CYTOMIC

Cytomic Data Watch Administration Guide_

Legal notice.

Registered trademarks.

Contact information.

Corporate Headquarters:

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

Calle Santiago de Compostela 12

Bilbao (Bizkaia) 48003 Spain.

https://www.pandasecurity.com/uk/about/contact/

Versión: 3.70.00-00

Autor: Cytomic

Fecha: 05/29/2020

About the Administration Guide

You can find the most recent version of this guide at:

https://info.cytomicmodel.com/guides/DataWatch/en/DATAWATCH-Guide-EN.pdf

Cytomic EDPR and Cytomic EDR guides

https://info.cytomicmodel.com/resources/guides/EPDR/latest/en/EPDR-guide-EN.pdf

https://info.cytomicmodel.com/resources/guides/EDR/latest/en/EDR-guide-EN.pdf

Technical information on modules and services compatible with Cytomic Data Watch.

You can find the Cytomic Insights Administration Guide at:

https://info.cytomicmodel.com/resources/guides/Insights/en/INSIGHTS-guide-EN.pdf

Technical Support

Cytomic provides global support services aimed at responding to specific questions regarding the operation of the company's products. The technical support team also generates documentation covering technical aspects of our products. This documentation is available in the eKnowledge Base portal.

To access specific information about the product, please go to the following URL:

https://www.cytomic.ai/support/data-watch/

Survey on the Administration Guide

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

https://es.surveymonkey.com/r/feedbackDWGuideEN

Contents

Part 1: Introduction to Cytomic Data Watch

Part 2: Cytomic Data Watch resources

Part 3: Additional information

Part 1

Introduction to Cytomic Data Watch

Chapter 1

Preface

This guide offers the information and procedures necessary to benefit fully from the Cytomic Data Watch service.

CHAPTER CONTENT

Who is this guide aimed at?

This documentation is aimed at technical personnel in IT departments of organizations that have contracted the Cytomic Data Watch service for Cytomic EDR and PCytomic EDPR.

This manual includes the procedures and settings required to interpret and fully benefit from the security information provided by the Cytomic Data Watch platform.

All the procedures and instructions in this guide apply both to Cytomic EDR and Cytomic EDPR. The term "Cytomic EDR" is used generically to refer to both of these advanced security products.

Icons

The following icons are used in the guide;

ⓘ	Additional information, such as an alternative way of performing a certain task.
⚠	Suggestions and recommendations.
💡	Important advice regarding the proper use of the options available in the Cytomic Data Watch service.

See another chapter or section in the guide for more information.

Chapter 2

Introduction

Cytomic Data Watch is a security module integrated into the Cytomic EDR product and designed to help organizations comply with data protection regulations as well as discovering and monitoring the personally identifiable information stored in the corporate IT infrastructure.

CHAPTER CONTENT

Current status of data protection regulations

The evolution of data protection regulations, along with a considerable increase in the amount of advanced threats in circulation, have combined to generate greater interest in overhauling the security protocols that protect the personal information of companies' customers and employees. This personal data, regardless of its status (*data in use*, *data in motion,* or *data at rest*) has to comply with new security requirements, which derive from:

- **Compliance with new European regulations**: from May 2018, the GDPR issues fines of up to €20 million or 4% of a previous year's turnover for failure to comply with the regulations. All companies within the EU that compile and store the personally identifiable data (PII) of customers, employees and suppliers resident in the EU are subject to these rules.
- **The greater volume of unstructured data in companies**: data stored in office application files (Word, Excel, text files, HTML, etc.) represents 80 percent of the data handled by organizations, and is spread, with no real control, across the servers, desktops, laptops, and other devices of employees, partners and contractors, etc.
- **The publication of confidential data**: it is increasingly common for IT attacks to reveal massive amounts of personal data of customers. Such attacks can be perpetrated by financially motivated outsiders or negligent or disgruntled insiders, among others.

Good data security governance practices are key to mitigating these risks and ensuring compliance with the regulations.

Personal data protection requirements

This new personal data protection scenario gives rise to high-level requirements for organizations, including:

- Controlling the personal data stored in unstructured files on workstations and servers and accessed by hundreds of authorized employees.
- Demonstrating compliance with the legislation at any given time via continuous monitoring.
- Notifying any data leaks to the authorities (*DPA - Data Protection Authority*) and affected customers within 72 hours.

These requirements, however, must be met without increasing the complexity of the products and tools used by the organization to manage IT security.

What is Cytomic Data Watch? Main benefits

Files classified as PII (Personally Identifiable Information) are files that contain information that can be used to identify individuals related to the organization (customers, employees, providers, etc.). This information is of a highly personal nature and includes different types of data, such as social security numbers, phone numbers, email addresses, etc. Cytomic Data Watch identifies, audits, and monitors,

in real time, the complete lifecycle of PII files: from data at rest, operations carried out on them, and their external transfer.

Cytomic Data Watch doesn't just monitor files with personal information: its monitoring capabilities extend to any type of file, such as those containing confidential or sensitive corporate information.

Identification and audits

- Find and identify the files stored on users' computers, email, and network servers which Cytomic Data Watch classified as PII or which match the monitoring rules defined by the administrator.
- Reduce the risk of leaks and evaluate the efficacy of existing security policies. Use the key information provided by the module to improve and adapt your policies and inform users of good practices and other measures.

Monitoring and detection

- Implement proactive measures for accessing and acting on files with reports and alerts in real time about their use and any suspicious or unauthorized exfiltration/infiltration.
- To avoid fines or damage to corporate reputation, the module alerts immediately notify of any possible theft of personal data. The information collected in the Cytomic Data Watch tables, the dashboards, and the predefined reports allow real-time analysis of the complete lifecycle of an incident: who carried out each action, when, where, on which computer or server, and what media was used.

Simplified management

Cytomic Data Watch is a module of Cytomic EDR and Cytomic EDPR and therefore does not require any additional deployment. It is activated immediately, without intervention from the administrator and managed quickly and simply from the same cloud platform.

Cytomic Data Watch and the GDPR

The GDPR (General Data Protection Regulation) is the new legal framework in the EU that replaces the previous data protection directive.

Its aim is to protect personal data and provide a reference point for developing safe procedures for processing, storing and, where necessary, destroying personal data handled by organizations. The law grants eight specific rights to individuals regarding how companies can use the data that is directly and personally related to them.

- Right to be informed.
- Right of access by the data subject.
- Right to rectification.
- Right to erasure ('right to be forgotten').

- Right to restriction of processing.
- Right to data portability.
- Right to object.
- Right not to be subject to automated decision-making.

It also sets out very strict rules that govern what happens if the rules regarding access to personal data are violated and the consequences (fines) that organizations may suffer.

GDPR articles related to the Cytomic Data Watch features

Cytomic Data Watch helps comply with the following articles of the GDPR:

- **Article 17: Right to erasure ('right to be forgotten')**

This article demands that organizations implement the necessary resources to ensure the deletion, without undue delay, of the personal data concerning a customer, at their request.

Cytomic Data Watch allows organizations to perform custom searches to find all files on the network that contain personal data of any individual who wants to exercise their right to erasure.

- **Article 32: Security of processing**

This requires the implementation of appropriate technical and organizational measures to ensure a level of security appropriate to the risk. It also requires the evaluation of the risks of processing data and the implementation of measures for controlling data usage and access.

Cytomic Data Watch provides information about how PII files are distributed on the network and their access by users: the computers used and the types of actions being carried out. This makes it possible to verify that the data is accessed only by authorized personnel and if the company security policies are correct, to assess the risk in the management of PII.

- **Article 33: Notification of a personal data breach to the supervisory authority**

This requires that the competent authority is notified within 72 hours whenever there is a breach of security regarding personal data, if it may represent a risk to the rights and freedoms of natural persons.

Cytomic Data Watch analyzes the incident to assess its impact, showing which computers, users, and files have been compromised and identifying the type of leak: if it was caused by malware, by unauthorized external communication of data (exfiltration), or by actions from within the company (infiltration).

- **Article 35: Data protection impact assessment**

This requires an assessment of the impact of data processing operations on the protection of personal data where it is likely that such processing, due to its nature, scope, context, or purpose, represents a high risk to the rights and freedoms of natural persons.

Cytomic Data Watch automatically identifies files containing personally identifiable information and monitors the actions taken on them, and the users who execute them. As such it is possible to know the quantity, type, volume, or use of personal information so that the impact and risk of processing can be evaluated.

- **Article 39: Tasks of the data protection officer (DPO)**

This establishes the figure of the DPO (data protection officer) to monitor compliance with the regulation and offer advice regarding data protection impact assessment and monitor its performance.

Cytomic Data Watch provides the DPO with graphical tools to support the supervision, assessment, and understanding of the risks associated with the processing of personal data.

Cytomic Data Watch features related to the GDPR

The basic information from which Cytomic Data Watch builds the security intelligence for the processing of personal data is summarized as follows:

Information	Fields/Operations
Discovery/automatic classification of unstructured files as either PII files or not PII files.	
Information about PII files.	• Name. • Type. • Extension. • Size. • Type of personal information in the file.
Information about email messages containing monitored files.	• Message sender and recipient. • Date the message was sent and received • Size, name, and hash of the file found in the message.
Classification of processes acting on the PII files.	• Malware. • Pending classification. • Goodware.
Type of action taken on the PII files.	• Create. • Open. • Rename. • Delete. • Copy – Paste.
Classification of actions taken on the PII files.	• Data leaking or communication actions (data exfiltration). • Data introduction operations (data infiltration).

Table 2.1: basic information collected from users' computers

Information	Fields/Operations
Users that take actions on the PII files.	
Location of computers with PII files within the corporate IT infrastructure.	

Table 2.1: basic information collected from users' computers

Cytomic Data Watch service features

Cytomic Data Watch deploys technology on computers that is specifically designed to collect detailed information about any PII files discovered, as well as any files defined by the administrator. This information is received by the Threat Intelligence Platform, where it is processed and enriched to be sent to the Advanced Visualization Tool for advanced visualization and presentation.

Data Discovery

- Creation of an inventory of unstructured files containing personally identifiable information, along with the number of times that each information type appears in order to assess its relevance.
- Information about the characteristics of all files discovered.
- Display of computers containing files discovered as per the monitoring rules configured by the network administrator.
- Display of the characteristics of email messages containing attachments classified as PII or which match the monitoring rules defined by the network administrator.

Data Monitoring

- Monitoring of the actions carried out on PII files or files that match any of the monitoring rules defined by the network administrator (data in use).
- Up-to-date inventory of the PII files found on each computer on the network (data at rest).
- History of attempts to copy or transfer files between computers (data in motion), indicating the means used in the operation (email client, Web browser, FTP, etc.).

Data Visualization

- Real-time synchronization to the Cytomic Data Watch server to show the results of the discovery and continuous monitoring of files.
- Tools to interpret the events recorded on PII files at rest, in use, and in motion, both in real time and retrospectively throughout their lifecycle.

Cytomic Data Watch architecture

Cytomic Data Watch comprises the following components:

- Cytomic Data Watch server **(1).**
- Computers monitored by Cytomic EDR or Cytomic EDPR **(2).**
- Advanced Visualization Tool server and Web management console **(3).**
- Network administrator computer for managing the service **(4).**
- Applications/Dashboards **(5).**
- PII knowledge tables **(6).**

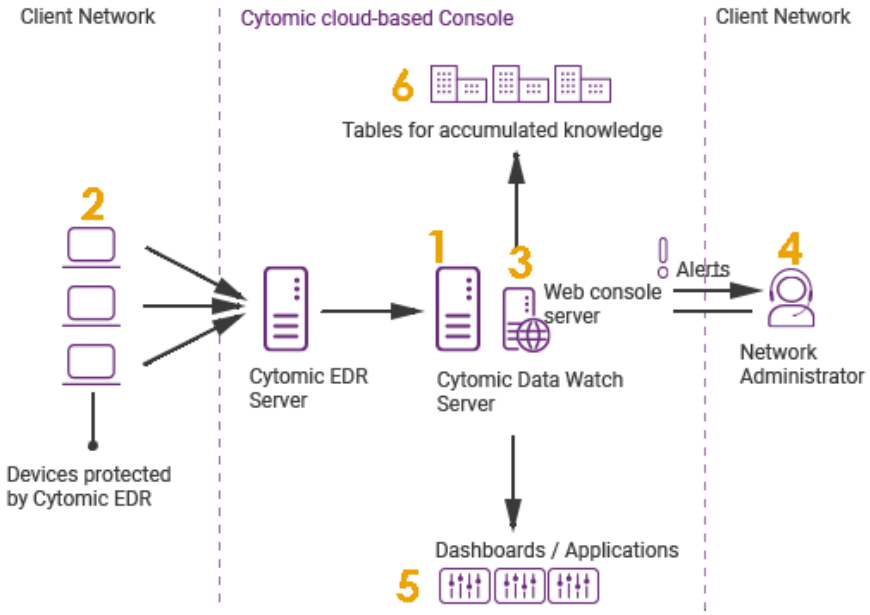


Figure 2.1: general architecture of Cytomic Data Watch

Cloud-hosted infrastructure

All the infrastructure directly involved in the service (Cytomic Data Watch server, Cytomic EDR server, and Advanced Visualization Tool server) is deployed in the Cytomic cloud, with the following advantage:

- **No maintenance costs for the customer**

As the servers do not have to be physically installed on customers' premises, customers can forget about the costs arising from the purchasing and maintenance of hardware (warranty management, technical problems, storage of spare parts, etc.).

Neither will they have to worry about costs associated with operating systems, databases, licenses, or other factors associated with on-premise solutions.

Similarly, the outlay derived from needing specialized personnel to maintain the solution also disappears.

- **Access to the service from anywhere at any time**

The service is accessible from any computer, overcoming any problems that could occur in companies with an infrastructure spared across various sites.

For this reason, it is not necessary to have specific communication deployments, such as VPNs, or special router configurations to enable access to the management console from outside the customer's local network.

- **Service available 24/7, 365 days a year**

This is a high availability service, with no limit on the number of monitored computers. Customers do not need to design or implement complex redundant infrastructure configurations. Nor do they require specific technical personnel to maintain service availability.

Cytomic Data Watch server

This is a high-availability server farm that harvests all the events related to files generated on users' computers and servers. Its main functions are to:

- Collect the information continuously monitored and gathered by the Cytomic EDR agents in real time.
- Store all the data in a table that can be easily accessed by the administrator.
- Build the data sources that will feed the charts displayed by Advanced Visualization Tool in the management console.
- Generate configurable alerts for situations that could potentially jeopardize personal data.

Protected computers and Cytomic EDR server

Users' computers continually send the actions executed by processes to the cloud-hosted Cytomic EDR server. This server automatically generates security intelligence through Machine Learning technologies on Big Data repositories. This security intelligence is added to the events collected from the protected computers and sent directly to the Cytomic Data Watch server. This operational structure provides the following advantages:

- The information received by the Cytomic Data Watch server is already processed by the Cytomic EDR server and, as such, contains the security intelligence that will help identify if the process acting on files is goodware or malware.
- Data packets are only sent once from the computers protected by Cytomic EDR, saving bandwidth and the need to install SIEM servers locally in every location, which would be much more complex and expensive to maintain.
- No additional configuration is required, neither in the Cytomic EDR console, nor on the protected computers. The Cytomic EDR servers will automatically and transparently send all necessary

information to the Cytomic Data Watch server.

To classify unstructured files, Cytomic Data Watch requires the Microsoft Office 2007 Filter Pack or later version.

