CYTOMIC

Guía de administración
Cytomic Data Watch_

Aviso legal.

Marcas registradas.

Información de contacto.

Oficinas centrales:
Cytomic (Unidad de Negocio de Panda Security)
Calle Santiago de Compostela 12
Bilbao (Bizkaia) 48003 España.
https://www.pandasecurity.com/spain/about/contact/

Versión: 3.62.00-01

Autor: Cytomic

Fecha: 05/10/2020

Acerca de la Guía de administración

Para obtener la versión más reciente de esta guía consulta la dirección web:

https://info.cytomicmodel.com/guides/DataWatch/es/DATAWATCH-Guia-ES.pdf

Guía de administración de Cytomic EDR y Cytomic EDPR

https://info.cytomicmodel.com/guides/EPDR/latest/es/EPDR-guia-ES.pdf

https://info.cytomicmodel.com/guides/EDR/latest/es/EDR-guia-ES.pdf

Información técnica sobre módulos y servicios compatibles con Cytomic Data Watch

Para acceder a la Guía de administración de Cytomic Insights consulta la siguiente URL:

https://info.cytomicmodel.com/resources/guides/Insights/es/INSIGHTS-guia-ES.pdf

Soporte técnico

Cytomic ofrece un soporte técnico global cuyo objetivo principal es responder a cuestiones especificas sobre el funcionamiento de sus productos. El equipo de soporte técnico también genera documentación sobre detalles técnicos del producto, que ofrece a través de su portal eKnowledge Base.

- Para acceder a información específica del producto consulta la siguiente URL:

https://www.cytomic.ai/es/soporte/data-watch/

Encuesta sobre la Guía de administración

Evalúa esta guía para administradores y enviamos sugerencias y peticiones para próximas versiones de la documentación en:

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

Tabla de contenidos

Parte 1: Introducción a Cytomic Data Watch

Parte 2: Recursos de Cytomic Data Watch

Parte 1

Introducción a Cytomic Data Watch

Capítulo 1

Prólogo

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

CONTENIDO DEL CAPÍTULO

¿A quién está dirigida esta guía?

La presente documentación está dirigida al personal técnico del departamento de IT de las empresas que tengan contratado el servicio Cytomic Data Watch para los productos Cytomic EDR y Cytomic EDPR.

En este manual técnico se recogen los procedimientos y configuraciones necesarios para interpretar y sacar provecho de la información de seguridad suministrada por la plataforma Cytomic Data Watch

Todos los procedimientos e indicaciones en esa guía técnica aplican tanto al producto Cytomic EDR como Cytomic EDPR. En esta documentación se menciona “Cytomic EDR” de forma genérica, englobando ambos productos de seguridad avanzada.

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.

Consejo importante de cara a un uso correcto de las opciones de Cytomic Data Watch.

Consulta en otro capítulo o punto del manual.

Capítulo 2

Introducción al servicio

Cytomic Data Watch es un módulo de seguridad integrado en el producto Cytomic EDR que ayuda a cumplir con las regulaciones y a dar visibilidad y supervisar la información almacenada en la infraestructura IT de las empresas.

CONTENIDO DEL CAPÍTULO

Estado actual de las regulaciones de protección de datos

El desarrollo de nuevas regulaciones sobre protección de datos, unido al considerable incremento de amenazas avanzadas en circulación, han provocado un gran interés en la renovación de los protocolos de seguridad que protegen la información personal de clientes y trabajadores de las empresas. Esta información personal, sin importar el estado en que se encuentre (en uso - *data in use*, en tránsito - *data in motion* o almacenada - *data in rest*) tiene que cumplir con nuevos requisitos de seguridad, que se desprenden de:

- **El cumplimiento de nuevas regulaciones europeas**: desde mayo del 2018 la GDRP aplica multas de hasta 20M€ o el 4% de la facturación anual del periodo anterior por su incumplimiento. Todas las empresas de la UE que recopilen y almacenen datos personales (*PII*) de sus empleados, clientes y proveedores residentes en la UE estarán afectadas.
- **El mayor volumen de datos no estructurados en las empresas**: la información almacenada en ficheros ofimáticos (Word, Excel, archivos de texto, html, etc.) representa el 80% de los datos manejados por las organizaciones. Toda esta información se encuentra dispersa sin control por servidores, dispositivos y portátiles de empleados y colaboradores (partners, consultores, etc.).
- **La publicación de datos confidenciales**: cada vez son más frecuentes los casos en los que un ataque informático revela de forma masiva información personal de clientes. Estos ataques son llevados a cabo por actores con motivaciones muy diversas: desde atacantes externos con objetivos lucrativos, a insiders negligentes o malintencionados.

Las buenas prácticas en el gobierno de la seguridad de los datos (*Data Security Governance*) son la clave para mitigar estos riesgos y asegurar el éxito en el cumplimiento de las regulaciones.

Requisitos en la protección de datos personales

De estas nuevas necesidades en la protección de datos personales surgen requisitos de alto nivel para las organizaciones, entre los que se cuentan:

- Controlar los datos personales distribuidos en un número indeterminado de ficheros sin estructura interna, que residen en puestos y servidores a los que acceden cientos de usuarios autorizados.
- Demostrar el cumplimiento de la ley vigente en cualquier momento mediante monitorización continua.
- Notificar las filtraciones de datos a la autoridad local (*DPA - Data Protection Authority*) y a los clientes afectados en un plazo de 72 horas.

Estos requisitos se deben cubrir sin incrementar la complejidad del conjunto de productos y herramientas utilizadas por la organización para gestionar la seguridad de las infraestructuras IT.

Principales beneficios de Cytomic Data Watch

Los ficheros clasificados como PII (Personally Identifiable Information) son archivos que contienen información que permite identificar a personas que guardan algún tipo de relación con la empresa

(clientes, trabajadores, proveedores, etc.). Esta información es de carácter personal y su tipo es muy variado, entre los que se cuentan números de la seguridad social, números de teléfono y direcciones de correo electrónico, entre otros. Cytomic Data Watch descubre, audita y monitoriza en tiempo real el ciclo de vida completo de los ficheros PII: desde datos en reposo, las operaciones efectuadas sobre ellos y su transferencia al exterior.

Cytomic Data Watch no se ciñe únicamente al control de los ficheros con información personal: sus capacidades de monitorización se pueden ampliar a cualquier tipo de fichero, como por ejemplo aquellos que contengan información confidencial o delicada para la empresa.

Descubre y audita

- Localiza e Identifica los ficheros almacenados en los equipos de los usuarios, en su correo electrónico y en los servidores de la red que Cytomic Data Watch ha clasificado como PII o que coinciden con las reglas de monitorización definidas por el administrador.
- Reduce el riesgo de filtraciones y evalúa la eficiencia de las políticas de seguridad existentes, ofreciendo información clave para alimentar su diseño y facilitar la comunicación de buenas prácticas y medidas de protección adicionales a los usuarios.

Monitoriza y detecta

- Implementa medidas proactivas de acceso y operación sobre los ficheros encontrados mediante informes y alertas en tiempo real que reflejan su uso y comunicación sospechosa o no autorizada.
- Para evitar multas y daños a la reputación de las empresas, las alertas notifican inmediatamente del posible robo de información. Los datos recogidos en las tablas de Cytomic Data Watch, los paneles y los informes predefinidos permiten analizar en tiempo real el ciclo de vida completo de un incidente: quién hizo cada operación, cuándo, dónde, en qué equipo o servidor, y cuál es el medio utilizado para ello.

Simplifica la gestión

Cytomic Data Watch es un módulo de Cytomic EDR y Cytomic EDPR, y por lo tanto no requiere ningún despliegue adicional: su activación es inmediata, desatendida para el administrador y gestionada desde la misma plataforma Cloud, de forma muy rápida y sencilla.

Cytomic Data Watch y la GDPR

GDPR (*General Data Protection Regulation - Regulación General de Protección de datos*) es el nuevo marco legal en la Unión Europea que remplaza a la anterior Directiva de Protección de Datos.

Su objetivo es proteger la información que puede ser utilizada para identificar a las personas y ofrecer una referencia en el desarrollo de procedimientos seguros para procesar, almacenar y, finalmente, destruir los datos personales gestionados por las organizaciones, cuando éstos ya no sean necesarios.

La GDPR concede ocho derechos específicos a los individuos acerca de cómo las compañías pueden usar la información que esté directa y personalmente relacionada con ellos.

- Derecho a estar informado.
- Derecho al acceso
- Derecho a la corrección "Rectificación"
- Derecho de eliminación "Derecho a ser olvidado".
- Derecho a restringir el procesamiento.
- Derecho a la portabilidad de los datos.
- Derecho a objetar el procesamiento.
- Derecho a no ser sujeto de toma de decisiones automáticas.

Además, establece normas muy estrictas que rigen lo que sucede si se viola el acceso a datos personales y las consecuencias sanciones que las organizaciones pueden sufrir en tal caso.

Artículos de la GDPR relacionados con Cytomic Data Watch

Cytomic Data Watch ayuda a cumplir con los artículos de la GDPR mostrados a continuación:

- **Artículo 17: derecho de supresión ("el derecho al olvido")**

Requiere implementar los recursos necesarios para garantizar el borrado sin retrasos de los datos personales almacenados en la empresa, bajo petición del cliente.

Cytomic Data Watch permite configurar búsquedas personalizadas para localizar los ficheros donde aparecen datos de las personas que deseen ejercitar su derecho de supresión.

- **Artículo 32: seguridad de datos personales**

Requiere aplicar medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo. Además, debe evaluar los peligros del tratamiento de los datos personales, estableciendo medidas de control de acceso y uso.

Cytomic Data Watch ofrece información sobre los ficheros PII accedidos por los usuarios, en qué equipos y qué tipo de operaciones están ejecutando. De esta forma es posible comprobar que el acceso a la información personal solo lo llevan a cabo las personas autorizadas para su tratamiento, y el grado de efectividad de las políticas establecidas por la compañía en lo relativo a la gestión de PII.

- **Artículo 33: Notificación de una violación de seguridad a la autoridad de control**

Requiere una notificación a la autoridad competente en un plazo no superior a 72 horas cuando se produce una violación de seguridad de los datos personales, si ésta constituye un riesgo para los derechos y las libertades de las personas físicas.

Cytomic Data Watch analiza el incidente para valorar el impacto. Por un parte, muestra qué equipos, usuarios y ficheros han sido comprometidos y, por otra, revela el tipo de filtración: si se ha producido

por ejecutar malware, por comunicar de forma no autorizada información al exterior o si se trata movimientos laterales (infiltración) llevados a cabo desde dentro de la compañía.

- **Artículo 35: evaluación del impacto relativo a la protección de datos**

Requiere una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales cuando sea probable que ese tipo de tratamiento en particular por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas.

Cytomic Data Watch identifica de forma automática los ficheros que contienen información disponible para identificar a personas y monitoriza no solo las operaciones que se realizan sobre éstos, sino también a los usuarios que las ejecutan. De esta manera es posible conocer la cantidad, tipología, volumen o uso de la información personal, y evaluar el impacto y el riesgo en su tratamiento.

- **Artículo 39: funciones del delegado de protección de datos**

Requiere la figura del DPO (delegado de protección de datos) para supervisar el cumplimiento del Reglamento, ofrecer el asesoramiento sobre la evaluación del impacto relativa a la protección de datos y actuar como contacto para cuestiones acerca de su tratamiento.

Cytomic Data Watch aporta al DPO herramientas gráficas en las que apoyarse para cumplir con su labor de supervisión, asesoramiento y entendimiento de los riesgos asociados a las operaciones de tratamiento.

Funciones de Cytomic Data Watch relacionadas con la GDPR

La información base sobre la cual Cytomic Data Watch construye toda la inteligencia de seguridad para el tratamiento de datos personales se resume en:

Información	Campos / operaciones
Descubrimiento / clasificación automática de los ficheros sin estructura interna como PIIF o no PIIF.	
Información sobre los ficheros PII.	• Nombre. • Tipo. • Extensión. • Tamaño. • Tipo de información personal encontrada en el fichero.
Información de los correos electrónicos que contienen ficheros monitorizados	• Origen y destino del correo electrónico. • Fecha de envío y recepción del correo electrónico. • Tamaño, nombre y hash del fichero encontrado en el mensaje de correo.

Tabla 2.1: información base recogida de los equipos de usuario

Información	Campos / operaciones
Clasificación de los procesos que actúan sobre ficheros PIIs.	• Malware. • Pendiente de clasificar. • Goodware.
Tipo de operación ejecutada sobre ficheros PIIs.	• Creación • Apertura • Renombrado • Borrado • Copia - Pega
Clasificación de las operaciones ejecutadas sobre ficheros PII.	• Operaciones de fuga o comunicación de datos (data exfiltration). • Operaciones de introducción de datos (data infiltration).
Usuarios que actúan sobre los ficheros PII.	
Localización de los equipos con PII en la infraestructura IT de la organización.	

Tabla 2.1: información base recogida de los equipos de usuario

Características del servicio Cytomic Data Watch

Cytomic Data Watch despliega en el equipo tecnología diseñada específicamente para recoger información detallada sobre los ficheros PII encontrados en el mismo, así como de los ficheros definidos por el administrador. Dicha información es recibida por la plataforma Threat Intelligence Platform, donde es procesada y enriquecida para ser posteriormente enviada a la herramienta Advanced Visualization Tool para su presentación y visualización avanzada.

Descubrimiento

- Creación de un inventario de los ficheros sin estructura interna que contienen entidades que identifican a personas, junto al número total de éstas encontrado en cada fichero, para determinar su relevancia.
- Información de las características de los ficheros encontrados.
- Visualización de los equipos que contienen ficheros localizados mediante las reglas de monitorización configuradas por el administrador de la red.
- Visualización de las características de los mensajes de correo que contienen ficheros adjuntos clasificados como PII, o que coinciden con las reglas de monitorización establecidas por el administrador de la red.

Monitorización

- Seguimiento de las operaciones efectuadas sobre ficheros clasificados como PII o que cumplan

con alguna de las reglas de monitorización establecidas por el administrador (data in use).

- Mantenimiento del inventariado de los archivos PII almacenados en cada equipo de la empresa (data at rest).
- Registro de las operaciones de copia y transferencia de ficheros entre equipos (data in motion), indicando su origen (cliente de correo, navegador, FTP, etc.).

Visualización

- Sincronización en tiempo real con el servidor Cytomic Data Watch para mostrar los resultados del descubrimiento y la monitorización continua de ficheros.
- Herramientas para explotar los eventos registrados sobre los ficheros en reposo, uso y tránsito, tanto en tiempo real como retrospectivamente a lo largo de su ciclo de vida.

Arquitectura Cytomic Data Watch

Cytomic Data Watch está formado por los elementos mostrados a continuación:

- Servidor Cytomic Data Watch **(1).**
- Equipos monitorizados por Cytomic EDR o Cytomic EDPR **(2).**
- Servidor Advanced Visualization Tool con la consola Web de administración **(3).**
- Equipo del administrador de la red para la gestión del servicio **(4).**
- Aplicaciones / Dashboards **(5).**
- Tablas de conocimiento PII **(6).**

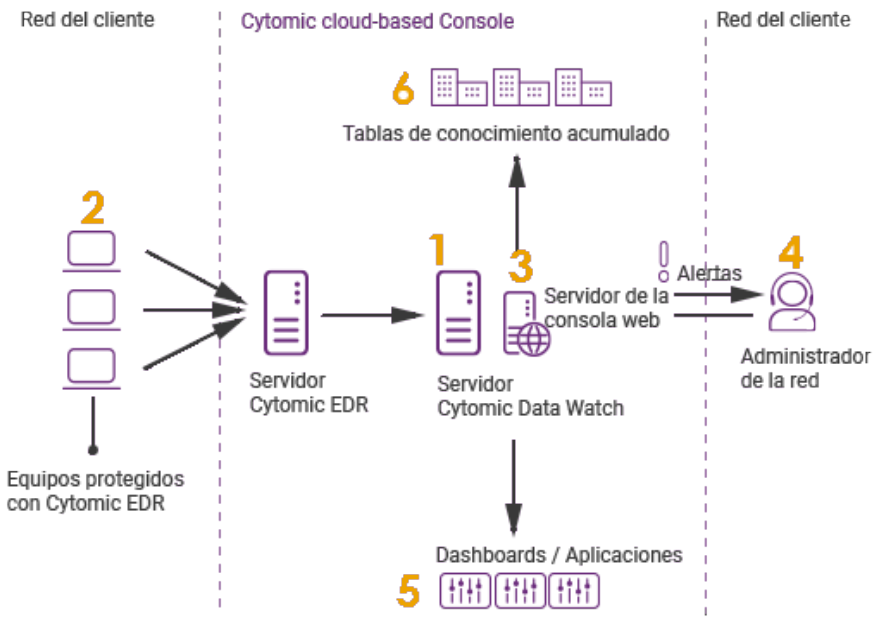

Figura 2.1: arquitectura general de Cytomic Data Watch

Infraestructura alojada en la nube

Toda la infraestructura directamente implicada con el servicio (servidor Cytomic Data Watch, servidor Cytomic EDR y servidor Advanced Visualization Tool) está desplegada en la nube de Cytomic, ofreciendo los beneficios mostrados a continuación:

- **Sin costes de mantenimiento para el cliente**

Desaparecen los costes relacionados con la adquisición de hardware y su mantenimiento (gestión de las garantías, averías y almacenamiento de componentes de recambio, etc.) al no requerir la instalación de servidores en las oficinas del cliente.

