>	Contains an entry for each operation in which the process accessed the Windows Registry.
<b>RemediationOps</b>	Contains detection, blocking, and disinfection events from the security solution installed on the workstation or server.
<b>ScriptOps</b>	Contains an entry for each operation performed by a script-type process.
<b>SystemOps</b>	Contains an entry for each operation performed by the Windows operating system WMI engine.
<b>UserNotification</b>	Contains an entry for each notification displayed to the user and response (if

Table	Description
	any).

Table 9.1: Tables available on the Tables tab

This table indicates the fields included in each table.

Table	Fields
<b>BandwidthUsage</b>	DateTime, LocalDateTime, PandaTimeStatus, TimeStamp, MUID, ClientId, EventType, ParentPid, ParentMd5, ParentDrive, ParentPath, ParentFilename, BytesSent, BytesReceived, LoggedUser, TTPs, IOAIds, TelemetryType, Date, InsertionDateTime.
<b>DataAccess</b>	DateTime, LocalDateTime, PandaTimeStatus, TimeStamp, Muid, ClientId, EventType, ParentPid, ParentMd5, ParentDrive, ParentPath, ParentFilename, ParentAttributes, ChildPath, ChildFilename, ChildAttributes, LoggedUser, Config, TTPs, IOAIds, TelemetryType, Date, InsertionDateTime.
<b>Detection</b>	DateTime, LocalDateTime, PandaTimeStatus, TimeStamp, Muid, ClientId, EventType, ParentMd5, WinningTech, DetectionId, Date, InsertionDateTime.
<b>DeviceOps</b>	DateTime, LocalDateTime, PandaTimeStatus, TimeStamp, Muid, ClientId, EventType, NotificationType, DeviceType, UniqueId, IsDenied, IdName, ClassName, FriendlyName, Description, Manufacturer, PhoneDescription, TTPs, IOAIds, TelemetryType, Date, InsertionDateTime.
<b>DnsOps</b>	DateTime, LocalDateTime, PandaTimeStatus, TimeStamp, Muid, ClientId, EventType, ParentCount, ParentPid, ParentMd5, ParentDrive, ParentPath, ParentFilename, FailedQueries, QueriedDomainCount, DomainList, TTPs, IOAIds, TelemetryType, Date, InsertionDateTime.
<b>Download</b>	DateTime LocalDateTime, PandaTimeStatus, TimeStamp, Muid, ClientId, EventType, ParentMd5, ParentDrive, ParentPath, ParentFilename, ParentPid, ChildMd5, ChildDrive, ChildPath, ChildFilename, ChildUrl, LoggedUser, TTPs, IOAIds, TelemetryType, Date, InsertionDateTime.
<b>Evidences</b>	EvidenceDateTime, TimeStamp, Muid, ClientId, HuntingRuleName, HuntingRuleId, HuntingRuleMode, HuntingRuleSeverity, HuntingRuleMitre, Details, InsertionDateTime.

Table	Fields
<b>Indicators</b>	AlertDateTime, TimeStamp, Muid, ClientId, HuntingRuleName, HuntingRuleId, HuntingRuleType, HuntingRuleMode, HuntingRuleSeverity, HuntingRuleMitre, Details, Occurrences, PandaAlertId, InsertionDateTime.
<b>LoginOutOps</b>	DateTime LocalDateTime, PandaTimeStatus, TimeStamp, Muid, ClientId, EventType, Actiontype, SessionType, ErrorCode, Username, Interactive, RemoteMachineName, Remotelp, RemotePort, Times, TTPs, IOAIds, TelemetryType, Date, InsertionDateTime.
<b>NetworkOps</b>	DateTime, LocalDateTime, PandaTimeStatus, TimeStamp, Muid, ClientId, EventType, ParentPid, ParentMd5, ParentDrive, ParentPath, ParentFilename, Protocol, Remotelp, RemotePort, LocalIp, LocalPort, Direction, LoggedUser, Ipv4Status, DetectionId, Hostname, Times, SocketOpFlags, ALProtocolExpected, ALProtocolDetected, CipherType, ConnectionState, ProxyConnection, ContentEncoding, TTPs, IOAIds, TelemetryType, Redirection, InitialDomain, Method, HeaderHttp, RuleId, Entropy, Date, InsertionDateTime.
<b>ProcessOps</b>	DateTime, LocalDateTime, PandaTimeStatus, TimeStamp, Muid, ClientId, EventType, Operation, ParentStatus, ParentMd5, ParentDrive, ParentPath, ParentFilename, ParentPid, ParentAttributes, ChildStatus, ChildMd5, ChildDrive, ChildPath, ChildFilename, ChildPid, ChildAttributes, ChildClassification, CommandLine, RemediationResult, Action, ServiceLevel, WinningTech, DetectionId, LoggedUser, Remotelp, RemoteMachineName, RemoteUsername, TTPs, IOAIds, TelemetryType, Date, InsertionDateTime, Key, Value, ValueData.
<b>RegistryOps</b>	DateTime, LocalDateTime, PandaTimeStatus, TimeStamp, Muid, ClientId, EventType, ParentPid, ParentMd5, ParentDrive, ParentPath, ParentFilename, RegistryAction, Key, Value, ValueDataLength, ValueData, LoggedUser, Config, TTPs, IOAIds, TelemetryType, Date, InsertionDateTime.
<b>RemediationOps</b>	DateTime, LocalDateTime, PandaTimeStatus, TimeStamp, Muid, ClientId, EventType, ParentMd5, ParentDrive, ParentPath, ParentPid, ParentFilename, ChildMd5, ChildSha256, ChildDrive, ChildPath, ChildFilename, CommandLine, WinningTech, DetectionId, Action, RemediationData, RemediationResult, ServiceLevel, Remotelp, RemoteMachineName, RemoteUsername, LoggedUser, ExploitOrigin, Url,

Table	Fields
	ChildClassification, NapOriginIp, NapOriginPort, NapDestinationIp, NapDestinationPort, NapDirection, NapOccurrences, NapAttack, AttackerDeviceId, Risk, RuleId, Date, InsertionDateTime.
<b>ScriptOps</b>	DateTime, LocalDateTime, PandaTimeStatus, TimeStamp, Muid, ClientId, EventType, ParentMd5, ParentDrive, ParentPath, ParentFilename, ParentPid, ParentAttributes, ChildMd5, ChildDrive, ChildPath, ChildFilename, ChildAttributes, ChildFileSize, ChildClassification, CommandLine, ServiceLevel, LoggedUser, TTPs, IOAIds, TelemetryType, Date, InsertionDateTime.
<b>SystemOps</b>	DateTime, LocalDateTime, PandaTimeStatus, TimeStamp, Muid, ClientId, EventType, Type, ObjectName, CommandLine, MachineName, Username, IsLocal, ExtendedInfo, ChildMd5, RemoteMachineName, RemoteIp, IsSessionInteractive, Times, TTPs, IOAIds, TelemetryType, Date, InsertionDateTime, ParentPid.
<b>UserNotification</b>	DateTime, LocalDateTime, PandaTimeStatus, TimeStamp, Muid, ClientId, EventType, ParentMd5, ParentDrive, ParentPath, ParentFilename, ChildMd5, ChildDrive, ChildPath, ChildFilename, ChildClassification, ChildFirstSeen, WinningTech, DetectionId, RemediationResult, BlockReason, ServiceLevel, Date, InsertionDateTime.

Table 9.2: Fields available in each table

## Meaning of Date-type Fields

Cytomic Orion supports multiple date-type fields that help differentiate the source of the data and prevent frequent errors that can occur when analysts work with events:

- **TimeStamp**: Actual UTC date in epoch format (number of seconds that elapsed since 00:00:00 UTC on 1 January 1970) when the event occurred on the client's computer. This date originates from an internal calculation in Cytomic Orion. It might not match the date on the computer where the event was logged if the latter is misconfigured.
- **DateTime**: The same as TimeStamp but in Date:Time format.
- **Date**: The same as TimeStamp but in Date format.
- **LocalDateTime**: The computer date (in UTC format) at the time the logged event occurred. This date depends on the computer settings. As a result, it can be incorrect.
- **PandaTimeStatus**: Contents of the DateTime, Date, and LocalDateTime fields:

- **0:** Actual date not supported because it is an old event.
- **1:** Actual date, supported but obtained by means of a calculation because the Cytomic server was unavailable.
- **2:** Actual date provided by the Cytomic server.
- **InsertionDateTime:** Date in UTC format at the time Cytomic logged the event sent by the computer on the company servers. This date is always later than the other dates because the events are queued to be processed.

## Predefined (2)

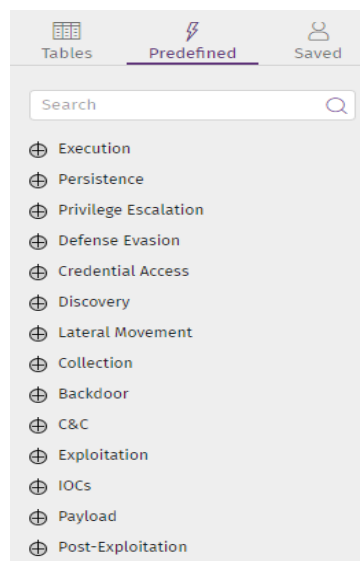


Figure 9.3: First-level group tree in the query library

This tab shows the query library created by Cytomic. This library is divided into 14 groups and sub-groups that represent the MITRE tactics and techniques most frequently seen in a cyberattack or an infection.

Double-click a group to show the nodes, sub-nodes, and the predefined queries below it. Double-click a query to load it into the **Advanced SQL query** panel along with its name and description.

Predefined queries cannot be edited, but they can be copied and then edited by analysts. See [Query Management Bar \(1\)](#).

This table shows the available groups and a general description of the types of predefined queries they contain:

Group	Description
<b>Execution</b>	Shows the execution of processes suspected of belonging to an attack because they are used in a different way than usual: unusual parameters, execution of PowerShell, Autolt, or WMI scripts, etc.
<b>Persistence</b>	Shows the execution of actions by processes that try to gain persistence on the

Group	Description
	affected computer to survive system reboots.
<b>Privilege Escalation</b>	Shows actions taken to obtain more elevated permissions than those inherited based on the initial execution context.
<b>Defense Evasion</b>	Shows actions taken to evade defenses established by the network administrator, such as bypassing the local firewall, stopping the installed antivirus process, exploiting the SMB protocol to cause infections, etc.
<b>Credential Access</b>	Shows unauthorized access to the computer SAM to get user credentials.
<b>Discovery</b>	Shows actions taken to collect information through programs such as <code>whoami</code> , <code>nbstat</code> , <code>qprocess</code> , and others.
<b>Lateral Movement</b>	Shows actions taken to spread the malware to other computers on the network to collect information and maximize a hacker chances of success.
<b>Backdoor</b>	Shows backdoor installation attempts to remotely access computers.
<b>Exploitation</b>	Shows attempts to exploit vulnerable processes.
<b>IOCs</b>	Shows processes that run known IOCs (Indicators of Compromise).
<b>Payload</b>	Detects the execution of Bitcoin mining programs.
<b>Post-Exploitation</b>	Shows processes that take actions which usually occur after a vulnerable process has been exploited (create users, stop services, etc.).
<b>PUPs</b>	Shows typical actions taken by processes classified as PUP (potentially unwanted programs). These actions usually correspond to the installation of browser toolbars and similar resources to show ads on clients' computers.

Table 9.3: Groups of available predefined queries

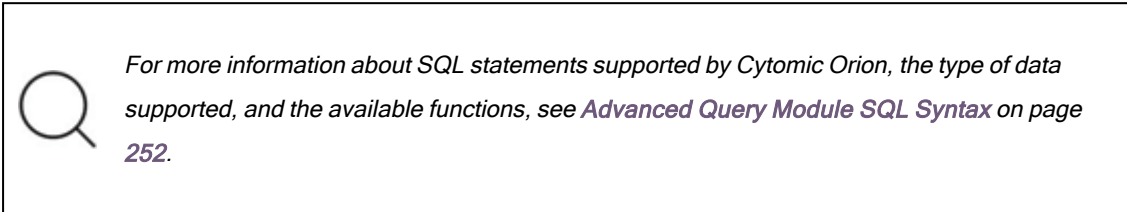
## Saved (3)

This tab includes all the queries the analyst has created and saved over time. These queries are visible to the user accounts created in each MSSP/MDR vendor or SOC individually. Therefore, they are not shared among the different MSSPs/MDR vendors.



Saved queries are grouped by the type and sub-type you chose when you created them, giving rise to a tree structure which analysts can search easily to find a specific query.

## Advanced SQL Query Panel



This panel enables you to create SQL statements from scratch or edit previously saved SQL statements. It contains these elements:






Figure 9.4: Query editor panel



- **Query management bar (1):** Enables you to delete, run, stop, and save existing queries.
- **Query name and description (2):**
- **Query creation panel (3):** Enables you to create a new query or edit an existing query. Every line is numbered. Additionally, the console highlights the SQL language syntax (keywords, reserved symbols, etc.) as well as character strings in blue to make reading SQL statements easier.

### Query Management Bar (1)

This bar enables you to perform actions to manage queries. It shows these icons:

- **Delete query** : Deletes the saved query created by the SOC analyst and selected in the library panel. You cannot delete queries predefined by Cytomic.
- **Clear query** : Deletes the content of the **Advanced SQL query** panel.
- **Save query** : When you click this icon, a dialog box opens where you can enter the query name and the tactic and technique it will belong to in the group tree. Click **OK**. The query is added to the



repository of saved queries. For more information about how to view the queries created by the MSSP/MDR vendor analysts, see [Saved \(3\)](#).

- **Send query**  and **Stop query** : These icons enable you to run and stop the execution of the query shown in the **Advanced SQL query** panel. Syntax and communication errors appear in the results panel. You can also run a query by pressing Control + Enter on your keyboard. See [Results Panel \(3\)](#).

### Results Panel (3)

This panel shows query results in table format and indicates whether there are syntax errors in the SQL statement or problems with the server. For more information about how to filter and search for data within the table, see [Tools for Configuring Lists](#) on page 36.

The results panel provides these tools:

- **Search** : You can type only a partial string. Searches are performed on the content of all fields returned by the SQL statement.
- **Results**: Indicates the number of results shown by the SQL statement.
- **Time zone**: Set the time zone for date fields and for the content of searches.
- **Export** : Saves the SQL statement results to a CSV file. The columns in the file correspond to the columns in the list.

### Context Menu Associated with Result Tables

When you right-click an item in the table, a context menu opens that shows different options that enable you to quickly access other areas of the console:

Option	Description
<b>Investigate computer</b>	Requires the MUID and DateTime fields. It opens the investigation console to show the events logged on the selected computer, on the specified date.
<b>Add entity of interest</b>	Marks an entity to show it in the <b>Entities of interest</b> sub-panel in the associated investigation to rapidly access the information.
<b>Show computers with parent file</b>	Requires the ParentMD5 field. It searches for computers with events that match the value entered in the ParentMD5 field. See <a href="#">File Investigation: MD5</a> on page 174.
<b>Show computers with child file</b>	Requires the ChildMD5 field. It searches for computers with events that match the value entered in the ChildMD5 field. See <a href="#">From a Newly Created or Ongoing Investigation</a> on page 173.

Option	Description
<b>Automated investigation</b>	Shows a lists of all notebook templates created. When the analyst opens a template, Cytomic Orion automatically populates all compatible parameters in the template with the results of the selected row. See <a href="#">Investigations with Notebooks</a> on page 204.
<b>Computer details</b>	Shows information about the computer. Requires the MUID field.

Table 9.4: Context menu for the result table

## SQL Statement Optimization

Cytomic Orion keeps an index for each of the tables that store the events collected from workstations and servers. By using the fields that make up the index in `WHERE` clauses, the solution speeds up queries. Otherwise, the database engine is forced to search the table completely to find the requested information. The fields that make up the index are as follows:

- ClientID
- MUID
- DateTime

## Wizard-guided Queries Module

### Access the Wizard-guided Queries Module

The Wizard-guided Queries module streamlines the creation of queries through a wizard that removes the need to know the SQL language syntax and speeds up technician analyses.

To access the **Wizard-guided queries** tab:

- In the top menu, select **Investigations**. Select the investigation that contains the indicator that you want to investigate, or create a new investigation by clicking the **New investigation** button in the upper-right corner of the page. For more information, see [Create an Investigation](#) on page 95.
- In the tab menu, click the **+** icon to open the context menu. Select **Advanced SQL query**. The wizard page opens. This page has the structure described in [General Structure of the Query Wizard](#).

### Required Permissions

The user account requires the **Access to the query wizard** permission to use this resource. The results that analysts get are restricted to those clients visible to their user accounts. See [Access, Control, and Monitor the Analysis Console](#) on page 44.

## General Structure of the Query Wizard

To create a query with the wizard, you must configure these parameter blocks:

Figure 9.5: Main parameter blocks in the query wizard

- **Type (1):** This is the data source against which you want to run the query. The drop-down menu lists the tables shown in **Tables (1)**. It is equivalent to the `FROM [table]` clause in SQL.
- **Clients (2):** Filters data by client. Analysts can filter data only by the clients they have visibility to.



*You must specify at least one client in each query.*

- **Date (3):** Filters data by date. It is equivalent to clause `WHERE Timestamp [comparer] DateTime`.
  - Choose a comparer: **greater than**, **less than**, **equal to**, **greater than or equal to**, or **less than or equal to**.
  - Select the date to compare: **Today**, **Yesterday**, or a specific date.
- **Columns (4):** This is the data you want to retrieve. It is equivalent to the columns in the `SELECT [column1, column2, ...]` clause in SQL.
- **Condition (6):** It is equivalent to the `WHERE` clause in SQL. See later for more information about this clause.
- **Sort by (7):** Results are sorted by the content of the specified fields, in ascending (**Asc**) or descending (**Desc**) order. It is equivalent to the `ORDER BY [field1, field2, ...]` clause in SQL. If you specify more than one field, results are sorted according to the order of the fields in the block.

- **Limit (8):** Limits the number of records retrieved by a query. It is equivalent to the `LIMIT` or `TOP` clauses in SQL.

## Condition Block Structure

The **Condition** block is equivalent to the `WHERE` clause in SQL and allows a high degree of flexibility to specify the search conditions.

Figure 9.6: Condition block structure with two groups related by the logical operator AND

The **Condition** block is divided into condition groups. Within a condition group, there can be a single condition (block (6)) or multiple conditions (block (2)).

## Conditions

A simple condition (6) consists of a column name (7), a comparison operator (8) (see [Comparison Operators](#)) and the value to be compared against (9). Additionally, it can have an associated Boolean negation operator (3).

A compound condition (2) consists of multiple simple conditions connected through the AND and OR operators (4).

## Groups

Each new group you create is equivalent to entering a simple or compound condition in parentheses in the `WHERE` clause of the corresponding SQL statement.

You can create multiple groups with the **New group** (1) button and connect them with the logical operator AND/OR (5).

Additionally, you can create one or more groups of simple or compound conditions within a group by using the second-level **New group** (10) button.

## Comparison Operators

- **containsAny:** This operator is equivalent to the “Like” operator in SQL. It searches for a character substring.
- **equals::** This operator searches for an exact character string.

- **endsWithAny**: This operator is used to search for a character substring at the end of a string.
- **startsWithAny**: This operator is used to search for a character substring at the beginning of a string.
- **containsInOrder**: This operator searches for three character substrings in the specified order. Specifying a single string is equivalent to using the **containsAny** operator. The operator will show results that contain all the strings you indicate (logical operator AND) in the order you specify.
- **Boolean operators**: The basic logical operators are supported ('<', '>', '>=', '<=', '==').
- **matches**: This operator enables you to write a regular expression in Java format. For more information about the format of regular expressions, escape characters, and other details about RegEx implementation in Java, see <https://docs.oracle.com/javase/8/docs/api/java/util/regex/Pattern.html>.

### Case-sensitive Searches

By default, all character string-type conditions are case insensitive, although analysts can change this through the associated drop-down menu.



Figure 9.7: Drop-down menu to set the comparison type for character string-type fields

The **ParentFilename** and **ChildFilename** fields are stored in the data lake in lowercase because they are taken from the **ParentPath** and **ChildPath** fields respectively. After they are extracted, a normalization process is automatically run in which all uppercase letters are changed to lowercase. Any hunting rule where you specify 'case sensitive' and uses uppercase letters to search in the **ParentFilename** or **ChildFilename** fields will not return any results. However, the **ParentPath** and **ChildPath** fields are not subject to this normalization process and are stored in the data lake as they are. In this case, it makes sense to use the 'case sensitive' or 'case insensitive' options according to the analyst's requirements.

### Results Panel

This panel presents results in table format. For more information about how to filter and search for data within the table, see [Tools for Configuring Lists](#) on page 36.

*You can copy and paste the result table to a text file or an Excel spreadsheet. To do that, click an item in the table and drag the mouse pointer until you select all items you require. Then, press Ctrl-C on your keyboard.*

### Context Menu Associated with Result Tables

When you right-click an item in the table, a context menu opens that shows different options that enable you to quickly access other areas of the analysis console:

Option	Description
<b>Investigate computer</b>	Requires the MUID and DateTime fields. It opens the investigation console to show the events logged on the selected computer, on the specified date.
<b>Add entity of interest</b>	Marks an entity to show it in the <b>Entities of interest</b> sub-panel in the associated investigation to rapidly access the information.
<b>Show computers with parent file</b>	Requires the ParentMD5 field. It searches for computers with events that match the value entered in the ParentMD5 field. See <a href="#">File Investigation: MD5</a> on page 174.
<b>Show computers with child file</b>	Requires the ChildMD5 field. It searches for computers with events that match the value entered in the ChildMD5 field. See <a href="#">From a Newly Created or Ongoing Investigation</a> on page 173.
<b>Automated investigation</b>	Shows a lists of all notebook templates created. When the analyst opens a template, Cytomic Orion automatically populates all compatible parameters in the template with the results of the selected row. See <a href="#">Investigations with Notebooks</a> on page 204.
<b>Computer details</b>	Shows information about the computer. Requires the MUID field.

Table 9.5: Context menu for the result table

# Chapter 10

## Assisted Investigations

Assisted investigations make it easier for an analyst to search for information about an indicator in the data lake. This tool has the advantage of not requiring knowledge of SQL or the database schema that Cytomic Orion uses to store the telemetry gathered from user computers.

An assisted investigation works in a similar way to that of a setup wizard: the process involves a series of searches, which in turn depend on the results generated in the previous steps. As analysts progress through the process, the investigation reveals new searches that enable them to navigate the data lake naturally, as if it were a conversation.

### CHAPTER CONTENTS

---

<b>Create Assisted Investigations and Investigation Context</b> .....	<b>160</b>
Create an Assisted Investigation from a Computer Entity of Interest .....	161
Create an Assisted Investigation from an Indicator .....	161
Create an Assisted Investigation from an Event .....	162
<b>Structure of an Assisted Investigation</b> .....	<b>162</b>
<b>Types of Searches in Assisted Investigations</b> .....	<b>164</b>

## Create Assisted Investigations and Investigation Context

To help refine the analysis, assisted investigations have access to a subset of the entire data lake available in Cytomic Orion. This subset of events is referred to as the context. It is relative to the starting point of the investigation decided by the analyst:

- **Entity of Interest - Computer**
- **Indicator**
- **Event**



Regardless of the investigation starting point, Cytomic Orion always adds the ID of the client to whom the computer belongs to the context, and the computer MUID. It also establishes a period covering the last three days from the moment the assisted investigation began.


Although the context is established the moment an analyst creates the assisted investigation, it can change during the course of the investigation if data is accessed outside the established parameters. In this case, the console shows the message **Investigation scope changed!** and displays the new context to be applied from that moment on.

## Create an Assisted Investigation from a Computer Entity of Interest

When you create an assisted investigation from a Computer entity of interest, Cytomic Orion uses this information to generate the context:

- Unique identifier of the client to whom the computer belongs
- Computer ID
- Three-day period from the creation of the investigation

To create an assisted investigation from a Computer entity of interest:

- In the top menu, select **Investigations**. A list appears and shows all investigations created.
- Select an investigation. The investigation opens with the assigned indicators.
- In the **Entity of interest** panel, click the  icon for a computer. A context menu opens.
- Select **Assisted investigation**. The **Assisted investigation [#Name#]** page opens with the context taken from the selected computer.

## Create an Assisted Investigation from an Indicator

When you create an assisted investigation from an indicator, Cytomic Orion uses this information to generate the context:

- Unique identifier of the client to whom the computer belongs
- Computer ID
- Three-day period from the creation of the investigation

To create an assisted investigation from an indicator:

- In the top menu, select **Investigations**. A list appears and shows all investigations created.
- Select an investigation. The investigation opens with the assigned indicators.
- In the **Indicators** section, right-click on an indicator. A context menu opens.


- Select **Assisted investigation**. The **Assisted investigation [#Name#]** page opens with the context taken from the indicator.

## Create an Assisted Investigation from an Event

When you create an assisted investigation from an event, Cytomic Orion uses this information to generate the context:

- Parent process MD5
- Parent process file name
- Child process MD5
- Child process file name
- Command line
- Unique identifier of the client to whom the computer belongs
- Computer ID
- Three-day period from the creation of the investigation

To create an assisted investigation from an event:

- In the top menu, select **Investigations**. A list appears and shows all investigations created.
- Select an investigation. The investigation opens with the assigned indicators.
- In the **Entities of Interest** section, click the  icon for a computer. A context menu opens.
- Select **Investigate computer**. The investigation console opens with the events logged on the computer for the current day.
- Right-click the event you want to investigate. A context menu opens.
- Select **Assisted investigation**. The **Assisted investigation [#Name#]** page opens with the context taken from the event.

## Structure of an Assisted Investigation

Assisted investigations have a structure based on searches and results. The searches an analyst can run are taken from the current context of the investigation. This way, the investigation shows only the searches available based on the previous result.

**Hello!**  
Start a new assisted investigation

This investigation is for client **WGC-1-CCF8B486C6C147FE8D65** and includes **3** days of data, from **2024-05-24T09:04:03.240000+0000** to **2024-05-27T09:04:03.240Z**: **1**

---

**Computer ID (MUID):** 8225CE94-1BC1-422F-92EB-0B28C37BDF90

How do you want to start the investigation?

---

Select a category: What are you searching for?

2
▼

Alerts in the machine
3
▼

4  
Run

Returns all IoAs in a machine

**Investigation scope changed!**

**Final client:** TESTACTIVITY-1 (previous value: WGC-1-CCF8B486C6C147FE8D65) **6**

**Final date:** 2025-05-11 (previous value: 2024-05-28T07:11:51.436Z)

**Final days:** 1 (previous value: 3)

1

Alerts in the machine 7

muid: [ 8225CE94-1BC1-422F-92EB-0B28C37BDF90 ] 8

9 10  
🗨️ 📷

11
Edit Values

Returns all IoAs for MUID 8225CE94-1BC1-422F-92EB-0B28C37BDF90

Filter...
12

13

Alert Date Time	Muid	Panda Alert Id
2024-05-25 09:19:15	8225CE941BC1422F92EB0B28C37BDF90	81D0681F-D80C-444C-8D66-F97897F3E
2024-05-25 09:19:15	8225CE941BC1422F92EB0B28C37BDF90	B32C0F9F-E6B3-4EA7-875E-AF32ED06C
Total Rows: 120		

Figure 10.1: Assisted investigation overview


Assisted investigations are divided into several sections:

- **Initial context (1):** Shows the client ID, the range of days it covers, and the identifier of the computer to which the investigation refers.
- **Select a category (2):** Filters the search types available based on the context of the investigation.
- **What are you searching for? (3):** Enables you to choose the search on the context defined. Only searches compatible with the data belonging to the context appear.
- **Run (4):** Runs the selected search.
- **Investigation scope changed (6):** If the data selected in the previous result does not belong to the context defined at the beginning of an investigation, a message appears indicating that the context has changed..

- **Search (7):** Search selected in the **What are you searching for?** drop-down menu, along with the sequence number. When an analyst runs a search and the results appear, the sequence number increases and results are added to the assisted investigation in order.
- **Search context (8):** Indicates the subset of context data used by the search.
- **Rate this search (9):** Enables analysts to rate the usefulness of the search.
- **Copy search results to comments (10):** Copies the search and results to the investigation **Comments** section. See **Comments (8)** on page 106.
- **Edit values (11):** Enables analysts to edit the values that make up the context of any search shown in the assisted investigation. If the context of an earlier search changes, a warning message appears and the investigation is deleted from that point on.
- **Result (13):** A table and/or graphic showing the result of the search. Double-click on a table row to expand the information or to define the new context to be used in the next search.
- **Use parent, Use child, Use both:** Use the selected data to assign to the parent process, the child process, or both when generating a new context to run the next search.

## Types of Searches in Assisted Investigations

In an assisted investigation, not all searches are available at all times: the investigation shows only searches compatible with the data set obtained from the result of the previous search.



*See **Format of the Events Used in Cytomic Orion** on page 374 for more information about the meaning of the fields in each result.*

The types of searches available and their description are:

Search name	Description
<p><b>Blocked operations on the computer</b></p>	<p>Returns the operations blocked on a specified computer.</p> <p><b>Input parameters:</b></p> <ul style="list-style-type: none"> <li>• <b>Computer ID (MUID):</b> Computer ID</li> </ul> <p><b>Result:</b></p> <p>List of blocked operation events associated with the computer.</p>
<p><b>Child process hierarchy</b></p>	<p>Returns the child process tree for the specified parent process.</p> <p><b>Input parameters:</b></p> <ul style="list-style-type: none"> <li>• <b>Process (Computer ID/MUID, File MD5, Process ID/PID):</b> Computer ID, file</li> </ul>

Search name	Description
	<p>MD5, process ID</p> <p><b>Result:</b></p> <p>List with the hierarchy of processes.</p>
<p><b>Command line information</b></p>	<p>Shows the decoded command line associated with the specified process and the indicators found.</p> <p><b>Input parameters:</b></p> <ul style="list-style-type: none"> <li>• <b>Computer ID (MUID):</b> Computer ID</li> <li>• <b>Command line:</b> Command line associated with the process</li> </ul> <p><b>Result:</b></p> <p>List of indicators found on the command line.</p>
<p><b>Computer indicators</b></p>	<p>Returns the list of indicators found on the specified computer.</p> <p><b>Input parameters:</b></p> <ul style="list-style-type: none"> <li>• <b>Computer ID (MUID):</b> Computer ID</li> </ul> <p><b>Result:</b></p> <p>List with the indicators found. For details, click an indicator. See <a href="#">Indicators List</a> on page <a href="#">66</a></p>
<p><b>Computer information by MUID or IP address</b></p>	<p>Returns information about the characteristics of a specified computer.</p> <p><b>Input parameters:</b></p> <ul style="list-style-type: none"> <li>• <b>Client:</b> Client ID</li> <li>• <b>Computer ID (MUID):</b> Computer ID</li> <li>• <b>Computer IP address:</b> IP address of the computer</li> </ul> <p><b>Result:</b></p> <p>Information about the characteristics of the computer. See <a href="#">Computer Details</a> on page <a href="#">112</a>.</p>
<p><b>Computer process activity</b></p>	<p>Returns the events logged on a specified computer.</p> <p><b>Input parameters:</b></p> <ul style="list-style-type: none"> <li>• <b>Computer ID (MUID):</b> Computer ID</li> <li>• <b>Process (Computer ID/MUID, File MD5, Process ID/PID):</b> Computer ID, file</li> </ul>

Search name	Description
	<p>MD5, process ID</p> <p><b>Result:</b></p> <p>List of the events with the operations logged on the computer.</p>
<p><b>Computer process indicators</b></p>	<p>Returns the list of indicators associated with a process on the specified computer.</p> <p><b>Input parameters:</b></p> <ul style="list-style-type: none"> <li>• <b>Process (Computer ID/MUID, File MD5, Process ID/PID):</b> Computer ID, file MD5, process ID</li> </ul> <p><b>Result:</b></p> <p>List with the indicators found. For details, click an indicator. See <a href="#">Indicators List</a> on page 66</p>
<p><b>Computers with a specific file</b></p>	<p>Returns a list of computers where a file you specified by its name was seen.</p> <p><b>Input parameters:</b></p> <ul style="list-style-type: none"> <li>• <b>File Name:</b> File name</li> </ul> <p><b>Result:</b></p> <p>List of computers where the file was seen.</p>
<p><b>Computers with a specific MD5</b></p>	<p>Returns a list of computers where a file you specified by its MD5 hash was seen.</p> <p><b>Input parameters:</b></p> <ul style="list-style-type: none"> <li>• <b>MD5:</b> File MD5 hash</li> </ul> <p><b>Result:</b></p> <p>List of computers where the file was seen.</p>
<p><b>Connections to a specific URL</b></p>	<p>Returns a list of computers that connected to a specified URL.</p> <p><b>Input parameters:</b></p> <ul style="list-style-type: none"> <li>• <b>Host Name:</b> Computer name</li> </ul> <p><b>Result:</b></p> <p>List with the computers that connected to the URL.</p>
<p><b>External MD5 information</b></p>	<p>Returns information provided by external sources about the file specified by its MD5.</p>

Search name	Description
	<p><b>Input parameters:</b></p> <ul style="list-style-type: none"> <li>• <b>Computer ID (MUID):</b> Computer ID</li> <li>• <b>MD5:</b> File MD5 hash</li> </ul> <p><b>Result:</b></p> <p>Information supplied by external sources:</p> <ul style="list-style-type: none"> <li>• VirusTotal</li> <li>• WHOIS</li> <li>• Urlscan.io</li> <li>• AbuseIPDB</li> <li>• AlienVault OTX</li> <li>• IBM X-Force</li> <li>• Intel471</li> </ul>
<p><b>File activity on the computer</b></p>	<p>Returns events related to the file specified by name.</p> <p><b>Input parameters:</b></p> <ul style="list-style-type: none"> <li>• <b>Computer ID (MUID):</b> Computer ID</li> <li>• <b>File Name:</b> File name</li> </ul> <p><b>Result:</b></p> <p>List of events related to the file.</p>
<p><b>File modifications</b></p>	<p>Returns a list of create, edit, and delete operations for the file specified by the name or MD5 hash. The protection software does not monitor all files on a computer, only those that:</p> <ul style="list-style-type: none"> <li>• Contain certificates or passwords</li> <li>• Run automatically when the operating system starts up</li> <li>• Are run from the task scheduler</li> <li>• Are stored in folders that are not used frequently</li> <li>• Are accessed by uncommon applications.</li> </ul> <p>The list of operations performed on a file is not always available when the file is specified by its MD5.</p> <p><b>Input parameters:</b></p>

Search name	Description
	<ul style="list-style-type: none"> <li>• <b>MD5:</b> File MD5 hash</li> <li>• <b>File Name:</b> File name</li> </ul> <p><b>Result:</b></p> <p>List of create, edit or delete events associated with the file.</p>
<p><b>File names associated with a URL</b></p>	<p>Returns a list of files stored on the computer downloaded from a specified URL.</p> <p>Select a file from the list to show a list of connections involved in downloading that specific file.</p> <p><b>Input parameters:</b></p> <ul style="list-style-type: none"> <li>• <b>Host Name:</b> Computer name</li> </ul> <p><b>Result:</b></p> <p>List of files associated with the URL.</p>
<p><b>File names for an MD5</b></p>	<p>Returns a list of file names for the specified MD5 hash.</p> <p><b>Input parameters:</b></p> <ul style="list-style-type: none"> <li>• <b>MD5:</b> File MD5 hash</li> </ul> <p><b>Result:</b></p> <p>List of file names.</p>
<p><b>IP address information</b></p>	<p>Returns a table with information provided by external sources about the specified IP address.</p> <p><b>Input parameters:</b></p> <ul style="list-style-type: none"> <li>• <b>IP address:</b> IP address of the computer</li> </ul> <p><b>Result:</b></p> <p>Information supplied by external sources:</p> <ul style="list-style-type: none"> <li>• VirusTotal</li> <li>• WHOIS</li> <li>• Urlscan.io</li> <li>• AbuseIPDB</li> <li>• AlienVault OTX</li> <li>• IBM X-Force</li> </ul>



Search name	Description
	<ul style="list-style-type: none"> <li>• Intel471</li> </ul>
<b>Login and logout information</b>	<p>Returns logins and logouts for the specified computer.</p> <p><b>Input parameters:</b></p> <ul style="list-style-type: none"> <li>• <b>Computer ID (MUID):</b> Computer ID</li> </ul> <p><b>Result:</b></p> <p>List with logins and logouts.</p>
<b>Logins and logouts on a client computers</b>	<p>Returns logins and logouts for the specified user.</p> <p><b>Input parameters:</b></p> <ul style="list-style-type: none"> <li>• <b>User:</b> User ID</li> </ul> <p><b>Result:</b></p> <ul style="list-style-type: none"> <li>• Line chart with login and logout attempts logged on the computer.</li> <li>• Table with information about login and logout attempts grouped by computer. Select a computer from the table to show the details of each login.</li> </ul>
<b>MD5 activity on a computer</b>	<p>Returns the activity of the file specified by its MD5 on a computer.</p> <p><b>Input parameters:</b></p> <ul style="list-style-type: none"> <li>• <b>Computer ID (MUID):</b> Computer ID</li> <li>• <b>MD5:</b> File MD5 hash</li> </ul> <p><b>Result:</b></p> <p>List of events related with the MD5 on the computer.</p>
<b>MD5 activity on client computers</b>	<p>Returns the activity of the file specified by its MD5 on all the client's computers.</p> <p><b>Input parameters:</b></p> <ul style="list-style-type: none"> <li>• <b>MD5:</b> File MD5 hash</li> </ul> <p><b>Result:</b></p> <p>List of events related with the MD5 on all the client's computers.</p>
<b>MD5s for a file name</b>	<p>Returns the names of all files seen on the client's computers for the specified MD5.</p>

Search name	Description
	<p><b>Input parameters:</b></p> <ul style="list-style-type: none"> <li>• <b>File Name:</b> File name</li> </ul> <p><b>Result:</b></p> <p>List of MD5s.</p>
<p><b>URLs associated with a file</b></p>	<p>Returns a list of URLs that contain the file specified by its name.</p> <p><b>Input parameters:</b></p> <ul style="list-style-type: none"> <li>• <b>File Name:</b> File name</li> </ul> <p><b>Result:</b></p> <p>List of URLs that contain the file name.</p>
<p><b>URLs associated with an MD5</b></p>	<p>Returns a list of URLs that contain the file specified by its MD5 hash.</p> <p><b>Input parameters:</b></p> <ul style="list-style-type: none"> <li>• <b>MD5:</b> File MD5 hash</li> </ul> <p><b>Result:</b></p> <p>List of URLs related to the MD5.</p>
<p><b>URLs associated with a user</b></p>	<p>Returns the URLs accessed by the specified user ID.</p> <p><b>Input parameters:</b></p> <ul style="list-style-type: none"> <li>• <b>User:</b> User ID</li> </ul> <p><b>Result:</b></p> <p>List of URLs accessed by the user.</p>
<p><b>USB devices</b></p>	<p>Returns a list of USB devices connected to the computer specified by its MUID.</p> <p><b>Input parameters:</b></p> <ul style="list-style-type: none"> <li>• <b>Computer ID (MUID):</b> Computer ID</li> </ul> <p><b>Result:</b></p> <p>List of USB devices connected to the computer with their characteristics.</p>
<p><b>User activity on client computers</b></p>	<p>Returns the activity of the specified user on the client's computers.</p> <p><b>Input parameters:</b></p> <ul style="list-style-type: none"> <li>• <b>User:</b> User ID</li> </ul>

Search name	Description
	<p><b>Result:</b></p> <p>List with a summary of the activity of the user on the client's computers.</p>
<p><b>User activity on a computer</b></p>	<p>Returns the activity of the specified user on the specified computer.</p> <p><b>Input parameters:</b></p> <ul style="list-style-type: none"> <li>• <b>Computer ID (MUID):</b> Computer ID</li> <li>• <b>User:</b> User ID</li> </ul> <p><b>Result:</b></p> <p>List of the user activity on the computer.</p>
<p><b>User indicators</b></p>	<p>Returns a list of indicators associated with the specified user on all the client's computers.</p> <p><b>Input parameters:</b></p> <ul style="list-style-type: none"> <li>• <b>User:</b> User ID</li> </ul> <p><b>Result:</b></p> <p>List of indicators associated with the user on the client's computers.</p>
<p><b>Users associated with connections to a specific computer</b></p>	<p>Returns the users who accessed the specified URL.</p> <p><b>Input parameters:</b></p> <ul style="list-style-type: none"> <li>• <b>User:</b> User ID</li> </ul> <p><b>Result:</b></p> <p>List of the users who accessed the URL.</p>

Table 10.1: Searches available in an assisted investigation

# Chapter 11

## Indicator Analysis Using the Investigation Console

Unlike the **Advanced SQL Query** module, which enables you to carry out analyses across the entire data lake generated by a client's IT infrastructure, the investigation console enables you to analyze events in depth on specific computers and specific dates. This resource provides all necessary tools for analysts to inspect the processes run on a computer in detail, and to graphically review information about their activity and relationships with other processes or items in the operating system.



*The retention period for the telemetry stored in the data lake is one year.*

### CHAPTER CONTENTS

---

<b>Access the Investigation Console</b> .....	<b>172</b>
From a Newly Created or Ongoing Investigation .....	173
From an Indicator .....	175
From the Investigation Console .....	176
From the Cytomic Orion API .....	176
<b>Investigation Console Structure</b> .....	<b>177</b>
Filters Side Panel .....	179
Central Panel .....	180

## Access the Investigation Console

Analysts can access the investigation console in different ways depending on the stage of the investigation:

- **From an investigation:** Shows events related to an identity belonging to the context of an investigation.
- **From an indicator:** Shows events related to a computer.
- **From the investigation console:** Searches for computers related to an event.
- **From the Cytomic Orion API:** Enables you to analyze items without associating them with existing investigations or indicators.

## From a Newly Created or Ongoing Investigation

To analyze an item belonging to an investigation:

- in the top menu, select **Investigations**. Create a new investigation. In the toolbar, click the **+** icon. Select **Computer investigation**. A dialog box opens where you can enter the details of the computer you want to analyze and the dates for the investigation.

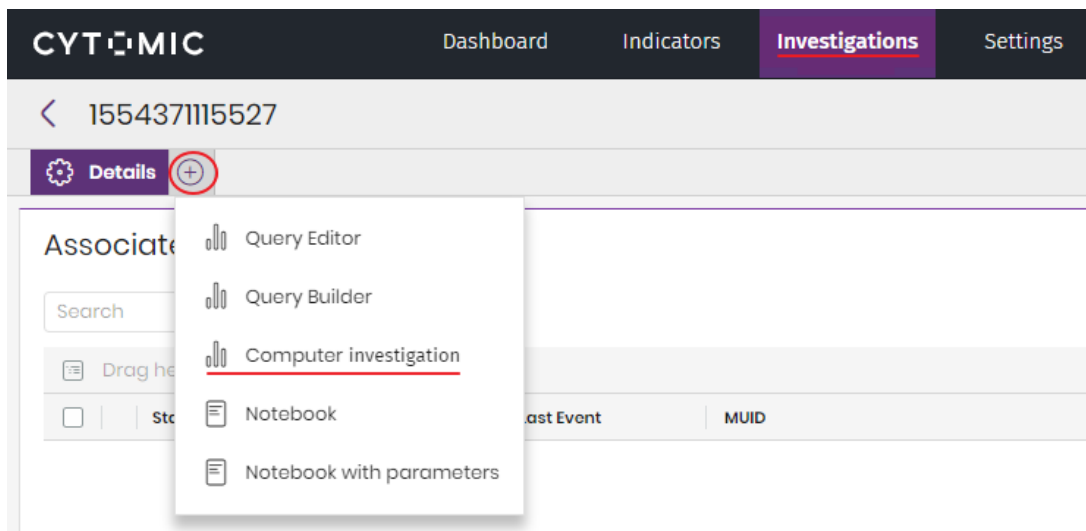


Figure 11.1: Investigation console access menu

- Select a checkbox depending on the item you want to investigate:
  - **MUID**
  - **MD5**
  - **MUID + MD5**
  - **Computer name**
- Enter the required information depending on the item you selected. The following sections detail the type of data required.

## Computer Investigation: MUID

- Enter the unique identifier of the computer you want to analyze, the time period for the investigation (maximum 48 hours), and the time zone for the period. To speed up the selection, click the **MUID** text box. A list opens that shows all compatible entities of interest created in the investigation. You can also enter an **MUID** directly.
- If you do not know the computer MUID, see [Tool for Converting a Computer Name to an MUID](#) on page 41.
- Click **OK**. A new tab is created that shows the computer name and its MUID in parenthesis. This tab contains the events found on the selected computer during the specified period.

## File Investigation: MD5

- Enter the hash of the file you want to investigate. To speed up the selection, click the **MD5** text box. A list opens that shows all compatible entities of interest created in the investigation.
- Click **OK**. A new tab is created that shows the file **MD5**. This tab contains the **Found computers** panel, which shows a list of all computers that have generated events associated with the target file MD5, as well as the date on which the events occurred and this information:

Machines found ⏪

muid	pandaaid	lastseen	firstseen	lastpath
331C892184F7FC656E0E46064...	82830995	2019/23/04 15:24:16	2018/16/07 10:21:53	WINDOWS
3975621EE914E882001616404C...	82830995	2018/06/12 09:32:...	2018/11/07 17:24:33	WINDOWS
6F95107DEB8C4694B56842BC...	82830995	2018/15/10 09:34:35	2018/22/08 17:22:...	WINDOWS
A49C8B5DF8CDE769C6658A1...	82830995	2018/22/07 23:55:...	2018/22/07 23:55:...	WINDOWS
A8A647C773EA3B404B319353...	82830995	2019/11/04 16:02:05	2019/16/03 11:21:56	WINDOWS
B38FE9B26F652F20150681C89...	82830995	2019/03/05 02:40:...	2019/25/03 08:58:...	WINDOWS

Figure 11.2: Found Computers panel

- **MUID**: The unique identifier of the computer where the events related to the file MD5 occurred.
- **Pandaaid**: The unique identifier of the client to which the computer belongs.
- **Lastseen**: The date on which an event that involves the file MD5 found on the selected computer was last logged.
- **Firstseen**: The date on which an event that involves the file MD5 found on the selected computer was first logged.
- **Lastpath**: The last logged path of the item found on the computer.

At the top of the panel, you can see a tool area:

- **Search:** A filter tool that enables you to type only a partial string. Searches are performed on the content of all columns in the list.
- **Number of results:** Number of entries shown in the list.

## Investigation of a File on a Computer: MUID and MD5

- Enter the unique identifier of the computer and the hash of the file you want to investigate. To speed up the selection, click the **MUID** and **MD5** text boxes. A list opens that shows all compatible entities of interest created in the investigation. You can also enter an **MUID** and an **MD5** directly.
- If you do not know the computer MUID, see [Tool for Converting a Computer Name to an MUID](#) on page 41.
- Click **OK**. A new tab is created that contains the **Found computers** panel, which shows a list of all computers that have generated events associated with the target file MD5, as well as the date on which the events occurred. See [File Investigation: MD5](#).

## Computer Investigation by Name

- Enter the name of the Windows computer you want to analyze, the time period for the investigation, and the time zone for the period.
- Select the client to which the computer belongs, because a computer name could belong to multiple clients.
- Click **OK**. A new tab is created that shows the computer name and its MUID in parenthesis. This tab contains data for the selected computer during the specified period.

## From an Indicator

### Investigation of a Computer Events

To carry out an in-depth investigation of a computer associated with an indicator generated by Cytomic Orion:

- In the top menu, select **Investigations**. Select the investigation that contains the indicator you want to analyze, or assign the indicator to a new investigation. For more information about how to assign one or more indicators to an investigation, see [Manually Assign and Remove Indicators from Investigations](#) on page 96.
- In the **Indicators** panel for the investigation, right-click the indicator you want to analyze. A drop-down menu appears.
- Select **Show computer events**. A new tab opens that shows the computer name and its MUID in parenthesis. This tab shows the events occurred on the computer associated with the indicator and the dates when they occurred.

## From the Investigation Console

### File Investigation

Cytomic Orion enables you to perform guided searches to find computers on the network where events have been logged on a specific file. Follow these steps:

- Open the investigation console by using any of the methods described in this section.
- Select the event in question. The **parentfilename** and **childfilename** fields contain the files involved in the event.
- Right-click the event. In the context menu that opens, choose one of these options:
  - **Show computers with parent file:** Searches for the MUIDs of the client's computers where the parent file was seen.
  - **Show computers with child file:** Searches for the MUIDs of the client's computers where the child file was seen.
- After you have selected an option, a page opens that shows two panels where you can select a computer to view its events. For a detailed description of the panels, see [Investigation Console Structure](#).

## From the Cytomic Orion API

In cases where you start a threat hunting job through the Cytomic Orion API, you can access the investigation console without having first created an investigation. In such cases, you can build a URL that enables you to directly open the investigation console to view the relevant events.

### File Investigation: MD5

The URL format is as follows:

<b>Command</b>	GET
<b>URL</b>	https://orion.cytomicmodel.com/forensics/md5/{md5}
<b>Required parameters in the URL</b>	<b>md5:</b> File hash.

Table 11.1: Format of the URL to open the investigation console for a file

### Computer Investigation: MUID

The URL format is as follows:

<b>Command</b>	GET
<b>URL</b>	https://orion.cytomicmodel.com/forensics/muid/{muid}?dateFrom={dateFrom}&dateTo={dateTo}&timezone={timezone}
<b>Required</b>	<ul style="list-style-type: none"> <li>• <b>MUID:</b> Computer identifier.</li> </ul>



<b>parameters in the URL</b>	<ul style="list-style-type: none"> <li>• <b>dateFrom</b>: Unix timestamp in milliseconds that shows the start date of the range of dates for which you want to show events.</li> <li>• <b>dateTo</b>: Unix timestamp in milliseconds that shows the end date of the range of dates for which you want to show events.</li> </ul>
<b>Optional parameters in the URL</b>	<ul style="list-style-type: none"> <li>• <b>timezone</b>: Time zone of the dates specified in the URL. If you do not specify it, the time zone set in the user account settings is used.</li> </ul>

Table 11.2: Format of the URL to open the investigation console for a computer

## Investigation of a File on a Computer: MD5 and MUID

The URL format is as follows:

<b>Command</b>	GET
<b>URL</b>	https://orion.cytomicmodel.com/forensics/muid/{muid}/md5/{md5}
<b>Required parameters in the URL</b>	<ul style="list-style-type: none"> <li>• <b>MUID</b>: Computer identifier.</li> <li>• <b>MD5</b>: File hash.</li> </ul>

Table 11.3: Format of the URL to open the investigation console for a file on a computer

## Investigation Console Structure

The investigation console is divided into multiple panels, depending on how you access it:

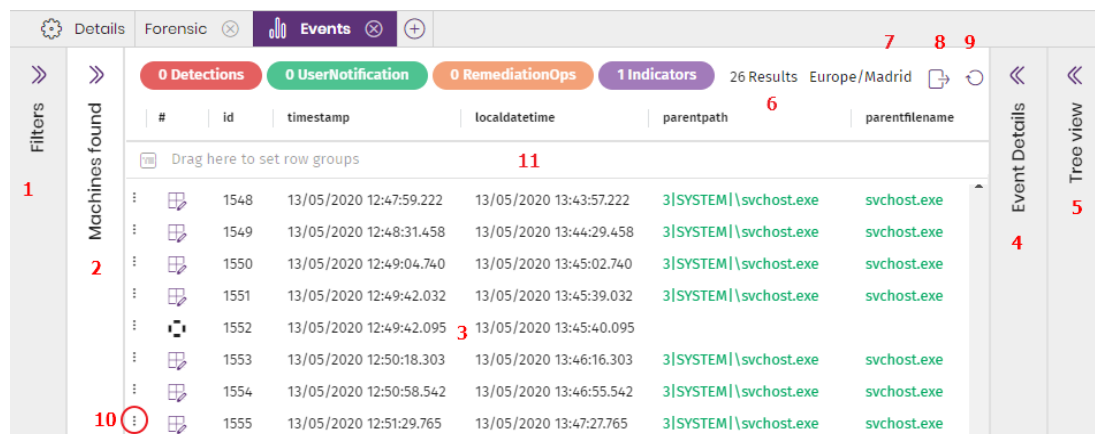


Figure 11.3: Investigation console panels

- **Filters left panel (1)**: Set filters and configure the way data is presented in the central and right panels to meet your needs.
- **Found computers side panel (2)**: If you started the investigation from a file MD5 (see [File Investigation: MD5](#)), a panel appears that shows a list of computers where events related to the

specified file were found.

- **Central panel (3)**: Shows a list of events found on the selected date and, optionally, a timeline.
- **Event details right panel (4)**: Shows fields for the event selected in the central panel
- **Process tree panel (5)**: Shows the parent-child hierarchy of all the processes and items logged on the specified date.
- **Number of results (6)**
- **Date (7)**: Set the time zone for the dates shown in the event list (3).
- **Export list (8)**: Downloads the list of events in CSV format to the analyst computer.
- **Refresh list (9)**
- **Context menu (10)**: Shows the actions analysts can take on the event.
  - Show computer events
  - Show computers with parent file
  - Show computers with child file
  - Execute notebook with parameters
  - Add entities of interest
  - Computer details
- **Tools for configuring the list (11)**: For more information about how to group the data in the list by columns and other resources for configuring how the event list is shown, see [Tools for Configuring Lists](#) on page 36.




## Filters Side Panel

The screenshot shows a mobile-style interface for the 'Filters' side panel. At the top, there's a title 'Filters' and a back arrow. Below that, the 'Computer' section displays 'MITREW10'. The 'Date' section has 'From' and 'To' fields, both showing '21/09/2023' with a calendar icon, and time pickers for '00:00' and '23:59'. The 'Time zone' is set to 'Europe/Madrid'. A prominent purple 'Apply' button is below. The 'Results' section has a search bar. 'Tactics' and 'Techniques/sub-techniques' each have an empty input field with '+' and 'i' icons. 'Indicators associated with events' has a '+ Add indicator' button. Finally, 'Options' includes checkboxes for 'Process tree' and 'Timeline'.

Figure 11.4: Filters panel

This panel shows global information about the investigation performed and enables you to filter and search for events of interest to draw conclusions.

- **Computer:** Shows the name or MUID of the investigated computer.
- **MD5:** Shows the MD5 of the file analyzed in the investigation.
- **Date:** Shows the time period for the investigation. When you click the text boxes, a calendar appears for you to change the date interval. The maximum period is 48 hours.
- **Time zone:** Set a time zone for the search. Results will appear in the central panel with the time zone you define,

- **Results:** Filters the event list by the content you enter in the text box. Searches are performed on all the columns of the entries in the list. You can type only a partial string.
- **Tactic:** To filter by tactic, enter part of the tactic name or click the  icon. A list appears that shows the tactics associated with the events in the list.
- **Technique/Sub-technique:** To filter by technique or sub-technique, enter part of the technique or sub-technique name or click the  icon. A list appears that shows the techniques or sub-techniques associated with the events in the list.
- **Add indicator:** To filter by indicator, enter part of the indicator name or click the  icon. A list appears that shows the indicators associated with the events in the list.
- **Options:** Enable or disable the timeline of events shown in the central panel and the process tree shown in the **Process tree** panel.

## Central Panel

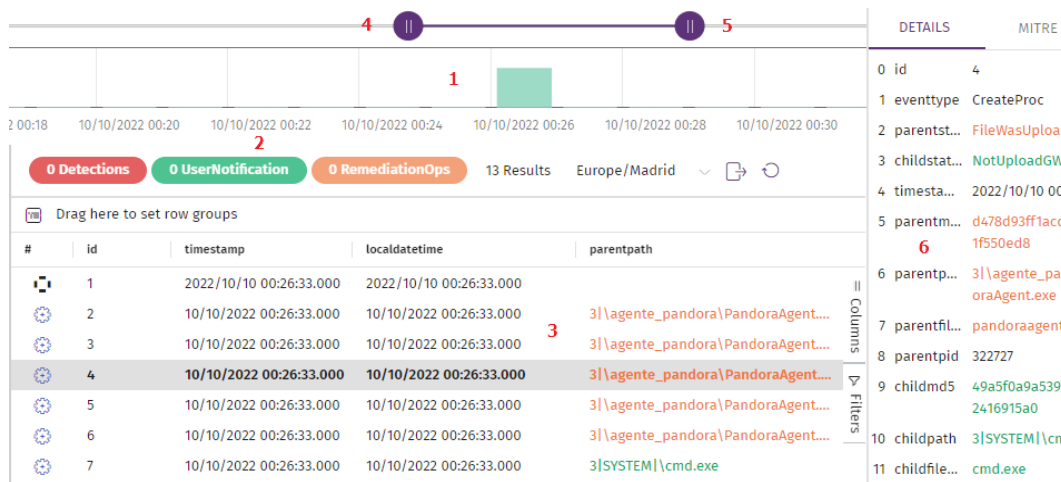


Figure 11.5: Analysis console central panel

This panel shows the list of events that corresponds to the computer and date you specify in the side panel (**Computer** and **Date** fields). The central panel is divided into three areas:

- **Bar graph (1):** Graphically shows the number of events in five-minute intervals. A large number of events in a short period of time could indicate activity related to an attack. See **Bar Graph**.
- **Events panel information bar (2):** Indicates the subset of events shown in the graph over the total number of events logged on the investigated computer on the specified day. See **Information Bar**.
- **Events sub-panel (3):** Shows the events monitored and collected by Cytomic Orion on the investigated computer on the specified day,



For more information about how to interpret and use the date-type fields in events, see [Meaning of Date-type Fields on page 150](#).

