CYTOMIC

Guía de uso de Orion_

Aviso legal

Marcas registradas

Información de contacto

Oficinas centrales:

Cytomic (Unidad de Negocio de Panda Security, S.L.)

Calle Santiago de Compostela 12

Bilbao (Bizkaia) 48003 España.

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

Versión: 2.34.00

Autor: Cytomic

Fecha: 6/6/2024

Documentación técnica de Cytomic Orion

Para obtener la versión más reciente de la Guía de uso consulta la dirección web:

https://info.cytomicmodel.com/resources/guides/Orion/es/ORION-guia-ES.pdf

Para consultar un tema específico, accede a la ayuda online del producto en la dirección web:

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

Para consultar las funciones especificas de la librería de Threat Hunting accede a la ayuda online en la dirección web:

https://info.cytomicmodel.com/resources/help/ORION/es/threathuntingAPI/index.htm

Para consultar las funciones especificas de la librería de Notebooks accede a la ayuda online en la dirección web:

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

Documentación técnica sobre módulos y servicios compatibles con Cytomic Orion

Para consultar el manual de integración con Service Now consulta la siguiente URL:

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

Para consultar el how-to de integración con MISP consulta la siguiente URL:

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

Encuesta sobre la Guía de uso de Cytomic Orion

Evalúa esta documentación y envíamos sugerencias y peticiones para próximas versiones en:

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

Tabla de contenidos

Capítulo 1

Prólogo

La Guía de uso contiene información básica y procedimientos de uso para obtener el máximo beneficio del producto Cytomic Orion.

CONTENIDO DEL CAPÍTULO

Audiencia

Esta documentación está dirigida a los analistas y threat hunters que buscan indicios de actividades peligrosas en el parque informático de las organizaciones. Estas actividades generalmente forman parte de ataques dirigidos a la infraestructura IT de las empresas mediante la ejecución de malware de muy reciente aparición, o que utilizan herramientas legítimas que forman parte del sistema operativo de los equipos. En ambos casos, estos ataques no se reconocen como tales por los proveedores de seguridad informática, pasando desapercibidos para las herramientas de seguridad tradicional.

Cytomic Orion esta dirigido tanto a MSSPs (Managed Security Service Provider) como a MDRs (Managed Detection Response), proveedores de seguridad que ofrecen sus servicios de investigación a un gran número de clientes. También esta dirigido a las empresas que hayan decidido proveer este servicio dentro de la organización mediante la constitución de un SOC interno (Security Operations Center, Centro de Operaciones de Seguridad).

Para interpretar correctamente la información ofrecida por el producto y extraer conclusiones que ayuden a fortalecer la seguridad de las empresas son necesarios conocimientos sobre las técnicas y tácticas utilizadas por los hackers para moverse por los sistemas IT de las organizaciones. También se requiere un conocimiento profundo sobre las plataformas atacadas con mayor frecuencia a nivel de procesos, sistema de ficheros y registro, así como entender los protocolos de red utilizados comúnmente en las redes corporativas.

¿Qué es Cytomic Orion?

Cytomic Orion es un servicio cloud que facilita las tareas de threat hunting, cuyo objetivo es detectar de forma temprana aquellos ataques informáticos que han sido diseñados para pasar inadvertidos a los sistemas de protección tradicionales (protección perimetral y protección local a los equipos de usuario y servidores). Con este juego de herramientas y el conocimiento recopilado por Cytomic, el analista podrá detectar patrones de ejecución sospechosos que frecuentemente utilizan herramientas legítimas del sistema operativo para aprovechar fallos y ganar acceso a los sistemas de información de las empresas.

Una vez detectada la amenaza, Cytomic Orion también facilita las labores de resolución ofreciendo la información necesaria para diseñar un correcto plan de respuesta.

Iconos

En esta guía se utilizan los siguientes iconos;

Aclaraciones e información adicional, como, por ejemplo, un método alternativo para realizar una determinada tarea.

Sugerencias y recomendaciones.

Consulta en otra sección de la Guía de uso.

Capítulo 2

Información básica de Cytomic Orion

Cytomic Orion es una herramienta que facilita el descubrimiento de ataques que utilizan tácticas de ocultación avanzadas, y que las medidas de protección instaladas en el equipo de usuario o servidor no son capaces de detectar.

La arquitectura general de Cytomic Orion y la funcionalidad ofrecida en cada uno de sus módulos han sido diseñadas para encajar con el reparto de roles en SOCs de medianas y grandes empresas, o pertenecientes a un MSSP / MDR.

CONTENIDO DEL CAPÍTULO

Objetivos del Threat Hunting

La transformación digital de la actividad desarrollada en las empresas y las naciones es una fuente de riqueza muy importante, y constituye uno de los elementos principales que los diferencia y destaca con respecto a sus competidores. Por esta razón, sus resultados son perseguidos por hackers informáticos cuyas nuevas motivaciones económicas, políticas y estratégicas han fomentado una sofisticación de sus actividades delictivas, propiciando una fuerte mejora en las técnicas que utilizaban hasta el momento para acceder de forma ilegítima a la propiedad intelectual ajena.

Nuevas técnicas y tácticas empleadas en los ciberataques

Conforme la proyección de empresas y estados en el mundo digital crece, también lo hacen los incentivos para desarrollar nuevas estrategias, más sofisticadas y diseñadas específicamente para sortear las soluciones de seguridad perimetral (cortafuegos, UTMs, SCMs, NGFW etc.) y local (antivirus, EDR, NGAV etc.) durante el mayor tiempo posible. Entre las nuevas tácticas empleadas por los ciberataques se encuentran:

- Reclutamiento de trabajadores y miembros de la plantilla de la empresa (insiders) que faciliten la incursión en sus sistemas.
- Empleo de herramientas legítimas ya instaladas en los sistemas que pasen inadvertidas a las soluciones de seguridad instaladas. Estas tácticas son conocidas como "living off the land".
- Empleo de ingeniería social para embaucar a usuarios y clientes de la empresa (phishing)y así propiciar la creación de un entorno que facilite la entrada en sus sistemas de información.
- Uso de múltiples vectores de infección para sortear las defensas de las organizaciones y ejecutar los movimientos laterales necesarios para ganar una posición de ventaja estratégica a la hora de conseguir objetivos de alto valor.

La proliferación de estas técnicas y tácticas avanzadas han propiciado la aparición de una nueva categoría de malware: los APT o Advanced Persistent Threats, ataques dirigidos a empresas con objetivos muy concretos y con capacidad de retrasar lo máximo posible la incorporación de su firma digital a los archivos de identificadores que los proveedores de seguridad informática manejan en sus soluciones tradicionales de protección. De esta manera, este tipo de ataques avanzados maximizan la ventana de oportunidad para conseguir sus objetivos.

Por esta razón, el enfoque de "sentarse y esperar" implantado por las herramientas de seguridad tradicional frente a APTs y amenazas equivalentes significa que el tiempo de exposición se extenderá por un **promedio de 175 días desde que se produce la intrusión hasta que ésta es visible y detectable.** Incluso en muchas ocasiones son fuentes externas, como pueden ser las fuerzas de orden público o las compañías de tarjetas de crédito, las que hacen el trabajo (generalmente tarde) de la solución de seguridad tradicional implantada en las empresas, un hecho que puede afectar severamente a la reputación de las empresas.

La respuesta: Threat Hunting

Los gobiernos y las corporaciones han identificado este riesgo y asignado mayores presupuestos a la creación de recursos especializados para conformar un nuevo grupo de profesionales enfocados en detectar y repeler este tipo de ciberataques. Este perfil técnico, llamado de forma genérica "Threat Hunter", cuenta con los conocimientos necesarios para detectar las técnicas y tácticas de los nuevos ciberataques, y dispone de un nuevo conjunto de herramientas avanzadas que completan los productos de seguridad tradicional ya instalados en las empresas.

Las herramientas de threat hunting permiten afrontar los principales retos de los SOCs en las empresas:

- La dificultad a la hora de encontrar personal cualificado que desempeñe las tareas de un analista de seguridad experimentado.
- El mayor número de situaciones potencialmente peligrosas que sufren las empresas tiene como resultado un desbordamiento de la capacidad del SOC, incrementando las probabilidades de que las alertas reales no sean investigadas por falta de tiempo o recursos.
- El mayor número de herramientas requeridas, el incremento en su sofisticación y la ausencia de una solución centralizada y única que cubra todas las necesidades del SOC requiere características avanzadas de integración para formar una pila de software flexible y bien compenetrada.

Por esta razón, empresas y naciones se ven obligados a lidiar con presupuestos mucho más abultados si quieren hacer frente a estos nuevos ataques y salvaguardar su propiedad intelectual y su credibilidad.

Beneficios de Cytomic Orion

Cytomic Orion es un servicio orientado a analistas de seguridad especializados cuyos beneficios principales son:

- Búsqueda proactiva y automatizada de amenazas avanzadas y ataques informático que no usan malware para conseguir sus objetivos, dificultando su detección mediante las herramientas tradiciones de seguridad.
- Búsqueda de TTPs (tácticas, técnicas y procedimientos) usadas por los hackers.
- Detectar los ataques en fases tempranas, antes de que se puedan conseguir sus objetivos.
- Establecer medidas de respuesta frente a las amenazas detectadas, incluyendo la contención de las brechas de seguridad, la reversión de las modificaciones efectuadas en los equipos de la red provocadas por el ataque y la recuperación de evidencias para elaborar las tareas de análisis forense posteriores.
- Se integra con facilidad con el resto de las herramientas del SOC.

Búsqueda proactiva de amenazas avanzadas

Cytomic Orion implementa un proceso continuo de monitorización y búsqueda de indicios bajo la premisa de que la amenaza de entrada de atacantes que consiguen "instalarse" en la red de las organizaciones es permanente. Para ello genera automáticamente hipótesis en forma de indicios que muestran las nuevas técnicas de evasión y movimientos laterales detectadas, ofreciendo al analista un punto de partida válido para profundizar en la investigación y validar estas hipótesis.

Figura 2.1: Fases de la cadena CKC

Detección de ataques en fases tempranas

La detección del atacante en las fases iniciales hace posible una reducción del riesgo, una aceleración de las capacidades de contención y una reducción de los costes operativos. Cytomic Orion permite detener ataques en cualquier de las fases definidas de la Cyber Kill Chain.

Búsqueda de TTPs

El framework ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge), desarrollado por Mitre Corp., fue creado hace 5 años y es un documento vivo y creciente de las tácticas y técnicas empleadas por los hackers, resultado del estudio de millones de ataques a redes empresariales.

El objetivo de Mitre es dividir y clasificar los ataques de una manera coherente y clara que facilite su identificación y descubrimiento. La mayoría de los atacantes utilizan una combinación de técnicas y tácticas para ocultar sus movimientos laterales, descubrir las vulnerabilidades de los sistemas y explotarlos, evadir las protecciones y aprovechar las debilidades y configuraciones inseguras de la red y los equipos.

Encontrar cada una de estas técnicas dentro de un ataque en curso es clave para identificar en qué fase de la CKC se encuentra el atacante. Esto contribuye a simplificar el análisis de la situación y a ganar en eficiencia al recoger las evidencias que ayuden a identificar los objetivos del hacker y permitan a la empresa diseñar un plan detallado de respuesta.

Por este motivo, las reglas expertas y de threat hunting de Cytomic Orion se corresponden con las técnicas descritas en el framework ATT&CK, facilitando su interpretación y acelerando la puesta en marcha de los mecanismos de resolución.

Medidas de respuesta

La respuesta a incidentes constituye un proceso compuesto por una serie de pasos secuenciales dirigidos y ejecutados por el CSIRT (Equipo de respuesta a incidentes de seguridad informática), muchos de ellos asistidos por las herramienta de resolución remota incorporadas en Cytomic Orion:

Contener el daño y minimizar el riesgo

Actuando rápidamente se pueden reducir los efectos reales de un ataque, minimizando su importancia. El objetivo de la fase de contención es proteger la información confidencial de la organización en el curso del ataque descubierto sin entorpecer las tareas del equipo de respuesta ante incidentes. Esto incluye proteger contra pérdida o modificación los archivos de sistema, que pueden tener como consecuencia períodos prolongados sin servicio.

Identificar el tipo y la gravedad del ataque

Para poder recuperarse de forma eficaz de un ataque se debe determinar la gravedad de la situación de peligro que han sufrido los equipos. Para ello es necesario determinar la naturaleza del ataque, su punto de origen y la fecha en la que se inició, su intención, localizar los equipos puestos en peligro y los archivos a los que se ha tenido acceso no autorizado.

Recopilar pruebas

En muchos casos, si el entorno ha sufrido un ataque intencionado puede ser necesario poner una denuncia ante las autoridades. Para posibilitar esta opción, es necesario recoger evidencias del ataque: ficheros manipulados, trazas de red, procesos ejecutados y otros elementos del equipo comprometido.

Recuperación de los equipos

La forma de recuperar el servicio dependerá generalmente del alcance del incidente de seguridad, con planes de acción que cubren desde la eliminación de ficheros y procesos hasta la restauración de copias de seguridad anteriores al inicio del incidente.

Integración con las herramientas del SOC

Cytomic Orion incorpora varias APIs para facilitar su integración con el resto de herramientas desplegadas en el SOC. De esta forma, las organizaciones pueden construir un stack de herramientas con las ventajas indicadas a continuación:

- Capacita al SOC para ofrecer una respuesta homogénea ante los múltiples tipos de incidentes y situaciones que enfrentará.
- Minimiza el intercambio manual de información entre las distintas herramientas implantadas.
- Facilita el avance en la automatización de las tareas más repetitivas, ahorrando tiempo y esfuerzo de los técnicos, que podrán invertirlo en tareas más productivas.

Arquitectura de Cytomic Orion

Cytomic Orion es un servicio de threat hunting avanzado que se integra con las distintas herramientas utilizadas en los SOCs de la empresas para ejecutar las tareas de su competencia:

- Triaje / filtrado de indicios.
- Procesos de investigación.
- Establecimiento de las directrices de contención y respuesta.
- Reporte de la actividad maliciosa detectada y las acciones emprendidas para mitigar sus efectos.

Para ello Cytomic Orion analiza toda la información recogida por Cytomic EDR: la monitorización de las acciones y eventos producidos por los procesos ejecutados en los equipos de usuario y servidores se envía a la nube y se enriquece con información de contexto y de seguridad para generar la telemetría. Esta telemetría es interpretada por Cytomic Orion para generar indicios que los técnicos del SOC investigarán en busca de actividades maliciosas.

A continuación se muestra el esquema general de los distintos módulos de Cytomic Orion y los actores y fuentes de datos que interactúan con el entorno, así como se introducen los conceptos más frecuentemente utilizados en esta Guía de uso.

La arquitectura de Cytomic Orion se divide en tres grandes grupos:

- Actores del SOC / MSSP / MDR.
- Procesos y tecnologías de la plataforma.
- Inteligencia, integración y fuentes de datos externas

Actores del SOC / MSSP / MDR

Figura 2.2: Actores del SOC / MSSP / MDR

En los SOCs de tamaño mediano y grande se produce una especialización del personal técnico que lo integra, distribuido en un número variable de capas según sea su tamaño y grado de desarrollo:

- **Nivel 1 (Tier 1)**: formado por los analistas que ejecutan el triaje de indicios. Examinan y catalogan las hipótesis producidas por Cytomic Orion y crean investigaciones que agrupan indicios similares para asignárselas a los técnicos de nivel 2 y 3, que las analizarán en profundidad. Adicionalmente, el nivel 1 descarta las hipótesis falsas que reflejan un

funcionamiento normal de los procesos monitorizados, actuando como filtro que evita un desbordamiento en niveles superiores.

- **Nivel 2 (Tier 2)**: formado por los analistas que reciben las investigaciones generadas en el nivel 1 y son susceptibles de constituir una amenaza para la empresa. Este nivel es el encargado de profundizar en los indicios asociados para localizar los verdaderos intentos de intrusión, valorar los daños causados y establecer los métodos de resolución y contención pertinentes.
- **Nivel 3 (Tier 3)**: formado por analistas de perfil alto en seguridad que generan nuevas hipótesis usando métodos diferentes de investigación basados en información externa, tales como boletines de seguridad emitidos por terceros, CVEs (Common Vulnerabilities & Exposures), portales y páginas web especializados en seguridad y otros. No requieren del triaje de indicios realizado en el nivel 1 para iniciar su actividad.
- **Gestor del SOC**: es el encargado de coordinar los esfuerzos de los analistas, reasignar investigaciones, derivar recursos y tiempo a los clientes más prioritarios y evaluar el desempeño y los resultados de las investigaciones ya concluidas.

Procesos y tecnologías de la plataforma

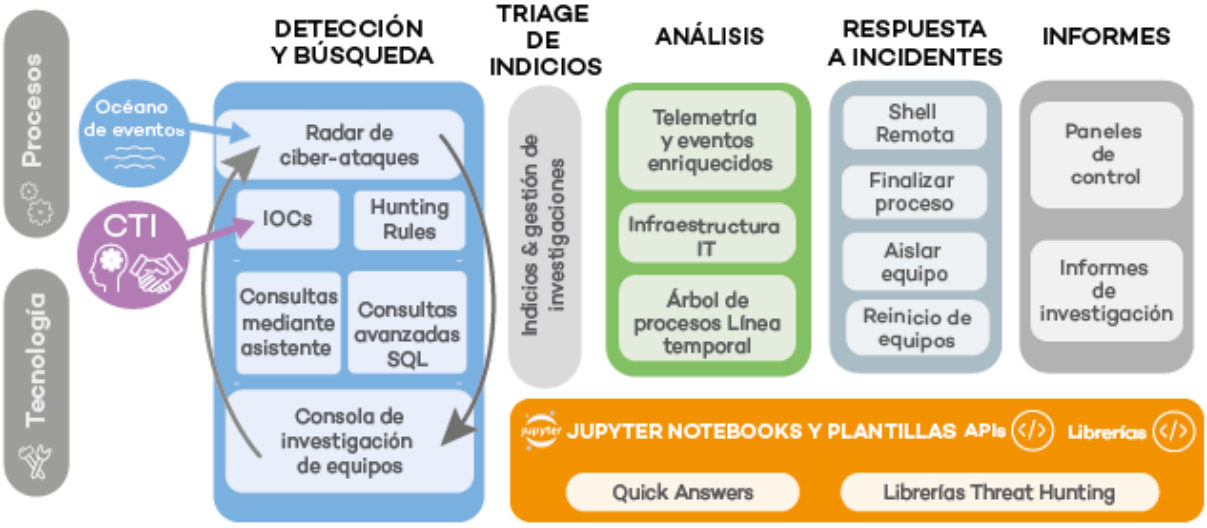


Figura 2.3: Procesos y tecnologías de la plataforma

Proceso	Tecnología	Descripción
Detección y búsqueda	**CTI (Cyber Threat Intelligence)**	Plataforma de código abierto que centraliza y almacena inteligencia de seguridad relativa al malware de reciente aparición. Facilita la investigación del crimen y espionaje informáticos.
	Océano de datos	Fuente de datos utilizada por Cytomic Orion para

Proceso	Tecnología	Descripción
		ejecutar los procesos de hunting y retrospectivas. Formado por toda la telemetría recogida de los equipos de la organización, cuyo origen es la monitorización de los procesos ejecutados en los equipos de usuario y servidores de la empresa. El tiempo de retención de la telemetría en el océano de datos es de 1 año.
	Radar de Ciber-ataques en tiempo real	Comprueba de forma automática y en tiempo real el océano de datos en busca de patrones de eventos sospechosos que pueden formar parte de un ataque informático.
	Reglas de Hunting (Hunting rules)	Describen patrones de acciones que el Radar de ciber-ataques busca en el flujo de telemetría producido por los procesos ejecutados en los equipos del cliente. Consulta **Indicios y reglas de hunting** en la página **70** y **Gestión de Hunting rules** en la página **85**.
	IOCs	Estándar de la industria que permite describir condiciones susceptibles de comprometer la seguridad de las organizaciones. Siendo un concepto similar al del fichero de firmas utilizado por las herramientas de protección contra el malware, su formato es abierto, con lo que se favorece su compartición e intercambio. El radar de Ciber-ataques admite IOCs para buscar patrones en tiempo real.
	Consultas mediante asistente	Construye consultas de forma sencilla y guiada para recuperar información tabulada del océano de datos. Consulta **Módulo de consultas avanzadas SQL** en la página **156**
	Consultas avanzadas	Construye búsquedas complejas mediante código en lenguaje SQL. Consulta **Módulo de consultas avanzadas SQL** en la página **156**.

Proceso	Tecnología	Descripción
	Consola de investigación de equipos	Analiza de forma retrospectiva los procesos ejecutados en un equipo de usuario o servidor para profundizar en las condiciones que propiciaron la creación del indicio generado por el Radar de ciber-ataques en tiempo real. Consulta **Análisis de indicios con la consola de investigación** en la página **186**.
Triaje de indicios	**Filtrado manual de los indicios generados por el Radar de ciber-ataques y realizado por el equipo de analistas de nivel 1. Su objetivo es separar los indicios que representan ataques reales de los falsos positivos para evitar la sobrecarga de tareas en el nivel 2 y centrar la atención de los analistas en los casos que suponen un peligro para la organización.**	
Análisis	**Incluye las funcionalidades de la consola de investigación, los diagramas de grafos y los recursos implementados en el agente instalado en los equipos de la infraestructura IT de la empresa.**	
	Árbol de procesos	Representa las relaciones padre - hijo de los procesos ejecutados en los equipos del parque informático. Consulta **Diagramas de grafos** en la página **202**.
	Línea temporal	Lista todos los eventos producidos, ordenados por su marca de tiempo para facilitar la visualización de la progresión del ataque.
	Listado de eventos enriquecidos	Listado completo de eventos producidos y enriquecidos con la inteligencia de seguridad de Cytomic. Consulta **Análisis de indicios con la consola de investigación** en la página **186**.
	Infraestructura IT	Acceso completo al estado de los recursos y procesos de los equipos de la infraestructura IT del cliente. Consulta **Investigación en la infraestructura IT con OSQuery** en la página **248**
Respuesta a incidentes	**Herramientas para resolver de forma remota las brechas de seguridad y recuperar información que servirá como entrada en los procesos de**	

Proceso	Tecnología	Descripción
	análisis forense sobre los equipos afectados. Consulta Herramientas de respuesta en la página **254.**	
Jupyter Notebooks	**Automatización de los análisis retrospectivos, generando informes y permitiendo compartir técnicas de hunting entre analistas. Consulta** Investigación con notebooks en la página **220.**	
	Respuestas rápidas	Fragmentos de código reutilizables que funcionan de forma independiente y resuelven problemas concretos que se presentan frecuentemente en el día a día de los analistas. Consulta **Herramientas de respuesta** en la página **254**.
	Plantillas	Notebooks predefinidos y publicados por Cytomic o por los propios clientes para ser compartidos y utilizados como base por los analistas en la automatización de las tareas de hunting. Consulta **Gestión de plantillas** en la página **230**.

Tabla 2.1: Procesos y tecnologías de la plataforma Cytomic Orion

Inteligencia y fuentes de datos

Figura 2.4: Inteligencia y fuentes de datos

Fuente de datos	Descripción
Librería de consultas	Acelera y facilita las labores de hunting de los analistas. Construida y mantenida por el equipo de threat hunters de Cytomic y por los analistas de los SOCs que utilizan Cytomic Orion. Consulta **Investigar el flujo de eventos** en la página **155**.
Librería de	Accede al océano de datos desde los notebooks y acelera el desarrollo de

Fuente de datos	Descripción
Threat hunting	procedimientos de análisis. Consulta el enlace **https://info.cytomicmodel.com/resources/help/ORION/es/threathuntingAPI/index.htm** para obtener información específica de esta librería.
API IOCs	Habilita el uso de fuentes de inteligencia de seguridad externas para importar nuevos identificadores de compromiso, ampliando las capacidades de análisis de las Hunting rules. Consulta **API de IOCs** en la página **332**
API Indicios	Integra Cytomic Orion con plataformas de ticketing para automatizar y mejorar el seguimiento de los incidentes detectados. Consulta **API de indicios** en la página **349**
API de conocimiento	Comparte con aplicaciones de terceros información extendida sobre los ficheros vistos en el parque informático del cliente y de los equipos que los almacenan. Consulta **API de conocimiento** en la página **342**
API de respuesta a incidentes	Permite a aplicaciones de terceros o desarrolladas por el propio SOC aislar, retirar el aislamiento y reiniciar los equipos del parque informático del cliente que estén bajo la amenaza de un ciberataque. Consulta **API de respuesta** en la página **352**
API de acceso a OSQuery	Obtiene información muy detallada sobre el estado de los recursos y procesos que se ejecutan en el equipo del usuario. Consulta **API de acceso a OSQuery** en la página **356**
Plantillas de Notebooks	El equipo de threat hunters de Cytomic desarrolla y mantiene una librería de plantillas de notebooks que automatizan los análisis retrospectivos más complejos, y son utilizados como base por los analistas del SOC para sus propios desarrollos.
Respuestas rápidas	El equipo de threat hunters de Cytomic construye y mantiene una librería de fragmentos de código reutilizables, centrados en resolver problemas muy concretos. Estos fragmentos pueden servir como base para el desarrollo de Notebooks más complejos por parte de los analistas del SOC.

Tabla 2.2: Fuentes de datos disponibles en Cytomic Orion

El océano de datos y la monitorización de procesos

Cytomic Orion se apoya en las sondas instaladas en los equipos de usuario y servidores para monitorizar de forma continua la ejecución de todos los procesos cargados en la memoria RAM de los equipos, tanto si han sido clasificados previamente como goodware como si se trata de procesos del sistema, procesos sin clasificar (desconocidos), malware o PUPs. Cualquier proceso clasificado como goodware que haya sido comprometido (por ejemplo mediante exploits que aprovechen alguna vulnerabilidad descubierta en el proceso) será igualmente monitorizado y su telemetría enviada al océano de datos. De esta forma, el analista podrá investigar y comprobar cual fue la secuencia que llevó a la explotación de esa vulnerabilidad y los efectos que produce en el proceso comprometido, para poder organizar las labores de resolución que considere oportunas.

De la misma forma, los programas clasificados como sospechosos por los motores heurísticos de la solución de seguridad local serán también monitorizados y enviada su telemetría para que el analista pueda determinar si su comportamiento es legítimo, o por el contrario muestran una cadena de ejecución de acciones que puede ser interpretada como peligrosa y dañina para los intereses de la organización.

Características de Cytomic Orion

Cytomic Orion incorpora todos los bloques funcionales necesarios para centralizar las herramientas de threat hunting requeridas por los analistas en un SOC interno o que forme parte de un MSSP / MDR dedicado a dar servicios de seguridad a clientes externos.

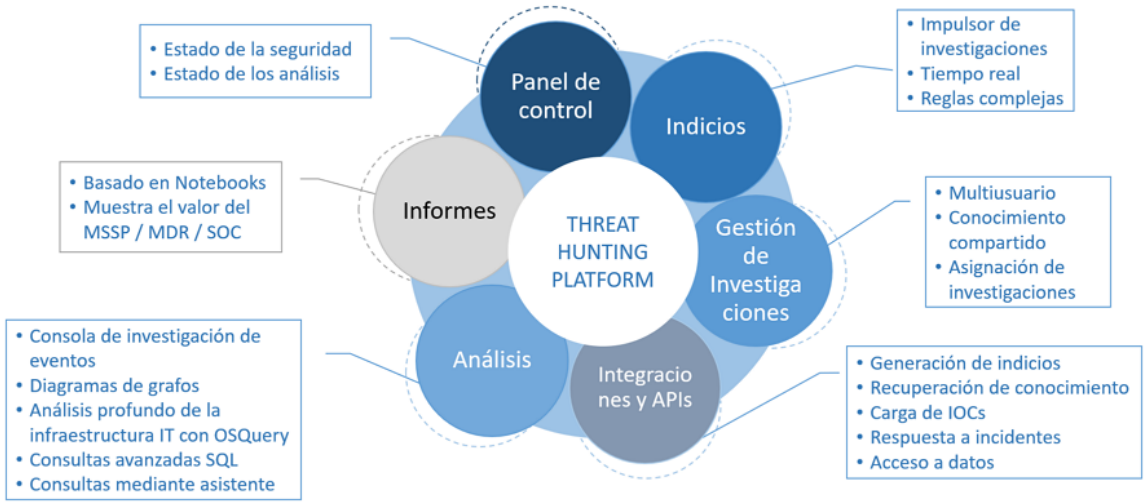


Figura 2.5: Diagrama resumen de características de Cytomic Orion

Las principales características de Cytomic Orion son:

Generación automática de hipótesis

Los indicios son el punto de entrada más frecuente a la hora de iniciar un proceso de investigación. Son avisos que genera el Radar de cyber-ataques en tiempo real y que reflejan un patrón de ejecución anómalo que los analistas deberán de revisar, en un proceso que se conoce como "triaje de indicios" o "validación de alertas".

Generación de indicios adaptada a cada cliente

Los analistas de Cytomic inspeccionan de forma transversal la telemetría generada por los equipos de los clientes. Como resultado de esta investigación, generan Hunting rules que el Radar de ciberataques utiliza para detectar patrones y secuencias de acciones que pueden pertenecer a la ejecución de un ataque. Para adaptar la detección de patrones a la casuística particular de cada cliente, los analistas del SOC también tiene la capacidad de desarrollar sus propias Hunting rules que generan indicios para ser investigados.

Entorno de investigación compartido

Cytomic Orion entrega a los analistas un recurso donde almacenar toda la información que se va generando a lo largo del tiempo en los procesos de investigación sobre los indicios estudiados. En Cytomic Orion este recurso recibe el nombre de Investigación, y puede ser utilizado y compartido entre varios analistas.

Filtrado flexible de eventos monitorizados

Para facilitar la búsqueda transversal en el océano de datos formado por toda la actividad monitorizada de los equipos de usuario y servidores, Cytomic Orion ofrece un motor SQL con el que los analistas pueden construir consultas avanzadas y ejecutar búsquedas de actividades sospechosas que den soporte a sus investigaciones.

Generación de consultas mediante asistente

Adicionalmente, para los analistas no acostumbrados a trabajar con el lenguaje SQL, Cytomic Orion ofrece un asistente de consultas que crea búsquedas sencillas de forma rápida y sin errores.

Investigación en profundidad de la actividad en los equipos

Ofrece al analista una consola de investigación de equipos que reúne las herramientas necesarias para visualizar y revisar todos los eventos producidos en un equipo de usuario o servidor, y así profundizar y concretar la investigación en curso. La consola de investigación de equipos permite visualizar el flujo de eventos de dos formas:

- **Árbol de procesos**: muestra de forma rápida la relación padre - hijo existente entre procesos.
- **Gráfico de línea temporal**: muestra la cronología de eventos para valorar el desarrollo del ataque.

Investigación en detalle del estado de los equipos

El acceso a la librería de OSQuery ofrece una visión muy detallada del estado de todos los equipos que forman la infraestructura IT del cliente. Esta información es utilizada por los analistas del SOC para profundizar en las investigaciones abiertas así como para confirmar y completar las evidencias encontradas mediante la inspección de eventos monitorizados.

Automatización y compartición de los análisis y búsquedas

Cytomic Orion da soporte a los Jupyter Notebooks, donde el analista puede codificar en lenguaje Python algoritmos que le ayuden en su investigación para compartirlos con el resto de miembros de su equipo y así automatizar y acelerar los procesos de análisis y búsquedas.

Adicionalmente, Cytomic Orion permite la reutilización y compartición del código generado en las automatizaciones a través de Plantillas y Respuestas rápidas.

Gráficas del estado de la investigación

Los notebooks disponibles en Cytomic Orion permiten mostrar de forma visual los hallazgos del analista a través de librerías de uso muy popular tales como `mathplotlib` y otros. Consulta **Librerías disponibles en los notebooks** en la página **242**.

Los notebooks del tipo diagrama de grafos representan el flujo de telemetría en forma de nodos y relaciones, con el objetivo de simplificar la interpretación de las operaciones ejecutadas por el software instalado en los equipos del cliente. Consulta **Diagramas de grafos** en la página **202**.

Panel de control

Visualiza estadísticas para que el gestor de SOC pueda comprobar de un vistazo los equipos de la organización de mayor riesgo potencial, así como ver el estado de las investigaciones iniciadas por los analistas.

Herramientas de respuesta a incidentes

Cytomic Orion incorpora herramientas para contener los ataques en curso y mitigar sus efectos. El equipo de contención de incidentes podrá aislar de la red los equipos afectados, controlar los procesos y servicios en ejecución así como enviar y recuperar ficheros del equipo. También ofrece la posibilidad de lanzar una línea de comandos remota con herramientas especializadas para profundizar en la investigación y ejecutar procedimientos específicos para la resolución de problemas.

Integración con herramientas de terceros

Cytomic Orion incorpora una API REST para integrarse con las herramientas más frecuentemente utilizadas en el SOC (herramientas de ticketing, plataformas para el intercambio de inteligencia de seguridad etc.). Las funciones expuestas a la aplicación de terceros se dividen en cinco bloques: IOCs, Indicios, OSQuery, Conocimiento y Respuesta. Configurando los permisos apropiados desde la consola de Cytomic Orion se limita el acceso de la aplicación de terceros a los bloques de

funciones necesarios. El alcance de la información devuelta por Cytomic Orion se establece indicando los clientes que formarán parte de la respuesta a las llamadas de la API.

Cytomic Orion implementa un acceso a la API seguro: para la comunicación con la aplicación de terceros se utiliza el protocolo HTTPS y es necesario completar la fase de autenticación / autorización según el estándar OAuth.

Perfil de usuario del producto

Cytomic Orion es un producto destinado a threat hunters, profesionales de seguridad que desarrollan su actividad en proveedores de servicios administrados (MSSPs / MDRs) y en los SOCs de las organizaciones. Estos cazadores de amenazas y analistas de ciberseguridad utilizan de forma proactiva técnicas manuales o asistidas para detectar incidentes de seguridad diseñados para sortear los sistemas de protección instalados en los equipos de usuario y servidores. Los cazadores de amenazas intentan descubrir los incidentes que permanecen ocultos para las organizaciones, ofreciendo una línea de defensa adicional contra las amenazas persistentes avanzadas (APT).

Para detectar incidentes de seguridad, el analista usa habilidades de pensamiento crítico e intuiciones desarrolladas por la experiencia para observar patrones de ejecución normales e identificar anomalías en el comportamiento de los procesos en funcionamiento. Un threat hunter debe tener un conocimiento considerable del negocio desarrollado por la empresa y un entendimiento de las operaciones cotidianas que se desarrollan en su interior. De esta forma será capaz de extraer los eventos extraordinarios y susceptibles de pertenecer a la cadena de ataque de un hacker del flujo de eventos habituales, minimizando los falsos positivos. Adicionalmente, se requiere tener buenas habilidades de comunicación para compartir los resultados de las investigaciones. Es especialmente importante para el analista mantenerse al día con las últimas tendencias de seguridad.

En lugar de tratar de infiltrarse en el entorno desde el exterior, como sucede durante las pruebas de penetración, los analistas de seguridad trabajan con el supuesto de que los adversarios ya han entrado en el sistema. Analizan cuidadosamente todo el entorno, utilizan análisis de comportamiento y un enfoque basado en hipótesis para encontrar situaciones inusuales que puedan indicar la presencia de actividad maliciosa.

Responsabilidades de un analista de seguridad

Los threat hunters tienen como objetivo detectar las amenazas informáticas avanzadas. Su trabajo es rastrear y neutralizar a los adversarios que no pueden ser detectados con otros métodos tradicionales. Las amenazas que buscan pueden ser lanzadas tanto por insiders, como puede ser un empleado de la organización, como por atacantes externos, que pueden pertenecer a grupos del crimen organizado.

Una vez identificadas las amenazas potenciales, los analistas de seguridad recopilan la mayor cantidad de información posible sobre el comportamiento, los objetivos y los métodos de los hackers. También organizan y analizan los datos recopilados para determinar las tendencias en el

entorno de seguridad de la organización, hacen predicciones para el futuro y eliminan las vulnerabilidades actuales.

Habilidades y conocimientos requeridos

- **Experiencia en seguridad informática**: los threat hunters deben tener experiencia en seguridad de la información, seguridad cibernética o ingeniería de redes. También deben tener experiencia práctica en análisis forense, análisis de datos, técnicas de ingeniera inversa aplicables al malware, seguridad de redes y en equipos de usuario y servidores, seguimiento de adversarios y otras tareas relacionadas con la seguridad en entornos informáticos.
- **Comprender el panorama de la seguridad informática**: además de la experiencia práctica, los threat hunters también deben tener un conocimiento profundo de los métodos utilizados por el malware actual y pasado, las metodologías de ataque y las TTP (tácticas, técnicas y procedimientos). Los TTP evolucionan rápidamente con el tiempo, por lo que contar con un conocimiento actualizado sobre este tema es crucial para una búsqueda exitosa de amenazas informáticas.
- **Conocimiento de los sistemas operativos y protocolos de red**: es indispensable un amplio conocimiento del funcionamiento interno de los sistemas operativos y de los detalles de los diferentes protocolos de red utilizados en las empresas (pila TCP / IP, NetBIOS, protocolos del nivel de aplicación más comunes etc).
- **Habilidades de programación**: los cazadores deben dominar al menos un lenguaje de scripting. En la actualidad el lenguaje de script más difundido por su versatilidad y utilizado en entornos de seguridad es Python. También es necesario saber cómo analizar y manipular registros, automatizar tareas y realizar análisis de datos complejos.
- **Habilidades de redacción de informes y presentación gráfica de datos**: la preparación de informes de seguridad y diferentes documentos técnicos es una parte esencial de la caza de amenazas cibernéticas, por lo que los analistas también deben tener excelentes habilidades técnicas de redacción e informes.
- **Otras habilidades**: habilidades analíticas, de investigación y de resolución de problemas. Los analistas de seguridad son roles que tienden a trabajar de forma autónoma, con una administración mínima. Sin embargo, también deben tener habilidades interpersonales y de colaboración, ya que suelen trabajar junto con otros profesionales de otros campos de la seguridad de la información.

Sistemas operativos, navegadores e idiomas compatibles

Compatibilidad con sondas instaladas en el equipo de usuario y servidor

Para analizar y almacenar la telemetría generada por la monitorización de procesos ejecutados en los equipos, Cytomic Orion requiere la instalación y ejecución de uno de los siguientes productos de seguridad:

- Cytomic EPDR
- Cytomic EDR

Compatibilidad con sistemas operativos

Cytomic Orion monitoriza los eventos producidos por los procesos ejecutados en los sistemas operativos mostrados a continuación:

- **Windows**
  - **Estaciones de trabajo**: Windows XP SP3, Windows Vista, Windows 7, Windows 8, Windows 10 y Windows 11.
  - **Servidores**: Windows 2003 SP2, Windows 2008, Windows Server Core 2008, Windows Small Business Server 2011, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019 y Windows Server 2022.
  - **Versiones con procesador ARM**: Windows 10 Home y Pro. Windows 11 Home y Pro.
  - **Servidores Exchange**: 2003 al 2019.
- **macOS**
  - **Sistemas operativos**: macOS 10.10 Yosemite y superiores.
- **Linux**
  - **Sistemas operativos 64 bits**: Ubuntu 14.04 LTS y superiores, Fedora 23 y superiores, Debian 8 y superiores, RedHat 6.0 y superiores, CentOS 6.0 y superiores, LinuxMint 18 y superiores, SuSE Linux Enterprise 11.2 y superiores, Oracle Linux 6 y superiores. No requiere sistema de ventanas instalado.
  - **Sistemas operativos 32 bits**: RedHat 6.0 a 6.10 y CentOS 6.0 a 6.10.

Consulta la web de soporte en ***https://www.pandasecurity.com/spain/support/card?id=700009*** *para comprobar la última versión del kernel de Linux soportada por Cytomic Orion.*

*Consulta **https://info.cytomicmodel.com/resources/guides/EDR/latest/es/EDR-guia-ES.pdf** y **https://info.cytomicmodel.com/resources/guides/EPDR/latest/es/EPDR-guia-ES.pdf** para obtener un listado más detallado de los requisitos de Cytomic EPDR y Cytomic EDR.*

Compatibilidad con navegadores web

La consola de administración es compatible con las últimas versiones de los navegadores mostrados a continuación:

- Chrome
- Microsoft Edge
- Firefox

Idiomas compatibles con la consola web

- Español
- Inglés

Requisitos para utilizar las herramientas de respuesta

Para utilizar las herramientas de acceso remoto y linea de comandos es necesario que tanto el equipo del usuario como el cortafuegos perimetral de la red del cliente permitan el trafico desde y hacia las URLs siguientes:

- dir.rc.pandasecurity.com por el puerto 443.
- eu01.rc.pandasecurity.com por los puertos 8080 y 443.
- eu02.rc.pandasecurity.com por los puertos 8080 y 443.
- eu03.rc.pandasecurity.com por los puertos 8080 y 443.
- eu04.rc.pandasecurity.com por los puertos 8080 y 443.
- eu05.rc.pandasecurity.com por los puertos 8080 y 443.
- eu06.rc.pandasecurity.com por los puertos 8080 y 443.
- ams01.rc.pandasecurity.com por los puertos 8080 y 443.
- ams02.rc.pandasecurity.com por los puertos 8080 y 443.

Capítulo 3

La consola de análisis

Cytomic Orion utiliza las últimas tecnologías de desarrollo web para ofrecer una consola de análisis alojada en la nube que permite interactuar cómoda y ágilmente con el servicio de seguridad. Sus principales características son:

- **Adaptable:** diseño "responsive" que se adapta al tamaño de la pantalla del equipo empleado para administrar el servicio.
- **Amigable**: interface desarrollado con tecnología Ajax que evita las recargas de páginas completas.
- **Flexible**: interface adaptable que almacena los ajustes realizados para posteriores accesos.
- **Homogénea**: patrones de usabilidad bien definidos para minimizar la curva de aprendizaje del analista.

CONTENIDO DEL CAPÍTULO

Beneficios de la consola de análisis

La consola Web, también llamada "consola de análisis" o simplemente "consola", es la herramienta principal de los analistas para desarrollar el triaje de indicios y los procesos de investigación. Al tratarse de un servicio Web, hereda una serie de características que facilitan el trabajo en el SOC:

Única herramienta para el proceso de hunting

Todos los analistas del SOC independientemente del nivel al que pertenezcan tienen disponible toda la funcionalidad necesaria para desarrollar los procesos de investigación, sin requerir herramientas externas adicionales de terceros.

La funcionalidad se ofrece desde una única consola Web, lo que favorece la integración de las distintas herramientas y evita tener que utilizar varios productos de distintos proveedores.

Procesos centralizados para SOCs remotos y equipos de usuario desplazados

La consola Web está alojada en la nube de Cytomic, por lo que no son necesarias configuraciones de VPN ni redirecciones de puertos en los routers corporativos para su acceso desde el exterior de la oficina: cualquier analista puede acceder al servicio en cualquier momento y lugar, e iniciar un triaje de indicios o un proceso de investigación sobre cualquier equipo de usuario o servidor, independientemente de la red a la que esté conectado o si está en itinerancia o en su hogar.

Ni el MSSP / MDR ni la compañía que subcontrata los servicios de seguridad necesita invertir en infraestructuras IT, tales como servidores, licencias de sistemas operativos o bases de datos, ni es necesaria una gestión del mantenimiento / garantía del hardware para asegurar el funcionamiento del servicio.

Gestión de la seguridad desde cualquier equipo

La consola Web es de tipo "responsive / adaptable" con lo que se ajusta al tamaño de la pantalla del equipo utilizado por el analista. De esta manera se puede gestionar la seguridad desde cualquier lugar y en cualquier momento, mediante un PC de escritorio o un laptop.

Requisitos de la consola de análisis

Para acceder a la consola Web utiliza la siguiente URL:

https://orion.cytomicmodel.com

Es necesario cumplir con el siguiente listado de requisitos:

- Contar con unas credenciales validas (usuario y contraseña).

Para más información sobre cómo crear una cuenta Cytomic de acceso a la consola Web consulta ***Acceso, control y supervisión de la consola de análisis** en la página **47**.*

- Un navegador compatible certificado. Se requiere la última versión de los navegadores compatibles mostrados a continuación:
    - Chrome
    - Microsoft Edge

- Firefox

- Conexión a Internet y comunicación por el puerto 443.

Federación con IDP

Cytomic Orion delega la gestión de las credenciales en un Proveedor de Identidades (Identity Provider, IDP), una aplicación centralizada responsable de gestionar las identidades de los usuarios de la consola web.

Con una única cuenta Cytomic el administrador de la red tiene acceso a todos los productos contratados con Cytomic de forma segura y sencilla.

*Consulta **Acceso, control y supervisión de la consola de análisis** en la página **47** para obtener más información sobre el IDP y la creación de cuentas Cytomic.*

Estructura general de la consola de análisis

La consola Web cuenta con recursos que facilitan una experiencia de trabajo homogénea y coherente en los distintos niveles del SOC, tanto para realizar el triaje de indicios como para realizar un proceso de investigación.

El objetivo de la consola es entregar al analista una herramienta sencilla, pero a la vez flexible y potente, que le permita comenzar a realizar investigaciones de forma productiva en el menor período de tiempo posible.

A continuación, se incluye una descripción de los elementos básicos de la consola y su modo de uso.

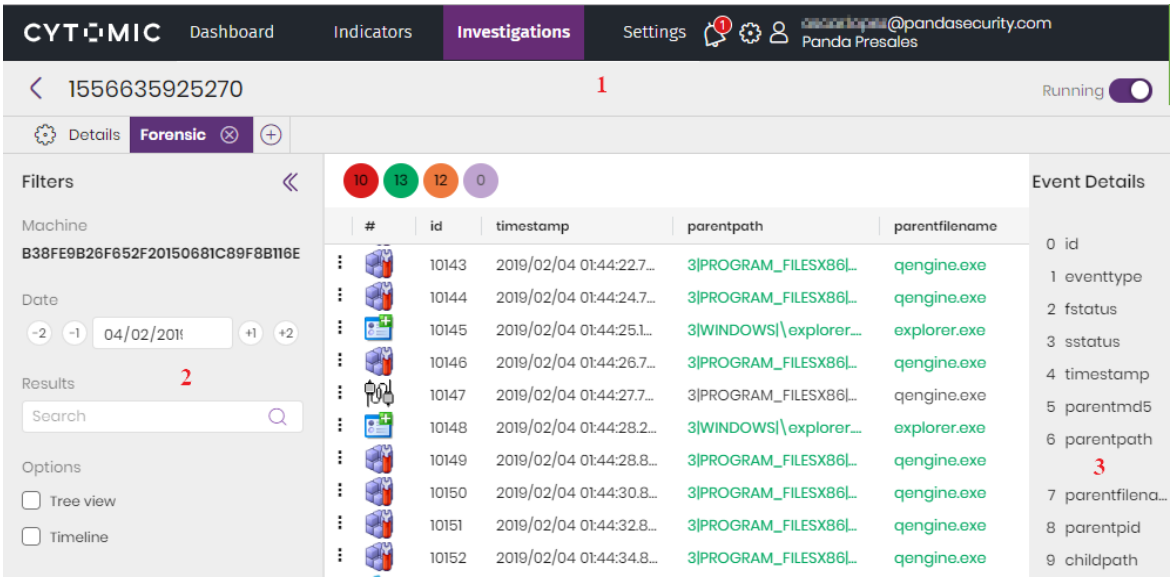


Figura 3.1: Vista general de la consola de análisis

Menú superior (1)

La distribuye toda su funcionalidad en varias zonas o áreas accesibles desde el menú superior:

- Dashboard
- Indicios
- Investigaciones
- Configuración
- Gestión del producto
- Cuenta de usuario

Zona Dashboard

Muestra el panel de control de la consola desde el cual el analista y el gestor del SOC tienen acceso de forma gráfica a toda la información sobre los procesos de investigación realizados, y a los indicios generados. Los widgets del panel de control son accionables: al hacer clic con el puntero del ratón en los distintos puntos del gráfico la consola cambiará de zona para mostrar los datos que Cytomic Orion utilizó al generar la gráfica.

*Consulta **Visibilidad de la actividad en Cytomic Orion** en la página **133** para obtener más información.*

Zona Indicios

Muestra el listado de hipótesis que el Radar de ciber-ataques en tiempo real ha generado para que los analistas de Nivel 1 realicen el triaje y generen a partir de ellas las investigaciones que serán desarrolladas por los técnicos de Nivel 2. El módulo de indicios contiene todas las herramientas necesarias para su gestión (cambio de estado, filtrado, información básica del equipo que disparó el indicio etc).

*Consulta **Indicios y reglas de hunting** en la página **70** para obtener más información*

Zona Investigaciones

Contiene el listado de investigaciones generadas, las herramientas básicas para su gestión y la información que los describen y que los analistas de Nivel 2 utilizan para su desarrollo.

*Consulta **Gestión de investigaciones** en la página **99** para obtener más información.*

Zona notificaciones

Para acceder a las comunicaciones de carácter general que Cytomic pone en conocimiento de todos los usuarios de la consola, haz clic en el icono  . Las notificaciones se muestran ordenadas según su fecha de aparición, y pueden incluir información sobre:

- Paradas programadas de mantenimiento.
- Avisos de vulnerabilidades críticas.
- Consejos de seguridad.

Cada comunicación tiene asociado un nivel de prioridad:

- Importante
- Aviso
- Informativa

El número del icono indica la cantidad de notificaciones web que no se han leído todavía. Cuando se despliega el panel de notificaciones, todo su contenido se considera leído, el número del icono de notificaciones se establece a 0 y deja de visualizarse.

Archivar notificaciones

Para archivar una notificación web, haz clic en su icono de aspa ✕ asociado. Las notificaciones así archivadas no se volverán a mostrar en el desplegable.

Para acceder a las notificaciones archivadas haz clic en el enlace **Ver todas las notificaciones**.

Las notificaciones con una antigüedad mayor a un mes se consideran caducadas y se eliminan de la zona de notificaciones.

Notificaciones persistentes

Son notificaciones importantes que no incorporan el icono de aspa, de forma que no es posible archivarlas manualmente.

Notificaciones siempre visibles

Algunas comunicaciones se consideran de lectura obligada, y se muestran justo debajo del menú superior. Estas notificaciones se apilan si hay más de una, y abarcan todo el ancho de la pantalla. La importancia de la notificación se indica con los mismos colores que las notificaciones normales.

Si el analista cierra una notificación siempre visible haciendo clic en el icono del aspa, ésta se vuelve a mostrar de forma automática cada vez que el usuario navega por la consola de análisis.

Las notificaciones siempre visibles también aparecen en el panel de notificaciones y no se pueden archivar manualmente.

Zona Configuración

Desde el panel lateral izquierdo se permite establecer ciertos parámetros para regular el acceso a la consola y al servicio así como su presentación gráfica:

- **Usuarios**: gestiona las cuentas de usuario que accederán a la consola, sus permisos y la visibilidad que tendrán de los equipos de los clientes del SOC. Consulta **Acceso, control y supervisión de la consola de análisis** en la página **47**.
- **Aplicaciones autorizadas**: establece los permisos para acceder a las distintas APIs desde aplicaciones de terceros. Consulta **Integración de Cytomic Orion con las herramientas del SOC** en la página **314**.
- **Clientes**: gestiona y ordena los clientes accesibles por el SOC mediante grupos. Consulta **Configuración de la visibilidad de clientes** en la página **55**.
- **IOCs**: lista los indicadores de compromiso cargados mediante la API de Cytomic Orion. Consulta **API de IOCs** en la página **332**.
- **Hunting Rules**: gestiona las reglas que analizan la telemetría enviada por los equipos monitorizados en busca de patrones de eventos sospechosos de pertenecer a la CKC de un ataque informático. Consulta **Gestión de Hunting rules** en la página **85**
- **Reglas de eliminación**: gestiona las reglas que eliminan automáticamente los indicios considerados no útiles para el analista. Consulta **Eliminar indicios de forma automática** en la página **77**.
- **Investigaciones automatizadas**: crea y publica notebooks que posteriormente los analistas del SOC podrán tomar como base para desarrollar sus investigaciones. Consulta **Uso de plantillas en notebooks** en la página **229**.
- **Respuestas rápidas**: crea y publica pequeños fragmentos de código reutilizables para que los analistas del SOC puedan combinarlos para acelerar el desarrollo de investigaciones. Consulta **Uso de Respuestas rápidas en notebooks** en la página **232**.
- **Plantillas de grafos**: crea y publica diagramas de grafos que posteriormente los analistas del SOC podrán tomar como base para desarrollar sus investigaciones. Consulta **Uso de plantillas en notebooks** en la página **229**
- **Mis preferencias**:
    - **Notificarme cada vez que me asignen una investigación**: Cytomic Orion envía un correo electrónico al usuario de la consola que recibió la asignación de una investigación. Por defecto esta opción está desactivada.
    - **Enviarme por correo electrónico las notificaciones sobre nuevas versiones, comunicaciones de Cytomic, etc.**
    - **Notificarme por correo electrónico cuando los datos consumidos en consultas se aproximen a la cuota máxima**: consulta **Dashboard Datos asignados** en la página

151.

- **Tema**: cambia la apariencia de la consola.
- **Zona horaria predeterminada**: establece la zona horaria de los eventos mostrados en la consola. Internamente, todos los eventos monitorizados y gestionados en Cytomic Orion están referidos a la zona horaria UTC+0. Dado que es posible que un SOC investigue a equipos que pertenecen a otras zonas horarias, el analista puede establecer una zona horaria alternativa por defecto para toda la consola. Una vez seleccionada, los datos de tipo fecha mostrados en la consola se ajustarán a la zona horaria elegida, y los datos de tipo fecha introducidos por el analista se traducirán internamente a UTC+0 según la zona horaria establecida. Además, a lo largo de la consola se pueden seleccionar distintos husos horarios en cada listado o cuadro de texto de tipo fecha para trabajar con diferentes zonas horarias simultáneamente.

- **Registro de actividad**: almacena las operaciones realizadas por las cuentas de usuario del SOC. Consulta **Registro de actividad de las cuentas de usuario** en la página **65**.

Zona Gestión del producto

Muestra un menú desplegable con las siguientes entradas de configuración:

Entrada	Descripción
Ayuda online	Acceso a las ayudas del producto.
Guía de uso de Orion	Acceso a la guía de uso.
Acuerdo de licencia	EULA (End User License Agreement).
Idioma	Cambia el idioma de la consola.
Acerca de Cytomic Orion	Muestra información de la versión.

Tabla 3.1: Menú Gestión del producto

Zona Cuenta de usuario

Muestra un menú desplegable con las siguientes entradas de configuración:

Entrada	Descripción
Configurar mi perfil	Modifica la información de la cuenta utilizada.
Cambiar de	Lista las cuentas accesibles por el administrador y permite seleccionar una

Entrada	Descripción
cuenta	para operar con la consola.
Cerrar sesión	Finaliza la sesión en la consola y devuelve el control a la pantalla de IdP.

Tabla 3.2: Menú Cuenta de usuario

Panel lateral izquierdo (2)

Contiene herramientas de filtrado que facilitan la localización de información mostrada en el panel central. El panel izquierdo varía dependiendo del área elegida en el menú superior.

En los casos en los que el panel central contenga mucha información y se quiera ganar espacio, es posible ocultar el panel de la izquierda haciendo clic en el icono «.

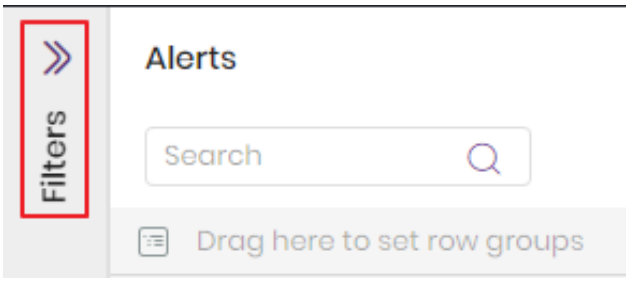


Figura 3.2: Panel oculto

Un panel replegado tiene el aspecto mostrado en la figura **Panel oculto**. Para volver a mostrarlo haz clic en el icono ».

Panel lateral derecho (3)

Contiene información extendida sobre los elementos seleccionados en el panel central. Al igual que el panel izquierdo, es posible ocultar y mostrar el panel derecho haciendo clic en los iconos « y ».

Panel central (4)

Recoge toda la información relevante de la zona o área elegida por el analista. En la figura **Vista general de la consola de análisis** se muestra la consola de investigación de equipos. Consulta **Análisis de indicios con la consola de investigación** en la página **186** para obtener más información sobre este recurso.

En los paneles que contienen registros con un elevado número de campos puede expandirse la información mostrada por defecto seleccionando un registro. Al hacerlo, se desplegará un

subpanel deslizante con la información completa y un icono situado en la esquina superior derecha para replegarlo nuevamente.

Elementos básicos de la consola de análisis

La consola web utiliza varios recursos comunes para permitir la interacción del analista con el servicio. A continuación, se muestra una lista de los controles y su modo de uso.

Menú de pestañas

Se trata de una barra de menú que selecciona el contenido mostrado en el panel central y sirve para mostrar los distintos módulos accesibles.

Dependiendo de la zona elegida, el menú de pestañas puede ser modificable y retiene su configuración para que el analista pueda continuar su tarea en el punto donde lo dejó.

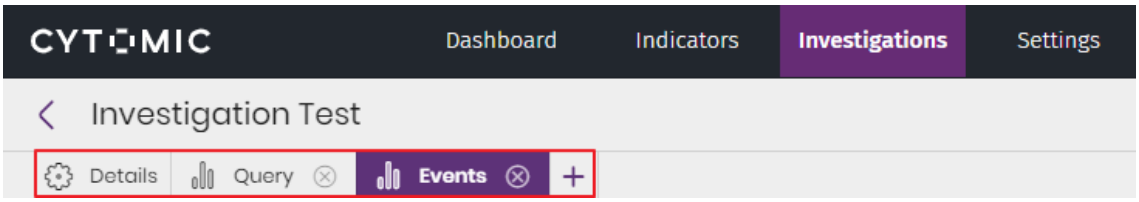


Figura 3.3: Menú de pestañas configurable

- Para seleccionar uno de los módulos disponibles haz clic en su nombre.
- Para crear una nueva entrada del menú de pestañas haz clic en el icono
- Para borrar una entrada del menú de pestañas pasa el puntero del ratón por encima de la entrada a borrar y haz clic en el icono . El módulo y toda su configuración serán eliminados.

Otros menús de pestañas no son configurables y presentan el aspecto mostrado en la figura **Menú de pestañas fijo**

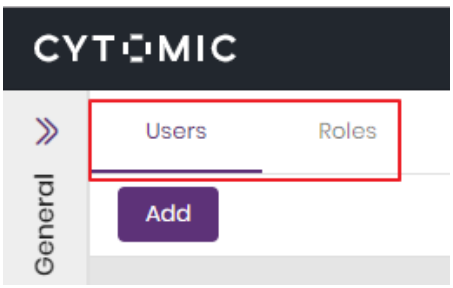


Figura 3.4: Menú de pestañas fijo

Sub paneles

Cuando el panel central presenta información de diferentes tipos, la ventana se divide en subpaneles.

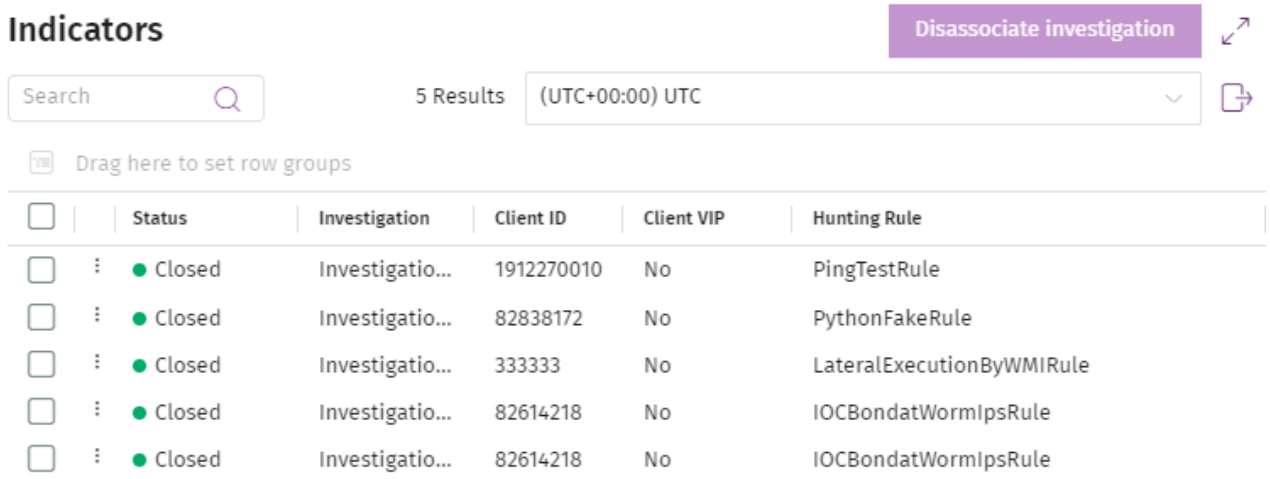


Figura 3.5: Subpanel de indicios en una investigación

Los subpaneles se pueden expandir para abarcar toda la pantalla si la cantidad de datos mostrados es grande:

- Para expandir subpanel haz clic en el botón ↙↗.
- Para contraer un subpanel haz clic en el botón ↗↙.

Algunos subpaneles tienen sus propias herramientas de búsqueda y filtrado, que solo afectan a los datos mostrados en el subpanel asociado. Consulta **Herramientas de búsqueda**.

Herramientas para configurar los listados

Los listados en Cytomic Orion son totalmente configurables para facilitar al analista la lectura de los datos presentados. A continuación se describen las herramientas disponibles para configurar los listados. La mayor parte de las herramientas de configuración se acceden mediante el menú de contexto ≡ que se muestra al pasar el puntero del ratón por encima de la cabecera de la columna.

Seleccionar todos los elementos de un listado

Haz clic en la casilla ☐ situada en la cabecera del listado para seleccionar tanto los elementos visibles como los no visibles.

Las casillas de selección admiten varios estados:

Icono	Descripción
☐	Elemento no seleccionado.

Icono	Descripción
	Elemento seleccionado.
	Todos los elementos de la lista o grupo están seleccionados.
	Algunos (no todos) los elementos de la lista o grupo están seleccionados.

Tabla 3.3: Estados de las casillas de selección

Ordenar columnas

Para cambiar el orden de las columnas del listado haz clic en el nombre de la columna a mover y, sin soltar el botón del ratón, arrástrala hasta la nueva posición.

Agregar y quitar columnas

Para mostrar u ocultar columnas de un listado sigue los pasos indicados a continuación:

- Haz clic en el icono de contexto de cualquier columna. Se mostrará un menú desplegable con varias pestañas.
- Haz clic en la pestaña del menú desplegable y selecciona las columnas que se mostrarán en el listado.
- Para localizar de forma rápida una columna dentro del menú desplegable utiliza la caja de texto **Filtrar**. El listado de columnas disponibles se actualizará de forma automática.
- Una vez seleccionadas las columnas haz clic en una zona de pantalla. El listado se actualizará de forma automática con la nueva configuración de columnas.

Agrupar registros por columnas

En la parte superior del listado se muestra la barra de agrupaciones **(1)**  . Se trata de un control de tipo recipiente donde el analista puede arrastrar las columnas que formarán el criterio de agrupación.

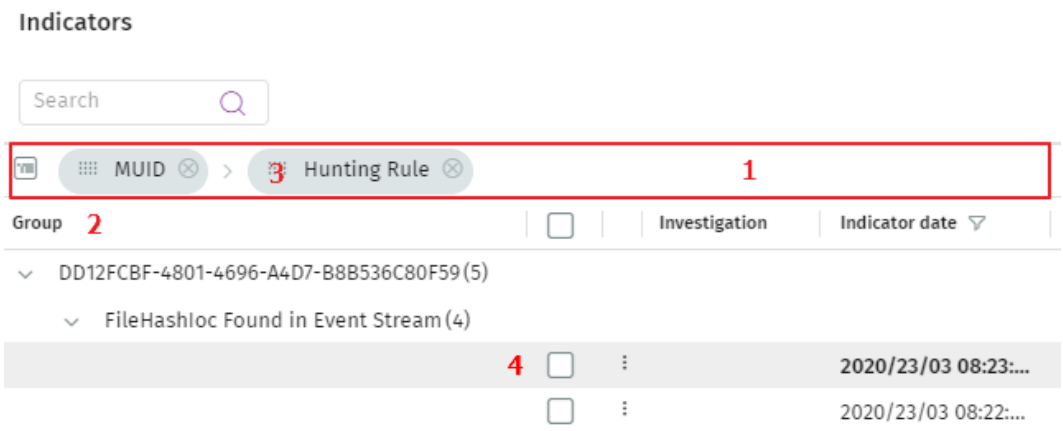


Figura 3.6: Listado agrupado por las columnas MUID y Hunting Rule

Para agrupar los resultados de un listado por una columna, arrastra el nombre de la columna al control de agrupación **(1)**,o sigue los pasos mostrados a continuación:

- Haz clic en el icono de contexto ≡ de cualquier columna. Se mostrará un menú desplegable con varias pestañas.
- Haz clic en la pestaña ≡ del menú desplegable y selecciona la opción **Group by (nombre de la columna)**

Una vez establecida la nueva agrupación el listado se actualizará con cambios mostrados a continuación:

- Se crea una columna en la parte izquierda del listado con el nombre "**group**". Esta columna mostrará el contenido de las agrupaciones **(2)**.
- Las columnas seleccionadas como criterios de agrupación se muestran en la barra de agrupación en el orden en que se agregaron **(3)**.
- Se añaden los iconos ⌄ y › para desplegar o contraer un grupo de resultados.
- Para borrar una agrupación haz clic en el icono ⊗ de la agrupación a borrar en la barra de agrupación.
- Si el criterio de agrupación está formado por más de una columna se respeta el orden elegido: se agrupará el listado por la columna elegida en primer lugar y, dentro de cada grupo de filas resultante se volverá a agrupar por la segunda columna, y así sucesivamente.
- Para cambiar el orden de aparición de la agrupación haz clic en su nombre y arrástrala a derecha o izquierda dentro de la barra de agrupaciones.
- Para cambiar el orden las agrupaciones según el número de elementos que contienen haz clic en el nombre de la columna **Group**.

Seleccionar todos los elementos de un grupo

Para seleccionar todos los elementos que pertenecen a un grupo haz clic en la casilla de selección **(4)** asociada al grupo.

No es posible seleccionar varios grupos de un mismo nivel simultáneamente. Al seleccionar un grupo, la consola retirará el resto de selecciones.

Fijar columnas

En los listados donde hay un gran número de columnas es necesario manejar la barra de desplazamiento horizontal para visualizar aquellas columnas que no entran en la ventana. Para dejar columnas fijas utiliza la función de **Fijar columna**:

- Haz clic en el icono de contexto ≡ de cualquier columna. Se mostrará un menú desplegable con varias pestañas.
- Haz clic en la pestaña ≡ del menú desplegable
- Selecciona la opción **Fijar columna** y elige el lugar donde se colocará la columna: a la izquierda del listado << o a la derecha >>
- Para dejar de fijar una columna previamente fijada elige la opción **No fijar** <>.

Redimensionar columnas

Para cambiar el ancho de una columna haz clic en el icono separador situado entre los nombres de las columnas y arrástralo a derecha o izquierda.

Redimensionar columnas según su contenido

Para ajustar el ancho de una columna a su contenido sigue los pasos mostrados a continuación:

- Haz clic en el icono de contexto ≡ de cualquier columna. Se mostrará un menú desplegable con varias pestañas.
- Haz clic en la pestaña ≡ del menú desplegable y selecciona la opción **Redimensionar columna**.
- Para ajustar el ancho de todas las columnas haz clic en **Redimensionar todas**.

Filtrado de información a nivel de columna

Para filtrar las filas del listado según el contenido de una celda concreta sigue los pasos mostrados a continuación:

- Haz clic en el icono de contexto ≡ de cualquier columna. Se mostrará un menú desplegable con varias pestañas.
- Haz clic en la pestaña ▽ del menú desplegable y elige un criterio de filtrado disponible.

Dependiendo del tipo de dato que almacene la columna se ofrecen distintos criterios de filtrado:

- **Para columnas de tipo fecha**: introduce las dos fechas para mostrar el rango de registros que se encuentre dentro del intervalo establecido, o introduce una única fecha para

mostrar los registros que pertenecen a esa fecha concreta.

- **Para columnas de tipo texto**: escribe el texto que actuará como filtro y la lógica de filtrado: **igual - no igual** para concordancias exactas, **contiene - no contiene** para concordancias parciales en cualquier punto de la cadena de caracteres y **empieza por - termina por** para concordancias al principio o al final de la cadena de caracteres.
- **Para columnas de tipo enumeración**: selecciona los elementos de la enumeración que actuarán como filtro.

Restaurar la configuración de las columnas

- Haz clic en el icono de contexto ≡ de cualquier columna. Se mostrará un menú desplegable con varias pestañas.
- Haz clic en la pestaña ≡ del menú desplegable y selecciona la opción **Resetear columnas.**

Mostrar y ocultar columnas y filtros

Los listados incorporan una barra lateral con dos accesos directos que permiten:

- Visualizar u ocultar de forma rápida las columnas y filtros del listado.
- Ordenar de forma rápida las columnas del listado.
- Mostrar las columnas en el caso de que previamente se hayan ocultado todas por error.

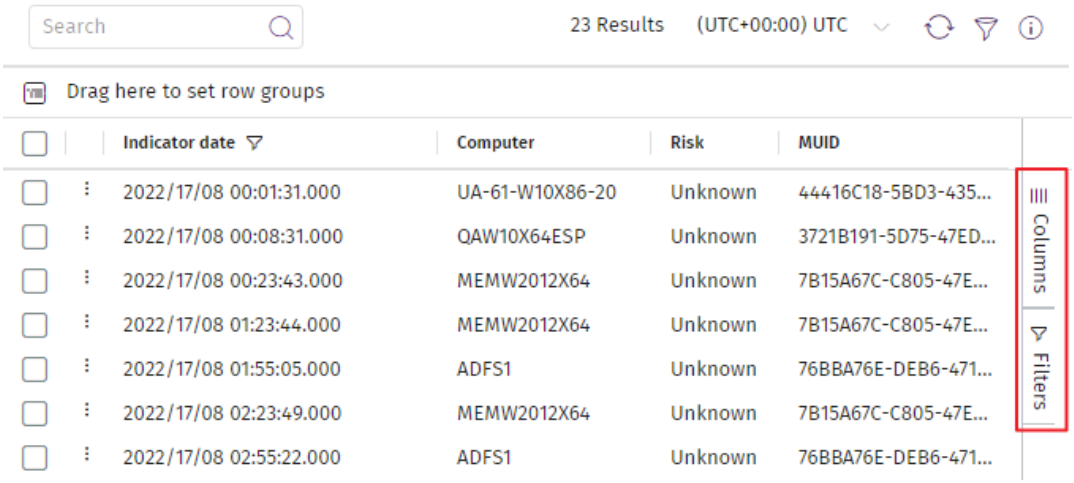


Figura 3.7: Barra de accesos directos a las columnas y filtros del listado

Herramientas de búsqueda

Las herramientas de búsqueda muestran los registros de información más interesantes para el analista. Para efectuar una búsqueda global sobre un listado, escribe la cadena de caracteres a buscar en la caja de texto y haz clic en el icono 🔍.

A diferencia de **Herramientas para configurar los listados** donde se aplicaban filtros en columnas concretas, en este apartado se describen las herramientas de búsqueda que aplican a todas las columnas de su listado asociado.

Se establecen las siguientes características comunes a las herramientas de búsqueda:

- Se admiten búsquedas parciales al comienzo, final o en el interior de una cadena de texto.
- La búsqueda se extiende a todas las columnas del listado.
- La búsqueda se aplicará sobre el listado del panel o subpanel asociado. En la figura **Controles de búsqueda asociados al listado de su panel** se muestran dos controles de búsqueda (**1**, **2** y **3**) asociados a sus respectivos paneles (**1**, **2** y **3**).

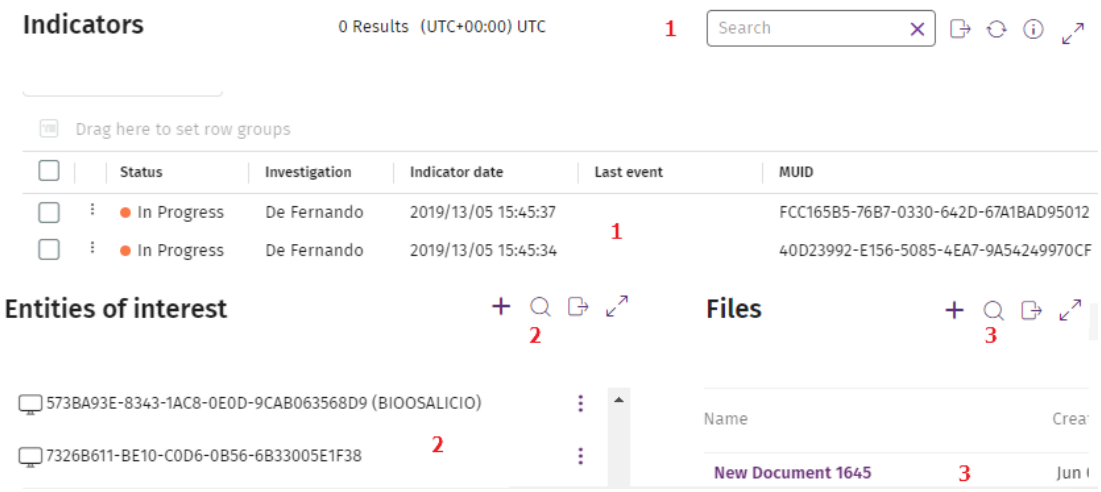


Figura 3.8: Controles de búsqueda asociados al listado de su panel

Herramientas de filtrado

Son controles que permiten hacer un selección de valores que se aplica como filtro al listado. Aparecen en el panel izquierdo en algunas de las zonas de la consola. Dependiendo de la zona de la consola y de los listados que incluya se mostrarán unos filtros u otros.

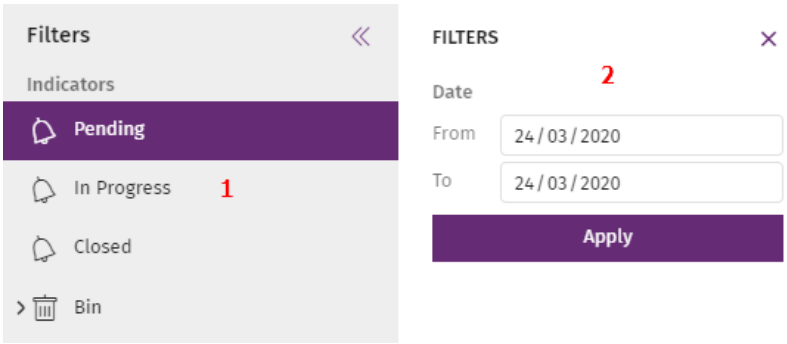


Figura 3.9: Controles de filtrado

Los tipos de herramienta de filtrado más frecuentes son:

- **Filtros de estado (1)**: filtran por un estado concreto de entre todos los disponibles.
- **Filtros por rango de fechas (2)**: filtran por un intervalo temporal.

Menús de contexto

Despliegan grupos de opciones que agilizan el trabajo del analista. Algunos menús de contexto están representados mediante el icono ⋮ pero otros solo se muestran haciendo clic con el botón de la derecha del ratón sobre un elemento de la consola. Por ejemplo, en los listados de indicios dentro de una investigación, al hacer clic con el botón de la derecha sobre una alerta se muestra la posibilidad de abrir la consola de investigación con el identificador del equipo y la fecha que aparece en el registro de la alerta.

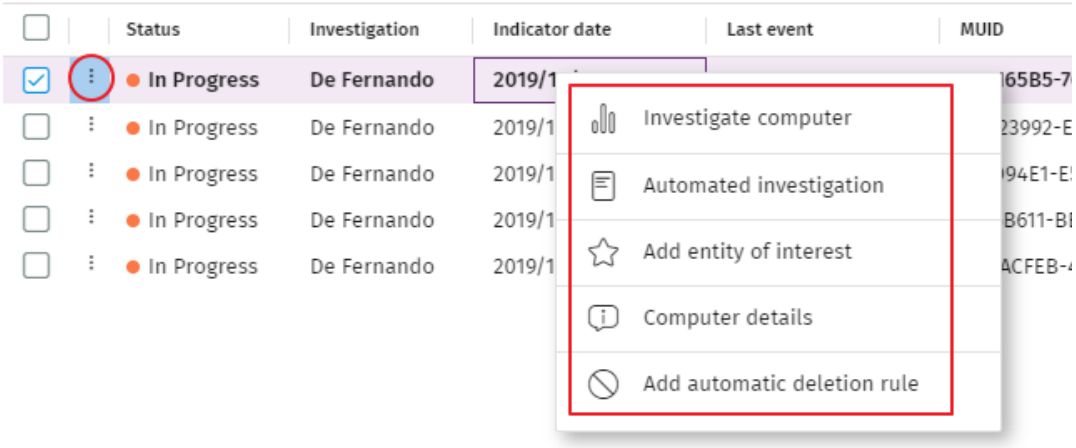


Figura 3.10: Menú de contexto del área Investigaciones e icono

Herramienta de conversión de nombres de equipo a MUID

Cytomic Orion identifica a los equipos de los clientes de forma única mediante una cadena de caracteres formada por grupos de letras y números separados por guión. De esta forma es posible referenciar equipos sin ambigüedad, ya que un nombre de equipo concreto puede ser utilizado por varios clientes gestionados por un mismo SOC. Para facilitar la manipulación de equipos y evitar memorizar MUIDs, Cytomic Orion ofrece una herramienta de conversión que traduce el nombre del equipo (más fácil de recordar por el analista) a su MUID correspondiente. Esta herramienta se invoca a través del icono 🔍 en las cajas de texto donde se requiera la introducción de un MUID. El funcionamiento de la herramienta de traducción es el siguiente:

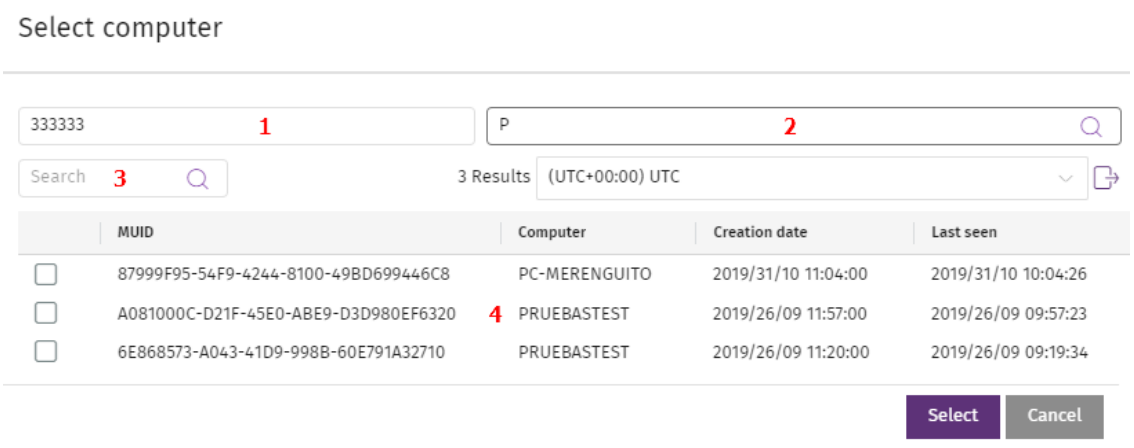


Figura 3.11: Herramienta de conversión de nombre de equipo a MUID

- Escribe en la caja de texto **Cliente (1)** el cliente del SOC al que pertenece el equipo.
- Escribe algún carácter del nombre del equipo en la caja de texto **Buscar equipo (2)**. Automáticamente se rellenará la caja de texto **(4)** con los equipos que contienen los caracteres indicados.
- Para filtrar los resultados utiliza la caja de texto de búsqueda **(3)**.
- Selecciona el equipo buscado y haz clic en **Seleccionar**. El MUID del equipo se copiará en la caja de texto que invocó la herramienta de conversión de nombres.

Cajas de texto multivalor

Algunas cajas de texto admiten listas de valores que el analista puede introducir de forma manual, o pegando desde el porta papeles:

- **Desde el porta papeles**: pulsa `control + v` para volcar el contenido del porta papeles. Es necesario que los valores de la lista estén separados por el carácter "," para que la consola pueda interpretarlos como elementos independientes.
- **Con el icono ⊕ asociado a la caja de texto**: al hacer clic en el icono se abre una ventana emergente de donde el analista selecciona los elementos a añadir.

Otros controles

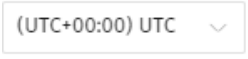
Icono	Descripción
	Agrega un elemento.
	Elimina un elemento
	Cambia el estado (activado o desactivado) de un elemento
	Recarga el contenido del panel asociado.
	Exporta los resultados mostrados en el panel asociado en formato csv.
	Establece la zona horaria. En los listados de elementos ajusta los datos de tipo fecha a la zona horaria elegida. En las cajas de texto permite establecer una zona horaria para las búsquedas.

Tabla 3.4: Otros controles utilizados en la consola de análisis

Capítulo 4

Acceso, control y supervisión de la consola de análisis

Cytomic EDR implementa varios recursos diseñados para limitar, controlar y supervisar el acceso a su consola web, y las acciones que el analista tiene permitido ejecutar en ésta:

- Cuenta de usuario.
- Roles asignados a las cuentas de usuario.
- Registro de la actividad de las cuentas de usuario.

CONTENIDO DEL CAPÍTULO

Conceptos generales

Cuenta de usuario

Es un recurso formado por un conjunto de datos que Cytomic Orion utiliza para permitir el acceso de los analistas a la consola web, y establecer las acciones que éstos podrán realizar sobre los equipos de los usuarios.

Las cuentas de usuario son utilizadas únicamente por los analistas del SOC que acceden a la consola web de Cytomic Orion. Cada analista puede tener una o más cuentas de usuario asignadas.

Las principales características de las cuentas de usuario son:

- Son cuentas gestionadas por el propio analista, que puede crear o borrar cuentas nuevas, cambiar su contraseña, añadir o quitar permisos o activar la verificación en dos pasos.
- Una cuenta de usuario permite acceder a todos los productos contratados con Cytomic a través de Cytomic Central
- Una cuenta de usuario puede tener acceso a distintos clientes. El analista podrá elegir el producto al que desea acceder en Cytomic Central, y después seleccionar la consola a la que desee acceder en la ventana **Selecciona cuenta**.

Cytomic Central

Es el portal que centraliza el acceso a todos los productos del portfolio de Cytomic. Una cuenta de usuario creada en un producto de Cytomic da acceso a este portal, desde donde el analista puede acceder a la distintas consolas de los productos contratados.

Para más información, consulta ***http://nexus-documents.cytomic.ai/AdvancedGuide/NEXUS-Manual-ES.pdf***

Cuenta de cliente SOC / MSSP

Es un recurso formado por datos confidenciales asociados al SOC / MSSP que tiene contratado algún producto con Cytomic. La dirección fiscal, el nombre completo, NIF y otros datos forman parte de la cuenta del SOC / MSSP.

Gestión de cuentas de usuario

Una cuenta de usuario está formada por varias piezas de información que se generan en el momento de su creación:

- **Login de la cuenta**: identifica al usuario que accede a la consola.
- **Contraseña de la cuenta**: permite o impide el acceso a la consola de análisis.

- **Rol asignado**: establece los equipos sobre los cuales la cuenta tiene capacidad de administración, y las acciones que puede ejecutar sobre ellos.
- **Cliente**: establece la visibilidad del analista sobre los equipos de usuario y servidores administrados por el MSSP / SOC.

Crear la primera cuenta de usuario

El procedimiento para crear la primera cuenta de usuario es distinto al utilizado para crear cuentas posteriores. La primera cuenta de usuario siempre tendrá asignado el rol Control total, que permite al analista realizar cualquier operación en la consola. Esta cuenta no se puede borrar ni modificar.

Recibe el mensaje de correo de bienvenida

- Al adquirir Cytomic Orion recibirás un mensaje de correo electrónico procedente de Cytomic.
- Haz clic en el enlace **Haz clic aquí** del mensaje para acceder a la web desde donde podrás crear la primera cuenta de usuario.

Completa el formulario Crea tu cuenta Cytomic

- Escribe tu dirección de email y haz clic en el botón **Crear**. Recibirás un nuevo mensaje de correo electrónico en la dirección especificada en el formulario para activar la cuenta creada.

Activa la cuenta de usuario

- Haz clic en el botón de activación del mensaje recibido para confirmar la dirección proporcionada al crear la cuenta de usuario. Si el botón no funciona, copia en el navegador el enlace que se muestra en el mensaje. Se abrirá la ventana **Cytomic Cuenta**.
- Escribe la contraseña de la cuenta de usuario creada. Se requieren al menos 8 caracteres, de los cuales al menos uno debe ser numérico y otro debe ser una letra.
- Elige el país y haz clic en el botón **Activar cuenta**. Se mostrará la ventana **Un segundo y terminamos**.
- Escribe tu nombre y apellidos, tu fecha de nacimiento, número de teléfono y dirección y haz clic en el botón **Guardar**, o salta este paso haciendo clic en el botón **Ahora no**. Se mostrará el acuerdo de licencia de Cytomic Central.
- Haz clic en el botón **Aceptar y continuar**. Se abrirá la ventana Cytomic Central, desde donde podrás acceder a todos los servicios contratados con Cytomic.

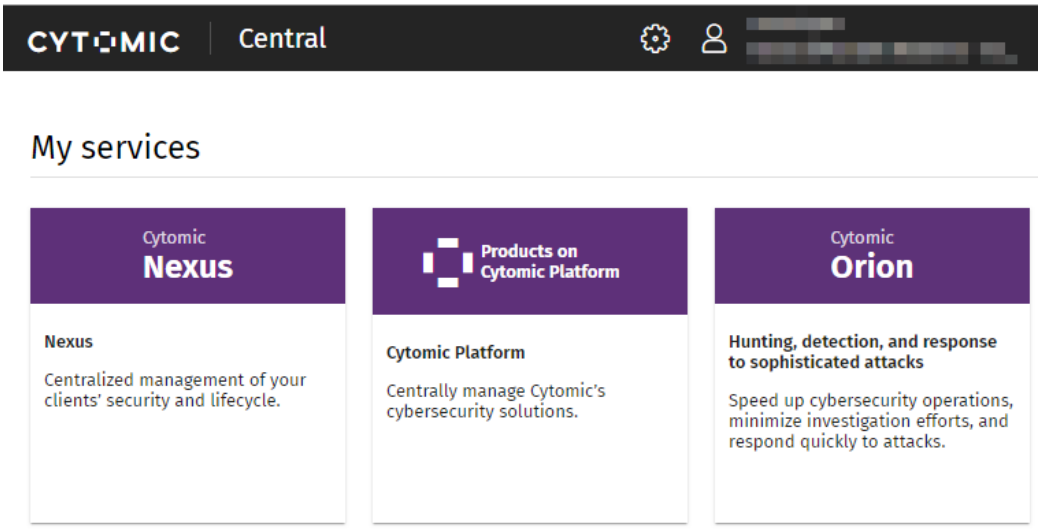


Figura 4.1: Ventana Cytomic Central

- Para acceder a la consola de Cytomic Orion, haz clic en el panel Cytomic Orion que encontrarás en **Mis servicios**. La primera vez que accedas se abrirá un asistente para aceptar los acuerdos de licencia y confidencialidad:
  - Haz clic en el botón **Aceptar y continuar** de la ventana **Acuerdo de licencia**.
  - Haz clic en el botón **Ir al acuerdo sobre tratamiento de datos** de la ventana **Acuerdo sobre tratamiento de datos**.
  - Haz clic en el botón **Aceptar** de la ventana **Data Processing Agreement**. Se abrirá la consola Cytomic Orion.

Crear cuentas de usuario sucesivas

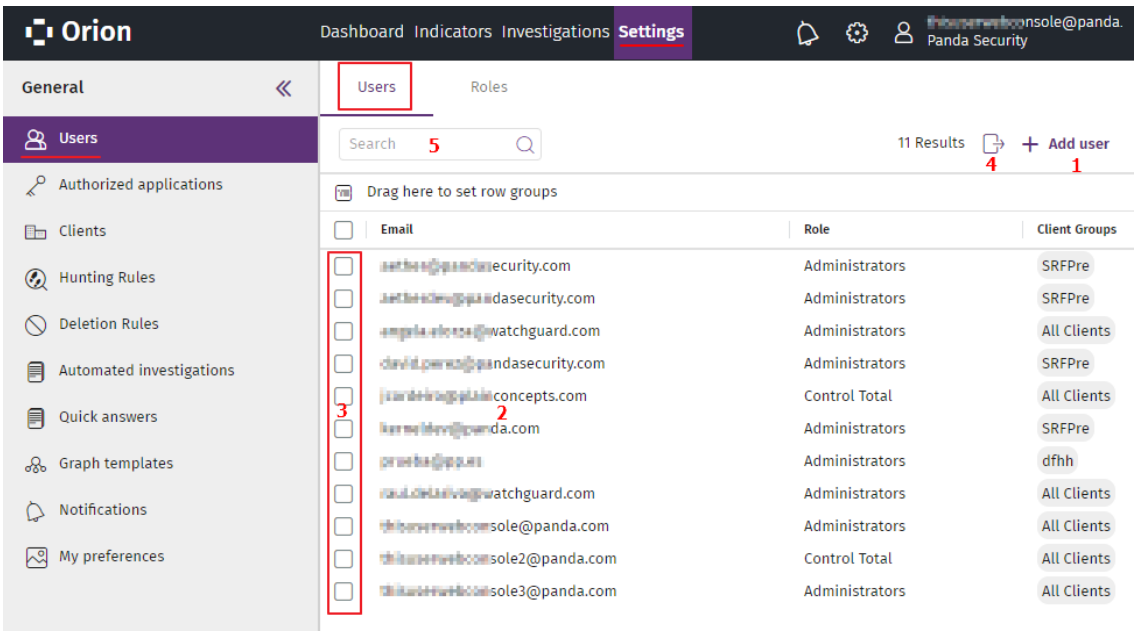


Figura 4.2: Listado de usuarios

Una vez creada la primera cuenta de usuario, el analista tendrá acceso a la consola de Cytomic Orion, desde donde se pueden crear el resto de cuenta de usuario que necesite.

- Comprueba que el usuario tiene asignado el permiso **Gestión de usuarios, permisos y clientes**. Consulta **Descripción de los permisos implementados**.
- En el menú superior **Configuración** haz clic en el menú lateral **Usuarios**.
- Haz clic en la pestaña **Usuarios**. Se mostrará el listado de usuarios creados en la consola de administración.
- Haz clic en el botón **Añadir usuario (1)**. Se abrirá la ventana **Añadir usuario**.
- Escribe la cuenta de correo del usuario de la consola en el campo **Email de acceso** y la descripción si es necesaria.
- Indica el rol que tendrá asignada la cuenta de usuario. Consulta **Descripción de los permisos implementados**.
- Para indicar la visibilidad de los clientes que tendrá la cuenta del usuario:
  - Haz clic en el icono  , en el campo **Clientes sobre los que tiene permiso el usuario**. Se abrirá la ventana **Selecciona grupos de clientes**.
  - Haz clic en las casillas de selección para añadir los grupos de clientes a los que el analista tendrá acceso.
  - Haz clic en el botón **Aceptar**.

*Para obtener mas información acerca de la visibilidad de la cuenta de usuario consulta **Configuración de la visibilidad de clientes***

- Haz clic en el botón **Guardar**. Cytomic Orion enviará un correo a la cuenta de correo indicada para que el usuario pueda generar una contraseña de acceso y aceptar los términos de la licencia y el tratamiento de sus datos.

Para los MSSP / SOC que tienen varios productos de Cytomic contratados, si la cuenta de correo ya existía en los sistemas de Cytomic no se enviará el correo de activación. La cuenta podrá acceder a Cytomic Orion con las credenciales utilizadas en otros productos.

Cambiar los datos personales de una cuenta de usuario

- Haz clic en el icono  situado en la parte superior derecha de la consola de administración. Se abrirá un menú desplegable.
- Haz clic en **Configurar mi perfil**.

Cytomic Central

- Se abrirá la ventana **Cytomic cuenta**.
- Haz clic en el panel izquierdo **Información personal** y escribe en el formulario los datos personales de la cuenta.
- Haz clic en el botón **Guardar**. Los cambios se almacenarán en el servidor de Cytomic.

Cambiar la dirección de correo o la contraseña de una cuenta de usuario

- Haz clic en el icono  situado en la parte superior derecha de la consola de administración. Se abrirá un menú desplegable.
- Haz clic en **Configurar mi perfil**.

Cytomic Central

- Se abrirá la ventana **Cytomic cuenta**.
- Haz clic en el panel izquierdo **Inicio de sesión** y en los enlaces **Cambiar dirección de email** o **Cambiar contraseña**. Se abrirá una ventana para validar la información antigua e introducir la nueva.
- Haz clic en el botón **Cambiar**.

Acceso al listado de usuarios

- En el menú superior **Configuración** haz clic en el panel de la izquierda **Usuarios**.
- Haz clic en la pestaña **Usuarios**. Se mostrará un listado con todas las cuentas de usuario creadas en Cytomic Orion con la información mostrada a continuación:

Campo	Descripción
Email	Dirección de correo electrónico asociada al usuario.
Rol	Grupo de permisos asociados a la cuenta de usuario.

Campo	Descripción
Grupos de clientes	Grupo de clientes sobre los cuales la cuenta tiene visibilidad

Tabla 4.1: Campos del listado Usuarios

Borrar cuentas de usuarios

- Comprueba que el usuario tiene asignado el permiso **Gestión de usuarios, permisos y clientes**. Consulta **Descripción de los permisos implementados**.
- En el menú superior **Configuración** haz clic en el menú lateral **Usuarios.**
- Haz clic en la pestaña **Usuarios**. Se mostrará el listado de usuarios creados en la consola de análisis.
- Haz clic en las casillas de selección **(3)** asociadas a los usuarios que quieres eliminar.
- Haz clic en el icono situado en la barra de herramientas. Se abrirá una ventana de confirmación.
- Haz clic en el botón **Aceptar**. Los usuarios borrados no podrán acceder a la consola web ni a la librería de threat hunting, ni recibirán notificaciones por correo. Sin embargo, las investigaciones, notebooks e información de auditoria generada por el usuario permanecerán en el sistema. Los usuarios borrados pueden seguir siendo utilizados en los filtros de investigaciones siempre que hayan creado alguna o tengan investigaciones asignadas.

Reactivar un usuario

Un usuario borrado puede ser nuevamente dado de alta siguiendo el procedimiento normal para crear usuarios. En este caso, toda la información que generó volverá a ser asignada a su cuenta.

Exportar el listado de usuarios

Para descargar el listado de usuarios en un fichero excel, haz clic en el icono **(4)** situado en la parte superior derecha de la ventana.

Buscar usuarios

Escribe en la caja de texto **(5)** la cadena a buscar dentro de cualquiera de los campos del listado. Se admiten subcadenas de búsqueda.

Activar la verificación en dos pasos

Cytomic Orion es compatible con el estándar 2FA (Two Factor Authentication), que añade una capa de seguridad adicional a la establecida en el esquema básico "usuario - contraseña". De esta manera, cuando el analista accede a la consola web, se introduce un elemento nuevo en el

sistema de autenticación básico: un código que solo posee el propietario de la cuenta. Este código es aleatorio y solo puede generase en un dispositivo concreto, normalmente el teléfono móvil o tablet personal del administrador de Cytomic Orion.