Tampoco aplican los costes de sistemas operativos, bases de datos, licencias y otros elementos característicos de soluciones On-Premise.

Debido a las condiciones indicadas, los costes de mano de obra imputables al personal técnico especialista relativo al mantenimiento de la solución también desaparecen.

- **Acceso al servicio desde cualquier momento y lugar**

El servicio es accesible desde cualquier equipo, eliminando los problemas que aparecen en empresas con estructuras distribuidas en varios centros de trabajo.

No es necesaria la instalación de recursos específicos de conectividad como VPNs o configuraciones del router que permitan el acceso a la consola de gestión desde fuera de la red del cliente.

- **Servicio 24/7 los 365 días del año**

El servicio se ofrece en alta disponibilidad, sin límite de equipos monitorizados. El cliente no necesita diseñar ni ejecutar complicados despliegues de infraestructura en redundancia, ni se requiere personal técnico especializado para mantener el compromiso de servicio.

Servidor Cytomic Data Watch

Se trata de una granja de servidores configurados en alta disponibilidad, que recogen todos los eventos relativos a los ficheros almacenados o creados en los equipos de la red. Sus principales tareas son:

- Recoger la información monitorizada y enviada por los agentes Cytomic EDR de forma continua y en tiempo real.
- Almacenar todos los datos en una tabla de acceso rápido para el administrador.
- Construir las fuentes de datos que alimentarán las gráficas mostradas por Advanced Visualization Tool en la consola de administración.
- Generar alertas configurables que muestren situaciones potencialmente comprometedoras para los datos personales.

Equipos protegidos y el servidor Cytomic EDR

Inicialmente los equipos envían de forma continuada las acciones que ejecutan los procesos al servidor Cytomic EDR, alojado en la nube. Este servidor genera inteligencia de seguridad de forma automática mediante tecnologías Machine Learning, que será añadida a los eventos recogidos y enviados directamente al servidor Cytomic Data Watch. Este esquema de funcionamiento presenta las siguientes ventajas:

- La información recibida por el servidor Cytomic Data Watch ya ha sido previamente procesada por el Servidor Cytomic EDR, de forma que contiene la inteligencia de seguridad necesaria para ayudar al administrador a determinar si el proceso que manipuló los ficheros es goodware o malware.
- Los paquetes de información solo se envían una única vez desde los equipos protegidos por Cytomic EDR, ahorrando ancho de banda del cliente y la instalación de servidores SIEM locales en cada oficina, una arquitectura mucho más compleja y cara de mantener.
- No se requiere ninguna configuración adicional ni en la consola de Cytomic EDR, ni en los equipos protegidos. El servidor de Cytomic EDR enviará toda la información necesaria de forma automática y transparente al servidor Cytomic Data Watch.

Para clasificar los ficheros no estructurados, Cytomic Data Watch requiere la instalación de la versión Microsoft Office 2007 de la librería Microsoft Filter Pack o una superior.

*Consulta el capítulo "**Requisitos de hardware, software y red**" en la página **99** para obtener un listado completo de requisitos. Consulta la FAQ **https://www.pandasecurity.com/spain/support/card?id=50116** que describe cómo instalar Microsoft Filter Pack.*

Servidor Advanced Visualization Tool y la consola web

Es el encargado de generar los widgets, dashboards y aplicaciones gráficas que muestran los datos recogidos, de forma ordenada y fácil de interpretar.

Además, aloja la consola de administración, accesible desde cualquier lugar y en cualquier momento mediante un navegador web compatible.

*Consulta el apartado "**Requisitos de acceso a la consola Web Advanced Visualization Tool**" en la página **28**.*

Advanced Visualization Tool implementa funcionalidades mediante el conjunto de herramientas y recursos mostrados a continuación:

- Una amplia variedad de widgets gráficos configurables que facilitan la visualización de la actividad recogida sobre los ficheros PII.
- Paneles de control configurables por el administrador con toda la información relevante para el departamento de IT.

- Alertas configurables y generadas en tiempo real para descubrir situaciones potencialmente peligrosas.
- Herramientas gráficas para visualizar y manipular las tablas de conocimiento, que contienen toda la información de las acciones recogidas sobre ficheros monitorizados.
- Herramientas avanzadas para la búsqueda y procesamiento de la información almacenada: filtrado, agrupación, operaciones avanzadas con datos, generación de nuevos widgets con información, etc.

Aplicaciones / paneles de control

La información más relevante para el equipo técnico de IT se muestra mediante las aplicaciones mostradas a continuación, accesibles desde la consola Web de administración:

- **Files and machines with PII**: identifica los ficheros PII de la red, mostrando los equipos donde residen y las operaciones efectuadas sobre ellos, tanto si están almacenados en el sistema de ficheros del equipo como en el cliente de correo electrónico .
- **User monitored files**: muestra información de los ficheros que cumplen con las reglas de monitorización creadas por el administrador. En el caso de encontrar ficheros monitorizados dentro de un mensaje de correo, muestra sus detalles, tales como el origen, destino y la fecha de envío y recepción, entre otros.
- **User operations in PII files**: muestra las operaciones que ejecutan los usuarios sobre los PIIF, distinguiendo el dispositivo físico donde residen (disco duro interno, almacenamiento USB, etc.).
- **Risk of PII extraction**: muestra las operaciones sospechosas de producir una fuga de información personal.

*Para más información sobre las aplicaciones consulta el capítulo "**Aplicaciones configuradas**" en la página **47**.*

Tablas de conocimiento PII

Cytomic Data Watch almacena la información de los ficheros monitorizados en varias tablas con las siguientes características:

- **Almacenamiento en bruto**: producto de la monitorización de los equipos de usuario y servidores, y completado con información de la inteligencia de seguridad generada por el servidor Cytomic EDR.
- **Almacenamiento continuo**: se monitorizan todos los procesos sin interrupción y se envía la información para su almacenamiento.
- **Almacenamiento en tiempo real**.

Esta información se toma como base para generar las aplicaciones y gráficas mostradas en Adaptive Visualization Tool, permitiendo el filtrado y transformación de los datos (agrupaciones, ordenación, búsquedas, etc.).

*Consulta el capítulo "**Tablas de conocimiento PII**" en la página **83** para más información sobre el significado de los campos.*

¿Cómo funciona Cytomic Data Watch?

Para cumplir con los requisitos de confidencialidad de la información, Cytomic Data Watch implementa el servicio mediante cinco procesos bien diferenciados, que se distribuyen entre los distintos elementos de la arquitectura mostrada en el apartado "**Arquitectura Cytomic Data Watch**":

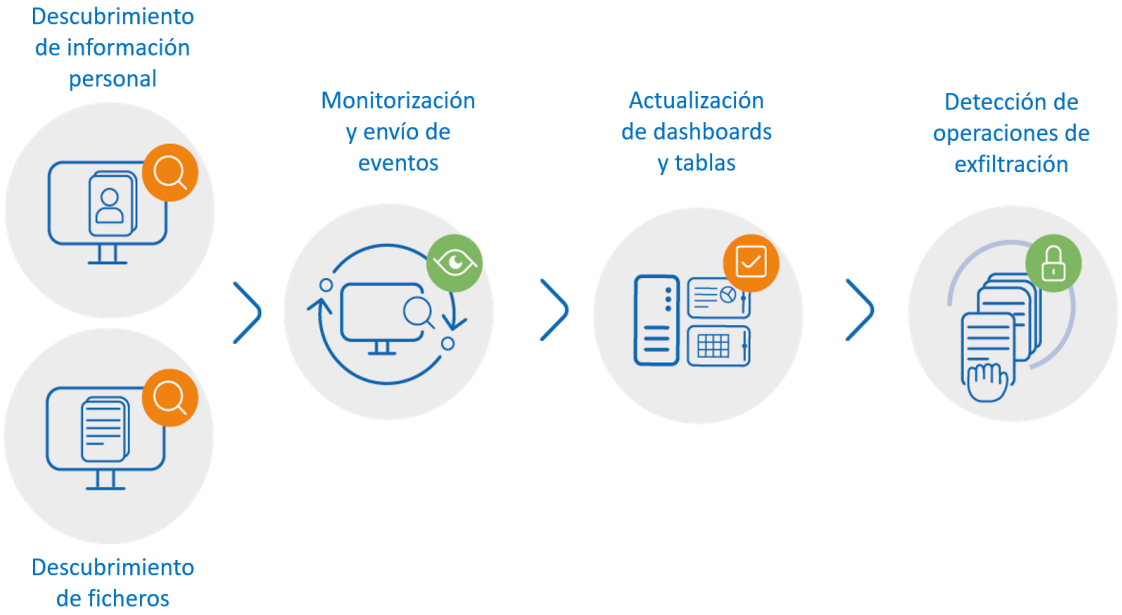

Figura 2.2: flujo completo de procesos implementado en Cytomic Data Watch

Descubrimiento de información personal

Este proceso se ejecuta en los equipos protegidos por Cytomic EDR. El agente escanea todos los dispositivos de almacenamiento masivo conectados al puesto de usuario o servidor (discos duros locales, externos, memorias USBs y discos RAM) en busca de ficheros sin estructura interna que contengan información personal.

Esta búsqueda se lanza automáticamente al activar por primera vez el módulo Cytomic Data Watch desde la consola de administración de Cytomic EDR.

Consulta la ayuda online del producto Cytomic EDR para activar el servicio Cytomic Data Watch desde la consola de administración.

Cytomic Data Watch localiza aquellos ficheros que contienen datos personales que permiten identificar a clientes, trabajadores y otras personas físicas, y que requieren a las empresas un protocolo de tratamiento específico con el objetivo de salvaguardar los derechos de los titulares de dicha información.

Cada pieza o grupo de palabras con significado propio referido a un tipo concreto de información personal recibe el nombre de "entidad". Cytomic Data Watch soporta varios tipos de entidades: tarjetas de crédito, cuentas bancarias y números de teléfono entre muchos otros.

Debido a la naturaleza ambigua y variable del lenguaje natural en sus múltiples idiomas, una misma entidad puede presentarse de formas muy diferentes, por lo que es necesario aplicar algoritmos flexibles y adaptables para su detección. De manera general, el análisis de entidades aplica formatos o expresiones predefinidas, y utiliza el contexto local en torno a esa detección o la presencia o ausencia de determinadas palabras clave para evitar falsos positivos.

Una vez realizada la identificación de entidades, esta información se evalúa para determinar si es suficiente para identificar a un cliente o usuario concreto, y por lo tanto es susceptible de ser protegida por protocolos de manipulación específicos que permitan a la empresa cumplir con la normativa vigente (GDPR, PCI, etc.). Esta evaluación combina un modelo Machine learning supervisado y un modelo experto basado en ponderación de entidades y análisis del contexto global del documento para finalmente clasificar un fichero con entidades detectadas como un fichero PII a proteger.

Tipos de información personal soportados

Cytomic EDR aplica algoritmos de Machine Learning y expresiones regulares en cada fichero compatible encontrado para buscar información personal. Los datos reconocidos como PII son los siguientes:

- Cuentas bancarias.
- Direcciones IP.
- Direcciones y códigos postales.
- Localidades y países.
- Nombres y apellidos.
- Número de carnet de conducir.
- Número de identidad personal.

- Número de pasaporte.
- Número de la seguridad social.
- Números de teléfono.
- Tarjetas de crédito.

Países soportados

Los formatos y contenidos de los datos PII cambian dependiendo del país de la persona a la que se refieren. Actualmente se soportan los siguientes orígenes:

- Alemania.
- Austria.
- Bélgica.
- Dinamarca.
- España.
- Finlandia.
- Francia.
- Hungría.
- Irlanda.
- Italia.
- Noruega.
- Países Bajos.
- Portugal.
- Suecia.
- Suiza.
- Reino Unido.

Dispositivos de almacenamiento masivo soportados

Los ficheros pueden residir en los siguientes medios de almacenamiento masivo:

- Discos duros locales.
- Memorias USB.
- Discos virtuales RAM.
- CDROMS, DVDs, Blu Ray, etc.

Tipos de fichero soportados

Cytomic Data Watch busca información en los formatos de ficheros mostrados a continuación:

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

*Para ver un listado completo de las extensiones de los ficheros soportados consulta el capítulo "***Extensiones soportadas***" en la página* **91**.

Confidencialidad de los datos

Una vez completado el análisis Cytomic EDR comunica al servidor Cytomic Data Watch únicamente el número veces que encontró cada una de las entidades soportadas.

No se envía el contenido parcial o total de los ficheros PII al servidor Cytomic Data Watch, y, por lo tanto, no abandonan el equipo donde se encontraron.

Terminado el proceso de búsqueda y clasificación, Cytomic EDR monitorizará todas las acciones ejecutadas sobre ficheros PII reportándolas al servidor Cytomic Data Watch.

Descubrimiento de ficheros mediante reglas de monitorización

Además de monitorizar automáticamente los ficheros clasificados como PII, Cytomic Data Watch admite otros tipos de ficheros, que el administrador puede indicar mediante las reglas de monitorización. Estas reglas se introducen en la consola de Cytomic EDR, tal y como se explica en la **Guía de administración**.

Cytomic Data Watch también monitoriza los ficheros que viajan por correo electrónico como adjuntos, ya sean de tipo PII o que cumplan con las reglas de monitorización establecidas por el administrador.

Monitorización y envío de eventos

Por cada acción que un proceso ejecuta sobre un fichero se almacena un único evento con información detallada de los elementos involucrados. Cada evento generado queda definido por tres parámetros:

- Proceso padre que efectúa la operación.
- Acción realizada.

- Hash del fichero que contiene datos personales.

Proceso que ejecuta la acción

Cytomic Data Watch almacena información del proceso que llevó a cabo una acción sobre el fichero:

- Usuario que lanzó el proceso.
- Ruta y nombre del proceso.
- Hash del proceso.
- Nombre del equipo donde se ejecuta el proceso y su dirección IP.
- Clasificación del proceso (goodware, malware o en clasificación) para valorar si se trata de un potencial robo de datos.

Fichero que recibe la acción

Excepto en el caso de copiado y pegado de datos que se explica más adelante, Cytomic Data Watch almacena la información del fichero afectado:

- Ruta y nombre del fichero.
- Hash del fichero.
- Dispositivo donde reside el fichero (disco duro local, disco duro externo, memoria USB o disco RAM virtual).

Tipo de acción

Cytomic Data Watch detecta varios tipos de acciones que afectan a los ficheros:

- Creación.
- Apertura.
- Borrado.
- Modificación.
- Copiado y pegado del fichero.
- Renombrado.

En el caso de una operación de copiado y pegado de información, Cytomic Data Watchmonitoriza el portapapeles del equipo en busca de datos PII. El evento de detección se produce cuando el usuario pega los datos en el documento, mostrándose el proceso origen de los datos y el proceso destino.

La monitorización del portapapeles no identifica los ficheros origen y destino de la información, aunque sí muestra los procesos involucrados.

Actualización de dashboards y tablas de conocimiento

En función de la información que los agentes de Cytomic EDR envían, el servidor Cytomic Data Watch evalúa si los ficheros reportados contienen datos personales. Si finalmente se trata de un PIIF se acumulan todos los eventos recibidos para alimentar los diferentes widgets distribuidos en las aplicaciones. Adicionalmente, Cytomic Data Watch envía al servidor todos los eventos producidos sobre los ficheros que coinciden con las reglas de monitorización establecidas por el administrador.

Finalmente, Cytomic Data Watch vuelca toda la información recibida en las tablas de conocimiento PII para que el administrador pueda filtrar, buscar y analizar la información. Los datos se almacenan por un espacio de 12 meses para poder realizar un análisis forense completo con las herramientas implementadas en la consola de Cytomic Data Watch.