## Bar Graph

This graph shows the number of events occurred per unit of time on the Y axis, and the time stamp in hour:minutes format on the X axis. Move your mouse cursor over the graph to see the number of events logged at the relevant time.

After you select a date in the side panel, you can change the time interval to focus on the activity logged at a specific time or change the interval shown. To do this, use the buttons (5) in the top bar (4), or the time configuration settings (1).

### Top Bar (4)

Click the center of the bar and drag it left or right to change the interval for the activity shown in the graph.

### Top Bar Buttons (5)

Click the buttons in the top bar and drag them left or right to change the time range for the activity shown in the graph

### Details Panel (6)

Select an event in the list (3) to open the Details and MITRE panel. For more information, see [Details and MITRE Side Panel](#).

### Bar Graph (1)

Click anywhere in the graph and drag your mouse cursor to define a new window to view the activity. The graph updates with a new zoom level and a new time period for the data shown.

## Information Bar




Figure 11.6: Investigation console information bar

- (1) Color labels that show the number of found events. Click a label to open a floating panel that shows the events of the selected type. Click an event. The panel hides and the event appears selected in the events sub-panel. The available types of events are these:
  - **Detections:** Threat detection events generated by the security software installed on the workstation or server.
  - **UserNotification:** Events that involved showing a pop-up window to the user, prompting for an action that could affect the security of the computer.
  - **RemediationOps:** Events that involved the security software installed on the computer taking

action.

- **Indicators:** Generated indicators.




*For a description of the fields in each event type, see [Format of the Events Used in Cytomic Orion](#) on page 374.*

- (2) Number of entries shown in the events sub-panel.
- (3) **Time zone:** Set a time zone for the events shown.
- (4) **Export:** Download a file in CSV format that contains the list of events.
- (5) **Refresh:** Requests the list from the server and updates the events shown.







### Events Sub-panel





















This panel shows the events monitored on the computer and collected by Cytomic Orion. The information appears in a table that provides access to the filtering, sorting, and search tools described in [Tools for Configuring Lists](#) on page 36.



*With particularly long lists, the panel shows the first 150,000 events that occurred in the selected time period. In such case, the message **Showing the first 150,000 events for the selected time range** appears. To show events that might have been lost, configure a new time range.*

The events sub-panel consists of a number of columns that describe each event. The first column shows an icon that represents the type of event logged.

Icon	Description	Icon	Description
	Process created		Executable file created
	Executable file edited		Library loaded
	Executable program deleted		Executable file edited

Icon	Description	Icon	Description
	Directory created		Compressed file created
	Compressed file opened		Registry entry created that points to an executable file
	Registry entry edited that points to an executable file		Remote process thread created
	Exploit detected		Unclassified event
	File downloaded		Network operation
	Unknown process that was not blocked because there is no interactive session on the computer		Document opened
	Registry operation		Script file created
	Script file run		Threat detected
	Size of data transmitted over the network		WMI event logged by SYSMON which modifies the computer operating system settings
	Failed DNS resolution		Device control operation










Icon	Description	Icon	Description
	The agent showed a pop-up message on the user computer		Start of an interactive session on the computer
	End of an interactive session on the computer		Action taken by the security software installed on the computer
	Internal administrative event		Computer restart
	Operation performed by an executable file whose creation was not logged		The security software detected an executable file whose creation was not logged either because of a temporary problem or because the file existed before the security software was installed
	Remote process created		

Table 11.4: Event icons and descriptions

When you right-click an event or the corresponding icon, a context menu opens and shows these options:

- **Show computer events:** Opens a new tab that shows the events logged on the computer.
- **Show computers with parent file:** Opens a new tab in the investigation console that shows a list of computers where events were logged that involved the event parent file.
- **Show computers with child file:** Opens a new tab in the investigation console that shows a list of computers where events were logged that involved the event child file.
- **Execute notebook with parameters:** Opens a new tab with a notebook. See [Access and Create Notebooks](#) on page 208.
- **Add entities of interest:** Adds an entity of interest to the investigation. See [Entities of Interest Panel](#) on page 107.
- **Computer details:** Shows basic information about the hardware and Cytomic security software installed on the computer. See [Computer Details](#) on page 112.

## Details and MITRE Side Panel

When you select an event, a side panel opens that shows two tabs: **Details** and **MITRE**. This panel contains all the telemetry collected for the event and information from MITRE regarding the associated tactics and



techniques.

- For more information about the meaning of the fields on the **Details** tab, see chapter **Format of the Events Used in Cytomic Orion** on page 374.
- For more information about the data on the **MITRE** tab, see **Details Panel** on page 69

### Show AMSI (AntiMalware Scan Interface) Buffer

SystemOps events can store the content of the AMSI buffer with the script that generated the event. To show the AMSI buffer:

- In the events sub-panel, select a SystemOps event. The event fields appear in the **Event details** side panel.
- Click the **View script** link. A dialog box opens that shows the content of the stored script.
- To copy the script to the clipboard, click **Copy**.
- To download the script to the analyst computer, click **Download**.

### Show Static Information for the File Associated with an Event

Cytomic Orion can show static data for a binary file if the data was previously sent to Cytomic servers. Files are automatically sent as part of the typical scanning and classification processes performed by the security software installed on the user computer.



*Sometimes, the Cytomic server has the files requested by the analyst, but the scan has not started or finished. In this case, the console shows a message that prompts the analyst to retry the operation a few minutes later.*

To show static information for a file:

- Select an event associated with a binary file (for example, a CreateProc event). The event fields appear in the **Event details** side panel.
- If Cytomic Orion can access static information for the file, it shows the **Show static information** section associated with the parent process and the child process.
- Click **Show static information**. A tab opens that shows these sections:
  - **File capabilities**: Technique, tactic, and description of the file features.
  - **Strings**: Character strings found in the file.
  - **Sections**: Shows the different sections in the binary file. For more information, see <https://learn.microsoft.com/en-us/archive/msdn-magazine/2002/february/inside-windows-win32-portable-executable-file-format-in-detail> and <https://learn.microsoft.com/en-us/archive/msdn-magazine/2002/march/inside-windows-an-in-depth-look-into-the-win32-portable-executable-file-format-part-2>.

- **Imports:** Functions the file imports to be able to run.
- **Exports:** Functions the file exports.

## Process Tree Panel

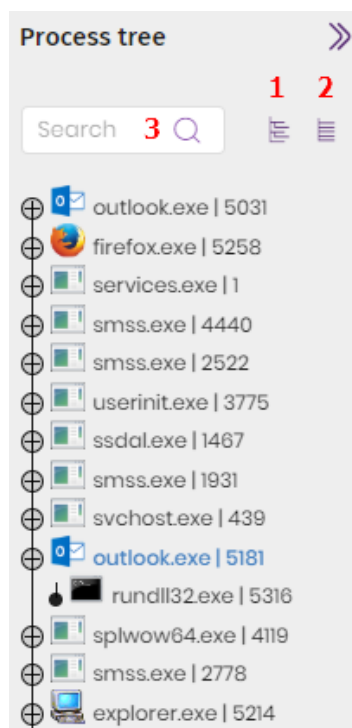


Figure 11.7: Process tree

This tree shows the hierarchy of all the processes run on the computer. For each notebook, this information appears:

- Process icon.
- Name of the executable file that generated the process in memory.
- Process ID (PID).

The process tree enables you to take these actions:

- To show the child processes of a process, click the  $\oplus$  icon.
- To find an event associated with a process, select the process in the process tree. Click the event. The event appears selected in the events sub-panel.
- To collapse or expand the tree branches, click the **(1)** and **(2)** icons.
- To filter the process tree, use the text box **(3)**. The tree shows only the processes that contain part of or the complete string you specify.



# Chapter 12

## Graphs

The execution flow of a cyberattack is made up of multiple processes and operations that are logged in the Cytomic Orion data lake. Because of this, and given the massive amount of information that SOC analysts have to process, Cytomic Orion provides a special type of notebook that makes viewing and interpreting such data easier. This resource uses a special type of diagram, known as 'graph', which illustrates events with nodes and arrows to show entities and the relationship between them.

The information shown on a graph is equivalent to the information shown in the investigation console or in advanced queries, but organized and presented in a clearer, easier-to-interpret way.



*The retention period for the telemetry stored in the data lake is one year.*

### CHAPTER CONTENTS

---

<b>Access Graphs</b> .....	<b>188</b>
<b>Information Shown on Graphs</b> .....	<b>189</b>
<b>Graph Structure</b> .....	<b>190</b>
<b>Graph Settings</b> .....	<b>191</b>
<b>Information Contained in Graphs</b> .....	<b>198</b>
Process Tree Template .....	198
New Users in a Client Template .....	202

## Access Graphs

There are two ways for SOC technicians to view a graph representing the events logged on a computer, depending on the phase of the analysis:

- From an investigation created by a Tier 1 technician, by adding a graph-type notebook.
- From the investigation console, when the analyst identifies a suspicious item.

## From an Investigation



*For more information about how to create and access an investigation, see [Manage Investigations](#) on page 92.*

Open the investigation where the chain of events suspected of belonging to a cyberattack is found.

- In the **Files** panel in the lower-right corner of the page, click the **+** icon. A context menu opens.

Or

- In the toolbar at the top of the page, click the **+** icon. A context menu opens.
- Select **Graphs**. The **New graphical investigation** dialog box opens. This dialog box shows a list of all graph templates defined.
- Select a template based on the type of data you want the graph to show. For more information about the available templates, see [Information Shown on Graphs](#). If the template requires parameters, a form is shown for you to enter the necessary information.

## From the Investigation Console



*For more information about how to access and use the investigation console, see [Indicator Analysis Using the Investigation Console](#) on page 172.*

Open the investigation console. Find a computer on the network that contains an event suspected of belonging to an attack sequence:

- Right-click the event you want to investigate. A context menu opens.
- Select **Graphs**. The **New graphical investigation** dialog box opens. This dialog box shows a list of all graph templates defined.
- Select a template based on the type of data you want the graph to show. For more information about the available templates, see [Information Shown on Graphs](#). If the template requires parameters, a form is shown for you to enter the necessary information.

## Information Shown on Graphs

To narrow the type of information shown on a graph, analysts have templates that enable them to:

- Limit the type of information shown based on the selected template.
- Set the parameters of the graph to show entities of interest to the analyst and the relationship between them, within the type of information selected.

## Available Graph Templates

- **Process Tree:** A parameterized template that shows processes and the relationship between them and other entities in the selected interval. For more information about how to use a graph generated with this template, see [Process Tree Template](#).
- **New users in a client:** A parameterized template that shows new users who logged in to the client's computers. To do this, it collects all users who logged in in a previous period taken as reference, and compares them to the users who logged in in the period to analyze. For more information about how to use a graph generated with this template, see [New Users in a Client Template](#).

## Graph Structure

This section provides a description of the information panels and tools available in a graph:

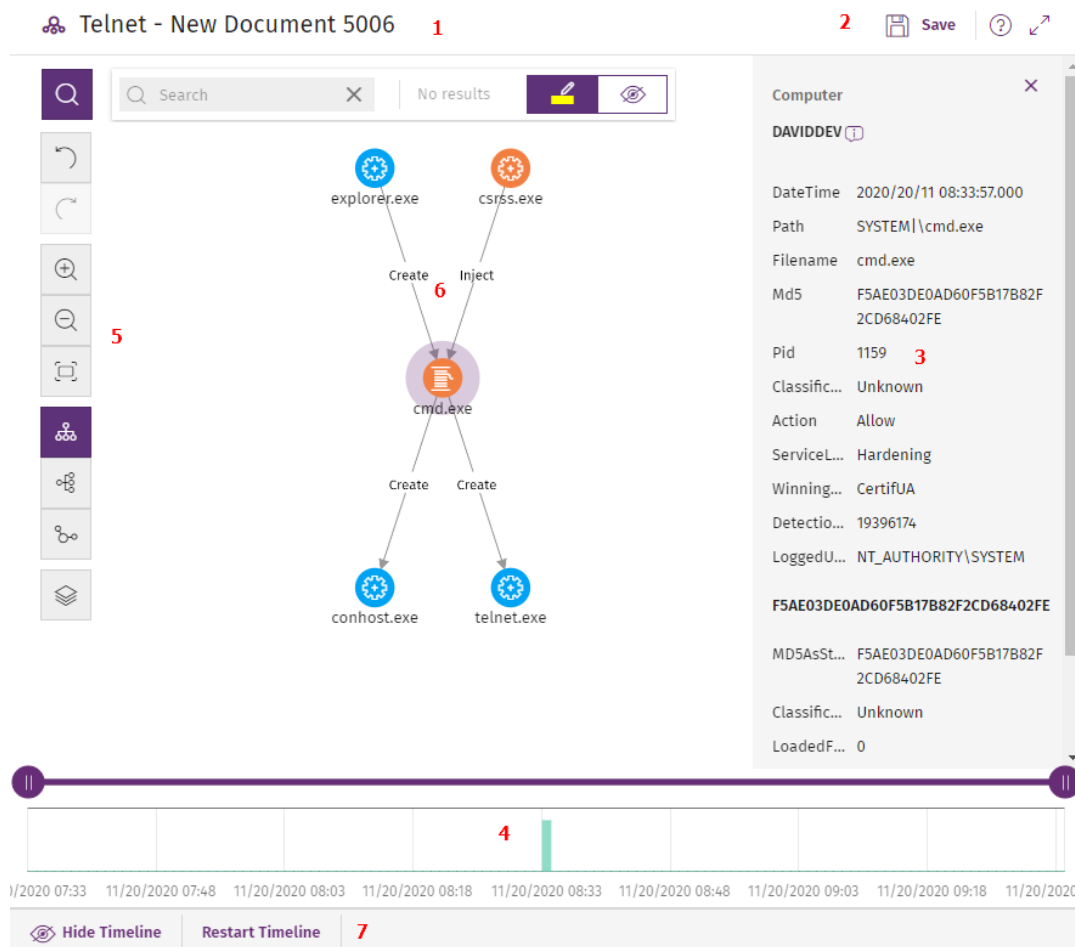





Figure 12.1: Graph and tools

- **Graph name (1):** Click a graph name to edit it.
- **Notebook toolbar (2):**
  - Click  to save changes to the graph within the context of an investigation.
  - Click  to open the web help for information about a graph feature.
  - Click  to maximize or minimize the graph.
- **Information panel for the selected item (3):** Shows information pertaining to the selected node or line. For more information about the meaning of the fields in the panel, see chapter [Format of the Events Used in Cytomic Orion](#) on page 374.
- **Timeline (4):** Shows a histogram with green bars that represent the events carried out by a threat. You can increase or reduce the interval at which the events shown occurred. For more information about how to use this resource, see [Timeline](#).
- **Graph toolbar (5):** Enables you to change the appearance of the graph, undo and redo changes, and search for or filter nodes. See [Graph Settings](#).
- **Graph (6):** Illustrates a set of events with nodes and arrows to show entities and the relationship between them. The numbers on the arrow indicate the order in which the events were recorded.
- **Timeline controls (7):** Enable you to hide, show, or reset the timeline. See [Timeline](#).

## Graph Settings

There are two resources to change the appearance and the amount of information shown on a graph to adapt it to the analyst needs:

- The graph toolbar, on the left side of the page.
- Contextual menus. To access them, right-click a node or a node group.

By default, the graph is shown horizontally **(6)** and has a sufficient level of zoom to make sure you can see all nodes without having to move the view.

## Graph Toolbar



Figure 12.2:  
Toolbar

- To undo the last action performed on the graph, click the **(1)** icon.
- To redo the last action performed on the graph, click the **(2)** icon.
- To zoom in the graph, click the **(3)** icon.
- To zoom out from the graph, click the **(4)** icon.
- To return to the default zoom setting, click the **(5)** icon.
- To change the graph orientation to horizontal, click the **(6)** icon.
- To change the graph orientation to vertical, click the **(7)** icon.
- To show or hide information layers in the graph., click the **(8)** icon. See [Hide and Show Layers](#).

## Context Menus

Right-click a node or node group to open its context menu. Options that are not available to you based on the status of the node are disabled.



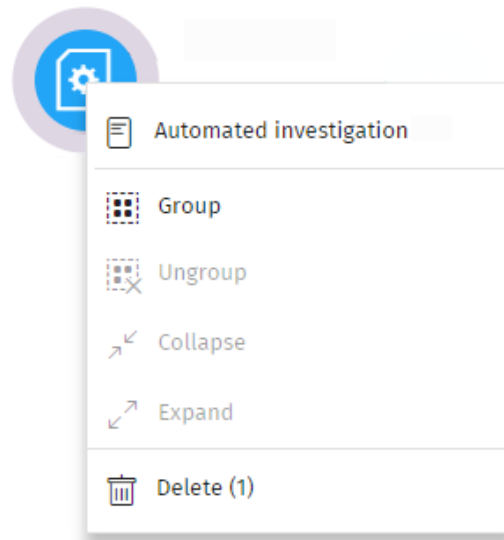


Figure 12.3: Context menu

## Hide and Show Layers

To show or hide information layers in the graph, click the **(8)** icon. A drop-down opens that shows these options:

- **Execution sequence:** Hides or shows numbers on the events to determine the order in which events occurred. See [Arrow Styles](#).
- **Name of relationships:** Hides or shows the names of the events. See [Format of the Events Used in Cytomic Orion](#) on page 374.
- **Name of entities.**

## Select Nodes on the Graph

- **To select a single node on the graph:** Click the node.
- **To select multiple non-contiguous nodes on the graph:** Press and hold the Ctrl or Shift key and click the nodes you want to select.
- **To select multiple contiguous nodes on the graph:** press and hold the Ctrl or Shift key, and click an empty area of the graph. Drag the mouse to draw a selection box that covers all the nodes you want to select.

When you select and right-click several nodes on the graph, the options that apply to all selected nodes show in the context menu.

## Move and Delete Nodes from the Graph

### To move all nodes and lines on the graph:

Click an empty area of the graph. Drag the graph in the appropriate direction.

**To move a single node:**

Select the node and drag it to a new location. All lines that connect the node with its neighbors move and adjust themselves to the new location of the node.

**To delete a single node using the keyboard:**

- Select the node you want to delete. Press the Del key. A dialog box opens and shows the total number of nodes that will be deleted from the graph. This includes the selected node and its child nodes.
- Click **OK**.

**To delete a single node using the mouse:**

When you delete a node from the graph, you delete the selected node and its child nodes.

- Right-click the node you want to delete. The context menu opens.
- Select **Delete (x)**. (x indicates the number of nodes that will be affected by the delete operation). A dialog box opens and shows the total number of nodes that will be deleted from the graph. This includes the selected node and its child nodes.
- Click **OK**.

**To delete multiple nodes:**

- Click the nodes you want to delete. Right-click one of the nodes. The context menu opens.
- Select **Delete (x)**. A dialog box opens and shows the total number of nodes that will be deleted from the graph. This includes the selected nodes and their child nodes.
- Click **OK**.

## Group Nodes

With graphs that contain a large number of items, analysts can group nodes that are related to one another to simplify the chart.

Node groups can have two states:

- **Expanded:** They show the nodes that make up the group.
- **Collapsed:** They hide the nodes that make up the group.


A node group is an entity with these characteristics:

- The actions you take on a node group affect all nodes that make up the group.
- You can group nodes of different types.
- When you delete a group, you delete all nodes that make up the group from the graph.
- When you collapse a group, all relationships between the nodes in the group and external nodes are represented as if they were established with the group. Arrows that reflect relationships of the same

type (same type of event) are also grouped (see **Collapsed node group**).

- The empty area of an expanded group represents the set of nodes in the group. For example, to open the context menu for all nodes in a group, right-click an empty area of the expanded group. Likewise, if you select **Delete**, you will delete all nodes in the group.
- A node belonging to an expanded group behaves in the same way as a node that is not in a group: you can move it individually, open its context menu, delete it, etc.
- A group can consist of nodes only, other groups only, or a combination of nodes and groups.

**To group a set of nodes:**

- Select multiple nodes on the graph. Right-click one of the nodes. A context menu opens.
- Select **Group** . A rectangle appears that contains all nodes in the group.

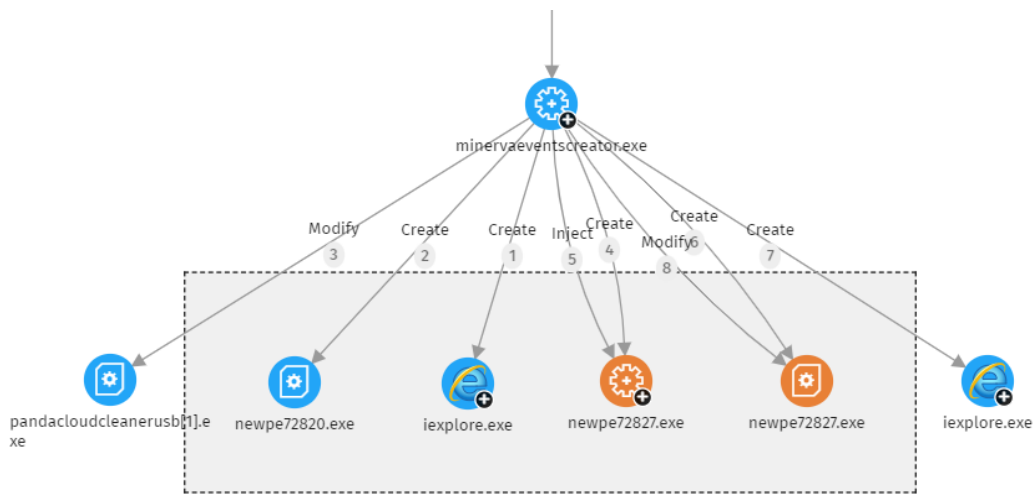



Figure 12.4: Node group

- Right-click an empty area of the rectangle. The context menu for the group opens.
- Select **Collapse** . The grouped nodes are replaced with a small square and all relationships with the nodes in the group point to the square.

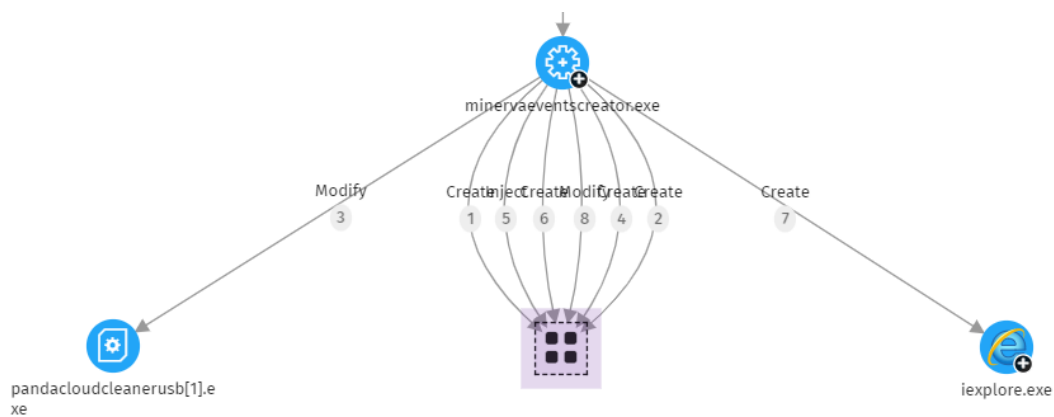




Figure 12.5: Collapsed node group

**To expand a collapsed node group:**

- Right-click the collapsed node group. A context menu opens.
- Select **Expand** . The previously collapsed nodes are shown in the rectangle.

**To ungroup nodes:**

- Right-click the node group. A context menu opens.
- Select **Ungroup** . The nodes reappear on the graph and the rectangle disappears.

**Information about Collapsed Groups**

**Types of Grouped Nodes**

A node group can contain nodes classified as goodware, malware, or unclassified. This is indicated by the color of the group.



Color	Description
	Group with blocked items.
	Group with items classified as goodware.

Table 12.1: Colors used in groups

**Number of Grouped Nodes**

In the upper-left corner, you can see the number of nodes that would be shown on the graph if the group were not collapsed. This number does not have anything to do with the total number of nodes (parent nodes,

child nodes, etc.) the group can contain. It shows only the number of nodes that were visible prior to being collapsed.

## Search for Nodes

The search bar enables analysts to highlight nodes of interest and access their details quickly.



Figure 12.6: Search bar in graphs

- (1): Click to show or hide the search bar.
- (2): Type the character string you want to search for. The search runs in real time only on the names and details of nodes. The content of arrows is excluded from searches. To clear the search, click the **X** icon.



*To avoid showing orphan nodes in search results, the parent node is always included, even if it does not match the entered pattern.*

- (3): Restricts searches on graphs to certain types of entities. To extend searches to include more than one type of entity, expand the drop-down menu and select the types of entities that you want to search for. To search across all types of entities again, click **Clear search**. The logical operator that is applied when you run a search across multiple types of entities is OR.
- (4) Restricts searches on graphs to the entities that have been classified by Cytomic Orion as the values you set in the drop-down menu. To extend searches to include more than one type of classification, expand the drop-down menu and select the types of classifications that you want to search for. To run a new search ignoring the classification of entities, click **Clear search**. The logical operator that is applied when you run a search across nodes with different classifications is OR.
- The logical operator that is applied when you run a search by entity and by classification simultaneously is AND.
- (5): Indicates the number of nodes that match the search pattern entered. When you enable the highlighting tool (4) and click the **▼** icon, a drop-down menu appears:
  - **Select found nodes**: Selects the nodes that match the search pattern entered. To show the context menu, right-click one of the selected items.
  - **Select all nodes except found nodes**: Selects nodes that do not match the search pattern entered. To show the context menu, right-click one of the selected items.
- (6): Highlights found items in yellow.
- (7): Hides items that do not match the search pattern entered.

The searches you run on nodes belonging to an expanded group behave in the aforementioned way. However, with nodes in a collapsed group, they behave differently:

- If the search is performed with the highlighting tool enabled **(6)**, the group is highlighted if any of the nodes in the group match the search criteria. Otherwise, the group is not highlighted.
- If the search is performed with the hiding tool enabled **(7)**, the group is shown if at least one of the nodes in the group matches the search criteria. Otherwise, the group is not shown on the graph.

## Timeline

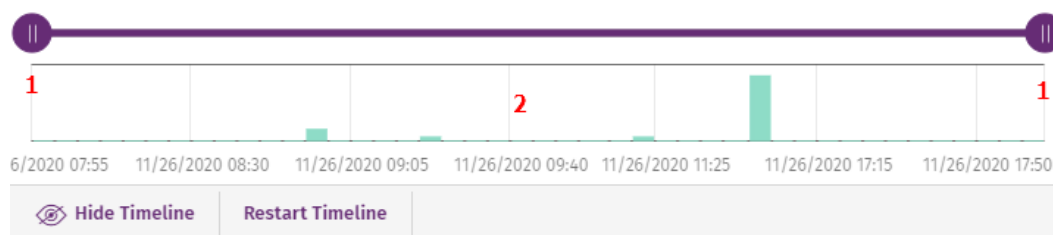


Figure 12.7: Timeline controls

The timeline enables you to blur the nodes and relationships that occurred outside a selected time range. This way, you can concentrate on the most relevant data for your investigation.

The timeline includes a histogram with green bars **(2)** that represent the events carried out by a threat. Point to the bars to show a tooltip of the number of events and the date they were logged..

### To select a specific interval on the timeline:

- Drag the gray interval selectors **(1)** to the left or right. The graph shows the events and nodes that occurred within the interval.
- Other events and nodes are blurred.

### To hide and show the timeline:

- To hide the panel, click **Hide timeline**.
- To show it again, click **Show timeline**.
- Click **Reset timeline** to return to the default timeline setting.

## Information Contained in Graphs

Graphs use color codes, panels, and other resources to provide information about entities and the relationship between them. These resources vary depending on the template you use.

## Process Tree Template

This template provides a graphical representation of the execution tree of a specific process, where nodes represent entities that participate in an operation (such as processes, files, or communication or operation

targets) and arrows represent operations.

The resources used to present this information are:

- **Template parameters:** Filter the type of information shown initially on the graph.
- **Node colors:** Indicate the item classification.
- **Node icons:** Indicate the item type.
- **Status icons:** Indicate the action taken on the item.
- **Arrow colors:** Indicate whether the item was blocked or not.
- **Arrow types:** Indicate the number and direction of the actions executed between the nodes.
- **Arrow labels:** When you click the label of an arrow, an information panel appears on the right that shows information about the action taken by the process.
- **Node labels:** When you click the label of a node, an information panel appears on the right that shows information about the entity.

### Template Parameters

- **Parentpid:** Parent process ID. It determines the specific execution instance of the program shown as start node on the graph.
- **muid:** Identifiers of the computers where the process you want to investigate was run.
- **parentmd5:** Parent process MD5.
- **date\_event:** Date of the event you want to represent on the graph. The graph shows events that correspond to the time interval that is between the day before and the day after the indicated date.

### Node Colors



Color	Description
	Item classified as malware.
	<ul style="list-style-type: none"> <li>• Item classified as a PUP.</li> <li>• Item classified as a suspicious item.</li> <li>• Unclassified item.</li> </ul>
(Original color)	Item classified as goodware.

Table 12.2: Color codes used in Process Tree template nodes

### Node Icons













Icon	Description	Icon	Description
	Process. If it belongs to a known software package, the process icon is shown.		Compressed file
	Remote thread		Executable file
	Library		Script file
	Protection		Windows registry branch value
	Folder		URL used in a communication
	Non-executable file		IP address in a communication

Table 12.3: Icons used in template nodes

### Status Icons





Icon	Description	Icon	Description
	File deleted		File quarantined
	File disinfected		Process deleted

Table 12.4: Icons used to indicate the action taken on the node



## Node Labels

The labels indicate the name of the entity. When you click an entity, an information panel appears on the right that shows the fields that describe it.

## Arrow Colors

The color of the arrows indicates whether Cytomic EDR or Cytomic EPDR blocked or allowed the action.

- **Red:** The action was classified as a threat and blocked by the protection software. See the meaning of the following actions in the **action** field in **Fields in the Events Received by Cytomic Orion** on page 375.
  - Block
  - BlockTimeout
  - BlockExploit
  - BlockBL
  - Disinfect
  - Delete
  - Quarantine
  - KillProcess
  - IPBlocked
- **Black:** The action was allowed.

## Arrow Styles

- **Arrow thickness:** Represents the number of times the same type of action was executed between two nodes. The greater the number of actions, the thicker the arrow. When you click an arrow, the information panel shows the dates when the first and last actions in the group occurred.
- **Arrow direction:** Indicates the direction of the action.
- **Numbers:** The numbers on the arrows indicate the order in which the event was recorded.

## Arrow Labels

The label of an arrow indicates the name of the action taken by the process. When you click the label of an arrow, an information panel appears on the right that shows fields that describe the event that occurred.


## Node Levels Shown by Default

By default, the graph is displayed horizontally with the node selected by the analyst at the center of the graph. It is surrounded by a subset of nodes related to that node:

- The graph displays three levels of nodes above the main node.
- The graph displays nodes one level below the main node.

The graph can show up to a maximum of 25 nodes at the same level. When there are more than 25 nodes, the graph shows no nodes.

## Show Child Nodes

An  icon in the bottom left corner of a node indicates that the node has hidden child nodes. To show child nodes, right-click the node. A context menu opens. Select one of the available options:

- **Show parent:** Shows the parent nodes of the selected node.
- **Show all activity (number):** Shows all the child nodes of the node regardless of the type. The maximum number of nodes shown is 25. The total number of events that link the parent node with the child node shows.
- **Show children:** Opens a drop-down list. Select the type of child nodes to show and select the number of nodes for each type. The types of nodes include:
  - **Data files:** Files with unidentified information.
  - **Script files:** Files with command sequences.
  - **Downloads:** Data files downloaded from the Internet/network.
  - **DNS:** Domains that failed to resolve the IP.
  - **Windows registry entries**
  - **Compressed files**
  - **PE files:** Executable files.
  - **Remote threads**
  - **IPs:** IP addresses for either end of the communication.
  - **Libraries**
  - **Processes**
  - **Protection:** Action taken by the antivirus.

When you select and right-click several nodes on the graph, the options that apply to all selected nodes show in the context menu.

## Investigation with Notebooks

To start an automated investigation on a node in the graph, right-click the graph and select **Automated investigation**. A list appears with all available templates. For more information about automated investigations, see [Investigations with Notebooks](#) on page 204.

## New Users in a Client Template

This template shows the new users that logged in to a client's computers. To do this, the template executes the following tasks:

- Collects all users who logged in to the client’s computers in a previous period taken as reference (group A)
- Collects all users who logged in to the client’s computers in the period the analyst wants to analyze (group B)
- Calculates the result of subtracting the number of users in group B from the number of users in group A:
  - Users in group B who were not in group A are the new users shown on the graph.
  - Users in both group A and group B are discarded.
  - Users in group A are discarded.

The resources used to present this information are:

- **Template parameters:** Filter the type of information shown initially on the graph.
- **Node icons:** Indicate the item type.
- **Node labels:** When you click the label of a node, an information panel appears on the right that displays information about the entity.

### Template Parameters

- **client:** Client where new users are searched for.
- **train\_date\_from:** Lower bound of the time period taken as reference for the comparison.
- **train\_date\_to:** Upper bound of the time period taken as reference for the comparison.
- **test\_date\_from:** Lower bound of the time period in which new users are searched for.
- **test\_date\_to:** Upper bound of the time period in which new users are searched for.

### Node Icons



Icon	Description	Icon	Description
	User account		Computer

Table 12.5: Icons used in template nodes

### Node Labels

The labels indicate the name of the entity. When you click an entity, an information panel appears on the right that shows the fields that describe it.

# Chapter 13

## Investigations with Notebooks

JupyterLab is an open-source web-based technology highly popular among the research community. It enables you to configure an interactive work environment to dynamically develop solutions in multiple programming languages. It also enables you to combine code blocks, text, images, or graphs into a single document, and is widely used by analysts from different areas for data cleaning and transformation, numerical simulation, statistical modeling, data visualization, machine learning, and much more.

Cytomic Orion incorporates the JupyterLab technology to provide security analysts with a well-known, industry-tested environment to share and automate investigations and configure tailor-made reports with graphical representations of results to make the most of their findings.

Notebooks are dynamic, interactive documents that provide analysts with these benefits:

- Ability to easily share investigation code with other SOC technicians to speed up the investigation process.
- Ability to visually show investigation results to clients.
- Ability to interactively leverage the data collected and shown in notebooks.

### CHAPTER CONTENTS

---

<b>Concepts and Definitions</b> .....	<b>205</b>
<b>Main Benefits of Notebooks</b> .....	<b>208</b>
<b>Access and Create Notebooks</b> .....	<b>208</b>
<b>List of Notebooks Created in an Investigation</b> .....	<b>209</b>
<b>Notebook Structure</b> .....	<b>209</b>
<b>Run a Notebook</b> .....	<b>211</b>
<b>Use Notebook Templates</b> .....	<b>212</b>
Template Management Access .....	212
Template Management .....	213

---

<b>Use Quick Answers with Notebooks</b> .....	<b>215</b>
Quick Answer Overview .....	215
Quick Answer Management .....	216
<b>Use Parameters in Templates and Quick Answers</b> .....	<b>218</b>
<b>Notebook Management Quick Guide</b> .....	<b>220</b>
Working Method with Notebooks .....	220
<b>Libraries Available in Notebooks</b> .....	<b>223</b>


## Concepts and Definitions

To make the most of the JupyterLab technology included in Cytomic Orion, we recommend you get familiar with these concepts:

### Notebook

A notebook is a web representation of all the inputs and outputs that have occurred over time regarding the interactive execution of one or multiple code snippets, including explanations in text format, images, and more elaborate object representations. This way, a notebook can serve as the record of a session started by the analyst, interleaving executable code with explanatory text and output.

### Cell

A notebook consists of a sequence of cells. A cell is the basic unit of a notebook. A cell consists of a text box that accepts one or more code lines. To run a cell, press the `Shift + Enter` keys simultaneously on your keyboard, or click the  icon in the notebook toolbar.

The execution behavior of a cell is determined by the cell type:

#### Code Cells

A code cell enables you to write code using the Python language, supported by the Cytomic Orion kernel. When you execute a code cell, the code it contains is sent to the kernel associated with the notebook. The results that are returned from this computation appear in the notebook as the cell output. The output is not limited to text; many other forms of output are also possible, including `matplotlib` figures and `pandas` tables.

Cells consist of these elements:

```
In [6]: communications = machine.get_communications(port='RDP')
cn = communications.to_dataframe()
3 if not cn.empty:
    times = [d.date() for d in cn['DateTime']]
    cn.DateTime = times
    rp = reports.group(input=cn, by=['Muid', 'DateTime'], name='Connections')
else:
    rp = pd.DataFrame()
print_dataframe(rp, format='table')
1
executed in 7.15s, finished 17:05:52 2019-04-16
```

	Muid	DateTime	Connections
	71602133F3F8B1D1223D04556F8487EA	2019-02-01	5681
	71602133F3F8B1D1223D04556F8487EA	2019-02-04	2401
	71602133F3F8B1D1223D04556F8487EA	2019-02-03	1130
	71602133F3F8B1D1223D04556F8487EA	2019-02-15	747
	71602133F3F8B1D1223D04556F8487EA	2019-01-31	41

Figure 13.1: General structure of a notebook cell

- (1) Text box where the analyst includes the code snippets they want to run.
- (2) Output area. In figure **General structure of a notebook cell**, the output appears in table format.
- (3) **Execution control**: Indicates the cell is a code cell and shows its status:
  - [Numeric]: Number of times the cell has been executed.
  - [\*]: The cell is being evaluated/executed.

### Markdown Cells

A Markdown cell enables you to document the processes implemented in the notebook, using rich text. The Markdown language provides a simple way to mark up text, that is, to specify which parts of the text should be emphasized (italics), bold, form lists, etc. You can also use it to provide structure for your notebook, with headings and tables of contents that enable you to add links to sections of the notebook. When a Markdown cell is executed, the Markdown code is converted into the corresponding formatted rich text. Markdown allows arbitrary HTML code for formatting.

**Contents**

- ▼ Potential RDP Attack Report
  - 1.1 Connection attempts in the last 15 days
    - 1.1.1 TOP 50 source IPs for RDP connections
    - 1.1.2 Geolocation
    - 1.1.3 Recommendations

2

```
In [0]: test_date = "2019-04-02"
test_numdays = 34
MUID = "###"
```

```
In [2]: %matplotlib inline
from TH import *
```

executed in 1.52s, finished 17:05:44 2019-04-16

```
In [3]: tst_period = TimePeriod(to_date=test_date, num_days=test_numdays)
machine = Machine(muid=MUID, period=tst_period)
```

executed in 9ms, finished 17:05:44 2019-04-16

```
In [4]: from IPython.display import HTML, display
```

executed in 28ms, finished 17:05:44 2019-04-16

1 Potential RDP Attack Report. 1

Analysis of connection attempts to port 3389 (Remote Desktop Protocol - RDP).

Figure 13.2: Formatted Markdown cell and table of contents for the notebook

- (1) Markdown cell with level 1 header-type text.
- (2) Automatically generated table of contents based on the header-type Markdown cells included in the notebook.



For more information about how to write Markdown cells, see <https://daringfireball.net/projects/markdown/basics>

## Kernel

The kernel is a runtime environment on the server that interprets the content of cells and generates output. The implemented kernel is compatible with Python version 3.6.

## Quick Answers

Quick answers are reusable, independent code snippets that you can quickly add to a notebook. Quick answers run autonomously. Quick answers are small programs that make up a complete library of solutions to common problems for the majority of security analysts. For more information, see [Notebook Management Quick Guide](#).

## Templates

Templates are notebooks stored on the Cytomic Orion platform that resolve common problems. Analysts can import, share, or edit templates, and use them as the basis for the creation of new notebooks that suit their needs. Cytomic has a constantly-updated template library available to all its clients. For more information about templates, see [Template Management](#).

## Parameters

Templates and quick answers might require input data to work correctly, such as a computer identifier (MUID) or the date when automation will retrieve data. When you run a notebook or a quick answer with parameters, a dialog box opens that prompts you to enter the required information. The data you enter is copied to the first cell in the notebook.

## Libraries

The notebook kernel in Cytomic Orion has access to a large number of external libraries written in Python and other compiled languages that make analysis, data handling, and the graphical presentation of results easier. These libraries are widely used by the analyst community. Additionally, Cytomic Orion provides access to a Threat Hunting library that makes investigation automation easier.

For a list of all the libraries available in the Cytomic Orion notebooks, see [Libraries Available in Notebooks](#).

## Main Benefits of Notebooks

- The ability to edit code directly in your browser, with automatic syntax highlighting, indentation, and tab completion.
- The ability to execute code on the server from the browser, with the results of investigations attached to the code which generated them.
- The ability to display the result of investigations with rich graphical and textual elements by using third-party libraries such as `matplotlib`.
- The ability to edit rich text in your browser using the Markdown markup language, which can provide commentary for the code.
- The ability to easily include mathematical notation within cells using `LaTeX`, and rendered natively by `mathJax`.
- The ability to naturally share the source code used by analysts in investigations, without sending files or controlling versions.
- The ability to easily design quick responses to security incidents that are run centrally and interactively.
- The ability to share investigation results, with options to export results to formats more suited to data sending.

## Access and Create Notebooks



*To use all features provided by notebooks, the analyst access account must have the **Investigations with notebooks** permission group assigned. For more information, see [Understanding Permissions](#) on page 56.*

Notebooks are an essential tool which are a part of created investigations. An investigations can have all the notebooks the analyst deems necessary to complete their analysis.

To access a previously created notebook:

- In the top menu, select **Investigations**. Select the investigation to which the notebook you want to access belongs.
- Select a notebook in the **Notebooks** sub-panel in the lower-right corner of the investigation page.

### Create a Notebook from an Investigation Toolbar

- In the top menu, select **Investigations**. Create a new investigation, or select the investigation for which you want to create the notebook. For more information about investigations and how to create



them, see [Manage Investigations](#) on page 92.

- In the toolbar, click the **+** icon. Select **Manual investigation**.

## Create a Notebook from an Investigation Sub-panel

- In the top menu, select **Investigations**. Create a new investigation, or select the investigation for which you want to create the notebook. For more information about investigations and how to create them, see [Manage Investigations](#) on page 92.
- In the **Files** sub-panel, click the **+** icon. Select **Manual investigation**.

## List of Notebooks Created in an Investigation

To access the list and get information about the notebooks created in an investigation, select **Investigations** in the top menu. Select an investigation. In the lower-right corner of the page, you can see the **Files** sub-panel. For more information about the meaning of the columns in the list, see [Files Sub-panel \(6\)](#) on page 105.

## Notebook Structure

A notebook in Cytomic Orion follows the same layout as a Jupyter notebook. This image shows the parts that make up a notebook:

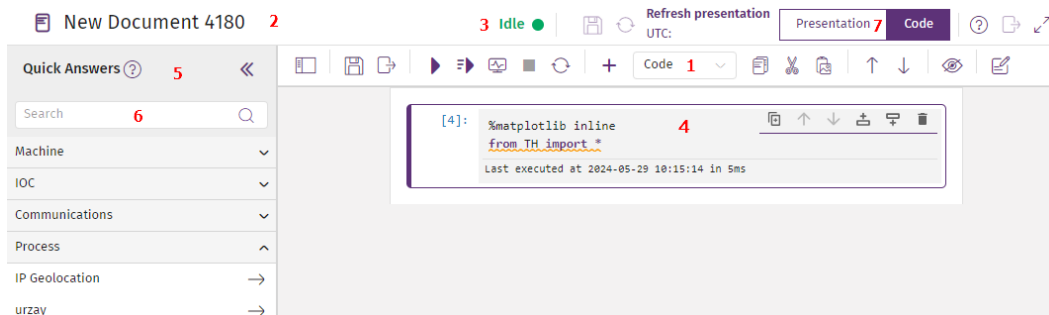
























Figure 13.3: General structure of a notebook




- **Notebook toolbar (1):** Provides the most commonly-used actions to interact with the notebook.
  - **Show/hide table of contents** : Shows/hides the table of contents built from the headers included in Markdown cells.
  - **Save** : Stores the notebook content on the server.
  - **Convert to PDF** : Hides code cells and saves cell output to a PDF or HTML file, including tables, charts, diagrams and other static items.
  - **Run cell** : Sends the cell content to the kernel and collects the output.

- **Run all cells** : Sends the content of all cells sequentially and collects the output for each cell.
- **Run presentation** : Runs all of the notebook cells and turns the notebook into a presentation. See [Run a Notebook](#).
- **Interrupt the kernel** : Interrupts the cell execution.
- **Restart and clear output** : Stops the kernel, starts it again, and clears all the existing cell outputs.
- **Add cell** : Creates a new cell below the selected cell.
- **Cell type**: Specifies whether the cell is a code or Markdown cell.
- **Copy cell** : Copies the cell to the clipboard.
- **Cut cell** : Copies the cell to the clipboard and deletes it from the notebook.
- **Paste cell** : Inserts, in the notebook, the cell you previously copied to the clipboard.
- **Move cell up** : Moves the cell position one step up.
- **Move cell down** : Moves the cell position one step down.
- **Hide cells** : Deletes the Python code to show only the outputs of the run cells.
- **Create quick answer** : Adds a quick answer to the library. See [Quick Answer Management](#).
- **Notebook name (2)**: To change the name of the notebook, click the text box. A dialog box opens that prompts you to enter the new name. Click **OK**. The new name is assigned to the notebook.
- **Kernel status (3)**: Specifies whether the notebook execution engine is stopped (**Idle**) or running a cell (**Busy**).
- **Notebook cell (4)**: A cell is the basic unit of a notebook. A cell consists of a text box that accepts one or more code lines and a group of icons to perform quick actions:
  - : Makes a copy of the selected cell below it.
  - : Moves the selected cell up.
  - : Moves the selected cell down.
  - : Adds a new cell above the selected cell.
  - : Adds a new cell below the selected cell.
  - : Deletes the selected cell.


- **Quick answers list (5):** Quick answers are small code snippets that speed up analyst investigation tasks. See [Quick Answer Management](#).
- **Search box (6):** Enter a full or partial quick answer name to add the quick answer to the notebook.
- **View mode (7):** Switch between code entering mode (**Code**) and output presentation mode (**Presentation**). For more information, see [Run a Notebook](#).

## Run a Notebook

Cytomic Orion supports multiple ways of running a notebook:

- **Run a cell:** In the toolbar, click the  icon. The output of running a single cell appears immediately after it.
- **Run all cells:** In the toolbar, click the  icon. The output of running each cell appears immediately after it.
- **Run the whole notebook:** Click the  icon, or select **Presentation** mode. This mode is aimed at sharing output. For more information about this mode, see [Run a Notebook](#).

### Access Presentation Mode

To access this mode, click the **Presentation** button, or the  icon in the toolbar. An animation appears that indicates the notebook is running. When the process is complete, the output appears.

### Presentation Mode Controls

Presentation mode provides a number of controls that enable analysts to interact with the notebook:

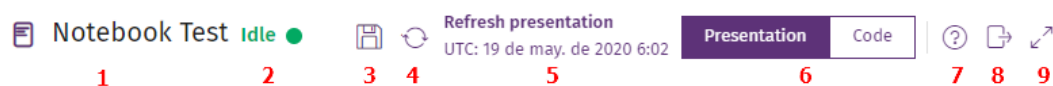



Figure 13.4: Notebook presentation mode controls

- **Notebook name (1):**
- **Kernel status (2):** Indicates whether the notebook execution engine is stopped (**Idle**) or running a cell (**Busy**).
- **Save (3):** Saves the notebook output.
- **Refresh (4):** Runs the notebook again and shows the output.
- **Last run (5):** Date, time, and time zone information for the last time the notebook was run.
- **Presentation mode (6):** In **Code** mode, the notebook shows the output associated with each cell individually. In **Presentation** mode, the code is hidden and the notebook shows the output only, enabling interaction with the analyst.
- **Help (7):** Opens the web help in a side panel.

- **Convert (8):** Saves the notebook output to a PDF or HTML file, including tables, charts, diagrams, and other static items.
- **Maximize (9):** Hides all Cytomic Orion menus and accessory items to display the output in full-screen mode.

### Presentation Mode Persistence


When you run a notebook in presentation mode, the calculated data is saved to the platform. This way, if you access the notebook later, it automatically loads the saved output from the last time it was run.



*When a notebook shows the data saved from a previous execution, it temporarily loses its interactive features. Click the refresh icon (4) to recover this feature.*

## Use Notebook Templates

Templates are notebooks stored on the Cytomic Orion platform that you can use as a basis for developing new notebooks. Analysts can run, share, and edit templates.



*To manage templates, the analyst access account must have the **Create notebooks from automated investigation templates** and **Manage investigation notebook templates** permissions assigned. For more information, see [Understanding Permissions](#) on page 56.*

### Template Management Access

To access the template management page, select **Settings** in the top menu. In the left panel, select **Templates**. A page opens that shows a list of all created templates and the **Add template** button. This information is shown for each template:

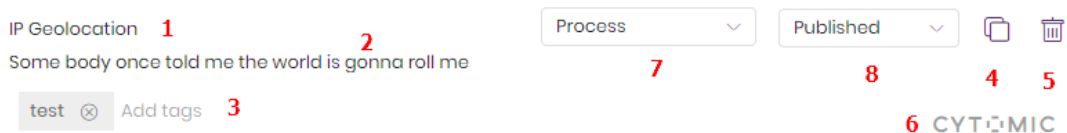


Figure 13.5: General structure of a template

- **Template name (1):** Set by the analyst who created the template.
- **Template description (2):** Text that describes the purpose of the template.
- **Tags (3):** Further describe the template and make it easier to search for it.
- **Copy icon (4):** See [Copy a Template](#).

- **Delete icon (5):** See [Delete a Template](#).
- **Logo (6):** Indicates the source of the template.
  - **Templates published by Cytomic:** Templates developed by Cytomic malware analysts. They have certified good performance. These templates are available to all Cytomic Orion clients. Clients cannot edit them. To edit them, the SOC analyst must copy the template and then edit the copy.
  - **Templates created by clients:** Templates developed by Cytomic Orion users. These templates can be shared only among analysts belonging to the same MSSP/MDR vendor, or SOC.
- **Category (7):** Class the template belongs to. Set by the analyst who created the template.
- **Status (8):** See [Publish a Template](#)

## Template Management


### Template Management Access

To access the template management page, select **Settings** in the top menu. In the left panel, select **Templates**. A page opens that shows a list of all created templates and the **Add template** button.

### Create a Template

- In the top menu, select **Settings**. In the left panel, select **Templates**.
- Click the **Add template** button. A new entry is added at the end of the template list.


### Copy a Template

- In the top menu, select **Settings**. In the left panel, select **Templates**.
- Click the  icon for the template you want to copy. A copy of the template is made, with the text string “[Copy] - “ prepended to its name.



*To edit a template created by Cytomic, you must first copy it. You cannot directly edit a template created by Cytomic.*

### Delete a Template

- In the top menu, select **Settings**. In the left panel, select **Templates**.
- Click the  icon for the template you want to delete. A confirmation dialog box opens.

## Publish a Template


- In the top menu, select **Settings**. In the left panel, select **Templates**.
- Click the drop-down menu. Select **Published**.

After you publish a template, it can be accessed by all of the MSSP/MDR vendor/SOC accounts. If the template is **Not Published**, it can be accessed only by the analyst account that created it.

## Edit a Template Attributes

- To edit the name, tags, or description of a template, click the attribute and enter the new value.
- In the case of tags, a drop-down menu appears that shows all available tags. To create a new tag, enter its value in the Tags field. The new tag is added to the drop-down menu for all created templates.

## Edit a Template Content

Click the template. The notebook content opens. After you have edited the content, click the  button in the notebook toolbar, or press `Ctrl+s`.

## Create a Notebook from a Template

To launch the wizard for creating a notebook based on a template:


- In the top menu, select **Investigations**. Create a new investigation, or select the investigation for which you want to create the notebook. For more information about investigations and how to create them, see [Manage Investigations](#) on page 92.
- In the toolbar, click the **+** icon. Select **Automated investigation**. A dialog box opens. Select the template you want to base the notebook on.
  - Use the **Search** text box to select the tags that will serve as filters to find a specific template. When you click the text box, a drop-down menu opens that shows all available tags. After you select a tag, it acts as first-level filter. Select more tags successively to set second, third, and more level filters.
  - If the template requires parameters, a dialog box opens that shows the names of the parameters and the data type you are expected to specify. See [Use Parameters in Templates and Quick Answers](#).

After you complete the wizard steps, the console takes these actions:

- Creates a new notebook with the contents of the template and the selected parameters.
- Assigns the collected values to the notebook variables in the first cell, so that the analyst does not need to know the names of the variables.
- Automatically includes a **Context\_params** variable in semicolon-delimited CSV format. This variable contains the content of the associated indicator and its headers.

## Use Quick Answers with Notebooks

Quick answers are small code snippets you can quickly add to notebooks. Quick answers are developed by analysts and by Cytomic threat hunters.



To create quick answers, the analyst access account must have the **Create quick answers permission** assigned. For more information, see [Understanding Permissions](#) on page 56.

### Quick Answer Overview

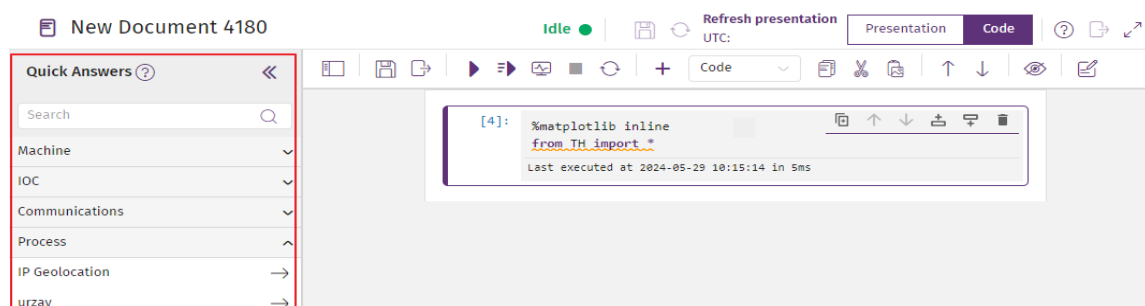


Figure 13.6: Location of quick answers in a notebook

There are two types of quick answers based on their source:

- **Quick answers published by Cytomic:** Quick answers developed by Cytomic malware analysts. They have certified good performance. These quick answers are available to all Cytomic Orion clients. Clients cannot edit them. To edit them, the analyst must copy the quick answer and then edit the copy.
- **Quick answers created by clients:** Quick answers developed by Cytomic Orion users. These quick answers can be shared only among analysts belonging to the same MSSP/MDR vendor, or SOC.

Each quick answer has these attributes assigned:

- (1) Quick answer name.
- [2] Description.
- (3) Tags (0 to N) to make it easier to search for the quick answer.
- (4) Icon for copying the quick answer.
- (5) Icon for deleting the quick answer.
- (6) Cytomic logo. It indicates whether the quick answer is certified.
- (7) MITRE category that corresponds to the tactic and technique used in the quick answer.
- (8) Quick answer publishing status.