Requisitos para activar 2FA

- Acceso a un teléfono móvil o tablet personal con cámara de fotos integrada.
- Descarga la aplicación gratuita WatchGuard AuthPoint (o una aplicación equivalente) en:
  - **iOS**: **https://apps.apple.com/app/watchguard-authpoint/id1335115425**
  - **Android** : **https://play.google.com/store/apps/details?id=com.watchguard.authpoint**

Activar 2FA

- Haz clic en el icono situado en la parte superior derecha de la consola de análisis. Se abrirá un menú desplegable.
- Haz clic en **Configurar mi perfil**.

Cytomic Central

- Se abrirá la ventana **Cytomic cuenta**.
- Haz clic en el panel izquierdo **Inicio de sesión** y en el enlace **Activar** de la sección **Verificación en dos pasos**. Se abrirá la ventana **Sincronización con la app de autenticación**.
- Si es la primera vez que utilizas la aplicación WatchGuard AuthPoint en tu dispositivo móvil, pulsa el botón **Activar**. Si ya la has utilizado anteriormente, pulsa en el icono del QR situado en la esquina superior derecha. Se abrirá la cámara de fotos del dispositivo móvil.

Figura 4.3: Escaneo del código QR con WatchGuard Authpoint

- Enfoca con la cámara el código QR que se muestra en la consola de Cytomic Orion. Se añadirá una nueva entrada en WatchGuard AuthPoint y se empezarán a generar tokens cada 30 segundos.
- Escribe el código generado por WatchGuard AuthPoint en la consola de Cytomic Orion para enlazar el dispositivo con la cuenta de usuario, y haz clic en el botón **Verificar**. Se abrirá una ventana con el mensaje **Se ha activado la verificación en dos pasos**.
- Haz clic en el botón **Aceptar**.

Acceder a la consola web mediante una cuenta con 2FA activado desde Cytomic Central

- Accede a **https://central.cytomic.ai/Login** escribe el usuario y la contraseña y haz clic en el botón **Iniciar sesión**.
- Introduce el código de verificación generado por WatchGuard AuthPoint en tu dispositivo móvil y haz clic en el botón **Verificar**. Se abrirá la ventana **Cytomic Central**.

Forzar la activación de 2FA a todos los usuarios de la consola

Es necesario que la cuenta de usuario que forzará el uso de 2FA tenga el permiso **Gestión de usuarios, permisos y clientes** y visibilidad completa sobre el parque informático. Consulta **Descripción de los permisos implementados**

- En el menú superior **Configuración** haz clic en el panel lateral **Usuarios** y en la pestaña **Seguridad**.
- Activa la opción **Exigir tener activada la verificación en dos pasos para acceder a esta cuenta**.
- Si la cuenta de usuario que activa la funcionalidad 2FA para todos los usuarios de la consola no tiene activada la verificación en dos pasos para su propia cuenta, se mostrará una ventana de aviso que le permitirá acceder a la **Cuenta Cytomic** para activarlo. Consulta **Activar 2FA**.

Configuración de la visibilidad de clientes

Para distribuir el trabajo según su prioridad o volumen dentro del SOC, las cuentas de usuario creadas pueden tener limitado el acceso a determinados clientes, y así segmentar y asignar las investigaciones a grupos determinados de threat hunters. Un analista sin acceso a un cliente no podrá realizar ninguna tarea de análisis sobre ese cliente.

Acceso a la configuración de visibilidad de clientes

Accede a la configuración de visibilidad en el menú superior **Configuración**, panel lateral izquierdo **Clientes**.

Creación de un grupo nuevo y asignación de clientes

La configuración de visibilidad se realiza mediante grupos de clientes. El administrador del SOC tendrá que crear tantos grupos de clientes como combinaciones de acceso sean necesarias para los analistas. De esta forma, si un conjunto de analistas necesita acceso a los clientes 1, 2 y 4, y otro conjunto de analistas necesita acceso a los clientes 2, 3 y 4, será necesario crear 2 grupos de acceso distintos y asignar un grupo u otro a la cuenta de usuario de cada analista.

Una cuenta de usuario puede tener varios grupos de clientes asignados. Los clientes accesibles serán la suma de todos los clientes que pertenecen a los grupos asignados a la cuenta de usuario.

Para visualizar los grupos creados y sus clientes asignados

- Accede a la configuración de visibilidad en el menú superior **Configuración**, panel lateral izquierdo **Clientes**.
- En el panel **Grupos** se mostrará un listado de los grupos ya creados junto al número de clientes que contiene.
- Adicionalmente, se mostrará el grupo especial **Todos los clientes**, utilizado para la gestión de grupos mostrada más adelante en este mismo apartado.
- Para mostrar los clientes que pertenecen a un grupo haz clic en el grupo. El panel clientes se actualizará con el nombre de los clientes del grupo, el identificador único del cliente, su nombre y los grupos a los que pertenece el cliente.

Para crear un grupo nuevo y asignar clientes:

- En la parte superior de la pantalla haz clic en el icono + del panel **Grupos**.
- Escribe el nombre del grupo y haz clic en el botón **Aceptar**.

Para borrar un grupo:

- Pasa el puntero del ratón por el nombre del grupo a borrar. Se mostrará el menú de contexto.
- Haz clic en el menú de contexto y selecciona la opción **Eliminar grupo**.

Si el grupo ya ha sido asignado a una cuenta de usuario, el sistema mostrará un mensaje de error.

Para cambiar el nombre de un grupo:

- Pasa el puntero del ratón por el grupo a modificar. En el menú de contexto elige la opción **Cambiar nombre**. Se abrirá una ventana solicitando el nuevo nombre de grupo.
- Escribe el nombre nuevo del grupo y haz clic en **Aceptar**.

Para asignar clientes nuevos a un grupo ya creado:

- Haz clic en el grupo especial **Todos los clientes** del panel de grupos.
- Haz clic en el icono para desplegar la caja de texto de búsqueda y localizar los clientes de rápidamente.
- Haz clic en las casillas de selección de los clientes que formarán parte del grupo y haz clic en el botón **Asignar a un grupo** de la barra de herramientas. Los clientes seleccionados formarán parte del grupo.

Para borrar clientes de un grupo:

- Haz clic en el grupo al que pertenecen los clientes a borrar en el panel **Grupo** y selecciónalos.
- Haz clic en el botón **Eliminar** de un grupo. Se mostrará una ventana de confirmación. Haz clic en el botón **Aceptar**. Desde ese momento las cuentas de usuario que tengan asignado ese grupo no podrán acceder al cliente borrado a no ser que el cliente pertenezca a otro grupo también asignado a la cuenta del usuario.

Para asignar un grupo de clientes a una cuenta de usuario

- Accede al menú superior **Configuración**, panel lateral izquierdo **Usuarios** y haz clic en la pestaña **Usuarios**. Se mostrará un listado de los usuarios ya creados en Cytomic Orion.
- Haz clic en un usuario y en el icono situado en el apartado **Clientes sobre los que tiene permiso el usuario**. Se mostrará una ventana con todos los grupos creados.
- Elige los grupos a los que tendrá acceso la cuenta de usuario haciendo clic en las casillas de selección y haz clic en el botón **Aceptar**. Desde ese momento la cuenta de usuario tendrá acceso a los datos almacenados en Cytomic Orion correspondientes a los clientes miembros de los grupos seleccionados.

Para asignar todos los clientes que gestiona el SOC a una cuenta de usuario

- Accede al menú superior **Configuración**, panel lateral izquierdo **Usuarios** y haz clic en la pestaña **Usuarios**. Se mostrará un listado de los usuarios ya creados en Cytomic Orion.
- Haz clic en un usuario y en el icono situado en el apartado **Clientes sobre los que tiene permiso el usuario**. Se mostrará una ventana con todos los grupos creados.
- Elige el grupo especial **All clients**, que contiene de forma automática todos los clientes que administra el SOC. Desde ese momento, la cuenta de usuario tendrá acceso a todos los datos almacenados en Cytomic Orion de todos los clientes gestionados por el SOC.

Gestión de roles y permisos

Conceptos básicos

Roles

Un rol es una configuración específica de permisos que se aplica a una o más cuentas de usuario. Una cuenta de usuario estará autorizada a ver o modificar determinados recursos de la consola, dependiendo de rol que tenga asignado.

Una cuenta de usuario solo puede tener un único rol asignado, aunque un mismo rol puede estar asignado a una o más cuentas de usuario.

Un rol está formado por los siguientes elementos:

- **Nombre del rol**: designado en el momento de la creación del rol, su objetivo es meramente identificativo.
- **Visibilidad**: restringe el acceso a determinados equipos de la red.
- **Juego de permisos**: determina las acciones concretas que las cuentas de usuario pueden ejecutar sobre los equipos que pertenecen a los grupos definidos con accesibles.

¿Por qué son necesarios los roles?

En un SOC de tamaño pequeño, todos los técnicos van a acceder a la consola con el rol **Control total** sin ningún tipo de límite; sin embargo, en MSSPs / MDRs medianos o grandes con un parque informático amplio para administrar y multitud de clientes, es muy posible que sea necesario organizar o segmentar el acceso a los equipos, aplicando dos criterios:

Según la cantidad de equipos a administrar

Los MSSPs / MDRs con un parque de equipos a analizar de tamaño grande pueden necesitar dividirlo por clientes y asignarlos a analistas para repartir el trabajo y mejorar los tiempos de respuesta. Un analista concreto solo podrá investigar los equipos pertenecientes a ese grupo de clientes.

Otra opción puede contemplar la prioridad del cliente, agrupándolos según su importancia y asignándolos a equipos de trabajo de diferente dimensionamiento o habilidades.

Según los conocimientos o perfil del técnico

Los MSSPs / MDRs se dividen en capas, normalmente 3, que facilitan la distribución del trabajo de análisis para evitar los cuellos de botella. Dependiendo de las habilidades de cada analista, éste pertenecerá a un nivel u otro, y por lo tanto tendrá acceso a ciertos recursos de la consola de análisis y no a otros, siempre acorde a sus tareas y responsabilidades.

Estos dos criterios descritos se pueden solapar, dando lugar a una matriz de configuraciones flexible y fácil de establecer y mantener, que permite delimitar perfectamente las funciones de la consola para cada analista, dependiendo de la cuenta de usuario con la que acceden al sistema.

El rol Control total

Una licencia de uso de Cytomic Orion incluye un rol de **Control total** predefinido. A este rol pertenece la cuenta de usuario creada por defecto, y con ella es posible realizar absolutamente todas las acciones disponibles en la consola.

El rol **Control total** no se puede borrar, modificar ni visualizar, y cualquier cuenta de usuario puede pertenecer a este rol previa asignación en la consola de análisis.

Permiso

Un permiso regula el acceso a una sección concreta de la consola de administración. Existen varios permisos que establecen el acceso a otros tantos aspectos de la consola de Cytomic Orion. Una configuración particular de todos los permisos disponibles forma un rol, que puede ser asignado a una o más cuentas de usuario.

Visibilidad

Cada cuenta de usuario puede configurar la seguridad de un subconjunto de equipos determinado por su visibilidad, de entre todos los equipos integrados en la consola de Cytomic Orion.

Crear y configurar roles

En el menú superior **Configuración** haz clic en el panel izquierdo **Usuarios** y haz clic en la pestaña **Roles** para realizar todas las acciones necesarias relativas a la creación y modificación de roles:

Crear un rol

- En el menú superior **Configuración** haz clic en el panel de la izquierda **Usuarios.** y en la pestaña **Roles**. Se abrirá una ventana con el listado de roles creados.
- Haz clic en el botón **Añadir**. Se abrirá la ventana **Añadir rol**.
- En el campo **Nombre** escribe el nombre del rol y en el campo **Descripción** una descripción opcional.
- Activa o desactiva los permisos.
- Haz clic en el botón **Añadir**.

Limitaciones en la creación de usuarios y roles

Para evitar una situación de escalado de permisos, los usuarios con el permiso **Gestión de usuarios, permisos y clientes**activo tienen las siguientes limitaciones a la hora de crear roles o asignarlos a otros usuarios ya creados:

- Una cuenta de usuario solo puede crear roles nuevos con los mismos permisos o menos de los que tiene asignada.

- Una cuenta de usuario sólo puede editar los permisos que tenga activos en los roles ya existentes. El resto permanecerán desactivados.
- Una cuenta de usuario no puede asignar un rol a un usuario si ese rol tiene más permisos asignados que la cuenta de usuario.
- Una cuenta de usuario no puede copiar un rol si ese rol tiene más permisos asignados que la cuenta de usuario.

Borrar un rol

- En el menú superior **Configuración** haz clic en el panel de la izquierda **Usuarios.**
- Haz clic en la pestaña **Roles**. Se mostrará el listado de roles creados.
- Haz clic sobre el icono de un rol para borrarlo. Si al borrar un rol éste ya tiene cuentas de usuario asignadas, se cancela el proceso de borrado.

Copiar un rol

- En el menú superior **Configuración** haz clic en el panel de la izquierda **Usuarios.**
- Haz clic en la pestaña **Roles**. Se mostrará el listado de roles creados.
- Haz clic sobre el icono de un rol para copiarlo. Se abrirá la ventana **Copiar rol** con la configuración del rol copiado.
- Modifica la configuración del rol copiado y haz clic en el botón **Guardar**.

Modificar un rol

- En el menú superior **Configuración** haz clic en el panel de la izquierda **Usuarios**.
- Haz clic en la pestaña **Roles**. Se mostrará el listado de roles creados.
- Haz clic en el rol a editar. Se abrirá la ventana **Editar rol**.
- Modifica la configuración del rol y haz clic en el botón **Guardar**.

Descripción de los permisos implementados

Acceso a consultas avanzadas

- **Al activar**: el usuario de la cuenta tiene acceso a la zona **Investigaciones** y puede crear una pestaña de **Consultas avanzadas** para diseñar sentencias SQL y así explorar el océano de datos recogido por Cytomic Orion en busca de operaciones sospechosas.
- **Al desactivar**: el usuario de la cuenta tiene acceso a la zona **Investigaciones** pero no puede crear ni visualizar ni modificar las pestañas de **Consultas avanzadas**.

Acceso a OSQuery

- **Al activar**: el usuario de la cuenta tiene acceso a la zona **Investigaciones** y puede crear una pestaña de tipo **Consulta OSQuery** para crear un notebook utilizado en la exploración de la infraestructura IT de los clientes del SOC.
- **Al desactivar**: el usuario de la cuenta tiene acceso a la zona **Investigaciones** pero no puede crear ni visualizar ni modificar las pestañas de tipo **Consulta OSQuery**.

Acceso al asistente para consultas

- **Al activar**: el usuario de la cuenta tiene acceso a la zona **Investigaciones** y puede crear una pestaña de **Asistente de consultas** para diseñar búsquedas de forma sencilla y visual, y así explorar el océano de datos recogido por Cytomic Orion en busca de operaciones sospechosas.
- **Al desactivar**: el usuario de la cuenta tiene acceso a la zona **Investigaciones** pero no puede crear ni visualizar ni modificar las pestañas de tipo **Asistente de consultas**.

Aislar/desaislar equipos

- **Al activar**: el usuario de la cuenta puede restringir las comunicaciones de los equipos de los clientes del SOC para aislarlos si están en peligro o para contener los efectos de un ataque.
- **Al desactivar**: el usuario de la cuenta no puede restringir las comunicaciones de los equipos de los clientes del SOC para aislarlos si están en peligro o para contener los efectos de un ataque.

Borrado de IOCs sobre todos los clientes

- **Al activar**: el usuario de la cuenta puede ejecutar llamadas a la API de Cytomic Orion para borrar IOCs previamente cargados en la plataforma.
- **Al desactivar**: el usuario de la cuenta no puede ejecutar llamadas a la API de Cytomic Orion para borrar IOCs previamente cargados en la plataforma.

Búsqueda de IOCs

- **Al activar**: el usuario de la cuenta puede ejecutar llamadas a la API de Cytomic Orion para buscar en los equipos de los clientes los IOCs previamente cargados en la plataforma.
- **Al desactivar**: el usuario de la cuenta no puede ejecutar llamadas a la API de Cytomic Orion buscar en los equipos de los clientes los IOCs previamente cargados en la plataforma.

Crear Hunting Rules y reglas de notificación sobre todos los clientes

- **Al activar**: el usuario de la cuenta puede crear Hunting rules y reglas de notificación que afecten a todos los clientes sin importar la configuración de visibilidad que tenga asociada la cuenta.
- **Al desactivar**: el usuario de la cuenta no puede crear Hunting rules y reglas de notificación que afecten a todos los clientes.

Crear Notebook para investigación manual

- **Al activar**: el usuario de la cuenta puede crear editar y borrar Notebooks para automatizar las investigaciones.
- **Al desactivar**: el usuario de la cuenta no puede crear, editar ni borrar Notebooks.

Crear Notebook desde plantilla para investigación automatizada

- **Al activar**: el usuario de la cuenta tiene acceso a la opción **Investigación automatizada** accesible desde la barra de pestañas de una investigación para crear un notebook utilizando una plantilla previamente creada en Cytomic Orion.
- **Al desactivar**: el usuario de la cuenta no tiene acceso a la opción **Investigación automatizada** y por lo tanto no puede crear un notebook utilizando plantillas.

Crear Quick answers

- **Al activar**: el usuario de la cuenta puede crear y borrar pequeños fragmentos de código (Respuestas rápidas) para acelerar el desarrollo de investigaciones.
- **Al desactivar**: el usuario de la cuenta no puede crear ni borrar pequeños fragmentos de código (Respuestas rápidas) para acelerar el desarrollo de investigaciones.

Crear reglas de notificación de indicios

- **Al activar**: el usuario de la cuenta puede crear, modificar y borrar reglas de notificación de indicios generados por Hunting rules para los clientes que tenga visibilidad.
- **Al desactivar**: el usuario de la cuenta no puede crear, modificar ni borrar reglas de notificación de indicios generados por Hunting rules.

Eliminar indicios y gestionar reglas de eliminación automática de indicios

- **Al activar**: el usuario de la cuenta puede borrar indicios y crear, editar y borrar reglas de eliminación de indicios.
- **Al desactivar**: el usuario de la cuenta no puede borrar indicios ni crear, editar ni borrar reglas

de eliminación de indicios, aunque sí puede listar las reglas preexistentes y ver los indicios eliminados por cada una de las reglas.

Gestionar plantillas de Notebooks de investigación

- **Al activar**: el usuario de la cuenta puede acceder a la zona **Configuración**, panel lateral **Investigaciones automatizadas** para crear, editar, publicar y borrar plantillas de Notebooks.
- **Al desactivar**: el usuario de la cuenta no puede acceder a la zona **Configuración**, panel lateral **Investigaciones automatizadas**.

Gestionar Hunting rules

- **Al activar**: el usuario de la cuenta puede crear, editar y activar o desactivar Hunting rules.
- **Al desactivar**: el usuario de la cuenta no puede crear, editar o activar / desactivar Hunting rules aunque si puede listar las reglas preexistentes y ver su definición, si fueron creadas por una cuenta del SOC.

Gestionar reglas de asignación automática de indicios

- **Al activar**: el usuario de la cuenta puede crear, borrar, modificar o listar nuevas reglas de asignación automática de indicios a investigaciones.
- **Al desactivar**: el usuario de la cuenta no puede acceder a la zona **Configuración**, panel lateral **Reglas de asignación**.

Gestión de usuarios, permisos y clientes

- **Al activar**: el usuario de la cuenta puede crear nuevos usuarios y roles, asignando permisos en función del perfil del analista y del nivel de servicio que se le haya asignado dentro del SOC y configurando la visibilidad de los clientes. Este permiso es común asignarlo a usuarios gestores del SOC.
- **Al desactivar**: el usuario de la cuenta no puede acceder a la zona **Configuración**, panel lateral **Usuarios** ni **Clientes**.

Importación de IOCs sobre todos los clientes

- **Al activar**: el usuario de la cuenta puede ejecutar llamadas a la API de Cytomic Orion para cargar nuevos IOCs en la plataforma.
- **Al desactivar**: el usuario de la cuenta no puede ejecutar llamadas a la API de Cytomic Orion para cargar nuevos IOCs en la plataforma.

Reiniciar equipos

- **Al activar**: el usuario de la cuenta puede invocar la secuencia de reinicio de los equipos de los clientes del SOC.
- **Al desactivar**: el usuario de la cuenta no puede invocar la secuencia de reinicio de los equipos de los clientes del SOC.

Shell remoto y visualizar los comandos ejecutados

- **Al activar**: el usuario de la cuenta puede abrir una linea de comandos remota en los equipos de los clientes del SOC.
- **Al desactivar**: el usuario de la cuenta no puede abrir una linea de comandos remota en los equipos de los clientes del SOC.

Ver el dashboard de consumo de datos

- **Al activar**: el usuario de la cuenta puede abrir el dashboard de consumo de datos haciendo clic en el panel **Consumo de datos**.
- **Al desactivar**: el usuario de la cuenta no puede abrir el dashboard de consumo de datos.

Ver nombres de los clientes

- **Al activar**: la consola mostrará el nombre del cliente al que pertenecen los equipos y no un simple identificador numérico.
- **Al desactivar**: impide visualizar el nombre del cliente investigado, mostrándose únicamente su identificador numérico. De esta forma el analista no podrá vincular los datos mostrados en Cytomic Orion a clientes concretos, respetando de esta manera los acuerdos de confidencialidad firmados y la legislación en materia de protección de datos (GDPR y otras normativas).

Ver nombres de los equipos

- **Al activar**: la consola mostrará el nombre del equipo y no solo un identificador numérico.
- **Al desactivar**: impide visualizar el nombre del equipo analizado, mostrándose únicamente su identificador numérico. De esta forma el analista no podrá asociar los datos mostrados en Cytomic Orion a equipos concretos, respetando de esta manera los acuerdos de confidencialidad firmados y la legislación en materia de protección de datos (GDPR y otras normativas).

Ver registro de actividad de la organización

- **Al activar**: el usuario de la cuenta tiene acceso a la opción **Registro de actividad**, accesible desde el menú superior **Configuración** para listar las acciones ejecutadas por las cuentas de usuario que han sido realizadas fuera de una investigación.
- **Al desactivar**: el usuario de la cuenta no tiene acceso a la opción **Registro de actividad**.

Visualización de grafos

- **Al activar**: el usuario de la cuenta tiene acceso a la opción **Grafos**, accesible desde una investigación o desde un evento mostrado en la consola de investigación, para visualizar un notebook de tipo grafo.
- **Al desactivar**: el usuario de la cuenta no tiene acceso a la opción **Grafos**.

Registro de actividad de las cuentas de usuario

Cytomic Orion registra las acciones ejecutadas en la consola por los analistas del SOC fuera del entorno de una investigación. Para obtener información sobre las acciones registradas dentro de una investigación, consulta **Registro de actividad asociado a una investigación** en la página 127.

Acceso al registro de actividad de usuario

Haz clic en el menú superior **Configuración** y en el panel lateral **Registro de la actividad**. Se mostrará el listado Registro de actividad de usuario.

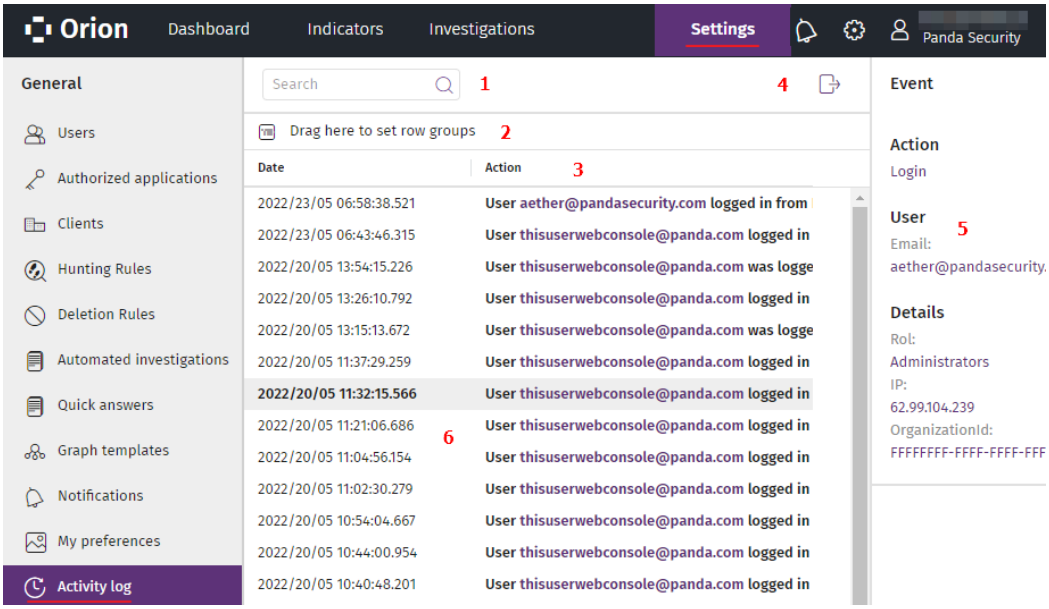


Figura 4.4: Listado Registro de actividad de usuario

- **Herramienta de búsqueda (1)**: busca en el contenido de los campos **Acción**, **Usuario** y **Tipo de acción** para filtrar los registros presentados. Admite búsquedas parciales de cadenas.

Consulta **Herramientas de búsqueda** en la página **43**.

- **Herramienta de agrupación (2)**: agrupa los registros según el campo elegido. Para obtener más información sobre la herramienta de agrupación, consulta **Agrupar registros por columnas** en la página **40**.
- **Ordenar listado (3)**: haz clic en la cabecera de la columna para ordenar las filas según el campo elegido. Haz clic nuevamente en la misma columna para variar el criterio de ordenación (ascendente o descendente). Consulta **Ordenar columnas** en la página **40**.
- **Exportar (4)**: vuelca el listado en un fichero csv.
- **Panel lateral (5)**: al seleccionar un registro muestra su información extendida asociada. Consulta **Información adicional del evento registrado**.
- **Panel central (6)**: muestra un listado de registros de actividad que coinciden con los criterios de búsqueda establecidos. A continuación se indican los campos incluidos en el listado:

Campo	Descripción
Fecha	Fecha en la que se ha producido la acción registrada.
Acción	Tipo de acción registrada junto a la cuenta de usuario que la inició e información adicional. Consulta **Acciones registradas en Cytomic Orion** .
Usuario	Nombre de la cuenta que inició la acción. Este campo no se muestra por defecto.
Tipo de acción	Clase de acción registrada. Este campo no se muestra por defecto.

Tabla 4.2: Campos del listado Registro de actividad

Acciones registradas en Cytomic Orion

Tipo de acción	Descripción
Login	El usuario inició la sesión.
Logout por falta de actividad	El usuario de la consola no realizó ninguna acción en 2 horas y Cytomic Orion terminó su sesión de forma automática por seguridad.
Logout	El usuario terminó su sesión.

Tipo de acción	Descripción
Creación de plantilla de respuesta rápida / plantilla de investigación automática / plantilla de grafo	El usuario creó la plantilla de respuesta rápida, la plantilla de investigación o la plantilla de grafo indicado.
Modificación de plantilla de respuesta rápida / plantilla de investigación automática / plantilla de grafo	El usuario modificó la plantilla de respuesta rápida, la plantilla de investigación o la plantilla de grafo indicada.
Borrado de plantilla de respuesta rápida / plantilla de investigación automática / plantilla de grafo	El usuario borró la plantilla de respuesta rápida, la plantilla de investigación o la plantilla de grafo indicada.
Actualización de la descripción o categoría de la plantilla de respuesta rápida / plantilla de investigación automática / plantilla de grafo	El usuario actualizó la descripción o la categoría de la plantilla de respuesta rápida, la plantilla de investigación o la plantilla de grafo indicada.
Renombrar la plantilla de respuesta rápida / plantilla de investigación automática / plantilla de grafo	El usuario cambió el nombre de la plantilla de respuesta rápida, la plantilla de investigación o la plantilla de grafo indicada.
Copia la plantilla de respuesta rápida / plantilla de investigación automática / plantilla de grafo	El usuario copió la plantilla de respuesta rápida o la plantilla del grafo indicada.
Desactivar la verificación en dos pasos	El usuario desactivó la verificación en dos pasos para su cuenta.
Activar la verificación en dos pasos	El usuario activó la verificación en dos pasos para su cuenta.
Crear hunting rule	El usuario creó una hunting rule.
Modificar hunting rule	El usuario modificó una hunting rule.
Borrar hunting rule	El usuario borró una hunting rule.

Tabla 4.3: Tipos de acciones registradas

Información adicional del evento registrado

Campo	Descripción
Acción	Acción registrada. Consulta **Acciones registradas en Cytomic Orion** .
Email	Dirección de correo electrónico de la cuenta que ejecutó la acción registrada.
Rol	Rol de la cuenta que ejecutó la acción registrada.
IP	Dirección IP pública del último dispositivo de red que utilizó el analista para conectarse con la consola.
OrganizationID	Identificador del SOC / MSSP al que pertenece la cuenta del usuario.
notebookId	Identificador del documento sobre el que se realiza la operación.
oldNotebookDescription	Descripción del notebook anterior a su modificación.
newNotebookDescription	Nueva descripción asociada al notebook.
notebookName	Nombre del notebook sobre el que realiza la operación.
documentName	Nombre del documento sobre el que realiza la operación.
oldNotebookName	Nombre del notebook anterior a su cambio.
newNotebookName	Nuevo nombre del notebook.
imageId	Identificador de la imagen de Jupyter que el notebook utilizó como base.
documentId	Identificador del documento sobre el que se

Campo	Descripción
	realiza la operación.
documentVersionid	Identificador del número de versión interno del documento.
documentIsManualSave	• **True**: el documento se salvó de forma manual. • **False**: el documento se salvó de forma automática.
oldCategoryId	Categoría del notebook anterior a su cambio.
newCategoryId	Nueva categoría del notebook.
discriminator	Tipo de documento sobre el que se realiza la operación: • **0**: Sin establecer • **1**: Documento • **2**: Plantilla • **3**: Respuesta rápida • **4**: Grafo • **5**: OsQuery
sourceNotebookId	Identificador del notebook del que se ha hecho la copia.
targetNotebookId	Identificado del nuevo notebook copiado.

Tabla 4.4: Campos del panel derecho

Capítulo 5

Indicios y reglas de hunting

En la mayoría de las situaciones, los analistas del SOC inician el proceso de hunting a partir de la aparición de un nuevo indicio o hipótesis. Cytomic Orion genera un indicio cuando detecta en la telemetría registrada en los equipos del cliente un patrón sospechoso de pertenecer a la CKC de un ciberataque. Esta hipótesis será analizada por el técnico de nivel 1 para determinar si se trata de un falso positivo, o por el contrario es una posible amenaza a investigar. El proceso de filtrado se conoce como "triaje de indicios" y su objetivo es entregar a los técnicos de nivel 2 aquellas hipótesis que se corresponden a situaciones anómalas y que deben ser investigadas con más profundidad.

CONTENIDO DEL CAPÍTULO

Conceptos básicos del sistema de indicios

Las reglas de hunting (Hunting rules)

Son una descripción de patrones de eventos sospechosos de pertenecer a la CKC de un ataque informático. Son creadas por dos grupos de analistas diferentes:

- Los analistas de Cytomic que, con ayuda de los sistemas automáticos de ML (Machine Learning), analizan de forma transversal todo el flujo de eventos generado por los clientes de Cytomic Orion para crear y probar nuevas reglas de hunting.
- Los analistas del SOC que quieren adaptar los indicios generados al parque informático de los clientes que administran, activando y desactivando las reglas existentes y creando nuevas en función de los eventos producidos.

*Consulta **Gestión de Hunting rules** en la página **85**.*

Características de los indicios

Cuando la monitorización de procesos da como resultado una secuencia de eventos que coincide con la descrita por una regla de hunting, Cytomic Orion genera un indicio. Este indicio estará asociado siempre a la regla de hunting que lo generó y al equipo donde fue encontrado.

Los atributos clave que deberán considerarse por parte de los analistas son los siguientes:

- **Momento en que Cytomic Orion registró el ultimo evento que generó el indicio**: determina cuando se ha producido la situación sospechosa de pertenecer a la CKC de un ciberataque, para que el analista pueda investigar en profundidad el estado del equipo en ese preciso momento.
- **Nombre del equipo e identificador**: un indicio hace referencia a un único equipo. Si se produce la misma cadena de eventos sospechosos en varios equipos se generará un indicio por cada equipo.
- **Número de veces que se repite el indicio**: si se detecta un mismo patrón de indicios forma continuada en un mismo equipo, Cytomic Orion solo genera un indicio, indicando el número de repeticiones. Consulta **Agrupación de indicios**.
- **Estado del indicio**: indica si el indicio está pendiente de investigación, ya ha sido investigado o está en curso.
- **Severidad del indicio**: indica si el indicio se corresponde a un ataque que, por su forma de operar, puede tener un gran impacto en el funcionamiento normal de los sistema de información de la empresa. Este impacto se puede traducir en grandes pérdidas económicas para las organizaciones y por lo tanto los analistas deben utilizar este atributo para priorizar los análisis.
- **Regla de hunting asociada**: el indicio lleva asociada una única regla de hunting que fue la que Cytomic Orion utilizó para localizar el patrón de eventos sospechoso. El nombre de la regla de hunting es descriptivo y sirve de pauta para dirigir la investigación.

Esquema básico del proceso de generación de indicios

El esquema mostrado a continuación resume el proceso de generación de indicios.

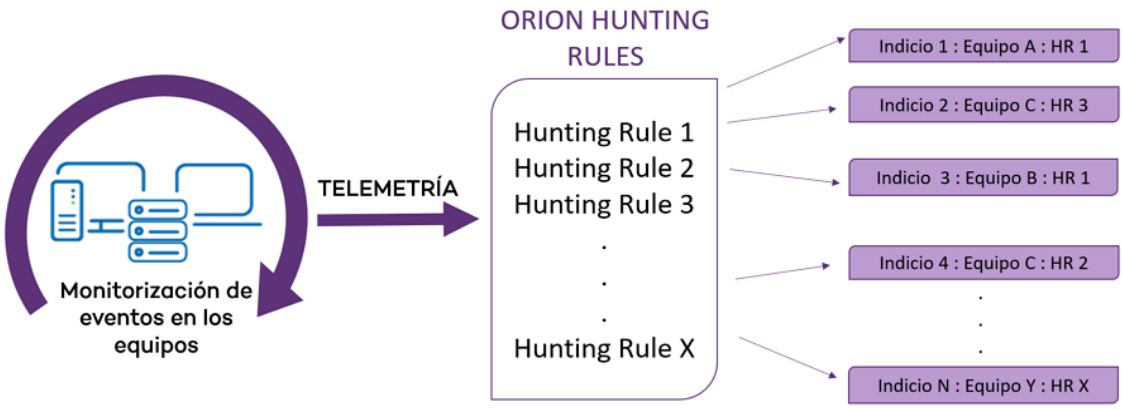


Figura 5.1: Esquema de generación de indicios en base a reglas de hunting

Acceso a la zona Indicios

Haz clic en el menú superior **Indicios**. Se mostrará una ventana dividida en varias secciones:

- **Panel de filtrado (1)**: el panel lateral izquierdo contiene herramientas de filtrado de indicios que facilitan al analista la asignación de éstos a las investigaciones y eliminar aquellos que se consideran sin valor.
- **Panel de búsqueda (2)**: busca por contenido los indicios de interés para el analista.
- **Panel de indicios (3)**: listado con todos los indicios generadas en los equipos de los clientes del MSSP / MDR, así como las herramientas necesarias para que el Nivel 1 de analistas del SOC pueda gestionarlos y generar las investigaciones necesarias.

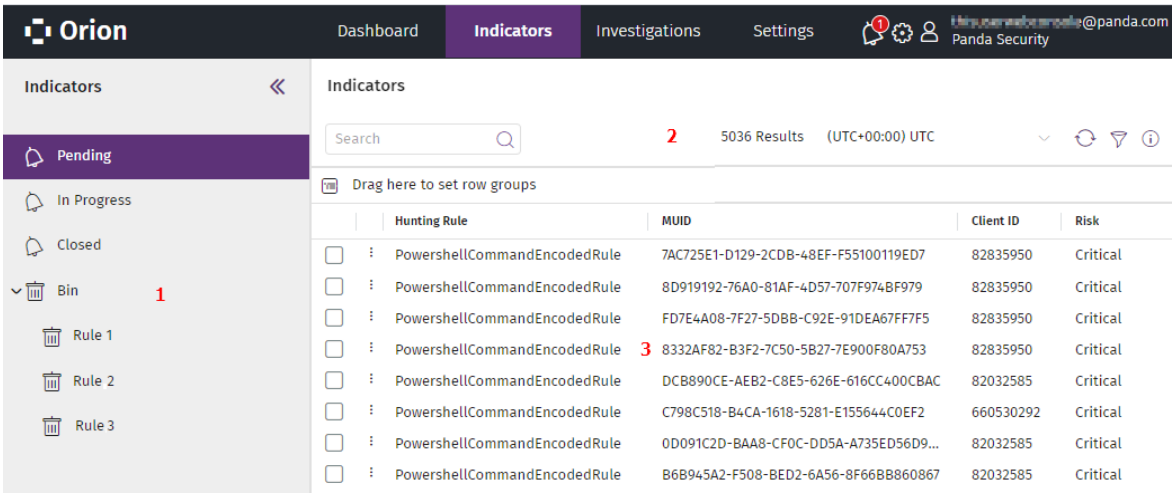


Figura 5.2: Vista general de la zona Indicios

Listado de indicios

El panel de indicios contiene los indicios generados por las reglas de hunting y los campos que describen a cada uno de ellos.

Campo	Descripción
Hunting Rule	Nombre de la regla de hunting que generó el indicio y descripción de los artefactos que monitoriza en el equipo del cliente.
Estado	Indica si el indicio ha sido asignado a una investigación y el estado del mismo. • **En curso**: el indicio está asignado a una investigación y un técnico de Nivel 2 lo está analizando. • **Pendientes**: el indicio todavía no ha sido asignado a una investigación. • **Finalizado**: el indicio fue asignado a una investigación y se resolvió.
Investigación	Nombre de la investigación asociada para los indicios en estado **En investigación** o **Finalizado**.
Fecha indicio	Fecha en la que se generó el indicio.
Último evento	Fecha en la que se registró en el equipo del usuario o servidor el último evento que desembocó en la generación del indicio. Esta fecha puede no coincidir con **Fecha indicio** si se produjo un retraso al generar el indicio, como por ejemplo debido a una interrupción en la conexión entre el servidor de Cytomic Orion y el equipo.
Equipo	Nombre del equipo del cliente involucrado en el indicio.
Grupo	Grupo en la consola de Cytomic EPDR al que pertenece el equipo.
Fecha de eliminación	Fecha en la que una regla de eliminación se aplicó al indicio y éste entró en la papelera.
Eliminado por	Nombre de la regla de eliminación que movió el indicio a la papelera.
MUID	Identificador único del equipo del cliente involucrado en el indicio.
ID Cliente	Identificador único del cliente al que pertenece el equipo involucrado en el indicio.

Campo	Descripción
Riesgo	Importancia del impacto del indicio detectado: **Crítica**, **Riesgo alto**, **Riesgo medio**, **Riesgo bajo**.
MITRE	Táctica, técnica y subtécnica asociada a la hunting rule, según la especificación MITRE. Si hay más de un par de tácticas & técnicas, se separan con el carácter '#'. Para más información consulta **Panel de detalles**.
Ocurrencias	Número de veces que Cytomic Orion detecta el mismo tipo de indicio de forma repetida en el mismo equipo. Consulta **Agrupación de indicios**.
Detalles	Descripción del indicio y nombre de la hunting rule asociada que indica el tipo de eventos sospechosos registrados para que el equipo de Nivel 1 pueda hacer el triaje.
Sistemas operativos	Sistemas operativos donde busca indicios la Hunting rule que ha detectado el evento sospechoso.

Tabla 5.1: Campos del listado Indicios

El panel indicios contiene la información adicional siguiente:

- **Número de indicios encontrados aplicando los criterios de selección establecidos**: se muestra en la parte superior del listado (**2**).
- **Uso horario**: cambia el uso horario configurado por defecto para toda la consola en la zona Indicios, establécelo mediante el control situado en la parte superior del listado (2). Esta configuración afectará tanto al campo **Fecha indicio** de los listados como al formato de la fecha introducido en el panel de filtrado. Consulta **Zona Configuración** en la página **35**.

Agrupación de indicios

Con el objetivo de no entorpecer la labor de investigación de los analistas con listados de indicios repetidos demasiado largos, Cytomic Orion agrupa los indicios dependiendo del lugar donde se han detectado.

Indicios detectados en el servidor

Si las reglas de hunting catalogan como posible amenaza un patrón de eventos que se repite en la telemetría que un equipo envía al servidor, Cytomic Orion genera los siguientes indicios:

- Un primer indicio con el campo **Ocurrencias** a 1 cuando detecta el primer patrón en el equipo.

- Un indicio cada hora que agrupa todas las detecciones que se han producido en ese intervalo y en ese equipo. El campo **Ocurrencias** contiene el número de repeticiones detectado.

Indicios detectados en el equipo

Si el software de protección instalado en el equipo cataloga como posible amenaza un patrón de eventos que se repite en ese equipo, Cytomic Orion genera los siguientes indicios:

- Un primer indicio con el campo **Ocurrencias** a 1 cuando el equipo detecta el primer patrón.
- Un indicio cada 6 horas que agrupa todas las detecciones que se han producido en ese intervalo. El campo **Ocurrencias** contiene el número de repeticiones detectado.

Panel de detalles

Haz clic en el icono situado en la esquina superior derecha para desplegar el panel derecho **Detalles**. Se mostrarán 2 pestañas:

- **Detalles**: muestra todos los campos del indicio seleccionado. Consulta **Listado de indicios**
- **MITRE**: muestra el detalle de la táctica y técnica MITRE asociada a la hunting rule que generó el indicio. Si la hunting rule está asociada a más de una técnica, el panel MITRE agrupa la información en varios desplegables, uno por cada técnica. Toda la información de la pestaña MITRE se recoge de la fuente oficial accesible en la dirección web**https://attack.mitre.org/matrices/enterprise/**

Campo	Descripción
Táctica	Nombre de la táctica de la matriz MITRE relacionada con la hunting rule del indicio. Las tácticas vienen identificadas por una cadena de caracteres con el formato TAXXXX.
Técnica	Nombre de la técnica de la matriz MITRE relacionada con la hunting rule del indicio. Las técnicas vienen identificadas por una cadena de caracteres con el formato TXXXX.
Subtécnica	Nombre de la subtécnica de la matriz MITRE relacionada con la hunting rule del indicio. Las subtécnicas viene identificadas por una cadena de caracteres con el formato TXXXX.YYY.
Plataforma	Sistemas operativos afectados por la técnica & táctica
Permisos necesarios	Permisos que requiere el atacante para desarrollar el ataque descrito en la técnica & táctica.

Campo	Descripción
Descripción	Descripción de la técnica & táctica según los datos publicados por MITRE.

Tabla 5.2: Campos de la pestaña MITRE

Filtrado y agrupación de indicios

Cytomic Orion incorpora múltiples herramientas de filtrado de indicios que permiten al analista localizar de forma rápida y flexible la información que necesita.

Filtrado por estado del indicio

En el panel izquierdo (**1**) se muestra la herramienta de filtrado de indicios por su estado. Haz clic en un estado representado por el icono y el listado se actualizará:

- **En curso**: el indicio está asignada a una investigación y un analista de Nivel 2 lo está investigando.
- **Pendientes**: el indicio todavía no ha sido asignado a una investigación.
- **Cerrada**: el indicio fue asignado a una investigación y se ha resuelto.

Filtrado por característica del indicio

El propio listado de indicios contiene herramientas para filtrar los registros mostrados en función del contenido de las columnas, y permite ordenar y configurar el listado según las necesidades del analista. Para obtener más información sobre las herramientas comunes de Cytomic Orion consulta **Herramientas para configurar los listados** en la página **39**.

Búsqueda de indicios por contenido

En la parte superior del listado se incluye una herramienta que soporta búsquedas parciales y se extiende al contenido de todos los campos del listado. Para obtener más información consulta **Herramientas de búsqueda** en la página **43**.

Filtrado de indicios por intervalo

El filtro establecido se aplicará sobre la fecha de creación del último evento asociado al indicio (campo **Último evento** del indicio).

- Haz clic en el icono (**2**). Se mostrará el panel lateral de filtrado.
- Selecciona en el campo **Fecha** el tipo de filtro que deseas:
  - **Últimas 24 horas**
  - **Últimos 7 días**

- **Personalizado**: establece la fecha y la hora del intervalo.

- Selecciona la zona horaria para realizar el filtrado.
- Haz clic en el botón **Aplicar**. El listado de indicios (**3**) se actualizará.

Ordenar y agrupar indicios en el listado

Para cambiar el orden de los resultados y la forma en la que se visualizan los indicios en el listado, consulta **Herramientas para configurar los listados** en la página **39**.

Eliminar indicios de forma manual

Las reglas de hunting definidas de forma ambigua generan grandes cantidades de indicios que pueden ser considerados como falsos positivos. Este exceso de ruido tiende a sobrecargar de trabajo a los analistas de nivel 1 a la hora de afrontar las tareas de triaje. Para evitar esta situación, Cytomic Orion permite mover indicios de forma manual a la papelera.

Permisos requeridos

Para eliminar y gestionar las reglas de eliminación de indicios es necesario el que la cuenta del analista tenga el permiso **Eliminar indicios y gestionar reglas de eliminación automática de indicios** asignado a su rol. Para obtener más información sobre roles y permisos consulta **Descripción de los permisos implementados** en la página **60**.

Mover uno o más indicios a la papelera

- Haz clic en las casillas de selección asociadas a los indicios a borrar. Solo se pueden eliminar los indicios en estado **Pendiente**.
- Haz clic en el icono **Eliminar** de la barra de herramientas. Los indicios pasarán automáticamente a la papelera, en la rama **Eliminado manualmente**.

> *Los indicios marcados como eliminados se retienen durante 7 días en la papelera, trascurrido ese tiempo serán eliminados definitivamente de Cytomic Orion.*

Eliminar indicios de forma automática

El analista puede crear reglas de eliminación para definir criterios de filtrado dentro del flujo de indicios generado por Cytomic Orion. Una vez que se detecta un indicio que coincide con los criterios definidos por una regla de eliminación, se le asigna el estado **Eliminado** y se retira del listado de indicios. Los indicios marcados como **Eliminados** pasan a la papelera temporalmente, pero si un indicio fue asignado previamente a una investigación no se eliminará de ésta.

> *Los indicios marcados como eliminados se retienen durante 7 días en la papelera, trascurrido ese tiempo serán eliminados definitivamente de Cytomic Orion.*

Añadir una regla de eliminación

Las reglas de eliminación se crean a partir de un único indicio. Antes de comenzar el procedimiento para crear una regla, comprueba que solo un indicio de la lista está seleccionado.

- En el menú superior **Indicios**, selecciona un indicio con las casillas de selección.
- Haz clic en el botón **Añadir regla de eliminación automática (4)** situado en la barra de herramientas. Se mostrará una ventana con los detalles del indicio que se eliminará.

ó

- Haz clic en el menú de contexto **(2)** situado junto a la casilla de selección, o con el botón de la derecha del ratón en cualquier campo del indicio para mostrar el menú desplegable. Selecciona la opción **Añadir regla de eliminación automática**.
- Establece los campos descriptivos de la regla de eliminación:
  - **Nombre**:nombre de la regla de eliminación.
  - **Descripción**: texto descriptivo donde el analista puede indicar los motivos de la eliminación de indicios.
- Establece los campos asociados a la regla que se utilizarán para describir los indicios a eliminar:
  - **ID de cliente**: especifica los identificadores de cliente asociados a los indicios a eliminar. Todas las reglas de eliminación deben tener definido al menos un cliente. Haz clic en el icono ⊕ para elegir los clientes, o copia y pega una lista de identificadores de cliente separados por comas.
  - **Hunting Rule**: nombre de la Hunting rule que generó los indicios a eliminar. Es un campo opcional.
  - **MUID**: especifica los identificadores de los equipos asociados a los indicios a eliminar. Haz clic en el icono ⊕ para elegir los MUIDs o copia y pega una lista de MUIDs se parados por comas. Es un campo opcional.
  - **Equipo**: especifica los nombres de los equipos donde se originaron los indicios a eliminar. Haz clic en el icono ⊕ para elegir los equipos o copia y pega una lista de nombres de equipos separados por comas. Es un campo opcional.
  - **Detalles**: permite especificar el campo **Detalles** de los indicios a eliminar. Establece el contenido del campo exacto con la opción **Igual a**, o de forma flexible mediante

una expresión regular con la opción **RegEx**. Consulta **Gestión de las reglas de eliminación** para más información.

Por defecto, las reglas de eliminación se crean de la forma más restrictiva posible, y es labor del analista desactivar aquellos campos opcionales innecesarios para flexibilizar la regla.

En el caso de que una regla de eliminación tenga varios criterios establecidos se aplicará el operador lógico AND entre ellos. De esta manera que solo se filtrarán aquellos indicios que cumplan con todos los criterios establecidos en la regla de eliminación.

Expresiones regulares

*Consulta el enlace **https://docs.microsoft.com/en-us/dotnet/standard/base-types/regular-expression-language-quick-reference** para obtener más información sobre la sintaxis admitida en la expresiones regulares.*
*Para validar las expresiones regulares desarrolladas consulta el enlace **http://regexstorm.net/tester.***

Cytomic Orion soporta el formato Regex C para describir patrones flexibles en el campo **Detalles** de los indicios. Como en la mayoría de lenguajes utilizados para describir patrones de caracteres, es necesario "escapar" aquellos que se consideran especiales o propios del lenguaje utilizado. Con este fin se utiliza el carácter "\" en el caso de Regex C.

Para facilitar el desarrollo de expresiones regulares se incluye un panel de previsualización que permite comprobar si los patrones a buscar coinciden con la expresión regular escrita hasta el momento.

Para generar una expresión regular, haz clic en el desplegable **RegEx** del campo **Detalles**. El contenido del campo se actualizará con una expresión regular que cumpla con el contenido del panel de previsualización. Todos los caracteres especiales son "escapados" de forma automática por la consola para facilitar al analista la modificación de la expresión regular.

Ejemplo de exclusión utilizando expresiones regulares en el campo detalle

Se quiere retirar del panel Indicios todas las ejecuciones de la herramienta `net.exe` cuando intenta añadir al grupo de administradores el usuario `"gcch\GG_SEC_IBM_PC_Admins"` por ser una acción exenta de riesgo pero muy frecuente.

El indicio generado por Cytomic Orion en esta situación es le siguiente:

```
{
       "contents":
       [
              {
              "ChildPath": "SYSTEM|\net.exe",
```

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

En el campo Detalles de la consola de Cytomic Orion el indicio se muestra en formato compacto:

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

La expresión regular que filtra los indicios por el contenido del campo Detalle según los criterios establecidos por el analista sería:

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

El panel de previsualización permite comprobar que la expresión regular definida genera el patrón de caracteres que concuerda con el contenido del campo detalle del indicio.

Gestión de las reglas de eliminación

Para gestionar las reglas de eliminación de forma centralizada, en el menú superior **Configuración**, haz clic en el panel lateral **Reglas de eliminación**. Se mostrará un listado con todas las reglas de eliminación creadas hasta el momento.

Listado de reglas de eliminación

Campo	Descripción
Nombre	Nombre de la regla de eliminación asignado por el analista.
Fecha de creación	Fecha en la que se creó la regla de eliminación.
Fecha de modificación	Fecha en la que se modificó por última vez la regla de eliminación.
Descripción	Descripción asignada por el analista.
Hunting Rule	Nombre de la regla de hunting que generó el indicio y descripción de los artefactos que monitoriza en el equipo del cliente.

Campo	Descripción
Indicios eliminados los últimos 30 días	Número de indicios que la regla eliminó en los últimos 30 días. El analista puede utilizar este campo para determinar el grado de utilidad de una regla de eliminación.
Fecha de última eliminación	Fecha y hora en la que la regla de eliminación se activó por última vez. El analista puede utilizar este campo para determinar el grado de utilidad de una regla de eliminación.

Tabla 5.3: Campos del listado de reglas de eliminación

Editar reglas de eliminación

Cuando un analista comprueba que una regla está eliminando indicios valiosos, tiene la posibilidad de editarla. Para ello sigue los pasos mostrados a continuación:

- Haz clic en la opción **Papelera** del panel lateral para desplegar las reglas de eliminación creadas.
- Haz clic en el icono de contexto asociado a la regla de eliminación que quieres editar. Se mostrará un menú desplegable.
- Elige la opción **Editar regla de eliminación automática** y establece los nuevos criterios de eliminación de indicios:
    - **Nombre**: nombre de la regla de eliminación.
    - **Descripción**: texto descriptivo donde el analista puede indicar los motivos de la eliminación de indicios.
    - **ID de cliente**: especifica el identificador del cliente al que pertenece el equipo donde se detectó el indicio a eliminar.
    - **Hunting Rule**: nombre de la hunting rule asociada a la regla de eliminación.
    - **MUID**: especifica el identificador del equipo donde se detectó el indicio a eliminar.
    - **Nombre del equipo**: nombre del equipo donde se detectó el indicio a eliminar.
    - **Detalles**: permite especificar el campo **Detalles** de los indicios a eliminar. Establece el contenido del campo exacto con la opción **Igual a**, o de forma flexible mediante una expresión regular con la opción **RegEx**. Para más información consulta **Expresiones regulares** en la página **275**.

Los indicios que ya fueron afectados por la regla de eliminación no sufrirán ningún cambio y por lo tanto seguirán sin mostrarse en el listado principal, aunque seguirán mostrándose al hacer clic en la regla editada.

Borrar reglas de eliminación

Cuando un analista comprueba que una regla está eliminando indicios valiosos, tiene la posibilidad de eliminarla:

- Haz clic en la opción **Papelera** del panel lateral para desplegar las reglas de eliminación creadas.
- Haz clic en el icono de contexto asociado a la regla de eliminación que quieres borrar. Se mostrará un menú desplegable.
- Elige la opción **Eliminar**. Los indicios recientes afectados por la regla de eliminación volverán a mostrarse en el listado con el estado **Pendiente**. Los indicios anteriores a 7 días no se pueden recuperar.

Exportar listado

Haz clic en el icono para descargar un fichero .csv con el contenido del listado **Reglas de eliminación**.

Recuperar indicios y gestionar la papelera

Ordenar y agrupar las reglas de eliminación definidas

Para facilitar la búsqueda de un indicio ya eliminado, la papelera los agrupa de forma automática mediante la regla de eliminación que se aplicó para su borrado. Puesto que pueden existir muchas reglas de eliminación definidas, Cytomic Orion implementa herramientas para ordenarlas y agruparlas de diferentes maneras:

- Haz clic en el menú superior **Indicios** y en el icono situado en el panel izquierdo. Inicialmente se mostrarán todas las reglas de eliminación definidas sin ningún criterio de ordenación ni agrupación.
- Haz clic en el menú de contexto de la papelera. Se mostrará la opción **Ordenar** por con los siguientes criterios:
    - **Fecha de modificación**: las reglas de eliminación creadas se ordenan por la fecha en la que fueron modificadas por última vez.
    - **Hunting rule**: las reglas de eliminación se agrupan por su Hunting rule asociada. Se crearán tantas agrupaciones distintas como Huntings rules distintas haya utilizado Cytomic Orion para generar los indicios que eliminó el analista.
    - **Nombre**: las reglas de eliminación se ordenan por su nombre.
    - **Ascendente**: indica la dirección del criterio de ordenación de las reglas de eliminación.

- **Descendente**: indica la dirección del criterio de ordenación de las reglas de eliminación.

Recuperar uno o varios indicios de la papelera

- Haz clic en el menú superior **Indicios** y en el icono de la papelera situado en el panel izquierdo. Las reglas de eliminación se mostrarán en forma de árbol dependiendo de los criterios de ordenación y agrupación elegidos para la papelera.
- Si es un dato conocido, haz clic en la regla de eliminación asociada al indicio para filtrar de forma el listado de indicios mostrado en el panel de la derecha.
- Haz clic en las casillas de selección asociadas a los indicios a recuperar y en la opción **Mover a pendientes** de la barra de herramientas. Los indicios cambiarán su estado a **Pendiente** y se dejarán de mostrar en la papelera de indicios.

Recuperar todos los indicios borrados por una regla de eliminación

Si por error una regla de eliminación ha movido a la papelera indicios valiosos para los analistas del SOC, sigue los pasos mostrados a continuación para recuperarlos:

- Haz clic en el menú superior **Indicios** y en el icono de la papelera situado en el panel izquierdo. Las reglas de eliminación se mostrarán en forma de árbol dependiendo de los criterios de ordenación y agrupación elegidos.
- En la papelera haz clic en la regla de eliminación asociada al indicio, y en el menú de contexto de la regla en la opción **Mover todos los indicios de esta regla**. Se mostrará un desplegable con los estados disponibles de los indicios eliminados por la regla.
- Selecciona el estado **Pendiente**. Todos los indicios que contenía la regla de eliminación se volverán a incorporar al listado de indicios con el estado elegido.

Mostrar todos los indicios almacenados en la papelera

Haz clic en la opción **Papelera** del panel lateral. El panel central se actualizará con todos los indicios que fueron marcados como eliminados en los últimos 7 días.

Mostrar los indicios eliminados por una regla

Al hacer clic en la opción **Papelera** del panel lateral izquierdo se desplegarán todas las reglas de eliminación creadas por el analista. Haz clic en una regla de eliminación concreta para mostrar los indicios eliminados que han coincidido con los criterios establecidos en esa regla de eliminación en particular.

Guía de buenas prácticas para gestionar indicios

Para que el Nivel 1 de analistas del SoC pueda gestionar los indicios generados por Cytomic Orion en función de su importancia sigue los consejos mostrados a continuación. Para manejar las herramientas de agrupación y filtrado consulta **Herramientas para configurar los listados** en la página **39**.

- Ordena los indicios según su fecha de creación haciendo dos veces clic en el nombre de la columna **Último evento** para mostrar en primer lugar los más recientes.
- Filtra los indicios según su estado para localizar de forma fácil aquellos que tengan estado **Pendiente**.
- Añade una agrupación con la columna **Riesgo**. La agrupación **Crítica** contiene los indicios más peligrosos para la organización y los que es más probable que necesiten ser asignados a una investigación para su posterior revisión.
- Para revisar los indicios generadas por una misma regla de hunting agrúpalos arrastrando la columna **Hunting Rule** a la barra de agrupación. Es muy probable que una misma regla de hunting genere varios indicios relacionados.
- Para revisar las situaciones en las que una misma regla de hunting produce de forma continua un número muy alto de indicios, considera ordenar los registros mediante el campo **Repeticiones última hora**.
- Fíjate en el campo **Detalles** de los indicios ya que contiene una descripción de la regla de Hunting que provocó su creación. Con el nombre y el campo **Detalles** el analista podrá determinar el punto de inicio del triaje o de la investigación. Si este campo no se muestra en el listado de indicios sigue los pasos indicados en **Agregar y quitar columnas** en la página **40**.
- Agrupa las reglas según su técnica y táctica para asignarlas a técnicos especializados en estrategias concretas de ataque.

Capítulo 6

Gestión de Hunting rules

Cytomic Orion analiza el flujo de telemetría enviado por los equipos de la red en busca de patrones de eventos sospechosos de pertenecer a la CKC de un ataque informático. Cada uno de estos patrones se almacena en una Hunting rule, siendo el radar de ciberataques el encargado de compararlas con el flujo de telemetría para generar indicios cuando se produce una concordancia.

En Cytomic Orion las Hunting rules tienen dos posibles orígenes:

- Los analistas de Cytomic y los sistemas automáticos de ML (Machine Learning) analizan de forma continuada el flujo de eventos recibido para crear y probar nuevas Hunting rules. Estas reglas son visibles para todos los clientes de Cytomic Orion.
- Eventualmente, los propios analistas de cada SOC pueden generar sus propias Hunting rules, que serán visibles únicamente para su organización.

CONTENIDO DEL CAPÍTULO

El listado de Hunting rules

Acceso al listado de Hunting rules

Haz clic en el menú superior **Configuración**, panel lateral **Hunting rules**, pestaña **Hunting Rules**. Se mostrará un listado con todas las Hunting rules creadas hasta la fecha.

Permisos requeridos

La cuenta de usuario no requiere permisos especiales para acceder al listado de Hunting rules.

Listado de Hunting rules

Contiene las Hunting rules creadas hasta la fecha, tanto por Cytomic como por los analistas del SOC. El ámbito de actuación de las Hunting rules creadas por los analistas es local al SOC de forma que solo serán visibles por las cuentas de usuario que pertenecen a su SOC.

Campo	Descripción
Nombre	Nombre de la Hunting rule. Los indicios generados por una Hunting rule indicarán su nombre en el campo **Hunting rule** del listado **Indicios**. Consulta **Listado de indicios** en la página **73**.
Riesgo	Importancia del impacto del indicio generado por la Hunting rule: **Crítica**, **Riesgo alto**, **Riesgo medio**, **Riesgo bajo**, **Desconocida**.
Creado por	Cuenta de usuario del SOC que creó la Hunting rule. Si se trata de una regla interna de Cytomic Orion, se mostrará el logotipo de Cytomic.
Propietario	Nombre de la organización a la que pertenece la cuenta de usuario que creó la Hunting rule. Si se trata de una regla interna de Cytomic Orion, se mostrará el logotipo de Cytomic.
Estado	• **Desactivada**: la regla fue desactivada manualmente por el analista y no generará nuevos indicios hasta su reactivación. • **Activada**: el radar de ciberataques inspecciona el flujo de eventos recogido de los equipos del cliente y lo compara con la Hunting rule para generar indicios. • **Desactivada automáticamente**: el radar de ciberataques detectó que la Hunting rule genera demasiados indicios y la desactivó de forma automática para prevenir bajadas de rendimiento. Consulta **Cambiar el estado de una Hunting rule**.

Campo	Descripción
MITRE	Táctica, técnica y subtécnica asociada a la hunting rule, según la especificación MITRE. Si hay más de un par táctica & técnica, se separa con el carácter '#'. Para más información consulta **Panel de detalles** en la página **75**.
Fecha de creación	Fecha en la que fue creada la Hunting rule.
Fecha modificación	Fecha de la última modificación que se realizó sobre la definición de la Hunting rule.
Cambio de estado	Fecha en la que ha producido el último cambio de estado.
Sistemas operativos	Sistemas operativos en los que la Hunting rule busca indicios.

Tabla 6.1: Campos del listado Hunting rules

Gestionar Hunting rules

Visualizar la definición de una Hunting rule

Haz clic en el nombre de una Hunting rule para mostrar el asistente de creación de reglas. Si el analista tiene permisos suficientes, podrá modificar los parámetros de la regla; en caso contrario todos los controles se muestran desactivados. Consulta **Gestionar Hunting rules**.

Exportar el listado de Hunting rules

Para descargar el listado de Hunting rules en un fichero excel haz clic en el icono situado en la parte superior derecha de la ventana. Consulta **Listado de Hunting rules** para obtener información sobre el significado de los campos incluidos en el fichero excel.

Buscar Hunting rules

Para realizar una búsqueda sobre el campo **Nombre** utiliza la caja de texto **Buscar** situada en la parte superior del listado de Hunting rules. Se admiten búsquedas parciales.

Ordenar Hunting rules

Para ordenar y agrupar el contenido de los campos del listado utiliza los recursos descritos en **Herramientas para configurar los listados** en la página **39** .

Actualizar el listado de Hunting rules

Para reflejar los cambios producidos en las Hunting rules listadas, o mostrar las nuevas altas o bajas, haz clic en el icono ↻ situado en la parte superior derecha de la ventana.

Cambiar el estado de una Hunting rule

> *La cuenta de usuario utilizada para acceder a la consola de análisis deberá tener asignado el permiso **Gestión de Hunting Rules**. Consulta **Descripción de los permisos implementados** en la página **60** para obtener más información sobre permisos y roles.*

- Haz clic en las casillas de selección de las reglas que quieres cambiar el estado
- Haz clic en el botón **Activar** o **Desactivar** de la barra de herramientas situada en la parte superior de la ventana. Las reglas afectadas cambiaran su estado indicado en el campo **Estado** del listado.

Desactivación automática de una Hunting rule

Para que Cytomic Orion desactive automáticamente una Hunting rule debe cumplirse por lo menos una de las dos condiciones siguientes:

- La Hunting rule impacta de forma significativa en el rendimiento del Radar de ciberataques.
- La Hunting rule genera una gran cantidad de indicios.

Si una Hunting rule consume muchos recursos, Cytomic Orion la desactivará automáticamente. En tal caso se ejecutarán las siguientes acciones:

- Se mostrará un aviso en la parte superior de la pantalla indicando que algunas regla se han desactivado automáticamente.
- Se actualizará el estado de las reglas desactivadas a **Desactivada automáticamente**.
- Cytomic Orion enviará un correo electrónico cada lunes con una relación de las Hunting rules detenidas en la semana anterior. El correo se envía a las cuenta de SOC que tengan asignado alguno de los permisos siguientes:
    - Gestionar Hunting Rules.
    - Crear Hunting Rules y reglas de notificación sobre todos los clientes.
    - Crear reglas de notificación de indicios.

Haz clic en el enlace **Ver Hunting rules detenidas** del aviso para mostrar unicamente las reglas detenidas de forma automática por Cytomic Orion.

Gestionar Hunting rules

Acceso al listado de Hunting rules

Haz clic en el menú superior **Configuración**, panel lateral **Hunting rules**, pestaña **Hunting Rules**. Se mostrará un listado con todas las Hunting rules creadas hasta la fecha.

Permisos requeridos

La cuenta de usuario utilizada para acceder a la consola de análisis, deberá tener asignado el permiso **Gestión de Hunting Rules**. Consulta**Gestión de Hunting rules** para más información.

Un analista únicamente puede crear Hunting rules que inspeccionen los eventos generados por los equipos de los clientes sobre los que tenga visibilidad. Para simplificar la gestión de roles, Cytomic Orion incorpora el permiso **Crear Hunting Rules y reglas de notificación sobre todos los clientes** que permite crear Hunting rules sin importar la visibilidad de la cuenta utilizada. Para obtener más información sobre permisos y roles, consulta **Descripción de los permisos implementados** en la página **60**.

Crear una Hunting rule

- Haz clic en el enlace **Añadir Hunting rule** o en el icono + situado en la parte superior derecha de la ventana. Se mostrará el asistente de creación de reglas.
- Escribe los datos mostrados a continuación:

Campo	Descripción
Nombre	Nombre de la Hunting rule. Los indicios generados por una Hunting rule incluirán su nombre en el campo **Hunting rule** del listado **Indicios**. Consulta **Listado de indicios** en la página **73**.
Descripción	Notas del analista asociadas a la Hunting rule.
Estado	• **Desactivada**: la regla está desactivada manualmente por el analista y no generará nuevos indicios hasta su reactivación. • **Activada**: el radar de ciberataques inspecciona el flujo de eventos recogido de los equipos del cliente y lo compara con la Hunting rule para generar indicios.
Riesgo	Importancia del impacto del indicio generado por la Hunting rule: **Crítica**, **Riesgo alto**, **Riesgo medio**, **Riesgo bajo**, **Desconocida**.
MITRE	Táctica, técnica y subtécnica asociada a la hunting rule, según la

Campo	Descripción
	especificación MITRE. Una misma hunting rule puede tener asociada varias tácticas, técnicas y subtécnicas. Haz clic en los iconos ⊕ y ⊖ para añadir o quitar tácticas. Se requiere que cada táctica tenga siempre una técnica asociada, pero una técnica puede no tener definida una subtécnica. Para más información consulta **Panel de detalles** en la página **75**
Clientes	Indica los clientes cuyo flujo de eventos será inspeccionado por la Hunting rule. • **Todos los clientes**: se muestra solo si la cuenta del analista tiene asignado el rol **Crear Hunting Rules sobre todos los clientes**. • **Los siguientes clientes**: añade clientes copiando y pegando una lista separada por comas, o mediante la ventana de clientes que se muestra al hacer clic en el icono ⊕. • **Todos los clientes excepto estos**: se muestra solo si la cuenta del analista tiene asignado el rol **Crear Hunting Rules sobre todos los clientes**. Añade clientes para excluir copiando y pegando una lista separada por comas, o mediante la ventana de clientes que se muestra al hacer clic en el icono ⊕.
Sistemas Operativos	Limita la búsqueda de la Hunting rule a los sistemas operativos indicados.

Tabla 6.2: Campos de una Hunting rule

- Define la Hunting rule con el asistente de consultas.
- Ejecuta el proceso de validación para comprobar que la Hunting rule no impacta en el rendimiento del Radar de ciberataques. Consulta **Validar una Hunting rule**.

Una vez creada, el Radar de ciberataques comenzará a comparar de forma inmediata la telemetría recibida con la nueva Hunting rule.

Estructura general del asistente

Los bloques utilizados para construir una Hunting rule con el asistente son los siguientes:

- **Tipo (1)**: es el tipo de eventos que se buscarán en el flujo de telemetría analizado por la Hunting rule. Equivale a la cláusula `FROM [tabla]` de SQL. En el desplegable se listan las tablas mostradas en **Tablas (1)** en la página **157**.

- **Condición (2)**: equivale a la clausula `WHERE` de la sentencia SQL. Consulta más adelante para una descripción en detalle de esta cláusula.
- **Información del indicio (3)**: indica el contenido de los campos que se añadirán al indicio cuando éste sea generado por la Hunting rule.

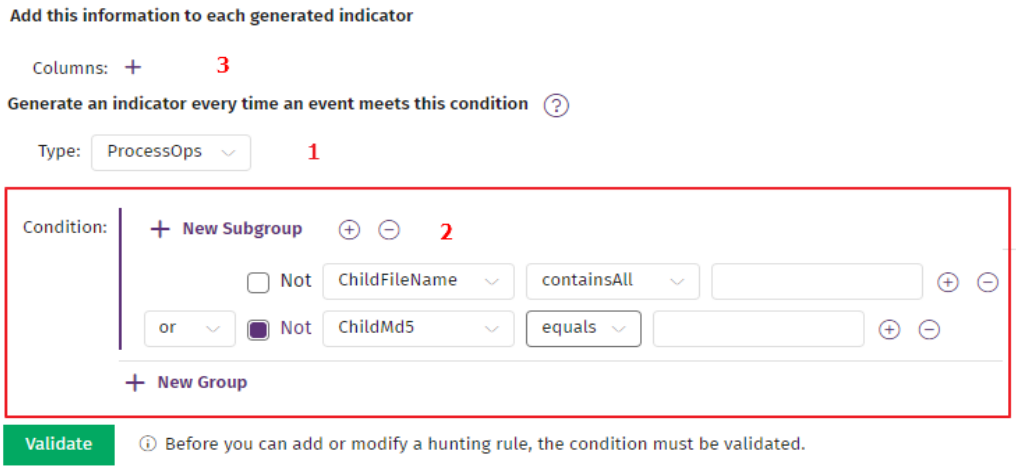


Figura 6.1: Bloques principales del constructor de consultas

Estructura del bloque Condición

El bloque **Condición** equivale a la clausula `WHERE` de SQL y admite un alto grado de flexibilidad a la hora de especificar las condiciones de búsqueda.

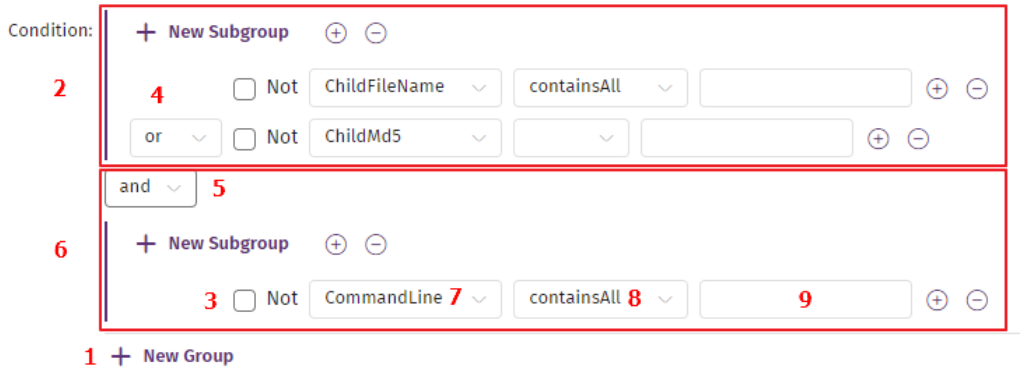


Figura 6.2: Estructura del bloque Condición con dos grupos relacionados por el operador lógico AND

El bloque **Condición** se divide en grupos de condiciones. Dentro de un grupo de condiciones puede haber una única condición (bloque **(6)**) o varias (bloque **(2)**).

Condiciones

Una condición simple **(6)** está formada por el nombre de una columna **(7)**, un operador de comparación **(8)** (consulta **Operadores de comparación**)y el valor a comparar **(9)** . Adicionalmente, puede tener asociado un operador booleano de negación **(3)**.

Una condición compuesta **(2)** está formada por varias condiciones simples que se relacionan entre sí mediante los operadores AND y OR **(4)**.

Grupos

Cada nuevo grupo creado es equivalente a introducir una condición simple o compuesta rodeada de paréntesis en la clausula `WHERE` de la sentencia SQL correspondiente.

Se pueden crear varios grupos con el botón **Nuevo grupo (1)** que se relacionarán entre sí mediante un operador lógico AND / OR **(5)**.

A su vez, dentro de un grupo se pueden crear uno o más grupos de condiciones simples o compuestas mediante los botones **Nuevo grupo (10)** de segundo nivel.

Operadores de comparación

- **ContainsAny**: operador equivalente al "like" de SQL, busca una subcadena de caracteres.
- **equals**: busca una cadena de caracteres exacta.
- **endsWithAny**: busca una subcadena de caracteres al final de la cadena.
- **startsWithAny**: busca una subcadena de caracteres al inicio de la cadena.
- **containsInOrder** : busca hasta 3 subcadenas de caracteres en el orden indicado. Especificar una única cadena es equivalente a la opción **ContainsAny**. Se mostrarán los resultados que contengan todas las cadenas especificadas (operador lógico AND) y en el orden establecido.
- **Operadores booleanos**: se admiten los operadores logicos básicos ('<','>','>=','<=',==')
- **matches** : permite escribir una expresión regular en formato java. Para obtener más información sobre el formato de las expresiones regulares, los caracteres de escape y otros detalles de la implementación RegEx en Java consulta **https://docs.oracle.com/javase/8/docs/api/java/util/regex/Pattern.html.**

Búsquedas sensibles a mayúsculas

Por defecto, todas las condiciones de tipo cadena de caracteres se establecen sin tener en cuenta mayúsculas y minúsculas ("case insensitive"), pero el analista puede cambiar este comportamiento estableciéndolo en el desplegable asociado.

Figura 6.3: Desplegable para establecer el tipo de comparación en campos de tipo cadenas de caracteres

Los campos **ParentFilename** y **ChildFilename** se almacenan en el océano de datos en minúsculas, ya que se extraen de los campos **ParentPath** o **ChildPath** respectivamente. Después de la extracción, se ejecuta de forma automática un proceso de normalización en el que se cambian todas las mayúsculas por minúsculas. Cualquier Hunting rule donde se especifique "case sensitive" y utilice letras en mayúsculas para buscar en **ParentFilename** o **ChildFilename** no devolverá ningún resultado. Sin embargo, los campos **ParentPath** o **ChildPath** no sufren este proceso de normalización, y se almacenan en el océano de datos tal cual. En este caso sí tiene sentido utilizar "case sensitive" o "case insensitive" según las necesidades del analista.

Validar una Hunting rule

Para evitar que Cytomic Orion desactive las Hunting rules definidas por los analistas debido a una sobrecarga del Radar de ciberataques, es necesario probar las reglas diseñadas antes de almacenarlas en la plataforma. El proceso de verificación ejecuta la Hunting rule sobre el océano de datos de los clientes del SOC limitado a los últimos siete días y comprueba el número de indicios generados. En función del numero de indicios genera un código de color y permite o impide guardar la Hunting rule en la plataforma.

Es necesario ejecutar el proceso de validación cada vez que se crea una Hunting rule o se modifica una existente:

- Una vez definida o modificada la Hunting rule haz clic en el botón **Validar**. Se ejecutará un test interno que comprobará el número de indicios diarios que genera la regla.
- Si la Hunting rule genera muchos indicios, el botón **Guardar** se deshabilita impidiendo salvarla.
- Modifica la Hunting rule hasta que supere el test y haz clic en el botón **Guardar**.

Códigos de color y rangos de indicios encontrados

- **Rojo**: al menos un día de la semana ha superado los 100 indicios. Se requiere modificar la definición de la Hunting rule y repetir la validación hasta obtener un resultado naranja o verde.
- **Naranja**: al menos un día de la semana está entre 80 y 100 indicios. Se advierte de que la Hunting rule podría ser desactivada a lo largo del tiempo por el Radar de ciberataques ya que está cerca del límite de 100 indicios. Al hacer clic en el botón **Aceptar y continuar** se habilitará el botón **Guardar**.
- **Verde**: todos los días de la semana quedan por debajo de los 80 indicios. Las probabilidades de que el Radar de ciberataques desactive la regla a lo largo del tiempo son muy bajas. Se habilita el botón **Guardar** directamente.

Editar una Hunting rule

- Para abrir el asistente de consultas, haz clic en el nombre de la Hunting rule. Solo se pueden editar las reglas diseñadas por los técnicos del SOC. Las reglas creadas por Cytomic no mostrarán su definición.
- Para asignar nuevos valores a la definición de la Hunting rule, consulta **Crear una Hunting rule**.
- Una vez finalizada la edición, es necesario validar la Hunting rule antes de guardarla. Consulta **Validar una Hunting rule**.
- Haz clic en el botón **Guardar**. Los cambios se aplicarán en el momento y el Radar de ciberataques actualizará los patrones que busca en la telemetría recibida de los equipos.

> *No se permite guardar una hunting rule modificada que haga referencia a técnicas, tácticas o subtécnicas que estén en desuso. Si una técnica, táctica o subtécnica MITRE asociada a la hunting rule en edición está en desuso, la consola la resaltará mediante un recuadro rojo. Sin embargo, una hunting rule sí puede ser activada o desactivada haciendo referencia a técnicas, tácticas o subtécnicas que estén en desuso.*

Borrar una Hunting Rule

- Selecciona las casillas de las Hunting rules que quieres borrar.
- Haz clic con el botón derecho del ratón y selecciona **Eliminar**, o haz clic en la barra de acciones **Eliminar**.

Reglas de notificación por correo electrónico

Una regla de notificación envía los indicios detectados en los equipos de uno o más clientes a una o varias cuentas de correo. De esta forma se evita que el analista tenga que acceder una y otra vez a la consola de análisis para comprobar el estado del parque informático de los clientes que investiga.

Acceso al listado de Notificaciones por correo electrónico

Haz clic en el menú superior **Configuración**, panel lateral **Hunting rules**, pestaña **Notificaciones por correo electrónico**. Se mostrará un listado con todas las Hunting rules creadas hasta la fecha.

Permisos requeridos

La cuenta de usuario utilizada para acceder a la consola de análisis deberá tener asignado el permiso **Crear reglas de notificación de indicios**, y disponer de visibilidad sobre los clientes que generan las notificaciones.

Para simplificar la gestión de roles, Cytomic Orion incorpora el permiso **Crear Hunting Rules y reglas de notificación sobre todos los clientes**, que permite crear reglas de notificación independientemente de la visibilidad de la cuenta utilizada. Para obtener más información sobre permisos y roles, consulta **Descripción de los permisos implementados** en la página **60**.

Crear una regla de notificación

Un analista puede crear regla de notificación tanto sobre las Hunting rules creadas en el SOC / MSSP al que pertenece como sobre las publicadas por Cytomic.

- Haz clic en el menú superior **Configuración**, panel lateral **Hunting rules** y en la pestaña **Notificaciones por correo electrónico**. Se abrirá una ventana con todas las reglas de notificación creadas por el analista.
- Haz clic en el botón **Añadir notificación** situado en la parte superior derecha de la ventana. Se mostrará el panel **Añadir notificación.**
- Escribe en los campos siguientes del panel:
    - **Nombre**: nombre de la regla de notificación a crear.
    - **Descripción**: texto explicativo asociado a la regla.
    - **Notificar indicios detectados en equipos de los siguientes clientes**: indica los clientes afectados por la nueva regla de notificación:
    - Selecciona **Todos los clientes** si la cuenta del analista tiene asignado el permiso **Crear Hunting Rules y reglas de notificación sobre todos los clientes** (consulta **Descripción de los permisos implementados** en la página **60**) .
    - Selecciona **Los siguientes clientes** y añade los clientes con el icono ⊕ si la regla de notificación afecta a los indicios generados en clientes específicos. La cuenta del analista debe tener visibilidad sobre esos clientes (consulta **Configuración de la visibilidad de clientes** en la página **55**). Este campo permite pegar un listado de clientes separado por el carácter ",".
    - **Notificar indicios generados por las siguientes Hunting Rules**: indica las Hunting rules que serán monitorizadas.
    - Selecciona **Todas las Hunting rules** si quieres monitorizar todas las Hunting rules creadas en el SOC.
    - Selecciona **Todas las Hunting rules de los siguientes niveles de riesgo** si quieres monitorizar solo las Hunting rules de un determinado nivel de riesgo.
    - Selecciona **Las siguientes Hunting rules** si quieres monitorizar Hunting rules concretas.
    - **Notificar en las siguientes direcciones de correo electrónico**: indica las direcciones que recibirán los correos electrónicos que contienen los indicios generados por las Hunting rules configuradas para su monitorización.
    - **Límite de notificaciones**: indica el número de correos electrónicos enviados por unidad de tiempo.

Editar regla de notificación

Para editar una regla de notificación, el analista tiene que tener visibilidad sobre todos los clientes asociados con la regla.

Haz clic en la regla de notificación a editar. Se mostrará la ventana **Editar notificación**. Para obtener una descripción de los campos de la regla de notificación, consulta **Crear una regla de notificación**.

Listado de reglas de notificación

Haz clic en el menú superior **Configuración**, panel lateral **Hunting rules** y en la pestaña **Notificaciones por correo electrónico**. Se mostrará una ventana con todas las reglas de notificación creadas por el analista y su información asociada:

- **Nombre**: nombre de la regla de notificación.
- **Destinatarios**: número de direcciones de correo electrónico que recibirán las notificaciones.
- **Límite de notificaciones**: número de correos electrónicos enviados por la unidad de tiempo elegida.

Gestión del listado de reglas de notificaciones

Buscar, filtrar y ordenar regla de notificación

Para ordenar, buscar, filtrar o agrupar reglas de notificación, consulta **Herramientas para configurar los listados** en la página **39**.

Borrar reglas de notificación

Haz clic en las casillas de selección asociadas a las reglas de notificación que quieres borrar y en el icono de la barra de herramientas.

Información enviada por correo electrónico a los destinatarios de la notificación

Campo	Descripción
De	Remitente del correo electrónico.
Enviado el	Fecha y hora de envío del correo electrónico.
Asunto	Indicio de tipo "nombre de la Hunting rule asociada a la notificación" en el cliente "nombre del cliente".
Hunting rule	Nombre de la regla de Hunting que generó el indicio, y descripción de los artefactos que monitoriza en el equipo del cliente.
Sistema operativo	Lista de sistemas operativos separados por comas que generaron el indicio.

Campo	Descripción
Fecha indicio	Fecha en la que se generó el indicio.
Último evento	Fecha en la que se registró en el equipo del usuario o servidor el último evento que desencadenó la generación del indicio. Esta fecha puede no coincidir con **Fecha indicio** si se produjo un retraso al generar el indicio, como por ejemplo debido a una interrupción en la conexión entre el servidor de Cytomic Orion y el equipo del cliente.
Repeticiones última hora	Número de veces que Cytomic Orion generó el mismo indicio en la última hora.
ID cliente	Identificador único del cliente al que pertenece el equipo involucrado en el indicio.
Equipo	Nombre del equipo del cliente involucrado en el indicio.
MUID	Identificador único del equipo del cliente involucrado en el indicio.
Riesgo	Importancia del impacto del indicio detectado: **Crítica**, **Riesgo alto**, **Riesgo medio**, **Riesgo bajo**.
MITRE	Categoría de la técnica y táctica de la Hunting rule mapeada según la especificación MITRE.
Detalles	Contenido de los campos relevantes del evento que generó el indicio

Tabla 6.3: Descripción de los campos del correo electrónico enviado por la regla de notificación

Notificaciones por cambios en el modelo MITRE

Cytomic Orion descarga el modelo de técnicas, tácticas y subtécnicas MITRE dos veces al día. Si se detecta un cambio en este esquema que implique eliminar alguna técnica o táctica, se comprobarán Cytomic Oriontodas las hunting rules creadas hasta el momento para verificar que sus técnicas y tácticas asociadas estén en vigor.

Los usuarios de Cytomic Orion reciben una notificación por correo electrónico cada lunes con las hunting rules que se requieren actualizar si cumplen las condiciones siguientes:

- La cuenta de usuario tiene asignados al menos uno de los permisos siguientes:
    - Gestionar Hunting Rules.
    - Crear Hunting Rules y reglas de notificación sobre todos los clientes.
    - Crear reglas de notificación de indicios.
- Al menos una técnica, táctica o subtécnica MITRE asociada a una hunting rule está en desuso.

Para obtener más información sobre los permisos asociados a una cuenta de usuario consulta ***Gestión de roles y permisos*** *en la página* ***58****.*

Adicionalmente, cuando Cytomic Orion descargue un modelo MITRE actualizado y detecte una táctica o técnica en desuso relacionada con una hunting rule, se mostrará en la parte superior de la consola una notificación durante 12 horas indicando el nombre de la hunting rule afectada.

Capítulo 7

Gestión de investigaciones

Cytomic Orion implementa un repositorio donde se registran y almacenan de forma automática todos los hallazgos descubiertos por los técnicos del SOC a lo largo de un análisis. Este recurso recibe el nombre de "Investigación".

En su mayor parte, los analistas de nivel 1 que previamente han hecho el triaje de indicios crean las investigaciones. Si existen elementos suficientes como para sospechar de la existencia de un ciberataque, el analista creará una nueva investigación que agrupe los indicios relacionadas con dicho ataque. De esta manera, los técnicos de nivel 2 dispondrán de un marco de estudio bien definido y un entorno donde compartir toda la información generada.

Cada una de las acciones ejecutadas por los técnicos del SOC en el marco de una investigación quedarán guardadas para su posterior consulta. De esta forma, es posible llevar un control del consumo de datos derivado de las actividades de investigación, y de los accesos a los equipos de los clientes del SOC efectuadas por los analistas, entre otros elementos.

CONTENIDO DEL CAPÍTULO

El listado de investigaciones

Acceso al listado de investigaciones

Haz clic en el menú superior **Investigaciones**. Se mostrará un listado con todas las investigaciones creadas hasta la fecha, su información asociada y herramientas de búsqueda y gestión.

Una investigación se mostrará en el listado si la cuenta de usuario con la que el analista ha accedido a la consola web tiene visibilidad sobre todos los clientes implicados en esa investigación. En caso contrario no será visible para el analista.

Listado de investigaciones

Se muestra una ventana dividida en varias secciones:

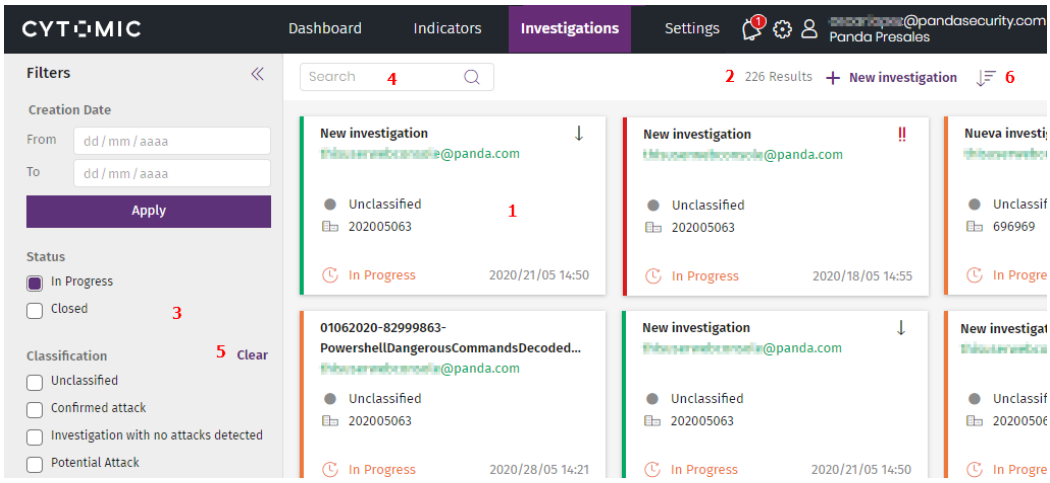


Figura 7.1: Vista general del listado de investigaciones

- **Panel de investigaciones (1)**: contiene una colección de tarjetas, cada una de ellas se corresponde con una investigación ya creada. Para conocer la información mostrada en cada tarjeta consulta **Formato de una tarjeta Investigación**.
- **Panel de filtrado (3)**: ayuda al analista seleccionar las investigaciones de su interés. Consulta **Filtrar investigaciones**
- **Búsqueda (4)**: localiza investigaciones por su nombre. Consulta **Buscar investigaciones**

- **Ordenar listado (6)**: muestra la lista de investigaciones según el criterio de ordenación elegido.
- **Crear una nueva investigación (2)**: muestra el asistente para generar una nueva investigación. Consulta **Crear una investigación**

Formato de una tarjeta Investigación

Por cada investigación se muestra una tarjeta con la información siguiente:

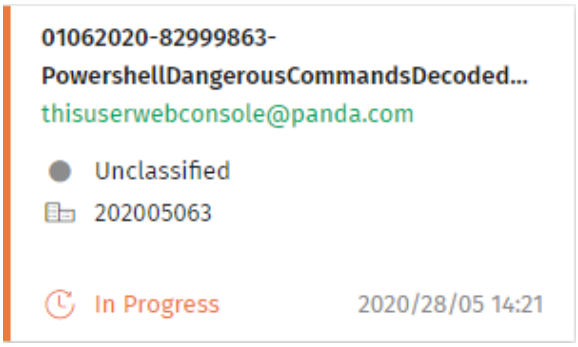


Figura 7.2: Formato de una tarjeta de investigación

- **Nombre (1)**: Cytomic Orion establece como nombre inicial la cadena de caracteres "nueva investigación".
- **Usuario (2)**: cuenta de usuario asignada a la investigación. En verde si coincide con la cuenta de usuario que accede a la consola, en gris si es otra cuenta de usuario.
- **Clasificación (3)**: indica cómo está catalogada la investigación:
  - **Sin clasificar** ●: investigación pendiente de analizar.
  - **Ataque confirmado** ●: la investigación de los indicios desembocó en la detección de un ataque.
  - **Investigación sin ataques detectados** ●: la investigación de los indicios no detectó ningún ataque.
  - **Ataque potencial** ●: la investigación de los indicios no es concluyente, pero se ha determinado una alta probabilidad de desembocar en un ataque.
- **Clientes (4)**: nombre de los clientes asignados a la investigación. Si la cuenta que accede a la consola web no tiene permisos suficientes se mostrará su identificador.
- **Estado (5)**:
  - **En curso**: la investigación continua abierta.
  - **Cerrada**: la investigación se ha dado por concluida. La tarjeta se muestra atenuada (en gris).
- **Fecha de inicio (6)**: fecha y hora en la que se creó la investigación.

- **Prioridad**: se indica la prioridad de la investigación mediante un código de color que se aplica en los bordes de la tarjeta, y con un icono en la parte superior derecha de la tarjeta.
    - **Critico** ‼: el peligro detectado en la investigación de los indicios es muy alto. El código de color asignado es el rojo.
    - **Alta** ❗: el peligro detectado en la investigación de los indicios es alto. El código de color asignado es el naranja.
    - **Media**: el peligro detectado en la investigación de los indicios es medio. El código de color asignado es el verde.
    - **Baja** ↓: el peligro detectado en la investigación de los indicios es bajo. El código de color asignado es el gris.

Buscar, ordenar y filtrar investigaciones

Buscar investigaciones

Utiliza la caja de texto (**4**) situada en la parte superior del panel de investigaciones para buscar sobre el atributo **Nombre**. Se admiten búsquedas parciales.

Filtrar investigaciones

En el panel lateral izquierdo (**3**) se muestran varias herramientas de filtrado:

- **Fecha de creación**: muestra las investigaciones creadas dentro del rango indicado en los controles **Desde** y **Hasta**. Introduce las fechas y haz clic en el botón **Aplicar** para actualizar el listado.
- **Estado** : muestra las investigaciones según su estado **En curso** (abierto) o **Cerrada** (finalizado).
- **Clasificación**: filtra por cómo está catalogada la investigación (**Sin clasificar**, **Ataque confirmado**, **Investigación sin ataques detectados**, **Ataque potencial**). Consulta **Subpanel descripción (3)** para obtener más información acerca de la clasificación de una investigación.
- **Prioridad**: filtra por el impacto que el posible ataque investigado pueda tener en los activos de la empresa (**Sin establecer**, **Crítico**, **Alta**, **Media**, **Baja**). Consulta **Subpanel descripción (3)** para obtener más información acerca de la prioridad de una investigación.
- **Asignada a**: muestra las investigaciones asignadas a uno o varios analistas. Al seleccionar este filtro, en primer lugar se mostrarán las investigaciones asignadas al propio analista, después aquellas sin asignar y, finalmente, las investigaciones asignadas a otras cuentas de usuario ordenadas alfabéticamente por su nombre.
- **Creado por**: muestra las investigaciones creadas por uno o varios analistas.

- **Clientes**: muestra las investigaciones que involucran a determinados clientes del MSSP / MDR.

Para restablecer un criterio de filtrado haz clic en el enlace **Limpiar**.

Ordenar investigaciones

Haz clic en el icono (**6**) para desplegar un panel con los atributos de las investigaciones que se utilizarán como criterios de ordenación del listado. Adicionalmente, podrás elegir si el criterio de ordenación elegido es ascendente o descendente.

Crear una investigación

Para crear una investigación nueva sin indicios asignados:

- Haz clic en el botón **Nueva investigación** situado en la parte superior derecha de la ventana **(2)**. Se mostrará un listado de los clientes accesibles por la cuenta de usuario que crea la investigación.
- Selecciona los clientes que forman parte de la investigación y haz clic en el botón **Aceptar**. Se creará una nueva investigación sin indicios y con los clientes asignados.

Para crear una investigación y asignar uno o varios indicios a la misma:

- Consulta **Asignar y retirar indicios a investigaciones manualmente**.

Asignar y retirar indicios a investigaciones manualmente

Un indicio solo se puede asignar a una única investigación. Por lo tanto, un indicio con una investigación ya asignada no podrá asignarse a otra investigación, a no ser que previamente sea desasignado de ésta o movido.

Solo se pueden asignar indicios a investigaciones si éstos no han sido previamente excluidos mediante una regla de eliminación. Consulta **Eliminar indicios de forma manual** en la página **77**.

Crear una nueva investigación que contenga uno o varios indicios

- Haz clic en el menú superior **Indicios** y en las casillas de selección de los indicios con estado **Pendiente** que se asignarán a la nueva investigación.
- Haz clic en el botón **Investigar Indicio** situado en la barra de herramientas o haz clic con el botón de la derecha en el indicio para mostrar el menú de contexto y selecciona la opción **Investigar indicio**. Se creará una nueva investigación a la que se le asignarán los indicios elegidos y un nombre generado automáticamente.

o

- Haz clic en las casillas de selección de los indicios con estado **Pendiente** que se asignarán a la nueva investigación.
- Haz clic en el menú de contexto situado junto a la casilla de selección o con el botón de la derecha en cualquier campo del indicio para mostrar un menú desplegable. Selecciona la opción **Investigar indicio**.