Detección de operaciones de exfiltración e infiltración de ficheros

Cytomic Data Watch detecta ciertas operaciones en aquellos procesos con capacidad de enviar datos al exterior o recibirlos. Los algoritmos de Machine Learning implementados en Cytomic Data Watch asignan una probabilidad de que estas operaciones formen parte de un incidente de fuga o comunicación de información no autorizada. En estos casos, Cytomic Data Watch asigna una clasificación (Infiltration o Exfiltration) a la operación, indicando al administrador la existencia de una alta probabilidad de incidente de seguridad.

*Consulta el capítulo "**Listado de procesos**" en la página **93** para obtener la relación de los programas que pueden formar parte de un incidente asociado a la publicación o extracción de datos.*

Perfil de usuario de Cytomic Data Watch

Este servicio está dirigido fundamentalmente al departamento de IT de las empresas, y en especial al DPO, que desarrolla alguna o todas las tareas mostradas a continuación:

- Audita los equipos de usuario y servidores en busca de ficheros PII y de otros tipos de ficheros que contienen información confidencial o sensible, y que residen en los medios de almacenamiento conectados al equipo o en el cliente de correo electrónico.
- Controla y monitoriza las operaciones que se ejecutan sobre los ficheros auditados.Valora si existe riesgo de fuga de información personal en función del usuario, clasificación del proceso (goodware o malware) y tipo de operaciones efectuadas sobre los PIIF.
- Detecta tendencias que permitan anticiparse a posibles brechas de seguridad que deriven en una infiltración de PII.
- Vela por el cumplimiento de la GDPR.

Capítulo 3

La consola web

En este capítulo se describe la estructura general de la consola Web de administración y los elementos que la componen.

La consola Web es la herramienta principal del administrador para visualizar el estado de la seguridad de la red que gestiona.

CONTENIDO DEL CAPÍTULO

Características y acceso a la consola web

Al tratarse de un servicio Web centralizado, la consola de administración posee una serie de características que influyen positivamente en la forma de trabajo del departamento de IT:

- **Única herramienta para la explotación de la información sobre PII**

La consola web incluye herramientas gráficas pre-configuradas que permiten visualizar de forma fácil toda la información generada sobre los ficheros PII encontrados en la red.

Esta funcionalidad se ofrece desde una única consola Web, favoreciendo la integración de las distintas herramientas y eliminando la complejidad de utilizar varios productos de distintos proveedores.

- **Acceso a información consolidada sin necesidad de infraestructura en las oficinas del cliente**

Ya que el servidor que aloja la consola Web opera desde las instalaciones de Cytomic no es necesario instalar ni mantener infraestructuras específicas en las oficinas del cliente.

Adicionalmente, al estar alojado en la nube, el servidor es accesible para todas las oficinas del cliente, presentando los datos consolidados desde un único repositorio. Esto facilita la interpretación de la información y permite sacar conclusiones de forma más rápida.

Requisitos de acceso a la consola Web Advanced Visualization Tool

Para acceder a la consola Web es necesario cumplir con el siguiente listado de requisitos:

- Un navegador compatible certificado (otros navegadores pueden funcionar).
  - Mozilla Firefox.
  - Google Chrome.

Los navegadores no listados pueden funcionar, pero es posible que no se soporten todas las versiones. Por esta razón se recomienda el uso de los navegadores indicados anteriormente.

- Conexión a Internet y comunicación por el puerto 443.
- Resolución mínima 1280x1024, recomendada 1920x1080.
- Equipo con capacidad de proceso adecuada para la generación de los gráficos y listados en tiempo real.
- Ancho de banda suficiente para poder mostrar en tiempo real toda la información recogida en los equipos de los usuarios.

Acceso a la consola Web Advanced Visualization Tool

La consola Web es accesible mediante SSO a través de la consola de administración Cytomic EDR, sin necesidad de introducir nuevas credenciales.

Para acceder al entorno sigue los pasos mostrados a continuación:

- En el menú superior de la consola haz clic en **Estado**.

- En el panel lateral haz clic en **Advanced Visualization Tool**.

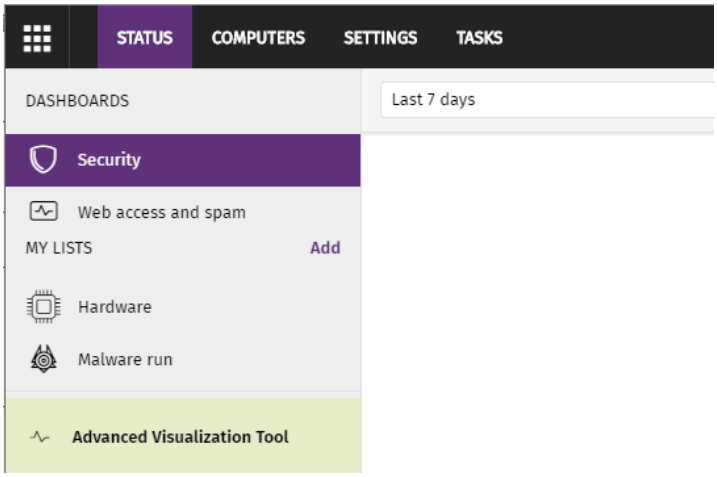

Figura 3.1: acceso al servicio Advanced Visualization Tool desde la consola Cytomic EDR

Estructura general de la consola Web

La consola Web está diseñada de tal forma que facilite al administrador una experiencia homogénea y coherente, tanto en la visualización y búsqueda de la información de seguridad como en las tareas de configuración de nuevos paneles de control a su medida. El objetivo final es entregar una herramienta sencilla, pero a la vez flexible y potente, que permita al administrador visualizar el estado de la información personal que reside en ficheros desestructurados de forma rápida y con una curva de aprendizaje suave.

Vista general del menú lateral

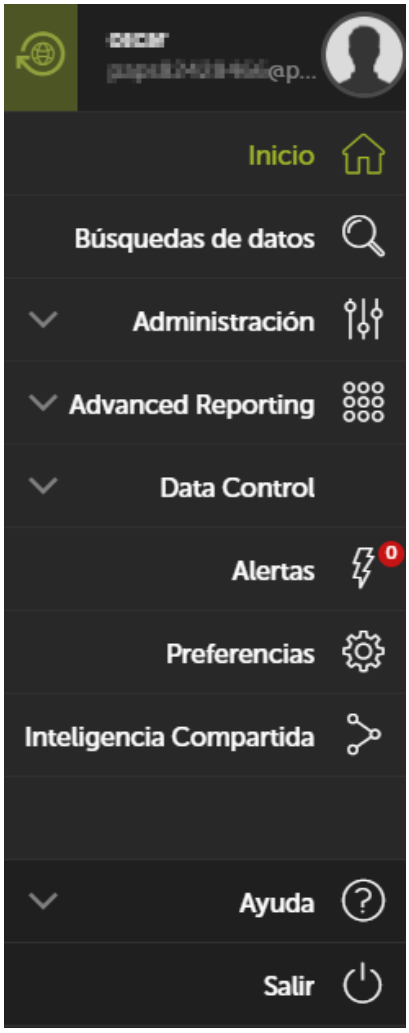

Figura 3.2: menú lateral

El menú lateral está situado a la izquierda de la pantalla y es accesible en todo momento.

Inicialmente el menú lateral esta replegado, mostrando únicamente los iconos de las opciones. Al acercar el ratón a la zona izquierda de la ventana, o haciendo clic en una sección libre del menú lateral, éste se desplegará mostrando etiquetas descriptivas de cada icono.

A continuación, se presentan de forma general las opciones del menú lateral:

Inicio

Devuelve al usuario a la página inicial de la consola Web.

Búsquedas de datos

Permite acceder a la tabla de conocimiento acumulado. Desde aquí el administrador podrá visualizar los datos tal y como son enviados por los equipos protegidos por Cytomic EDR.

Conforme el administrador vaya accediendo a las tablas de conocimiento, éstas aparecerán bajo la entrada Búsquedas como accesos directos, para facilitar su acceso posterior.

*Consulta el capítulo "**Tablas de conocimiento PII**" en la página **83** para más información acerca de sus campos.*

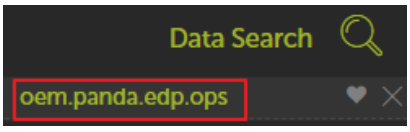

Figura 3.3: acceso directo a la tabla de conocimiento

Administración 

Permite configurar nuevas alertas.

> *Para más información acerca del funcionamiento de las alertas pre-configuradas consulta el apartado "**Alertas predefinidas**" en la página **64**. Para más información sobre cómo crear y gestionar alertas nuevas consulta el apartado "**Creación de alertas**" en la página **69**.*

Advanced Reporting 

Desplegable con las aplicaciones disponibles para el producto Cytomic Insights.

> *Para más información consulta la Guía para el usuario de Cytomic Insights.*

Data Control 

Se incluyen las aplicaciones mostradas a continuación:

- **Files and machines with PII**: identifica los ficheros PII de la red, mostrando los equipos donde residen y las operaciones efectuadas sobre ellos, tanto si están almacenados en el sistema de ficheros del equipo como en el cliente de correo electrónico.
- **User monitored files**: muestra información de los ficheros que cumplen con las reglas de monitorización creadas por el administrador. En el caso de encontrar ficheros monitorizados dentro de un mensaje de correo, muestra sus detalles, tales como el origen, destino y la fecha de envío y recepción, entre otros.
- **User operations in PII files**: muestra las operaciones que ejecutan los usuarios sobre los PIIF, distinguiendo el dispositivo físico donde residen (disco duro interno, almacenamiento USB, etc.).
- **Risk of PII extraction**: muestra las operaciones sospechosas de producir una fuga de información personal.

> *Para más información sobre las aplicaciones consulta el capítulo "**Aplicaciones configuradas**" en la página **47**.*

Alertas 

Muestra una ventana con toda la información relativa a las alertas recibidas.

Preferencias 

En esta sección se pueden configurar las preferencias para el usuario logeado y para todos los usuarios que accedan al servicio.

Salir 

Ejecuta un logout de la consola Cytomic Data Watch y muestra la pantalla de login IDP (Identity Provider).

Parte 2

Recursos de Cytomic Data Watch

Capítulo 4: Introducción a las aplicaciones

Capítulo 5: Aplicaciones configuradas

Capítulo 6: Alertas

Capítulo 4

Introducción a las aplicaciones

Los *dashboards* son aplicaciones pre configuradas que muestran al administrador de la red información referida a aspectos concretos de la red gestionada.

Los dashboards incluidos en la consola Web de administración son:

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

Todos los dashboards están organizados siguiendo un esquema común para facilitar su interpretación, detallado más adelante en este mismo capítulo.

Además, las aplicaciones generan alertas que advierten en tiempo real al administrador de la red de condiciones anómalas.

*Para crear nuevas alertas aparte de las ya configuradas como parte de las aplicaciones, consulta el apartado "***Alertas predefinidas***" en la página* **64**.

CONTENIDO DEL CAPÍTULO

Acceso a las aplicaciones y a las alertas

Acceso a los dashboards / aplicaciones

Accede a los dashboards desde el menú lateral, sección **Cytomic Data Watch**.

Acceso a las alertas

Accede a las alertas pre configuradas desde el menú lateral **Administración**, **Configuración de alertas**.

La pantalla de suscripción de alertas se utiliza para buscar alertas configuradas mediante los paneles superiores, asignar políticas y activar y desactivar alertas individuales.

Recursos y elementos comunes de los dashboards

Intervalo de datos mostrados

Cada aplicación tiene dos controles que permiten definir el rango de los datos mostrados en pantalla:

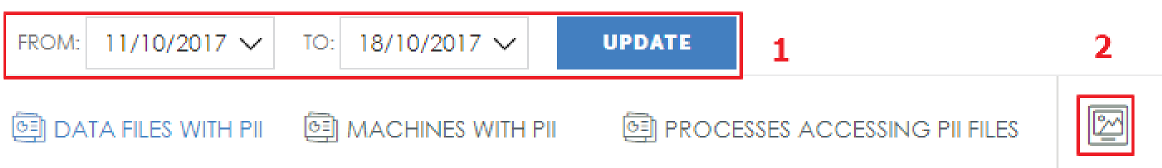

Figura 4.1: controles para la configuración de intervalo de datos a mostrar

- **Rango de fechas (1)**: establece el intervalo de tiempo que se muestra en los widgets del dashboard seleccionado. El intervalo establecido aplica a los widgets de todas las pestañas de un mismo dashboard.
- **Captura de pantalla (2)**: abre una ventana independiente con el contenido de la pestaña en formato gráfico, para su descarga e impresión.

> ⚠ *Es posible que el sistema anti pop-ups del navegador impida mostrar la nueva ventana. Deshabilita esta funcionalidad en el navegador para poder ver las ventanas emergentes.*

Pestañas

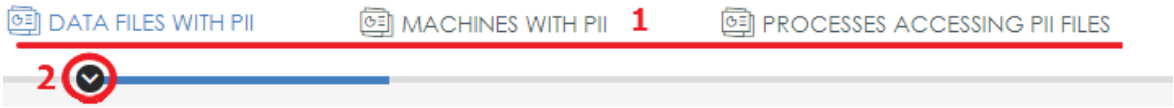

Figura 4.2: menú pestañas

Las pestañas dividen la información en áreas según sea el nivel de detalle de los datos que muestran: información de tipo general o informes más detallados y/o desglosados.

Cada pestaña contiene herramientas que se muestran a continuación:

- **Título de la pestaña (1)**: describe la información contenida en la pestaña. Para seleccionar una pestaña haz clic en el su título. Las pestañas de tipo **Detailed information** contienen tablas de datos que se pueden utilizar en informes.
- **Menú de acceso rápido (2)**: haz clic en la flecha para mostrar un menú desplegable que permite saltar directamente a una sección dentro de la pestaña.

Secciones

La información dentro de una pestaña está estructurada en secciones. Una sección es una agrupación de widgets que contienen información relacionada.

Haz clic en el botón de la flecha para ocultar o mostrar una sección completa.

Figura 4.3: acceso a las secciones de una pestaña

Widgets

Son controles que muestran los datos utilizando tablas y gráficas avanzadas.

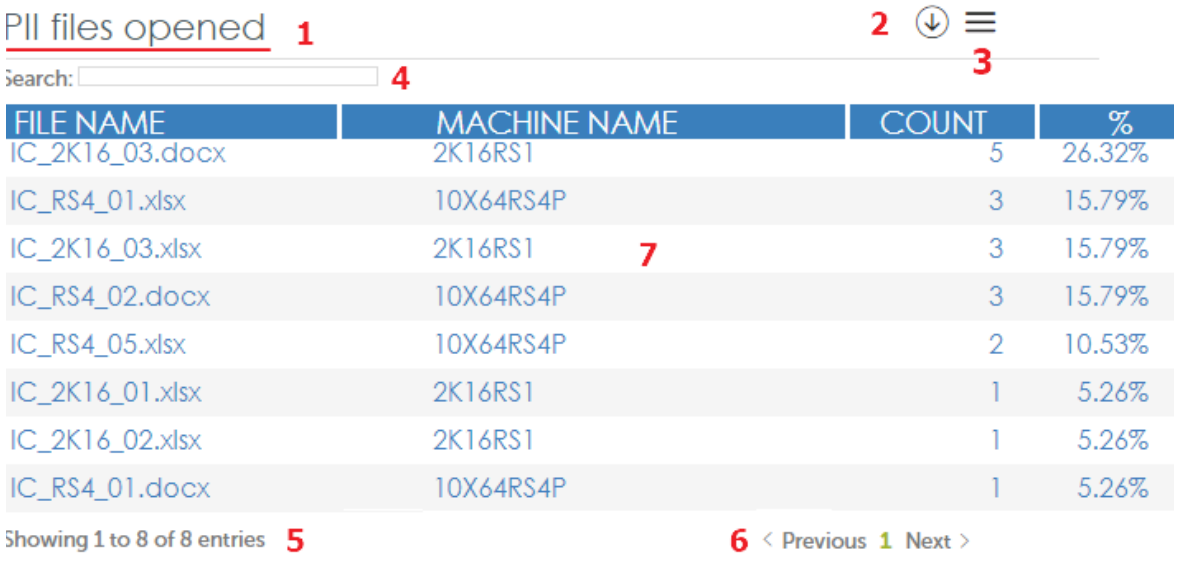

Figura 4.4: ejemplo de widget

Cada widget está compuesto por varios elementos, aunque dependiendo de su tipo algunos no estarán disponibles:

- **Nombre del widget (1)**: indica el tipo de información mostrada.
- **Botón de mostrar / ocultar (2)**  : oculta o muestra el contenido del widget según el administrador lo considere necesario.
- **Menú widget (3)** : contiene cuatro opciones:
  - **Screenshot**: abre en una nueva página web un volcado del contenido del widget para poder guardarlo como gráfico, imprimirlo, etc.