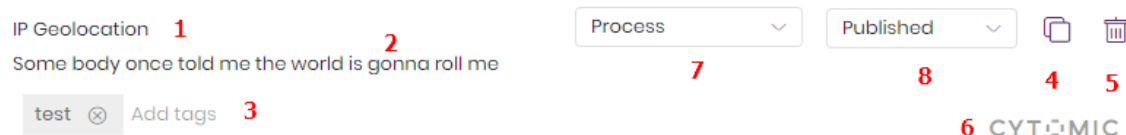


Figure 13.7: Quick answer overview


## Quick Answer Management

### Access Quick Answers

Quick answers are a resource available to analysts from the left panel of any previously created notebook.

### Create a Quick Answer

You can create quick answers from two areas of the console:


- In a notebook, point to a free cell and enter the quick answer code. A quick answer takes a single cell.
- Click the  icon. A page opens that prompts you to enter the quick answer name, a description, one or more tags to make it easier to search for the quick answer, and the MITRE category for the tactic and technique used.

Click **OK**. The quick answer is added to the relevant category in the Quick Answers panel on the left side of the notebook.

Or:

- In the top menu, select **Settings**. In the left panel, select **Quick answers**.
- Click **Add quick answer**. A new entry is added at the end of the list.
- Select the quick answer to add code to it.

### Copy a Quick Answer


- In the top menu, select **Settings**. In the left panel, select **Quick answers**.
- Click the  icon for the quick answer you want to copy. A copy of the quick answer is made, with the text string “[Copy] - “ prepended to its name.



*To edit a quick answer created by Cytomic, you must first copy it. You cannot directly edit a quick answer published by Cytomic.*



## Delete a Quick Answer

- Go to the **Quick answers** panel on the left side of a notebook. Select the quick answer you want to delete. In the lower-left corner, a sub-panel opens that shows the quick answer name and description.
- Click the  icon. A confirmation dialog box opens. Click **OK**. The quick answer is deleted from the panel.



*When an analyst deletes a quick answer, it cannot be accessed by any of the MSSP/MDR vendor/SOC accounts. You cannot undo this action. Use it carefully.*

## Publish a Quick Answer


- In the top menu, select **Settings**. In the left panel, select **Quick answers**.
- Click the drop-down menu. Select **Published**.

After you publish a quick answer, it can be accessed by all of the MSSP/MDR vendor/SOC accounts. If the quick answer is **Not Published**, it can be accessed only by the analyst account that created it.

## Edit a Quick Answer Attributes


- To edit the name, tags, or description of a quick answer, click the attribute and enter the new value.
- In the case of tags, a drop-down menu appears that shows all available tags. To create a new tag, enter its value in the Tags field. The new tag is added to the drop-down menu for all created quick answers.

## Edit a Quick Answer Content

Click the quick answer. The notebook content opens. After you have edited the content, click the  button in the notebook toolbar, or press `Ctrl+s`.

## Add the Code Contained in a Quick Answer to a Notebook

To add the code contained in a quick answer to a notebook:

- Click the cell where you want to add the quick answer code.
- Click the  icon associated with the quick answer, or double-click the quick answer name. The quick answer code is added to the selected cell.
- To view the information associated with a quick answer, click the quick answer name. A panel appears in the lower-left corner that shows the quick answer name and description.

- To insert the quick answer code in a new cell, click the **Insert content** link. A cell with the new content is created immediately after the selected cell.
- If the quick answer requires parameters, a dialog box opens that shows the name of the parameters and the data type you are expected to specify.

## Parameters



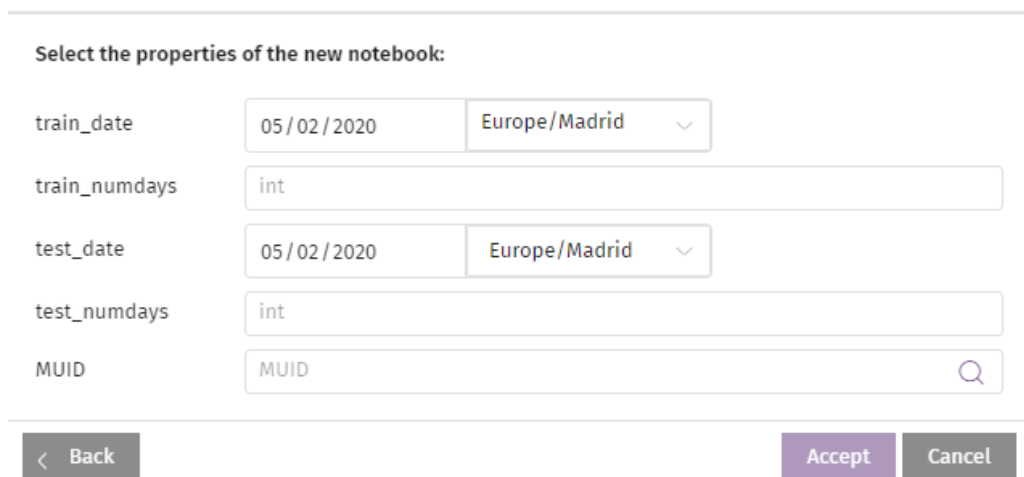
The dialog box is titled "Parameters:" and contains a single parameter entry. The parameter name is "muid" and its value is "MUID". To the right of the value field is a search icon. At the bottom right of the dialog are two buttons: "Accept" (purple) and "Cancel" (grey).

Figure 13.8: Parameter request dialog box for a quick answer

# Use Parameters in Templates and Quick Answers

To assign a value to a notebook variable interactively, analysts can define parameters in templates and in quick answers. A parameter is a variable specifically declared which, when the notebook is run, shows a dialog box that prompts the analyst for the value of the variable. This way, Cytomic Orion speeds up the process of assigning values to notebook variables without the analyst having to edit or modify the code.

## New notebook using template ?



The dialog box is titled "New notebook using template ?" and contains the heading "Select the properties of the new notebook:". Below this heading are five parameter entries:

- train\_date**: Value field contains "05/02/2020", dropdown menu contains "Europe/Madrid".
- train\_numdays**: Value field contains "int".
- test\_date**: Value field contains "05/02/2020", dropdown menu contains "Europe/Madrid".
- test\_numdays**: Value field contains "int".
- MUID**: Value field contains "MUID", search icon to the right.

At the bottom left is a "Back" button with a left arrow. At the bottom right are "Accept" (purple) and "Cancel" (grey) buttons.

Figure 13.9: Parameter request dialog box for a template

When you run a notebook created from a template that requires parameters, a parameter request dialog box appears, similar to the one in figure [Parameter request dialog box for a template](#). In this dialog box, the analyst must enter the values of the parameters the notebook will receive.

## Parameter Format

The format you must use to define a template parameter is:

```
VariableName = "" # type:type
```

For each line with the above format that exists in the template, an entry is added to the parameter request dialog box. If a list-type parameter is added, a text box appears for the analyst to specify the relevant parameters separated by carriage returns.

## Add Parameters to a Template or Quick Answer

To add parameters to a template:

In the first cell, add a line for each parameter with the aforementioned format.

These types of parameters are supported:

Type	Description
<b>string</b>	Character string.
<b>int</b>	Integers.
<b>date</b>	Dates.
<b>list</b>	Lists of character strings.
<b>MUID</b>	Drop-down menu with the entity of interest MUID.
<b>client</b>	Drop-down menu with the the entity of interest client.
<b>MD5</b>	Drop-down menu with the entity of interest MD5.

Table 13.1: Types of parameters supported in templates

## Automatic Assignment of Parameter Values Based on the Context

When running a notebook that requires parameters, analysts must manually assign the value of each parameter in the parameter request dialog box. In notebooks that require many parameters, this task can take some time. To speed up the process of assigning values, Cytomic Orion can read the context of the entity of interest from which you launch the notebook. For example, if the analyst launches a notebook from an indicator, Cytomic Orion can read the fields of the specific indicator and load their contents into the appropriate parameters in the parameter request dialog box.

For Cytomic Orion to associate a field of an entity of interest with a specific parameter required by a notebook that you want to run, these conditions must be met:

- The parameter name and the field name must match.
- The parameter must be declared with a basic type (int or string)

For example, an analyst defines a notebook that requires a computer MUID. To speed up the process of assigning the MUID value when the notebook is launched from an indicator, the analyst must declare the 'MUID' parameter with a string, because that is the name of the field that contains a computer MUID in the indicators generated by Cytomic Orion.

## Assignment of Default Values to Parameters

The format you must use to assign a default value to a parameter in a template is:

```
VariableName = "123" # type:type
```

Automatic assignment of values to parameters based on the entity context has priority over assignment of default values. That is, when you open a notebook and the parameter request dialog box appears, if the solution cannot populate a parameter field with the context information, the default value specified in the parameter declaration is added. Similarly, if a notebook has default parameters assigned, and the values of those parameters can also be automatically assigned from the entity context, the values that are finally applied are the values generated from the entity context.

## Notebook Management Quick Guide




*For a complete list of Jupyter notebook keyboard shortcuts and available actions, see <https://gist.github.com/discdiver/9e00618756d120a8c9fa344ac1c375ac>.*

A notebook operation is based on running cells independently, so analysts must create such cells with the supported types and run them to get output.

## Working Method with Notebooks

With notebooks, you work on computational problems in pieces or cells that you can run independently. All variables declared and functions defined in an already run cell are kept in memory so that subsequent cells can use them. Taking the approach of working on problems in pieces or cells enables you to run sections of code separately without breakpoints, because each cell is run independently and shows its output. This way, you can edit and run each cell as many times as you want until you get the expected output.

To clear the output generated by a previous execution of a notebook cells, you must restart the associated kernel with the  button in the toolbar.

## Edit Mode and Command Mode


Notebooks have two different modes:

- In edit mode, the analyst can edit or run the content of the selected cell identified by a purple border.
- In command mode, the analyst can add cells, delete them, or change their order.
- To enter command mode, press ESC or click anywhere outside the cell.
- To enter edit mode, click the text box of the cell you want to edit, or use the arrow keys to navigate to the cell and press `Enter`.
- When you click an icon in the notebook toolbar, you enter command mode automatically.



## Select a Cell in the Notebook

- **To select a cell in command mode:** Use the arrow keys. You can also use `k` and `j`.
- **To select a cell in edit mode:** Click the cell text box.
- **To select multiple consecutive cells in command mode:** Use the `Shift + Arrow` keys, or `Shift + k` and `Shift + j`, or click the first cell, press `Shift` and click the last cell.

## Add a Cell to the Notebook

Select a cell. In the notebook toolbar, click the  icon. A new **code** type cell is created below the selected cell.

To control where the cell is inserted:

- **To create a cell above the selected cell:** In command mode, press `A` or click the  icon.
- **To create a cell below the selected cell:** In command mode, press `B` or click the  icon.

## Change the Cell Type of a Notebook Cell


Select one or multiple cells. In the notebook toolbar, click the drop-down menu.

To change the cell type using the keyboard, select the cell in command mode and press these keys:


- To change the cell to code: `Y`.
- To change the cell to Markdown: `M`.

## Delete a Notebook Cell

In command mode, use the arrow keys to select the cell you want to delete. Press the `d` key twice. The cell is deleted, along with its output, if any.

You can also delete a cell by clicking the cell  icon.


## Run a Notebook Cell

Select a cell. In the notebook toolbar, click the  icon. The cell runs and shows its output.

To run a cell using the keyboard:

- **To run a cell with the keyboard:** Select the cell and press `Ctrl + Enter`.
- **To run a cell with the keyboard and move to the next cell:** Press `Shift + Enter`. This is useful if you want to run a series of consecutive cells individually without needing to select them independently.
- **To run a cell with the keyboard and insert a new cell immediately below it:** Press `Alt + Enter`. This is useful if you want to quickly add new code or notes to your notebook.





## Run all Notebook Cells

In the notebook toolbar, click the  icon. The notebook shows each cell output below the cell. The cell code is not hidden.


## Run All Notebook Cells in Presentation Mode

In the notebook toolbar, click the  icon. The notebook enters presentation mode, hiding code sections.

## Sort the Notebook Cells


- Select a cell. In the toolbar, click the  and  icons.
- Click the cell  and  icons.
- Click the sequence number for the cell you want to move. Drag it to a new position.

## Save a Notebook



- In the notebook toolbar, click the  icon.
- In command mode, press `Ctrl + s`.



## Stop and Restart Kernel Execution

To clear cell output, or if the kernel gets stuck in an infinite loop, we recommend that you restart the kernel.

- **To restart the kernel:** In the notebook toolbar, click the  icon.
- **To interrupt the kernel in command mode:** Press `i` and `i`.
- **To restart the kernel in command mode:** Press `0` and `0`.

## Copy, Cut, and Paste Cells

- **To copy one or more cells using the toolbar:** Select the cells. Click .
- **To copy one or more cells using the keyboard:** Select the cells in command mode. Press `c`.
- **To cut one or more cells using the toolbar:** Select the cells. Click .
- **To cut one or more cells using the keyboard:** Select them in command mode. Press `x`.

- **To paste one or more cells below an existing cell using the toolbar:** Select the cell. Click .
- **To paste one or more cells above an existing cell using the keyboard:** Select the cell in command mode. Press Shift + v.
- **To paste one or more cells below an existing cell using the keyboard:** Select the cell in command mode. Press v.
- **To duplicate a cell:** Click the cell  icon. A copy of the cell is created below it.

## Merge Cells

- To merge two consecutive cells of the same type in command mode, press Shift + m.


## Enable Code Autocomplete and Get Help

- **To get completion suggestions for your code as you type:** Press Tab.
- **To call help for a function:** Press Shift + Tab.

## Move Cursor Within a Cell

- **To move the cursor to the start of the cell:** Press Ctrl + Home.
- **To move the cursor to the end of the cell:** Press Ctrl + End.
- **To move the cursor one word right:** Press Ctrl + Right.
- **To move the cursor one word left:** Press Ctrl + Left.

## Other Operations

- **To hide code using the keyboard in command mode:** Press O.
- **To hide code using the toolbar:** Click .
- **To show or hide line numbers within cells:** In command mode, press l.
- **To show a list of keyboard shortcuts:** In command mode, press h.
- **To merge two consecutive cells of the same type:** In command mode, press Shift + m.

# Libraries Available in Notebooks

This section shows a list of all the third-party libraries available to analysts in the Cytomic Orion notebooks, grouped by type, along with a brief description and useful resources.

In addition to third-party libraries, Cytomic Orion provides all clients with multiple libraries that help automate analyses and show results graphically. For a complete description of the APIs defined in the libraries, their objects, methods, and data enumerations, see these links:

- **Threat Hunting library** : See <https://info.cytomicmodel.com/resources/help/ORION/es/threathuntingAPI/index.html>
- **Widgets library** : See <https://info.cytomicmodel.com/resources/help/ORION/es/Notebooklib/index.html>

## Databases

Name	Description
<b>Psycopg</b>	Access library to PostgreSQL databases. It fully implements the Python Database API Specification 2.0. <a href="http://initd.org/psycopg/docs/">http://initd.org/psycopg/docs/</a>
<b>Pyodbc</b>	Access library to ODBC databases. Compatible with Microsoft SQL Server, MySQL, Oracle, and others. <a href="https://github.com/mkleehammer/pyodbc/wiki">https://github.com/mkleehammer/pyodbc/wiki</a>
<b>maxminddb</b>	Accesses MaxMind DB files, a binary file format that stores data indexed by IP address subnets (IPv4 or IPv6). <a href="https://pypi.org/project/maxminddb/">https://pypi.org/project/maxminddb/</a>

Table 13.2: Available database libraries

## Graphs

Name	Description
<b>branca</b>	Graphical library. <a href="https://python-visualization.github.io/branca/">https://python-visualization.github.io/branca/</a>
<b>folium</b>	Graphical library for handling interactive leaflet maps. <a href="https://python-visualization.github.io/folium/">https://python-visualization.github.io/folium/</a>
<b>Graphviz</b>	Graph visualization library for representing structural information as diagrams of abstract graphs and networks. <a href="https://graphviz.readthedocs.io/en/stable/">https://graphviz.readthedocs.io/en/stable/</a>
<b>Iplotter</b>	Interactive charting library. <a href="https://github.com/niloch/iplotter">https://github.com/niloch/iplotter</a>



Name	Description
<b>ipywidgets</b>	<p>Uses Python controls to create GUIs that make interacting with users easier.</p> <p><a href="https://ipywidgets.readthedocs.io/en/stable/">https://ipywidgets.readthedocs.io/en/stable/</a></p>
<b>matplotlib</b>	<p>2D mapping library that creates high-quality charts: histograms, bar charts, scatter plots, etc.</p> <p><a href="https://matplotlib.org/users/index.html">https://matplotlib.org/users/index.html</a></p>
<b>networkx</b>	<p>Package for the creation, manipulation, and study of the structure, dynamics, and functions of complex networks.</p> <p><a href="https://networkx.github.io/documentation/networkx-2.3/">https://networkx.github.io/documentation/networkx-2.3/</a></p>
<b>pivottablejs</b>	<p>Implementation of Pivot Table (aka Pivot Grid, Pivot Chart, Cross-Tab) graphs with drag'n'drop functionality.</p> <p><a href="https://pypi.org/project/pivottablejs/">https://pypi.org/project/pivottablejs/</a></p>
<b>pydot</b>	<p>DOT language interface used by the <code>Graphviz</code> suite of programs.</p> <p><a href="https://github.com/pydot/pydot">https://github.com/pydot/pydot</a></p>
<b>pygal</b>	<p>Library for creating bar charts, pie charts, line charts, radar charts, etc.</p> <p><a href="http://pygal.org/en/stable/documentation/index.html">http://pygal.org/en/stable/documentation/index.html</a></p>
<b>seaborn</b>	<p>Data visualization library based on <code>matplotlib</code>. It provides a high-level interface for drawing attractive and informative statistical charts.</p> <p><a href="https://seaborn.pydata.org/">https://seaborn.pydata.org/</a></p>
<b>widgetsnbextension</b>	<p>HTML interactive widgets.</p> <p><a href="https://pypi.org/project/widgetsnbextension/">https://pypi.org/project/widgetsnbextension/</a></p>
<b>basemap</b>	<p>Library for building 2D maps. Designed to meet the needs of oceanographers and meteorologists</p> <p><a href="https://matplotlib.org/basemap/">https://matplotlib.org/basemap/</a></p>
<b>igraph</b>	<p>Collection of network analysis tools that emphasize efficiency, portability, and ease of use,</p>

Name	Description
<b>cufflinks</b>	Library that makes it easy to create charts from Pandas Dataframes. <a href="https://plot.ly/ipython-notebooks/cufflinks/">https://plot.ly/ipython-notebooks/cufflinks/</a>

Table 13.3: Available libraries for graph processing

## Python and Others

Name	Description
<b>future</b>	Compatibility with future Python versions.
<b>PyJWT</b>	Encodes and decodes JSON Web Tokens (JWT). <a href="https://pyjwt.readthedocs.io/en/latest/">https://pyjwt.readthedocs.io/en/latest/</a>
<b>pyparsing</b>	Develops grammars to generate interpreters. <a href="https://github.com/pyparsing/pyparsing">https://github.com/pyparsing/pyparsing</a>
<b>pytz</b>	Operations with time zones. <a href="http://pytz.sourceforge.net/">http://pytz.sourceforge.net/</a>
<b>selenium</b>	Web browser automation. This library automates web apps for tests, repetitive management tasks, etc. <a href="https://www.seleniumhq.org/docs/">https://www.seleniumhq.org/docs/</a>
<b>plotly</b>	Develops data analytics web apps. This library enables you to build data visualization interfaces. <a href="https://dash.plot.ly/">https://dash.plot.ly/</a>
<b>pixiedust</b>	Add-on to Jupyter notebooks to improve the user experience of working with data.. <a href="https://pixiedust.github.io/pixiedust/">https://pixiedust.github.io/pixiedust/</a>
<b>cyjupyter</b>	Widget for visualizing network graphs. <a href="https://github.com/cytoscape/cytoscape-jupyter-widget">https://github.com/cytoscape/cytoscape-jupyter-widget</a>
<b>pillow</b>	API for generating bitmap images, based on PIL.

Name	Description
<b>cairosvg</b>	Converts SVG files to PDF and PNG. <a href="https://cairosvg.org/documentation/">https://cairosvg.org/documentation/</a>
<b>tqdm</b>	Progress bar control. <a href="https://tqdm.github.io/">https://tqdm.github.io/</a>

Table 13.4: Available libraries that extend Python capabilities

## Data

Name	Description
<b>geolIP2</b>	API for accessing the GeolIP2 service. This service is used to get geographic location data from an IP address. <a href="https://geolip2.readthedocs.io/en/latest/">https://geolip2.readthedocs.io/en/latest/</a>
<b>ipaddr</b>	Inspects and manipulates IP addresses. <a href="https://docs.python.org/3/howto/ipaddress.html">https://docs.python.org/3/howto/ipaddress.html</a>
<b>kiwisolver</b>	Incremental constraint solving toolkit that efficiently solves systems of linear equalities and inequalities. Constraints can be either requirements or preferences. They are specified initially, and the solver updates the constrained variables to have values that satisfy the constraints <a href="https://github.com/google/kiwi-solver">https://github.com/google/kiwi-solver</a>
<b>numpy</b>	Fundamental package for scientific computing. It enables you to manipulate arrays, linear algebra routines, and Fourier transforms, generate random numbers, and more. <a href="https://docs.scipy.org/">https://docs.scipy.org/</a>
<b>pandas</b>	Library that provides high-performance, easy-to-use data structures and data analysis tools. It aims to be the fundamental high-level building block for doing practical, real-world data analysis. <a href="http://pandas.pydata.org/pandas-docs/stable/getting_started/overview.html">http://pandas.pydata.org/pandas-docs/stable/getting_started/overview.html</a>
<b>pefile</b>	Enables you to parse and work with Portable Executable (PE) files. Most of the information contained in the PE headers is accessible as well as all sections' details and their data.

Name	Description
	<a href="https://github.com/erocarrera/pefile">https://github.com/erocarrera/pefile</a>
<b>pip-date</b>	Lightweight command-line toolkit to show the installation or modification times of all your pip packages.
<b>sciPy</b>	Math software for scientific and engineering calculations. <a href="https://docs.scipy.org/doc/scipy/reference/">https://docs.scipy.org/doc/scipy/reference/</a>
<b>qgrid</b>	An interactive grid for sorting, filtering, and editing DataFrames. <a href="https://qgrid.readthedocs.io/en/latest/">https://qgrid.readthedocs.io/en/latest/</a>
<b>statsmodels</b>	A module for the estimation of statistical models, as well as for conducting statistical tests, and statistical data exploration. <a href="https://www.statsmodels.org/stable/index.html">https://www.statsmodels.org/stable/index.html</a>
<b>scikit-learn</b>	Tools for data mining, data analysis, and machine learning. <a href="https://scikit-learn.org/stable/documentation.html">https://scikit-learn.org/stable/documentation.html</a>

Table 13.5: Available libraries for data processing



# Chapter 14

## IT Infrastructure Investigation with OSQuery

OSQuery is a framework for collecting and organizing information about the infrastructure of a SOC clients. It provides this information to analysts through a relational data model.

Analysts write SQL statements to get information about the hardware, software, running processes, file system, registry, etc., of computers. Analysts can then use this information in their investigations or to respond to incidents.



Contact your assigned sales representative to enable the OSQuery feature for devices that meet the requirements specified in [OSQuery Requirements](#).

### CHAPTER CONTENTS

---

<b>Introduction to OSQuery</b> .....	<b>230</b>
<b>Use Cases for Analysts</b> .....	<b>231</b>
<b>Access OSQuery</b> .....	<b>232</b>
<b>Send OSQuery Queries</b> .....	<b>233</b>
<b>OSQuery Statement Results</b> .....	<b>233</b>

## Introduction to OSQuery

OSQuery is a set of libraries that compile information on a device operating system and store it in a relational database. OSQuery enables analysts to flexibly explore the stored data with SQL queries. The tables show

essential operating system components, such as running processes, loaded kernel modules, open network connections, installed browser plugins, hardware events, or file hashes.

To build SQL queries compatible with OSQuery, you must understand the OSQuery data schema. For more information about the tables and fields used to organize the information collected from investigated devices, see <https://osquery.io/schema/4.2.0/>.

## OSQuery Integration with Cytomic Orion

Cytomic Orion mainly uses notebooks to run OSQuery statements, compile the data received, and present it to analysts in a clear way. Analysts do not have to create notebooks from scratch. They have access to a set of templates that collect the required parameters, send queries to affected devices, and gather results. For more information about how to access the OSQuery feature, see [Access OSQuery](#). For more information about how results are presented, see [OSQuery Statement Results](#).

This feature is also available through the integration API. See [OSQuery Access API](#) on page 331

## OSQuery Requirements

- Cytomic EPDR or Cytomic EDR version 3.71 and higher must be installed on the computers from which you want to retrieve infrastructure information.
- Windows operating system.
- You must send queries compatible with OSQuery version 4.02.00.

## Use Cases for Analysts

To showcase the capabilities of OSQuery and help situate this feature in the analysis and incident response process, we provide these use cases:

- Assess the scope of an attack.
- Find processes listening on a port.
- Find running processes whose files have been deleted.

### Assess the Scope of an Attack

When the execution of a malicious process is detected during the incident response phase, an analyst might want to check whether the process is running on other devices on the network. To assess the scope of the attack, launch a query using the name of the process, or even the name of a file opened by the process. This way, the analyst can identify which devices have been compromised.

```
SELECT      processes.pid          FROM      processes      WHERE
processes.name='string'

SELECT process_open_files.pid FROM process_open_files WHERE
process_open_files.path LIKE '%string%'
```

## Find Processes Listening on a Port

Many malicious processes receive commands from a central command-and-control (C&C) server. A typical task for analysts is to detect new processes that are listening on unusual ports. To do this, you can get a list of all open sockets on each computer and compare that list to a previous list to see the differences.

```
SELECT listening_ports.pid,listening_ports.port,listening_
ports.address, processes.name, processes.path FROM
listening_ports INNER JOIN processes ON processes.pid =
listening_ports.pid
```

## Find Running Processes Whose Files Have Been Deleted

Attackers often leave malicious processes running but delete the original files from the hard disk. Such an anomalous situation could indicate the presence of a suspicious process.

```
SELECT processes.name, processes.path, processes.pid FROM
processes WHERE on_disk = 0
```

# Access OSQuery

To retrieve information about the IT infrastructure, you must send SQL statements to the platform from one of these areas of the console:

- From the **Indicators** sub-panel of an investigation:
  - In the top menu, select **Investigations**. In the list, select an investigation.
  - Select one or more indicators. In the toolbar, select **OSQuery query**. You can also click the context menu icon for an indicator and select **OSQuery query**.
  - The **New OSQuery query** dialog box opens. The **Computers** field is automatically populated with the MUIDs of the relevant computers.
- From the tab bar of an **Investigation**:
  - In the top menu, select **Investigations**. In the list, select an investigation.
  - In the tab bar, click the **+** icon. Select **OSQuery query**.
- From the **Files** sub-panel of an investigation:
  - In the top menu, select **Investigations**. In the list, select an investigation.
  - In the **Files** sub-panel, click the **+** icon. Select **OSQuery query**.



Regardless of the option you select, the **New OSQuery query** dialog box opens. See [Send OSQuery Queries](#).

Additionally, you can also access the OSQuery feature through the Cytomic Orion integration API. For more information about the OSQuery specific methods and how to use the API, see [OSQuery Access API](#) on page 331.



## Send OSQuery Queries

The **New OSQuery** query dialog box contains these fields:

- **Notebook name:** The data collected from the client infrastructure is presented in a notebook. This field indicates the notebook name.
- **Description:** Describes the type of data collected with the OSQuery query and other information the analyst might want to add.
- **Computers:** Indicates the computers from which the data is collected:
  - **All computers of the following clients:** Use the  icon to select the names or IDs of the clients whose computers will receive the OSQuery statement. You cannot specify individual computers.
  - **The following computers:** Use the  icon to select the IDs (MUIDs) of the computers that will will receive the OSQuery statement You can add computers belonging to multiple clients.
- **Maximum wait time:** OSQuery queries can affect computers that are turned off. As such, it will not be possible to collect the requested information. Cytomic Orion tries to collect the requested information within the period you specify in the **Maximum wait time** field. After this time, all requests are canceled and the process is considered complete.
- **Query:** The SQL statement in OSQuery format. For more information about the data schema, see <https://osquery.io/schema/4.2.0/>.

## OSQuery Statement Results

The results of running an OSQuery statement are presented in a closed-format notebook as shown below:

## OSQuery query 1

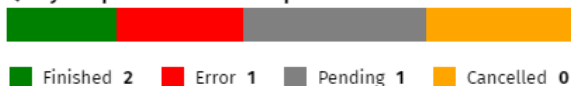
On 17/06/2020 at 15:25:30, the user `thisuserwebconsole@panda.com` launched the following OSQuery query:

Description:	Denis OS Query
Computers:	All computers of the following clients: 696969, 9E5E22EC, 1912270010
Maximum waiting time:	12 hours
Query:	<code>select name,pid from processes</code>

## Query progress 2

[Update progress](#) [Download progress details](#)

Query completed on 3 of 4 computers



## Results 3

[Update result table](#) [Download all results](#) 4

Filter... 5 Updated on: 17/06/2020 15:29

Customer Id	Device Id	Hostname	Name	Pid
9E5E22EC	7518bb8e-9e5a-4b82-adaf-b4c77c32ece5	AUTOE2EW201264	[System Pr...	0
9E5E22EC	7518bb8e-9e5a-4b82-adaf-b4c77c32ece5	AUTOE2EW201264	System	4
9E5E22EC	7518bb8e-9e5a-4b82-adaf-b4c77c32ece5	AUTOE2EW201264	smss.exe	460

Figure 14.1: Notebook with an OSQuery statement results

*For more information about how to manage and use notebooks in Cytomic Orion, see [Investigations with Notebooks](#) on page 204.*


- **Notebook information (1):** Contains the data provided by the analyst at the time they created the OSQuery statement: statement name, description, duration, scope, and the statement in SQL language.
- **Progress information (2):** Contains multiple data series indicating the number of computers that completed the operation successfully:
  - **Finished:** Number of computers that completed the operation successfully and sent data.
  - **Error:** Number of computers that returned an error.
  - **Pending:** Number of computers that still have not returned data.
  - **Canceled:** Number of computers that did not return data within the time specified in the **Maximum wait time** field.
- **OSQuery statement results (3):** Contains a table that shows the data returned by the OSQuery statement, as well as filter and download tools.

- **Data download controls (4)**: Download two files with comma-separated data, one file with data reported by computers and another file with query status information.
- **Filter (5)**: Show data table rows that match the search terms you enter. You can type only a partial string. Searches are performed on all fields in the table.
- **Data table (6)**: Contains a table that shows the fields requested by the analyst in the OSQuery statement. The maximum number of entries shown is 10,000. When this number is exceeded, a warning message is shown and the analyst is prompted to download the table (4). All result tables show three additional fields:
  - **Customer Id**: This is the identifier of the client to whom the information belongs.
  - **Device Id**: This is the identifier used in Cytomic EDR or Cytomic EPDR to designate the computer to which the information belongs.
  - **Hostname**: Name of the computer to which the information belongs.

## Run Statements in the Background and Presentation Mode



For more information about this notebook run mode, see [Presentation Mode Persistence](#) on page 212.

Because OSQuery queries can take a long time to complete if the **Maximum wait time** field is set to a long time period and computers are slow to respond, an analyst might close the notebook before the query is complete. However, because OSQuery libraries run in the background, the statement continues to run even if you have closed the notebook. With presentation mode, when you reopen the notebook, it shows the results collected until just before it was closed, not the data collected from the time the notebook was closed until it was reopened. To refresh the information, click **Update result table** or **Update progress** in the notebook, or the  icon in the toolbar to update the entire notebook content.

# Chapter 15

## Response Tools

When an analyst detects suspicious activity on a company's workstations or servers, tools are required so that the incident response team can shut down a potential security breach, restore the computer to its previous state, and gather the evidence required to carry out a more thorough analysis.

Cytomic Orion provides a complete set of tools to help perform the remediation tasks remotely from the console used by the security analyst.

### CHAPTER CONTENTS

---

<b>Requirements</b> .....	<b>236</b>
<b>Access the Response Tools</b> .....	<b>237</b>
<b>Description of Response Tools</b> .....	<b>239</b>
Isolate Computer .....	239
Restart Computer .....	241
Process Manager .....	242
Service Manager .....	243
File Transfer .....	244
Remote Command Line .....	245
Command Line Tools .....	245

## Requirements

To use the remote access and remote command line tools, the user computer and the perimeter firewall on the client's network must allow traffic to and from these URLs and ports:

- [dir.rc.pandasecurity.com](https://dir.rc.pandasecurity.com) through port 443.
- [eu01.rc.pandasecurity.com](https://eu01.rc.pandasecurity.com) through ports 8080 and 443.
- [eu02.rc.pandasecurity.com](https://eu02.rc.pandasecurity.com) through ports 8080 and 443.

- eu03.rc.pandasecurity.com through ports 8080 and 443.
- eu04.rc.pandasecurity.com through ports 8080 and 443.
- eu05.rc.pandasecurity.com through ports 8080 and 443.
- eu06.rc.pandasecurity.com through ports 8080 and 443.
- ams01.rc.pandasecurity.com through ports 8080 and 443.
- ams02.rc.pandasecurity.com through ports 8080 and 443.

## Access the Response Tools

### Tools Available in Cytomic Orion

#### Remote Management Tools

- **Isolate computer:** Restricts the network traffic sent to or received by a computer to prevent the spread of threats to other computers and the exfiltration of confidential information.
- **Restart computer:** Forces a computer to restart.

#### Remote Access Tools

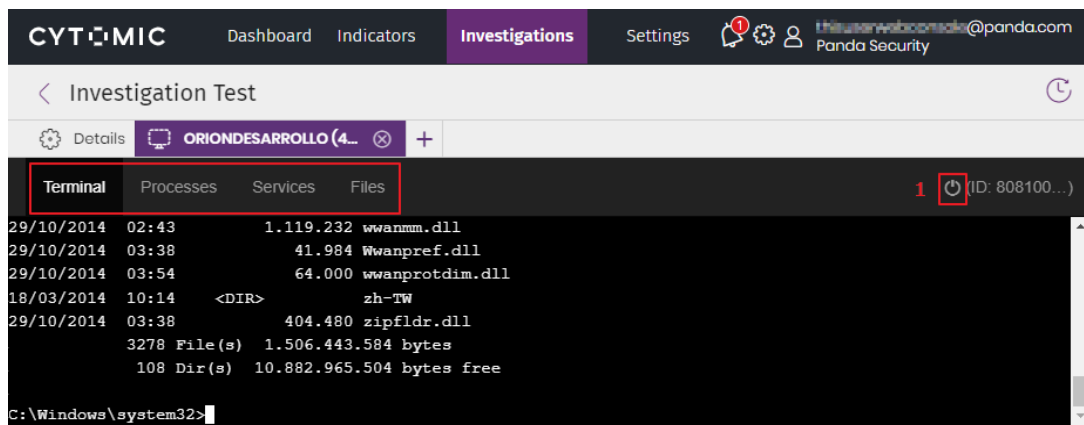


Figure 15.1: General menu for accessing the remote access tools

- **Remote command line:** Remote shell with administrator permissions. It enables you to perform operations on the target computer file system and run programs on the computer.
- **Process manager:** Shows a list of running processes on the target computer and enables you to stop them.
- **Service manager:** Shows a list of installed services on the target computer and enables you to start and stop them.
- **File transfer:** Enables you to send and receive files to and from the target computer.

- **Command line tools:** Set of programs accessible from the remote command line. These programs are intended to collect information to enhance investigations, recover data for forensic analysis, and remedy security breaches:
  - **delete:** Deletes files from the target computer hard disk.
  - **dump:** Dumps the memory assigned to processes to disk.
  - **netinfo:** Shows information about network interfaces.
  - **pcap:** Captures network packets and dumps them to the computer hard disk.
  - **ports:** Shows processes with open ports on the computer.
  - **process:** Shows the processes loaded in memory and their modules.
  - **url:** Shows a history of all URLs opened from the computer browser.

## Access the Response Tools

You can access all remediation tools in Cytomic Orion from the entities of interest associated with an investigation (for more information, see [Entities of Interest Panel](#) on page 107).

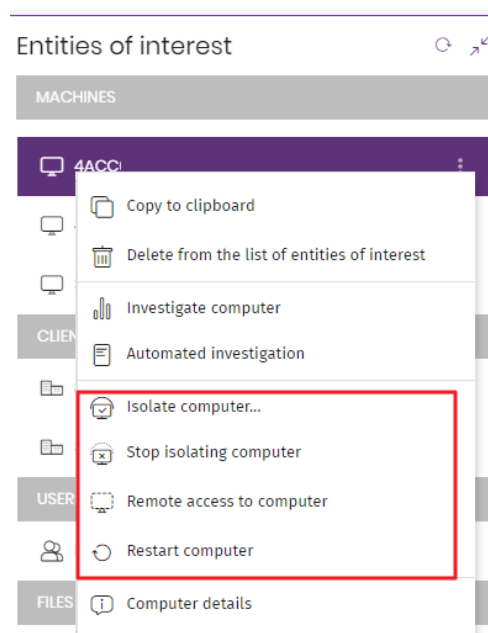



Figure 15.2: Access the response tools from the Entities of Interest sub-panel

To run a response tool:

- In the top menu, select **Investigations**. Select the investigation whose computer you want to investigate.
- In the **Entities of interest** sub-panel, find the **Computer**-type entity to which you want to connect to resolve the incident.

- From the entity context menu, select one of these options: **Isolate computer**, **Stop isolating computer**, **Restart computer**, and **Remote access to computer**. A confirmation message opens.
- Click **Yes**. A connection message opens. Next, the analyst console shows the available response tools (Process manager, Service manager, and File transfer) and the command line interface connected to the remote computer. (See figure [General menu for accessing the remote access tools](#)).
- To access the response tools, run the `rt` command from the command line. A menu opens that shows the available actions and the parameters you can use.
- To close the connection to the remote computer, click the  icon in the upper-right of the connection window (1 in figure [General menu for accessing the remote access tools](#)).

## Description of Response Tools


### Isolate Computer

Cytomic Orion enables you to isolate computers on demand to prevent the spread of threats and to block the exfiltration of confidential data.

When you isolate a computer, the solution blocks all communications, except for those it requires:



- Access to the computer from the analysis console so the incident response team can resolve possible problems with the tools provided by Cytomic Orion.
- Communications required by the Cytomic EDR and Cytomic EPDR security products to work correctly.


All other products and services installed on the affected workstation or server cannot communicate through the Internet/network.

To isolate a computer, select  **Isolate computer** in the context menu associated with the relevant entity of interest.

### Computer Isolation Statuses

The **Isolate computer** and **Stop isolating computer** operations are performed in real time. However, they might be delayed if the target computer is offline. To show the exact situation of a computer, Cytomic Orion distinguishes among four different isolation statuses through these icons:

- **Isolating** : The analyst launched a request to isolate one or more computers and the request is being processed.
- **Isolated** : The isolation process has completed and the computer communications are restricted.

- **Stopping isolation** : The analyst launched a request to stop isolating one or more computers and the request is being processed.
- **Not isolated**: The process to stop isolating a computer has completed. The computer is allowed to communicate with other computers based on the settings configured in other products or in the operating system.

These icons also appear next to the computers shown in the **Entities of interest** sub-panel of an investigation.

## Allowed Communications on an Isolated Computer

Cytomic Orion denies all communications to and from isolated computers except those required to perform remote forensic analysis and to use the response tools. These sections list the allowed and blocked communications.

Allowed processes and services:

### System Processes:

- All services required for the computer to be part of the corporate network: DHCP services to obtain IP addresses, ARP, WINS and DNS host name resolution services, etc.

### Cytomic Orion Processes:

- Services required to communicate with the default gateway.
- Services required to communicate with the Cytomic cloud in order to send the information collected from the monitoring of processes, and enable administrators to perform remote management tasks in the web console.

### Cytomic EDR:

- Services required to communicate with the default gateway.
- Services required to communicate with the Cytomic cloud in order to allow the protection engines to work, download signature files, and enable administrators to perform remote management tasks in the web console.
- Services required to communicate with the Cytomic cloud for the correct operation of the modules compatible with Cytomic EDR (Cytomic Patch, Cytomic Encryption, Cytomic Data Watch).
- Services required by an isolated machine with the discovery computer role to perform discovery tasks.
- Services required by an isolated machine with the cache role to act as a file server.
- Services required by a machine with the Cytomic proxy role assigned to act as a connection proxy.

## Blocked Communications on an Isolated Computer

All communications that are not listed in the section above are denied. This includes:



- Connection to the operating system's Windows Update service.




*The Cytomic Patch module remains operational on isolated computers.*

- Web browsing, FTP, mail, and other Internet protocols.
- SMB file transfer between PCs on the network.
- Remote installation of the Cytomic EDR security product.

## Restart Computer

There are cases where the incident response team might need to manually restart the remote computer:

- To manually reduce the attack surface, the incident response team might need to restart the target computer to release certain files and processes. For example, when you install operating system or application patches, when you update certain critical tools installed on the computer, such as the security solution to improve its threat detection capabilities, etc.
- When the computer is not working correctly.

To restart a computer, select  **Restart computer** in the context menu associated with the relevant entity of interest.

## Process Manager

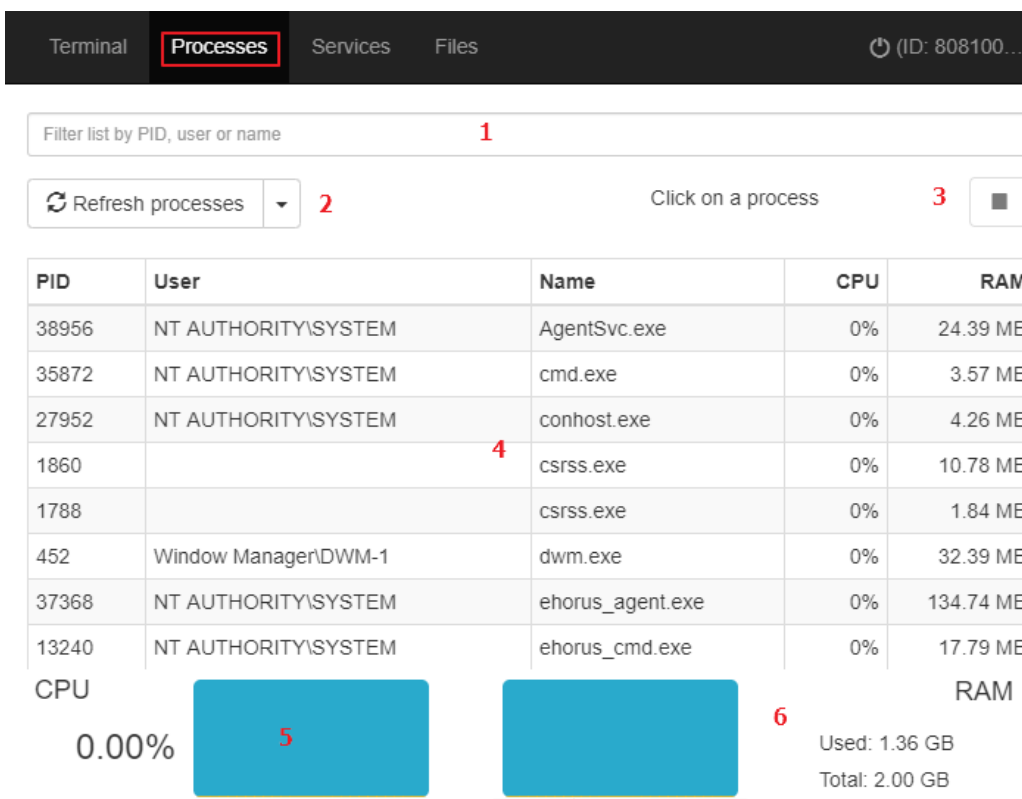


Figure 15.3: Process management tool

The process management tool shows information about all processes in the remote computer memory, including the RAM and CPU used. You can search for, stop, and start processes on the computer. The tool is divided into these areas:

- **Search bar (1):** Filter the list by a process name or PID. You can type only a partial string.
- **Auto refresh (2):** Specify the frequency that Cytomic Orion refreshes the information in the table.
- **Stop button (3):** Stops the selected process.
- **Process list (4):** Shows all processes in the remote computer memory.
- **CPU (5):** Shows the total CPU used by the processes and a line chart representing CPU usage since you opened the process management tool.
- **Memory (6):** Shows the total memory (RAM) used by the processes and a line chart representing memory usage since you opened the process management tool.

The process list (4) shows information about each process in the remote computer memory:

Field	Description
PID	Process ID.

Field	Description
User	User account that loaded the process.
Name	Process name.
CPU	CPU used by the process.
RAM	Memory used by the process

Table 15.1: Fields in the Processes list

## Service Manager

Terminal Processes **Services** Files (ID: 808100...)

Filter 1

Refresh services 2 Click on a service 3

Name	Description	Status
ActiveX Installer (AxInstSV)	Provides User Account Control and and if disabled the installation of ActiveX controls will behave according	Not Running
App Readiness	Gets apps ready for use the first	Not Running
Application Experience	Processes application compatib 4	Not Running
Application Identity	Determines and verifies the ider	Not Running
Background Intelligent Transfer Service	Transfers files in the backgroundd programs and other information.	Running
Background	Windows infrastructure service	Running

Figure 15.4: Service management tool

The service management tool shows all services configured on the remote computer and enables you to find specific services to change their status. The tool is divided into these areas:

- **Search bar (1):** Filter the list by a service name or description. You can type only a partial string.
- **Auto refresh (2):** Specify the frequency that Cytomic Orion refreshes the information in the list.
- **Service stop and start button (3):** Stop or start the selected service.
- **Service list (4):** Shows all services loaded in the remote computer memory.

The service list (4) shows information about each service configured on the remote computer.

Field	Description
Name	Service name.
Description	Service description.
Status	Service status: <ul style="list-style-type: none"> <li><b>Running</b>: The service is running.</li> <li><b>Not running</b>: The service is stopped.</li> </ul>

Table 15.2: Fields in the Services list

## File Transfer

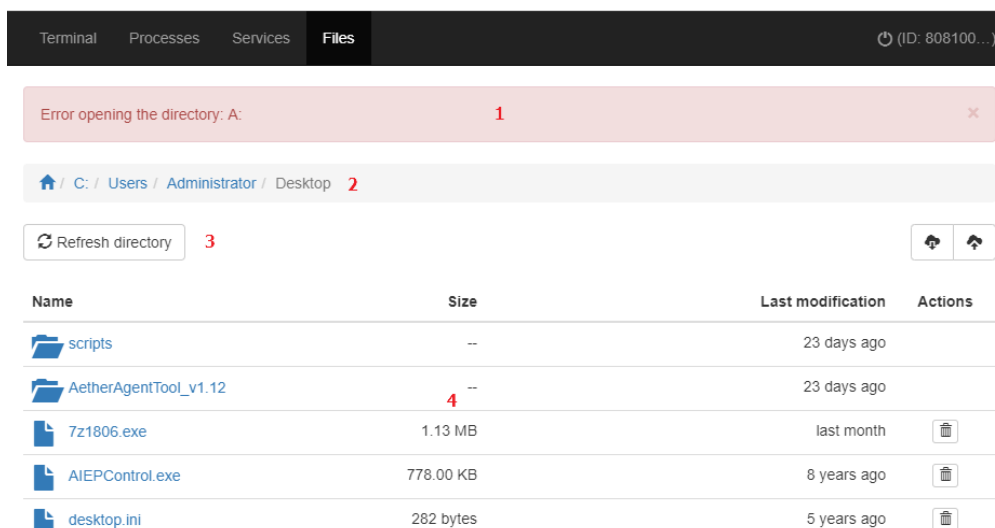





Figure 15.5: File management tool

The file management tool enables you to transfer files to and from your computer to the remote computer. You can also navigate the file system on the remote computer and delete files. The tool is divided into these areas:

- **Message bar (1)**: If there are errors when you try to get access to the remote computer file system, a message bar shows.
- **Path (2)**: The file path shows at the top of the window. To change directories, click another drive or folder in the file path. To show the list of devices connected to the computer, click  in the file path.
- **Auto refresh (3)**: Specify the frequency that Cytomic Orion refreshes the directory.
- **File list (4)**: Shows the list of files in the selected path (2).
- **Folders** : Click a folder to view the files it contains. The path (2) is updated automatically.
- **Delete** : Deletes the selected file and removes it from the computer.

The file list (4) shows information about each file found on the remote computer.


Field	Description
<b>Name</b>	Name of the file.
<b>Size</b>	Size of the file.
<b>Last modification</b>	Date when the file was last modified.
<b>Actions</b>	Actions you can take on the file. <ul style="list-style-type: none"> <li>•  Deletes the file.</li> </ul>

Table 15.3: Fields in the Files list

## Remote Command Line

The remote command line enables you can run commands compatible with the `cmd.exe` interpreter on the remote Windows computer. You can launch programs that generate text output. The remote command line runs under the `LOCAL_SYSTEM` account on the remote computer and is installed here:

```
C:\Program Files (x86)\Panda Security\Panda Aether Agent\Remote
access\
```

## Command Line Tools

Cytomic Orion supports `rt.exe`. This program provides access to a set of tools you can use to respond to security incidents. These tools enable you to recover information to perform a subsequent forensic analysis, and restore devices affected by a security breach to their original state.

You can access the `rt.exe` program from the remote command line. The program has the following syntax:

```
rt.exe [command] [-h|--help]
```

Consider these rules regarding the `rt.exe` program:

- Each command indicates an action to take and each command supports different parameters.
- Wildcards `*` and `?` are not supported.
- Some parameters allow partial searches that use substrings of characters that represent the start, middle, or end of a string. For example, to search for "malware", you can enter these substrings: "mal" or "ware".

- If a command supports dumping output to a file, this is specified with `-f`.
- To separate multiple items of the same type, enter the pipe character (`|`)

These sections describe the parameters supported by each command.

## Delete Command

This command deletes the files specified with the parameters `-n`, `-m`, or `-s` which are in the path indicated by the parameter `-p`. If the file is in use, the `delete` command returns an error.

Short form	Full parameter	Description	Notes
<b>h</b>	<b>-help</b>	Opens command help.	
<b>-f</b>	<b>--force</b>	Deletes files permanently.	
<b>-r</b>	<b>--restore</b>	Restores selected files from the Recycle Bin.	Restores files to their original location.
<b>-p</b>	<b>--path</b>	Absolute path from the root directory where you want to search for files to delete. The solution only deletes files in the specified path.	<ul style="list-style-type: none"> <li>• Use the backslash character (<code>\</code>) to separate folders.</li> <li>• Wildcards are not supported.</li> </ul>
<b>-n</b>	<b>--name</b>	Names of the files you want to delete.	<ul style="list-style-type: none"> <li>• To specify multiple files, separate file names with the pipe character (<code> </code>).</li> <li>• Wildcards are not supported.</li> </ul>
<b>-m</b>	<b>--md5</b>	MD5 values of the files you want to delete.	<ul style="list-style-type: none"> <li>• To specify multiple MD5 values, separate values with the pipe character (<code> </code>).</li> <li>• Wildcards are not supported.</li> </ul>
<b>-s</b>	<b>--sha256</b>	SHA256 values of the files you want to	<ul style="list-style-type: none"> <li>• To specify multiple</li> </ul>

Short form	Full parameter	Description	Notes
		delete.	SHA256 values, separate values with the pipe character ( ). <ul style="list-style-type: none"> <li>Wildcards are not supported.</li> </ul>

Table 15.4: Parameters supported by the delete command

## Dump Command

This command dumps to disk the memory space allocated to a system or user process.

Short form	Full parameter	Description	Notes
<b>h</b>	<b>-help</b>	Opens command help.	
<b>-p</b>	<b>--pid</b>	PID of the process to dump.	For information on how to dump the PID of the process, go to <a href="#">Process Command</a> .
<b>-s</b>	<b>--system</b>	Kernel dump.	Supported values: <ul style="list-style-type: none"> <li><b>mini</b>: Short dump of the stack content.</li> <li><b>kernel</b>: Full dump.</li> <li><b>full</b>: Dump of the entire physical memory of the computer, even if it is not in use.</li> </ul>
<b>-f</b>	<b>--filename</b>	Name of the file that contains the dump.	
<b>-z</b>	<b>--zip</b>	Stores the dump in a ZIP file.	

Table 15.5: Parameters supported by the dump command

## Netinfo Command

Used with the `-a` parameter, this command shows the settings of the network interfaces installed on the computer.

Short form	Full parameter	Description	Notes
<b>h</b>	<b>-help</b>	Opens command help.	
<b>-a</b>	<b>--all</b>	Shows the settings of the network interfaces installed on the computer.	
<b>-f</b>	<b>--filename</b>	Name of the file that contains the data.	
<b>-z</b>	<b>--zip</b>	Stores the dump in a ZIP file.	

Table 15.6: Parameters supported by the netinfo command

## Pcap Command

This command captures the network traffic sent and received by the remote computer. Specify the start and end of the capture with the parameters `-a start| stop`. Packet capture generates temporary files on the computer so there must be sufficient hard disk space. The end result is a PCAP file that can be used directly by the Wireshark/Ethereal program.

Short form	Full parameter	Description	Notes
<b>h</b>	<b>-help</b>	Opens command help.	
<b>-a</b>	<b>--action</b>	Executes an action: <ul style="list-style-type: none"> <li>• <b>start</b>: Starts the capture process.</li> <li>• <b>stop</b>: Stops the capture process.</li> <li>• <b>queryStatus</b>: Shows the status of the capture process.</li> </ul>	
<b>-m</b>	<b>--maxsize</b>	Maximum size of the packet to capture,	<ul style="list-style-type: none"> <li>• in megabytes (MB).</li> <li>• Default value: 200 MB.</li> </ul>
<b>-i</b>	<b>--maxtime</b>	Maximum capture time,	<ul style="list-style-type: none"> <li>• in seconds.</li> <li>• Default value: 86400 seconds (1 day).</li> </ul>
<b>-f</b>	<b>--filename</b>	Name of the file that contains the data.	



Short form	Full parameter	Description	Notes
-z	--zip	Stores the dump in a ZIP file.	

Table 15.7: Parameters supported by the pcap command

## Ports Command

Used with the `-a` parameter, this command shows the sockets open on the computer and the processes that opened them.

Short form	Full parameter	Description	Notes
<b>h</b>	<b>-help</b>	Opens command help.	
<b>-a</b>	<b>--all</b>	Shows all open ports and their associated processes.	
<b>-p</b>	<b>--pid</b>	Filters the results by process PID.	
<b>-n</b>	<b>--name</b>	Filters the results by process name.	You can type only a partial string.
<b>-f</b>	<b>--filename</b>	Name of the file that contains the data.	

Table 15.8: Parameters supported by the ports command

## Process Command

Used with the `-a` parameter, this command shows all processes loaded in the memory of the computer and their modules.

Short form	Full parameter	Description	Notes
<b>h</b>	<b>-help</b>	Opens command help.	
<b>-a</b>	<b>--all</b>	Shows all processes loaded in the memory of the computer and their modules.	
<b>-p</b>	<b>--pid</b>	Filters the results by process PID, showing the process modules.	

Short form	Full parameter	Description	Notes
-u	--user	Shows the processes launched by a user and their modules.	
-f	--filename	Name of the file that contains the data.	

Table 15.9: Parameters supported by the process command

## Url Command

Used with the `-a any` parameter, this command shows all the URLs accessed by users through the remote computer's web browser. This command requires that the Cytomic EDR web access control feature is enabled.

Short form	Full parameter	Description	Notes
h	-help	Opens command help.	
-a	--action	Filters the URL list by the action taken by the web access control feature. <ul style="list-style-type: none"> <li>• <b>allow</b>: Shows allowed URLs.</li> <li>• <b>deny</b>: Shows denied URLs.</li> <li>• <b>any</b>: Shows all visited URLs.</li> </ul>	
-c	--count	Maximum number of URLs to show.	Default value: unlimited.
-g	--category	Filters the URL list by the category assigned by the web access control feature.	
-b	--begindate	Enables you to specify the start date to show visited URLs from.	<ul style="list-style-type: none"> <li>• <b>Date format</b>: "YYYY-MM-DD HH:MM".</li> <li>• <b>Default value</b>: 30 days before the date you run the command.</li> </ul>
-e	--enddate	Enables you to specify the end date to show visited URLs up to.	<ul style="list-style-type: none"> <li>• <b>Date format</b>: "YYYY-MM-DD HH:MM".</li> </ul>

Short form	Full parameter	Description	Notes
			<ul style="list-style-type: none"><li>• <b>Default value:</b> Date you run the command.</li></ul>
<b>-n</b>	<b>--urlpattern</b>	Filters URLs by substring.	
<b>-u</b>	<b>--userpattern</b>	Filters URLs by user.	
<b>-f</b>	<b>--filename</b>	Name of the file that contains the data.	
<b>-z</b>	<b>--zip</b>	Stores the dump in a ZIP file.	