Añadir inicios a una investigación ya existente

- Haz clic en el menú superior **Indicios** y en las casillas de selección de los indicios con estado **Pendiente** que se asignarán a la nueva investigación.
- Haz clic en el botón **Añadir a investigación existente** en la barra de herramientas, o haz clic con el botón de la derecha del ratón en el indicio para mostrar el menú de contexto y elige **Añadir a investigación existente**.
- Se mostrará una ventana con un listado que contiene las investigaciones creadas, y una caja de búsqueda que permite localizar investigaciones según el contenido de los campos del listado:
    - **Id**: Identificador interno de la investigación.
    - **Nombre**: nombre de la investigación asignado por el analista.
    - **Estado**: estado de la investigación. Consulta **Formato de una tarjeta Investigación**.
    - **Clasificación**: clasificación de la investigación. Consulta **Formato de una tarjeta Investigación**
    - **Asignada a**: cuenta de usuario de la consola de análisis que tiene asignada la investigación.
- Con las casillas de selección elige la investigación a la que se asignará el indicio y haz clic en **Aceptar**.

o

- Haz clic en las casillas de selección de los indicios con estado **Pendiente** que se asignarán a la investigación.
- Haz clic en el menú de contexto situado junto a la casilla de selección o con el botón de la derecha en cualquier campo del indicio para mostrar un menú desplegable. Selecciona la opción **Añadir a una investigación**.

Una vez asignada un indicio en estado **Pendiente** a una investigación, éste pasará a estado **En curso** hasta que sea cerrado, momento en que el indicio tomará el estado **Finalizado**.

Desasignar indicios de investigaciones

El analista puede desasignar indicios desde el listado de indicios o desde la investigación asignada al indicio.

Selecciona los indicios con las casillas de selección dentro del panel de indicios y haz clic en el botón **Quitar de esta investigación**. También tienes acceso a esta opción haciendo clic con el botón derecho del ratón para mostrar el menú de contexto.

Mover indicios entre investigaciones

Mover un indicio implica desasignarlo de una investigación y asignarlo a otra investigación diferente en un único paso:

- En el menú superior **Investigaciones** haz clic en la investigación que contiene el indicio a mover.
- Selecciona los indicios con las casillas de selección dentro del panel de indicios, y haz clic en el botón **Mover a otra investigación** de la barra de herramientas, o haz clic con el botón derecho del ratón para mostrar el menú de contexto.
- Se mostrará una ventana con un listado que contiene las investigaciones creadas, y una caja de búsqueda que permite localizar investigaciones según el contenido de los campos del listado:
    - **Id**: Identificador interno de la investigación.
    - **Nombre**: nombre de la investigación asignado por el analista.
    - **Estado**: estado de la investigación. Consulta **Formato de una tarjeta Investigación**.
    - **Asignada a**: cuenta de usuario de la consola de análisis que tiene asignada la investigación.
- Selecciona la investigación destino en la ventana de listado de investigaciones y haz clic en el botón **Aceptar**.

Mover indicios desde una investigación a otra nueva

En caso de no querer desasignar un indicio antes de asignarlo a una investigación nueva, el analista puede crear una investigación y mover el indicio en un único paso:

- En el menú superior **Investigaciones**, haz clic en la investigación que contiene el indicio a asignar, o en el menú superior **Indicios**, haz clic en el panel lateral **En curso** para mostrar todos los indicios asignados a investigaciones.
- Dentro del panel de indicios, selecciona los indicios mediante las casillas de selección . En la barra de herramientas haz clic en el botón **Añadir a una nueva investigación**, o haz clic con el botón derecho del ratón para mostrar el menú de contexto. Se creará una investigación nueva y se asignarán automáticamente los indicios seleccionados.

Asignar y retirar indicios a investigaciones automáticamente

Cytomic Orion permite asignar indicios a investigaciones de forma automática mediante reglas de asignación.

Acceso al listado de Regla de asignación

Selecciona el menú superior **Configuración** y haz clic en el panel lateral **Reglas de asignación**. Se mostrará un listado con todas las reglas de asignación creadas hasta el momento.

Permisos requeridos

Para poder acceder al listado de reglas de asignación, la cuenta de usuario utilizada deberá tener asignado el permiso **Gestionar reglas de asignación automática de indicios** .

Crear una regla de asignación

Un analista puede crear reglas de asignación que aceleren las primeras etapas del triaje de indicios. De esta forma, según las características de los indicios generados por el radar de ciber ataques, éstos se asignarán de forma automática a la investigación elegida por el analista.

Para crear una regla de asignación:

- Selecciona el menú superior **Indicios** y en el panel lateral haz clic en **Pendientes**. Se abrirá una ventana con todos los indicios generados por el radar de ciber ataques que todavía no han sido asignados a una investigación.
- Haz clic en el botón **Añadir regla de asignación automática** en la barra de herramientas, o haz clic con el botón de la derecha del ratón en el indicio para mostrar el menú de contexto y elige **Añadir regla de asignación automática**. Se abrirá una ventana para definir las condiciones que el indicio tendrá que cumplir para aplicarse la regla de asignación:
  - **Investigación**: establece la investigación que recibirá los indicios que satisfagan las condiciones indicadas en la regla. Haz clic en el icono  , se abrirá una nueva ventana con un listado de todas las investigaciones ya creadas. Elige una y haz clic en el botón **Aceptar**.
  - **Nombre de la regla**: nombre de la regla de asignación.
  - **Descripción**: texto explicativo asociado a la regla de asignación.
  - **Id. de cliente**: la regla se aplica sobre los indicios detectados en el parque de la lista de clientes indicados. Se requiere que la cuenta del analista tenga visibilidad sobre los clientes que añade. Consulta **Gestión de roles y permisos** en la página **58**.
  - **Hunting rule**: la regla se aplica sobre los indicios generados por el radar de ciber ataques que fueron detectados con la hunting rule indicada.

- **MUID**: la regla se aplica sobre los indicios detectados en la lista de equipos de usuario con los identificadores indicados.
- **Nombre de equipo**: la regla se aplica sobre los indicios detectados en los equipos de usuario con los nombres indicados.
- **Detalles**: permite especificar el contenido del campo **Detalles** de los indicios a asignar. Establece el contenido del campo exacto con la opción **Igual a**, o de forma flexible mediante una expresión regular con la opción **RegEx**. Para más información consulta **Expresiones regulares** en la página **275**.
- **Ejecutar esta regla automáticamente**: al crear la regla, ésta se aplicará no solo a los indicios que se creen en el futuro sino también a los indicios ya generados en el intervalo de 7 días desde el momento de la creación de la regla.

Editar una regla de asignación

Para editar una regla de asignación, la cuenta del analista tiene que tener asignada una visibilidad que incluya a todos los clientes afectados por la regla a editar. Consulta **Gestión de roles y permisos** en la página **58**.

- Selecciona el menú superior **Configuración** y en el panel lateral haz clic en **Reglas de asignación**. Se mostrará un listado con todas las reglas de asignación creadas hasta el momento.
- Haz clic en una regla de asignación. Se mostrará una ventana con las propiedades de la regla.
- Modifica las propiedades de la regla de asignación y haz clic en el botón **Guardar**.

Una vez editada la regla de asignación, se comenzará a aplicar sobre los nuevos indicios generados. Los indicios anteriores no son tratados por la regla de asignación modificada. Si quieres aplicar la regla de asignación a los indicios generados en el pasado consulta **Ejecutar manualmente una regla de asignación**.

Ejecutar manualmente una regla de asignación

Para aplicar una regla de asignación sobre los indicios generados en los últimos 7 días:

- Selecciona el menú superior **Configuración** y en el panel lateral haz clic en **Reglas de asignación**. Se mostrará un listado con todas las reglas de asignación creadas hasta el momento.
- Selecciona las casillas asociadas a una o varias reglas de asignación. Se activará la barra de herramientas.
- Haz clic en **Ejecutar regla**. Las reglas seleccionadas se aplicarán sobre los indicios generados los últimos 7 días y éstos se moverán a las investigaciones apropiadas.

Listado de reglas de asignación

Contiene las reglas de asignación creadas hasta la fecha.

Para acceder al listado de reglas de asignación selecciona en el menú superior **Configuración** y en el panel lateral haz clic en **Reglas de asignación**. El listado mostrará los campos siguientes:

Campo	Descripción
Nombre	Nombre de la regla de asignación.
Fecha de creación	Fecha en la que fue creada la regla de asignación.
Fecha de modificación	Fecha en la que fue modificada por última vez la regla de asignación.
Descripción	Descripción de la regla de asignación.
Hunting rule	Hunting rule asociada a la regla de asignación.
Investigación	Nombre de la investigación a la que se moverán los indicios que cumplan las condiciones definidas en la regla de asignación.

Tabla 7.1: Campos del listado Reglas de asignación

Gestionar el listado de reglas de asignación

Buscar, filtrar y ordenar reglas de asignación

Para ordenar, buscar, filtrar o agrupar reglas de asignación, consulta **Herramientas para configurar los listados** en la página **39**.

Borrar reglas de asignación

Selecciona las casillas asociadas a las reglas de asignación que quieres borrar y en el icono de la barra de herramientas.

Estructura de una investigación

Acceso a una investigación

- Haz clic en el menú superior **Investigaciones**. Se mostrarán todas las investigaciones creadas hasta el momento.
- Utiliza las herramientas de filtrado y búsqueda para localizar una investigación concreta.
- Haz clic en una investigación. Se mostrará una ventana con toda la información asociada a la investigación.

Acceso a la investigación asociada a un indicio

Para localizar de forma rápida la investigación asignada a un indicio concreto sigue los pasos mostrados a continuación:

- Haz clic en el menú superior **Indicios** y elige un indicio en estado **En curso** o **Finalizado**.
- Haz clic en el menú de contexto situado a la derecha de la casilla de selección del indicio, o haz clic con el botón de la derecha del ratón en cualquier campo del indicio. Se mostrará un menú de contexto.
- Haz clic en la opción **Ir a la investigación**. Se mostrará la zona **Investigaciones** con los datos de la investigación asociada al indicio en pantalla.

La ventana de investigación

Al hacer clic en un elemento del listado de investigaciones accesible desde el menú superior **Investigaciones**, se abre la ventana de investigación que consta de varios subpaneles y una barra de herramientas:

Nombre de la investigación (1)

Haz clic para editar el nombre de la investigación.

Barra de pestañas (2)

Añade una herramienta de análisis persistente a la investigación; se guardará su estado y sobrevivirá al cierre de la ventana de investigación. Haz clic en el icono + para mostrar un menú desplegable con las herramientas disponibles:

- **Consulta avanzada SQL**: construye búsquedas mediante el lenguaje SQL sobre el océano de datos almacenado en Cytomic Orion y recogido de la monitorización de los procesos ejecutados en los equipos del cliente. Consulta **Investigar el flujo de eventos** en la página **155** para obtener más información sobre las consultas avanzadas y el asistente de consulta.

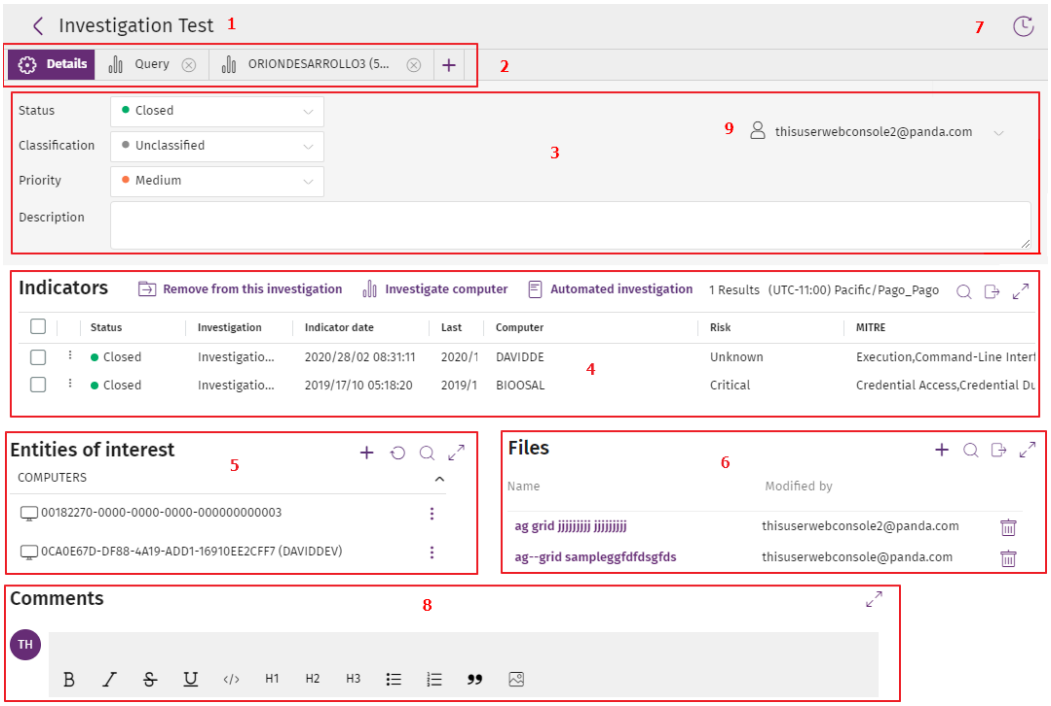


Figura 7.3: Vista general de un caso

- **Consultas mediante asistente** : construye búsquedas sobre el océano de datos almacenado en Cytomic Orion a través de un asistente, sin necesidad de que el analista tenga conocimientos del lenguaje SQL. Consulta **Investigar el flujo de eventos** en la página **155** para obtener más información sobre las consultas avanzadas y el asistente de consultas.

- **Consulta OSQuery** : construye sentencias SQL para obtener información relativa al hardware, software, procesos en ejecución, sistema de ficheros, registro etc. de los equipos. El analista puede utilizar esta información en sus investigaciones, o como parte del procedimiento de respuesta ante un incidente. Consulta **Investigación en la infraestructura IT con OSQuery** en la página **248**.

- **Investigación de equipos**: abre la consola de investigación para analizar en profundidad los eventos generados en un equipo concreto en el día elegido. Se muestran todos los eventos recogidos de todos los procesos ejecutados en ese equipo y día, así como sus relaciones padre - hijo. Consulta **Análisis de indicios con la consola de investigación** en la página **186** para obtener más información sobre la consola de investigación.

- **Investigación manual**: añade un nuevo notebook en blanco al panel de notebooks (**4**) de la investigación. Se abrirá el editor de notebooks con el módulo de Respuestas Rápidas en el panel izquierdo. Consulta **Investigación con notebooks** en la página **220** para obtener más información sobre los notebooks en Cytomic Orion.

- **Investigación automatizada** : muestra una ventana con las plantillas accesibles por el analista a partir de la cual se creará un nuevo notebook. Consulta **Investigación con notebooks** en la página **220** para obtener más información sobre los notebooks en Cytomic

Orion.

- **Grafos**: visualiza el flujo de los procesos ejecutados en la infraestructura IT del cliente. Representa de forma gráfica mediante nodos y y flechas las entidades de los eventos almacenados en el océano de datos y cómo se relacionan entre ellas. Consulta **Diagramas de grafos** en la página **202**.

Ordenar y agrupar pestañas en paneles

Si el analista necesita visualizar dos pestañas / herramientas simultáneamente, es posible dividir en dos la ventana de investigación y agrupar en cada lado y de forma ordenada las pestañas que necesite:

- Añade a la investigación en curso todas las pestañas que necesites. Consulta **Barra de pestañas (2)** .
- Para ordenar las pestañas, haz clic en una de ellas, arrástrala a derecha o izquierda y suelta el botón del ratón.
- Para crear un panel nuevo y dividir en dos la ventana de investigación, haz clic en una pestaña y muévela a la parte derecha de la barra de pestañas. La zona de la ventana donde se creará el panel se resaltará. Al soltar el botón del ratón se creará el panel nuevo con la pestaña arrastrada.
- Puedes mover pestañas de un panel a otro y crear pestañas nuevas en cada panel de forma independiente.
- Para variar el tamaño de los paneles, haz clic en la barra vertical que los separa y mueve el ratón a derecha o izquierda.
- Si cierras todas las pestañas de un panel, éste desaparecerá completamente de la ventana **Investigaciones**.

Subpanel descripción (3)

Establece el estado de la investigación a través de una serie de atributos:

Atributo	Valores
Estado	Indica si los indicios están siendo investigados por los técnicos o ya fueron analizados. • **Cerrada**: la investigación a finalizado. El estado de los indicios asignados pasa a **Finalizado**. • **En curso**: la investigación permanece abierta. El estado de los indicios asignados permanece en **En curso**.
Clasificación	Indica como está catalogada la investigación:

Atributo	Valores
	• **Sin clasificar**: investigación pendiente de analizar. • **Ataque confirmado**: la investigación de los indicios desembocó en la detección de un ataque. • **Investigación sin ataques detectados**: la investigación de los indicios no detectó ningún ataque. • **Ataque potencial**: la investigación de los indicios no es concluyente, pero se ha determinado una alta probabilidad de desembocar en un ataque.
Prioridad	Indica el impacto que el posible ataque investigado pueda tener en los activos de la empresa: • **Sin establecer**: el impacto no se ha determinado por el momento. • **Crítico**: el peligro detectado en la investigación de los indicios es muy alto. El código de color asignado es el rojo. • **Alta**: el peligro detectado en la investigación de los indicios es alto. El código de color asignado es el naranja. • **Media**: el peligro detectado en la investigación de los indicios es medio. El código de color asignado es el verde. • **Baja**: el peligro detectado en la investigación de los indicios es bajo. El código de color asignado es el gris.
Descripción	Caja de texto libre para indicar una descripción detallada del estado de la investigación.

Tabla 7.2: Atributos del subpanel descripción

Subpanel Indicios (4)

Listado con los indicios asignados a la investigación. Consulta **Herramientas para configurar los listados** en la página **39** para obtener información acerca de cómo ordenar, filtrar y agrupar los indicios asignados a la investigación. Consulta **Listado de indicios** en la página **73** para obtener información sobre el significado de los campos de la zona **Indicios**.

El subpanel **Indicios** dispone de las herramientas siguientes:

- **Resultados** : indica el número de indicios mostrados en el subpanel asociados a la investigación.

- **Zona horaria**: permite establecer la zona horaria de los campos **Fecha indicio** y **Último evento**. La zona horaria definida también afectará al contenido de las búsquedas.
- **Buscar**: al hacer clic en el icono se muestra una caja de texto donde introducir la búsqueda. Se admiten las búsquedas parciales, y se efectúan sobre el contenido de todos los campos del indicio.
- **Exportar**: salva en un fichero .csv el contenido del subpanel. Las columnas incluidas en el fichero se corresponden con las mostradas en el listado.
- **Información del indicio**: maximiza el subpanel y despliega el panel derecho **Detalles** que contiene 2 pestañas:
  - **Detalles**: muestra todos los campos del indicio seleccionado.
  - **MITRE**: muestra el detalle de la táctica y técnica MITRE asociada a la hunting rule que generó el indicio.
- **Maximizar**: amplía el subpanel a pantalla completa.

Al hacer clic en un indicio se muestra la barra de herramientas con las opciones siguientes:

Opción	Descripción
Quitar de esta investigación	Elimina el indicio de la investigación, que pasará a estado **Pendiente**.
Investigar equipo	Abre la consola de investigación sobre el equipo involucrado en el indicio para mostrar los eventos registrados en la fecha indicada. Consulta **Análisis de indicios con la consola de investigación** en la página **186**.
Investigación automatizada	Muestra una lista de las plantillas de notebooks creadas. El analista podrá abrir una plantilla y Cytomic Orion rellenará automáticamente los parámetros compatibles de la plantilla con los campos del indicio seleccionado. Consulta **Investigación con notebooks** en la página **220**.
Añadir entidad de interés	Marca una entidad para mostrarla en el subpanel Entidades de interés en la investigación asociada y así permitir un acceso más rápido a la información. Consulta **Panel Entidades de interés**.
Detalles del equipo	Muestra información del equipo. Consulta **Detalles del equipo**.
Añadir regla de eliminación	Esta entrada solo se muestra al seleccionar un único indicio. Consulta **Eliminar indicios de forma manual** en la página **77** para

Opción	Descripción
automática	obtener información sobre el filtrado de indicios.

Tabla 7.3: Barra de herramientas de indicios

Estas opciones también son accesibles a través del menú de contexto de un indicio, al hacer clic sobre él con el botón derecho del ratón.

Subpanel Entidades de interés (5)

Lista que recoge los elementos que el analista ha seleccionado a lo largo de su investigación por considerarlos importantes. Consulta **Panel Entidades de interés**para obtener más información.

Subpanel Ficheros (6)

Listado de los notebooks que los analistas de nivel 1 y 2 han generado mediante las herramientas Investigación automatizada e Investigación manual. Por cada notebook se muestra la siguiente información:

- **Nombre**: nombre del notebook.
- **Creado**: fecha de creación del notebook.
- **Modificado**: fecha de la última modificación del notebook.
- **Modificado por**: cuenta de usuario de la consola que efectuó la última modificación.
- **Borrar** : borra el notebook asociado.

Además, el subpanel **Ficheros** tiene una barra de herramientas con los siguientes elementos:

- **Crear notebook** : muestra un menú desplegable para elegir el tipo de notebook a crear:
  - **Consulta OSQuery**: añade un nuevo notebook para construir una sentencia SQL que obtiene información relativa al hardware, software, procesos en ejecución, sistema de ficheros, registro etc. de los equipos. Consulta **Investigación en la infraestructura IT con OSQuery** en la página **248**.
  - **Investigación manual**: añade un nuevo notebook en blanco al panel de **Ficheros (6)** de la investigación. Se abrirá el editor de notebooks con el módulo de Respuestas Rápidas en el panel izquierdo. Consulta **Investigación con notebooks** en la página **220** para obtener más información sobre los notebooks en Cytomic Orion.
  - **Investigación automatizada**: muestra una ventana con las plantillas accesibles por el analista, a partir de las cuales se creará el nuevo notebook. Consulta **Investigación con notebooks** en la página **220** para obtener más información sobre los notebooks en Cytomic Orion.

- **Grafos**: añade un notebook que representa de forma gráfica el flujo de telemetría generada por la infraestructura IT del cliente y almacenado en el océano de datos. Consulta **Diagramas de grafos** en la página **202**

>  *Consulta **Investigación con notebooks** en la página **220**para obtener más información.*

- **Buscar** : al hacer clic en el icono se muestra una caja de texto donde introducir la búsqueda. Filtra el listado del subpanel buscando en el contenido de todos los campos del listado de notebooks. Admite búsquedas parciales.
- **Exportar** : salva en un fichero .csv el contenido del subpanel. Las columnas incluidas en el fichero se corresponden con las mostradas en el listado.
- **Maximizar** : amplia el subpanel a pantalla completa.

Registro de actividad (7)

Registra las acciones efectuadas por el analista, indicando la cuenta de usuario utilizada, el tipo de acción y el elemento que recibió la acción. Consulta **Registro de actividad asociado a una investigación**.

Comentarios (8)

El analista puede introducir las notas y aclaraciones que considere necesarias para compartir con el resto de técnicos del SOC el estado de la investigación. La caja de texto admite texto enriquecido e imágenes mediante el uso de la barra de herramientas situada en la parte inferior. También puede editar y eliminar sus propias notas con los iconos y que se muestran en la esquina superior derecha al pasar el puntero del ratón por encima de un comentario ya guardado.

Asignar la investigación a un analista (9)

Al crear una investigación, ésta quedará asignada al analista. Cualquier analista con acceso a la investigación puede asignársela a otro técnico, siempre y cuando éste último tenga visibilidad sobre todos los clientes involucrados.

Al hacer clic en el nombre del analista asignado a la investigación, se mostrará un desplegable con todas las cuentas de usuario que tienen visibilidad sobre los clientes que forman parte de la investigación. Al elegir un nuevo analista se lanzarán las siguientes acciones:

- El nuevo propietario de la investigación recibirá un correo con la información descrita en la tabla **Atributos del subpanel descripción** si tiene la opción **Notificarme cada vez que me asignen una investigación** en el menú superior **Configuración** , panel lateral **Mis**

preferencias.

- El cambio de propietario quedará registrado en el **Registro de actividad**. Consulta **Registro de actividad asociado a una investigación**.

Para dejar la investigación sin asignar haz clic en el nombre del analista y pulsa la tecla borrar del teclado. El caso quedará sin asignar y se generará una entrada en **Registro de actividad**.

Persistencia de los cambios y colaboración

Opción	Descripción
Investigar equipo	Abre la consola de investigación sobre el equipo involucrado en el indicio para mostrar los eventos registrados en la fecha indicada. Consulta **Análisis de indicios con la consola de investigación** en la página **186**.
Investigación automatizada	Muestra una lista de las plantillas de notebooks creadas. El analista podrá abrir una plantilla y Cytomic Orion rellenará automáticamente los parámetros compatibles de la plantilla con los campos del indicio seleccionado. Consulta **Investigación con notebooks** en la página **220**.
Añadir entidad de interés	Marca una entidad para mostrarla en el subpanel Entidades de interés en la investigación asociada y así permitir un acceso más rápido a la información. Consulta **Panel Entidades de interés**.
Detalles del equipo	Muestra información del equipo. Consulta **Detalles del equipo**.
Añadir regla de eliminación automática	Esta entrada solo se muestra al seleccionar un único indicio. Consulta **Eliminar indicios de forma manual** en la página **77** para obtener información sobre el filtrado de indicios.

Tabla 7.4: Menú de contexto de un indicio

Una investigación es un recipiente que almacena todas las evidencias estudiadas y recogidas por los analistas. Todos los cambios que se producen en la investigación (modificación o adición de notebooks, adición de herramientas de análisis, configuración del listado de indicios etc.) se mantienen entre sesiones sin necesidad de salvar su estado de forma explícita.

Panel Entidades de interés

En el subpanel **Entidades de interés** de una investigación se almacenan las distintas entidades con las que el analista ha interactuado y que consideró importantes, o que valoró apropiado anotar

para una revisión posterior. Por esta razón, este recurso se utiliza como un repositorio de elementos de acceso rápido, que además actúa como un histórico, mostrando la dirección que está tomando la investigación.

Acceso al panel Entidades de interés

Para acceder al subpanel **Entidades de interés** abre la investigación asociada desde el menú superior **Investigaciones** y haz clic en la barra de pestañas **Detalles**. En la parte inferior izquierda de la ventana se encuentra el panel **Entidades de interés**.

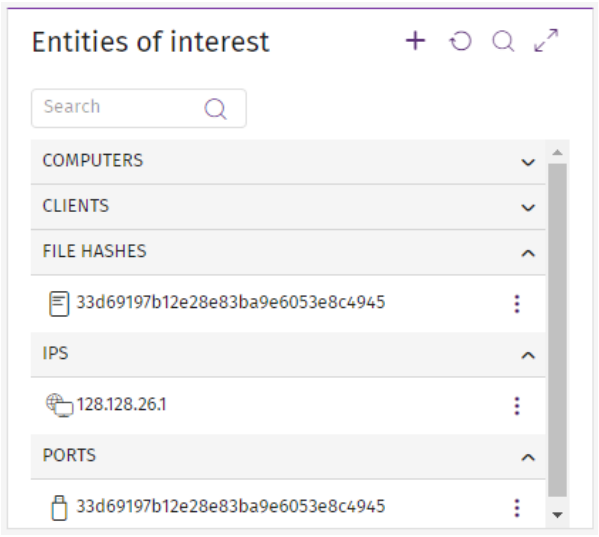


Figura 7.4: Panel Entidades de interés

Las entidades en el panel se muestran agrupadas por su tipo. Haz clic en el título de la agrupación para desplegar u ocultar las entidades del grupo.

Tipos de entidades de interés

Cada entidad de interés tiene un tipo asociado, que se elige en el momento de su anotación:

Nombre	Descripción
Equipo	MUID del equipo investigado.
Cliente	Nombre e identificador del cliente del equipo investigado. Si la cuenta de acceso a la consola web no tiene permisos suficientes se mostrará solo su identificador.
Usuario	Cuenta de usuario del equipo investigado que ejecuta el programa.
Hash de fichero	Nombre del fichero almacenado en el equipo investigado.

Nombre	Descripción
IP	Dirección IP del equipo investigado.
Puerto	Puerto del proceso ejecutado en el equipo investigado.
Dominio	Dominio que pertenece a una comunicación desde o hacia el equipo investigado.
URL	Dirección web accedida desde el equipo investigado.
Path de fichero	Ruta dentro del sistema de ficheros del equipo investigado.
Nombre de fichero	Nombre del fichero almacenado en el equipo investigado.

Tabla 7.5: Tipos de entidades de interés

El tipo de dato asignado a la entidad determinará las acciones que Cytomic Orion permitirá sobre ésta, de modo que es necesario que el analista asigne el tipo de entidad correctamente.

Gestión de entidades

Una entidad de interés siempre está asociada a una investigación concreta. En la mayor parte de los casos el encargado de realizar esta asociación es el técnico, cuando a lo largo de su análisis detecta elementos que considera interesante retener para su consulta posterior. Adicionalmente, Cytomic Orion también agrega de forma automática algunas entidades de interés en el transcurso de la investigación.

Desde el subpanel **Entidades de interés** es posible actuar sobre las entidades añadidas o borrarlas. Para ejecutar una acción sobre una entidad sigue los pasos mostrados a continuación:

- Despliega el grupo al que pertenece la entidad dentro del panel **Entidades de interés**.
- Haz clic sobre el icono ⋮ asociado a la entidad para desplegar el menú de contexto y elige una acción. Dependiendo del tipo de entidad se mostrarán ciertas acciones, algunas de ellas relacionadas con tareas de resolución de problemas.

Añadir entidades de forma automática

Cytomic Orion agrega de forma automática al panel de **Entidades de interés** las entidades objeto de estudio. Las situaciones y entidades agregadas automáticamente a la investigación son las siguientes:

- **Cuando el analista añade un indicio a la investigación**: identificador del equipo (MUID) e identificador del cliente.
- **Cuando el analista abre una consola de investigación**: hash del fichero (MD5) y / o identificador del equipo (MUID).

Añadir entidades de forma guiada

El analista puede añadir una entidad al subpanel **Entidades de interés** desde la opción ☆ **Añadir entidad de interés**. Esta opción se muestra en los siguientes elementos de la consola de análisis, al hacer clic con el botón derecho del ratón para mostrar el menú de contexto:

- En los indicios asignados a una investigación.
- Haciendo clic en el icono ⋮ asociado a un indicio. Consulta el capitulo **Indicios y reglas de hunting** en la página **70** para obtener más información.
- En los resultados de una consulta avanzada SQL. Consulta el capitulo **Investigar el flujo de eventos** en la página **155** para obtener más información.
- En los eventos de un equipo mostrados en la consola de investigación. Consulta el capitulo **Análisis de indicios con la consola de investigación** en la página **186** para obtener más información.

Cytomic Orion establece el tipo de la entidad de interés añadida en función del campo donde el analista muestre el menú de contexto. Si por ejemplo el analista hace clic con el botón derecho del ratón sobre el campo **Equipo** de un indicio, Cytomic Orion añadirá la entidad de interés con el tipo **Equipo** asignado de forma automática, aunque posteriormente el analista podrá cambiarlo eligiendo un nuevo tipo del desplegable mostrado.

Para añadir una entidad al subpanel de **Entidades de interés** sigue los pasos mostrados a continuación:

- Localiza el dato a añadir y haz clic con el botón de la derecha para mostrar el menú de contexto.
- Elige la opción ☆ **Añadir entidad de interés**. Se abrirá una ventana donde especificar el tipo de entidad a añadir.
- Pulsa **Aceptar**. En ese momento la entidad se añadirá en el subpanel **Entidades de interés** y Cytomic Orion permitirá actuar sobre ella.

Añadir entidades de forma libre

Para añadir una entidad de un tipo arbitrario, haz clic en el icono + en el subpanel **Entidades de interés**. Se mostrará un desplegable con el tipo de entidad a añadir y la caja de texto **Entidad** para introducir su valor. La consola analizará los datos introducidos para comprobar que se ajustan al formato esperado según el tipo elegido.

Para acelerar la configuración de entidades, la caja de texto **Entidad** permite filtrar entre todas las entidades disponibles en el caso del tipo elegido. Escribe letra a letra el nombre de la entidad y se mostrará un desplegable con las entidades compatibles con los caracteres introducidos para poder seleccionar la apropiada.

Borrar una entidad de interés

- En el menú superior **Investigaciones** haz clic en la investigación que contiene la entidad de interés y en la barra de pestañas **Detalles**. Se mostrarán los paneles asociados a la investigación en curso.
- En el panel **Entidades de interés** pasa por encima del icono de la entidad de interés a borrar y elige en el menú de contexto la opción **Eliminar de la lista de entidades de interés**.
- Haz clic en **Aceptar** y la entidad se borrará.

Acciones disponibles sobre las entidades de interés

Las entidades de interés ya agregadas tienen asociado un menú de contexto que facilita al analista la operación y navegación por la consola Web.

Acción	Descripción	Disponible en los tipos de entidad
Copiar al portapapeles	Copia al portapapeles del equipo la información correspondiente a la entidad para poder utilizarla en otro punto de la consola de análisis.	Todas
Eliminar de la lista de entidades de interés	Borra la entidad de la lista de entidades de interés asociadas a la investigación.	Todas
Investigar equipo	Abre una ventana con la consola de investigación tomando como parámetro el MUID del equipo para mostrar los eventos producidos en la fecha seleccionada. Consulta **Análisis de indicios con la consola de investigación** en la página **186** para obtener más información.	Equipo
Notebook de investigación	Abre el listado de plantillas que permite generar un nuevo notebook tomando como parámetro el MUID del equipo. Consulta **Investigación con notebooks** en la página **220** para obtener más información.	Equipo

Acción	Descripción	Disponible en los tipos de entidad
Aislar equipo	Impide la comunicación del equipo aislado con la red. Consulta **Herramientas de respuesta** en la página **254** para obtener más información.	Equipo
Dejar de aislar equipo	Restablece las comunicaciones del equipo previamente aislado. Consulta **Gestión de investigaciones** para obtener mas información.	Equipo
Acceso remoto al equipo	Acceso remoto a recursos de gestión del equipo. Consulta **Herramientas de respuesta** en la página **254** para obtener más información.	Equipo
Reiniciar equipo	Inicia la secuencia de reinicio del equipo. Consulta **Herramientas de respuesta** en la página **254** para obtener más información.	Equipo
Detalles del equipo	Muestra una ventana con información detallada del equipo. Consulta la tabla **Detalles del equipo** para conocer el significado de cada campo.	Equipo

Tabla 7.6: Acciones disponibles según la entidad

Herramientas del panel Entidades de interés

El panel **Entidades de interés** incorpora en la parte superior las siguientes herramientas:

- **Añadir entidad de interés** : consulta **Añadir entidades de forma libre**.
- **Recargar panel** : vuelve a pedir al servidor la lista de entidades de interés y las muestra en el subpanel.
- **Buscar** : al hacer clic en el icono se muestra una caja de texto donde introducir la búsqueda. Se admiten las búsquedas parciales y se efectúan sobre el contenido de todos los cambios de la entidad de interés.
- **Maximizar** : amplia el subpanel a pantalla completa.

Detalles del equipo

Sección	Campo	Descripción
General		
	Direcciones IP	Listado con todas las direcciones IP (principal y alias) del equipo.
	Ruta de directorio activo	Ruta dentro del árbol de directorio activo de la empresa donde se encuentra el equipo.
	Grupo	Grupo dentro del árbol de grupos en Cytomic EDR o Cytomic EPDR al que pertenece el equipo. Para cambiar el grupo del equipo haz clic en el botón **Cambiar**.
	Sistema operativo	Nombre del sistema operativo instalado en el equipo.
Información del cliente		
	Id del cliente	Identificador de cliente al que pertenece el equipo en los sistemas de Cytomic Orion.
	Nombre del cliente	Nombre del cliente.
	Fecha de creación	Fecha en la que se dio de alta el cliente en los sistemas de Cytomic.
Equipo		
	Nombre	Nombre del equipo en la red del cliente.
	Tipo de sistema	Tipo de equipo: • Equipo de sobremesa • Servidor • Equipo portátil • Dispositivo móvil (smartphone, tablet, etc.)
	Id de plataforma	Tipo de sistema operativo instalado en el equipo.

Sección	Campo	Descripción
		• Windows • Linux • macOS • Sin definir
	MUID	Identificador único que identifica al equipo dentro de Cytomic Orion.
	Direcciones IP	Listado con todas las direcciones IP (principal y alias) del equipo.
	Direcciones físicas (MAC)	Dirección física de las tarjetas de red instaladas en el equipo.
	Dominio	Dominio Windows al que pertenece el equipo. Vacío si no pertenece a un dominio.
	Ruta de directorio activo	Jerarquía de unidades organizativas donde se encuentra alojado el equipo.
	Grupo	Grupo dentro del árbol de grupos en Cytomic EDR o Cytomic EPDR al que pertenece el equipo. Para cambiar el grupo del equipo haz clic en el botón **Cambiar**.
	Sistema operativo	Nombre del sistema operativo instalado en el equipo.
	Máquina virtual	Indica si el equipo es físico o está virtualizado.
	Es equipo no persistente	Indica si el sistema operativo de la máquina virtual reside en un dispositivo de almacenamiento que perdura entre reinicios o por el contrario se regenera a su estado original.
	Licencias	Licencias de productos de Cytomic instalados en el equipo.
	Estado de la	• Asignada

Sección	Campo	Descripción
	licencia	• No asignada
	Versión del agente	Versión interna del agente Cytomic instalado en el equipo.
	Idioma del agente	Idioma en el que Cytomic EDR o Cytomic EPDR muestra al usuario del equipo la consola local y los mensajes emergentes.
	Aislamiento	Muestra el estado del aislamiento del equipo: • Aislado • Aislando • Dejando de aislar • No aislado
	Reinicio solicitado	El equipo tiene pendiente una petición de reinicio.
	Fecha de creación	Fecha en la que se instaló el agente en el equipo del usuario y éste se registró en la nube de Cytomic.
	Última conexión	Fecha de la última conexión del software de cliente con la nube de Cytomic. Como mínimo el agente de comunicaciones contactará cada 4 horas.
	Último reinicio	Fecha en la que se inició el equipo por última vez.
Seguridad		
	Protección avanzada	Indica si está activado el módulo de Protección avanzada de Cytomic EDR o Cytomic EPDR en el equipo del usuario y en qué modo está configurado (Audit, Hardering o Lock).
	Antivirus de archivos	Indica si está activado el módulo de protección del sistema de ficheros de Cytomic EDR o Cytomic EPDR en el equipo del usuario.
	Antivirus de	Indica si está activada la protección de los protocolos

Sección	Campo	Descripción
	correo	empleados en el envío y recepción de correos electrónicos del equipos del usuario.
	Antivirus para navegación web	Indica si está activada la protección frente al malware descargado de páginas web en el equipo del usuario.
	Firewall	Indica si está activado el módulo de protección frente al tráfico de red generado por aplicaciones en el equipo del usuario.
	Control de dispositivos	Indica si está activado el módulo de protección frente a la infección a través de dispositivos de almacenamiento externos, o que permitan conectar el equipo del usuario a Internet sin pasar por la infraestructura de comunicaciones de la organización (módems USB y otros dispositivos).
	Antivirus del servidor Exchange	Indica si está activado el módulo de protección frente a virus recibidos en servidores Microsoft Exchange.
	Antispam del servidor Exchange	Indica si está activado el módulo de protección frente a los correos electrónicos no deseados en servidores Microsoft Exchange.
	Filtro de contenidos del servidor Exchange	Indica si está activado el módulo de protección frente a los correos recibidos en servidores Microsoft Exchange que llevan ficheros adjuntos con extensiones peligrosas.
	Control de acceso a páginas web	Indica si está activado el módulo de protección frente a la navegación en el equipo del usuario por páginas web no autorizadas por el administrador.
	Gestión de parches	Indica si está activado el módulo de instalación de parches y actualizaciones de sistemas operativos Windows y aplicaciones de terceros en el equipo del usuario.

Sección	Campo	Descripción
	Data Control	Indica si esta activado el módulo de seguimiento de la información personal.
	Antirrobo	Indica si esta activado el modulo que mitiga la exposición de datos ante robos de dispositivos móviles Android.
	Cifrado	Indica si está activado el módulo de cifrado de archivos en el equipo del usuario.
	Estado del control de búsqueda de datos	Indica si el equipo tiene asignado un perfil de configuración de Cytomic Data Watch que le permita recibir búsquedas de ficheros y reportar sus resultados.
Protección		
	Estado de actualización de la protección	Indica si el módulo de la protección instalado en el equipo del usuario coincide con la última versión publicada por Cytomic. • Actualizado • No actualizado (7 días sin actualizar desde la publicación) • Pendiente de reinicio.
	Versión de la protección	Versión del módulo de la protección del producto Cytomic EDR o Cytomic EPDR instalado en el equipo del usuario.
	Estado de actualización del conocimiento	Indica si el fichero de firmas descargado en el equipo del usuario coincide con la última versión publicada por Cytomic. • Actualizado • No actualizado (3 días sin actualizar desde la publicación)
	Fecha de actualización del	Fecha en la que se ha producido la última descarga del fichero de firmas en el equipo del usuario.

Sección	Campo	Descripción
	conocimiento	
Protección de datos		
	Inventario de información personal	Indica si se permite examinar los ficheros de los medios de almacenamiento soportados en equipo del cliente para generar una base de datos en el propio equipo y así acelerar la recuperación de su contenido.
	Seguimiento de información personal	Indica si están instaladas en el equipo del cliente las extensiones para poder acceder a los ficheros de ofimática de la suite Microsoft Office.
	Estado de la indexación	Indica el estado del motor de indexado de Cytomic Data Watch: • No indexado • Indexado • Indexado (solo el texto) • Indexado (todo el contenido) • Indexando

Tabla 7.7: Campos de la ventana Detalles del equipo

Registro de actividad asociado a una investigación

Cada acción que los técnicos del SOC ejecutan en el contexto de una investigación, se registra junto a información adicional que ayuda a determinar su tipo y origen. Esta información permite conocer qué repercusión tendrán en la seguridad las acciones de los analistas sobre los equipos del cliente y sobre su infraestructura.

Acceso al registro de actividad asociado a una investigación

En el menú superior **Investigaciones** haz clic en la investigación de la lista y en el icono (**Registro de actividad)** situado en la parte superior derecha. Se abrirá una ventana con el listado de acciones que los técnicos del SOC ejecutaron dentro de la investigación elegida, junto a varias herramientas que facilitan la búsqueda y filtrado de información.

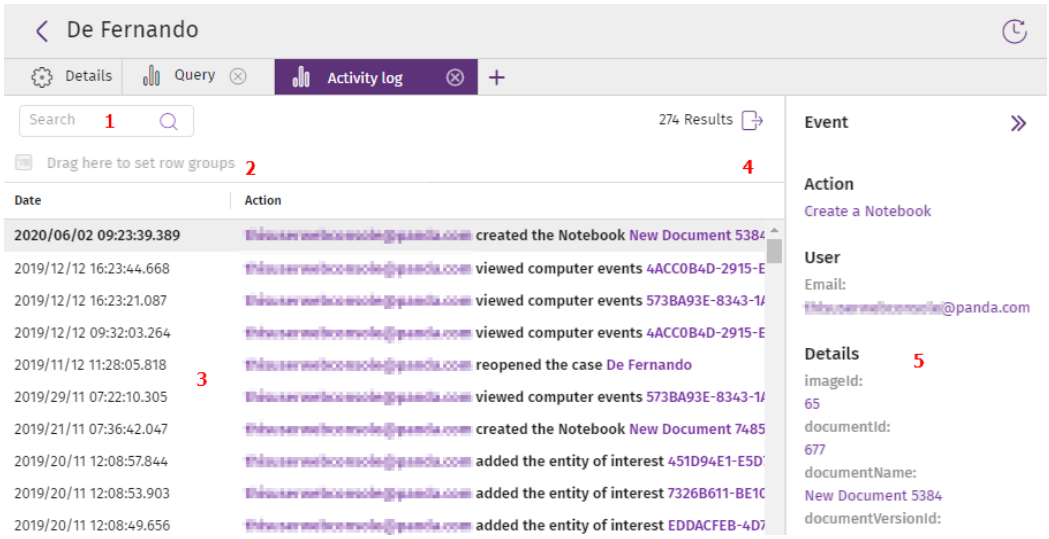


Figura 7.5: Ventana Registro de actividad asociado a una investigación

- **Herramienta de búsqueda (1)**: busca en el contenido de todos los campos del listado para filtrar los registros presentados. Admite búsquedas parciales de cadenas.
- **Herramienta de agrupación (2)**: agrupa los registros según el campo elegido. Para obtener más información sobre la herramienta de agrupación consulta **Herramientas de filtrado** en la página **44**.
- **Exportar (4)**: vuelca el listado en un fichero csv.
- **Panel lateral (5)**: al seleccionar un registro muestra su información extendida asociada.
- **Panel central (3)**: muestra un listado de registros de actividad que coincidan con los criterios de búsqueda establecidos. A continuación se indican los campos incluidos en el listado:

Campo	Descripción
Fecha	Fecha en la que es ha producido la acción registrada.
Acción	Tipo de acción registrada junto a la cuenta de usuario que la inició e información adicional. Consulta**Registro de actividad asociado a una investigación**para obtener más información.
Usuario	Nombre de la cuenta que inició la acción. Este campo no se muestra por defecto.
Tipo de acción	Clase de acción registrada. Este campo no se muestra por defecto.

Tabla 7.8: Campos del listado Registro de actividad

Acciones registradas en Cytomic Orion

Acción	Descripción
Crear una investigación	El usuario de la consola asignó uno o más indicios a una investigación nueva.
Renombrar una investigación	El usuario de la consola actualizó el nombre de una investigación.
Cambiar la clasificación de una investigación	El usuario de la consola cambió la clasificación de una investigación.
Cambiar la prioridad de una investigación	El usuario de la consola cambió la prioridad de una investigación.
Añadir o quitar clientes de una investigación	El usuario de la consola modificó entidades de interés de tipo cliente asignadas a una investigación.
Cerrar una investigación	El usuario de la consola cerró una investigación.
Reabrir una investigación	El usuario de la consola volvió a asignar el estado **En curso** o **Pendiente** a un indicio asignado a una investigación.
Añadir indicios a una investigación	El usuario de la consola asignó un indicio a una investigación existente.
Quitar indicios a una investigación	El usuario de la consola dejó de asignar a una investigación un indicio asignado previamente.
Asignar una investigación a un usuario	El usuario de la consola cambió el usuario asignado a una investigación.
Retirar una	El usuario de la consola quitó la asignación de la investigación.

Acción	Descripción
investigación	
Lanzar una consulta	El usuario de la consola ejecutó una consulta SQL.
Cancelar una consulta	El usuario de la consola detuvo la ejecución de una consulta SQL.
Resultado de una consulta	Una consulta SQL finalizó su ejecución.
Estadísticas de una consulta	Muestra datos de la consulta SQL ejecutada (sentencia SQL completa, número de bytes leídos etc). Este campo puede utilizarse para determinar el consumo de datos de Cytomic Orion.
Error en la consulta	La ejecución de una consulta SQL finalizó con error.
Investigar equipo	El usuario de la consola abrió una consola de investigación a partir del MUID de un equipo del cliente.
Investigar archivo	El usuario de la consola abrió una consola de investigación a partir del MD5 de un fichero.
Investigar equipo	El usuario de la consola abrió una consola de investigación a partir del nombre de un equipo del cliente.
Crear un Notebook	El usuario de la consola inicio un análisis mediante la creación de un notebook.
Actualizar un Notebook	El usuario de la consola trabajó en un análisis modificando un notebook.
Visualizar un Notebook	El usuario de la consola abrió un notebook para visualizarlo.
Cambiar el nombre de un Notebook	El usuario de la consola renombró un notebook.

Acción	Descripción
Eliminar un Notebook	El usuario de la consola borró un notebook.
Convertir un Notebook a PDF	El usuario de la consola ha obtenido un informe en pdf a partir de los resultados de un notebook.
Ejecutar un Notebook	El usuario de la consola obtuvo resultados de un análisis ejecutando un notebook.
Iniciar acceso remoto de un equipo	Cytomic Orion ha recuperado de la plataforma las credenciales necesarias para que el analista que realizó la petición de acceso remoto pueda acceder al equipo investigado y utilizar las herramientas de resolución. Para acceder al registro de comandos ejecutados por el analista, consulta **Registro de operaciones remotas**.
Intentar iniciar acceso remoto de un equipo	Cytomic Orion intentó recuperar de la plataforma las credenciales necesarias para acceder remotamente al equipo investigado pero el proceso terminó en error.
Solicitar reiniciar equipos	El usuario de la consola inició el proceso de reinicio remoto de un equipo.
Solicitar aislar equipos	El usuario de la consola inició el proceso de aislamiento de un equipo.
Solicitar dejar de aislar equipos	El usuario de la consola inició el proceso para sacar del aislamiento a un equipo.
Añadir entidades de interés	El usuario de la consola añadió una entidad de interés a una investigación.
Eliminar entidades de interés	El usuario de la consola retiró una entidad de interés de una investigación.

Tabla 7.9: Campos del listado Registro de actividad

Registro de operaciones remotas

Los comandos ejecutados como parte de un acceso remoto a un equipo se registran de forma independiente y más detallada.

Acceso al registro de operaciones remotas

- En el menú superior **Investigaciones** haz clic en la investigación y en el icono  (**Registro de actividad)** situado en la parte superior derecha. Se abrirá una ventana con el listado de acciones que los técnicos del SOC ejecutaron dentro de la investigación elegida.
- En el panel central **(3)** haz clic en un registro de tipo **Iniciar acceso remoto de un equipo**. Se mostrarán sus detalles en el panel lateral **(5)**.
- En el panel lateral **(5)** localiza el atributo **sessionId** y haz clic en su contenido. Se abrirá la ventana **Detalles de la sesión remota**.

Campo	Descripción
Session Id	Identificador de la sesión asignada por Cytomic Orion.
Fecha	Fecha en la que se inició el acceso remoto.
Dirección IP	Dirección IP del equipo accedido.
Categoría	• **Archivos**: operación relacionada con ficheros. • **Procesos**: operación relacionada con procesos. • **Servicios**: operación relacionada con servicios. • **Terminal**: línea de comandos remota. • **Conexión**: estado de la conexión remota.
Acción	Acción ejecutada en el equipo remoto y registrada por Cytomic Orion.

Tabla 7.10: Campos del listado Detalles de la sesión remota

Capítulo 8

Visibilidad de la actividad en Cytomic Orion

Cytomic Orion muestra un resumen de la actividad principal registrada en la consola mediante recursos gráficos llamados widgets. Un panel de control agrupa a los widgets que contienen información de una misma área. Los analistas y el gestor del SOC utilizan los paneles de control para comprobar de un vistazo el estado de la seguridad de la red del cliente y la marcha de los análisis planificados.

Los paneles de control disponibles son:

- **Investigaciones de indicios**: consulta **Panel Investigaciones e indicios**.
- **MITRE**: consulta **Panel MITRE**.
- **Consumo de datos**: consulta **Consumo de datos** .

CONTENIDO DEL CAPÍTULO

Panel Investigaciones e indicios

Muestra información de los indicios detectados, el estado de las investigaciones creadas, los equipos y clientes con más probabilidad de sufrir un ataque informático y las Hunting rules que agrupan el mayor número de indicios registrados en la plataforma.

Para acceder al panel de control:

- Selecciona en el menú superior **Dashboard** y en el panel lateral haz clic en **Investigaciones e indicios.** Se abrirá una ventana con los widgets del panel de control.
- Selecciona el intervalo de los datos que se mostrarán en los widgets:
  - Últimas 24 horas
  - Últimos 7 días
  - Último mes
  - Último año

Investigaciones abiertas

Muestra el total de investigaciones que permanecen en estado **En curso** y las divide en dos grupos: las abiertas por la cuenta de usuario que accede al panel de control y las investigaciones abiertas por otras cuentas de usuario.

Figura 8.1: Panel Investigaciones abiertas

Descripción de las series

Serie	Descripción
Otros	Investigaciones en estado **En curso** abiertas por otras cuentas de usuario diferentes a la utilizada para acceder a la consola de análisis.
Mías	Investigaciones en estado **En curso** abiertas por la cuentas de

Serie	Descripción
	usuario que accede a la consola de análisis.

Tabla 8.1: Descripción de las series del widget Investigaciones abiertas

Indicios pendientes de investigar

Muestra el total de indicios que todavía no han sido asignados a una investigación y por lo tanto no han sido analizados, y el total de indicios que, estando asignados a una investigación, todavía no han sido cerrados y por lo tanto no se ha concluido su análisis.

Figura 8.2: Panel Indicios pendientes de investigar

Descripción de las series

Serie	Descripción
Total	Suma total de indicios en estado En curso y Pendiente
Criticas	Indicios cuya Severidad es 1 (Crítica)
Riesgo alto	Indicios cuya Severidad es 2 (Riesgo alto)
Riesgo medio	Indicios cuya Severidad es 3 (Riesgo medio)
Riesgo bajo	Indicios cuya Severidad es 4 (Riesgo bajo)

Tabla 8.2: Descripción de las series del widget Indicios pendientes de investigar

Equipos con más riesgo

Muestra los equipos donde Cytomic Orion ha detectado un mayor riesgo, contabilizando el número de indicios asignados y su criticidad. El listado está ordenado para mostrar primero los equipos con más indicios críticas detectados, luego los equipos con más indicios de riesgo alto, luego medio y finalmente bajo.

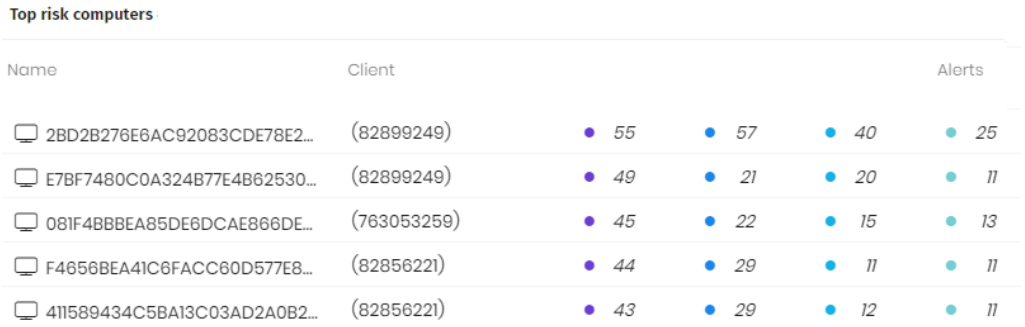


Figura 8.3: Panel Equipos con más riesgo

Descripción de las series

Campo	Descripción
Nombre	Identificador del equipo.
Cliente	Identificador del cliente.
Indicios	Número de indicios encontrados agrupadas por severidad • Indicios críticos. • Indicios de riesgo alto. • Indicios de riesgo medio. • Indicios de riesgo bajo.

Tabla 8.3: Descripción de las series Equipos con más riesgo

Hunting rules con más riesgo

Muestra las Reglas de hunting que más indicios han provocado, ordenados por criticidad, junto al número de equipos distintos afectados y el número de indicios donde se detectaron. El listado está ordenado para mostrar primero las Reglas de hunting críticas, luego las de riesgo alto, luego medio y finalmente bajo. Dentro de cada categoría de severidad, las reglas se ordenan por el número de indicios generados.

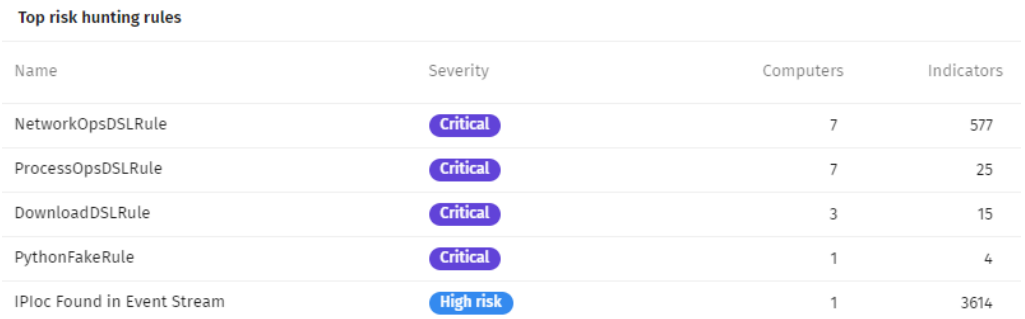


Figura 8.4: Panel Hunting rules con más riesgo

Descripción de las series

Campo	Descripción
Nombre	Identificador de la Regla de hunting.
Criticidad	Severidad asociada a la Regla de hunting.
Equipos	Número de equipos distintos donde se generó una alerta.
Indicios	Número de indicios generados por la Regla de hunting.

Tabla 8.4: Descripción de las series Hunting rules con más riesgo

Clientes con más riesgo

> *Este widget unicamente se muestra en MSSPs, / MDR donde puede haber múltiples clientes a administrar.*

Muestra los clientes cuyos equipos del parque informático tienen un mayor número de indicios pendientes o en curso asignados. El listado se ordena por severidad, mostrándose primero los clientes con mayor número de indicios críticos, luego de riesgo alto, medio y finalmente bajo.

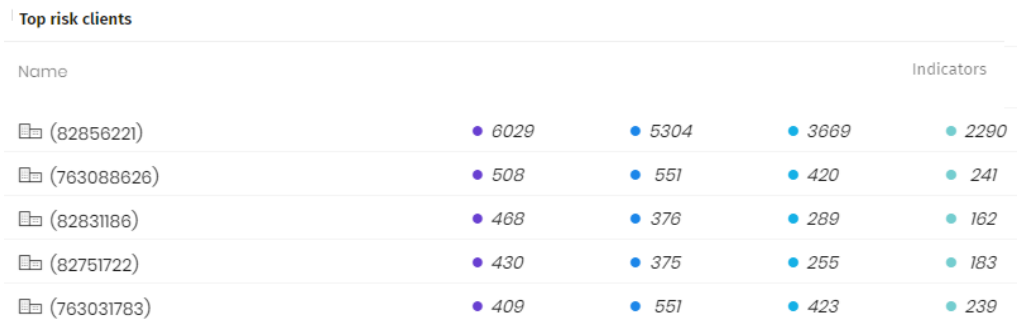


Figura 8.5: Clientes con más riesgo

Descripción de las series

Campo	Descripción
Nombre	Identificador del cliente. • Indicios críticos. • Indicios de riesgo alto. • Indicios de riesgo medio. • Indicios de riesgo bajo.

Tabla 8.5: Descripción de las series Hunting rules con más riesgo

Indicios

Diagrama de líneas que muestra el número de indicios generados a lo largo del tiempo según su criticidad. El diagrama incluye cuatro series de datos, una por cada nivel de severidad soportado en Cytomic Orion.

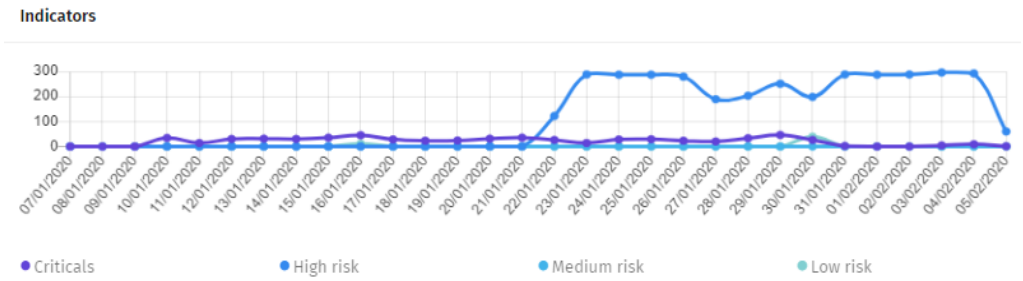


Figura 8.6: Panel Indicios

Descripción de las series

Serie	Descripción
●	Indicios críticas.
●	Indicios de riesgo alto.
●	Indicios de riesgo medio.
●	Indicios de riesgo bajo.

Tabla 8.6: Descripción de la serie Indicios

Panel MITRE

Muestra en la matriz de MITRE ATT&CK la distribución de indicios detectados agrupados por su táctica y técnica asociadas.

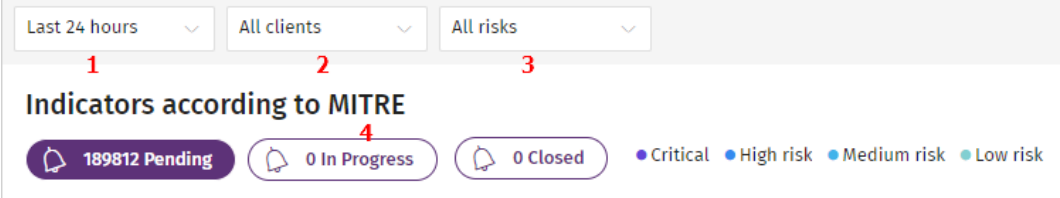


Figura 8.7: Panel Indicios según MITRE

Para acceder al panel de control:

- Selecciona en el menú superior **Dashboard** y en el panel lateral haz clic en **MITRE.** Se abrirá una ventana con los widgets del panel de control .
- Selecciona el intervalo de los datos que se mostrarán en los widgets **(1)**:
    - Últimas 24 horas
    - Últimos 7 días
    - Último mes
- Selecciona el cliente del que se mostrarán los indicios **(2)**
    - **Selecciona cliente**: muestra los indicios de todos los clientes.
    - **Identificador de cliente**: muestra los indicios del cliente seleccionado.
- Selecciona el nivel de riesgo de la técnica y táctica mostradas en la matriz **(3)**:
    - Todos los riesgos
    - Crítico
    - Riesgo alto
    - Riesgo medio
    - Riesgo bajo
- Selecciona el estado de los indicios que se mostrarán en la matriz **(4)**:
    - **Pendiente**: indicios sin asignar a una investigación.
    - **En curso**: indicios asignados a una investigación abierta.
    - **Finalizado**: indicios asignados a una investigación finalizada.

Descripción de las series

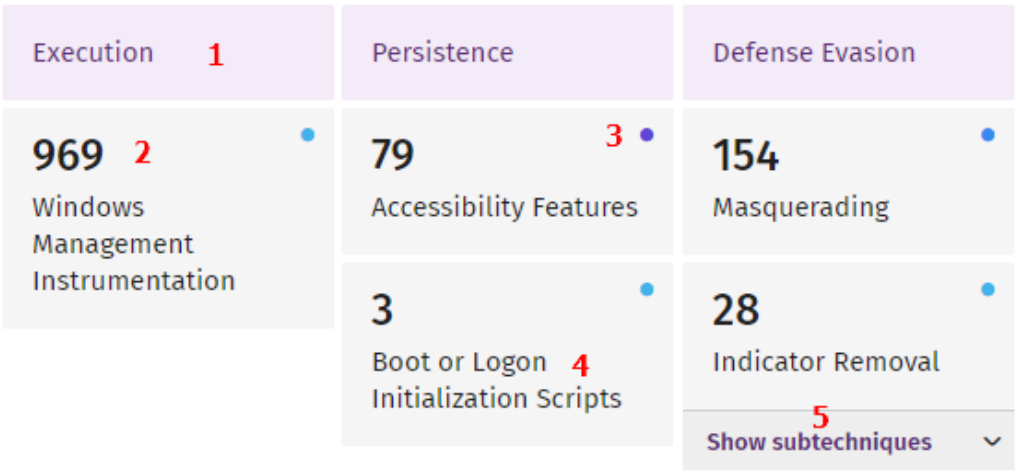


Figura 8.8: Panel Indicios según MITRE

Serie	Descripción
(1)	Técnica MITRE.
(2)	Número de indicios encontrados con la técnica y táctica indicadas.
(3)	Riesgo asociado a la técnica y táctica de los indicios agrupados.
(4)	Táctica MITRE.
(5)	Desplegable con las subtécnicas. Por cada una se indica el número de indicios encontrados que tienen esa subtécnica asignada. No todos los indicios tienen subtécnica asignada.

Tabla 8.7: Descripción de las series del widget Indicios según MITRE

Visualizar los indicios de una técnica y táctica

Haz clic en la casilla correspondiente a la técnica (**2**) o subtécnica (**5**) de interés. Se mostrará el listado **Inidicios** con un listado de los indicios asociados a la técnica o subtécnica seleccionada.

Consumo de datos

Cytomic Orion pone a disposición de los analistas un conjunto de herramientas que les permiten buscar en el océano de datos información del parque de equipos que investigan. El almacenamiento de información en el océano de datos no está limitado para los usuarios de la consola, pero la recuperación de esta información se monitoriza para determinar el volumen de datos consumido por cada MSSP.

Cytomic Orion establece unos límites de uso orientativos, que no afectan a ni a la capacidad máxima del océano de datos ni al ancho de banda consumido al recuperar datos de éste. Esta información solo se ofrece como guía para comparar el consumo de ancho de banda asignado a cada MSSP / SOC con el recomendado por Cytomic.

Volumen de datos y recursos para monitorizar el consumo

Volumen de datos asignado

Cada MSSP tiene asignado un volumen de consumo de datos anual de 5 Gigabytes por cada equipo que gestiona. Los analistas que acceden al océano de datos utilizan el volumen asignado al SOC de forma discrecional: un único usuario puede utilizar todos los datos asignados anualmente en un mismo día para investigar un único equipo de un cliente concreto del MSSP o, por el contrario, todos los analistas pueden repartirse el volumen de datos asignado para investigar varios o todos los equipos de los clientes del MSSP.

Recursos para monitorizar el consumo de datos

Para controlar el consumo de datos en cada MSSP, Cytomic Orion pone a disposición de los usuarios de la consola varios recursos complementarios:

- **Data consumed in advanced queries**: notebook que muestra la cantidad de datos consumida por cuenta de usuario. Consulta **Notebook Data consumed in advanced queries**.
- **Dashboard Consumo de datos por usuario**: conjunto de paneles que muestran, tanto de forma consolidada como desglosada, los datos consumidos por las cuentas de usuario del MSSP. Consulta **Dashboard Consumo de datos por usuario**.
- **Dashboard Consumo de datos por consultas**: conjunto de paneles que muestran, tanto de forma consolidada como desglosada, el consumo de cada operación del MSSP que implique acceso al océano de datos. Consulta **Dashboard Consumo de datos por consulta**.
- **Dashboard Consumo de datos por cliente**: conjunto de paneles que muestran, tanto de forma consolidada como desglosada, los datos consumidos por cada cliente que gestiona el MSSP. Consulta **Dashboard Consumo de datos por cliente**.
- **Dashboard Datos asignados**: histórico de cambios en el volumen de datos asignados al MSSP. Consulta **Dashboard Datos asignados**.
- **Correo de notificación**: alerta a los usuarios de la consola cuando el consumo de datos sobrepasa ciertos umbrales establecidos. Consulta **Email de notificación de consumo**.

Notebook Data consumed in advanced queries

Para visualizar el volumen de datos que ha consumido cada cuenta de usuario de la consola, es necesario crear y ejecutar un notebook a partir de la plantilla **Data consumed in advanced queries**.

Acceso al notebook

- Haz clic en el menú superior **Investigaciones** y elige una investigación ya abierta o crea una nueva:
    - Haz clic en el icono **Nueva investigación** + situado en la parte superior derecha de la ventana.
    - Selecciona los clientes del MSSP sobre los que se realizará la investigación. En este caso este dato no es relevante ya que el objetivo es ejecutar un notebook a partir de una plantilla.
- En el panel **Archivos** haz clic en el icono +. Se abrirá un menú desplegable.
- Haz clic en la opción **Investigación automatizada** del menú desplegable y elige la plantilla **Data consumed in advanced queries**. Se abrirá la ventana de parámetros.
- Escribe en `date_from` y `date_to` el límite superior e inferior del intervalo cuyo consumo quieres analizar y haz clic en el botón **Aceptar**.

El intervalo máximo permitido es de 6 meses. Si defines un intervalo mayor, la consola mostrará un error.

Contenido del notebook Data consumed in advanced queries

El notebook **Data consumed in advanced queries** contiene una serie de campos que muestran el volumen de datos consumidos, medidos en Gigabytes, y pertenecientes al intervalo indicado:

Campo	Descripción
Total consumption	Acumulado de todas las cuentas de usuario que gestiona el MSSP.
Average consumption per day	Media diaria de todas las cuentas de usuario que gestiona el MSSP.

Tabla 8.8: Sección Data consumption

Campo	Descripción
Email	Dirección de correo de la cuenta de usuario.
Total Notebook	Volumen de datos solicitados al océano de datos desde los notebooks.

Campo	Descripción
(GB)	
Total Exploration (GB)	Volumen de datos solicitados al océano de datos mediante las consultas SQL.
Total (GB)	Volumen de información solicitada al océano de datos por cada cuenta de usuario. Es la suma de todos los conceptos anteriores.
Average (GB)	Media diaria de consumo en el periodo indicado.

Tabla 8.9: Sección Data consumption per user

Campo	Descripción
Email	Dirección de correo de la cuenta de usuario.
Clients	Visibilidad de los clientes de la cuenta de usuario. Consulta **Configuración de la visibilidad de clientes** en la página **55**.
Total (GB)	Volumen de información solicitada al océano de datos por cada cuenta de usuario.

Tabla 8.10: Sección Consumption per user and clients users have access to

Panel de control Consumo de datos

Muestra el consumo de datos en el año en curso, y el volumen de datos asignado al MSSP.

Permisos requeridos

La cuenta de usuario no requiere permisos especiales para visualizar el panel. **Consumo de datos** siempre está visible.

Acceso al panel

Haz clic en el menú superior **Dashboard**. En el panel lateral se muestra **Consumo de datos**.

Consumo de datos

Este panel muestra el consumo de datos acumulado de todas las cuentas del SOC en el año en curso.

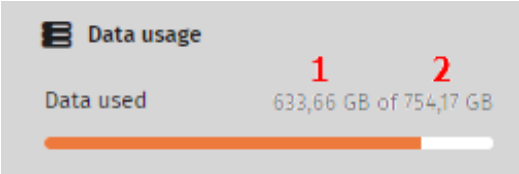


Figura 8.9: Panel Consumo de datos

Descripción de las series

Serie	Descripción
(1)	Suma total de datos consumidos por el MSSP en el año actual.
(2)	Total de los datos asignados al MSSP.
Barra	Porcentaje de los datos consumidos en el año: • **Verde**: consumo menor del 80%. • **Amarillo**: consumo entre el 80% y 90%. • **Naranja**: consumo entre el 90% y 100%. • **Rojo**: consumo mayor del 100%.

Tabla 8.11: Descripción de las series del panel Consumo de datos

Dashboard Consumo de datos por usuario

Muestra el consumo de datos del MSSP desglosado por cuenta de usuario.

Permisos requeridos

La cuenta de usuario requiere el permiso **Ver el dashboard de consumo de datos** para acceder al contenido del dashboard.

Acceso al panel

- Haz clic en el menú superior **Dashboard** y en el panel lateral **Consumo de datos**.
- Haz clic en el menú de pestañas **Usuarios**.

Consumo de datos por usuario

El dashboard contiene los elementos siguientes:

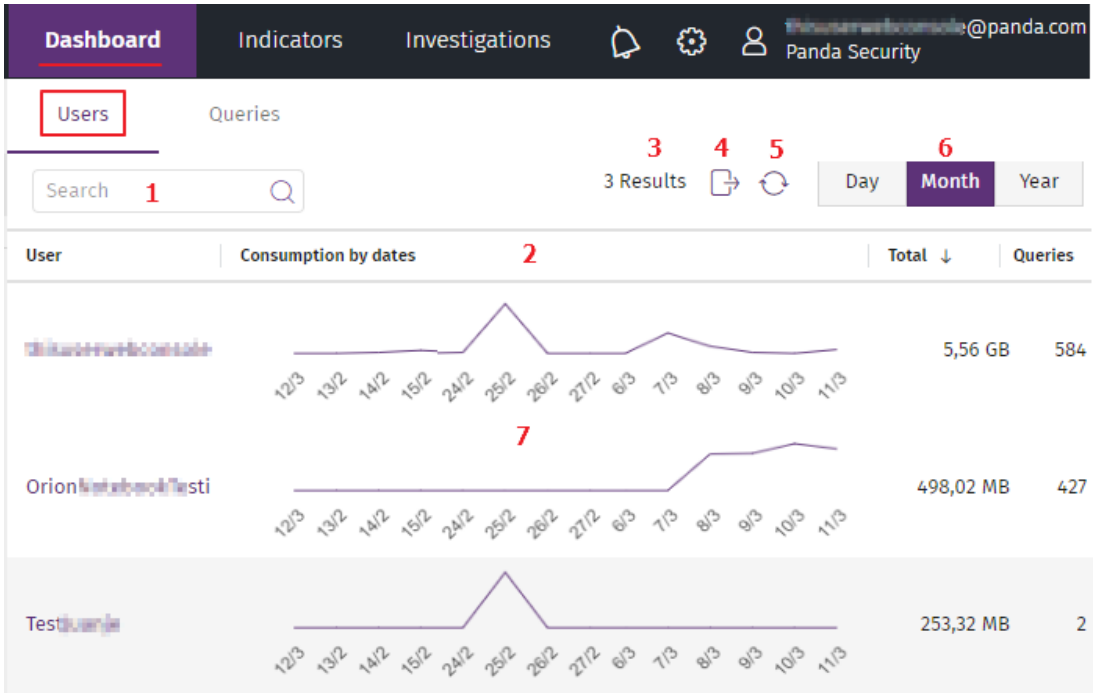


Figura 8.10: Dashboard Consumo de datos por usuario

- **Búsqueda (1)**: filtra los resultados tomando el campo **Usuario**. Acepta subcadenas.
- **Ordenar columnas (2)**: consulta **Herramientas para configurar los listados** en la página **39**.
- **Resultados (3)**: número de cuentas de usuario con datos sobre consumo mostradas en el dashboard.
- **Exportar (4)**: descarga un fichero Excel con el contenido del dashboard en el equipo del analista.
- **Recarga (5)**: recarga el contenido del dashboard para actualizar los datos.
- **Rango de fechas (6)**:
  - **Día**: muestra los datos acumulados de las últimas 24 horas.
  - **Mes**: muestra los datos acumulados de los últimos 30 días.
  - **Año**: muestra los datos acumulados de los últimos 12 meses.
- **Gráficas Consumo por usuario (7)**: indica la evolución del consumo por cada cuenta de usuario del MSSP en el intervalo establecido **(6)**:

Columna	Descripción
Usuario	Nombre de la cuenta de usuario del MSSP.

Columna	Descripción
Consumo por fechas	Gráfica de líneas que muestra la evolución del consumo de datos.
Total	Volumen de datos consumidos por la cuenta de usuario.
Consultas	Número de operaciones de lectura realizadas contra el océano de datos.

Tabla 8.12: Descripción de las series de la gráfica Consumo por usuario

Dashboard Consumo de datos por consulta

Muestra el consumo de datos de una cuenta de usuario del MSSP desglosado por sus operaciones contra el océano de datos.

Permisos requeridos

La cuenta de usuario requiere el permiso **Ver el dashboard de consumo de datos** para acceder al contenido del dashboard.

Acceso al panel

- Haz clic en el menú superior **Dashboard** y en el panel lateral **Consumo de datos**.
- Haz clic en el menú de pestañas **Usuarios**.
- Configura el intervalo adecuado y haz clic en una cuenta de usuario. Se mostrará el dashboard **Consumo de datos por consulta** para esa cuenta de usuario.

Consumo de datos por consulta

El dashboard contiene los elementos siguientes:

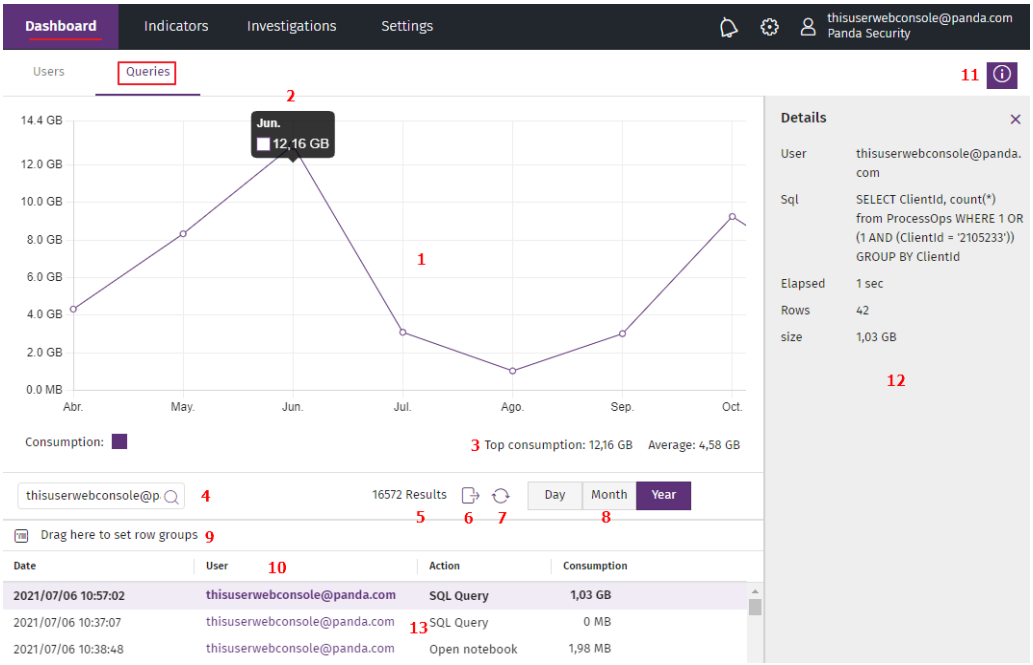


Figura 8.11: Dashboard Consumo de datos por consulta

- **Gráfica de lineas (1)**: muestra la evolución del consumo de la cuenta de usuario seleccionada.
- **Tooltip (2)**: pasa el ratón por los puntos de la gráfica de lineas para mostrar un tooltip con el contenido de la coordenada X e Y del punto seleccionado.
- **Estadísticas de consumo (3)**: muestra el pico de consumo y el máximo de datos recomendado por Cytomic en el intervalo elegido.
- **Buscar (4)**: filtra el listado de operaciones registradas según el contenido de los campos **Fecha**, **Usuario** y **Acción**.
- **Resultados (5)**: número de operaciones contra el océano de datos registradas en el intervalo establecido en **(8)**.
- **Exportar**: descarga un fichero en formato Excel con el contenido del listado **(13)**.
- **Recargar (7)**: refresca el contenido del listado **(13)**.
- **Rango de fechas (8)**:
  - **Día**: muestra los datos acumulados de las últimas 24 horas.
  - **Mes**: muestra los datos acumulados de los últimos 30 días.
  - **Año**: muestra los datos acumulados de los últimos 12 meses.
- **Agrupar columnas (9)**: consulta **Agrupar registros por columnas** en la página **40**.
- **Ordenar columnas (10)**: consulta **Ordenar columnas** en la página **40**.
- **Botón de detalle**: muestra u oculta el panel **Detalle (12)**.

- **Detalle (12)**: panel de datos que contiene la información de la operación seleccionada en **(13)**:

Columna	Descripción
Usuario	Nombre de la cuenta de usuario del MSSP.
Sql	Sentencia SQL registrada que recupera información del océano de datos.
Tiempo	Tiempo que tarda en ejecutarse la sentencia SQL.
Lineas	Número de filas recuperadas del océano de datos.
Tamaño	Volumen de información recuperada del océano de datos.

Tabla 8.13: Descripción del panel de detalle

- **Listado (13)**: operaciones contra el océano de datos que se han registrado en la cuenta de usuario en el intervalo indicado en **(8)**.

Atributo	Descripción
Fecha	Fecha en la que se ejecutó la operación que recupera información del océano de datos.
Usuario	Cuenta de usuario del MSSP que ejecutó la operación.
Acción	Módulo o herramienta que recupera información del océano de datos: • **Consulta SQL**: abarca las consultas generadas con el módulo Consulta avanzada SQL y Consultas mediante asistente. Consulta **Investigar el flujo de eventos** en la página **155**. • **Abrir notebook**: incluye las consultas generadas en un notebook. Consulta **Investigación con notebooks** en la página **220**. • **Consulta desde aplicación**: incluye la información recuperada mediante llamadas a la API de Cytomic. Consulta **Integración de Cytomic Orion con las herramientas del SOC** en la página **314**.

Atributo	Descripción
Consumo	Número de filas recuperadas del océano de datos.

Tabla 8.14: Descripción del panel de detalle

Dashboard Consumo de datos por cliente

Muestra el consumo de datos que se han registrado en las investigaciones realizadas sobre los clientes gestionados por el MSSP.

Permisos requeridos

La cuenta de usuario requiere el permiso **Ver el dashboard de consumo de datos** para acceder al contenido del dashboard.

Acceso al panel

- Haz clic en el menú superior **Dashboard** y en el panel lateral **Consumo de datos**.
- Haz clic en el menú de pestañas **Clientes**.
- Configura el intervalo adecuado. Se mostrará el dashboard **Consumo de datos por cliente**.

Calculo del consumo de datos compartidos por cliente

Dado que una misma consulta o investigación puede afectar a varios clientes de forma simultánea, es necesario repartir de forma equitativa el consumo de datos compartido entre ellos.

Para repartir el consumo entre varios clientes, se establece un peso o porcentaje de consumo en función del número de licencias de cada cliente. A continuación se muestra un ejemplo del cálculo del porcentaje de datos consumidos:

El analista del SOC lanza una consulta sobre los equipos de tres de sus clientes, que consume un total de 250 Megabytes. La distribución de licencias de los tres clientes es la siguiente:

- Cliente 1: 57 licencias
- Cliente 2: 3 licencias
- Cliente 3: 7 licencias

El total de licencias entre los tres clientes es 57 + 3 + 7 = 67 licencias.

La distribución de porcentajes es:

- Cliente 1: 57 / 67 = 0,85 (el 85% del volumen del tráfico consumido por la consulta se le imputará al cliente 1).

- Cliente 2: 3 / 67 = 0,04 (el 4% del volumen del tráfico consumido por la consulta se le imputará al cliente 2).
- Cliente 3: 7 / 67 = 0.10 (el 10% del volumen del tráfico consumido por la consulta se le imputará al cliente 3).

El consumo imputado a cada cliente es:

- Cliente 1: 250 * 0,85 = 212 Mbytes
- Cliente 2: 250 * 0,04 = 10 Mbytes
- Cliente 3: 250 * 0,10 = 25 Mbytes

Consumo de datos por cliente

El dashboard contiene los elementos siguientes:

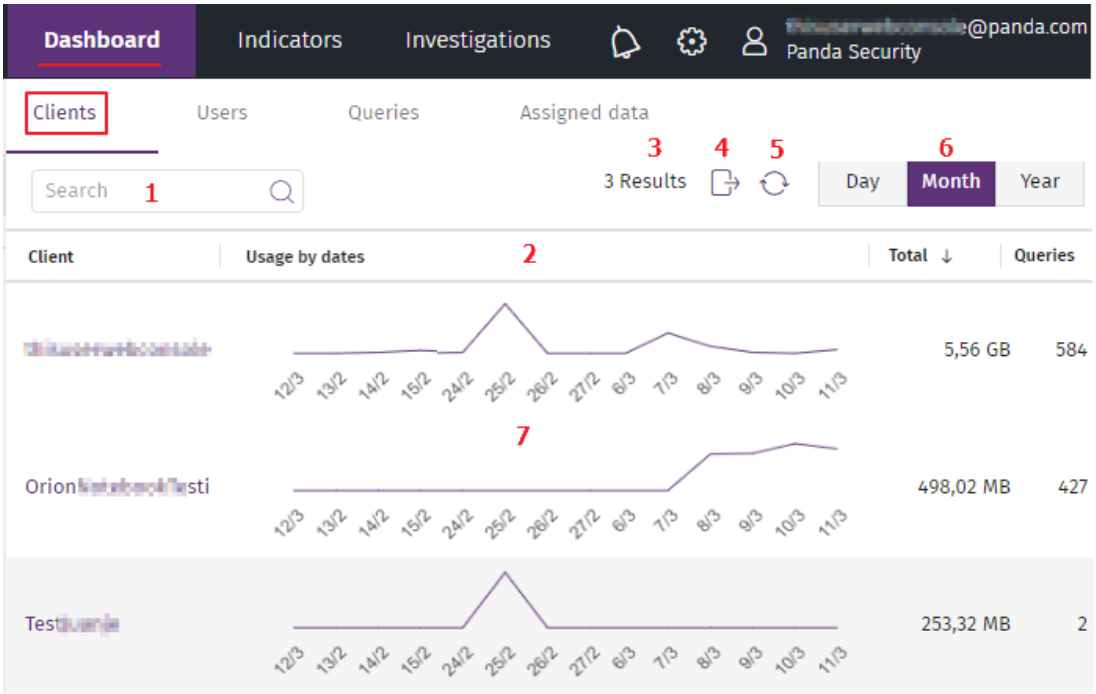


Figura 8.12: Dashboard Consumo de datos por usuario

- **Búsqueda (1)**: filtra los resultados tomando el campo **Cliente**. Acepta subcadenas.
- **Ordenar columnas (2)**: consulta **Herramientas para configurar los listados** en la página **39**.
- **Resultados (3)**:número de clientes con datos sobre consumo mostrados en el dashboard.
- **Exportar (4)**:descarga un fichero Excel en el equipo del analista con el contenido del dashboard.
- **Recarga (5)**: recarga el contenido del dashboard para actualizar los datos.
- **Rango de fechas (6)**:

- **Día**: muestra los datos acumulados de las últimas 24 horas.
- **Mes**: muestra los datos acumulados de los últimos 30 días.
- **Año**: muestra los datos acumulados de los últimos 12 meses.

- **Gráficas Consumo por cliente (7)**: indica la evolución del consumo por cada cliente del MSSP en el intervalo establecido **(6)**:

Columna	Descripción
Cliente	Nombre del cliente del MSSP.
Consumo por fechas	Gráfica de lineas que muestra la evolución del consumo de datos.
Total	Volumen de datos consumidos por el cliente.
Consultas	Número de operaciones de lectura realizadas contra el océano de datos.

Tabla 8.15: Descripción de las series de la gráfica Consumo por cliente

Dashboard Datos asignados

Muestra el histórico de cambios en el volumen de datos asignados al MSSP en el último año.

Puesto que Cytomic Orion asigna al MSSP un volumen de 5 Gigabytes de datos por equipo administrado, si se produce un cambio en el número de equipos gestionados, el volumen total de datos se ajustará proporcionalmente.

Permisos requeridos

La cuenta de usuario requiere el permiso **Ver el dashboard de consumo de datos** para acceder al contenido del dashboard.

Acceso al panel

- Haz clic en el menú superior **Dashboard** y en el panel lateral **Consumo de datos**.
- Haz clic en el menú de pestañas **Datos asignados**.

Histórico de datos asignados

El dashboard contiene los siguientes elementos:

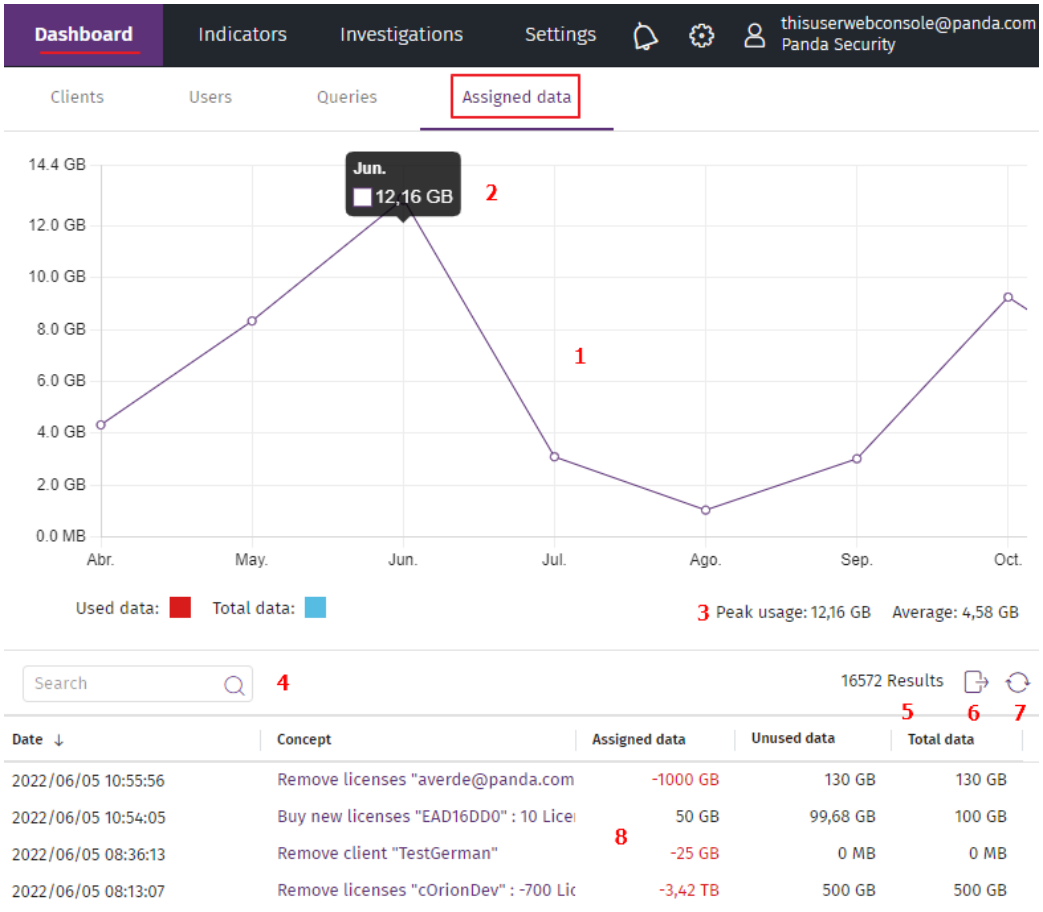


Figura 8.13: Dashboard Datos asignados

- **Gráfica de lineas (1)**: muestra la evolución de los datos asignados al MSSP y la de los datos consumidos.
- **Tooltip (2)**: desliza el ratón sobre los puntos de la gráfica de lineas. Se mostrará un tooltip con el contenido de la coordenada X e Y del punto seleccionado.
- **Estadísticas de consumo (3)**: muestra el pico de consumo y el máximo de datos recomendado por Cytomic en el intervalo elegido.
- **Buscar (4)**: filtra el listado de operaciones registradas según el contenido del campo **Concepto**.
- **Resultados (5)**: número de cambios registrados en la asignación de datos.
- **Exportar**: descarga un fichero en formato Excel con el contenido del listado **(8)**.
- **Recargar (7)**: refresca el contenido del listado **(8)**.
- **Listado (8)**: registro de los cambios en la asignación del volumen de datos en el ultimo año.

Atributo	Descripción
Fecha	Fecha en la que se ha producido el cambio en la asignación del volumen de

Atributo	Descripción
	datos.
Concepto	Tipo de cambio registrado: • **Reducción de licencias**: se reduce el volumen de datos asignado al MSSP en 5 Gbytes por cada equipo que ha dejado de administrar. • **Compra de licencias**: se incrementa el volumen de datos asignado al MSSP en 5 Gbytes por cada nuevo equipo administrado. • **Baja de cliente**: se reduce el volumen de datos asignado al MSSP correspondiente al total de equipos que pertenecen al cliente que ya no administra. • **Nuevo cliente**: se incrementa el volumen de datos asignado al MSSP correspondiente al número de equipos que pertenecen al cliente nuevo.
Datos asignados	Incremento o disminución del volumen de datos asignados al MSSP que se corresponde con el cambio registrado.
Datos sin utilizar	Resta del volumen de datos asignado menos el volumen de datos utilizado en el momento en que se registró el cambio de volumen.
Datos totales	Total de datos asignados al MSSP después de la operación registrada.

Tabla 8.16: Descripción del listado

Email de notificación de consumo

Los analistas reciben una notificación por correo electrónico cuando cualquiera de las cuentas que acceden a la consola de Cytomic Orion registra un consumo mayor que el establecido para el SOC / MSSP. Consulta **Volumen de datos asignado**.

Destinatarios de la notificación

Para recibir la notificación por correo electrónico, es necesario cumplir con los siguientes requisitos:

- La cuenta tiene asociado el permiso **Ver el dashboard de consumo de datos**. Consulta **Descripción de los permisos implementados** en la página **60**.
- La cuenta tiene activada la opción **Notificarme por correo electrónico cuando los datos consumidos en consultas se aproximen a la cuota máxima** en el menú superior **Configuración**, menú lateral **Mis preferencias**.

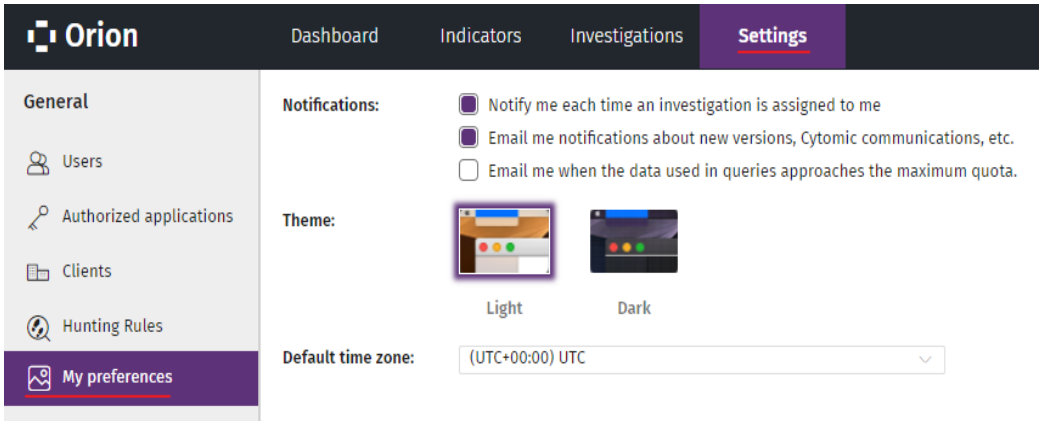


Figura 8.14: Ventana para activar las notificaciones por volumen de datos consumidos

Cuando Cytomic Orion detecta que alguna de las cuentas excede el volumen de datos total asignado al SOC / MSSP, envía una notificación a todos los usuarios que cumplen los requisitos.

Número de notificaciones enviadas

Cytomic Orion establece tres tramos en el consumo de datos: 80%, 90% y 100%. Cuando un usuario de la consola supera alguno de los límites establecidos, se envía un correo de notificación. Para minimizar el envío de correos, solo se envía el correo una única vez por cada límite sobrepasado.

Si el volumen de datos asignado al MSSP / SOC varía, se volverá a enviar un correo cada vez que se sobrepase alguno de los límites establecidos.

Información suministrada en el correo electrónico

Campo	Descripción
Asunto del correo	Indica el tramo superado, con el siguiente código de color: • **80% y 90%**: color naranja. • **100%**: color rojo.
Fecha	Fecha en la que se registró el consumo por encima del tramo indicado en el asunto del correo.
Datos consumidos	Volumen de datos consumidos cuando se envió la notificación.
Cuota permitida	Volumen total de datos asignados al SOC / MSSP.