*See chapter "**Hardware, software and network requirements**" on page **99** for a full list of requirements. See the following FAQ **https://www.pandasecurity.com/uk/support/card?id=50116** for more information on how to install Microsoft Filter Pack.*

Advanced Visualization Tool server and Web management console

This generates the widgets, dashboards, and graphical applications that display the collected data in an ordered and easy-to-understand way.

The server also hosts the management console, accessible from any place at any time through any ordinary compatible browser.

*For more information, see section "**Requirements for accessing the Advanced Visualization Tool console**" on page **28**.*

Advanced Visualization Tool implements functionalities through the tools and resources described below:

- A wide range of widgets that enable visualization of the actions taken on the PII files.
- Dashboards that can be configured by the administrator with information for the IT department.
- Configurable alerts that are generated in real time to reveal potentially dangerous situations.
- Graphical resources to view and work with the knowledge tables containing all information about the actions taken on the monitored files.
- Advanced tools for searching and processing the information stored: filters, groupings, advanced operations with data, generation of new widgets with information, etc.

Applications/Dashboards

The most relevant information for the IT team is displayed through the applications below, accessible from the Web management console:

- **Files and machines with PII**: Identifies PII files on the network, showing the computers they are on and the actions taken on them, both for files stored on a computer's file system or email client.
- **User monitored files**: Shows information about the files that match the monitoring rules defined by the administrator. If a file with personal data is found in an email message, information is provided about the message sender and recipient, the date the message was sent and received, etc.
- **User operations on PII files**: Shows the operations that users take on the PII files, detailing the physical device they are on (hard disk, USB drive, etc.)

- **Risk of PII extraction**: Displays actions that could represent a leak of personal data.

*For more information about applications, see chapter "**Configured applications**" on page **47**.*

PII knowledge tables

Cytomic Data Watch stores the information gathered from monitored files in several tables with the following features:

- **Raw data storage**: This is the result of the monitoring of workstations and servers, along with the security intelligence information generated by the Cytomic EDR server.
- **Continuous storage**: All processes are continuously monitored and the information sent for storage.
- **Real-time storage**.

This information is the base for generating the applications and charts displayed in Advanced Visualization Tool, allowing the filtering and transformation of data (grouping, organization, searches, etc.).

*See chapter "**PII knowledge tables**" on page **83** for more information about the meaning of each field in the tables.*

How does Cytomic Data Watch work?

To satisfy data confidentiality requirements, Cytomic Data Watch implements the service via five different processes that run on different components of the architecture shown in section "**Cytomic Data Watch architecture**":

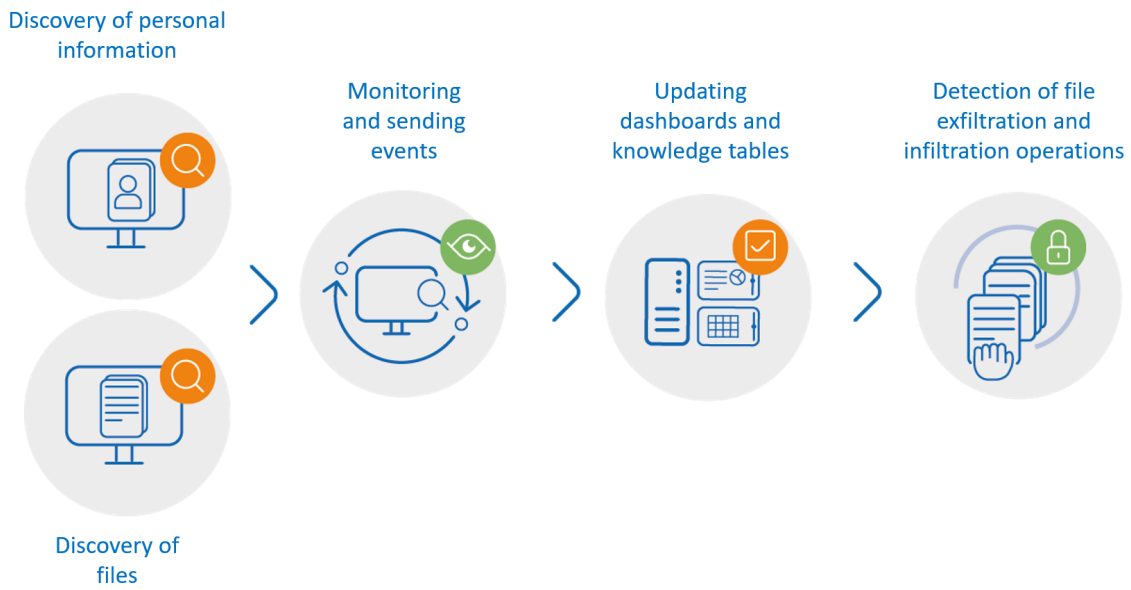


Figure 2.2: complete flow of processes in Cytomic Data Watch

Discovery of personal information

This process runs on the computers protected by Cytomic EDR. The agent scans all mass storage devices connected to the workstation or server (local hard drives, external hard drives, USB drives, and RAM disks) for unstructured files that contain personal information.

This search is launched automatically when the Cytomic Data Watch module is enabled for the first time from the Cytomic EDR management console.

> *See the Cytomic EDR online help for details on enabling Cytomic Data Watch from the management console.*

Cytomic Data Watch is designed to find those files on the network that contain personally identifiable information of customers, employees, and other natural individuals, and which require organizations to implement specific data processing protocols in order to protect the rights of data subjects.

Each word or group of words with their ow meaning referring to a certain type of personal data is called 'entity'. Cytomic Data Watch supports various types of entities, including credit card numbers, bank account numbers, and telephone numbers among many others.

Given the highly ambiguous and variable nature of natural language, each entity can have different formats depending on the language, and so it is necessary to apply flexible, adaptable algorithms for the detection of personally identifiable information. Generally, analyzing entities consists of applying a set of predefined formats or expressions to data and uses the local context surrounding the detection, as well as the presence or absence of certain keywords, to avoid false positives.

Once an entity is identified, the aforementioned information is evaluated to determine if it is enough to identify a specific user or customer and to be protected with specific processing protocols that enable the organization to comply with the applicable legislation (GDPR, PCI, etc.). This evaluation process leverages a monitored machine learning model and a mature model based on the analysis of entities and the global context of documents to finally classify a file with detected entities as a PII file to protect.

Types of personal information supported

Cytomic EDR applies Machine Learning algorithms and regular expressions to each compatible file discovered in order to detect personal information. The data recognized as PII are as follows:

- Bank account numbers.
- IP addresses.
- Addresses and ZIP/postal codes.
- Locations (cities) and countries.
- First names and last names.
- Driver's license numbers.
- Personal ID numbers.
- Passport numbers.
- Social security numbers.
- Phone numbers.
- Credit card numbers.

Supported countries

The format and content of PII data differs depending on the country of origin of the person. Currently, the following countries are supported:

- Germany.
- Austria.
- Belgium.
- Denmark.
- Spain.
- Finland.

- France.
- Hungary.
- Ireland.
- Italy.
- Norway.
- Netherlands.
- Portugal.
- Sweden.
- Switzerland.
- United Kingdom.

Mass storage devices supported

The files can be on any of the following mass storage devices:

- Local hard disks.
- USB storage devices.
- Virtual RAM drives.
- CD-ROMS, DVDs, Blu-Ray discs, etc.

File types supported

Cytomic Data Watch searches for data on the following file types:

- Office.
- OpenOffice.
- PDF.
- TXT.
- HTML.
- CSV.

*For the complete list of file extensions supported, see chapter "**Extensiones soportadas**" on page **91**.*

Data confidentiality

Once a scan is complete, Cytomic EDR sends the Cytomic Data Watch server the number of times it found each of the supported entities.

> *Neither the data file nor its partial or complete content is sent to the Cytomic Data Watch server. Consequently, data files never leave the computers on which they are hosted.*

Once the search and classification process is complete, Cytomic EDR monitors all the actions taken on PII files and reports them to the Cytomic Data Watch server.

Discovering files using monitoring rules

In addition to automatically monitoring files classified as PII, Cytomic Data Watch supports other types of files specified by the administrator using monitoring rules. These rules are entered in the Cytomic EDR console, as explained in the **Administration Guide**.

Cytomic Data Watch can also monitor email attachments, both files classified as PII and files that match the monitoring rules defined by the administrator.

Monitoring and sending events

For every action that a process takes on a file, a single event is stored with detailed information concerning the elements involved. Each generated event is defined by three parameters:

- Parent process responsible for the action.
- Action taken.
- Hash of the file containing personal data.

Process that took the action

Cytomic Data Watch stores the following information about the process that took the action on the file:

- User that launched the process.
- Process name and path.
- Hash of the process.
- Name of the computer on which the process was run and its IP address.
- Classification of the process (goodware, malware, or pending classification) to assess whether it is a potential case of data theft.

File that received the action

Except in the case of copy and paste operations, which are discussed later, Cytomic Data Watch stores the following data about the affected file:

- File name and path.
- File hash.
- Host device (local hard disk, external hard disk, USB memory, or virtual RAM drive).

Type of action

Cytomic Data Watch detects several types of actions that can affect files:

- Create.
- Open.
- Delete.
- Edit.
- Copy and paste of the file.
- Rename.

In the case of copy and paste operations, Cytomic Data Watch monitors the computer's clipboard searching for PII. A detection event will occur when the user pastes the personal data into a document and will indicate the data source and target processes.

Clipboard monitoring does not identify the data source and target files, but shows the involved processed instead.

Updating dashboards and knowledge tables

Depending on the information sent by the Cytomic EDR agents, the Cytomic Data Watch server evaluates whether the reported files contain personal data. If it is actually a PII file, all events received are accumulated to feed the various widgets in the applications. Additionally, Cytomic Data Watch sends the server all events related to files matching the monitoring rules defined by the administrator.

Finally, Cytomic Data Watch dumps all the data received into the PII knowledge tables so that the administrator can filter, search, and analyze it. This data is stored for 12 months, allowing administrators to perform full forensic analyses with the tools implemented in the Cytomic Data Watch console.

Detection of file exfiltration and infiltration operations

Cytomic Data Watch monitors certain actions taken by processes that could send or receive data. In such cases, the Machine Learning algorithms implemented in Cytomic Data Watch assess the probability that those operations are part of an unauthorized data exfiltration/infiltration attempt.

Cytomic Data Watch assigns a classification (Infiltration or Exfiltration) to the operation, indicating the high probability of a security incident to the administrator.

*See chapter "**Process list**" on page **93** for a list of the programs that can be part of an incident associated with the exfiltration or infiltration of personal data.*

Cytomic Data Watch user profile

This service is primarily aimed at the IT department of organizations and, in particular, the DPO, who can carry out some or all of the tasks below:

- Audit workstations and servers looking for PII files and other types of files containing confidential or sensitive information in storage devices connected to the computer or in email clients.
- Monitor the actions taken on audited files.Evaluate if there is a risk of data leakage, based on the user, process (goodware or malware), and the type of operation performed on the PII file.
- Detect trends that could help anticipate potential security breaches that could lead to the infiltration/exfiltration of PII files.
- Enable compliance with the GDPR.

Chapter 3

The Web console

This chapter describes the general structure of the Web management console and its components. The Web console is the main tool for administrators to view the security status of their network.

CHAPTER CONTENT

Features and access to the Web console

As a centralized Web service, the console offers a series of features that positively affect the way the IT department can work with it:

- **A single tool for leveraging data about PII**

The Web console provides preconfigured graphical tools that allow administrators to easily view all the collected information about the PII files found on the network.

This information is delivered via a single Web console, enabling the integration of various tools and removing the complexity of using products from different vendors.

- **Access to consolidated information without the need to support infrastructure across all locations**

As the server that hosts the Web console is hosted by Cytomic, there is no need to install or maintain specific infrastructure on customers' premises.

Moreover, as it is hosted in the cloud, the server can be accessed from all customers' offices, presenting consolidated data from a single repository. This simplifies data interpretation and speeds up decision making.

Requirements for accessing the Advanced Visualization Tool console

In order for you to access the Web console, your system must meet the following requirements:

- Have a certified/supported browser (others may be compatible)
- Mozilla Firefox
- Google Chrome

> *Other browsers may also work, but some of their versions may not be supported. As such it is advisable to use one of the browsers listed above*

- Internet connection and communication through port 443.
- Minimum screen resolution 1280x1024 (1920x1080 recommended).
- A sufficiently powerful computer to generate charts and lists in real time.
- Sufficient bandwidth to display all the information collected from users' computers in real time

Accessing the Advanced Visualization Tool Web console

The **Advanced Visualization Tool** Web console can be accessed via SSO from the **Cytomic EDR** management console, with no need to enter new credentials.

Follow the steps below to access the environment:

- Click the **Status** menu at the top of the Web console.
- From the side panel, click **Advanced Visualization Tool**.

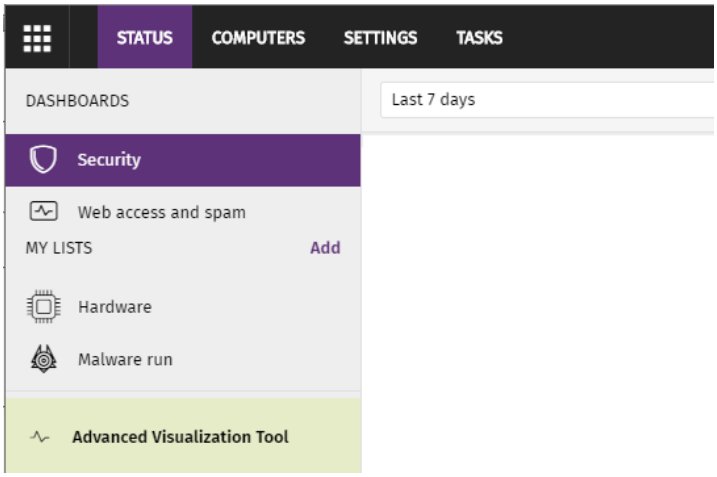


Figure 3.1: accessing the Advanced Visualization Tool service from the Cytomic EDR console

Structure of the Advanced Visualization Tool Web console

The Web console is designed to deliver a uniform and coherent experience to administrators, both in terms of visualization and the search for information as well as configuring custom data widgets. The end goal is to deliver a simple yet powerful and flexible tool that allows administrators to rapidly view the status of the personal data stored in the organization's unstructured files without a steep learning curve.

Side menu overview

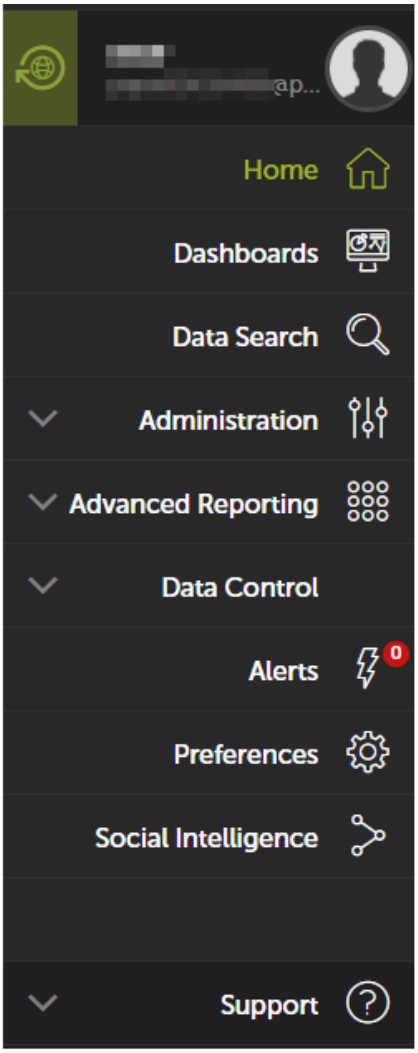


Figure 3.2: side menu

The side menu is located to the left of the screen and can be accessed at any time.