Table 15.10: Parameters supported by the url command

# Chapter 16

## Advanced Query Module SQL Syntax

Cytomic Orion implements an SQL dialect which is similar to the one used in other relational database engines, such as MySQL or Microsoft SQL Server, and used to create statements in the **Advanced SQL Query** module

### CHAPTER CONTENTS

---

<b>Supported Data Types</b> .....	<b>252</b>
<b>Regular Expressions</b> .....	<b>256</b>
<b>Select Clause Syntax</b> .....	<b>256</b>
<b>Regular Functions</b> .....	<b>262</b>
<b>Aggregate Functions</b> .....	<b>289</b>

## Supported Data Types

This section describes the data types supported in Cytomic Orion and special considerations when you use them, if any.

### Integers (INT and UINT)

Fixed-length integers, with or without a sign.

#### Signed Integer Range

- Int8 - [-128 : 127]
- Int16 - [-32768 : 32767]
- Int32 - [-2147483648 : 2147483647]
- Int64 - [-9223372036854775808 : 9223372036854775807]

## Unsigned Integer Range

- UInt8 - [0 : 255]
- UInt16 - [0 : 65535]
- UInt32 - [0 : 4294967295]
- UInt64 - [0 : 18446744073709551615]

## Decimal Numbers (DECIMALX)

Signed fixed point numbers that keep precision during add, subtract and multiply operations. For division, least significant digits are discarded (not rounded).

### Parameters

- **P - Precision.** Valid range: [1: 38]. Determines how many decimal digits the number can have (including the fraction).
- **S - Scale.** Valid range: [0: P]. Determines how many decimal digits the fraction can have.

### Decimal Value Ranges

- Decimal32 (S) -  $(-1 * 10^{(9 - S)}, 1 * 10^{(9 - S)})$
- Decimal64 (S) -  $(-1 * 10^{(18 - S)}, 1 * 10^{(18 - S)})$
- Decimal128 (S) -  $(-1 * 10^{(38 - S)}, 1 * 10^{(38 - S)})$

For example, Decimal32(4) can contain numbers from -99999.9999 to 99999.9999 with 0.0001 step.

### Internal Representation

Internally data is represented as normal signed integers with respective bit width. Real value ranges that can be stored in memory are a bit larger than specified above, which are checked only on conversion from string.

Because modern CPUs do not support 128 bit integers natively, operations on Decimal128 are emulated. Because of this, Decimal128 works significantly slower than Decimal32/Decimal64.

### Operations and Result Type

Binary operations on decimal result in a wider result type (with any order of arguments).

- Decimal64 (S1) Decimal32 (S2) -> Decimal64 (S)
- Decimal128 (S1) Decimal32 (S2) -> Decimal128 (S)
- Decimal128 (S1) Decimal64 (S2) -> Decimal128 (S)

Rules for scale:

- add, subtract:  $S = \max(S1, S2)$
- multiply:  $S = S1 + S2$ .
- divide:  $S = S1$ .

For similar operations between decimal and integers, the result is a decimal of the same size as the argument.

Operations between decimal and Float32/Float64 are not defined. If you really need them, you can explicitly convert one of the arguments by using `toDecimal32`, `toDecimal64`, `toDecimal128` or `toFloat32`, `toFloat64`. Keep in mind that the result will lose precision and type conversion is a computationally expensive operation.

Some functions on decimal return result as Float64 (for example, `var stddev`). Intermediate calculations might still be performed in decimal, which might lead to different results between Float64 and decimal inputs with the same values.

### Overflow Checks

During calculations on decimal, integer overflows might happen. Excessive digits in the fraction are discarded (not rounded). Excessive digits in the integer part will lead to an exception.

Overflow checks lead to operations slowdown. Overflow checks happen not only on arithmetic operations, but also on value comparison.

### Boolean Values

There is not a separate type for boolean values. They use the `UInt8` type, restricted to the values 0 or 1.

### Character Strings (STRING)

Strings of an arbitrary length. The length is not limited. The value can contain an arbitrary set of bytes, including null bytes. The `String` type replaces the types `VARCHAR`, `BLOB`, `CLOB`, and others from other DBMSs.

#### Encodings

Cytomic Orion does not support the concept of encodings. Strings can contain an arbitrary set of bytes, which are stored and output as-is. If you need to store texts, we recommend using UTF-8 encoding. As the analysis console supports UTF-8, you can read and write your values without making conversions. Similarly, certain functions for working with strings have separate variations that work under the assumption that the string contains a set of bytes representing a UTF-8 encoded text. For example, the `length` function calculates the string length in bytes, while the `lengthUTF8` function calculates the string length in Unicode code points, assuming that the value is UTF-8 encoded.

### Fixed-length Character Strings (FIXEDSTRING)

`FixedString(N)` is a fixed-length string of N bytes (not characters or code points).

To declare a column of `FixedString` type, use this syntax:

```
<column_name> FixedString (N)
```

Where `N` is a natural number.

The `FixedString` type is efficient when data has the length of precisely `N` bytes. In all other cases, it is likely to reduce efficiency.

Examples of values that can be efficiently stored in `FixedString`-typed columns:

- The binary representation of IP addresses (`FixedString(16)` for IPv6).
- Language codes (en\_US, ru\_RU, etc.).
- Currency codes (USD, RUB, etc.).
- The Binary representation of hashes (`FixedString(16)` for MD5, `FixedString(32)` for SHA256).

To store UUID values, use the `UUID` data type.

When inserting data, Cytomic Orion:

- Complements the string with null bytes if the string contains fewer than `N` bytes.
- Throws the `Too large value for FixedString(N)` exception if the string contains more than `N` bytes.

When you select data, Cytomic Orion does not remove the null bytes at the end of the string. If you use the `WHERE` clause, you should add null bytes manually to match the `FixedString` value. This behaviour differs from MySQL for the `CHAR` type (where strings are padded with spaces, and the spaces are removed for output),

Note that the length of the `FixedString(N)` value is constant. The `length` function returns `N` even if the `FixedString(N)` value is filled only with null bytes, but the `empty` function returns 1 in this case

## Date (DATE)

A date. Stored in two bytes as the number of days since 1970-01-01. It allows storing values from just after the beginning of the Unix Epoch to the upper threshold defined in 2105. The minimum value is 0000-00-00.

The date value is stored without the time zone.

## Date and Time (DATETIME)

`DateTime` is stored in four bytes as a Unix timestamp. It allows storing values in the same range as the one defined for the `Date` type. Time is stored with a precision of up to one second (without leap seconds).

## Time Zones

The `DateTime` type is converted from text (divided into component parts) to binary and back, using the system's time zone at the time the server starts. In text format, information about daylight savings is lost.

By default, the client switches to the timezone of the server when it connects. So, when you work with a textual date (for example, when you save text dumps), keep in mind that there might be ambiguity during changes for daylight savings time, and there might be problems matching data if the time zone changed.

## Nullable

Nullable (TypeName) allows to store a special marker (NULL) that denotes "missing value" alongside normal values allowed by TypeName. For example, a Nullable(Int8) type column can store Int8 type values, and the rows that do not have a value store NULL.

## Regular Expressions

Some parameters of functions used in SQL statements require the use of regular expressions. The syntax allowed in those expressions is Golang. For more information, see <https://github.com/google/re2/wiki/Syntax>.

Before you use a regular expression in an SQL statement in Cytomic Orion, we recommend that you validate its syntax. Go to <https://regex101.com/> and choose Golang as the language to validate the expression you want to use.

## Select Clause Syntax

This section shows the general syntax of an SQL statement:

```
SELECT [DISTINCT] expr_list
      [FROM [db.] table | (subquery) | table_function]
      [SAMPLE sample_coeff]
      [GLOBAL] [ANY|ALL] [INNER | LEFT | RIGHT | FULL | CROSS] [OUTER] JOIN
      (subquery) | table USING columns_list
      [PREWHERE expr]
      [WHERE expr]
      [GROUP BY expr_list] [WITH TOTALS]
      [HAVING expr]
      [ORDER BY expr_list]
      [LIMIT [n, ]m]
      [UNION ALL...]
      [LIMIT n BY columns]
```

### FROM Clause

The FROM clause specifies the source to read data from: a table, a subquery, or a JOIN clause. Subqueries must be specified in parenthesis. Unlike standard SQL, you do not need to specify a synonym after a subquery. For compatibility purposes, you can write 'name AS' after a subquery, but the specified name will not be used.

### SAMPLE Clause

The SAMPLE clause allows for approximated query processing.



When you use the `SAMPLE` clause, the query is not performed on all the data, but only on a certain fraction of the data (sample). For example, if you need to calculate statistics for a number of events, it is enough to execute the query on the 1/10 fraction of all the events and then multiply the result by 10.

Approximated query processing can be useful in these cases:

- When you want to speed up result collection.
- When your raw data is not accurate, so approximation does not noticeably degrade the quality of results.

The features of data sampling are these:

- Data sampling is a deterministic mechanism. The result of the same query is always the same.
- Sampling works consistently for different tables. For tables with a single sampling key, a sample with the same coefficient always selects the same subset of possible data. This means that you can use the sample in subqueries in the `IN` clause. Also, you can join samples using the `JOIN` clause.
- Sampling allows reading less data from a disk. Note that you must specify the sampling key correctly.

For the `SAMPLE` clause this syntax is supported::

Syntax	Description
<code>SAMPLE k</code>	Number from 0 to 1. The query is run on a $k$ fraction of data. For example, <code>SAMPLE 0.1</code> runs the query on 10% of data.
<code>SAMPLE n</code>	$n$ is a sufficiently large integer. The query is run on a sample of at least $n$ rows (but not significantly more than this). For example, <code>SAMPLE 10000000</code> runs the query on a minimum of 10,000,000 rows.
<code>SAMPLE k OFFSET m</code>	$k$ and $m$ are the numbers from 0 to 1. The query is run on a sample of $k$ fraction of the data. The data used for the sample is offset by $m$ fraction.

Table 16.1: Parameters supported by the `SAMPLE` clause

## JOIN Clause

Join indicates a join operation in relational algebra that combines columns from one or more tables, creating a new group that can be stored in a table or be used as is. Join produces a new table by combining columns from one or multiple tables by using values common to each. Supported types of `JOIN` in Cytomic Orion:

- **INNER JOIN (or JOIN):** Compares each row of table A with rows of table B to find all pairs of rows that satisfy the join-predicate specified in the `ON` clause. When the join-predicate is satisfied by matching non-NULL values, column values for each matched pair of rows of A and B are combined

into a result row.

- **LEFT JOIN (or LEFT OUTER JOIN):** Always contains all rows of the "left" table (A), even if the join-condition does not find any matching row in the "right" table (B). This means that if the `ON` clause matches 0 (zero) rows in B (for a given row in A), the join will still return a row in the result (for that row)—but with `NULL` in each column from B.
- **RIGHT JOIN (or RIGHT OUTER JOIN):** Always contains all rows of the "right" table (B), even if the join-condition does not find any matching row in the "left" table (A). This means that if the `ON` clause matches 0 (zero) rows in A (for a given row in B), the join will still return a row in the result (for that row)—but with `NULL` in each column from A.
- **FULL JOIN (or FULL OUTER JOIN):** Combines the effect of applying both `LEFT JOINS` and `RIGHT JOINS`. Where rows in the full outer joined tables do not match, the result set will have `NULL` values for every column of the table that lacks a matching row. For those rows that do match, a single row is produced in the result set (containing columns populated from both tables).
- **CROSS JOIN (or , )::** Returns the Cartesian product of rows from tables in the join. In other words, it produces rows which combine each row from the first table with each row from the second table.
- **ANY or ALL modifier:** If `ALL` is specified and the right table has several matching rows, the data is multiplied by the number of rows. This is the normal behavior of a `JOIN` clause in standard SQL. If `ANY` is specified and the right table has several matching rows, only the first one found is joined. If the right table has only one matching row, the results of `ANY` and `ALL` are the same.

## WHERE Clause

If there is a `WHERE` clause, it must contain an expression with the `UInt8` type. This is usually an expression with comparison and logical operators. This expression is used to filter data before all the transformations included in the statement.

## PREWHERE Clause

This clause has the same meaning as the `WHERE` clause. The difference is in which data is read from the table. With `PREWHERE`, at first only the columns necessary for executing the clause are read. Then, the other columns are read that are needed for running the rest of the query, but only those blocks where the `PREWHERE` expression is true.

`PREWHERE` filters data more efficiently and allows to read a lot less data from disk for query execution.

## GROUP BY Clause

This clause groups results by one or more columns. For grouping, Cytomic Orion interprets `NULL` as a value.

If the `WITH TOTALS` modifier is specified, another row is calculated. This row has key columns containing default values (zeros or empty lines), and columns of aggregate functions with the values calculated across all the rows (the "total" values). This extra row is only produced in JSON, TabSeparated\*, and Pretty formats. In JSON formats, this row is output as a separate 'totals' field. In TabSeparated formats, the row comes after the main result, preceded by an empty row. In Pretty formats, the row is output as a separate table after the main result.

You can use `WITH TOTALS` in subqueries, including subqueries in the `JOIN` clause (in this case, the respective total values are combined).



*As opposed to MySQL (and conforming to standard SQL, the `GROUP BY` statement does not support positional arguments. For example, `GROUP BY 1, 2` is interpreted as group by constant (that is, all rows in one).*

## LIMIT N BY Columns Clause

This clause selects the first `N` rows for each group of columns. `LIMIT N BY` is not related to `LIMIT`. They can both be used in the same query. `LIMIT N BY` can contain any number of columns or expressions.

## HAVING Clause

This clause enables you to filter the aggregation results produced by `GROUP BY`. It is similar to the `WHERE` clause, but the difference is that `WHERE` is performed before aggregation (`GROUP BY`), while `HAVING` is performed after it. You cannot use `HAVING` if aggregation is not performed.



*As opposed to MySQL (and conforming to standard SQL, the `GROUP BY` statement does not support positional arguments.*

## ORDER BY Clause

The `ORDER BY` clause contains a list of expressions, which can each be attributed with a `DESC` (descending) or `ASC` (ascending) modifier which determine the sorting direction. If the direction is not specified, `ASC` is assumed. The sorting direction applies to a single expression, not to the entire list.

Rows that have identical values for the list of sorting expressions are output in an arbitrary order, which can also be non-deterministic (different each time). If the `ORDER BY` clause is omitted, the order of the rows is also undefined, and might be non-deterministic as well.

### COLLATE

For sorting by String values, you can specify `COLLATE` to specify the alphabet you want to use. Example: `ORDER BY SearchPhrase COLLATE 'tr'` - for sorting by keyword in ascending order, using the Turkish alphabet, case insensitive, assuming that strings are UTF-8 encoded.

You can specify `COLLATE` or not for each expression independently. If you specify `ASC` or `DESC`, specify `COLLATE` after it. When you use `COLLATE`, sorting is always case-insensitive.

We recommend that you use `COLLATE` only for final sorting of a small number of rows, because sorting with `COLLATE` is less efficient than normal sorting by bytes.

### NaN and NULL Sorting Order:

- **With the NULLS FIRST modifier:** First NULL, then NaN, then other values.
- **With the NULLS LAST modifier:** First the values, then NaN, then NULL.
- **Default:** The same as with the NULLS LAST modifier.

When floating point numbers are sorted, NaNs are separate from the other values. Regardless of the sorting order, NaNs come at the end. In other words, for ascending sorting they are placed as if they are larger than all the other numbers, while for descending sorting they are placed as if they are smaller than the rest.

## SELECT Clause

Expressions specified in the `SELECT` clause are calculated after all the operations in the clauses described above are finished. If expressions in the `SELECT` clause contain aggregate functions, then the solution processes aggregate functions and the expressions used as their arguments during the `GROUP BY` aggregation. These expressions work as if they apply to separate rows in the result.

## DISTINCT Clause

If you specify `DISTINCT`, only a single row remains out of all the sets of fully matching rows in the result. It is possible to obtain the same result by applying `GROUP BY` across the same set of values as specified as `SELECT` clause, without using any aggregate functions. But there are few differences from the `GROUP BY` approach:

- `DISTINCT` can be applied together with `GROUP BY`.
- When you omit `ORDER BY` and define `LIMIT`, the query stops running immediately after the required number of different rows has been read.
- Data blocks are output as they are processed, without waiting for the entire query to finish running.

`DISTINCT` works with `NULL` as if `NULL` were a specific value. In other words, in the `DISTINCT` results, different combinations with `NULL` occur only once.

## LIMIT m Clause

This clause selects the first `m` rows from the result.

`LIMIT n, m` selects the first `m` rows from the result after skipping the first `n` rows. The `LIMIT m OFFSET n` syntax is equivalent. `n` and `m` must be non-negative integers.

If there is no `ORDER BY` clause that explicitly sorts results, the choice of rows for the result might be arbitrary and non-deterministic.

## UNION ALL Clause

You can use this clause to combine any number of queries. Only `UNION ALL` is supported. `UNION` (`UNION DISTINCT`) is not supported. If you need `UNION DISTINCT`, you can write `SELECT DISTINCT` from a subquery containing `UNION ALL`. Queries that are parts of `UNION ALL` can be run simultaneously, and their results can be mixed together.

The structure of results (the number and type of columns) must match for the queries. But the column names can differ. In this case, the column names for the final result will be taken from the first query. Type casting is performed for unions. For example, if two queries that are being combined have the same field with non-Nullable and Nullable types from a compatible type, the resulting `UNION ALL` has a Nullable type field.

You cannot enclose queries that are parts of `UNION ALL` in brackets. `ORDER BY` and `LIMIT` are applied to separate queries, not to the final result. If you need to apply a conversion to the final result, you can put all the queries with `UNION ALL` in a subquery in the `FROM` clause.

## IN Operators

In this section, we cover the `IN`, `NOT IN`, `GLOBAL IN`, and `GLOBAL NOT IN` operators separately, because their functionality is quite rich.

The left side of the `IN` operator is either a single column or a tuple. For example `SELECT UserID IN (123, 456) FROM ...`

If the left side is a single column that is in the index, and the right side is a set of constants, the system uses the index for processing the query.

The right side of the operator can be a set of constant expressions, a set of tuples, the name of a database table, or a `SELECT` subquery in brackets. The subquery can specify more than one column for filtering tuples. For example:

```
SELECT (CounterID, UserID) IN (SELECT CounterID, UserID FROM ...) FROM ....
```

The columns to the left and right of the `IN` operator should have the same type.

The `IN` operator and the subquery can occur in any part of the query, including in aggregate functions and lambda functions.

### NULL Processing

During request processing, the `IN` operator assumes that the result of an operation with `NULL` is always equal to 0, regardless of whether `NULL` is on the right or left side of the operator. `NULL` values are not included in any dataset, do not correspond to each other, and cannot be compared.

## The Asterisk Symbol (\*)

You can put an asterisk in any part of a query instead of an expression. When the query is analyzed, the asterisk is expanded to a list of all table columns. There are only a few cases when using an asterisk is justified:

- When you create a table dump.
- For tables that contain just a few columns.
- For getting information about what columns are in a table. In this case, set `LIMIT 1`. We recommend that you use the `DESC TABLE` query.
- When there is strong filtration on a small number of columns, use `PREWHERE`.

- In subqueries (because columns that are not needed for the external query are excluded from subqueries).

In all other cases, we do not recommend that you use the asterisk due to performance issues.

## Regular Functions

Regular functions work as if they are applied to each row separately (for each row, the result of the function does not depend on the other rows). Regular functions have these characteristics:

- **Strong typing:** In contrast to standard SQL, Cytomic Orion does not make implicit conversions between types. Each function works for a specific set of types. This means that sometimes you need to use type conversion functions.
- **Common subexpression elimination:** All expressions in a query that have the same AST (the same record or same result of syntactic parsing) are considered to have identical values. Such expressions are concatenated and executed once. Identical subqueries are also eliminated this way.
- **Types of results:** All functions return a single return as the result (not multiple values, and not zero values). The type of result is usually defined only by the types of arguments, not by the values.
- **Constants:** For simplicity, certain functions can only work with constants for some arguments. For example, the right argument of the `LIKE` operator must be a constant. Almost all functions return a constant for constant arguments. The exception is functions that generate random numbers. The `now` function returns different values for queries that were run at different times, but the result is considered a constant, since constancy is only important within a single query. A constant expression is also considered a constant (for example, the right half of the `LIKE` operator can be constructed from multiple constants).
- **NULL processing:** If at least one of the arguments of the function is `NULL`, the function result is also `NULL`, except in functions where it is specified otherwise.
- **Constancy:** Functions cannot change the values of their arguments - any changes are returned as the result. Thus, the result of calculating separate functions does not depend on the order in which the functions are written in the query.
- **Error handling:** Some functions can generate an exception if the data is invalid. In this case, the query is canceled and Cytomic Orion returns an error message to the client.
- **Argument evaluation:** In almost all programming languages, certain arguments might not be evaluated with some operators, such as `&&`, `||`, and `?:`. In Cytomic Orion, the arguments of functions (operators) are always evaluated. This is because whole parts of the columns are evaluated at the same time instead of calculating each row separately.

These are the most important functions:

## Arithmetic Functions

For all arithmetic functions, the result type is calculated as the smallest number type that the result fits in, if there is such a type. The minimum is taken simultaneously based on the number of bits, whether it is signed, and whether it is a floating-point number. If there are not enough bits, the highest bit type is taken.

Arithmetic functions work for any pair of types from UInt8, UInt16, UInt32, UInt64, Int8, Int16, Int32, Int64, Float32, or Float64.

Function	Description
<b>plus(a, b)</b> <b>a + b operator</b>	Calculates the sum of two numbers. You can also add integer numbers with a date (Date) or date and time (DateTime). In the case of a date, adding an integer means adding the corresponding number of days. For a date with time, it means adding the corresponding number of seconds.
<b>minus(a, b)</b> <b>a - b operator</b>	Calculates the difference between two numbers. The result is always signed. You can also calculate integer numbers from a date (Date) or date with time (DateTime).
<b>divide (a, b)</b> <b>a / b operator</b>	Calculates the quotient of the numbers. The result type is always a floating-point type. It is not integer division. For integer division, use the <code>intDiv</code> function. When dividing by zero you get <code>inf</code> , <code>-inf</code> , or <code>nan</code> .
<b>intDiv (a, b)</b>	Calculates the quotient of the numbers. Divides into integers, rounding down (by the absolute value). An exception is thrown when dividing by zero or when dividing a minimal negative number by minus one.
<b>intDivOrZero (a, b)</b>	Differs from <code>intDiv</code> in that it returns zero when dividing by zero or when dividing a minimal negative number by minus one.
<b>module (a, b)</b> <b>a % b operator</b>	Calculates the remainder after division.. If arguments are floating-point numbers, they are pre-converted to integers. The remainder is taken in the same sense as in C++. Truncated division is used for negative numbers. An exception is thrown when dividing by zero or when dividing a minimal negative number by minus one.
<b>negate(a)</b> <b>-a operator</b>	Calculates a number with the reverse sign. The result is always signed.
<b>abs (a)</b>	Calculates the absolute value of the number (a). That is, if $a < 0$ , it returns $-a$ . For unsigned types it does not do anything. For signed integer types, it returns an unsigned number.

Function	Description
<b>gcd (a, b)</b>	Returns the greatest common divisor of the numbers. An exception is thrown when dividing by zero or when dividing a minimal negative number by minus one.
<b>lcm(a, b)</b>	Returns the least common multiple of the numbers. An exception is thrown when dividing by zero or when dividing a minimal negative number by minus one.

Table 16.2: Arithmetic functions

## Comparison Functions

Comparison functions always return 0 or 1 (UInt8). These types can be compared:

- Numbers.
- Character strings (String) and fixed-length character strings (FixedString(N)).
- Dates (Date).
- Dates with times (DateTime)

For example, you cannot compare a date with a string. You have to use a function to convert the string to a date, or vice versa.

Strings are compared by bytes. A shorter string is smaller than all strings that start with it and that contain at least one more character..

The comparison operators are:

- **Equals:**  $a = b$  and  $a == b$
- **NotEquals:**  $a != b$  and  $a <> b$
- **Less:**  $a < b$
- **Greater:**  $a > b$
- **LessOrEquals:**  $a <= b$
- **GreaterOrEquals:**  $a >= b$

## Logical Functions

Logical functions accept any numeric types, but return a UInt8 number equal to 0 or 1.

Zero as an argument is considered "false," while any non-zero value is considered "true".

- **AND:** AND
- **OR:** OR



- **Not:** NOT
- **Xor:** XOR

## Type Conversion Functions

The basic supported conversions are:

- **Conversion to unsigned data types:** toUInt8, toUInt16, toUInt32, toUInt64.
- **Conversion to signed data types:** toInt8, toInt16, toInt32, toInt64, toFloat32, toFloat64, toDate, toDateTime.
- **Conversion to zero if error:** toUInt8OrZero, toUInt16OrZero, toUInt32OrZero, toUInt64OrZero, toInt8OrZero, toInt16OrZero, toInt32OrZero, toInt64OrZero, toFloat32OrZero, toFloat64OrZero, toDateOrZero, toDateTimeOrZero.
- **Conversion to null if error:** toUInt8OrNull, toUInt16OrNull, toUInt32OrNull, toUInt64OrNull, toInt8OrNull, toInt16OrNull, toInt32OrNull, toInt64OrNull, toFloat32OrNull, toFloat64OrNull, toDateOrNull, toDateTimeOrNull.

These are more complex data type conversions:

Function	Description
<b>toDecimal32(value, S), toDecimal64(value, S), toDecimal128(value, S)</b>	Converts <code>value</code> to decimal of precision <code>S</code> . The <code>value</code> can be a number or a string. The <code>S</code> parameter specifies the number of decimal places.
<b>toString</b>	<p>Functions for converting between numbers, strings (but not fixed strings), dates (Dates), and dates with times (DateTimes). All these functions accept one argument.</p> <p>When converting to or from a string, the value is formatted or parsed using the same rules as for the tab-separated format (TSV). If the string cannot be parsed, an exception is thrown and the request is canceled.</p> <p>When converting dates to numbers or vice versa, the date corresponds to the number of days since the beginning of the Unix epoch (1/1/1970).</p> <p>The date and date-with-time formats for the <code>toDate/toDateTime</code> functions are defined as follows:</p> <pre>YYYY-MM-DD YYYY-MM-DD hh: mm: ss</pre> <p>As an exception, if converting from UInt32, Int32, UInt64, or</p>

Function	Description
	<p>Int64 numeric types to Date, and if the number is greater than or equal to 65536, the number is interpreted as a Unix timestamp (and not as the number of days). This allows support for the common occurrence of writing <code>toDate (unix_timestamp)</code>, which otherwise would be an error and would require writing <code>toDate (toDateTime (unix_timestamp))</code>.</p> <p>Conversion between a date (Date) and date with time (DateTime) is performed the natural way: by adding a null time or deleting the time.</p> <p>Conversion between numeric types uses the same rules as assignments between different numeric types in C++.</p> <p>Additionally, the <code>toString</code> function of the <code>DateTime</code> argument can take a second String argument containing the name of the time zone.</p>
<b>toFixedString(s, N)</b>	<p>Converts a String type argument to a FixedString(N) type (a string with fixed length N). N must be a constant. If the string has fewer bytes than N, it is passed with null bytes to the right. If the string has more bytes than N, an exception is thrown.</p>
<b>toStringCutToZero(s)</b>	<p>Accepts a String or FixedString argument. It returns the String with the content truncated at the first zero byte found.</p>
<b>reinterpretAsUInt8,</b> <b>reinterpretAsUInt16,</b> <b>reinterpretAsUInt32,</b> <b>reinterpretAsUInt64</b>  <b>reinterpretAsInt8,</b> <b>reinterpretAsInt16,</b> <b>reinterpretAsInt32,</b> <b>reinterpretAsInt64</b>  <b>reinterpretAsFloat32,</b> <b>reinterpretAsFloat64</b>  <b>reinterpretAsDate,</b> <b>reinterpretAsDateTime</b>	<p>These functions accept a string and interpret the bytes placed at the beginning of the string as a number (little endian). If the string isn't long enough, the functions work as if the string is padded with the necessary number of null bytes. If the string is longer than needed, the extra bytes are ignored. A date (Date) is interpreted as the number of days since the beginning of the Unix Epoch (1/1/1970), and a date with time (DateTime) is interpreted as the number of seconds since the beginning of the Unix Epoch.</p>

Function	Description
<b>reinterpretAsString</b>	This function accepts a number or date (Date) or date with time (DateTime), and returns a string containing bytes representing the corresponding value in little endian format. Null bytes are dropped from the end. For example, a UInt32 type value of 255 is a string that is one byte long.
<b>reinterpretAsFixedString</b>	This function accepts a number or date (Date) or date with time (DateTime), and returns a FixedString containing bytes representing the corresponding value in little endian format. Null bytes are dropped from the end. For example, a UInt32 type value of 255 is a FixedString that is one byte long.
<b>CAST(x, t)</b>	Converts <i>x</i> to the <i>t</i> data type.
<b>toIntervalYear, toIntervalQuarter, toIntervalMonth, toIntervalWeek, toIntervalDay, toIntervalHour, toIntervalMinute, toIntervalSecond</b>	Converts a Number type argument to a Interval type (duration). The interval type is actually very useful, you can use this type of data to perform arithmetic operations directly with Date or DateTime.
<b>parseDateTimeBestEffort</b>	Parses a number type argument to a Date or DateTime type. Unlike toDate and toDateTime, <code>parseDateTimeBestEffort</code> can return a more complex date format.
<b>parseDateTimeBestEffortOrNull</b>	Same as for <code>parseDateTimeBestEffort</code> , except that it returns null when it encounters a date format that cannot be processed.
<b>parseDateTimeBestEffortOrZero</b>	Same as for <code>parseDateTimeBestEffort</code> , except that it returns zero date or zero date time when it encounters a date format that cannot be processed.

Table 16.3: Type conversion functions

## Functions for Working with Dates and Times

All functions for working with the date and time that have a logical use for the time zone can accept a second optional time zone argument. Only time zones that differ from UTC by a whole number of hours are supported

Function	Description
<b>toTimeZone</b>	Converts time (Date) or date and time (DateTime) to the specified time zone.
<b>toYear</b>	Converts a date (Date) or date with time (DateTime) to a UInt16 number containing the year number.
<b>toQuarter</b>	Converts a date (Date) or date with time (DateTime) to a UInt8 number containing the quarter number.
<b>toMonth</b>	Converts a date (Date) or date with time (DateTime) to a UInt8 number containing the month number (1-12).
<b>toDayOfYear</b>	Converts a date (Date) or date with time (DateTime) to a UInt8 number containing the number of the day of the year (1-366).
<b>toDayOfMonth</b>	Converts a date (Date) or date with time (DateTime) to a UInt8 number containing the number of the day of the month (1-31).
<b>toDayOfWeek</b>	Converts a date (Date) or date with time (DateTime) to a UInt8 number containing the number of the day of the week (Monday is 1, and Sunday is 7).
<b>toHour</b>	Converts a date (Date) or date with time (DateTime) to a UInt8 number containing the number of the hour in 24-hour time (0-23). This function assumes that if clocks are moved ahead for daylight saving time, it is by one hour and occurs at 2 A.M., and if clocks are moved back, it is by one hour and occurs at 3 A.M.
<b>toMinute</b>	Converts a date (Date) or date with time (DateTime) to a UInt8 number containing the number of the minute of the hour (0-59).
<b>toSecond</b>	Converts a date (Date) or date with time (DateTime) to a UInt8 number containing the number of the second in the minute (0-59). Leap seconds are not accounted for.
<b>toUnixTimestamp</b>	Converts a date (Date) or date with time (DateTime) to a unix timestamp.
<b>toStartOfYear</b>	Rounds down a date (Date) or date with time (DateTime) to the first

Function	Description
	day of the year. It returns the date (Date).
<b>toStartOfISOYear</b>	Rounds down a date (Date) or date with time (DateTime) to the first day of ISO year. It returns the date (Date).
<b>toStartOfQuarter</b>	Rounds down a date (Date) or date with time (DateTime) to the first day of the quarter (1 January, 1 April, 1 July, or 1 October). It returns the date (Date).
<b>toStartOfMonth</b>	Rounds down a date (Date) or date with time (DateTime) to the first day of the month. It returns the date (Date).
<b>toMonday</b>	Rounds down a date (Date) or date with time (DateTime) to the nearest Monday. It returns the date (Date).
<b>toStartOfDay</b>	Rounds down a date (Date) or date with time (DateTime) to the start of the day.
<b>toStartOfHour</b>	Rounds down a date (Date) or date with time (DateTime) to the start of the hour.
<b>toStartOfMinute</b>	Rounds down a date (Date) or date with time (DateTime) to the start of the minute.
<b>toStartOfFiveMinute</b>	Rounds down a date (Date) or date with time (DateTime) to the start of the five-minute interval.
<b>toStartOfTenMinutes</b>	Rounds down a date (Date) or date with time (DateTime) to the start of the ten-minute interval.
<b>toStartOfFifteenMinutes</b>	Rounds down a date (Date) or date with time (DateTime) to the start of the fifteen-minute interval.
<b>toTime</b>	Converts a date (Date) or date with time (DateTime) to a certain fixed date, while preserving the time.
<b>toRelativeYearNum</b>	Converts a date (Date) or date with time (DateTime) to the number of the year, starting from a certain fixed point in the past.

Function	Description
<b>toRelativeQuarterNum</b>	Converts a date (Date) or date with time (DateTime) to the number of the quarter, starting from a certain fixed point in the past.
<b>toRelativeMonthNum</b>	Converts a date (Date) or date with time (DateTime) to the number of the month, starting from a certain fixed point in the past.
<b>toRelativeWeekNum</b>	Converts a date (Date) or date with time (DateTime) to the number of the week, starting from a certain fixed point in the past.
<b>toRelativeDayNum</b>	Converts a date (Date) or date with time (DateTime) to the number of the day, starting from a certain fixed point in the past.
<b>toRelativeHourNum</b>	Converts a date (Date) or date with time (DateTime) to the number of the hour, starting from a certain fixed point in the past.
<b>toRelativeMinuteNum</b>	Converts a date (Date) or date with time (DateTime) to the number of the minute, starting from a certain fixed point in the past.
<b>toRelativeSecondNum</b>	Converts a date (Date) or date with time (DateTime) to the number of the second, starting from a certain fixed point in the past.
<b>toISOYear</b>	Converts a date (Date) or date with time (DateTime) to a UInt16 number containing the ISO year number.
<b>toISOWeek</b>	Converts a date (Date) or date with time (DateTime) to a UInt8 number containing the ISO week number.
<b>now</b>	Accepts zero arguments. It returns the current time at the time of function execution. This function returns a constant.
<b>today</b>	Accepts zero arguments. It returns the current date at the time of function execution. The same as <code>toDate (now ())</code> .
<b>yesterday</b>	Accepts zero arguments. It returns yesterday's date at the time of function execution. The same as <code>today () - 1</code> .
<b>timeSlot</b>	Rounds the time to the half hour.
<b>toYYYYMM</b>	Converts a date (Date) or date with time (DateTime) to a UInt32

Function	Description
	number containing the year and month number (YYYY * 100 + MM).
<b>toYYYYMMDD</b>	Converts a date (Date) or date with time (DateTime) to a UInt32 number containing the year and month number (YYYY * 10000 + MM * 100 + DD).
<b>toYYYYMMDDhhmmss</b>	Converts a date (Date) or date with time (DateTime) to a UInt64 number containing the year and month number (YYYY * 10000000000 + MM * 100000000 + DD * 1000000 + hh * 10000 + mm * 100 + ss).
<b>addYears, addMonths, addWeeks, addDays, addHours, addMinutes, addSeconds, addQuarters</b>	This function adds a Date/DateTime interval to a Date/DateTime variable and then return the Date/DateTime.
<b>subtractYears, subtractMonths, subtractWeeks, subtractDays, subtractHours, subtractMinutes, subtractSeconds, subtractQuarters</b>	This function subtracts a Date/DateTime interval to a Date/DateTime variable and then return the Date/DateTime.
<b>dateDiff('unit', t1, t2, [timezone])</b>	Returns the difference between two times expressed in <code>unit</code> e.g. hours. <code>t1</code> and <code>t2</code> can be Date or DateTime. If <code>timezone</code> is specified, it is applied to both arguments. If not, timezones from data types <code>t1</code> and <code>t2</code> are used. If the timezones are not the same, the result is unspecified.  Supported unit values: <code>second, minute, hour, day, week, month, quarter, year</code> .
<b>formatDateTime(Time, Format[, Timezone])</b>	This function formats <code>Time</code> according to the format specified in the <code>Format</code> string. For more information about the format parameters, see table <a href="#">Format codes for the formatDateTime function</a> .

Table 16.4: Functions for working with dates and times

## Format Codes for the formatDateTime Function

Code	Description	Example
<b>%C</b>	Year divided by 100 and truncated to integer (00-99).	20
<b>%d</b>	Day of the month, zero-padded (01-31).	02
<b>%D</b>	Short MM/DD/YY date, equivalent to %m/%d/%y.	01/07/2023
<b>%e</b>	Day of the month, space-padded ( 1-31)	2
<b>%F</b>	Short YYYY-MM-DD date, equivalent to %Y-%m-%d.	2023-01-07
<b>%H</b>	Hour in 24h format (00-23).	22
<b>%I</b>	Hour in 12h format (01-12).	10
<b>%j</b>	Day of the year (001-366).	007
<b>%m</b>	Month as a decimal number (01-12).	01
<b>%M</b>	Minute (00-59).	33
<b>%n</b>	New-line character. '\n'.	
<b>%p</b>	AM or PM.	PM
<b>%R</b>	24-hour HH:MM time, equivalent to %H:%M.	22:33
<b>%S</b>	Second (00-59).	44
<b>%t</b>	Horizontal-tab character ('\t').	
<b>%T</b>	ISO 8601 time format (HH:MM:SS), equivalent to %H:%M:%S.	22:33:44
<b>%u</b>	ISO 8601 weekday as number with Monday as 1 (1-7).	2



Code	Description	Example
<b>%V</b>	ISO 8601 week number (01-53).	01
<b>%w</b>	Weekday as a decimal number with Sunday as 0 (0-6).	2
<b>%y</b>	Year, last two digits (00-99).	23
<b>%Y</b>	Year	2023
<b>%%</b>	A % sign.	

Table 16.5: Format codes for the formatDateTime function

## Functions for Working with Strings

Function	Description
<b>empty</b>	Returns 1 for an empty string or 0 for a non-empty string. The result type is UInt8. A string is considered non-empty if it contains at least one byte, even if this is a space or a null byte.
<b>notEmpty</b>	Returns 0 for an empty string or 1 for a non-empty string. The result type is UInt8. The function also works for arrays.
<b>length</b>	Returns the length of a string in bytes (not in characters, and not in code points). The result type is UInt64.
<b>lengthUTF8</b>	Returns the length of a string in Unicode code points (not in characters), assuming that the string contains a set of bytes that make up UTF-8 encoded text. If this assumption is not met, it does not throw an exception. The result type is UInt64.
<b>char_length, CHAR_LENGTH</b>	Returns the length of a string in Unicode code points (not in characters), assuming that the string contains a set of bytes that make up UTF-8 encoded text. If this assumption is not met, it does not throw an exception. The result type is UInt64.
<b>character_length, CHARACTER_LENGTH</b>	Returns the length of a string in Unicode code points (not in characters), assuming that the string contains a set of bytes that make up UTF-8 encoded text. If this assumption is not met, it

Function	Description
	does not throw an exception. The result type is UInt64.
<b>lower, lcase</b>	Converts ASCII Latin symbols in a string to lowercase.
<b>upper, ucase</b>	Converts ASCII Latin symbols in a string to uppercase.
<b>lowerUTF8</b>	Converts a string to lowercase, assuming the string contains a set of bytes that make up a UTF-8 encoded text. It does not detect the language. If the length of the UTF-8 byte sequence is different for upper and lower case of a code point, the result could be incorrect. If the string contains a set of bytes that is not UTF-8, then the behavior is undefined.
<b>upperUTF8</b>	Converts a string to uppercase, assuming the string contains a set of bytes that make up a UTF-8 encoded text. It does not detect the language. If the length of the UTF-8 byte sequence is different for upper and lower case of a code point, the result could be incorrect. If the string contains a set of bytes that is not UTF-8, then the behavior is undefined.
<b>isValidUTF8</b>	Returns 1, if the set of bytes constitutes valid UTF-8-encoded text, otherwise 0.
<b>reverse</b>	Reverses the string (as a sequence of bytes).
<b>reverseUTF8</b>	Reverses a sequence of Unicode code points, assuming that the string contains a set of bytes representing a UTF-8 text. Otherwise, it does not throw an exception.
<b>concat(s1, s2, ...)</b>	Concatenates the strings listed in the arguments, without a separator.
<b>concatAssumeInjective(s1, s2, ...)</b>	Same as <code>concat</code> , the difference is that you need to ensure that <code>concat (s1, s2, s3) -&gt; s4</code> is injective. It is used for optimization the <code>GROUP BY</code> clause.
<b>substring(s, offset, length), mid(s, offset, length), substr(s, offset, length)</b>	Returns a substring starting with the byte from the <code>offset</code> index that is <code>length</code> bytes long. Character indexing starts from one (as in standard SQL). The <code>offset</code> and <code>length</code> arguments must be

Function	Description
	constants.
<b>substringUTF8(s, offset, length)</b>	The same as <code>substring</code> , but for Unicode code points. It works under the assumption that the string contains a set of bytes representing a UTF-8 encoded text. If this assumption is not met, it does not throw an exception.
<b>appendTrailingCharIfAbsent(s, c)</b>	If the <code>s</code> string is non-empty and does not contain the <code>c</code> character at the end, it appends the <code>c</code> character to the end.
<b>convertCharset(s, from, to)</b>	Returns the string <code>s</code> that was converted from the encoding in <code>from</code> to the encoding in <code>to</code> .
<b>base64Encode(s)</b>	Encodes the <code>s</code> string into base64.
<b>base64Decode(s)</b>	Decodes the base64-encoded string <code>s</code> into its original string. In case of failure, it raises an exception.
<b>tryBase64Decode(s)</b>	Similar to <code>base64Decode</code> , but in case of error an empty string is returned.
<b>endsWith(s, suffix)</b>	Returns 1 if the string ends with the specified suffix, otherwise it returns 0.
<b>startsWith(s, prefix)</b>	Returns 1 if the string starts with the specified prefix, otherwise it returns 0.
<b>trimLeft(s)</b>	Returns a string that removes the whitespace characters on the left side.
<b>trimRight(s)</b>	Returns a string that removes the whitespace characters on the right side.
<b>trimBoth(s)</b>	Returns a string that removes the whitespace characters on either side.

Table 16.6: Functions for working with strings

## Functions for Searching Strings

The search is case-sensitive by default in all these functions. There are separate variants for case insensitive search.

Function	Description
<b>position(haystack, needle), locate(haystack, needle)</b>	<p>Searches for the substring <code>needle</code> in the string <code>haystack</code>. It returns the position (in bytes) of the found substring, starting from 1, or returns 0 if the substring was not found.</p> <p>For a case-insensitive search, use the function <code>positionCaseInsensitive</code>.</p>
<b>positionUTF8(haystack, needle)</b>	<p>The same as <code>position</code>, but the position is returned in Unicode code points. It works under the assumption that the string contains a set of bytes representing a UTF-8 encoded text. If this assumption is not met, it does not throw an exception.</p> <p>For a case-insensitive search, use the function <code>positionCaseInsensitiveUTF8</code>.</p>
<b>multiSearchFirstPosition(haystack, [needle1, needle2, ..., needlen])</b>	<p>The same as <code>position</code> but returns the leftmost offset of the string <code>haystack</code> that matches some of the <code>needle</code>.</p> <p>For a case-insensitive search or/and in UTF-8 format use functions <code>multiSearchFirstPositionCaseInsensitive</code>, <code>multiSearchFirstPositionUTF8</code>, <code>multiSearchFirstPositionCaseInsensitiveUTF8</code>.</p>
<b>multiSearchFirstIndex(haystack, [needle1, needle2, ..., needlen])</b>	<p>Returns the index <code>i</code> (starting from 1) of the leftmost found <code>needle</code> in the string <code>haystack</code> and 0 otherwise.</p> <p>For a case-insensitive search or/and in UTF-8 format use functions: <code>multiSearchFirstIndexCaseInsensitive</code>, <code>multiSearchFirstIndexUTF8</code>, <code>multiSearchFirstIndexCaseInsensitiveUTF8</code>.</p>
<b>multiSearchAny(haystack, [needle1, needle2, ..., needlen])</b>	<p>Returns 1, if at least one string <code>needle</code> matches the string <code>haystack</code> and 0 otherwise.</p> <p>For a case-insensitive search or/and in UTF-8 format use functions: <code>multiSearchAnyCaseInsensitive</code>, <code>multiSearchAnyUTF8</code>, <code>multiSearchAnyCaseInsensitiveUTF8</code>.</p> <p><b>Note:</b> In all <code>multiSearch *</code> functions, the number of <code>needle</code></p>

Function	Description
	parameters should be less than 28.
<b>match(haystack, pattern)</b>	<p>Checks whether the string matches the pattern regular expression. The syntax of the re2 regular expressions is more limited than the syntax of the Perl regular expressions.</p> <p>It returns 0 if it does not match, or 1 if it matches.</p> <p>Note that the backslash symbol (\) is used for escaping in the regular expression. The same symbol is used for escaping in string literals. So, in order to escape the symbol in a regular expression, you must write two backslashes (\\) in a string literal.</p> <p>The regular expression works with the string as if it is a set of bytes. The regular expression cannot contain null bytes. For patterns to search for substrings in a string, it is better to use <code>LIKE</code> or <code>position</code>, because they work much faster.</p>
<b>multiMatchAny(haystack, [pattern1, pattern2, ..., patternn])</b>	<p>The same as <code>match</code>, but it returns 0 if none of the regular expressions are matched and 1 if any of the patterns matches. For patterns to search substrings in a string, it is better to use <code>multiSearchAny</code>, because it works much faster.</p> <p>Note: The length of any of the <code>haystack</code> string must be less than 232 bytes, otherwise an exception is thrown.</p>
<b>multiMatchAnyIndex(haystack, [pattern1, pattern2, ..., patternn])</b>	The same as <code>multiMatchAny</code> , but it returns any index that matches the <code>haystack</code> .
<b>multiFuzzyMatchAny(haystack, distance, [pattern1, pattern2, ..., patternn])</b>	The same as <code>multiMatchAny</code> , but it returns 1 if any pattern matches the <code>haystack</code> within a constant edit distance. This function is in an experimental mode and can be extremely slow.
<b>multiFuzzyMatchAnyIndex(haystack, distance, [pattern1, pattern2, ..., patternn])</b>	<p>The same as <code>multiFuzzyMatchAny</code>, but it returns any index that matches the <code>haystack</code> within a constant edit distance.</p> <p>Note: <code>multiFuzzyMatch</code> * functions do not support UTF-8 regular expressions, and such expressions are treated as bytes.</p>
<b>extract(haystack, pattern)</b>	Extracts a fragment of a string using a regular expression. If <code>haystack</code> does not match the <code>pattern</code> regex, an empty string is returned. If the regex doesn't contain subpatterns, it takes the

Function	Description
	fragment that matches the entire regex. Otherwise, it takes the fragment that matches the first subpattern.
<b>like(haystack, pattern), haystack LIKE pattern operator</b>	<p>Checks whether a string matches a simple regular expression. The regular expression can contain the metasymbols '%' and '_'.</p> <ul style="list-style-type: none"> <li>• '%': indicates any quantity of any bytes (including zero characters).</li> <li>• '_': indicates any one byte..</li> </ul> <p>Use the backslash (\) for escaping metasymbols. See the note on escaping in the description of the <code>match</code> function.</p> <p>For regular expressions such as <code>%needle%</code> the code is more optimal and works as fast as the <code>position</code> function. For other regular expressions, the code is the same as for the <code>match</code> function.</p>
<b>notLike(haystack, pattern), haystack NOT LIKE pattern operator</b>	The same thing as <code>like</code> , but negative.

Table 16.7: Functions for searching strings

## Functions for Replacing in Strings

Function	Description
<b>replaceOne(haystack, pattern, replacement)</b>	Replaces the first occurrence, if it exists, of the <code>pattern</code> substring in <code>haystack</code> with the <code>replacement</code> substring. <code>pattern</code> and <code>replacement</code> must be constants.
<b>replaceAll(haystack, pattern, replacement), replace(haystack, pattern, replacement)</b>	Replaces all occurrences of the <code>pattern</code> substring in <code>haystack</code> with the <code>replacement</code> substring.
<b>replaceRegexpOne (haystack, pattern, replacement)</b>	Replacement using the <code>pattern</code> regular expression. A re2 regular expression. It replaces only the first occurrence, if it exists. A pattern can be specified as <code>replacement</code> . This pattern can include substitutions <code>\0</code> - <code>\9</code> . The substitution <code>\0</code> includes the entire regular expression.

Function	Description
	<p>Substitutions <code>\1 - \9</code> correspond to the subpattern numbers. To use the <code>\</code> character in a template, escape it using <code>\</code>. Also keep in mind that a string literal requires an extra escape.</p> <p><b>Example. Copying a string ten times:</b></p> <pre>SELECT replaceRegexpOne ('Hello, World!', '. *', '\\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0') AS res</pre> <p><b>Result:</b></p> <pre>Hello, World! Hello, World! Hello, World! Hello, World! Hello, World! Hello, World! Hello, World! Hello, World! Hello, World! Hello, World! ;</pre>
<p><b>replaceRegexpAll</b> (haystack, pattern, replacement)</p>	<p>This does the same thing as <code>replaceRegexpOne</code>, but replaces all the occurrences.</p> <p><b>Example:</b></p> <pre>SELECT replaceRegexpAll('Hello, World!', '.', '\\0\\0') AS res</pre> <pre>HHeellllloo,, WWoorrrlidd!!</pre> <p>If a regular expression worked on an empty substring, the replacement is not made more than once.</p> <p><b>Example:</b></p> <pre>SELECT replaceRegexpAll('Hello, World!', '^', 'here: ') AS res</pre> <pre>here: Hello, World!</pre>
<p><b>regexpQuoteMeta(s)</b></p>	<p>The function adds a backslash before some predefined characters in the string. Predefined characters: <code>'0', '\\', ' ', '('', ')', '^', '\$', '.', '['', ']', '?', '*', '+', '{', ':', '-'</code>.</p> <p>This implementation slightly differs from <code>re2</code>. It escapes zero byte as <code>\0</code> instead of <code>\x00</code>, and escapes only required characters.</p>

Table 16.8: Functions for replacing in strings

## Mathematical Functions

All these functions return a Float64 number. The accuracy of the result is close to the maximum precision possible, but the result might not coincide with the machine representable number nearest to the corresponding real number.

Function	Description
<b>e()</b>	Returns a Float64 number that is close to the number e.
<b>pi()</b>	Returns a Float64 number that is close to the number $\pi$ .
<b>exp(x)</b>	Accepts a numeric argument and returns a Float64 number close to the exponent of the argument.
<b>log(x), ln(x)</b>	Accepts a numeric argument and returns a Float64 number close to the natural logarithm of the argument.
<b>exp2(x)</b>	Accepts a numeric argument and returns a Float64 number close to 2 to the power of x.
<b>log2(x)</b>	Accepts a numeric argument and returns a Float64 number close to the binary logarithm of the argument.
<b>exp10(x)</b>	Accepts a numeric argument and returns a Float64 number close to 10 to the power of x.
<b>log10(x)</b>	Accepts a numeric argument and returns a Float64 number close to the decimal logarithm of the argument.
<b>sqrt(x)</b>	Accepts a numeric argument and returns a Float64 number close to the square root of the argument.
<b>cbrt(x)</b>	Accepts a numeric argument and returns a Float64 number close to the cubic root of the argument.
<b>erf(x)</b>	If $x$ is non-negative, then $\text{erf}$ is the probability that a random variable having a normal distribution with standard deviation $s$ takes the value that is separated from the expected value by more than $x$ .
<b>erfc(x)</b>	Accepts a numeric argument and returns a Float64 number close to $1 - \text{erf}(x)$ , but without loss of precision for large



Function	Description
	$x$ values.
<b>lgamma(x)</b>	The logarithm of the gamma function.
<b>tgamma(x)</b>	Gamma function.
<b>sin(x)</b>	The sine.
<b>cos(x)</b>	The cosine.
<b>tan(x)</b>	The tangent.
<b>asin(x)</b>	The arc sine.
<b>acos(x)</b>	The arc cosine.
<b>atan(x)</b>	The arc tangent.
<b>pow(x, y), power(x, y)</b>	Takes two numeric arguments $x$ and $y$ . It returns a Float64 number close to $x$ to the power of $y$ .
<b>intExp2</b>	Accepts a numeric argument and returns a UInt64 number close to 2 to the power of $x$ .
<b>intExp10</b>	Accepts a numeric argument and returns a UInt64 number close to 10 to the power of $x$ .

Table 16.9: Arithmetic functions

## Rounding Functions

Function	Description
<b>floor(x[, N])</b>	<p>Returns the largest round number that is less than or equal to <math>x</math>. A round number is a multiple of <math>1/10N</math>, or the nearest number of the appropriate data type if <math>1/10N</math> is not exact. <math>N</math> is an integer constant, optional parameter. By default it is zero, which means to round to an integer. <math>N</math> may be negative.</p> <p>Examples:</p> <pre>floor (123.45, 1) = 123.4</pre>

Function	Description
	<p><code>floor (123.45, -1) = 120.</code></p> <p><code>x</code> is any numeric type. The result is a number of the same type. For integer arguments, it makes sense to round with a negative <code>N</code> value. For a non-negative <code>N</code>, the function does not do anything.</p>
<b>ceil(x[, N]), ceiling(x[, N])</b>	Returns the smallest round number that is greater than or equal to <code>x</code> . In every other way, it is the same as the <code>floor</code> function.
<b>round(x[, N])</b>	<p>Rounds <code>x</code> to a specified number of decimal places (<code>N</code>). It rounds to the nearest even integer. In case when given number has equal distance to surrounding numbers, the function returns the number that has the closest even digit.</p> <p>Parameters:</p> <ul style="list-style-type: none"> <li>• <b>x</b>: The number to be rounded. It can be any expression returning the numeric data type.</li> <li>• <b>N</b>: An integer value. <ul style="list-style-type: none"> <li>• If <code>N &gt; 0</code> then the function rounds the value to the right of the decimal point.</li> <li>• If <code>N &lt; 0</code> then the function rounds the value to the left of the decimal point.</li> <li>• If <code>N = 0</code> then the function rounds the value to integer. In this case, the argument can be omitted.</li> </ul> </li> </ul> <p>Returned value:</p> <p>The rounded number of the same type as the input number.</p>
<b>roundToExp2 (num)</b>	Accepts a number. If the number is less than one, it returns 0. Otherwise, it rounds the number down to the nearest (whole non-negative) degree of two..

Table 16.10: Rounding functions

## Random Number Generation Functions

Non-cryptographic generators of pseudo-random numbers are used. All the functions accept zero arguments or one argument. If an argument is passed, it can be any type, and its value is not used for anything. The only purpose of this argument is to prevent common subexpression elimination, so that two different instances of the same function return different columns with different random numbers.

Function	Description
<b>rand</b>	Returns a pseudo-random UInt32 number, evenly distributed among all UInt32-

Function	Description
	type numbers. It uses a linear congruential generator.
<b>rand64</b>	Returns a pseudo-random UInt64 number, evenly distributed among all UInt64-type numbers. It uses a linear congruential generator.
<b>randConstant</b>	Returns a pseudo-random UInt64 number, evenly distributed among all UInt64-type numbers.