Tabla 8.17: Descripción del correo de notificación

Capítulo 9

Investigar el flujo de eventos

Cytomic Orion ofrece dos módulos muy flexibles y potentes para recuperar de forma selectiva información almacenada en el océano de datos de Cytomic: **Consultas avanzadas SQL** y **Consultas mediante asistente**. Ambos módulos recuperan la información generada por la monitorización de cada proceso ejecutado en el parque del cliente, mediante consultas creadas por el propio analista o diseñadas por Cytomic. Esta información se utiliza en el triaje de indicios y para profundizar en las investigaciones en curso.

Cytomic Orion distribuye en varias tablas toda esta información según su tipo, y la mantiene en la plataforma a disposición del analista durante 1 año.

El tiempo de retención de la telemetría en el océano de datos es de 1 año.

CONTENIDO DEL CAPÍTULO

Módulo de consultas avanzadas SQL

Acceso al módulo de consultas avanzadas SQL

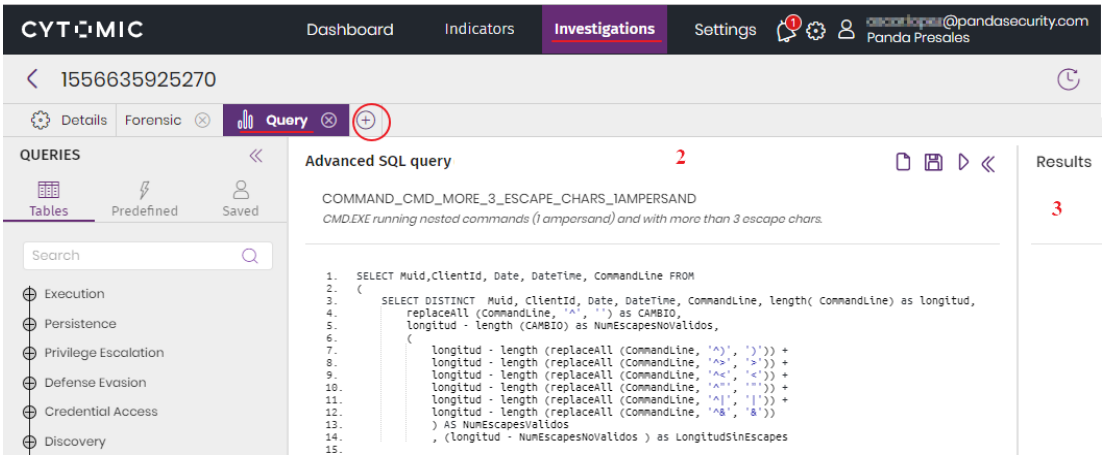


Figura 9.1: Pestaña Exploración de procesos

- En el menú superior **Investigaciones**, haz clic en la investigación que contiene el indicio generado por las reglas de hunting, o crea una investigación nueva haciendo clic en el botón **Nueva investigación** situado en la parte superior derecha de la ventana. Consulta **Crear una investigación** en la página **103**para obtener más información.
- En el menú de pestañas pasa el ratón por encima del + para desplegar el menú de contexto y elige **Consulta avanzada SQL**. Se abrirá la ventana del editor de consultas libre con la siguiente estructura:
    - **Panel lateral Consultas (1)** : permite acceder a las consultas previamente almacenadas y al modelo de datos.
    - **Panel Consulta avanzada SQL (2)**: permite construir nuevas consultas o modificar las diseñadas previamente.
    - **Panel de resultados (3)**: presenta los resultados de la ejecución de consultas.

Permisos requeridos

La cuenta de usuario requiere el permiso **Acceso a consultas avanzadas** para poder ejecutar sentencias SQL. Los resultados que obtiene el analista estarán limitados por la visibilidad de los clientes asociada a su cuenta de usuario. Consulta **Acceso, control y supervisión de la consola de análisis** en la página **47**.

Panel lateral Consultas (1)

Permite acceder a las consultas previamente almacenadas por el analista o diseñadas por Cytomic. Contiene los siguientes elementos:

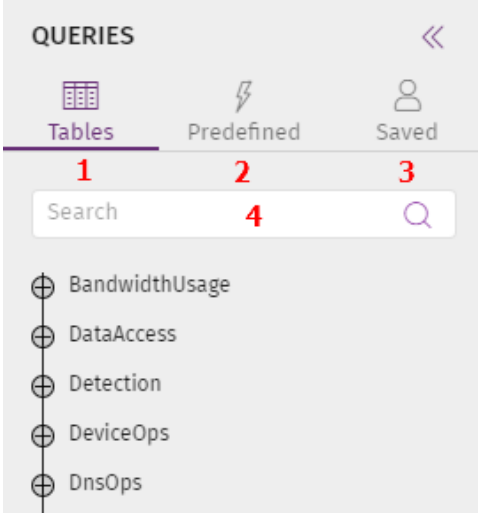


Figura 9.2: Panel lateral Consultas

- **Tablas (1):** contiene el modelo de datos utilizado por Cytomic Orion para organizar la información recogida en la monitorización de procesos.
- **Predefinidas (2)**: son las sentencias SQL diseñadas por el analista que ha guardado por utilizarlas de forma recurrente.
- **Guardadas (3)**: librería de sentencias SQL organizadas en árbol y diseñadas por Cytomic.
- **Buscar (4)**: caja de texto para localizar las consultas de forma rápida.

Tablas (1)

> *Para obtener el significado de los campos incluidos en el modelo de datos consulta el capítulo* ***Formato de los eventos utilizados en Cytomic Orion*** *en la página* ***402***

Muestras las tablas y los campos disponibles para que el analista construya sus propias consultas. Para acelerar el desarrollo haz clic en un campo y éste se copiará automáticamente en el panel **Consulta avanzada SQL**, en la posición marcada por el cursor.

En la pestaña **Tablas** se incluye toda la información recogida de los equipos del parque del cliente, organizada en 14 tablas que representan distintas técnicas y acciones ejecutadas frecuentemente por los procesos que forman parte de un ataque informático:

Tabla	Descripción
BandwidthUsage	Contiene un registro con el volumen de información manejada en cada operación de transferencia de datos ejecutada por el proceso.

Tabla	Descripción
DataAccess	Contiene un registro por cada operación ejecutada por el proceso y que se corresponda a un acceso a ficheros de datos alojados en dispositivos internos de almacenamiento masivo.
Detection	Contiene un registro por cada detección realizada por las protecciones activadas del software de seguridad Cytomic EDR instalado en el equipo.
DeviceOps	Contiene un registro por cada acceso a un dispositivo externo ejecutado por el proceso.
DnsOps	Contiene un registro por cada acceso al servidor de nombres DNS ejecutado por el proceso.
Download	Contiene un registro por cada descarga de datos ejecutada por el proceso.
Evidences	Contiene un registro por cada indicio detectado sin agrupar.
Indicators	Contiene el registro de indicios agrupados. Para conocer cómo Cytomic Orion agrupa los indicios, consulta **Agrupación de indicios** en la página **74**. La tabla **Indicators** coincide con el listado de indicios mostrado en la consola de Cytomic Orion. Consulta **Listado de indicios** en la página **73**.
LoginOutOps	Contiene un registro por cada operación de inicio o cierre de sesión efectuado por el usuario.
NetworkOps	Contiene un registro por cada operación de red ejecutada por el proceso.
ProcessOps	Contiene eventos de procesos que realizan operaciones con el disco duro del equipo.
RegistryOps	Contiene una entrada por cada acceso al registro de Windows realizado por el proceso.
RemediationOps	Contiene los eventos de detección, bloqueo y desinfección de la

Tabla	Descripción
	solución de seguridad instalada en el equipo del usuario o servidor.
ScriptOps	Contiene un registro por cada operación ejecutada por un proceso de tipo script.
SystemOps	Contiene un registro por cada operación ejecutada por el motor WMI del sistema operativo Windows.
UserNotification	Contiene un registro por cada notificación que se le presenta al usuario junto a su respuesta si la hubiera.

Tabla 9.1: Tablas disponibles en la pestaña Tablas

A continuación se indican los campos incluidos en cada tabla.

Tabla	Campos
BandwidthUsage	DateTime, LocalDateTime, PandaTimeStatus, TimeStamp, MUID, ClientId, EventType, ParentPid, ParentMd5, ParentDrive, ParentPath, ParentFilename, BytesSent, BytesReceived, LoggedUser, Date, InsertionDateTime.
DataAccess	DateTime, LocalDateTime, PandaTimeStatus, TimeStamp, MUID, ClientId, EventType, ParentPid, ParentMd5, ParentDrive, ParentPath, ParentFilename, ParentAttributes, ChildPath, ChildFilename, ChildAttributes, LoggedUser, ConfigString, Date, InsertionDateTime.
Detection	DateTime, LocalDateTime, PandaTimeStatus, TimeStamp, MUID, ClientId, EventType, ParentMd5, WinningTech, DetectionId, Date, InsertionDateTime.
DeviceOps	DateTime, LocalDateTime, PandaTimeStatus, TimeStamp, MUID, ClientId, EventType, NotificationType, DeviceType, UniqueId, IsDenied, IdName, ClassName, FriendlyName, Description, Manufacturer, PhoneDescription, Date, InsertionDateTime.
DnsOps	DateTime, LocalDateTime, PandaTimeStatus, TimeStamp, MUID, ClientId, EventType, ParentCount, ParentMd5, ParentPid, ParentPath, FailedQueries, QueriedDomainCount, DomainList, Date, InsertionDateTime.

Tabla	Campos
Download	DateTime, LocalDateTime, PandaTimeStatus, TimeStamp, MUID, ClientId, EventType, ParentMd5, ParentDrive, ParentPath, ParentFilename, ChildMd5, ChildDrive, ChildPath, ChildFilename, ChildUrl, LoggedUser, Date, InsertionDateTime.
Evidences	EvidenceDateTime, TimeStamp, Muid, ClientId, HuntingRuleName, HuntingRuleId, HuntingRuleMode, HuntingRuleSeverity, HuntingRuleMitre, Details, InsertionDateTime, TTLDays
Indicators	AlertDateTime, TimeStamp, Muid, ClientId, HuntingRuleName, HuntingRuleId, HuntingRuleType, HuntingRuleMode, HuntingRuleSeverity, HuntingRuleMitre, Details, Occurrences, PandaAlertId, InsertionDateTime, TTLDays
LoginOutOps	DateTime, LocalDateTime, PandaTimeStatus, TimeStamp, MUID, ClientId, EventType, Actiontype, SessionType, ErrorCode, Username, Interactive, RemoteMachineName, RemoteIp, RemotePort, Date, InsertionDateTime.
NetworkOps	DateTime, LocalDateTime, PandaTimeStatus, TimeStamp, MUID, ClientId, EventType, ParentPid, ParentMd5, ParentDrive, ParentPath, ParentFilename, Protocol, RemoteIp, RemotePort, LocalIp, LocalPort, Direction, LoggedUser, Ipv4Status, DetectionId, Hostname, Times, Date, InsertionDateTime.
ProcessOps	DateTime, LocalDateTime, PandaTimeStatus, TimeStamp, MUID, ClientId, EventType, Operation, ParentStatus, ParentMd5, ParentDrive, ParentPath, ParentFilename, ParentPid, ParentAttributes, ChildStatus, ChildMd5, ChildDrive, ChildPath, ChildFilename, ChildPid, ChildAttributes, ChildClassification, CommandLine, RemediationResult, Action, ServiceLevel, WinningTech, DetectionId, LoggedUser, RemoteIp, RemoteMachineName, RemoteUsername, Date, InsertionDateTime.
RegistryOps	DateTime, LocalDateTime, PandaTimeStatus, TimeStamp, MUID, ClientId, EventType, ParentPid, ParentMd5, ParentDrive, ParentPath, ParentFilename, RegistryAction, Key, Value, ValueDataLength, ValueData, LoggedUser, ConfigString, Date, InsertionDateTime.

Tabla	Campos
RemediationOps	DateTime, LocalDateTime, PandaTimeStatus, TimeStamp, MUID, ClientId, EventType, ParentMd5, ParentDrive, ParentPath, ParentFilename, ChildMd5, ChildDrive, ChildPath, ChildFilename, CommandLine, WinningTech, DetectionId, Action, ServiceLevel, RemoteIp, RemoteMachineName, RemoteUsername, LoggedUser, ExploitOrigin, Url, ChildClassification, Date, InsertionDateTime.
ScriptOps	DateTime, LocalDateTime, PandaTimeStatus, TimeStamp, MUID, ClientId, EventType, ParentMd5, ParentDrive, ParentPath, ParentFilename, ParentPid, ParentAttributes, ChildMd5, ChildDrive, ChildPath, ChildFilename, ChildAttributes, ChildFileSize, ChildClassification, CommandLine, ServiceLevel, LoggedUser, Date, InsertionDateTime.
SystemOps	DateTime, LocalDateTime, PandaTimeStatus, TimeStamp, MUID, ClientId, EventType, Type, ObjectName, CommandLine, MachineName, Username, IsLocal, ExtendedInfo, ChildMd5, Date, InsertionDateTime.
UserNotification	DateTime, LocalDateTime, PandaTimeStatus, TimeStamp, MUID, ClientId, EventType, ParentMd5, ParentDrive, ParentPath, ParentFilename, ChildMd5, ChildDrive, ChildPath, ChildFilename, ChildClassification, ChildFirstSeen, WinningTech, DetectionId, RemediationResult, BlockReason, ServiceLevel, Date, InsertionDateTime.

Tabla 9.2: Campos disponibles por tabla

Significado de los campos de tipo fecha

Cytomic Orion soporta varios campos de tipo fecha que ayudan a diferenciar el origen del dato, y a prevenir errores frecuentes que se dan cuando el analista trabaja con eventos:

- **TimeStamp**: fecha real UTC en formato epoch (número de segundos transcurridos desde el 1 de enero de 1970) del momento en que se produjo el evento en el equipo del cliente. Es una fecha procedente de un cálculo interno de Cytomic Orion que puede no coincidir con la fecha del equipo donde se registró el evento si este último la tiene mal configurada.
- **DateTime**: igual que TimeStamp pero en formato Fecha:Hora.
- **Date**: igual que TimeStamp pero en formato Fecha.

- **LocalDateTime**: fecha en formato UTC que tenía el equipo en el momento en que se produjo el evento registrado. Esta fecha depende de la configuración del equipo y por lo tanto puede ser errónea.
- **PandaTimeStatus**: contenido de los campos DateTime, Date y LocalDateTime:
  - **0**: fecha real no soportada por ser un evento antiguo.
  - **1**: fecha real soportada pero obtenida mediante un calculo por no encontrarse disponible el servidor Cytomic.
  - **2**: fecha real proporcionada por el servidor Cytomic.
- **InsertionDateTime**: fecha en formato UTC del momento en el que Cytomic registró en sus servidores el evento enviado por el equipo. Esta fecha siempre será algo posterior al resto de fechas ya que los eventos se encolan para ser procesados.

Predefinidas (2)

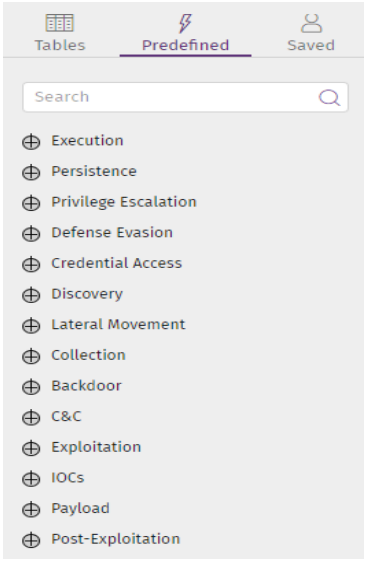


Figura 9.3: Árbol de grupos de primer nivel de la biblioteca de consultas

Muestra la biblioteca de consultas diseñada por Cytomic, ordenada en 14 grupos y subgrupos que representan las técnicas y tácticas descritas por MITRE más frecuentemente vistas en el contexto de un ataque informático o de una infección.

Al hacer doble clic en un grupo se mostrarán los nodos y subnodos y las consultas predefinidas que cuelgan del mismo. Al hacer doble clic en una consulta, ésta se cargará en el panel **Consulta avanzada SQL** junto a su nombre y su descripción.

Las consultas predefinidas no se pueden modificar pero pueden ser copiadas y modificadas por el analista. Consulta **Barra de gestión de consultas (1)**.

A continuación se muestran los grupos disponibles y una descripción general del tipo de consultas predefinidas que contienen:

Grupo	Descripción
Execution	Muestra la ejecución de procesos sospechosos de pertenecer a un ataque por ser utilizados de forma diferente a la habitual: parámetros poco habituales, ejecución de scripts PowerShell, Autoit o WMI, etc.
Persistence	Muestra la ejecución de acciones por parte de procesos que intentan ganar persistencia en el equipo para sobrevivir a un reinicio del sistema.
Privilege Escalation	Muestra la ejecución de acciones encaminadas a ganar permisos superiores a los heredados según el contexto de ejecución inicial.
Defense Evasion	Muestra la ejecución de acciones encaminadas a evitar las defensas configuradas por el administrador de la red, como por ejemplo evitar la configuración del cortafuegos local, forzar la detención del proceso de antivirus instalado, evitar la infección de otros tipos de malware vía protocolo SMB, etc.
Credential Access	Muestra el acceso no autorizado a la SAM del equipo para obtener las credenciales de usuario.
Discovery	Muestra las acciones ejecutadas para obtener información del entorno de ejecución del malware mediante programas tales como `whoamI`, `nbstat`, `qprocess` y otros.
Lateral Movement	Muestra las acciones encaminadas a propagar el malware a otros equipos dentro de la red para recoger información y ganar una posición de ventaja que maximice las probabilidades de éxito del hacker.
Backdoor	Muestra los intentos de instalación de una puerta trasera para acceder al equipo de forma remota.
Exploitation	Muestra los intentos de explotación de procesos vulnerables.
IOCs	Muestra los procesos que ejecutan IOCs (indicadores de compromiso) conocidos.
Payload	Detecta la ejecución de programas de minado de Bitcoins.
Post-Exploitation	Muestra los procesos que ejecutan acciones que se suceden comúnmente después de haber explotado un proceso vulnerable (creación de usuarios,

Grupo	Descripción
	parada de servicios, etc).
PUPS	Muestra las acciones típicas de procesos clasificados como PUP (programas no deseados) generalmente relativas a la instalación de barras de navegación y recursos similares para mostrar publicidad en el equipo del cliente.

Tabla 9.3: Grupos de consultas predefinidas disponibles

Guardadas (3)

Contiene todas las consultas que el analista ha diseñado y guardado a lo largo del tiempo. Estas consultas son visibles por las cuentas de usuario creadas en cada MSSP / MDR o SOC de forma individual, y por lo tanto no son compartidas entre distintos MSSPs / MDRs.

Las consultas almacenadas se agrupan en función del tipo y subtipo elegido en su creación, formando un árbol que el analista puede navegar de forma sencilla para localizar la consulta que necesite ejecutar.

Panel Consulta avanzada SQL

> *Para obtener información sobre las cláusulas SQL compatibles con Cytomic Orion, los tipos de datos admitidos y las funciones disponibles consulta* ***Sintaxis SQL del módulo Consultas avanzadas*** *en la página* ***271****.*

Permite construir desde cero o modificar una sentencia SQL previamente almacenada. Contiene los siguientes elementos:

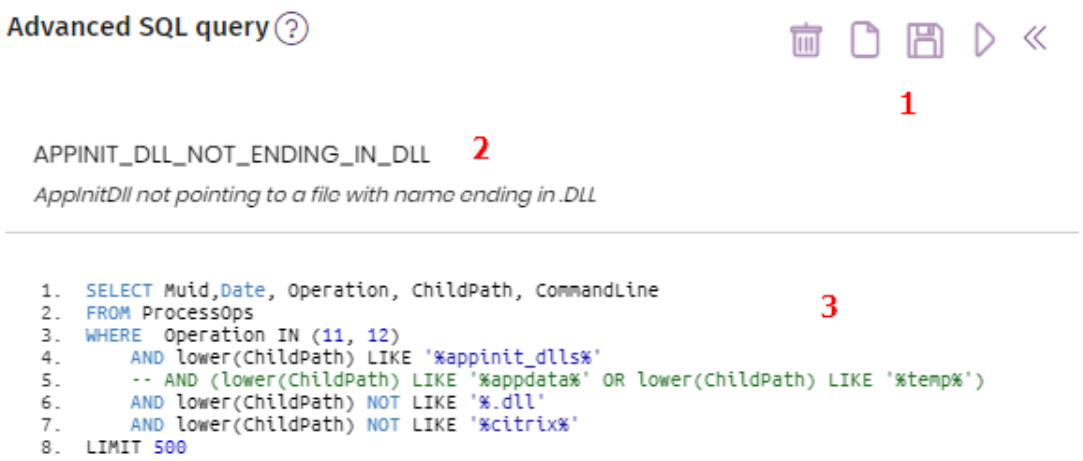


Figura 9.4: Panel editor de consultas

- **Barra de gestión de consultas (1)**: permite borrar, ejecutar, detener y salvar una consulta ya diseñada.
- **Nombre de la consulta y descripción (2)**.
- **Panel de diseño de la consulta (3)**: permite escribir la consulta o modificar una previamente diseñada. Cada línea está numerada y la consola resalta en color azul la sintaxis del lenguaje SQL (palabras clave, símbolos reservados etc.) así como las cadenas de caracteres, para facilitar su lectura.

Barra de gestión de consultas (1)

Permite ejecutar acciones para gestionar las consultas. Contiene los iconos mostrados a continuación:

- **Borrar consulta** : borra la consulta almacenada definida por el analista del SOC y seleccionada en el panel biblioteca. Las consultas predefinidas por Cytomic no se pueden borrar.
- **Limpiar consulta**: borra el contenido del panel **Consulta avanzada SQL**.
- **Salvar consulta** : al hacer clic en este icono se abre una ventana para introducir el nombre de la consulta y la táctica y técnica a la que pertenecerá dentro del árbol de grupos. Al hacer clic en el botón **Aceptar** la consulta se añadirá al repositorio de consultas almacenadas. Para mostrar las búsquedas diseñadas por los analistas del MSSP / MDR consulta **Guardadas (3)**.
- **Enviar consulta** y detener consulta : permite ejecutar y detener la ejecución de la consulta mostrada en el panel **Consulta avanzada SQL**. Los errores de sintaxis y comunicación se mostrarán en el panel de resultados. También es posible ejecutar la consulta pulsando la combinación Control + Enter en el teclado. Consulta **Panel de resultados (3)**.

Panel de resultados (3)

Presenta los resultados en formato tabla e indica si hay algún error de sintaxis en la sentencia SQL o problema con el servidor. Para filtrar y buscar datos dentro de la tabla consulta **Herramientas para configurar los listados** en la página **39**.

El panel de resultados dispone de las herramientas siguientes:

- **Buscar** : admite búsquedas parciales que se efectúan sobre el contenido de todos los campos devueltos por la sentencia SQL.
- **Resultados**: indica el número de resultados mostrados por la sentencia SQL.
- **Zona horaria**: establece la zona horaria de los campos de tipo fecha y del contenido de las búsquedas.

- **Exportar** : salva en un fichero .csv los resultados de la sentencia SQL. Las columnas incluidas en el fichero se corresponden con las mostradas en el listado.

Menú de contexto asociado a las tablas de resultados

Al hacer clic con el botón derecho del ratón se muestra un menú de contexto con diferentes opciones que permiten al analista acceder a otras áreas de la consola de forma rápida:

Opción	Descripción
Investigar equipo	Requiere los campos MUID y DateTime. Abre la consola de investigación para mostrar los eventos registrados en el equipo y fecha indicados.
Añadir entidad de interés	Marca una entidad para mostrarla en el subpanel **Entidades de interés** en la investigación asociada, y así permitir un acceso más rápido a la información.
Mostrar equipos con el archivo padre	Requiere el campo ParentMD5. Lanza una búsqueda de los equipos que tienen algún evento registrado en el campo ParentMD5. Consulta **Investigación de un fichero: MD5** en la página **188**.
Mostrar equipos con el archivo hijo	Requiere el campo ChildMD5. Lanza una búsqueda de los equipos que tienen algún evento registrado en el campo ChildMD5. Consulta **Desde una investigación recién creada o en curso** en la página **187**.
Investigación automatizada	Muestra una lista de las plantillas de notebooks creadas. El analista podrá abrir una plantilla y Cytomic Orion rellenará automáticamente sus parámetros compatibles con los resultados de la fila seleccionada. Consulta **Investigación con notebooks** en la página **220**.
Detalles del equipo	Muestra información del equipo. Requiere el campo MUID.

Tabla 9.4: Menú de contexto de la tabla resultados

Optimización de las sentencias SQL

Cytomic Orion mantiene un índice para cada una de las tablas que almacenan los eventos recogidos de los equipos de usuario y servidores. Al utilizar los campos que forman el indice en las clausulas `WHERE` se acelera de forma muy notable la ejecución de las consultas, de otra forma, el motor de base de datos se ve obligado a recorrer la tabla pertinente al completo en busca de la información solicitada. Los campos que forman el indice son los siguientes:

- ClientID
- MUID
- DateTime

Módulo Asistente para consultas

Acceso al módulo Consultas mediante asistente

El módulo Consultas mediante asistente simplifica el diseño de búsquedas a través de un asistente visual que evita conocer la sintaxis del lenguaje SQL y por lo tanto acelera los análisis de los técnicos.

Para acceder a la pestaña **Consultas mediante asistente** sigue los pasos mostrados a continuación:

- En el menú superior **Investigaciones**, haz clic en la investigación que contiene el indicio generado por las reglas de hunting a investigar, o crea una investigación nueva haciendo clic en el botón **Nueva investigación** situado en la parte superior derecha de la ventana. Consulta **Crear una investigación** en la página **103** para obtener más información.
- En el menú de pestañas pasa el ratón por encima del + para desplegar el menú de contexto y elige **Consultas mediante asistente**. Se abrirá la ventana del asistente con la estructura mostrada en**Estructura general del asistente de consultas**.

Permisos requeridos

La cuenta de usuario requiere el permiso **Acceso al asistente para consultas** para poder utilizar este recurso. Los resultados que obtiene el analista estarán limitados por la visibilidad de los clientes asociada a su cuenta de usuario. Consulta **Acceso, control y supervisión de la consola de análisis** en la página **47**.

Estructura general del asistente de consultas

Los bloques utilizados para construir una búsquedas con el asistente de consultas son los siguientes:

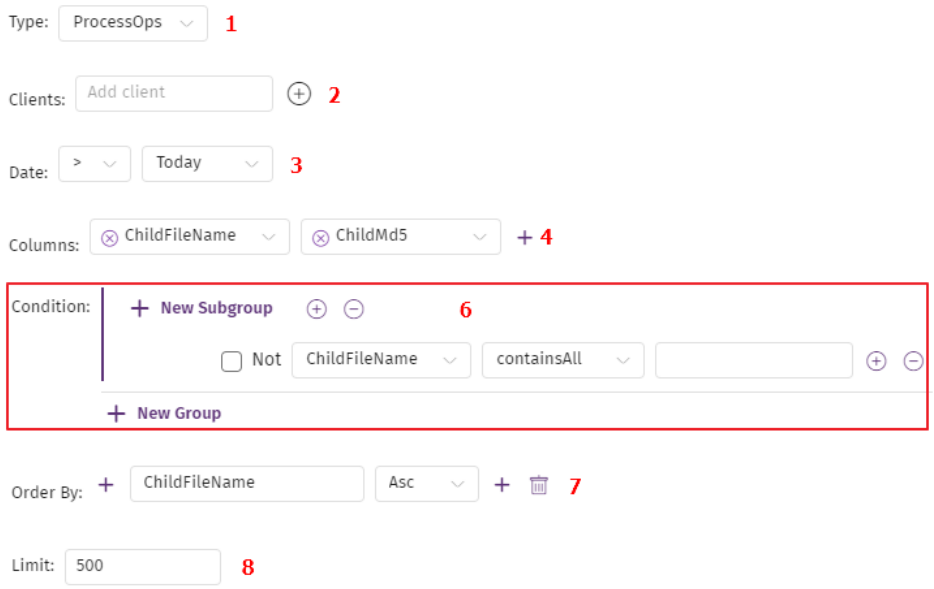


Figura 9.5: Bloques principales del constructor de consultas

- **Tipo (1)**: es la fuente de datos contra la que se ejecutará la consulta. En el desplegable se listan las tablas mostradas en **Tablas (1)**. Equivale a la cláusula `FROM [tabla]` de SQL.
- **Clientes (2)**: filtra los datos por cliente. El analista solo se puede filtrar por aquellos clientes sobre los que tiene visibilidad.

> *Es obligatorio especificar al menos un cliente en cada consulta.*

- **Fecha (3)**: condición que filtra los datos mostrados en la búsqueda. Equivale a una cláusula `WHERE Timestamp [comparador] DateTime`.
  - Elige el tipo de comparador: **mayor**, **menor**, **igual**, **mayor que** o **menor que**.
  - Selecciona la fecha a comparar: **Hoy**, **Ayer** o una fecha específica.
- **Columnas (4)**: son los datos a recuperar. Equivalente a las columnas de la cláusula `SELECT [columna1, columna2...]` de SQL.
- **Condición (6)**: equivale a la clausula `WHERE` de SQL. Consulta más adelante para una descripción en detalle de esta cláusula.
- **Ordenar por (7)**: los resultados son ordenados tomando como referencia el contenido de los campos indicados, de forma ascendente **Asc** o descendente **Desc**. Equivale a la clausula `ORDER BY [campo1, campo2...]` de SQL. Si se indica más de un campo se ordenará según la disposición de los campos en el bloque.
- **Limite (8)**: limita el número de registros devueltos en la búsqueda. Equivale a la clausula `LIMIT` o `TOP` de SQL.

Estructura del bloque Condición

El bloque condición equivale a la clausula `WHERE` de SQL y admite un alto grado de flexibilidad a la hora de especificar las condiciones de búsqueda.

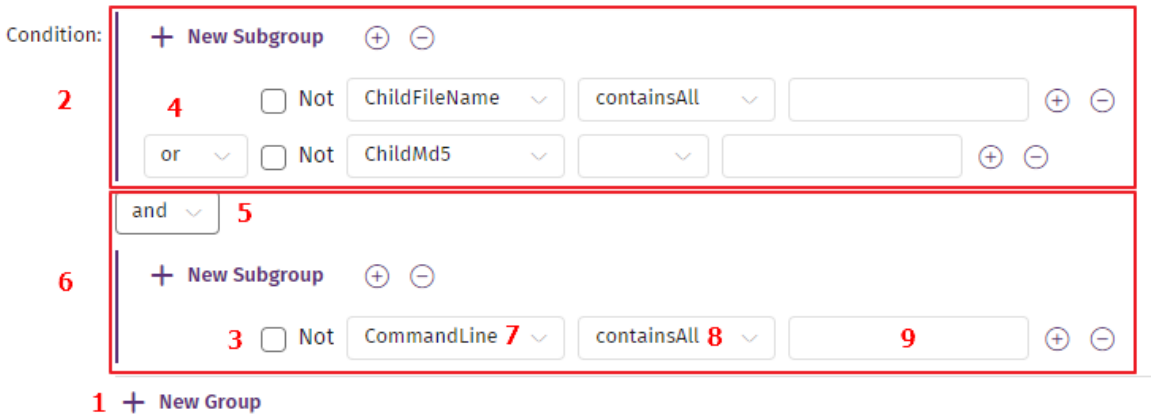


Figura 9.6: Estructura del bloque Condición con dos grupos relacionados por el operador lógico AND

El bloque **Condición** se divide en grupos de condiciones. Dentro de un grupo de condiciones puede haber una única condición (bloque **(6)**) o varias (bloque **(2)**).

Condiciones

Una condición simple **(6)** está formada por el nombre de una columna **(7)**, un operador de comparación **(8)** (consulta **Operadores de comparación**) y el valor a comparar **(9)** . Adicionalmente, puede tener asociado un operador booleano de negación **(3)**.

Una condición compuesta **(2)** está formada por varias condiciones simples que se relacionan entre sí mediante los operadores AND y OR **(4)**.

Grupos

Cada nuevo grupo creado es equivalente a introducir una condición simple o compuesta rodeada de paréntesis en la clausula `WHERE` de la sentencia SQL correspondiente.

Se pueden crear varios grupos con el botón **Nuevo grupo (1)** que se relacionarán entre sí mediante un operador lógico AND / OR **(5)**.

A su vez, dentro de un grupo se pueden crear uno o más grupos de condiciones simples o compuestas mediante los botones **Nuevo grupo (10)** de segundo nivel.

Operadores de comparación

- **ContainsAny**: operador equivalente al "like" de SQL, busca una subcadena de caracteres.
- **equals**: busca una cadena de caracteres exacta.
- **endsWithAny**: busca una cadena de caracteres al final.
- **startsWithAny**: busca una cadena de caracteres al inicio.

- **containsInOrder** : busca hasta 3 subcadenas de caracteres en el orden indicado. Especificar una única cadena es equivalente a la opción **ContainsAny**. Se mostrarán los resultados que contengan todas las cadenas especificadas (operador lógico AND) y en el orden establecido.
- **Operadores booleanos**: se admiten los operadores logicos básicos ('<','>','>=','<=','==')
- **matches** : permite escribir una expresión regular en formato java. Para obtener más información sobre el formato de las expresiones regulares, los caracteres de escape y otros detalles de la implementación RegEx en Java consulta **https://docs.oracle.com/javase/8/docs/api/java/util/regex/Pattern.html.**

Búsquedas sensibles a mayúsculas

Por defecto, todas las condiciones de tipo cadena de caracteres se establecen sin tener en cuenta mayúsculas y minúsculas ("case insensitive"), pero el analista puede cambiar este comportamiento estableciéndolo en el desplegable asociado.

Figura 9.7: Desplegable para establecer el tipo de comparación en campos de tipo cadenas de caracteres

Los campos **ParentFilename** y **ChildFilename** se almacenan en el océano de datos en minúsculas, ya que se extraen de los campos **ParentPath** o **ChildPath** respectivamente. Después de la extracción, se ejecuta de forma automática un proceso de normalización en el que se cambian todas las mayúsculas por minúsculas. Cualquier Hunting rule donde se especifique "case sensitive" y utilice letras en mayúsculas para buscar en **ParentFilename** o **ChildFilename** no devolverá ningún resultado. Sin embargo, los campos **ParentPath** o **ChildPath** no sufren este proceso de normalización, y se almacenan en el océano de datos tal cual. En este caso sí tiene sentido utilizar "case sensitive" o "case insensitive" según las necesidades del analista.

Panel de resultados

Presenta los resultados en formato tabla. Para filtrar y buscar datos dentro de la tabla consulta **Herramientas para configurar los listados** en la página **39**.

> *Es posible copiar y pegar la tabla de resultados a un fichero de texto o Excel. Para ello haz clic en un elemento de la tabla y arrastra el ratón hasta completar la selección. Después presiona ctrl+c en el teclado.*

Menú de contexto asociado a las tablas de resultados

Al hacer clic con el botón derecho del ratón se muestra un menú de contexto con diferentes opciones que permiten al analista acceder a otras áreas de la consola de análisis de forma rápida:

Opción	Descripción
Investigar equipo	Requiere los campos MUID y DateTime. Abre la consola de investigación para mostrar los eventos registrados en el equipo y fecha indicados.
Añadir entidad de interés	Marca una entidad para mostrarla en el subpanel **Entidades de interés** en la investigación asociada y así permitir un acceso más rápido a la información.
Mostrar equipos con el archivo padre	Requiere el campo ParentMD5. Lanza una búsqueda de los equipos que tienen algún evento registrado en el campo ParentMD5. Consulta **Investigación de un fichero: MD5** en la página **188**.
Mostrar equipos con el archivo hijo	Requiere el campo ChildMD5. Lanza una búsqueda de los equipos que tienen algún evento registrado en el campo ChildMD5. Consulta **Desde una investigación recién creada o en curso** en la página **187**.
Investigación automatizada	Muestra una lista de las plantillas de notebooks creadas. El analista podrá abrir una plantilla y Cytomic Orion rellenará automáticamente sus parámetros compatibles con los resultados de la fila seleccionada. Consulta **Investigación con notebooks** en la página **220**.
Detalles del equipo	Muestra información del equipo. Requiere el campo MUID.

Tabla 9.5: Menú de contexto de la tabla resultados

Capítulo 10

Investigaciones asistidas

Las investigaciones asistidas facilitan al analista la búsqueda de información sobre un indicio en el océano de eventos. Esta herramienta presenta la ventaja de no requerir conocimientos de SQL ni del esquema de la base de datos que Cytomic Orion utiliza para almacenar la telemetría recogida de los equipos de los usuarios.

El funcionamiento de una investigación asistida es similar al de un asistente de configuración: el proceso se desarrolla como una secuencia de preguntas, que a su vez dependen de las respuestas generadas en los pasos previos. Conforme el analista avanza en el proceso, la investigación muestra nuevas preguntas que le permiten navegar el océano de eventos de forma natural, como si de una conversación se tratara.

CONTENIDO DEL CAPÍTULO

Acceso a las investigaciones asistidas y contexto de la investigación

Para delimitar el análisis, las investigaciones asistidas acceden a un subconjunto de todo el océano de datos disponible en Cytomic Orion. Este subconjunto de eventos se conoce como contexto, y depende del punto de inicio que el analista elige para comenzar su investigación:

- **Entidad de interés Equipo**
- **Indicio**

- **Evento**

Al margen del punto de partida, Cytomic Orion siempre añade al contexto el identificador del cliente al que pertenece el equipo involucrado en la investigación, y el MUID del equipo. Además, establece un intervalo que abarca los 3 últimos días desde el momento en que se inició la investigación asistida.

Aunque el contexto se establece cuando el analista crea la investigación asistida, es posible que ésta cambie en el transcurso de su análisis si accede a datos fuera de los parámetros establecidos. En este caso, la consola mostrará el mensaje **Investigation scope changed!** e indicará el nuevo contexto que se aplicará a partir de ese momento.

Acceso a las investigaciones asistidas desde una entidad de interés Equipo

Al crear una investigación asistida desde una entidad de interés Equipo, Cytomic Orion utiliza la siguiente información para generar el contexto:

- Identificador de cliente al que pertenece el equipo
- Identificador de equipo
- Intervalo de 3 días desde la creación de la investigación

Para crear una investigación asistida desde una entidad de interés Equipo:

- Haz clic en el menú superior **Investigaciones**. Se mostrará el listado de investigaciones creadas.
- Selecciona una investigación. Se abrirá la investigación con los indicios asignados.
- En el panel **Entidades de interés**, haz clic en el icono ⋮ de un equipo. Se mostrará un menú de contexto.
- Selecciona **Investigaciones asistidas**. Se abrirá la ventana **Investigaciones asistidas [#Nombre#]** con el contexto tomado del equipo elegido.

Acceso a las investigaciones asistidas desde un indicio

Al crear una investigación asistida desde un indicio, Cytomic Orion utiliza la siguiente información para generar el contexto:

- Identificador de cliente al que pertenece el equipo
- Identificador de equipo
- Intervalo de 3 días desde la creación de la investigación

Para crear una investigación asistida desde un indicio:

- Haz clic en el menú superior **Investigaciones**. Se mostrará el listado de investigaciones creadas.
- Selecciona una investigación. Se abrirá la investigación con los indicios asignados.
- En la sección **Indicios**, haz clic con el botón derecho en el indicio de tu interés. Se mostrará un menú de contexto.
- Selecciona **Investigaciones asistidas**. Se abrirá la ventana **Investigaciones asistidas [#Nombre#]** con el contexto tomado del indicio elegido.

Acceso a las investigaciones asistidas desde un evento

Al crear una investigación asistida desde un evento, Cytomic Orion utiliza la siguiente información para generar el contexto:

- MD5 del proceso padre
- Nombre del fichero del proceso padre
- MD5 del proceso hijo
- Nombre del fichero del proceso hijo
- Linea de comandos
- Identificador de cliente al que pertenece el equipo
- Identificador del equipo
- Intervalo de 3 días desde la creación de la investigación

Para crear una investigación asistida desde un evento:

- Haz clic en el menú superior **Investigaciones**. Se mostrará el listado de investigaciones creadas.
- Selecciona una investigación. Se abrirá la investigación con los indicios asignados.
- En la sección **Entidades de interés**, haz clic en el icono ⋮ de un equipo. Se mostrará un menú de contexto.
- Selecciona **Investigar equipo**. Se abrirá la consola de investigación con los eventos registrados en el día actual en el equipo.
- Haz clic con el botón derecho en el evento que quieres investigar. Se abrirá el menú de contexto.
- Selecciona **Investigación asistida**. Se abrirá la ventana **Investigaciones asistidas [#Nombre#]** con el contexto tomado del evento elegido.

Estructura de una investigación asistida

Las investigaciones asistidas presentan una estructura basada en preguntas y respuestas. Las preguntas que el analista puede realizar se extraen del contexto actual de la investigación, de este modo, la investigación solo mostrará las preguntas disponibles en función de la respuesta anterior.

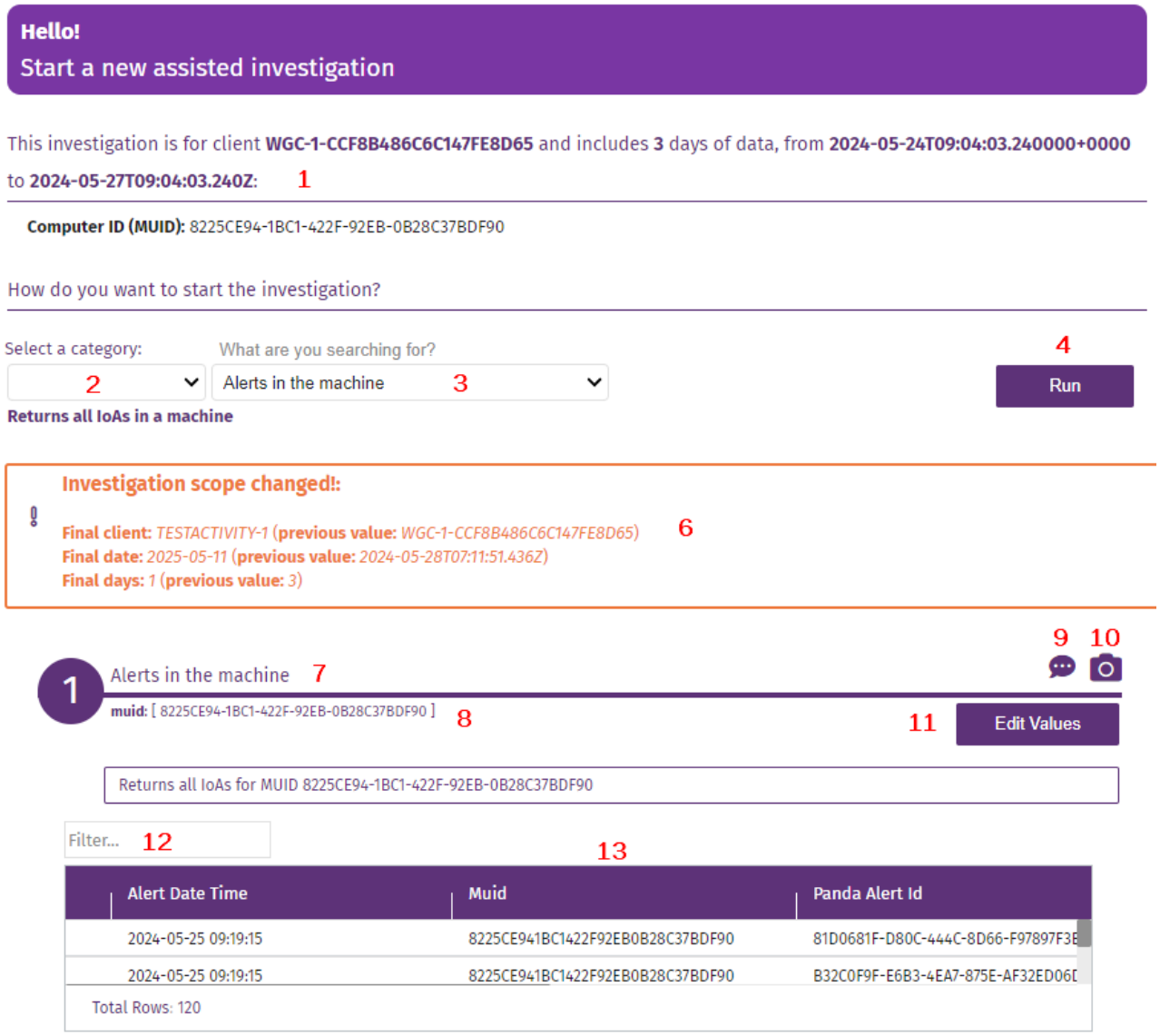


Figura 10.1: Vista general de una investigación asistida

Una investigación asistida se divide en varias secciones:

- **Contexto inicial (1)**: muestra el identificador del cliente, el intervalo de días que abarca y el identificador del equipo al que se refiere la investigación.
- **Select a category (2)**: filtra los tipos de preguntas disponibles según el contexto de la investigación.

- **What are you searching for? (3)**: permite elegir la pregunta que buscará en el contexto definido. Solo se muestran la preguntas compatibles con los datos que forman parte del contexto.
- **Run (4)**: lanza la pregunta seleccionada.
- **Investigation scope changed (6)**: si los datos seleccionados en la respuesta anterior no pertenecen al contexto definido en el inicio de la investigación, se muestra un mensaje informativo indicando que el contexto ha cambiado.
- **Pregunta (7)**: pregunta elegida en el desplegable **What are you searching for?** junto al número de secuencia. Conforme el analista realiza preguntas y se muestran las respuestas, el número de secuencia se incrementa y las respuestas se añaden de forma ordenada a la investigación asistida.
- **Contexto de la pregunta (8)**: indica el subconjunto de datos del contexto que utiliza la pregunta.
- **Rate this search (9)**: le permite al analista valorar la utilidad de la pregunta.
- **Copy search results to comments (10)**: copia la pregunta y la respuesta al apartado **Comentarios** de la investigación. Consulta **Comentarios (8)** en la página **115**.
- **Edit Values (11)**: permite modificar los valores que forman parte del contexto de cualquier pregunta mostrada en la investigación asistida. Si el contexto de una pregunta anterior cambia, se muestra un mensaje de advertencia y se elimina toda la investigación a partir de ese punto.
- **Respuesta (13)**: tabla y / o gráfico de respuesta a la pregunta enviada. El analista puede hacer doble clic en una fila de la tabla para expandir la información o para definir el nuevo contexto que se utilizara en la siguiente pregunta.
- **Use parent, Use child, Use both**: utiliza los datos seleccionados para asignarlos al proceso padre, hijo, o ambos al generar el nuevo contexto para ejecutar la siguiente pregunta.

Tipos de preguntas en investigaciones asistidas

En una investigación asistida no todas las preguntas están disponibles en todo momento: la investigación solo muestra las preguntas compatibles con el conjunto de datos obtenido de la respuesta previa.

*Consulta **Formato de los eventos utilizados en Cytomic Orion** en la página **402** para conocer el significado de los campos devueltos en cada respuesta.*

Los tipos de preguntas disponibles y su descripción son:

Nombre de la pregunta	Descripción
Blocked operations on the computer	Obtiene las operaciones bloqueadas registradas en el equipo especificado. **Parámetros de entrada:** • **Computer ID (MUID):** identificador del equipo **Resultado:** Listado de los eventos de operaciones bloqueadas asociados al equipo.
Child process hierarcy	Obtiene el árbol de procesos hijo del proceso padre especificado. **Parámetros de entrada:** • **Process (Computer ID/MUID, File MD5, Process ID/PID):** identificador del equipo, MD5 del fichero, identificador del proceso **Resultado:** Listado con la jerarquía de procesos.
Command line information	Muestra la linea de comandos decodificada asociada al proceso especificado y los indicios encontrados. **Parámetros de entrada:** • **Computer ID (MUID):** identificador del equipo • **Command line**: linea de comandos asociada al proceso **Resultado:** Listado de indicios encontrados en la linea de comandos.
Computer indicators	Obtiene el listado de indicios encontrados en el equipo especificado. **Parámetros de entrada:** • **Computer ID (MUID):** identificador del equipo **Resultado:**

Nombre de la pregunta	Descripción
	Listado con los indicadores encontrados. Para obtener los detalles haz clic en un indicio. Consulta **Listado de indicios** en la página **73**.
Computer information by MUID or IP address	Obtiene información de las características del equipo especificado. **Parámetros de entrada:** • **Client:** identificador del cliente • **Computer ID (MUID):** identificador del equipo • **Computer IP address:** dirección IP del equipo **Resultado:** Información de las características del equipo. Consulta **Detalles del equipo** en la página **122**.
Computer process activity	Obtiene los eventos registrados en el equipo especificado. **Parámetros de entrada:** • **Computer ID (MUID):** identificador del equipo • **Process (Computer ID/MUID, File MD5, Process ID/PID):** identificador del equipo, MD5 del fichero, identificador del proceso **Resultado:** Listado de eventos con las operaciones registradas en el equipo.
Computer process indicators	Obtiene el listado de indicios asociados a un proceso del equipo especificado. **Parámetros de entrada:** • **Process (Computer ID/MUID, File MD5, Process ID/PID):** identificador del equipo, MD5 del fichero, identificador del proceso **Resultado:** Listado con los indicadores encontrados. Para

Nombre de la pregunta	Descripción
	obtener los detalles haz clic en un indicio. Consulta **Listado de indicios** en la página **73**.
Computers with a specific file	Obtiene una lista de los equipos donde se ha visto el fichero especificado por su nombre. **Parámetros de entrada:** • **File Name:** nombre del fichero **Resultado:** Listado de los equipos donde se ha visto el fichero.
Computers with a specific MD5	Obtiene una lista de los equipos donde se ha visto el fichero especificado por su hash MD5. **Parámetros de entrada:** • **MD5:** hash MD5 del fichero **Resultado:** Listado de los equipos donde se ha visto el fichero.
Connections to a specific URL	Obtiene una lista de equipos que se conectaron a la URL especificada. **Parámetros de entrada:** • **Host Name:** nombre del equipo **Resultado:** Listado con los equipos que se conectaron a la URL.
External MD5 information	Obtiene información suministrada por proveedores externos del fichero especificado por su MD5. **Parámetros de entrada:** • **Computer ID (MUID):** identificador del equipo • **MD5:** hash MD5 del fichero **Resultado:** Información suministrada por los proveedores: • VirusTotal

Nombre de la pregunta	Descripción
	• WHOIS • Urlscan.io • AbuseIPDB • AlienVault OTX • IBM X-Force • Intel471
File activity on the computer	Obtiene los eventos relacionados con el fichero especificado por su nombre. **Parámetros de entrada:** • **Computer ID (MUID):** identificador del equipo • **File Name:** nombre del fichero **Resultado:** Listado con los eventos relacionados con el fichero.
File modifications	Obtiene una lista de las operaciones de creación, modificación y borrado del fichero especificado por el nombre o hash MD5. El software de protección no monitoriza todos los ficheros del equipo, solo aquellos que: • Contienen certificados o contraseñas • Se inician automáticamente cuando arranca el sistema operativo • Se ejecutan desde el programador de tareas • Están almacenados en carpetas poco frecuentes • Son accedidos por aplicaciones atípicas. La lista de operaciones ejecutadas sobre un fichero puede no estar disponible cuando se el fichero se especifica por su MD5. **Parámetros de entrada:** • **MD5:** hash MD5 del fichero • **File Name:** nombre del fichero

Nombre de la pregunta	Descripción
	Resultado: Listado de los eventos de creación, modificación o borrado asociados al fichero.
File names associated with a URL	Obtiene una lista de ficheros almacenados en el equipo descargados desde una URL especificada. Al seleccionar un fichero de la lista devuelta, se muestra la lista de conexiones involucradas en la descarga de ese fichero en particular. **Parámetros de entrada:** • **Host Name:** nombre del equipo **Resultado:** Lista de ficheros asociados con la URL.
File names for an MD5	Obtiene un listado de nombres de fichero del hash MD5 especificado. **Parámetros de entrada:** • **MD5:** hash MD5 del fichero **Resultado:** Listado de nombres de fichero.
IP address information	Obtiene una tabla con la información asociada a la IP especificada suministrada por los proveedores externos **Parámetros de entrada:** • **IP Address**: dirección IP del equipo **Resultado:** Información suministrada por los proveedores externos: • VirusTotal • WHOIS • Urlscan.io

Nombre de la pregunta	Descripción
	• AbuseIPDB • AlienVault OTX • IBM X-Force • Intel471
Login and logout information	Obtiene los inicios y cierres de sesión del equipo especificado. **Parámetros de entrada:** • **Computer ID (MUID):** identificador del equipo **Resultado:** Listado con los inicios y cierres de sesión.
Logins and logouts on a client computers	Obtiene los inicios y cierres de sesión del usuario especificado. **Parámetros de entrada:** • **User**: identificador de usuario **Resultado:** • Diagrama de lineas con los intentos de inicio y cierre de sesión registrados en el equipo. • Tabla con la información de intentos de inicio y cierre de sesión agrupada por equipo. Al seleccionar un equipo de la tabla se muestra el detalle de cada inicio de sesión
MD5 activity on a computer	Obtiene la actividad del fichero especificado por su MD5 en un equipo. **Parámetros de entrada:** • **Computer ID (MUID):** identificador del equipo • **MD5:** hash MD5 del fichero **Resultado:** Listado con los eventos relacionados con el MD5 en el equipo.

Nombre de la pregunta	Descripción
MD5 activity on client computers	Obtiene la actividad del fichero especificado por su MD5 en todos los equipos del cliente. **Parámetros de entrada:** • **MD5:** hash MD5 del fichero **Resultado:** Listado con los eventos relacionados con el MD5 en el equipo.
MD5s for a file name	Obtiene todos los nombres de fichero vistos en los equipos del cliente para el MD5 especificado. **Parámetros de entrada:** • **File Name:**nombre del fichero **Resultado:** Listado de MD5s.
URLs associated with a file	Obtiene una lista de URLs que contienen el fichero especificado por su nombre. **Parámetros de entrada:** • **File Name:**nombre del fichero **Resultado:** Listado de URLs que contienen el nombre del fichero.
URLs associated with an MD5	Obtiene una lista de URLs relacionadas con el fichero especificado por su hash MD5. **Parámetros de entrada:** • **MD5:** hash MD5 del fichero **Resultado:** Listado de URLs relacionadas con el MD5.
URLs associated with a user	Obtiene las URLs accedidas por el identificador de usuario especificado.

Nombre de la pregunta	Descripción
	Parámetros de entrada: • **User:** identificador de usuario **Resultado:** Lista de URLs accedidas por el usuario.
USB devices	Obtiene una lista de los dispositivos USB conectados al equipo especificado por su MUID. **Parámetros de entrada:** • **Computer ID (MUID):** identificador del equipo **Resultado:** Lista de dispositivos USB conectados al equipo con sus características.
User activity on client computers	Obtiene la actividad del usuario especificado en los equipos del cliente. **Parámetros de entrada:** • **User:** identificador de usuario **Resultado:** Listado con un resumen de la actividad del usuario registrada en los equipos del cliente.
User activity on a computer	Obtiene la actividad del usuario especificado en el equipo especificado. **Parámetros de entrada:** • **Computer ID (MUID):** identificador del equipo • **User:** identificador de usuario **Resultado:** Listado con la actividad del usuario en el equipo.
User indicators	Obtiene una lista de indicios asociada al usuario especificado en todos los equipos del cliente. **Parámetros de entrada:**

Nombre de la pregunta	Descripción
	• **User:** identificador de usuario **Resultado:** Listado de indicios asociados al usuario en los equipos del cliente.
Users associated with connections to a specific computer	Obtiene los usuarios que acceden a la URL especificada. **Parámetros de entrada:** • **User:** identificador de usuario **Resultado:** Listado de usuarios que acceden a la URL.

Tabla 10.1: Preguntas disponibles en una investigación asistida

Capítulo 11

Análisis de indicios con la consola de investigación

A diferencia del módulo de consultas avanzadas, donde se realizaban análisis transversales en todo el océano de datos generado por el parque informático del cliente, la consola de investigación habilita el análisis de eventos en profundidad, en equipos y fechas concretas. Este recurso ofrece todas las herramientas necesarias para que el técnico pueda inspeccionar en detalle los procesos ejecutados en un equipo de la red del cliente, y examine de forma gráfica su actividad y su relación con otros procesos y elementos del sistema operativo.

El tiempo de retención de la telemetría en el océano de datos es de 1 año.

CONTENIDO DEL CAPÍTULO

Acceso a la consola de investigación

Dependiendo de la etapa en la que se encuentra la investigación, el analista puede acceder a la consola de investigación desde varios puntos:

- **Desde una investigación**: muestra los eventos relacionados con una entidad que pertenece al contexto de una investigación.
- **Desde un indicio**: muestra los eventos relacionados con un equipo.
- **Desde la propia consola de investigación**: busca los equipos relacionados con un evento.
- **Desde la API de Cytomic Orion**: análisis de elementos sin asociar a investigaciones ni a indicios previos.

Desde una investigación recién creada o en curso

Para realizar un análisis de un elemento cualquiera perteneciente a una investigación, sigue los pasos mostrados a continuación:

- En el menú superior **Investigaciones** crea una nueva investigación. En la barra de herramientas haz clic en el + y elige **Investigación de equipos**. Se abrirá una ventana emergente para introducir los datos del equipo a analizar y la fecha en la que se centrará la investigación.

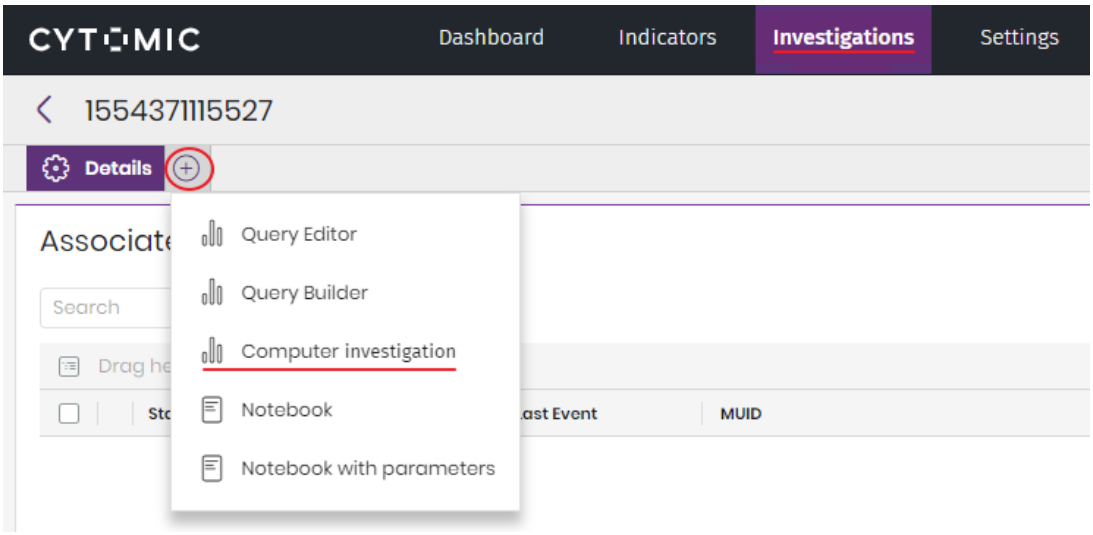


Figura 11.1: Ventana de acceso a la consola de investigación

- Haz clic en el selector dependiendo del elemento que se quiera investigar:
  - **MUID**
  - **MD5**

- **MUID + MD5**
- **Nombre del equipo**

- Introduce la información dependiendo del selector. En los apartados siguientes se detallan los tipos de datos requeridos.

Investigación de un equipo: MUID

- Escribe el identificador único del equipo a analizar, el intervalo en el que se centrará la investigación (máximo 48 horas) y zona horaria del intervalo elegido. Para acelerar la selección haz clic en la caja de texto **MUID** y se desplegarán todas las entidades de interés compatibles creadas en la investigación. También puedes escribir un MUID directamente.
- Si no conoces el MUID del equipo consulta **Herramienta de conversión de nombres de equipo a MUID** en la página **45**.
- Haz clic en el botón **Aceptar**. Se creará una nueva pestaña con el nombre del equipo y entre paréntesis su MUID, que contendrá los eventos del equipo seleccionado en la fecha indicada.

Investigación de un fichero: MD5

- Escribe el hash del fichero a investigar. Para acelerar la selección haz clic en la caja de texto **MD5** y se desplegarán todas las entidades de interés compatibles creadas en la investigación.
- Haz clic en el botón **Aceptar**. Se creará una nueva pestaña con el MD5, y que contendrá el panel **Equipos encontrados** con un listado de todos los equipos que han generado eventos que involucran al fichero MD5 buscado, así como la fecha en la que se han producido dichos eventos y la información mostrada a continuación:

Figura 11.2: Panel de Equipos encontrados

- **MUID**: identificador único del equipo donde se han producido los eventos relacionados con el fichero MD5.
- **Pandaid**: identificador único del cliente al que pertenece el equipo encontrado.
- **Lastseen**: fecha en la que se registró por última vez un evento que involucra al fichero MD5 encontrado en el equipo seleccionado.
- **Firstseen**: fecha en la que se registró por primera vez un evento que involucra al fichero MD5 encontrado en el equipo seleccionado.
- **Lastpath**: última ruta registrada del elemento buscado en el equipo.

En la parte superior de la ventana se muestra la zona de herramientas:

- **Buscar**: herramienta de filtrado que admite la búsqueda por subcadenas en el contenido de todos los campos del listado.
- **Numero de resultados**: número de registros mostrados en el listado.

Investigación de un fichero almacenado en un equipo: MUID y MD5

- Escribe el identificador único del equipo y el hash del fichero a investigar. Para acelerar la selección haz clic en las cajas de texto **MUID y MD5** para desplegar todas las entidades de interés compatibles creadas en la investigación. También puedes escribirlas directamente.
- Si no conoces el MUID del equipo consulta **Herramienta de conversión de nombres de equipo a MUID** en la página **45**.
- Haz clic en el botón **Aceptar**. Se creará una nueva pestaña que contendrá el panel **Equipos encontrados** con un listado de todos los equipos que han generado eventos que involucran al fichero MD5 buscado, así como la fecha en la que se han producido dichos eventos. Consulta **Investigación de un fichero: MD5**.

Investigación de un equipo por su nombre

- Escribe el nombre del equipo Windows a analizar, el intervalo en el que se centrará la investigación y la zona horaria del intervalo elegido.
- Escribe el cliente al que pertenece el equipo, dado que un mismo nombre de equipo podría repetirse en varios clientes.
- Haz clic en el botón **Aceptar**. Se creará una nueva pestaña con el nombre del equipo con su MUID entre paréntesis, y que contendrá los datos del equipo seleccionado en la fecha indicada.

Desde un indicio

Investigación de los eventos de un equipo

Para realizar una investigación en profundidad sobre un equipo involucrado en un indicio generado por Cytomic Orion sigue los pasos mostrados a continuación:

- En el menú superior **Investigacione**s, haz clic en la investigación que contiene el indicio a analizar o asigna el indicio a una nueva investigación. Consulta **Asignar y retirar indicios a investigaciones manualmente** en la página **103** para obtener información sobre como asignar uno o más indicios a una investigación.
- En el panel de indicios de la investigación haz clic con el botón de la derecha sobre el indicio a analizar. Se mostrará un menú emergente.
- Haz clic en la opción **Mostrar eventos del equipo** para crear una nueva pestaña con el nombre del equipo y entre paréntesis su MUID, y que contendrá los eventos del equipo involucrado en el indicio y la fecha en la que se han producido.

Desde la consola de investigación

Investigación de un fichero

Para buscar otros equipos de la red donde se han registrado eventos sobre un fichero concreto, Cytomic Orion facilita este tipo de búsqueda guiada. Para ello sigue los pasos mostrados a continuación:

- Abre una consola de investigación con un método de los expuestos en este apartado.
- Haz clic sobre el evento en cuestión: los campos **parentfilename** y **childfilename** contienen los ficheros involucrados en el evento.
- Con el botón de la derecha haz clic en el evento y elige una de las siguientes opciones del menú de contexto:
    - **Mostrar equipos con el archivo padre**: busca los MUIDs de los equipos del cliente donde fue visto el fichero padre.
    - **Mostrar equipos con el archivo hijo:** busca los MUIDs de los equipos del cliente donde fue visto el fichero hijo.
- Una vez elegida la opción se mostrará una ventana con dos paneles donde elegir el equipo para mostrar sus eventos. Consulta **Estructura de la consola de investigación** para una descripción detallada de los paneles.

Desde la API de Cytomic Orion

En los casos en los que las tareas de threat hunting se inicien a través de la API de Cytomic Orion, es posible acceder a la consola de investigación sin pasar por la creación de una investigación

previa. En estos casos, el analista puede construir una URL que le permita abrir directamente la consola de investigación para visualizar los eventos involucrados.

Investigación de un fichero: MD5

El formato de la URL a construir es el siguiente:

Comando	GET
URL	https://orion.cytomicmodel.com/forensics/md5/{md5}
Parámetros requeridos en la URL	**md5**: hash del fichero.

Tabla 11.1: Formato de la URL para abrir la consola de investigación sobre un fichero

Investigación de un equipo: MUID

El formato de la URL a construir es el siguiente:

Comando	GET
URL	https://orion.cytomicmodel.com/forensics/muid/{muid}?dateFrom={dateFrom}&dateTo={dateTo}&timezone={timezone}
Parámetros requeridos en la URL	• **MUID**: identificador del equipo. • **dateFrom**: timestamp Unix en milisegundos con la fecha inferior del intervalo de eventos a mostrar. • **dateTo**: timestamp Unix en milisegundos con la fecha superior del intervalo de eventos a mostrar.
Parámetros opcionales en la URL	• **timezone**: zona horaria de las fechas especificadas en la URL. Si no se indica se toma la establecida en la configuración de la cuenta de usuario.

Tabla 11.2: Formato de la URL para abrir la consola de investigación sobre un equipo

Investigación de un fichero en un equipo: MD5 y MUID

El formato de la URL a construir es el siguiente:

Comando	GET
URL	https://orion.cytomicmodel.com/forensics/muid/{muid}/md5/{md5}
Parámetros requeridos en la URL	• **MUID**: identificador del equipo • **MD5**: hash del fichero

Tabla 11.3: Formato de la URL para abrir la consola de investigación sobre un fichero en un equipo

Estructura de la consola de investigación

La consola de investigación se divide en varios paneles, dependiendo del punto de entrada:

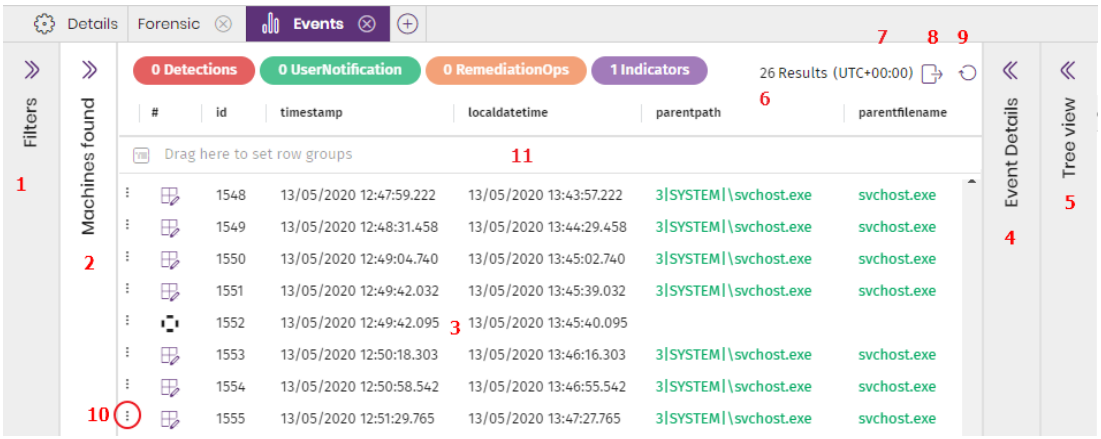


Figura 11.3: Paneles de la consola de investigación

- **Panel lateral izquierdo Filtros (1)**: establece filtros y configura la presentación de los datos en el panel central y derecho para ajustarse a las necesidades de la investigación del analista.
- **Panel lateral Equipos encontrados (2)**: >si la investigación se inició desde un fichero MD5 (consulta **Investigación de un fichero: MD5**) se mostrará un panel con un listado de los equipos que tienen eventos relacionados con el fichero indicado.
- **Panel central (3)**: muestra los eventos de la fecha seleccionada en forma de listado y opcionalmente en forma de serie temporal.
- **Panel lateral derecho Detalles del evento (4)**: muestra los campos del evento seleccionado en el panel central.
- **Panel Árbol de Procesos (5)**: muestra la jerarquía padre – hijo de todos los procesos y elementos registrados en el día investigado.
- **Numero de resultados (6) obtenidos**
- **Fecha (7)**: establece la zona horaria de las fechas mostradas en el listado de eventos **(3)**.
- **Exportar listado (8)**: descarga en el equipo del analista el listado de eventos en formato csv.
- **Recargar el listado (9)**
- **Menú de contexto (10)**: muestra las acciones sobre el evento que el analista utiliza con mayor frecuencia.
    - Mostrar eventos del equipo
    - Mostrar equipos con el archivo padre
    - Mostrar equipos con el archivo hijo
    - Ejecutar notebook con parámetros

- Añadir entidades de interés
- Detalles del equipo

- **Herramientas para configurar el listado (11)**: consulta **Herramientas para configurar los listados** en la página **39** para obtener mas información sobre cómo agrupar el listado por columnas y otros recursos que permiten configurar el modo en que se muestra el listado de eventos.

Panel lateral Filtros

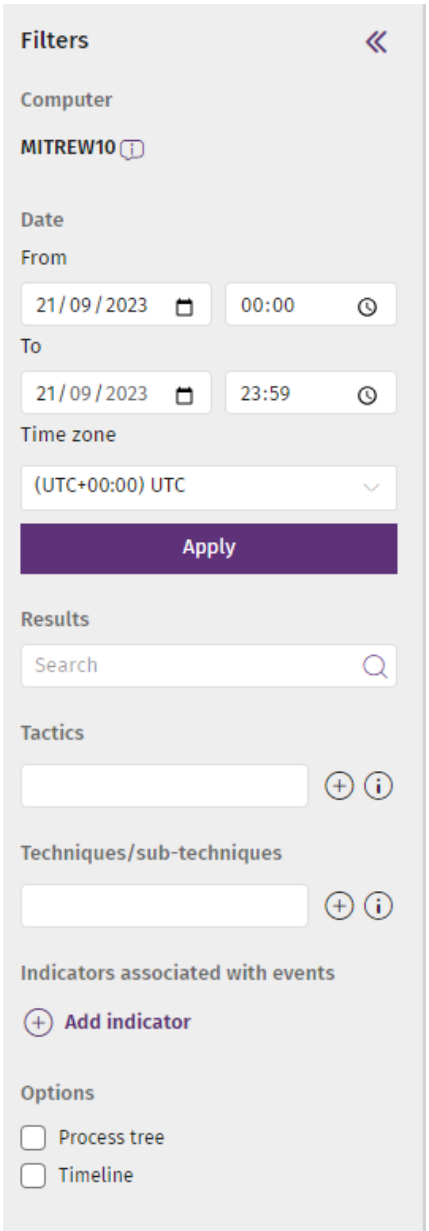


Figura 11.4: Panel Filtros

Presenta información global sobre la investigación realizada y permite filtrar y buscar los eventos de interés para facilitar la obtención de conclusiones por parte del analista.

- **Equipo**: muestra el nombre o el MUID del equipo investigado.
- **MD5**: muestra el MD5 del fichero analizado en la investigación.
- **Fecha**: muestra el intervalo de tiempo investigado. Al hacer clic en las cajas de texto se mostrará un calendario para cambiar el límite del intervalo. El intervalo máximo admitido es 48 horas.
- **Zona horaria**: establece la zona horaria de la búsqueda. Los resultados se mostrarán en la zona horaria definida en el panel central.
- **Resultados**: filtra el listado de eventos con el contenido introducido en la caja de texto. La búsqueda se extiende a todos los campos de los registros presentados en el listado y acepta búsquedas parciales.
- **Táctica**: para filtrar por táctica escribe una parte de su nombre o haz clic en el icono ⊕. Se mostrará un listado de las tácticas asociadas a los eventos mostrados en el listado.
- **Técnica / subtécnica**: para filtrar por técnica o subtécnica escribe una parte de su nombre o haz clic en el icono ⊕. Se mostrará un listado de las técnicas o subtécnicas asociadas a los eventos mostrados en el listado.
- **Añadir indicio**: para filtrar por indicio escribe una parte de su nombre o haz clic en el icono ⊕. Se mostrará un listado de los indicios asociados a los eventos mostrados en el listado.
- **Opciones**: activa y desactiva la serie temporal de eventos mostrada en el panel central y la vista de procesos en árbol mostrada en el panel **Árbol de procesos**.

Panel central

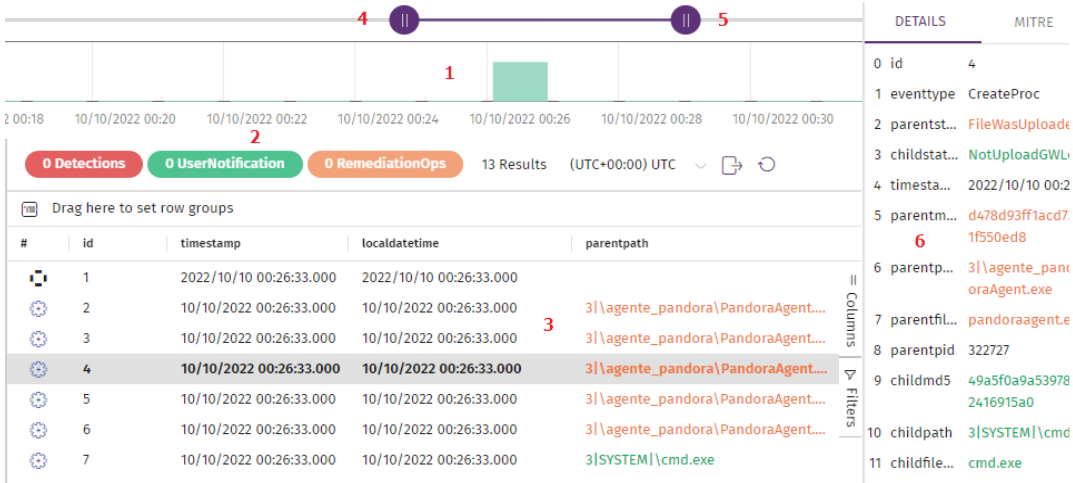


Figura 11.5: Panel central de la consola de análisis

Muestra el listado de eventos correspondiente al equipo y fecha indicados en el panel lateral **Filtros** (campos **Equipo** y **Fecha**). El panel central se divide en tres áreas:

- **Diagrama de barras (1)**: muestra de forma gráfica el número de eventos en intervalos de 5 minutos. Un pico de eventos en un intervalo de tiempo pequeño puede significar actividad sospechosa de pertenecer a un ataque. Consulta **Diagrama de barras** .
- **Barra de información del panel de registros (2)**: indica el subconjunto de eventos mostrados en la gráfica sobre el total de registrados en el día y en el equipo investigado. Consulta **Barra de información**.
- **Subpanel de eventos (3)**: muestra los eventos monitorizados y recogidos por Cytomic Orion correspondientes al intervalo mostrado por la serie temporal para ese equipo y día.

*Consulta **Significado de los campos de tipo fecha** en la página **161** para obtener información sobre cómo interpretar y utilizar los campos de tipo fecha incluidos en los eventos.*

Diagrama de barras

Indica en el eje de las abscisas el número de eventos producidos por unidad de tiempo y en el eje de las coordenadas la marca temporal en formato hora:minutos. Al pasar el ratón por la gráfica se mostrará un globo informativo que indica el número de eventos registrados en ese momento.

Una vez definido el día a mostrar mediante el panel lateral, el analista puede cambiar el rango del intervalo para centrarse en la actividad registrada en un momento determinado, o cambiar el intervalo de visualización. Para ello, utiliza la barra superior **(4)**, los botones que la rodean **(5)** o la propia serie temporal **(1)**.

Barra superior (4)

Haz clic en la parte central de la barra y arrástrala hacia la izquierda o la derecha para cambiar el intervalo de visualización de actividad mostrada en el gráfico.

Botones que rodean la barra superior (5)

Haz clic en los botones que rodean la barra superior y arrástralos a izquierda o derecha para cambiar el rango del intervalo de actividad mostrado en el gráfico.

Panel de detalles (6)

Haz clic en un evento del listado **(3)** para mostrar el panel de detalles y MITRE. Para más información consulta **Panel lateral Detalles y MITRE**.

Diagrama de barras (1)

Haz clic en un punto del diagrama y arrastra el ratón para definir una nueva ventana de visualización de la actividad. El gráfico se actualizará con el nuevo nivel de zoom y el nuevo intervalo de datos mostrado.

Barra de información

Figura 11.6: Barra de información de la consola de investigación

- **(1)** Etiquetas de colores con el número de eventos encontrados. Al hacer clic en cada una de las etiquetas se mostrará un panel flotante con los eventos del tipo elegido. Al hacer clic en uno de los eventos el panel se ocultará y el cursor se posicionará en el registro elegido dentro del subpanel de eventos. Los tipos disponibles se muestran a continuación:
  - **Detecciones**: eventos de detección de amenaza por parte de la solución de seguridad instalada en el equipo de usuario o servidor.
  - **UserNotification**: eventos que implicaron mostrar una ventana emergente al usuario para forzar una decisión que puede afectar a la seguridad de su equipo.
  - **RemediationOps**: eventos que implican la ejecución de una decisión por parte del software de seguridad instalado en el equipo.
  - **Indicios**: indicios generados.

> *Para obtener una descripción de los campos mostrados en cada tipo de evento consulta* ***Formato de los eventos utilizados en Cytomic Orion*** *en la página* ***402****.*

- **(2)** Número de registros mostrados en el subpanel de eventos.
- **(3) Zona horaria**: establece la zona horaria en la que se mostrarán los eventos.
- **(4) Exportar**: descarga un fichero en formato csv con la lista de eventos visualizada.
- **(5) Recargar**: vuelve a pedir el listado al servidor con los eventos actualizados hasta el momento.

Subpanel de eventos

Muestra los eventos monitorizados en el equipo y recogidos por Cytomic Orion. Los registros se muestran en formato tabla con acceso a las herramientas de filtrado, ordenación y búsqueda mostradas en **Herramientas para configurar los listados** en la página **39**.

> *En caso de listados especialmente largos se mostrarán los primeros 150.000 eventos del intervalo seleccionado. Se mostrará el mensaje* ***Se están mostrando los 150 mil primeros eventos del intervalo de tiempo seleccionado****, informando de la excesiva longitud del listado. Para mostrar los eventos que se hayan podido perder configura un nuevo intervalo.*

El subpanel de eventos esta formado por columnas que describen cada uno de los eventos. La primera de ellas incluye un icono que representa el tipo de evento registrado.

Icono	Descripción	Icono	Descripción
	Crear proceso		Crear fichero ejecutable
	Modificar fichero ejecutable		Cargar librería
	Borrar programa ejecutable		Modificar fichero ejecutable
	Crear directorio		Crear archivo comprimido
	Abrir archivo comprimido		Crear rama del registro que apunta a un fichero ejecutable
	Modificar rama del registro que apunta a un fichero ejecutable		Crear hilo de proceso remoto
	Detección de exploit		Evento sin clasificar
	Descargar archivos		Operación de red

Icono	Descripción	Icono	Descripción
	Proceso desconocido que no se bloqueó por no haber iniciada una sesión interactiva en el equipo		Apertura de documento
	Operación sobre el registro		Crear un fichero de tipo script
	Ejecutar un fichero de tipo script		Detección de amenaza
	Tamaño de datos transferido por la red		Evento WMI recogido por SYSMON que modifica la configuración del sistema operativo del equipo.
	Resolución DNS fallida		Operación de control de dispositivos
	El agente muestra un mensaje emergente en el equipo del usuario		Inicio de sesión interactiva en el equipo
	Finalización de sesión interactiva en el equipo		Acción ejecutada por la protección instalada en el equipo
	Evento interno administrativo		Reinicio de equipo
	Operación realizada por un ejecutable cuya creación no fue registrada.		La protección detecta un ejecutable del cual no se tiene registro de su creación, bien por un problema transitorio, bien por existir antes de la instalación de la protección

Icono	Descripción	Icono	Descripción
	Crear proceso remoto		

Tabla 11.4: Iconos y descripción del tipo de evento asociado

Al hacer clic con el botón de la derecha en un evento o en el icono ⋮ asociado, se muestra un menú de contexto con las acciones más frecuentemente utilizadas por el analista que involucran al evento;

- **Mostrar eventos del equipo**: abre una nueva pestaña con los eventos registrados en el equipo referido por el evento.
- **Mostrar equipos con el archivo padre**: abre una nueva pestaña en la consola de investigación con un listado de los equipos que registraron eventos que involucran al archivo padre del evento.
- **Mostrar equipos con el archivo hijo**: abre una nueva pestaña en la consola de investigación con un listado de los equipos que registraron eventos que involucran al archivo hijo del evento.
- **Ejecutar notebook con parámetros**: abre una nueva pestaña con un notebook. Consulta **Acceso y creación de notebooks** en la página **225**.
- **Añadir entidades de interés**: agrega una entidad de interés a la investigación. Consulta **Panel Entidades de interés** en la página **116**.
- **Detalles del equipo**: muestra información básica del hardware y software de seguridad Cytomic instalado en el equipo. Consulta **Detalles del equipo** en la página **122**.

Panel lateral Detalles y MITRE

Al hacer clic sobre un evento se carga el panel lateral con las pestañas **Detalles** y **MITRE**, que contiene toda la telemetría recogida para ese evento y la información MITRE de las tácticas y técnicas asociadas.

- Para conocer el significado de los campos incluidos en la pestaña **Detalle** consulta el capítulo **Formato de los eventos utilizados en Cytomic Orion** en la página **402**.
- Para obtener información de la pestaña **MITRE** consulta **Panel de detalles** en la página **75**

Mostrar buffer AMSI (Antimalware Scan Interface)

Los eventos de tipo SystemOps pueden almacenar el contenido del buffer AMSI con el script que generó el evento. Para mostrar el buffer AMSI:

- Selecciona el evento SystemOps en el subpanel de eventos. Se mostrarán sus campos asociados en el panel lateral **Detalles del evento**.

- Haz clic en el enlace **Ver script**. Se abrirá una ventana con el contenido del script almacenado.
- Para copiar al portapapeles el script haz clic en **Copiar**.
- Para descargar el script en el equipo del analista haz clic en **Descargar**.

Mostrar información estática del fichero asociado al evento

Cytomic Orion puede mostrar los datos estáticos asociados a un fichero binario:

- Selecciona un evento que esté asociado a un fichero binario (por ejemplo un evento CreateProc). Se mostrarán los campos del evento en el panel lateral **Detalles del evento**.
- Si Cytomic Orion tiene acceso a la información estática del fichero, añadirá el apartado **Mostrar información estática** asociado al proceso padre y al proceso hijo.
- Haz clic en **Mostrar información estática**. Se abrirá una nueva pestaña con los apartados siguientes:
    - **File capabilities**: técnica, táctica y descripción de las funcionalidades detectadas en el fichero.
    - **Strings**: cadenas de caracteres encontradas en el fichero.
    - **Imports**: funciones que importa el fichero para poderse ejecutar.
    - **Exports**: funciones que exporta el fichero.

Panel árbol de procesos

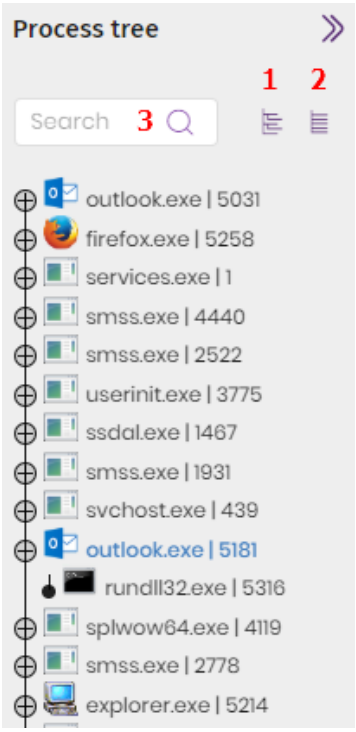


Figura 11.7: Árbol de procesos

En este árbol se muestra la jerarquía de todos los procesos ejecutados en el equipo. Por cada proceso se muestra la siguiente información:

- Icono del proceso.
- Nombre del fichero ejecutable que generó el proceso en memoria.
- PID del proceso.

El árbol de proceso permite las acciones siguientes:

- Para mostrar los procesos hijo de un proceso dado haz clic en el icono ⊕.
- Para localizar el evento que involucró al proceso haz clic en el proceso del árbol de procesos. El listado de eventos se posicionará en el evento correspondiente.
- Para contraer o expandir las ramas del árbol haz clic en los iconos (**1**) y (**2**).
- Para filtrar el árbol de procesos utiliza el cuadro de texto (**3**). Únicamente se mostrarán los procesos que contengan parte o toda la cadena indicada.

Capítulo 12

Diagramas de grafos

El flujo de ejecución de un ataque informático está formado por multitud de procesos y operaciones que quedan registradas en el océano de datos de Cytomic Orion. Dado el gran volumen de información a tratar por el analista del SOC, Cytomic Orion facilita su visualización e interpretación mediante un tipo especial de notebook. Este recurso utiliza un tipo especial de diagrama, conocido como "diagrama de grafos", que representa de forma gráfica mediante nodos y flechas las entidades involucradas y las relaciones que la unen.

La información mostrada en un diagrama de grafos es equivalente a la mostrada en la consola de investigación o en las consultas avanzadas, pero ordenada y presentada de forma más clara y fácil de interpretar para el analista.

El tiempo de retención de la telemetría en el océano de datos es de 1 año.

CONTENIDO DEL CAPÍTULO

Acceso al diagrama de grafos

A la hora de representar en forma de diagrama de grafos los eventos registrados en un equipo, el técnico del SOC puede partir de dos puntos de la consola, dependiendo de la etapa del análisis en la que se encuentre:

- Desde una investigación creada por los técnicos de primer nivel, añadiendo un nuevo notebook de tipo grafo.
- Desde la consola de investigación, cuando el analista ha localizado un evento sospechoso.

Desde una investigación

Para obtener información sobre cómo crear y acceder a una investigación consulta ***Gestión de investigaciones*** *en la página* ***99****.*

El analista abre la investigación nueva o en curso donde se encuentra la cadena de eventos sospechosa de pertenecer a un ataque informático:

- En el panel **Archivos** situado en la parte inferior derecha de la ventana, haz clic en el icono +. Se mostrará el menú de contexto.

o

- En la barra de herramientas situada en la parte superior de la ventana, haz clic en el icono +. Se mostrará el menú de contexto.
- Haz clic en la opción **Grafos**. Se abrirá la ventana **Nueva Investigación gráfica** con el listado de plantillas de grafos definidas.
- Selecciona una plantilla según el tipo de datos a mostrar en el diagrama. Para conocer las plantillas disponibles consulta **Información representada en los diagramas de grafos**. Si la plantilla requiere parámetros, se mostrará una ventana de tipo formulario para introducirlos.

Desde la consola de investigación

Para obtener información sobre cómo acceder y utilizar la consola de investigación consulta ***Análisis de indicios con la consola de investigación*** *en la página* ***186****.*

El analista abre la consola de investigación y localiza en un equipo de la red un evento sospechoso de pertenecer a una secuencia de ataque:

- Haz clic con el botón derecho del ratón sobre en el evento a investigar. Se mostrará un menú de contexto.
- Haz clic en la opción **Grafos**. Se abrirála ventana **Nueva investigación gráfica** con el listado de plantillas de grafos definidas.

- Selecciona una plantilla según el tipo de datos a mostrar en el diagrama. Para conocer las plantillas disponibles consulta **Información representada en los diagramas de grafos**. Si la plantilla requiere parámetros, se mostrará una ventana de tipo formulario para introducirlos.

Información representada en los diagramas de grafos

Para acotar el tipo de información que se muestra en un grafo, el analista dispone de plantillas, que permiten:

- Limitar el tipo de información mostrada según la plantilla elegida.
- Parametrizar el grafo para mostrar las entidades de interés para el analista y sus relaciones, dentro del tipo de información elegida.

Plantillas de grafos disponibles

- **Process Tree**: plantilla parametrizada que muestra los procesos y sus relaciones con otras entidades en el intervalo elegido. Para obtener más detalles de cómo utilizar un grafo generado con esta plantilla consulta **Plantilla Process Tree**.
- **New users in a customer**: plantilla parametrizada que muestra los usuarios nuevos que iniciaron sesión en los equipos de un cliente. Para ello, recopila todos los usuarios que iniciaron sesión en un periodo anterior tomado como referencia, y lo compara con los usuarios que iniciaron sesión en el periodo a estudiar. Para obtener más detalles de cómo utilizar un grafo generado con esta plantilla consulta **Plantilla New users in a customer**.

Estructura de un diagrama de grafos

A continuación se muestran los diferentes paneles de información y herramientas disponibles en los diagramas de grafos.

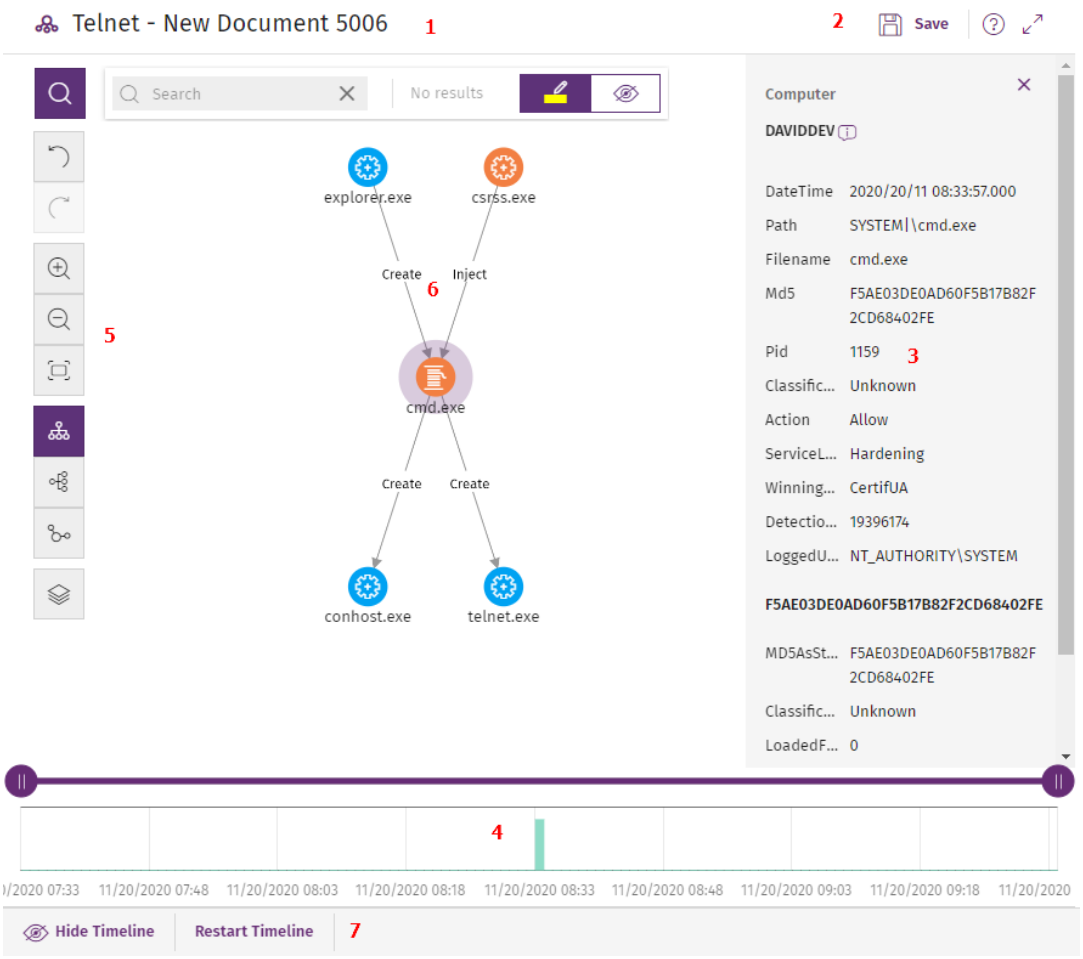


Figura 12.1: Diagrama de grafos y herramientas

- **Nombre del grafo (1)**: haz clic para editar el nombre del diagrama.
- **Barra de herramientas del notebook (2)**:
  - Haz clic en para guardar los cambios del grafo dentro del contexto de una investigación.
  - Haz clic en para mostrar la ayuda web asociada a la funcionalidad de diagramas de grafos.
  - Haz clic en para maximizar o minimizar el diagrama.
- **Panel informativo del elemento seleccionado (3)**: muestra información del nodo o de la linea seleccionada. Para obtener el significado de los campos incluidos en el modelo de datos consulta el capítulo **Formato de los eventos utilizados en Cytomic Orion** en la página **402**.
- **Línea de tiempo (4)**: muestra un histograma de barras de color verde para representar el número de eventos registrados en cada momento. Permite ampliar o reducir el intervalo al que pertenecen los eventos mostrados. Para obtener información sobre cómo utilizar este

recurso consulta **Línea de tiempo**.

- **Barra de herramientas del grafo (5)**: permite modificar la forma en la que se visualiza el diagrama en la pantalla, hacer y deshacer cambios, y buscar o filtrar nodos. Consulta **Configuración del diagrama de grafos**.
- **Diagrama (6)**: representación gráfica de un conjunto de eventos que utiliza nodos y flechas para mostrar entidades y sus relaciones. El orden en el que se ha registrado la creación de los eventos incluidos en el grafo se indica mediante un número en cada flecha.
- **Controles de la línea de tiempo (7)**: oculta, muestra o restaura la línea de tiempo. Consulta **Línea de tiempo**.

Configuración del diagrama de grafos

Para modificar el aspecto y la cantidad de información mostrada en un diagrama de grafos y acomodarlo a las necesidades del analista, se implementan dos recursos principales:

- La barra de herramientas del diagrama de grafos, accesible desde la parte izquierda de la pantalla.
- Los menús contextuales , accesibles al hacer clic con el botón derecho del ratón sobre un nodo o sobre una agrupación de nodos.

Por defecto, el diagrama se muestra con orientación horizontal **(6)** y con un nivel de zoom suficiente como para que todos los nodos sean visibles sin necesidad de desplazar la pantalla.

Barra de herramientas del diagrama de grafos

Figura 12.2: Barra de herramientas

- Para deshacer la última acción ejecutada sobre el diagrama, haz clic en el icono **(1)**.
- Para rehacer la última acción deshecha del diagrama, haz clic en el icono **(2)**.
- Para ampliar el diagrama, haz clic en el icono **(3)**.
- Para alejar el diagrama, haz clic en el icono **(4)**.
- Para restaurar la configuración del zoom a la establecida inicialmente, haz clic en el icono **(5)**.
- Para cambiar la orientación del diagrama a horizontal, haz clic en el icono **(6)**.
- Para cambiar la orientación del diagrama a vertical, haz clic en el icono **(7)**.
- Para mostrar u ocultar las distintas capas de información incluidas en el grafo, haz clic en el icono **(8)**. Consulta **Ocultar y mostrar capas**.

Menús de contexto

Al hacer clic con el botón derecho del ratón sobre un nodo o una agrupación, se muestra el menú de contexto. Las opciones que no es posible utilizar dependiendo del estado del nodo se deshabilitan, mostrándose con un color atenuado.