Initially, this menu only displays the icons for each option. By moving the mouse pointer to the left of the screen, or clicking a free section of the side menu, a description of each icon is displayed.

Below you can see the main options of the side menu:

Home

This takes users back to the Home page of the Web console.

Data Search

This lets you access the accumulated knowledge table. From here, administrators can view the data as it has been sent from the computers protected by Cytomic EDR.

As administrators access the knowledge tables, they appear under the Search option as shortcuts, to make it easier to access them

.

> *See chapter "**PII knowledge tables**" on page **83** for more information about the fields included in the accumulated knowledge table*

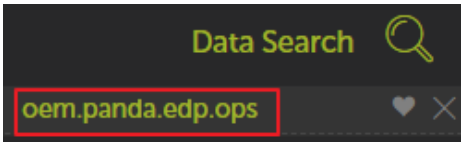


Figure 3.3: shortcut to the knowledge table

Administration

This lets you configure new alerts.

> *For more information about pre-configured alerts, see section "**Predefined alerts**" on page **64**. For more information about how to create and configure new alerts, see section "**Creating alerts**" on page **69**.*

Advanced Reporting

Drop-down menu with the available applications for Cytomic Insights.

> *For more information, refer toCytomic Insights guide.*

Data Control

This includes the applications described below:

- **Files and machines with PII**: This displays the workstations and servers that contain PII files, the PII files found on the network, and the processes that have performed operations on them.
- **User operations on PII files**: This displays the actions taken by users on PII files, and the physical device where the personal data resided (internal hard drive, USB drive, etc.).
- **Risk of PII extraction**: Suspicious operations that could lead to a personal data breach.

Alerts

This displays a window with information about the alerts received.

Preferences

This section offers a series of options that can be configured for the logged-in user and for others that access the service.

Log out

Here you can log out of the Cytomic Data Watch console. It then displays the IDP (Identity Provider) login screen.

Part 2

Cytomic Data Watch resources

Chapter 4

Introduction to the applications

The dashboards are preconfigured applications that provide the network administrator with specific information about the network.

The dashboards included in the Web management console are as follows:

- Files and machines with PII
- User operations on PII files
- Risk of PII extraction

All the dashboards have a common layout, described later in this section, in order to facilitate data interpretation.

The applications also generate alerts that warn administrators in real time of potential problems.

> *To create new alerts in addition to those that are already configured in the applications, see section "**Predefined alerts**" on page **64**.*

CHAPTER CONTENTS

Accessing applications and alerts

Accessing the dashboards/applications

Access to the dashboards is available through the side menu, in the **Cytomic Data Watch** section.

The **Alerts Subscription** screen is used to look for configured alerts, to assign policies, and enable and disable individual alerts.

Resources and common dashboard items

Time periods for the data displayed

Each application has two controls for defining the time period for the data displayed on screen:

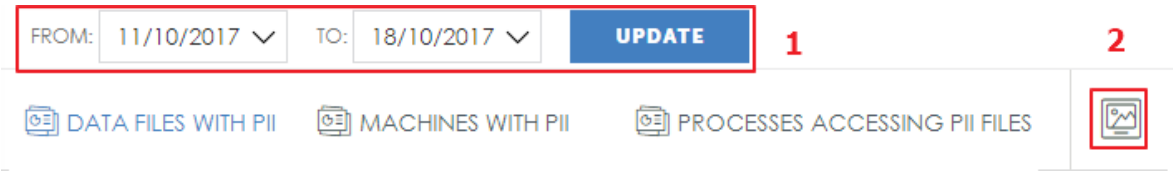


Figure 4.1: date range picker

- **Date range (1):** This lets you set the time period displayed in the widgets of the selected dashboard. The period will apply to the widgets of all the tabs on the dashboard.
- **Screenshot (2):** This opens an independent window with the content of the tab in graph format so it can be downloaded and printed.

> *The browser pop-up protection may prevent you from seeing the new window. Disable this feature in the browser in order to see the window*

The browser pop-up protection may prevent you from seeing the new window. Disable this feature in the browser in order to see the window.

Tabs

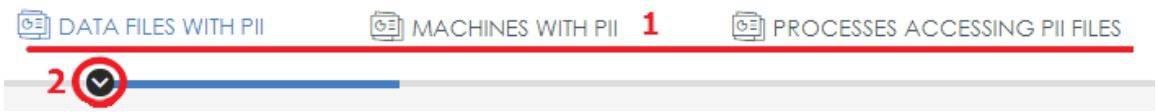


Figure 4.2: console tabs

The tabs divide the information into different areas according to the level of detail of the data displayed: general information or more detailed reports and data breakdowns.

Each tab offers access to the tools displayed below:

- **Tab name (1):** This describes the information contained in the tab. To select a tab, simply click on the name. The **Detailed information** tabs contain data tables that can be used in reports.
- **Shortcut menu (2):** Click the arrow to display a drop-down menu that takes you directly to any section within the tab.

Sections

The information within a tab is divided into sections. Each section is a group of widgets with related information.

Click the arrow button to display or hide a complete section.

Figure 4.3: accessing a tab's sections

Widgets

These are controls that display the data using tables and advanced graphs.

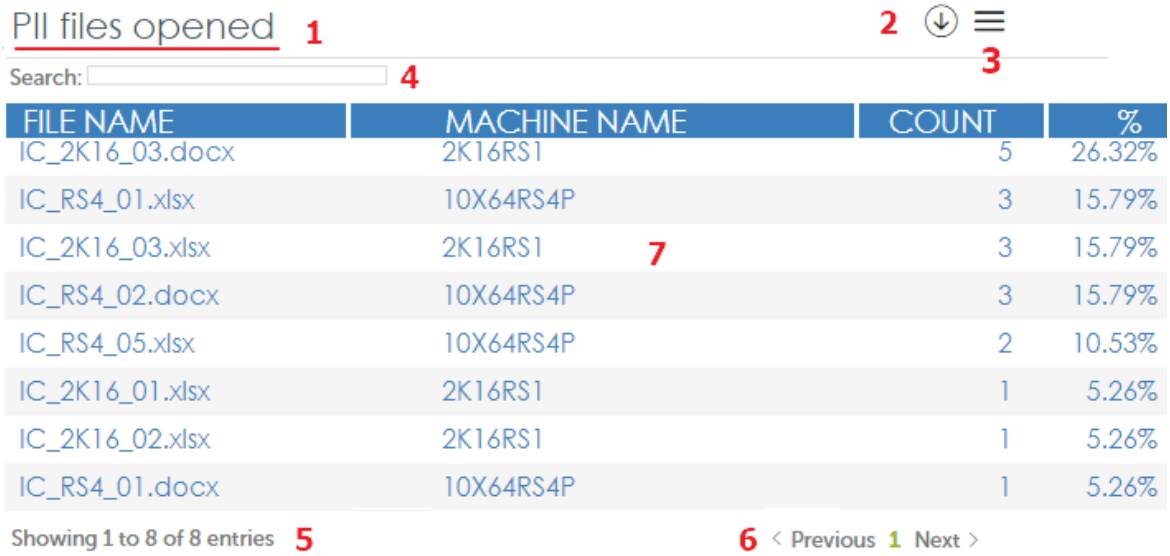


Figure 4.4: console widget

Each widget comprises the following items (some may be missing depending on the widget type):

- **Widget name (1)**: This indicates the type of information displayed.
- **Display/hide button (2)**: This lets you hide or display the widgets you want.
- **Widget menu (3)**: This contains four options:
  - **Screenshot**: This opens the widget content on a new page so it can be saved as a graph, printed, etc.

> *The browser pop-up protection may prevent you from seeing the new window. Disable this feature in the browser in order to see the window*

  - **Download Data**: This downloads the data viewed with the widget. The data is downloaded in .CSV format separated by commas, so it can be imported into other applications.
  - **Zoom**: enlarges the size of the selected widget.
  - **Go to query**: This displays the knowledge table associated with the widget and which is the source for its data, along with the settings for the filters, groups and operations.

> *The Go to query option lets you see the precise configuration of the data source that feeds the widget, including the selected time period. This way, administrators can experiment with the chart displayed using the SQL statement. More information is available later in this chapter.*

- **Support**: Support window with hotkeys assigned to the widgets to browse the data displayed.
- **Search (4)**: text box for filtering the widget content.
- **Summary (5)**: in table widgets, this indicates the number of rows displayed.
- **Pagination controls (6)**: in table widgets, they let you move forward and backwards from one set of rows to another.
- **Information item (7)**: tables and charts of various types that display information.

Widget types

The data is represented through a range of charts (Voronoi diagram, line and bar charts, pie charts, etc.) and more detailed data tables.

Counter

Figure 4.5: counter widget

This is the simplest type of widget. It shows the number of occurrences of a certain event over a period of time.

Calendar charts

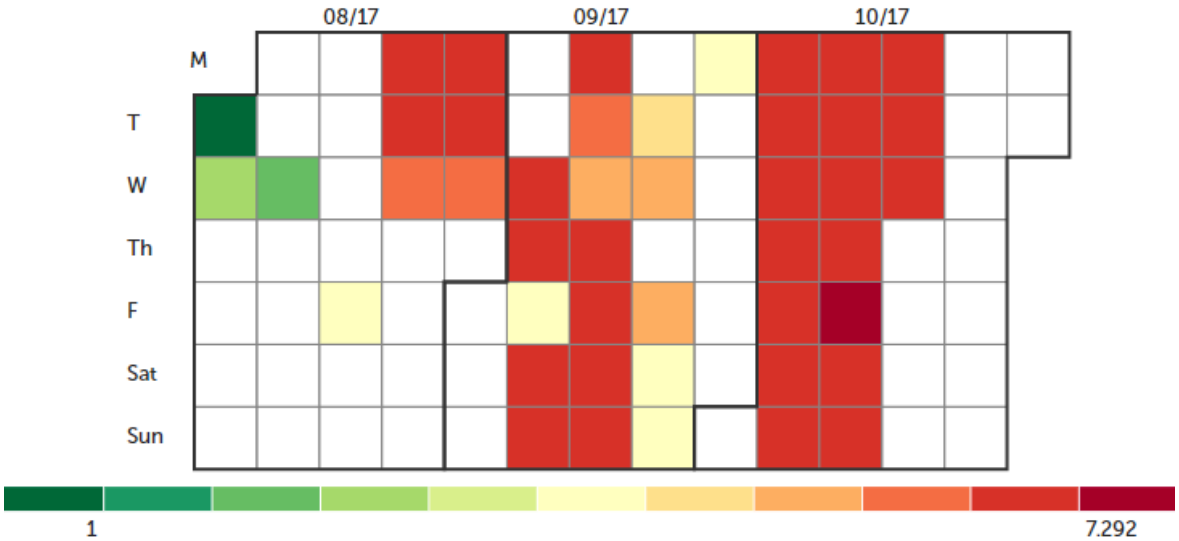


Figure 4.6: calendar chart

This represents the real values of the events detected throughout a year.

Each box represents a day in each month. The boxes are grouped into blocks that represent the months of the year.

In turn, each box is colored according to the number of events in the day. The color range (green - red) lets you quickly compare days against each other, thereby giving a better view of the development of the indicators monitored.

Move the mouse pointer over a box to see the corresponding color in the key, and a tooltip with the date and the exact number of events.

Bar chart

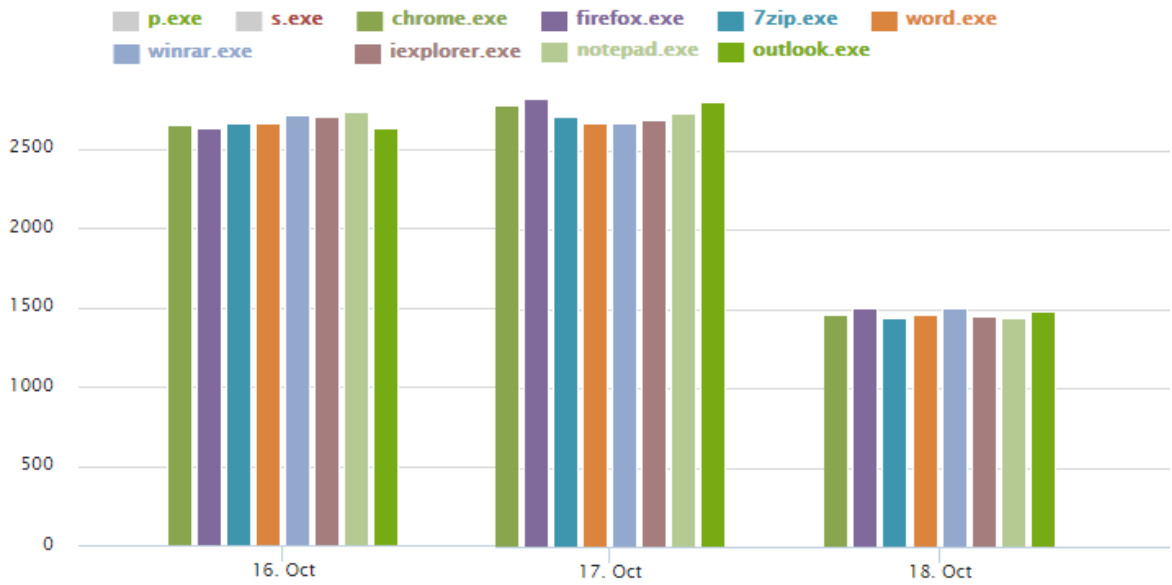


Figure 4.7: bar chart

Bar charts let you see, in a single chart, the development of several different concepts, represented by different colors in the key at the top of the chart.

Place the mouse pointer over the data and a tooltip will indicate the date and time of the measurement and the value of the concept at that moment.

Line chart.

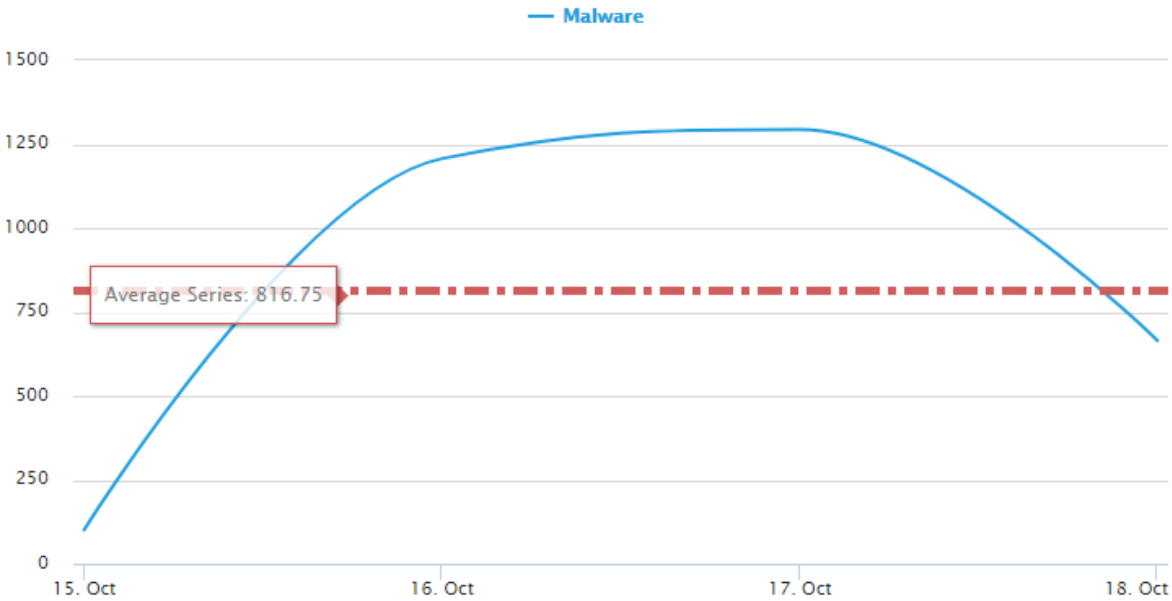


Figure 4.8: Line chart

Shows the development or evolution of one of several concepts, represented by different colors in the key at the top of the chart.