Table 16.11: Functions for generating random numbers

## Encoding Functions

Function	Description
<b>hex</b>	Accepts arguments of types: String, UInt, Date, or DateTime. It returns a string containing the argument's hexadecimal representation. It uses uppercase letters A-F. It does not use 0x prefixes or h suffixes. For character strings, all bytes are simply encoded as two hexadecimal numbers. Numbers are converted to big endian format. Date is encoded as the number of days since the beginning of the Unix epoch. DateTime is encoded as the number of seconds since the beginning of the Unix epoch.
<b>unhex(str)</b>	Accepts a string containing any number of hexadecimal digits, and returns a string containing the corresponding bytes. It supports both uppercase and lowercase letters A-F. The number of hexadecimal digits does not have to be even. If it is odd, the last digit is interpreted as the younger half of the 00-0F byte. If the argument string contains anything other than hexadecimal digits, an exception is not thrown. If you want to convert the result to a number, you can use the <code>reverse</code> and <code>reinterpretAsType</code> functions.
<b>bitmaskToList(num)</b>	Accepts an integer. It returns a string containing the list of powers of two that total the source number when summed. They are comma-separated without spaces in text format, in ascending order.

Table 16.12: Encoding functions

## Functions for Working with URLs

Function	Description
<b>protocol</b>	Returns the protocol. Examples: <code>http</code> , <code>ftp</code> , <code>mailto</code> , <code>imap</code> , etc.
<b>domain</b>	Returns the domain.
<b>domainWithoutWWW</b>	Returns the domain and removes no more than one 'www.' from the beginning of it, if present
<b>topLevelDomain</b>	Returns the top-level domain. Example: <code>.com</code> .
<b>firstSignificantSubdomain</b>	Returns the "first significant subdomain". <ul style="list-style-type: none"> <li>The first significant subdomain is a second-level domain if it is 'com', 'net', 'org', or 'co'.</li> <li>Otherwise, it is a third-level domain.</li> </ul>
<b>cutToFirstSignificantSubdomain</b>	Returns the part of the domain that includes top-level subdomains up to the "first significant subdomain" (see the explanation above).
<b>path</b>	Returns the path. The path does not include the query string.
<b>pathFull</b>	The same as above, but including query string and fragment. Example: <code>/top/news.html?page=2#comments</code>
<b>queryString</b>	Returns the query string. The query string does not include the initial question mark, #, or anything after #.
<b>fragmenttext</b>	Returns the fragment identifier. It does not include the initial hash # symbol.
<b>queryStringAndFragment</b>	Returns the query string and fragment identifier.
<b>extractURLParameter(URL, name)</b>	Returns the value of the <code>name</code> parameter in the URL, if present. Otherwise, an empty string. If there are many parameters with this name, it returns the first occurrence. This

Function	Description
	function works under the assumption that the parameter name is encoded in the URL exactly the same way as in the passed argument.
<b>extractURLParameters(URL)</b>	Returns an array of name=value strings corresponding to the URL parameters. The values are not decoded in any way.
<b>extractURLParameterNames(URL)</b>	Returns an array of name strings corresponding to the names of URL parameters. The values are not decoded in any way.
<b>URLHierarchy(URL)</b>	<p>Returns an array containing the URL, truncated at the end by the symbols /,? in the path and query-string. Consecutive separator characters are counted as one. The cut is made in the position after all the consecutive separator characters.</p> <p>Example:</p> <pre data-bbox="691 992 1345 1308">URLPathHierarchy ('https://example.com/browse/CONV-6788') = [   '/browse/',   '/browse/CONV-6788' ]</pre>
<b>URLPathHierarchy(URL)</b>	The same as above, but without the protocol and host in the result. The /' element (root) is not included.
<b>decodeURLComponent(URL)</b>	Returns the decoded URL.
<b>cutWWW</b>	Removes no more than one 'www.' from the beginning of the URL's domain, if present.
<b>cutQueryString</b>	Removes the query string. The question mark is also removed.
<b>cutFragment</b>	Removes the fragment identifier. The number sign is also removed.
<b>cutQueryStringAndFragment</b>	Removes the query string and fragment identifier. The

Function	Description
	question mark and number sign are also removed.
<b>cutURLParameter(URL, name)</b>	Removes the 'name' URL parameter, if present. This function works under the assumption that the parameter name is encoded in the URL exactly the same way as in the passed argument.

Table 16.13: Functions for working with URLs

## Functions for Working with IP Addresses

Function	Description
<b>IPv4NumToString (num)</b>	Takes a UInt32 number. Interprets it as an IPv4 address in big endian. It returns a string containing the corresponding IPv4 address in the format A.B.C.d (dot-separated numbers in decimal form).
<b>IPv4StringToNum(s)</b>	The reverse function of <code>IPv4NumToString</code> . If the IPv4 address has an invalid format, it returns 0.
<b>IPv4NumToStringClassC (num)</b>	Similar to <code>IPv4NumToString</code> , but using xxx instead of the last octet.
<b>IPv6NumToString(x)</b>	Accepts a FixedString(16) value containing the IPv6 address in binary format. It returns a string containing this address in text format. IPv6-mapped IPv4 addresses are output in the format ::ffff:111.222.33.44.
<b>IPv6StringToNum(s)</b>	The reverse function of <code>IPv6NumToString</code> . If the IPv6 address has an invalid format, it returns a string of null bytes. HEX can be uppercase or lowercase.
<b>IPv4ToIPv6(x)</b>	Takes a UInt32 number. Interprets it as an IPv4 address in big endian. It returns a FixedString(16) value containing the IPv6 address in binary format.
<b>cutIPv6(x, bitsToCutForIPv6, bitsToCutForIPv4)</b>	Accepts a FixedString(16) value containing the IPv6 address in binary format. It returns a string containing the address of the specified number of bits removed in text format.

Function	Description
<b>IPv4CIDRtoIPv4Range(ipv4, cidr)</b>	Accepts an IPv4 and an UInt8 value containing the CIDR. It returns a tuple with two IPv4 containing the lower range and the higher range of the subnet.
<b>IPv6CIDRtoIPv6Range(ipv6, cidr)</b>	Accepts an IPv6 and an UInt8 value containing the CIDR. It returns a tuple with two IPv6 containing the lower range and the higher range of the subnet.

Table 16.14: Functions for working with IP addresses

## Functions for Working with Nullable Arguments

Function	Description
<b>isNull(x)</b>	<p>Checks whether the argument is NULL.</p> <p>Parameters:</p> <ul style="list-style-type: none"> <li><b>x</b>: A value with a non-compound data type.</li> </ul> <p>Returned value:</p> <ul style="list-style-type: none"> <li><b>1</b>: If x is NULL.</li> <li><b>0</b>: If x is not NULL.</li> </ul>
<b>isNotNull(x)</b>	<p>Parameters:</p> <ul style="list-style-type: none"> <li><b>x</b>: A value with a non-compound data type.</li> </ul> <p>Returned value:</p> <ul style="list-style-type: none"> <li><b>0</b>: If x is NULL.</li> <li><b>1</b>: If x is not NULL.</li> </ul>
<b>coalesce(x,...)</b>	<ul style="list-style-type: none"> <li><b>Parameters</b>: Any number of parameters of a non-compound type. All parameters must be compatible by data type.</li> <li><b>Returned values</b>: The first non-NULL argument. NULL, if all arguments are NULL.</li> </ul>
<b>ifNull</b>	Returns an alternative value if the main argument is NULL.

Function	Description
<b>ifNull (x, alt)</b>	<p>Parameters:</p> <ul style="list-style-type: none"> <li>• <b>x</b>: The value to check for NULL.</li> <li>• <b>alt</b>: The value that the function returns if <b>x</b> is NULL.</li> </ul> <p>Returned values</p> <ul style="list-style-type: none"> <li>• The value <b>x</b>, if <b>x</b> is not NULL.</li> <li>• The value <b>alt</b>, if <b>x</b> is NULL.</li> </ul>
<b>nullIf(x,y)</b>	<p>Returns NULL if the arguments are equal.</p> <p>Parameters:</p> <ul style="list-style-type: none"> <li>• <b>x, y</b>: Values for comparison. They must be compatible types, or the solution generates an exception.</li> </ul> <p>Returned values:</p> <ul style="list-style-type: none"> <li>• NULL, if the arguments are equal.</li> <li>• The <b>x</b> value, if the arguments are not equal.</li> </ul>
<b>assumeNotNull(x)</b>	<p>Parameters:</p> <ul style="list-style-type: none"> <li>• <b>x</b>: The original value.</li> </ul> <p>Returned values</p> <ul style="list-style-type: none"> <li>• The original value from the non-Nullable type, if it is not NULL.</li> <li>• The default value for the non-Nullable type if the original value was NULL.</li> </ul>
<b>toNullable(x)</b>	<p>Converts the argument type to Nullable.</p> <p>Parameters:</p> <ul style="list-style-type: none"> <li>• <b>x</b>: The value of any non-compound type.</li> </ul> <p>Returned value:</p> <ul style="list-style-type: none"> <li>• The input value with a non-Nullable type.</li> </ul>

Table 16.15: Functions for working with Nullable aggregates



# Aggregate Functions

Unlike regular functions, which work as if they are applied to each row separately, aggregate functions accumulate data from multiple rows (that is, they depend on the whole set of rows).

Function	Description
<b>count()</b>	<p>Counts the number of rows in a table. It accepts zero arguments and returns <code>UInt64</code>. The <code>COUNT (DISTINCT x)</code> syntax is not supported. The separate <code>uniq</code> function is used for this purpose.</p> <p><code>SELECT count() FROM table</code> statements are not optimized because the number of entries in the table is not stored separately. Internally, Cytomic Orion selects a small column of the table and counts the number of values in it.</p>
<b>any(x)</b>	<p>Selects the first encountered value. You can run the query in any order and even in a different order each time, so the result of this function is indeterminate. To get a determinate result, you can use the <code>min</code> or <code>max</code> function instead of <code>any</code>.</p> <p>In some cases, you can rely on the order of execution. This applies to cases when <code>SELECT</code> comes from a sub-query that uses <code>ORDER BY</code>.</p> <p>When a <code>SELECT</code> query has the <code>GROUP BY</code> clause or at least one aggregate function, Cytomic Orion requires that all expressions in the <code>SELECT</code>, <code>HAVING</code>, and <code>ORDER BY</code> clauses be calculated from aggregate functions. In other words, each column selected from the table must be used either in keys or inside aggregate functions</p>
<b>anyHeavy(x)</b>	<p>Selects a frequently occurring value. If there is a value that occurs more than in half the cases in each of the query execution threads, this value is returned. Usually, the result is non-deterministic.</p>
<b>anyLast(x)</b>	<p>Selects the last value encountered.</p>
<b>min(x)</b>	<p>Returns the minimum value.</p>
<b>max(x)</b>	<p>Returns the maximum value.</p>
<b>argMin(arg, val)</b>	<p>Calculates the <code>arg</code> value for a minimum <code>val</code> value. If there are several different values of <code>arg</code> for minimum values of <code>val</code>, the solution returns the first of these values encountered.</p>

Function	Description
<b>argMax(arg, val)</b>	Calculates the <code>arg</code> value for a maximum <code>val</code> value. If there are several different values of <code>arg</code> for maximum values of <code>val</code> , the solution returns the first of these values encountered.
<b>sum(x)</b>	Calculates the sum. It only works for numbers.
<b>sumWithOverflow(x)</b>	Calculates the sum of the numbers, using the same data type for the result as for the input parameters. If the sum exceeds the maximum value for this data type, the function returns an error.
<b>avg(x)</b>	Calculates the arithmetic mean. It only works for numbers. The result is always <code>Float64</code> .
<b>uniq(x)</b>	Calculates the approximate number of different values of the argument. It works for numbers, strings, <code>Dates</code> , <code>DateTimes</code> , and multiple arguments and tuple type arguments.  It provides the result deterministically (it does not depend on the query processing order).
<b>uniqExact(x)</b>	Calculates the exact number of different argument values. We recommend that you use the <code>uniq</code> function. Use the <code>uniqExact</code> function if you absolutely need an exact result.
<b>quantile(level)(x)</b>	This calculates the <code>x</code> quantile of <code>level</code> order. <code>level</code> is a constant floating-point number from 0 to 1.  If you omit the <code>level</code> parameter, 0.5 is taken by default (median calculation).  This function takes numbers, <code>Dates</code> , and <code>DateTimes</code> , and returns: <ul style="list-style-type: none"> <li>• <b>For numbers:</b> <code>Float64</code></li> <li>• <b>For Dates:</b> <code>Date</code></li> <li>• <b>For DateTimes:</b> <code>DateTime</code></li> </ul> The precision of this function is relatively low. Use <code>quantileExact(level)(x)</code> for maximum precision.  The result is non-deterministic (it depends on the query processing order).

Function	Description
<b>quantileExact(level)(x)</b>	Exactly computes the quantile of level <code>level</code> .
<b>median(x)</b>	Calculates the median of a numeric data sample.
<b>varSamp(x)</b>	Represents an unbiased estimate of the variance of a random variable. The values passed as arguments represent a sample of the total population. The function returns Float64.
<b>varPop(x)</b>	Calculates the variance of the population passed as argument.
<b>stddevSamp(x)</b>	Represents an unbiased estimate of the standard deviation of a random variable. The values passed as arguments represent a sample of the total population. The function returns Float64.
<b>stddevPop(x)</b>	Calculates the standard deviation of the population passed as argument.
<b>covarSamp(x, y)</b>	Represents an unbiased estimate of the covariance of two random variables. The values passed as arguments represent two samples of the total population. The function returns Float64.
<b>covarPop(x, y)</b>	Calculation of the covariance of two random variables. The values passed as arguments represent two populations. The function returns Float64.
<b>corr(x, y)</b>	Calculates the Pearson correlation coefficient.

Table 16.16: Aggregate functions

# Chapter 17

## Cytomic Orion Integration with SOC Tools

Given the increase in the variety of devices that require protection, the number of threats in circulation, and the infection vectors they use, organization SOCs are simply overwhelmed by the amount and diversity of incidents they have to manage. This situation leads organizations to incorporate new and increasingly sophisticated tools to automate the processes of incident analysis, containment, and remediation. This new range of services covers many areas and requires continuous exchange of information, often manually, between applications.

These new tools create greater difficulty when it comes to consistently and homogeneously executing the procedures implemented in the SOC. As a result, response times are highly variable and the quality of service obtained depends directly on the type of incident being handled, the set of tools used, and the technical team that used them.

Cytomic Orion implements multiple APIs that facilitate integration with the set of tools used in the SOC as well as automated management of the resources involved in incidents and incident response.



*The retention period for the telemetry stored in the data lake is one year.*

### CHAPTER CONTENTS

---

<b>Test the Functionality of APIs in Cytomic Orion</b> .....	<b>293</b>
Postman Project .....	293
Sample Code in Python .....	294
<b>SOC Integration Architecture</b> .....	<b>294</b>
<b>Types of APIs Available in Cytomic Orion</b> .....	<b>295</b>
<b>Requirements and Access to the Cytomic Orion APIs</b> .....	<b>296</b>
General Requirements .....	296

Enable Access to the API from External Programs .....	296
<b>Cytomic Orion and OAuth Authentication .....</b>	<b>298</b>
Basic Concepts .....	298
OAuth Data Flow .....	299
<b>Cytomic Orion API Specification .....</b>	<b>307</b>
IOC API .....	308
Knowledge API .....	318
Indicator API .....	325
Response API .....	328
OSQuery Access API .....	331
Data/Advanced Query Access API .....	338
Investigation Management API .....	339

## Test the Functionality of APIs in Cytomic Orion

To support analysts and developers, Cytomic provides these resources:

- Postman project
- Sample code in Python

### Postman Project

Postman is a collaboration platform for building APIs. You can use Postman to design, build, and test APIs along with colleagues. Cytomic Orion uses Postman to enable and speed up the adoption of this technology by developers


The Cytomic Orion API is available as a Postman project for all clients and enables them to make calls from this environment and view the results without having to write a single line of code.



You can download and install Postman from <https://www.getpostman.com/>.

To send requests to the Cytomic Orion API from Postman:

- Download `file` `Postman.Orion.API.zip` from <https://info.cytomicmodel.com/resources/guides/Orion/en/Postman.Orion.API.zip> and extract it to your desktop.
- Open Postman and import the files `APIOrion.postman_collection.json` and `APIOrion.postman_environment.json`. To do this, select **File** and **Import**.
- Generate a new application in the Cytomic Orion console (see [Enable Access to the API from External Programs](#)). Save the user name and password.

- Click the  icon in the upper-right corner of the Postman page. Copy the user name and password from the previous step in the `username` and `password` fields of the **CURRENT VALUE** column.
- If it is the first time you send a request in the session, run the `Authentication API` method in the **Authentication** branch to get an access token and a refresh token.
- In the **1.0** branch in the Postman left panel, select the API call you want to make. Click **Send**. The program creates the correct HTTP request based on the API specification and the provided parameters, and shows the server response along with the HTTP code that indicates whether or not it was successful.

## Sample Code in Python

Cytomic provides a PY file compatible with Python 3.0 and higher that contains basic examples of all of the API methods. To run the sample code:

- Download `file Orion_API.zip` from <https://info.cytomicmodel.com/resources/guides/Orion/en/Postman.Orion.API.zip> and extract it to your desktop.
- Download a Python 3.x interpreter from <https://www.python.org/downloads/>.
- Run `file Orion_API.v1.1.py` directly with the interpreter or with an IDE such as Spyder or similar (see <https://www.spyder-ide.org/>)

## SOC Integration Architecture

Cytomic Orion integrates with third-party tools and applications developed in the SOC through multiple REST APIs. This diagram shows how Cytomic Orion integrates with SOC resources:

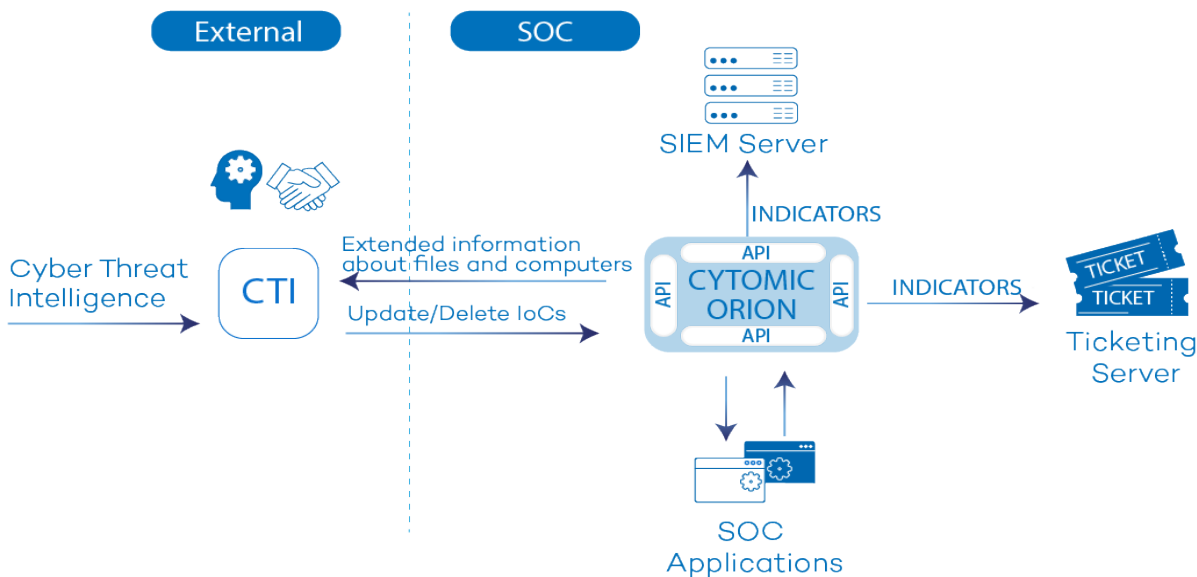


Figure 17.1: Cytomic Orion integration with multiple SOC products

Elements in the diagram:

- **CTI (Cyber Threat Intelligence)**: An open platform for exchanging cybersecurity information. It monitors, collects, and analyzes potential cyberthreats targeting organizations, thus enabling security teams to design defensive and remediation actions. Cytomic Orion is compatible with MISP (<http://www.misp-project.org/>).



See the integration guide at <https://www.vanimpe.eu/2020/03/10/integrating-misp-and-cytomic-orion/>

- **Ticketing**: Tools that ensure the correct management of indicators. These tools enable you to create, assign, and follow up on investigations until they are closed, and collect key performance indicators (KPIs) that show the value of the SOC security service. Cytomic Orion is compatible with ServiceNow (<https://www.servicenow.com/products/servicenow/>).



Download the integration guide from <https://info.cytomicmodel.com/resources/guides/Orion/en/ORION-snowguide-EN.pdf>

- **SOC Apps**: Applications created in the SOC that use the Cytomic Orion API to resolve specific problems.
- **SIEM (Security Information and Event Management)**: Tools that combine security information management and security event management to enable real-time monitoring and analysis of the security-related events generated by applications and hardware on the network.

## Types of APIs Available in Cytomic Orion

The methods SOC applications and third-party solutions can use are divided into five categories:

- **Indicator query**: Returns a list of indicators of potential attacks logged in the Cytomic Orion platform in the specified period.
- **File and computer information query**: Returns information about the classification of files detected on computers. It also returns information about the devices that make up the IT infrastructure.
- **IOC management**: Receives new indicators of compromise that Cytomic Orion uses in its analysis of the flow of events generated by the company's computers to detect new malware.
- **Response tools**: Invokes mechanisms to resolve and mitigate the impact of any potential attacks detected by the Cytomic Orion platform.
- **OSQuery access**: Send OSQuery statements to get information about the client's IT infrastructure.

- **Investigations:** Enables you to create, modify, and delete investigations.
- **Data access:** Access to the data lake. This is equivalent to the advanced SQL query module.



*For more information about each of the available APIs, see [Cytomic Orion API Specification](#).*

## Requirements and Access to the Cytomic Orion APIs

### General Requirements

To use the Cytomic Orion APIs, make sure these requirements are met:

- You must have HTTPS access to the <https://auth.pandasecurity.com/oauth/token> server on port 443 for authentication on the Cytomic Orion OAuth server.
- You must have HTTPS access to the API server (<https://api.orion.cytomic.ai>) on port 443 to send requests.
- You must have an application-type account created in the Cytomic Orion console. For more information, see [Enable Access to the API from External Programs](#).
- You must have software that uses the Cytomic Orion API:
  - A smartphone app.
  - A native application.
  - A client-server web application or single-page application (SPA).
  - A plug-in that runs on a third-party solution.

### Enable Access to the API from External Programs

To enable access to the Cytomic Orion API from an application:



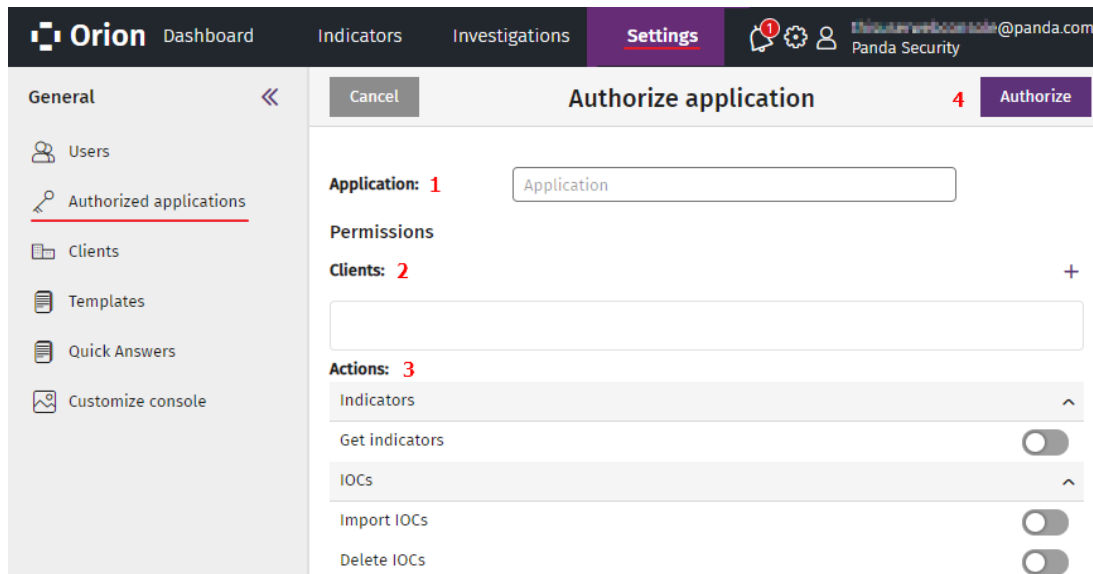


Figure 17.2: Page for enabling API access from a third-party application

- In the top menu, select **Settings**. In the side menu, select **Authorized applications**. Click **Authorize application**. A page opens for you to enter the information required to validate the application through the OAuth protocol.
- In the **Application (1)** field, enter the name of the program that you want to access the API. This is a descriptive field. It has no effect on the process described in this section.
- **Clients (2)**: Click the **+** icon to configure the SOC clients from which you want to retrieve data in each call to the Cytomic Orion API.
- **Actions (3)**: Specifies the sources of information the application can access.
  - **Get indicators**: See [Indicator API](#).
  - **Import IOCs**: See [Import and Search for IOCs in the Telemetry Generated by a Client's Computers](#).
  - **Delete IOCs**: See [Delete IOCs Imported onto the Platform](#).
  - **Search for IOCs**: See [List IOCs Loaded onto the Platform by Attributes](#)
  - **View information about a file, get the computers on which it was seen, and view details about the computers**: See [Knowledge API](#).
  - **Isolate/deisolate computers**: See [Isolate Computers](#) and [Deisolate Computers](#).
  - **Restart computers**: See [Restart](#).
  - **Access to OSQuery**: See [OSQuery Access API](#).
  - **Access to data/Access to advanced queries**: See [Get Information from the Data Lake](#).
- Click **Authorize**. Cytomic Orion registers the application on the platform and shows the user name and password generated.

- Keep the **Username** character string in a safe place. This string is used as the content of the `username` field in requests from the application.
- Save the **Password** character block. This block must be used as the content of the `password` field in requests from the application.



*The password block is shown only once in the Cytomic Orion console: when you create the application. If you lose the password, you cannot retrieve it. In such case, you must delete the application and create it again with a different password. Do the same if the password is compromised.*

- Regardless of the credentials generated in the `username` and `password` fields, the OAuth authentication system requires that you specify these client credentials:
  - **client\_id**: aaf1461b714646a8a593197641df9665
  - **client\_secret**: cnmB6rbT4xoZsnTzwHsgBpm1BtD-k\_-1VKpZEI6blvM
  - **client\_id** : **client\_secret**:  
 YWFmMTQ2MWI3MTQ2NDZhOGE1OTMxOTc2NDZkZjk2NjU6Y25tQjZyYlQ0e  
 G9ac25Uendlc2dCcG0xQnRELWtLTFWS3BaRWw2Ykl2TQ==

When the procedure is complete, the application must authenticate on the Cytomic Orion platform using the OAuth protocol, as described in section [Cytomic Orion and OAuth Authentication](#).

## Cytomic Orion and OAuth Authentication

OAuth (Open Authorization) is an open, widely used industry standard that allows delegated access to protected resources. The main scenario for which OAuth was designed is that of a user who needs to grant permission to websites or third-party applications to access protected information without exposing the user's login credentials. OAuth, therefore, provides secure delegated access to an owner's resources on behalf on the owner, and specifies the processes required for the owner to authorize third-party access without sharing the owner's credentials.

Designed specifically to work with Hypertext Transfer Protocol (HTTP), OAuth essentially allows access tokens to be issued to third-party programs by an authorization server, with the approval of the resource owner..

Cytomic Orion uses the OAuth standard to authenticate and authorize requests from applications that access its APIs.

### Basic Concepts

These concepts are key to understanding how the OAuth protocol works. Cytomic Orion uses a subset of the features included in OAuth to control access to the APIs provided to clients.

- **API:** The resource used by third-party applications. Access to the APIs is controlled or protected by OAuth.
- **Application:** The third-party application that requests authorization to access the protected resource (the API). To do this, it uses the credentials assigned to the application account.
- **Application account:** The account that owns the resource for which access is controlled or protected (the API). For more information about how to create the application user name and password, see [Enable Access to the API from External Programs](#).
- **User name and password:** The user ID and password for the application account. They correspond to the `username` and `password` parameters in the OAuth standard. For more information about how to create the application user name and password, see [Enable Access to the API from External Programs](#).
- **Authentication server:** The system that creates and validates the application account credentials sent by the third-party applications. Cytomic Orion delegates validation of the `username` and `password` credentials to the IdP server (Cytomic Identity Provider).
- **Client\_id and client\_secret:** The ID and password assigned to the Cytomic Orion client. See [Enable Access to the API from External Programs](#).
- **Authorization server:** The server with which the application interacts when it requests access to a protected resource. Cytomic Orion delegates this task to the CAS (Cytomic Authorization Server). To control access, the CAS receives the `client_id` and `client_secret` credentials from the application, and provides it with a short-lived token which defines the scope of access.
- **Access token:** The character string used by the application to access the protected resource (the API). The access token describes the scope of access, the access duration, and other relevant information. Tokens are opaque strings for the client application. They are issued by the CAS and are meaningful only for the CAS.
- **Refresh token:** When the application accesses the resource for the first time, it is granted an access token and a refresh token. When the access token expires, the application uses the refresh token to requests a new access token without restarting the authentication and authorization processes.

## OAuth Data Flow

An application must get an access token before using any API in Cytomic Orion. To do this, certain information must be exchanged with the CAS server.

## Protocol Used for the Data Exchange

OAuth uses the HTTPS protocol to exchange information flows between the application and the CAS server to get authorization for the Cytomic Orion APIs. This data exchange uses the HTTP protocol POST command. For security reasons, all commands sent and responses received travel encrypted using HTTPS.

## Access Types Supported by the CAS Server and Data Required

The OAuth protocol supports multiple types of authentication and authorization depending on the application that accesses the Cytomic Orion API. In the specific case of Cytomic Orion, the type of access allowed by the CAS server is “password”, which must be specified in the “grant\_type” parameter of the initial request from the application.

With grant\_type password, the CAS server requires this data to allow access to the Cytomic Orion API for an application:

- **User name and Password:** The identifier for the application account and the password, created in the Cytomic Orion console. See [Enable Access to the API from External Programs](#).
- **Client\_id, Client\_secret:** The client ID and password. See [Enable Access to the API from External Programs](#).

## Information Flows Generated to Authorize Access

Communication in the authentication phase between the application and the CAS server works as follows:

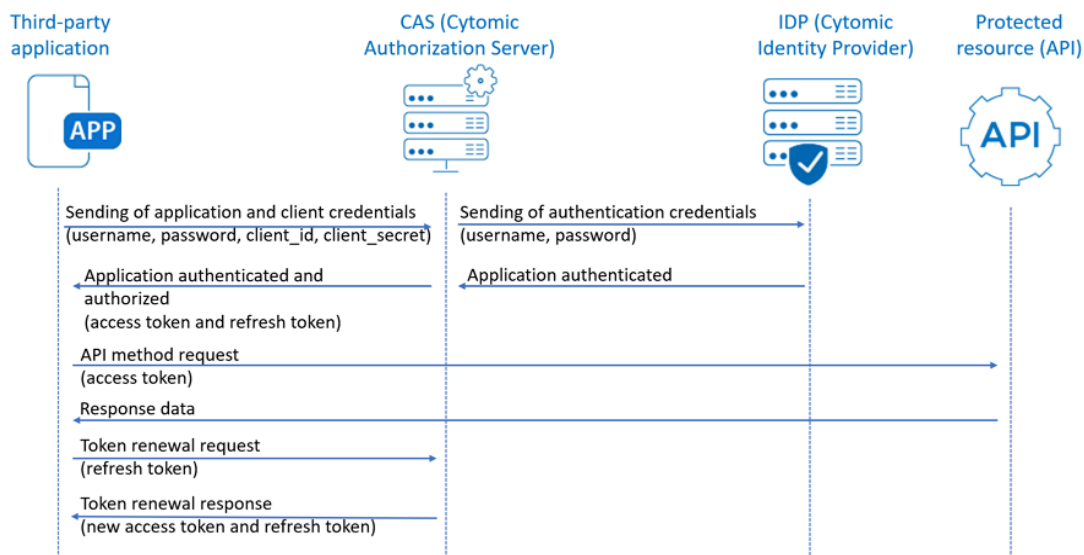


Figure 17.3: OAuth communication between an application and the CAS server

The diagram illustrates a complete OAuth data exchange:

- The application sends its credentials and the client’s credentials to the CAS server. The CAS server validates the application credentials on the IdP server. If validation is successful, it checks the client’s credentials to generate and issue both an access token and a refresh token.
- The application uses the access token to access the Cytomic Orion API and retrieve the required data.
- After the access token expires, the CAS server rejects it. The application sends the refresh token to get a new access token and a new refresh token.

## Authentication, Authorization, and Access Token Generation

### The Application Requests the Authorization Token

The application sends an HTTPS POST command to the CAS server (<https://auth.pandasecurity.com>) with these parameters:

```
POST /oauth/token HTTP/1.1
Host: auth.pandasecurity.com
Content-Type: application/x-www-form-urlencoded; charset=utf-8

grant_type=password
&client_id={CLIENT_ID}
&client_secret={CLIENT_SECRET}
&username={USER_NAME}
&password={USER_PASSWORD}
&scope={SCOPE}
```

Alternatively, you can use an Authorization header to specify the `client_id` and `client_secret` encoded as Base64:

```
POST /oauth/token HTTP/1.1
Host: auth.pandasecurity.com
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Authorization: Basic client_id:client_secret.

grant_type=password
&username={USER_NAME}
&password={USER_PASSWORD}
&scope={SCOPE}
```

The meaning of the parameters is this:

Parameter	Description
<b>grant_type</b>	Required. It sets the value to "password". It indicates that the application will directly provide the credentials of the application account to which the protected resource belongs.
<b>client_id</b>	Required. It is the ID of the Cytomic Orion client to which the application belongs.
<b>client_secret</b>	Required. It is the password of the Cytomic Orion client to which the application belongs.
<b>username</b>	Required. The name of the account of the application created in the Cytomic Orion console. See <a href="#">Enable Access to the API from External Programs</a> .

Parameter	Description
<b>password</b>	Required. The password of the account of the application created in the Cytomic Orion console. See <a href="#">Enable Access to the API from External Programs</a> .
<b>scope</b>	The scope of access. It sets the value to "orion.api".

Table 17.1: Parameters required by the CAS server to get the access token

### Successful Response from the CAS Server

The response is a JSON object with the access token and other data:

```
HTTP/1.1 200
{
  "access_token": "{ACCESS_TOKEN}",
  "refresh_token": "{REFRESH_TOKEN}",
  "expires_in": {EXPIRATION_TIME},
  "token_type": {TOKEN_TYPE}
}
```

The meaning of the fields is this:

Field	Description
<b>access_token</b>	Access token. It consists of a character string encoded in Base64.
<b>refresh_token</b>	Refresh token. It consists of a character string encoded in Base64.
<b>expiration_time</b>	The time in seconds that the access token is valid for.
<b>token_type</b>	By default, "Bearer". It indicates that the token is a self-contained token that contains all the resources required to authorize access. The CAS server issues signed JWT (JSON Web Token) access tokens.

Table 17.2: Response from the CAS server with the access token and the refresh token

### Unsuccessful Response from the CAS Server

The server could not generate a valid token with the information supplied:

```
HTTP/1.1 400 Bad request
{
  "error": "{ERROR_CODE}",
  "error_description": "{ERROR_DESC}"
}
```

```
"error_uri": "{ERROR_URI}"
}
```

The meaning of the fields is this:

Field	Description
<b>error</b>	Error code: see table <a href="#">Return Codes</a> .
<b>error_description</b>	Brief description of the error. The content of this field is not prepared to be shown directly to the application user. Messages should instead be adapted to the application.
<b>error_uri</b>	Optional.

Table 17.3: Incorrect response from the CAS server

## Refresh an Expired Access Token

Because the scope of access for an application can change over time, the access token that an application uses to access the Cytomic Orion API expires in 20 minutes, after which time the Cytomic Orion API rejects it and prevent access to the resource. To prevent the sending of the parameters specified in section [Authentication, Authorization, and Access Token Generation](#), whenever an access token expires, the application sends the refresh token to the CAS server. As such, the refresh token acts as a reference to the original conditions that led to the authorization of the application on the CAS server. If these conditions have not changed, the CAS server reissues an access token to the application. The refresh token has a longer lifespan than the access token.

### Send the Refresh Token

The application sends an HTTPS POST command to the CAS server ([auth.pandasecurity.com](https://auth.pandasecurity.com)) with these parameters:

```
POST /oauth/token HTTP/1.1
Host: auth.pandasecurity.com
Content-Type: application/x-www-form-urlencoded; charset=utf-8

grant_type = refresh_token
&refresh_token = {REFRESH_TOKEN}
&client_id = {CLIENT_ID}
&client_secret = {CLIENT_SECRET}
&scope = {ORIGINAL_SCOPE}
```

The meaning of the parameters is this:

Parameter	Description
<b>grant_type</b>	Required. It sets the value to <code>refresh_token</code> to indicate that the application sends a refresh token in exchange for the CAS server issuing a new access token.
<b>refresh_token</b>	The refresh token required for the CAS server to generate a new access token.
<b>client_id</b>	Required. This is the ID of the Cytomic Orion client.
<b>client_secret</b>	Required. This is the password of the Cytomic Orion client.
<b>scope</b>	Optional. If you do not include it, the CAS server returns an access token with the same scope as the original request. If you include it, it must contain the same scope as the original request.

Table 17.4: Parameters required by the CAS server to generate a new access token

### Successful Response from the CAS Server

The CAS server response to the application is the same as the one generated in the original request for the access token. The CAS server can include a new refresh token which will be used the next time the access token is renewed. If the CAS server does not include a new refresh token, it is assumed that the previous token is still valid.

### Unsuccessful Response from the CAS Server

The server could not generate a valid token with the information supplied:

```
HTTP/1.1 400 Bad request
{
  "error": "invalid_request"
}
```

### Error Codes

Code	Description
<b>200</b>	The operation completed successfully.
<b>400</b>	Error.

Table 17.5: Return codes



## Error Messages

Error code	Description
<b>unrecognized_client_id</b>	The client ID is incorrect or does not exist. Contact the Cytomic support department.
<b>unrecognized_client_secret</b>	The client password is incorrect or does not correspond to the <code>client_id</code> sent. Contact the Cytomic support department.
<b>unauthorized_client</b>	The client is authenticated but is not authorized to make the request.
<b>invalid_client</b>	Any other error related to the validation of clients' credentials. Contact the Cytomic support department.
<b>unsupported_grant_type</b>	The <code>grant_type</code> sent is not supported. Use "password".
<b>invalid_grant</b>	The access token received is invalid (it is not recognized or has expired), or the application is not authorized to access the API.
<b>invalid_scope</b>	The scope received is incorrect. This parameter must always be "orion.api".
<b>access_denied</b>	Wrong user name or password.
<b>invalid_request</b>	The request has an incompatible parameter or does not have all the required parameters.
<b>temporarily_unavailable</b>	The CAS server is currently unable to handle the request due to a temporary overloading or maintenance.
<b>server_error</b>	Internal server error.

Table 17.6: Authorization process error messages

## Example of How to Get an Access Token and a Refresh Token from the CAS Server

This example shows a call to the CAS server with the `username`, `password`, `client_id`, `client_secret`, `grant_type`, and `scope` parameters required to retrieve the access token and the refresh token needed for future calls to the Cytomic Orion API.

```

#Uses the requests library to connect to the OAuth server
import requests
from requests.auth import HTTPBasicAuth
#Sets the client_id, client_secret, username, password, and scope
client_id = 'aaf1461b7a8a593199665'
client_secret = 'YaDzUdHmlrivXYaAFhJDFiNe5x0mI4'
username = '7e0aa013282249cdebd15a08f84d'
password = 'jEshWDjjs2h6bCxrZKCy8iVbBHncCzMxxUe362CfUwz0eAKXRdlz9uOuVzFp3g'
grant_type = 'password'
token_url = 'https://auth.pandasecurity.com/oauth/token'
scope = 'orion.api'
headers = {
    'Content-Type': 'application/x-www-form-urlencoded',
}
#Configures the HTTP message body. The client_id and
#client_secret credentials are set in the message headers
body = {
    'username': username,
    'password': password,
    'scope': scope,
    'grant_type': 'password'
}
#Encodes the client_id and client_password in Base64 and launches the HTTPS
request
r = requests.post(token_url, auth=HTTPBasicAuth(client_id, client_secret),
headers=headers, data=body, verify=False)
#If there are no errors, the response is converted to a JSON object to
enable #access
if r.status_code==200:
    data = r.json()
#Loads the access and refresh tokens on the variables
token_access=data['access_token']
token_refresh=data['refresh_token']

```

## Example of How to Use an Access Token and a Refresh Token

All calls to the Cytomic Orion API must include, in the HTTP headers, the access token generated after the authentication and authorization process. However, 20 minutes after the access token is issued, it expires and you must get a new one by using the refresh token. For this reason, you must check each call to the Cytomic Orion API to make sure it does not return an invalid token error. If that is the case, request a new access token and retry the request with the new token.

```

#Example call to the indicator API
#Sets the required parameters
alert_from='1572595090000' #from 11/01/2019
alert_to='1575187090000' #until 12/01/2019

```

```

#Prepares the HTTP header with the access token to make the
call to the API
h_request = {
    'Authorization': f'Bearer {access_token}',
    'Accept': 'application/json'
}

url_alert =
f'https://api.orion.cytomic.ai/api/v1/applications/alerts/
{alert_from}/{alert_to}'
r = requests.get(url_alert, headers=h_request, verify=False)
#After authentication is successful, checks whether the
access token has expired in each call
if r.status_code==401:
    body_refresh = {
        'grant_type': 'refresh_token',
        'refresh_token': token_refresh,
        'client_id': client_id,
        'client_secret': client_secret,
    }
    #Requests a new access token and a new refresh token
    r = requests.post(token_url, headers=headers,
data=body_refresh, verify=False)
    data = r.json()
    #Updates variables with the new access and refresh
tokens
    token_access=data['access_token']
    token_refresh=data['refresh_token']

```

## Cytomic Orion API Specification



*All calls to the Cytomic Orion API must include the access token you got by following the steps in **Authentication, Authorization, and Access Token Generation** through the Authorization: **Bearer {token}** header.*

This section describes the various calls to the Cytomic Orion API, their syntax, the meaning of the parameters used and their format, as well as the results returned.

Cytomic Orion uses a REST interface to exchange information between the platform and third-party applications: The protocol for transferring messages between both terminals is HTTPS, whereas the format used to encapsulate complex data types is JSON.

### General Structure of a Call

In each call to the Cytomic Orion API, the third-party application must specify some or all of these parameters:

- **HTTPS method:** The HTTP command used in the request:
  - **GET:** The call requests information. The required parameters are passed only in the URL.
  - **POST:** The call requests information. The required parameters are passed in the HTTP message body and optionally in the URL.
- **URL:** Resource path. The path includes parameters specified in square brackets in the specification. Optional parameters are specified with the “query string” format.
- **Body:** The area of the HTTP message where the data is included. The body comes after the headers. It contains complex type parameters in POST calls.
- **HTTP return code:** Specifies whether the call was successful or failed. For a list of the codes returned by each call to the Cytomic Orion API, see [Return Codes](#).

## Data Types

Most parameters are integers or character strings. You can pass these parameters to a call either in the URL path or in `querystring` format. In the response, they appear in the message body.

All date-type parameters require the UNIX Timestamp format in milliseconds. If an analyst enters a date in seconds, Cytomic Orion converts it automatically to milliseconds.

Both in calls and responses, lists of one to "n" JSON objects are used for the most complex data types in the body of the HTTP message.

## Return Codes

Return codes are common to all calls and are specified in the `status` header of the HTTP message, in the `status: code` format:

Code	Description
200	Operation completed successfully.
400	Missing or malformed parameter.
401	Authentication failed.
403	Authorization failed.

Table 17.7: Return codes

## IOC API

This API enables you to manage the indicators of compromise (IOCs) obtained from external sources on the Cytomic Orion platform.

## Import and Search for IOCs in the Telemetry Generated by a Client's Computers

Loads one or more IOCs of the same type onto the platform. You can configure those IOCs for two types of searches:

- **Retrospective searches (optional):** These searches examine, only once, the flow of events generated by the client's computers over the last year since an IOC is imported. A single indicator is generated in the console for each computer/IOC pair found.
- **Real-time searches:** These searches examine, in real time, the information generated by processes running on the client's computers. A single indicator is generated in the console for each computer/IOC pair every hour. The search ends when the time indicated in the TTL field expires.

### Request

<b>Command</b>	POST
<b>URL</b>	/api/v1/applications/iocs/{iocType}
<b>Required parameters in the URL</b>	<ul style="list-style-type: none"> <li>• <b>iocType:</b> Specifies the type of IOCs you want to import. All the IOCs imported in the same call must be of the same type. <ul style="list-style-type: none"> <li>• <b>Hash:</b> The JSON object with the description of the IOC you want to import must contain the MD5 value of the file that poses a threat.</li> <li>• <b>Url:</b> The JSON object with the description of the IOC you want to import must contain the URL accessed by the threat. You must include the protocol in the URL. For example: <a href="https://www.google.com/test">https://www.google.com/test</a>.</li> <li>• <b>IP:</b> The JSON object with the description of the IOC you want to import must contain the source or target IP address of the communication established by the threat.</li> <li>• <b>Domain:</b> The JSON object with the description of the IOC you want to import must contain the source or target domain of the communication established by the threat.</li> </ul> </li> </ul>
<b>Optional querystring parameters in the URL</b>	<ul style="list-style-type: none"> <li>• <b>retrospective:</b> Examines, only once, the flow of events stored by Cytomic and generated by the SOC computers up until the present date.</li> </ul>
<b>Required parameters in the HTTP message body</b>	<p>List of JSON objects with descriptions of the IOCs. You can include only one of these parameters in the JSON object. All of the IOCs must be of the same type.</p> <p>Possible fields in the JSON object:</p> <ul style="list-style-type: none"> <li>• <b>hash:</b> MD5 value of the file that contains the threat.</li> <li>• <b>url:</b> URL requested by the threat.</li> </ul>

	<ul style="list-style-type: none"> <li>• <b>ip</b>: Source or target IP address of the communication established by the threat.</li> <li>• <b>domain</b>: Source or target domain of the communication established by the threat.</li> <li>• <b>additionalData, source, policy, description</b>: Description fields of the IOC. Not used by the platform.</li> <li>• <b>daysToExpiration</b>: Number of days the IOCs remain on the platform, after which they are deleted along with any associated searches.</li> </ul>
<b>Headers</b>	<ul style="list-style-type: none"> <li>• <b>Accept</b>: application/json</li> <li>• <b>Content-Type</b>: application/json-patch+json</li> </ul>

Table 17.8: Format of the call to import IOCs

**Response**

JSON object field	Description
<b>success</b>	"true"
<b>message</b>	"n {iocType} added": Indicates the number of IOCs successfully loaded onto the platform and their type.
<b>error</b>	"null"
<b>PandaAlertId</b>	Internal identifier assigned to the IOC.

Table 17.9: Response JSON object when IOCs are successfully loaded

**Delete IOCs Imported onto the Platform**

Deletes IOCs previously imported onto the platform, interrupting any retrospective or real-time searches that might be in progress.

**Request**

<b>Command</b>	POST
<b>URL</b>	/api/v1/applications/iocs/{iocType}/eraser/
<b>Required parameters in the URL</b>	<ul style="list-style-type: none"> <li>• <b>iocType</b>: Indicates the type of IOCs you want to delete. All IOCs deleted in the same call must be of the same type.</li> <li>• <b>Hash</b>: The JSON object with the description of the IOC you want to delete must contain a file MD5 value.</li> </ul>

	<ul style="list-style-type: none"> <li>• <b>Url:</b> The JSON object with the description of the IOC you want to delete must contain a URL.</li> <li>• <b>IP:</b> The JSON object with the description of the IOC you want to delete must contain a communication source or target IP address.</li> <li>• <b>Domain:</b> The JSON object with the description of the IOC you want to delete must contain a communication source or target domain.</li> </ul>
<b>Required parameters in the HTTP message body</b>	<p>List of JSON objects with descriptions of the IOCs you want to delete. You can include only one of these parameters in the JSON object. All of the IOCs must be of the same type. Possible fields in the JSON object:</p> <ul style="list-style-type: none"> <li>• <b>hash:</b> A file MD5 value.</li> <li>• <b>url:</b> URL.</li> <li>• <b>ip:</b> A communication source or target IP address.</li> <li>• <b>domain:</b> A communication source or target domain.</li> <li>• <b>additionalData, source, policy, description:</b> Description fields of the IOC. Not used by the platform.</li> </ul>
<b>Headers</b>	<ul style="list-style-type: none"> <li>• <b>Accept:</b> application/json</li> <li>• <b>Content-Type:</b> application/json-patch+json</li> </ul>

Table 17.10: Format of the call to delete IOCs

## Response

JSON object field	Description
<b>success</b>	"true"
<b>message</b>	"n {iocType} deleted": Indicates the number of IOCs successfully deleted from the platform and their type.
<b>error</b>	"null"
<b>PandaAlertId</b>	Internal identifier assigned to the IOC.

Table 17.11: Response JSON object when IOCs are successfully deleted

## List IOCs Loaded onto the Platform by Attributes

Shows the list of IOCs loaded onto the platform according to their attributes and when they were imported.

**Request**

<b>Command</b>	POST
<b>URL</b>	/api/v1/applications/iocs/{iocType}/getter/
<b>Required parameters in the URL</b>	<ul style="list-style-type: none"> <li>• <b>iocType</b>: Indicates the type of IOCs you want to list.</li> <li>• <b>Hash</b>: The JSON object with the description of the IOC you want to list must contain a file MD5 value.</li> <li>• <b>Url</b>: The JSON object with the description of the IOC you want to list must contain a URL.</li> <li>• <b>IP</b>: The JSON object with the description of the IOC you want to list must contain a communication source or target IP address.</li> <li>• <b>Domain</b>: The JSON object with the description of the IOC you want to list must contain a communication source or target IP domain.</li> </ul>
<b>Required parameters in the HTTP message body</b>	<p>List of JSON objects with descriptions of the IOCs you want to list. You can include only one of these parameters in the JSON object. All of the IOCs must be of the same type (specified in the iocType field). Possible fields in the JSON object:</p> <ul style="list-style-type: none"> <li>• <b>hash</b>: A file MD5 value.</li> <li>• <b>url</b>: URL.</li> <li>• <b>ip</b>: A communication source or target IP address.</li> <li>• <b>domain</b>: A communication source or target domain.</li> </ul>
<b>Headers</b>	<ul style="list-style-type: none"> <li>• <b>Accept</b>: application/json</li> <li>• <b>Content-Type</b>: application/json-patch+json</li> </ul>

Table 17.12: Format of the call to list IOCs by features

**Response**

JSON object field	Description
<b>iocType</b>	<p>Indicates the type of the IOCs in the list.</p> <ul style="list-style-type: none"> <li>• <b>Hash</b>: The JSON object with the description of the listed IOC contains a file MD5 value.</li> <li>• <b>Url</b>: The JSON object with the description of the listed IOC contains a URL.</li> <li>• <b>IP</b>: The JSON object with the description of the listed IOC contains a communication source or target IP address.</li> <li>• <b>Domain</b>: The JSON object with the description of the listed IOC contains a communication source or target domain.</li> </ul>



JSON object field	Description
KeyValueAsString	IOC value.
locJson	<ul style="list-style-type: none"> <li>• <b>hash</b>: A file MD5 value.</li> <li>• <b>url</b>: URL.</li> <li>• <b>ip</b>: A communication source or target IP address.</li> <li>• <b>domain</b>: A communication source or target domain.</li> <li>• <b>DaysToExpiration</b>: Number of days the IOC remains on the platform.</li> <li>• <b>additionalData, source, policy, description</b>: Description fields of the IOC. Not used by the platform.</li> </ul>
DeploymentDateUTC	Date the IOC was loaded onto the platform.
ExpirationDateUTC	Date the IOC will be deleted from the platform.
LastRetroScanUTC	Date on which a retrospective search for the IOC was last run.
PandaAlertId	Internal identifier assigned to the IOC.

Table 17.13: Response JSON object to a request to list IOCs

## List IOCs by Date Loaded onto the Platform

Shows the list of IOCs loaded onto the platform by date of publication.

### Request

Command	GET
URL	/api/v1/applications/iocs/{iocType}
Required parameters in the URL	<ul style="list-style-type: none"> <li>• <b>iocType</b>: Indicates the type of IOCs you want to list. <ul style="list-style-type: none"> <li>• <b>Hash</b>: Lists IOCs that specify an MD5.value.</li> <li>• <b>Url</b>: Lists IOCs that specify a URL.</li> <li>• <b>IP</b>: Lists IOCs that specify a communication source or target IP address.</li> <li>• <b>Domain</b>: Lists IOCs that specify a communication source or target IP domain.</li> </ul> </li> </ul>
Required parameters in the HTTP message body	<ul style="list-style-type: none"> <li>• <b>From</b>:: Unix timestamp in milliseconds with the start date of the interval for which you want to list IOCs.</li> </ul>

	<ul style="list-style-type: none"> <li>• <b>to</b>: Unix timestamp in milliseconds with the end date of the interval for which you want to list IOCs.</li> <li>• <b>includeDeleted</b>: Filters the list of IOCs based on whether they belong to a deletion rule.             <ul style="list-style-type: none"> <li>• <b>True</b>: The IOC belongs to a deletion rule.</li> <li>• <b>False</b>: The IOC does not belong to a deletion rule</li> </ul> </li> </ul>
<b>Headers</b>	<b>Accept</b> : application/json

Table 17.14: Format of the call to list IOCs by date loaded onto the platform

**Response**

JSON object field	Description
<b>locType</b>	<p>Indicates the type of the IOCs in the list.</p> <ul style="list-style-type: none"> <li>• <b>Hash</b>: The JSON object with the description of the listed IOC contains a file MD5 value.</li> <li>• <b>Url</b>: The JSON object with the description of the listed IOC contains a URL.</li> <li>• <b>IP</b>: The JSON object with the description of the listed IOC contains a communication source or target IP address.</li> <li>• <b>Domain</b>: The JSON object with the description of the listed IOC contains a communication source or target domain.</li> </ul>
<b>KeyValueAsString</b>	IOC value.
<b>locJson</b>	<ul style="list-style-type: none"> <li>• <b>hash</b>: A file MD5 value.</li> <li>• <b>url</b>: URL.</li> <li>• <b>ip</b>: A communication source or target IP address.</li> <li>• <b>domain</b>: A communication source or target domain.</li> <li>• <b>DaysToExpiration</b>: Number of days the IOC remains on the platform.</li> <li>• <b>additionalData, source, policy, description</b>: Description fields of the IOC. Not used by the platform.</li> </ul>
<b>DeploymentDateUTC</b>	Date the IOC was loaded onto the platform.
<b>ExpirationDateUTC</b>	Date the IOC will be deleted from the platform.

JSON object field	Description
LastRetroScanUTC	Date on which a retrospective search for the IOC was last run.
PandaAlertId	Internal identifier assigned to the IOC.

Table 17.15: Response JSON object to the call to list IOCs by date loaded onto the platform

## Search for IOCs Retrospectively

Searches for patterns in all events generated so far on the SOC clients' computers. It returns a list of JSON objects with the IOCs found. The call to this method has a maximum execution time of 90 seconds. It shows all results at the end of the search. If, after the maximum execution time has passed, Cytomic Orion has not been able to retrieve all available threats, the connection terminates without returning any results.

### Request

Command	POST
URL	/api/v1/applications/iocs/{iocType}/retrospectivesearcher
Required parameters in the URL	<ul style="list-style-type: none"> <li>• <b>iocType</b>: Indicates the type of IOCs you want to search for. All IOCs in the same call must be of the same type.</li> <li>• <b>FileHashloc</b>: The JSON object with the description of the IOC you want to search for must contain the MD5 value of the file that poses a threat.</li> <li>• <b>Url</b>: The JSON object with the description of the IOC you want to search for must contain a URL requested by the threat.</li> <li>• <b>IP</b>: The JSON object with the description of the IOC you want to search for must contain the source or target IP address of the communication established by the threat.</li> <li>• <b>Domain</b>: The JSON object with the description of the IOC you want to search for must contain the source or target domain of the communication established by the threat.</li> </ul>
Required parameters in the HTTP message body	<p>List of JSON objects with descriptions of the IOCs. You can include only one of these parameters in the JSON object. All of the IOCs must be of the same type.</p> <p>Possible fields in the JSON object:</p> <ul style="list-style-type: none"> <li>• <b>hash</b>: MD5 value of the file that contains the threat.</li> <li>• <b>url</b>: URL requested by the threat.</li> <li>• <b>ip</b>: Source or target IP address of the communication established by the threat.</li> <li>• <b>domain</b>: Source or target domain of the communication established by the threat.</li> </ul>

	<ul style="list-style-type: none"> <li>• <b>additionalData, source, policy, description:</b> Description fields of the IOC. Not used by the platform.</li> </ul>
<b>Headers</b>	<ul style="list-style-type: none"> <li>• <b>Accept:</b> application/json</li> <li>• <b>Content-Type:</b> application/json-patch+json</li> </ul>

Table 17.16: Format of the call to run a retrospective search

### Response

List of JSON objects with descriptions of the attributes of the IOCs found.