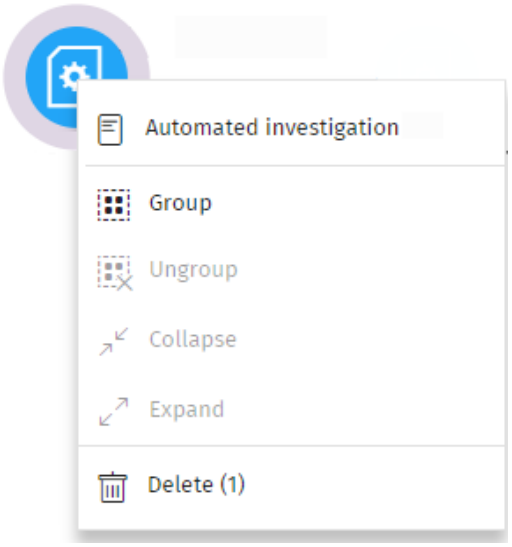


Figura 12.3: Menú de contexto

Ocultar y mostrar capas

Para ocultar parte de la información incluida en el grafo y mostrar los aspectos más relevantes del mismo, haz clic en el icono **(8)**. Se mostrará un menú desplegable con las siguientes opciones:

- **Secuencia de ejecución**: oculta o muestra la numeración de los eventos que permite determinar su orden de ejecución en el equipo del usuario. Consulta **Estilos de las flechas**.
- **Nombres de la relaciones**: oculta o muestra el nombre de los eventos. Consulta **Formato de los eventos utilizados en Cytomic Orion** en la página **402**.
- **Nombres de las entidades**.

Seleccionar nodos del diagrama

- **Para seleccionar un único nodo del diagrama**: haz clic en el nodo con el botón izquierdo del ratón.
- **Para seleccionar varios nodos dispersos del diagrama**: mantén presionada la tecla Ctrl o Mayúsculas y haz clic en los nodos con el botón izquierdo del ratón.
- **Para seleccionar varios nodos contiguos del diagrama**: mantén presionada la tecla Ctrl o Mayúsculas, haz clic en una zona libre del diagrama y arrastra el ratón hasta abarcar los nodos a seleccionar.

Al seleccionar varios nodos del diagrama y hacer clic con el botón derecho del ratón, se mostrarán únicamente las opciones del menú de contexto comunes a todos los nodos seleccionados.

Mover y borrar nodos del diagrama

Para mover todos los nodos y líneas del diagrama:

Haz clic en un espacio libre y arrastra el ratón en la dirección apropiada.

Para mover un único nodo:

Selecciona el nodo y arrástralo en la dirección apropiada. Todas las líneas que conectan al nodo con sus vecinos se ajustarán a su nueva posición.

Para eliminar un nodo con el teclado:

- Selecciona el nodo deseado y pulsa Supr. Se mostrará un mensaje indicando el número total de nodos que se eliminarán del grafo: el propio nodo y todos sus descendientes.
- Haz clic en el botón **Aceptar**.

Para eliminar un nodo con el ratón:

Cuando se borra un nodo del grafo, también se borran todos sus descendientes.

- Haz clic con el botón derecho del ratón sobre el nodo a borrar. Se mostrará el menú de contexto.
- Selecciona la opción **Borrar (x)** (**x** indica el número de nodos que se verán afectados por la operación de borrado). Se mostrará un mensaje indicando el número total de nodos que se eliminarán del grafo: el propio nodo y todos sus descendientes.
- Haz clic en el botón **Aceptar**.

Para borrar varios nodos:

- Selecciona los nodos a borrar y haz clic en cualquiera de ellos con el botón derecho del ratón. Se mostrará el menú de contexto.
- Selecciona la opción **Borrar (x)**. Se mostrará un mensaje indicando el número total de nodos

que se eliminarán del grafo: los nodos seleccionados y todos sus descendientes.

- Haz clic en el botón **Aceptar**.

Agrupar nodos

En los grafos que contienen una gran cantidad de elementos, el analista puede agrupar nodos que guarden algún tipo de relación para simplificar el diagrama.

Las agrupaciones de nodos tienen dos estados:

- **Expandida**: si muestra los nodos que la forman.
- **Colapsada**: si oculta los nodos que la forman.

Una agrupación de nodos es una entidad por sí misma, con las siguientes características:

- Las acciones aplicadas sobre un grupo de nodos afectan a todos los nodos que lo componen.
- Se pueden agrupar nodos de diferentes tipos.
- Eliminar una agrupación equivale a eliminar del grafo todos los nodos que la componen.
- Al colapsar un grupo, todas las relaciones de sus miembros con nodos externos se representan como si estuvieran establecidas con la agrupación. Las flechas que reflejen relaciones de un mismo tipo (mismo tipo de evento) también se agrupan (consulta **Grupo de nodos colapsado**).
- El espacio vacío de una agrupación expandida, representa al conjunto de nodos agrupados. Por ejemplo, para mostrar el menú de contexto de todos los nodos de una agrupación haz clic con el botón derecho del ratón en un espacio vacío de la agrupación expandida. De la misma forma, si seleccionas la opción **Eliminar**, borrarás todos los nodos que pertenecen a la agrupación.
- Un nodo que pertenece a una agrupación expandida conserva el comportamiento normal de un nodo del grafo sin agrupar: se podrá mover de forma individual, mostrar su menú de contexto, borrar, etc.
- Una agrupación puede estar formada solo por nodos, solo por grupos, o por una mezcla de ambos.

Para agrupar un conjunto de nodos:

- Selecciona varios nodos del diagrama y haz clic con el botón de la derecha del ratón. Se abrirá el menú de contexto.
- En el menú selecciona **Agrupar**  . Se creará un rectángulo de agrupación que contiene los nodos agrupados.

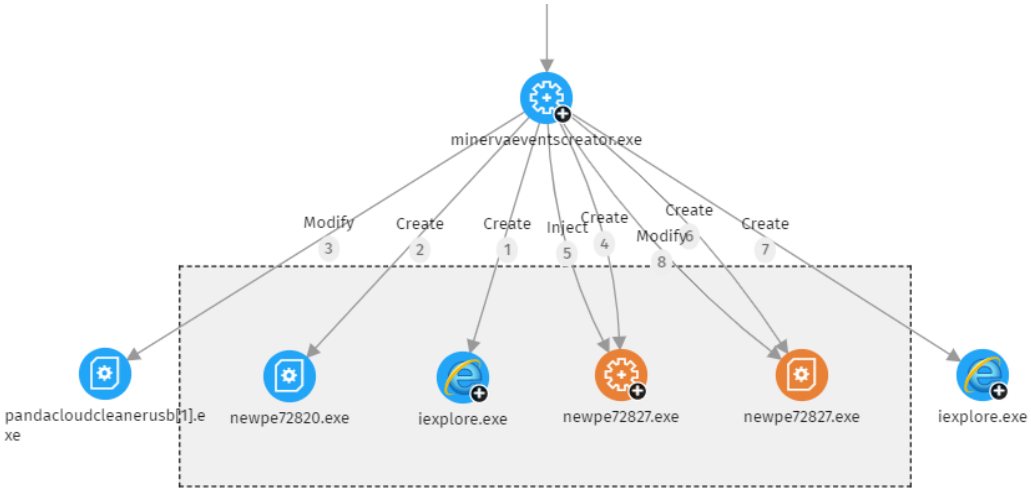


Figura 12.4: Agrupación de nodos

- Haz clic con el botón derecho del ratón en una zona despejada del rectángulo de agrupación. Se abrirá el menú de contexto de la agrupación.
- En el menú selecciona **Colapsar**. Los nodos agrupados se sustituyen por un cuadrado de tamaño inferior y todas las relaciones de los nodos agrupados se mueven al cuadrado de agrupación.

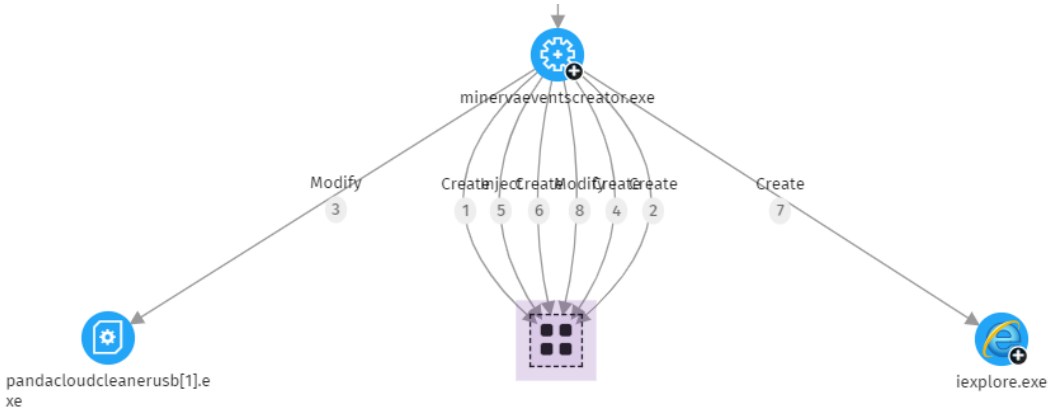


Figura 12.5: Grupo de nodos colapsado

Para expandir un grupo de nodos colapsado:

- Selecciona con el botón derecho del ratón el grupo de nodos colapsado. Se abrirá el menú de contexto.
- Selecciona la opción **Expandir**. Los nodos colapsados se mostrarán junto al rectángulo de agrupación.

Para deshacer una agrupación de nodos:

- Selecciona con el botón derecho del ratón el grupo de nodos. Se abrirá el menú de contexto.
- Selecciona la opción **Desagrupar**. Los nodos agrupados se mostrarán en el grafo y el rectángulo de agrupación desaparecerá.

Información de una agrupación colapsada

Tipo de nodos agrupados

Una agrupación puede contener nodos clasificados como goodware, malware o sin clasificar. Esta situación se refleja en el color utilizado para representar la agrupación.

Color	Descripción
	Agrupación con elementos bloqueados.
	Agrupación con elementos clasificados como goodware.

Tabla 12.1: Códigos de color utilizados en las agrupaciones

Número de nodos agrupados

En la esquina superior izquierda se muestra el número de nodos que se mostrarían en el diagrama en caso de que la agrupación no estuviera colapsada. Este número no tiene nada que ver con el número de nodos total (padres, hijos, etc) que puede contener la agrupación, ya que solo se cuentan los nodos que se han expandido previamente.

Buscar nodos

La barra de búsqueda permite resaltar los nodos que interesan al analista y acceder de forma rápida a sus detalles.

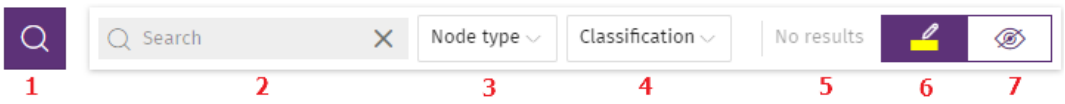


Figura 12.6: Barra de búsqueda de grafos

- **(1)**: Haz clic para mostrar u ocultar la barra de búsqueda.
- **(2)**: Escribe la cadena de caracteres a buscar. La búsqueda se ejecuta en tiempo real sobre el nombre y el detalle de los nodos, y se excluye el contenido de las flechas. Para limpiar la búsqueda, haz clic en el icono ✕.

Para evitar mostrar nodos huérfanos en los resultados de las búsquedas siempre se incluye el nodo padre, aunque no coincida con el patrón introducido.

- **(3)**: Limita las búsquedas en el grafo a determinados tipos de entidades. Para extender la búsqueda a más de un tipo de entidad, expande el desplegable y selecciona los tipos de entidad que deseas. Para volver a buscar en todos los tipos de entidad, haz clic en la opción **Limpiar búsqueda**. El operador lógico aplicado al establecer una búsqueda sobre varios tipos de entidad es OR.
- **(4)** Limita las búsquedas en el grafo a las entidades que han sido clasificados por Cytomic Orion a los valores indicados en el desplegable. Para extender la búsqueda a más de una clasificación, expande el desplegable y selecciona las clasificaciones que deseas. Para volver a buscar sin tener en cuenta la clasificación de las entidades, haz clic en la opción **Limpiar búsqueda**. El operador lógico aplicado al establecer una búsqueda sobre nodos con distintas clasificaciones es OR.
- El operador lógico al definir a la vez una búsqueda por entidad y una búsqueda por clasificación es AND.
- **(5)**: Indica el número de nodos que coinciden con el patrón de búsqueda introducido. Cuando la herramienta de resaltado está activada **(4)**, al hacer clic en el icono ⌄ se muestra un desplegable:
    - **Seleccionar los nodos encontrados**: selecciona los nodos que coinciden con el patrón de búsqueda introducido. Para mostrar el menú de contexto, haz clic con el botón derecho del ratón en cualquier elemento seleccionado.
    - **Seleccionar todos los nodos menos los encontrados**: selecciona los nodos que no coinciden con el patrón de búsqueda introducido. Para mostrar el menú de contexto, haz clic con el botón derecho del ratón en cualquier elemento seleccionado.
- **(6)**: Resalta los elementos encontrados con el color amarillo.
- **(7)**: Oculta los elementos que no coinciden con el patrón de búsqueda introducido.

Las búsquedas realizadas sobre nodos agrupados expandidos se comportan de la forma indicada, pero si se trata de un grupo colapsado, tienen un comportamiento diferente:

- Si la búsqueda se realiza en modo resaltado **(4)**, se iluminará la agrupación si uno de los nodos que la componen coincide con la búsqueda. En caso contrario, la agrupación no se iluminará.
- Si la búsqueda se realiza en modo ocultación **(5)**, la agrupación se mostrará si por lo menos uno de los nodos que la componen coincide con la búsqueda. En caso contrario, la agrupación no se mostrará en el grafo.

Línea de tiempo

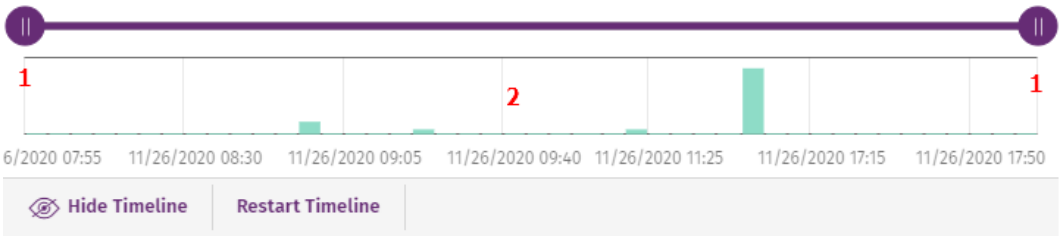


Figura 12.7: Controles de la línea de tiempo

La línea de tiempo permite atenuar los nodos y las relaciones que se registraron fuera del intervalo definido por el analista. De esta manera, los eventos del océano de datos que no resultan de interés, pasan a un segundo plano en el diagrama, y permiten al analista centrarse en los más relevantes.

La línea de tiempo utiliza un histograma de barras de color verde situado en su parte inferior **(2)** para representar el número de eventos registrados en cada momento. Al pasar el puntero del ratón sobre las barras se muestra una etiqueta que indica el número de eventos y la fecha en la que se registraron.

Para definir un intervalo mediante la línea de tiempo:

- Haz clic en **(1)** y arrástralo hacia izquierda y derecha. El histograma se ampliará o reducirá para adaptarse al nuevo intervalo definido.
- El notebook atenuará los nodos y relaciones del diagrama de grafos que queden fuera del nuevo intervalo definido.

Para ocultar / mostrar la línea de tiempo:

- Para eliminar el panel Haz clic en **Ocultar línea de tiempo**.
- Para volver a visualizar el panel haz clic en **Mostrar línea de tiempo**.
- Haz clic en **Reiniciar la línea de tiempo** para restaurar la línea de tiempo a su configuración original.

Información contenida en diagramas de grafos

Los diagramas de grafos utilizan códigos de color, paneles y otros recursos que aportan información sobre las entidades representadas y sus relaciones. Estos recursos dependen de la plantilla utilizada.

Plantilla Process Tree

Esta plantilla muestra de forma gráfica el árbol de ejecución de un proceso concreto, donde los nodos representan las entidades que participan en una operación (procesos, ficheros o destino de

una comunicación u operación) y las flechas la operación propiamente dicha.

Los recursos utilizados para reflejar la información son:

- **Parámetros de la plantilla**: filtra la información de partida del diagrama.
- **Colores de los nodos**: indica la clasificación del elemento.
- **Iconos de los nodos**: indica el tipo de elemento.
- **Iconos de estado**: indica la acción que se ejecutó sobre el elemento.
- **Colores de las flechas**: indica si el elemento fue bloqueado.
- **Estilos de las flechas**: indica el número y el sentido de las acciones ejecutadas entre los dos nodos.
- **Etiquetas de las flechas**: al hacer clic muestra información en el panel de la derecha sobre la acción ejecutada por el proceso.
- **Etiquetas del nodo**: al hacer clic muestra información en el panel de la derecha sobre la entidad.

Parámetros de la plantilla

- **parentpid**: identificador del proceso padre. Determina la instancia de ejecución específica de un programa que se mostrará como nodo inicial en el diagrama de grafos.
- **MUID**: identificadores de los equipos donde se ejecutó el proceso a investigar.
- **parentmd5**: MD5 del proceso padre.
- **date_event**: fecha del evento a representar en el grafo. El gráfico muestra los eventos que pertenecen al intervalo comprendido entre el día anterior y posterior al indicado.

Colores de los nodos

Color	Descripción
	Elemento clasificado como malware.
	• Elemento clasificado como PUP. • Elemento clasificado como sospechoso. • Elemento sin clasificar.
(Color original)	Elemento clasificado como goodware.

Tabla 12.2: Códigos de color utilizados en los nodos de una plantilla Process Tree

Iconos de los nodos

Icono	Descripción	Icono	Descripción
	Proceso. Si pertenece a un paquete de software conocido se mostrará su icono.		Archivo comprimido
	Hilo remoto		Archivo ejecutable
	Librería		Archivo de tipo script
	Protección		Valor de la rama del registro Windows
	Carpeta		URL en una comunicación
	Archivo no ejecutable		Dirección IP en una comunicación

Tabla 12.3: Códigos de color utilizados en los nodos de una plantilla

Iconos de estado

Icono	Descripción	Icono	Descripción
	Fichero borrado		Fichero en cuarentena
	Fichero desinfectado		Proceso eliminado

Tabla 12.4: Iconos utilizados para indicar el estado del nodo

Etiquetas de los nodos

Indica el nombre de la entidad. Al hacer clic sobre ella, se muestra el panel derecho con los campos que la describen.

Colores de las flechas

Indica si Cytomic EDR o Cytomic EPDR bloquearon la ejecución de la acción por haber clasificado al proceso como una amenaza.

- **Rojo**: la acción fue bloqueada por el software de protección. Consulta el significado de las acciones siguientes en el campo **action** de **Campos de los eventos recibidos en Cytomic Orion** en la página **402**.
    - Block
    - BlockTimeout
    - BlockExploit
    - BlockBL
    - Disinfect
    - Delete
    - Quarantine
    - KillProcess
    - IPBlocked
- **Negro**: la acción fue permitida.

Estilos de las flechas

- **Grosor de la flecha**: representa el número de acciones de un mismo tipo ejecutadas entre un par de nodos. Cuanto mayor sea el número de acciones agrupadas, mayor será el grosor de la flecha dibujada. Al hacer clic en la flecha, el panel informativo mostrará la fecha en la que se ha producido la primera y la última acción de la agrupación.
- **Sentido de la flecha**: refleja el sentido de la acción.
- **Numeración**: cada flecha incluye un número que refleja el orden en el que se registró el evento al que representa.

Etiquetas utilizadas en las flechas

Indica el nombre de la acción ejecutada por el proceso. Al hacer clic, se muestra el panel derecho con los campos del evento registrado.

Niveles representados por defecto

Inicialmente, una plantilla Tree Process muestra el nodo seleccionado por el analista como centro del diagrama, junto a un subconjunto de nodos vecinos que lo rodean, de todos los disponibles en

el océano de datos:

- **3 niveles superiores de nodos**: se muestran los nodos padres, abuelos y bisabuelos del nodo principal.
- **1 nivel inferior de nodos**: se muestran los nodos hijos del nodo principal.

El número máximo de nodos del mismo nivel que se muestran es 25. Por encima de este número no se representarán nodos para evitar la generación de gráficos muy sobrecargados.

Mostrar los nodos hijos

Si un nodo del grafo tiene nodos hijos ocultos, se indica con el icono ⊕ en su parte inferior derecha.

Para mostrar sus nodos hijos, haz clic en el nodo con el botón derecho del ratón. Se mostrará un menú de contexto. Dependiendo del tipo de nodo se mostrarán las siguientes opciones:

- **Mostrar padre**: muestra los nodos padre del nodo seleccionado.
- **Mostrar toda su actividad (número)**: muestra todos los nodos hijos del nodo seleccionado sin importar su tipo. El número máximo de nodos mostrados es 25. Se indica el número total de eventos que relacionan el nodo padre con sus hijos.
- **Mostrar hijos**: muestra un desplegable con el tipo de nodos hijo a mostrar y el número de nodos de cada tipo:
    - **Archivos de datos**: ficheros que contienen información de tipo no identificado.
    - **Archivos de script**: ficheros con secuencias de comandos.
    - **Descargas**: ficheros de datos descargados de la red.
    - **DNS**: dominios que fallaron al resolver su IP.
    - **Entradas del registro de Windows**
    - **Ficheros comprimidos**
    - **Ficheros PE**: ficheros ejecutables.
    - **Hilos remotos**
    - **IPs**: dirección IP del extremo de la comunicación.
    - **Librerías**
    - **Procesos**
    - **Protección**: acción del antivirus.

Al seleccionar varios nodos del diagrama y hacer clic con el botón derecho del ratón se mostrarán únicamente las opciones del menú de contexto comunes a todos los nodos seleccionados.

Investigación con notebook

Para iniciar una investigación automatizada sobre un nodo del grafo, haz clic con el botón derecho del ratón en el grafo y selecciona **Investigación automatizada**. Se mostrará el listado de

plantillas disponibles. Para obtener más información sobre investigaciones automatizadas consulta **Investigación con notebooks** en la página **220**.

Plantilla New users in a customer

Muestra los usuarios nuevos que iniciaron sesión en los equipos de un cliente. Para ello, la plantilla ejecuta las siguientes tareas:

- Recopilar todos los usuarios que iniciaron sesión en los equipos del cliente en un periodo anterior tomado como referencia (conjunto A).
- Recopilar todos los usuarios que iniciaron sesión en los equipos del cliente en el periodo de interés para el analista (conjunto B).
- Calcular la resta de conjuntos B - A:
    - Los usuarios que pertenecen al conjunto B y no pertenecen al conjunto A son los usuarios nuevos representados en el diagrama.
    - Los usuarios que pertenecen al conjunto A y al conjunto B se descartan.
    - Los usuarios que pertenecen al conjunto A se descartan.

Los recursos utilizados para reflejar la información son:

- **Parámetros de la plantilla**: filtra la información de partida del diagrama.
- **Iconos de los nodos**: indica el tipo de elemento.
- **Etiquetas del nodo**: al hacer clic muestra información en el panel de la derecha sobre la entidad.

Parámetros de la plantilla

- **client**: cliente donde se buscarán los usuarios nuevos.
- **train_ date_ from** : límite inferior del periodo que se toma como referencia para la comparación.
- **train_ date_ to** : límite superior del periodo que se toma como referencia para la comparación.
- **test_date_from**: límite inferior del periodo donde se buscarán nuevos usuarios.
- **test_date_to**: límite superior del periodo donde se buscarán nuevos usuarios.

Iconos de los nodos

Icono	Descripción	Icono	Descripción
	Cuenta de usuario		Equipo

Tabla 12.5: Códigos de color utilizados en los nodos de una plantilla

Etiquetas de los nodos

Indica el nombre de la entidad. Al hacer clic sobre ella, se muestra el panel derecho con los campos que la describen.

Capítulo 13

Investigación con notebooks

JupyterLab es una tecnología web open source ampliamente difundida en la comunidad investigadora, que permite configurar un entorno de trabajo interactivo para desarrollar soluciones en diversos lenguajes de programación de manera dinámica. Integrar en un mismo tipo de documento bloques de código, texto, imágenes o gráficas, y es utilizado frecuentemente por analistas de diversas áreas para transformar y cribar datos, realizar simulación numérica, modelado estadístico, machine learning y otras muchas tareas.

Cytomic Orion integra la tecnología JupyterLab para ofrecer al analista de seguridad un entorno bien conocido y probado por la industria para automatizar y compartir sus investigaciones, a la vez que le permite configurar informes "a la carta", utilizando representaciones gráficas de los resultados que le ayuden a poner en valor sus hallazgos.

Los notebooks son documentos dinámicos e interactivos que aportan al analista los beneficios siguientes:

- Compartir de forma fácil el código de la investigación con otros técnicos del SOC para acelerar su desarrollo.
- Presentar de forma visual los resultados de las investigaciones a los clientes.
- Explotar los datos recogidos y mostrados en el notebook de forma interactiva.

CONTENIDO DEL CAPÍTULO

Conceptos y definiciones

Para sacar partido de la tecnología JupyterLab integrada en Cytomic Orion es recomendable asimilar los conceptos mostrados a continuación:

Notebook

Es una representación web de todas las entradas y salidas que se han producido a lo largo del tiempo en torno a uno o varios fragmentos de código ejecutados de forma interactiva, incluyendo explicaciones en formato texto, imágenes y representaciones de objetos más elaboradas. En cierta forma, un notebook es el registro de una sesión iniciada por el analista, mezclando código ejecutable con textos explicativos y sus resultados.

Celda

Un notebook está formado por una secuencia de celdas. La celda es la unidad básica del notebook y consiste en una caja de texto que acepta una o más líneas de código y se ejecuta pulsando simultáneamente las teclas '`mayus + Enter`' o haciendo clic en el icono ▷ de la barra de herramientas del notebook.

El comportamiento de la ejecución de una celda viene determinado por su tipo:

Celdas de código

Permiten escribir código en lenguaje Python, soportado por el kernel de Cytomic Orion. Cuando una celda ejecuta el código que contiene, éste se envía al kernel asociado que lo interpretará y devolverá los resultados directamente a la celda ejecutada. El resultado de la ejecución de una celda no está limitado a texto sino que puede incluir gráficos con `matplotlib`, tablas con `pandas`, etc.

Una celda está formada por las partes indicadas a continuación:

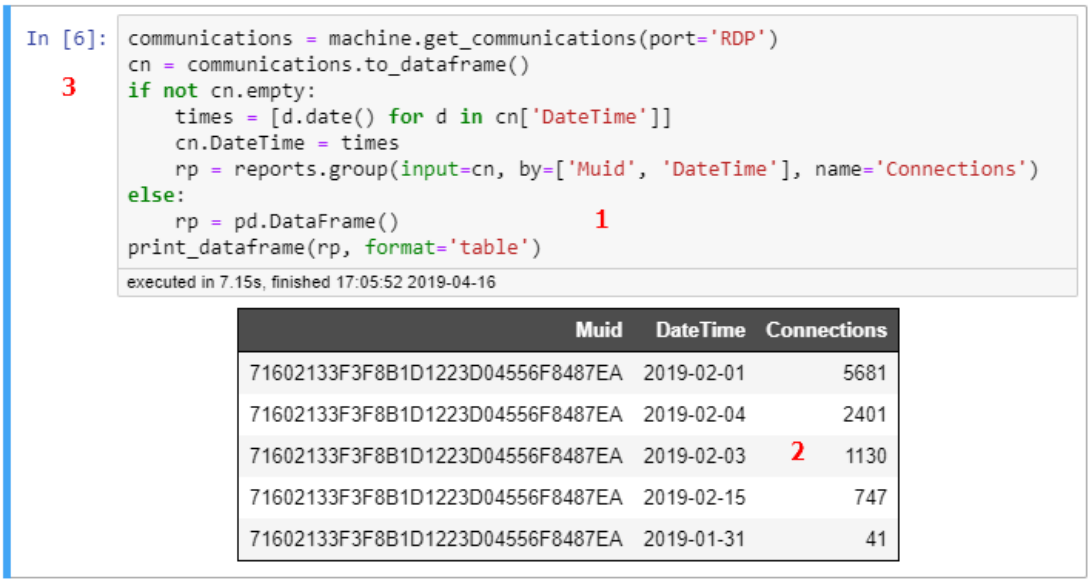


Figura 13.1: Estructura general de una celda de un notebook

- **(1)** Caja de texto donde el analista incluye lo fragmentos de código a ejecutar.
- **(2)** Zona de resultados. En la figura **Estructura general de una celda de un notebook** se muestran en formato tabla.
- **(3) Control de ejecución**: indica que la celda es de tipo código y muestra su estado:
  - **[Numérico]**: número de veces que se ha ejecutado la celda.
  - **[*]**: la celda se está evaluando / ejecutando.

Celdas Markdown:

Permiten documentar los procesos implementados en el notebook utilizando texto enriquecido. El lenguaje Markdown es una forma sencilla de decorar secciones de textos con negritas, itálicas, listas y otros recursos estándar de maquetación de textos. También puede ser utilizado para estructurar el notebook con cabeceras e índices que permiten añadir enlaces a sus distintas secciones. Cuando una celda de tipo Markdown se ejecuta, su código se renderiza para mostrar el texto enriquecido, admitiendo código HTML para el formateo.

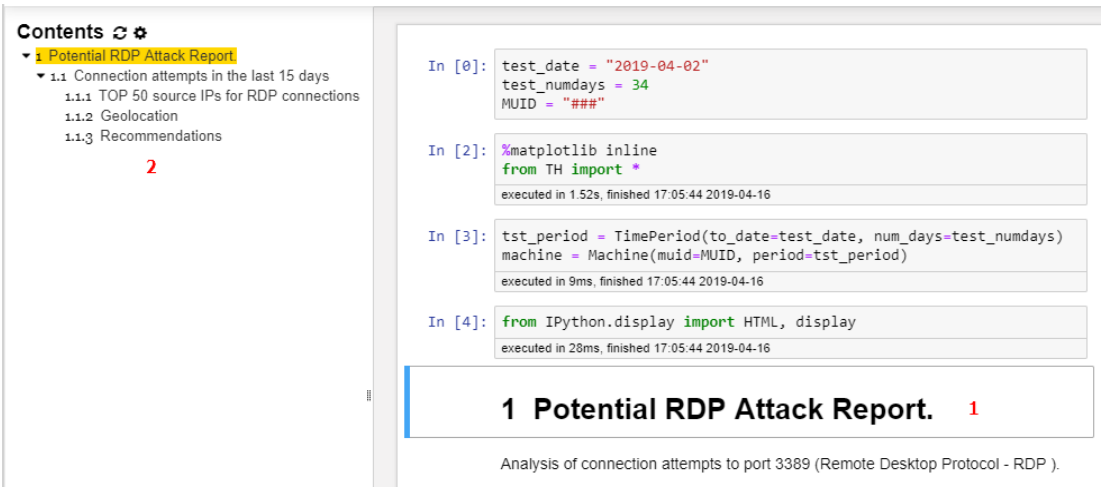


Figura 13.2: Celda Markdown renderizada y tabla de contenidos correspondiente al notebook

- **(1)** Celda Markdown con un texto de tipo cabecera nivel 1.
- **(2)** Tabla de contenidos generada automáticamente en base a las celdas Markdown de tipo cabecera contenidas en el notebook.

> *Para obtener más información acerca de cómo escribir celdas de tipo Markdown consulta el enlace* ***https://daringfireball.net/projects/markdown/basics***

Kernel

Es el entorno de ejecución en el servidor que interpreta el contenido de las celdas y genera los resultados. El kernel implementado es compatible con Python versión 3.6.

Respuestas rápidas

Son fragmentos de código independientes y reutilizables que se pueden añadir a un notebook de forma rápida y se ejecutan de forma autónoma. Las Respuestas rápidas son pequeños programas que conforman una completa biblioteca de soluciones a problemas comunes para la mayor parte de los analistas de seguridad. Consulta **Guía rápida de manejo de notebooks** para obtener más información.

Plantillas

Son notebooks almacenados en la plataforma Cytomic Orion que resuelven problemas comunes y que pueden ser importados, compartidos o modificados por los analistas, tomándolos como base para crear nuevos notebooks que se ajusten a sus necesidades. Cytomic mantiene una librería de plantillas que actualiza de forma constante y que pone a disposición de todos sus clientes. Consulta **Gestión de plantillas** para obtener más información acerca de las plantillas.

Parámetros

Las plantillas y las Respuestas rápidas pueden requerir datos de entrada para funcionar correctamente, como por ejemplo el identificador del equipo (MUID) o la fecha en la que la automatización recuperará los datos. Al ejecutar un notebook o una Respuesta rápida con parámetros se mostrará una ventana pidiendo la información necesaria al analista. Los datos introducidos se copiarán en la primera celda del notebook.

Librerías

El kernel del notebook en Cytomic Orion tiene acceso a un gran número de librerías externas escritas en Python y en otros lenguajes compilados que facilitan el análisis, la manipulación de datos y la presentación gráfica de resultados. Estas librerías son muy utilizadas por la comunidad de analistas y, adicionalmente, Cytomic Orion incluye acceso a la librería de Threat Hunting que facilita la automatización de las investigaciones.

Consulta **Librerías disponibles en los notebooks** para obtener un listado de todas las librerías disponibles en los notebooks de Cytomic Orion.

Principales beneficios de los notebooks

- Edición de código directamente desde el navegador: resalta automáticamente la sintaxis del lenguaje, aplica indentaciones y completa las sentencias con el tabulador.
- Ejecuta código en el servidor y muestra los resultados directamente en el navegador del analista.
- Muestra el resultado de la investigación utilizando elementos gráficos y textuales complejos mediante el uso de librerías externas, tales como `matplotlib`.
- Edición de texto avanzada en el navegador utilizando el lenguaje de marcas Markdown para comentar el código.
- Facilitad al incluir textos en notación matemática con `LaTex` y renderizado de forma nativa con `mathJax`.
- Permite compartir el código fuente utilizado por los analistas en las investigaciones de forma natural, sin necesidad de enviar ficheros ni ejercer un control de versiones.
- Permite diseñar de forma ágil Respuestas rápidas ante incidentes de seguridad que se ejecutan de forma centralizada e interactiva.
- Favorece la compartición de los resultados de una investigación, facilitando la exportación a formatos más adaptados para su envío.

Acceso y creación de notebooks

> *Para utilizar de forma completa los notebooks, la cuenta de acceso del analista deberá tener asignado el grupo de permisos **Investigaciones mediante Notebooks**. Para más información consulta**Descripción de los permisos implementados** en la página **60**.*

Los notebooks son una herramienta esencial que forma parte de las investigaciones creadas. Una investigación puede contener todos los notebooks que el analista considere necesarios para realizar sus análisis.

Para acceder a un notebook previamente creado sigue los pasos mostrados a continuación:

- En el menú superior **Investigaciones** elige la investigación a la que pertenece el notebook de la lista mostrada.
- Haz clic en un notebook del subpanel de notebooks situado abajo a la derecha de la ventana de la investigación.

Crear un notebook desde la barra de herramientas de una investigación

- En el menú superior **Investigaciones** elige la investigación de la lista a la que pertenecerá el notebook o crea una nueva investigación. Consulta **Gestión de investigaciones** en la página **99** para obtener más información acerca de las investigaciones y como crearlas.
- En la barra de herramientas haz clic en el icono + y elige **Investigación manual**.

Crear un notebook desde el subpanel de una investigación

- En el menú superior **Investigaciones** elige de la lista la investigación a la que pertenecerá el notebook o crea una nueva investigación. Consulta **Gestión de investigaciones** en la página **99** para obtener más información acerca de las investigaciones y como crearlas.
- En el subpanel **Archivos** haz clic en el icono + y elige **Investigación manual**.

Listado de notebooks creados en una investigación

Para acceder al listado y obtener información de los notebooks creados en una investigación haz clic en el menú superior **Investigaciones**. En la parte inferior derecha se mostrará el subpanel **Notebooks**. Consulta **Subpanel Ficheros (6)** en la página **114** para obtener información sobre el significado de los campos del listado.

Estructura de un notebook

Un notebook en Cytomic Orion sigue un esquema equivalente al de los notebooks de Jupyter. En la imagen mostrada a continuación se detallan las partes que lo forman:

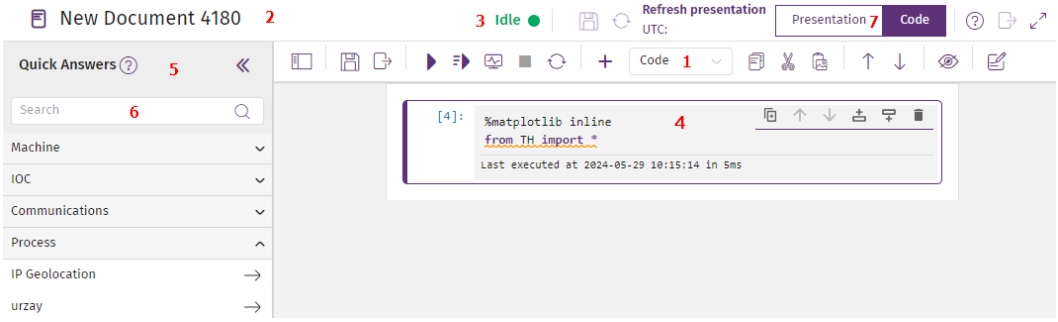


Figura 13.3: Esquema general de un notebook

- **Barra de herramientas del Notebook (1)**: ofrece las acciones más utilizadas para interactuar con el notebook.
    - **Mostrar tabla de contenidos**: muestra la tabla de contenidos construida en base a las cabeceras incluidas en las celdas de tipo Markdown.
    - **Salvar**: almacena en el servidor el contenido del notebook.
    - **Convertir**: oculta las celdas de código y salva en PDF o HTML el resultado de éstas, incluyendo las tablas, gráficos, diagramas y otros elementos estáticos.
    - **Ejecutar celda**: envía el contenido de la celda al kernel y recoge los resultados.
    - **Ejecutar todo**: envía el contenido de todas las celdas de forma secuencial y recoge los resultados de cada una de ellas.
    - **Ejecutar presentación**: ejecuta todas las celdas del notebook y muestra el modo presentación. Consulta **Ejecutar un notebook**.
    - **Detener la ejecución**: interrumpe la ejecución de la celda.
    - **Reiniciar el kernel**: limpia la sesión iniciada. Todas las variables creadas por la ejecución previa de celdas son destruidas.
    - **Añadir una celda**: crea una nueva celda debajo de la celda seleccionada.
    - **Establecer el tipo de celda**: indica si es una celda de tipo código o Markdown.
    - **Copiar**: guarda la celda en el portapapeles.
    - **Cortar**: guarda la celda en el portapapeles y la borra del notebook.
    - **Pegar**: inserta en el notebook la celda guardada previamente en el portapapeles.
    - **Subir celda**: mueve la posición de la celda un paso hacia arriba.

- **Bajar celda** : mueve la posición de la celda un paso hacia abajo.
- **Ocultar código** : elimina el código en Python para mostrar únicamente los resultados de las celdas ejecutadas.
- **Nueva Respuesta** : añade una Respuesta rápida a la biblioteca. Consulta **Gestión de Respuestas rápidas**.
- **Nombre del Notebook (2)**: para cambiar el nombre del notebook haz clic en el cuadro de texto. Se abrirá una ventana pidiendo el nuevo nombre. Al hacer clic en **Aceptar** se asignará el nuevo nombre al notebook.
- **Estado del kernel (3)**: indica si el motor de ejecución del notebook está parado (**Inactivo**) o trabajando en la ejecución de alguna celda (**Ocupado**).

- **Celda del notebook (4)**: es la unidad básica del notebook y consiste en una caja de texto que acepta una o más líneas de código y un grupo de iconos para realizar operaciones rápidas:
  - : copia la celda debajo de la actual.
  - : mueve la celda una posición hacia arriba.
  - : mueve la celda una posición hacia abajo.
  - : inserta una celda vacía encima de la actual.
  - : inserta una celda vacía debajo de la actual.
  - : borra la celda actual.
- **Listado de Respuestas rápidas (5)**: son pequeños fragmentos de código que agilizan el desarrollo de las investigaciones de los analistas. Consulta **Gestión de Respuestas rápidas**.
- **Cuadro de búsqueda (6)**: escribe el nombre parcial o completo de la Respuesta rápida que quieres localizar para agregar al notebook.
- **Modo de visualización (7)**: permite alternar entre el modo de introducción de código (**Código**) y el modo de presentación de resultados (**Presentación**). Consulta **Ejecutar un notebook** para más información.

Ejecutar un notebook

Cytomic Orion soporta varios modos de ejecución de los notebooks:

- **Ejecución de una celda**: mediante el icono en la barra de herramientas, orientado al desarrollo del notebook, muestra los resultados de una única celda inmediatamente después de la misma.

- **Ejecución de todas las celdas**: mediante el icono en la barra de herramientas, presenta los resultados de cada una de las celdas inmediatamente después de las mismas.
- **Ejecución del notebook completo**: mediante el icono o seleccionando el modo **Presentación**, orientado a compartir los resultados. Consulta **Ejecutar un notebook** para obtener más información sobre este modo.

Acceso al modo presentación

Para acceder a este modo haz clic en el botón **Presentación** o en el icono de la barra de herramientas. Se mostrará una animación indicando la ejecución del notebook para finalmente mostrar los resultados.

Controles del modo presentación

A parte de la información generada por el notebook, el modo presentación habilita una serie de controles que le permiten al analista interactuar con el mismo:

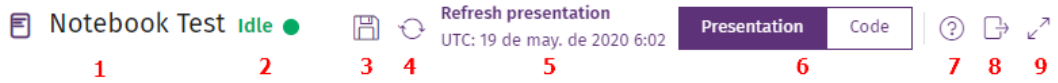


Figura 13.4: Controles del modo presentación de un notebook

- **Nombre del notebook (1)**.
- **Estado del kernel (2)** :indica si el motor de ejecución del notebook está parado (**Inactivo**) o trabajando en la ejecución de alguna celda (**Ocupado**).
- **Grabar (3)**: guarda los resultados del notebook.
- **Recarga (4)**: vuelve a ejecutar el notebook y presenta los resultados.
- **Fecha de la última ejecución (5)**: fecha, hora y zona horaria del momento en que se ejecutó el notebook por última vez.
- **Modo de presentación (6)**: en el modo **Código**, el notebook muestra los resultados de forma individual asociado a cada celda de código. En el modo **Presentación**, el código se oculta y el notebook muestra únicamente los resultados, permitiendo la interacción con el analista.
- **Ayuda (7)**: muestra el panel lateral de ayuda web.
- **Convertir (8)**: salva en PDF o HTML el resultado del notebook, incluyendo las tablas, gráficos, diagramas y otros elementos estáticos.
- **Maximizar (9)**: oculta todos los menús y elementos accesorios de Cytomic Orion para presentar los resultados de forma limpia en pantalla.

Persistencia del modo presentación

Cuando un analista ejecuta un notebook en modo presentación, los datos calculados se salvan en la plataforma. De esta forma, si se accede al notebook posteriormente éste cargará los resultados guardados de automáticamente, mostrando su última ejecución.

> *Al mostrar los datos almacenados de una ejecución anterior el notebook pierde temporalmente sus características interactivas. Haz clic en icono de recarga* ***(2)*** *para recuperar esta funcionalidad.*

Uso de plantillas en notebooks

Las plantillas son notebooks almacenados en la plataforma Cytomic Orion que pueden ser tomadas como base para desarrollar nuevos notebooks. También puede ser ejecutadas, compartidas o modificadas por los analistas.

> *Para gestionar plantillas la cuenta de acceso del analista deberá tener asignada los permisos* ***Crear Notebook desde plantilla para investigación automatizada*** *y* ***Gestionar plantillas de Notebooks de investigación****. Para más información consulta* ***Descripción de los permisos implementados*** *en la página* ***60****.*

Acceso a la gestión de plantillas

Para acceder a la pantalla de gestión de plantillas haz clic en el menú superior **Configuración** y en el panel lateral izquierdo **Plantillas**. Se mostrará un listado de plantillas ya creadas y el botón **Añadir plantilla** con la información siguiente:

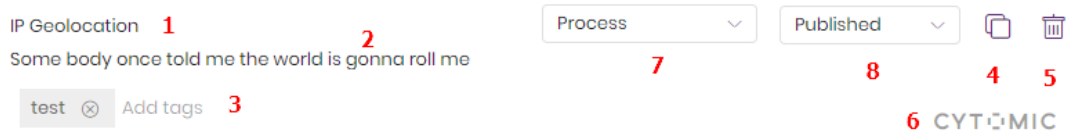


Figura 13.5: Esquema general de una plantilla

- **Nombre de la plantilla (1)**: elegida por el técnico que creó la plantilla.
- **Descripción de la plantilla (2)**: bloque de texto libre que describe el objetivo de la plantilla.
- **Etiquetas (3)**: facilitan la localización y descripción de la plantilla.
- **Herramienta de copia (4)**: consulta **Duplicar una plantilla**.
- **Herramienta de borrado (5)**: consulta **Borrar una plantilla**.
- **Logotipo (6)**: indica la procedencia de la plantilla.
    - **Plantillas publicadas por Cytomic** : son plantillas desarrolladas por los analistas expertos en malware de Cytomic cuyo buen funcionamiento ha sido certificado. Estas plantillas están disponibles para todos los clientes de Cytomic Orion y no

pueden ser modificadas por éstos aunque sí se admite la modificación de las copias efectuadas por los analistas del SOC.

- **Plantillas de cliente**: son plantillas desarrolladas por los usuarios de Cytomic Orion. Solo se pueden compartir entre los analistas de un mismo MSSP / MDR o SOC.

- **Categoría (7)**: clase a la que pertenece la plantilla. Elegida por el técnico que creo la plantilla.
- **Estado (8)**: consulta **Publicar una plantilla**

Gestión de plantillas

Acceso a la gestión de plantillas

Para acceder a la pantalla de gestión de plantillas, haz clic en **Configuración** en el menú superior y en **Plantillas** en el panel lateral. Se mostrará una lista de las plantillas ya creadas y el botón **Añadir plantilla**.

Crear una plantilla

- Haz clic en el menú superior **Configuración** y en el panel lateral izquierdo **Plantillas**.
- Haz clic en el botón **Añadir plantilla**. Se añadirá una nueva entrada al final del listado de plantillas.

Duplicar una plantilla

- Haz clic en el menú superior **Configuración** y en el panel lateral izquierdo **Plantillas**.
- Haz clic en el icono de la plantilla a copiar. La plantilla se copiará añadiendo la cadena "[Copy] - " al comienzo de su nombre.

> *Para modificar una plantilla creada por Cytomic es necesario previamente duplicarla. Las plantillas originales de Cytomic no pueden ser modificadas.*

Borrar una plantilla

- Haz clic en el menú superior **Configuración** y en el panel lateral izquierdo **Plantillas**.
- Haz clic en el icono de la plantilla a borrar. Se abrirá una ventana pidiendo confirmación.

Publicar una plantilla

- Haz clic en el menú superior **Configuración** y en el panel lateral izquierdo **Plantillas**.
- Haz clic en el desplegable y elige **Publicada**.

Una vez que la plantilla esté publicada será accesible por todas las cuentas pertenecientes al MSSP / MDR o SOC. Si la plantilla aparece como **No publicada** solo será accesible por la cuenta que la creó.

Modificar los atributos de una plantilla

- Para modificar el nombre, las etiquetas o la descripción de una plantilla haz clic en el atributo y escribe el nuevo valor.
- En el caso de las etiquetas se mostrará un desplegable con todas las que estén disponibles. Para crear una etiqueta nueva escribe su valor en el campo etiquetas y pasará a estar disponible en el desplegable del resto de plantillas creadas.

Modificar el contenido de una plantilla

Haz clic en la plantilla. Se mostrará el contenido en un notebook. Una vez modificado haz clic en el botón de la barra de herramientas del notebook o presiona '`Ctrl+s`'.

Crear un notebook desde una plantilla

Para lanzar el asistente de creación de un notebook tomando como base una plantilla sigue los pasos mostrados a continuación:

- En el menú superior **Investigaciones** elige la investigación de la lista a la que pertenecerá el notebook o crea una nueva investigación. Consulta **Gestión de investigaciones** en la página **99** para obtener más información acerca de las investigaciones y como crearlas.
- En la barra de herramientas haz clic en el + y elige **Investigación automatizada**. Se abrirá una ventana donde elegir la plantilla en la que se basará el nuevo notebook:
    - Utiliza la caja de texto **Buscar** para establecer las etiquetas que actuarán como filtro para facilitar la búsqueda de la plantilla. Al hacer clic en la caja de texto se mostrará un desplegable con todas las etiquetas disponibles. Una vez seleccionada una etiqueta, ésta actuará como filtro de primer nivel. Seleccionando más etiquetas de forma sucesiva se establecerán filtros de 2º, 3º nivel, etc.
    - Si la plantilla tiene parámetros se abrirá una ventana para indicar su contenido junto al nombre del notebook y una descripción. Por cada parámetro se indica el tipo y su nombre. Consulta **Uso de parámetros en plantillas y Respuestas rápidas**.

Una vez completado el asistente, la consola ejecuta los pasos siguientes:

- Crea un nuevo notebook con el contenido de la plantilla y los parámetros seleccionados.
- Asigna en la primera celda los valores recogidos a las variables del notebook para evitar que el analista tenga que conocer el nombre de éstas.
- Incluye de forma automática una variable **Context_params** en formato csv separado por el carácter ";" con el contenido del indicio asociado y sus cabeceras.

Uso de Respuestas rápidas en notebooks

Las Respuestas rápidas son pequeños fragmentos de código que se pueden añadir a un notebook de forma rápida y que son desarrollados por los analistas y por los threat hunters de Cytomic.

> *Para crear una Respuesta rápida, la cuenta de acceso del analista deberá tener asignado el permiso **Crear Quick Answers**. Para más información consulta **Descripción de los permisos implementados** en la página **60***

Esquema general de una Respuesta rápida

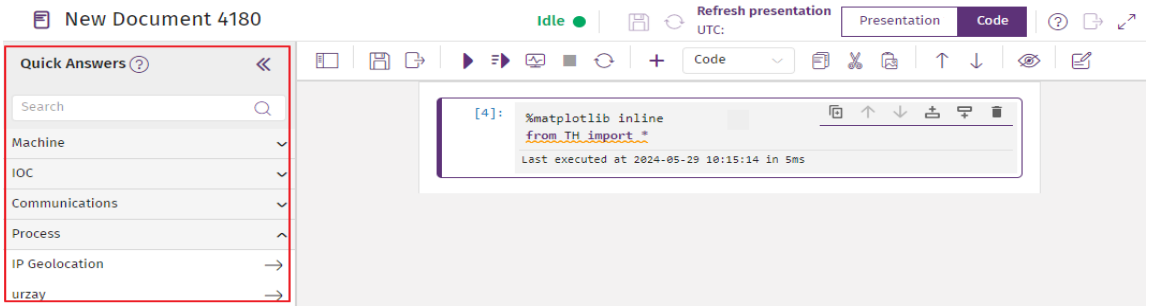


Figura 13.6: Localización de las Respuestas rápidas en el notebook

Dependiendo de su origen las Respuestas rápidas se dividen en dos tipos:

- **Respuestas rápidas publicadas por Cytomic**: desarrolladas por los analistas expertos en malware de Cytomic cuyo buen funcionamiento ha sido certificado. Están disponibles para todos los clientes de Cytomic Orion y no pueden ser modificadas por éstos aunque sí se admite la modificación de las copias efectuadas por los analistas.
- **Respuestas rápidas de cliente**: desarrolladas por los usuarios de Cytomic Orion. Solo se pueden compartir entre los analistas de un mismo MSSP / MDR o SOC.

Cada Respuesta rápida tiene asignada los atributos siguientes:

- **(1)** Nombre de la Respuesta rápida.
- **(2)** Descripción.
- **(3)** Etiquetas (de 0 a n) para facilitar la localización de la Respuesta rápida.
- **(4)** Icono para duplicar la Respuesta rápida.
- **(5)** Icono para borrar la Respuesta rápida.
- **(6)** Logotipo Cytomic que indica si la Respuesta rápida está certificada.
- **(7)** Categoría MITRE correspondiente a la técnica y táctica utilizada en la Respuesta rápida.
- **(8)** Estado de la publicación de la Respuesta rápida.

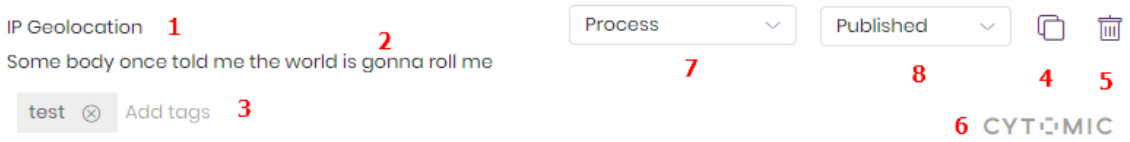


Figura 13.7: Esquema general de una Respuesta rápida

Gestión de Respuestas rápidas

Acceso a la Respuesta rápida

Las Respuestas rápidas son un recurso accesible por el analista desde el panel lateral izquierdo de cualquier notebook previamente creado.

Crear una Respuesta rápida

Se pueden crear Respuestas rápidas desde dos lugares en la consola:

- En un notebook posiciona el cursor en una celda libre y escribe el código que formará parte de la Respuesta rápida. Una Respuesta rápida abarca una única celda.
- Haz clic en el icono , se abrirá una ventana para introducir el nombre de la Respuesta rápida, una descripción, una o varias etiquetas que facilitarán su búsqueda y la categoría MITRE correspondiente a la técnica y táctica utilizadas.

Al hacer clic en el botón **Aceptar**, la Respuesta rápida se agregará en la categoría correspondiente del panel de Respuesta rápida situado en el lateral izquierdo del notebook.

O bien:

- Desde el menú superior **Configuración**, haz clic en el panel lateral izquierdo **Respuesta rápida**.
- Haz clic en el botón **Añadir Respuestas rápidas**. Se añadirá una nueva entrada al final del listado.
- Haz clic en la Respuesta rápida para añadirle código.

Duplicar una Respuesta rápida

- Haz clic en el menú superior **Configuración** y en el panel lateral izquierdo **Respuestas rápidas**.
- Haz clic en el icono de la Respuesta rápida a copiar. La Respuesta rápida se copiará añadiendo la cadena "[Copy] - " al comienzo de su nombre.

Para modificar una Respuesta rápida creada por Cytomic es necesario duplicarla previamente. Las Respuestas rápidas publicadas por Cytomic no pueden ser modificadas.

Borrar una Respuesta rápida

- Haz clic en la Respuesta rápida situada en el panel **Respuestas rápidas**, en el lateral izquierdo del notebook. En la esquina inferior izquierda se mostrará un subpanel con el nombre de la Respuesta rápida y su descripción.
- Haz clic en el botón . Se abrirá una ventana de configuración. Haz clic en el botón **Aceptar** y la Respuesta rápida se eliminará del panel.

Cuando un analista borra una Respuesta rápida, ésta no será accesible para todas las cuentas del MSSP / MDR / SOC. Esta operación no se puede deshacer. Utilízala con precaución.

Publicar una Respuesta rápida

- Haz clic en el menú superior **Configuración** y en el panel lateral izquierdo **Respuestas rápidas**.
- Haz clic en el desplegable y elige **Publicada**.

Una vez que la Respuesta rápida esté publicada será accesible por todas las cuentas pertenecientes al MSSP / MDR o SOC. Si la Respuesta rápida está **No publicada** solo será accesible por la cuenta del analista que la creó.

Modificar los atributos de una Respuesta rápida

- Para modificar el nombre, las etiquetas o la descripción de una Respuesta rápida haz clic en el atributo y escribe el nuevo valor.
- En el caso de las etiquetas, se mostrará un desplegable con todas las que estén disponibles. Para crear una etiqueta nueva escribe su valor en el campo etiquetas y pasará a estar disponible en el desplegable para todas las Respuestas rápidas creadas.

Modificar el contenido de una Respuesta rápida

Haz clic en la Respuesta rápida. Se mostrará el contenido del notebook. Una vez modificado haz clic en el botón de la barra de herramientas del notebook o presiona '`Ctrl+s`'.

Agregar el código contenido en una Respuesta rápida a un notebook

Para añadir el código que contiene una Respuesta rápida al notebook sigue los pasos mostrados a continuación:

- Haz clic en la celda donde se agregará el código correspondiente a la Respuesta rápida.
- Haz clic en el icono → asociado a la Respuesta rápida o doble clic en el nombre. El código que contiene se añadirá a la celda seleccionada.
- Para mostrar la información asociada a una Respuesta rápida haz clic en su nombre. Se mostrará un panel en la esquina inferior izquierda con los datos: nombre y descripción.
- Para insertar el código de la Respuesta rápida en una celda nueva haz clic en el enlace **Insertar contenido**. Se creará una celda con el nuevo contenido inmediatamente después de la celda seleccionada.
- Si la Respuesta rápida requiere parámetros se mostrará una ventana de contenido variable donde se indica el nombre del parámetro y el tipo de dato que se espera.

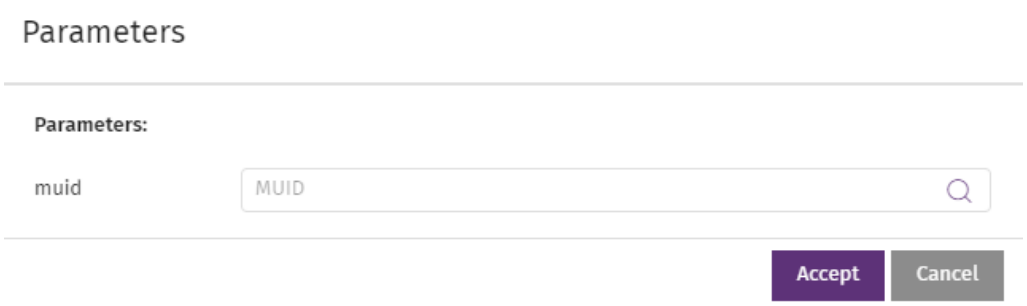


Figura 13.8: Ventana de solicitud de parámetros en una Respuesta rápida

Uso de parámetros en plantillas y Respuestas rápidas

Para asignar un valor a una variable de un notebook de forma interactiva, el analista puede definir parámetros en las plantillas y en las Respuestas rápidas. Un parámetro es una variable declarada de forma específica que, cuando se ejecuta el notebook, muestra una ventana que solicita su valor al analista. De esta forma, Cytomic Orion acelera la asignación de valores a las variables del notebook sin necesidad de que el analista edite o modifique su código.

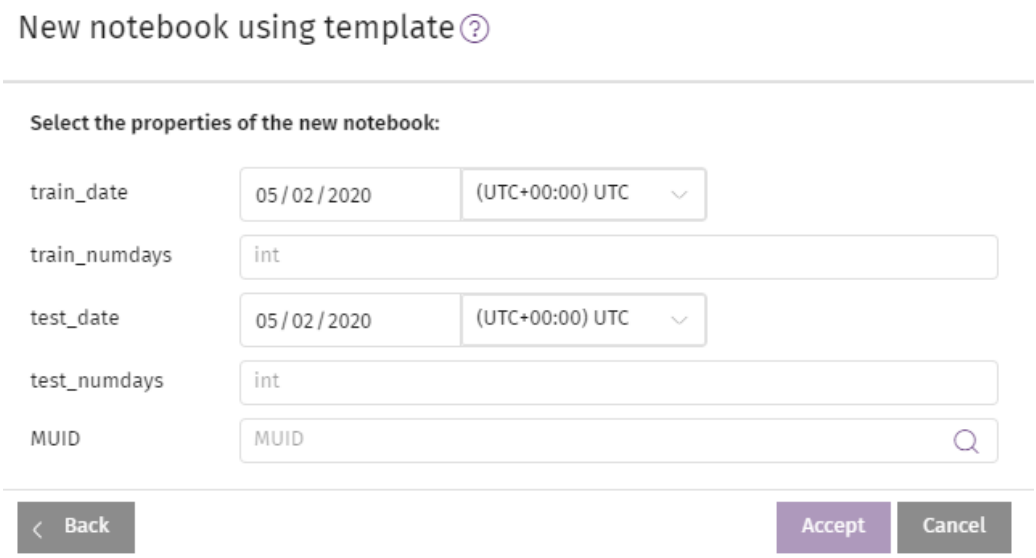


Figura 13.9: Ventana de solicitud de parámetros en una plantilla

Al ejecutar un notebook creado a partir de una plantilla con parámetros definidos, se muestra una ventana de petición de parámetros similar a la figura **Ventana de solicitud de parámetros en una plantilla**. En esta ventana el analista escribe los valores de los parámetros que recibirá el notebook.

Formato de un parámetro

El formato para definir un parámetro en una plantilla es el siguiente:

```
NombreDeVariable = "" # type:tipo
```

Por cada línea que exista en la plantilla con el formato indicado, se añade una entrada en la ventana de petición de parámetros. Si se indica un parámetro de tipo lista, se mostrará una caja de texto donde introducir los diferentes parámetros separados por retorno de carro.

Añadir parámetros a una plantilla o Respuesta rápida

Para añadir parámetros a una plantilla, sigue los pasos mostrados a continuación:

En la primera celda añade una línea por cada parámetro con el formato indicado.

Los tipos de parámetros admitidos son:

Tipo	Descripción
string	Cadena de caracteres.
int	Números enteros.
date	Fechas.
list	Listas de elementos de tipo cadena de

Tipo	Descripción
	caracteres.
MUID	Desplegable con la entidad de interés MUID.
client	Desplegable con la entidad de interés cliente.
MD5	Desplegable con la entidad de interés MD5.

Tabla 13.1: tipos de parámetros soportados en las plantillas

Asignación automática del valor de los parámetros según el contexto

Al ejecutar un notebook con parámetros, el analista debe asignar manualmente el valor de cada uno de ellos en la ventana de petición de parámetros. En notebooks con muchos parámetros definidos, esta tarea puede llegar a ser larga. Para acelerar la asignación de valores, Cytomic Orion es capaz de leer el contexto de la entidad de interés a partir de la cual se lanza el notebook. Por ejemplo, si el analista lanza un notebook a partir de un indicio, Cytomic Orion es capaz de leer los campos de ese indicio en particular y cargar su contenido en los parámetros apropiados de la ventana de petición de parámetros.

Para que Cytomic Orion pueda relacionar un campo de una entidad de interés con un parámetro concreto definido en el notebook a ejecutar, es necesario que se cumplan los requisitos siguientes:

- Que el nombre del parámetro y el nombre del campo coincidan.
- Que el parámetro esté declarado con un tipo básico (int o string).

Por ejemplo, el analista define un notebook que requiere como entrada el MUID de un equipo. Para acelerar la introducción del MUID cuando el notebook es invocado desde un indicio, declarará el parámetro con el nombre "MUID" de tipo string, ya que es así como se llama el campo que contiene el MUID del equipo en los indicios generados por Cytomic Orion.

Asignación de valores por defecto a los parámetros

El formato para asignar en una plantilla un valor por defecto a un parámetro es el siguiente:

```
VariableName = "123" # type:type
```

La asignación automática de valores a los parámetros según el contexto de la entidad, tiene prioridad sobre la asignación de valores por defecto. De esta forma, cuando se abre el notebook y se muestra la ventana de petición de parámetros, si no es posible rellenar el parámetro con el contexto, se añade el valor por defecto indicado en la declaración del parámetro. Igualmente, si un notebook tiene parámetros asignados por defecto, y a su vez el valor de esos mismos

parámetros puede asignarse automáticamente desde el contexto de la entidad, el valor que finalmente se aplicará será el generado por el contexto de la entidad.

Guía rápida de manejo de notebooks

> *Consulta el enlace* ***https://gist.github.com/discdiver/9e00618756d120a8c9fa344ac1c375ac*** *para acceder a un listado completo de los atajos de teclado y acciones disponibles.*

Un notebook basa su funcionamiento en la ejecución de celdas independientes, por lo que el analista necesitará generar dichas celdas con los tipos soportados y ejecutarlas para obtener resultados.

Método de trabajo con notebook

El flujo de trabajo normal con un notebook consiste en dividir el problema a resolver en partes o celdas que se pueden ejecutar de forma independiente. Todas las variables declaradas y funciones definidas en una celda ya ejecutada se mantienen en memoria, de manera que celdas posteriores puedan utilizarlas. El enfoque de dividir la solución del problema en celdas permite ejecutar secciones de código de forma libre sin necesidad de puntos de interrupción (breakpoints) ya que cada celda se ejecuta de forma independiente y muestra sus resultados, permitiendo modificarla y repetir su ejecución las veces como el analista considere necesario hasta obtener el resultado esperado.

Para limpiar el estado generado por la ejecución previa de celdas del notebook es necesario reiniciar el kernel asociado con el botón de la barra de herramientas.

Modo de edición y modo de comandos

Un notebook soporta dos modos de funcionamiento:

- En el modo edición el analista puede editar o ejecutar el contenido de la celda seleccionada marcada con el color morado.
- En el modo de comandos el analista puede añadir celdas, borrarlas o cambiar su orden.
- Para cambiar al modo de comandos pulsa la tecla escape o haz clic en una zona libre del notebook.
- Para cambiar a modo de edición haz clic en la caja de texto de la celda a editar o con los cursores selecciona una celda con la tecla `Enter`.
- Al hacer clic en un icono de la barra de herramientas del notebook se pasa a modo comandos de forma automática.

Seleccionar celdas del notebook

- **Para seleccionar una celda en modo comandos**: utiliza las teclas de cursor o las teclas '`k`' y '`j`'.
- **Para seleccionar una celda en modo edición**: haz clic con el ratón en la caja de texto de la celda.
- **Para seleccionar varias celdas contiguas en modo comandos**: utiliza las teclas '`mayus + cursor`' o '`mayus + k`' y '`mayus + j`' o haz clic en el ratón en la primera celda, pulsa la tecla '`mayus`' y haz clic en la última celda.

Añadir una celda al notebook

Selecciona una celda y haz clic en el icono ⊕ de la barra de herramientas del notebook. Se creará una nueva celda de tipo **código** justo debajo de la celda elegida.

Para controlar el lugar donde se insertará la celda:

- **Para crear una celda encima de la celda seleccionada**: en modo comandos pulsa la tecla '`A`' o haz clic en el icono  .
- **Para crear una celda debajo de la celda seleccionada**: en modo comandos pulsa la tecla '`B`' o haz clic en el icono  .

Cambiar el tipo de una celda del notebook

Selecciona una o varias celdas y haz clic en el desplegable de la barra de herramientas del notebook.

Para cambiar el tipo de celda con el teclado sitúate en la celda en modo comando y presiona las teclas siguientes:

- Para convertir la celda a tipo código: '`Y`'.
- Para convertir la celda a tipo Markdown: '`M`'.

Borrar una celda del notebook

Sitúate con los cursores en el modo comando sobre la celda a borrar y presiona dos veces seguidas la tecla '`d`'. La celda se borrará junto a los resultados de su ejecución si los hubiera.

También puedes borrar una celda haciendo clic en el icono  de la celda.

Ejecutar una celda del notebook

Selecciona una celda y haz clic en el icono  de la barra de herramientas del notebook. La celda se ejecutará y mostrará los resultados.

Otras formas de ejecución con el teclado son:

- **Para ejecutar una celda con el teclado**: selecciónala y presiona '`ctrl + enter`'.
- **Para ejecutar una celda con el teclado y posicionar el cursor en la siguiente celda**: presiona '`mayus + enter`'. De esta forma se pueden ejecutar de forma individual una serie de celdas contiguas sin necesidad de seleccionarlas de forma independiente.
- **Para ejecutar una celda con el teclado e insertar una celda vacía inmediatamente a continuación:** presiona '`alt + enter`'. Esta forma de ejecución permite encadenar ediciones de celdas y ejecuciones sin necesidad de crear explícitamente una celda para poder escribir el nuevo código a ejecutar.

Ejecutar todas las celdas del notebook

Haz clic en el icono de la barra de herramientas del notebook. El notebook presentara el resultado de cada celda debajo de la misma. El código de las celdas no se ocultará.

Ejecutar todas las celdas del notebook en modo presentación

Haz clic en el icono de la barra de herramientas del notebook. El notebook pasará a modo presentación ocultando las secciones de código.

Ordenar las celdas del notebook

- Selecciona la celda y haz clic en los iconos y de la barra de herramientas.
- Haz clic en los iconos y de la celda.
- Haz clic en el número de secuencia de la celda que quieres mover y arrástrala hasta su nueva posición.

Salvar un notebook

- Haz clic en el icono de la barra de herramientas del notebook.
- En modo comandos presiona '`ctrl + s`'.

Detener y reiniciar la ejecución del kernel

En los casos en los que se quiera limpiar la sesión generada por la ejecución de celdas, o si el kernel ha entrado en un bucle infinito es recomendable reiniciar el kernel.

- **Para reiniciar el kernel**: haz clic en el icono dela barra de herramientas del notebook.
- **Para interrumpir el kernel en modo comandos**: presiona las teclas 'i'y'i'.
- **Para reiniciar el kernel en modo comandos**: presiona las teclas '0'y'0'.

Copiar, cortar y pegar celdas

- **Para copiar una o más celdas con la barra de herramientas**: selecciónalas y haz clic en el botón .
- **Para copiar una o más celdas con el teclado:** selecciónalas en modo comandos y presiona la tecla 'c'.
- **Para cortar una o más celdas con la barra de herramientas**: selecciónalas y haz clic en el botón .
- **Para cortar una o más celdas con el teclado**: selecciónalas en modo comandos y presiona la tecla 'x'.
- **Para pegar una o más celdas debajo de una celda ya existente con la barra de herramientas**: selecciona la celda y haz clic en el botón .
- **Para pegar una o más celdas encima de una celda ya existente con el teclado**: selecciónala en modo comandos y presiona las teclas 'mayus + v'.
- **Para pegar una o más celdas debajo de una celda ya existente con el teclado**: selecciónala en modo comandos y presiona la tecla 'v'.
- **Para duplicar una celda**: haz clic en el icono de la celda y una copia se añadiá inmediatamente debajo de ella.

Fusionar el contenido de dos celdas

- Para fusionar el contenido de dos celdas contiguas del mismo tipo en modo comandos presiona las teclas 'mayus + m'.

Completar código y ayuda

- **Para completar una sentencia parcialmente introducida:** presiona la tecla 'tabulador'.
- **Para mostrar la ayuda de una función**: presiona las teclas 'mayus + tabulador'.

Movimiento del cursor dentro de una celda

- **Para ir al comienzo de una celda**: presiona las teclas 'ctrl + inicio'.
- **Para ir al final de una celda**: presiona las teclas 'ctrl + fin'.
- **Para posicionar el curso en la palabra siguiente**: presiona las teclas 'ctrl + cursor derecho'.
- **Para posicionar el curso en la palabra anterior**: presiona las teclas 'ctrl + cursor izquierdo'.

Otras operaciones

- **Para ocultar el código con el teclado en modo comandos**: presiona la tecla 'O'.
- **Para ocultar el código con la barra de herramientas**: haz clic en el icono  .
- **Para mostrar u ocultar números de línea dentro de las celdas**: en modo comandos presiona la letra 'l'.
- **Para mostrar una ventana de ayuda de atajos de teclado**: en modo comandos presiona la tecla 'h'.
- **Para unir el contenido de dos celdas del mismo tipo contiguas**: en modo comandos presiona las teclas 'mayus + m'.

Librerías disponibles en los notebooks

A continuación se incluye un listado de todas las librerías de terceros disponibles para el analista en los notebooks de Cytomic Orion agrupadas por tipo, junto a una breve descripción y recursos de ayuda para poder utilizarlas.

Adicionalmente a las librerías de terceros, Cytomic Orion pone a disposición de todos sus clientes varias librerías que ayudan a automatizar los análisis y mostrar sus resultados de forma gráfica. Para obtener una descripción completa de las APIs definidas en la librerías sus objetos, métodos y enumeraciones de datos consulta los enlaces siguientes:

- **Librería de threat hunting**: consulta el enlace **https://info.cytomicmodel.com/resources/help/ORION/es/threathuntingAPI/index.html**
- **Librería de widgets**: consulta el enlace **https://info.cytomicmodel.com/resources/help/ORION/es/Notebooklib/index.html**

Bases de datos

Nombre	Descripción
Psycopg	Librería de acceso a bases de datos PostgreSQL. Implementa al completo las especificaciones de Python DB API 2.0 **http://initd.org/psycopg/docs/**
Pyodbc	Librería ODBC de acceso a bases de datos. Compatible con Microsoft SQL Server, MySQL y Oracle entre otras. **https://github.com/mkleehammer/pyodbc/wiki**
maxminddb	Accede a ficheros de tipo MaxMind DB, un formato binario para almacenar datos indexados por subredes IP (IPv4 o IPv6).

Nombre	Descripción
	https://pypi.org/project/maxminddb/

Tabla 13.2: Librerías disponibles de bases de datos

Gráficos

Nombre	Descripción
branca	Librería gráfica. https://python-visualization.github.io/branca/
folium	Librería gráfica para manipular mapas interactivos de tipo leaflet. https://python-visualization.github.io/folium/
Graphviz	Librería de visualización gráfica para representar información de estructura, tal como diagramas de gráficos y redes abstractas. https://graphviz.readthedocs.io/en/stable/
Iplotter	Generación de gráficos interactivos. https://github.com/niloch/iplotter
ipywidgets	Utiliza controles Python para construir una GUI que facilita la interacción con el usuario. https://ipywidgets.readthedocs.io/en/stable/
matplotlib	Biblioteca de trazado 2D que produce gráficas de alta calidad: histogramas, gráficos de barras, diagramas de dispersión, etc. https://matplotlib.org/users/index.html
networkx	Crea y manipula gráficas de redes complejas para ayudar al estudio de su estructura, dinámica y funciones. https://networkx.github.io/documentation/networkx-2.3/
pivottablejs	Implementación de gráficos de tipo Pivot Table (Pivot Grid, Pivot Chart, Cross-Tab) con funcionalidad de arrastrar y soltar. https://pypi.org/project/pivottablejs/

Nombre	Descripción
pydot	Interface para el lenguaje DOT usado por `Graphviz`. **https://github.com/pydot/pydot**
pygal	Librería para generar gráficos de barras, tarta, líneas, radar etc. **http://pygal.org/en/stable/documentation/index.html**
seaborn	Biblioteca de visualización de datos basada en `mathplotlib`. Proporciona una interfaz de alto nivel para dibujar gráficos estadísticos atractivos e informativos. **https://seaborn.pydata.org/**
widgetsnbextension	Widgets HTML interactivos. **https://pypi.org/project/widgetsnbextension/**
basemap	Biblioteca para crear mapas en 2D. Orientado a cubrir las necesidades de oceanógrafos y meteorólogos. **https://matplotlib.org/basemap/**
igraph	Colección de herramientas de análisis de red con énfasis en la eficiencia, la portabilidad y la facilidad de uso.
cufflinks	Librería que facilita la generación de gráficos desde un Dataframe Pandas. **https://plot.ly/ipython-notebooks/cufflinks/**

Tabla 13.3: Librerías disponibles para manipulación de gráficos

Python y otros

Nombre	Descripción
future	Compatibilidad con versiones de Python futuras.
PyJWT	Codifica y decodifica JSON Web Tokens (JWT) **https://pyjwt.readthedocs.io/en/latest/**
pyparsing	Construye gramáticas para generar intérpretes.

Nombre	Descripción
	https://github.com/pyparsing/pyparsing
pytz	Operaciones con zonas horarias. **http://pytz.sourceforge.net/**
selenium	Automatización de navegadores web. Automatiza aplicaciones web para pruebas, tareas repetitivas de administración etc. **https://www.seleniumhq.org/docs/**
plotly	Creación de aplicaciones web analíticas. Construye aplicaciones de visualización de datos con interface de usuario. **https://dash.plot.ly/**
pixiedust	Complemento de los notebooks Jupyter para mejorar la experiencia del usuario al trabajar con datos. **https://pixiedust.github.io/pixiedust/**
cyjupyter	Widget para visualizar diagramas de tipo red. **https://github.com/cytoscape/cytoscape-jupyter-widget**
pillow	API para la generación de imágenes bitmap basado en PIL.
cairosvg	Conversor de ficheros VG en PDF y PNG. **https://cairosvg.org/documentation/**
tqdm	Control de barra de progreso. **https://tqdm.github.io/**

Tabla 13.4: Librerías disponibles que extienden las capacidades de Python

Datos

Nombre	Descripción
geoIP2	API de acceso al servicio geoIP2, utilizado para obtener datos geográficos a partir de una dirección IP. **https://geoip2.readthedocs.io/en/latest/**

Nombre	Descripción
ipaddr	Inspecciona y manipula direcciones IP. **https://docs.python.org/3/howto/ipaddress.html**
kiwisolver	Conjunto de herramientas para resolver de manera eficiente sistemas de igualdades y desigualdades lineales con restricciones incrementales. Las restricciones pueden ser requisitos o preferencias. Éstas se especifican inicialmente y el resolvedor las actualiza para que tengan valores que satisfagan las restricciones. **https://github.com/google/kiwi-solver**
numpy	Paquete fundamental para computación científica. Permite la manipulación de matrices, álgebra lineal, transformadas de Fourier y generación de números aleatorios, entre otros. **https://docs.scipy.org/**
pandas	Biblioteca que proporciona acceso a estructuras de datos de alto rendimiento y fáciles de usar y herramientas de análisis de datos. Pretende ser el bloque de construcción fundamental de alto nivel para realizar análisis prácticos de datos del mundo real. **http://pandas.pydata.org/pandas-docs/stable/getting_started/overview.html**
pefile	Analiza y trabaja con archivos Portable Executable (PE). Accede a la mayor parte de la información contenida en los encabezados del PE, así como los detalles de todas las secciones y sus datos. **https://github.com/erocarrera/pefile**
pip-date	Conjunto de herramientas de línea de comandos ligero para mostrar los tiempos de instalación o modificación de todos sus paquetes pip.
sciPy	Software para cálculos matemáticos, científicos y de ingeniería. **https://docs.scipy.org/doc/scipy/reference/**
qgrid	Espacio de trabajo interactivo para ordenar, filtrar y editar DataFrames. **https://qgrid.readthedocs.io/en/latest/**
statsmodels	Estimación de modelos estadísticos y realización de pruebas estadísticas y

Nombre	Descripción
	exploración de datos. **https://www.statsmodels.org/stable/index.html**
scikit-learn	Herramientas para el minado de datos, análisis y machine learning. **https://scikit-learn.org/stable/documentation.html**

Tabla 13.5: Librerías disponibles para la manipulación de datos

Capítulo 14

Investigación en la infraestructura IT con OSQuery

OSQuery es un framework que recoge y organiza toda la información de la infraestructura de los clientes del SOC, y la pone a disposición del analista a través de un modelo de datos relacional.

El analista diseñará sentencias SQL para obtener información relativa al hardware, software, procesos en ejecución, sistema de ficheros, registro etc. de los equipos, que podrá utilizar en sus investigaciones o como parte del procedimiento de respuesta ante un incidente.

*Contacta con tu comercial asignado para activar la funcionalidad de OSQuery en los equipos que cumplan con los requisitos indicados en **Requisitos de OSQuery**.*

CONTENIDO DEL CAPÍTULO

Introducción a OSQuery

OSQuery es un conjunto de librerías que recopilan información del sistema operativo del equipo y la almacenan en una base de datos relacional, permitiendo al analista su exploración de forma flexible mediante consultas SQL. Las tablas representan los diferentes conceptos que forman un

sistema operativo, como pueden ser procesos en ejecución, módulos de kernel cargados, conexiones de red abiertas, complementos de navegador instalados, eventos de hardware o hashes de archivos.

Para construir consultas SQL compatibles con OSQuery es necesario conocer su esquema de datos. Consulta la documentación accesible en **https://osquery.io/schema/4.2.0/** para obtener la relación de tablas y campos utilizados para organizar la información recogida del equipo investigado.

Integración de OSQuery con Cytomic Orion

Cytomic Orion utiliza principalmente los notebooks para ejecutar sentencias OSQuery, recoger los datos recibidos y presentarlos de forma clara al analista. No se requiere desarrollar un notebook desde 0, en su lugar el analista tiene acceso a una plantilla que recoge los parámetros necesarios, envía las sentencias a los equipos implicados y recopila los resultados. Consulta **Acceso a OSQuery** para acceder a la funcionalidad y **Resultados de una sentencia OSQuery** para obtener información sobre la presentación de los datos recogidos.

Adicionalmente, esta funcionalidad también está disponible a través de la API de integración. Consulta **API de acceso a OSQuery** en la página **356**.

Requisitos de OSQuery

- Cytomic EPDR o Cytomic EDR versión 3.71 o superior instalado en los equipos de los que se quiere recuperar información de infraestructura.
- Sistema operativo Windows.
- Envío de sentencias compatibles con OSQuery versión 4.02.00.

Casos de uso para el analista

Para mostrar las capacidades de OSQuery y ayudar a ubicar esta funcionalidad en el proceso de análisis y respuesta ante incidentes, se plantean los siguientes casos de uso:

- Delimitar el alcance de un ataque.
- Encontrar los procesos que escuchan en un puerto.
- Encontrar procesos en ejecución cuyo fichero ha sido eliminado.

Delimitar el alcance de un ataque

Cuando se ha detectado la ejecución de un proceso malicioso en la fase de respuesta a un incidente, el analista puede querer comprobar si se está ejecutando en otros equipos de la red. Para delimitar el alcance del ataque puede lanzar una consulta utilizando el nombre del proceso, o incluso el nombre de un archivo que haya abierto. De esta forma sabrá qué equipos se encuentran comprometidos.

```
SELECT processes.pid FROM processes WHERE
processes.name='string'

SELECT process_open_files.pid FROM process_open_files WHERE
process_open_files.path LIKE '%string%'
```

Encontrar los procesos que escuchan en un puerto

Muchos procesos maliciosos reciben comandos de un servidor central C&C. Una labor habitual del analista es detectar procesos nuevos que escuchan en puertos poco comunes. Esto se puede realizar obteniendo todos los sockets abiertos de cada equipo y comparando la lista con una anterior para detectar las diferencias.

```
SELECT listening_ports.pid,listening_ports.port,listening_
ports.address, processes.name, processes.path FROM
listening_ports INNER JOIN processes ON processes.pid =
listening_ports.pid
```

Encontrar procesos en ejecución cuyo fichero ha sido eliminado

Con frecuencia, los atacantes dejan un proceso malicioso en ejecución pero eliminan el fichero original del disco duro. Esta situación anómala podría ser un indicador de un proceso sospechoso.

```
SELECT processes.name, processes.path, processes.pid FROM
processes WHERE on_disk = 0
```

Acceso a OSQuery

Para recuperar información de la infraestructura IT es necesario enviar a la plataforma sentencias SQL desde uno de los siguientes puntos de la consola:

- Desde el subpanel **Indicios** de una investigación:
  - Haz clic en el menú superior **Investigaciones** y abre una investigación de la lista.
  - Selecciona uno o varios indicios y haz clic en la opción **Consulta OSQuery** de la barra de herramientas, o haz clic en el icono del menú de contexto asociado a un indicio y selecciona **Consulta OSQuery**.
  - En este caso, el campo **Equipos** de la ventana **Nueva consulta OSQuery** se rellenará con los MUIDs de los equipos seleccionados de forma automática.
- Desde la barra de pestañas de una **Investigación**:
  - Haz clic en el menú superior **Investigaciones** y abre una investigación de la lista.
  - Haz clic en el icono + de la barra de pestañas y selecciona **Consulta OSQuery**.
- Desde el subpanel **Archivos** de una investigación:
  - Haz clic en el menú superior **Investigaciones** y abre una investigación de la lista.
  - Haz clic en el icono + del subpanel **Archivos** y selecciona **Consulta OSQuery**.

Independientemente de la opción elegida, se mostrará la ventana **Nueva consulta OSQuery**. Consulta **Enviar consultas OSQuery**.

Adicionalmente también es posible acceder a la funcionalidad de OSQuery a través de la API de integración de Cytomic Orion. Consulta **API de acceso a OSQuery** en la página **356**para obtener más información sobre el manejo de la API y sobre los métodos específicos de OSQuery.

Enviar consultas OSQuery

La ventana **Nueva consulta OSQuery** consta de los siguientes campos:

- **Nombre del notebook**: los datos recogidos de la infraestructura del cliente se presentarán en un notebook con el nombre especificado en este campo.
- **Descripción**: descripción del tipo de datos obtenidos con la sentencia OSQuery y otra información que quiera añadir el analista.
- **Equipos**: lo datos se obtendrán de los equipos especificados:
  - **Todos los equipos de los siguientes clientes**: indica los nombres o identificadores de los clientes mediante el icono ⊕ cuyos equipos recibirán la sentencia OSQuery. No permite especificar equipos individuales.
  - **Los siguientes equipos**: indica los identificadores (MUIDs) de los equipos mediante el icono ⊕ que recibirán la sentencia OSQuery. Se pueden añadir equipos pertenecientes a diferentes clientes.
- **Tiempo máximo de espera**: las peticiones OSQuery pueden involucrar a equipos apagados por lo que no será posible obtener de ellos la información solicitada. Cytomic Orion intentará recuperar la información durante el intervalo indicado en el campo **Tiempo máximo de espera**, transcurrido el cual todas las peticiones serán canceladas y el proceso se dará por finalizado.
- **Consulta**: sentencia SQL en formato OSQuery. Consulta **https://osquery.io/schema/4.2.0/** para más información sobre el esquema de datos.

Resultados de una sentencia OSQuery

Los resultados de la ejecución de una sentencia OSQuery se presentan en un notebook de formato cerrado, que se muestra a continuación:

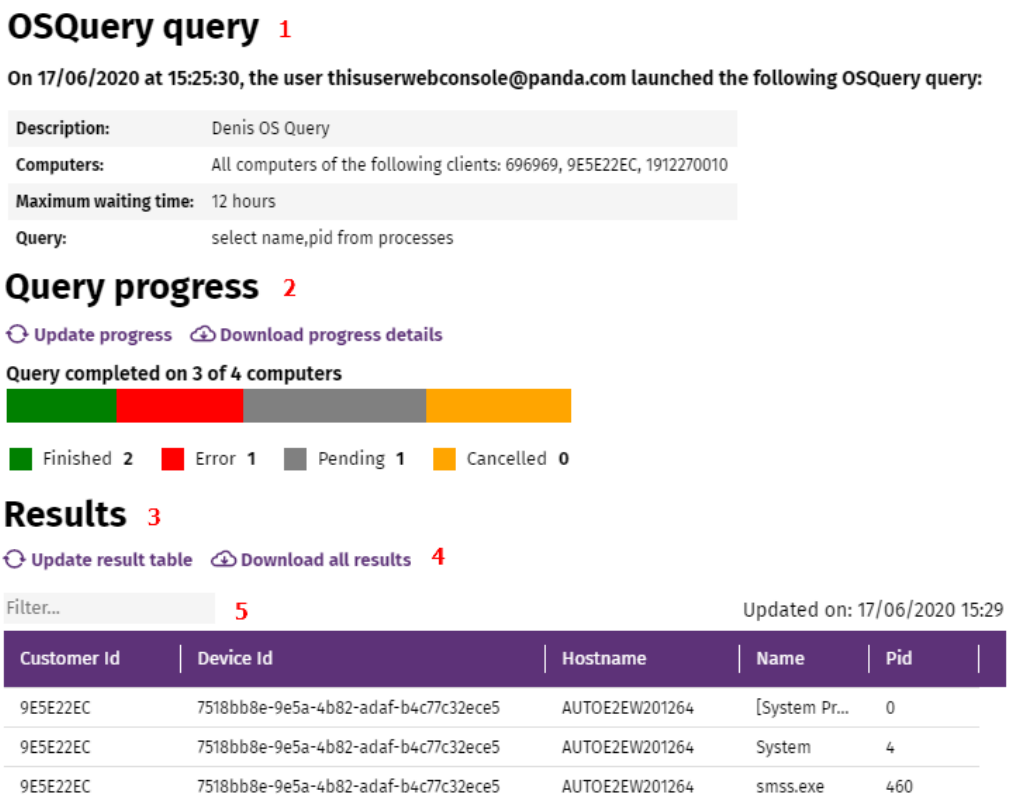


Figura 14.1: Notebook con los resultados de una sentencia OSQuery

> *Consulta **Investigación con notebooks** en la página **220** para obtener más información sobre cómo gestionar y utilizar notebooks en Cytomic Orion.*

- **Información del notebook (1)**: contiene los datos suministrados por el analista en el momento en que se creó la sentencia OSQuery: nombre de la sentencia, descripción, duración, ámbito de ejecución y la propia sentencia en lenguaje SQL.
- **Información de progreso (2)**: contiene varias series de datos indicando el número de equipos que completaron con éxito la operación:
  - **Finished**: número de equipos que completaron con éxito la operación y enviaron datos.
  - **Error**: número de equipos que devolvieron un error.
  - **Pending**: número de equipos que todavía no han devuelto información.
  - **Cancelled**: número de equipos que no devolvieron datos después de que haya pasado el tiempo especificado en el campo **Tiempo máximo de espera**.
- **Resultados de la sentencia OSQuery (3)**: contiene una tabla con los datos devueltos por la sentencia OSQuery y herramientas de filtrado y descarga de la información.

- **Controles para la descarga de datos (4)**: descarga dos ficheros con la información separada por comas, uno con los datos reportados por los equipos y otro con la información de estado de la petición.
- **Filtro (5)**: muestra las filas de la tabla de datos que coincidan con el criterio establecido. Admite búsquedas parciales en todos los campos de la tabla.
- **Tabla de datos (6)**: contiene una tabla con los campos solicitados por el analista en la sentencia OSQuery. El número máximo de registros mostrados es de 10.000, una vez superado se mostrará un mensaje de advertencia y se invitará al analista a su descarga **(4)**. En todas las tablas de resultados se incluyen tres campos adicionales:
  - **Customer id**: es el identificador del cliente al que pertenece la información del registro.
  - **Device Id**: es el identificador del equipo utilizado en Cytomic EDR y Cytomic EPDR al que pertenece la información del registro.
  - **Hostname**: nombre del equipo al que pertenece la información del registro.

Ejecución de sentencias en segundo plano y el modo presentación

*Consulta **Persistencia del modo presentación** en la página **228** para obtener más información sobre este modo de ejecución de los notebooks.*

Debido a que las peticiones OSQuery se pueden alargar mucho en el tiempo si el campo **Tiempo máximo de espera** tiene un valor alto y los equipos afectados tardan en ser accesibles, es posible que el analista cierre el notebook antes de que la petición se haya completado. No obstante, debido a que las librerías OSQuery trabajan en segundo plano, la sentencia seguirá su curso aunque el notebook haya sido cerrado. Gracias al modo presentación, al abrir de nuevo el notebook éste mostrará los resultados recogidos justo antes de su cierre, pero no la información recogida desde el momento en que se cerró hasta su reapertura. Para actualizar la información haz clic en la opción **Update results table** o **Update progress** del notebook, o en el icono  de la barra de herramientas para actualizar el notebook completo.

Capítulo 15

Herramientas de respuesta

Una vez que el analista ha detectado actividad sospechosa en la estación de trabajo o servidor de la empresa, es necesario contar con herramientas para que el equipo de respuesta a incidentes pueda cerrar la posible brecha de seguridad, devolver el equipo a su estado anterior y recoger todas las evidencias requeridas para realizar un análisis posterior más exhaustivo.

Cytomic Orion incluye un completo conjunto de herramientas que ayudarán a ejecutar las tareas de resolución de forma remota y desde la misma consola que maneja el analista de seguridad.

CONTENIDO DEL CAPÍTULO

Requisitos

Para utilizar las herramientas de acceso remoto y de linea de comandos es necesario que tanto el equipo del usuario como el cortafuegos perimetral de la red del cliente permitan el trafico desde y hacia las URLs siguientes:

- dir.rc.pandasecurity.com por el puerto 443.
- eu01.rc.pandasecurity.com por los puertos 8080 y 443.
- eu02.rc.pandasecurity.com por los puertos 8080 y 443.
- eu03.rc.pandasecurity.com por los puertos 8080 y 443.
- eu04.rc.pandasecurity.com por los puertos 8080 y 443.
- eu05.rc.pandasecurity.com por los puertos 8080 y 443.
- eu06.rc.pandasecurity.com por los puertos 8080 y 443.
- ams01.rc.pandasecurity.com por los puertos 8080 y 443.
- ams02.rc.pandasecurity.com por los puertos 8080 y 443.

Acceso a las herramientas de respuesta

Herramientas disponibles en Cytomic Orion

Herramientas de gestión remota

- **Aislar equipos**: limita el tráfico de red que envía o recibe el equipo para evitar la propagación de amenazas y la extracción de datos confidenciales.
- **Reiniciar equipos**: fuerza la secuencia de reinicio del equipo.

Herramientas de acceso remoto

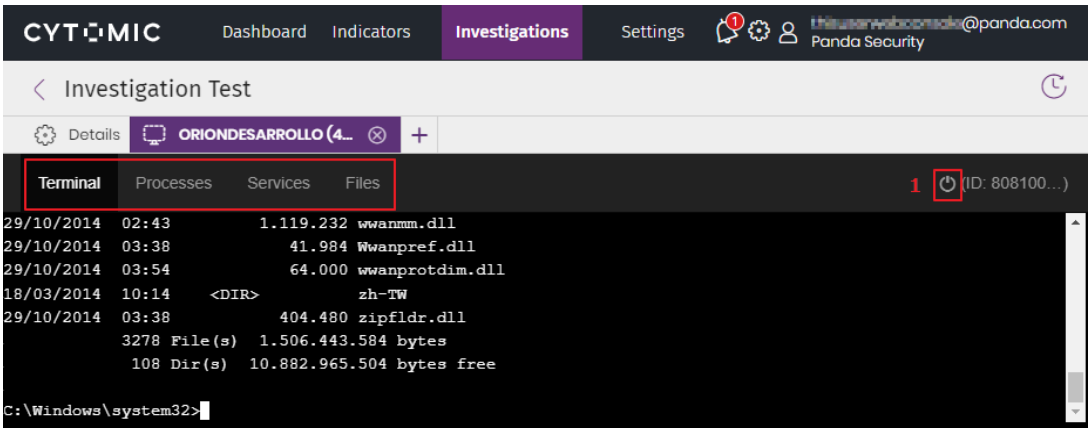


Figura 15.1: Menú general de acceso a las herramientas de acceso remoto al equipo

- **Línea de comandos remota**: shell remota con permisos de administrador que permite ejecutar operaciones sobre el sistema de ficheros y lanzar programas en el equipo.
- **Gestor de procesos**: muestra un listado con los procesos en ejecución y permite su parada.

- **Gestor de servicios**: muestra un listado con los servicios instalados en el equipo y permite su arranque y parada.
- **Transferencia de ficheros**: envío y recepción de ficheros desde / hacia el equipo.
- **Herramientas de línea de comandos**: conjunto de programas accesibles desde la línea de comandos remota orientados a recoger información para profundizar en la investigación del analista, recuperar datos para realizar análisis forense y resolver las brechas de seguridad:
    - **delete**: borra ficheros en todo el disco duro del equipo.
    - **dump**: vuelca en disco la memoria asignada a procesos.
    - **netinfo**: muestra la información de las interfaces de red.
    - **pcap**: captura paquetes de red y los vuelca al disco duro del equipo.
    - **ports**: muestra los procesos que tienen puertos abiertos en el equipo.
    - **process**: muestra los procesos cargados en memoria y sus módulos.
    - **url**: muestra un listado histórico con todas las URLs accedidas desde el navegador instalado en el equipo.