Place the mouse pointer over the data and a tooltip will indicate the date and time of the measurement and the value of the concept at that moment

Frequency table

Top 10 PII files opened

FILE NAME	COUNT	%
Sample1PII.rtf	192	24.49%
Sample1PII.docx	136	17.35%
Sample3_PII.rtf	96	12.24%
Sample2_PII.txt	48	6.12%
Sample1PII (2).zip	40	5.10%
Sample1PII.doc	40	5.10%
Sample1PII.zip	40	5.10%
Sample1PII.odp	24	3.06%
Sample1PII.pptx	24	3.06%
Sample1PII.ppt	24	3.06%

Figure 4.9: frequency table

This table displays the number of times that a specific type of event has occurred in a defined period of time. The values displayed can be absolute numbers (Count), relative numbers expressed as a percentage of the total number of recorded events (%), or both

The first line in the table shows the column headers plus the icon for sorting the data in ascending or descending order.

Voronoi diagram

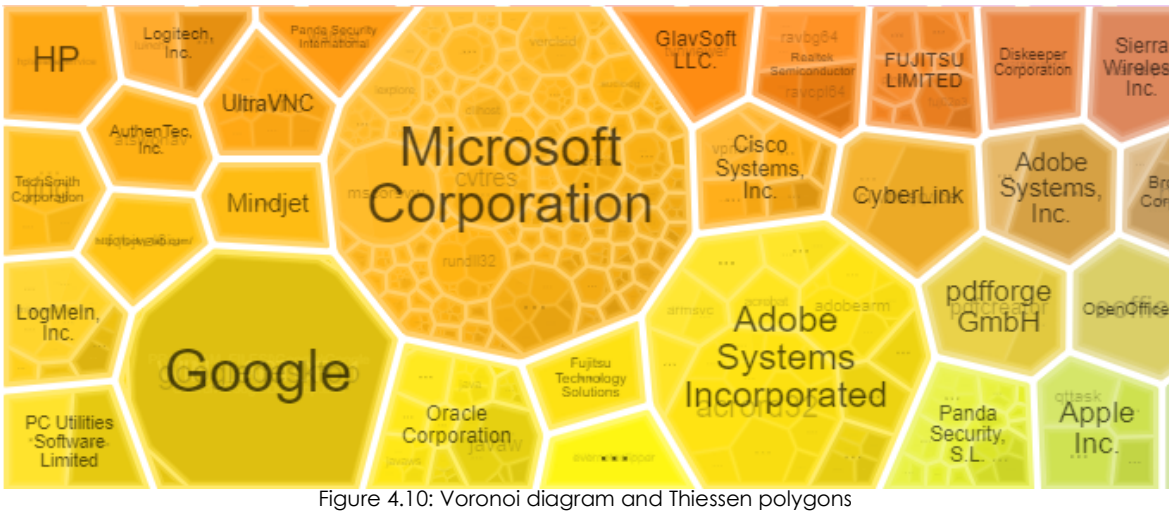


Figure 4.10: Voronoi diagram and Thiessen polygons

A Voronoi diagram shows information from the corresponding knowledge table in the form of groups of data. It uses polygons of various shapes and sizes whose area represents a relative (percentage) number of items shown inside.

- **Navigating a Voronoi diagram**

A polygon can comprise other polygons representing groups of lower-level data.

As such there is a hierarchy of levels of groups ranging from the more general to the more specific. Voronoi diagrams allow you to navigate through the different levels of data groups:

- Double-click using the left mouse button on a group of data to access the lower level.
- From there, double-click using the right mouse button to return to the previous level.

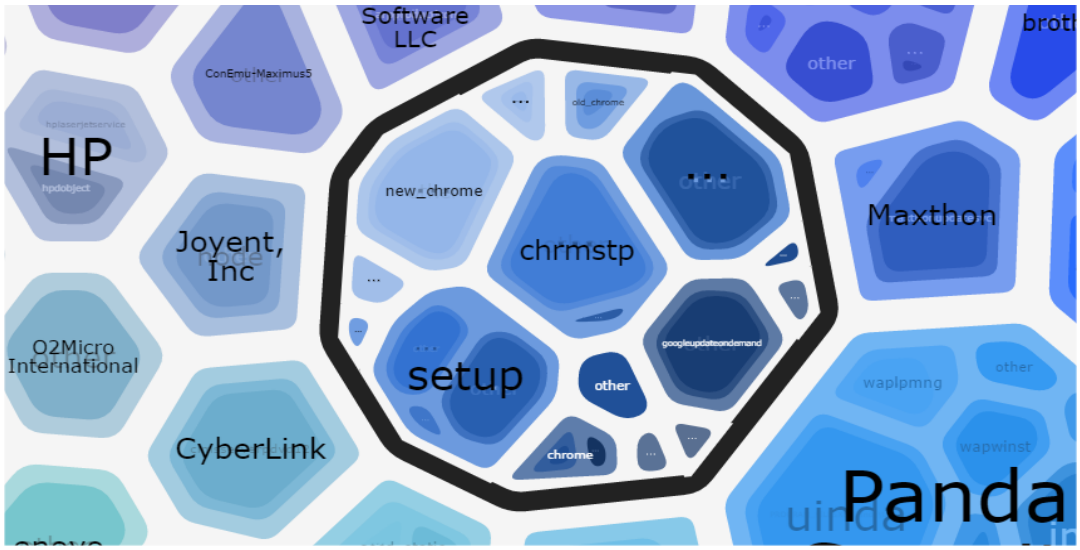


Figure 4.11: zooming in into a polygon by double-clicking on it

Place the mouse pointer on a group to display the number of items in the group and the percentage that they represent of the total.

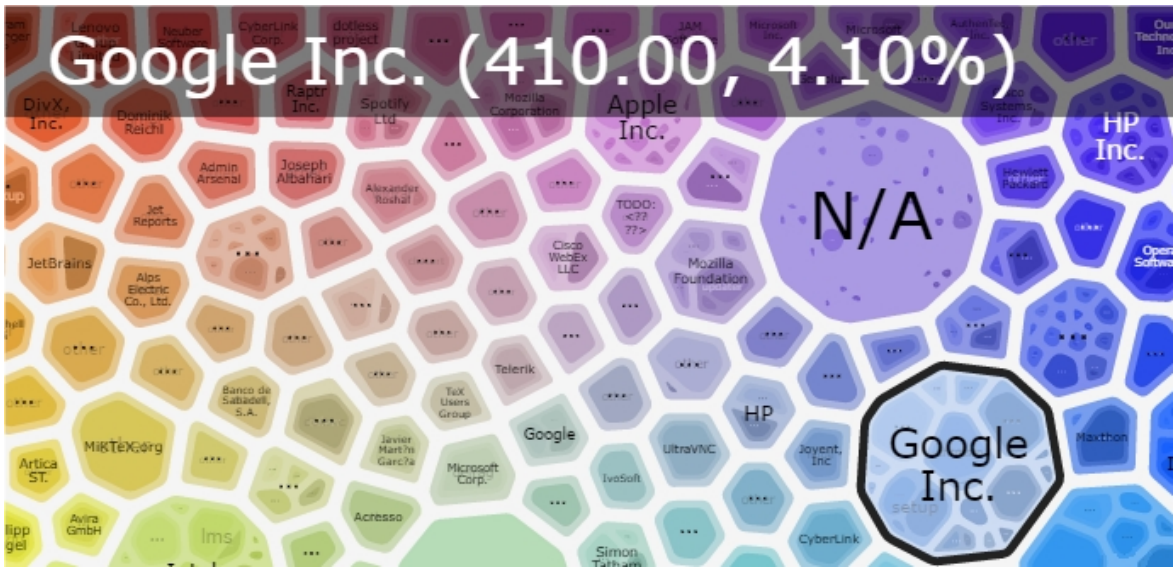


Figure 4.12: data displayed within a polygon

- **Diagram controls**

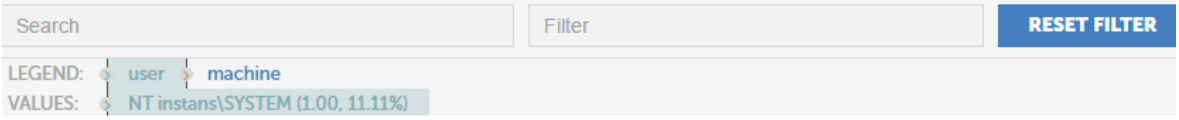


Figure 4.13: controls for configuring the data displayed in a Voronoi diagram

A widget containing a Voronoi diagram offers the following controls:

Control	Description
Search	This finds a polygon in the Voronoi diagram, and expands it to show the groups it comprises. This is the same as double-clicking with the left mouse button on a polygon in the diagram. To undo a search, double-click with the right mouse button.
Filter	This shows the polygons that contain groups coinciding with the filter criteria.
Reset filter	This clears the filter. It does not undo searches. To undo a search, double-click with the right mouse button.
Legend	This indicates the knowledge table fields used to group the information displayed. The order of the fields indicates the group hierarchy and can be altered simply by dragging them to the left or right to establish a new hierarchy.
Values	In combination with the fields shown in the **Legend** control, this indicates the value of a specific field. By selecting a polygon, either with the search tool, or by double-clicking it, the **Values** field will take the value of the search or the selected polygon.

Table 4.1: Voronoi diagram controls

When navigating a Voronoi diagram, the highlighted field in **Legend** will take the value of the selected polygon. The adjacent fields will indicate the data layer that will be accessed upon double-clicking it using the left mouse button (drill down to the value shown on the right of the highlighted field), or upon double-clicking it using the right mouse button (exit to the value shown on the left of the highlighted field).

- **Sample Voronoi diagram**

The following example illustrates how a Voronoi diagram works.

Depending on the **Legend**, the starting point is a chart that groups the data in the following order:

- **Level 1 AlertType**: indicates the type of threat detected on the network.
- **Level 2 Machinename**: indicates the name of the computer where the threat was detected.
- **Level 3 executionStatus**: indicates whether or not it was executed.
- **Level 4 itemPath**: indicates the file path and name.

- **Level 5 itemName**: indicates the name of the threat.

Figure 4.14: example of the first data layer in a Voronoi diagram

At first, the diagram displays Level 1: the data grouped by **AlertType**, the first **Legend** field, highlighted in blue.

The second legend field is **MachineName,** so by double-clicking on one of the **AlertType** groups in the diagram (e.g. Malware) the second level will be displayed grouping the data according to **MachineName**. The Voronoi diagram will look like this:

The **Values** field is refreshed displaying the **Level 1** selection (**AlertType=Malware**) and its content, the **Level 2**, with the data grouped by **MachineName**, highlighted in blue.

Follow this process to navigate through the Voronoi diagram up to the last level, or move backwards through the diagram by double-clicking with the right mouse button.

If you want to establish an alternative order of grouping, simply drag the fields shown in **Legend** to the left or to the right in order to set the new order.

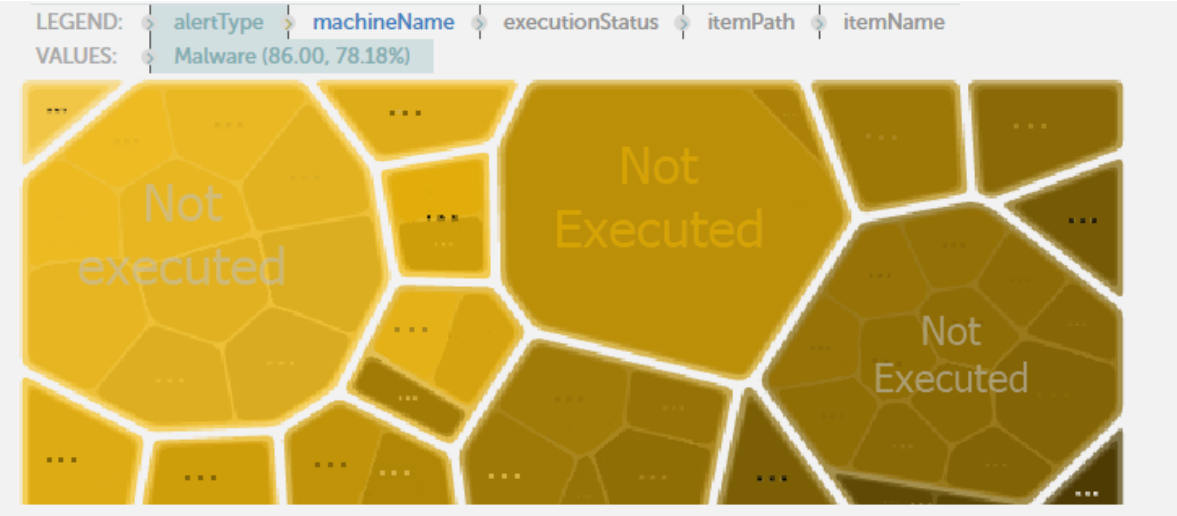


Figure 4.15: example of the second data layer in a Voronoi diagram

For example, if you want to first determine which computers have run some type of malware and then the name of the threat -in order to determine its characteristics-, then finally the computers on which it was executed, you can configure the grouping order as follows:

- Level 1 ExecutionStatus
- Level 2 ItemName
- Level 3 Machinename

Figure 4.16: new configuration for an alternative order of grouping

By double-clicking **Executed** in the Voronoi diagram, you can see the names of the items run; clicking one of these will display the computers on which it has been executed.

Generating new charts based on the widgets provided

By clicking the ☰ icon in each widget and selecting **Go to Search,** the corresponding knowledge table that feeds that widget will open.

Each knowledge table has a series of transformations, filters and groups designed to present the most important data clearly and accurately. These transformations are in SQL language and can be edited to adapt to the customer's needs.

> *It is not possible to overwrite the widgets provided, but you can generate new widgets using the original ones as a base.*

Modifying the SQL statement associated with a widget

Once you are in the knowledge table associated with a widget, click the icon in the toolbar. A window with the preset SQL statement will open. After editing the statement, click **Run** to test the execution. The data in the table will be updated immediately.

You can also modify the SQL statement by adding new filters, groups and data transformations via the toolbar.

SQL statement favorites

After changing the SQL statement and ensuring that the generated data is correct, it can then be saved for later access, by marking it as a **Favorite**. To do this, follow these steps:

- Opening a knowledge table will display a new entry in the sidebar, below the **Search** icon.
- A heart icon will be displayed to the right of the name of the entry.
- Click this icon and the SQL statement will be marked as **Favorite**, and will appear in the list of favorites

Favorites can be found in the side menu **Administration**, **Alerts Configuration**.

Chapter 5

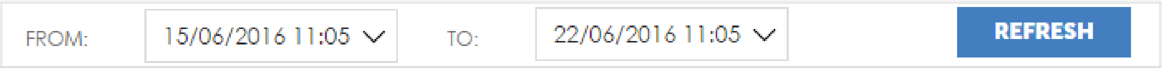
Configured applications

This chapter describes how the applications provided with Cytomic Data Watch operate, regarding the interpretation of both charts and tables.