JSON object field	Description
<b>MUID</b>	Computer ID in Cytomic Orion.
<b>clientid</b>	Client ID.
<b>firstSeen</b>	Date the IOC was first seen on the client’s computer.
<b>lastSeen</b>	Date the IOC was last seen on the client’s computer.
<b>ioc</b>	Description of the IOC found. <ul style="list-style-type: none"> <li>• <b>iockey:</b> IOC value.</li> <li>• <b>type:</b> IOC type (FileHash, Url, IP, Domain).</li> <li>• <b>source, policy, description:</b> Description fields entered when you imported the IOC. .</li> </ul>
<b>PandaAlertId</b>	Internal identifier assigned to the IOC.

Table 17.17: Response JSON object to a request to run a retrospective search

### List of IOCs in the Cytomic Orion Console

To view a list of loaded IOCs in the console, select **Settings** in the top menu. In the side menu, select **IOCs**. A list appears that shows information equivalent to that provided in the response to API calls for listing the IOCs loaded onto the platform. See [List IOCs Loaded onto the Platform by Attributes](#) or [List IOCs by Date Loaded onto the Platform](#).

Field	Description
<b>IOC type</b>	Type of the data that appears in the <b>IOC value</b> field. It matches the content of the API <b>iocType</b> parameter.

Field	Description
IOC value	Value used in IOC searches. It matches the content of the API <b>KeyValueAsString</b> parameter.
Import date	Date the IOC was created. It matches the content of the API <b>DeploymentDateUTC</b> parameter.
Expiration date	Date the IOC will be deleted from the platform. It matches the content of the API <b>ExpirationDateUTC</b> parameter.
Additional data	It matches the content of the API <b>additionalData</b> parameter.
Source	It matches the content of the API <b>source</b> parameter.
Policy	It matches the content of the API <b>policy</b> parameter.
Description	It matches the content of the API <b>description</b> parameter.

Table 17.18: Fields in the IOCs list

## Examples of IOC API Calls

This example loads multiple IOCs that identify source and target traffic related to C&C (Command & Control) networks, checks whether they are loaded, runs a retrospective search, and deletes them.

When you load the list of IOCs, Cytomic Orion retrospectively examines, only once, the telemetry stored over the last year and generates indicators if it finds threats that match the loaded IOCs. Additionally, it examines, in real time, the events occurred on computers until the IOC expiration date (10 days).

```
#IOC type
iocType='IPIoc'
#IOC data
ioc_data=[{'ip':'192.168.0.1'},{'ip':'192.168.0.2'},{'ip':'192.168.0.3'}]
#Headers for the API call including the access token
h_request_ioc = {
    'Authorization': f'Bearer {access_token}',
    'Accept': 'application/json',
    'Content-Type': 'application/json-patch+json'
}
#Aim: To load three IOCs of type IP (IPIoc) onto the server
#Enable retrospective search
retrospective=True
#Call URL
url_ioc_add = f' https://api.orion.cytomic.ai/api/v1/applications/iocs/'
```

```

{iocType}?retrospective={retrospective}'
#Returns a JSON object with the number of successfully loaded IOCs
r = requests.post(url_ioc_add, headers=h_request_ioc, json=ioc_data,
verify=False)
ioc_add=r.json()
#Aim: To check the IOCs loaded onto the platform
#Call URL
url_          ioc_          list          =
f'          https://api.orion.cytomic.ai/api/v1/applications/iocs/
{iocType}/getter/'
r = requests.post(url_ioc_list, headers=h_request_ioc,
json=ioc_data, verify=False)
#Returns a JSON object with a description of the loaded IOCs
of the specified type and the
#load date
iocs_list=r.json()
#Aim: To start a retrospective search for a list of IOCs
#Call URL
url_          ioc_          search          =
f'          https://api.orion.cytomic.ai/api/v1/applications/iocs/
{iocType}/retrospectivesearcher/'
r = requests.post(url_ioc_search, headers=h_request_ioc,
json=ioc_data, verify=False)
#Returns a list of JSON objects with the IOCs found on the
client's network
iocs_found=r.json()
#Aim: To delete previously loaded IOCs
#Call URL
url_          ioc_          del          =
f'          https://api.orion.cytomic.ai/api/v1/applications/iocs/
{iocType}/eraser/'
#Returns a JSON object with the number of successfully
deleted IOCs
r = requests.post(url_ioc_del, headers=h_request_ioc,
json=ioc_data, verify=False)
ioc_del=r.json()
    
```

### Knowledge API

This API gets data about the computers that belong to the client's IT infrastructure and the files they store.

#### Get the Details of a File

Gets the classification of a file assigned by Cytomic from its MD5 hash and other information.

**Request**

<b>Command</b>	GET
<b>URL</b>	/api/v1/applications/forensics/md5/ {md5}/info
<b>Required parameters in the URL</b>	<b>md5:</b> File hash.

<b>Headers</b>	<b>Accept:</b> application/json
----------------	---------------------------------

Table 17.19: Format of the call to get a file details

## Response

JSON object with a description of the file attributes.

JSON object field	Description
<b>filename</b>	Name of the file.
<b>filesize</b>	Size of the file in bytes.
<b>lastSeen</b>	Date the file was last logged in the Cytomic global knowledge.
<b>firstSeen</b>	Date the file was first logged in the Cytomic global knowledge.
<b>classification</b>	Value indicated in the <code>classificationName</code> field.
<b>classificationName</b>	Classification of the file generated by Cytomic EDR: <ul style="list-style-type: none"> <li>• <b>-1:</b> Unknown</li> <li>• <b>0:</b> Unknown</li> <li>• <b>1:</b> Goodware</li> <li>• <b>2:</b> Malware</li> <li>• <b>3:</b> Suspicious</li> <li>• <b>4:</b> Compromised</li> <li>• <b>5:</b> GWNotConfirmed</li> <li>• <b>6:</b> PUP</li> <li>• <b>7:</b> GwUnwanted</li> <li>• <b>8:</b> GwRanked</li> </ul>

Table 17.20: Fields of the JSON object indicating the file attributes

## Get the Details of Multiple Files

Gets the classification of a list of files assigned by Cytomic from their MD5 hashes and other information.

### Request

<b>Command</b>	POST
<b>URL</b>	/api/v1/forensics/md5/batch/sample
<b>Headers</b>	<ul style="list-style-type: none"> <li>• <b>Accept:</b> application/json</li> <li>• <b>Content-Type:</b> application/json-patch+json</li> </ul>

Table 17.21: Format of the call to get information about a list of files

### Response

List of JSON objects with descriptions of the attributes of the files

JSON object field	Description
<b>filename</b>	Name of the file.
<b>filesize</b>	Size of the file in bytes.
<b>lastSeen</b>	Date the file was last logged in the Cytomic global knowledge.
<b>firstSeen</b>	Date the file was first logged in the Cytomic global knowledge.
<b>classification</b>	Value indicated in the <code>classificationName</code> field.
<b>classificationName</b>	Classification of the file generated by Cytomic EDR: <ul style="list-style-type: none"> <li>• <b>-1:</b> Unknown</li> <li>• <b>0:</b> Unknown</li> <li>• <b>1:</b> Goodware</li> <li>• <b>2:</b> Malware</li> <li>• <b>3:</b> Suspicious</li> <li>• <b>4:</b> Compromised</li> <li>• <b>5:</b> GWNNotConfirmed</li> <li>• <b>6:</b> PUP</li> <li>• <b>7:</b> GwUnwanted</li> <li>• <b>8:</b> GwRanked</li> </ul>

Table 17.22: Fields of the JSON object indicating the file attributes



## Get the Computers Where a File Was Detected

Gets a list of MUIDs of the client's computers where a certain MD5 hash was detected.

### Request

<b>Command</b>	GET
<b>URL</b>	/api/v1/applications/forensics/md5/{md5}/muids
<b>Required parameters in the URL</b>	<b>MD5:</b> File hash.
<b>Headers</b>	<b>Accept:</b> application/json

Table 17.23: Format of the call to get the computers where a file was detected

### Response

List of JSON objects with information about the computers where a file was detected.

JSON object field	Description
<b>MUID</b>	Unique ID of the computer.
<b>clientId</b>	Unique ID of the client the computer belongs to.
<b>lastSeen</b>	Date the file was last seen on a computer on the client's network.
<b>firstSeen</b>	Date the file was first seen on a computer on the client's network.
<b>lastPath</b>	Path of the file on the computer where it was last seen.

Table 17.24: Fields of the JSON object with the description of the computers where a file was detected

## Get the Details of Multiple Computers

Gets information about one or more computers in the client's IT infrastructure.

### Request

<b>Command</b>	POST
<b>URL</b>	/api/v1/applications/forensics/muid/info
<b>Required parameters in the</b>	JSON object with the list of MUIDs of the

<b>HTTP message body</b>	computers.
<b>Headers</b>	<ul style="list-style-type: none"> <li>• <b>Accept:</b> application/json</li> <li>• <b>Content-Type:</b> application/json-patch+json</li> </ul>

Table 17.25: Format of the call to get information about computers

### Response

List of JSON objects with details of the computers.

Field	Description
<b>MUID</b>	Unique ID of the computer.
<b>machineName</b>	Name of the computer.
<b>lastSeenUtc</b>	UTC-0 date on which the computer last communicated with the Cytomic cloud.
<b>creationDate</b>	Date on which the Cytomic EDR protection was installed on the computer.
<b>clientId</b>	Unique ID of the client the computer belongs to.
<b>clientName</b>	Name of the client.
<b>clientCreationDate</b>	Date on which the client integrated their first computer onto the Cytomic Orion platform.

Table 17.26: Format of the JSON object that describes a computer

### Get a Computer MUID

Gets the MUID of a computer in the client’s IT infrastructure from the computer name.

#### Request

<b>Command</b>	GET
<b>URL</b>	/api/v1/applications/clients/{ClientId}/machine-name/{MachineName}/muid
<b>Required parameters in the URL</b>	<ul style="list-style-type: none"> <li>• <b>ClientId:</b> Unique ID of the client.</li> <li>• <b>MachineName:</b> Name of the computer whose MUID you</li> </ul>

	want to get. It allows character substrings.
<b>Headers</b>	<b>Accept:</b> application/json

Table 17.27: Format of the call to get a computer MUID

### Response

List of JSON objects with the names and other additional information about the computers that match the substring specified in the **MachineName** field of the request.

Field	Description
<b>MUID</b>	Unique ID of the computer.
<b>machineName</b>	Name: Full name of the computer.
<b>lastSeenUtc</b>	UTC-0 date on which the computer last communicated with the Cytomic cloud.
<b>creationDate</b>	Date on which the Cytomic EDR protection was installed on the computer.

Table 17.28: Format of the JSON object that contains a computer MUID

## Get the Details of a Computer

Gets the full details of a computer in the client's IT infrastructure.

### Request

<b>Command</b>	GET
<b>URL</b>	/api/v1/remediations/muids/{muid}/detail
<b>Required parameters in the URL</b>	<b>MUID:</b> Unique identifier of the computer.
<b>Headers</b>	<b>Accept:</b> application/json

Table 17.29: Format of the call to get a computer details

### Response

JSON object with a computer details. For a full description of the fields, see [Computer Details](#) on page 112.

## Get the Date When One or More Computers Were Last Seen

Gets the date when a client's computers were first seen and last seen.

- If you do not send the optional parameter **machineName**, you get data for all of the client's computers.
- If you send the optional parameter **machineName**, you get data for the computer you specified.

### Request

<b>Command</b>	GET
<b>URL</b>	/api/v1/clients/{pandaClientId}/machines
<b>Required parameters in the URL</b>	<b>pandaClientId</b> : Client ID.
<b>Optional parameters in the URL</b>	<b>machineName</b> : Name of the computer.
<b>Headers</b>	<b>Accept</b> : application/json

Table 17.30: Format of the call to get dates for one or more computers

### Response

List of JSON objects with data for the computers.

JSON object field	Description
<b>MUID</b>	ID of the computer.
<b>Machine Name</b>	Name of the computer.
<b>LastSeenUtc</b>	Date the computer last connected to the Cytomic cloud.
<b>CreationDate</b>	Date the file was first logged in the Cytomic cloud.

Table 17.31: Fields in the JSON object with the computer attributes

## Example of How to Get Extended Information about Computers and Files

This example gets a list of all the computers where a file was detected, and shows information about the computers and the file.

```
#Headers for the API call including the access token
h_request_know = {
    'Authorization': f'Bearer {access_token}',
    'Accept': 'application/json'
}

#Aim: To get information about an MD5 hash
#File MD5 hash
md5='6cff0673ce2002a2fe2218642605187a'

#Call URL
url_md5_info = f'https://api.orion.cytomic.ai/api/v1/applications/forensics/md5/{md5}/info'
r = requests.get(url_md5_info, headers=h_request_know, verify=False)
#Returns a JSON object with information about the file
file=r.json()

#Aim: To get a list of computers where the MD5 hash was detected
#Call URL
```

```

url_      computers      =      f'
https://api.orion.cytomic.ai/api/v1/applications/forensics/md5/{md5}/muids'

r = requests.get(url_computers, headers=h_request_know,
verify=False)

#Returns a list of JSON objects with information about each
computer

computers=r.json()

#Aim: To get extended information about each computer where
the MD5 hash was detected

#For each computer, the MUID is extracted from the JSON
object and a call is made to the #extended information API.

for computer in computers:

    #Computer MUID
    muid=computer['muid']

    #Call URL
    url_      computers_      info      =      f'
https://api.orion.cytomic.ai/api/v1/applications/forensics/m
uid/{muid}/info'

    r = requests.get(url_computers_info, headers=h_
request_know, verify=False)

    #Returns a JSON object with information about the
computer

    computer_info=r.json()

```

## Indicator API

### Get Generated Indicators



*This API method retrieves the first 30,000 indicators generated in the interval you set. To retrieve all the indicators, run multiple calls consecutively with different shorter intervals. The indicator retrieval interval must not exceed one month. Otherwise, the call returns an error.*

This API gets a list of JSON objects with the indicators generated in Cytomic Orion in the specified period. You can also filter the results by type of indicator.

#### Request

<b>Command</b>	GET
<b>URL</b>	/api/v1/applications/alerts/{from}/{to}
<b>Optional querystring parameters in the URL</b>	<ul style="list-style-type: none"> <li>• <b>statuses:</b> Filters the indicators retrieved by whether they have been assigned to an investigation.</li> <li>• <b>Pending:</b> The indicator has not been assigned to an investigation yet.</li> <li>• <b>InProgress:</b> The indicator has been assigned to an investigation</li> </ul>

	<p>that is still open.</p> <ul style="list-style-type: none"> <li>• <b>Closed:</b> The indicator was assigned to an investigation which is now closed.</li> <li>• <b>MUID:</b> Filters the indicators retrieved by the computer MUID.</li> <li>• <b>clientid:</b> Filters the indicators retrieved by the client ID.</li> <li>• <b>huntingrule:</b> Filters the indicators retrieved by the name of the associated hunting rule.</li> <li>• <b>Caseid:</b> Filters the indicators retrieved by the investigation ID.</li> <li>• <b>machineName:</b> Filters the indicators retrieved by the computer name.</li> <li>• <b>from:</b> Unix timestamp (in milliseconds) with the start date of the interval for which you want to retrieve indicators.</li> <li>• <b>to:</b> Unix timestamp (in milliseconds) with the end date of the interval for which you want to retrieve indicators.</li> <li>• <b>showExcluded:</b> Filters the indicators retrieved by whether they belong to a deletion rule.             <ul style="list-style-type: none"> <li>• <b>True:</b> The indicator belongs to a deletion rule and is in the bin.</li> <li>• <b>False:</b> The indicator does not belong to a deletion rule</li> </ul> </li> <li>• <b>showDetails:</b> Retrieves (or not) the indicator details:             <ul style="list-style-type: none"> <li>• <b>true:</b> The indicator details are sent in the Details field.</li> <li>• <b>false:</b> The Details field is empty (null).</li> </ul> </li> </ul>
<b>Headers</b>	<ul style="list-style-type: none"> <li>• <b>Accept:</b> application/json</li> </ul>

Table 17.32: Format of the call to get generated indicators

### Response

List of JSON objects with a description of the indicators found.

Field	Description
<b>id</b>	Indicator ID.
<b>MUID</b>	Unique identifier of the computer on which the indicator was generated.
<b>timestamp</b>	Date the indicator was generated.
<b>clientid</b>	Unique identifier of the client the computer belongs to.

Field	Description
<b>huntingRule</b>	Name of the hunting rule that generated the indicator.
<b>HuntingRuleId</b>	ID of the hunting rule that generated the indicator.
<b>status</b>	<p>Indicates whether the indicator was assigned to an investigation and the indicator status.</p> <ul style="list-style-type: none"> <li>• <b>0 (In progress)</b>: The indicator is assigned to an investigation and a Tier 2 analyst is investigating it.</li> <li>• <b>1 (Pending)</b>: The indicator has not been assigned to an investigation yet.</li> <li>• <b>2 (Closed)</b>: The indicator was assigned to an investigation which is now closed.</li> </ul>
<b>details</b>	Indicator description. Along with the indicator name, it specifies the types of suspicious events logged so that the Tier 1 team can triage the incident.
<b>alertDateTime</b>	Date the indicator was generated.
<b>lastHourEvidenceCount</b>	Number of times Cytomic Orion generated the same indicator in the last hour.
<b>severity</b>	<p>Severity of the impact of the threat:</p> <ul style="list-style-type: none"> <li>• <b>0</b>: Undefined</li> <li>• <b>1</b>: Critical</li> <li>• <b>2</b>: High</li> <li>• <b>3</b>: Medium</li> <li>• <b>4</b>: Low</li> <li>• <b>1000</b>: Unknown</li> </ul>
<b>mitre</b>	Category of the technique and tactic associated with the hunting rule, mapped to the MITRE matrix.
<b>excluded</b>	Indicates whether Cytomic Orion showed the indicator on the management console or the indicator is excluded.

Field	Description
machineName	Name of the client's computer where the indicator was detected.
caseId	Unique identifier of the investigation assigned to the indicator, if created.
caseName	Name of the investigation assigned to the indicator, if created.
directLink	URL to access the page that describes the indicator. Used in integration with third-party software.

Table 17.33: Format of the JSON object that describes an indicator

### Example of API Call to List Indicators

This example provides a list of all the indicators generated in Cytomic Orion from 11/01/2019 to 12/01/2019, which have not been assigned to an investigation yet (status Pending).

```
#Headers for the API call including the access token.
h_request_alert = {
    'Authorization': f'Bearer {access_token}',
    'Accept': 'application/json'}

#start date, end date, and filter criteria
alert_from='1572595090000'
alert_to='1575187090000'
state='Pending'}

#Aim: To get a list of all indicators generated between two dates that have
not been assigned to an investigation yet
#call URL
url_alert = f' https://api.orion.cytomic.ai/api/v1/applications/alerts/
{alert_from}/{alert_to}?statuses={state}'
r = requests.get(url_alert, headers=h_request_alert, verify=False)
#Returns a list of JSON objects with information about each indicator
alerts=r.json()
```

### Response API

#### Isolate Computers

Isolate computers on the network to prevent threats from spreading and/or block the exfiltration of confidential data.

#### Request

Command	POST
---------	------



<b>URL</b>	/api/v1/applications/remediations/muids/isolate
<b>Required parameters in the HTTP message body</b>	<p>JSON object with the list of MUIDs of the computers you want to isolate.</p> <ul style="list-style-type: none"> <li>• <b>MUIDs:</b> List of MUIDs.</li> </ul>
<b>Headers</b>	<ul style="list-style-type: none"> <li>• <b>Accept:</b> application/json</li> <li>• <b>Content-Type:</b> application/json-patch+json</li> </ul>

Table 17.34: Format of the call to isolate computers

## Response

List of JSON objects, each with the operation result.

JSON object field	Description
<b>MUID</b>	MUID of the computer affected by the operation.
<b>deviceId</b>	Deprecated field.
<b>requestAccepted</b>	True
<b>errorCode</b>	"null"
<b>errorMessage</b>	"null"

Table 17.35: Response JSON object to a request to isolate computers

## Deisolate Computers

Deisolate computers on the network after you have prevented threats from spreading and/or blocked the exfiltration of confidential data.

### Request

<b>Command</b>	POST
<b>URL</b>	/api/v1/applications/remediations/muids/deisolate
<b>Required parameters in the HTTP message body</b>	<p>JSON object with the list of MUIDs of the computers you want to deisolate.</p> <ul style="list-style-type: none"> <li>• <b>MUIDs:</b> List of MUIDs.</li> </ul>
<b>Headers</b>	<ul style="list-style-type: none"> <li>• <b>Accept:</b> application/json</li> <li>• <b>Content-Type:</b> application/json-patch+json</li> </ul>

Table 17.36: Format of the call to deisolate computers

## Response

List of JSON objects, each with the operation result.

JSON object field	Description
MUID	MUID of the affected computer.
deviceId	Deprecated field.
requestAccepted	True
errorCode	"null"
errorMessage	"null"

Table 17.37: Response JSON object to a request to isolate computers

## Restart

Restart a list of computers to update software or troubleshoot computer problems.

### Request

Command	POST
URL	/api/v1/applications/remediations/muids/reboot
Required parameters in the HTTP message body	<p>JSON object with the list of MUIDs of the computers you want to restart.</p> <ul style="list-style-type: none"> <li>• <b>MUIDs:</b> List of MUIDs.</li> </ul>
Headers	<ul style="list-style-type: none"> <li>• <b>Accept:</b> application/json</li> <li>• <b>Content-Type:</b> application/json-patch+json</li> </ul>

Table 17.38: Format of the call to restart computers

### Response

List of JSON objects, each with the operation result.

JSON object field	Description
MUID	MUID of the affected computer.
deviceId	Deprecated field.
requestAccepted	True

JSON object field	Description
<code>errorCode</code>	"null"
<code>errorMessage</code>	"null"

Table 17.39: Response JSON object to a request to restart computers

## Example of API call to Isolate, Deisolate, and Restart Computers

This example isolates, deisolates, and restarts computers with these MUIDs: "3333-4444" and "5555-6666".

```
#Headers for the API call including the access token
h_request_remediation = {
    'Authorization': f'Bearer {access_token}',
    'Accept': 'application/json',
    'Content-Type': 'application/json-patch+json'
}
#JSON object with the list of MUIDs
muids_data={'muids':['3333-4444','5555-6666']}
#Aim: To isolate a list of computers
#call URL
url_          isolate          =
f'
https://api.orion.cytomic.ai/api/v1/applications/remediations/muids/isolate'
r = requests.post(url_isolate, headers=h_request_remediation, json=muids_
data, verify=False)
#Returns a JSON object with the operation result
isolate=r.json()
#Aim: To deisolate a list of computers
#call URL
url_          deisolate          =          f'
https://api.orion.cytomic.ai/api/v1/applications/remediations/muids/deisola
te'
r = requests.post(url_deisolate, headers=h_request_remediation, json=muids_
data, verify=False)
#Returns a JSON object with the operation result
deisolate=r.json()
#Aim: To restart a list of computers
#call URL
url_          reboot          =
f'
https://api.orion.cytomic.ai/api/v1/applications/remediations/muids/reboot'
r = requests.post(url_reboot, headers=h_request_remediation, json=muids_
data, verify=False)
#Returns a JSON object with the operation result
reboot=r.json()
```

## OSQuery Access API

The OSQuery API requires you to send two different requests in a specific order:

1. Send the OSQuery statement to computers so that the Cytomic EPDR agent prepares the information stored in the database on each computer and sends it to the Cytomic platform. Two API calls are available (`/api/v1/osQuery/client` and `/api/v1/osQuery/machine`) depending on whether you want to retrieve information from all computers of one or more clients or from a specific list of computers. As a result, you get an operation ID for each client that reports information from their computers.
2. Send each operation ID to get the download URL of the file with information from each client's computers, or to get the query status.
3. Download a file for each client. This file contains all the information collected from the client's computers. You can access this resource through the URL obtained in step 2 which, for security reasons, remain active only for five minutes. After this time, go back to step 2 to get a new download URL

Because there might be computers that are turned off or unavailable, OSQuery statements can be extended indefinitely over time. That is why you must specify a TTL (Time To Live) value, after which Cytomic Orion considers the operation to be completed.

### Send a Request to Get Information from One or Multiple Computers

Run an OSQuery-compatible SQL statement on specific computers that belong to the IT infrastructure of one or more clients.

#### Request

<b>Command</b>	POST
<b>URL</b>	<code>/api/v1/osQuery/machine</code>
<b>Required parameters in the HTTP message body</b>	<p>JSON object with the OSQuery query and a list of MUIDs.</p> <ul style="list-style-type: none"> <li>• <b>query</b>: OSQuery-compatible SQL statement.</li> <li>• <b>Ttl</b>: Maximum wait time in minutes for getting the results. 0 to 24 hours.</li> <li>• <b>MUIDs</b>: List of identifiers of the computers where you want the statement to run.</li> </ul>
<b>Headers</b>	<ul style="list-style-type: none"> <li>• <b>Accept</b>: <code>application/json</code></li> <li>• <b>Content-Type</b>: <code>application/json-patch+json</code></li> </ul>

Table 17.40: Format of the call to get information from one or multiple computers

#### Response

List of JSON objects, each with the ID of the operation performed for a client.

JSON object field	Description
<b>pandaID</b>	Identifier of the client to which the computers that returned data belong.
<b>operationId</b>	Identifier of the operation performed. This is necessary to access the URL that contains the OSQuery query results. See <a href="#">Get an OSQuery Query Results</a> .
<b>MUIDs</b>	List of identifiers of the client's computers that returned data

Table 17.41: JSON object with information from one or multiple computers

## Send a Request to Get Information from All Computers of One or Multiple Clients

Run an OSQuery-compatible SQL statement on all computers belonging to the IT infrastructure of specific clients.

### Request

<b>Command</b>	POST
<b>URL</b>	/api/v1/osQuery/client
<b>Required parameters in the HTTP message body</b>	<p>JSON object with the OSQuery query and a list of client IDs.</p> <ul style="list-style-type: none"> <li>• <b>query</b>: OSQuery-compatible SQL statement.</li> <li>• <b>Ttl</b>: Maximum wait time in minutes for getting the results. 0 to 24 hours.</li> <li>• <b>pandaIDs</b>: List of identifiers of the clients where you want the statement to run.</li> </ul>
<b>Headers</b>	<ul style="list-style-type: none"> <li>• <b>Accept</b>: application/json</li> <li>• <b>Content-Type</b>: application/json-patch+json</li> </ul>

Table 17.42: Format of the call to get information from the computers of one or more clients

### Response

List of JSON objects, each with information from a client.

JSON object field	Description
<b>pandaID</b>	Identifier of the client to which the computers that returned data belong.
<b>operationId</b>	Identifier of the operation performed. This is necessary to access the URL that

JSON object field	Description
	contains the OSQuery query results. See <a href="#">Get an OSQuery Query Results</a> .
<b>MUIDs</b>	List of identifiers of the client's computers that returned data

Table 17.43: JSON object with information from all of a client's computers

## Get an OSQuery Query Results

Get the URL that points to the file that contains the data collected from the specified computers.

### Request

<b>Command</b>	POST
<b>URL</b>	/api/v1/osQuery/state
<b>Required parameters in the HTTP message body</b>	<p>List of JSON objects, each with the ID of the operation whose data you want to retrieve.</p> <ul style="list-style-type: none"> <li>• <b>pandaId</b>: Identifier of the client to which the computers that returned data belong.</li> <li>• <b>operationId</b>: Identifier of the operation performed.</li> </ul>
<b>Headers</b>	<ul style="list-style-type: none"> <li>• <b>Accept</b>: application/json</li> <li>• <b>Content-Type</b>: application/json-patch+json</li> </ul>

Table 17.44: Format of the call to get an OSQuery query results

### Response

List of JSON objects, one for each client, with information about the query results.

JSON object field	Description
<b>panda</b>	Identifier of the client to which the computers that returned data belong.
<b>operationId</b>	Identifier of the operation performed.
<b>url</b>	Download URL for the file that contains the information collected from computers. This link is valid for five minutes, For more information about the file format, see <a href="#">Download File Format</a> .
<b>counters</b>	JSON object with the operation statistics:

JSON object field	Description
	<ul style="list-style-type: none"> <li>• <b>totalOperationElements</b>: Number of computers to which the request for information was sent.</li> <li>• <b>totalSuccess</b>: Number of computers that returned information successfully.</li> <li>• <b>totalPartiallySucceeded</b>: Number of computers that returned information but there were problems interpreting the results.</li> <li>• <b>totalError</b>: Number of computers that returned an error code.</li> <li>• <b>errors</b>: List of JSON objects with the errors received from computers. See <a href="#">Error Types</a>.                             <ul style="list-style-type: none"> <li>• <b>errorCode</b>: Error code.</li> <li>• <b>errorDescription</b>: Error description.</li> <li>• <b>occurrences</b>: Number of computers where the error occurred.</li> </ul> </li> </ul>

Table 17.45: Response JSON object with the URL and operation result

### Monitor Computers Turned Off, Unavailable, or with Delayed Responses

**totalOperationElements** is equal to the sum of **totalSuccess** + **totalPartiallySucceeded** + **totalError** if all computers respond, either with information or with an error. Because OSQuery statements can take an unspecified time to run, if **totalOperationElements** is not equal to the sum of **totalSuccess** + **totalPartiallySucceeded** + **totalError** this means there are computers on the client’s network that have not responded yet. In such case, you must send the **operationId** repeatedly until the **totalOperationElements** value is the right one or until the timeout established in the **ttl** field occurs.

### Download File Format

The file that contains the data collected from the client’s computers has these features:

- **Name**: “osquery\_” + operation ID.
- **Format**: Text.
- **Header**: File fields separated by the “;” character.
- **Body**: Lines with the content of the fields extracted by OSQuery from the computer database.

### Error Types

Name	Code	Description	Comments
<b>ErrorExecutingOsQuery</b>	201	near "name": syntax error	OSQuery is compatible with the 4.2.0 data schema. See <a href="#">OSQuery Requirements on page 231</a> and check the

Name	Code	Description	Comments
			OSQuery statement syntax.
<b>ErrorOsNotSupported</b>	202	Operating system not supported	OSQuery is compatible with Windows systems. See <a href="#">OSQuery Requirements</a> on page 231.
<b>ErrorOsQueryNotInstalled</b>	203	OSQuery not installed	OSQuery is available from version 3.71 of Cytomic EDR. See <a href="#">OSQuery Requirements</a> on page 231.

Table 17.46: Error codes and their meanings

### Get an OSQuery Query Status

Get a list of JSON objects with information about the status of in-progress or completed operations.

#### Request

<b>Command</b>	POST
<b>URL</b>	/api/v1/osQuery/info
<b>Required parameters in the HTTP message body</b>	<p>List of JSON objects, each with the ID of the operation whose status you want to retrieve.</p> <ul style="list-style-type: none"> <li>• <b>pandaId</b>: Identifier of the client to which the computers that returned data belong.</li> <li>• <b>operationId</b>: Identifier of the operation performed.</li> </ul>
<b>Optional parameters in the HTTP message body</b>	<ul style="list-style-type: none"> <li>• <b>trackingStateType</b>: Returns only operations with the specified status:</li> <li>• <b>Pending (0)</b>: In-progress operations.</li> <li>• <b>Success (1)</b>: Operations completed successfully.</li> <li>• <b>PartiallySucceeded (2)</b>: Operations for which results were received from some computers.</li> <li>• <b>Error (3)</b>: Operations that failed.</li> <li>• <b>Canceled (4)</b>: Operations canceled because</li> </ul>



	they timed out.
<b>Headers</b>	<ul style="list-style-type: none"> <li>• <b>Accept:</b> application/json</li> <li>• <b>Content-Type:</b> application/json-patch+json</li> </ul>

Table 17.47: Format of the call to get the status of a list of OSQuery queries

## Response

List of JSON objects, one for each client, with information about the query results.

JSON object field	Description
<b>panda</b>	Identifier of the client to which the operation belongs.
<b>operationId</b>	Identifier of the operation performed.
<b>info</b>	<p>List of JSON objects, one for each client operation, with information about the operation status:</p> <ul style="list-style-type: none"> <li>• <b>pandaId:</b> Identifier of the client affected by the operation.</li> <li>• <b>hostname:</b> Name of the computer affected by the operation.</li> <li>• <b>deviceId:</b> Identifier of the computer affected by the operation.</li> <li>• <b>trackingStateType:</b> Operation status. <ul style="list-style-type: none"> <li>• <b>Pending (0):</b> In-progress operation.</li> <li>• <b>Success (1):</b> Operation completed successfully.</li> <li>• <b>PartiallySucceeded (2):</b> Operation for which results were received from some computers.</li> <li>• <b>Error (3):</b> The operation failed. See <b>Error Types</b>.</li> <li>• <b>Canceled (4):</b> Operation canceled because it timed out.</li> </ul> </li> <li>• <b>date:</b> Date the operation status last changed.</li> <li>• <b>errorCode:</b> Error code.</li> <li>• <b>errorDescription:</b> Error description.</li> </ul>

Table 17.48: Response JSON object with the operation status

### Error Types

Name	Code	Description	Comments
ErrorExecutingOsQuery	201	near "name": syntax error	OSQuery is compatible with the 4.2.0 data schema. See <a href="#">OSQuery Requirements</a> on page 231 and check the OSQuery statement syntax.
ErrorOsNotSupported	202	Operating system not supported	OSQuery is compatible with Windows systems. See <a href="#">OSQuery Requirements</a> on page 231.
ErrorOsQueryNotInstalled	203	OSQuery not installed	OSQuery is available from version 3.71 of Cytomic EDR. See <a href="#">OSQuery Requirements</a> on page 231.

Table 17.49: Error codes and their meanings

## Data/Advanced Query Access API

Cytomic Orion API that provides an interface to access the data lake. It is equivalent to the advanced SQL query module.

### Get Information from the Data Lake

#### Request

Command	POST
URL	/api/v1/applications/explorations
Required parameters in the HTTP message body	JSON object with the SQL statement you want to run. <ul style="list-style-type: none"> <li>• <b>sql</b>: SQL statement.</li> </ul>
Headers	<ul style="list-style-type: none"> <li>• <b>Accept</b>: application/json</li> <li>• <b>Content-Type</b>: application/json-patch+json</li> </ul>

Table 17.50: Format of the call to retrieve information from the data lake

## Response

List of JSON objects, one for each result row. The fields in the JSON object depend on the fields requested in the SQL statement.

JSON object field	Description
Name of the requested file	Value of the field requested in the SQL statement.

Table 17.51: Response JSON object with the requested data

## Investigation Management API

This API enables you to create, edit, and delete investigations and indicator assignment rules.

### Create Investigation

Create investigations with associated clients and indicators.

#### Request

Command	POST
URL	/api/v1/applications/cases
Required parameters in the HTTP message body	<p>JSON object with these parameters:</p> <ul style="list-style-type: none"> <li><b>name:</b> Investigation name.</li> <li><b>Triggers:</b> List of the IDs of the indicators associated with the investigation.</li> <li><b>clientsIds:</b> List of the IDs of the clients associated with the investigation.</li> </ul>
Headers	<ul style="list-style-type: none"> <li><b>Accept:</b> */*</li> <li><b>Content-Type:</b> application/json;charset=UTF-8</li> </ul>

Table 17.52: Format of the call to create an investigation

#### Response

JSON object field	Description
id	Investigation ID.
name	Investigation name.

JSON object field	Description
<b>status</b>	<p>Indicates whether the investigation indicators are being reviewed by technicians or were already analyzed.</p> <ul style="list-style-type: none"> <li>• <b>0</b>: Investigation closed.</li> <li>• <b>1</b>: Investigation in progress.</li> </ul>
<b>created</b>	<p>Investigation creation date.</p>
<b>clientInfos</b>	<p>List of JSON objects with the clients assigned to the investigation.</p> <ul style="list-style-type: none"> <li>• <b>pandaClientId</b>: Client ID.</li> <li>• <b>name</b>: Client name.</li> </ul>
<b>classification</b>	<p>Indicates the investigation classification:</p> <ul style="list-style-type: none"> <li>• <b>0</b>: (Unclassified) Investigation pending analysis.</li> <li>• <b>1</b>: (Confirmed attack) The indicator investigation resulted in the detection of an attack.</li> <li>• <b>2</b>: (Investigation without detected attacks) The indicator investigation did not find any attacks.</li> <li>• <b>3</b>: (Potential attack) The indicator investigation is inconclusive, but the indicators have a high probability of being an attack.</li> </ul>
<b>priority</b>	<p>Indicates the impact that the possible attack investigated could have on the company assets:</p> <ul style="list-style-type: none"> <li>• <b>0</b>: (Undefined) The impact has not yet been determined.</li> <li>• <b>1</b>: (Critical) The risk level detected in the indicator investigation is very high.</li> <li>• <b>2</b>: (High) The risk level detected in the indicator investigation is high.</li> <li>• <b>3</b>: (Medium) The risk level detected in the indicator investigation is medium.</li> <li>• <b>4</b>: (Low) The risk level detected in the indicator investigation is low.</li> </ul>

JSON object field	Description
<b>description</b>	Detailed description of the investigation status.
<b>assignedTo</b>	null
<b>assignedToEmail</b>	null

Table 17.53: Response JSON object to a request to create an investigation

## Get Investigation Details

Retrieves the characteristics of an investigation.

### Request

<b>Command</b>	GET
<b>URL</b>	/api/v1/applications/cases/{caseId}
<b>Required parameters in the URL</b>	<ul style="list-style-type: none"> <li><b>caseId</b>: Investigation ID.</li> </ul>
<b>Headers</b>	<ul style="list-style-type: none"> <li><b>Accept</b>: */*</li> </ul>

Table 17.54: Format of the call to get the details of an investigation

### Response

JSON object field	Description
<b>id</b>	Investigation ID.
<b>name</b>	Investigation name.
<b>createdBy</b>	User account that created the investigation.
<b>status</b>	<p>Indicates whether the investigation indicators are being reviewed by technicians or were already analyzed.</p> <ul style="list-style-type: none"> <li><b>0</b>: Investigation closed.</li> <li><b>1</b>: Investigation in progress.</li> </ul>
<b>created</b>	Investigation creation date.
<b>clientInfos</b>	List of JSON objects with the clients assigned to the investigation.

JSON object field	Description
	<ul style="list-style-type: none"> <li>• <b>pandaClientId</b>: Client ID.</li> <li>• <b>name</b>: Client name.</li> </ul>
<b>classification</b>	<p>Indicates the investigation classification:</p> <ul style="list-style-type: none"> <li>• <b>0</b>: (Unclassified) Investigation pending analysis.</li> <li>• <b>1</b>: (Confirmed attack) The indicator investigation resulted in the detection of an attack.</li> <li>• <b>2</b>: (Investigation without detected attacks) The indicator investigation did not find any attacks.</li> <li>• <b>3</b>: (Potential attack) The indicator investigation is inconclusive, but the indicators have a high probability of being an attack.</li> </ul>
<b>priority</b>	<p>Indicates the impact that the possible attack investigated could have on the company assets:</p> <ul style="list-style-type: none"> <li>• <b>0</b>: (Undefined) The impact has not yet been determined.</li> <li>• <b>1</b>: (Critical) The risk level detected in the indicator investigation is very high.</li> <li>• <b>2</b>: (High) The risk level detected in the indicator investigation is high.</li> <li>• <b>3</b>: (Medium) The risk level detected in the indicator investigation is medium.</li> <li>• <b>4</b>: (Low) The risk level detected in the indicator investigation is low.</li> </ul>
<b>description</b>	Detailed description of the investigation status.
<b>assignedTo</b>	ID of the user account assigned to the investigation.
<b>assignedToEmail</b>	User account assigned to the investigation.

Table 17.55: Response JSON object to a request to get the details of an investigation

## Search for Investigations

Gets a list of JSON objects with all the investigations that match the parameters set in the call. The details of each investigation found are included.

The search applies a logical OR between the parameters specified in the call JSON object. If a parameter can take a list of values, a logical OR is applied between them.

### Request

<b>Command</b>	POST
<b>URL</b>	/api/v1/applications/cases/filter
<b>Required parameters in the HTTP message body</b>	<p>JSON object with the investigation filtering parameters.</p> <ul style="list-style-type: none"> <li>• <b>from</b>: Unix timestamp in milliseconds with the start date of the period for which you want to filter the investigations.</li> <li>• <b>to</b>: Unix timestamp in milliseconds with the end date of the period for which you want to filter the investigations.</li> <li>• <b>statuses</b>: Status list (1: In progress, 2: Closed).</li> <li>• <b>Emails</b>: Email address list.</li> <li>• <b>clients</b>: Client name list.</li> <li>• <b>classifications</b>: Classification list (0: Unclassified, 1: Confirmed attack, 2: Investigation without detected attacks, 3: Potential attack)</li> <li>• <b>priorities</b>: Priority list (0: Undefined, 1: Critical, 2: High, 3: Medium, 4: Low)</li> <li>• <b>assignedToEmails</b>: Email address list (none: Not assigned, Email: Email address).</li> </ul>
<b>Headers</b>	<ul style="list-style-type: none"> <li>• <b>Accept</b>: */*</li> <li>• <b>Content-Type</b>: application/json;charset=UTF-8</li> </ul>

Table 17.56: Format of the call to search for investigations

### Response

List of JSON objects with all investigations found.

JSON object field	Description
id	Investigation ID.

JSON object field	Description
<b>name</b>	Investigation name.
<b>status</b>	<p>Indicates whether the investigation indicators are being reviewed by technicians or were already analyzed.</p> <ul style="list-style-type: none"> <li>• <b>0</b>: Investigation closed.</li> <li>• <b>1</b>: Investigation in progress.</li> </ul>
<b>created</b>	Investigation creation date.
<b>clientInfos</b>	<p>List of JSON objects with the clients assigned to the investigation.</p> <ul style="list-style-type: none"> <li>• <b>pandaClientId</b>: Client ID.</li> <li>• <b>name</b>: Client name.</li> </ul>
<b>classification</b>	<p>Indicates the investigation classification:</p> <ul style="list-style-type: none"> <li>• <b>0</b>: (Unclassified) Investigation pending analysis.</li> <li>• <b>1</b>: (Confirmed attack) The indicator investigation resulted in the detection of an attack.</li> <li>• <b>2</b>: (Investigation without detected attacks) The indicator investigation did not find any attacks.</li> <li>• <b>3</b>: (Potential attack) The indicator investigation is inconclusive, but the indicators have a high probability of being an attack.</li> </ul>
<b>priority</b>	<p>Indicates the impact that the possible attack investigated could have on the company assets:</p> <ul style="list-style-type: none"> <li>• <b>0</b>: (Undefined) The impact has not yet been determined.</li> <li>• <b>1</b>: (Critical) The risk level detected in the indicator investigation is very high.</li> <li>• <b>2</b>: (High) The risk level detected in the indicator investigation is high.</li> <li>• <b>3</b>: (Medium) The risk level detected in the indicator investigation is medium.</li> </ul>



JSON object field	Description
	<ul style="list-style-type: none"> <li>• <b>4:</b> (Low) The risk level detected in the indicator investigation is low.</li> </ul>
<b>description</b>	Detailed description of the investigation status.
<b>assignedTo</b>	ID of the user account assigned to the investigation.
<b>assignedToEmail</b>	User account assigned to the investigation.

Table 17.57: Response JSON object to a request to search for investigations

## Update Investigation

Modifies the characteristics of an investigation.

### Request

<b>Command</b>	PUT
<b>URL</b>	/api/v1/applications/cases/{caseId}
<b>Required parameters in the URL</b>	<ul style="list-style-type: none"> <li>• <b>caseId:</b> Investigation ID.</li> </ul>
<b>Required parameters in the HTTP message body</b>	<p>JSON object with the investigation information.</p> <ul style="list-style-type: none"> <li>• <b>name:</b> The new name of the investigation.</li> <li>• <b>classification:</b> The new classification of the investigation (0: Unclassified, 1: Confirmed attack, 2: Investigation without detected attacks, 3: Potential attack)</li> <li>• <b>priority:</b> The new priority of the investigation (0: Undefined, 1: Critical, 2: High, 3: Medium, 4: Low)</li> <li>• <b>description:</b> The new description of the investigation.</li> <li>• <b>assignedTo:</b> Consoler user assigned to the investigation.</li> </ul>
<b>Headers</b>	<ul style="list-style-type: none"> <li>• <b>Accept:</b> */*</li> <li>• <b>Content-Type:</b> application/json;charset=UTF-8</li> </ul>

Table 17.58: Format of the call to update an investigation

**Response**

JSON object field	Description
<b>id</b>	Investigation ID.
<b>name</b>	Investigation name.
<b>status</b>	<p>Indicates whether the investigation indicators are being reviewed by technicians or were already analyzed.</p> <ul style="list-style-type: none"> <li>• <b>0</b>: Investigation closed.</li> <li>• <b>1</b>: Investigation in progress.</li> </ul>
<b>created</b>	Investigation creation date.
<b>clientInfos</b>	<p>List of JSON objects with the clients assigned to the investigation.</p> <ul style="list-style-type: none"> <li>• <b>pandaClientId</b>: Client ID.</li> <li>• <b>name</b>: Client name.</li> </ul>
<b>classification</b>	<p>Indicates the investigation classification:</p> <ul style="list-style-type: none"> <li>• <b>0</b>: (Unclassified) Investigation pending analysis.</li> <li>• <b>1</b>: (Confirmed attack) The indicator investigation resulted in the detection of an attack.</li> <li>• <b>2</b>: (Investigation without detected attacks) The indicator investigation did not find any attacks.</li> <li>• <b>3</b>: (Potential attack) The indicator investigation is inconclusive, but the indicators have a high probability of being an attack.</li> </ul>
<b>priority</b>	<p>Indicates the impact that the possible attack investigated could have on the company assets:</p> <ul style="list-style-type: none"> <li>• <b>0</b>: (Undefined) The impact has not yet been determined.</li> <li>• <b>1</b>: (Critical) The risk level detected in the indicator investigation is very high.</li> <li>• <b>2</b>: (High) The risk level detected in the indicator</li> </ul>

JSON object field	Description
	investigation is high. <ul style="list-style-type: none"> <li>• <b>3:</b> (Medium) The risk level detected in the indicator investigation is medium.</li> <li>• <b>4:</b> (Low) The risk level detected in the indicator investigation is low.</li> </ul>
<b>description</b>	Detailed description of the investigation status.
<b>assignedTo</b>	ID of the user account assigned to the investigation.
<b>assignedToEmail</b>	User account assigned to the investigation.

Table 17.59: Response JSON object to a request to update an investigation

## Update Clients for an Investigation

Updates the clients assigned to an investigation.

### Request

<b>Command</b>	PUT
<b>URL</b>	/api/v1/applications/cases/{caseId}/clients
<b>Required parameters in the URL</b>	<ul style="list-style-type: none"> <li>• <b>caseId:</b> Investigation ID.</li> </ul>
<b>Required parameters in the HTTP message body</b>	JSON object with the list of clients assigned to the investigation. <ul style="list-style-type: none"> <li>• <b>clientsIds:</b> List of the IDs of the clients assigned to the investigation.</li> </ul>
<b>Headers</b>	<ul style="list-style-type: none"> <li>• <b>Accept:</b> */*</li> <li>• <b>Content-Type:</b> application/json;charset=UTF-8</li> </ul>

Table 17.60: Format of the call to update the clients assigned to an investigation

### Response

JSON object field	Description
<b>id</b>	Investigation ID.

JSON object field	Description
<b>name</b>	Investigation name.
<b>status</b>	<p>Indicates whether the investigation indicators are being reviewed by technicians or were already analyzed.</p> <ul style="list-style-type: none"> <li>• <b>0</b>: Investigation closed.</li> <li>• <b>1</b>: Investigation in progress.</li> </ul>
<b>created</b>	Investigation creation date.
<b>clientInfos</b>	<p>List of JSON objects with the clients assigned to the investigation.</p> <ul style="list-style-type: none"> <li>• <b>pandaClientId</b>: Client ID.</li> <li>• <b>name</b>: Client name.</li> </ul>
<b>classification</b>	<p>Indicates the investigation classification:</p> <ul style="list-style-type: none"> <li>• <b>0</b>: (Unclassified) Investigation pending analysis.</li> <li>• <b>1</b>: (Confirmed attack) The indicator investigation resulted in the detection of an attack.</li> <li>• <b>2</b>: (Investigation without detected attacks) The indicator investigation did not find any attacks.</li> <li>• <b>3</b>: (Potential attack) The indicator investigation is inconclusive, but the indicators have a high probability of being an attack.</li> </ul>
<b>priority</b>	<p>Indicates the impact that the possible attack investigated could have on the company assets:</p> <ul style="list-style-type: none"> <li>• <b>0</b>: (Undefined) The impact has not yet been determined.</li> <li>• <b>1</b>: (Critical) The risk level detected in the indicator investigation is very high.</li> <li>• <b>2</b>: (High) The risk level detected in the indicator investigation is high.</li> <li>• <b>3</b>: (Medium) The risk level detected in the indicator investigation is medium.</li> </ul>

JSON object field	Description
	<ul style="list-style-type: none"> <li>• <b>4:</b> (Low) The risk level detected in the indicator investigation is low.</li> </ul>
<b>description</b>	Detailed description of the investigation status.
<b>assignedTo</b>	ID of the user account assigned to the investigation.
<b>assignedToEmail</b>	User account assigned to the investigation.

Table 17.61: Response JSON object to a request to update an investigation clients

## Close Investigation

Closes investigations whose indicators have been analyzed and resolved.

### Request

<b>Command</b>	PUT
<b>URL</b>	/api/v1/applications/cases/{caseId}/close
<b>Required parameters in the URL</b>	<ul style="list-style-type: none"> <li>• <b>caseId:</b> Investigation ID.</li> </ul>
<b>Headers</b>	<ul style="list-style-type: none"> <li>• <b>Accept:</b> application/json</li> <li>• <b>Content-Type:</b> application/json-patch+json</li> </ul>

Table 17.62: Format of the call to close investigations

### Response

JSON object field	Description
<b>id</b>	Investigation ID.
<b>name</b>	Investigation name.
<b>status</b>	<p>Indicates whether the investigation indicators are being reviewed by technicians or were already analyzed.</p> <ul style="list-style-type: none"> <li>• <b>0:</b> Investigation closed.</li> <li>• <b>1:</b> Investigation in progress.</li> </ul>

JSON object field	Description
<b>created</b>	Investigation creation date.
<b>clientInfos</b>	<p>List of JSON objects with the clients assigned to the investigation.</p> <ul style="list-style-type: none"> <li>• <b>pandaClientId</b>: Client ID.</li> <li>• <b>name</b>: Client name.</li> </ul>
<b>classification</b>	<p>Indicates the investigation classification:</p> <ul style="list-style-type: none"> <li>• <b>0</b>: (Unclassified) Investigation pending analysis.</li> <li>• <b>1</b>: (Confirmed attack) The indicator investigation resulted in the detection of an attack.</li> <li>• <b>2</b>: (Investigation without detected attacks) The indicator investigation did not find any attacks.</li> <li>• <b>3</b>: (Potential attack) The indicator investigation is inconclusive, but the indicators have a high probability of being an attack.</li> </ul>
<b>priority</b>	<p>Indicates the impact that the possible attack investigated could have on the company assets:</p> <ul style="list-style-type: none"> <li>• <b>0</b>: (Undefined) The impact has not yet been determined.</li> <li>• <b>1</b>: (Critical) The risk level detected in the indicator investigation is very high.</li> <li>• <b>2</b>: (High) The risk level detected in the indicator investigation is high.</li> <li>• <b>3</b>: (Medium) The risk level detected in the indicator investigation is medium.</li> <li>• <b>4</b>: (Low) The risk level detected in the indicator investigation is low.</li> </ul>
<b>description</b>	Detailed description of the investigation status.
<b>assignedTo</b>	ID of the user account assigned to the investigation.

JSON object field	Description
<b>assignedToEmail</b>	User account assigned to the investigation.

Table 17.63: Response JSON object to a request to create an investigation

## Reopen a Closed Investigation

Reopens previously closed investigations.

### Request

<b>Command</b>	PUT
<b>URL</b>	/api/v1/applications/cases/{caseId}/reopen
<b>Required parameters in the URL</b>	<ul style="list-style-type: none"> <li>• <b>caseId</b>: Investigation ID.</li> </ul>
<b>Headers</b>	<ul style="list-style-type: none"> <li>• <b>Accept</b>: */*</li> <li>• <b>Content-Type</b>: application/json;charset=UTF-8</li> </ul>

Table 17.64: Format of the call to reopen an investigation

### Response

JSON object field	Description
<b>id</b>	Investigation ID.
<b>name</b>	Investigation name.
<b>status</b>	<p>Indicates whether the investigation indicators are being reviewed by technicians or were already analyzed.</p> <ul style="list-style-type: none"> <li>• <b>0</b>: Investigation closed.</li> <li>• <b>1</b>: Investigation in progress.</li> </ul>
<b>created</b>	Investigation creation date.
<b>clientInfos</b>	<p>List of JSON objects with the clients assigned to the investigation.</p> <ul style="list-style-type: none"> <li>• <b>pandaClientId</b>: Client ID.</li> <li>• <b>name</b>: Client name.</li> </ul>

JSON object field	Description
<b>classification</b>	<p>Indicates the investigation classification:</p> <ul style="list-style-type: none"> <li>• <b>0:</b> (Unclassified) Investigation pending analysis.</li> <li>• <b>1:</b> (Confirmed attack) The indicator investigation resulted in the detection of an attack.</li> <li>• <b>2:</b> (Investigation without detected attacks) The indicator investigation did not find any attacks.</li> <li>• <b>3:</b> (Potential attack) The indicator investigation is inconclusive, but the indicators have a high probability of being an attack.</li> </ul>
<b>priority</b>	<p>Indicates the impact that the possible attack investigated could have on the company assets:</p> <ul style="list-style-type: none"> <li>• <b>0:</b> (Undefined) The impact has not yet been determined.</li> <li>• <b>1:</b> (Critical) The risk level detected in the indicator investigation is very high.</li> <li>• <b>2:</b> (High) The risk level detected in the indicator investigation is high.</li> <li>• <b>3:</b> (Medium) The risk level detected in the indicator investigation is medium.</li> <li>• <b>4:</b> (Low) The risk level detected in the indicator investigation is low.</li> </ul>
<b>description</b>	Detailed description of the investigation status.
<b>assignedTo</b>	ID of the user account assigned to the investigation.
<b>assignedToEmail</b>	User account assigned to the investigation.

Table 17.65: Response JSON object to a request to reopen an investigation

### Add Indicators to an Investigation

Adds indicators to a previously created investigation. An indicator can be assigned to only one investigation. If the indicator you want to assign is already assigned to another investigation, the call returns an error. To move indicators from one investigation to another, see [Move Indicators from One Investigation to Another](#).