Acceso a las herramientas de respuesta

Todas las herramientas de resolución incorporadas en Cytomic Orion son accesibles desde las entidades de interés asociadas a una investigación (para obtener más información consulta **Panel Entidades de interés** en la página **116**). Para lanzar una herramienta de respuesta sigue los pasos mostrados a continuación:

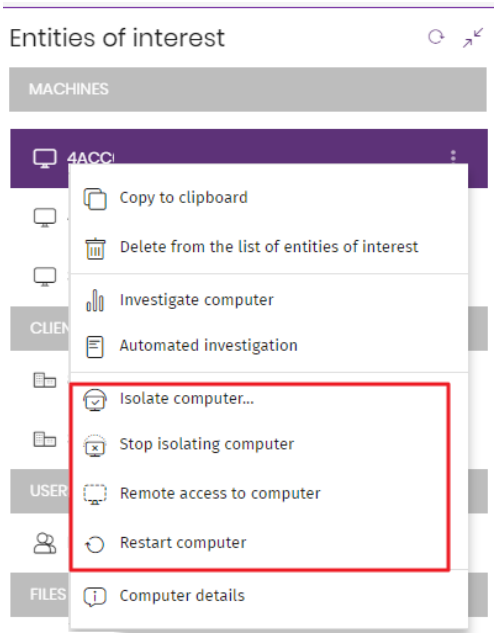


Figura 15.2: Acceso a las herramientas de respuesta desde el subpanel Entidades de interés

Para lanzar una herramienta de respuesta sigue los pasos mostrados a continuación:

- En el menú superior **Investigaciones** haz clic en la investigación donde se descubrió el equipo objeto de estudio.
- En el subpanel **Entidades de interés** localiza la entidad de tipo **Equipo** a la que quieres conectarte para resolver el incidente.
- En el menú de contexto de la entidad elige las opciones **Aislar equipo**, **Dejar de aislar equipo**, **Reiniciar equipo** y **Acceso remoto al equipo**. Se mostrará una ventana pidiendo confirmación.
- Haz clic en el botón **Si**. Se mostrará una pantalla de conexión y finalmente, la consola del analista presentará las utilidades de respuesta disponibles (Gestión de procesos, Gestor de servicios y Transferencia de ficheros) y la línea de comandos conectada al equipo remoto. (Ver Figura **Menú general de acceso a las herramientas de acceso remoto al equipo**).
- Para acceder a las utilidades de respuesta ejecuta el comando `rt` desde la línea de comandos. Se mostrará un menú que te indicará las acciones disponibles y los parámetros a utilizar.
- Para cerrar la conexión con el equipo remoto haz clic en el icono situado en la parte superior derecha de la ventana de conexión (**1** en la Figura **Menú general de acceso a las herramientas de acceso remoto al equipo**).

Descripción de las herramientas de respuesta

Aislar equipos

Cytomic Orion aísla bajo demanda los equipos de la red para evitar la propagación de las amenazas y la comunicación y extracción de información confidencial.

Cuando un equipo está aislado, sus comunicaciones quedan restringidas a los servicios mostrados a continuación:

- El acceso al equipo desde la consola de análisis para que el equipo de respuesta a incidentes pueda solucionar el problema mediante las herramientas suministradas por Cytomic Orion.
- Las comunicaciones necesarias para el buen funcionamiento del producto de seguridad Cytomic EDR y Cytomic EPDR.

El resto de productos y servicios instalados en el equipo de usuario o servidor dejarán de comunicarse por la red.

Para aislar un equipo haz clic en la opción **Aislar equipos** del menú de contexto asociado a la entidad de interés.

Estados de los equipos aislados

Las operaciones **Aislar un equipo** y **Dejar de Aislar un equipo** se ejecutan en tiempo real, pero el proceso puede retrasarse si el equipo no está conectado a Internet. Para reflejar su situación exacta, Cytomic Orion distingue los 4 estados a través de los iconos mostrados a continuación:

- **Aislando** : el analista lanzó una petición para aislar uno o más equipos y se está procesando.
- **Aislado** : el proceso de aislamiento se completó y el equipo tiene restringidas sus comunicaciones.
- **Dejando de aislar**: el analista lanzó una petición para dejar de aislar uno o más equipos y se está procesando.
- **No aislado** : el proceso para retirar el aislamiento del equipo se completó. Las comunicaciones se permiten acorde a la configuración definida en otros productos, o en el propio sistema operativo.

Estos iconos acompañan a los equipos mostrados en el subpanel **Entidades de interés** de la investigación.

Comunicaciones permitidas en un equipo aislado

Cytomic Orion deniega todas las comunicaciones en un equipo aislado excepto las necesarias para poder comunicarse con éste y utilizar las herramientas de respuesta. A continuación, se indican las comunicaciones permitidas y denegadas.

Procesos y servicios permitidos en un equipo aislado:

Procesos de sistema:

- Los servicios necesarios para formar parte de la red corporativa: obtención de IP por DHCP, ARP, nombre de equipo por WINS, DNS etc.

Procesos de Cytomic Orion:

- Comunicación con el gateway por defecto.
- Comunicación con la nube de Cytomic para el envío de la información generada en la monitorización de procesos y administración remota mediante la consola web.

Cytomic EDR:

- Comunicación con el gateway por defecto.
- Comunicación con la nube de Cytomic para el funcionamiento de los motores de protección, descarga de ficheros de firmas y administración remota mediante la consola web.

- Comunicación con la nube de Cytomic para el funcionamiento de los módulos compatibles con Cytomic EDR (Cytomic Patch, Cytomic Encryption, Cytomic Data Watch).
- Descubrimiento de equipos en equipos aislados con el rol de descubridor asignado.
- Servidor de ficheros en un equipo aislado con el rol de cache asignado.
- Proxy de conexiones en un equipo con el rol de proxy Cytomic asignado.

Comunicaciones bloqueadas en un equipo aislado

Todas las comunicaciones que no estén incluidas en el punto anterior son denegadas, entre ellas:

- Conexión con el servicio Windows Update del sistema operativo.

El módulo Cytomic Patch sí permanecerá operativo en un equipo aislado.

- Navegación web, ftp, correo y otros protocolos de Internet.
- Transferencia de ficheros por SMB entre los PCs de la red.
- Instalación remota de equipos con Cytomic EDR.

Reiniciar equipos

Es posible que el equipo de respuesta a incidentes necesite reiniciar de forma manual el equipo remoto si se encuentra en alguno de los casos mostrados a continuación:

- Para reducir manualmente la superficie de exposición puede ser necesario realizar ciertas modificaciones en los equipos que requieren liberar mediante un reinicio los ficheros y procesos involucrados: al instalar parches del sistema operativo o de algunas aplicaciones en uso, al actualizar algunas herramientas críticas instaladas en el equipo tales como la solución de seguridad para mejorar sus capacidades de detección de amenazas, etc.
- En situaciones de mal funcionamiento del equipo.

Para reiniciar un equipo haz clic en la opción **Reiniciar equipos** del menú de contexto asociado a la entidad de interés.

Gestión de procesos

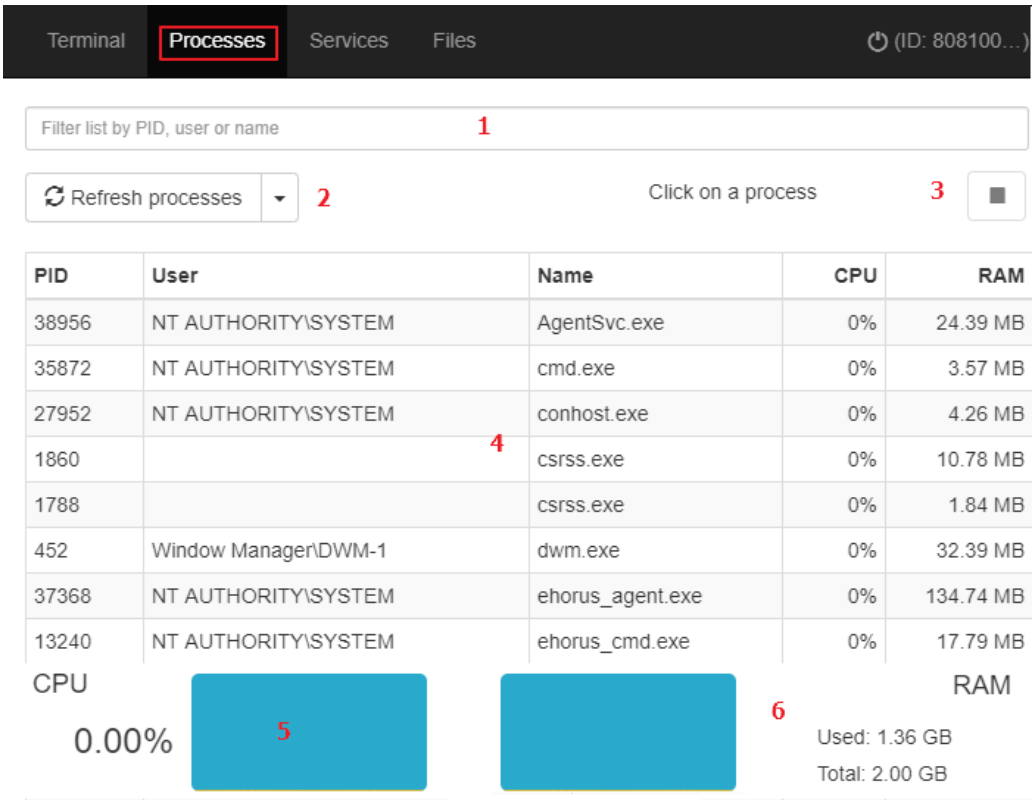


Figura 15.3: Herramienta de gestión de procesos

La herramienta de gestión de procesos muestra todos los procesos cargados en la memoria del equipo y permite localizar uno concreto y pararlo remotamente. Adicionalmente ofrece información sobre la memoria RAM consumida y CPU. Para ello cuenta con los elementos siguientes:

- **Herramienta de búsqueda (1)**: filtra el listado por el PID o por el nombre indicado. Permite búsquedas parciales.
- **Actualización automática del listado (2)**: define el intervalo que deberá transcurrir para que Cytomic Orion recargue la lista de procesos.
- **Botón de parada (3)**: detiene la ejecución del programa seleccionado.
- **Listado de procesos (4)**: muestra el listado de procesos cargados en la memoria del equipo.
- **CPU (5)**: indica el porcentaje de CPU utilizada por todos los procesos cargados en memoria y muestra un histórico en forma de diagrama de líneas con los consumos desde que se abrió la herramienta gestión de procesos.
- **Memoria (6)**: indica el porcentaje de memoria utilizada por todos los procesos cargados y muestra un histórico en forma de diagrama de líneas con los consumos desde que se abrió la herramienta gestión de procesos.

El listado de procesos **(4)** muestra información de cada proceso cargado en la memoria del equipo:

Campo	Descripción
PID	Identificador del proceso.
User	Cuenta de usuario que cargó el proceso.
Name	Nombre del proceso.
CPU	CPU consumida del proceso.
RAM	Memoria consumida por el proceso.

Tabla 15.1: Campos del listado Procesos

Gestión de servicios

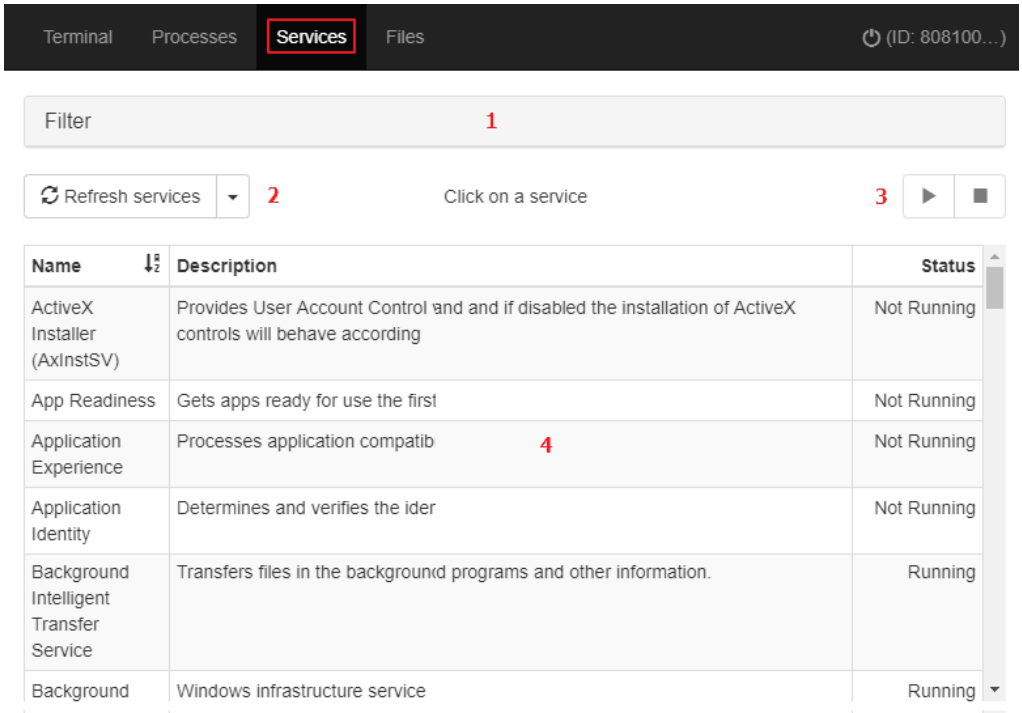


Figura 15.4: Herramienta de gestión de servicios

La herramienta de gestión de servicios muestra todos los servicios configurados en el equipo, permite localizar uno concreto y modificar su estado. Para ello cuenta con los elementos siguientes:

- **Herramienta de búsqueda (1)**: filtra el listado por el nombre o descripción indicado. Permite búsquedas parciales mediante subcadenas.
- **Actualización automática del listado (2)**: define el intervalo que deberá transcurrir para que Cytomic Orion actualice la lista de servicios.
- **Botón de inicio y parada de servicio (3)**: detiene o inicia la ejecución del servicio seleccionado.
- **Listado de servicios (4)**: muestra el listado de servicios cargados en la memoria del equipo.

El listado de servicios **(4)** muestra información de cada servicio configurado en el equipo:

Campo	Descripción
Nombre	Identificador del servicio.
Descripción	Descripción del servicio.
Status	Estado del servicio: • **Running**: servicio en ejecución. • **Not running**: servicio detenido.

Tabla 15.2: Campos del listado Servicios

Transferencia de ficheros

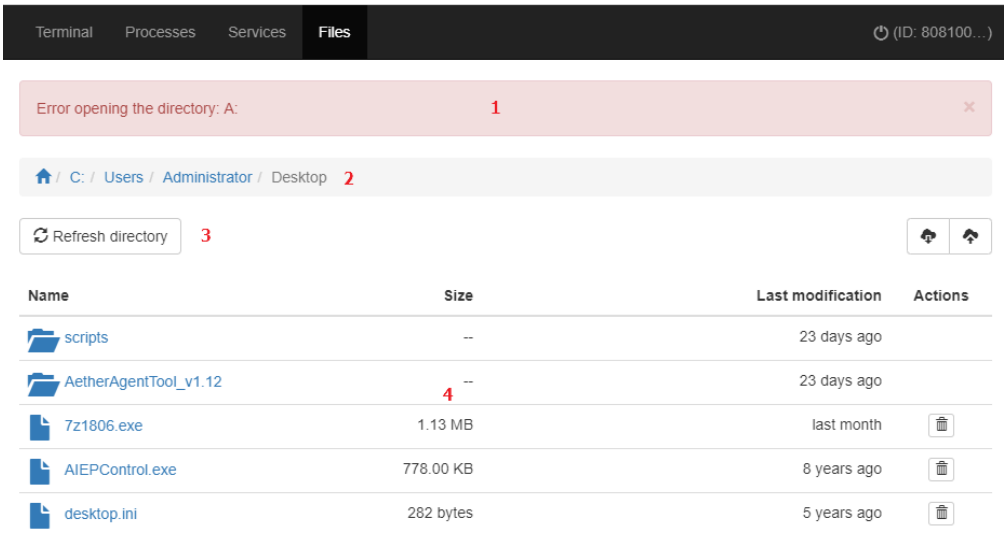


Figura 15.5: Herramienta de gestión de ficheros

La herramienta de gestión de ficheros permite transferir ficheros en las dos direcciones desde el equipo del analista al equipo remoto. Además permite navegar por el sistema de ficheros del equipo remoto y borrar archivos. Para ello cuenta con los elementos siguientes:

- **Zona de mensajes (1)**: muestra los errores que se pueden producir al acceder al sistema de ficheros del equipo remoto.
- **Ruta de navegación (2)**: muestra la ruta del sistema de ficheros que se visualiza en la zona de listado y permite cambiar de directorio de forma rápida haciendo clic en una carpeta o mostrar el listado de dispositivos conectados al equipo con el icono .
- **Actualización automática del listado (3)**: permite definir el intervalo que deberá transcurrir para que Cytomic Orion actualice la lista de ficheros.
- **Listado de ficheros (4)**: muestra el listado de ficheros que contiene la ruta de navegación **(2)**.
- **Carpetas** : haz clic en una carpeta para mostrar los ficheros que contiene. Se actualizará la ruta de navegación **(2)** automáticamente.
- **Borrar**: borra el fichero seleccionado sin pasar por la papelera de reciclaje.

El listado de ficheros **(4)** muestra la información relativa de cada fichero configurado en el equipo:

Campo	Descripción
Name	Nombre del fichero.
Size	Tamaño del fichero.
Last modification	Fecha en la que se modificó por última vez el fichero.
Actions	Acciones a ejecutar sobre el fichero: • Borra el fichero.

Tabla 15.3: Campos del listado Ficheros

Linea de comandos remota

La línea de comandos remota permite ejecutar comandos compatibles con el intérprete `cmd.exe` y lanzar programas que tengan salida de texto. Se ejecuta bajo la cuenta LOCAL_SYSTEM del equipo remoto y se encuentra instalada en la siguiente ruta:

```
C:\Program Files (x86)\Panda Security\Panda Aether Agent\Remote access\
```

Herramientas de línea de comandos

Cytomic Orion incorpora el programa `rt.exe` que da acceso a un conjunto de utilidades para el equipo de respuesta a incidentes. Con estas herramientas el técnico podrá recuperar información

para realizar un análisis forense posterior, así como devolver al estado original el equipo afectado por la brecha de seguridad.

El programa `rt.exe` es accesible desde la línea de comandos remota y sigue la sintaxis indicada:

```
rt.exe [command] [-h|--help]
```

Las consideraciones indicadas a continuación afectan de forma general al comando `rt.exe`:

- `command` indica una acción a realizar. Cada una de ellas soporta distintos parámetros.
- No se soportan los caracteres comodín "*", "?".
- Algunos parámetros permiten búsquedas parciales por subcadenas al comienzo, final y en el interior de la cadena. Por ejemplo para filtrar la cadena "armario" se admiten las búsquedas por "ar", "mar" e "io".
- Si el comando soporta el volcado de la salida a un fichero, éste se especifica con `-f`.
- Para separar varios elementos del mismo tipo se usa el carácter " | ".

A continuación se incluyen los parámetros soportados por cada comando.

Comando "delete"

Borra los ficheros indicados con el parámetro `-n`, `-m` o `-s` que se encuentren en la ruta indicada por el parámetro `-p`. Si el fichero está en uso el comando `delete` devolverá un error.

Parámetro corto	Parámetro largo	Descripción	Anotaciones
-h	**--help**	Ayuda del comando.	
-f	**--force**	Borra los ficheros definitivamente sin pasar por la papelera de reciclaje.	
-r	**--restore**	En vez de borrar, recupera de la papelera de reciclaje los ficheros indicados.	Los ficheros se restauran a su localización original.
-p	**--path**	Ruta absoluta desde el directorio raíz a partir de la cual se buscarán los ficheros a borrar. Solo se borrarán los ficheros que pertenezcan a la ruta indicada.	• El carácter separador de carpetas es "\". • No se soportan caracteres

Parámetro corto	Parámetro largo	Descripción	Anotaciones
			comodín.
-n	**--name**	Nombre de los ficheros a borrar.	• Para indicar varios ficheros se utiliza el carácter " | ". • No se soportan caracteres comodín.
-m	**--md5**	md5 de los ficheros a borrar.	• Para indicar varios md5s se utiliza el carácter " | ". • No se soportan caracteres comodín.
-s	**--sha256**	sha256 de los ficheros a borrar.	• Para indicar varios sha256 se utiliza el carácter " | ". • No se soportan caracteres comodín.

Tabla 15.4: Parámetros del comando delete

Comando "dump"

Vuelca a disco el espacio de memoria asignado a un proceso de usuario o de sistema.

Parámetro corto	Parámetro largo	Descripción	Anotaciones
-h	**--help**	Ayuda del comando.	
-p	**--pid**	PID del proceso a volcar.	Consulta el **Comando "process"** para obtener el

Parámetro corto	Parámetro largo	Descripción	Anotaciones
			PID del proceso a volcar.
-s	**--system**	Volcado del kernel.	Valores admitidos: • **mini**: volcado corto con el contenido de la pila. • **kernel**: volcado completo. • **full**: volcado de toda la memoria física del equipo, aunque no esté en uso.
-f	**--filename**	Nombre del fichero donde se guardará el volcado.	
-z	**--zip**	El volcado se almacenará en un fichero comprimido en formato zip.	

Tabla 15.5: Parámetros del comando dump

Comando "netinfo"

Muestra la configuración de las interfaces de red instaladas en el equipo con el parámetro `-a`.

Parámetro corto	Parámetro largo	Descripción	Anotaciones
-h	**--help**	Ayuda del comando.	
-a	**--all**	Muestra por pantalla la configuración de las interfaces de red instaladas en el equipo.	
-f	**--filename**	Nombre del fichero donde se guardará la información.	

Parámetro corto	Parámetro largo	Descripción	Anotaciones
-z	**--zip**	El volcado se almacenará en un fichero comprimido en formato zip.	

Tabla 15.6: Parámetros del comando netinfo

Comando "pcap"

Captura el tráfico de red recibido y enviado desde el equipo. El inicio y finalización de la captura se indica mediante el parámetro `-a start| stop`. La captura de paquetes genera ficheros temporales en el equipo por lo que es necesario espacio suficiente en el disco duro. El resultado final es un fichero con formato pcap directamente utilizable por Wireshark.

Parámetro corto	Parámetro largo	Descripción	Anotaciones
-h	**--help**	Ayuda del comando.	
-a	**--action**	Ejecuta una acción: • **start**: inicia el proceso de captura. • **stop**: finaliza el proceso de captura. • **queryStatus**: muestra el estado del proceso de captura.	
-m	**--maxsize**	Tamaño máximo del paquete a capturar.	• Especificado en megabyes. • Valor por defecto: 200 Mbytes.
-i	**--maxtime**	Tiempo máximo de captura.	• Especificado en segundos. • Valor por defecto: 86400 segundos (1 día).

Parámetro corto	Parámetro largo	Descripción	Anotaciones
-f	**--filename**	Nombre del fichero donde se almacenará la información.	
-z	**--zip**	El volcado se almacenará en un fichero comprimido en formato zip.	

Tabla 15.7: Parámetros del comando pcap

Comando "ports"

Con el parámetro `-a` muestra los sockets abiertos en el equipo y los procesos que los abrieron.

Parámetro corto	Parámetro largo	Descripción	Anotaciones
-h	**--help**	Ayuda del comando.	
-a	**--all**	Muestra todos los puertos abiertos y su proceso asociado.	
-p	**--pid**	Filtra el resultado por el PID de un proceso.	
-n	**--name**	Filtra el resultado por el nombre de un proceso.	Soporta búsquedas parciales por subcadenas.
-f	**--filename**	Nombre del fichero donde se almacenará la información.	

Tabla 15.8: Parámetros del comando ports

Comando "process"

Con el parámetro `-a` muestra todos los procesos cargados en la memoria del equipo y sus módulos.

Parámetro corto	Parámetro largo	Descripción	Anotaciones
-h	**--help**	Ayuda del comando.	
-a	**--all**	Muestra todos los procesos cargados en la memoria del equipo y sus módulos.	
-p	**--pid**	Filtra el resultado por el PID de un proceso mostrando sus módulos.	
-u	**--user**	Muestra los procesos lanzados por un usuario y sus módulos.	
-f	**--filename**	Nombre del fichero donde se almacenará la información.	

Tabla 15.9: Parámetros del comando process

Comando "url"

Con el parámetro `-a any` muestra todas las URLs accedidas por los usuarios del equipo mediante el navegador Web instalado. Este comando requiere tener activado el módulo webfilter de Cytomic EDR.

Parámetro corto	Parámetro largo	Descripción	Anotaciones
-h	**--help**	Ayuda del comando.	
-a	**--action**	Filtra el listado de URLs según la acción ejecutada por el módulo Webfilter: • **allow**: muestra las URLs permitidas por el módulo Webfilter. • **deny**: muestra las URLs denegadas por el módulo Webfilter. • **any**: muestra todas las	

Parámetro corto	Parámetro largo	Descripción	Anotaciones
		URLs navegadas.	
-c	**--count**	Número máximo de URLs a mostrar.	Valor por defecto: sin límite.
-g	**--category**	Filtra el listado de URLs según la categoría asignada por el módulo Webfilter.	
-b	**--begindate**	Establece la fecha de inicio desde la que se mostrarán las URLs navegadas.	• **Formato de la fecha**: "`YYYY-MM-DD HH:MM`". • **Valor por defecto**: 30 días hacia atrás de la fecha de ejecución del comando.
-e	**--enddate**	Establece la fecha de finalización hasta la que se mostrarán las URLs navegadas.	• **Formato de la fecha**: "`YYYY-MM-DD HH:MM`". • **Valor por defecto**: fecha de ejecución del comando.
-n	**--urlpattern**	Filtra las URLs por subcadena.	
-u	**--userpattern**	Filtra las URLs por usuario.	
-f	**--filename**	Nombre del fichero donde se guardará la información.	
-z	**--zip**	El volcado se almacenará en un fichero comprimido en formato zip.	

Tabla 15.10: Parámetros del comando url

Capítulo 16

Sintaxis SQL del módulo Consultas avanzadas

Cytomic Orion implementa un dialecto SQL muy similar al utilizado en otros motores de bases de datos relacionales, tales como MySQL o Microsoft SQL Server, y empleado para construir sentencias en el módulo **Consultas avanzadas SQL**.

CONTENIDO DEL CAPÍTULO

Tipos de datos soportados

Esta sección describe los tipos de datos admitidos en Cytomic Orion y las consideraciones especiales al utilizarlos.

Enteros (INT y UINT)

Números enteros de tamaño fijo, con o sin signo.

Rango de enteros con signo

- Int8 - [-128 : 127]
- Int16 - [-32768 : 32767]
- Int32 - [-2147483648 : 2147483647]
- Int64 - [-9223372036854775808 : 9223372036854775807]

Rango de enteros sin signo

- UInt8 - [0 : 255]
- UInt16 - [0 : 65535]
- UInt32 - [0 : 4294967295]
- UInt64 - [0 : 18446744073709551615]

Decimales (DECIMALX)

Números de punto fijo que mantienen la precisión durante las operaciones de suma, resta y multiplicación. Para la división, los dígitos menos significativos se descartan (no se redondean).

Parámetros

- **P - Precisión**. Rango válido: [1: 38]. Determina cuántos dígitos decimales puede tener el número incluyendo la parte decimal.
- **S - escala**. Rango válido: [0: P]. Determina cuántos dígitos decimales puede tener la parte decimal.

Rangos de valores decimales

- Decimal32 (S) - (-1 * 10 ^ (9 - S), 1 * 10 ^ (9 - S))
- Decimal64 (S) - (-1 * 10 ^ (18 - S), 1 * 10 ^ (18 - S))
- Decimal128 (S) - (-1 * 10 ^ (38 - S), 1 * 10 ^ (38 - S))

Por ejemplo, Decimal32 (4) puede contener números desde -99999.9999 hasta 99999.9999 en incrementos de 0.0001.

Representación interna

Los datos internos se representan como enteros con signo con el número de bits apropiado. Los rangos de valores reales que se pueden almacenar en memoria son algo más grandes que los especificados anteriormente, los cuales verifican únicamente en operaciones de conversión desde una cadena.

Debido a que CPUs modernas no admiten los enteros de 128 bits de forma nativa, se emulan las operaciones en Decimal128. Debido a esto, Decimal128 funciona significativamente más lento que Decimal32 / Decimal64.

Operaciones y tipo de resultado

Las operaciones binarias en decimal dan como resultado un tipo de resultado más amplio (con cualquier orden de argumentos).

- Decimal64 (S1) Decimal32 (S2) -> Decimal64 (S)
- Decimal128 (S1) Decimal32 (S2) -> Decimal128 (S)
- Decimal128 (S1) Decimal64 (S2) -> Decimal128 (S)

Reglas para escalado:

- sumar, restar: S = max (S1, S2)
- Multiplicación: S = S1 + S2.
- dividir: S = S1.

Para operaciones similares entre decimal y enteros, el resultado es el decimal del mismo tamaño que el argumento.

Las operaciones entre Decimal y Float32 / Float64 no están definidas. Si realmente son necesarias puedes convertir explícitamente uno de los argumentos usando `toDecimal32, toDecimal64, toDecimal128 o toFloat32, toFloat64`. Ten en cuenta que el resultado perderá precisión y la conversión de tipos es una operación costosa.

Algunas funciones en Decimal devuelven el resultado como Float64 (por ejemplo, `var` o `stddev`). Los cálculos intermedios aún se pueden realizar en decimal, lo que puede llevar a resultados diferentes entre las entradas en coma flotante y decimal con los mismos valores.

Controles de desbordamiento

Durante los cálculos en decimal se pueden producir un desbordamiento de enteros. Los dígitos de más en la parte decimal se descartan (no se redondean). Los dígitos de más en la parte entera darán lugar a una excepción.

Los controles de desbordamiento provocan una ralentización en la ejecución de las operaciones. Las comprobaciones de desbordamiento no solo se producen en operaciones aritméticas sino también en la comparación de valores:

Booleanos (UINT8)

No hay un tipo independiente para valores booleanos, se utiliza el tipo UInt8 restringido a los valores 0 y 1.

Cadenas de caracteres (STRING)

String representa una cadena de caracteres de longitud arbitraria sin límite. El valor puede contener un conjunto arbitrario de bytes, incluidos bytes nulos. Este tipo de dato reemplaza los tipos VARCHAR, BLOB, CLOB y otros equivalentes de otros DBMS.

Codificaciones

Cytomic Orion no soporta el concepto de codificaciones. Las cadenas pueden contener un conjunto arbitrario de bytes, que se almacenan y reproducen tal cual. Si necesita almacenar textos, se recomendamos utilizar la codificación UTF-8. Dado que la consola de analisi soporta UTF-8 se pueden leer y escribir sus valores sin hacer conversiones. De manera similar, ciertas funciones para trabajar con cadenas tienen variaciones que funcionan bajo el supuesto de que la cadena contiene un conjunto de bytes que representan un texto codificado en UTF-8. Por ejemplo, la función `length` calcula la longitud de la cadena en bytes, mientras que la función `lengthUTF8`

calcula la longitud de la cadena en puntos de código Unicode, asumiendo que el valor está codificado en UTF-8.

Cadenas de caracteres fijas (FIXEDSTRING)

FixedString(N) es una cadena de longitud fija de N bytes (ni caracteres ni puntos de código).

Para declarar una columna del tipo FixedString usa la siguiente sintaxis:

```
<column_name> FixedString (N)
```

Donde `N` es un número natural.

El tipo FixedString es eficiente cuando los datos tienen una la longitud de exactamente `N` bytes. En todos los demás casos, es probable que el rendimiento caiga.

Ejemplos de los valores que se pueden almacenar de manera eficiente en columnas de tipo FixedString:

- Representación binaria de direcciones IP (FixedString (16) para IPv6).
- Códigos de idioma (ru_RU, en_US ...).
- Códigos de moneda (USD, RUB ...).
- Representación binaria de hashes (FixedString (16) para MD5, FixedString (32) para SHA256).

Para almacenar valores UUID, use el tipo de datos UUID.

Al insertar datos, Cytomic Orion ejecuta las siguientes tareas:

- Completa la cadena con bytes nulos si la cadena contiene menos de `N` bytes.
- Lanza la excepción `Too large value for FixedString(N)` si la cadena contiene más de `N` bytes.

Al seleccionar los datos Cytomic Orion no elimina los bytes nulos al final de la cadena. Si usa la cláusula `WHERE` debes agregar bytes nulos manualmente para que coincida con el valor de FixedString. Este comportamiento difiere del comportamiento de MySQL para el tipo CHAR (donde las cadenas se rellenan con espacios y los espacios se eliminan para la salida).

Ten en cuenta que la longitud del valor FixedString (N) es constante. La función de longitud devuelve `N` incluso si el valor de FixedString (N) se llena solo con bytes nulos, pero la función vacía devuelve 1 en este caso.

Fecha (DATE)

Date almacena en dos bytes el número de días de la fecha desde 1970-01-01. Permite almacenar valores desde el comienzo de la época de Unix hasta el umbral superior definido en el año 2105. El valor mínimo se muestra como 0000-00-00.

La fecha se almacena sin la zona horaria.

Fecha y hora (DATETIME)

DateTime se almacena en cuatro bytes como una marca de tiempo Unix y permite almacenar valores en el mismo rango que el definido para el tipo Date. El tiempo se almacena con una precisión de hasta un segundo (sin segundos bisiestos).

Zonas horarias

El tipo DateTime se convierte de texto (dividido en sus partes) a binario y viceversa utilizando la zona horaria del sistema en el momento en que se inicia el servidor. En formato de texto la información sobre el horario de verano se pierde.

De forma predeterminada el cliente cambia a la zona horaria del servidor cuando se conecta. Por lo tanto, cuando trabaje con una fecha de texto (por ejemplo, al guardar volcados de texto), tenga en cuenta que puede haber ambigüedades durante los cambios en el horario de verano y puede haber problemas para hacer coincidir los datos si la zona horaria cambia.

Nullable

Nullable (TypeName) permite almacenar una marcador especial (NULL) que representa a un valor nulo junto con los valores normales permitidos por TypeName. Por ejemplo, una columna de tipo Nullable (Int8) puede almacenar valores de tipo Int8, y las filas que no tienen un valor almacenarán `NULL`.

Expresiones regulares

Algunos parámetros de funciones utilizadas en sentencias SQL requieren el uso de expresiones regulares. La sintaxis admitida en estas expresiones es Golang. Para consultar los detalles consulta **https://github.com/google/re2/wiki/Syntax**.

Antes de utilizar una expresión regular en una sentencia SQL en Cytomic Orion, es recomendable validar su sintaxis. Utiliza el sitio **https://regex101.com/** y elige Golang como lenguaje para comprobar previamente la expresión utilizada.

Sintaxis cláusula Select

A continuación se muestra la sintaxis general de la cláusula SQL:.

```
SELECT [DISTINCT] expr_list
       [FROM [db.] table | (subquery) | table_function]
       [SAMPLE sample_coeff]
       [GLOBAL]  [ANY|ALL]  [ INNER | LEFT | RIGHT | FULL | CROSS ]  [OUTER]  JOIN
(subquery)|table USING columns_list
       [PREWHERE expr]
       [WHERE expr]
       [GROUP BY expr_list] [WITH TOTALS]
```

```
[HAVING expr]
[ORDER BY expr_list]
[LIMIT [n, ]m]
[UNION ALL...]
[LIMIT n BY columns]
```

Cláusula FROM

La cláusula FROM especifica la tabla desde la cual se obtendrán los datos, una subquery o incluir una JOIN. Las subconsultas deben de ir entre paréntesis y a diferencia del SQL estándar, no es necesario especificar un sinónimo después de una subconsulta. Por compatibilidad, es posible escribir 'nombre AS' después de una subconsulta, pero el nombre especificado no se utilizará.

Cláusula SAMPLE

Permite el procesamiento de consultas por aproximación.

Cuando se utiliza la cláusula `SAMPLE`, la consulta no se ejecuta teniendo en cuenta todos los datos, sino solo en una cierta fracción de ellos. Por ejemplo, si necesita calcular estadísticas de un determinado evento, es suficiente ejecutar la consulta en una fracción del 1/10 de todos los eventos y luego multiplicar el resultado por 10.

El procesamiento de consultas aproximado puede ser útil en los siguientes casos:

- Cuando se quiere acelerar la obtención de resultados.
- Cuando las datos sin procesar no reducen notablemente la calidad de los resultados.

Las características del muestreo de datos se enumeran a continuación:

- El muestreo de datos es un mecanismo determinista. El resultado de la misma consulta es siempre el mismo.
- El muestreo funciona consistentemente para diferentes tablas. Para tablas con una sola clave de muestreo, una muestra con el mismo coeficiente siempre selecciona el mismo subconjunto de datos posibles. Esto significa que puedes usar la muestra en subconsultas en la cláusula IN. Además, puedes unir muestras utilizando la cláusula JOIN.
- El muestreo permite leer menos datos del disco. Ten en cuenta que debes especificar la clave de muestreo correctamente.

A continuación se indica la sintaxis admitida en la cláusula `SAMPLE`.

Sintaxis	Descripción
SAMPLE k	Número de 0 a 1. La consulta se ejecuta en una fracción `k` de muestra de datos. Por ejemplo, `SAMPLE 0.1` ejecuta la consulta en el 10% de los datos.
SAMPLE n	`n` es un entero grande. La consulta se ejecuta en una muestra de al menos `n` filas (pero no significativamente más que el número indicado). Por ejemplo,

Sintaxis	Descripción
	`SAMPLE 10000000` ejecuta la consulta en un mínimo de 10,000,000 de filas.
SAMPLE k OFFSET m	`k` y `m` son los números del 0 al 1. La consulta se ejecuta en una fracción `k` de muestra de los datos pero la consulta se aplica sobre la fracción desplazada indicada por `m`.

Tabla 16.1: Parámetros admitidos por la cláusula SAMPLE

Cláusula JOIN

Indica una operación de unión en álgebra relacional que combina columnas de una o más tablas creando un nuevo conjunto que puede almacenarse en una tabla o utilizarse tal cual. Es una forma de combinar columnas de una o más tablas usando valores comunes de cada una. Los tipos de JOINS soportados en Cytomic Orion son los siguientes:

- **INNER JOIN (o JOIN)**: compara cada una de las filas de A con las de B para encontrar todos los pares de filas que satisfacen el predicado de unión indicado en la cláusula `ON`. Cuando se satisface el predicado de unión haciendo coincidir valores no nulos, los valores de columna de cada par de filas coincidentes de A y B se combinan en una única fila de resultados.
- **LEFT JOIN (o LEFT OUTER JOIN)**: el resultado siempre contiene todas las filas de la tabla "izquierda" (A), incluso si la condición de unión no encuentra ninguna fila coincidente en la tabla "derecha" (B). Esto significa que si la cláusula `ON` coincide con 0 (cero) filas en B (para una fila dada en A), la unión devolverá las filas de A pero con `NULL` en cada columna de B.
- **RIGHT JOIN (o RIGHT OUTER JOIN)**: el resultado siempre contiene todas las filas de la tabla "derecha" (B), incluso si la condición de unión no encuentra ninguna fila coincidente en la tabla "izquierda" (A). Esto significa que si la cláusula `ON` coincide con 0 (cero) filas en A (para una fila dada en B), la unión devolverá las filas de B pero con `NULL` en cada columna de A.
- **FULL JOIN (o FULL OUTER JOIN)**: combina el efecto de aplicar uniones `LEFT JOIN` y `RIGHT JOIN`. Cuando las filas en las tablas no coincidan, el conjunto de resultados tendrá valores `NULL` para cada columna de la tabla que carece de una fila coincidente. Para aquellas filas que sí coinciden, se generará una sola fila en el conjunto de resultados (que contiene columnas con los datos de ambas tablas).
- **CROSS JOIN (o ,)**: devuelve el producto cartesiano de las filas de las tablas, produciendo tantas filas como combinaciones resultantes de cada fila de la primera tabla con cada fila de la segunda tabla.
- **Modificador ANY o ALL**: Si se especifica `ALL` y la tabla derecha tiene varias filas coincidentes, los datos se multiplicarán por el número de filas. Este es el comportamiento normal de una cláusula `JOIN` en SQL estándar. Si se especifica `ANY` y la tabla de la derecha

tiene varias filas coincidentes, solo se unirá la primera que se encuentre. Si la tabla de la derecha tiene solo una fila coincidente, los resultados de `ANY` y `ALL` son los mismos.

Cláusula WHERE

Si se incluye una cláusula `WHERE`, ésta debe contener una expresión que dé como resultado un dato de tipo UInt8, que suele ser una expresión de comparación mediante operadores lógicos. Esta expresión se utiliza para filtrar datos antes de todas las transformaciones incluidas en la sentencia.

Cláusula PREWHERE

Esta cláusula tiene el mismo significado que la cláusula `WHERE`. La diferencia está en que cuando se utiliza `PREWHERE`, primero se leen las columnas necesarias para ejecutarla y posteriormente se leen el resto de otras columnas necesarias para ejecutar la consulta, pero solo aquellos bloques donde la expresión `PREWHERE` sea verdadera.

`PREWHERE` filtra de forma efectiva los datos y reduce el volumen a leer del disco duro.

Cláusula GROUP BY

Agrupa el conjunto de resultados mediante una o más columnas. Para crear la agrupación Cytomic Orion interpreta los datos `NULL` como un valor.

Si se especifica el modificador `WITH TOTALS`, se calculará una fila adicional, que contendrá valores predeterminados (ceros o líneas vacías) y columnas de funciones agregadas con los valores calculados en todas las filas (valores "totales"). Esta fila adicional se genera en los formatos JSON, TabSeparated y Pretty. En formato JSON, esta fila se muestra como un campo de 'totales' separado. En formato TabSeparated, la fila aparecerá después del resultado principal, precedida por una fila vacía. En formato Pretty, la fila se muestra como una tabla separada después del resultado principal.

Puedes utilizar `WITH TOTALS` en subconsultas, incluyéndolas en la cláusula JOIN (en este caso, se combinan los valores totales respectivos).

La cláusula `GROUP BY` no admite argumentos por posición. Esto difiere de MySQL pero se ajusta a SQL estándar. Por ejemplo, `GROUP BY 1, 2` se interpretará como agrupación por constantes (es decir, agregación de todas las filas en una).

Cláusula LIMIT N BY columnas

Selecciona las `N` filas superiores para cada grupo de columnas. `LIMIT N BY` no tiene relación con `LIMIT` y ambas pueden ser utilizados en la misma consulta. `LIMIT N BY` puede contener cualquier número de columnas o expresiones.

Cláusula HAVING

Permite filtrar el resultado recibido de `GROUP BY` de forma similar a la como lo hace la cláusula `WHERE`. `WHERE` y `HAVING` se diferencian en que `WHERE` se ejecuta antes de la agregación (`GROUP BY`), mientras que `HAVING` después. Si no se realiza una agregación `HAVING` no se puede utilizar.

La cláusula `GROUP BY` no admite argumentos por posición. Esto difiere de MySQL pero se ajusta al lenguaje SQL estándar.

Cláusula ORDER BY

La cláusula `ORDER BY` contiene una lista de expresiones a las que se les puede asignar una dirección de ordenación (`DESC` - descendente o `ASC` - ascendente, si no se especifica la dirección, se asume `ASC`). La dirección de clasificación se aplica a una sola expresión, no a toda la lista.

Las filas que tienen valores idénticos para la lista de expresiones de clasificación se muestran en un orden arbitrario, que también puede ser no determinista (diferente cada vez). Si se omite la cláusula `ORDER BY`, el orden de las filas tampoco está definido, y puede no ser determinista.

COLLATE

Al ordenar por valores de tipo cadena de caracteres (string) puedes añadir `COLLATE` para especificar el alfabeto utilizado, por ejemplo `ORDER BY SearchPhrase COLLATE 'tr'`, que ordena por palabra clave en orden ascendente, usando el alfabeto turco, sin distinción de mayúsculas y minúsculas y asumiendo que las cadenas están codificadas en UTF-8.

`COLLATE` se puede especificar o no para cada expresión de forma independiente. Si se utiliza `ASC` o `DESC`, añade después `COLLATE`. Cuando se usa `COLLATE`, la clasificación siempre distingue entre mayúsculas y minúsculas.

Solo se recomienda usar `COLLATE` para clasificar grupos de filas pequeños ya que es menos eficiente que la clasificación normal por bytes.

Orden de clasificación NaN y NULL:

- **Con el modificador NULLS FIRST**: primero `NULL`, luego `NaN`, luego otros valores.
- **Con el modificador NULLS LAST**: primero los valores, luego `NaN` y luego `NULL`.
- **Predeterminado**: modificador `LAST NULLS`.

Cuando se ordenan los números en punto flotante, los resultados `NaN` se separarán del resto de valores. Independientemente del orden de clasificación, los `NaN` se situarán al final, es decir, para la clasificación ascendente se consideran como los números más grandes posibles, mientras que para la clasificación descendente se colocan como si fueran los más pequeños.

Cláusula SELECT

Las expresiones especificadas en la cláusula `SELECT` se analizan una vez que se completan los cálculos para todas las cláusulas enumeradas anteriormente. Más específicamente, se analizan las expresiones que están por encima de las funciones agregadas, si existen. Las funciones agregadas y todo lo que está debajo de ellas se calcula durante la agregación (`GROUP BY`). Estas expresiones funcionan como si se aplicaran a filas separadas en el resultado.

Cláusula DISTINC

Si se especifica `DISTINCT`, solo se muestra una fila por cada conjunto de filas que coincidan completamente en el resultado. El resultado será el mismo que si se hubiera especificado `GROUP BY` en todos los campos especificados en la cláusula `SELECT` sin funciones agregadas, con las diferencias mostradas a continuación:

- `DISTINCT` se puede utilizar junto con `GROUP BY`.
- Cuando se omite `ORDER BY` y se incluye `LIMIT`, la consulta deja de ejecutarse inmediatamente después de que se hayan leído el número requerido de filas diferentes.
- Los bloques de registros se muestran a medida que se procesan, sin esperar a que la consulta completa termine de ejecutarse.

`DISTINCT` funciona con `NULL` como si `NULL` fuera un valor específico. En otras palabras, en los resultados `DISTINCT`, las combinaciones diferentes con `NULL` solo se producen una vez.

Cláusula LIMIT m

Selecciona las primeras m filas del resultado.

`LÍMIT n, m` selecciona las primeras `m` filas del resultado después de omitir las primeras `n` filas. La sintaxis `LIMIT m OFFSET n` también es compatible. `n` y `m` deben ser enteros no negativos.

Si no hay una cláusula `ORDER BY` que ordene explícitamente los resultados, el resultado puede ser arbitrario y no determinista.

Cláusula UNION ALL

Combina cualquier número de consultas. Sólo se admite `UNION ALL`, `UNION (UNION DISTINCT)` no está soportado. Si necesitas `UNION DISTINCT` puedes utilizar `SELECT DISTINCT` desde una subconsulta que contenga `UNION ALL`. Las consultas que forman parte de `UNION ALL` se pueden ejecutar simultáneamente y sus resultados se pueden combinar.

La estructura de los resultados (el número y el tipo de columnas) debe coincidir para las consultas pero los nombres de las columnas pueden diferir. En este caso, los nombres de columna para el resultado final se tomarán de la primera consulta. Para uniones se realizan conversiones de tipos automáticas, por ejemplo, si dos consultas que se combinan tienen el mismo campo con tipos que no admiten Nullable y que aceptan Nullable, siendo tipos compatibles, la `UNION ALL` resultante tendrá un campo de un tipo que admita Nullable.

Las consultas que forman parte de `UNION ALL` no se pueden incluir entre paréntesis. `ORDER BY` y `LIMIT` se aplican a consultas separadas, no al resultado final. Si necesitas aplicar una conversión al resultado final, puede indicar todas las consultas con `UNION ALL` en una subconsulta en la cláusula `FROM`.

Operadores IN

Los operadores `IN`, `NOT IN`, `GLOBAL IN` y `GLOBAL NOT IN` se cubren por separado en este apartado, ya que su funcionalidad es bastante flexible.

El lado izquierdo de una expresión que utiliza `IN` es una única columna o una tupla. Por ejemplo `SELECT UserID IN (123, 456) FROM ...`

Si el lado izquierdo es una columna que pertenece al índice y el lado derecho es un conjunto de constantes, el sistema utilizará el índice para procesar la consulta.

El lado derecho del operador puede ser un conjunto de expresiones constantes, un conjunto de tuplas, el nombre de una tabla de base de datos o una subconsulta `SELECT` entre paréntesis. La subconsulta puede especificar más de una columna para filtrar las tuplas. Por ejemplo

```
SELECT (CounterID, UserID) IN (SELECT CounterID, UserID FROM ...) FROM ....
```

Las columnas a la izquierda y derecha del operador IN deben tener el mismo tipo.

El operador IN y la subconsulta pueden aparecer en cualquier parte de la consulta, incluidas las funciones agregadas y las funciones lambda.

Procesamiento de datos NULL

Durante el procesamiento de una solicitud, el operador `IN` asume que el resultado de una operación con `NULL` siempre es igual a 0, independientemente de si `NULL` está en el lado derecho o izquierdo de la expresión. Los valores `NULL` no se incluyen en ningún conjunto de datos, no se corresponden entre sí y no se pueden comparar.

Uso del asterisco (*)

Puedes incluir un asterisco en cualquier parte de una consulta en lugar de una expresión. Cuando se analiza la consulta, el asterisco se expande a una lista de todas las columnas de la tabla. El uso de un asterisco es raramente justificable:

- Al crear un volcado de tabla.
- Para tablas que contienen pocas columnas.
- Para obtener información sobre qué columnas están en una tabla. En este caso, establece `LÍMIT 1` pero es mejor usar `DESC TABLE`.
- Cuando haya muchas posibilidades de filtrar datos sobre un pequeño número de columnas utiliza `PREWHERE`.
- En subconsultas (ya que las columnas que no son necesarias para la consulta externa se excluyen de las subconsultas).

En todos los demás casos no se recomienda utilizar el asterisco por cuestiones de rendimiento.

Funciones regulares

Las funciones regulares se aplican a cada fila por separado, de modo que el resultado de la función no depende de otras filas, y tienen las características mostradas a continuación:

- **Tipado estricto**: a diferencia del SQL estándar, Cytomic Orion no hace conversiones implícitas entre tipos. Cada función recibe un conjunto específico de tipos, eso quiere decir que en ocasiones será necesario usar funciones de conversión de tipos.
- **Eliminación de subexpresiones comunes**: todas las expresiones en una consulta que tienen el mismo AST (el mismo registro o el mismo resultado del análisis sintáctico) se consideran que tienen valores idénticos. Tales expresiones son concatenadas y ejecutadas una sola vez. Las subconsultas idénticas también se eliminan de esta manera.
- **Tipos de resultados**: todas las funciones devuelven un único valor como resultado (no varios valores ni ningún valor). Generalmente el tipo del resultado se define únicamente por el tipo de argumentos, no por su valor.
- **Constantes**: por simplicidad ciertas funciones solo pueden trabajar con constantes para algunos argumentos. Por ejemplo, el argumento correcto del operador `LIKE` debe ser una constante. La mayor parte de las funciones devuelven una constante si reciben argumentos constantes, la excepción son las funciones que generan números aleatorios. La función `now` devuelve diferentes valores para las consultas que se ejecutaron en diferentes momentos, pero el resultado se considera una constante, ya que solo es relevante dentro de una única consulta. Una expresión constante también se considera una constante (por ejemplo, la mitad derecha del operador `LIKE` se puede construir a partir de varias constantes).
- **Procesamiento nulo**: si al menos uno de los argumentos de la función es `NULL`, el resultado de la función también es `NULL` excepto en las funciones que se indique lo contrario.
- **Constancia**: las funciones no pueden cambiar los valores de sus argumentos: los cambios se devuelven como resultado. Por lo tanto, el resultado del cálculo de funciones separadas no depende del orden en que se escriben las funciones en la consulta.
- **Manejo de errores**: algunas funciones pueden generar una excepción si los datos no son válidos. En este caso, la consulta se cancela y Cytomic Orion devuelve un texto de error al cliente.
- **Evaluación de argumentos**: en casi todos los lenguajes de programación, ciertos argumentos podrían no ser evaluados con algunos operadores, como `&&`, `||` y `?:`. En Cytomic Orion los argumentos de las funciones (operadores) siempre se evalúan. Esto se debe a que se evalúan a la vez partes completas de las columnas en lugar de calcular cada fila por separado.

A continuación se muestran las funciones más frecuentemente utilizadas:

Aritméticas

Para todas las funciones aritméticas, el tipo del resultado se calcula como el tipo asociado al número más pequeño en el que se ajuste el resultado, si existe tal tipo. El mínimo se toma de forma simultánea en función del número de bits, si tiene signo y si es decimal. Si no hay suficientes bits, se toma el tipo siguiente.

Las funciones aritméticas funcionan con cualquier par de tipos UInt8, UInt16, UInt32, UInt64, Int8, Int16, Int32, Int64, Float32 o Float64.

Función	Descripción
plus(a, b) **Operador a + b**	Calcula la suma de dos números. Se permite sumar números enteros a un tipo Date o DateTime. En el caso de un Date, sumar un número entero significa incrementar el número correspondiente de días. Para un DateTime, significa sumar el número correspondiente de segundos.
minus(a, b) **Operador a - b**	Calcula la diferencia de dos números. El resultado siempre tiene signo. También se pueden calcular números enteros a partir de Date o DateTime.
divide (a, b) **Operador a / b**	Calcula el cociente de los números. El tipo de resultado es siempre un tipo de dato en coma flotante, no una división entera. Para la división entera, usa la función `intDiv`. Cuando se divide por cero, se devuelve `inf`, `-inf` o `nan`.
intDiv (a, b)	Calcula el cociente de dos números. Se divide en enteros redondeando hacia abajo según su valor absoluto. Se produce una excepción al dividir por cero o al dividir un número negativo mínimo por menos uno.
intDivOrZero (a, b)	Difiere de `intDiv` en que devuelve cero al dividir por cero o al dividir un número negativo mínimo por menos uno.
modulo(a, b) **Operador a % b**	Calcula el resto de la división. Si los argumentos son números en coma flotante, se convierten previamente a enteros. El resto se trata de la misma forma que en C++. Para números negativos se trunca la división. Se lanza una excepción al dividir por cero o al dividir un número negativo mínimo por menos uno.
negate(a) **operador -a**	Calcula un número con el signo inverso. El resultado siempre tiene signo.
abs (a)	Calcula el valor absoluto del número (`a`). Es decir, si a <0, devuelve `a`. Para los tipos sin signo no hace nada. Para los tipos de enteros con signo,

Función	Descripción
	devuelve un número sin signo.
gcd (a, b)	Devuelve el máximo común divisor de dos números. Se lanza una excepción al dividir por cero o al dividir un número negativo mínimo por menos uno.
lcm(a, b)	Devuelve el mínimo común múltiplo de dos números. Se lanza una excepción al dividir por cero o al dividir un número negativo mínimo por menos uno.

Tabla 16.2: Funciones aritméticas

Comparación

Las funciones de comparación siempre devuelven 0 o 1 (Uint8). Se pueden comparar los siguientes tipos:

- Números.
- Cadenas de caracteres (String) y Cadenas de caracteres fijas (FixedString(N)).
- Fechas (Date).
- Fechas con hora (DateTime).

Por ejemplo, no se permite comparar una fecha con una cadena, es necesario utilizar una función para convertir la cadena en una fecha, o viceversa.

Las cadenas se comparan por bytes. Una cadena más corta es más pequeña que todas las cadenas que comienzan por ella y que contienen al menos un carácter más.

Los operadores de comparación son:

- **Igualdad**: `a = b y a == b`
- **Desigualdad**: `a != b y a <> b`
- **Menor que**: `a < b`
- **Mayor que**: `a > b`
- **Menor o igual que**: `a <= b`
- **Mayor o igual que**: `a >= b`

Lógicas

Las funciones lógicas aceptan cualquier tipo numérico pero devuelven un número UInt8 igual a 0 o 1.

El cero como argumento se considera "falso", mientras que cualquier valor distinto de cero se considera "verdadero".

- **Y**: `AND`
- **O**: `OR`
- **Negación**: `NOT`
- **Xor**: `XOR`

Conversión de tipos

A continuación se muestran las conversiones básicas soportadas:

- **Conversión a tipos sin signo**: toUInt8, toUInt16, toUInt32, toUInt64.
- **Conversión a tipos con signo**: toInt8, toInt16, toInt32, toInt64, toFloat32, toFloat64, toDate, toDateTime.
- **Conversión o cero si error**: toUInt8OrZero, toUInt16OrZero, toUInt32OrZero, toUInt64OrZero, toInt8OrZero, toInt16OrZero, toInt32OrZero, toInt64OrZero, toFloat32OrZero, toFloat64OrZero, toDateOrZero, toDateTimeOrZero.
- **Conversión o nulo si error:** toUInt8OrNull, toUInt16OrNull, toUInt32OrNull, toUInt64OrNull, toInt8OrNull, toInt16OrNull, toInt32OrNull, toInt64OrNull, toFloat32OrNull, toFloat64OrNull, toDateOrNull, toDateTimeOrNull.

A continuación se muestran tipos de conversiones más complejas:

Función	Descripción
toDecimal32(value, S), toDecimal64(value, S), toDecimal128(value, S)	Convierte `value` a un decimal de precisión `S`. `value` puede ser un número o una cadena. El parámetro `S` especifica el número de decimales.
toString	Familia de funciones para convertir entre números, Strings (pero no FixedStrings), Dates y DateTimes. Todas estas funciones aceptan un argumento. Cuando se convierte desde o hacia una cadena, el valor se formatea o analiza utilizando las mismas reglas que para el formato TSV (texto separado por tabuladores). Si la cadena no puede analizarse se lanza una excepción y se cancela la solicitud. Al convertir las fechas en números o viceversa, la fecha corresponde al número de días desde la aparición del sistema operativo Unix (1/1/1970).

Función	Descripción

	Los formatos de fecha y fecha con hora para las funciones `toDate` / `toDateTime` se definen de la siguiente manera:
	`YYYY-MM-DD`
	`YYYY-MM-DD hh: mm: ss`
	Como excepción, en la conversión de los tipos numéricos UInt32, Int32, UInt64 o Int64 a Date si el número es mayor o igual a 65536, el número se interpreta como un timestamp (y no como el número de días). Esto permite escribir `toDate (unix_timestamp)`, que de lo contrario sería un error y requeriría escribir `toDate (toDateTime (unix_timestamp))`.
	La conversión entre un tipo Date a DateTime se realiza de forma natural: agregando una hora nula o eliminando la hora.
	La conversión entre tipos numéricos usa las mismas reglas que las asignaciones entre diferentes tipos numéricos en C ++.
	Además, la función `toString` con un argumento de tipo `DateTime` puede tomar un segundo argumento de tipo String que contiene el nombre de la zona horaria.

toFixedString(s, N)	Convierte un argumento de tipo String en un tipo FixedString (N) (cadena con una longitud fija `N`). `N` debe ser una constante. Si la cadena tiene menos bytes que `N`, se añaden con bytes nulos a la derecha. Si la cadena tiene más bytes que `N`, se lanza una excepción.
toStringCutToZero(s)	Acepta un argumento String o FixedString y devuelve la cadena con el contenido truncado en el primer byte cero encontrado.
reinterpretAsUInt8, **reinterpretAsUInt16**, **reinterpretAsUInt32**, **reinterpretAsUInt64** **reinterpretAsInt8**,	Estas funciones aceptan una cadena e interpretan los bytes al principio de la cadena como un número little endian. Si la cadena no es lo suficientemente larga, las funciones funcionan como si la cadena se completara con el número necesario de bytes nulos. Si la cadena es

Función	Descripción
reinterpretAsInt16, reinterpretAsInt32, reinterpretAsInt64 **reinterpretAsFloat32, reinterpretAsFloat64** **reinterpretAsDate, reinterpretAsDateTime**	más larga de lo necesario se ignoran los bytes adicionales. Un tipo Date se interpreta como el número de días desde la aparición del sistema operativo Unix (1/1/1970), y un DateTime se interpreta como el número de segundos desde el comienzo de Unix.
reinterpretAsString	Acepta un número, un Date o un DateTime y devuelve una cadena que contiene bytes que representan el valor correspondiente en formato little endian. Los bytes nulos se eliminan del final. Por ejemplo, un valor de tipo UInt32 de 255 es una cadena que tiene un byte de tamaño.
reinterpretAsFixedString	Acepta un número, un Date o un DateTime y devuelve un FixedString que contiene bytes que representan el valor correspondiente en formato little endian. Los bytes nulos se eliminan del final. Por ejemplo, un valor de tipo UInt32 de 255 es un FixedString que tiene de tamaño un byte.
CAST(x, t)	Convierte '`x`' al tipo de dato '`t`'.
toIntervalYear, toIntervalQuarter, toIntervalMonth, toIntervalWeek, toIntervalDay, toIntervalHour, toIntervalMinute, toIntervalSecond	Convierte un argumento de tipo numérico en otro de tipo intervalo (duración). El tipo de dato intervalo es muy útil ya que se puede usar para realizar operaciones aritméticas directamente con Date o DateTime.
parseDateTimeBestEffort	Convierte un argumento de tipo de número a un tipo Date o DateTime. A diferencia de toDate y toDateTime, `parseDateTimeBestEffort` puede devolver un formato de fecha más complejo.
parseDateTimeBestEffortOrNull	Igual que `parseDateTimeBestEffort`, excepto que devuelve nulo cuando encuentra un formato de fecha que no se puede procesar.

Función	Descripción
parseDateTimeBestEffortOrZero	Igual que `parseDateTimeBestEffort`, excepto que devuelve la fecha cero cuando encuentra un formato de fecha que no se puede procesar.

Tabla 16.3: Funciones para la conversión de tipos

Tratamiento de fechas y horas

Las funciones para el tratamiento de fechas y horas que lo necesiten pueden recibir un parámetro opcional indicando la zona horaria. Solo se admiten las zonas horarias que difieren de UTC en un número entero de horas.

Función	Descripción
toTimeZone	Convierte un tipo Date o DateTime a la zona horaria especificada.
toYear	Convierte un tipo Date o DateTime en un número UInt16 que contiene el número del año.
toQuarter	Convierte un tipo Date o DateTime en un número UInt8 que contiene el número de trimestre.
toMonth	Convierte un tipo Date o DateTime en un número UInt8 que contiene el número del mes (1-12).
toDayOfYear	Convierte un tipo Date o DateTime en un número UInt8 que contiene el número del día del año (1-366).
toDayOfMonth	Convierte un tipo Date o DateTime en un número UInt8 que contiene el número del día del mes (1-31).
toDayOfWeek	Convierte un tipo Date o DateTime en un número UInt8 que contiene el número del día de la semana (el lunes es 1 y el domingo es 7).
toHour	Convierte un tipo Date o DateTime en un número UInt8 que contiene el número de la hora en 24 horas (0-23). Esta función asume que si los relojes se adelantan para ajustarse al horario de verano, se hace por 1 hora y ocurre a las 2 am, y si los relojes

Función	Descripción
	se atrasan para ajustarse al horario de invierno, se hace por 1 hora y ocurre a las 3 am.
toMinute	Convierte un tipo Date o DateTime en un número UInt8 que contiene el número del minuto de la hora (0-59).
toSecond	Convierte un tipo Date o DateTime en un número UInt8 que contiene el número del segundo en el minuto (0-59). Los segundos intercalares (segundos bisiestos) no se tienen en cuenta.
toUnixTimestamp	Convierte un tipo Date o DateTime en una marca de tiempo de Unix.
toStartOfYear	Redondea un tipo Date o DateTime al primer día del año y devuelve un Date.
toStartOfISOYear	Redondea un tipo Date o DateTime al primer día del año ISO y devuelve un Date.
toStartOfQuarter	Redondea un tipo Date o DateTime al primer día del trimestre (1 de enero, 1 de abril, 1 de julio o 1 de octubre) y devuelve un Date.
toStartOfMonth	Redondea un tipo Date o DateTime al primer día del mes y devuelve un Date.
toMonday	Redondea un tipo Date o DateTime al lunes más cercano y devuelve un Date.
toStartOfDay	Redondea un tipo Date o DateTime al comienzo del día.
toStartOfHour	Redondea un tipo Date o DateTime al comienzo de la hora.
toStartOfMinute	Redondea un tipo Date o DateTime al comienzo del minuto.
toStartOfFiveMinute	Redondea un tipo Date o DateTime al inicio del intervalo de cinco minutos.

Función	Descripción
toStartOfTenMinutes	Redondea un tipo Date o DateTime al inicio del intervalo de diez minutos.
toStartOfFifteenMinutes	Redondea tipo Date o DateTime al inicio del intervalo de quince minutos.
toTime	Convierte un tipo Date o DateTime en una fecha fija determinada, al tiempo que conserva la hora.
toRelativeYearNum	Convierte un tipo Date o DateTime al número del año, comenzando a partir de un determinado punto en el pasado.
toRelativeQuarterNum	Convierte un tipo Date o DateTime o fecha en el número del trimestre, a partir de un determinado punto fijo en el pasado.
toRelativeMonthNum	Convierte un tipo Date o DateTime en el número del mes, a partir de un determinado punto fijo en el pasado.
toRelativeWeekNum	Convierte un tipo Date o DateTime en el número de la semana, a partir de un determinado punto fijo en el pasado.
toRelativeDayNum	Convierte un tipo Date o DateTime en el número del día, a partir de un determinado punto fijo en el pasado.
toRelativeHourNum	Convierte un tipo Date o DateTime en el número de la hora, a partir de un determinado punto fijo en el pasado.
toRelativeMinuteNum	Convierte un tipo Date o DateTime en el número del minuto, a partir de un cierto punto fijo en el pasado.
toRelativeSecondNum	Convierte un tipo Date o DateTime en el número del segundo, a partir de un cierto punto fijo en el pasado.
toISOYear	Convierte un tipo Date o DateTime en un número UInt16 que contiene el número del año ISO.
toISOWeek	Convierte un tipo Date o DateTime en un número UInt8 que contiene el número de la semana ISO.

Función	Descripción
now	No requiere argumentos. Devuelve la hora actual en el momentos de la ejecución de la función. Esta función devuelve una constante.
today	No requiere argumentos. Devuelve la fecha actual en el momentos de la ejecución de la función. Equivalente a `toDate (now ())`.
yesterday	No requiere argumentos. Devuelve la fecha de ayer en el momentos de la ejecución de la función. Equivalente a `today () - 1`.
timeSlot	Redondea el tiempo a la media hora.
toYYYYMM	Convierte un a tipo Date o DateTime en un número UInt32 que contiene el año y el mes (YYYY * 100 + MM).
toYYYYMMDD	Convierte un tipo Date o DateTime en un número UInt32 que contiene el año y el mes (YYYY * 100 + MM).
toYYYYMMDDhhmmss	Convierte un tipo Date o DateTime en un número UInt32 que contiene el año y el mes (YYYY * 10000 + MM * 100 + DD).
addYears, addMonths, addWeeks, addDays, addHours, addMinutes, addSeconds, addQuarters	La función agrega un intervalo de tipo Date / DateTime a una variable Date / DateTime y luego devuelve Date / DateTime.
subtractYears, subtractMonths, subtractWeeks, subtractDays, subtractHours, subtractMinutes, subtractSeconds, subtractQuarters	La función resta un intervalo de tipo Date / DateTime a una variable Date / DateTime y devuelve Date / DateTime.
dateDiff('unit', t1, t2, [timezone])	Devuelve la diferencia entre dos horas expresada en en el formato expresado en `unit`, por ejemplo '`hours`'. `t1` y `t2`

Función	Descripción
	pueden ser tipos Date o DateTime. Si se especifica `timezone`, se aplicará a ambos argumentos. Si no, se usan las zonas horarias de los tipos de datos `t1` y `t2`. Si las zonas horarias no son las mismas, el resultado no se especifica. Unidades soportadas: `second, minute, hour, day, week, month, quarter, year`.
formatDateTime(Time, Format[, Timezone])	La función formatea `Time` según el formato indicado en `Format`. Consulta la tabla **Códigos de formateo para la función formatDateTime** para obtener los parámetros de formateo.

Tabla 16.4: Funciones para la manipulación de fechas

Códigos de formateo de la función formatDateTime

Código	Descripción	Ejemplo
%C	Año dividido por 100 y truncado a entero (00-99).	20
%d	Día del mes en dos dígitos completando con cero (01-31).	02
%D	Fecha corta MM / DD / YY, equivalente a %m/%d/%y.	01/02/2018
%e	Día del mes, espacio relleno (1-31).	2
%F	Fecha corta YYYY-MM-DD, equivalente a% Y-% m-% d 2018-01-02.	2018-01-02
%H	Hora en formato 24h (00-23).	22
%I	Hora en formato de 12h (01-12).	10
%j	Día del año (001-366).	002
%m	Mes como un número decimal (01-12).	01

Código	Descripción	Ejemplo
%M	Minuto (00-59).	33
%n	Carácter de nueva línea. '\n'.	
%p	AM o PM.	PM
%R	Tiempo HH:MM en formato 24 horas, equivalente a %H:%M.	22:33
%S	Segundo (00-59).	44
%t	Carácter de tabulación horizontal '\t'.	
%T	Formato de tiempo ISO 8601 HH:MM:SS, equivalente a %H:%M:%S.	22:33:44
%u	Día laborable ISO 8601 en formato número con lunes como 1 (1-7).	2
%V	Número de la semana ISO 8601 (01-53).	01
%w	Día de la semana como un número decimal con domingo como 0 (0-6).	2
%y	Últimos dos dígitos del año(00-99).	18
%Y	Año	2018
%%	Carácter '%'	

Tabla 16.5: Códigos de formateo para la función formatDateTime

Tratamiento de cadenas de caracteres

Función	Descripción
empty	Devuelve 1 si la cadena es vacía y 0 si es una cadena no vacía. El tipo de resultado es UInt8. Una cadena se considera no vacía si contiene al menos un byte, incluso si se trata de un espacio o un byte nulo.

Función	Descripción
notEmpty	Devuelve 0 si la cadena es vacía o 1 si es una cadena no vacía. El tipo de resultado es UInt8. La función también funciona para matrices.
length	Devuelve la longitud de una cadena en bytes (no en caracteres ni puntos de código (code points)). El tipo de resultado es UInt64.
lengthUTF8	Devuelve la longitud de una cadena en puntos de código (code points) Unicode (no en caracteres), asumiendo que la cadena contiene un conjunto de bytes codificados en UTF-8. Si este supuesto no se cumple no se lanza una excepción. El tipo de resultado es UInt64.
char_length, CHAR_LENGTH	Devuelve la longitud de una cadena en puntos de código (code points) Unicode (no en caracteres), asumiendo que la cadena contiene un conjunto de bytes codificados en UTF-8. Si este supuesto no se cumple no se lanza una excepción. El tipo de resultado es UInt64.
character_length, CHARACTER_ LENGTH	Devuelve la longitud de una cadena en puntos de código (code points) Unicode (no en caracteres), asumiendo que la cadena contiene un conjunto de bytes codificados en UTF-8. Si este supuesto no se cumple no se lanza una excepción. El tipo de resultado es UInt64.
lower, lcase	Convierte una cadena ASCII Latin a minúsculas.
upper, ucase	Convierte una cadena ASCII Latin a mayúsculas.
lowerUTF8	Convierte una cadena en minúsculas asumiendo que la cadena contiene un conjunto de bytes codificados en UTF-8. sta función no detecta el idioma de la cadena. Si la longitud de la secuencia de bytes UTF-8 es diferente para mayúsculas y minúsculas de puntos de código el resultado puede ser incorrecto. El comportamiento no está definido si la cadena contiene bytes que no son UTF-8.
upperUTF8	Convierte una cadena en mayúsculas, asumiendo que la

Función	Descripción
	cadena contiene un conjunto de bytes codificados en UTF-8. Esta función no detecta el idioma. Si la longitud de la secuencia de bytes UTF-8 es diferente entre mayúsculas y minúsculas en puntos de código el resultado puede ser incorrecto. El comportamiento no está definido si la cadena contiene bytes no UTF-8.
isValidUTF8	Devuelve 1 si el conjunto de bytes esta codificado en UTF-8, de lo contrario revuelve 0.
reverse	Invierte la cadena (interpretada como una secuencia de bytes).
reverseUTF8	Invierte una secuencia de puntos Unicode asumiendo que la cadena contiene bytes codificados en UTF-8. En caso contrario no lanza una excepción.
concat(s1, s2, ...)	Concatena las cadenas enumeradas en los argumentos sin separadores.
concatAssumeInjective(s1, s2, ...)	Igual que `concat` pero requiere que `concat (s1, s2, s3) -> s4` sea inyectiva. Se usa para optimizar la cláusula `GROUP BY`.
substring(s, offset, length), mid (s, offset, length), substr(s, offset, length)	Devuelve una subcadena que comienza con el byte del índice `offset` y una longitud de bytes `length`. La indexación de caracteres comienza desde uno (como en el estándar SQL). Los argumentos `offset` y `length` deben ser constantes.
substringUTF8(s, offset, length)	Lo mismo que la función `substring` pero para puntos de código Unicode. Funciona asumiendo que la cadena bytes codificados en UTF-8. Si no se cumple no se lanza una excepción.
appendTrailingCharIfAbsent(s, c)	Si la cadena `s` no está vacía y no contiene el carácter `c` al final lo agrega.
convertCharset(s, from, to)	Devuelve la cadena `s` que fue convertida desde la

Función	Descripción
	codificación especificada en `from` a la codificación en `to`.
base64Encode(s)	Codifica la cadena `s` en base64.
base64Decode(s)	Decodifica la cadena `s` codificada en base64 en su cadena original. En caso de fallo lanza una excepción.
tryBase64Decode(s)	Similar a `base64Decode`, pero en caso de error se devuelve una cadena vacía.
endsWith(s, suffix)	Devuelve 1 si la cadena termina con el sufijo especificado, de lo contrario devuelve 0.
startsWith(s, prefix)	Devuelve 1 si la cadena comienza con el prefijo especificado, de lo contrario devuelve 0.
trimLeft(s)	Devuelve una cadena que elimina los caracteres de espacio en blanco al comienzo.
trimRight(s)	Devuelve una cadena que elimina los caracteres de espacio en blanco al final.
trimBoth(s)	Devuelve una cadena que elimina los caracteres de espacio en blanco al comienzo y al final.

Tabla 16.6: Funciones para la manipulación de cadenas

Búsqueda de cadenas de caracteres

La búsqueda distingue entre mayúsculas y minúsculas por defecto en todas funciones mostradas a continuación. Hay variantes separadas para búsquedas sin distinción.

Función	Descripción
position(haystack, needle), locate(haystack, needle)	Busca la subcadena `needle` en la cadena `haystack` y devuelve la posición (en bytes) de la subcadena encontrada, comenzando desde 1, o devuelve 0 si no se encontró. Para búsquedas que no distingan mayúsculas y minúsculas,

Función	Descripción
	usa la función `positionCaseInsensitive`.
positionUTF8(haystack, needle)	Igual que `position`, pero la posición se devuelve en puntos de código Unicode. Funciona asumiendo que la cadena contiene un conjunto de bytes codificados en UTF-8. Si este supuesto no se cumple no lanza una excepción. Para una búsqueda que no distinga mayúsculas y minúsculas, usa la función `positionCaseInsensitiveUTF8`.
multiSearchFirstPosition (haystack, [needle1, needle2, ..., needlen])	Igual que `position`, pero devuelve el desplazamiento más a la izquierda de `haystack` que coincida con algún parámetro `needle`. Para una búsqueda sin distinción de mayúsculas y / o en formato UTF-8, utiliza las funciones `multiSearchFirstPositionCaseInsensitive`, `multiSearchFirstPositionUTF8`, `multiSearchFirstPositionCaseInsensitiveUTF8`.
multiSearchFirstIndex (haystack, [needle1, needle2, ..., needlen])	Devuelve el índice `i` (comenzando desde 1) del parámetro `needle` que se encuentre más a la izquierda en la cadena `haystack`, y 0 en caso contrario. Para una búsqueda sin distinción de mayúsculas y / o en formato UTF-8, utiliza las funciones: `multiSearchFirstIndexCaseInsensitive`, `multiSearchFirstIndexUTF8`, `multiSearchFirstIndexCaseInsensitiveUTF8`.
multiSearchAny(haystack, [needle1, needle2, ..., needlen])	Devuelve 1, si al menos un parámetro `needle` coincide con la cadena `haystack` y 0 en caso contrario. Para una búsqueda sin distinción de mayúsculas y / o en formato UTF-8, utiliza las funciones: `multiSearchAnyCaseInsensitive`, `multiSearchAnyUTF8`, `multiSearchAnyCaseInsensitiveUTF8`. Nota: en todas las funciones `multiSearch*`, el número de parámetros `needle` debe ser inferior a 28.

Función	Descripción
match(haystack, pattern)	Comprueba si la cadena coincide con la expresión regular del patrón. La sintaxis de las expresiones regulares es más limitada que la sintaxis de las expresiones regulares de Perl. Devuelve 0 si no coincide o 1 si coincide. Ten en cuenta que el símbolo de barra invertida (\) se utiliza como carácter de escape en la expresión regular y el mismo símbolo se utiliza para escapar en literales de cadena. De este modo, para escapar en una expresión regular hay que utilizar dos barras invertidas (\\). La expresión regular funciona como si la cadena de caracteres fuera un conjunto de bytes. La expresión regular no puede contener bytes nulos. Para que los patrones busquen subcadenas en una cadena, es mejor usar `LIKE` o `position`, ya que funcionan mucho más rápido.
multiMatchAny(haystack, [pattern1, pattern2, ..., patternn])	Igual que `match`, pero devuelve 0 si ninguna de las expresiones regulares coincide y 1 si coincide alguno de los patrones. Para que los patrones busquen subcadenas en una cadena, es mejor usar `multiSearchAny` ya que funciona mucho más rápido. Nota: la longitud de cualquiera de las cadenas de `haystack` debe ser inferior a 232 bytes, de lo contrario se lanzará una excepción.
multiMatchAnyIndex (haystack, [pattern1, pattern2, ..., patternn])	Lo mismo que `multiMatchAny` pero devuelve cualquier índice que coincida con `haystack`.
multiFuzzyMatchAny (haystack, distance, [pattern1, pattern2, ..., patternn])	Igual que `multiMatchAny` pero devuelve 1 si cualquier patrón coincide con el `haystack` dentro de una distancia especificada en `distance` como constante. Esta función es experimental y puede ser muy lenta.
multiFuzzyMatchAnyIndex (haystack, distance, [pattern1, pattern2, ..., patternn])	Igual que `multiFuzzyMatchAny`, pero devuelve cualquier índice que coincida con el `haystack` dentro de una distancia especificada en `distance` como constante. Nota: las funciones `multiFuzzyMatch *` no son compatibles con las expresiones regulares UTF-8, y dichas expresiones se

Función	Descripción
	tratan como bytes.
extract(haystack, pattern)	Extrae un fragmento de una cadena usando una expresión regular. Si `haystack` no coincide con la expresión regular `pattern` se devuelve una cadena vacía. Si la expresión regular no contiene subpatrones, toma el fragmento que coincide con la expresión regular completa. De lo contrario, toma el fragmento que coincide con el primer subpatrón.
like(haystack, pattern), haystack LIKE pattern operator	Comprueba si una cadena coincide con una expresión regular simple. La expresión regular puede contener los símbolos '`%`' y '`_`'. • **'%'**: indica cualquier cantidad de bytes (incluyendo cero caracteres). • **'_':** indica cualquier byte. Utiliza la barra '`\`' para escapar los símbolos. Consulta la nota sobre cómo escapar en la descripción de la función `match`. Para expresiones regulares como `%needle%`, el código está más optimizado y funciona tan rápido como la función `position`. Para otras expresiones regulares, el código es el mismo que para la función `match`.
notLike(haystack, pattern), haystack NOT LIKE pattern operator	Igual a `like`, pero en negativo.

Tabla 16.7: Funciones de búsqueda de cadenas de caracteres

Sustitución de cadenas de caracteres

Función	Descripción
replaceOne(haystack, pattern, replacement)	Reemplaza la primera aparición, si existe, de la subcadena `pattern` en `haystack` con la subcadena `replacement`. `pattern` y `replacement` deben ser constantes.
replaceAll(haystack, pattern, replacement),	Reemplaza todas las apariciones de la subcadena `pattern` en `haystack` con la subcadena `replacement`.

Función	Descripción
replace(haystack, pattern, replacement)	

replaceRegexpOne (haystack, pattern, replacement)	Reemplaza la primera ocurrencia, si existe utilizando la expresión regular `pattern` del tipo 're2'. Se puede especificar un patrón en `replacement`. Este patrón puede incluir sustituciones `\0 - \9`. La sustitución `\0` incluye la expresión regular completa. Las sustituciones `\1 - \9` corresponden a los números del subpatrón. Para usar el carácter `\` en una plantilla, escápala usando '`\`'. Ten en cuenta que los literales de cadena requieren un escape adicional.
	Ejemplo: copiar una cadena diez veces:
	`SELECT replaceRegexpOne ('Hola, mundo!', '. *', '\\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0) AS res`
	Resultado:
	`¡Hola, mundo! ¡Hola, mundo! ¡Hola, mundo! ¡Hola, mundo! ¡Hola, mundo! ¡Hola, mundo! ¡Hola, mundo! ¡Hola, mundo! ¡Hola, mundo! ¦`

replaceRegexpAll (haystack, pattern, replacement)	Lo mismo que `replaceRegexpOne` pero reemplaza todas las ocurrencias.
	Ejemplo:
	`SELECT replaceRegexpAll('Hello, World!', '.', '\\0\\0') AS res`
	`HHeellllloo,, WWoorrlldd!!`
	Si una expresión regular funcionó en una subcadena vacía, la sustitución no se realiza más de una vez.
	Ejemplo:
	`SELECT replaceRegexpAll('Hello, World!', '^', 'here: ') AS res`
	`here: Hello, World!`

regexpQuoteMeta(s)	Agrega una barra invertida antes de algunos caracteres predefinidos en la cadena. Caracteres predefinidos: `'0', '\', '|', '(', ')', '^', '$', '.', '[', ']', '?', '*' ,`

Función	Descripción
	`'+', '{', ':', '-'`. Esta implementación difiere ligeramente de re2. Escapa de cero bytes con `\0` en lugar de con `\x00` y escapa solo los caracteres requeridos.

Tabla 16.8: Funciones para la sustitución de cadenas de caracteres

Matemáticas

Todas estas funciones devuelven un número Float64. La precisión del resultado es la máxima posible pero en ocasiones el resultado no coincide con el número representable más cercano al número real correspondiente.

Función	Descripción
e()	Devuelve el número e como Float64.
pi()	Devuelve el número pi como Float64.
exp(x)	Acepta un argumento numérico y devuelve el exponente del argumento como Float64.
log(x), ln(x)	Acepta un argumento numérico y devuelve el logaritmo natural del argumento como Float64.
exp2(x)	Acepta un argumento numérico y devuelve el número 2 elevado a x como Float64.
log2(x)	Acepta un argumento numérico y devuelve el logaritmo en base 2 como Float64.
exp10(x)	Acepta un argumento numérico y devuelve el número 10 elevado a x como Float64 .
log10(x)	Acepta un argumento numérico y devuelve el logaritmo en base 10 como Float64.
sqrt(x)	Acepta un argumento numérico y devuelve la raíz cuadrada como Float64.

Función	Descripción
cbrt(x)	Acepta un argumento numérico y devuelve la raíz cúbica como Float64.
erf(x)	Si `x` no es negativo, entonces `erf` devuelve la probabilidad de que una variable aleatoria que sigue una distribución normal con una desviación estándar `s` tome un valor mayor del valor esperado `x`.
erfc(x)	Acepta un argumento numérico y devuelve `1 - erf (x)` como Float64 sin pérdida de precisión para valores grandes de `x`.
lgamma(x)	Logaritmo de la función gamma.
tgamma(x)	Función gamma.
sin(x)	Devuelve el seno de x.
cos(x)	Devuelve el coseno de x.
tan(x)	Devuelve la tangente de x.
asin(x)	Devuelve el arco seno.
acos(x)	Devuelve el arco coseno.
atan(x)	Devuelve el arco tangente.
pow(x, y), power(x, y)	Toma dos argumentos numéricos `x` e `y` y devuelve `x` elevado a la potencia de `y` como Float64.
intExp2	Acepta un argumento numérico y devuelve 2 elevado a `x` como UInt64.
intExp10	Acepta un argumento numérico y devuelve 10 elevando a `x` como UInt64.

Tabla 16.9: Funciones aritméticas

Redondeo

Función	Descripción

floor(x[, N])	Devuelve el número redondeado más grande menor o igual que `x`. Un número redondeado es un múltiplo de 1 / 10N, o el número más cercano del tipo de datos apropiado si 1 / 10N no es exacto. `N` es una constante entera y es un parámetro opcional (por defecto es cero, lo que implica redondear a un entero). `N` puede ser negativo).
	Ejemplos:
	`floor (123.45, 1) = 123.4`
	`floor (123.45, -1) = 120.`
	x es cualquier tipo numérico y el resultado es un número del mismo tipo. Para los argumentos enteros lo normal es redondear con un valor negativo de `N`. Para una `N` no negativa la función no hace nada.

ceil(x[, N]), ceiling(x[, N])	Devuelve el número redondeado más pequeño mayor o igual a `x`. En el resto de funcionalidad es igual a la función `floor`.

round(x[, N])	Redondea `x` a un valor a una cifra con un número específico de decimales `N`. La función devuelve el número más cercano posible. En caso de que el número dado este a la misma distancia que otros números contiguos la función devuelve el número que tiene el dígito par más cercano.
	Parámetros:
	• **x**: el número a redondear. Puede ser cualquier expresión que devuelva un tipo de datos numérico.
	• **N**: valor entero.
	  • Si `N` > 0, la función redondea el valor a la derecha del punto decimal.
	  • Si `N` <0, la función redondea el valor a la izquierda del punto decimal.
	  • Si `N` = 0, la función redondea el valor a entero. En este caso el argumento puede ser omitido.
	Valor devuelto:
	El número redondeado del mismo tipo que el número de entrada.

Función	Descripción
roundToExp2 (num)	Acepta un número y si el menor que 1 devuelve 0, de lo contrario redondea el número hasta el grado más cercano (total no negativo) de 2.

Tabla 16.10: Funciones de redondeo

Generación de números aleatorios

Se utilizan generadores no criptográficos de números pseudoaleatorios. Todas las funciones aceptan cero o un argumento. Si se pasa un argumento puede ser de cualquier tipo pero su valor no se utilizará. El único propósito de este argumento es evitar la eliminación de subexpresiones idénticas de modo que dos subexpersiones diferentes de utilicen la misma función devuelvan columnas diferentes con diferentes números aleatorios.

Función	Descripción
rand	Devuelve un número UInt32 pseudoaleatorio distribuido uniformemente entre todos los números de tipo UInt32. Utiliza un generador lineal congruencial.
rand64	Devuelve un número UInt64 pseudoaleatorio distribuido uniformemente entre todos los números de tipo UInt64. Utiliza un generador lineal congruencial.
randConstant	Devuelve un número UInt32 pseudoaleatorio. El valor es uno para bloques diferentes.

Tabla 16.11: Funciones para generar números aleatorios

Codificación

Función	Descripción
hex	Acepta argumentos de tipo String, UInt, Date y DateTime. Devuelve una cadena que contiene la representación hexadecimal del argumento utilizando letras mayúsculas A-F. No se utiliza prefijos '0x' ni sufijos 'h'. Para las cadenas de caracteres, todos los bytes se codifican como dos números hexadecimales. Los números se convierten a formato big endian. Date se codifica como el número de días desde el comienzo de Unix. DateTime se codifica como el número de segundos desde el comienzo de Unix.

Función	Descripción
unhex(str)	Acepta un String que contiene cualquier número de dígitos hexadecimales y devuelve un String que contiene los bytes correspondientes. Admite letras mayúsculas y minúsculas A-F. El número de dígitos hexadecimales no tiene que ser par. Si es impar, el último dígito se interpretará como la primera mitad del byte 00-0F. Si la cadena del argumento contiene dígitos no hexadecimales no se lanza una excepción. Si deseas convertir el resultado en un número utiliza las funciones `reverse` y `reinterpretAsType`.
bitmaskToList (num)	Acepta un entero y devuelve una cadena que contiene la lista de potencias de dos que suman el número de origen. Los resultados se devuelven separados por comas sin espacios en formato de texto, en orden ascendente.

Tabla 16.12: Funciones de codificación

Tratamiento de URLs

Función	Descripción
protocol	Devuelve el protocolo de la URL. Ejemplos: `http, ftp, mailto, imap,` etc.
domain	Devuelve el dominio de la URL.
domainWithoutWWW	Devuelve el dominio y elimina un 'www' desde el principio de la cadena si está presente.
topLevelDomain	Devuelve el dominio de nivel superior. Ejemplo: `.com`.
firstSignificantSubdomain	Devuelve el "primer subdominio significativo": • Si es 'com', 'net', 'org' o 'co' se devuelve un dominio de segundo nivel. • En caso contrario se devuelve un dominio de tercer nivel.
cutToFirstSignificantSubdomain	Devuelve la parte del dominio que incluye subdominios de nivel superior hasta el "primer subdominio

Función	Descripción
	significativo" (consulta la explicación anterior).
path	Devuelve la ruta de la URL sin incluir los parámetros de la consulta.
pathFull	Igual que la función anterior pero incluyendo la cadena de consulta y el fragmento. Ejemplo: `/top/news.html?page=2#comments`
queryString	Devuelve la cadena de consulta. No se incluye el signo de interrogación inicial, ni '`#`' ni los caracteres tras '`#`'.
fragmenttext	Devuelve el identificador de fragmento. No se incluye el símbolo '`#`'.
queryStringAndFragment	Devuelve la cadena de consulta y el identificador de fragmento.
extractURLParameter(URL, name)	Devuelve el valor del parámetro `name` en la URL, si está presente o una cadena vacía. Si hay muchos parámetros con este nombre, devuelve la primera aparición. Esta función funciona bajo el supuesto de que el nombre del parámetro está codificado en la URL exactamente de la misma manera que en el argumento pasado.
extractURLParameters(URL)	Devuelve una matriz de cadenas de nombre igual al valor correspondiente a los parámetros de URL. Los valores no se decodifican de ninguna manera.
extractURLParameterNames(URL)	Devuelve una matriz de cadenas correspondientes a los nombres de los parámetros de URL. Los valores no se decodifican de ninguna manera.
URLHierarchy(URL)	Devuelve una matriz que contiene la URL, truncada al final por los símbolos '/' y '?' en la ruta y cadena de consulta. Los caracteres separadores consecutivos se cuentan como uno. El corte se realiza en la posición después de todos los caracteres separadores

Función	Descripción
	consecutivos. Ejemplo: `URLPathHierarchy ('https://example.com/browse/CONV-6788') = [ '/browse/', '/browse/CONV-6788' ]`
URLPathHierarchy(URL)	Lo mismo que arriba, pero sin el protocolo y el host en el resultado. El elemento '/' (raíz) no está incluido.
decodeURLComponent(URL)	Devuelve la URL decodificada.
cutWWW	Elimina un 'www' desde el principio del dominio de la URL, si está presente.
cutQueryString	Elimina la cadena de consulta y el signo de interrogación.
cutFragment	Elimina el identificador del fragmento y el signo del número.
cutQueryStringAndFragment	Elimina la cadena de consulta y el identificador de fragmento. El signo de interrogación y el signo del número también se eliminan.
cutURLParameter(URL, name)	Elimina el parámetro de URL 'nombre', si está presente. Esta función funciona bajo el supuesto de que el nombre del parámetro está codificado en la URL exactamente de la misma manera que en el argumento pasado.

Tabla 16.13: Funciones para el tratamiento de URLs

Tratamiento de direcciones IP

Función	Descripción
IPv4NumToString (num)	Toma un número UInt32, lo interpreta como una dirección IPv4 en big endian y devuelve un String que contiene la dirección

Función	Descripción
	IPv4 correspondiente en el formato A.B.C.D (números separados por puntos en forma decimal).
IPv4StringToNum(s)	Función inversa de `IPv4NumToString`. Si la dirección IPv4 tiene un formato no válido, devuelve 0.
IPv4NumToStringClassC (num)	Similar a `IPv4NumToString`, pero usando xxx en lugar del último octeto.
IPv6NumToString(x)	Acepta un valor FixedString (16) que contiene la dirección IPv6 en formato binario. Devuelve una cadena que contiene esta dirección en formato texto. Las direcciones IPv4 asignadas a IPv6 se envían en el formato :: ffff: 111.222.33.44.
IPv6StringToNum(s)	Función inversa de `IPv6NumToString`. Si la dirección IPv6 tiene un formato no válido, devuelve una cadena de bytes nulos. HEX puede ser mayúscula o minúscula.
IPv4ToIPv6(x)	Toma un número UInt32, lo interpreta como una dirección IPv4 en big endian y devuelve un valor de FixedString (16) que contiene la dirección IPv6 en formato binario.
cutIPv6(x, bitsToCutForIPv6, bitsToCutForIPv4)	Acepta un valor FixedString (16) que contiene la dirección IPv6 en formato binario. Devuelve una cadena que contiene la dirección del número especificado de bits eliminados en formato texto.
IPv4CIDRtoIPv4Range(ipv4, cidr)	Acepta un valor de IPv4 y UInt8 que contiene el CIDR y devuelve una tupla con dos IPv4 que contienen el rango inferior y el rango superior de la subred.
IPv6CIDRtoIPv6Range(ipv6, cidr)	Acepta un valor de IPv6 y UInt8 que contiene el CIDR y devuelve una tupla con dos IPv6 que contienen el rango inferior y el rango superior de la subred.

Tabla 16.14: Funciones para el tratamiento de direcciones IP

Tratamiento de argumentos nulos

Función	Descripción
isNull(x)	Comprueba si el argumento es NULL. Parámetros: • **x**: valor de tipo de datos no compuesto. Valor devuelto: • **1**: si x es NULL. • **0**: si x no es NULL.
isNotNull (x)	Parámetros: • **x**: valor con un tipo de datos no compuesto. Valor devuelto: • **0**: si x es NULL. • **1**: si x no es NULL.
coalesce(x,...)	• **Parámetros**: cualquier número de parámetros de tipo no compuesto. Todos los parámetros deben ser compatibles por tipo de datos. • **Valores devueltos**: el primer argumento no NULL y NULL, si todos los argumentos son NULL.
ifNull	Devuelve un valor alternativo si el argumento principal es NULL.
ifNull (x, alt)	Parámetros: • **x**: valor para verificar NULL. • **alt**: valor que devuelve la función si `x` es NULL. Valores devueltos • El valor `x`, si `x` no es NULL. • El valor `alt`, si `x` es NULL.
nullIf(x,y)	Devuelve NULL si los argumentos son iguales. Parámetros: • **x, y**: valores de comparación. Deben ser tipos

Función	Descripción
	compatibles o se generará una excepción. Valores devueltos: • NULL, si los argumentos son iguales. • El valor de x, si los argumentos no son iguales.
assumeNotNull(x)	Parámetros: • **x**: valor original. Valores devueltos • El valor original del tipo no anulable, si no es NULL. • El valor predeterminado para el tipo no anulable si el valor original era NULL.
toNullable(x)	Convierte el tipo de argumento a Nullable. Parámetros: • x: valor de cualquier tipo no compuesto. Valor devuelto: • valor de entrada con un tipo Nullable.

Tabla 16.15: Funciones para el tratamiento de argumentos nulos

Funciones de agregación

A diferencia de las funciones regulares que funcionaban como si se aplicaran a cada fila por separado, las funciones agregadas acumulan valores de varias filas (es decir, dependen de todo el conjunto de filas).