CHAPTER CONTENT

Setting the time period

The three applications provided have a control option at the top of the screen to allow you to set the data time period.



FROM: 15/06/2016 11:05 TO: 22/06/2016 11:05

Figure 5.1: date range picker

Administrators must select the most appropriate time interval to view the status of the personal data held by the company. The various widgets and time intervals will help the administrator spot suspicious trends.

Wider date ranges

When the date range set is wider (months or days), the data will be displayed as a history or an evolution of activity over time.

Narrower date ranges

By selecting a narrower range of dates, such as the current day, administrators can determine the current status of the personal data held by the company, but will lose the perspective of data over time.

Files and machines with PII

Finds those files and computers on the network that store confidential information, and shows those processes that act on it. It is divided into three tabs: **Data files with PII**, **Machines with PII** and **Processes accessing PIIF**. Each of these tabs is described below.

Data files with PII

Shows the personal data files found on the organization's workstations and servers.

It is divided into two sections:

- **General View**: shows a summary of the PII files found, the computers that store them and how they have been used.
- **Files reclassified as not having PII**: shows those PII files that have undergone a change of status.

General view

This diagram shows those computers on the network that contain most personal data files, and provides additional information such as users, files and operations performed. The Voronoi diagram lets you drill down into each computer to access the various information layers.

- **Aim**: to give an overview of those computers in the organization that store most PII files.
- **Type of widget**: Voronoi diagram.
- **Data displayed**:

Level	Description
First level (machineName)	Workstation/server name.
Second level (user)	Name of the computer user.
Third level (op)	Type of operation performed on the PII file.
Fourth level (Extension)	PII file extension.
Fifth (document)	Shows the specific document.

Table 5.1: 'General view' widget data

- **Grouping**: computer, user, operation, extension.

Distribution of PII files by extension

This widget shows the types of personal data files most used in the organization. This information can be used to update corporate security policies in order to prevent the use of certain file formats deemed not safe enough to store customer or user information.

- **Aim**: to show the format of the files where personal data is most frequently found.
- **Type of widget**: pie chart.
- **Data displayed**: PII files grouped by extension.
- **Grouping**: file extension.

PII files opened

This widget shows the PII files most frequently accessed over the selected time period. It helps administrators identify frequently accessed files that may need additional security measures or access restrictions.

- **Aim**: to show those files most frequently accessed and which contain personal data.

- **Fields**:

Level	Description
File name	PII file name.
Machine name	Name of the computer where the PII file resides.
Count	Counter showing the number of events.
%	Accesses to the file as a percentage of the total accesses to PII files on the network

Table 5.2: fields in the 'PII files opened' widget

Files reclassified as not having PII

- **Aim**: to show those files initially classified as PII, but which later were reclassified due to an update of the Cytomic Data Watch algorithm.
- **Fields**:

Level	Description
User	User account who accessed the PII file.
Machine name	Name of the computer where the PII file resides.
Machine IP	IP address of the computer where the PII file resides.
File name	PII file name
Count	Counter showing the number of occurrences on the network.

Table 5.3: fields in the 'Files reclassified as not having PII' widget

Machines with PII

This tab shows the computers on the network with most activity on personal data files. The information is divided into two sections:

- **Most active machines**: shows the workstations and servers with most activity on PII files.
- **Machines with malware**: shows the workstations and servers with PII files accessed by processes classified as malware by Cytomic EDR.

Top 10 machines with operations on PII files

This widget shows the 10 computers where most PII file operations have taken place regardless of the type of action (open, copy, move, etc.). It allows administrators to identify the computers where most personal data files are accessed in order to establish specific control measures.

- **Aim**: To show the 10 computers with most operations on PII files.

- **Fields**:

Field	Description
Machine name	Workstation/server name.
Count	Number of PII file operations performed over the selected period.
%	Number of PII file operations performed on the computer as a percentage of the operations performed on all computers on the network.

Table 5.4: fields in the 'Top 10 machines with operations on PII files' widget

Top 10 machines with exfiltration operations

This widget shows the 10 computers that have sent most personal data files out of the network. This information allows administrators to detect massive data leaks from certain computers.

- **Aim**: To show the computers from which most personal data files have been sent out of the network.
- **Fields**:

Field	Description
Machine name	Name of the workstation or server from which personal data has been extracted.
Count	Number of exfiltration events.
%	Exfiltration events per machine as a percentage of the total number of exfiltration events registered on the entire network.

Table 5.5: fields in the 'Top 10 machines with exfiltration operations' widget

Top 100 machines sending attachments with PII

- **Aim**: To show the 100 computers that have sent most email messages with attachments classified as PII.
- **Fields**:

Field	Description
Machine	Name of the computer from which attachments with PII were sent.
Count	Number of attachments with PII sent.
%	Number of attachments with PII sent from the computer as a percentage of the total number of attachments with PII sent from all computers on the network

Table 5.6: fields in the 'Top 100 machines sending attachments with PII' widget

Machines with malware accessing PII files

This widget shows the 10 computers where most malicious processes have been detected accessing personal data. This information allows administrators to detect infected computers and assess the impact of any incident affecting personal data, as demanded by the GDPR.

- **Aim**: to show the computers where most personal data files have been accessed by processes classified as malware.
- **Fields**:

Field	Description
Machine name	Workstation/server name.
Count	Number of accesses.
%	Accesses per computer as a percentage of the total number of accesses detected on all computers on the network.

Table 5.7: fields in the 'Machines with malware accessing PII files' widget

Processes accessing PII files

This tab is divided into two sections:

- **Processes accessing PII**: shows the processes found on the network that have accessed personal data files.
- **Malware processes**: shows the processes that have accessed personal data and have been classified by **Cytomic EDR** as malware.

Top processes accessing PII files

This widget shows a history of the processes that have performed most operations on PII files. This information allows administrators to detect anomalous increases in the number of operations which may indicate a massive data exfiltration/infiltration attack.

- **Aim**: To show the 10 processes most frequently used to operate on PII files.
- **Type of widget**: Bar chart.
- **Data displayed**: History of the number of operations performed on PII files, grouped by the top 10 processes used to perform them.
- **Grouping**: Process.

Number of malware processes accessing PII files

This widget allows administrators to anticipate security incidents associated with data theft (by Trojans, APTs) or data hijacking (ransomware).

- **Aim**: To show the evolution of the number of accesses to PII files by processes classified as malware by Cytomic EDR.

- **Type of widget**: Line chart.
- **Data displayed**: Evolution of the total number of operations performed on PII files. Monthly access average.
- **Grouping**: Processes classified as malware.

Distribution of processes by category

This widget compares the number of safe processes to the number of malware processes, allowing administrators to detect deviations that may indicate an attack on the organization.

- **Aim**: To show the number of processes classified as malware compared to the rest of processes.
- **Type of widget**: Pie chart.
- **Data displayed**: Percentage of safe vs malicious processes.
- **Grouping**: Process classification (malware, goodware, suspicious).

User operations on PII files

Shows the types of operations performed on the personal data files run in the organization as well as the type of device that contained the data (fixed or mobile device).

User operations

- **User operations**: Shows the types of operations performed on personal data files, and the users involved in data exfiltration/infiltration operations.
- **Types of operations**: Shows the types of operations performed on personal data files, as well as the type of device that contained the data (fixed or mobile device).

User operations on PII files by device type

This widget shows a full list of the users that have handled PII files stored on any type of device in the organization. This information enables administrators to establish additional security measures for those users who use most personal data or store it on mobile devices.

- **Aim**: To show the users that have performed operations on personal data files as well as additional information.
- **Fields**:

Field	Description
User	User account who ran the program that accessed the personal data file.

Table 5.8: fields in the 'User operations on PII files by device type' widget

Field	Description
DeviceType	Type of device that contained the accessed file. Refer to chapter "**PII knowledge tables**" on page **83** for more information about the **DeviceType** field and the values it can take.
Operation	Operation performed on the PII file. Refer to chapter "**PII knowledge tables**" on page **83** for more information about the **Operation** field and the values it can take.
Count	Number of operations performed by the user of the relevant type and on the relevant type of device.
%	Operations as a percentage of the total number of registered operations.

Table 5.8: fields in the 'User operations on PII files by device type' widget

Calendar of user operations on removable drives

This widget monitors the operations performed on personal data files residing on removable drives, showing their evolution over the last month. This information can be used to identify potential data leaks since the devices monitored in the widget are removable.

- **Aim**: To show the evolution of the operations performed on personal data files residing on external storage devices.
- **Type of widget**: Calendar chart.
- **Data displayed**: Number of operations performed on PII files residing on external devices, grouped by day of the month.
- **Grouping**: Day of the month.

Users involved in exfiltration operations

This widget shows the number of data exfiltration/infiltration operations per network user. This information allows administrators to identify those users who are accessing and using personal data unlawfully.

- **Aim**: To show the number of data exfiltration/infiltration operations per user.
- **Fields**:

Field	Description
User	User account who ran the program that exfiltrated/infiltrated personal data files.
Exfiltration flag	Indicates whether the operation performed on the PII file was data exfiltration or infiltration.
Count	Number of registered operations of the relevant type.
%	Operations as a percentage of the total number of registered operations.

Table 5.9: fields in the 'Users involved in exfiltration operations' widget

Types of operations

Distribution of types of operations on PII files

This widget shows the most common operations performed on personal data files. This information enables administrators to identify deviations from the usual number of operations that may indicate a security breach.

- **Aim**: To show the percentage of the various types of operations performed on personal data files.
- **Type of widget**: Pie chart.
- **Data displayed**: The percentage of each type of operation.
- **Grouping**: Operation type.

Distribution of operations on removable devices

This widget gives an indication of the danger level of the operations performed on personal data files. If the higher percentage of operations takes place on removable devices, the administrator will be able to take measures aimed at reducing the likelihood of a data breach.

- **Aim**: To compare the percentage of operations performed on personal data files residing on removable devices with the percentage of operations performed on personal data files residing on fixed devices.
- **Type of widget**: pie chart.
- **Data displayed**: percentage of operations performed on fixed and removable devices.
- **Grouping**: type of device.

Most active users

Shows the users in the organization most likely to be responsible for a data breach based on the number of operations they perform on personal data files and the malware run on their devices.

- **Active users by operation type**: shows the users that have performed most operations on PII files.
- **Top users running malware**: shows the users that have run most processes classified as malware.

Top 10 users involved in create operations

This widget helps administrators identify those users who have generated most unstructured personal data files in the organization.

- **Aim**: to show the users that have created most personal data files.

- **Fields**:

Field	Description
User	User account who ran the program that created the personal data file.
Count	Number of registered operations of the relevant type.
%	Operations as a percentage of the total number of registered operations.

Table 5.10: fields in the 'Top 10 users involved in create operations' widget

Top 10 users involved in open operations

- **Aim**: to show the users who have accessed most personal data files.
- **Fields**:

Field	Description
User	User account who ran the program that opened the personal data file.
Count	Number of registered operations of the relevant type.
%	Operations as a percentage of the total number of registered operations.

Table 5.11: fields in the 'Top 10 users involved in open operations' widget

Top 10 users involved in copy-paste operations

- **Aim**: to show the users who have performed most copy-paste operations with personal data files.
- **Fields**:

Field	Description
User	User account who copied-pasted the personal data file.
Count	Number of registered operations of the relevant type.
%	Operations as a percentage of the total number of registered operations.

Table 5.12: fields in the 'Top 10 users involved in copy-paste operations' widget

Top 10 users involved in rename operations

- **Aim**: to show the users that have renamed most personal data files.
- **Fields**:

Field	Description
User	User account who renamed the personal data file.
Count	Number of registered operations of the relevant type.

Table 5.13: fields in the 'Top 10 users involved in rename operations' widget

Field	Description
%	Operations as a percentage of the total number of registered operations.

Table 5.13: fields in the 'Top 10 users involved in rename operations' widget

Top 10 users running malware

This widget shows the users that use infected workstations or servers and launch processes classified as malware with their credentials, either voluntarily or involuntarily (botnets, accidental infections, etc.).

- **Aim**: To show the users who have performed most operations on personal data files using processes classified as malware.
- **Fields**:

Field	Description
User	User account who ran the malware that accessed personal data.
Count	Number of registered operations of the relevant type.
%	Operations as a percentage of the total number of registered operations.

Table 5.14: fields in the 'Top 10 users running malware' widget

Top 100 users sending attachments with PII

- **Aim**: To show the 100 users that have sent most email messages with attachments classified as PII.
- **Fields**:

Field	Description
User	Name of the user that sent email messages with attachments classified as PII.
Count	Number of attachments with PII sent.
%	Number of attachments with PII sent by the user as a percentage of the total number of attachments with PII sent by all users con the network.

Table 5.15: fields in the 'Top 100 users sending attachments with PII' widget

Top 100 users receiving attachments with PII

- **Aim**: To show the 100 users that have received most email messages with attachments classified as PII.
- **Fields**:

Field	Description
User	Name of the user that received email messages with attachments classified as PII.
Count	Number of attachments with PII received.

Table 5.16: fields in the 'Top 100 users receiving attachments with PII' widget

Field	Description
%	Number of attachments with PII received by the user as a percentage of the total number of attachments with PII received by all users con the network.

Table 5.16: fields in the 'Top 100 users receiving attachments with PII' widget

Risk of PII exfiltration

Shows the operations performed on personal data files that Cytomic Data Watch classifies as involving a risk of data exfiltration/infiltration.

Risk of exfiltration

Number of operations with files at risk of exfiltration

This widget shows the evolution of the accesses to personal data files classified by **Cytomic Data Watch** as unauthorized data exfiltration/infiltration. A sudden spike on the chart may represent a data breach in the organization.

- **Aim**: to show the evolution of accesses to PII files classified as data infiltration, exfiltration or both.
- **Type of widget**: line chart.
- **Data displayed**: operations classified as unauthorized exfiltration or infiltration of data.
- **Grouping**: action type (infiltration, exfiltration, both).

Operations with files at risk of exfiltration and infiltration

- **Aim**: to compare the percentage of data exfiltration operations, data infiltration operations and operations combining both data exfiltration and infiltration.
- **Type of widget**: pie chart.
- **Data displayed**: percentage of each type of operation.
- **Grouping**: operation type.

Top 10 largest files at risk of exfiltration

Operations performed on large personal data files pose a bigger threat as they may result in a massive data breach. These operations must be monitored and controlled very closely.

- **Aim**: to show a list of the largest personal data files that have been accessed in your organization.

- **Fields**:

Field	Description
Document name	Name of the PII document.
User	User account who accessed the document.
Machine IP	IP address of the computer where the PII file resides.
Machine Name	Name of the computer where the PII file resides.
Document size (MB)	Document size (in megabytes).

Table 5.17: fields in the 'Top 10 largest files at risk of exfiltration' widget

User monitored files

Shows aggregated information about the files found on the network as per the monitoring rules defined by the administrator, and the email messages that contain them. For information on how to manage monitoring rules and enable/disable the tracking of email messages containing monitored files, go to the Cytomic EDR Web console and see the `Administration Guide`.

Files

Top 100 rules with most operations on monitored files

- **Aim**: To show the 100 rules that have generated most monitored operations. This widget can be used to determine how effective the rules defined by the administrator are in finding files on the customer's network.
- **Fields**:

Field	Description
Rule	Name of the file monitoring rule.
Count	Number of operations recorded by the rule.
%	Number of operations recorded by the rule as a percentage of the total number of operations recorded by all monitoring rules.