**Request**

<b>Command</b>	POST
<b>URL</b>	/api/v1/applications/cases/{caseId}/triggers
<b>Required parameters in the URL</b>	<ul style="list-style-type: none"> <li>• <b>caseId</b>: Investigation ID.</li> </ul>
<b>Required parameters in the HTTP message body</b>	<p>JSON object with these parameters:</p> <ul style="list-style-type: none"> <li>• <b>triggerIds</b>: List of IDs of the indicators assigned to the investigation.</li> </ul>
<b>Headers</b>	<ul style="list-style-type: none"> <li>• <b>Accept</b>: */*</li> <li>• <b>Content-Type</b>: application/json;charset=UTF-8</li> </ul>

Table 17.66: Format of the call to assign indicators to an investigation

**Response**

JSON object field	Description
<b>id</b>	Investigation ID.
<b>name</b>	Investigation name.
<b>status</b>	<p>Indicates whether the investigation indicators are being reviewed by technicians or were already analyzed.</p> <ul style="list-style-type: none"> <li>• <b>0</b>: Investigation closed.</li> <li>• <b>1</b>: Investigation in progress.</li> </ul>
<b>created</b>	Investigation creation date.
<b>clientInfos</b>	<p>List of JSON objects with the clients assigned to the investigation.</p> <ul style="list-style-type: none"> <li>• <b>pandaClientId</b>: Client ID.</li> <li>• <b>name</b>: Client name.</li> </ul>
<b>classification</b>	<p>Indicates the investigation classification:</p> <ul style="list-style-type: none"> <li>• <b>0</b>: (Unclassified) Investigation pending analysis.</li> <li>• <b>1</b>: (Confirmed attack) The indicator investigation</li> </ul>

JSON object field	Description
	<p>resulted in the detection of an attack.</p> <ul style="list-style-type: none"> <li>• <b>2:</b> (Investigation without detected attacks) The indicator investigation did not find any attacks.</li> <li>• <b>3:</b> (Potential attack) The indicator investigation is inconclusive, but the indicators have a high probability of being an attack.</li> </ul>
<b>priority</b>	<p>Indicates the impact that the possible attack investigated could have on the company assets:</p> <ul style="list-style-type: none"> <li>• <b>0:</b> (Undefined) The impact has not yet been determined.</li> <li>• <b>1:</b> (Critical) The risk level detected in the indicator investigation is very high.</li> <li>• <b>2:</b> (High) The risk level detected in the indicator investigation is high.</li> <li>• <b>3:</b> (Medium) The risk level detected in the indicator investigation is medium.</li> <li>• <b>4:</b> (Low) The risk level detected in the indicator investigation is low.</li> </ul>
<b>description</b>	Detailed description of the investigation status.
<b>assignedTo</b>	ID of the user account assigned to the investigation.
<b>assignedToEmail</b>	User account assigned to the investigation.

Table 17.67: Response JSON object to a request to assign indicators to an investigation

### Delete Indicators from an Investigation

Deletes indicators from an investigation.

#### Request

<b>Command</b>	DEL
<b>URL</b>	/api/v1/applications/cases/{caseId}/triggers
<b>Required parameters in the</b>	<ul style="list-style-type: none"> <li>• <b>caseId:</b> Investigation ID.</li> </ul>

<b>URL</b>	
<b>Required parameters in the HTTP message body</b>	<p>JSON object with these parameters:</p> <ul style="list-style-type: none"> <li>• <b>triggerIds</b>: List of IDs of the indicators assigned to the investigation.</li> </ul>
<b>Headers</b>	<ul style="list-style-type: none"> <li>• <b>Accept</b>: */*</li> <li>• <b>Content-Type</b>: application/json;charset=UTF-8</li> </ul>

Table 17.68: Format of the call to remove indicators from an investigation

## Response

JSON object field	Description
<b>id</b>	Investigation ID.
<b>name</b>	Investigation name.
<b>status</b>	<p>Indicates whether the investigation indicators are being reviewed by technicians or were already analyzed.</p> <ul style="list-style-type: none"> <li>• <b>0</b>: Investigation closed.</li> <li>• <b>1</b>: Investigation in progress.</li> </ul>
<b>created</b>	Investigation creation date.
<b>clientInfos</b>	<p>List of JSON objects with the clients assigned to the investigation.</p> <ul style="list-style-type: none"> <li>• <b>pandaClientId</b>: Client ID.</li> <li>• <b>name</b>: Client name.</li> </ul>
<b>classification</b>	<p>Indicates the investigation classification:</p> <ul style="list-style-type: none"> <li>• <b>0</b>: (Unclassified) Investigation pending analysis.</li> <li>• <b>1</b>: (Confirmed attack) The indicator investigation resulted in the detection of an attack.</li> <li>• <b>2</b>: (Investigation without detected attacks) The indicator investigation did not find any attacks.</li> <li>• <b>3</b>: (Potential attack) The indicator investigation is inconclusive, but the indicators have a high</li> </ul>

JSON object field	Description
	probability of being an attack.
<b>priority</b>	<p>Indicates the impact that the possible attack investigated could have on the company assets:</p> <ul style="list-style-type: none"> <li>• <b>0:</b> (Undefined) The impact has not yet been determined.</li> <li>• <b>1:</b> (Critical) The risk level detected in the indicator investigation is very high.</li> <li>• <b>2:</b> (High) The risk level detected in the indicator investigation is high.</li> <li>• <b>3:</b> (Medium) The risk level detected in the indicator investigation is medium.</li> <li>• <b>4:</b> (Low) The risk level detected in the indicator investigation is low.</li> </ul>
<b>description</b>	Detailed description of the investigation status.
<b>assignedTo</b>	ID of the user account assigned to the investigation.
<b>assignedToEmail</b>	User account assigned to the investigation.

Table 17.69: Response JSON object to a request to remove indicators from an investigation

### Move Indicators from One Investigation to Another

Copies indicators from one investigation to another, previously created investigation and deletes them from the original investigation. Because an indicator can be assigned to only one investigation, when you assign indicators with this method, the solution automatically removes the indicators from the original investigation to assign them to the investigation specified in the call.

#### Request

<b>Command</b>	POST
<b>URL</b>	/api/v1/applications/cases/{caseId}/triggers/move
<b>Required parameters in the URL</b>	<ul style="list-style-type: none"> <li>• <b>caseId:</b> Investigation ID.</li> </ul>
<b>Required parameters in the</b>	JSON object with these parameters:

<b>HTTP message body</b>	<ul style="list-style-type: none"> <li>• <b>triggerIds</b>: List of IDs of the indicators assigned to the investigation.</li> </ul>
<b>Headers</b>	<ul style="list-style-type: none"> <li>• <b>Accept</b>: */*</li> <li>• <b>Content-Type</b>: application/json;charset=UTF-8</li> </ul>

Table 17.70: Format of the call to move indicators from one investigation to another

## Response

JSON object field	Description
<b>id</b>	Investigation ID.
<b>name</b>	Investigation name.
<b>status</b>	<p>Indicates whether the investigation indicators are being reviewed by technicians or were already analyzed.</p> <ul style="list-style-type: none"> <li>• <b>0</b>: Investigation closed.</li> <li>• <b>1</b>: Investigation in progress.</li> </ul>
<b>created</b>	Investigation creation date.
<b>clientInfos</b>	<p>List of JSON objects with the clients assigned to the investigation.</p> <ul style="list-style-type: none"> <li>• <b>pandaClientId</b>: Client ID.</li> <li>• <b>name</b>: Client name.</li> </ul>
<b>classification</b>	<p>Indicates the investigation classification:</p> <ul style="list-style-type: none"> <li>• <b>0</b>: (Unclassified) Investigation pending analysis.</li> <li>• <b>1</b>: (Confirmed attack) The indicator investigation resulted in the detection of an attack.</li> <li>• <b>2</b>: (Investigation without detected attacks) The indicator investigation did not find any attacks.</li> <li>• <b>3</b>: (Potential attack) The indicator investigation is inconclusive, but the indicators have a high probability of being an attack.</li> </ul>

JSON object field	Description
priority	<p>Indicates the impact that the possible attack investigated could have on the company assets:</p> <ul style="list-style-type: none"> <li>• <b>0:</b> (Undefined) The impact has not yet been determined.</li> <li>• <b>1:</b> (Critical) The risk level detected in the indicator investigation is very high.</li> <li>• <b>2:</b> (High) The risk level detected in the indicator investigation is high.</li> <li>• <b>3:</b> (Medium) The risk level detected in the indicator investigation is medium.</li> <li>• <b>4:</b> (Low) The risk level detected in the indicator investigation is low.</li> </ul>
description	Detailed description of the investigation status.
assignedTo	ID of the user account assigned to the investigation.
assignedToEmail	User account assigned to the investigation.

Table 17.71: Response JSON object to a request to move indicators between investigations

## Add a Comment to an Investigation

Adds a comment to a previously created investigation.

### Request

Command	POST
URL	/api/v1/applications/cases/{caseId}/comment
Required parameters in the URL	<ul style="list-style-type: none"> <li>• <b>caseId:</b> Investigation ID.</li> </ul>
Required parameters in the HTTP message body	<p>JSON object with these parameters:</p> <ul style="list-style-type: none"> <li>• <b>data:</b> Comment content.</li> </ul>
Headers	<ul style="list-style-type: none"> <li>• <b>Accept:</b> */*</li> <li>• <b>Content-Type:</b> application/json;charset=UTF-8</li> </ul>

Table 17.72: Format of the call to add a comment to an investigation

## Response

JSON object field	Description
<b>id</b>	Comment ID.
<b>caseId</b>	Investigation ID.
<b>userId</b>	ID of the user who added the comment.
<b>userEmail</b>	Email address of the user who added the comment.
<b>data</b>	Comment content.
<b>created</b>	Date the comment was created.
<b>isDeleted</b>	<ul style="list-style-type: none"> <li>• <b>false</b>: The comment is visible.</li> <li>• <b>true</b>: The comment was deleted.</li> </ul>
<b>authorizedApplicationName</b>	Name of the application that added the comment. If the comment was added from the console, this field shows the user account email address.

Table 17.73: Response JSON object to a request to add a comment to an investigation

## Get an Investigation Comments

Gets an investigation comments.

### Request

<b>Command</b>	GET
<b>URL</b>	/api/v1/applications/cases/{caseId}/comment
<b>Required parameters in the URL</b>	<ul style="list-style-type: none"> <li>• <b>caseId</b>: Investigation ID.</li> </ul>
<b>Headers</b>	<ul style="list-style-type: none"> <li>• <b>Accept</b>: */*</li> </ul>

Table 17.74: Format of the call to get an investigation comments

### Response

List of JSON objects with the investigation comments.

JSON object field	Description
<b>id</b>	Comment ID.
<b>caseId</b>	Investigation ID.
<b>userId</b>	ID of the user who added the comment.
<b>userEmail</b>	Email address of the user who added the comment.
<b>data</b>	Comment content.
<b>created</b>	Date the comment was created.
<b>isDeleted</b>	<ul style="list-style-type: none"> <li>• <b>false</b>: The comment is visible.</li> <li>• <b>true</b>: The comment was deleted.</li> </ul>
<b>authorizedApplicationName</b>	Name of the application that added the comment. If the comment was added from the console, this field shows the user account email address.

Table 17.75: Response JSON object to a request to get an investigation comments

## Update an Investigation Comment

Edits an investigation comment.

### Request

<b>Command</b>	POST
<b>URL</b>	/api/v1/applications/cases/{caseId}/comment/{caseCommentId}
<b>Required parameters in the URL</b>	<ul style="list-style-type: none"> <li>• <b>caseId</b>: Investigation ID.</li> <li>• <b>caseCommentId</b>: Comment ID.</li> </ul>
<b>Required parameters in the HTTP message body</b>	JSON object with these parameters: <ul style="list-style-type: none"> <li>• <b>data</b>: Comment content.</li> </ul>
<b>Headers</b>	<ul style="list-style-type: none"> <li>• <b>Accept</b>: */*</li> <li>• <b>Content-Type</b>:</li> </ul>



```
application/json;charset=UTF-8
```

Table 17.76: Format of the call to update an investigation comment

**Response**

JSON object field	Description
<b>id</b>	Comment ID.
<b>caseId</b>	Investigation ID.
<b>userId</b>	ID of the user who added the comment.
<b>userEmail</b>	Email address of the user who added the comment.
<b>data</b>	Comment content.
<b>created</b>	Date the comment was created.
<b>isDeleted</b>	<ul style="list-style-type: none"> <li>• <b>false</b>: The comment is visible.</li> <li>• <b>true</b>: The comment was deleted.</li> </ul>
<b>authorizedApplicationName</b>	Name of the application that added the comment. If the comment was added from the console, this field shows the user account email address.

Table 17.77: Response JSON object to a request to update an investigation comment

**Delete Comments from an Investigation**

Deletes a comment from an investigation.

**Request**

<b>Command</b>	DEL
<b>URL</b>	/api/v1/applications/cases/{caseId}/comment/{caseCommentId}
<b>Required parameters in the URL</b>	<ul style="list-style-type: none"> <li>• <b>caseId</b>: Investigation ID.</li> <li>• <b>caseCommentId</b>: Comment ID.</li> </ul>
<b>Headers</b>	<ul style="list-style-type: none"> <li>• <b>Accept</b>: */*</li> </ul>

- **Content-Type:** application/json;charset=UTF-8

Table 17.78: Format of the call to delete a comment from an investigation

**Response**

JSON object field	Description
<b>id</b>	Comment ID.
<b>caseId</b>	Investigation ID.
<b>userId</b>	ID of the user who added the comment.
<b>userEmail</b>	Email address of the user who added the comment.
<b>data</b>	Comment content.
<b>created</b>	Date the comment was created.
<b>isDeleted</b>	<ul style="list-style-type: none"> <li>• <b>false:</b> The comment is visible.</li> <li>• <b>true:</b> The comment was deleted.</li> </ul>
<b>authorizedApplicationName</b>	Name of the application that added the comment. If the comment was added from the console, this field shows the user account email address.

Table 17.79: Response JSON object to a request to delete a comment from an investigation

**Get the Types of Supported Entities of Interest**

Gets a list of JSON objects with the types of entities supported by Cytomic Orion and their IDs.

**Request**

<b>Command</b>	GET
<b>URL</b>	/api/v1/applications/entities-of-interest/types
<b>Headers</b>	<ul style="list-style-type: none"> <li>• <b>Accept:</b> */*</li> </ul>

Table 17.80: Format of the call to get the types of entities of interest supported by Cytomic Orion

**Response**

List of JSON objects with information about the types of entities of interest supported by Cytomic Orion.

JSON object field	Description
<b>id</b>	ID of the type of entity of interest
<b>name</b>	Name of the entity of interest.

Table 17.81: Response JSON object to a request to get the types of entities of interest supported by Cytomic Orion

## Add Entities of Interest to an Investigation

Adds multiple entities of interest of the same type to a previously created investigation.

### Request

<b>Command</b>	POST
<b>URL</b>	/api/v1/applications/cases/{caseId}/entities-of-interest
<b>Required parameters in the URL</b>	<ul style="list-style-type: none"> <li><b>caseId</b>: Investigation ID.</li> </ul>
<b>Required parameters in the HTTP message body</b>	JSON object with these parameters: <ul style="list-style-type: none"> <li><b>entityId</b>: Entity type ID.</li> <li><b>entities</b>: List with the names of the entities.</li> </ul>
<b>Headers</b>	<ul style="list-style-type: none"> <li><b>Accept</b>: */*</li> <li><b>Content-Type</b>: application/json;charset=UTF-8</li> </ul>

Table 17.82: Format of the call to add entities of interest to an investigation

### Response

List of JSON objects with information about the entities of interest associated with the investigation.

JSON object field	Description
<b>id</b>	ID of the entity of interest.
<b>typeId</b>	Type of entity of interest.
<b>entity</b>	Name of the entity of interest.
<b>metadata</b>	Additional information associated with the entity of interest.

JSON object field	Description
	For computer- or client-type entities, this field stores the computer or client name.
<b>comments</b>	Comments associated with the entity of interest. These comments are not shown in the analysis console.

Table 17.83: Response JSON object to a request to add entities of interest to an investigation

## Get an Investigation Entities of Interest

Gets a list of JSON objects with the entities of interest associated with an investigation.

### Request

<b>Command</b>	GET
<b>URL</b>	/api/v1/applications/cases/{caseId}/entities-of-interest
<b>Required parameters in the URL</b>	<ul style="list-style-type: none"> <li><b>caseId</b>: Investigation ID.</li> </ul>
<b>Headers</b>	<ul style="list-style-type: none"> <li><b>Accept</b>: */*</li> </ul>

Table 17.84: Format of the call to get an investigation entities of interest

### Response

JSON object field	Description
<b>id</b>	ID of the entity of interest.
<b>typeId</b>	Type of entity of interest.
<b>entity</b>	Name of the entity of interest.
<b>metadata</b>	Additional information associated with the entity of interest. For computer- or client-type entities, this field stores the computer or client name.
<b>comments</b>	Comments associated with the entity of interest. These comments are not shown in the analysis console.

Table 17.85: Response JSON object to a request to get an investigation entities of interest

## Delete Entities of Interest from an Investigation

Deletes entities of interest from an investigation.

### Request

<b>Command</b>	DEL
<b>URL</b>	/api/v1/applications/cases/{caseId}/entities-of-interest/{eoid}
<b>Required parameters in the URL</b>	<ul style="list-style-type: none"> <li>• <b>caseId</b>: Investigation ID.</li> <li>• <b>eoid</b>: ID of the entity of interest.</li> </ul>
<b>Headers</b>	<ul style="list-style-type: none"> <li>• <b>Accept</b>: */*</li> <li>• <b>Content-Type</b>: application/json;charset=UTF-8</li> </ul>

Table 17.86: Format of the call to delete entities of interest from an investigation

### Response

JSON object field	Description
<b>id</b>	ID of the entity of interest.
<b>typeid</b>	Type of entity of interest.
<b>entity</b>	Name of the entity of interest.
<b>metadata</b>	Additional information associated with the entity of interest. For computer- or client-type entities, this field stores the computer or client name.
<b>comments</b>	Comments associated with the entity of interest. These comments are not shown in the analysis console.

Table 17.87: Response JSON object to a request to delete entities of interest from an investigation

## Create Rules to Assign Indicators to an Investigation

Creates an assignment rule to automatically move new indicators that meet certain criteria to an investigation. The rule contains the investigation and the characteristics of the indicators you want to assign to it.

**Request**

<b>Command</b>	POST
<b>URL</b>	/api/v1/alerts/triggers/automation-rules
<b>Required parameters in the HTTP message body</b>	<p>JSON object with the parameters that describe the characteristics of the indicators you want to move to the chosen investigation:</p> <ul style="list-style-type: none"> <li>• <b>caseId</b>: ID of the investigation that receives the indicators that meet the conditions set in the assignment rule.</li> <li>• <b>isRegexDetails</b>: Boolean value indicating whether the assignment rule <b>details</b> field contains a regular expression (True) or plain text (False).</li> <li>• <b>description</b>: Description of the assignment rule.</li> <li>• <b>details</b>: Contents of the indicator <b>Details</b> field.</li> <li>• <b>huntingRule</b>: ID of the hunting rule that generated the indicator.</li> <li>• <b>machineNames</b>: List with the names of the computers associated with the indicators.</li> <li>• <b>muids</b>: List with the IDs of the computers associated with the indicators.</li> <li>• <b>name</b>: Name of the assignment rule.</li> <li>• <b>pandaClientIds</b>: List with the IDs of the clients associated with the indicator.</li> <li>• <b>detailsFromTrigger</b>: Regular expression associated with the content of the indicator <b>Details</b> field.</li> </ul>
<b>Headers</b>	<ul style="list-style-type: none"> <li>• <b>Accept</b>: */*</li> <li>• <b>Content-Type</b>: application/json;charset=UTF-8</li> </ul>

Table 17.88: Format of the call to create an assignment rule

**Response**

JSON object field	Description
<b>id</b>	ID of the assignment rule.
<b>caseId</b>	ID of the investigation that receives the indicators that meet the conditions set in the assignment rule.

JSON object field	Description
<b>caseName</b>	Name of the investigation that receives the indicators that meet the conditions set in the assignment rule.
<b>modified</b>	Date the assignment rule was last modified.
<b>created</b>	Date the assignment rule was created.
<b>isRegexDetails</b>	Boolean value indicating whether the assignment rule <b>details</b> field contains a regular expression (True) or plain text (False).
<b>isDeleted</b>	Not used.
<b>description</b>	Description of the assignment rule.
<b>details</b>	Contents of the indicator <b>Details</b> field.
<b>huntingRule</b>	ID of the hunting rule that generated the indicator.
<b>machineNames</b>	List with the names of the computers associated with the indicators.
<b>muids</b>	List with the IDs of the computers associated with the indicators.
<b>name</b>	Name of the assignment rule.
<b>pandaClientIds</b>	List with the IDs of the clients associated with the indicator.
<b>detailsFromTrigger</b>	Contents of the <b>Details</b> field in the original indicator used as the template to create the assignment rule.

Table 17.89: Response JSON object to a request to create an assignment rule

## Edit Indicator Assignment Rules

Changes the conditions that describe the indicators that are moved to an existing investigation.

Request	
Command	PUT
URL	/api/v1/alerts/triggers/automation-rules/{id}
Required parameters in the URL	<ul style="list-style-type: none"> <li>• <b>id</b>: ID of the assignment rule you want to edit.</li> </ul>
Required parameters in the HTTP message body	<p>JSON object with the parameters that describe the new characteristics of the indicators you want to move to the chosen investigation:</p> <ul style="list-style-type: none"> <li>• <b>caseId</b>: ID of the investigation that receives the indicators that meet the conditions set in the assignment rule.</li> <li>• <b>isRegexDetails</b>: Boolean value indicating whether the assignment rule <b>details</b> field contains a regular expression (True) or plain text (False).</li> <li>• <b>description</b>: Description of the assignment rule.</li> <li>• <b>details</b>: Contents of the indicator <b>Details</b> field.</li> <li>• <b>huntingRule</b>: ID of the hunting rule that generated the indicator.</li> <li>• <b>machineNames</b>: List with the names of the computers associated with the indicators.</li> <li>• <b>muids</b>: List with the IDs of the computers associated with the indicators.</li> <li>• <b>name</b>: Name of the assignment rule.</li> <li>• <b>pandaClientIds</b>: List with the IDs of the clients associated with the indicator.</li> <li>• <b>detailsFromTrigger</b>: Regular expression associated with the content of the indicator <b>Details</b> field.</li> </ul>
Headers	<ul style="list-style-type: none"> <li>• <b>Accept</b>: */*</li> <li>• <b>Content-Type</b>: application/json;charset=UTF-8</li> </ul>

Table 17.90: Format of the call to edit an assignment rule



**Response**

<b>JSON object field</b>	<b>Description</b>
<b>id</b>	ID of the assignment rule.
<b>caseId</b>	ID of the investigation that receives the indicators that meet the conditions set in the assignment rule.
<b>caseName</b>	Name of the investigation that receives the indicators that meet the conditions set in the assignment rule.
<b>modified</b>	Date the assignment rule was last modified.
<b>created</b>	Date the assignment rule was created.
<b>isRegexDetails</b>	Boolean value indicating whether the assignment rule <b>details</b> field contains a regular expression (True) or plain text (False).
<b>isDeleted</b>	Not used.
<b>description</b>	Description of the assignment rule.
<b>details</b>	Contents of the indicator <b>Details</b> field.
<b>huntingRule</b>	ID of the hunting rule that generated the indicator.
<b>machineNames</b>	List with the names of the computers associated with the indicators.
<b>muids</b>	List with the IDs of the computers associated with the indicators.
<b>name</b>	Name of the assignment rule.
<b>pandaClientIds</b>	List with the IDs of the clients associated with the indicator.
<b>detailsFromTrigger</b>	Contents of the <b>Details</b> field in the original indicator used as the template to create the assignment rule.

Table 17.91: Response JSON object to a request to edit an assignment rule

## Delete Indicator Assignment Rules

Deletes assignment rules.

### Request

Command	DELETE
URL	/api/v1/alerts/triggers/automation-rules
Required parameters in the HTTP message body	<p>JSON object with parameters that include the IDs of the assignment rules you want to delete:</p> <ul style="list-style-type: none"> <li>• <b>id</b>: List with the IDs of the assignment rules you want to delete.</li> </ul>
Headers	<ul style="list-style-type: none"> <li>• <b>Accept</b>: */*</li> </ul>

Table 17.92: Format of the call to delete assignment rules

### Response

HTTP status code: 200. Empty response.

## Run Indicator Assignment Rules

Applies an existing assignment rule to the indicators created in the previous 7 days.

### Request

Command	POST
URL	/api/v1/alerts/triggers/automation-rules/{id}/retrospective
Required parameters in the URL	<ul style="list-style-type: none"> <li>• <b>caseId</b>: Investigation ID.</li> </ul>
Headers	<ul style="list-style-type: none"> <li>• <b>Accept</b>: */*</li> </ul>

Table 17.93: Format of the call to run an assignment rule

### Response

HTTP status code: 200. Empty response.

## Get the Characteristics of an Assignment Rule

Gets the characteristics of an assignment rule, including the conditions the indicators must meet to be moved to the specified investigation.

### Request

Command	GET
URL	/api/v1/alerts/triggers/automation-rules/{id}
Required parameters in the URL	<ul style="list-style-type: none"> <li>• <b>caseId</b>: Investigation ID.</li> </ul>

**Headers**

- **Accept:** \*/\*

Table 17.94: Format of the call to get the characteristics of an assignment rule

**Response**

JSON object field	Description
<b>id</b>	ID of the assignment rule.
<b>caseId</b>	ID of the investigation that receives the indicators that meet the conditions set in the assignment rule.
<b>caseName</b>	Name of the investigation that receives the indicators that meet the conditions set in the assignment rule.
<b>modified</b>	Date the assignment rule was last modified.
<b>created</b>	Date the assignment rule was created.
<b>isRegexDetails</b>	Boolean value indicating whether the assignment rule <b>details</b> field contains a regular expression (True) or plain text (False).
<b>isDeleted</b>	Not used.
<b>description</b>	Description of the assignment rule.
<b>details</b>	Contents of the indicator <b>Details</b> field.
<b>huntingRule</b>	ID of the hunting rule that generated the indicator.
<b>machineNames</b>	List with the names of the computers associated with the indicators.
<b>muids</b>	List with the IDs of the computers associated with the indicators.
<b>name</b>	Name of the assignment rule.
<b>pandaClientIds</b>	List with the IDs of the clients associated with the indicator.

JSON object field	Description
<b>detailsFromTrigger</b>	Contents of the <b>Details</b> field in the original indicator used as the template to create the assignment rule.

Table 17.95: Response JSON object to a request to get the details of an assignment rule

### Get a List of Indicator Assignment Rules

Gets a list of JSON objects containing the indicator assignment rules created by analysts and their characteristics.

#### Request

<b>Command</b>	GET
<b>URL</b>	/api/v1/alerts/triggers/automation-rules
<b>Headers</b>	<ul style="list-style-type: none"> <li>• <b>Accept:</b> */*</li> </ul>

Table 17.96: Format of the call to get the list of created assignment rules

#### Response

List of JSON objects containing the indicator assignment rules created and their characteristics.

JSON object field	Description
<b>id</b>	ID of the assignment rule.
<b>caseId</b>	ID of the investigation that receives the indicators that meet the conditions set in the assignment rule.
<b>caseName</b>	Name of the investigation that receives the indicators that meet the conditions set in the assignment rule.
<b>modified</b>	Date the assignment rule was last modified.
<b>created</b>	Date the assignment rule was created.
<b>isRegexDetails</b>	Boolean value indicating whether the assignment rule <b>details</b> field contains a regular expression (True) or plain text (False).
<b>isDeleted</b>	Not used.
<b>description</b>	Description of the assignment rule.

JSON object field	Description
<b>details</b>	Contents of the indicator <b>Details</b> field.
<b>huntingRule</b>	ID of the hunting rule that generated the indicator.
<b>machineNames</b>	List with the names of the computers associated with the indicators.
<b>muids</b>	List with the IDs of the computers associated with the indicators.
<b>name</b>	Name of the assignment rule.
<b>pandaClientIds</b>	List with the IDs of the clients associated with the indicator.
<b>detailsFromTrigger</b>	Contents of the <b>Details</b> field in the original indicator used as the template to create the assignment rule.

Table 17.97: Response JSON object to a request to list the assignment rules created

## Format of the Events Used in Cytomic Orion

To generate effective analysis and response processes in the face of detected incidents, SOC technicians require accurate information about the status of the IT infrastructure they investigate.

Cytomic EDR and Cytomic EPDR monitor the processes that run on clients' computers and send the generated telemetry data to the Cytomic cloud. All this information is stored in the data lake hosted in the Cytomic cloud, where it is available to analysts through a variety of tools included in Cytomic Orion.

Telemetry data is stored in the data lake in a structured format called 'event', which consists of several fields. Analysts need to understand the meaning of each of these fields to correctly interpret the logged information.

### CHAPTER CONTENTS

---

<b>Fields in the Events Received by Cytomic Orion</b> .....	<b>375</b>
---	------------

An event is a record that consists of fields that describe an action taken by a process on a computer. Each type of event includes a specific number of fields.

Cytomic Orion presents the event flow in multiple ways in the analyst console:

- **Table:** All events of the same type are stored in a table that you can query using SQL statements. For more information, see [Advanced SQL Query Module](#) on page 145.
- **List:** You can see the content of the event fields directly in the investigation console, where a list can contain events of multiple types in chronological order. For more information see [Indicator Analysis Using the Investigation Console](#) on page 172.
- **Graphs:** The event information is used to build graphs that help analysts interpret the process execution sequence and the relationships established between the actors involved in a cyberattack.
- **Searches:** Event information is shown in assisted investigations to show results and create new searches that guide analysts through the investigation. See [Assisted Investigations](#) on page 160.

## Fields in the Events Received by Cytomic Orion

This table lists all the fields included in the events stored by Cytomic Orion along with their meaning, data types, and possible values in the case of enumerations.

Field	Description	Field Type
<b>accountid</b>	Client ID.	Character string
<b>accesstype</b>	<p>File access mask:</p> <ul style="list-style-type: none"> <li>• <b>(54) WMI_CREATEPROC</b>: Local WMI.</li> </ul> <p>For all other operations:</p> <ul style="list-style-type: none"> <li>• <a href="https://docs.microsoft.com/en-us/windows/win32/secauthz/access-mask">https://docs.microsoft.com/en-us/windows/win32/secauthz/access-mask</a></li> <li>• <a href="https://docs.microsoft.com/en-us/windows/win32/fileio/file-access-rights-constants">https://docs.microsoft.com/en-us/windows/win32/fileio/file-access-rights-constants</a></li> <li>• <a href="https://docs.microsoft.com/en-us/windows/win32/fileio/file-security-and-access-rights">https://docs.microsoft.com/en-us/windows/win32/fileio/file-security-and-access-rights</a></li> </ul>	Bitmask
<b>accnube</b>	The agent installed on the client's computer can access the Cytomic cloud.	Boolean
<b>action</b>	<p>Type of action taken by the Cytomic EDR or Cytomic EPDR agent, by the user, or by the affected process:</p> <ul style="list-style-type: none"> <li>• <b>0 (Allow)</b>: The agent allowed the process to run.</li> <li>• <b>1 (Block)</b>: The agent blocked the process from running.</li> <li>• <b>2 (BlockTimeout)</b>: The agent displayed a pop-up message to the user but the user did not respond in time.</li> <li>• <b>3 (AllowWL)</b>: The agent allowed the process to run because it is on the local goodwill allowlist.</li> </ul>	Enumeration

Field	Description	Field Type
	<ul style="list-style-type: none"> <li>• <b>4 (BlockBL)</b>: The agent blocked the process from running because it is on the local malware blocklist.</li> <li>• <b>5 (Disinfect)</b>: The agent disinfected the process.</li> <li>• <b>6 (Delete)</b>: The agent classified the process as malware and deleted it because it could not be disinfected.</li> <li>• <b>7 (Quarantine)</b>: The agent classified the process as malware and moved it to quarantine folder on the computer.</li> <li>• <b>8 (AllowByUser)</b>: The agent displayed a pop-up message to the user and the user responded with 'Allow execution'.</li> <li>• <b>9 (Informed)</b>: The agent displayed a pop-up message to the user.</li> <li>• <b>10 (Unquarantine)</b>: The agent removed the file from the quarantine folder.</li> <li>• <b>11 (Rename)</b>: The agent renamed the file. This action is used only for testing.</li> <li>• <b>12 (BlockURL)</b>: The agent blocked the URL.</li> <li>• <b>13 (KillProcess)</b>: The agent closed the process.</li> <li>• <b>14 (BlockExploit)</b>: The agent stopped an attempt to exploit a vulnerable process.</li> <li>• <b>15 (ExploitAllowByUser)</b>: The user did not allow the exploited process to be closed.</li> <li>• <b>16 (RebootNeeded)</b>: The agent requires that the computer be rebooted to block the exploit attempt.</li> <li>• <b>17 (ExploitInformed)</b>: The agent displayed a pop-up message to the user, reporting an attempt to exploit a</li> </ul>	



Field	Description	Field Type
	<p>vulnerable process.</p> <ul style="list-style-type: none"> <li>• <b>18 (AllowSonGWInstaller)</b>: The agent allowed the process to run because it belongs to an installation package classified as goodware.</li> <li>• <b>19 (EmbebedInformed)</b>: The agent sent internal operation information to the cloud to improve detection routines.</li> <li>• <b>21 (SuspendProcess)</b>: The monitored process tried to suspend the antivirus service.</li> <li>• <b>22 (ModifyDiskResource)</b>: The monitored process tried to modify a resource protected by the agent shield.</li> <li>• <b>23 (ModifyRegistry)</b>: The monitored process tried to modify a registry key protected by the agent shield.</li> <li>• <b>24 (RenameRegistry)</b>: The monitored process tried to rename a registry key protected by the agent shield.</li> <li>• <b>25 (ModifyMarkFile)</b>: The monitored process tried to modify a file protected by the agent shield.</li> <li>• <b>26 (UncertainAction)</b>: Error monitoring the process operation.</li> <li>• <b>28 (AllowFGW)</b>: The agent allowed the operation performed by the monitored process because it is on the local goodware allowlist.</li> <li>• <b>29 (AllowSWAuthorized)</b>: The agent allowed the operation performed by the monitored process because the administrator marked the file as authorized software.</li> <li>• <b>30 (InformNewPE)</b>: The agent reported the appearance of a new file on the</li> </ul>	

Field	Description	Field Type
	<p>computer because the Drag and Drop feature is turned on in Cytomic Data Watch.</p> <ul style="list-style-type: none"> <li>• <b>31 (ExploitAllowByAdmin):</b> The agent allowed the operation performed by the monitored process because the network administrator excluded the exploit.</li> <li>• <b>32 (IPBlocked):</b> The agent blocked IPs to mitigate an RDP (Remote Desktop Protocol) attack.</li> <li>• <b>33 (AllowSonMsiGW):</b> The file is allowed to run because it is from a signed installer.</li> <li>• <b>34 (IsolateHost):</b> Isolates a computer through a command from the management console.</li> <li>• <b>35 (RDPOff):</b> Ends the isolation that was in response to an RDP attack.</li> <li>• <b>36 (UNisolateHost):</b> Ends the isolation of a computer through a command from the management console.</li> <li>• <b>37 (Allowed by Global Audit):</b> The item is allowed because the security software is configured in Audit mode.</li> </ul>	
<b>actiontype</b>	<p>Indicates the session type:</p> <ul style="list-style-type: none"> <li>• <b>0 (Login):</b> Login on the client's computer.</li> <li>• <b>1 (Logout):</b> Logout on the client's computer.</li> <li>• <b>-1 (Unknown):</b> Unable to determine session type.</li> </ul>	Enumeration
<b>advancedrulesconf</b>	Cytomic EDR or Cytomic EPDR advanced security policy settings.	Character string
<b>age</b>	Date the file was last modified.	Date

Field	Description	Field Type
<b>alrtdatetime</b>	UTC date when the event that triggered the indicator occurred on the client's computer. Information regarding the time is included. To understand this field, see <a href="#">pandatimestatus</a> .	Date
<b>alprotocoldetected</b>	Application level protocol detected in the connection or one of these values: <ul style="list-style-type: none"> <li>• <b>0 (NNS_AL_PROTOCOL_UNKNOWN):</b> Could not determine the protocol.</li> <li>• <b>1 (NNS_AL_PROTOCOL_PENDING):</b> Analyzing the application protocol to determine the type.</li> </ul>	Enumeration
<b>alprotocolexpected</b>	Application level protocol expected according to the connection port or one of these values: <ul style="list-style-type: none"> <li>• <b>0 (NNS_AL_PROTOCOL_UNKNOWN):</b> Could not determine the protocol.</li> <li>• <b>1 (NNS_AL_PROTOCOL_PENDING):</b> Analyzing the application protocol to determine the type.</li> </ul>	Enumeration
<b>analysistime</b>	Time elapsed analyzing the file.	Character string
<b>attackerDeviceId</b>	Identifier of the device that connected to a computer protected by Endpoint Access Enforcement.	Character string
<b>blockreason</b>	Reason for the pop-up message displayed on the computer: <ul style="list-style-type: none"> <li>• <b>0:</b> The file was blocked because it is unknown and the Cytomic EPDR or Cytomic EDR advanced protection mode is set to Hardening or Lock.</li> <li>• <b>1:</b> The file was blocked by local rules.</li> <li>• <b>2:</b> The file was blocked because the</li> </ul>	Enumeration

Field	Description	Field Type
	<p>source is untrusted.</p> <ul style="list-style-type: none"> <li>• <b>3</b>: The file was blocked by a context rule.</li> <li>• <b>4</b>: The file was blocked because it is an exploit.</li> <li>• <b>5</b>: The file was blocked after asking the user to close the process.</li> <li>• <b>6</b>: Malware was blocked on Linux / macOS.</li> </ul>	
<b>bytesreceived</b>	Total bytes received by the monitored process.	Numeric value
<b>bytessent</b>	Total bytes sent by the monitored process.	Numeric value
<b>callstack</b>	See <a href="#">childfilesize</a> .	Numeric value
<b>childattributes</b>	<p>Attributes of the child process:</p> <ul style="list-style-type: none"> <li>• <b>0x0000000000000001 (ISINSTALLER)</b>: Self-extracting (SFX) file.</li> <li>• <b>0x0000000000000002 (ISDRIVER)</b>: Driver-type file.</li> <li>• <b>0x0000000000000008 (ISRESOURCESDLL)</b>: Resource DLL-type file.</li> <li>• <b>0x0000000000000010 (EXTERNAL)</b>: File from outside the computer.</li> <li>• <b>0x0000000000000020 (ISFRESHUNK)</b>: File recently added to the Cytomic knowledge base.</li> <li>• <b>0x0000000000000040 (ISDISSINFECTABLE)</b>: File for which there is a recommended disinfection action.</li> <li>• <b>0x0000000000000080 (DETEVENT_DISCARD)</b>: The event-based context detection technology did not detect</li> </ul>	Enumeration

Field	Description	Field Type
	<p>anything suspicious.</p> <ul style="list-style-type: none"> <li>• <b>0x0000000000000100 (WAITED_FOR_VINDEX):</b> Execution of a file whose creation had not been registered.</li> <li>• <b>0x0000000000000200 (ISACTIONSEND):</b> The local technologies did not detect malware in the file and it was sent to Cytomic for classification.</li> <li>• <b>0x0000000000000400 (ISLANSHARED):</b> File stored on a network drive.</li> <li>• <b>0x0000000000000800 (USERALLOWUNK):</b> File with permission to import unknown DLLs.</li> <li>• <b>0x0000000000001000 (ISSESSIONREMOTE):</b> Event originating from a remote session.</li> <li>• <b>0x0000000000002000 (LOADLIB_TIMEOUT):</b> The time elapsed between when the protection intercepted the loading of the library and when it was scanned exceeded 1 second. As a result, the scan changed from synchronous to asynchronous to avoid impacting performance.</li> <li>• <b>0x0000000000004000 (ISPE):</b> Executable file.</li> <li>• <b>0x0000000000008000 (ISNOPE):</b> Non-executable file.</li> <li>• <b>0x0000000000020000 (NOSHELL):</b> The agent did not detect the execution of a shell command on the system.</li> <li>• <b>0x0000000000080000 (ISNETNATIVE):</b> NET Native file.</li> <li>• <b>0x0000000000100000 (ISSERIALIZER):</b></li> </ul>	

Field	Description	Field Type
	<p>Serializer file.</p> <ul style="list-style-type: none"> <li>• <b>0x000000000200000 (PANDEX):</b> File included in the list of processes created by Cytomic Patch.</li> <li>• <b>0x000000000400000 (SONOFGWINSTALLER):</b> File created by an installer classified as goodware.</li> <li>• <b>0x000000000800000 (PROCESS_EXCLUDED):</b> File not scanned because of the Cytomic Orion exclusions.</li> <li>• <b>0x000000001000000 (INTERCEPTION_TXF):</b> The intercepted operation was originated by an executable whose image on the disk is being modified.</li> <li>• <b>0x000000002000000 (HASMACROS):</b> Microsoft Office document with macros.</li> <li>• <b>0x000000000800000 (ISPEARM):</b> Executable file for ARM microprocessors.</li> <li>• <b>0x000000001000000 (ISDYNFILTERED):</b> The file was allowed on the computer because there are no technologies to classify it.</li> <li>• <b>0x000000002000000 (ISDISINFECTED):</b> The file was disinfected.</li> <li>• <b>0x000000004000000 (PROCESSLOST):</b> The operation was not logged.</li> <li>• <b>0x000000008000000 (OPERATION_LOST):</b> Operation with a pre-scan report for which the post-scan report has not been received yet.</li> <li>• <b>0x0000002000000000 (SAFE_BOOT_MODE):</b> The computer started in Safe Mode.</li> </ul>	

Field	Description	Field Type
	<ul style="list-style-type: none"> <li>• <b>0x0000004000000000 (PANDA_SIGNED)</b>: File signed by Panda Security.</li> </ul>	
<b>childattmask</b>	See <b>childattributes</b> .	
<b>childblake</b>	Blake2 signature of the child file.	Character string
<b>childclassification</b>	<p>Classification of the child process that performed the logged action.</p> <ul style="list-style-type: none"> <li>• <b>0 (Unknown)</b>: File in the process of classification.</li> <li>• <b>1 (Goodware)</b>: File classified as goodware.</li> <li>• <b>2 (Malware)</b>: File classified as malware.</li> <li>• <b>3 (Suspect)</b>: The file is in the process of classification and it is highly likely to be malware.</li> <li>• <b>4 (Compromised)</b>: Process compromised by an exploit attack.</li> <li>• <b>5 (GWNotConfirmed)</b>: The file is in the process of classification and it is highly likely to be malware.</li> <li>• <b>6 (Pup)</b>: File classified as an unwanted program.</li> <li>• <b>7 (GwUnwanted)</b>: Equivalent to PUP.</li> <li>• <b>8 (GwRanked)</b>: Process classified as goodware.</li> <li>• <b>-1 (Unknown)</b></li> </ul>	Enumeration
<b>childdrive</b>		
<b>childfilename</b>	Child process name.	Character string
<b>childfilesize</b>	Size of the child file logged by the agent.	Numeric value

Field	Description	Field Type
<b>childfiletime</b>	Date of the child file logged by the agent.	Date
<b>childfirstseen</b>	Date the file was first seen.	Date
<b>childmd5</b>	Child file hash.	Character string
<b>childpath</b>	Path of the child file that performed the logged operation.	Character string
<b>ChildPID</b>	Child process ID.	Numeric value
<b>childsha256</b>	SHA256 signature of the child process that performed the operation.	Character string
<b>childstatus</b>	<p>Child process status.</p> <ul style="list-style-type: none"> <li>• <b>0 (StatusOk)</b>: Status OK.</li> <li>• <b>1 (NotFound)</b>: Item not found.</li> <li>• <b>2 (UnexpectedError)</b>: Unknown error.</li> <li>• <b>3 (StaticFiltered)</b>: File identified as malware using static information contained in the Cytomic EDR or Cytomic EPDR protection.</li> <li>• <b>4 (DynamicFiltered)</b>: File identified as malware using local technology implemented in Cytomic EDR or Cytomic EPDR.</li> <li>• <b>5 (FileIsTooBig)</b>: File too big.</li> <li>• <b>6 (PEUploadNotAllowed)</b>: File send was disabled.</li> <li>• <b>11 (FileWasUploaded)</b>: File sent to the cloud for analysis.</li> <li>• <b>12 (FiletypeFiltered)</b>: Resource DLL, NET Native, or Serializer-type file.</li> <li>• <b>13 (NotUploadGWLocal)</b>: Goodware file not saved to the cloud.</li> <li>• <b>14 (NotUploadMWdisinfect)</b>: Disinfected</li> </ul>	Enumeration



Field	Description	Field Type
	malware file not saved to the cloud.	
<b>childurl</b>	File download URL. See <a href="#">url</a> .	Character string
<b>ciphertype</b>	Scan of the SSL/TLS protocol and its HTTPS characteristics (for example TLS_RSA_WITH_AES_128_GCM_SHA256).	Character string
<b>classname</b>	Type of device where the process resides. It corresponds to the class specified in the .INF file associated with the device.	Character string
<b>commandline</b>	Command line configured as a task to be run through WMI.	Character string
<b>confadvancedrules</b>	See <a href="#">advancedrulesconf</a> .	Character string
<b>configservicelevel</b>	Agent execution mode configuration. This can be temporarily different from the execution mode in progress. See <a href="#">servicelevel</a>	Enumeration
<b>configstring</b>	See <a href="#">extendedinfo</a> .	Character string
<b>connectionstate</b>	Connection status notified. <ul style="list-style-type: none"> <li>• <b>0 (E_NNS_CONNECTION_STATE_UNKNOWN)</b>: Unknown connection status.</li> <li>• <b>1 (E_NNS_CONNECTION_STATE_ESTABLISHED)</b>: Connection established.</li> <li>• <b>2 (E_NNS_CONNECTION_STATE_FAILED)</b>: Failed connection attempt.</li> <li>• <b>3 (E_NNS_CONNECTION_STATE_DENIED_BY_FW)</b>: Connection denied by the firewall or other security software</li> </ul>	Enumeration

Field	Description	Field Type
	technology.	
<b>contentencoding</b>	Encoding used in the content of the HTTP connection.  See <a href="https://www.iana.org/assignments/http-parameters/http-parameters.xml">https://www.iana.org/assignments/http-parameters/http-parameters.xml</a>	Character string
<b>copy</b>	Name of the service that triggered the event.	Character string
<b>datacontainer</b>	Unique name of the object within the WMI hierarchy.	Character string
<b>date</b>	UTC date when the event occurred on the client's computer. No information regarding the time is included. To understand this field, see <a href="#">pandatetimestatus</a> .	Numeric value
<b>datetime</b>	UTC date when the event occurred on the client's computer. Information regarding the time is included. To understand this field, see <a href="#">pandatetimestatus</a> .	Numeric value
<b>description</b>	See <a href="#">extendedinfo</a> .	Character string
<b>destinationip</b>	IP address of the target computer in a network connection scanned by Network Attack Protection.	IP address
<b>destinationport</b>	Port of the target computer in a network connection scanned by Network Attack Protection.	Numeric value
<b>details</b>	Summary in the form of a group of relevant fields from the event.  <b>eventtype 1 (ProcessOps)</b>  Contains the <a href="#">commandline</a> field.  <b>eventtype 14 (Download)</b>	Character string

Field	Description	Field Type
	<p>Contains the <b>url</b> field.</p> <p><b>eventtype 22 (NetworkOps)</b></p> <p>Contains the <b>direction</b>, <b>ipv4status</b>, <b>protocol</b>, and <b>remoteport</b> fields.</p> <p><b>eventtype 27 (RegistryOps)</b></p> <p>Contains the <b>valuedata</b> field.</p> <p><b>eventtype 31 (ScriptLaunch)</b></p> <p>Contains the <b>commandline</b> field.</p> <p><b>eventtype 46 (DnsOps)</b></p> <p>Contains the <b>domainlist</b> field.</p> <p><b>eventtype 47 (DeviceOps)</b></p> <p>Contains the <b>devicetype</b> field.</p> <p><b>eventtype 50 (UserNotification)</b></p> <p>Contains the <b>parentfilename</b> field.</p> <p><b>eventtype 52 (LoginOutOp)</b></p> <p>Contains the <b>eventtype</b>, <b>sessiontype</b>, <b>loggeduser</b>, <b>remotemachinename</b>, and <b>remoteip</b> fields.</p> <p><b>eventtype 99 (RemediationOps)</b></p> <p>Contains the <b>remoteip</b>, <b>remotemachinename</b>, <b>commandline</b>, and <b>detectionid</b> fields.</p> <p><b>eventtype 555 (IOA)</b></p> <p>Contains the <b>extendedinfo</b> field.</p>	
<b>detectionid</b>	Unique identifier of the detection.	Character string
<b>deviceid</b>	See <b>attackerDeviceid</b> .	Numeric value
<b>devicetype</b>	<p>Type of drive where the process or file that triggered the operation resides.</p> <ul style="list-style-type: none"> <li>• <b>0 (UNKNOWN)</b>: Unknown.</li> <li>• <b>1 (CD_DVD)</b>: CD or DVD drive.</li> </ul>	Enumeration

Field	Description	Field Type
	<ul style="list-style-type: none"> <li>• <b>2 (USB_STORAGE)</b>: USB storage device.</li> <li>• <b>3 (IMAGE)</b>: Image file.</li> <li>• <b>4 (BLUETOOTH)</b>: Bluetooth device.</li> <li>• <b>5 (MODEM)</b>: Modem.</li> <li>• <b>6 (USB_PRINTER)</b>: USB printer.</li> <li>• <b>7 (PHONE)</b>: Mobile phone.</li> <li>• <b>8 (KEYBOARD)</b>: Keyboard.</li> <li>• <b>9 (HID)</b>: Mouse.</li> </ul>	
<p><b>direction</b></p>	<p><b>eventtype 22 (NetworkOps):</b> Network connection direction.</p> <ul style="list-style-type: none"> <li>• <b>0 (UnKnown)</b>: Unknown.</li> <li>• <b>1 (Incoming)</b>: Connection established from outside the network to a computer on the client's network.</li> <li>• <b>2 (Outgoing)</b>: Connection established from a computer on the client's network to a computer outside the network.</li> <li>• <b>3 (Bidirectional)</b>: Bidirectional.</li> </ul> <p><b>eventtype 99 (RemediationOps) - napdirection</b> Network connection direction.</p> <ul style="list-style-type: none"> <li>• <b>0 (UnKnown)</b>: Unknown.</li> <li>• <b>1 (Incoming)</b>: Connection established from outside the network to a computer on the client's network.</li> <li>• <b>2 (Outgoing)</b>: Connection established from a computer on the client's network to a computer outside the network.</li> <li>• <b>3 (Bidirectional)</b>: Bidirectional.</li> </ul>	<p>Enumeration</p>
<p><b>domainlist</b></p>	<p>See <a href="#">list</a>.</p>	

Field	Description	Field Type
<b>entropy</b>	Entropy of the POST message content to classify the likelihood of data theft and extraction.	Character string
<b>entropia</b>	See <b>entropy</b> .	Numeric value
<b>errorcode</b>	<p>Error code returned by the operating system when there is a failed login attempt.</p> <ul style="list-style-type: none"> <li>• <b>1073741724 (Invalid username)</b>: The user name does not exist.</li> <li>• <b>1073741730 (Login server is unavailable)</b>: The server required to validate the login is not available.</li> <li>• <b>1073741718 (Invalid password)</b>: The user name is correct but the password is incorrect.</li> <li>• <b>1073741715 (Invalid username or authentication info)</b>: The user name or the authentication information is wrong.</li> <li>• <b>1073741714 (Invalid username or password)</b>: Unknown user name or wrong password.</li> <li>• <b>1073741260 (Account blocked)</b>: Access blocked.</li> <li>• <b>1073741710 (Account disabled)</b>: Account disabled.</li> <li>• <b>1073741713 (User account day restriction)</b>: An attempt was made to log in at a restricted time.</li> <li>• <b>1073741712 (Invalid workstation for login)</b>: An attempt was made to log in from an unauthorized computer.</li> <li>• <b>1073741604 (Sam server is invalid)</b>: The validation server has failed. Cannot perform operation.</li> <li>• <b>1073741421 (Account expired)</b>: The</li> </ul>	Enumeration

Field	Description	Field Type
	<p>account has expired.</p> <ul style="list-style-type: none"> <li>• <b>1073741711 (Password expired)</b>: The password has expired.</li> <li>• <b>1073741517 (Clock difference is too big)</b>: The connected computers' clocks are too far out of sync.</li> <li>• <b>1073741276 (Password change required on reboot)</b>: The user password must be changed on next boot.</li> <li>• <b>1073741275 (Windows error (no risk))</b>: A bug in Windows and not a risk.</li> <li>• <b>1073741428 (Domains trust failed)</b>: The login request failed because the trust relationship between the primary domain and the trusted domain failed.</li> <li>• <b>1073741422 (Netlogon not initialized)</b>: An attempt was made to log in, but the Netlogon service was not started.</li> <li>• <b>1073741074 (Session start error)</b>: An error occurred during login.</li> <li>• <b>1073740781 (Firewall protected)</b>: The computer you are logging in to is protected by an authentication firewall. The specified account is not allowed to authenticate to the machine.</li> <li>• <b>1073741477 (Invalid permission)</b>: The user has requested a type of login that has not been granted.</li> </ul>	
<b>errorevent</b>	See <a href="#">extendedinfo</a> .	Character string
<b>errorstring</b>	See <a href="#">extendedinfo</a> .	Character string
<b>eventtype</b>	<p>Event type logged by the agent.</p> <ul style="list-style-type: none"> <li>• <b>1 (ProcessOps)</b>: The process performed operations on the computer hard disk.</li> </ul>	Enumeration

Field	Description	Field Type
	<ul style="list-style-type: none"> <li>• <b>14 (Download):</b> The process downloaded data.</li> <li>• <b>15 HostsFileModification:</b> The process modified the Hosts file on Windows systems.</li> <li>• <b>22 (NetworkOps):</b> The process performed network operations.</li> <li>• <b>25 EventNotBlocked:</b> The item was not blocked because the computer was starting up.</li> <li>• <b>26 (DataAccess):</b> The process accessed data files hosted on internal mass-storage devices.</li> <li>• <b>27 (RegistryOps):</b> The process accessed the Windows Registry.</li> <li>• <b>30 (ScriptOps):</b> Operation performed by a script-type process.</li> <li>• <b>31 (ScriptOps):</b> Operation performed by a script-type process.</li> <li>• <b>40 (Detection):</b> Detection made by Cytomic EDR active protections.</li> <li>• <b>42 (BandwidthUsage):</b> Volume of information handled in each data transfer operation performed by the process.</li> <li>• <b>45 (SystemOps):</b> Operation performed by the Windows operating system WMI engine.</li> <li>• <b>46 (DnsOps):</b> The process accessed the DNS name server.</li> <li>• <b>47 (DeviceOps):</b> The process accessed an external device.</li> <li>• <b>50 (UserNotification):</b> Notification displayed to the user and response (if any).</li> <li>• <b>52 (LoginOutOps):</b> Login or logout</li> </ul>	

Field	Description	Field Type
	<p>operation performed by the user.</p> <ul style="list-style-type: none"> <li>• <b>99 (RemediationOps):</b> Detection, blocking, and disinfection events from the Cytomic EDR or Cytomic EPDR agent.</li> <li>• <b>100 (HeaderEvent):</b> Administrative event with information about the protection software settings and version, as well as computer and client information.</li> <li>• <b>199 (HiddenAction):</b> Detection event that did not trigger an alert.</li> <li>• <b>555 IOA:</b> IOA generation event.</li> </ul>	
<b>evidencedatetime</b>		
<b>exploitorigin</b>	<p>Origin of the process exploit attempt.</p> <ul style="list-style-type: none"> <li>• <b>1 (URL):</b> URL address.</li> <li>• <b>2 (FILE):</b> File.</li> </ul>	Enumeration
<b>extendedinfo</b>	<p><b>eventtype 1 (ProcessOps) - errorstrings:</b></p> <p>Character string with debug information on the security product settings.</p> <p>When the <b>operation</b> field of an event is set to <b>DirCreate</b>, <b>CMOpened</b>, or <b>CMPCreat</b>, the <b>errorstring</b> field acts as an event grouping counter:</p> <p>In any one-hour period, the first 50 events are logged individually. After the limit of 50 events in one hour is reached, additional events of the same type are grouped together and not sent until the first event of the same type is logged in a new hour period. At this point, the grouped event is sent with the <b>errorstring</b> field including both the grouped events and the first 50 events, and the counter is reset.</p> <p><b>eventtype 26 (DataAccess):</b></p>	Character string



Field	Description	Field Type
	<ul style="list-style-type: none"> <li>Version of the MVMF.xml file in use (M0, M1, M2, etc.)</li> </ul> <p><b>eventtype 27 (RegistryOps):</b></p> <ul style="list-style-type: none"> <li>Version of the PSNMVMF.dat file in use (M0, M1, M2, etc.)</li> </ul> <p><b>eventtype 40 (Detection) - infodiscard:</b></p> <p>Quarantine file internal information.</p> <p><b>eventtype 45 (SystemOps):</b></p> <p>Additional information about <b>Type</b> events:</p> <ul style="list-style-type: none"> <li><b>1 (Active script event creation):</b> Name and path of the executed script.</li> <li><b>6 (Add user group):</b> Group SID.</li> <li><b>7 (Delete user group):</b> Group SID.</li> <li><b>8 (User group admin):</b> Group SID.</li> <li><b>9 (User group rdp):</b> Group SID.</li> <li><b>14 (Login attemp):</b> Logon Process field of the Windows event viewer.</li> <li><b>15 (Scheduler tasks):</b> String with details of the task created (LogonProcess, LogonType, LogonAuthType, TaskOperationType).</li> <li><b>16 (Special privileges):</b> LogonType field of the Windows event viewer.</li> <li><b>18 (WFP filter operation):</b> Filter name.</li> </ul> <p><b>eventtype 47 (DeviceOps) - description</b></p> <ul style="list-style-type: none"> <li>Description of the USB device type that performed the operation.</li> </ul> <p><b>eventtype 61 (ErrorEvents):</b></p> <ul style="list-style-type: none"> <li>Raw content of the malformed event when it cannot be parsed.</li> </ul> <p><b>eventtype 99 (RemediationOps) - remediationdata:</b></p>	

Field	Description	Field Type
	<p>String of characters with these fields separated by *:</p> <ul style="list-style-type: none"> <li>• <b>Path</b>: Path and name of the process ended by the security software or sent to quarantine.</li> <li>• <b>InfoDiscard</b>: Quarantine file internal information.</li> </ul> <p><b>eventtype 555 (IOA)</b>: Details of the processes that generated the IOA.</p>	
<b>failedqueries</b>	Number of failed DNS resolution requests sent by the process in the last hour.	Numeric value
<b>firstseen</b>	See <a href="#">childfirstseen</a>	Date
<b>friendlyname</b>	An easily readable device name.	Character string
<b>guidrule</b>	See <a href="#">ruleid</a> .	
<b>headerhttp</b>	<p>HTTP header dump when the security software detects communications that use HTTP tunnels.</p> <p>This field shows information only if the security software Audit mode is enabled.</p>	Character string
<b>hostname</b>	See <a href="#">remotemachinename</a>	Character string
<b>huntingruleid</b>	See <a href="#">ruleid</a> .	Character string
<b>huntingrulemitre</b>	TTPs associated with the hunting rule.	Character string
<b>huntingrulemode</b>	Indicates whether the rule is enabled in the Threat Engine to generate indicators.	Boolean
<b>huntingrulename</b>	Name of the cyberattack radar rule that detected the indicator.	Character string

Field	Description	Field Type
<b>huntingruleseverity</b>	Severity of the impact of the indicator generated by the hunting rule: <ul style="list-style-type: none"> <li>• <b>0</b>: Not set.</li> <li>• <b>1</b>: Critical.</li> <li>• <b>2</b>: High.</li> <li>• <b>3</b>: Medium.</li> <li>• <b>4</b>: Low.</li> <li>• <b>1000</b>: Unknown.</li> </ul>	Enumeration
<b>huntingruletype</b>	Type of hunting rule. <ul style="list-style-type: none"> <li>• <b>1</b>: Rule run in the threat engine.</li> <li>• <b>2</b>: RDP attack detection rule.</li> <li>• <b>3</b>: IOC applied retrospectively to the stored telemetry.</li> <li>• <b>4</b>: IOC applied to the telemetry flow in real time.</li> <li>• <b>5</b>: Rule run on the user computer.</li> </ul>	Enumeration
<b>idname</b>	Device name.	Character string
<b>indicatortimestamp</b>	See <a href="#">ioatimestamp</a> .	Date
<b>infodiscard</b>	See <a href="#">extendedinfo</a> .	Character string
<b>initialdomain</b>	See <a href="#">url</a> .	Character string
<b>insertiondatetime</b>	Date in UTC format at the time the Cytomic Orion servers logged the event sent by the computer. This date is always later than the other dates because the events are queued to be processed.	Date
<b>interactive</b>	Indicates whether the login is an interactive login.	Binary value
<b>IOAId</b>	Indicator ID.	Character string

Field	Description	Field Type
<b>IOAIds</b>	When a sequence of events follows a pattern described in the MITRE matrix, Cytomic Orion creates an indicator (IOA) and adds the indicator ID to all the events related to it.	Numeric value
<b>ioatimestamp</b>	UTC date in epoch format (number of seconds elapsed since 1 January 1970) at the time the last event that triggered the indicator occurred.	Date
<b>ipv4status</b>	IP address type: <ul style="list-style-type: none"> <li>• 0 (Private)</li> <li>• 1 (Public)</li> </ul>	Enumeration
<b>isdestinationipv6</b>		
<b>isdenied</b>	Indicates whether the reported action was denied.	Binary value
<b>islocal</b>	Indicates whether the task was created on the local computer or on a remote computer.	Binary value
<b>islocalipv6</b>	Indicates whether the IP address is IPv6 or IPv4.	Boolean
<b>isremoteipv6</b>	Indicates whether the IP address is IPv6 or IPv4.	Boolean
<b>isessioninteractive</b>	See <a href="#">interactive</a> .	Binary value
<b>key</b>	Affected registry branch or key.	Character string
<b>lastquery</b>	Last query sent to the cloud by the Cytomic EDR or Cytomic EPDR agent.	Date
<b>list</b>	<b>eventtype 46 (DnsOps) - DomainList:</b> <ul style="list-style-type: none"> <li>• List of domains sent by the process to the DNS server for resolution and number of</li> </ul>	Character string

Field	Description	Field Type
	<p>resolutions per domain, with the format {domain_name,number#domain_name,number}.</p> <p><b>eventtype 99 (RemediationOps) - url:</b></p> <ul style="list-style-type: none"> <li>List of 10 URLs obtained from the process monitor in the event of the detection of an exploit.</li> </ul>	
<b>localdatetime</b>	<p>The computer date (in UTC format) at the time the logged event occurred. This date depends on the computer settings. As a result, it can be incorrect.</p>	Date
<b>localip</b>	<p><b>eventtype 22 (NetworkOps) - localip</b></p> <p>Contains the IP address of the computer on which the event was logged, regardless of the connection direction (<b>direction</b> field). See <a href="#">remoteip</a> and <a href="#">direction</a>.</p> <p><b>eventtype 99 (RemediationOps) - naporiginip:</b></p> <p>IP address of the source computer in a network connection scanned by Network Attack Protection.</p>	IP address
<b>localport</b>	<p><b>eventtype 22 (NetworkOps) - localport</b></p> <p>Contains the port of the computer on which the event was logged or of the other end of the connection depending on the <b>direction</b> field:</p> <ul style="list-style-type: none"> <li><b>direction = 1</b> (inbound connection). This contains the port of the other end of the connection.</li> <li><b>direction = 2</b> (outbound connection). This contains the port of the computer on which the event is logged.</li> </ul> <p>See <a href="#">direction</a>.</p>	Numeric value

Field	Description	Field Type
	<p><b>eventtype 99 (RemediationOps) - naporiginport:</b></p> <p>Port of the source computer in a network connection scanned by Network Attack Protection.</p>	
<b>loggeduser</b>	The user that was logged in to the computer at the time the event was generated.	Character string
<b>machinename</b>	Name of the computer that ran the process.	Character string
<b>manufacturer</b>	Device manufacturer.	Character string
<b>method</b>	<p>HTTP connection method when the security software detects communications that use HTTP tunnels.</p> <ul style="list-style-type: none"> <li>• 1 - GET</li> <li>• 2 - POST</li> </ul> <p>This field shows information only if the security software Audit mode is enabled.</p>	Numeric value
<b>MUID</b>	Internal ID of the client's computer.	Character string
<b>napattack</b>	<p>Network attack direction.</p> <ul style="list-style-type: none"> <li>• <b>1:</b> The naporiginip and naporiginport fields contain the IP address and port of the attacking computer.</li> <li>• <b>2:</b> The napdestinationip and napdestinationport fields contain the IP address and port of the attacking computer.</li> </ul>	Numeric value
<b>napdestinationip</b>	See <b>destinationip</b> .	
<b>napdestinationport</b>	See <b>destinationport</b> .	
<b>napdirection</b>	See <b>direction</b> .	