Es posible que el sistema anti pop-ups del navegador impida ver la nueva ventana. Deshabilita esta funcionalidad en el navegador para poder ver las ventanas emergentes.

  - **Download data**: descarga los datos en bruto visualizados en el widget. Los datos se descargan en formato .csv separado por comas, para poder ser importados en otras aplicaciones.
  - **Zoom:** aumenta el tamaño de la visualización del widget seleccionado.
  - **Go to query**: muestra la tabla de conocimiento asociada al widget que le sirve de fuente de datos, junto con la configuración de filtros, agrupaciones y operaciones aplicadas.

El menú Go to query permite visualizar la configuración exacta de la fuente de datos que alimenta el widget, incluido el intervalo de tiempo seleccionado. De esta forma el administrador puede experimentar con variaciones de la gráfica mostrada tomando como base la sentencia SQL utilizada. Consulta más adelante en este mismo capítulo para obtener más información.

- **Ayuda**  : ventana de ayuda, con las teclas de acceso rápido asignadas para los widgets que permitan la navegación de los datos mostrados.
- **Buscar (4)**: caja de texto que permite filtrar el contenido del widget.
- **Resumen (5)**: en los widgets de tipo tabla indica el numero de filas mostradas.
- **Paginación (6)**: permite avanzar y retroceder por bloques de filas en los widgets de tipo tabla.
- **Elemento de información (7)**: son tablas y gráficos de diversos tipos que muestran la información.

Tipos de widgets

Los datos se representan mediante gráficos de diversos tipos (Voronoi, diagramas de líneas y barras, diagramas de tarta, etc.) y con tablas de información más detallada.

Contador

Figura 4.5: widget de tipo contador

Es el widget más sencillo. Representa un acumulado de ocurrencias en el rango de fechas establecido.

Gráficos Calendario

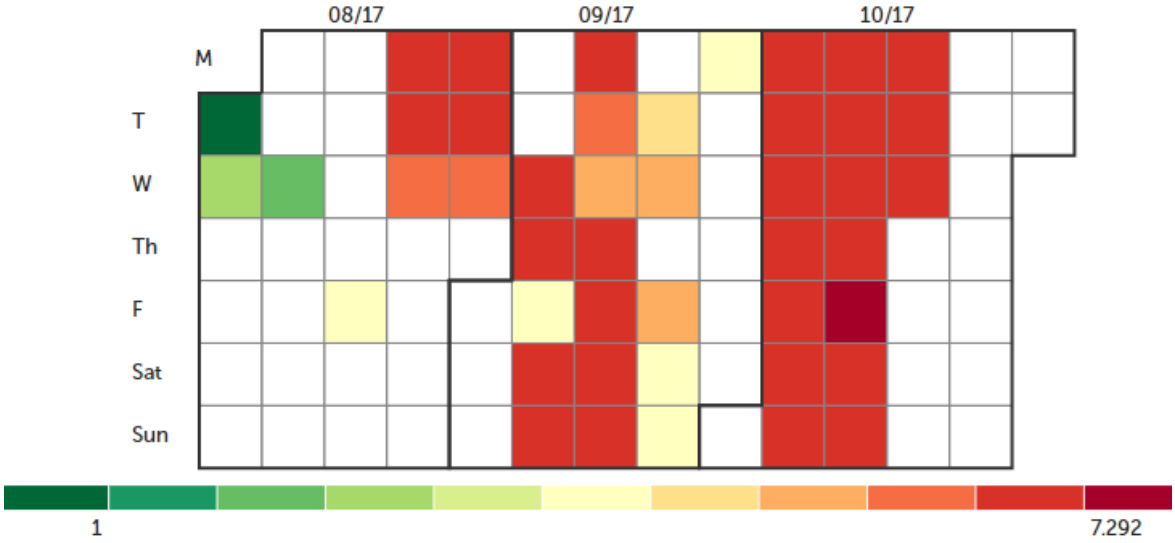

Figura 4.6: gráfica de tipo calendario

Representa los valores absolutos de las ocurrencias detectadas a lo largo de un año.

Cada casilla del control muestra un día del mes. Las casillas se agrupan mediante bloques representando los meses del año.

A su vez, cada casilla toma un color que muestra de forma relativa el número de ocurrencias en el día. La gama de color utilizado (verde - rojo) permite comparar rápidamente días entre sí, con el objetivo de tener una mejor visión de la evolución de los indicadores monitorizados.

Al pasar el puntero del ratón por encima de una casilla se iluminará el tono de color correspondiente en la leyenda, y se presenta un tooltip con la fecha y el número de ocurrencias exactas.

Gráfico de barras

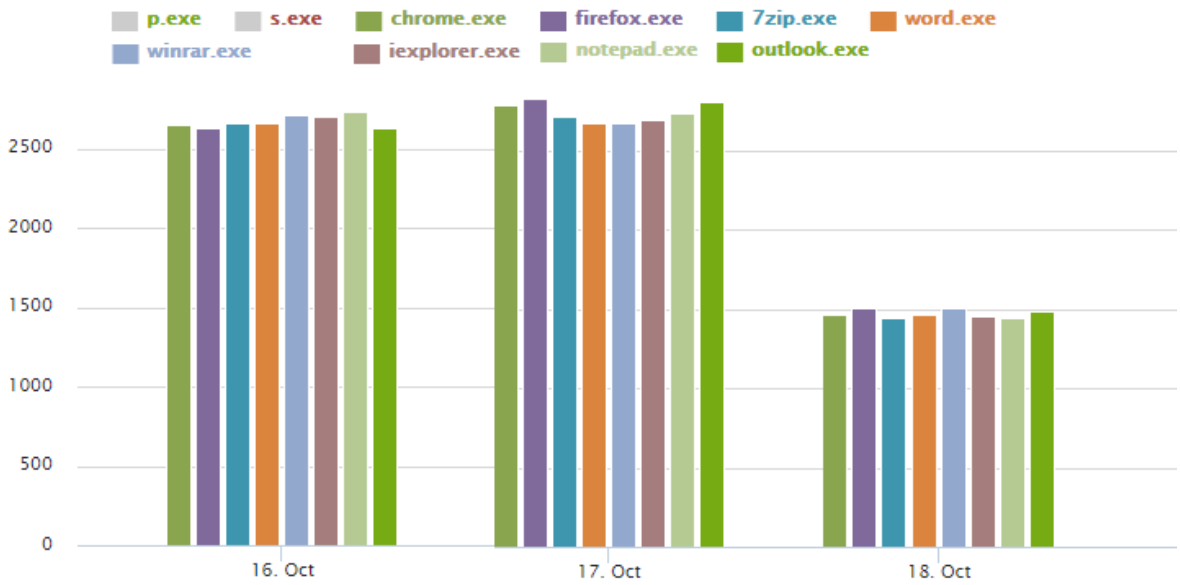

Figura 4.7: gráfica de barras

Muestra en un mismo gráfico la evolución de varias series, representadas por distintos colores y explicadas en la leyenda situada en la parte superior.

Al pasar el ratón por encima de los datos se muestra un tooltip que indica la fecha y la hora de la medición y el valor de la serie en ese momento.

Gráfico de líneas

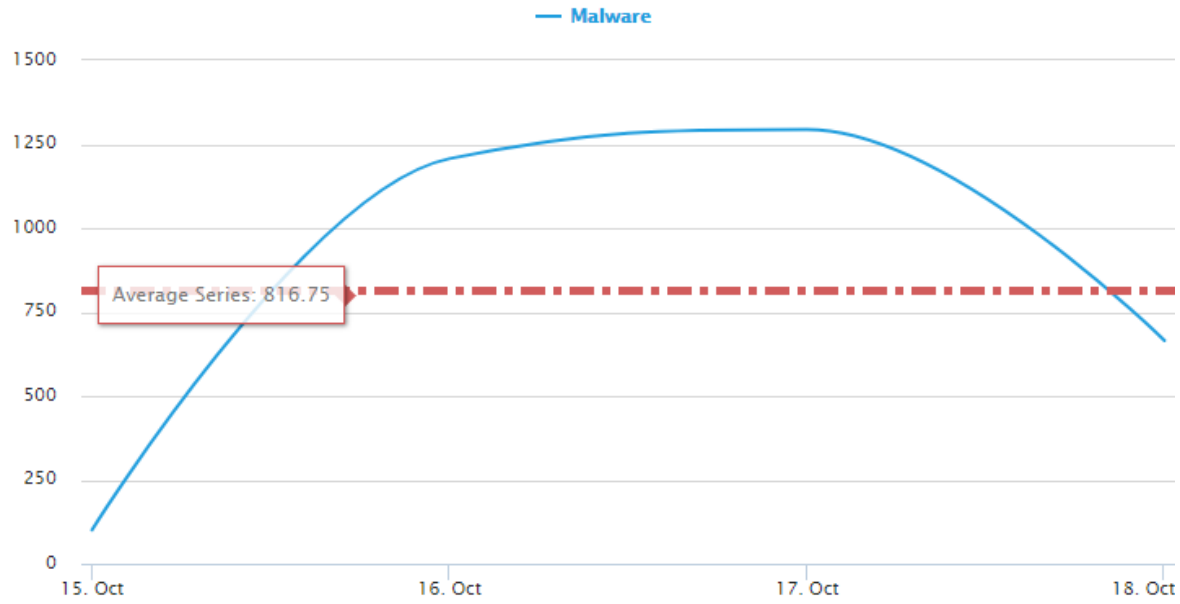

Figura 4.8: gráfico de líneas

Refleja una tendencia o evolución de una o varias series de datos, representadas por distintos colores y explicadas en la leyenda situada en la parte superior.

Al pasar el ratón por encima de los datos se muestra un tooltip que indica la fecha y la hora de la medición y el valor de la serie en ese momento.

Tabla de frecuencia

Top 10 PII files opened

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

Figura 4.9: tabla de frecuencias

Muestra en una tabla el número de veces que se ha producido cierto tipo de evento dentro del rango de tiempo establecido. El contador puede aparecer en valores absolutos (**Count**), relativos (**%**) en forma de porcentaje sobre el total de eventos registrados, o ambos.

En la primera línea de la tabla se muestran las etiquetas que describen las columnas y un icono junto al nombre que ordena la tabla de forma ascendente o descendente, tomando como referencia la columna elegida.

Gráfico Voronoi

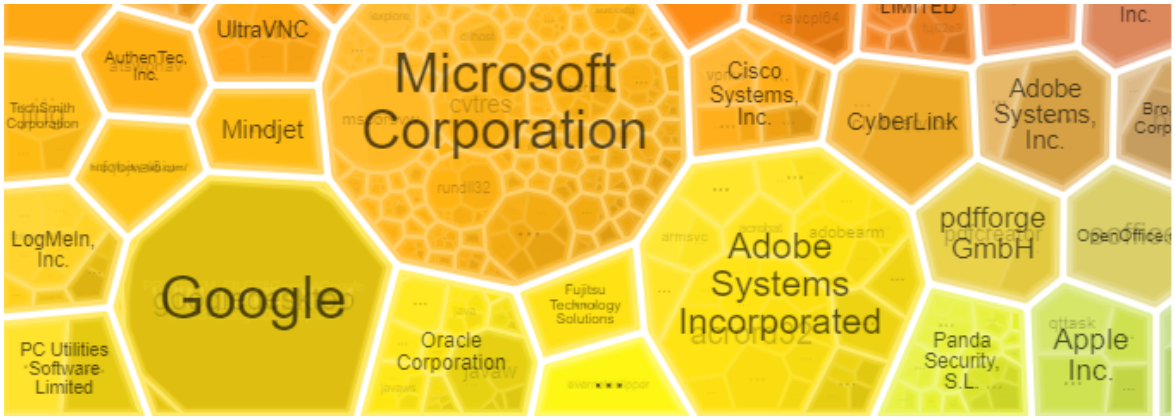

Figura 4.10: gráfica de polígonos de Thiessen o Voronoi

Muestra mediante agrupaciones de datos la información contenida en la tabla de conocimiento que lleva asociada. Para ello, utiliza polígonos de diversos tamaños y formas cuya área representa de forma relativa (porcentual) el número de elementos mostrados en su interior.

- **Navegación dentro de un gráfico Voronoi**

Un polígono puede estar formado a su vez por otros polígonos que representan agrupaciones de datos de nivel inferior. De esta forma, se establece una jerarquía de niveles de agrupaciones que van

desde las más generales hasta las más específicas. Las gráficas Voronoi permiten navegar a través de los diferentes niveles de agrupaciones de datos:

- Haz doble clic con el botón izquierdo del ratón en una agrupación de datos para acceder al nivel inferior.
- Haz doble clic con el botón derecho del ratón para regresar a la agrupación del nivel anterior.

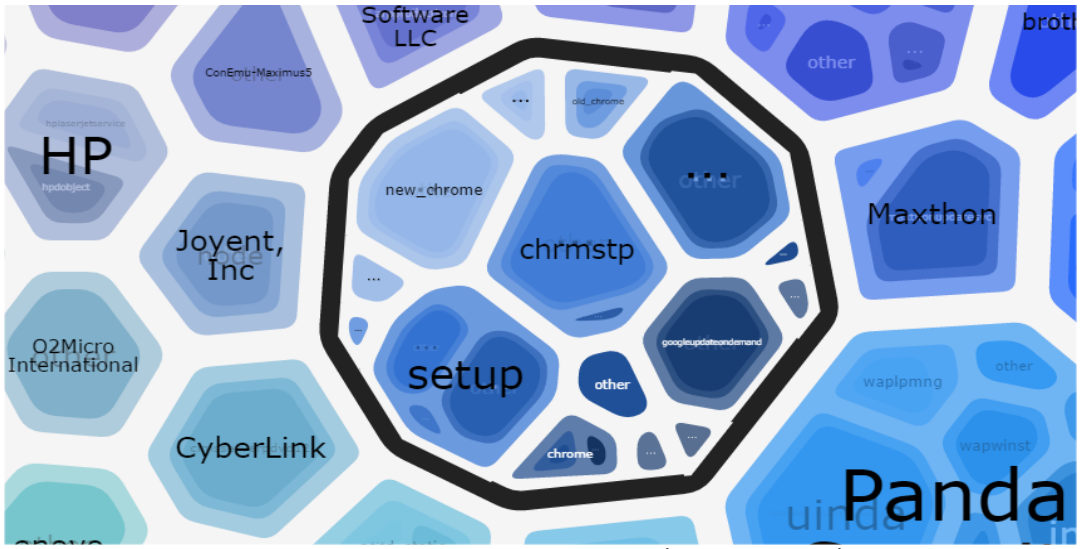

Figura 4.11: zoom in mediante doble clic en un polígono de una gráfica Voronoi

Al situar el puntero del ratón sobre un área de agrupación se mostrará el número de elementos que la integran y el porcentaje que dichos elementos representan sobre el total.