Table 5.18: fields in the 'Top 100 rules with most monitored operations on files' widget

Top 100 monitored files with most operations

- **Aim**: To show the 100 files for which most operations have been recorded by the monitoring rules defined.

- **Fields**:

Field	Description
File Name	Name of the monitored file.
Count	Number of recorded operations for the file.
%	Number of recorded operations for the file as a percentage of the total number of recorded operations for all monitored files.

Table 5.19: fields in the 'Top 100 files with most monitored operations' widget

Top 100 machines with most operations on monitored files

- **Aim**: To show the 100 computers where most operations have been recorded by the monitoring rules defined.
- **Fields**:

Field	Description
Machine	Name of the computer with monitored files.
Count	Number of recorded operations performed on the monitored files.
%	Number of recorded operations performed on the computer's monitored files as a percentage of the total number of recorded operations performed on all monitored files on the network.

Table 5.20: fields in the 'Top 100 machines with most monitored operations on files' widget

Attachments

Top 100 machines sending monitored attachments

- **Aim**: To show the 100 computers that have sent most email messages with monitored attachments.
- **Fields**:

Field	Description
Machine	Name of the computer from which monitored attachments were sent.
Count	Number of monitored attachments sent.
%	Number of monitored attachments sent from the computer as a percentage of the total number of monitored attachments sent from all computers on the network

Table 5.21: fields in the 'Top 100 machines sending monitored attachments' widget

Top 100 users sending monitored attachments

- **Aim**: To show the 100 users that have sent most email messages with monitored attachments.

- **Fields**:

Field	Description
User	Name of the user that sent email messages with monitored attachments.
Count	Number of monitored attachments sent.
%	Number of monitored attachments sent by the user as a percentage of the total number of monitored attachments sent by all users on the network.

Table 5.22: fields in the 'Top 100 users sending monitored attachments' widget

Top 100 users receiving monitored attachments

- **Aim**: To show the 100 users that have received most email messages with monitored attachments.
- **Fields**:

Field	Description
User	Name of the user that received email messages with monitored attachments.
Count	Number of monitored attachments received.
%	Number of monitored attachments received by the user as a percentage of the total number of monitored attachments received by all users on the network.

Table 5.23: fields in the 'Top 100 users receiving monitored attachments' widget

Chapter 6

Alerts

The Cytomic Data Watch alert system allows administrators to keep up-to-speed with events that take place on the network that require their attention, without having to go to the Web console. It is therefore a key module in minimizing the reaction time of the IT department when faced with potential data exfiltration situations in the organization.

The alert system is fully configurable by the network administrator, including the frequency for sending alerts, the conditions required for generating them and the delivery method used.

CHAPTER CONTENT

Predefined alerts

Cytomic Data Watch provides a number of predefined alerts that inform network administrators of the potentially dangerous operations detected across the network.

Follow the steps below to configure these predefined alerts:

- On the side menu, click **Administration** and then **Alerts configuration**.
- On the panel on the left, click **Cytomic EDR**. On the panel on the right, click **Data Access Control**.
- The panel at the bottom will display all predefined alerts. Click an alert to view its description.

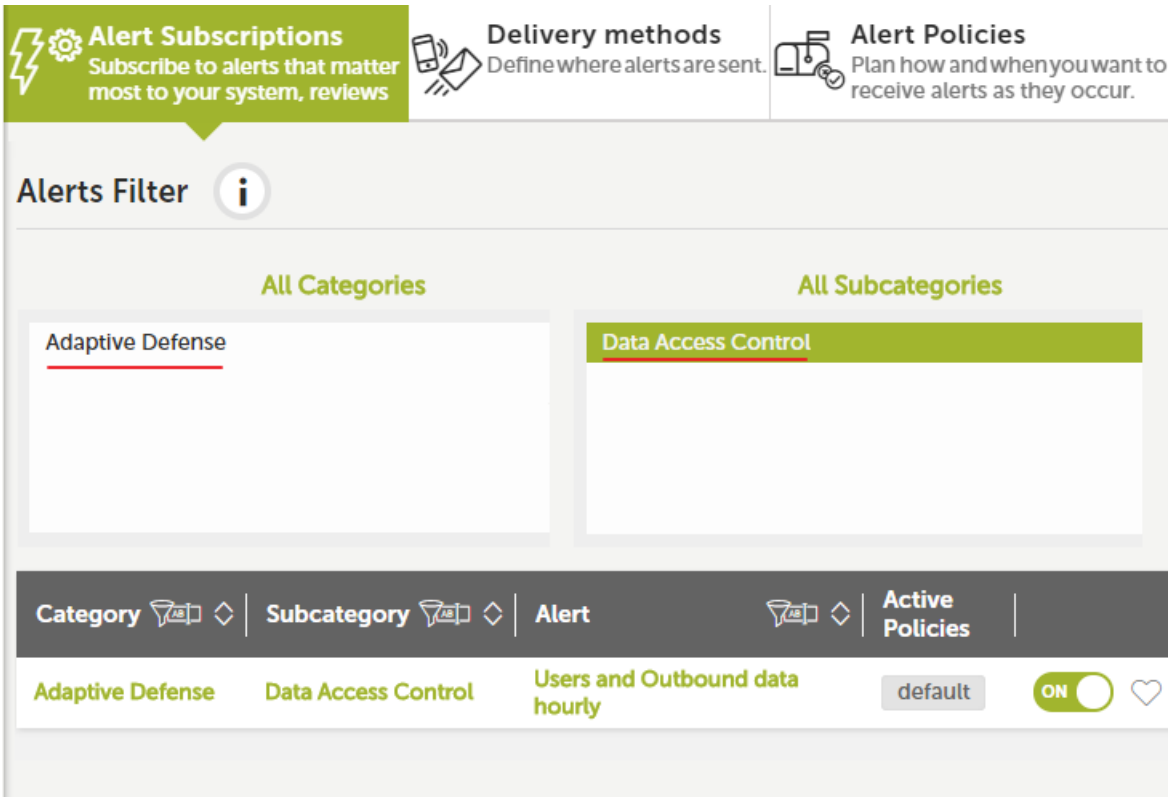


Figure 6.1: alert management window

The predefined alerts are:

- Too many operations by process.
- Malware detected.
- Too many exfiltration operations by user.

- User Operations.
- User rename operations.
- User create operations.
- User open operations.
- User copy-paste operations.
- Data leak.

Too many operations by process

Aim: generates an alert every time a process performs more than 50 operations on one or more PII files in a 10-second interval.

Linq:

```
FROM oem.panda.edp.ops
SELECT machineName AS machine, peek(fatherPath,re(".*\\\\(.*)$"), 1) AS  process
WHERE isnotnull(fatherPath)
GROUP EVERY 10s BY machine, process EVERY 10s
SELECT count() AS count
WHERE count > 50
```

Malware detected

Aim: generates an alert every time a malicious process performs an operation on a PII document.

Linq:

```
FROM oem.panda.edp.ops
WHERE fatherCat = "Malware"
```

Too many exfiltration operations by user

Aim: generates an alert every time a user performs more than 5 operations classified as "data exfiltration" in a 2-minute interval.

Linq:

```
FROM oem.panda.edp.ops
WHERE NOT deviceType = "Fixed" AND exfiltrationFlag = "EXFILTRATION"
GROUP EVERY 2m BY user EVERY 2m
SELECT count() AS count
WHERE count > 5
```

User Operations

Aim: generates an alert every time a user performs more than 5 percent of all exfiltration operations detected in a 4-hour interval.

Linq:

```
FROM oem.panda.edp.ops
WHERE has(exfiltrationFlag, "OK","BOTH")
GROUP EVERY 30m EVERY 0
SELECT count() AS count

FROM oem.panda.edp.ops
WHERE has(exfiltrationFlag, "OK","BOTH")
GROUP EVERY 30m BY user EVERY 0
SELECT count() AS count
```

User rename operations

Aim: generates an alert every time a user performs more than 5 percent of all file rename operations detected in a 4-hour interval.

Linq:

```
FROM oem.panda.edp.ops
WHERE op="Rename"
GROUP EVERY 30m BY user EVERY 0
SELECT count() AS count

FROM oem.panda.edp.ops
WHERE op="Rename"
GROUP every 30m BY user EVERY 0
SELECT count() AS count
```

User create operations

Aim: generates an alert every time a user performs more than 5 percent of all file create operations detected in a 4-hour interval.

Linq:

```
FROM oem.panda.edp.ops
WHERE op="Create"
GROUP EVERY 30m EVERY 0
SELECT count() AS count

FROM oem.panda.edp.ops
WHERE op="Create"
GROUP every 30m BY user EVERY 0
SELECT count() AS count
```

User open operations

Aim: generates an alert every time a user performs more than 5 percent of all file open operations detected in a 4-hour interval.

Linq:

```
FROM oem.panda.edp.ops
WHERE op="Open" AND NOT user="NT AUTHORITY\\SYSTEM"
GROUP EVERY 30m EVERY 0
SELECT count() AS count

FROM oem.panda.edp.ops
WHERE op="Open" AND NOT user="NT AUTHORITY\\SYSTEM"
GROUP EVERY 30m BY user EVERY 0
SELECT count() AS count
```

User copy-paste operations

Aim: generates an alert every time a user performs more than 5 percent of all content copy and paste operations detected in a 4-hour interval.

Linq:

```
FROM oem.panda.edp.ops
WHERE op="Copy-Paste"
GROUP EVERY 30m EVERY 0
SELECT count() AS count

FROM oem.panda.edp.ops
WHERE op="Copy-Paste"
GROUP every 30m BY user EVERY 0
SELECT count() AS count
```

Data leak

Aim: generates an alert every time an exfiltration operation is performed on a document larger than 25 MB.

Linq:

```
FROM oem.panda.edp.ops
WHERE docSize >= 26214400 AND exfiltrationFlag = "EXFILTRATION"
```

Alert system architecture

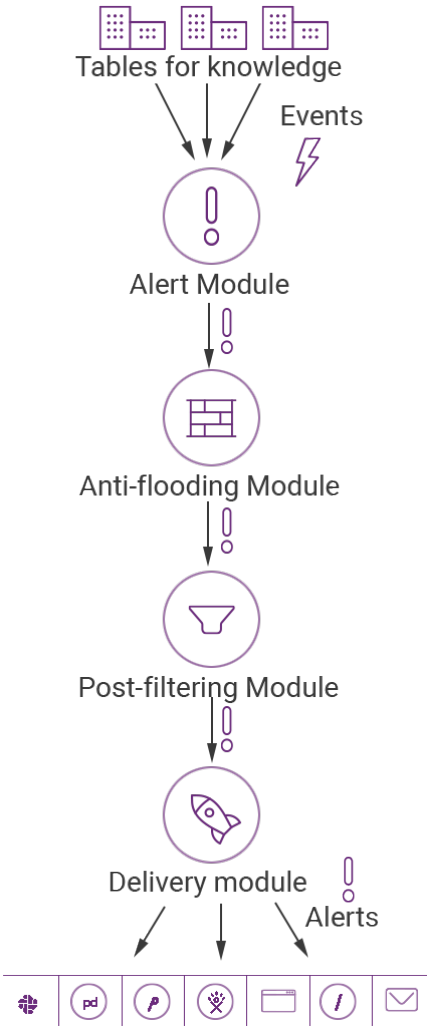


Figure 6.2: modules implemented in the alert generation flow

The Cytomic Data Watch alert system comprises several fully configurable modules. The sequence of processes involved in the generation of alerts is as follows:

- **Generation of events**: Each entry in a knowledge table generates a unique event that can later be converted into one or more alerts.
- **Alert module**: The events that meet certain criteria defined by administrators in the alerts module will generate an alert.
- **Antiflooding module**: This prevents the problem of a 'storm of alerts', allowing the alert generation module to be temporarily disconnected from the generation of events on exceeding a certain threshold defined by the administrator. This prevents the generation of a flood of alerts.
- **Post filter ing module**: This handles the alerts once they are generated, changing their properties or even selectively eliminating them in line with the criteria established by the administrator.
- **Delivery module**: This allows the delivery of the alerts to administrators in a number of ways: Email, HTTP-JSON, Service Desk, Jira, Pushover, Pagerduty y Slack. For more information, refer to "**Creating delivery conditions**".

Process for configuring the alerts

Setting up a new alert requires a series of steps, some of them mandatory, some of them optional, in order for the alert to work correctly.

These steps are listed below along with a brief description of the process.

1. **Creating the alerts (mandatory)**: Creating an alert requires you to define the type of event you want from the knowledge table, and to establish that it will generate an alert.
2. **Editing the alert subscription (optional)**: This lets you enable or disable the newly created alert. Alerts are enabled automatically when they are created.
3. **Set the delivery criteria (mandatory for the first alert)**: The delivery settings allow you to determine

the delivery method and specify associated information. For example, if you specify delivery by email, you must indicate the recipient's email account.

4. **Creating an antiflooding policy (optional)**: This sets maximum thresholds for generating alerts in order to avoid mass mailings. Administrators who prefer to receive all generated alerts shouldn't use any antiflooding policy.
5. **Creating a new delivery policy (mandatory for the first alert)**: The delivery policy lets you define the following parameters for delivering alerts:
   - **Assigning the antiflooding policy** (point 4).
   - **Assigning the delivery schedule**: Alerts will only be sent in line with the calendar settings.
   - **Delivery method** (point 3).
6. **Assigning a delivery policy** (point 5) to the alert created (point 1).
7. **Creating post filter s (optional)**: If you want to edit the alert before it is sent you have to create a post filter.

The block diagram that comprises an alert is as follows:

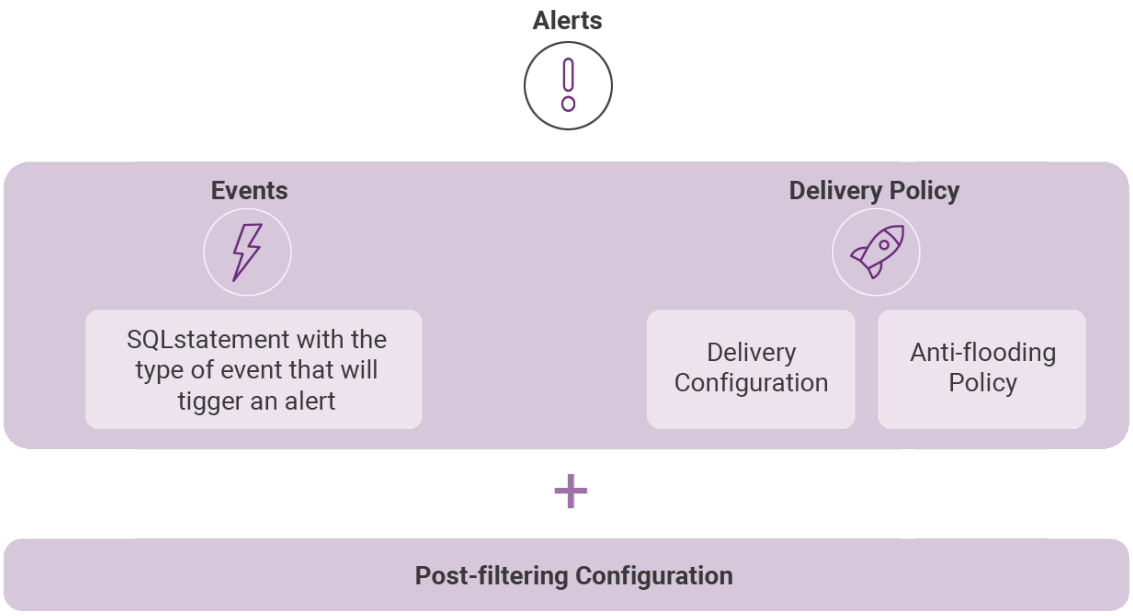


Figure 6.3: logical components of an alert

Creating alerts

Alerts are created from the associated knowledge table. To create an alert, follow these steps.