Field	Description	Field Type
<b>napoccurrences</b>	See <b>times</b> .	
<b>naporiginip</b>	See <b>localip</b> .	
<b>naporiginport</b>	See <b>localport</b> .	
<b>notificationtype</b>	Internal use.	Character string
<b>numcacheclassifiedelements</b>	Number of items whose classification is cached in the security software.	Numeric value
<b>objectname</b>	See <b>datacontainer</b> .	
<b>occurrences</b>	Number of grouped indicators. See <b>Indicator Grouping</b> on page 68	Numeric value
<b>opstatus</b>	<ul style="list-style-type: none"> <li>• <b>0</b>: Send to the Advanced Reporting Tool.</li> <li>• <b>2</b>: Do not send to the Advanced Reporting Tool.</li> </ul>	Enumeration
<b>opentstamp</b>	Date of the WMI notification for WMI_CREATEPROC (54) events.	Bitmask
<b>opentimestamp</b>		
<b>operation</b>	<p><b>eventtype 1 (ProcessOps)</b></p> <p>Type of operation performed by the process.</p> <ul style="list-style-type: none"> <li>• <b>0 (CreateProc)</b>: Process created.</li> <li>• <b>1 (PECreat)</b>: Executable program created.</li> <li>• <b>2 (PEModif)</b>: Executable program modified.</li> <li>• <b>3 (LibraryLoad)</b>: Library loaded.</li> <li>• <b>4 (SvcInst)</b>: Service installed.</li> <li>• <b>5 (PEMapWrite)</b>: Executable program mapped for write access.</li> </ul>	Enumeration

Field	Description	Field Type
	<ul style="list-style-type: none"> <li>• <b>6 (PEDelet)</b>: Executable program deleted.</li> <li>• <b>7 (PERenam)</b>: Executable program renamed.</li> <li>• <b>8 (DirCreate)</b>: Folder created.</li> <li>• <b>9 (CMPCreat)</b>: Compressed file created.</li> <li>• <b>10 (CMOpened)</b>: Compressed file opened.</li> <li>• <b>11 (RegKExeCreat)</b>: A registry branch that points to an executable file was created.</li> <li>• <b>12 (RegKExeModif)</b>: A registry branch was modified, which now points to an executable file.</li> <li>• <b>15 (PENeverSeen)</b>: Executable program never seen before by Cytomic Orion.</li> <li>• <b>17 (RemoteThreadCreated)</b>: Remote thread created.</li> <li>• <b>18 (ProcessKilled)</b>: Process killed.</li> <li>• <b>25 (SamAccess)</b>: Access to the computer SAM.</li> <li>• <b>30 (ExploitSniffer)</b>: Sniffing exploit technique detected.</li> <li>• <b>31 (ExploitWSAStartup)</b>: WSAStartup exploit technique detected.</li> <li>• <b>32 (ExploitInternetReadFile)</b>: InternetReadFile exploit technique detected.</li> <li>• <b>34 (ExploitCMD)</b>: CMD exploit technique detected.</li> <li>• <b>39 (Load16bitsFilesByNtvm.exe)</b>: 16-bit file loaded by ntvdm.exe.</li> <li>• <b>43 (Heuhooks)</b>: Anti-exploit technology detected.</li> <li>• <b>54 (Create process by WMI)</b>: Process</li> </ul>	



Field	Description	Field Type
	<p>created by a modified WMI.</p> <ul style="list-style-type: none"> <li>• <b>55 (AttackProduct)</b>: Attack detected on the agent service, a file, or registry key.</li> <li>• <b>61 (OpenProcess LSASS)</b>: LSASS process opened.</li> <li>• <b>89 (LoadDrvVulnerable)</b>: A process loaded a vulnerable driver after the operating system started up.</li> <li>• <b>200 (MitreReadComplete)</b>: MITRE event that indicates a file was read.</li> <li>• <b>201 (MitreCreateFile)</b>: MITRE event that indicates a file was created.</li> <li>• <b>202 (MitreModifyFile)</b>: MITRE event that indicates a file was modified.</li> <li>• <b>207 (LoadDriver)</b>: MITRE event that indicates a driver was loaded.</li> <li>• <b>208 (NopeDelete)</b>: MITRE event that indicates a non-executable file was deleted.</li> </ul> <p><b>eventtype 45 (SystemOps) - type</b></p> <p>Type of WMI operation performed by the process.</p> <ul style="list-style-type: none"> <li>• <b>0 (Command line event creation)</b>: WMI launched a command line in response to a change in the database.</li> <li>• <b>1 (Active script event creation)</b>: A script was run in response to receiving an event.</li> <li>• <b>2 (Event consumer to filter consumer)</b>: This event is generated whenever a process subscribes to receive notifications. The name of the created filter is received.</li> <li>• <b>3 (Event consumer to filter query)</b>: This event is generated whenever a process</li> </ul>	

Field	Description	Field Type
	<p>subscribes to receive notifications. The query run by the process to subscribe is received.</p> <ul style="list-style-type: none"> <li>• <b>4 (Create User):</b> A user account was added to the operating system.</li> <li>• <b>5 (Delete User):</b> A user account was deleted from the operating system.</li> <li>• <b>6 (Add user group):</b> A group was added to the operating system.</li> <li>• <b>7 (Delete user group):</b> A group was deleted from the operating system.</li> <li>• <b>8 (User group admin):</b> A user was added to the admin group.</li> <li>• <b>9 (User group rdp):</b> A user was added to the RDP group.</li> <li>• <b>13 (WMI query):</b> WMI query on the computer.</li> <li>• <b>14 (Login attemp):</b> Attempt to login on another computer.</li> <li>• <b>15 (Scheduler tasks):</b> Operation is logged in the task scheduler.</li> <li>• <b>16 (Special privileges):</b> Escalation of privileges on login.</li> <li>• <b>17 (AMSI buffer scan request):</b> AMSI scan request for a buffer containing a script.</li> <li>• <b>18 (WFP filter operation):</b> A WFP (Windows Filtering Platform) filter was created or deleted.</li> </ul>	
<p><b>Operationflags/ integrityLevel</b></p>	<p><b>eventtype 1 (ProcessOps) - operationflags</b></p> <p>Indicates the integrity level assigned by Windows to the item. See <a href="https://learn.microsoft.com/en-us/windows/win32/secauthz/mandatory-">https://learn.microsoft.com/en-us/windows/win32/secauthz/mandatory-</a></p>	<p>Numeric value</p>

Field	Description	Field Type
	<p><b>integrity-control.</b></p> <ul style="list-style-type: none"> <li>• <b>0X0000</b> Untrusted level</li> <li>• <b>0x1000</b> Low integrity level</li> <li>• <b>0x2000</b> Medium integrity level</li> <li>• <b>0x3000</b> High integrity level</li> <li>• <b>0x4000</b> System integrity level</li> <li>• <b>0x5000</b> Protected</li> </ul> <p><b>eventtype 22 (NetworkOps) - SocketOpFlags</b></p> <p>Specifies the grouping algorithm used to minimize the logging of network connections with identical source and destination IP addresses and ports. Grouping occurs over time periods. Only one connection from the group is logged when the period ends. The time period varies depending on the number of connections logged:</p> <ul style="list-style-type: none"> <li>• <b>0x00000001 (Flag realtime):</b> This indicates that the event was logged in real time. This applies only to events that are not grouped.</li> <li>• <b>0x00000002 (Standard grouping):</b> 15 minutes</li> <li>• <b>0x00000004 (L1 grouping):</b> 500 connections 2 hours</li> <li>• <b>0x00000008 (L2 grouping):</b> 1000 connections 6 hours</li> <li>• <b>0x00000010 (L3 grouping):</b> 5000 connections 12 hours</li> <li>• <b>0x00000020 (L4 grouping):</b> 10000 connections 24 hours</li> </ul> <p>When the specified number of connections is logged at the current grouping level, the grouping level increases. Every hour the</p>	

Field	Description	Field Type
	number of logged connections is re-evaluated to lower the grouping level, if required.	
<b>operationstatus</b>	See <b>opstatus</b> .	Numeric value
<b>opstatus</b>	Indicates whether the event must be sent to the Cytomic Insights: <ul style="list-style-type: none"> <li>• <b>0</b>: Send.</li> <li>• <b>1</b>: Filtered by the agent.</li> <li>• <b>2</b>: Do not send.</li> </ul>	Enumeration
<b>origusername</b>	User of the computer which performed the operation.	Character string
<b>pandaalertid</b>	Internal ID of the indicator.	Character string
<b>pandaaid</b>	See <b>accountid</b> .	Numeric value
<b>pandatimestatus</b>	Indicates the algorithm used to calculate the dates in the <b>Date</b> , <b>DateTime</b> , and <b>TimeStamp</b> fields: <ul style="list-style-type: none"> <li>• <b>0 (Version not supported)</b>: The computer does not support synchronization of its time settings to Cytomic settings.</li> <li>• <b>1: (Recalculated Panda Time)</b>: The computer has fixed and synced the computer's time settings to Cytomic settings.</li> <li>• <b>2: (Panda Time OK)</b>: The computer time settings are correct.</li> <li>• <b>3: (Panda Time calculation error)</b>: Error fixing the computer time settings.</li> </ul>	Enumeration
<b>parentattributes</b>	Attributes of the parent process. <ul style="list-style-type: none"> <li>• <b>0x0000000000000001 (ISINSTALLER)</b>:</li> </ul>	Enumeration

Field	Description	Field Type
	<p>Self-extracting (SFX) file.</p> <ul style="list-style-type: none"> <li>• <b>0x0000000000000002 (ISDRIVER):</b> Driver-type file.</li> <li>• <b>0x0000000000000008 (ISRESOURCESDLL):</b> Resource DLL-type file.</li> <li>• <b>0x0000000000000010 (EXTERNAL):</b> File from outside the computer.</li> <li>• <b>0x0000000000000020 (ISFRESHUNK):</b> File recently added to the Cytomic knowledge base.</li> <li>• <b>0x0000000000000040 (ISDISSINFECTABLE):</b> File for which there is a recommended disinfection action.</li> <li>• <b>0x0000000000000080 (DETEVENT_DISCARD):</b> The event-based context detection technology did not detect anything suspicious.</li> <li>• <b>0x0000000000000100 (WAITED_FOR_VINDEX):</b> Execution of a file whose creation had not been registered.</li> <li>• <b>0x0000000000000200 (ISACTIONSEND):</b> The local technologies did not detect malware in the file and it was sent to Cytomic for classification.</li> <li>• <b>0x0000000000000400 (ISLANSHARED):</b> File stored on a network drive.</li> <li>• <b>0x0000000000000800 (USERALLOWUNK):</b> File with permission to import unknown DLLs.</li> <li>• <b>0x0000000000001000 (ISSESSIONREMOTE):</b> Event originating from a remote session.</li> </ul>	

Field	Description	Field Type
	<ul style="list-style-type: none"> <li>• <b>0x0000000000002000 (LOADLIB_TIMEOUT)</b>: The time elapsed between when the protection intercepted the loading of the library and when it was scanned exceeded 1 second. As a result, the scan changed from synchronous to asynchronous to avoid impacting performance.</li> <li>• <b>0x0000000000004000 (ISPE)</b>: Executable file.</li> <li>• <b>0x0000000000008000 (ISNOPE)</b>: Non-executable file.</li> <li>• <b>0x0000000000020000 (NOSHELL)</b>: The agent did not detect the execution of a shell command on the system.</li> <li>• <b>0x0000000000080000 (ISNETNATIVE)</b>: NET Native file.</li> <li>• <b>0x0000000000100000 (ISSERIALIZER)</b>: Serializer file.</li> <li>• <b>0x0000000000200000 (PANDEX)</b>: File included in the list of processes created by Cytomic Patch.</li> <li>• <b>0x0000000000400000 (SONOFGWINSTALLER)</b>: File created by an installer classified as goodware.</li> <li>• <b>0x0000000000800000 (PROCESS_EXCLUDED)</b>: File not scanned because of the Cytomic Orion exclusions.</li> <li>• <b>0x0000000001000000 (INTERCEPTION_TXF)</b>: The intercepted operation was originated by an executable whose image on the disk is being modified.</li> <li>• <b>0x0000000002000000 (HASMACROS)</b>: Microsoft Office document with macros.</li> <li>• <b>0x0000000008000000 (ISPEARM)</b>:</li> </ul>	

Field	Description	Field Type
	<p>Executable file for ARM microprocessors.</p> <ul style="list-style-type: none"> <li>• <b>0x0000000010000000 (ISDYNFILTERED)</b>: The file was allowed on the computer because there are no technologies to classify it.</li> <li>• <b>0x0000000020000000 (ISDISINFECTED)</b>: The file was disinfected.</li> <li>• <b>0x0000000040000000 (PROCESSLOST)</b>: The operation was not logged.</li> <li>• <b>0x0000000080000000 (OPERATION_LOST)</b>: Operation with a pre-scan report for which the post-scan report has not been received yet.</li> <li>• <b>0x0000002000000000 (SAFE_BOOT_MODE)</b>: The computer started in Safe Mode.</li> <li>• <b>0x0000004000000000 (PANDA_SIGNED)</b>: File signed by Panda Security.</li> </ul>	
<b>parentattmask</b>	See <a href="#">parentattributes</a> .	
<b>parentblake</b>	Blake2 signature of the parent file that performed the operation.	Character string
<b>parentcount</b>	Number of processes with DNS failures.	Numeric value
<b>parentdrive</b>		
<b>parentfilename</b>	Parent file name.	Character string
<b>parentmd5</b>	Parent file hash.	Character string
<b>parentpath</b>	Path of the parent file that performed the logged operation.	Character string

Field	Description	Field Type
<b>parentpid</b>	Parent process ID.	Numeric value
<b>parentstatus</b>	<ul style="list-style-type: none"> <li>• <b>0 (StatusOk)</b>: Status OK.</li> <li>• <b>1 (NotFound)</b>: Item not found.</li> <li>• <b>2 (UnexpectedError)</b>: Unknown error.</li> <li>• <b>3 (StaticFiltered)</b>: File identified as malware using static information contained in the Cytomic EDR or Cytomic EPDR protection.</li> <li>• <b>4 (DynamicFiltered)</b>: File identified as malware using local technology implemented in Cytomic EDR or Cytomic EPDR.</li> <li>• <b>5 (FileIsTooBig)</b>: File too big.</li> <li>• <b>6 (PEUploadNotAllowed)</b>: File send was disabled.</li> <li>• <b>11 (FileWasUploaded)</b>: File sent to the cloud for analysis.</li> <li>• <b>12 (FiletypeFiltered)</b>: Resource DLL, NET Native, or Serializer-type file.</li> <li>• <b>13 (NotUploadGWLocal)</b>: Goodware file not saved to the cloud.</li> <li>• <b>14 (NotUploadMWdisinfect)</b>: Disinfected malware file not saved to the cloud.</li> </ul>	Enumeration
<b>pecreationsource</b>	<p>Type of drive where the process was created:</p> <ul style="list-style-type: none"> <li>• <b>(0)</b> : The device type cannot be determined.</li> <li>• <b>(1)</b> : The device path is invalid. For example, the external storage media was extracted.</li> <li>• <b>(2)</b> : Removable storage media.</li> <li>• <b>(3)</b> : Internal storage media.</li> </ul>	Numeric value



Field	Description	Field Type
	<ul style="list-style-type: none"> <li>• <b>(4)</b> : Remote storage media (for example, a network drive).</li> <li>• <b>(5)</b>: CD-ROM.</li> <li>• <b>(6)</b>: RAM disk.</li> </ul>	
<b>phonedescription</b>	Phone description if the operation involved a device of this type.	Character string
<b>pid</b>	Identifier of the process that started the session.	Numeric value
<b>protocol</b>	<p>Communications protocol used by the process.</p> <ul style="list-style-type: none"> <li>• <b>6 (TCP)</b></li> <li>• <b>12 (RDP)</b></li> <li>• <b>17 (UDP)</b></li> </ul>	Enumeration
<b>proxyconnection</b>	The connection is through a proxy.	Boolean
<b>querieddomaincount</b>	See <b>times</b> .	Numeric value
<b>realservicelevel</b>	<p>Current agent mode (this can be temporarily different from the mode assigned in the settings).</p> <p>See <b>servicelevel</b></p>	Enumeration
<b>redirection</b>	<p>HTTP redirection detected.</p> <p>This field shows information only if the security software Audit mode is enabled.</p>	Boolean
<b>registryaction</b>	<p>Type of operation performed on the Windows registry of the computer.</p> <ul style="list-style-type: none"> <li>• <b>0 (CreateKey)</b>: A new registry branch was created.</li> <li>• <b>1 (CreateValue)</b>: A value was assigned to a registry branch.</li> </ul>	Enumeration

Field	Description	Field Type
	<ul style="list-style-type: none"> <li>• <b>2 (ModifyValue)</b>: A registry branch value was modified.</li> </ul>	
<b>remediationdata</b>	See <b>extendedinfo</b> .	
<b>remediationresult</b>	<p>User's response to the pop-up message shown by Cytomic EPDR or Cytomic EDR.</p> <ul style="list-style-type: none"> <li>• <b>0 OK</b>: The client accepted the message.</li> <li>• <b>1 (Timeout)</b>: The pop-up message disappeared due to lack of action by the user.</li> <li>• <b>2 (Angry)</b>: The user chose the option to not block the item from the pop-up message displayed.</li> <li>• <b>3 (Block)</b>: The item was blocked because the user did not reply to the pop-up message.</li> <li>• <b>4 (Allow)</b>: The user accepted the solution.</li> <li>• <b>-1 (Unknown)</b></li> </ul>	Enumeration
<b>remoteip</b>	<p><b>eventtype 1 (ProcessOps)</b></p> <p>IP address of the remote computer that executed the action on the monitored computer.</p> <p><b>eventtype 22 (Networkops)</b></p> <p>Contains the IP address of the other end of the connection, regardless of the connection direction (<b>direction</b> field). See <b>localip</b> and <b>direction</b>.</p> <p><b>eventtype 45 (SystemOps)</b></p> <p>IP address of the computer connected to the monitored computer to execute a WMI request.</p>	IP address
<b>remotemachinename</b>	<p><b>eventtype 1 (ProcessOps)</b></p> <p>Name of the remote computer that executed</p>	Character string

Field	Description	Field Type
	<p>the action on the monitored computer.</p> <p><b>eventtype 22 (Networkops) - hostname</b></p> <p>Name of the remote computer.</p> <p><b>eventtype 45 (SystemOps)</b></p> <p>Name of the computer connected to the monitored computer to execute a WMI request.</p>	
<b>remoteport</b>	<p>Contains the port of the computer on which the event was logged or of the other end of the connection depending on the <b>direction</b> field:</p> <ul style="list-style-type: none"> <li>• <b>direction = 1</b> (inbound connection). This contains the port of the computer on which the event was logged.</li> <li>• <b>direction = 2</b> (outbound connection). This contains the port of the other end of the connection.</li> </ul> <p>See <b>localport</b> and <b>direction</b>.</p>	Numeric value
<b>remoteusername</b>	Name of the remote user that performed the operation on the monitored computer.	Character string
<b>responseclassification</b>	<p>Process classification.</p> <ul style="list-style-type: none"> <li>• <b>0 (Unknown)</b>: File in the process of classification.</li> <li>• <b>1 (Goodware)</b>: File classified as goodware.</li> <li>• <b>2 (Malware)</b>: File classified as malware.</li> <li>• <b>3 (Suspect)</b>: The file is in the process of classification and it is highly likely to be malware.</li> <li>• <b>4 (Compromised)</b>: Process compromised by an exploit attack.</li> <li>• <b>5 (GWNotConfirmed)</b>: The file is in the</li> </ul>	Enumeration

Field	Description	Field Type
	<p>process of classification and it is highly likely to be malware.</p> <ul style="list-style-type: none"> <li>• <b>6 (Pup)</b>: File classified as an unwanted program.</li> <li>• <b>7 (GwUnwanted)</b>: Equivalent to PUP.</li> <li>• <b>8 (GwRanked)</b>: Process classified as goodware.</li> <li>• <b>-1 (Unknown)</b></li> </ul>	
<p>risk</p>	<p>Status of the device that initiated the connection to the protected computer. This status caused the blocking or monitoring of the connection by the Endpoint Access Enforcement technology.</p> <ul style="list-style-type: none"> <li>• <b>0 (E_NNS_MACHINE_PROTECTION_STATUS_UNKNOWN)</b>: The status of the protection on the connecting computer is unknown.</li> <li>• <b>1 (E_NNS_MACHINE_PROTECTION_STATUS_PROTECTION_ENABLED)</b>: The status of the protection on the connecting computer is enabled.</li> <li>• <b>2 (E_NNS_MACHINE_PROTECTION_STATUS_NON_MANAGED)</b>: The connecting computer does not have security software installed or the software is from another vendor.</li> <li>• <b>3 (E_NNS_MACHINE_PROTECTION_STATUS_DIFFERENT_ACCOUNT)</b>: The connecting computer has compatible security software installed but it is managed by another account.</li> <li>• <b>4 (E_NNS_MACHINE_PROTECTION_STATUS_PROTECTION_DISABLED)</b>: The connecting computer has compatible security software installed but it is</li> </ul>	<p>Enumeration</p>

Field	Description	Field Type
	<p>disabled.</p> <ul style="list-style-type: none"> <li>• <b>5 (E_NNS_MACHINE_PROTECTION_STATUS_RISK_MEDIUM)</b>: The risk level of the connecting computer is medium.</li> <li>• <b>6 (E_NNS_MACHINE_PROTECTION_STATUS_RISK_HIGH)</b>: The risk level of the connecting computer is high.</li> <li>• <b>7 (E_NNS_MACHINE_PROTECTION_STATUS_RISK_CRITICAL)</b>: The risk level of the connecting computer is critical.</li> </ul>	
<b>riskdetected</b>	See <b>risk</b> .	
<b>ruleid</b>	<p><b>eventtype 555 (IOA) - huntingruleid:</b> Identifier of the cyberattack radar rule that detected the indicator.</p> <p><b>eventtype 22 (IOA) - ruleid:</b> Snort rule that detected communications that use HTTP tunnels. This field shows information only if the security software Audit mode is enabled.</p>	Character string
<b>servicelevel</b>	<p>Agent execution mode.</p> <ul style="list-style-type: none"> <li>• <b>0 (Learning)</b>: The agent does not block any items but monitors all running processes.</li> <li>• <b>1 (Hardening)</b>: The agent blocks all unclassified programs coming from an untrusted source, and items classified as malware.</li> <li>• <b>2 (Block)</b>: The agent blocks all unclassified executables and items classified as malware.</li> <li>• <b>-1 (N/A)</b></li> </ul>	Enumeration
<b>sessiondate</b>	Date the antivirus service was last started or	Date

Field	Description	Field Type
	last time it was started since the last update.	
<b>sessiontype</b>	<p>Login type:</p> <ul style="list-style-type: none"> <li>• <b>0 (System Only):</b> Session started with a system account.</li> <li>• <b>2 (Local):</b> Session created physically through a keyboard or through KVM over IP.</li> <li>• <b>3 (Remote):</b> Session created remotely in shared folders or printers. This login type uses secure authentication.</li> <li>• <b>4 (Scheduled):</b> Session created by the Windows task scheduler.</li> <li>• <b>5 (Service):</b> Session created when a service that needs to run in the user session is launched. The session is deleted when the service stops.</li> <li>• <b>7 (Blocked):</b> Session created when a user tries to join a previously blocked session.</li> <li>• <b>8 (Remote Unsecure):</b> Same as type 3 but the password is sent in plain text.</li> <li>• <b>9 (RunAs):</b> Session created when the “RunAs” command is used under an account other than the account used to log in, and the “/netonly” parameter is specified. If the “/netonly” parameter is not specified, a type 2 session is created.</li> <li>• <b>10 (TsClient):</b> Session created when accessing through “Terminal Service”, “Remote Desktop” or “Remote Assistance”. It identifies a remote user connection.</li> <li>• <b>11 (Domain Cached):</b> User session created with domain credentials cached on the machine, but with no connection to</li> </ul>	Enumeration

Field	Description	Field Type
	<p>the domain controller.</p> <ul style="list-style-type: none"> <li>• <b>-1 (Unknown)</b></li> </ul>	
<b>sha256</b>	See <b>childsha256</b> .	Character string
<b>shash</b>	Alphanumeric character pattern followed by the hash of the child process.	Character string
<b>socketopflags</b>	See <b>Operationflags/ integrityLevel</b> .	
<b>TelemetryType</b>	<ul style="list-style-type: none"> <li>• <b>0: Normal telemetry.</b> The event does not belong to an indicator that follows a pattern described in the MITRE matrix.</li> <li>• <b>1: Resent event.</b> The event was originally sent as a type 0 event (normal telemetry), but later it was detected that it belongs to an attack pattern described in the MITRE matrix. The event was resent with the TTPs and IOAIds fields completed.</li> <li>• <b>2: Accumulated events:</b> To save resources, part of the telemetry generated for the client is retained until the security software detects a MITRE attack pattern. Then, all accumulated events are sent.</li> </ul>	Enumeration
<b>timeout</b>	The local scan took too long to complete and the process was delegated to other mechanisms that do not impact performance.	Boolean
<b>times</b>	<p><b>eventtype 22 (NetworkOps)</b></p> <p>Number of repetitions of a connection created by the same process on the same path, with the same localIP, RemoteIP, and RemotePort.</p> <p><b>eventtype 45 (SystemOps)</b></p>	Numeric value

Field	Description	Field Type
	<p>Number of WMI requests per table and process grouped in a one-hour period.</p> <p><b>eventtype 46 (DnsOps) - querieddomaincount</b></p> <p>Number of different domains sent by the process for which there was a DNS resolution failure in the last hour.</p> <p><b>eventtype 99 (RemediationOps) - napocurrences</b></p> <p>Number of times the same type of network attack targeting the same IP address has been logged in a one-hour period.</p>	
<b>timestamp</b>	<p>UTC date in epoch format (number of seconds elapsed since 1 January 1970) at the time the event occurred on the client's computer. To understand this field, see <a href="#">pandatimestatus</a>.</p>	Date
<b>totalresolutiontime</b>	<p>Indicates the time it took the cloud to respond, and whether the error code query failed.</p> <ul style="list-style-type: none"> <li>• <b>0</b>: The cloud was not queried.</li> <li>• <b>&gt;0</b>: Time in milliseconds it took the cloud to respond to the query.</li> <li>• <b>&lt;0</b>: Cloud query error code.</li> </ul>	Numeric value
<b>TTPs</b>	List of the MITRE tactics, techniques, and sub-techniques associated with the event.	Character string
<b>type</b>	See <a href="#">operation</a> .	Enumeration
<b>uniqueid</b>	Unique ID of the device.	Character string
<b>url</b>	<p><b>eventtype 14 (Download) - childurl</b></p> <p>Download URL launched by the process that generated the logged event.</p>	Character string



Field	Description	Field Type
	<p><b>eventtype 22 (NetworkOps) - inicitaldomain</b></p> <p>Source domain when the security software detects an HTTP redirection.</p> <p>This field shows information only if the security software Audit mode is enabled.</p>	
<b>username</b>	See <b>loggeduser</b> .	
<b>value</b>	<p>Type of operation performed on the Windows registry of the computer.</p> <ul style="list-style-type: none"> <li>• <b>0 (CreateKey)</b>: A new registry branch was created.</li> <li>• <b>1 (CreateValue)</b>: A value was assigned to a registry branch.</li> <li>• <b>2 (ModifyValue)</b>: A registry branch value was modified.</li> </ul>	Enumeration
<b>valuedata</b>	<p>Data type of the value contained in the registry branch.</p> <ul style="list-style-type: none"> <li>• <b>00 (REG_NONE)</b></li> <li>• <b>01 (REG_SZ)</b></li> <li>• <b>02 (REG_EXPAND_SZ)</b></li> <li>• <b>03 (REG_BINARY)</b></li> <li>• <b>04 (REG_DWORD)</b></li> <li>• <b>05 (REG_DWORD_BIG_ENDIAN)</b></li> <li>• <b>06 (REG_LINK)</b></li> <li>• <b>07 (REG_MULTI_SZ)</b></li> <li>• <b>08 (REG_RESOURCE_LIST)</b></li> <li>• <b>09 (REG_FULL_RESOURCE_DESCRIPTOR)</b></li> <li>• <b>0A (REG_RESOURCE_REQUIREMENTS_LIST)</b></li> <li>• <b>0B (REG_QWORD)</b></li> </ul>	Enumeration

Field	Description	Field Type
	<ul style="list-style-type: none"> <li>• 0C (REG_QWORD_LITTLE_ENDIAN)</li> </ul>	
<b>valuedatalength</b>	Size of the data stored in the Windows registry.	Numeric value
<b>verbosemode</b>	The computer is configured in Verbose mode.	Binary value
<b>version</b>	Operating system version of the computer that ran the vulnerable software.	Character string
<b>versionagent</b>	Installed agent version.	Character string
<b>versionantiexploit</b>	See <a href="#">vantiexploit</a> .	Character string
<b>versionbloomfilter</b>	See <a href="#">vbloomfilter</a> .	Character string
<b>versioncontroller</b>	Psnmctrl.dll DLL version.	Character string
<b>versiondetectevent</b>	Deteven.dll DLL version.	Character string
<b>versiondetection</b>		
<b>versiondetevenfilter</b>	See <a href="#">vdetevenfilter</a> .	
<b>versionfilterantiexploit</b>	See <a href="#">vfilterantiexploit</a> .	
<b>versionioaplg</b>	See <a href="#">vioaplg</a> .	
<b>versionproduct</b>	Installed protection product version.	Character string
<b>versionransomevent</b>	See <a href="#">vransomevent</a> .	
<b>versionsherlockplg</b>	See <a href="#">vsherlockplg</a> .	
<b>versiontabledetection</b>	See <a href="#">vtabledetevent</a> .	
<b>versionableransom</b>	See <a href="#">vableransomevent</a> .	

Field	Description	Field Type
<b>versionttpplg</b>	See <b>vtppplg</b> .	
<b>vantiexploit</b>	Version of the PSNMVHookPlg32 and PSNAntiExploitPLG.dll DLLs.	Character string
<b>vbloomfilter</b>	Version of the Bloom filter file that contains the local goodwill cache.	Character string
<b>vdeteventfilter</b>	Version of the filter file for the contextual detection technology (deteventfilter).	Character string
<b>vioaplg</b>	PSNIOAPIg.dll DLL version.	Character string
<b>vtabledetevent</b>	TblEven.dll DLL version.	Character string
<b>vtableramsomevent</b>	TblRansomEven.dll DLL version.	Character string
<b>vramsomeevent</b>	RansomEvent.dll DLL version.	Character string
<b>vsherlockplg</b>	PSNEVMGRAG.dll DLL version.	Character string
<b>vtfilterantiexploit</b>	PSNAEHookPlg32.dll DLL version.	Character string
<b>vtppplg</b>	PSNMitrePlg.dll DLL version.	Character string
<b>winningtech</b>	<p>Cytomic EPDR or Cytomic EDR agent technology that raised the event:</p> <ul style="list-style-type: none"> <li>• <b>0 (Unknown)</b></li> <li>• <b>1 (Cache)</b>: Locally cached classification.</li> <li>• <b>2 (Cloud)</b>: Classification downloaded from the cloud.</li> <li>• <b>3 (Context)</b>: Local context rule.</li> <li>• <b>4 (Serializer)</b>: Binary type.</li> <li>• <b>5 (User)</b>: The user was asked about the action to take.</li> <li>• <b>6 (LegacyUser)</b>: The user was asked about the action to take.</li> </ul>	Enumeration

Field	Description	Field Type
	<ul style="list-style-type: none"> <li>• <b>7 (NetNative)</b>: Binary type.</li> <li>• <b>8 (CertifUA)</b>: Detection by digital certificates.</li> <li>• <b>9 (LocalSignature)</b>: Local signature.</li> <li>• <b>10 (ContextMinerva)</b>: Cloud-hosted context rule.</li> <li>• <b>11 (Blockmode)</b>: The agent was in Hardening or Lock mode when the process was blocked from running.</li> <li>• <b>12 (Metasploit)</b>: Attack created with the Metasploit Framework.</li> <li>• <b>13 (DLP)</b>: Data Leak Prevention technology.</li> <li>• <b>14 (AntiExploit)</b>: Technology that identifies attempts to exploit vulnerable processes.</li> <li>• <b>15 (GWFilter)</b>: Technology that identifies goodware processes.</li> <li>• <b>16 (Policy)</b>: Cytomic EPDR advanced security policies.</li> <li>• <b>17 (SecAppControl)</b>: Security app control technologies.</li> <li>• <b>18 (ProdAppControl)</b>: Productivity app control technologies.</li> <li>• <b>19 (EVTContext)</b>: Linux contextual technology.</li> <li>• <b>20 (RDP)</b>: Technology to detect/block RDP (Remote Desktop Protocol) intrusions and attacks.</li> <li>• <b>21 (AMSI)</b>: Technology to detect malware in AMSI notifications.</li> <li>• <b>-1 (Unknown)</b></li> </ul>	
<b>wdocs</b>	Base-64 encoded list of all documents that	Character string

Field	Description	Field Type
	were open when an exploit detection occurred.	

Table 18.1: List of the fields that make up the events stored by Cytomic Orion

# Glossary

---

## A

---

### **Access token**

This is a character string used by the application to access the protected Cytomic Orion resource (the API). The access token describes the scope of access, including the duration, and other relevant information. The tokens are opaque for the client application. They are emitted by, and only relevant for, the CAS server.

### **Antivirus**

Protection module based on conventional technologies (firmware files, heuristic analysis, anti-exploit, etc.) which detects and removes computer viruses and other threats.

### **Application (with respect to the integration API)**

Third-party development to be integrated with Cytomic Orion by means of the integration API.

### **APT (Advanced Persistent Threat)**

Set of strategies implemented by hackers designed to infect a client's network using several infectious vectors in tandem in order to go unnoticed by conventional antivirus systems for long periods of time. Their main objective is financial (theft of confidential company information for blackmailing, theft of intellectual property, etc.) or political.

### **ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge)**

Set of resources developed by Mitre Corp. to describe and classify cyber-criminals' dangerous behavior based on observations from all over the world. ATT&CK is an organized list of attackers' known behaviors divided into tactics and techniques; it is expressed in a matrix and also through STIX and TAXII. As this list is a complete representation of behavior that hackers use to infiltrate corporate networks, it is a useful resource for organizations when developing defensive, preventive, and problem-solving mechanisms.

### **Authentication server (with respect to the Integration API)**

System that creates and validates the third-party account credentials of the application using the integration API. Cytomic Orion delegates validation of the username and password credentials to the IdP server (Identity Provider).

### **Authorization server (with respect to the Integration API)**

Server with which the application using the integration API interacts to request access to a protected resource. Cytomic Orion delegates this task to the CAS (Authorization Server).

---

## C

---

### **CAS (Cytomic Orion Authorization Server)**

Authorization server used in the Integration API. Refer to “Authorization server (with respect to the Integration API)” for more details.

### **Cell**

Minimum unit of a notebook. It consists of a multi-line text box hosting a code in a language compatible with the notebook’s kernel and the results of its execution.

### **CKC (Cyber Kill Chain)**

In 2011, Lockheed-Martin Corporation described a new framework or model to defend computer networks, detailing that cyber-attacks occur in phases and that each one of them can be interrupted through established controls. Since then, the Cyber Kill Chain has been adopted by data security organizations to define cyber-attack phases. These phases begin with remote reconnaissance of the target’s assets and extend to data exfiltration.

### **Client\_id and client\_secret (with respect to the integration API)**

The identifier and password assigned to the Cytomic Orion client. To get a client\_id and client\_secret contact the Cytomic sales department.

### **Cloud (Cloud Computing)**

This term is used to describe a global network of inter-connected servers that operate as a single ecosystem and designed to store and manage data, run applications, or deliver content or services (video streaming, webmail, office software, security services, etc.). Instead of accessing files and data from a personal or local computer, the user accesses them online from any device connected to the Internet. In short, the information is available wherever you go whenever you need it.

### **Compromised process**

Vulnerable processes that have been affected by an exploit and that can compromise a computer’s security.

### **CTI (Cyber Threat Intelligence)**

This is an open platform for exchanging cyber-security information, and which monitors, collects and analyzes potential cyber-threats targeting organizations, thereby enabling the design of defensive and remedial actions.

### **CVE (Common Vulnerabilities and Exposures)**

Information defined and stored by Mitre Corp. about known security vulnerabilities. Each entry has a unique identification number, offering a common nomenclature for public knowledge of these types of problems, thus facilitating the sharing of data about such vulnerabilities.

---

**Cyber-attack radar**

Search engine implemented in Cytomic Orion that uses the events lake formed by telemetry collected from computers and the hunting rules describing TTPs (Tactics, Techniques, and Procedures) employed by hackers. When the cyber-attack radar detects a TTP, it generates an indicator.

---

**D****DNS (Domain Name System)**

Service that translates domain names with several types of information, usually IP addresses.

**Dwell time**

Time that a threat has remained undetected on a network computer.

---

**E****EDR (Endpoint Detection & Response)**

EDR is the answer to the fact that conventional antivirus will never be able to avoid all cyber-attacks. EDR assumes threats will avoid prevention defenses, so it focuses on monitoring computers in order to detect behavior indicating malicious activity and capture data for security research. The majority of EDR has some level of automated response, but depending on the time the threat is exposed before it is discovered, it may be necessary to employ manual resolution initiatives. Like NGAV, EDR solutions use ML (Machine Learning) techniques and AI (Artificial Intelligence) to extrapolate and determine whether a behavior is malicious based on continuously-updating big data sets.

**Event**

Each relevant action monitored by Cytomic EDR or Cytomic EPDR and performed by processes on workstations and servers generates an event which is enriched and sent to Cytomic Orion's platform. It is stored so the analyst can later investigate it individually or together with the rest of the events.

**Events lake**

Collection of all the telemetry generated by processes performed on desktops and servers, and stored in Cytomic Orion's servers, where the analyst can run searches in order to complete their analysis.

**Exploit**

Generally speaking, an exploit is a data sequence especially designed to provoke a controlled error when running a vulnerable program. After provoking the error, the compromised process will mistakenly interpret part of the data sequence as executable code, thus triggering actions which are dangerous to the computer's security.



---

## F

---

### **Firewall**

This technology blocks network traffic which coincides with patterns defined by the administrator through rules. This way it restricts or blocks communications by certain applications running on the computer, thereby reducing the attack surface.

## G

---

### **GDPR (General Data Protection Regulation)**

Regulation regarding data protection for European Union residents.

### **Geolocate**

Positioning a device on a map according to its coordinates.

### **Goodware**

File classified as legitimate and safe after examination.

### **Graph**

A notebook that uses the telemetry flow generated by the client's IT infrastructure as source of information and provides a graphical representation of the logged entities and their relationships, making them easier for analysts to interpret.

## H

---

### **Hunting rule**

Description of a TTP (Tactics, Techniques, and Procedures) recognized by Cytomic Orion, and used by the cyber-attack radar to search the events lake for execution patterns suspected of belonging to a cyber-attack.

## I

---

### **Identifiers File/Firmware File**

File containing patterns that an antivirus uses to detect threats.

### **IdP (Identity Provider)**

Authentication server used by Cytomic Orion in the integration API. Refer to "Telemetry" for more details.

### **Indicator**

Hypothesis generated by Cytomic Orion. It warns the Tier 1 analyst from MSSP/MDR/SOC about the detection of a TTP pattern described in a hunting rule.

**Indicator triage**

System of checks developed by MPPS/MDR/SOC Tier 1 technicians to filter alerts generated by Cytomic Orion and thus delivering to Tier 2 only those cases with the highest likelihood of being a cyber-attack. The indicator triage removes false positives, thereby reducing the workload at SOC Tier 2.

**Infection vector**

Means of entry or procedure used by malware to infect a computer. Common infection vectors include Web browsing, email, and pendrives.

**Integration API**

REST APIs which Cytomic Orion deploys to allow integration with third-party tools or applications developed in the SOC.

**Investigation**

Repository of shared data created by MSSP/MDR/SOC Tier 1 analysts and contributed to by Tier 2 and Tier 3 analysts with findings produced during an investigation.

**IOCs**

Industry standard for describing conditions that can compromise the security of organizations. As it is a similar concept to the signature file used by malware protection tools, its format is open, allowing it to be shared and exchanged and enabling an administrator to easily extend the detection capacity of the security solution installed on network computers.

**IP address**

Number that logically and hierarchically identifies the network interface of a device (usually a computer) inside a network using IP protocol.

**L**

---

**Lateral movements**

Operations performed by hackers inside a corporate network through which they intend to gain an advantageous position in order to reach their targets. It usually implies the spread of malware to other computers within the network, installation of backdoors facilitating the access to several corporate subnets, etc.

**M**

---

**Malware**

General term used for programs with malicious codes (MALicious softWARE), such as viruses, Trojans, worms, or any other threat affecting the security and integrity of computer systems. Malware infiltrates and damages a computer with several objectives and without the owner's knowledge.

---

**MD5 (Message-Digest Algorithm 5)**

Cryptographic reduction algorithm that gets a 128-bit signature (hash or digest) uniquely representing a sequence or string. The MD5 hash calculated on a file is useful for its unequivocal identification or for confirming that it has not been tampered with or changed.

**MDR (Managed Detection and Response)**

A new class of security service that groups experts, proprietary technology, and the practical knowledge necessary to overcome deficiencies in the MSSP model by pro-actively and rapidly searching for, investigating, and solving cyber-threats.

**MITRE (The MITRE Corporation)**

Non-profit company operating multiple federally-financed research and development sites dedicated to addressing security-related issues. It offers practical solutions in defense and intelligence, aviation, civilian systems, national security, judiciary, health, and cyber-security. It is the creator of the ATT&CK framework. It is the creator of the ATT&CK framework.

**MSSP**

Companies offering managed security services for those organizations wishing to outsource them.

**MUID**

Character string used by Cytomic Orion to uniquely identify each of the client's workstations and servers.

---

**N****NGAV**

Unlike conventional antivirus solutions, which fundamentally base their detection capacities on firmware files stored on a local drive, in the cloud, or a combination of both, NGAV uses advanced techniques to detect malware. It can include self-learning techniques (Machine Learning), exploit detection, use of IOCs (Indicators of Compromise), metadata analysis, and other techniques to search for the TTPs used by attackers.

**NGFW**

The natural evolution of firewalls to which advanced functionalities of malware detection, content filtering, Web traffic filtering, VPN services, remote network access, and intrusion detection systems, among others, are added.

**Notebook**

Web representation of all the input and output that occurred over time regarding one or several code fragments run interactively, including explanations in text format, images, and more elaborate object representations.

---

### **Notification rule**

Sends the indicators detected on one or more clients' computers to one or more email accounts to prevent analysts from recurrently accessing the analysis console in order to check the status of the IT network of the clients they investigate.

## **O**

---

### **OAuth (Open Authorization)**

An open and widely used industry standard for allowing delegated access to protected resources. The main scenario for which OAuth was designed was that of a user that needs to grant permission to access protected information on websites or third-party applications, but without having to share login credentials. OAuth therefore provides secure delegated access to the owner's resources under the owner's name, and specifies the processes required for the owner to authorize third-party access without having to share credentials.

## **P**

---

### **Phishing**

An attempt to illegally obtain confidential user information through deception. Usually, the target information includes passwords, credit card details, bank account numbers, or information that may be used to enable remote access to the organization's network.

### **Potentially Unwanted Programs (PUP)**

Programs that are invisibly or discreetly introduced on the computer, taking advantage of the installation of another program which is the one the user intended to install.

### **Python**

Multi-paradigm, interpreted, and multi-platform programming language whose philosophy emphasizes code readability. It has an open source license compatible with the GNU General Public License from version 2.1.1.

## **Q**

---

### **Quick answers**

Independent, small blocks of code which solve particular issues and which analysts can incorporate in notebooks in order to speed up research automation.

## **R**

---

### **Refresh token**

When the application accesses the resource for the first time it is given an access token and a refresh token. When the access token expires, the application requests a new one by using the refresh token and without having to go back through the authentication and authorization process.

---

**Responsive / Adaptable (RWD, Responsive Web Design)**

Set of techniques which allow the development of Web pages which automatically adapt to the size and resolution of the device used to view them.

**Role**

A specific set of permissions applied to one or more user accounts which authorizes viewing or editing certain console resources.

---

**S****SCM (Secure Content Management)**

Network devices operating transparently to offer safe Internet content to users of a corporate network. They include network antivirus systems, firewall, intruder detection/prevention systems (IDS/IPS), Web filtering systems, antispam protection, etc.

**SIEM (Security Information and Event Management)**

Tools that combine the management of the information and security events generated on the client's IT infrastructure, providing real-time analysis of security alerts generated by the applications and hardware on the network.

**SOC (Security Operations Center)**

Company department which monitors, and controls security in the company's IT infrastructure and prevents attacks.

**SQL (Structured Query Language)**

Standard and interactive programming language used to gather information from a database and to update it. Though SQL is both an ANSI and an ISO standard, many database products support SQL with extensions belonging to standard language. Queries take the form of command language which allows selection, inserting, updating, and determining the data location, among other operations.

**Suspicious program**

Program which after being analyzed on a computer, is considered as having a strong chance of being malware.

---

**T****Telemetry**

Information retrieved from desktops and servers which is sent to Cytomic Orion's infrastructure stored in the cloud to feed the events lake. Telemetry is the result of the enrichment of information obtained from monitoring processes with data provided by the advanced protection solution installed on the computer.

---

## **Template**

Notebook used by analysts as the basis for automating research. As each new investigation does not start from scratch, templates speed up the creation of notebooks and enable them to be reused and shared.

## **Threat hunter**

Analyst specialized in investigating indicators within companies' IT infrastructure activities, which can result in discovering computer attacks that go undetected by conventional security solutions installed on computers.

## **Threat hunting**

Set of specialized technologies and human resources allowing the detection of lateral movements and other early threat indicators before they run actions which are harmful for a company.

## **Threat hunting library**

Python library implemented in Cytomic Orion and used by analysts in notebooks to enhance the automation of their investigations.

## **Ticketing**

Tools that ensure that any indicators of threats are correctly managed. Cases are created, assigned and followed until they are closed. KPIs are collected to show the degree of compliance of the SOC security service.

## **Tier**

Internal division of technical staff in a SOC/MSSP/MDR based on several criteria, such as technical knowledge of client infrastructure, communication skills, programming knowledge, etc.

## **TTP (Tactics, Techniques and Procedures)**

A TTP describes the tactical approach used during a cyber-attack. It is used to analyze the attack and to profile the source of the threat. 'Tactics' describes how an attacker decides to execute the attack from beginning to end. 'Techniques' describes the technological approach to achieve intermediate results during the attack. 'Procedures' define the organizational approach of the attack. Knowing the enemy's tactics helps to predict future attacks and to detect them in the early phases. Understanding the techniques used during an attack allows for the identification of blind spots in the organization and the implementation of countermeasures. Finally, analysis of the procedures used by attackers can help to understand what they are looking for inside the targeted infrastructure.

---

## **U**

### **User (console)**

Resource formed by a set of information that Cytomic Orion uses to control administrators' access to the Web console and to set which actions they can perform on the network's computers.

---

**User (network)**

Company workers using computers to do their job.

**UTM (Unified Threat Management)**

Network devices with multiple features related to security, such as network antivirus systems, firewall, intrusion detection/prevention systems (IDS/IPS), web filtering systems, anti-spam protection, etc. UTM devices are designed to protect entire networks of desktops and servers, and they can integrate other services related to security, such as endpoints in private networks, proxy services, etc.

---

**V****VDI (Virtual Desktop Infrastructure)**

Virtualization desktop solution which consists of hosting virtual machines in a data center which users can access from a remote terminal. The purpose is to centralize and streamline management and to reduce maintenance costs. There are two types of VDI environments: Persistent: storage space assigned to each user is maintained between restarts, including installed software, data, and operating system updates. Non-persistent: storage space assigned to each user is eliminated when the VDI restarts, returning to the initial state and eliminating all changes.

**Vulnerable process**

Programs which are not capable of successfully interpreting data received from other processes due to programming errors. When receiving a specially-designed data sequence (exploit), hackers can provoke a process malfunction, which leads to the execution of code that compromises computer security.

---

**W****Widget (Panel)**

Panel formed by a configurable diagram representing a particular aspect of the security of the client's network. The set of widgets forms Cytomic Orion's dashboard.

**Window of opportunity**

Time elapsed between when the first computer in the world was infected by a new strain of malware until the moment it has been analyzed and incorporated into antivirus firmware files in order to protect computers against infection. During this time, malware can infect computers without conventional antivirus systems being aware of its existence. Its detection and containment depends on advanced protection systems and threat hunters.