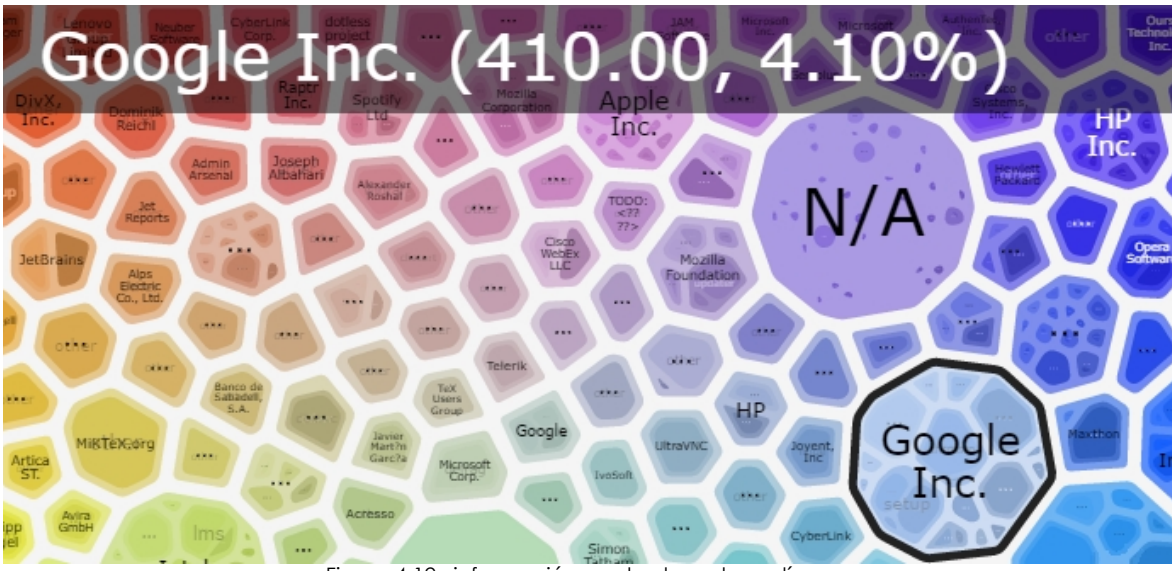

Figura 4.12: información mostrada en los polígonos

- **Controles del diagrama**

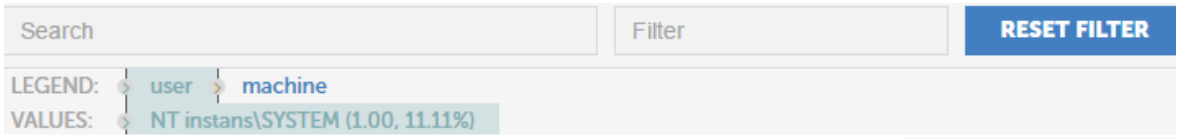

Figura 4.13: controles para configurar los datos mostrados en una gráfica Voronoi

Un widget que contiene una gráfica Voronoi incluye los controles siguientes para su manejo:

Control	Descripción
Search	Localiza un polígono en el gráfico Voronoi y lo amplia mostrando las agrupaciones que lo forman. Es equivalente a hacer doble clic con el botón izquierdo sobre un polígono de la gráfica. Para deshacer una búsqueda es necesario hacer doble clic con el botón derecho del ratón.
Filter	Muestra solo los polígonos que contienen agrupaciones coincidentes con el filtro establecido.
Reset filter	Limpia el filtro aplicado, pero no deshace las búsquedas. Para revertir una búsqueda es necesario hacer doble clic con el botón derecho del ratón.
Legend	Indica los campos de la tabla de conocimiento que son utilizados para agrupar la información. El orden de los campos indica la jerarquía de agrupaciones y puede ser alterado simplemente arrastrándolos hacia la izquierda o derecha para establecer una nueva jerarquía.
Values	En combinación con los campos mostrados en el control **Legend**, indica el valor que toma un determinado campo. Al seleccionar un polígono (mediante la búsqueda haciendo doble clic en el mismo), el campo **Values** tomará el valor de la búsqueda o del polígono seleccionado.

Tabla 4.1: controles de las gráficas Voronoi

Al navegar por los niveles del Voronoi el campo resaltado en **Legend** tomará el valor del polígono seleccionado. Los valores adyacentes del campo resaltado indican la capa de datos que se mostrará al hacer doble clic con el botón izquierdo del ratón (profundizar, valor de **Legend** situado a la derecha) o al hacer doble clic con el botón derecho (salir, valor de **Legend** situado a la izquierda).

- **Gráfica Voronoi de ejemplo**

Para ilustrar la funcionalidad y manejo de un gráfico Voronoi se muestra el siguiente ejemplo.

Según **Legend** el punto de partida es una gráfica que agrupa los datos en el siguiente orden:

- **Nivel 1 AlertType**: indica el tipo de amenaza detectada en la red.
- **Nivel 2 Manichename**: indica el nombre de la máquina donde se detectó la amenaza.
- **Nivel 3 executionStatus**: indica si se llegó a ejecutar.
- **Nivel 4 itemPath**: indica la ruta y el nombre del fichero de la amenaza.

- **Nivel 5 itemName**: indica el nombre de la amenaza.

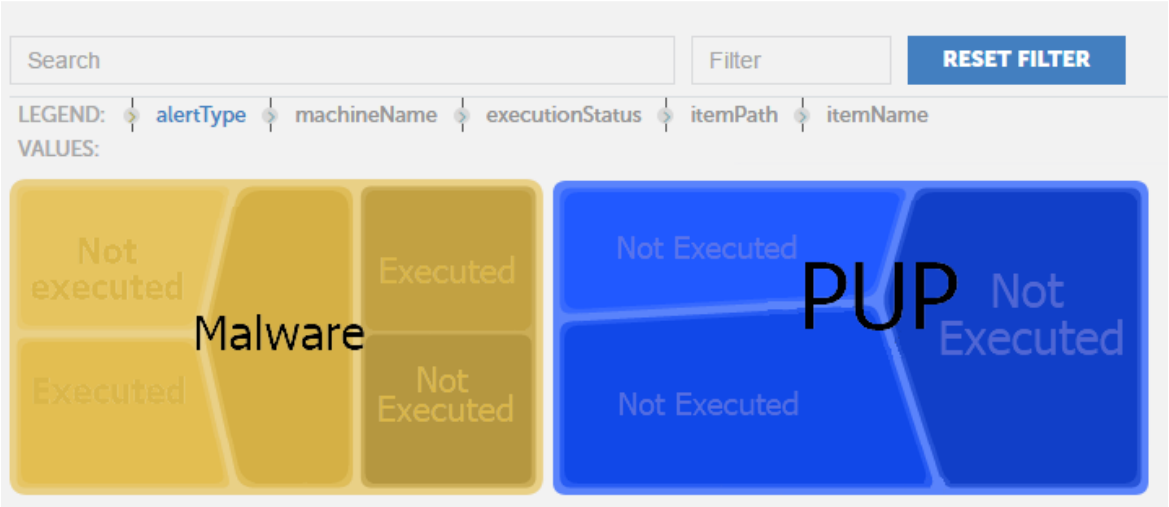

Figura 4.14: ejemplo de la primera capa o agrupación en una gráfica Voronoi

Inicialmente el gráfico muestra el Nivel 1: los datos agrupados por el campo **AlertType**, el primer campo **Legend**, resaltado a color Azul.

El segundo campo en la leyenda es **MachineName** de modo que al hacer doble clic en uno de los grupos **AlertType** del gráfico (por ejemplo, en Malware) se mostrará el segundo nivel agrupando los datos por el campo **MachineName**. El aspecto del gráfico Voronoi será el siguiente:

El campo **Value** se actualiza mostrando la selección del **Nivel 1 (AlertTye=Malware) y** se muestra su interior, el **Nivel 2**, con los datos agrupados por el campo **MachineName**, resaltado en color azul.

Siguiendo este procedimiento podremos navegar el gráfico Voronoi hasta llegar al último nivel, o retrocediendo haciendo doble clic con el botón de la derecha del ratón.

Para variar el orden de agrupación y reflejar una nueva jerarquía de ordenación arrastra hacia la izquierda o derecha los campos mostrados en **Legend**.

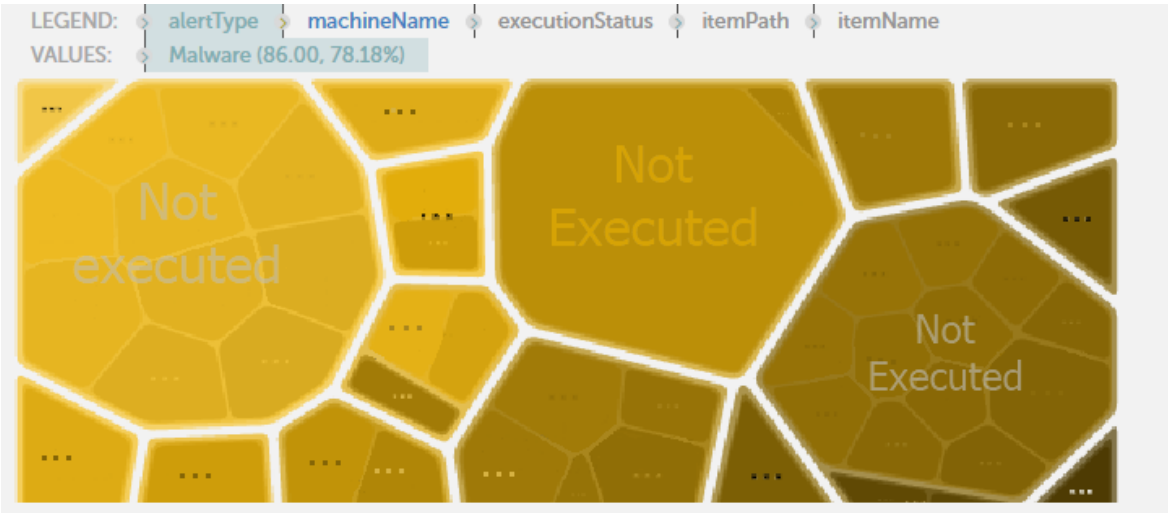

Figura 4.15: ejemplo de la segunda capa de agrupación en una gráfica Voronoi

Por ejemplo, si quieres determinar en primer lugar cuales son los equipos que han ejecutado algún tipo de malware y después el nombre de la amenaza ejecutada para podernos informar mejor de sus características, y finalmente los equipos donde se ejecutó, configura el orden de agrupación como se muestra a continuación:

- Nivel 1 ExecutionStatus
- Nivel 2 ItemName
- Nivel 3 Manichename

Figura 4.16: ejemplo de configuración para definir un nuevo orden de agrupación

Haz doble clic en **Executed** el gráfico Voronoi para mostrar el nombre de los elementos ejecutados; Haz clic en uno de ellos para mostrar los equipos donde se ejecutó ese elemento.

Generación de nuevas gráficas

Haz clic en el icono ☰ de cada widget y selecciona la opción **Go to Search** para abrir la tabla de conocimiento asociada que alimenta con datos el widget en particular.

Cada tabla de conocimiento tiene configuradas una serie de transformaciones, filtros y agrupaciones que la preparan para ofrecer los datos más importantes de forma clara y precisa. Estas transformaciones vienen descritas en lenguaje SQL, y son editables para su adaptación a las necesidades de los clientes.

> *No se permite sobrescribir la configuración de los widgets suministrados, pero sí es posible generar nuevos widgets tomando como base los ya existentes.*

Modificación de la sentencia SQL asociada a un widget

En la tabla de conocimiento asociada al widget, haz clic en el icono  de la barra de herramientas. Se abrirá una ventana con la sentencia SQL predefinida. una vez modificada haz clic en el botón **Run** para comprobar la ejecución. Los datos de la tabla se actualizarán de forma inmediata.

También es posible modificar la sentencia SQL añadiendo nuevos filtros, agrupaciones y transformaciones de datos a través de la barra de herramientas.

Sentencias SQL favoritas

Una vez modificada la sentencia SQL y comprobado que los datos que genera son los correctos, puedes salvarla para su acceso posterior marcándola como **Favorita**. Para ello sigue estos pasos:

- Al abrir una tabla de conocimiento aparecerá una nueva entrada en el menú lateral, debajo del icono de **Búsquedas**.
- A la derecha del nombre de la entrada aparecerá el icono de un corazón.
- Haz clic en este icono y la sentencia SQL se marcará como **Favorita** y aparecerá en el listado de consultas favoritas.

Las consultas **Favoritas** se muestran en el menú lateral **Administración**, **Configuración de alertas**.

Capítulo 5

Aplicaciones configuradas

En este capítulo se detalla el funcionamiento de las aplicaciones incluidas en Cytomic Data Watch en lo relativo a la interpretación de las gráficas y tablas.

CONTENIDO DEL CAPÍTULO

Intervalo de los datos a mostrar

Todas las aplicaciones tienen un control en la parte superior que permite especificar el intervalo de los datos a mostrar.

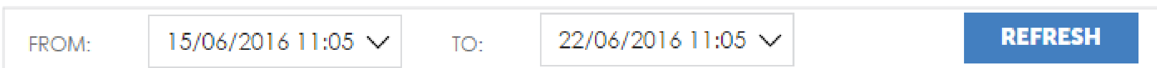

Figura 5.1: herramienta para establecer el rango de datos a mostrar

El administrador debe especificar rangos apropiados para visualizar el estado de la información personal almacenada en la red. A través de los widgets y cambiando los intervalos se podrán apreciar tendencias sospechosas.

Rangos de fechas amplios

Establece rangos de fechas amplios (meses o días) para mostrar progresiones o históricos de la actividad.

Rangos de fechas estrechos

Selecciona rangos de fechas estrechos, típicamente el día en curso, para determinar el estado actual de la información personal gestionada por la empresa. Con este enfoque se perderá la perspectiva temporal de los datos.

Files and machines with PII

Localiza los ficheros y equipos de la red que contienen información personal y muestra los procesos que los manipulan. Se divide en tres pestañas: **Data files with PII**, **Machines with PII** y **Processes accessing PII Files**, explicadas en los apartados siguientes.

Data files with PII

Muestra los ficheros con información personal encontrados en los equipos de usuario y servidores.

Se divide en dos secciones:

- **General View**: muestra un resumen general de los ficheros PII encontrados, de los equipos que los

contienen y de su uso.

- **Files reclassified to not having PII**: muestra los cambios de estado en los ficheros PII encontrados.

General view

Este gráfico localiza los equipos de la red que tienen más ficheros con información personal, y aporta información adicional acerca de los usuarios, ficheros y operaciones ejecutadas. El gráfico Voronoi permite navegar dentro de cada equipo para ver las distintas capas de información.

- **Objetivo**: mostrar una vista general de los equipos de la empresa que almacenan más ficheros PII.
- **Tipo de widget**: gráfico Voronoi.
- **Datos mostrados**:

Nivel	Descripción
Primero (machineName)	Nombre del equipo de usuario o servidor.
Segundo (user)	Nombre del usuario dentro del equipo.
Tercero (op)	Tipo de operación que se efectuó sobre el fichero PII.
Cuarto (Extension)	Extensión del fichero PII.
Quinto (document)	Muestra el documento concreto.

Tabla 5.1: datos del widget Gerenal view

- **Agrupación**: equipo, usuario, operación, extensión.

Distribution of PII files by extension

Este widget visualiza los tipos de fichero con información personal que son más utilizados en la empresa. Esta información se puede utilizar para actualizar la política de seguridad de la empresa, que impida el uso de ciertos formatos considerados no suficientemente fiables para albergar información de los clientes y/o usuarios.

- **Objetivo**: mostrar los formatos de fichero en los que se almacena más frecuentemente la información personal en la empresa.
- **Tipo de widget**: gráfico de tarta.
- **Datos mostrados**: ficheros PII agrupados por extensión.
- **Agrupación**: extensión del fichero.

PII files opened

Este widget proporciona información sobre los accesos a todos los ficheros PII durante el periodo de tiempo establecido. Ayuda al administrador a evaluar si determinados ficheros con un alto volumen de accesos deben ser protegidos con medidas adicionales, como la restricción de los accesos al mismo.

- **Objetivo**: mostrar los ficheros el número de accesos a cada fichero con información personal.
- **Campos**:

Campo	Descripción
File name	Nombre del fichero PII.
Machine name	Nombre del equipo donde se encuentra el fichero PII.
Count	Contador con el número de accesos.
%	Porcentaje de accesos al fichero del total formado por todos los ficheros PII detectados.

Tabla 5.2: campos del fichero PII files opened

Files reclassified as not having PII

- **Objetivo**: mostrar los ficheros que inicialmente fueron considerados como PII y que posteriormente, debido a una actualización del algoritmo de Cytomic Data Watch, ya no son clasificados de esta manera.
- **Campos**:

Campo	Descripción
User	Cuenta de usuario que accedió al fichero clasificado como PII.
Machine name	Nombre del equipo donde se encuentra el fichero PII.
Machine IP	Dirección IP del equipo que contiene el fichero PII.
File name	Nombre del fichero PII.
Count	Contador con el número de ocurrencias en la red.

Tabla 5.3: campos del widget PII Files reclassified not to having PII

Machines with PII

Esta pestaña muestra los equipos de la red con más actividad sobre ficheros que contienen información personal. La información se distribuye en dos secciones:

- **Most active machines**: muestra los equipos de usuario y servidores con más actividad sobre PII.
- **Machines with malware**: muestra los equipos de usuario y servidores que contienen PIIF accedidos por procesos que **Cytomic EDR** ha catalogado como malware.

Top 10 machines with operations on PII files

Este widget muestra los 10 equipos que han ejecutado más operaciones sobre ficheros con información personal, independientemente del tipo de operación de que se trate (apertura, copiado, movimiento, etc.). Proporciona al administrador la capacidad de determinar desde qué equipos se hacen más accesos y establecer medidas de control específicas.