1. Select the corresponding table in the **Search** side menu.
2. Apply the filters and data transformations required to generate the information you want and click the icon on the toolbar.

3. Set the alert parameters.

Parameter	Description
Subcategory	Tag that classifies the alert and enables later searches or filters.
Context	Tag that classifies the alert and enables later searches or filters.
Message	The alert subject.
Description	The alert content.

Table 6.1: alert parameters

4. Alert generation frequency.

Option	Description
Each	Generate an alert for each event entry in the table.
Several	Lets you define the frequency and thresholds for generating alerts.
Period	Time period to which the threshold applies.
Threshold	This determines the number of events in a given period that will trigger the sending of an event.
Counters	This lets you add columns from the knowledge table to the alert. The contents of a counter field can be incorporated into the subject or description of the alert simply by putting the field name preceded by the $ symbol.

Table 6.2: alert generation frequency

If, for example, a **Period** of 5 minutes is set and a **Threshold** of 30, no alert will be sent until there are 30 events. Event 60 will generate a second warning and so on until the five-minute period has concluded, at which time the event counter is reset to 0.

During the process of creating alerts, the volume of alerts generated according to the settings is checked. If the alert will generate more than 60 alerts per minute, the alert settings are invalid. In this case, increase the Threshold field to lower the number of alerts generated per minute.

Once the alert is created, the system will begin generating entries as the events defined in the alert occur. To view the generated alerts log, see the Alert Management section later.

Alert management

The generated alerts can be managed by clicking the **Alerts** side menu. Click the **Alerts** panel tab to display the following sections: **Alerts Overview** and **Alerts History.**

Alerts Overview

This view displays the alerts generated by the system through various charts. The charts can be configured by the administrator using several tools.

Figure 6.4: alert list configuration toolbar

- **Type of chart (1)**: This lets you choose the way that the alerts will be represented:
  - Line chart.
  - Timeline.
  - Calendar chart.
  - Voronoi diagram.
- Enable/disable pie chart (2).
- **Time period represented in the chart (3)**.
  - 1 hour.
  - 6 hours.
  - 12 hours.
  - 1 day.
  - 1 week.
  - 1 year.
- **Filter by alert status (4)**

Status	Description
Open	Only open alerts are displayed.
All alerts	All alerts are displayed.

Table 6.3: alert statuses

*See chapter "**Introduction to the applications**" on page **35** for more details about each type of chart.*

Alert History

This section shows a list of the alerts generated. Each alert has a number of fields that the system fills in as configured by the administrator when creating the alert:

Field	Description
Status	Watched; not read.
Type	Type of alert, taken from the Message field in the alert settings, described in the section on **Creating alerts** earlier in the chapter.
Detailed Information	Extract from the alert text taken from the **Description** field, described in the section on **Creating alerts** earlier in the chapter. Click **Detailed Information** in the alert to display the content.
Category	Alert category taken from the **Subcategory** and **Context** fields, described in the section on **Creating alerts** earlier in the chapter.
Priority	All alerts are generated with normal priority by default. To change the priority of an alert (**very low, low, normal, high, very high**) you have to configure a postfilter. Refer to the point on **Configuring post filters** later in this guide.
Created	Date and time of creation and the time elapsed since the alert was generated.
Menu	The final column in the **Alerts History** table displays a menu with options for each alert.
View alerts details	This lets you see all the information associated with the alert in a new window.
Create annotation	This lets you add a text to the alert. Completing the form will add an icon to the alert indicating that a technician made a comment about the alert. You can also convert a note into a task if the alert requires action over a period of time.
New filter	This lets you create post filters as described in the following section.
Delete	This lets you delete the alert.

Table 6.4: alert fields

Establishing filters in the alert history

Click the **Type**, **Category** or **Priority** fields of a specific alert to set a filter that will only display alerts that match the criteria set.

The applied filters will be shown in the filter bar.

Creating post filters

Post filters allow you to edit the features of the generated alerts before they are sent, as well as deleting them if they coincide with certain criteria.

The post filters are created from the **Alerts** section in the side menu. Click the icon of an alert that has been generated to display a drop-down menu with actions available.

The post filter screen comprises five sections:

Section 1: Description

This section specifies the name and criteria that alerts have to match for the filter to apply.

Field	Description
Name	Name of the filter.
Context	This sets the context of the alert as a filter condition.
Category	This sets the category of the alert as a filter condition.
Priority	This sets the priority of the alert as a filter condition.

Table 6.5: post filter fields

Section 2: Basic data

This section is not used.

Section 3: Extra data

In this section you can set criteria based on the content which alerts must meet for the post filter to be applied.

In the process of configuring an alert, a series of columns can be established in the **Counter** field. The contents of these columns is accessible from the alert body when it is generated using the $ symbol. The Extra data section allows you to choose from the dropdown menu those counters that you want to include as a filter condition.

Section 4: Filter dates

You can set one or more date ranges to act as a criterion. The post filter will not apply to alerts generated outside the established period.

Section 5: Action

- Mark as read.
- Change priority.
- False positive.
- Change notify method.
- Delete.

Post filter management

You can manage post filters from the **Alerts** side menu, by clicking **Post filters.** This window displays a list of the post filters configured with the following information:

Field	Description
Status	Enabled or disabled.
Name	Name given to the post filter when it was created.
Category	Category that determines whether the post filter is applied.
Context	Context that determines whether the post filter is applied.
Priority	Alert priority that determines whether the post filter is applied.
Conditions	Alert content that determines whether the post filter is applied.
Action	Internal command that the alert will apply.

Table 6.6: post filter settings

Creating delivery conditions

The delivery conditions are created through the side menu **Administration**, **Alerts Configuration**, then select the tab **Delivery methods.**

Select the delivery type in the left panel. The options are as follows:

- **Email**: The alerts are sent via email.
- **HTTP-JSON**: The alerts are sent via JSON objects.
- **Service desk**: The alerts are sent via Service Desk.
- **JIRA**: The alerts are sent via Jira server.
- **Pushover**: The alerts are sent in a Pushover account.
- **Pagerduty**: The alerts are sent in a PagerDuty account.
- **Slack**: The alerts are sent via the Slack service.

Once the type of delivery is selected, click the **New** button to set up a new type of delivery.

Email

This enables the sending of real-time alerts to email accounts.

The required fields are:

Field	Description
Name	Name of the delivery method.

Table 6.7: alert delivery via email settings

Field	Description
Email	Email account of the recipient.
Timezone	Sets the time and date for sending the email.
Language	The language in which the alert is received.

Table 6.7: alert delivery via email settings

HTTP-JSON

This enables the sending of real-time alerts via HTTP or HTTPS using JSON objects with POST method.

To improve security, in addition to using the HTTPS encryption protocol you can also enable Digest authentication.

The required fields are:

Field	Description
Name	Name of the delivery method.
URL	URL of the target server, specifying the protocol (HTTP or HTTPS) and the port (e.g. `http://localhost:8080/index.php`)
Timezone	Sets the time and date for sending the email.
Language	The language in which the alert is received.
User	This is only used when the **Authenticated** checkbox is selected.
Password	This is only used when the **Authenticated** checkbox is selected.

Table 6.8: alert delivery via HTTP-JSON settings

Once the settings have been saved, an HTTP message is sent with a code to validate the server. In the list of JSON Delivery methods, the new configuration will be displayed preceded by a red dot (status, pending validation). By clicking the red dot, a window will open requesting the code sent to the server. Once the delivery settings are entered, it will be fully operational.

Service Desk

This enables the real-time sending of alerts to Service Desk Plus servers, using two different methods: REST and SERVLET.

The required fields are:

Field	Description
Name	Name of the delivery settings.
URL	URL of the target server.
REST	`http://[SERVER]:[PORT]/sdpapi/request/`

Table 6.9: alert delivery via Service Desk settings

Field	Description
SERVLET	`http://[SERVER]:[PORT]/servlets/RequestServlet`
Delivery method	REST or SERVLET.
Timezone	Sets the time and date for sending the message.
Language	The language in which the alert is received.
User	Name of the technician assigned.
Technician Key	Technician key generated in the Service Desk administration panel.

Table 6.9: alert delivery via Service Desk settings

Once the settings have been saved, an HTTP message is sent with a code to validate the server. In the list of Service Desk delivery methods, the new configuration will be displayed preceded by a red dot (status, pending validation). By clicking the red dot, a window will open requesting the code sent to the server. Once the delivery settings are entered, it will be fully operational.

JIRA

This enables the real-time sending of alerts to Jira servers.

The required fields are:

Field	Description
Name	Name of the delivery settings.
URL	URL of the target server (e.g. `http://localhost:8090/rest/api/2/issue)`.
User	JIRA user name.
Password	JIRA password.
Issue Type	The type of task to be created in Jira. In the server URL, there will be a Json object with the projects created. The variable *issuetypes* will list the types of incidents permitted by the project.
Project key	Identifier of the project where the alert will be created. In the server URL, there will be a Json object with the projects created and their identifiers. The Key tag contains the identifiers of each project.
Timezone	Sets the time and date for sending the message.
Language	The language in which the alert is received.

Table 6.10: alert delivery via JIRA settings

Once the settings have been saved, an HTTP message is sent with a code to validate the server. In the list of JIRA delivery methods, the new configuration will be displayed preceded by a red dot (status, pending validation). By clicking the red dot, a window will open requesting the code sent to the server. Once the delivery settings are entered, it will be fully operational.

PushOver

This enables the real-time sending of alerts to PushOver servers.

The required fields are:

Field	Description
Name	Name of the delivery method.
Token Application	API Key of the application created in `https://pushover.net/apps`
User/group	API Key of the user or group to whom the alerts will be sent.
Device (optional)	Name of the device to which the alerts will be sent.
Title (optional)	Text that appears in the alert.
URL (optional)	Link sent in all alerts.
Url Title (optional)	Text that links to the URL above.
Sound (optional):	Type of notification to be sent.
Timezone	Sets the time and date for sending the message.
Language	The language in which the alert is received.

Table 6.11: alert delivery via PushOver settings

Once the settings have been saved, an HTTP message is sent with a code to validate the server. In the list of PushOver delivery methods, the new configuration will be displayed preceded by a red dot (status, pending validation). By clicking the red dot, a window will open requesting the code sent to the server. Once the delivery settings are entered, it will be fully operational.

PagerDuty

This enables the real-time sending of alerts to PagerDuty accounts.

The required fields are:

Field	Description
Name	Name of the delivery method.
Service Key	API Key of the PagerDuty service that receives the alert.
Client	Name or identifier that appears in the alert.
Client URL	Link sent in all alerts.
Timezone	Sets the time and date for sending the message.
Language	The language in which the alert is received.

Table 6.12: alert delivery via PagerDuty settings

Once the settings have been saved, an HTTP message is sent with a code to validate the server. In the list of PagerDuty delivery methods, the new configuration will be displayed preceded by a red dot

(status, pending validation). By clicking the red dot, a window will open requesting the code sent to the server. Once the delivery settings are entered, it will be fully operational.

SLACK

This enables the real-time sending of alerts via SLACK.

The required fields are:

Field	Description
Name	Name of the delivery settings.
Timezone	Lets you set the time and date for sending the alert.
Channel	Channel through which the alert is received.
Language	Language in which the alert is received.

Table 6.13: alert delivery via Slack settings

Once the settings have been saved, an HTTP message will be sent with a code to validate the server. Also, in the list of Slack delivery settings, the new settings will be displayed preceded by a red dot (status, pending validation). Click the red dot to open a window prompting you to enter the code sent to the server. Once entered, the delivery settings will be fully functional.

Delivery method management

Each of the Delivery methods created has a menu that allows it to be edited and/o deleted.

When editing a delivery method already created, a window is displayed with editing options.

Creating antiflooding policies

An antiflooding policy allows complete, temporary suspension of alert generation when the rate of alerts exceeds a certain threshold defined by the administrator in the policies.

Antiflooding policy creation is done from the side menu **Administration**, **Alerts Configuration**, then go to the **Alert Policies** tab, then the **Antiflooding Policy** tab.

Click **New** to display a window with the complete settings options of the policy.

Here you can set:

- Maximum number of alerts that can be received.
- Time period to which the previous criteria applies.
- A reminder if the alert is repeated after the established time period.

Editing antiflooding policies

Each of the antiflooding policies created has an associated menu that allows it to be edited and/or deleted.

When editing antiflooding policies already created, a window is displayed with editing options.

Creating alert policies or delivery methods

Alert policies, also called sending policies, let you define how the alerts generated are sent.

A sending policy is the nexus of the policies defined above (antiflooding policy and delivery methods).

Creating sending policies is carried out through the side menu **Administration**, **Alerts Configuration**, then go to the **Alert Policies** tab, then the **Sending Policy** tab.

Click **New** to display a window with the complete settings options of the sending policy:

Parameter	Description
Name	Name of the sending policy.
Default	This indicates whether the policy is to be treated as a default policy. If there are alerts that don't have a sending policy assigned, this will be assigned by default.
Antiflooding policy	This specifies the antiflooding policy to apply.
Schedule	This indicates the time period when the policy will be active.
Send method	This indicates the methods of delivery configured earlier that will be used to deliver the alert.

Table 6.14: sending policy parameters

Editing sending policies

Each of the sending policies created has an associated menu that allows it to be edited and/or deleted.

When editing sending policies already created, a window is displayed with editing options.

Configuring an alert sending policy

Sending policies are assigned to alerts through the side menu **Administration**, **Alert Configuration**, then go to the **Alert Subscriptions** tab.

Each alert has an icon which lets you select a sending policy.

Part 3

Additional information

Chapter 7: PII knowledge tables

Chapter 8: Extension list

Chapter 9: Process list

Chapter 10: Hardware, software and network requirements

Chapter 7

PII knowledge tables

Cytomic EDR collects information about the processes run on all workstations and servers across the network, whether goodware or malware. If those processes access PII files, the information is sent to the Cytomic Data Watch server, where it is organized into an easy-to-read table.

Each line of the table is an event monitored by Cytomic Data Watch, and provides information such as when the event occurred, the computer where it took place, its IP address, etc.

Oem.panda.edp.ops table

This table stores all information related to PII file monitoring.