Función	Descripción
count()	Cuenta el número de filas. Acepta cero argumentos y devuelve UInt64. La sintaxis `COUNT (DISTINCT x)` no es compatible. La función de agregación `uniq` separada sirve para este propósito. Las sentencias `SELECT count() FROM table` no están optimizada, porque el número de entradas en la tabla no se

Función	Descripción
	almacena por separado. Internamente Cytomic Orion seleccionará una columna pequeña de la tabla y contará el número de valores en ella.
any(x)	Selecciona el primer valor encontrado. La consulta se puede ejecutar en cualquier orden e incluso en un orden diferente cada vez, por lo que el resultado de esta función es indeterminado. Para obtener un resultado determinado utiliza la función `min` o `max` en lugar de `any`. En algunos casos el orden de ejecución es fijo, como por ejemplo en los casos en que `SELECT` proviene de una subconsulta que usa `ORDER BY`. Cuando una consulta `SELECT` tiene la cláusula `GROUP BY` o al menos una función de agregación, Cytomic Orion requiere que todas las expresiones en las cláusulas `SELECT`, `HAVING` y `ORDER BY` se calculen a partir de las funciones agregadas, es decir, cada columna seleccionada de la tabla debe usarse en claves o dentro de funciones e agregación.
anyHeavy(x)	Selecciona un valor que se ocurre produce con frecuencia. Si hay un valor que ocurre más que en la mitad de los casos en cada uno de los hilos de ejecución de la consulta, se devuelve este valor. Normalmente, el resultado no es determinista.
anyLast(x)	Selecciona el último valor encontrado.
min(x)	Devuelve el valor mínimo.
max(x)	Devuelve el valor máximo.
argMin(arg, val)	Calcula el valor `arg` para un valor `val` mínimo. Si hay varios valores diferentes de `arg` para valores mínimos de `val`, el primero de estos valores encontrados es la salida.
argMax(arg, val)	Calcula el valor `arg` para un valor `val` máximo. Si hay varios valores diferentes de `arg` para valores máximos de `val`, el primero de estos valores encontrados es la salida.
sum(x)	Devuelve la suma. Solo funcionacon números.

Función	Descripción
sumWithOverflow(x)	Calcula una suma de números utilizando el mismo tipo de datos para el resultado que para los parámetros de entrada. Si la suma excede el valor máximo para ese tipo de datos, la función devuelve un error.
avg(x)	Calcula la media. Solo funciona para números. El resultado es siempre Float64.
uniq(x)	Calcula el número aproximado de valores diferentes del argumento. Funciona para números, cadenas, Dates, DateTimes y para múltiples argumentos y argumentos de tipo tupla. El resultado es determinado (no depende del orden de procesamiento de la consulta).
uniqExact(x)	Calcula el número de valores diferentes del argumento con precisión y sin aproximaciones. Se recomienda utilizar la función `uniq`. Utiliza la función `uniqExact` si necesitas un resultado exacto.
quantile(level)(x)	Calcula `x`-ésimo cuantil de orden `level`. `level` es una constante y un número en coma flotante entre 0 a 1. Si se omite el parámetro `level` se toma por defecto 0.5 (cálculo de la mediana). Esta función acepta números, Dates y DateTimes y devuelve: • **Para números**: Float64 • **Para Dates**: Date • **Para DateTimes**: DateTime La precisión de esta función es relativamente baja. Utiliza `quantileExact(level)(x)` para máxima precisión. El resultado depende del orden de ejecución de la consulta y no es determinista.
quantileExact(level)(x)	Calcula el cuantil de `level` con precisión.

Función	Descripción
median(x)	Calcula la mediana.
varSamp(x)	Estimación sin sesgo de la varianza de una variable aleatoria. Los valores que se pasan como argumento representan una muestra de la población total. La función devuelve un Float64.
varPop(x)	Calcula la varianza de población pasada como argumento.
stddevSamp(x)	Estimación sin sesgo de la desviación típica de una variable aleatoria. Los valores que se pasan como argumento representan una muestra de la población total. La función devuelve un Float64.
stddevPop(x)	Calcula la desviación típica de población pasada como argumento.
covarSamp(x, y)	Estimación sin sesgo de la covarianza de dos variables aleatorias. Los valores que se pasan como argumentos representan dos muestras de la población total. La función devuelve un Float64.
covarPop(x, y)	Calculo de la covarianza de dos variables aleatorias. Los valores que se pasan como argumentos representan dos poblaciones. La función devuelve un Float64.
corr(x, y)	Calcula el índice de correlación Pearson.

Tabla 16.16: Funciones de agregación

Capítulo 17

Integración de Cytomic Orion con las herramientas del SOC

Debido al incremento en la variedad de dispositivos a proteger, del número de amenazas en circulación y de los vectores de infección que utilizan, los SOCs de las organizaciones se ven desbordados por la cantidad y diversidad de incidencias que gestionan. Esta situación empuja a las organizaciones a incorporar nuevas herramientas cada vez más sofisticadas para automatizar los procesos de análisis, contención y recuperación de los incidentes detectados. Este nuevo conjunto de servicios cubre ámbitos muy diversos, y requiere un intercambio constante de información, en muchas ocasiones de forma manual, entre las aplicaciones que la forman.

Todas estas nuevas herramientas conllevan una mayor dificultad a la hora de ejecutar de forma consistente y homogénea los procedimientos implantados en el SOC. Como resultado, se obtienen tiempos de respuesta muy variables y una calidad del servicio que depende directamente del tipo de problema gestionado, del conjunto de herramientas empleado y del equipo técnico que las utilizó.

Cytomic Orion implementa varias APIs que facilitan tanto la integración en el conjunto de herramientas implantadas en el SOC como la gestión automatizada de los recursos involucrados en un incidente o en su respuesta.

El tiempo de retención de la telemetría en el océano de datos es de 1 año.

CONTENIDO DEL CAPÍTULO

Prueba del funcionamiento de las APIs en Cytomic Orion

Para servir de apoyo a analistas y desarrolladores, Cytomic publica los recursos siguientes:

- Proyecto para la herramienta Postman.
- Código de ejemplo en formato Python.

Proyecto para la herramienta Postman

Postman es una plataforma colaborativa para el desarrollo de APIs. Puedes usar Postman para diseñar, construir y probar una API junto a otros compañeros. Cytomic Orion utiliza Postman para facilitar y acelerar la adopción de esta tecnología por parte de los desarrolladores.

La API de Cytomic Orion está disponible como proyecto Postman para todos sus clientes y les permite ejecutar llamadas desde este entorno y visualizar los resultados sin necesidad de escribir una sola linea de código.

*Consulta la página **https://www.getpostman.com/** para descargar una copia gratuita del programa Postman.*

Para lanzar peticiones a la API de Cytomic Orion desde Postman sigue los pasos mostrados a continuación:

- Descarga el fichero `Postman.Orion.API.zip` desde el enlace **https://info.cytomicmodel.com/resources/guides/Orion/es/Postman.Orion.API.zip** y descomprímelo en tu equipo.
- Inicia Postman e importa los dos ficheros `APIOrion.postman_ collection.json` y `APIOrion.postman_environment.json`. Para ello haz clic en **File** e **Import**.
- Genera una nueva aplicación en la consola de Cytomic Orion (consulta **Habilitar el acceso a la API desde programas externos**) y guarda el usuario y la contraseña.
- Haz clic en el icono 👁 situado en la parte superior derecha de la ventana de Postman y copia el usuario y contraseña obtenido en el paso anterior en los campos `username` y `password` de la columna **CURRENT VALUE**.
- Si es la primera vez que lanzas una petición en la sesión ejecuta el método `Authentication API` de la rama **Authentication** para obtener un token de acceso y de refresco.
- Selecciona en la rama **1.0** del panel izquierdo de Postman la llamada de la API a ejecutar y haz clic en el botón **Send**. El programa formará la petición HTTP correcta en base a la definición de la API y de los parámetros suministrados y visualizará la respuesta del servidor junto al código HTTP que indicará si fue un éxito o no.

Código de ejemplo en formato Python

Cytomic ofrece un fichero .py compatible con Python 3.0 y superior que contiene un ejemplo básico de todos los métodos de la API. Para ejecutar el código de ejemplo sigue los pasos mostrados a continuación:

- Descarga el fichero `Orion_ API.zip` del enlace **https://info.cytomicmodel.com/resources/guides/Orion/es/Orion_ API.zip** y descomprímelo en el escritorio.
- Descarga un intérprete de Python 3.x de **https://www.python.org/downloads/**.
- Ejecuta el fichero `Orion_API.v1.1.py` con el interprete directamente o con ayuda de un IDE tipo Spyder o similar (consulta **https://www.spyder-ide.org/**).

Arquitectura de integración en SOCs

Cytomic Orion se integra con herramientas de terceros o con aplicaciones desarrolladas en el propio SOC mediante varias APIs de tipo REST. A continuación se muestra un esquema general de integración de Cytomic Orion con los recursos del SOC:

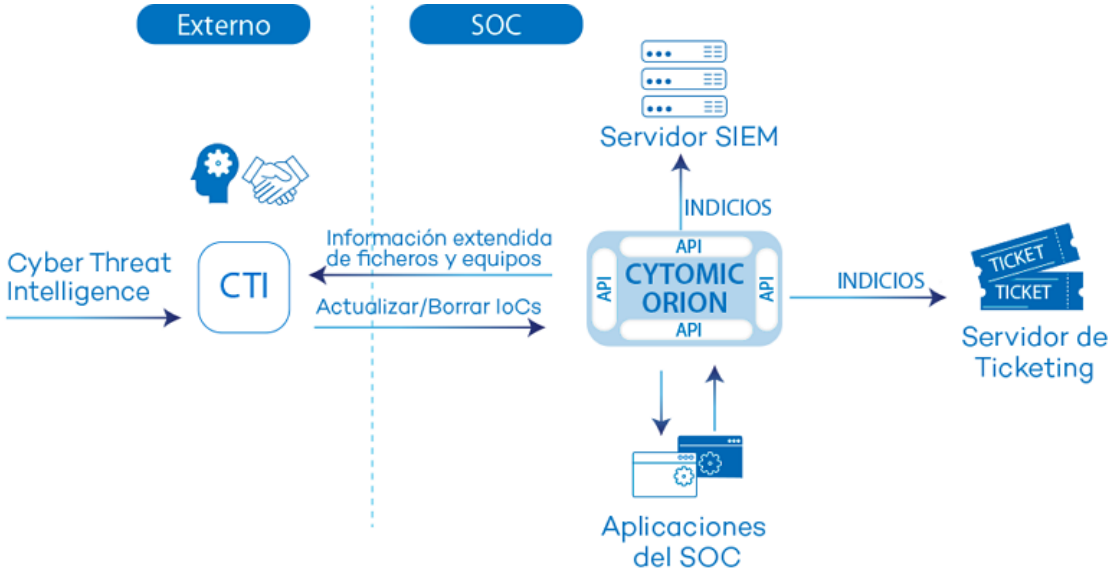


Figura 17.1: Esquema general de Cytomic Orion integrado con varios productos del SOC

Los actores representados en el diagraman son:

- **CTI (Cyber Threat Intelligence)**: plataforma abierta para el intercambio de información de ciberseguridad que monitoriza, recopila y analiza potenciales ciberamenazas contra las organizaciones, facilitando el diseño de acciones defensivas y resolutivas. Cytomic Orion es compatible con la plataforma MISP (**http://www.misp-project.org/**) .

> *Accede la guía de integración en **https://www.vanimpe.eu/2020/03/10/integrating-misp-and-cytomic-orion/***

- **Ticketing**: herramientas que garantizan la correcta gestión de los indicios, permitiendo crear, asignar y seguir los casos hasta su cierre, así como la recogida de KPIs que muestren el grado de cumplimiento del servicio de seguridad del SOC. Cytomic Orion es compatible con Service Now (**https://www.serem.com/productos/servicenow/**).

> *Descarga la guía de integración desde **https://info.cytomicmodel.com/resources/guides/Orion/en/ORION-snowguide-EN.pdf***

- **App SOC**: son aplicaciones creadas en el SOC que utilizan la API de Cytomic Orion para resolver problemas concretos.
- **SIEM** (**Security Information and Event Management**): herramientas que combinan la gestión de la información y de los eventos de seguridad generados en la infraestructura IT del

cliente, proporcionando un análisis en tiempo real de las alertas de seguridad generadas por las aplicaciones y el hardware de red.

Tipos de APIs disponibles en Cytomic Orion

Los métodos accesibles por las aplicaciones del SOC o por las soluciones de terceros se agrupan en cinco categorías:

- **Consulta de indicios**: devuelve un listado de indicios de potenciales ataques registrados en la plataforma Cytomic Orion en el intervalo indicado.
- **Consulta de información de archivos y equipos**: devuelve información sobre la clasificación de los ficheros vistos en los equipos. También devuelve información de los propios dispositivos que forman parte de la infraestructura IT.
- **Gestión de IOCs**: recibe nuevos indicadores de compromiso que Cytomic Orion utilizará en su análisis del flujo de eventos generado por los equipos de la organización para detectar malware de nueva creación.
- **Herramientas de respuesta**: invoca mecanismos para resolver y minimizar el impacto de los potenciales ataques registrados en la plataforma Cytomic Orion.
- **Acceso a OsQuery** : envía sentencias OSQuery para obtener información de la infraestructura IT del cliente.
- **Investigaciones**: permite crear, modificar y borrar investigaciones.
- **Acceso a datos** : acceso al océano de datos, equivalente al módulo de consultas avanzadas SQL.

*Consulta **Especificación de la API de Cytomic Orion** para obtener información concreta de cada una de las APIs disponibles.*

Requisitos y acceso a las APIs de Cytomic Orion

Requisitos generales

Para poder utilizar las APIs de Cytomic Orion es necesario cumplir con siguientes requisitos:

- Acceso HTTPS por el puerto 443 al servidor **https://auth.pandasecurity.com/oauth/token** para autenticarse en el servidor OAuth de Cytomic Orion.
- Acceso HTTPS por el puerto 443 al servidor de la API **https://api.orion.cytomic.ai** para enviar las peticiones.

- Una cuenta de tipo aplicación creada en la consola de Cytomic Orion. Consulta **Habilitar el acceso a la API desde programas externos** para más información.
- Un desarrollo software que utilice la API de Cytomic Orion:
    - Una aplicación de móvil.
    - Una aplicación nativa.
    - Un aplicación web de cliente servidor o SPA (single-page application).
    - Un plugin que se ejecute en una solución de terceros.

Habilitar el acceso a la API desde programas externos

Para habilitar el acceso de la API de Cytomic Orion a una aplicación sigue los pasos mostrados a continuación:

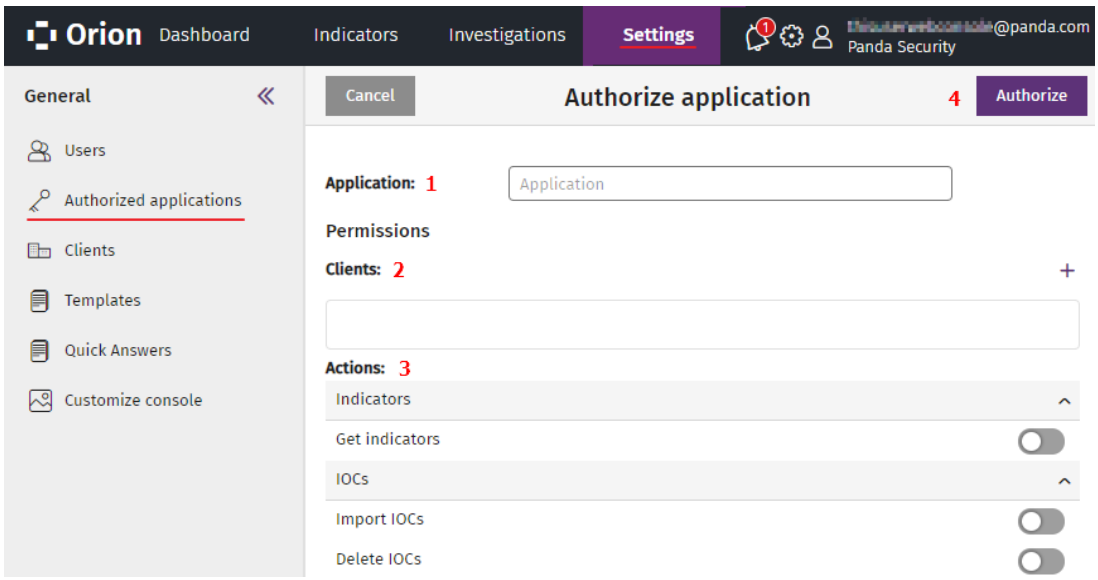


Figura 17.2: Ventana para habilitar el uso de la API por parte de una aplicación de terceros

- En el menú superior **Configuración**, panel lateral **Aplicaciones autorizadas** haz clic en el botón **Autorizar aplicación**. Se abrirá una ventana para introducir la información necesaria para validar la aplicación mediante el protocolo OAuth.
- Escribe en el campo **Aplicación (1)** el nombre del programa que accederá a la API. Este campo es descriptivo y no tiene efecto en el proceso aquí descrito.
- **Clientes (2)**: haz clic en el icono + para configurar los clientes del SOC de los cuales se recuperarán datos en cada llamada a la API de Cytomic Orion.
- **Acciones (3)**: indica las fuentes de información accesibles para la aplicación.
    - **Consultar indicios**: consulta **API de indicios**.
    - **Importación de IOCs**: consulta **Importar y buscar IOCs en la telemetría generada por los equipos del cliente**.

- **Borrado de IOCs**: consulta **Borrar IOCs importados en la plataforma**.
- **Búsqueda de IOCs**: consulta **Listar IOCs por atributos cargados en la plataforma**
- **Consultar información de un archivo, obtener los equipos en los que se ha visto y ver los detalles de los equipos**: consulta **API de conocimiento**.
- **Permitir aislar/quitar el aislamiento de equipos**: consulta **Aislar equipos** y **Quitar el aislamiento de equipos**.
- **Permitir reiniciar equipos**: consulta **Reinicio**.
- **Acceso a OSQuery**: consulta **API de acceso a OSQuery**.
- **Acceso a datos / Acceso a consultas avanzadas**: consulta **Obtener información del océano de datos**.

- Haz clic en el botón **Autorizar**. Cytomic Orion dará de alta la aplicación en la plataforma y mostrará el usuario y la contraseña generadas.
- Guarda en un sitio seguro la cadena de caracteres **Usuario**. Esta cadena se utilizará en las peticiones de la aplicación como contenido del campo `username`.
- Guarda el bloque de caracteres **Contraseña**. Este bloque deberá ser utilizado en las peticiones de la aplicación como contenido del campo `password`.

> *El bloque contraseña solo se muestra una vez en la consola de Cytomic Orion: cuando se crea la aplicación. Si pierdes la contraseña no será posible recuperarla y se requerirá borrar la aplicación y volverla a crear con otra contraseña diferente. Sigue este mismo procedimiento si la contraseña resulta comprometida.*

- Independientemente de las credenciales generadas en los campos `username` y `password`, el sistema de autenticación OAuth requiere indicar las siguientes credenciales de cliente:
  - **client_id**: aaf1461b714646a8a593197641df9665
  - **client_secret**: cnmB6rbT4xoZsnTzwHsgBpm1BtD-k_-1VKpZEl6blvM
  - **client_id**: **client_secret:** YWFmMTQ2MWI3MTQ2NDZhOGE1OTMxO

Una vez terminado el procedimiento, la aplicación necesitará autenticarse en la plataforma Cytomic Orion mediante el protocolo OAuth, descrito en **Cytomic Oriony autenticación OAuth**.

Cytomic Oriony autenticación OAuth

OAuth (Open Authorization) es un estándar abierto muy utilizado en la industria para permitir el acceso delegado a recursos protegidos. El principal escenario para el que OAuth fue diseñado es el de un usuario que necesita otorgar permisos de acceso a información protegida a sitios web o

aplicaciones de terceros, pero sin necesidad de compartir sus credenciales. Por lo tanto, OAuth proporciona un acceso delegado seguro a los recursos del propietario en su nombre, y especifica los procesos necesarios para que éste autorice el acceso a terceros sin compartir sus credenciales.

OAuth está diseñado específicamente para trabajar con el protocolo de transferencia de hipertexto (HTTP) y permite a un servidor de autorización emitir tokens de acceso a los programas de terceros con la aprobación del propietario del recurso.

Cytomic Orion utiliza el estándar OAuth para autenticar y autorizar las peticiones de las aplicaciones que acceden a las APIs que incorpora.

Conceptos básicos

Los conceptos mostrados a continuación son necesarios para comprender el funcionamiento del protocolo OAuth. Cytomic Orion utiliza un subconjunto de las funcionalidades incluidas en OAuth para regular el acceso a las APIs que expone a sus clientes.

- **API**: es el recurso a utilizar por las aplicaciones de terceros, y por lo tanto su acceso es controlado o protegido por OAuth.
- **Aplicación**: es la aplicación desarrollada por terceros que pide autorización para acceder al recurso protegido (la API). Para ello utiliza las credenciales asignadas a la cuenta de la aplicación.
- **Cuenta de la aplicación**: es la cuenta que posee el recurso cuyo acceso está controlado o protegido (la API). Consulta **Habilitar el acceso a la API desde programas externos** para crear el usuario y una contraseña de la aplicación.
- **Usuario y contraseña**: es el identificador de usuario y contraseña de la cuenta de la aplicación. Se corresponden con los parámetros `username` y `password` en el estándar OAuth. Consulta **Habilitar el acceso a la API desde programas externos** para crear el usuario y una contraseña de la aplicación.
- **Servidor de autenticación**: es el sistema que crea y valida las credenciales correspondientes a la cuenta de la aplicación, enviadas por las aplicaciones de terceros. Cytomic Orion delega en el servidor IdP (Cytomic Identity Provider) las tareas de validación de las credenciales `username` y `password`.
- **Client_id y client_secret**: es el identificador y la contraseña asignado al cliente de Cytomic Orion. Consulta **Habilitar el acceso a la API desde programas externos**.
- **Servidor de autorización**: es el servidor con el que la aplicación interactúa cuando solicita acceso a un recurso protegido. Cytomic Orion delega en el servidor CAS (Cytomic Authorization Server) esta tarea. Para regular el acceso, el servidor CAS recibe de la aplicación el `client_id` y `client_secret` y le entrega un token de duración limitada que describe su ámbito de acceso.

- **Token de acceso**: es la cadena de caracteres utilizada por la aplicación para acceder al recurso protegido (la API). El token de acceso describe el ámbito de acceso, la duración y otra información relevante. Los tokens son opacos para la aplicación cliente, son emitidos por el servidor CAS y solo tienen significado para éste.
- **Token de refresco**: cuando la aplicación accede al recurso por primera vez se le entrega un token de acceso y un token de refresco. Cuando el token de acceso caduca, la aplicación solicita uno nuevo mediante el token de refresco sin necesidad de volver a iniciar el proceso de autenticación y autorización.

Flujo de datos OAuth

La aplicación tiene que obtener un token de acceso antes de utilizar cualquier API en Cytomic Orion. Para ello es necesario intercambiar cierta información con el servidor CAS.

Protocolo utilizado en el intercambio de datos

OAuth utiliza el protocolo HTTPS para intercambiar flujos de información entre la aplicación y el servidor CAS para conseguir la autorización sobre las APIs de Cytomic Orion. En este intercambio de datos se utiliza el comando POST del protocolo HTTP. Por razones de seguridad todos los comandos enviados y las respuestas obtenidas viajan cifrados mediante HTTPS.

Tipo de acceso soportado por el servidor CAS y datos requeridos

El protocolo OAuth soporta varios tipos autenticación y autorización dependiendo de las características de la aplicación desarrollada que accederá a la API de Cytomic Orion. En el caso particular de Cytomic Orion, el tipo de acceso permitido por el servidor CAS será "`password`", que deberá ser indicado en el parámetro "`grant_type`" de la petición inicial de la aplicación.

Con el `grant_type` `password`, el servidor CAS requiere los siguientes datos para permitir el acceso a la API de Cytomic Orion para una aplicación registrada:

- **Usuario y Contraseña**: es el identificador de la cuenta de la aplicación y su contraseña, creada en la consola Cytomic Orion. Consulta **Habilitar el acceso a la API desde programas externos**.
- **Client_id, Client_secret**: es el identificador del cliente y su contraseña. Consulta **Habilitar el acceso a la API desde programas externos**.

Flujos de información generados para autorizar un acceso

El esquema de comunicación en la fase de autenticación entre la aplicación y el servidor CAS es el siguiente:

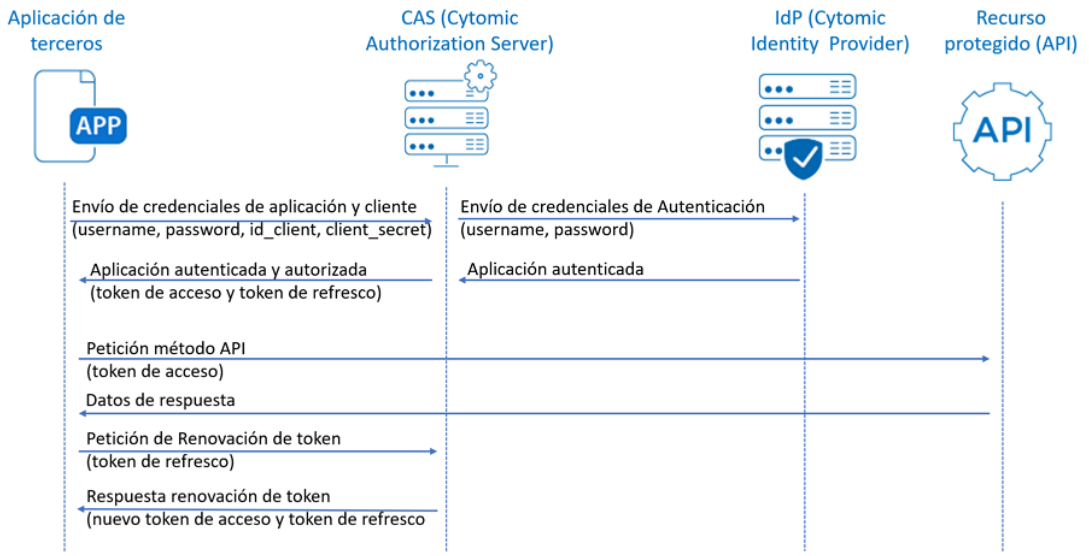


Figura 17.3: Esquema de comunicación OAuth entre una aplicación y el servidor CAS

En la figura se muestra un intercambio de datos OAuth completo:

- La aplicación envía sus credenciales y las del cliente al servidor CAS. El servidor CAS valida las credenciales de la aplicación en el servidor IdP y si es correcto comprueba las credenciales del cliente para generar y emitir un token de acceso y un token de refresco.
- Con el token de acceso la aplicación accede a la API de Cytomic Orion y recupera los datos requeridos.
- Una vez que el token de acceso caduca el servidor CAS lo rechaza. La aplicación envía el token de refresco para recuperar un nuevo token de acceso y de refresco.

Autenticación, autorización y obtención del token de acceso

Petición del token de autorización por parte de la aplicación

La aplicación envía un comando HTTPS POST al servidor CAS **https://auth.pandasecurity.com** con los parámetros siguientes:

```
POST /oauth/token HTTP/1.1
Host: auth.pandasecurity.com
Content-Type: application/x-www-form-urlencoded; charset=utf-8

grant_type =password
&client_id ={CLIENT_ID}
&client_secret = {CLIENT_SECRET}
&username = {USER_NAME}
&password = {USER_PASSWORD}
&scope ={SCOPE}
```

Alternativamente se puede utilizar una cabecera de tipo `Authorization` para indicar el `client_id` y `client_secret` codificado como base64:

```
POST /oauth/token HTTP/1.1
Host: auth.pandasecurity.com
Content-Type: application/x-www-form-urlencoded; charset=utf-8
Authorization: Basic client_id:client_secret.

grant_type=password
&username={USER_NAME}
&password={USER_PASSWORD}
&scope={SCOPE}
```

El significado de los parámetros es el siguiente:

Parámetro	Descripción
grant_type	Requerido. Establece el valor a "`password`". Indica que la aplicación será la que proveerá directamente las credenciales de la cuenta de la aplicación al que pertenece el recurso protegido.
client_id	Requerido. Es el identificador del cliente de Cytomic Orion al que pertenece la aplicación.
client_secret	Requerido. Es la contraseña del cliente de Cytomic Orion al que pertenece la aplicación.
username	Requerido. El nombre de la cuenta de la aplicación creada en la consola de Cytomic Orion. Consulta **Habilitar el acceso a la API desde programas externos**
password	Requerido. La contraseña de la cuenta de la aplicación creada en la consola de Cytomic Orion. Consulta **Habilitar el acceso a la API desde programas externos**
scope	Ámbito del acceso. Establece el valor a "`orion.api`".

Tabla 17.1: Parámetros requeridos por el servidor CAS para obtener el token de acceso

Respuesta correcta del servidor CAS

La respuesta es un objeto JSON con el token de acceso y otros datos:

```
HTTP/1.1 200
{
"access_token":"{ACCESS_TOKEN}",
"refresh_token":"{REFRESH_TOKEN}",
"expires_in":{EXPIRATION_TIME},
```

```
"token_type":{TOKEN_TYPE}
}
```

El significado de los campos es el siguiente:

Campo	Descripción
access_token	Token de acceso compuesto por una cadena de caracteres codificada en base64.
refresh_token	Token de refresco compuesto por una cadena de caracteres codificada en base64.
expiration_ time	Tiempo en segundos que durará el token de acceso.
token_type	Por defecto "bearer". Indica que se trata de un token autocontenido y que por tanto contiene todos los recursos necesarios para autorizar el acceso. El servidor CAS emite tokens de acceso JWT (Json Web Token) firmados.

Tabla 17.2: Respuesta del servidor CAS con el token de acceso y de refresco

Respuesta errónea del servidor CAS

El servidor no ha conseguido generar un token válido con la información suministrada:

```
HTTP/1.1 400 Bad request
{
"error":"{ERROR_CODE}",
"error_description":"{ERROR_DESC}"
"error_uri":"{ERROR_URI}"
}
```

El significado de los campos es el siguiente:

Campo	Descripción
error	Código de error: consulta la tabla **Códigos de retorno**.
error_ description	Descripción breve del error. El contenido de este campo no está preparado para ser mostrado directamente al usuario de la aplicación. En su lugar, se deberán adecuar las descripciones de los mensajes en función de la aplicación.

Campo	Descripción
error_uri	Opcional.

Tabla 17.3: Respuesta errónea del servidor CAS

Refresco de un token de acceso caducado

Debido a que el ámbito de acceso de una aplicación puede cambiar a lo largo del tiempo, el token de acceso que utiliza para acceder a la API de Cytomic Orion tiene una caducidad de 20 minutos, transcurridos los cuales la API de Cytomic Orion lo rechazará impidiendo el acceso al recurso. Para evitar el envío de los parámetros indicados en **Autenticación, autorización y obtención del token de acceso** cada vez que el token de acceso caduca, la aplicación envía al servidor CAS el token de refresco. De esta manera, el token de refresco es una referencia a las condiciones originales que propiciaron la autorización de la aplicación en el servidor CAS; si éstas condiciones no han variado, el servidor CAS volverá a enviar un token de acceso a la aplicación. El token de refresco tiene un tiempo de vida superior al token de acceso.

Envío del token de refresco

La aplicación envía al servidor CAS **auth.pandasecurity.com** un comando HTTPS POST con los parámetros siguientes:

```
POST /oauth/token HTTP/1.1
Host: auth.pandasecurity.com
Content-Type: application/x-www-form-urlencoded; charset=utf-8

grant_type = refresh_token
&refresh_token = {REFRESH_TOKEN}
&client_id = {CLIENT_ID}
&client_secret = {CLIENT_SECRET}
&scope = {ORIGINAL_SCOPE}
```

El significado de los parámetros es el siguiente:

Parámetro	Descripción
grant_type	Requerido. Establece el valor a `refresh_token` para indicar que la aplicación envía un token de refresco esperando a cambio del CAS un nuevo token de acceso.
refresh_token	Token de refresco necesario para que el servidor CAS genere un nuevo token de acceso.
client_id	Requerido. Es el identificador del cliente de Cytomic Orion.

Parámetro	Descripción
client_secret	Requerido. Es la contraseña del cliente de Cytomic Orion.
scope	Opcional. Si no se incluye, el servidor CAS devolverá un token de acceso con el mismo ámbito que la petición original. Si se incluye deberá contener el mismo ámbito que la petición original.

Tabla 17.4: Parámetros requeridos por el servidor CAS para obtener un nuevo token de acceso

Respuesta correcta del servidor CAS

La respuesta del servidor CAS a la aplicación es la misma que se generó en la petición original por el token de acceso. El servidor CAS puede incluir un nuevo token de refresco que será utilizado en la siguiente renovación del token de acceso. Si el servidor CAS no incluye un nuevo token de refresco se asume que el anterior sigue siendo válido.

Respuesta errónea del servidor CAS

El servidor no ha conseguido generar un token válido con la información suministrada:

```
HTTP/1.1 400 Bad request
{
"error":"invalid_request"
}
```

Códigos de error

Código	Descripción
200	Operación completada con éxito.
400	Error.

Tabla 17.5: Códigos de retorno

Mensajes de error

Código de error	Descripción
unrecognized_client_id	El identificador del cliente es erróneo o no existe. Contacta con el departamento de soporte de Cytomic.
unrecognized_client_secret	La contraseña del cliente es errónea o no se corresponde con el `client_id` enviado. Contacta con el departamento de soporte de Cytomic.

Código de error	Descripción
unauthorized_ client	El cliente está autenticado pero no está autorizado para hacer la petición.
invalid_client	Cualquier otro error relativo a la validación de las credenciales del cliente. Contacta con el departamento de soporte de Cytomic.
unsupported_ grant_type	El `grant_type` enviado no está soportado. Utiliza "`password`".
invalid_grant	El token de acceso recibido no es válido (no se reconoce o ha caducado) o la aplicación no tiene autorización para acceder a la API.
invalid_scope	El scope recibido no es correcto. Este parámetro siempre debe ser "`orion.api`".
access_denied	Usuario o contraseña erróneos.
invalid_request	La petición contiene un parámetro incompatible o no contiene todos los parámetros requeridos.
temporarily_ unavailable	El servidor CAS no puede procesar la petición debido a una sobrecarga temporal o a un proceso de mantenimiento.
server_error	Error interno del servidor.

Tabla 17.6: Mensajes de error en el proceso de autorización

Ejemplo para obtener un token de acceso y de refresco del servidor CAS

El ejemplo mostrado a continuación construye la llamada al servidor CAS con los parámetros `username`, `password`, `client_id`, `client_secret`, `grand_type` y `scope` apropiados para recuperar el token de acceso y el token de refresco necesarios para posteriores llamaras a la API de Cytomic Orion.

```
#utiliza la librería requests para conectar con el servidor OAuth
import requests
from requests.auth import HTTPBasicAuth
#establece el client_id, client_secret, username, password y scope
client_id = 'aaf1461b7a8a593199665'
```

```
client_secret = 'YaDzUdHmlrivXYaAFhJDFiNe5x0mI4'
username = '7e0aa013282249cdebd15a08f84d'
password = '
jEshWDjjS2h6bCxrZKCy8iVbBHNcCzMxxUe362CfUwz0eAKXRdlz9uOuVzFp
3g'
grant_type = 'password'
token_url = 'https://auth.pandasecurity.com/oauth/token'
scope = 'orion.api'
headers = {
       'Content-Type': 'application/x-www-form-urlencoded',
}
#configura el cuerpo del mensaje HTTP. Las credenciales del
client_id y
#client_secrent se establecen en las cabeceras del mensaje
body = {
       'username': username,
       'password': password,
       'scope': scope,
       'grant_type': 'password'
}
#codifica el client_id y client_password en base64 y lanza
la petición HTTPS
r = requests.post(token_url, auth=HTTPBasicAuth(client_id,
client_secret),
headers=headers, data=body, verify=False)
#si no hay errores convierte el cuerpo de la respuesta en un JSON para
facilitar #el acceso
if r.status_code==200:
       data = r.json()
#carga el token de acceso y de refresco en las variables
       token_access=data['access_token']
       token_refresh=data['refresh_token']
```

Ejemplo de uso del token de acceso y token de refresco

Todas las llamadas a la API de Cytomic Orion deben de incorporar en las cabeceras HTTP el token de acceso obtenido tras el proceso de autenticación y autorización. Sin embargo, transcurridos 20 minutos de la emisión del token de acceso, éste caduca y es necesario obtener uno nuevo a través del token de refresco. Por esta razón, es necesario comprobar en cada llamada a la API de Cytomic Orion que no devuelve un error de token inválido. Si éste es el caso solicita un nuevo token de acceso y reintenta la petición con el nuevo token.

```
#llamada de ejemplo a la API de indicios
#establece los parámetros necesarios
alert_from='1572595090000' #desde 1/11/2019
alert_to='1575187090000' #hasta 1/12/2019

#prepara la cabecera HTTP con el token de acceso para lanzar la llamada a la
API
```

```
h_request = {
        'Authorization': f'Bearer {token_access}',
        'Accept': 'application/json'
}


url_                alert                                   =
f'https://api.orion.cytomic.ai/api/v1/applications/alerts/
{alert_from}/{alert_to}'
r = requests.get(url_alert, headers=h_request, verify=False)
#una vez autenticado comprueba en cada llamada si el token
de acceso caducó
if r.status_code==401:
        body_refresh = {
        'grant_type':'refresh_token',
                'refresh_token':token_refresh,
                'client_id':client_id,
                'client_secret':client_secret,
        }
        #pide un nuevo token de acceso y refresco
        r    =    requests.post (token_ url,    headers=headers,
data=body_refresh,verify=False)
        data = r.json()
        #actualiza las variables con el nuevo token de acceso
y refresco
        token_access=data['access_token']
        token_refresh=data['refresh_token']
```

Especificación de la API de Cytomic Orion

Todas las llamadas a la API de Cytomic Orion deben de incluir el token de acceso obtenido en ***Autenticación, autorización y obtención del token de acceso*** *mediante la cabecera Authorization: Bearer {token}.*

En este apartado se incluyen las diferentes llamadas a la API de Cytomic Orion, su sintaxis, significado de los parámetros y su formato, así como los resultados devueltos.

Cytomic Orion utiliza una interface REST para intercambiar información entre la plataforma y las aplicaciones de terceros: El protocolo para el transporte de mensajes entre ambos extremos es HTTPS y para encapsular los tipos de datos complejos utiliza el estándar JSON.

Esquema general de una llamada

En cada llamada a la API de Cytomic Orion, la aplicación de terceros necesitará especificar algunos o todos los parámetros mostrados a continuación:

- **Tipo de método HTTPS**: comando HTTP utilizado en la petición:
  - **GET**: la llamada realiza una petición de información pasando los parámetros únicamente en la URL.
  - **POST**: la llamada realiza una petición de información pasando los parámetros en el cuerpo del mensaje HTTP y opcionalmente en la URL.
- **URL**: ruta relativa al recurso. Como parte de la ruta se incluyen los parámetros indicados mediante llaves en la especificación. Los parámetros opcionales se indican mediante el formato "query string".
- **Cuerpo**: hace referencia a la zona del mensaje HTTP donde se incluyen los datos, localizada después de las cabeceras. Contiene los parámetros de tipos complejos en las llamadas POST.
- **Código de retorno HTTP**: indica si la llamada tuvo éxito o terminó de forma errónea. Consulta **Códigos de retorno** para obtener un listado de los códigos devueltos por cada llamada a la API de Cytomic Orion.

Tipos de datos

La mayor parte de los parámetros son de tipo entero o cadena de caracteres. Estos parámetros pueden viajar en la llamada tanto en la ruta de la URL como en formato `querystring`. En la respuesta van incluidos en el cuerpo del mensaje.

Todos los parámetros de tipo fecha requieren el formato Unix Timestamp en milisegundos. Si el analista introduce una fecha en segundos, Cytomic Orion la convierte automáticamente al formato milisegundos.

Tanto en la llamada como en la respuesta, para los tipos de datos más complejos se utilizan listas de uno a "n" elementos de tipo JSONs en el cuerpo del mensaje HTTP.

Códigos de retorno

Los códigos de retorno son comunes a todas las llamadas y se indican en la cabecera `status` del mensaje HTTP, con el formato `status: código`:

Código	Descripción
200	Operación completada con éxito.
400	Parámetro mal formado o ausente.
401	Fallo en el proceso de autenticación.
403	Fallo en el proceso de autorización.

Tabla 17.7: Códigos de retorno

API de IOCs

Gestiona en la plataforma Cytomic Orion los identificadores de compromiso (IOCs) obtenidos de fuentes externas.

Importar y buscar IOCs en la telemetría generada por los equipos del cliente

Carga uno o más IOCs de un mismo tipo en la plataforma, los cuales podrán configurarse para realizar dos tipos de búsquedas:

- **Búsqueda retrospectiva (opcional)**: busca una única vez el IOC en el flujo de eventos generado por los equipos del cliente y acumulado durante el último año desde el momento de la importación. Esta búsqueda genera un único indicio en la consola por cada equipo / IOC encontrado.
- **Búsqueda en streaming**: busca el IOC desde el momento de la carga del IOC en la plataforma, generando un indicio en la consola por cada equipo / IOC / hora. La búsqueda terminará cuando se cumpla el tiempo indicado en el campo TTL. Este tipo de búsqueda se realiza sobre la información generada por los procesos en ejecución de los equipos del cliente.

Petición

Comando	POST
URL	/api/v1/applications/iocs/{iocType}

Parámetros requeridos en la URL	• **iocType**: indica el tipo de los IOCs a importar. Todos los IOCs importados en una misma llamada tienen que ser del mismo tipo.
	  • **Hash**: el JSON con la descripción del IOC a importar contiene un md5 del fichero que representa una amenaza.
	  • **Url**: el JSON con la descripción del IOC a importar contiene la URL a la que accede la amenaza. Es necesario incluir el protocolo en la URL, por ejemplo: **https://www.google.com/test**.
	  • **IP**: el JSON con la descripción del IOC a importar contiene la dirección IP (origen o destino) de la comunicación establecida por la amenaza.
	  • **Domain**: el JSON con la descripción del IOC a importar contiene el dominio (origen o destino) de la comunicación establecida por la amenaza.

Parámetros opcionales en la URL por	• **retrospective**: ejecuta una única búsqueda sobre todos los eventos almacenados por Cytomic y generados por los equipos del SOC hasta la fecha.

querystring	
Parámetros requeridos en el cuerpo del mensaje HTTP	Lista de JSONs con la descripción de los IOCs. Solo se puede incluir en el JSON uno de los parámetros mostrados a continuación. Todos los IOCs tienen que ser del mismo tipo. Los campos posibles del JSON son: • **hash**: md5 del fichero que contiene la amenaza. • **url**: URL solicitada por la amenaza. • **ip**: dirección IP (origen o destino) de la comunicación establecida por la amenaza. • **domain**: dominio (origen o destino) de la comunicación establecida por la amenaza. • **additionalData**, **source**, **policy**, **description**: campos descriptivos del IOC. No utilizados por la plataforma. • **daysToExpiration**: número de días que permanecerán los IOCs en la plataforma, pasados los cuales serán eliminados junto a sus búsquedas asociadas.
Cabeceras	• **Accept**: application/json • **Content-Type**: application/json-patch+json

Tabla 17.8: Formato de la llamada para importar IOCs

Respuesta

Campo del JSON	Descripción
success	"true"
message	**"n {iocType} added"**: indica el número de IOCs cargados con éxito en la plataforma y su tipo.
error	"null"
PandaAlertId	Identificador interno asignado al IOC.

Tabla 17.9: JSON de respuesta a la carga de IOCs con éxito

Borrar IOCs importados en la plataforma

Elimina los IOCs previamente importados en la plataforma, interrumpiendo a su vez las búsquedas en streaming y retrospectivas en curso.

Petición

Comando	POST
URL	/api/v1/applications/iocs/{iocType}/eraser/

Parámetros requeridos en la URL	• **iocType**: indica el tipo de los IOCs a borrar. Todos los IOCs borrados en una misma llamada tienen que ser del mismo tipo.
	  • **Hash**: el JSON con la descripción del IOC a borrar contiene un md5 del fichero.
	  • **Url**: el JSON con la descripción del IOC a borrar contiene una URL.
	  • **IP**: el JSON con la descripción del IOC a borrar contiene la dirección IP (origen o destino) de una comunicación.
	  • **Domain**: el JSON con la descripción del IOC a borrar contiene el dominio (origen o destino) de una comunicación establecida.

Parámetros requeridos en el cuerpo del mensaje HTTP	Lista de JSONs con la descripción de los IOCs a borrar. Solo se puede incluir en el JSON uno de los parámetros mostrados a continuación. Todos los JSONs tienen que ser del mismo tipo. Los campos posibles del JSON son: • **hash**: md5 un fichero. • **url**: URL . • **ip**: dirección IP (origen o destino) de una comunicación. • **domain**: dominio (origen o destino) de una comunicación. • **additionalData**, **source**, **policy**, **description**: campos descriptivos del IOC. No utilizados por la plataforma.
Cabeceras	• **Accept**: application/json • **Content-Type**: application/json-patch+json

Tabla 17.10: Formato de la llamada para borrar IOCs

Respuesta

Campo del JSON	Descripción
success	"true"
message	**"n {iocType} deleted"**: indica el número de IOCs borrados con éxito en la plataforma y su tipo.
error	"null"

Campo del JSON	Descripción
PandaAlertId	Identificador interno asignado al IOC.

Tabla 17.11: JSON de respuesta al borrado IOCs con éxito

Listar IOCs por atributos cargados en la plataforma

Muestra la lista de IOCs cargada en la plataforma según sus atributos y cuándo fueron importados.

Petición

Comando	POST
URL	/api/v1/applications/iocs/{iocType}/getter/

Parámetros requeridos en la URL	• **iocType**: indica el tipo de los IOCs a listar.
	  • **Hash**: el JSON con la descripción del IOC a listar contiene un md5 del fichero.
	  • **Url**: el JSON con la descripción del IOC a listar contiene una URL.
	  • **IP**: el JSON con la descripción del IOC a listar contiene la dirección IP (origen o destino) de una comunicación.
	  • **Domain**: el JSON con la descripción del IOC a listar contiene el dominio (origen o destino) de una comunicación establecida.

Parámetros requeridos en el cuerpo del mensaje HTTP	Colección de JSONs con la descripción de los IOCs a listar. Solo se puede incluir en el JSON uno de los parámetros mostrados a continuación. Todos los JSONs tienen que ser del mismo tipo especificado en el campo iocType. Los campos posibles del JSON son: • **hash**: md5 un fichero. • **url**: URL . • **ip**: dirección IP (origen o destino) de una comunicación. • **domain**: dominio (origen o destino) de una comunicación.
Cabeceras	• **Accept**: application/json • **Content-Type**: application/json-patch+json

Tabla 17.12: Formato de la llamada para listar IOCs por característica

Respuesta

Campo del JSON	Descripción
IocType	Indica el tipo de los IOCs listados. • **Hash**: el JSON con la descripción del IOC listado contiene un md5 del fichero. • **Url**: el JSON con la descripción del IOC listado contiene una URL. • **IP**: el JSON con la descripción del IOC listado contiene la dirección IP (origen o destino) de una comunicación. • **Domain**: el JSON con la descripción del IOC listado contiene el dominio (origen o destino) de una comunicación establecida.
KeyValueAsString	Valor del IOC.
IocJson	• **hash**: md5 un fichero. • **url**: URL . • **ip**: dirección IP (origen o destino) de una comunicación. • **domain**: dominio (origen o destino) de una comunicación. • **DaysToExpiration**: número de días que el IOC permanecerá en la plataforma. • **additionalData**, **source**, **policy**, **description**: campos descriptivos del IOC. No utilizados por la plataforma.
DeploymentDateUTC	Fecha en la que el IOC se cargó en la plataforma.
ExpirationDateUTC	Fecha en la que el IOC será borrado por la plataforma.
LastRetroScanUTC	Fecha en la que es inició una búsqueda retrospectiva por ultima vez con el IOC.
PandaAlertId	Identificador interno asignado al IOC.

Tabla 17.13: JSON de respuesta a la llamada para listar IOCs

Listar IOCs por fecha de carga en la plataforma

Muestra la lista de IOCs cargados en la plataforma según su fecha de publicación.

Petición

Comando	GET
URL	/api/v1/applications/iocs/{iocType}

Parámetros requeridos en la URL	• **iocType**: indica el tipo de los IOCs a listar.
	  • **Hash**: lista IOCs que especifican un md5.
	  • **Url**: lista IOCs que especifican una URL.
	  • **IP**: lista IOCs que especifican un dirección IP (origen o destino) de una comunicación.
	  • **Domain**: lista IOCs que especifican un dominio (origen o destino) de una comunicación establecida.

Parámetros requeridos en el cuerpo del mensaje HTTP	• **from**: timestamp Unix en milisegundos con la fecha inferior del intervalo de IOCs a listar.
	• **to**: timestamp Unix en milisegundos con la fecha superior del intervalo de IOCs a listar.
	• **includeDeleted**: filtra el listado de IOCs según su pertenencia o no a una regla de eliminación.
	  • **True**: el IOC pertenece a una regla de eliminación.
	  • **el IOC no pertenece a una regla de eliminación.**

Cabeceras	**Accept**: application/json

Tabla 17.14: Formato de la llamada para listar IOCs por fecha de carga en la plataforma

Respuesta

Campo del JSON	Descripción
IocType	Indica el tipo de los IOCs listados. • **Hash**: el JSON con la descripción del IOC listado contiene un md5 del fichero. • **Url**: el JSON con la descripción del IOC listado contiene una URL. • **IP**: el JSON con la descripción del IOC listado contiene la dirección IP (origen o destino) de una comunicación. • **Domain**: el JSON con la descripción del IOC listado contiene el dominio (origen o destino) de una comunicación establecida.
KeyValueAsString	Valor del IOC.

Campo del JSON	Descripción
IocJson	• **hash**: md5 un fichero. • **url**: URL . • **ip**: dirección IP (origen o destino) de una comunicación. • **domain**: dominio (origen o destino) de una comunicación. • **DaysToExpiration**: número de días que el IOC permanecerá en la plataforma. • **additionalData**, **source**, **policy**, **description**: campos descriptivos del IOC. No utilizados por la plataforma.
DeploymentDateUTC	Fecha en la que el IOC se cargó en la plataforma.
ExpirationDateUTC	Fecha en la que el IOC será borrado por la plataforma.
LastRetroScanUTC	Fecha en la que es inició una búsqueda retrospectiva por ultima vez con el IOC.
PandaAlertId	Identificador interno asignado al IOC.

Tabla 17.15: JSON de respuesta a la llamada para listar IOCs por fecha de carga en la plataforma

Búsqueda retrospectiva de un IOC

Busca patrones en los eventos generados hasta la fecha por los equipos de los clientes del SOC, y devuelve una lista de JSONs con los IOCs encontrados. La llamada a este método tiene un tiempo de ejecución máximo de 90 segundos y mostrará todos los resultados encontrados al final de la búsqueda. Si transcurrido el tiempo máximo, Cytomic Orion no ha podido recuperar todas la amenazas disponibles, la conexión se interrumpirá sin devolver ningún resultado.

Petición

Comando	POST
URL	/api/v1/applications/iocs/{iocType}/retrospectivesearcher

Parámetros requeridos en la URL	• **iocType**: indica el tipo de los IOCs a buscar. Todos los IOCs en una misma llamada tienen que ser del mismo tipo.
	  • **FileHash**: el JSON con la descripción del IOC a buscar contiene un md5 del fichero que representa una amenaza.
	  • **Url**: el JSON con la descripción del IOC a buscar contiene una URL

	pedida por la amenaza. • **IP**: el JSON con la descripción del IOC a buscar contiene la dirección IP (origen o destino) de la comunicación establecida por la amenaza. • **Domain**: el JSON con la descripción del IOC a buscar contiene el dominio (origen o destino) de la comunicación establecida por la amenaza.
Parámetros requeridos en el cuerpo del mensaje HTTP	Lista de JSONs con la descripción de los IOCs. Solo se puede incluir en el JSON uno de los parámetros mostrados a continuación. Todos los JSONs tienen que ser del mismo tipo. Los campos posibles del JSON son: • **hash**: md5 del fichero que contiene la amenaza. • **url**: URL solicitada por la amenaza. • **ip**: dirección IP (origen o destino) de la comunicación establecida por la amenaza. • **domain**: dominio (origen o destino) de la comunicación establecida por la amenaza. • **additionalData**, **source**, **policy**, **description**: campos descriptivos del IOC. No utilizados por la plataforma.
Cabeceras	• **Accept**: application/json • **Content-Type**: application/json-patch+json

Tabla 17.16: Formato de la llamada para ejecutar una búsqueda retrospectiva

Respuesta

Lista de JSONs con la descripción de los atributos de los IOCs encontrados

Campo del JSON	Descripción
MUID	Identificador del equipo dentro de Cytomic Orion.
clientid	Identificador del cliente.
firstSeen	Fecha de la primera aparición del IOC en el equipo del cliente.
lastSeen	Fecha de la ultima aparición del IOC en el equipo del cliente.
ioc	Descripción del IOC encontrado. • **iockey**: valor del IOC. • **type**: tipo del IOC (FileHash, Url, IP, Domain).

Campo del JSON	Descripción
	• **source**, **policy**, **description**: campos descriptivos introducidos en la importanción del IOC.
PandaAlertId	Identificador interno asignado al IOC.

Tabla 17.17: JSON de respuesta a la ejecución de una búsqueda retrospectiva

Listado de IOCs en la consola de Cytomic Orion

Para mostrar en la consola los IOCs cargados haz clic en el menú superior **Configuración**, panel lateral **IOCs**. Se mostrará un listado con información equivalente a la ofrecida en la respuesta de las llamadas a la API para listar los IOCs cargados en la plataforma. Consulta **Listar IOCs por atributos cargados en la plataforma** o **Listar IOCs por fecha de carga en la plataforma**.

Campo	Descripción
Tipo IOC	Tipo del dato indicado en el campo **Valor IOC**. Coincide con el contenido del parámetro **iocType** de la API.
Valor IOC	Valor utilizado en la búsqueda del IOC. Coincide con el contenido del parámetro **KeyValueAsString** de la API.
Fecha de importación	Fecha en la que se creó el IOC. Coincide con el contenido del parámetro **DeploymentDateUTC** de la API.
Fecha de exploración	Fecha en la que se borrará el IOC de la plataforma. Coincide con el contenido del parámetro **ExpirationDateUTC**.
Datos adicionales	Coincide con el contenido del parámetro **additionalData** de la API.
Fuente	Coincide con el contenido del parámetro **source** de la API.
Política	Coincide con el contenido del parámetro **policy** de la API.
Descripción	Coincide con el contenido del parámetro **description** de la API.

Tabla 17.18: Campos del listado IOCs

Ejemplos de llamadas a la API de IOCs

El siguiente ejemplo carga varios IOCs que identifican el tráfico origen o destino de redes C2C (Command & Control), comprueba que están cargados, ejecuta una búsqueda retrospectiva y los borra.

Al cargar la lista de IOCs, Cytomic Orion ejecutará una única búsqueda retrospectiva en la telemetría almacenada durante último año y generará indicios en caso de encontrar amenazas que coincidan con los IOCs cargados. Además, continuará buscando en el stream de eventos producidos hasta que se cumpla la fecha de caducidad del IOC (10 días).

```
#tipo de IOC
iocType='IPIoc'
#datos de los IOCs
ioc_data=[{'ip':'192.168.0.1'},{'ip':'192.168.0.2'},{'ip':'192.168.0.3'}]
#cabeceras para la llamada a la API incluyendo el token de acceso
h_request_ioc = {
       'Authorization': f'Bearer {token_access}',
       'Accept': 'application/json',
       'Content-Type': 'application/json-patch+json'
}
#Objetivo: cargar en el servidor 3 IOCS de tipo IP (IPIoC)
#activar búsqueda retrospectiva
retrospective=True
#URL de la llamada
url_ioc_add = f'https://api.orion.cytomic.ai/api/v1/applications/iocs/{iocType}?retrospective={retrospective}'
#devuelve un JSON con el número de IOC cargados con éxito
r = requests.post(url_ioc_add, headers=h_request_ioc, json=ioc_data, verify=False)
ioc_add=r.json()
 #Objetivo: comprobar los IOCs cargados en la plataforma
#URL de la llamada
url_ioc_list = f'https://api.orion.cytomic.ai/api/v1/applications/iocs/{iocType}/getter/'
r = requests.post(url_ioc_list, headers=h_request_ioc, json=ioc_data, verify=False)
#devuelve un JSON con la definición de los IOCs cargados del tipo indicado y su
#fecha de carga
iocs_list=r.json()
#Objetivo: inicia una búsqueda retrospectiva de una lista de IOCs
#URL de la llamada
url_ioc_search = f'https://api.orion.cytomic.ai/api/v1/applications/iocs/{iocType}/retrospectivesearcher/'
r = requests.post(url_ioc_search, headers=h_request_ioc, json=ioc_data, verify=False)
#devuelve una lista de JSONs con los IOCs encontrados en el parque del cliente
iocs_found=r.json()
#Objetivo: borra los IOCs previamente cargados
```

```
#URL de la llamada
url_ioc_del = f'https://api.orion.cytomic.ai/api/v1/applications/iocs/{iocType}/eraser/'
#devuelve un JSON con el número de IOCs borrados con éxito
r = requests.post(url_ioc_del, headers=h_request_ioc, json=ioc_data, verify=False)
ioc_del=r.json()
```

API de conocimiento

Obtiene datos sobre los equipos que pertenecen a la infraestructura IT del cliente y sobre los ficheros que almacenan.

Obtener las características de un fichero

Obtiene la clasificación de un fichero asignada por Cytomic a partir de su MD5 y otra información.

Petición

Comando	GET
URL	/api/v1/applications/forensics/md5/{md5}/info
Parámetros requeridos en la URL	**md5**: hash del fichero.
Cabeceras	**Accept**: application/json

Tabla 17.19: Formato de la llamada para obtener información de un fichero

Respuesta

JSON con la descripción de los atributos del fichero.

Campo del JSON	Descripción
filename	Nombre del fichero.
filesize	Tamaño del fichero en bytes.
lastSeen	Fecha en la que el fichero fue registrado por última vez en el conocimiento global de Cytomic.
firstSeen	Fecha en la que el fichero fue registrado por primera vez en el conocimiento global de Cytomic.
classification	Valor del enumerado indicado en el campo `classificationName`.

Campo del JSON	Descripción
classificationName	Clasificación del fichero generada por Cytomic EDR: • **-1**: Unknown • **0**: Unknown • **1**: Goodware • **2**: Malware • **3**: Suspct • **4**: Compromised • **5**: GWNotConfirmed • **6**: Pup • **7**: GwUnwanted • **8**: GwRanked

Tabla 17.20: Campos del JSON con los atributos del fichero

Obtener las características de varios ficheros

Obtiene la clasificación de una lista de ficheros asignada por Cytomic a partir de su MD5 y otra información.

Petición

Comando	POST
URL	/api/v1/forensics/md5/batch/sample
Cabeceras	• **Accept**: application/json • **Content-Type**: application/json-patch+json

Tabla 17.21: Formato de la llamada para obtener información de una lista de ficheros

Respuesta

Lista de JSONs con la descripción de los atributos de los ficheros.

Campo del JSON	Descripción
filename	Nombre del fichero.
filesize	Tamaño del fichero en bytes.

Campo del JSON	Descripción
lastSeen	Fecha en la que el fichero fue registrado por última vez en el conocimiento global de Cytomic.
firstSeen	Fecha en la que el fichero fue registrado por primera vez en el conocimiento global de Cytomic.
classification	Valor del enumerado indicado en el campo `classificationName`.
classificationName	Clasificación del fichero generada por Cytomic EDR: • **-1**: Unknown • **0**: Unknown • **1**: Goodware • **2**: Malware • **3**: Suspct • **4**: Compromised • **5**: GWNotConfirmed • **6**: Pup • **7**: GwUnwanted • **8**: GwRanked

Tabla 17.22: Campos del JSON con los atributos del fichero

Obtener los equipos que han visto un fichero

Obtiene una lista de MUIDs de los equipos del cliente que han visto un determinado md5.

Petición

Comando	GET
URL	/api/v1/applications/forensics/md5/{md5}/muids
Parámetros requeridos en la URL	**MD5**: hash del fichero.
Cabeceras	**Accept**: application/json

Tabla 17.23: Formato de la llamada para obtener los equipos que han visto un fichero

Respuesta

Lista de JSONs con información de los equipos que vieron el fichero.

Campo del JSON	Descripción
MUID	Identificador único del equipo.
clientId	Identificador único del cliente al que pertenece el equipo.
lastSeen	Fecha en la que el fichero fue visto por última vez en un equipo del parque del cliente.
firstSeen	Fecha en la que el fichero fue visto por primera vez en un equipo del parque del cliente.
lastPath	Ruta del fichero en el equipo donde se almacenaba la última vez que fue visto.

Tabla 17.24: Campos del JSON con la descripción de los equipos que han visto el fichero

Obtener las características de varios equipos

Obtiene información de uno o más equipos que pertenece la infraestructura IT del cliente.

Petición

Comando	POST
URL	/api/v1/applications/forensics/muid/info
Parámetros requeridos en el cuerpo del mensaje HTTP	JSON con la lista de MUIDs de los equipos.
Cabeceras	• **Accept**: application/json • **Content-Type**: application/json-patch+json

Tabla 17.25: Formato de la llamada para obtener información de los equipos

Respuesta

Lista de JSONs con la información de los equipos.

Campo	Descripción
MUID	Identificador único del equipo.
machineName	Nombre del equipo.
lastSeenUtc	Fecha en UTC-0 en la que el equipo se comunicó con la nube de Cytomic.
creationDate	Fecha en la que se instaló la protección Cytomic EDR en el equipo.
clientId	Identificador único del cliente al que pertenece el equipo.
clientName	Nombre del cliente.
clientCreationDate	Fecha en la que el cliente integró el primer equipo en la plataforma Cytomic Orion.

Tabla 17.26: Formato del JSON que describe a un equipo

Obtener el MUID de un equipo

Obtiene el MUID de un equipo que pertenece a la infraestructura IT del cliente a partir de su nombre.

Petición

Comando	GET
URL	/api/v1/applications/clients/{ClientId}/machine-name/{MachineName}/muid
Parámetros requeridos en la URL	• **ClientId**: identificador único del cliente. • **MachineName**: nombre del equipo a obtener su MUID. Admite subcadenas.
Cabeceras	**Accept**: application/json

Tabla 17.27: Formato de la llamada para obtener el MUID de un equipos

Respuesta

Lista de JSONs con el nombre y otra información complementaria de los equipos que coinciden con la subcadena indicada en el campo **MachineName** de la petición.

Campo	Descripción
MUID	Identificador único del equipo.
machineName	Nombre completo del equipo.
lastSeenUtc	Fecha en UTC-0 en la que el equipo se comunicó con la nube de Cytomic.
creationDate	Fecha en la que se instaló la protección Cytomic EDR en el equipo.

Tabla 17.28: Formato del JSON que contiene el MUID de un equipo

Obtener el detalle de un equipo

Obtiene la información completa de un equipo que pertenece a la infraestructura IT del cliente.

Petición

Comando	GET
URL	/api/v1/remediations/muids/{muid}/detail
Parámetros requeridos en la URL	**MUID**: identificador único del equipo.
Cabeceras	**Accept**: application/json

Tabla 17.29: Formato de la llamada para obtener el detalle de los equipos

Respuesta

JSON con información de detalle del equipo. Consulta **Detalles del equipo** en la página **122** para una descripción completa de los campos.

Obtener la fecha en la que se vio por última vez uno o más equipos

Obtiene la fecha en la que se vio por primera y por última vez equipos de un cliente.

- Si no se envía el parámetro opcional **machineName**, se reciben datos de todos los equipos del cliente.
- Si se envía el parámetro opcional **machineName**, se reciben datos del equipo concreto del cliente.

Petición

Comando	GET
URL	/api/v1/clients/{pandaClientId}/machines

Parámetros requeridos en la URL	**pandaClientId**: identificador del cliente.
Parámetros opcionales en la URL	**machineName**: nombre del equipo.
Cabeceras	**Accept**: application/json

Tabla 17.30: Formato de la llamada para obtener las fechas de uno o más equipos

Respuesta

Colección de JSONs con los datos de los equipos.

Campo del JSON	Descripción
MUID	Identificador del equipo.
MachineName	Nombre del equipo.
LastSeenUtc	Fecha de la última vez que el equipo conectó con la nube de Cytomic.
CreationDate	Fecha en la que el fichero fue registrado por primera vez en la nube de Cytomic.

Tabla 17.31: Campos del JSON con los atributos del equipo

Ejemplo para obtener información extendida de equipos y ficheros

El siguiente ejemplo lista todos los equipos que han visto un fichero y muestra la información de los equipos y del propio fichero.

```
#cabeceras para la llamada a la API incluyendo el token de acceso
h_request_know = {
       'Authorization': f'Bearer {token_access}',
       'Accept': 'application/json'
#Objetivo: obtener información de un md5
#md5 del fichero
md5='6cff0673ce2002a2fe2218642605187a'
#URL de la llamada
url_                md5_                info                                =
f'https://api.orion.cytomic.ai/api/v1/applications/forensics/md5/{md5}/info'
r = requests.get(url_md5_info, headers=h_request_know, verify=False)
#devuelve un JSON con información del fichero
file=r.json()
#Objetivo: obtiene ua lista de equipos que han visto el md5
#URL de la llamada
```

```
url_ computers = f'
https://api.orion.cytomic.ai/api/v1/applications/forensics/m
d5/{md5}/muids'
r = requests.get (url_ computers, headers=h_ request_ know,
verify=False)
#devuelve una lista de jsons con información de cada equipo
computers=r.json()
#Objetivo: obtener información extendida de cada equipo que
vio el md5.
#para cada equipo se extrae el muid del JSON y se llama a la
API de información #extendida.
for computer in computers:
    #muid del equipo
    muid=computer['muid']
    #URL de la llamada
    url_ computers_ info = f'
https://api.orion.cytomic.ai/api/v1/applications/forensics/m
uid/{muid}/info'
    r = requests.get (url_ computers_ info, headers=h_
request_know, verify=False)
    #devuelve un JSON con información del equipo
    computer_info=r.json()
```

API de indicios

Obtener los indicios generadas

> *Este método de la API recupera los primeras 30.000 indicios del intervalo establecido. Para recuperar todos los indicios ejecuta de forma sucesiva varias llamadas con distintos intervalos reducidos. El intervalo de recuperación de indicios no debe superar 1 mes, de lo contrario la llamada devolverá un error.*

Obtiene una lista de JSONs con los indicios generados en Cytomic Orion entre las fechas indicadas. Opcionalmente se permite filtrar por el tipo de indicio a buscar.

Petición

Comando	GET
URL	/api/v1/applications/alerts/{from}/{to}

Parámetros opcionales en la URL por querystring	• **statuses**: filtra la recuperación de indicios en función de si han sido asignados a una investigación.
	  • **Pending**: el indicio todavía no ha sido asignado a una investigación.
	  • **InProgress**: el indicio ha sido asignado a una investigación

	que está abierta para su estudio. • **Finished**: el indicio fue asignado a una investigación pero ya se cerró. • **MUID**: filtra la recuperación de indicios por el identificador único de equipo. • **clientid**: filtra la recuperación de indicios por el identificador único de cliente. • **huntingrule**: filtra la recuperación de indicios por el nombre de su huntingrule asociada. • **caseid**: filtra la recuperación de indicios por el identificador de la investigación. • **machineName**: filtra la recuperación de indicios por el nombre del equipo. • **from**: timestamp Unix en milisegundos con la fecha inferior del intervalo de indicios a recuperar. • **to**: timestamp Unix en milisegundos con la fecha superior del intervalo de indicios a recuperar. • **showExcluded**: filtra la recuperación de indicios según su pertenencia o no a una regla de eliminación. • **True**: el indicio pertenece a una regla de eliminación y permanece en la papelera. • **False**: el indicio no pertenece a una regla de eliminación. • **showDetails**: recupera o no los detalles del indicio: • **true**: se envía en el campo Details los detalles del indicio. • **false**: el campo Details se devuelve vacío (null).
Cabeceras	• **Accept**: application/json

Tabla 17.32: Formato de la llamada para obtener los indicios generadas

Respuesta

Lista de JSONs con la descripción de los indicios encontrados.

Campo	Descripción
id	Identificador del indicio.
MUID	Identificador único del equipo del cliente donde se ha producido el indicio.

Campo	Descripción
timestamp	Fecha en la que se generó el indicio.
clientid	Identificador único del cliente al que pertenece el equipo.
huntingRule	Nombre de la regla de hunting que generó el indicio.
HuntingRuleId	Identificador de la regla de hunting que generó el indicio.
status	Indica si el indicio ha sido asignada a una investigación y el estado de la investigación. • **0 (En curso)**: el indicio está asignada a una investigación y un analista de Nivel 2 la está investigando. • **1 (Pendiente)**: el indicio todavía no ha sido asignada a una investigación. • **2 (Cerrada)**: el indicio fue asignada a una investigación y ésta se resolvió.
details	Descripción del indicio. Junto con a su nombre indica el tipo de eventos sospechosos registrados para que el equipo de Nivel 1 pueda hacer el triaje.
alertDateTime	Fecha en la que se generó el indicio.
lastHourEvidenceCount	Número de veces que Cytomic Orion generó el mismo indicio en la última hora.
severity	Importancia del impacto de la amenaza detectada: • **0**: NotSet • **1**: Critical • **2**: High • **3**: Medium • **4**: Low • **1000**: Unknown
mitre	Categoría de la técnica y táctica de la hunting rule mapeada según la especificación MITRE.

Campo	Descripción
excluded	Indica si Cytomic Orion ha mostrado el indicio en la consola de administración o por el contrario el indicio está excluido.
machineName	Nombre del equipo del cliente involucrado en el indicio.
caseId	Identificador único de la investigación asignada al indicio si fue creada.
caseName	Nombre de la investigación asignada al indicio si fue creada.
directLink	URL para acceder a la página que describe el indicio. Utilizado en integraciones con software de terceros.

Tabla 17.33: Formato del JSON que describe a un indicio

Ejemplo de llamada a la API para listar indicios

El siguiente ejemplo lista todos los indicios generadas en Cytomic Orion desde el 1/11/2019 al 1/12/2019 y que todavía no han sido asignadas a una investigación (estado Pendiente).

```
#cabeceras para la llamada a la API incluyendo el token de acceso.
h_request_alert = {
       'Authorization': f'Bearer {token_access}',
       'Accept': 'application/json'}
#fecha de inicio, fecha de final y criterio de filtrado
alert_from='1572595090000'
alert_to='1575187090000'
state='Pending'}
#Objetivo: obtener el listado del indicio entre dos fechas que no han sido asignadas a una investigación
#URL de la llamada
url_ alert   =   f' https://api.orion.cytomic.ai/api/v1/applications/alerts/{alert_from}/{alert_to}?statuses={state}'
r = requests.get(url_alert, headers=h_request_alert, verify=False)
#devuelve una lista de JSONs con información de cada indicio
alerts=r.json()
```

API de respuesta

Aislar equipos

Aísla una lista de equipos de la red para evitar la propagación de las amenazas y /o la comunicación y extracción de información confidencial.

Petición

Comando	POST
URL	/api/v1/applications/remediations/muids/isolate
Parámetros requeridos en el cuerpo del mensaje HTTP	JSON con la lista de MUIDs de los equipos a aislar. • **MUIDs**: lista de MUIDs.
Cabeceras	• **Accept**: application/json • **Content-Type**: application/json-patch+json

Tabla 17.34: Formato de la llamada para aislar equipos

Respuesta

Lista de JSONs, cada uno de ellos con el resultado de la operación.

Campo del JSON	Descripción
MUID	MUID del equipo referido en la petición.
devideId	Campo obsoleto.
requestAccepted	True
errorCode	"null"
errorMessage	"null"

Tabla 17.35: JSON de respuesta al aislamiento de equipos

Quitar el aislamiento de equipos

Saca del estado del aislamiento los equipos de la red una vez resuelta la posibilidad de propagación de las amenazas y / o la comunicación y extracción de información confidencial.

Petición

Comando	POST
URL	/api/v1/applications/remediations/muids/deisolate
Parámetros requeridos en el cuerpo del	JSON con la lista de MUIDs de los equipos a sacar del aislamento. • **MUIDs**: lista de MUIDs.

mensaje HTTP	
Cabeceras	• **Accept**: application/json • **Content-Type**: application/json-patch+json

Tabla 17.36: Formato de la llamada para quitar el aislamiento

Respuesta

Lista de JSONs, cada uno de ellos con el resultado de la operación.

Campo del JSON	Descripción
MUID	MUID del equipo referido en la respuesta.
devideId	Campo obsoleto.
requestAccepted	True
errorCode	"null"
errorMessage	"null"

Tabla 17.37: JSON de respuesta al aislamiento de equipos

Reinicio

Inicia la secuencia de reinicio de una lista de equipos para completar una actualización de software o para corregir un mal funcionamiento del equipo.

Petición

Comando	POST
URL	/api/v1/applications/remediations/muids/reboot
Parámetros requeridos en el cuerpo del mensaje HTTP	JSON con la lista de MUIDs de los equipos a reiniciar. • **MUIDs**: lista de MUIDs.
Cabeceras	• **Accept**: application/json • **Content-Type**: application/json-patch+json

Tabla 17.38: Formato de la llamada para reiniciar equipos

Respuesta

Lista de JSONs, cada uno de ellos con el resultado de la operación.

Campo del JSON	Descripción
MUID	MUID del equipo referido en la respuesta.
devideId	Campo obsoleto.
requestAccepted	True
errorCode	"null"
errorMessage	"null"

Tabla 17.39: JSON de respuesta al reinicio de equipos

Ejemplo de llamada a la API para aislar, quitar el aislamiento y reiniciar equipos

El siguiente ejemplo aísla, quita el aislamiento y reinicia los equipos de MUIDs "3333-4444" y "5555-6666".

```
#cabeceras para la llamada a la API incluyendo el token de acceso
h_request_remediation = {
       'Authorization': f'Bearer {token_access}',
       'Accept': 'application/json',
       'Content-Type': 'application/json-patch+json'
}
#JSON con la lista de muids
muids_data={'muids':['3333-4444','5555-6666']}
#Objetivo: aísla una lista de equipos
#URL de la llamada
url_                    isolate                                          =
f'
https://api.orion.cytomic.ai/api/v1/applications/remediations/muids/isolate'
r = requests.post(url_isolate, headers=h_request_remediation, json=muids_
data, verify=False)
#devuelve un JSON con el resultado de la operación
isolate=r.json()
#Objetivo: retira el estado de aislamiento de una lista de equipos
#URL de la llamada
url_           deisolate                        =                        f'
https://api.orion.cytomic.ai/api/v1/applications/remediations/muids/deisola
te'
r = requests.post(url_deisolate, headers=h_request_remediation, json=muids_
data, verify=False)
#devuelve un JSON con el resultado de la operación
deisolate=r.json()
#Objetivo: reinicia una lista de equipos
```

```
#URL de la llamada
url_          reboot                    =                    f'
https://api.orion.cytomic.ai/api/v1/applications/remediation
s/muids/reboot'
r = requests.post(url_reboot, headers=h_request_remediation,
json=muids_data, verify=False)
#devuelve un JSON con el resultado de la operación
reboot=r.json()
```

API de acceso a OSQuery

La API de OSQuery requiere el envío de dos peticiones distintas en un orden determinado:

1. Envío de la sentencia OSQuery a los equipos para que el agente Cytomic EPDR prepare la información almacenada en la base de datos del equipo y la envíe a la plataforma Cytomic . Hay disponibles dos llamadas a la API (`/api/v1/osQuery/client` y `/api/v1/osQuery/machine`) dependiendo de si se quiere recuperar información de todos los equipos de uno o varios clientes, o de una lista de equipos concreta. Como resultado se obtiene un identificador de operación por cada cliente que reporta datos de sus equipos.
2. Envío de cada identificador de operación para obtener la URL de descarga del fichero, con la información de los equipos de cada cliente, o para obtener el estado de la petición.
3. Descarga de un fichero por cada cliente, que consolida toda la información recolectada de sus equipos. Este recurso es accesible a través de la URL obtenida en el paso 2 que, por motivos de seguridad, permanecerá activa durante un máximo de 5 minutos; una vez transcurridos es necesario volver al paso 2 para obtener una nueva URL de descarga.

Debido a que puede haber equipos apagados o inaccesibles, las sentencias OSQuery pueden extenderse indefinidamente en el tiempo. Por esta razón es necesario determinar un TTL o tiempo de vida máximo, pasado el cual Cytomic Orion dará por concluida la operación.

Enviar una petición para obtener información de uno o varios equipos

Ejecuta una sentencia SQL compatible con OSQuery en los equipos indicados que pertenecen a la infraestructura IT de uno o varios clientes.

Petición

Comando	POST
URL	/api/v1/osQuery/machine
Parámetros requeridos en el cuerpo del mensaje HTTP	JSON con la petición OSQuery y una lista de MUIDs. • **query**: sentencia SQL compatible con OSQuery. • **ttl**: máximo tiempo de espera en minutos para recibir los resultados. 0 para 24 horas. • **MUIDs**: lista de los identificadores de equipos donde

	se ejecutará la sentencia.
Cabeceras	• **Accept**: application/json • **Content-Type**: application/json-patch+json

Tabla 17.40: Formato de la llamada para obtener información de uno o varios equipos

Respuesta

Lista de JSONs, cada uno de ellos con el identificador de la operación de un cliente.

Campo del JSON	Descripción
pandaID	Identificador del cliente al que pertenecen los equipos que devolvieron datos.
operationId	Identificador de la operación realizada, necesario para consultar la URL con los resultados de la petición OSQuery. Consulta**Obtener el resultado de una petición OSQuery**.
MUIDs	Lista de identificadores de equipos del cliente que devolvieron resultados de la petición.

Tabla 17.41: JSON con la información de uno o varios equipos

Enviar una petición para obtener información de todos los equipos de uno o varios clientes

Ejecuta una sentencia SQL compatible con OSQuery en todos los equipos que pertenecen a la infraestructura IT de los clientes indicados.

Petición

Comando	POST
URL	/api/v1/osQuery/client
Parámetros requeridos en el cuerpo del mensaje HTTP	JSON con la petición OSQuery y una lista de identificadores de clientes. • **query**: sentencia SQL compatible con OSQuery. • **ttl**: máximo tiempo de espera en minutos para recibir los resultados. 0 para 24 horas. • **pandaIDs**: lista de los identificadores de los clientes donde se ejecutará la sentencia.

Cabeceras	• **Accept**: application/json • **Content-Type**: application/json-patch+json

Tabla 17.42: Formato de la llamada para obtener información de los equipos de uno o más clientes

Respuesta

Lista de JSONs, cada uno de ellos con información de un cliente.

Campo del JSON	Descripción
pandaID	Identificador del cliente al que pertenecen los equipos que devolvieron datos.
operationId	Identificador de la operación realizada, necesario para consultar la URL con los resultados de la petición OSQuery. Consulta**Obtener el resultado de una petición OSQuery**.
MUIDs	Lista de identificadores de equipos del cliente que devolvieron resultados de la petición.

Tabla 17.43: JSON con la información de todos los equipos de un cliente

Obtener el resultado de una petición OSQuery

Obtiene la URL que apunta al fichero con los datos de los equipos solicitados.

Petición

Comando	POST
URL	/api/v1/osQuery/state
Parámetros requeridos en el cuerpo del mensaje HTTP	Lista de JSONs, cada uno de ellos con el identificador de la operación cuyos datos se quieren recuperar. • **pandaId**: identificador del cliente al que pertenecen los equipos que devolvieron datos. • **operationId**: identificador de la operación ejecutada.
Cabeceras	• **Accept**: application/json • **Content-Type**: application/json-patch+json

Tabla 17.44: Formato de la llamada para obtener el resultado de una petición OSQuery

Respuesta

Lista de JSONs, uno por cliente, con información sobre el resultado de la petición.

Campo del JSON	Descripción
pandaId	Identificador del cliente al que pertenecen los equipos que devolvieron datos.
operationId	Identificador de la operación ejecutada.
url	Enlace de descarga del fichero con la información recogida de los equipos. Este enlace es válido durante 5 minutos. Consulta **Formato del fichero de descarga** para obtener información sobre el formato del fichero.

counters	JSON con las estadísticas de la ejecución:
	• **totalOperationElements**: número de equipos a los que se envió la petición para recuperar la información.
	• **totalSuccess**: número de equipos que devolvieron información de forma correcta.
	• **totalPartiallySucceeded**: número de equipos que devolvieron información pero hubo algún problema a la hora de interpretar los resultados.
	• **totalError**: número de equipos que devolvieron un código de error.
	• **errors**: lista de JSON con los distintos errores recibidos de los equipos. Consulta**Tipos de error implementados**
	  • **errorCode**: código de error.
	  • **errorDescription**: descripción del error.
	  • **occurrences**: número de equipos afectados por el error.

Tabla 17.45: JSON de respuesta con la URL y el resultado de la operación

Control de los equipos apagados, inaccesibles o con retraso en la respuesta

totalOperationElements es igual a la suma de **totalSuccess** + **totalPartiallySucceeded** + **totalError** en el caso de que todos los equipos respondan, bien con información o con un error. Como las sentencias OSQuery pueden tardar un tiempo indeterminado en ejecutarse, si **totalOperationElements** no es igual a la suma de **totalSuccess** + **totalPartiallySucceeded** + **totalError** quiere decir que todavía hay equipos en el cliente que no han respondido. En tal caso será necesario enviar el **operationId** sucesivas veces hasta que la suma coincida o hasta que el tiempo establecido en el campo **ttl** pase.

Formato del fichero de descarga

El fichero que contiene los datos de los equipos del cliente tiene las características siguientes:

- **Nombre**: "osquery_" + identificador de la operación.
- **Formato**: texto.
- **Cabecera**: campos del fichero separados por el carácter ";".
- **Cuerpo**: lineas con el contenido de los campos extraídos por OSQuery de la base de datos del equipo.

Tipos de error implementados

Nombre	Código	Descripción	Observaciones
ErrorExecutingOsQuery	201	near "name": syntax error	OSQuery es compatible con el esquema de datos 4.2.0. Consulta **Requisitos de OSQuery** en la página **249** y revisa la sintaxis de la sentencia OSQuery.
ErrorOsNotSupported	202	Error operating system not supported	OSQuery es compatible con sistemas Windows. Consulta **Requisitos de OSQuery** en la página **249**
ErrorOsQueryNotInstalled	203	Error OsQuery not installed	OSQuery está disponible a partir de la versión 3.71 de Cytomic EDR. Consulta **Requisitos de OSQuery** en la página **249**

Tabla 17.46: Códigos de error implementados y su significado

Obtener el estado de una petición OSQuery

Obtiene una lista de JSONs que indican el estado de las operaciones en curso o finalizadas.

Petición

Comando	POST

URL	/api/v1/osQuery/info
Parámetros requeridos en el cuerpo del mensaje HTTP	Lista de JSONs, cada uno de ellos con el identificador de la operación cuyo estado se quieren recuperar. • **pandaId**: identificador del cliente al que pertenecen los equipos que devolvieron datos. • **operationId**: identificador de la operación ejecutada.
Parámetros opcionales en el cuerpo del mensaje HTTP	• **trackingStateType**: devuelve únicamente las operaciones que tienen el estado indicado: • **Pending (0)**: operaciones en curso. • **Success (1)**: operaciones completadas con éxito. • **PartiallySucceeded (2)**: operaciones que recibieron resultados de algunos equipos. • **Error (3)**: operaciones no se pudieron ejecutar. • **Cancelled (4)**: operaciones canceladas por haber expiado el tiempo máximo definido sin haber sido completadas.
Cabeceras	• **Accept**: application/json • **Content-Type**: application/json-patch+json

Tabla 17.47: Formato de la llamada para obtener el estado de una lista de peticiones OSQuery

Respuesta

Lista de JSONs, uno por cliente, con información sobre el resultado de las peticiones.

Campo del JSON	Descripción
pandaId	Identificador del cliente al que pertenece la operación.
operationId	Identificador de la operación ejecutada.
info	Lista de JSONs, uno por cada operación del cliente, con su estado: • **pandaId**: identificador del cliente al que afecta la

Campo del JSON	Descripción

	operación.
	• **hostname**: nombre del equipo al que afecta la operación.
	• **deviceId**: identificador del equipo al que afecta la operación.
	• **trackingStateType**: estado de la operación.
	  • **Pending (0)**: operación en curso.
	  • **Success (1)**: operación completada con éxito.
	  • **PartiallySucceeded (2)**: operación que recibió resultados de algunos equipos.
	  • **Error (3)**: la operación no se pudo ejecutar. Consulta**Tipos de error implementados** .
	  • **Cancelled (4)**: operación cancelada por haber expiado el tiempo máximo definido sin haber terminado.
	• **date**: fecha en la que la operación cambió de estado por última vez.
	• **errorCode**: código de error.
	• **errorDescription**: descripción del error.

Tabla 17.48: JSON de respuesta con estado de la operación

Tipos de error implementados

Nombre	Código	Descripción	Observaciones
ErrorExecutingOsQuery	201	near "name": syntax error	OSQuery es compatible con el esquema de datos 4.2.0. Consulta **Requisitos de OSQuery** en la página **249** y revisa la sintaxis de la sentencia OSQuery.
ErrorOsNotSupported	202	Error operating system not	OSQuery es compatible con sistemas Windows.

Nombre	Código	Descripción	Observaciones
		supported	Consulta **Requisitos de OSQuery** en la página **249**
ErrorOsQueryNotInstalled	203	Error OSQuery not installed	OSQuery está disponible a partir de la versión 3.71 de Cytomic EDR. Consulta **Requisitos de OSQuery** en la página **249**

Tabla 17.49: Códigos de error implementados y su significado

API de acceso a datos / consultas avanzadas

Ofrece a través de la API de Cytomic Orion un interface de acceso al océano de datos, equivalente al módulo de consultas avanzadas SQL.

Obtener información del océano de datos

Petición

Comando	POST
URL	/api/v1/applications/explorations
Parámetros requeridos en el cuerpo del mensaje HTTP	JSON con la sentencia SQL a ejecutar. • **sql**: sentencia sql.
Cabeceras	• **Accept**: application/json • **Content-Type**: application/json-patch+json

Tabla 17.50: Formato de la llamada para recuperar información del océano de datos

Respuesta

Lista de JSONs, uno por cada fila de resultados. Los campos del JSON dependen de los campos pedidos en la sentencia SQL.

Campo del JSON	Descripción
Nombre del campo pedido	Valor del campo pedido en la sentencia SQL.

Tabla 17.51: JSON de respuesta con los datos solicitados

API de gestión de investigaciones

Permite crear, modificar y borrar investigaciones y reglas de asignación de indicios.

Crear investigación

Crea una investigación con clientes e indicios asociados.

Petición

Comando	POST
URL	/api/v1/applications/cases
Parámetros requeridos en el cuerpo del mensaje HTTP	JSON con los parámetros. • **name**: nombre de la investigación. • **triggers**: lista de identificadores de indicios asociados a la investigación. • **clientsIds**: lista de identificadores de clientes asociados a la investigación.
Cabeceras	• **Accept**: */* • **Content-Type**: application/json;charset=UTF-8

Tabla 17.52: Formato de la llamada para crear una investigación

Respuesta

Campo del JSON	Descripción
id	Identificador de la investigación.
name	Nombre de la investigación.
status	Indica si los indicios de la investigación están siendo revisados por los técnicos o ya fueron analizados.

Campo del JSON	Descripción
	• **0**: investigación cerrada. • **1**: investigación en curso.
created	Fecha de creación de la investigación.
clientInfos	Lista de JSONs con los clientes asignados a la investigación. • **pandaClientId**: identificador del cliente. • **name**: nombre del cliente.
classification	Indica cómo está catalogada la investigación: • **0**: (Sin clasificar) investigación pendiente de analizar. • **1**: (Ataque confirmado) la investigación de los indicios desembocó en la detección de un ataque. • **2**: (Investigación sin ataques detectados) la investigación de los indicios no detectó ningún ataque. • **3**: (Ataque potencial) la investigación de los indicios no es concluyente, pero se ha determinado una alta probabilidad de ser un ataque.
priority	Indica el impacto que el posible ataque investigado pueda tener en los activos de la empresa: • **0**: (Sin establecer) el impacto no se ha determinado por el momento. • **1**: (Crítico) el peligro detectado en la investigación de los indicios es muy alto. • **2**: (Alta) el peligro detectado en la investigación de los indicios es alto. • **3**: (Media) el peligro detectado en la investigación de los indicios es medio.

Campo del JSON	Descripción
	• **4**: (Baja) el peligro detectado en la investigación de los indicios es bajo.
description	Descripción detallada del estado de la investigación.
assignedTo	null
assignedToEmail	null

Tabla 17.53: JSON de respuesta a la creación de una investigación

Obtener detalles de investigación

Recupera las características de una investigación.

Petición

Comando	GET
URL	/api/v1/applications/cases/{caseId}
Parámetros requeridos en la URL	• **caseId**: identificador de la investigación.
Cabeceras	• **Accept**: */*

Tabla 17.54: Formato de la llamada para obtener los detalles de una investigación

Respuesta

Campo del JSON	Descripción
id	Identificador de la investigación.
name	Nombre de la investigación.
createdBy	Cuenta de usuario que creó la investigación.
status	Indica si los indicios de la investigación están siendo revisados por los técnicos o ya fueron analizados. • **0**: investigación cerrada. • **1**: investigación en curso.

Campo del JSON	Descripción
created	Fecha de creación de la investigación.
clientInfos	Lista de JSONs con los clientes asignados a la investigación. • **pandaClientId**: identificador del cliente. • **name**: nombre del cliente.
classification	Indica cómo está catalogada la investigación: • **0**: (Sin clasificar) investigación pendiente de analizar. • **1**: (Ataque confirmado) la investigación de los indicios desembocó en la detección de un ataque. • **2**: (Investigación sin ataques detectados) la investigación de los indicios no detectó ningún ataque. • **3**: (Ataque potencial) la investigación de los indicios no es concluyente, pero se ha determinado una alta probabilidad de ser un ataque.
priority	Indica el impacto que el posible ataque investigado pueda tener en los activos de la empresa: • **0**: (Sin establecer) el impacto no se ha determinado por el momento. • **1**: (Crítico) el peligro detectado en la investigación de los indicios es muy alto. • **2**: (Alta) el peligro detectado en la investigación de los indicios es alto. • **3**: (Media) el peligro detectado en la investigación de los indicios es medio. • **4**: (Baja) el peligro detectado en la investigación de los indicios es bajo.

Campo del JSON	Descripción
description	Descripción detallada del estado de la investigación.
assignedTo	Identificador de la cuenta de usuario asignada a la investigación.
assignedToEmail	Cuenta de usuario asignada a la investigación.

Tabla 17.55: JSON de respuesta a la obtención de detalles de una investigación

Buscar investigaciones

Obtiene una lista de JSONs con todas las investigaciones que coincidan con los parámetros establecidos en la llamada. Por cada investigación encontrada se incluyen sus detalles.

La búsqueda aplica un OR lógico entre los parámetros especificados en el JSON de la llamada. Si un parámetro admite una lista de valores, se aplica un OR lógico entre ellos.

Petición

Comando	POST
URL	/api/v1/applications/cases/filter
Parámetros requeridos en el cuerpo del mensaje HTTP	JSON con los parámetros de filtrado de investigaciones. • **from**: timestamp Unix en milisegundos con la fecha inferior del intervalo de investigaciones a listar. • **to**: timestamp Unix en milisegundos con la fecha superior del intervalo de investigaciones a listar. • **statuses**: lista de estados (1: En progreso, 2: Cerrada). • **emails**: lista de emails. • **clients**: lista de nombres de cliente. • **classifications**: lista de clasificaciones (0: Sin clasificar, 1: Ataque confirmado, 2: Investigación sin ataques detectados, 3: Ataque potencial) • **priorities**: lista de prioridades (0: Sin establecer, 1: Crítico, 2: Alto, 3: Medio, 4: Bajo) • **assignedToEmails**: lista de emails (none: Sin

	asignar, Email: dirección de correo).
Cabeceras	• **Accept**: */* • **Content-Type**: application/json;charset=UTF-8

Tabla 17.56: Formato de la llamada para buscar investigaciones

Respuesta

Lista de JSONs con las investigaciones encontradas.

Campo del JSON	Descripción
id	Identificador de la investigación.
name	Nombre de la investigación.
status	Indica si los indicios de la investigación están siendo revisados por los técnicos o ya fueron analizados. • **0**: investigación cerrada. • **1**: investigación en curso.
created	Fecha de creación de la investigación.
clientInfos	Lista de JSONs con los clientes asignados a la investigación. • **pandaClientId**: identificador del cliente. • **name**: nombre del cliente.
classification	Indica cómo está catalogada la investigación: • **0**: (Sin clasificar) investigación pendiente de analizar. • **1**: (Ataque confirmado) la investigación de los indicios desembocó en la detección de un ataque. • **2**: (Investigación sin ataques detectados) la investigación de los indicios no detectó ningún ataque. • **3**: (Ataque potencial) la investigación de los indicios no es concluyente, pero se ha

Campo del JSON	Descripción
	determinado una alta probabilidad de ser un ataque.
priority	Indica el impacto que el posible ataque investigado pueda tener en los activos de la empresa: • **0**: (Sin establecer) el impacto no se ha determinado por el momento. • **1**: (Crítico) el peligro detectado en la investigación de los indicios es muy alto. • **2**: (Alta) el peligro detectado en la investigación de los indicios es alto. • **3**: (Media) el peligro detectado en la investigación de los indicios es medio. • **4**: (Baja) el peligro detectado en la investigación de los indicios es bajo.
description	Descripción detallada del estado de la investigación.
assignedTo	Identificador de la cuenta de usuario asignada a la investigación.
assignedToEmail	Cuenta de usuario asignada a la investigación.

Tabla 17.57: JSON de respuesta a la búsqueda de investigaciones

Actualizar investigación

Modifica las características de una investigación.

Petición

Comando	PUT
URL	/api/v1/applications/cases/{caseId}
Parámetros requeridos en la URL	• **caseId**:identificador de la investigación.

Parámetros requeridos en el cuerpo del mensaje HTTP	JSON con la información de la investigación. • **name**: nuevo nombre de la investigación • **classification**: nueva clasificación de la investigación (0: Sin clasificar, 1: Ataque confirmado, 2: Investigación sin ataques detectados, 3: Ataque potencial) • **priority**: nueva prioridad de la investigación (0: Sin establecer, 1: Critico, 2: Alta, 3: Media, 4: Baja) • **description**: Nueva descripción de la investigación. • **assignedTo**: usuario de la consola asignado a la investigación.
Cabeceras	• **Accept**: */* • **Content-Type**: application/json;charset=UTF-8

Tabla 17.58: Formato de la llamada para actualizar una investigación

Respuesta

Campo del JSON	Descripción
id	Identificador de la investigación.
name	Nombre de la investigación.
status	Indica si los indicios de la investigación están siendo revisados por los técnicos o ya fueron analizados. • **0**: investigación cerrada. • **1**: investigación en curso.
created	Fecha de creación de la investigación.
clientInfos	Lista de JSONs con los clientes asignados a la investigación. • **pandaClientId**: identificador del cliente. • **name**: nombre del cliente.
classification	Indica cómo está catalogada la investigación: • **0**: (Sin clasificar) investigación pendiente de

Campo del JSON	Descripción
	analizar. • **1**: (Ataque confirmado) la investigación de los indicios desembocó en la detección de un ataque. • **2**: (Investigación sin ataques detectados) la investigación de los indicios no detectó ningún ataque. • **3**: (Ataque potencial) la investigación de los indicios no es concluyente, pero se ha determinado una alta probabilidad de ser un ataque.
priority	Indica el impacto que el posible ataque investigado pueda tener en los activos de la empresa: • **0**: (Sin establecer) el impacto no se ha determinado por el momento. • **1**: (Crítico) el peligro detectado en la investigación de los indicios es muy alto. • **2**: (Alta) el peligro detectado en la investigación de los indicios es alto. • **3**: (Media) el peligro detectado en la investigación de los indicios es medio. • **4**: (Baja) el peligro detectado en la investigación de los indicios es bajo.
description	Descripción detallada del estado de la investigación.
assignedTo	Identificador de la cuenta de usuario asignada a la investigación.
assignedToEmail	Cuenta de usuario asignada a la investigación.