- **Objetivo**: mostrar los 10 equipos con más operaciones sobre PIIF.
- **Campos**:

Campo	Descripción
Machine name	Nombre del equipo de usuario o servidor.
Count	Contador con el número de operaciones sobre PIIF en el plazo fijado.
%	Porcentaje de operaciones sobre PIIF por equipo sobre el total de equipos en la red en el plazo fijado.

Tabla 5.4: campos del widget Top 10 machines with operations on PII files

Top 10 machines with exfiltration operations

Este widget indica los 10 equipos que han enviado al exterior más ficheros con información personal. El administrador podrá detectar fugas masivas de información desde determinados equipos.

- **Objetivo**: mostrar los equipos con mayor número de transferencias hacia el exterior de ficheros que contienen información personal.
- **Campos**:

Campo	Descripción
Machine name	Nombre del equipo de usuario o servidor que envía ficheros PII.
Count	Contador con el número de eventos de envío.
%	Porcentaje de los envíos detectados por máquina frente al total de los equipos de la empresa.

Tabla 5.5: campos del widget op 10 machines with exfiltration operations

Top 100 machines sending attachments with PII

- **Objetivo**: muestra los 100 equipos que tienen el mayor número de correos enviados con ficheros adjuntos clasificados como PII.
- **Campos**:

Campo	Descripción
Machine	Nombre del equipo desde donde se envían los ficheros PII adjuntos.
Count	Número de ficheros PII adjuntos enviados.
%	Porcentaje de ficheros PII adjuntos enviados por el equipo sobre el total de ficheros PII enviados por todos los equipos.

Tabla 5.6: campos del widget Top 100 machines that send attachments that include PII

Machines with malware accessing PII files

Este widget muestra el top 10 de equipos en los que se han detectado procesos maliciosos accediendo a ficheros con información personal. Esto permite al administrador detectar equipos infectados además de facilitar la valoración de estos incidentes que afectan a información personal, según requiere el GDPR.

- **Objetivo**: mostrar los equipos que ejecutan más accesos a ficheros con información personal utilizando procesos clasificados como malware.
- **Campos**:

Campo	Descripción
Machine name	Nombre del equipo de usuario o servidor.
Count	Contador con el número de accesos.
%	Porcentaje de accesos realizados desde el equipo frente al total de accesos registrado para todos los equipos de la empresa.

Tabla 5.7: campos del widget Machines with malware accessing PII files

Processes accessing PII Files

Se divide en dos secciones:

- **Processes accessing PII**: muestra los procesos encontrados en la red que acceden a fichero con información personal.
- **Malware processes**: muestra los procesos que acceden a información personal y que **Cytomic EDR** clasifica como malware.

Top processes accessing PII files

Este widget muestra un histórico de los procesos que más operaciones ejecutan sobre ficheros PII. De esta manera el administrador detectará incrementos de operaciones anómalos que puedan servir como pista para una comunicación o fuga de datos masiva.

- **Objetivo**: mostrar los 10 procesos más utilizados en la red para operar sobre PIIF.
- **Tipo de widget**: gráfico de barras.
- **Datos mostrados**: histórico del número de operaciones ejecutadas sobre ficheros PIIF agrupadas por los 10 procesos más frecuentes.
- **Agrupación**: proceso.

Number of Malware processes accessing PII files

Este widget permite al administrador anticipar incidentes de seguridad relacionados con el robo de información (troyano, APT) o de destrucción/secuestro de la información, como el Ransomware, mostrando el acceso a información personal por procesos clasificados como "Malware".

- **Objetivo**: mostrar una evolución de los accesos a ficheros PII de los procesos clasificados por **Cytomic EDR** como malware.
- **Tipo de widget**: gráfico de líneas.
- **Datos mostrados**: evolución del número de operaciones ejecutadas sobre ficheros PIIF totales. Muestra la media de accesos mensual en una barra discontinua, con el nombre de Average.
- **Agrupación**: procesos clasificados como malware.

Distribution of processes by category

Este widget compara la cantidad de procesos seguros frente a los catalogados como malware, buscando cambios en sus proporciones que detecten posibles ataques a escala organizacional.

- **Objetivo**: mostrar el porcentaje de los procesos que operan con PII según su clasificación.
- **Tipo de widget**: gráfico de tarta.
- **Datos mostrados**: porcentaje de procesos por clasificación.
- **Agrupación**: clasificación de proceso (malware, goodware, monitoring y suspicious).

User operations on PII files

Muestra el tipo de operaciones sobre ficheros con información personal que se ejecutan en la empresa, revelando en qué clase de dispositivos se encontraban los datos (dispositivos portables o internos), como un indicio de potenciales problemas de comunicación y fuga de información.

User operations

- **User operations**: muestra los tipos de operación sobre PIIF y a los usuarios envueltos en operaciones clasificadas como comunicación o fuga de datos personales.
- **Type of operations**: tipo de operaciones ejecutadas sobre PIIF diferenciando la clase de medio de almacenamiento donde residen (portable o interno).

User operations on PII files by device type

Este widget muestra un listado completo de los usuarios que manejan ficheros PII que residen en cualquier tipo de medio de almacenamiento en la empresa. Con esta información, el administrador puede anticipar medidas de seguridad adicionales para los usuarios que estén haciendo un mayor uso de la información personal, o para aquellos que almacenan la información sobre dispositivos portátiles.

- **Objetivo**: mostrar a los usuarios que han efectuado operaciones sobre ficheros con información personal e información complementaria.

- **Campos**:

Campo	Descripción
User	Cuenta de usuario que ejecutó el programa que accede al fichero con datos personales.
DeviceType	Tipo de dispositivo que contiene el fichero accedido. Consulta en el capítulo "**Tablas de conocimiento PII**" en la página **83** el campo **DeviceType** para obtener un listado de los valores posibles.
Operation	Operación ejecutada sobre los ficheros PII. Consulta en el capítulo "**Tablas de conocimiento PII**" en la página **83** el campo **Operation** para obtener un listado de los valores posibles.
Count	Número de operaciones ejecutadas por el usuario del tipo y sobre el dispositivo indicados.
%	Porcentaje de operaciones sobre el total de operaciones registradas.

Tabla 5.8: campos del widget User operations by device type in PII files

Calendar of user operations on removable drives

Este widget monitoriza las operaciones sobre ficheros personales de la organización en unidades extraíbles, mostrando su evolución a lo largo del mes. Esta información puede utilizarse para localizar posibles fugas de información dado que los dispositivos referidos en el widget son portables.

- **Objetivo**: mostrar la evolución de las operaciones sobre ficheros con información personal que residen en dispositivos de almacenamiento externo.
- **Tipo de widget**: gráfico calendario.
- **Datos mostrados**: número de operaciones sobre PII en dispositivos externos agrupados por día del mes.
- **Agrupación**: día del mes.

Users involved in exfiltration operations

Este widget muestra el número de operaciones de introducción y extracción de ficheros con información personal ejecutadas por cada usuario de la red. Esta información es útil para el administrador para detectar usuarios que hacen un uso ilegítimo de la información.

- **Objetivo**: mostrar el número de operaciones por usuario relativas a la introducción y extracción de ficheros con información personal.
- **Campos**:

Campo	Descripción
User	Cuenta de usuario que ejecutó el programa con datos personales que extrae o introduce fichero en la red de la empresa.

Tabla 5.9: campos del widget Users involved in exfiltration operations

Campo	Descripción
Exfiltration flag	Indica si la operación ejecutada sobre el fichero PII fue de introducción o extracción de datos en el equipo del usuario o servidor.
Count	Número de operaciones registradas del tipo indicado.
%	Porcentaje de operaciones sobre el total de operaciones registradas.

Tabla 5.9: campos del widget Users involved in exfiltration operations

Types of operations

Distribution of types of operation in PII files

Este widget muestra las operaciones más frecuentemente ejecutadas sobre ficheros con información personal. El administrador podrá comprobar la variación en el volumen de operaciones y utilizarlo como indicador de eventos o incidentes relacionados con la información personal.

- **Objetivo**: mostrar el porcentaje de tipos de operaciones ejecutadas sobre ficheros con información personal.
- **Tipo de widget**: gráfico de tarta.
- **Datos mostrados**: porcentajes de tipos de operación.
- **Agrupación**: tipo de operación.

Distribution of operations in removable devices

Este widget muestra un índice para valorar la peligrosidad de las operaciones efectuadas sobre ficheros con información personal. Si el mayor porcentaje de operaciones se efectúa sobre dispositivos extraíbles, el administrador podrá tomar medidas que reduzcan las probabilidades de una filtración de datos.

- **Objetivo**: compara el porcentaje de operaciones efectuadas sobre ficheros con información personal que residen en dispositivos de almacenamiento fijo, frente a las operaciones sobre dispositivos extraibles.
- **Tipo de widget**: gráfico de tarta.
- **Datos mostrados**: porcentajes de tipos de operación sobre dispositivos fijos y extraíbles.
- **Agrupación**: tipo de dispositivo.

Most active users

Muestra los usuarios de la empresa más propensos a protagonizar fugas de información en función del número de operaciones que ejecutan sobre ficheros con datos personales y del malware ejecutado en sus puestos.

- **Active users by type of operation**: muestra los usuarios que más operaciones ejecutan sobre ficheros PII.

- **Top users running malware**: muestra los usuarios que ejecutan más procesos clasificados como malware.

Top 10 users involved in create operations

Este widget localiza a los usuarios clave de la organización que generan un mayor número de ficheros sin estructura de la empresa con información personal.

- **Objetivo**: mostrar los usuarios que crean más ficheros con información personal.
- **Campos**:

Campo	Descripción
User	Cuenta de usuario que ejecutó el programa que crea el fichero con datos personales.
Count	Número de operaciones registradas del tipo indicado.
%	Porcentaje de operaciones sobre el total de operaciones registradas.

Tabla 5.10: campos del widget Top 10 users involved in create operations

Top 10 users involved in open operations

- **Objetivo**: muestra los usuarios que acceden a más ficheros con información personal.
- **Campos**:

Campo	Descripción
User	Cuenta de usuario que ejecutó el programa que abre el fichero con datos personales.
Count	Número de operaciones registradas del tipo indicado.
%	Porcentaje de operaciones sobre el total de operaciones registradas.

Tabla 5.11: campos del widget Top 10 users involved in open operations

Top 10 users involved in copy-paste operations

- **Objetivo**: muestra los usuarios que copian y pegan más ficheros con información personal.
- **Campos**:

Campo	Descripción
User	Cuenta de usuario que copió o pegó el fichero con datos personales.
Count	Número de operaciones registradas del tipo indicado.
%	Porcentaje de operaciones sobre el total de operaciones registradas.

Tabla 5.12: campos del widget op 10 users involved in copy-paste operations

Top 10 users involved in rename operations

- **Objetivo**: muestra los usuarios que más veces cambian de nombre a ficheros con información personal.
- **Campos**:

Campo	Descripción
User	Cuenta de usuario que renombró el fichero con datos personales.
Count	Número de operaciones registradas del tipo indicado.
%	Porcentaje de operaciones sobre el total de operaciones registradas.

Tabla 5.13: campos del widget Top 10 users involved in rename operations

Top 10 users running malware

Este widget muestra los usuarios que utilizan equipos o servidores infectados y que lanzan procesos clasificados como malware con sus credenciales, bien de forma voluntaria o involuntaria (botnets, infecciones accidentales, etc.).

- **Objetivo**: muestra los usuarios que más operaciones ejecutaron sobre ficheros con información personal mediante procesos clasificados como malware.
- **Campos**:

Campo	Descripción
User	Cuenta de usuario que ejecuto el malware que opera con datos personales.
Count	Número de operaciones registradas del tipo indicado.
%	Porcentaje de operaciones sobre el total de operaciones registradas.

Tabla 5.14: campos del widget Top 10 users running malware

Top 100 users sending attachments with PII

- **Objetivo**: muestra los 100 usuarios que tienen el mayor número de correos enviados con ficheros PII adjuntos.
- **Campos**:

Campo	Descripción
User	Nombre del usuario que envía correos con ficheros PII adjuntos.
Count	Número de ficheros PII del usuario enviados por correo.
%	Porcentaje del número de ficheros PII del usuario enviados por correo sobre el total de ficheros PII de todos los usuarios enviados por correo.

Tabla 5.15: campos del widget TOP 100 users that send attachments that include PII

Top 100 users receiving attachments with PII

- **Objetivo**: muestra los 100 usuarios que tienen el mayor número de correos recibidos con ficheros PII adjuntos.
- **Campos**:

Campo	Descripción
User	Nombre del usuario que reciben correos con ficheros PII adjuntos.
Count	Número de ficheros PII del usuario y recibidos por correo.
%	Porcentaje del número de ficheros PII del usuario recibidos por correo sobre el total de ficheros PII de todos los usuarios recibidos por correo.

Tabla 5.16: campos del widget TOP 100 users that received attachments that include PII

Risk of PII exfiltration

Muestra las operaciones ejecutadas sobre ficheros con información personal que Cytomic Data Watch clasifica como riesgo de fuga o comunicación de datos.

Risk of exfiltration

Number of operations with files at risk of exfiltration

Este widget muestra la evolución de los accesos a ficheros con información personal clasificados por Cytomic Data Watch como pertenecientes a un incidente de comunicación de datos no autorizada. Un salto en la gráfica puede ser el síntoma de un robo de datos en la empresa.

- **Objetivo:** mostrar a lo largo del tiempo los accesos a ficheros PII que han sido clasificados en algún momento como entrada (infiltración), salida (exfiltración) de datos, o ambos (both).
- **Tipo de widget**: gráfico de líneas.
- **Datos mostrados**: operaciones clasificadas como comunicación o recepción de datos no autorizadas.
- **Agrupación**: tipo de acción (infiltración, exfiltración y ambos).

Operations with files at risk of exfiltration and infiltration

- **Objetivo**: mostrar la relación detectada entre el volumen de eventos monitorizados en la red y catalogados como recepción, envío de ficheros que contienen datos personales, y ambos.
- **Tipo de widget**: gráfico de tarta.
- **Datos mostrados**: porcentajes de clasificación de operaciones.
- **Agrupación**: clasificación de operación.

Top 10 largest files at risk of exfiltration

- **Objetivo**: mostrar los ficheros accedidos de mayor volumen y que contienen información personal.
- **Campos**:

Campo	Descripción
Document name	Nombre del documento PII.
User	Cuenta de usuario que accedió al documento.
Machine IP	Dirección IP del equipo que contiene el fichero PII.
Machine Name	Nombre del equipo que contiene el fichero PII.
Document size (MB)	Tamaño del documento en Megabytes.

Tabla 5.17: campos del widget Top 10 largest files at risk of exfiltration

User Monitored Files

Files

Top 100 rules with most operations on monitored files

- **Objetivo**: muestra las 100 reglas que han generado el mayor número de operaciones de monitorización. Este widget se utiliza para determinar cuan efectivas son las reglas definidas por el administrador a la hora de localizar ficheros en la red del cliente.
- **Campos**:

Campo	Descripción
Rule	Nombre de la regla que monitoriza ficheros.
Count	Número de operaciones registradas por la regla.
%	Porcentaje de operaciones registradas por la regla sobre el total de operaciones registradas por todas las reglas de monitorización.

Tabla 5.18: campos del widget Top 100 rules with operations on files monitored

Top 100 monitored files with most operations

- **Objetivo**: muestra los 100 ficheros que tienen el mayor número de operaciones registradas por las reglas de monitorización definidas.

- **Campos**:

Campo	Descripción
File Name	Nombre del fichero monitorizado.
Count	Número de operaciones registradas para el fichero indicado.
%	Porcentaje de operaciones monitorizadas del fichero sobre el total de operaciones registradas para todos los ficheros monitorizados.

Tabla 5.19: campos del widget Top 100 files monitored with most operations

Top 100 machines with most operations on monitored files

- **Objetivo**: muestra los 100 equipos que tienen el mayor número de operaciones de ficheros registradas por las reglas de monitorización definidas.
- **Campos**:

Campo	Descripción
Machine	Nombre del equipo con ficheros monitorizados.
Count	Número de operaciones registradas en los ficheros monitorizados del equipo.
%	Porcentaje de operaciones monitorizadas de los ficheros del equipo sobre el total de operaciones registradas para todos los ficheros monitorizados en todos los equipos.

Tabla 5.20: Top 100 machines with operations on files monitored

Attachments

Top 100 machines sending monitored attachments

- **Objetivo**: muestra los 100 equipos que tienen el mayor número de correos enviados con ficheros adjuntos monitorizados.
- **Campos**:

Campo	Descripción
Machine	Nombre del equipo desde donde se envían los ficheros adjuntos monitorizados.
Count	Número de ficheros adjuntos enviados monitorizados por el equipo.
%	Porcentaje de ficheros adjuntos enviados por el equipo sobre el total de ficheros monitorizados enviados por todos los equipos.