Name	Description	Values
evendate	Date when the event was logged on the Cytomic Data Watch server.	Date
serverdate	Workstation/server's date when the event was generated.	Date
machineName	Workstation/server name.	String
machineIP	Workstation/server IP address.	IP address
user	User name of the process that operated on the file.	String
exfiltrationFlag	Indicates whether the file has been the subject of an operation classified as data exfiltration, data infiltration, or both.	• INFILTRATION • EXFILTRATION • BOTH
docSize	Size of the PII file (in bytes).	Numeric

Table 7.1: oem.panda.edp.ops table

Name	Description	Values
op	Operation performed on the PII file.	• **Create** • **Modify** • **Open** • **Delete** • **Rename** • **Copy-Paste** • **OnDemand**: search launched from the console by the administrator
fatherHash	MD5 of the process that operated on the PII file. This field will be empty if **operation** is **On Demand.**	String
fatherPath	Path of the process that operated on the PII file. This field will be empty if **operation** is **On Demand.**	String
fatherCategory	Category of the process that operated on the PII file. This field will be empty if **operation** is **On Demand.**	• **Goodware** • **Malware** • **Monitoring**: Unknown process in the process of classification. • **PUP**: Unwanted program.
documentPath	Drive where the PII file that was operated on resides, along with its path, in the following format: DEVICE TYPE|PATH	String
documentName	Name of the file that was operated on. In rename operations, this field displays the **DocumentName** value of the original file, and the **DocumentName** value of the renamed file, in the following format: TARGET_NAME|ORIGINAL_NAME	• String • String | String
documentHash	Hash of the file that was operated on.	String
deviceType	Drive where the PII file that was operated on resides.	• 0: **UNKNOWN** • 1: **NO_ROOT_DIR**: The path is invalid or does not exist • 2: **REMOVABLE**: Mobile device (external hard drive, card reader, USB device, etc.) • 3: **FIXED**: Internal hard drive • 5: **CDROM** • 6: **RAMDISK** • String

Table 7.1: oem.panda.edp.ops table

Name	Description	Values
creditCard	Indicates whether Credit card number entities were found in the PII file or not.	Boolean
bankAccount	Indicates whether Bank account number entities were found in the PII file or not.	Boolean
personalID	Indicates whether ID card number entities were found in the PII file or not.	Boolean
driveLic	Indicates whether Driver's license number entities were found in the PII file or not.	Boolean
passPort	Indicates whether Passport number entities were found in the PII file or not.	Boolean
SSId	Indicates whether Social security number entities were found in the PII file or not.	Boolean
email	Indicates whether Email address entities were found in the PII file or not.	Boolean
IP	Indicates whether IP address entities were found in the PII file or not.	Boolean
name	Indicates whether First and last name entities were found in the PII file or not.	Boolean
address	Indicates whether Physical address entities were found in the PII file or not.	Boolean
phone	Indicates whether Phone number entities were found in the PII file or not.	Boolean
estimatedNumPII	Estimated number of found entities.	Numeric
Reclassified	• **True**: The file contained PII but doesn't contain it any more. • **False**: The file has not been reclassified and therefore contains PII.	Boolean

Table 7.1: oem.panda.edp.ops table

Oem.paps.edp.usrrules table

This table stores all information collected from the monitoring of the files specified in the rules defined by the administrator.

Name	Description	Values
evendate	Date when the event was logged on the **Cytomic Data Watch** server.	Date

Table 7.2: oem.paps.edp.usrrules table

Name	Description	Values
serverdate	Workstation/server's date when the event was generated.	Date
machineName	Workstation/server name.	Character string
machineIP	Workstation/server IP address.	IP address
user	Name of the logged-in user when the event was logged.	Character string
exfiltrationFlag	Indicates that the file has been the subject of an operation classified as data exfiltration, data infiltration, or both.	• INFILTRATION • EXFILTRATION • BOTH
docSize	Size of the file in bytes.	Numeric
op	Operation performed on the PII file.	• **Create** • **Modify** • **Open** • **Delete** • **Rename** • **Copy-Paste**
fatherHash	MD5 of the process that operated on the file.	Character string
fatherPath	Path of the process that operated on the file.	Character string
fatherCat	Category of the process that operated on the file.	• **Goodware** • **Malware** • **Monitoring**: Unknown process in the process of classification • **PUP**: Unwanted program
documentPath	Drive where the file that was operated on resides, along with its path, in the following format: DEVICE TYPE | PATH	Character string
documentName	Name of the file that was operated on. In rename operations, this field displays the **documentName** value of the original file and the **documentName** value of the renamed file, in the following format: TARGET_NAME | ORIGINAL_NAME	• Character string • Character string | Character string
documentHash	Hash of the file that was operated on.	Character string

Table 7.2: oem.paps.edp.usrrules table

Name	Description	Values
deviceType	Drive where the PII file that was operated on resides.	• **0:UNKNOWN** • **1:NO_ROOT_DIR**: The path is invalid or does not exist • **2:REMOVABLE**: Portable device (external hard drive, card reader, USB device, etc.) • **3**: **FIXED**: Internal hard drive • **5**: **CDROM** • **6**: **RAMDISK** • Character string
usrRules	Names of the rules entered in the Cytomic EDR console that are monitoring the file. They are separated with the "|" character.	Character string | Character string | Character string...

Table 7.2: oem.paps.edp.usrrules table

Oem.paps.edp.usrrulesmail table

This table stores all information collected from the email messages containing files monitored as per the rules defined by the administrator.

Name	Description	Values
evendate	Date when the event was logged on the **Cytomic Data Watch** server.	Date
serverdate	Workstation/server's date when the event was generated.	Date
machineName	Workstation/server name.	Character string
machineIP	Workstation/server IP address.	IP address
loggeduser	Name of the logged-in user when the event was logged.	Character string
msgID	Unique ID of the message.	Character string
msgTo	Email address of the message recipient.	Character string
msgFrom	Email address of the message sender.	Character string
msgSentDate	Date the message was sent. In received messages this field is Null.	Date
msgSubject	Message subject.	Character string
msgReceivedDate	Date the message was received. In sent messages this field is Null.	Character string

Table 7.3: oem.paps.edp.usrrulesmail table

Name	Description	Values
msgElement	Monitored item in the message.	"Attachment" character string
msgElementSize	Size of the monitored file.	Numeric
msgElementName	Name of the monitored file.	Character string
msgElementHash	MD5 of the monitored file.	Character string
msgExfiltrationFlag	Indicates that the file has been the subject of an operation classified as data exfiltration, data infiltration, or both.	• INFILTRATION • EXFILTRATION • BOTH
usrRules	Names of the rules entered in the Cytomic EDR console that are monitoring the file. They are separated with the "|" character.	Character string | Character string | Character string...

Table 7.3: oem.paps.edp.usrrulesmail table

Oem.paps.edp.mail table

This table stores all information collected from the email messages containing files classified as PII, as well as the characteristics of the files with personal data they contain.

Name	Description	Values
evendate	Date when the event was logged on the **Cytomic Data Watch** server.	Date
serverdate	Workstation/server's date when the event was generated.	Date
machineName	Workstation/server name.	Character string
machineIP	Workstation/server IP address.	IP address
LoggedUser	Name of the logged-in user when the event was logged.	Character string
msgID	Unique ID of the message.	Character string
msgTo	Email address of the message recipient.	Character string
msgFrom	Email address of the message sender.	Character string
msgSentDate	Date the message was sent. In received messages this field is Null.	Date
msgSubject	Message subject.	Character string
msgReceivedDate	Date the message was received. In sent messages this field is Null.	Character string
msgElement	Monitored item in the message.	"Attachment" character string

Table 7.4: oem.paps.edp.mail table

Name	Description	Values
msgElementSize	Size of the monitored file.	Numeric
msgElementName	Name of the monitored file.	Character string
msgElementHash	MD5 of the monitored file.	Character string
msgExfiltrationFlag	Indicates that the file has been the subject of an operation classified as data exfiltration, data infiltration, or both.	• INFILTRATION • EXFILTRATION • BOTH
creditCard	Indicates whether Credit card number entities were found in the PII file or not.	Boolean
bankAccount	Indicates whether Bank account number entities were found in the PII file or not.	Boolean
personalID	Indicates whether Personal ID number entities were found in the PII file or not.	Boolean
driveLic	Indicates whether Driver's license number entities were found in the PII file or not.	Boolean
passPort	Indicates whether Passport number entities were found in the PII file or not.	Boolean
SSId	Indicates whether Social security number entities were found in the PII file or not.	Boolean
email	Indicates whether Email address entities were found in the PII file or not.	Boolean
IP	Indicates whether IP address entities were found in the PII file or not.	Boolean
name	Indicates whether First and last name entities were found in the PII file or not.	Boolean
address	Indicates whether Physical address entities were found in the PII file or not.	Boolean
phone	Indicates whether Phone number entities were found in the PII file or not.	Boolean
estimatedNumPII	Estimated number of found entities.	Numeric

Table 7.4: oem.paps.edp.mail table

Chapter 8

Extension list

Next is a list of the extensions of the files that Cytomic Data Watch scans, looking for personal information of the organization's users and customers:

Extensiones soportadas

Suite name	Product	Extensions
Office	Word	• DOC • DOT • DOCX • DOCM • RTF
	Excel	• XLS • XLSM • XLSX • XLSB • .CSV
	PowerPoint	• PPT • PPS • PPSX • PPSM • SLDX • SLDM • POTX • PPTM • PPTX • POTM

Table 8.1: files in which Cytomic Data Watch searches for PII

Suite name	Product	Extensions
OpenOffice	Writer	• ODM • ODT • OTT • OXT • STW • SXG • SXW
	Draw	• ODG • OTG • STD
	Math	• ODF • SXM
	Base	• ODB
	Impress	• OTP • ODP • STI • SXI
	Calc	• OTS • ODS • SXC
Plain text		TXT
Web browsers	• Internet Explorer • Chrome • Opera • Other	• HTM • HTML • MHT • OTH
Mail client	• Outlook • Outlook Express	EML
Other	Adobe Acrobat Reader	PDF
	Extensible Markup Language	XML
	Contribute	STC
	ArcGIS Desktop	SXD

Table 8.1: files in which Cytomic Data Watch searches for PII

Chapter 9

Process list

Cytomic EDR monitors all processes running on users' workstations and servers, looking for operations performed on personal data files. This monitoring activity is reflected in PCytomic Data Watch's Advanced Visualization Tool applications and PII Knowledge Table. However, when it comes to determining if an operation is part of an incident categorized as unauthorized data exfiltration or infiltration, the Machine Learning algorithms examine the following subset of processes:

Data exfiltration processes

Type	Program name	Binary name
Web browser	Microsoft Edge	• browser_broker.exe • microsoftedge.exe • microsoftedgecp.exe
	Google Chrome	chrome.exe
	Comodo Dragon	dragon.exe
	Mozilla Firefox	firefox.exe
	Microsoft Internet Explorer	• iexplore.exe • msimn.exe
	Opera	opera.exe
	Yandex	yandex.exe
	Mozilla Prism	zdclient.exe
	Torch	torch.exe
	Apple Safari	safari.exe
Mail messaging	Microsoft Outlook	outlook.exe
	Mozilla Thunderbird	thunderbird.exe
	Windows Live Mail	wlmail.exe
	Yahoo Zimbra Desktop	zdesktop.exe

Table 9.1: processes monitored in data exfiltration discovery tasks, along with the program's trade name and software type

Type	Program name	Binary name
Chat messaging	Microsoft Skype	skype.exe
	Facebook Whatsapp	• whatsapp.exe • winuapentry.exe
	Fleep	• fleep.exe • fleep.browsersubprocess.exe
	Pidgin	• pidgin.exe
	Line	line.exe
	Telegram	telegram.exe
	Rocket chat	rocket.chat.exe
Video conferencing programs and collaboration tools	Spark	ciscocollabhost.exe
	Moxtra	moxtra.exe
	Ring Central	rincentral.exe
	Samepage	samepage.exe
	Yammer	yammer.exe
	Microsoft Teams	teams.exe
	Microsoft Lync	lync.exe
File storage	Dropbox	dropbox.exe
Media player	Line media player	linemediaplayer.exe
File transfer	PuTTY SFTP	psftp.exe
	WinSCP	winscp.exe
Windows administration	Putty	• pscp.exe • putty.exe
	Netcat	nc.exe
	Microsoft BITSAdmin Tool	bitsadmin.exe
Interpreter/Compiler	Microsoft Scripting Host	mshta.exe
	Java	• java.exe • javaw.exe
Database	Firebird SQL Server	fbserver.exe
Other		• browser.exe • stride.exe • wechatstore.exe

Table 9.1: processes monitored in data exfiltration discovery tasks, along with the program's trade name and software type

Data infiltration processes

Type	Program name	Binary name
Web browser	Microsoft Edge	• browser_broker.exe • microsoftedge.exe • microsoftedgecp.exe
	Google Chrome	chrome.exe
	Comodo Dragon	dragon.exe
	Mozilla Firefox	firefox.exe
	Microsoft Internet Explorer	• iexplore.exe • msimn.exe
	Opera	opera.exe
	Yandex	yandex.exe
	Mozilla Prism	zdclient.exe
	Torch	torch.exe
	Apple Safari	safari.exe
	Brave	brave.exe
	Vivaldi	vivaldi.exe
Web servers	Apache HTTP	httpd.exe
Office tools	Microsoft Excel	excel.exe
	Microsoft PowerPoint	powerpnt.exe
	Microsoft Word	winword.exe
	OpenOffice	• soffice.bin • soffice.exe
File reader	Adobe Reader	acrord32.exe
Reproductor de medios	Line media player	linemediaplayer.exe
Mail messaging	Microsoft Outlook	outlook.exe
	Mozilla Thunderbird	thunderbird.exe
	Windows Live Mail	wlmail.exe
	Yahoo Zimbra Desktop	zdesktop.exe
	Lotus Notes	nlnotes.exe
	Remark	mark5.exe

Table 9.2: processes monitored in data infiltration discovery tasks, along with the program's trade name and software type

Type	Program name	Binary name
Chat messaging	Microsoft Skype	skype.exe
	Facebook Whatsapp	• whatsapp.exe • winuapentry.exe
	Telegram	telegram.exe
	Pidgin	pidgin.exe
	Line	line.exe
	Fleep	• fleep.exe • fleep.browsersubprocess.exe
	Pidgin	pidgin.exe
Video conferencing programs and collaboration tools	Spark	ciscocollabhost.exe
	Microsoft Lync	lync.exe
	Moxtra	moxtra.exe
	Ring Central	rincentral.exe
	Samepage	samepage.exe
	Slack	slack.exe
	Microsoft Teams	teams.exe
	Yammer	yammer.exe
File transfer	PuTTY SFTP	psftp.exe
	WinSCP	winscp.exe
	Internet Download Manager	idman.exe
	IceCast	icecast2.exe
	uTorrent	utorrent.exe
Windows administration	Putty	• pscp.exe • putty.exe
	Netcat	nc.exe
	Microsoft BITSAdmin Tool	bitsadmin.exe
Windows component	Command line	conhost.exe
	Runtime Broker	runtimeBroker.exe
	WMI command line	wmic.exe
Interpreter/Compiler	Microsoft Scripting Host	mshta.exe
	Java	• java.exe • javaw.exe

Table 9.2: processes monitored in data infiltration discovery tasks, along with the program's trade name and software type

Type	Program name	Binary name
Database	Firebird SQL Server	fbserver.exe
Other	Varios	• browser.exe • bvs.exe • stride.exe • wechatstore.exe
	David InfoCenter	dvwin32.exe
	Ezvit Intellectservice	ezvit.exe

Table 9.2: processes monitored in data infiltration discovery tasks, along with the program's trade name and software type

Chapter 10

Hardware, software and network requirements

Cytomic Data Watch is a cloud service and, as such, the entire infrastructure required to provide the service to its customers is hosted on Cytomic's premises. This frees organizations from the need to deploy additional hardware or software across their corporate networks. Nevertheless, the computers and the network to protect need to meet a series of minimum requirements to ensure that the product works properly.

CHAPTER CONTENT

Management console access requirements

In order for you to access the Web console, your system must meet the following requirements:

- Have a certified/supported browser (others may be compatible)
  - Mozilla Firefox
  - Google Chrome

Other browsers may also work, but some of their versions may not be supported. That's why we recommend that the aforementioned Web browsers be used.

- Internet connection and communication through port 443.
- Minimum screen resolution 1280x1024 (1920x1080 recommended).

Hardware requirements

- Enough processing power to generate the module's charts and lists in real time.
- Enough bandwidth to display all the information collected from users' computers in real time.