Tabla 17.59: JSON de respuesta a la actualización de una investigación

Actualizar los clientes de una investigación

Actualiza los clientes asignados a una investigación.

Petición

Comando	PUT
URL	/api/v1/applications/cases/{caseId}/clients
Parámetros requeridos en la URL	• **caseId**: identificador de la investigación.
Parámetros requeridos en el cuerpo del mensaje HTTP	JSON con la lista de clientes asignados a la investigación. • **clientIds**: lista de identificadores de clientes asignados a la investigación.
Cabeceras	• **Accept**: */* • **Content-Type**: application/json;charset=UTF-8

Tabla 17.60: Formato de la llamada para actualizar los clientes asignados a una investigación

Respuesta

Campo del JSON	Descripción
id	Identificador de la investigación.
name	Nombre de la investigación.
status	Indica si los indicios de la investigación están siendo revisados por los técnicos o ya fueron analizados. • **0**: investigación cerrada. • **1**: investigación en curso.
created	Fecha de creación de la investigación.
clientInfos	Lista de JSONs con los clientes asignados a la investigación. • **pandaClientId**: identificador del cliente.

Campo del JSON	Descripción
	• **name**: nombre del cliente.
classification	Indica cómo está catalogada la investigación: • **0**: (Sin clasificar) investigación pendiente de analizar. • **1**: (Ataque confirmado) la investigación de los indicios desembocó en la detección de un ataque. • **2**: (Investigación sin ataques detectados) la investigación de los indicios no detectó ningún ataque. • **3**: (Ataque potencial) la investigación de los indicios no es concluyente, pero se ha determinado una alta probabilidad de ser un ataque.
priority	Indica el impacto que el posible ataque investigado pueda tener en los activos de la empresa: • **0**: (Sin establecer) el impacto no se ha determinado por el momento. • **1**: (Crítico) el peligro detectado en la investigación de los indicios es muy alto. • **2**: (Alta) el peligro detectado en la investigación de los indicios es alto. • **3**: (Media) el peligro detectado en la investigación de los indicios es medio. • **4**: (Baja) el peligro detectado en la investigación de los indicios es bajo.
description	Descripción detallada del estado de la investigación.
assignedTo	Identificador de la cuenta de usuario asignada a la investigación.

Campo del JSON	Descripción
assignedToEmail	Cuenta de usuario asignada a la investigación.

Tabla 17.61: JSON de respuesta a la actualización de los clientes de una investigación

Cerrar investigación

Cierra una investigación cuyos indicios han sido estudiados y resueltos.

Petición

Comando	PUT
URL	/api/v1/applications/cases/{caseId}/close
Parámetros requeridos en la URL	• **caseId**: identificador de la investigación.
Cabeceras	• **Accept**: application/json • **Content-Type**: application/json-patch+json

Tabla 17.62: Formato de la llamada para cerrar una investigación

Respuesta

Campo del JSON	Descripción
id	Identificador de la investigación.
name	Nombre de la investigación.
status	Indica si los indicios de la investigación están siendo revisados por los técnicos o ya fueron analizados. • **0**: investigación cerrada. • **1**: investigación en curso.
created	Fecha de creación de la investigación.
clientInfos	Lista de JSONs con los clientes asignados a la investigación.

Campo del JSON	Descripción
	• **pandaClientId**: identificador del cliente. • **name**: nombre del cliente.
classification	Indica cómo está catalogada la investigación: • **0**: (Sin clasificar) investigación pendiente de analizar. • **1**: (Ataque confirmado) la investigación de los indicios desembocó en la detección de un ataque. • **2**: (Investigación sin ataques detectados) la investigación de los indicios no detectó ningún ataque. • **3**: (Ataque potencial) la investigación de los indicios no es concluyente, pero se ha determinado una alta probabilidad de ser un ataque.
priority	Indica el impacto que el posible ataque investigado pueda tener en los activos de la empresa: • **0**: (Sin establecer) el impacto no se ha determinado por el momento. • **1**: (Crítico) el peligro detectado en la investigación de los indicios es muy alto. • **2**: (Alta) el peligro detectado en la investigación de los indicios es alto. • **3**: (Media) el peligro detectado en la investigación de los indicios es medio. • **4**: (Baja) el peligro detectado en la investigación de los indicios es bajo.
description	Descripción detallada del estado de la investigación.
assignedTo	Identificador de la cuenta de usuario asignada a la investigación.

Campo del JSON	Descripción
assignedToEmail	Cuenta de usuario asignada a la investigación.

Tabla 17.63: JSON de respuesta a la creación de una investigación

Reabrir una investigación cerrada

Vuelve a abrir una investigación previamente cerrada.

Petición

Comando	PUT
URL	/api/v1/applications/cases/{caseId}/reopen
Parámetros requeridos en la URL	• **caseId**: identificador de la investigación.
Cabeceras	• **Accept**: */* • **Content-Type**: application/json;charset=UTF-8

Tabla 17.64: Formato de la llamada para volver a abrir una investigación

Respuesta

Campo del JSON	Descripción
id	Identificador de la investigación.
name	Nombre de la investigación.
status	Indica si los indicios de la investigación están siendo revisados por los técnicos o ya fueron analizados. • **0**: investigación cerrada. • **1**: investigación en curso.
created	Fecha de creación de la investigación.
clientInfos	Lista de JSONs con los clientes asignados a la investigación. • **pandaClientId**: identificador del cliente.

Campo del JSON	Descripción
	• **name**: nombre del cliente.
classification	Indica cómo está catalogada la investigación: • **0**: (Sin clasificar) investigación pendiente de analizar. • **1**: (Ataque confirmado) la investigación de los indicios desembocó en la detección de un ataque. • **2**: (Investigación sin ataques detectados) la investigación de los indicios no detectó ningún ataque. • **3**: (Ataque potencial) la investigación de los indicios no es concluyente, pero se ha determinado una alta probabilidad de ser un ataque.
priority	Indica el impacto que el posible ataque investigado pueda tener en los activos de la empresa: • **0**: (Sin establecer) el impacto no se ha determinado por el momento. • **1**: (Crítico) el peligro detectado en la investigación de los indicios es muy alto. • **2**: (Alta) el peligro detectado en la investigación de los indicios es alto. • **3**: (Media) el peligro detectado en la investigación de los indicios es medio. • **4**: (Baja) el peligro detectado en la investigación de los indicios es bajo.
description	Descripción detallada del estado de la investigación.
assignedTo	Identificador de la cuenta de usuario asignada a la investigación.

Campo del JSON	Descripción
assignedToEmail	Cuenta de usuario asignada a la investigación.

Tabla 17.65: JSON de respuesta a la reapertura de una investigación

Añadir indicios a una investigación

Añade indicios a una investigación previamente creada. Un indicio solo puede asignarse a una investigación. Si le indicio a asignar ya estuviera asignado a otra investigación la llamada devolverá un error. Para mover indicios de una investigación a otra consulta **Mover indicios de una investigación a otra investigación**.

Petición

Comando	POST
URL	/api/v1/applications/cases/{caseId}/triggers
Parámetros requeridos en la URL	• **caseId**: identificador de la investigación.
Parámetros requeridos en el cuerpo del mensaje HTTP	JSON con los parámetros: • **triggerIds**: lista de identificadores de los indicios asignados a la investigación.
Cabeceras	• **Accept**: */* • **Content-Type**: application/json;charset=UTF-8

Tabla 17.66: Formato de la llamada para asignar indicios a una investigación

Respuesta

Campo del JSON	Descripción
id	Identificador de la investigación.
name	Nombre de la investigación.
status	Indica si los indicios de la investigación están siendo revisados por los técnicos o ya fueron analizados. • **0**: investigación cerrada.

Campo del JSON	Descripción
	• **1**: investigación en curso.
created	Fecha de creación de la investigación.
clientInfos	Lista de JSONs con los clientes asignados a la investigación. • **pandaClientId**: identificador del cliente. • **name**: nombre del cliente.
classification	Indica cómo está catalogada la investigación: • **0**: (Sin clasificar) investigación pendiente de analizar. • **1**: (Ataque confirmado) la investigación de los indicios desembocó en la detección de un ataque. • **2**: (Investigación sin ataques detectados) la investigación de los indicios no detectó ningún ataque. • **3**: (Ataque potencial) la investigación de los indicios no es concluyente, pero se ha determinado una alta probabilidad de ser un ataque.
priority	Indica el impacto que el posible ataque investigado pueda tener en los activos de la empresa: • **0**: (Sin establecer) el impacto no se ha determinado por el momento. • **1**: (Crítico) el peligro detectado en la investigación de los indicios es muy alto. • **2**: (Alta) el peligro detectado en la investigación de los indicios es alto. • **3**: (Media) el peligro detectado en la investigación de los indicios es medio. • **4**: (Baja) el peligro detectado en la

Campo del JSON	Descripción
	investigación de los indicios es bajo.
description	Descripción detallada del estado de la investigación.
assignedTo	Identificador de la cuenta de usuario asignada a la investigación.
assignedToEmail	Cuenta de usuario asignada a la investigación.

Tabla 17.67: JSON de respuesta a la asignación de indicios a una investigación

Eliminar indicios de una investigación

Borra indicios de una investigación.

Petición

Comando	DEL
URL	/api/v1/applications/cases/{caseId}/triggers
Parámetros requeridos en la URL	• **caseId**: identificador de la investigación.
Parámetros requeridos en el cuerpo del mensaje HTTP	JSON con los parámetros: • **triggerIds**: lista de identificadores de los indicios asignados a la investigación.
Cabeceras	• **Accept**: */* • **Content-Type**: application/json;charset=UTF-8

Tabla 17.68: Formato de la llamada para retirar indicios de una investigación

Respuesta

Campo del JSON	Descripción
id	Identificador de la investigación.
name	Nombre de la investigación.

Campo del JSON	Descripción
status	Indica si los indicios de la investigación están siendo revisados por los técnicos o ya fueron analizados. • **0**: investigación cerrada. • **1**: investigación en curso.
created	Fecha de creación de la investigación.
clientInfos	Lista de JSONs con los clientes asignados a la investigación. • **pandaClientId**: identificador del cliente. • **name**: nombre del cliente.
classification	Indica cómo está catalogada la investigación: • **0**: (Sin clasificar) investigación pendiente de analizar. • **1**: (Ataque confirmado) la investigación de los indicios desembocó en la detección de un ataque. • **2**: (Investigación sin ataques detectados) la investigación de los indicios no detectó ningún ataque. • **3**: (Ataque potencial) la investigación de los indicios no es concluyente, pero se ha determinado una alta probabilidad de ser un ataque.
priority	Indica el impacto que el posible ataque investigado pueda tener en los activos de la empresa: • **0**: (Sin establecer) el impacto no se ha determinado por el momento. • **1**: (Crítico) el peligro detectado en la investigación de los indicios es muy alto. • **2**: (Alta) el peligro detectado en la

Campo del JSON	Descripción
	investigación de los indicios es alto. • **3**: (Media) el peligro detectado en la investigación de los indicios es medio. • **4**: (Baja) el peligro detectado en la investigación de los indicios es bajo.
description	Descripción detallada del estado de la investigación.
assignedTo	Identificador de la cuenta de usuario asignada a la investigación.
assignedToEmail	Cuenta de usuario asignada a la investigación.

Tabla 17.69: JSON de respuesta a la retirada de indicios de una investigación

Mover indicios de una investigación a otra investigación

Copia indicios de una investigación a otra investigación previamente creada y los elimina de la investigación original. Como un indicio solo puede estar asignado a una investigación, asignar indicios con este método retira automáticamente los indicios de la investigación original para asignarlos a la investigación indicada en la llamada.

Petición

Comando	POST
URL	/api/v1/applications/cases/{caseId}/triggers/move
Parámetros requeridos en la URL	• **caseId**: identificador de la investigación.
Parámetros requeridos en el cuerpo del mensaje HTTP	JSON con los parámetros: • **triggerIds**: lista de identificadores de los indicios asignados a la investigación.
Cabeceras	• **Accept**: */* • **Content-Type**: application/json;charset=UTF-8

Tabla 17.70: Formato de la llamada para mover indicios de una investigación a otra investigación

Respuesta

Campo del JSON	Descripción
id	Identificador de la investigación.
name	Nombre de la investigación.
status	Indica si los indicios de la investigación están siendo revisados por los técnicos o ya fueron analizados. • **0**: investigación cerrada. • **1**: investigación en curso.
created	Fecha de creación de la investigación.
clientInfos	Lista de JSONs con los clientes asignados a la investigación. • **pandaClientId**: identificador del cliente. • **name**: nombre del cliente.
classification	Indica cómo está catalogada la investigación: • **0**: (Sin clasificar) investigación pendiente de analizar. • **1**: (Ataque confirmado) la investigación de los indicios desembocó en la detección de un ataque. • **2**: (Investigación sin ataques detectados) la investigación de los indicios no detectó ningún ataque. • **3**: (Ataque potencial) la investigación de los indicios no es concluyente, pero se ha determinado una alta probabilidad de ser un ataque.
priority	Indica el impacto que el posible ataque investigado pueda tener en los activos de la empresa: • **0**: (Sin establecer) el impacto no se ha

Campo del JSON	Descripción
	determinado por el momento. • **1**: (Crítico) el peligro detectado en la investigación de los indicios es muy alto. • **2**: (Alta) el peligro detectado en la investigación de los indicios es alto. • **3**: (Media) el peligro detectado en la investigación de los indicios es medio. • **4**: (Baja) el peligro detectado en la investigación de los indicios es bajo.
description	Descripción detallada del estado de la investigación.
assignedTo	Identificador de la cuenta de usuario asignada a la investigación.
assignedToEmail	Cuenta de usuario asignada a la investigación.

Tabla 17.71: JSON de respuesta al movimiento de indicios de una investigación a otra investigación

Añadir un comentario a una investigación

Añade un comentario a una investigación previamente creada.

Petición

Comando	POST
URL	/api/v1/applications/cases/{caseId}/comment
Parámetros requeridos en la URL	• **caseId**: identificador de la investigación.
Parámetros requeridos en el cuerpo del mensaje HTTP	JSON con los parámetros: • **data**: contenido del comentario.
Cabeceras	• **Accept**: */* • **Content-Type**: application/json;charset=UTF-8

Tabla 17.72: Formato de la llamada para añadir un comentario a una investigación

Respuesta

Campo del JSON	Descripción
id	Identificador del comentario.
caseId	Identificador de la investigación.
userId	Identificador del usuario que añadió el comentario.
userEmail	Dirección de correo del usuario que añadió el comentario.
data	Contenido del comentario.
created	Fecha en la que se creó el comentario.
isDeleted	• **false**: el comentario es visible. • **true**: el comentario se borró.
authorizedApplicationName	Nombre de la aplicación que añadió el comentario. Si se añade desde la consola se muestra la dirección de correo de la cuenta de usuario.

Tabla 17.73: JSON de respuesta al añadir un comentario a una investigación

Obtener comentarios de una investigación

Obtiene los comentarios de una investigación.

Petición

Comando	GET
URL	/api/v1/applications/cases/{caseId}/comment
Parámetros requeridos en la URL	• **caseId**: identificador de la investigación.
Cabeceras	• **Accept**: */*

Tabla 17.74: Formato de la llamada para obtener los comentarios de una investigación

Respuesta

Lista de JSONs con los comentarios de la investigación.

Campo del JSON	Descripción
id	Identificador del comentario.
caseId	Identificador de la investigación.
userId	Identificador del usuario que añadió el comentario.
userEmail	Dirección de correo del usuario que añadió el comentario.
data	Contenido del comentario.
created	Fecha en la que se creó el comentario.
isDeleted	• **false**: el comentario es visible. • **true**: el comentario se borró.
authorizedApplicationName	Nombre de la aplicación que añadió el comentario. Si se añade desde la consola se muestra la dirección de correo de la cuenta de usuario.

Tabla 17.75: JSON de respuesta al obtener los comentarios de una investigación

Actualizar comentario de una investigación

Modifica un comentario de una investigación.

Petición

Comando	POST
URL	/api/v1/applications/cases/{caseId}/comment/{caseCommentId}
Parámetros requeridos en la URL	• **caseId**: identificador de la investigación. • **caseCommentId**: identificador del comentario.
Parámetros requeridos en el	JSON con los parámetros:

cuerpo del mensaje HTTP	• **data**: contenido del comentario.
Cabeceras	• **Accept**: */* • **Content-Type**: application/json;charset=UTF-8

Tabla 17.76: Formato de la llamada para actualizar un comentario de una investigación

Respuesta

Campo del JSON	Descripción
id	Identificador del comentario.
caseId	Identificador de la investigación.
userId	Identificador del usuario que añadió el comentario.
userEmail	Dirección de correo del usuario que añadió el comentario.
data	Contenido del comentario.
created	Fecha en la que se creó el comentario.
isDeleted	• **false**: el comentario es visible. • **true**: el comentario se borró.
authorizedApplicationName	Nombre de la aplicación que añadió el comentario. Si se añade desde la consola se muestra la dirección de correo de la cuenta de usuario.

Tabla 17.77: JSON de respuesta al actualizar un comentario de una investigación

Eliminar comentarios de una investigación

Borra un comentario de una investigación.

Petición

Comando	DEL
URL	/api/v1/applications/cases/{caseId}/comment/{caseCommentId}
Parámetros requeridos en la URL	• **caseId**: identificador de la investigación. • **caseCommentId**: identificador del comentario.
Cabeceras	• **Accept**: */* • **Content-Type**: application/json;charset=UTF-8

Tabla 17.78: Formato de la llamada para eliminar un comentario de una investigación

Respuesta

Campo del JSON	Descripción
id	Identificador del comentario.
caseId	Identificador de la investigación.
userId	Identificador del usuario que añadió el comentario.
userEmail	Dirección de correo del usuario que añadió el comentario.
data	Contenido del comentario.
created	Fecha en la que se creó el comentario.
isDeleted	• **false**: el comentario es visible. • **true**: el comentario se borró.

Campo del JSON	Descripción
authorizedApplicationName	Nombre de la aplicación que añadió el comentario. Si se añade desde la consola se muestra la dirección de correo de la cuenta de usuario.

Tabla 17.79: JSON de respuesta al borrar un comentario de una investigación

Obtener los tipos de entidades de interés soportados

Obtiene una lista de JSONs con los tipos de entidades soportadas en Cytomic Orion y sus identificadores.

Petición

Comando	GET
URL	/api/v1/applications/entities-of-interest/types
Cabeceras	• **Accept**: */*

Tabla 17.80: Formato de la llamada para obtener los tipos de entidades de interés soportadas en Cytomic Orion

Respuesta

Lista de JSONs con la información de los tipos de entidades de interés soportadas en Cytomic Orion.

Campo del JSON	Descripción
id	Identificador del tipo de entidad de interés.
name	Nombre de la entidad de interés.

Tabla 17.81: JSON de respuesta al obtener el tipo de las entidades de interés soportadas en Cytomic Orion

Añadir entidades de interés a una investigación

Añade varias entidades de interés de un mismo tipo a una investigación previamente creada.

Petición

Comando	POST
URL	/api/v1/applications/cases/

	{caseId}/entities-of-interest
Parámetros requeridos en la URL	• **caseId**: identificador de la investigación.
Parámetros requeridos en el cuerpo del mensaje HTTP	JSON con los parámetros: • **entityId**: identificador del tipo de entidad. • **entities**: lista con los nombres de las entidades.
Cabeceras	• **Accept**: */* • **Content-Type**: application/json;charset=UTF-8

Tabla 17.82: Formato de la llamada para añadir entidades de interés a una investigación

Respuesta

Lista de JSONs con la información de las entidades de interés asociadas a la investigación.

Campo del JSON	Descripción
id	Identificador de la entidad de interés.
typeId	Tipo de entidad de interés.
entity	Nombre de la entidad de interés.
metadata	Información adicional asociada a la entidad de interés. Almacena el nombre si se trata de una entidad de tipo equipo o cliente.
comments	Campo de comentarios asociados a la entidad. No tiene reflejo en la consola de análisis.

Tabla 17.83: JSON de respuesta al añadir entidades de interés a una investigación

Obtener las entidades de interés de una investigación

Obtiene una lista de JSONs con las entidades de interés asociadas a una investigación.

Petición

Comando	GET
URL	/api/v1/applications/cases/{caseId}/entities-of-interest
Parámetros requeridos en la URL	• **caseId**: identificador de la investigación.
Cabeceras	• **Accept**: */*

Tabla 17.84: Formato de la llamada para obtener las entidades de interés de una investigación

Respuesta

Campo del JSON	Descripción
id	Identificador de la entidad de interés.
typeId	Tipo de entidad de interés.
entity	Nombre de la entidad de interés.
metadata	Información adicional asociada a la entidad de interés. Almacena el nombre si se trata de una entidad de tipo equipo o cliente.
comments	Campo de comentarios asociados a la entidad. No tiene reflejo en la consola de análisis.

Tabla 17.85: JSON de respuesta al obtener las entidades de interés de una investigación

Eliminar las entidades de interés de una investigación

Elimina una entidad de interés de una investigación.

Petición

Comando	DEL
URL	/api/v1/applications/cases/{caseId}/entities-of-interest/{eoiId}
Parámetros requeridos en la URL	• **caseId**: identificador de la investigación. • **eoiId**: identificador de la entidad de interés.

Cabeceras	• **Accept**: */* • **Content-Type**: application/json;charset=UTF-8

Tabla 17.86: Formato de la llamada para eliminar una entidad de interés de una investigación

Respuesta

Campo del JSON	Descripción
id	Identificador de la entidad de interés.
typeId	Tipo de entidad de interés.
entity	Nombre de la entidad de interés.
metadata	Información adicional asociada a la entidad de interés. Almacena el nombre si se trata de una entidad de tipo equipo o cliente.
comments	Campo de comentarios asociados a la entidad. No tiene reflejo en la consola de análisis.

Tabla 17.87: JSON de respuesta al borrar entidades de interés de una investigación

Crear reglas de asignación de indicios a una investigación

Crea una nueva regla de asignación que mueve automáticamente los nuevos indicios que satisfagan ciertos criterios a una investigación. La regla contiene la investigación y las características de los indicios que serán asignados a ésta.

Petición

Comando	POST
URL	/api/v1/alerts/triggers/automation-rules
Parámetros requeridos en el cuerpo del mensaje HTTP	JSON con los parámetros que describen las características de los nuevos indicios que se moverán a la investigación elegida: • **caseId**: identificador de la investigación que recibirá los indicios que cumplan las condiciones indicadas en la regla de asignación.

	• **isRegexDetails**: booleano que indica si el campo **details** de la regla de asignación contiene una expresión regular (True) o contiene texto plano (False). • **description**: descripción de la regla de asignación. • **details**: contenido del campo **Detalles** del indicio. • **huntingRule**: identificador de la Hunting Rule que generó el indicio. • **machineNames**: lista con los nombres de los equipos asociados a los indicios. • **muids**: lista con los identificadores de equipo asociados a los indicios. • **name**: nombre de la regla de asignación. • **pandaClientIds**: identificadores de cliente asociados al indicio. • **detailsFromTrigger**: expresión regular asociada al contenido del campo **Detalles** de los indicios.
Cabeceras	• **Accept**: */* • **Content-Type**: application/json;charset=UTF-8

Tabla 17.88: Formato de la llamada para crear una regla de asignación

Respuesta

Campo del JSON	Descripción
id	Identificador de la regla de asignación.
caseId	Identificador de la investigación que recibirá los indicios que cumplan las condiciones indicadas en la regla de asignación.
caseName	Nombre de la investigación que recibirá los indicios que cumplan las condiciones indicadas en la regla de asignación.
modified	Fecha en la que se modificó por última vez la regla de asignación.

Campo del JSON	Descripción
created	Fecha en la que se creó la regla de asignación.
isRegexDetails	Booleano que indica si el campo **details** de la regla de asignación contiene una expresión regular (True) o contiene texto plano (False).
isDeleted	Sin uso.
description	Descripción de la regla de asignación.
details	Contenido del campo **Detalles** del indicio.
huntingRule	Identificador de la Hunting Rule que generó el indicio.
machineNames	Lista con los nombres de los equipos asociados a los indicios.
muids	Lista con los identificadores de equipo asociados a los indicios.
name	Nombre de la regla de asignación.
pandaClientIds	Identificador de cliente asociados al indicio.
detailsFromTrigger	Contenido del campo **Detalles** del indicio original utilizado como plantilla para crear la regla de asignación.

Tabla 17.89: JSON de respuesta al crear una regla de asignación

Modificar reglas de asignación de indicios

Cambia las condiciones que describen qué indicios se moverán a una regla de asignación existente.

Petición

Comando	PUT
URL	/api/v1/alerts/triggers/automation-rules/{id}

Parámetros requeridos en la URL	• **id**: identificador de la regla de asignación a modificar.
Parámetros requeridos en el cuerpo del mensaje HTTP	JSON con los parámetros que describen las nuevas características de los indicios que se moverán a la investigación elegida: • **caseId**: identificador de la investigación que recibirá los indicios que cumplan las condiciones indicadas en la regla de asignación. • **isRegexDetails**: Booleano que indica si el campo **details** de la regla de asignación contiene una expresión regular (True) o contiene texto plano (False). • **description**: descripción de la regla de asignación. • **details**: contenido del campo **Detalles** del indicio. • **huntingRule**: identificador de la Hunting Rule que generó el indicio. • **machineNames**: lista con los nombres de los equipos asociados a los indicios. • **muids**: lista con los identificadores de equipo asociados a los indicios. • **name**: nombre de la regla de asignación. • **pandaClientIds**: identificadores de cliente asociados al indicio. • **detailsFromTrigger**: expresión regular asociada al contenido del campo **Detalles** de los indicios.
Cabeceras	• **Accept**: */* • **Content-Type**: application/json;charset=UTF-8

Tabla 17.90: Formato de la llamada para modificar una regla de asignación

Respuesta

Campo del JSON	Descripción
id	Identificador de la regla de asignación.
caseId	Identificador de la investigación que recibirá los indicios que cumplan las condiciones indicadas

Campo del JSON	Descripción
	en la regla de asignación.
caseName	Nombre de la investigación que recibirá los indicios que cumplan las condiciones indicadas en la regla de asignación.
modified	Fecha en la que se modificó por última vez la regla de asignación.
created	Fecha en la que se creó la regla de asignación.
isRegexDetails	Booleano que indica si el campo **details** de la regla de asignación contiene una expresión regular (True) o contiene texto plano (False).
isDeleted	Sin uso.
description	Descripción de la regla de asignación.
details	Contenido del campo **Detalles** del indicio.
huntingRule	Identificador de la Hunting Rule que generó el indicio.
machineNames	Lista con los nombres de los equipos asociados a los indicios.
muids	Lista con los identificadores de equipo asociados a los indicios.
name	Nombre de la regla de asignación.
pandaClientIds	Identificadores de cliente asociados al indicio.
detailsFromTrigger	Contenido del campo **Detalles** del indicio original utilizado como plantilla para crear la regla de asignación.

Tabla 17.91: JSON de respuesta al modificar una regla de asignación

Borrar reglas de asignación de indicios

Elimina una regla de asignación.

Petición

Comando	DELETE
URL	/api/v1/alerts/triggers/automation-rules
Parámetros requeridos en el cuerpo del mensaje HTTP	JSON con el parámetro que incluye los identificadores de las reglas de asignación a borrar: • **id**: lista con los identificadores de las reglas de asignación a borrar.
Cabeceras	• **Accept**: */*

Tabla 17.92: Formato de la llamada para borrar reglas de asignación

Respuesta

Código HTTP 200. Respuesta vacía.

Ejecutar reglas de asignación de indicios

Aplicar una regla de asignación previamente creada a los indicios generados los 7 días anteriores.

Petición

Comando	POST
URL	/api/v1/alerts/triggers/automation-rules/{id}/retrospective
Parámetros requeridos en la URL	• **caseId**: identificador de la investigación.
Cabeceras	• **Accept**: */*

Tabla 17.93: Formato de la llamada para ejecutar una regla de asignación

Respuesta

Código HTTP 200. Respuesta vacía.

Obtener las características de una regla de asignación de indicios

Obtiene la definición de la regla de asignación, que incluye las condiciones que los indicios tienen que cumplir para que sean movidos a la investigación especificada.

Petición

Comando	GET
URL	/api/v1/alerts/triggers/automation-rules/{id}
Parámetros requeridos en la URL	• **id**: identificador de la investigación.

Cabeceras	• **Accept**: */*

Tabla 17.94: Formato de la llamada para obtener la definición de una regla de asignación

Respuesta

Campo del JSON	Descripción
id	Identificador de la regla de asignación.
caseId	Identificador de la investigación que recibirá los indicios que cumplan las condiciones indicadas en la regla de asignación.
caseName	Nombre de la investigación que recibirá los indicios que cumplan las condiciones indicadas en la regla de asignación.
modified	Fecha en la que se modificó por última vez la regla de asignación.
created	Fecha en la que se creó la regla de asignación.
isRegexDetails	Booleano que indica si el campo **details** de la regla de asignación contiene una expresión regular (True) o contiene texto plano (False).
isDeleted	Sin uso.
description	Descripción de la regla de asignación.
details	Contenido del campo **Detalles** del indicio.
huntingRule	Identificador de la Hunting Rule que generó el indicio.
machineNames	Lista con los nombres de los equipos asociados a los indicios.
muids	Lista con los identificadores de equipo asociados a los indicios.

Campo del JSON	Descripción
name	Nombre de la regla de asignación.
pandaClientIds	Identificadores de cliente asociados al indicio.
detailsFromTrigger	Contenido del campo **Detalles** del indicio original utilizado como plantilla para crear la regla de asignación.

Tabla 17.95: JSON de respuesta a obtener los detalles de una regla de asignación

Obtener un listado de reglas de asignación de indicios

Obtiene una lista de JSONs con las reglas de asignación de indicios creadas por los analistas y los detalles de su definición.

Petición

Comando	GET
URL	/api/v1/alerts/triggers/automation-rules
Cabeceras	• **Accept**: */*

Tabla 17.96: Formato de la llamada para obtener el listado de reglas de asignación creadas

Respuesta

Lista de JSONs con las reglas de asignación creadas y su definición.

Campo del JSON	Descripción
id	Identificador de la regla de asignación.
caseId	Identificador de la investigación que recibirá los indicios que cumplan las condiciones indicadas en la regla de asignación.
caseName	Nombre de la investigación que recibirá los indicios que cumplan las condiciones indicadas en la regla de asignación.
modified	Fecha en la que se modificó por última vez la regla de asignación.

Campo del JSON	Descripción
created	Fecha en la que se creó la regla de asignación.
isRegexDetails	Booleano que indica si el campo **details** de la regla de asignación contiene una expresión regular (True) o contiene texto plano (False).
isDeleted	Sin uso.
description	Descripción de la regla de asignación.
details	Contenido del campo **Detalles** del indicio.
huntingRule	Identificador de la Hunting Rule que generó el indicio.
machineNames	Lista con los nombres de los equipos asociados a los indicios.
muids	Lista con los identificadores de equipo asociados a los indicios.
name	Nombre de la regla de asignación.
pandaClientIds	Identificadores de cliente asociados al indicio.
detailsFromTrigger	Contenido del campo **Detalles** del indicio original utilizado como plantilla para crear la regla de asignación.

Tabla 17.97: JSON de respuesta a listar las regla de asignación creadas

Capítulo 18

Formato de los eventos utilizados en Cytomic Orion

Para generar procesos de análisis y de respuesta efectivos ante los incidentes detectados, los técnicos del SOC requieren información precisa sobre el estado de la infraestructura IT que investigan.

Cytomic EDR y Cytomic EPDR monitorizan los procesos ejecutados en los equipos de los clientes y envían a la nube de Cytomic la telemetría generada. Toda esta información se almacena en el océano de datos, alojado en la nube de Cytomic, y queda a disposición del analista a través de diversas herramientas accesibles en Cytomic Orion.

La telemetría se almacena en el océano de datos utilizando un formato estructurado, que recibe el nombre de "evento", y que está formado por diversos campos. Es necesario comprender el significado de cada uno de estos campos para interpretar correctamente la información registrada.

CONTENIDO DEL CAPÍTULO

Campos de los eventos recibidos en Cytomic Orion

Un evento es un registro formado por campos que describen una acción ejecutada por un proceso dentro de un equipo. Cada tipo de evento tiene un número de campos determinado.

Cytomic Orion representa el flujo de eventos en la consola del analista de varias formas:

- **Tabla**: todos los eventos de un mismo tipo se almacenan en una misma tabla que se puede consultar mediante sentencias SQL. Para obtener más información consulta **Módulo de consultas avanzadas SQL** en la página **156**.
- **Listado**: el contenido de los campos de los eventos son directamente visibles desde la consola de investigación, donde en un mismo listado se incluyen eventos de varios tipos ordenados cronológicamente. Para obtener más información consulta **Análisis de indicios con la consola de investigación** en la página **186**.
- **Grafos**: la información de los eventos se utiliza para construir grafos que ayudan al analista a interpretar la secuencia de ejecución de los procesos y las relaciones que se establecen entre los distintos actores en un ataque informático.
- **Preguntas**: la información de los eventos se muestra en las investigaciones asistidas para mostrar los resultados y crear nuevas preguntas que guían al analista en la investigación. Consulta **Investigaciones asistidas** en la página **172**.

A continuación, se incluye una referencia de todos los campos incluidos en los eventos almacenados por Cytomic Orion junto a su significado, tipo de dato y valores posibles en el caso de enumeraciones.

Campo	Descripción	Tipo de campo
accesstype	Máscara de acceso al fichero: • **(54) WMI_CREATEPROC**: WMI Local. Para el resto de operaciones: • **https://docs.microsoft.com/en-us/windows/win32/secauthz/access-mask** • **https://docs.microsoft.com/en-us/windows/win32/fileio/file-access-rights-constants** • **https://docs.microsoft.com/en-us/windows/win32/fileio/file-security-and-access-rights**	Máscara de bits
accnube	El agente instalado en el equipo del cliente tiene acceso a la nube de Cytomic.	Booleano
action	Tipo de acción realizada por el agente Cytomic EDR o Cytomic EPDR, por el	Enumeración

Campo	Descripción	Tipo de campo
	usuario o por el proceso afectado: • **0 (Allow)**: el agente permite la ejecución del proceso. • **1 (Block)**: el agente bloquea la ejecución del proceso. • **2 (BlockTimeout)**: el agente muestra un mensaje emergente al usuario, pero éste no contesta a tiempo. • **3 (AllowWL):** el agente permite la ejecución del proceso por encontrarse en la lista blanca de goodware local. • **4 (BlockBL)**: el agente bloquea la ejecución del proceso por encontrarse en la lista negra de malware local. • **5 (Disinfect)**: el agente desinfecta el proceso. • **6 (Delete)**: el agente clasifica el proceso como malware y lo borra por no poderse desinfectar. • **7 (Quarantine)**: el agente clasifica el proceso como malware y lo mueve a la cuarentena del equipo. • **8 (AllowByUser)**: el agente muestra un mensaje emergente al usuario y éste responde con "permitir ejecución". • **9 (Informed)**: el agente muestra un mensaje emergente al usuario. • **10 (Unquarantine)**: el agente saca el fichero de la cuarentena. • **11 (Rename)**: el agente renombra el fichero (acción solo para tests). • **12 (BlockURL)**: el agente bloquea la	

Campo	Descripción	Tipo de campo
	URL. • **13 (KillProcess)**: el agente cierra el proceso. • **14 (BlockExploit)**: el agente detiene un intento de explotación de proceso vulnerable. • **15 (ExploitAllowByUser):** el usuario no permite cerrar el proceso explotado. • **16 (RebootNeeded)**: el agente requiere un reinicio del equipo para bloquear el intento de explotación. • **17 (ExploitInformed)**: el agente muestra un mensaje emergente al usuario, informando de un intento de explotación de proceso vulnerable. • **18 (AllowSonGWInstaller)**: el agente permite ejecutar el proceso por pertenecer a un paquete de instalación clasificado como goodware. • **19 (EmbebedInformed)**: el agente envía a la nube información interna de su funcionamiento para mejorar las rutinas de detección. • **21 (SuspendProcess)**: el proceso monitorizado intenta suspender el servicio del antivirus. • **22 (ModifyDiskResource):** el proceso monitorizado intenta modificar un recurso protegido por el escudo del agente. • **23 (ModifyRegistry):** el proceso monitorizado intenta modificar una clave de registro protegida por el	

Campo	Descripción	Tipo de campo
	escudo del agente. • **24 (RenameRegistry):** el proceso monitorizado intenta renombrar una clave de registro protegida por el escudo del agente. • **25 (ModifyMarkFile):** el proceso monitorizado intenta modificar un fichero protegido por el escudo del agente. • **26 (Undefined):** error al monitorizar la operación del proceso. • **28 (AllowFGW):** el agente permite la operación del proceso monitorizado por estar en la lista local de goodware. • **29 (AllowSWAuthorized):** el agente permite la operación del proceso monitorizado porque el administrador marcó el fichero como software autorizado. • **30 (InformNewPE):** el agente informa de la aparición de un nuevo fichero en el equipo cuando está activada la funcionalidad de Drag&Drop en Cytomic Data Watch. • **31 (ExploitAllowByAdmin):** el agente permite la operación del proceso monitorizado porque el administrador del parque excluyó el exploit. • **32 (IPBlocked)**: el agente bloquea IPs para mitigar un ataque por RDP (Remote Desktop Protocolo). • **37 (Allowed by Global Audit)**: el elemento se permite porque el software de seguridad está	

Campo	Descripción	Tipo de campo
	configurado en modo auditoria.	
actiontype	Indica el tipo de sesión: • **0 (Login)**: inicia la sesión en el equipo del cliente. • **1 (Logout)**: finaliza la sesión en el equipo del cliente. • **-1 (Desconocido)**: no se pudo determinar el tipo de sesión.	Enumeración
age	Fecha de última modificación del fichero.	Fecha
blockreason	Motivo de la aparición del mensaje emergente en el equipo: • **0:** bloqueo por fichero desconocido en el modo de protección avanzada (hardening o lock) de Cytomic EPDR o Cytomic EDR. • **1**: bloqueo por reglas locales. • **2**: bloqueo por regla de origen del fichero no fiable. • **3**: bloqueo por regla de contexto. • **4**: bloqueo por exploit. • **5**: bloqueo por petición al usuario para cerrar el proceso.	Enumeración
buffer AMSI	Script almacenado en el buffer AMSI asociado al evento.	Cadena de caracteres
bytesreceived	Total de bytes recibidos por el proceso monitorizado.	Numérico
bytessent	Total de bytes enviados por el proceso monitorizado.	Numérico

Campo	Descripción	Tipo de campo
callstack/sonsize	Tamaño en bytes del fichero hijo.	Numérico
childattributes	Atributos del proceso hijo: • **0x0000000000000001 (ISINSTALLER)**: fichero de tipo SFX (SelfExtractor). • **0x0000000000000002 (ISDRIVER)**: fichero de tipo Driver. • **0x0000000000000008 (ISRESOURCESDLL)**: fichero de tipo DLL de recursos. • **0x0000000000000010 (EXTERNAL)**: fichero procedente de fuera del equipo. • **0x0000000000000020 (ISFRESHUNK)**: fichero añadido recientemente al conocimiento de Cytomic. • **0x0000000000000040 (ISDISSINFECTABLE)**: fichero con acción recomendada de desinfección. • **0x0000000000000080 (DETEVENT_ DISCARD)**: la tecnología de detección de contexto por eventos no ha realizado ninguna detección. • **0x0000000000000100 (WAITED_FOR_ VINDEX)**: fichero ejecutado sin haberse monitorizado su creación. • **0x0000000000000200 (ISACTIONSEND)**: las tecnologías locales no detectan malware en el fichero y éste se envía a Cytomic para su clasificación. • **0x0000000000000400 (ISLANSHARED)**: fichero almacenado en una unidad de red.	Enumeración

Campo	Descripción	Tipo de campo
	• **0x0000000000000800 (USERALLOWUNK)**: fichero con permiso para importar DLL desconocidos. • **0x0000000000001000 (ISSESIONREMOTE)**: evento originado en una sesión remota. • **0x0000000000002000 (LOADLIB_ TIMEOUT)**: el tiempo transcurrido entre la interceptación de la carga de la librería y su análisis es mayor a 1 segundo, con lo que el análisis pasa de síncrono a asíncrono para no penalizar el rendimiento. • **0x0000000000004000 (ISPE)**: fichero ejecutable. • **0x0000000000008000 (ISNOPE)**: fichero no ejecutable. • **0x0000000000020000 (NOSHELL)**: el agente no detecta la ejecución de una shell en el sistema. • **0x0000000000080000 (ISNETNATIVE)**: fichero de tipo Net Native. • **0x0000000000100000 (ISSERIALIZER)**: fichero de tipo Serializer. • **0x0000000000200000 (PANDEX)**: fichero incluido en la lista de procesos creados por Cytomic Patch. • **0x0000000000400000 (SONOFGWINSTALLER)**: fichero creado por un instalador clasificado como goodware. • **0x0000000000800000 (PROCESS_ EXCLUDED)**: fichero no analizado por las exclusiones de Cytomic Orion.	

Campo	Descripción	Tipo de campo
	• **0x0000000001000000 (INTERCEPTION_TXF)**: la operación interceptada tiene como origen un ejecutable cuya imagen en disco está siendo modificada. • **0x0000000002000000 (HASMACROS):** documento Microsoft Office con macros. • **0x0000000008000000 (ISPEARM):** fichero ejecutable para microprocesadores ARM. • **0x0000000010000000 (ISDYNFILTERED)**: fichero permitido en el equipo al no haber tecnologías que lo clasifiquen. • **0x0000000020000000 (ISDISINFECTED)**: fichero desinfectado. • **0x0000000040000000 (PROCESSLOST)**: operación no registrada. • **0x0000000080000000 (OPERATION_ LOST)**: operación con pre-análisis, de la que no se ha recibido el post-análisis. • **0x0000002000000000 (SAFE_BOOT_ MODE)**: el equipo se inició en modo seguro. • **0x0000004000000000 (PANDA_ SIGNED)**: fichero firmado con la firma de Panda Security.	
childblake	Firma Blake2S del fichero hijo.	Cadena de caracteres
childclassification	Clasificación del proceso hijo que realiza la acción registrada.	Enumeración

Campo	Descripción	Tipo de campo
	• **0 (Unknown)**: fichero en proceso de clasificación. • **1 (Goodware)**: fichero clasificado como goodware. • **2 (Malware)**: fichero clasificado como malware. • **3 (Suspect)**: fichero en proceso de clasificación con alta probabilidad de resultar malware. • **4 (Compromised)**: proceso comprometido por un ataque de tipo exploit. • **5 (GWNotConfirmed)**: fichero en proceso de clasificación con alta probabilidad de resultar malware. • **6 (Pup)**: fichero clasificado como programa no deseado. • **7 (GwUnwanted)**: equivalente a PUP. • **8 (GwRanked)**: proceso clasificado como goodware. • **-1 (Unknown)**	
childfiletime	Fecha del fichero hijo registrado por el agente.	Fecha
childfilesize	Tamaño del fichero hijo registrado por el agente.	Numérico
childmd5	Hash del fichero hijo.	Cadena de caracteres
childpath	Ruta del fichero hijo que realiza la operación registrada.	Cadena de caracteres
childpid	Identificador del proceso hijo.	Numérico

Campo	Descripción	Tipo de campo
childurl	Url de descarga del fichero.	Cadena de caracteres
childstatus	Estado del proceso hijo. • **0 (StatusOk)**: estado OK. • **1 (NotFound)**: elemento no encontrado. • **2 (UnexpectedError)**: error desconocido. • **3 (StaticFiltered)**: fichero identificado como malware mediante información estática contenida en la protección de Cytomic EDR o Cytomic EPDR. • **4 (DynamicFiltered)**: fichero identificado como malware mediante tecnología local implementada en Cytomic EDR o Cytomic EPDR. • **5 (FileIsTooBig)**: fichero demasiado grande. • **6 (PEUploadNotAllowed)**: el envío de ficheros está desactivado. • **11 (FileWasUploaded)**: fichero enviado a la nube para su analisis. • **12 (FiletypeFiltered)**: fichero de tipo DLL de recursos, Net Native o Serializer. • **13 (NotUploadGWLocal)**: fichero goodware no guardado en la nube. • **14 (NotUploadMWdisinfect)**: fichero malware desinfectado no guardado en la nube.	Enumeración
classname	Tipo del dispositivo donde reside el proceso. Se corresponde con la clase indicada en el fichero .inf asociado al	Cadena de caracteres

Campo	Descripción	Tipo de campo
	dispositivo.	
configstring	Versión del fichero MVMF.xml en uso.	Cadena de caracteres
commandline	Línea de comandos configurada como tarea para ser ejecutada a través de WMI.	Cadena de caracteres
confadvancedrules	Configuración de las políticas de seguridad avanzada de Cytomic EDR o Cytomic EPDR.	Cadena de caracteres
copy	Nombre del servicio que desencadena el evento.	Cadena de caracteres
details	Resumen en forma de agrupación de campos relevantes del evento.	Cadena de caracteres
description	Descripción del dispositivo USB que realiza la operación.	Cadena de caracteres
detectionid	Identificador único de la detección realizada.	Numérico
devicetype	Tipo de unidad donde reside el proceso o fichero que desencadenó la operación registrada. • **0 (UNKNOWN)**: desconocida. • **1 (CD_DVD)**: unidad de CD o DVD. • **2 (USB_STORAGE)**: dispositivo de almacenamiento USB. • **3 (IMAGE)**: fichero de tipo imagen. • **4 (BLUETOOTH)**: dispositivo Bluetooth. • **5 (MODEM)**: modem. • **6 (USB_PRINTER)**: impresora USB. • **7 (PHONE)**: telefonía móvil.	Enumeración

Campo	Descripción	Tipo de campo
	• **8 (KEYBOARD)**: teclado. • **9 (HID)**: ratón.	
direction	Sentido de la conexión de red. • **0 (UnKnown)**: desconocido. • **1 (Incoming)**: conexión establecida desde el exterior hacia un equipo de la red del cliente. • **2 (Outgoing)**: conexión establecida desde un equipo de la red del cliente hacia el exterior. • **3 (Bidirectional)**: bidireccional.	Enumeración
domainlist	Lista de dominios enviados por el proceso al servidor DNS para su resolución y número de resoluciones por cada dominio.	{nombre_ dominio,numero#nombr e_dominio,numero}
domainname	Nombre del dominio al que el proceso intenta acceder/resolver.	Cadena de caracteres
entropía	Entropía del contenido del mensaje POST para categorizar la probabilidad de exfiltración de datos.	Numérico
errorcode	Código de error suministrado por el sistema operativo ante un inicio de sesión fallido. • **1073741724 (Invalid username)**: el nombre de usuario no existe. • **1073741730 (Login server is unavailable)**: el servidor necesario para validar el inicio de sesión no está disponible. • **1073741718 (Invalid password)**: el usuario es correcto pero la	Enumeración

Campo	Descripción	Tipo de campo
	contraseña es incorrecta. • **1073741715 (Invalid username or authentication info)**: el usuario o la información de autenticación es errónea. • **1073741714 (Invalid username or password)**: nombre desconocido o contraseña errónea. • **1073741260 (Account blocked)**: acceso bloqueado. • **1073741710 (Account disabled)**:cuenta deshabilitada. • **1073741713 (User account day restriction)**: intento de inicio de sesión en horario restringido. • **1073741712 (Invalid workstation for login)**: intento de inicio de sesión desde un equipo no autorizado. • **1073741604 (Sam server is invalid)**: error en el servidor de validación. No se puede realizar la operación. • **1073741421 (Account expired)**: cuenta caducada. • **1073741711 (Password expired)**: contraseña caducada. • **1073741517 (Clock difference is too big)**: los relojes de los equipos conectados tienen un desfase demasiado grande. • **1073741276 (Password change required on reboot)**: requiere que el usuario cambie la contraseña en el siguiente reinicio. • **1073741275 (Windows error (no risk))**: error de Windows que no	

Campo	Descripción	Tipo de campo
	implica riesgo. • **1073741428 (Domains trust failed)**: la solicitud de inicio de sesión falló porque la relación de confianza entre el dominio primario y el dominio confiable falló. • **1073741422 (Netlogon not initialized)**: intento de inicio de sesión, pero el servicio `Netlogon` no inicia. • **1073741074 (Session start error)**: error durante el inicio de sesión. • **1073740781 (Firewall protected)**: el equipo en el que se está iniciando sesión está protegido por un firewall de autenticación. La cuenta especificada no puede autenticarse en el equipo. • **1073741477 (Invalid permission)**: el usuario no tiene permisos para ese tipo de inicio de sesión.	
errorstring	Cadena de caracteres con información de depuración sobre la configuración del producto de seguridad.	Cadena de caracteres
eventtype	Tipo de evento registrado por el agente. • **1 (ProcessOps)**: proceso que realiza operaciones con el disco duro del equipo. • **14 (Download)**: descarga de datos ejecutada por el proceso. • **15 HostsFileModification**: modificación del fichero Hosts en sistemas Windows.	Enumeración

Campo	Descripción	Tipo de campo
	• **22 (NetworkOps)**: operación de red ejecutada por el proceso. • **25 EventNotBlocked**: el elemento no se bloqueó por estar el equipo en el proceso de inicio. • **26 (DataAccess)**: operación ejecutada por el proceso, que corresponde a un acceso a ficheros de datos alojados en dispositivos internos de almacenamiento masivo. • **27 (RegistryOps)**: el proceso accede al registro de Windows. • **30 (ScriptOps)**: operación ejecutada por un proceso de tipo script. • **31 (ScriptOps)**: operación ejecutada por un proceso de tipo script. • **40 (Detection)**: detección realizada por las protecciones activadas de Cytomic EDR. • **42 (BandwidthUsage)**: volumen de información manejada en cada operación de transferencia de datos ejecutada por el proceso. • **45 (SystemOps)**: operación ejecutada por el motor WMI del sistema operativo Windows. • **46 (DnsOps)**: acceso al servidor de nombres DNS ejecutado por el proceso. • **47 (DeviceOps)**: el proceso ejecuta un acceso a un dispositivo externo. • **50 (UserNotification)**: notificación que se le presenta al usuario junto a	

Campo	Descripción	Tipo de campo
	su respuesta si la hubiera. • **52 (LoginOutOps)**: operación de inicio o cierre de sesión efectuado por el usuario. • **99 (RemediationOps)**: eventos de detección, bloqueo y desinfección del agente Cytomic EDR o Cytomic EPDR. • **100 (HeaderEvent)**: evento administrativo con información de la configuración del software de protección, su versión e información del equipo y del cliente. • **199 (HiddenAction)**: evento de detección que no genera alerta. • **555 IOA**: evento de generación de IOA.	
exploitorigin	Origen del intento de explotación del proceso. • **1 (URL)**: dirección URL. • **2 (FILE)**: fichero.	Enumeración
extendedinfo	Información adicional sobre los eventos de tipo **Type**: • **0 (Command line event creation)**: vacío. • **1 (Active script event creation)**: Nombre del fichero del script. • **2 (Event consumer to filter consumer)**: vacío. • **3 (Event consumer to filter query)**: vacío. • **4 (Create User)**: vacío. • **5 (Delete User)**: vacío.	Cadena de caracteres

Campo	Descripción	Tipo de campo
	• **6 (Add user group)**: SID del grupo. • **7 (Delete user group)**: SID del grupo. • **8 (User group admin)**: SID del grupo. • **9 (User group rdp)**: SID del grupo.	
failedqueries	Número de peticiones de resolución DNS fallidas producidas por el proceso en la última hora.	Numérico
friendlyname	Nombre legible del dispositivo.	Cadena de caracteres
firstseen	Fecha en la que se ve el fichero por primera vez.	Fecha
headerhttp	Volcado de la cabecera HTTP cuando se detecta una comunicación por un túnel HTTP. Este campo solo incluye información si el modo auditoría del software de protección está activado.	Cadena de caracteres
hostname	Nombre del equipo que ejecuta el proceso.	Cadena de caracteres
initialdomain	Dominio origen cuando se detecta una redirección HTTP. Este campo solo incluye información si el modo auditoría del software de protección está activado.	Cadena de caracteres
infodiscard	Información interna del fichero de cuarentena.	Cadena de caracteres
IOAIds	Cuando una secuencia de eventos sigue un patrón descrito en la matriz MITRE, Cytomic Orion crea un indicio (IOA) y añade su identificador a todos los eventos que lo forman.	Numérico

Campo	Descripción	Tipo de campo
ipv4status	Tipo de direccionamiento IP: • **0 (Private)** • **1 (Public)**	Enumeración
isdenied	Indica si se ha denegado la acción reportada sobre el dispositivo.	Binario
islocal	Indica si la tarea se ha creado en el equipo local o en uno remoto.	Binario
interactive	Indica si es un inicio de sesión de usuario interactiva.	Binario
idname	Nombre del dispositivo.	Cadena de caracteres
key	Rama o clave del registro afectado.	Cadena de caracteres
lastquery	Última consulta del agente Cytomic EDR o Cytomic EPDR a la nube.	Fecha
localip	Dirección IP local del proceso.	Dirección IP
localport	Depende del campo **direction**: • **outgoing**: es el puerto del proceso que se ejecuta en el equipo protegido con Cytomic EDR y Cytomic EPDR. • **incoming**: es el puerto del proceso que se ejecuta en el equipo remoto.	Numérico
localdatetime	Fecha en formato UTC que tiene el equipo en el momento en que se produce el evento registrado. Esta fecha depende de la configuración del equipo y por lo tanto puede ser errónea.	Fecha
loggeduser	Usuario logueado en el equipo en el	Cadena de caracteres

Campo	Descripción	Tipo de campo
	momento de la generación del evento.	
machinename	Nombre del equipo que ejecuta el proceso.	Cadena de caracteres
manufacturer	Fabricante del dispositivo.	Cadena de caracteres
method	Método de la conexión HTTP cuando se detecta una comunicación a través de un túnel HTTP. • 1 - GET • 2 - POST Este campo solo incluye información si el modo auditoria del software de protección está activado.	Numérico
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres
objectname	Nombre único del objeto dentro de la jerarquía WMI.	Cadena de caracteres
opentstamp	Fecha de la notificación WMI cuando el evento es de tipo WMI_ CREATEPROC (54).	Máscara de bits
operation	Tipo de operación ejecutada por el proceso. • **0 (CreateProc)**: proceso creado. • **1 (PECreat)**: programa ejecutable creado. • **2 (PEModif)**: programa ejecutable modificado. • **3 (LibraryLoad)**: librería cargada. • **4 (SvcInst)**: servicio instalado.	Enumeración

Campo	Descripción	Tipo de campo
	• **5 (PEMapWrite)**: programa ejecutable mapeado para escritura. • **6 (PEDelet)**: programa ejecutable borrado. • **7 (PERenam)**: programa ejecutable renombrado. • **8 (DirCreate)**: carpeta creada. • **9 (CMPCreat)**: fichero comprimido creado. • **10 (CMOpened)**: fichero comprimido abierto. • **11 (RegKExeCreat)**: creada una rama del registro que apunta a un fichero ejecutable. • **12 (RegKExeModif)**: modificada una rama del registro que apunta a un fichero ejecutable. • **15 (PENeverSeen)**: programa ejecutable nunca visto en Cytomic Orion. • **17 (RemoteThreadCreated)**: hilo remoto creado. • **18 (ProcessKilled)**: proceso destruido. • **25 (SamAccess)**: acceso a la SAM del equipo. • **30 (ExploitSniffer)**: técnica Sniffer de explotación detectada. • **31 (ExploitWSAStartup)**: técnica WSAStartup de explotación detectada. • **32 (ExploitInternetReadFile)**: técnica InternetReadFile de explotación detectada.	

Campo	Descripción	Tipo de campo
	• **34 (ExploitCMD)**: técnica CMD de explotación detectada. • **39 (CargaDeFicheroD16bitsPorNtvdm.exe)**: carga de fichero de 16bits por ntvdm.exe. • **43 (Heuhooks)**: tecnología de antiexploit detectada. • **54 (Create process by WMI):** proceso creado por WMI modificado. • **55 (AttackProduct):** ataque detectado al servicio, a un fichero o a una clave de registro del agente. • **61 (OpenProcess LSASS):** apertura del proceso LSASS. • **89 (LoadDrvVulnerable)**: carga de driver vulnerable por un proceso después de iniciarse el sistema operativo. • **204 (MitreNopeDelete):** evento de MITRE que indica el borrado de un fichero no ejecutable.	
operationflags/ integrityLevel	Indica el nivel de integridad asignado por Windows al elemento. • **0x0000** Untrusted level • **0x1000** Low integrity level • **0x2000** Medium integrity level • **0x3000** High integrity level • **0x4000** System integrity level • **0x5000** Protected	Enumeración
operationstatus	Indica si el evento debe ser enviado a Cytomic Insights o no:	Numérico

Campo	Descripción	Tipo de campo
	• **0:** Enviar. • **1:** Filtrado por el agente. • **2:** No enviar.	
origusername	Usuario del equipo que realiza la operación.	Cadena de caracteres
pandaid	Identificador del cliente.	Numérico
pandaorionstatus	Indica el estado de la configuración horaria del equipo del cliente con respecto al reloj mantenido en Cytomic. • **0 (Version not supported)**: el cliente no soporta la sincronización de su configuración horaria con la de Cytomic. • **1: (Recalculated Panda Time)**: el cliente ha corregido su configuración horaria con la establecida en Cytomic. • **2: (Panda Time Ok)**: el cliente tiene establecida una configuración horaria correcta. • **3: (Panda Time calculation error)**: error al establecer la configuración horaria corregida.	Enumeración
pandatimestatus	Contenido de los campos DateTime, Date y LocalDateTime.	Fecha
parentattributes	Atributos del proceso padre. • **0x0000000000000001 (ISINSTALLER)**: fichero de tipo SFX (SelfExtractor). • **0x0000000000000002 (ISDRIVER)**: fichero de tipo Driver.	Enumeración

Campo	Descripción	Tipo de campo
	• **0x0000000000000008 (ISRESOURCESDLL)**: fichero de tipo DLL de recursos. • **0x0000000000000010 (EXTERNAL)**: fichero procedente de fuera del equipo. • **0x0000000000000020 (ISFRESHUNK)**: fichero añadido recientemente al conocimiento de Cytomic. • **0x0000000000000040 (ISDISSINFECTABLE)**: fichero con acción recomendada de desinfección. • **0x0000000000000080 (DETEVENT_ DISCARD)**: la tecnología de detección de contexto por eventos no ha realizado ninguna detección. • **0x0000000000000100 (WAITED_FOR_ VINDEX)**: fichero ejecutado sin haberse monitorizado su creación. • **0x0000000000000200 (ISACTIONSEND)**: las tecnologías locales no detectan malware en el fichero y éste se envía a Cytomic para su clasificación. • **0x0000000000000400 (ISLANSHARED)**: fichero almacenado en una unidad de red. • **0x0000000000000800 (USERALLOWUNK)**: fichero con permiso para importar DLL desconocidos. • **0x0000000000001000 (ISSESIONREMOTE)**: evento originado en una sesión remota. • **0x0000000000002000 (LOADLIB_**	

Campo	Descripción	Tipo de campo
	TIMEOUT): el tiempo transcurrido entre la interceptación de la carga de la librería y su análisis es mayor a 1 segundo, con lo que el análisis pasa de síncrono a asíncrono para no penalizar el rendimiento. • **0x0000000000004000 (ISPE)**: fichero ejecutable. • **0x0000000000008000 (ISNOPE)**: fichero de tipo no ejecutable. • **0x0000000000020000 (NOSHELL)**: el agente no detecta la ejecución de una shell en el sistema. • **0x0000000000080000 (ISNETNATIVE)**: fichero de tipo Net Native. • **0x0000000000100000 (ISSERIALIZER)**: fichero de tipo Serializer. • **0x0000000000200000 (PANDEX)**: fichero incluido en la lista de procesos creados por Cytomic Patch. • **0x0000000000400000 (SONOFGWINSTALLER)**: fichero creado por un instalador clasificado como goodware. • **0x0000000000800000 (PROCESS_ EXCLUDED)**: fichero excluido por las exclusiones de Cytomic Orion. • **0x0000000001000000 (INTERCEPTION_TXF)**: la operación interceptada tiene como origen un ejecutable cuya imagen en disco está siendo modificada. • **0x0000000002000000 (HASMACROS):** documento Microsoft Office con macros.	

Campo	Descripción	Tipo de campo
	• **0x0000000008000000 (ISPEARM):** fichero ejecutable para microprocesadores ARM. • **0x0000000010000000 (ISDYNFILTERED)**: fichero permitido en el equipo al no haber tecnologías que lo clasifiquen. • **0x0000000020000000 (ISDISINFECTED)**: fichero desinfectado. • **0x0000000040000000 (PROCESSLOST)**: operación no registrada. • **0x0000000080000000 (OPERATION_ LOST)**: operación con pre-análisis, de la que no se ha recibido el post-análisis. • **0x0000002000000000 (SAFE_BOOT_ MODE)**: el equipo se inició en modo seguro. • **0x0000004000000000 (PANDA_ SIGNED)**: fichero firmado con la firma de Panda Security.	
parentblake	Firma Blake2S del padre de la operación.	Cadena de caracteres
parentcount	Número de procesos con accesos DNS fallidos.	Numérico
parentmd5	Hash del fichero padre.	Cadena de caracteres
parentpath	Ruta del fichero padre que realizó la operación registrada.	Cadena de caracteres
parentpid	Identificador del proceso padre.	Numérico

Campo	Descripción	Tipo de campo
parentstatus	Estado del proceso padre. • **0 (StatusOk)**: estado OK. • **1 (NotFound)**: elemento no encontrado. • **2 (UnexpectedError)**: error desconocido. • **3 (StaticFiltered)**: fichero identificado como malware mediante información estática contenida en la protección de Cytomic EDR o Cytomic EPDR. • **4 (DynamicFiltered)**: fichero identificado como malware mediante tecnología local implementada en Cytomic EDR o Cytomic EPDR. • **5 (FileIsTooBig)**: fichero demasiado grande. • **6 (PEUploadNotAllowed)**: el envío de ficheros está desactivado. • **11 (FileWasUploaded)**: fichero enviado a la nube. • **12 (FiletypeFiltered)**: fichero de tipo DLL de recursos, Net Native o Serializer. • **13 (NotUploadGWLocal)**: fichero goodware no guardado en la nube. • **14 (NotUploadMWdisinfect)**: fichero malware desinfectado no guardado en la nube.	Enumeración
pecreationsource	Tipo de unidad donde fue creado el fichero: • **(0) Unknown**: el tipo de dispositivo no puede ser determinado.	Numérico

Campo	Descripción	Tipo de campo
	• **(1) No root dir**: ruta del dispositivo inválida. Por ejemplo, un medio de almacenamiento externo que ha sido extraído. • **(2) Removable media**: medio de almacenamiento extraíble. • **(3) Fixed media**: medio de almacenamiento interno. • **(4) Remote drive**: medio de almacenamiento remoto (por ejemplo unidad de red). • **(5) CD-ROM drive** • **(6) RAM disk**	
phonedescription	Descripción del teléfono si la operación involucró a un dispositivo de este tipo.	Cadena de caracteres
protocol	Protocolo de comunicaciones utilizado por el proceso. • **6 (TCP)** • **12 (RDP)** • **17 (UDP)**	Enumeración
querieddomaincount	Número de dominios diferentes con resolución fallida del proceso en la última hora.	Numérico
redirection	Se ha detectado una redirección HTTP. Este campo solo incluye información si el modo auditoría del software de protección está activado.	Booleano
regaction	Tipo de operación realizada en el registro del equipo. • **0 (CreateKey)**: crea una nueva	Enumeración

Campo	Descripción	Tipo de campo
	rama del registro. • **1 (CreateValue)**: asigna un valor a una rama del registro. • **2 (ModifyValue)**: modifica un valor de una rama del registro.	
remediationresult	Respuesta del usuario ante el mensaje emergente mostrado por Cytomic EPDR o Cytomic EDR. • **0 (Ok)**: el cliente acepta el mensaje. • **1 (Timeout)**: el mensaje emergente desaparece por la inacción del usuario. • **2 (Angry)**: el usuario elige rechazar el bloqueo desde el mensaje emergente. • **3 (Block)**: se produce un bloqueo porque el usuario no contesta al mensaje emergente. • **4 (Allow)**: el usuario acepta la solución. • **-1 (Unknown**)	Enumeración
remoteip	IP del equipo que inició la sesión remota.	Dirección IP
remotemachinename	Nombre del equipo que inicia la sesión remota.	Cadena de caracteres
remoteport	Depende del campo **direction**: • **incoming**: es el puerto del proceso que se ejecuta en el equipo protegido con Cytomic EDR y Cytomic EPDR. • **outcoming**: es el puerto del proceso que se ejecuta en el equipo remoto.	Numérico

Campo	Descripción	Tipo de campo
remoteusername	Nombre del equipo que inicia la sesión remota.	Cadena de caracteres
ruleid	Regla de Snort que detectó la comunicación a través de un túnel HTTP. Este campo solo incluye información si el modo auditoria del software de protección está activado.	Cadena de caracteres
sessiondate	Fecha de inicio del servicio del antivirus por última vez, o desde la última actualización.	Fecha
sessiontype	Tipo de creación o inicio de sesión: • **0 (System Only)**: sesión iniciada con una cuenta de sistema. • **2 (Local)**: sesión creada físicamente mediante un teclado o a través de KVM sobre IP. • **3 (Remote)**: sesión creada remotamente en carpetas o impresoras compartidas. Este tipo de inicio de sesión tiene autenticación segura. • **4 (Scheduled)**: sesión creada por el programador de tareas de Windows. • **-1 (Unknown)** • **5 (Service)**: sesión creada cuando arranca un servicio que requiere ejecutarse en la sesión de usuario. La sesión es eliminada cuando el servicio se detiene. • **7 (Blocked)**: un usuario intenta entrar en una sesión bloqueada previamente.	Enumeración

Campo	Descripción	Tipo de campo
	• **8 (Remote Unsecure)**: idéntico al tipo 3 pero la contraseña viaja en texto plano. • **9 (RunAs)**: sesión creada cuando se usa el comando "`RunAs`" bajo una cuenta diferente a la utilizada para iniciar la sesión, y especificando el parámetro "`/netonly`". Sin el parámetro "`/netonly`" se genera un tipo de sesión 2. • **10 (TsClient)**: sesión creada cuando se accede mediante "`Terminal Service`", "`Remote desktop`" o "`Remote Assistance`". Identifica una conexión de usuario remota. • **11 (Domain Cached)**: sesión de usuario creada con credenciales de dominio cacheadas en el equipo, pero sin conexión con el controlador de dominio.	
servicelevel	Modo de ejecución del agente. • **0 (Learning)**: el agente no bloquea ningún programa pero monitoriza los procesos ejecutados. • **1 (Hardening)**: el agente bloquea la ejecución de todos los programas sin clasificar cuyo origen no sea confiable, así como los programas clasificados como malware. • **2 (Block)**: el agente bloquea todos los ejecutables sin clasificar y los clasificados como malware. • **-1 (N/A)**	Enumeración
TelemetryType	• **0: telemetría normal**. El evento no pertenece a un indicio que siga un	Enumeración

Campo	Descripción	Tipo de campo
	patrón descrito en la matriz MITRE. • **1: evento reenviado**. El evento se envió inicialmente como tipo 0 (telemetría normal), pero tiempo después se ha detectado que pertenece a un patrón de ataque escrito en la matriz MITRE. El evento se vuelve a enviar con los campos TTPs e IOAIds completados. • **2: evento acumulado**: para ahorrar recursos, parte de la telemetría generada en el cliente se retiene hasta que el software de seguridad detecta un patrón de ataque MITRE. En ese momento se envían todos los eventos acumulados.	
timeout	El análisis en local tardó demasiado tiempo en completarse y el proceso se delega en otros mecanismos que no impacten en el rendimiento.	Booleano
times	Número de veces que se ha producido el mismo evento de comunicación en la última hora.	Numérico
timestamp	Marca de tiempo de la acción registrada en el equipo del cliente que genera el indicio.	Fecha
totalresolutiontime	Indica el tiempo que ha tardado la nube en responder, y si ha habido error en la consulta del código de error. • **0**: No se ha consultado a nube. • **>0:** Tiempo en ms que ha tardado la consulta a la nube. • **<0**: Código de error de la consulta a	Numérico

Campo	Descripción	Tipo de campo
	la nube.	
TTPs	Lista de las técnicas, tácticas y subtécnicas asociadas al evento MITRE.	Cadena de caracteres
type	Tipo de operación WMI ejecutada por el proceso. • **0 (Command line event creation)**: WMI lanza una línea de comandos como respuesta a un cambio en la base de datos. • **1 (Active script event creation)**: se ejecuta un script como respuesta a la recepción de un evento. • **2 (Event consumer to filter consumer)**: evento que se genera cada vez que un proceso se subscribe para recibir notificaciones. Se recibe el nombre del filtro creado. • **3 (Event consumer to filter query)**: evento que se genera cada vez que un proceso se subscribe para recibir notificaciones. Se recibe la consulta que ha ejecutado para suscribirse. • **4 (Create User)**: se añade una cuenta de usuario al sistema operativo. • **5 (Delete User)**: se borra una cuenta de usuario del sistema operativo. • **6 (Add user group)**: se añade un grupo al sistema operativo. • **7 (Delete user group)**: se borra un grupo dal sistema operativo. • **8 (User group admin)**: se añade un	Enumeración

Campo	Descripción	Tipo de campo
	usuario al grupo admin. • **9 (User group rdp)**: se añade un usuario al grupo rdp. • **18 (WFP filter operation)**: se crea o se elimina un filtro WFP (Windows Filtering Platform).	
uniqueid	Identificador único del dispositivo.	Cadena de caracteres
url	Url de descarga lanzada por el proceso que generó el evento registrado.	Cadena de caracteres
value	Tipo de operación realizada en el registro del equipo. • **0 (CreateKey)**: crea una nueva rama del registro. • **1 (CreateValue)**: asigna un valor a una rama del registro. • **2 (ModifyValue)**: modifica un valor en una rama del registro.	Enumeración
valuedata	Tipo del dato del valor contenido en la rama del registro. • **00 (REG_NONE)** • **01 (REG_SZ)** • **02 (REG_EXPAND_SZ)** • **03 (REG_BINARY)** • **04 (REG_DWORD)** • **05 (REG_DWORD_BIG_ENDIAN)** • **06 (REG_LINK)** • **07 (REG_MULTI_SZ)** • **08 (REG_RESOURCE_LIST)** • **09 (REG_FULL_RESOURCE_**	Enumeración

Campo	Descripción	Tipo de campo
	DESCRIPTOR) • **0A (REG_RESOURCE_REQUIREMENTS_LIST)** • **0B (REG_QWORD)** • **0C (REG_QWORD_LITTLE_ENDIAN)**	
vdetevent	Versión de la DLLdeteven.dll.	Cadena de caracteres
version	Versión del sistema operativo del equipo que ejecuta el software vulnerable.	Cadena de caracteres
versionagent	Versión del agente instalado.	Cadena de caracteres
versionbloomfilter	Versión del fichero bloomfilter que contiene la caché de goodware local.	Cadena de caracteres
versioncontroller	Versión de la DLL psnmvctrl.dll.	Cadena de caracteres
versiondetevenfilter	Versión del fichero de filtros para la tecnología de detección contextual (deteventfilter)	Cadena de caracteres
vtabledetevent	Versión de la DLL TblEven.dll.	Cadena de caracteres
vtableramsomevent	Versión de la DLL TblRansomEven.dll.	Cadena de caracteres
vramsomevent	Versión de la DLL RansomEvent.dll.	Cadena de caracteres
vantiexploit	Versión de la tecnología de antiexploit.	Cadena de caracteres
vtfilteraxtiexploit	Versión del filtro de la tecnología de antiexploit.	Cadena de caracteres
versionproduct	Versión del producto de protección instalado.	Cadena de caracteres

Campo	Descripción	Tipo de campo
winningtech	Tecnología del agente Cytomic EPDR o Cytomic EDR que provoca el evento. • **0 (Unknown)** • **1 (Cache)**: clasificación cacheada en local. • **2 (Cloud)**: clasificación descarga de la nube. • **3 (Context)**: regla de contexto local. • **4 (Serializer)**: tipo de binario. • **5 (User)**: premiso solicitado al usuario. • **6 (LegacyUser)**: permiso solicitado al usuario. • **7 (NetNative)**: tipo de binario. • **8 (CertifUA)**: detección por certificados digitales. • **9 (LocalSignature)**: firma local. • **10 (ContextMinerva)**: regla de contexto en la nube. • **11 (Blockmode)**: el agente estaba en modo hardening o lock cuando se bloqueó la ejecución del proceso. • **12 (Metasploit)**: ataque generado con el framework metaExploit. • **13 (DLP)**: tecnología Data Leak Prevention. • **14 (AntiExploit)**: tecnología de identificación de intento de explotación de proceso vulnerable. • **15 (GWFilter)**: tecnología de identificación de procesos goodware. • **16 (Policy)**: políticas de seguridad	Enumeración

Campo	Descripción	Tipo de campo
	avanzada de Cytomic EPDR. • **17 (SecAppControl)**: tecnologías control aplicaciones de seguridad. • **18 (ProdAppControl)**: tecnologías control aplicaciones de productividad. • **19 (EVTContext)**: tecnología contextual de Linux. • **20 (RDP)**: tecnología para detectar/bloquear ataques e intrusiones por RDP (Remote Desktop Protocol). • **21 (AMSI)**: tecnología para detectar malware en notificaciones AMSI. • **-1 (Unknown)**	
wsdocs	Lista de documentos abiertos codificada en base-64 cuando se produce un detección de exploit.	Cadena de caracteres

Tabla 18.1: Listado de los campos que conforman los eventos almacenados por Cytomic Orion

Glosario

A

Antivirus

Módulo de protección basado en tecnologías tradicionales (fichero de firmas, análisis heurístico, anti exploit etc), que detecta y elimina virus informáticos y otras amenazas.

API Integración

APIs de tipo REST que despliega para permitir su integración con herramientas de terceros o con aplicaciones desarrolladas en el propio SOC.

Aplicación (relativo a la API de integración)

Desarrollado realizado por terceros que quiere integrarse conCytomic Orion a través de la API de integración.

APT (Advanced Persistent Threat)

Conjunto de estrategias emprendidas por hackers orientadas a infectar la red del cliente, utilizando múltiples vectores de infección de forma simultánea para pasar inadvertidos a los antivirus tradicionales durante largos periodos de tiempo. Su objetivo principal es económico (robo de información confidencial de la empresa para chantaje, robo de propiedad intelectual etc) o político.

Archivo de identificadores / fichero de firmas

Fichero que contiene los patrones que el antivirus utiliza para detectar las amenazas.

ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge)

Conjunto de recursos desarrollados por la empresa Mitre Corp. para describir y categorizar los comportamientos peligrosos de los ciberdelincuentes, basados en observaciones a lo largo de todo el mundo. ATT&CK es una lista ordenada de comportamientos conocidos de los atacantes que se dividen en tácticas y técnicas, y se expresan a través de una matriz y también mediante STIX y TAXII. Ya que esta lista es una representación completa de los comportamientos que los hackers reproducen cuando se infiltran en las redes de las empresas, es un recurso útil para las organizaciones al desarrollar mecanismos tanto defensivos como preventivos y resolutivos.

C

CAS (Cytomic Authorization Server)

Servidor de autorización utilizado en la API de integración. Consulta "Servidor de autorización (relativo a la API de integración)" para más información.

Celda

Unidad mínima de un notebook que consiste en una caja de texto multilínea que alberga código en un lenguaje compatible con el kernel del notebook, y los resultados de su ejecución.

CKC (Cyber Kill Chain)

La empresa Lockheed-Martin describió en 2011 un nuevo marco o modelo para defender las redes informáticas, detallando que los ciberataques ocurren en fases y cada una de ellas puede ser interrumpida a través de controles establecidos. Desde entonces, la Cyber Kill Chain ha sido adoptada por organizaciones de seguridad de datos para definir las fases de los ataques cibernéticos. Estas fases abarcan desde el reconocimiento remoto de los activos del objetivo hasta la exfiltración de datos.

Client_id y client_secret (relativo a la API de integración)

Es el identificador y la contraseña asignado al cliente de Cytomic Orion. Para obtener un client_ id y client_secret contacta con el departamento comercial de Cytomic.

Cortafuegos

Ver Firewall.

CTI (Cyber Threat Intelligence)

Plataforma abierta para el intercambio de información de cyberseguridad que monitoriza, recopila y analiza potenciales ciberamenazas contra las organizaciones, facilitando el diseño de acciones defensivas y resolutivas.

CVE (Common Vulnerabilities and Exposures)

Lista de información definida y mantenida por Mitre Corp. sobre vulnerabilidades conocidas de seguridad. Cada referencia tiene un número de identificación único, ofreciendo una nomenclatura común para el conocimiento público de este tipo de problemas y así facilitar la compartición de datos sobre dichas vulnerabilidades.

D

Diagrama de grafos

Notebook que utiliza como fuente de información el flujo de telemetría que genera la infraestructura IT del cliente y representa de forma gráfica las entidades registradas y sus relaciones, facilitando al analista su interpretación.

Dirección IP

Número que identifica de manera lógica y jerárquica la interfaz de red de un dispositivo (habitualmente un ordenador) dentro de una red que utilice el protocolo IP.

DNS (Domain Name System)

Servicio que traduce nombres de dominio con información de diversos tipos, generalmente direcciones IP.

E

EDR (Endpoint Detection & Response)

EDR es la respuesta al hecho de que el antivirus tradicional nunca podrán evitar todos los ataques cibernéticos. El EDR asume que las amenazas evitarán las defensas de prevención, por lo que se enfoca en monitorizar los equipos para detectar comportamientos que indiquen actividad maliciosa, y captura datos para investigaciones de seguridad. La mayoría de los EDRs tiene algún nivel de respuesta automatizada pero dependiendo del tiempo de exposición de la amenaza antes de que sea descubierta, pueden requerirse iniciativas de resolución manuales. Al igual que con NGAV, las soluciones EDR utilizan técnicas de ML (Machine Learning) y AI (Inteligencia Artificial) para extrapolar y determinar si un comportamiento es malicioso, basándose en grandes conjuntos de datos que se actualizan constantemente.

Evento

Cada una de las acciones relevantes monitorizadas por Cytomic EDR o Cytomic EPDR ejecutadas por los procesos en el equipo de usuario o servidor genera un evento que es enriquecido y enviado a la plataforma Cytomic Orion. Allí se almacena en el océano de datos para que el analista pueda investigarlo posteriormente de forma individual o en conjunto con el resto de eventos producidos.

Exploit

De forma general un exploit es una secuencia de datos especialmente diseñada para provocar un fallo controlado en la ejecución de un programa vulnerable. Después de provocar el fallo, el proceso comprometido interpretará por error parte de la secuencia de datos como código ejecutable, desencadenando acciones peligrosas para la seguridad del equipo.

F

Firewall

También conocido como cortafuegos, es una tecnología que bloquea el tráfico de red que coincide con patrones definidos por el administrador mediante reglas. De esta manera, se limita o impide la comunicación de ciertas aplicaciones que se ejecutan en los equipos, restringiéndose la superficie de exposición del equipo.

G

GDPR (General Data Protection Regulation)

Normativa que regula la protección de los datos de los ciudadanos que viven en la Unión Europea.

Geolocalizar

Posicionar en un mapa un dispositivo en función de sus coordenadas.

Goodware

Fichero clasificado como legítimo y seguro tras su estudio.

I

IdP (Identity Provider)

Servidor de autenticación utilizado por en la API de integración. Consulta "Servidor de autenticación (relativo a la API de integración)" para más información.

Indicio

Hipótesis generada por Cytomic Orion que advierte al analista de nivel 1 del MSSP / MDR / SOC de la detección de un patrón TTP descrito en una regla de hunting dentro el océano de datos.

Investigación

Repositorio de datos compartido creado por los analistas de nivel 1 del MSSP / MDR / SOC y alimentado por los analistas de nivel 2 y 3 con los hallazgos producidos en el transcurso de una investigación.

IOCs

Estándar de la industria que permite describir condiciones susceptibles de comprometer la seguridad de las organizaciones. Siendo un concepto similar al del fichero de firmas utilizado por las herramientas de protección contra el malware, su formato es abierto, con lo que se favorece su compartición e intercambio y permite al administrador extender de forma sencilla las capacidades de detección de la solución de seguridad instalada en los equipos de la red.

L

Librería Threat hunting

Librería Python implementada en Cytomic Orion y utilizada por los analistas en los notebooks para acelerar la automatización de sus investigaciones.

M

Malware

Término general utilizado para referirse a programas que contienen código malicioso (MALicious softWARE), ya sean virus, troyanos, gusanos o cualquier otra amenaza que afecte a la seguridad e integridad de los sistemas informáticos. El malware se infiltra y daña un ordenador sin el conocimiento de su dueño, con finalidades muy diversas.

MD5 (Message-Digest Algorithm 5)

Algoritmo de reducción criptográfico que obtiene una firma (hash o digest) de 128 bits que representa de forma única una serie o cadena de entrada. El hash MD5 calculado sobre un fichero sirve para su identificación unívoca o para comprobar que no fue manipulado / cambiado.

MDR (Managed Detection and Response)

Es una nueva clase de servicio de seguridad que agrupa a expertos, tecnología propia y los conocimientos prácticos necesarios para superar las deficiencias del modelo MSSP al buscar, investigar y resolver de forma proactiva amenazas informáticas rápidamente.

MITRE (The MITRE Corporation)

Empresa sin ánimo de lucro que opera múltiples centros de investigación y desarrollo financiados con fondos federales dedicados a abordar problemas relativos a la seguridad. Ofrecen soluciones prácticas en los ámbitos de defensa e inteligencia, aviación, sistemas civiles, seguridad nacional, judicatura, salud y ciberseguridad. Son los creadores del framework ATT&CK.

Movimientos laterales

Operaciones realizadas por los hackers dentro de la red corporativa mediante las cuales se busca ganar una posición de ventaja que permita alcanzar sus objetivos. Generalmente implica la propagación de malware a otros equipos de la red, instalación de puertas traseras que faciliten el acceso a las distintas subredes de la empresa etc.

MSSP

Empresas que ofrecen servicios de seguridad administrados para aquellas organizaciones que quieran externalizarlos o subcontratarlos.

MUID

Cadena de caracteres que Cytomic Orion utiliza para identificar de forma única cada estación de trabajo o servidor del cliente.

N

NGAV

A diferencia de los antivirus tradicionales que fundamentalmente basan sus capacidades de detección en los ficheros de firmas alojados en local, en la nube o en una mezcla de ambos, los NGAV utilizan técnicas avanzadas para detectar el malware. Pueden incorporar técnicas de auto aprendizaje (Machine Learning), detección de exploits, uso de IOCs (indicadores de compromiso), análisis de metadatos y otras técnicas, para buscar los TTPs utilizados por los atacantes.

NGFW

Es la evolución natural de un cortafuegos al que se le añaden funcionalidades avanzadas de detección de malware, filtrado de contenidos, filtrado del tráfico web, servicios de VPN, acceso remoto a la red y sistemas de detección de intrusos, entre otros.

Nivel

División interna de la plantilla de técnicos que pertenecen a un SOC / MSSP / MDR según diversos criterios, como pueden ser sus conocimientos técnicos de las infraestructuras de sus clientes, habilidades de comunicación, conocimientos de programación etc.

Notebook

Representación web de todas las entradas y salidas que se han producido a lo largo del tiempo en torno a uno o varios fragmentos de código ejecutados de forma interactiva, incluyendo explicaciones en formato texto, imágenes y representaciones de objetos más elaboradas.

Nube (Cloud Computing)

Término que se utiliza para describir una red mundial de servidores conectados para funcionar como un único ecosistema y diseñados para almacenar y administrar datos, ejecutar aplicaciones o entregar contenido o servicios (streaming de vídeos, correo web, software de ofimática, servicios de seguridad etc). En lugar de acceder a archivos y datos desde un equipo personal o local, el usuario accede a ellos en línea desde cualquier dispositivo conectado a Internet, es decir, la información está disponible dondequiera que vaya y siempre que la necesite.

O

OAuth (Open Authorization)

Estándar abierto muy utilizado en la industria para permitir el acceso delegado a recursos protegidos. El principal escenario para el que OAuth fue diseñado es el de un usuario que necesita otorgar permisos de acceso a información protegida a sitios web o aplicaciones de terceros, pero sin necesidad de compartir sus credenciales. Por lo tanto, OAuth proporciona un

acceso delegado seguro a los recursos del propietario en su nombre, y especifica los procesos necesarios para que éste autorice el acceso a terceros sin compartir sus credenciales.

Océano de datos

Acumulación de toda la telemetría generada por los procesos ejecutados en los equipos de usuario y servidores y almacenada en los servidores deCytomic Orion, donde el analista puede ejecutar búsquedas para realizar sus análisis.

P

Phishing

Intento de conseguir de forma fraudulenta información confidencial de un usuario mediante el engaño. Normalmente la información que se trata de lograr tiene que ver con contraseñas, tarjetas de crédito, cuentas bancarias o información que pueda ser utilizada para facilitar el acceso remoto del atacante a la red de la organización.

Plantilla

Notebook que los analistas toman como base para desarrollar la automatización de sus investigaciones. Al no comenzar desde 0 cada nuevo análisis, las plantillas aceleran el desarrollo y adicionalmente favorecen la reutilización y compartición de notebooks.

Proceso comprometido

Son aquellos procesos vulnerables que han sido afectados por un exploit y pueden comprometer la seguridad del equipo.

Proceso vulnerable

Son programas que, debido a fallos de programación, no son capaces de interpretar correctamente los datos recibidos de otros procesos. Al recibir una secuencia de datos especialmente diseñada (exploit), los hackers pueden provocar un mal funcionamiento del proceso, induciendo la ejecución de código que compromete la seguridad del equipo.

Programas potencialmente no deseados (PUP)

Son programas que se introducen de forma invisible o poco clara en el equipo aprovechando la instalación de otro programa que es el que realmente el usuario desea instalar.

Python

Lenguaje de programación multiparadigma, interpretado y multiplataforma cuya filosofía hace hincapié en una sintaxis que favorece la generación de código legible. Posee una licencia de código abierto compatible con la Licencia pública general de GNU a partir de la versión 2.1.1.

R

Radar de ciber-ataques

Motor de búsqueda implementado en que toma como entrada el océano de datos formado por la telemetría recogida de los equipos de usuario y las reglas de hunting, que describen las TTPs (Tácticas, Técnicas y Procedimientos) empleados por los hackers. Cuando el Radar de ciber-ataques detecta una TTP genera un indicio.

Regla de Hunting

Descripción de una TTP (Tácticas, Técnicas y Procedimientos) reconocida por Cytomic Orion utilizada por el Radar de ciber-ataques para buscar en el océano de datos patrones de ejecución sospechosos de pertenecer a un ataque informático.

Regla de notificación

Envía los indicios detectados en los equipos de uno o más clientes a una o varias cuentas de correo con el objetivo de evitar que el analista acceda de forma recurrente a la consola de análisis para comprobar el estado del parque informático de los clientes que investiga.

Responsive / Adaptable (RWD, Responsive Web Design)

Conjunto de técnicas que permiten desarrollar páginas Web que se adaptan de forma automática al tamaño y resolución del dispositivo utilizado para visualizarlas.

Respuestas Rápidas

Pequeños bloques de código independientes que resuelven problemas concretos y que el analista puede incorporar en los notebooks para acelerar la automatización de sus investigaciones.

Rol

Configuración específica de permisos que se aplica a una o más cuentas de usuario y autoriza a ver o modificar determinados recursos de la consola.

S

SCM (Secure Content Management)

Dispositivos de red que operan de forma transparente para ofrecer contenidos seguros de Internet a los usuarios de una red corporativa. Integran sistemas de antivirus de red, firewall (cortafuegos), sistema de detección/prevención de intrusos (IDS / IPS), sistemas para filtrado web, protección antispam etc.

Servidor de autenticación (relativo a la API de integración)

Sistema que crea y valida las credenciales correspondientes a la cuenta de la aplicación que utiliza la API de integración, enviadas por las aplicaciones de terceros.Cytomic Orion delega en

el servidor IdP (Cytomic Identity Provider) las tareas de validación de las credenciales.

Servidor de autorización (relativo a la API de integración)

Servidor con el que la aplicación que utiliza la API de integración interactúa cuando solicita acceso a un recurso protegido. Cytomic Orion delega en el servidor CAS (Cytomic Authorization Server) esta tarea.

SIEM (Security Information and Event Management)

Herramientas que combinan la gestión de la información y de los eventos de seguridad generados en la infraestructura IT del cliente, proporcionando un análisis en tiempo real de las alertas de seguridad generadas por las aplicaciones y el hardware de red.

SOC (Centro de operaciones de Seguridad)

Departamento dentro de las organizaciones que previene, monitoriza y controla la seguridad en la infraestructura IT de la empresa.

Sospechoso

Programa que, tras un análisis de su comportamiento realizado en el equipo del usuario por el software de protección instalado, tiene una alta probabilidad de ser considerado malware.

SQL (Structured Query Language)

Lenguaje de programación estándar e interactivo para obtener información de una base de datos, así como para actualizarla. Aunque SQL es a la vez un ANSI y una norma ISO, muchos productos de bases de datos soportan SQL con extensiones propietarias al lenguaje estándar. Las consultas toman la forma de un lenguaje de comandos que permite seleccionar, insertar, actualizar y averiguar la ubicación de los datos, entre otras operaciones.

T

Telemetría

Información recuperada de los equipos de usuario y servidores que se envía a la infraestructura de alojada en la nube para conformar el océano de datos. La telemetría es el resultado del enriquecimiento de la información que proviene de la monitorización de los procesos ejecutados con los datos suministrada por la solución de protección avanzada instalada en el equipo.

Threat hunter

Analista especializado en la investigación de indicios dentro de la actividad de la infraestructura IT de las empresas, que pueden derivar en el descubrimiento de ataques informáticos que operan sin ser detectados por las soluciones de seguridad tradicionales instaladas en los equipos.

Threat hunting

Conjunto de tecnologías y recursos humanos especializados que permiten detectar los movimientos laterales y otros indicadores tempranos de las amenazas, antes de que ejecuten acciones nocivas para la empresa.

Ticketing

Herramientas que garantizan la correcta gestión de los indicios, permitiendo crear, asignar y seguir los casos hasta su cierre, así como la recogida de KPIs que muestren el grado de cumplimiento del servicio de seguridad del SOC.

Tiempo de exposición (dwell time)

Tiempo que una amenaza ha permanecido sin ser detectada en un equipo de la red.

Token de acceso

Es la cadena de caracteres utilizada por la aplicación de terceros para acceder al recurso protegido (la API) de Cytomic Orion. El token de acceso describe el ámbito de acceso, la duración y otra información relevante. Los tokens son opacos para la aplicación cliente, son emitidos por el servidor CAS y solo tienen significado para éste.

Token de refresco

Cuando una aplicación que usa el API de integración accede al recurso protegido por primera vez Cytomic Orion le entrega un token de acceso y un token de refresco. Cuando el token de acceso caduca, la aplicación solicita uno nuevo mediante el token de refresco sin necesidad de volver a iniciar el proceso de autenticación y autorización.

Triaje de indicios

Conjunto de comprobaciones desarrolladas por los técnicos de nivel 1 del MPPS / MDR / SOC para filtrar los indicios generados por Cytomic Orion y así entregar al nivel 2 unicamente aquellos casos con mayor probabilidad de pertenecer a un ataque informático real. El triaje de indicios elimina los falsos positivos, descongestionando el nivel 2 del SOC.

TTP (Tactics, Techniques and Procedures)

Una TTP describe el enfoque utilizado por un ataque informático para analizar sus operaciones y para perfilar el origen de la amenaza. La Táctica describe la forma en que un adversario elige llevar a cabo su ataque desde el comienzo hasta el final. La Técnica describe el enfoque tecnológico para lograr resultados intermedios durante el ataque. Los procedimientos definen el enfoque organizativo del ataque. Conocer las tácticas de un adversario ayuda a predecir los próximos ataques y detectarlos en las etapas iniciales. La comprensión de las técnicas utilizadas durante el ataque permite identificar los puntos ciegos de la organización e implementar contramedidas de antemano. Finalmente, el análisis de los procedimientos

utilizados por el adversario puede ayudar a comprender lo que el adversario está buscando dentro de la infraestructura del objetivo.

U

Usuario (consola)

Recurso formado por un conjunto de información que Cytomic Orion utiliza para regular el acceso de los administradores a la consola web y establecer las acciones que éstos podrán realizar sobre los equipos de la red.

Usuario (red)

Trabajadores de la empresa que utilizan equipos informáticos para desarrollar su trabajo.

UTM (Unified Threat Management)

Dispositivos de red con múltiples funciones relativas a la seguridad, entre las que se encuentran antivirus de red, firewall (cortafuegos), sistema de detección/prevención de intrusos (IDS / IPS), sistemas para filtrado web, protección antispam etc. Los dispositivos UTM están diseñados para proteger redes completas de equipos de usuario o servidores, así como pueden integrar otros servicios relacionados con la seguridad, tales como puntos finales de redes privadas, servicio de proxy etc.

V

VDI (Virtual Desktop Infrastructure)

Solución de virtualización de escritorio que consiste en alojar máquinas virtuales en un centro de datos al cual los usuarios acceden desde un terminal remoto con el objetivo de centralizar y simplificar la gestión y reducir los costes de mantenimiento. Se distinguen dos grupos de entornos VDI: Persistente: el espacio de almacenamiento asignado a cada usuario se respeta entre reinicios, incluyendo el software instalado, datos y actualizaciones del sistema operativo. No persistente: el espacio de almacenamiento asignado a cada usuario se elimina cuando la instancia VDI se reinicia, restaurándose a su estado inicial y deshaciendo todos los cambios efectuados.

Vector de infección

Puerta de entrada o procedimiento utilizado por el malware para infectar el equipo del usuario. Los vectores de infección más conocidos son la navegación web, el correo electrónico y los pendrives.

Ventana de oportunidad

Tiempo que transcurre desde que el primer equipo fue infectado a nivel mundial por una muestra de malware de reciente aparición hasta su estudio e incorporación a los ficheros de firmas de los antivirus para proteger a los equipos de su infección. Durante este periodo de

tiempo el malware puede infectar equipos sin que los antivirus tradicionales sean conscientes de su existencia, y queda en manos de las protecciones avanzadas y threat hunters su detección y contención.

W

Widget (Panel)

Panel formado por un gráfico configurable que representa un aspecto concreto de la seguridad de la red del cliente. El conjunto de widgets forma el dashboard o panel de control de Cytomic Orion.