Tabla 5.21: campos del widget Top 100 machines that sent attachments monitored

Top 100 users sending monitored attachments

- **Objetivo**: muestra los 100 usuarios que tienen el mayor número de correos enviados con ficheros

adjuntos monitorizados.

- **Campos**:

Campo	Descripción
User	Nombre del usuario que envía correos con ficheros adjuntos monitorizados.
Count	Número de ficheros del usuario monitorizados y enviados por correo.
%	Porcentaje del número de ficheros del usuario enviados por correo sobre el total de ficheros de todos los usuarios enviados por correo.

Tabla 5.22: campos del widget TOP 100 users that sent attachments monitored

Top 100 users receiving monitored attachments

- **Objetivo**: muestra los 100 usuarios que tienen el mayor número de correos recibidos con ficheros adjuntos monitorizados.

Campos:

Campo	Descripción
User	Nombre del usuario que recibe correos con ficheros adjuntos monitorizados.
Count	Número de ficheros del usuario monitorizados y recibidos por correo.
%	Porcentaje del número de ficheros del usuario recibidos por correo sobre el total de ficheros de todos los usuarios enviados por correo.

Tabla 5.23: campos del widget TOP 100 users that received attachments monitored

Capítulo 6

Alertas

El sistema de alertas de Cytomic Data Watch mantiene informado al administrador sobre los eventos producidos en la red que requieran de su atención, sin necesidad de acudir a la consola web. Se trata por lo tanto de un módulo decisivo a la hora de minimizar el tiempo de reacción del departamento de IT al enfrentarse a situaciones potencialmente peligrosas para la empresa.

El sistema de alertas es completamente configurable por el administrador de la red, incluyendo el ritmo de envío de alertas, las condiciones necesarias para su generación y el método de entrega empleado.

CONTENIDO DEL CAPÍTULO

Alertas predefinidas

Cytomic Data Watch incluye alertas predefinidas que informan al administrador de las actividades potencialmente peligrosas detectadas en la red.

Para acceder a la definición de las alertas predefinidas:

- Haz clic en el menú lateral **Administración**, **Configuración de las alertas**.
- En el panel de la izquierda haz clic en **Adaptive Defense**. En el panel de la derecha haz clic en **Data Access Control**.
- La parte inferior del panel es desplegará con las alertas definidas. Haz clic en una alerta para ver su descripción.

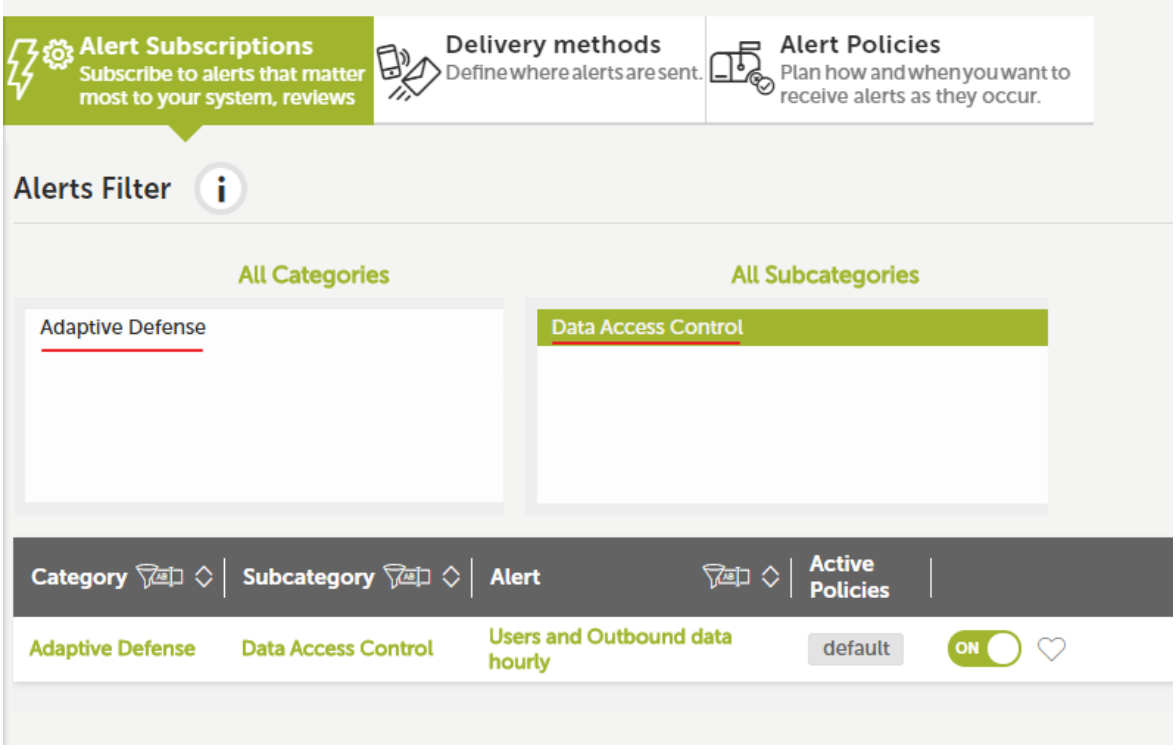

Figura 6.1: ventana de administración de alertas

Las alertas predefinidas son:

- Too many operations by process.
- Malware detected.

- Too many exfiltration operations by user.
- User Operations.
- User rename operations.
- User create operations.
- User open operations.
- User copy-paste operations.
- Data leak.

Too many operations by process

Objetivo: genera una alerta cada vez que un proceso ejecute más de 50 operaciones sobre uno o varios ficheros PII en un intervalo de 10 segundos.

Linq:

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

Malware detected

Objetivo: genera una alerta cuando proceso malicioso ejecuta una operación en un documento PII.

Linq:

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

Too many exfiltration operations by user

Objetivo: genera una alerta cuando un usuario ejecuta más de 5 operaciones clasificadas como de "exfiltración de datos" en un intervalo de 2 minutos.

Linq:

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

User Operations

Objetivo: genera una alerta cada vez que un usuario ejecuta más del 5% de operaciones de exfiltración sobre el total de operaciones de exfiltración registradas en un intervalo de cuatro horas.

Linq:

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

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

User rename operations

Objetivo: genera una alerta cada vez que un usuario ejecuta más del 5% de operaciones de renombrado de ficheros sobre el total de operaciones de renombrado registradas en un intervalo de cuatro horas.

Linq:

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

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

User create operations

Objetivo: genera una alerta cada vez que un usuario ejecuta más del 5% de operaciones de creación de ficheros sobre el total de operaciones de creación registradas en un intervalo de cuatro horas.

Linq:

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

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

User open operations

Objetivo: genera una alerta cada vez que un usuario ejecuta más del 5% de operaciones de apertura de ficheros sobre el total de operaciones de apertura registradas en un intervalo de cuatro horas.

Linq:

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

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

User copy-paste operations

Objetivo: genera una alerta cada vez que un usuario ejecuta más del 5% de operaciones de copiado y pegado de contenidos sobre el total de operaciones de copiado y pegado registradas en un intervalo de cuatro horas.

Linq:

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

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

Data leak

Objetivo: genera una alerta cada vez que se produce una operación de exfiltración sobre un documento de tamaño mayor a 25 Mbytes.

Linq:

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

Arquitectura del sistema de alertas

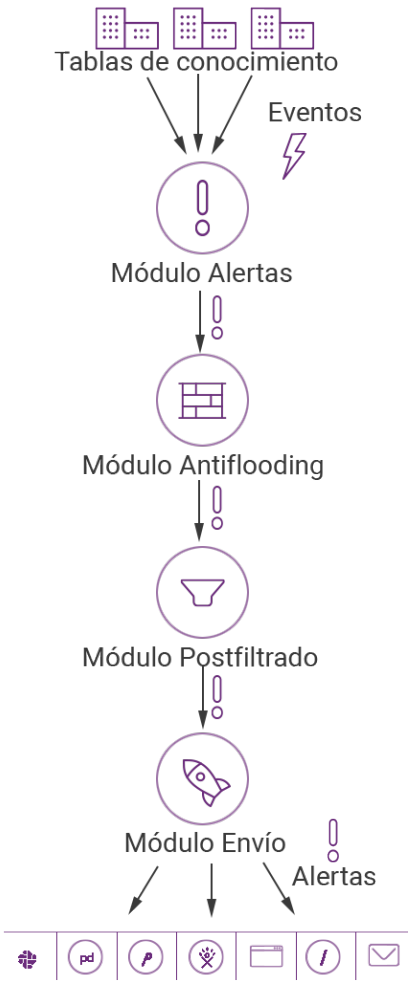

Figura 6.2: Módulos implementados en el flujo de generación de alertas

El sistema de alertas de Cytomic Data Watch está formado por varios módulos completamente configurables. La secuencia de procesos que involucran la generación de alertas es la siguiente:

- **Generación de eventos**: cada inserción en una tabla de conocimiento genera un único evento que puede ser convertido posteriormente en una o más alertas.
- **Módulo alertas**: los eventos que cumplan ciertos criterios definidos por el administrador en el módulo de alertas generarán una alerta.
- **Módulo Antiflooding**: evita el problema de "tormenta de alertas", permitiendo desconectar temporalmente el módulo de generación de alertas de la generación de eventos al superar ciertos umbrales definidos por el administrador. De esta forma se evita la generación excesiva de alertas.
- **Módulo Postfiltrado**: manipula las alertas una vez generadas, cambiando sus propiedades, o incluso eliminándolas de forma selectiva según los criterios definidos por el administrador.
- **Módulo de envío**: configura la entrega de alertas al administrador de la red de múltiples formas: Email, HTTP-JSON, Service Desk, Jira, Pushover, Pagerduty y Slack. Para más información consulta el apartado "**Creación de configuraciones de entrega**".

Proceso de configuración de alertas

La puesta en marcha de una nueva alerta requiere una serie de pasos, algunos de ellos obligatorios, otros de ellos opcionales, para su correcto funcionamiento.

A continuación se enumeran los pasos junto a una breve descripción del proceso.

1. **Creación de alertas (obligatorio)**: la creación de una alerta requiere definir el tipo de evento que se recoge de la tabla de conocimiento, y que será convertido en alerta.
2. **Modificación de la suscripción de alertas (opcional)**: activa o desactiva la alerta recién creada. Las alertas creadas se activan de forma automática.
3. **Crear una configuración de entrega (obligatorio para la primera alerta)**: las configuraciones de entrega determinan el método de entrega e indican su información asociada. Por ejemplo, en el

caso del establecimiento de una configuración de entrega por email, será necesario indicar la cuenta de correo destinatario.

4. **Crear una política Antiflooding (opcional)**: se establecen cuáles son los umbrales máximos de generación de alertas para evitar envíos masivos. Los administradores que prefieran recibir todas las alertas generadas no utilizarán ninguna política Antiflooding.
5. **Crear una nueva política de envío (obligatorio para la primera alerta)**: en una política de envío se definen los siguientes parámetros de envío de alertas:
   - **Asignación de la política antiflloding** (punto 4).
   - **Asignación de calendario de envío**: las alertas solo se enviarán en el calendario configurado.
   - **Método de entrega** (punto 3).
6. **Asignación de la política de envío** (punto 5) a la alerta creada (punto 1).
7. **Creación de postfiltros (opcional)**: para manipular la alerta generada antes de su envío es necesario crear un postfiltro.

El diagrama de bloques que forma una alerta es el siguiente:

Figura 6.3: componentes lógicos que forman una alerta

Creación de alertas

La creación de alertas se realiza desde la tabla de conocimiento asociada. Para ello ~~es necesario~~ sigue los pasos siguientes.

1. Seleccione la tabla apropiada en el menú lateral, **Búsqueda**.
2. Aplique los filtros y transformaciones de datos que sean necesarios para generar la información

necesaria, y haz clic en el icono  , en la barra de herramientas.

3. Configura los parámetros de la alerta.

Parámetro	Descripción
Subcategory	Etiqueta para clasificar la alerta y facilitar su búsqueda o filtrado posteriores.
Context	Etiqueta para clasificar la alerta y facilitar su búsqueda o filtrado posteriores.
Message	Asunto de la alerta.
Description	Contenido de la alerta.

Tabla 6.1: parámetros de una alerta

4. Establece el ritmo de generación de alertas.

Opción	Descripción
Each	Genera una alerta por cada evento de inserción en la tabla.
Several	Define un intervalo y un umbral para la generación de alertas.
Period	intervalo en el cual aplica el umbral.
Threshold	Umbral que establece cada cuantos eventos recibidos en el intervalo definido se envía una única alerta.
Counters	Añade columnas de la tabla de conocimiento a la alerta. El contenido de un campo contador podrá ser incorporado al asunto o descripción de la alerta simplemente poniendo el nombre del campo precedido por el símbolo $.

Tabla 6.2: frecuencias de envío de alertas

Si por ejemplo se define un **Period** de 5 minutos y un **Threshold** de 30, hasta el evento 30 no se enviará la primera alerta. El evento 60 generará la segunda alerta y así sucesivamente hasta cumplir los 5 minutos de **Period**, momento en el que el contador de eventos se reinicia a 0.

En el proceso de creación de alertas se comprueba el volumen de alertas que generará la configuración elegida. Si la definición de la alerta genera más de 60 alertas por minuto, la configuración de la alerta será inválida. Incrementar el campo Threshold suele ser suficiente para bajar el número de alertas generadas por minuto.

Una vez creada la alerta el sistema comenzará a generar registros según se vayan produciendo los eventos coincidentes con la definición de la alerta. Para ver el registro de alertas generado consulta más adelante el punto "**Gestión de alertas**".

Gestión de alertas

La gestión de las alertas generadas se realiza haciendo clic en el menú lateral **Alertas**. Haz clic en la pestaña **Panel de alertas** se mostrarán las secciones: **Vista general de alertas** e **Historial de alertas**.

Vista general de alertas

La vista general de alertas representa mediante varias gráficas las alertas producidas por el sistema.

Las gráficas son configurables por el administrador mediante la barra de herramientas.

Representa mediante varias gráficas las alertas producidas por el sistema. Las gráficas son configurables por el administrador mediante la barra de herramientas.

Figura 6.4: barra de herramientas para configurar los listados de alertas

- **Tipo de gráfica** (1): elige la forma de representar las alertas recibidas:
  - Gráfico de líneas.
  - Línea temporal agrupando las alertas próximas.
  - Gráfica de tipo calendario.
  - Gráfico de tipo Voronoi.
- **Activar / desactivar grafica de tarta** (2).
- **Intervalo de tiempo representado en la gráfica** (3):
  - 1 hora.
  - 6 horas.
  - 12 horas.
  - 1 día.
  - 1 semana.
  - 1 año.
- **Filtrado por estado de la alerta** (4):.

Estado	Descripción
Abierta	Solo se muestran las alertas en estado **Abierta.**
Todas las alertas	Se muestran todas las alertas.

Tabla 6.3: estados de una alerta

Consulta el capítulo "Aplicaciones configuradas" en la página 47 para obtener más detalles de cada tipo de gráfica.

Historial de alertas

En la sección **Historial** de alertas se muestra un listado las alertas generadas. Cada alerta tiene una serie de campos que el sistema completa según la configuración establecida por el administrador en el momento de creación de la alerta:

Campo	Descripción
Estado	Vista, no leída.
Tipo	Tipo de la alerta, tomado del campo **Message** en la configuración de la alerta, descrito en el punto **Creación de alertas** más arriba en este capítulo.
Información detallada	Extracto del cuerpo de la alerta tomada del campo **Description,** descrito en el punto **Creación de alertas** más arriba en este capítulo. Haz clic en el campo **Información detallada** de la alerta para desplegar su contenido.
Categoría	Categoría de la alerta tomada del campo **Subcategory** y **Context,** descrito en el punto **Creación de alertas** más arriba en este capítulo.
Prioridad	Todas las alertas se generan inicialmente con prioridad normal. Para cambiar la prioridad de una alerta generada (**muy baja**, **baja**, **normal**, **alta**, **muy alta**) configura un postfiltro. Consulta el punto **Configuración de posfiltros** más adelante.
Creada	Fecha, hora y tiempo transcurrido desde la generación de la alerta.
Menú	La última columna de la tabla de **Historial de alertas** permite desplegar un menú de opciones para cada alerta.
Ver detalles de alerta	Visualiza toda la información asociada a la alerta en una ventana independiente.
Crear anotación	Agrega un texto a la alerta. Al completar el formulario se añadirá un icono a la alerta indicando que un técnico hizo un comentario sobre la alerta. Convierte una anotación en una tarea si la alerta requiere de una intervención alargada en el tiempo.
Nuevo filtro	Crea postfiltros, descritos en el siguiente apartado.
Borrar	Borra la alerta.

Tabla 6.4: campos de una alerta

Establecimiento de filtros en el historial de alertas

Al hacer clic en el campo **Tipo**, **Categoría** o **Prioridad** de una alerta concreta se establece un filtro que muestra únicamente las alertas que coinciden con el criterio seleccionado.

Los filtros aplicados se muestran en la barra de filtros.

Creación de postfiltros

Los postfiltros modifican de forma discrecional las propiedades de las alertas generadas antes de su envío, y las borran si coinciden con los criterios definidos.

Los postfiltros se crean desde la ventana **Alertas** en el menú lateral, haciendo clic en el icono ooo de una alerta ya generada, para mostrar el menú desplegable de acciones. Haz clic en **Nuevo filtro** para acceder a la ventana de creación de filtros.

La pantalla de posfiltros está formada por cinco secciones:

- Descripción del postfiltro.
- Contenido base.
- Contenido extra.
- Filtros de fechas.
- Acción.

Sección 1: Descripción del postfiltro

En esta sección se especifica el nombre y las propiedades que han de cumplir las alertas para poder aplicar el postfiltro..

Campo	Descripción
Nombre	Nombre del nuevo postfiltro a crear.
Contexto	Establece como condición el contexto de la alerta para que el postfiltro sea aplicado.
Categoría	Establece como condición la categoría de la alerta para que el postfiltro sea aplicado.
Prioridad	Establece como condición la prioridad de la alerta para que el postfiltro sea aplicado.

Tabla 6.5: campos del postfiltro

Sección 2: Contenido base

Esta sección no tiene uso.

Sección 3: Contenido extra

Establece las condiciones en base al contenido de la alerta que tendrá que cumplir para que el postfiltro sea aplicado.

En el proceso de configuración de una alerta se establecen una serie de columnas en el campo **Counter**. El contenido de estas columnas es accesible desde el cuerpo de la alerta en el momento de su generación mediante el símbolo $, y con la sección **Contenido extra** elige del desplegable aquellos contadores que quieras incorporar como condición de filtrado.

Sección 4: Filtros de fechas

Establece uno o varios intervalos de fechas que actúen como condición. A todas las alertas que se generen fuera de los intervalos establecidos no se les aplicará el postfiltrado.

Sección 5: Acción

- Marcar como leído.
- Cambiar prioridad.
- Falso positivo.
- Cambiar método de envío.
- Eliminar.

Gestión de postfiltros

Haz clic en la pestaña **Post filtros** desde el menú lateral **Alertas** para mostrar un listado de los post filtros configurados con la información mostrada a continuación**.**

Campo	Descripción
Estado	Activo o inactivo.
Nombre	Nombre del postfiltro elegido por el administrador en su creación.
Categoría	Categoría que determina si el postfiltro se aplicará.
Contexto	Contexto que determina si el postfiltro se aplicará.
Prioridad	Prioridad de la alerta que determina si el postfiltro se aplicará.
Condiciones	Contenido de la alerta que determina si el postfiltro se aplicará.
Acción	Comando interno que aplicará el postfiltro.

Tabla 6.6: configuración de un postfiltro

Creación de configuraciones de entrega

Se crean en el menú lateral **Administración**, **Configuración de alertas**, en la pestaña **Configuración entrega**.

En el panel de la izquierda selecciona el tipo de entrega de entre los disponibles:

- **Email**: entrega de alertas por correo electrónico.
- **HTTP-JSON**: entrega de alertas mediante objetos JSON.
- **Service Desk**: entrega de alertas en un servidor Service Desk.
- **JIRA**: entrega de alertas en un servidor Jira.
- **PushOver**: entrega de alertas en una cuenta Pushover.
- **PagerDuty**: entrega de alertas en una cuenta PagerDuty.
- **Slack**: entrega las alertas a través del servicio Slack.

Una vez seleccionado el tipo de entrega, haz clic en el botón **Nuevo** para configurar un nuevo tipo de envío.

Email

Envía en tiempo real alertas a cuentas de correo.

Los campos requeridos son:

Campo	Descripción
Nombre	Nombre de la configuración de envío.
Email	Cuenta de correo de destinatario.
Huso horario	Ajusta la fecha y hora de envío del mail.
Idioma	Idioma en el que se recibe la alerta.

Tabla 6.7: configuración del método de envío de alertas por email

HTTP-JSON

Envía en tiempo real alertas por el protocolo HTTP o HTTPS utilizando objetos JSON mediante el método POST.

Para mejorar la seguridad, además de utilizar el protocolo de aplicación cifrado HTTPS se puede activar autenticación Digest.

Los campos requeridos son:

Campo	Descripción
Nombre	Nombre de la configuración de envío.
URL	URL del servidor destino indicando el protocolo (http o https) y el puerto (p.ej. `http://localhost:8080/index.php`)
Huso horario	Ajusta la fecha y hora de envío del mail.
Idioma	Idioma en el que se recibe la alerta.
Usuario	Solo se utiliza cuando la casilla de selección **Autenticado** ha sido marcada.
Contraseña	Solo se utiliza cuando la casilla de selección **Autenticado** ha sido marcada.

Tabla 6.8: configuración del método de envío de alertas HTTP-JSON

Una vez salvada la configuración se procederá al envío de un mensaje HTTP con un código para validar el servidor. En la lista de configuraciones de entrega JSON se mostrará la configuración nueva precedida de un punto de color rojo (estado, pendiente de validación). Haz clic en el punto rojo para abrir una ventana solicitando el código enviado al servidor. Una vez introducido la configuración de envío será plenamente funcional.

Service Desk

Envía en tiempo real alertas a servidores Service Desk Plus, utilizando dos métodos diferentes: REST y SERVLET.

Los campos requeridos son:

Campo	Descripción
Nombre	Nombre de la configuración de envío.
URL	URL del servidor destino.
REST	`http://[SERVER]:[PORT]/sdpapi/request/`
SERVLET	`http://[SERVER]:[PORT]/servlets/RequestServlet`
Método de envío	REST o SERVLET.
Huso horario	Ajusta la fecha y hora de envío del mail.
Idioma	Idioma en el que se recibe la alerta.
Usuario	Nombre del técnico asignado.
Technician Key	Llave del técnico generado en el panel de administración de Service Desk.

Tabla 6.9: configuración del método de envío de alertas Service desk

Una vez salvada la configuración se procederá al envío de un mensaje HTTP con un código para validar el servidor. En la lista de configuraciones de entrega Service desk se mostrará la configuración nueva precedida de un punto de color rojo (estado, pendiente de validación). Haz clic en el punto rojo para abrir una ventana solicitando el código enviado al servidor. Una vez introducido la configuración de envío será plenamente funcional.

JIRA

Envía en tiempo real alertas a servidores Jira.

Los campos requeridos son:

Campo	Descripción
Nombre	Nombre de la configuración de envío.
URL	URL del servidor destino (p.ej `http://localhost:8090/rest/api/2/issue.`)
Usuario	Nombre de usuario de JIRA.
Contraseña	Contraseña de JIRA.
Issue Type	Tipo de tarea que se creara en Jira. En la URL del servidor aparecerá un objeto Json con los proyectos creados. En la variable *issuetypes* se listan los tipos de incidencias permitidos por proyecto.

Tabla 6.10: configuración del método de envío de alertas JIRA

Campo	Descripción
Project key	Identificador del proyecto donde se creará la alerta. En la URL del servidor aparecerá un objeto Json con los proyectos creados y sus identificadores. La etiqueta Key contiene los identificadores de cada proyecto.
Huso horario	Ajusta la fecha y hora de envío del mail.
Idioma	Idioma en el que se recibe la alerta.

Tabla 6.10: configuración del método de envío de alertas JIRA

Una vez salvada la configuración se envía un mensaje HTTP con un código para validar el servidor. En la lista de configuraciones de entrega JIRA se mostrará la configuración nueva precedida de un punto de color rojo (estado, pendiente de validación). Haz clic en el punto rojo para abrir una ventana solicitando el código enviado al servidor. Una vez introducido la configuración de envío será plenamente funcional.

PushOver

Envía en tiempo real alertas a cuentas PushOver.

Los campos requeridos son:

Campo	Descripción
Nombre	Nombre de la configuración de envío.
Token Aplicación	API Key de la aplicación previamente creada en `https://pushover.net/apps`
Usuario/grupo	API Key del usuario o grupo al que desea enviar las alertas.
Dispositivo (opcional)	Nombre del dispositivo al que se quiere enviar las alertas.
Titulo (opcional)	Texto que aparecerá en el mensaje.
URL (opcional)	Link enviado en todas las alertas.
Título URL (opcional)	Texto que enlaza a la URL anterior.
Sonido (opcional)	Tipo de notificación que se desea recibir.
Huso horario	Ajusta la fecha y hora de envío del mail.
Idioma	Idioma en el que se recibe la alerta.

Tabla 6.11: configuración del método de envío de alertas Pushover

Una vez salvada la configuración se enviará un mensaje HTTP con un código para validar el servidor. En la lista de configuraciones de entrega Pushover se mostrará la configuración nueva precedida de un punto de color rojo (estado, pendiente de validación). Haz clic en el punto rojo para abrir una ventana solicitando el código enviado al servidor. Una vez introducido la configuración de envío será plenamente funcional.

PagerDuty

Envía en tiempo real alertas a cuentas PagerDuty.

Los campos requeridos son:

Campo	Descripción
Nombre	nombre de la configuración de envío.
Service Key	API KEY del servicio PagerDuty que recogerá la alerta.
Client	título o identificador que aparecerá en las alertas.
Client URL	enlace que se envía en todas las alertas.
Huso horario	ajusta la fecha y hora de envío del mail.
Idioma	idioma en el que se recibe la alerta.

Tabla 6.12: configuración del método de envío de alertas Pagerduty

Una vez salvada la configuración se envía un mensaje HTTP con un código para validar el servidor. En la lista de configuraciones de entrega Pagerduty se mostrará la configuración nueva precedida de un punto de color rojo (estado, pendiente de validación). Haz clic en el punto rojo para abrir una ventana solicitando el código enviado al servidor. Una vez introducido la configuración de envío será plenamente funcional.

SLACK

Envío en tiempo real de alertas por medio de SLACK.

Los campos requeridos son:

Campo	Descripción
Nombre	nombre de la configuración de envío.
Huso horario	ajusta la fecha y hora de envío de la alerta.
Canal	medio por el que se recibe el mensaje.
Webhook URL	URL del servidor de destino.
Idioma	idioma en el que se recibe la alerta.

Tabla 6.13: configuración del método de envío de alertas Slack

Una vez salvada la configuración se procederá al envío de un mensaje HTTP con un código para validar el servidor. En la lista de configuraciones de entrega Slack se mostrará la configuración nueva precedida de un punto de color rojo (estado, pendiente de validación). Al hacer clic en el punto rojo se abrirá una ventana solicitando el código enviado al servidor. Una vez introducido la configuración de envío será plenamente funcional.

Gestión de configuraciones de entrega

Cada una de las configuraciones de entrega creadas tiene asociado un menú para su edición y/o borrado.

Al editar una configuración de entrega ya creada se mostrará una ventana con las opciones para su modificación.

Creación de políticas antiflooding

Una política antiflooding interrumpe completa y temporalmente la generación de alertas cuando su ritmo sobrepasa cierto umbral definido por el administrador en la política.

La creación de políticas antiflooding se realiza desde el menú lateral **Administración**, **Creación de alertas**, en la pestaña **Política de alertas**, pestaña lateral **Política antiflooding**.

Haciendo clic en **Nuevo** se mostrará una ventana con la configuración completa de la política.

Parámetro	Descripción
Nombre	Nombre de la política de envío.
Por defecto	Indica si la política de envío es tratada como política por defecto. En el caso de existir alertas que no tengan una política de envió asignada se aplicará ésta por defecto.
Política Antiflooding	Indica la política antiflooding a aplicar.
Calendario	Marca los rangos de tiempo en los que la política de envío estará activa.
Configuración de envío	Indica una o varías formas de envío configuradas previamente, que se utilizaran para despachar la alerta.

Tabla 6.14: para metro de la política de envío

Edición de políticas de envío

Cada una de las políticas de envío creadas tiene asociado un menú que permite su edición y/o borrado.

Al editar una política de envío ya creada se mostrará una ventana con las opciones para su modificación.

Configuración de la política de envío de una alerta

La asignación de políticas de envío a las alertas creadas se realiza desde el menú lateral **Administración**, **Creación de alertas**, en la pestaña **Suscripción de alertas**.

Cada alerta tiene un icono  asociado que con el que seleccionar una política de envío de entre todas las creadas.

Parte 3

Información adicional

Capítulo 7: Tablas de conocimiento PII

Capítulo 8: Listado de extensiones

Capítulo 9: Listado de procesos

Capítulo 10: Requisitos de hardware, software y red

Capítulo 7

Tablas de conocimiento PII

Cytomic EDR recoge la información de los procesos ejecutados en los puestos de usuario y servidores tanto si son goodware como malware. Si estos procesos acceden a ficheros PII la información se envía al servidor Cytomic Data Watch, que se encargará de organizarla en tablas de fácil acceso para el administrador.

Cada línea de la tabla se corresponde a un evento supervisado por Cytomic Data Watch y ofrece información del momento en que ocurrió el evento, el equipo donde se registró, su dirección IP, etc.

Tabla oem.panda.edp.ops

Almacena toda la información recogida de la monitorización de los ficheros PII.

Nombre	Descripción	Valores
evendate	Fecha de inserción del evento en el servidor Cytomic Data Watch.	Fecha
serverdate	Fecha del equipo de usuario o servidor cuando se generó el evento.	Fecha
machineName	Nombre del equipo de usuario o servidor.	Cadena de caracteres
machineIP	IP del equipo de usuario o servidor.	Dirección IP
user	Nombre de usuario del proceso que actuó sobre el fichero.	Cadena de caracteres
exfiltrationFlag	Indica que el fichero ha sido objeto de una operación clasificada como de entrada de datos, fuga o comunicación de datos o ambas.	• INFILTRATION • EXFILTRATION • BOTH
docSize	Tamaño del fichero PII en Bytes.	Numérico

Tabla 7.1: tabla oem.panda.edp.ops

Nombre	Descripción	Valores
op	Operación ejecutada sobre el fichero PII.	• **Create** • **Modify** • **Open** • **Delete** • **Rename** • **Copy-Paste** • **OnDemand**: fichero PII encontrado en el análisis bajo demanda lanzado desde la consola web.
fatherHash	MD5 del proceso que opera sobre el fichero PII. Este campo aparece vacío si **operation** es **On Demand.**	Cadena de caracteres
fatherPath	Ruta del proceso que opera sobre el fichero PII. Este campo aparece vacío si **operation** es **On Demand.**	Cadena de caracteres
fatherCat	Categoría del proceso que opera sobre el fichero PII. Este campo aparece vacío si **operation** es **On Demand.**	• **Goodware** • **Malware** • **Monitoring**: proceso desconocido en clasificación • **PUP**: programa no deseado
documentPath	Unidad donde se encuentra el fichero PII sobre el cual se opera y su ruta, en formato DEVICE TYPE|PATH.	Cadena de caracteres
documentName	Nombre del fichero sobre el que se actúa. En las operaciones de renombrado, este campo contiene el **DocumentName** del fichero sin renombrar y el **DocumentName** del fichero renombrado en formato NOMBRE_DESTINO|NOMBRE_ORIGEN.	• Cadena de caracteres • Cadena de caracteres | Cadena de caracteres
documentHash	Hash del fichero sobre el que se ejecuta la operación.	Cadena de caracteres
deviceType	Unidad donde se encuentra el fichero PII sobre el cual se actúa.	• **0**:**UNKNOWN** • **1**:**NO_ROOT_DIR**: ruta invalida o no existente • **2**:**REMOVABLE**: dispositivo portátil (disquetera, lector de tarjetas, dispositivo USB, etc.)

Tabla 7.1: tabla oem.panda.edp.ops

Nombre	Descripción	Valores
		• **3**: **FIXED**: disco duro interno • **5**: **CDROM** • **6**: **RAMDISK** • Cadena de caracteres
creditCard	Indica si se encontraron o no entidades de tipo Tarjetas de crédito en el fichero PII.	Booleano
bankAccount	Indica si se encontraron o no entidades de tipo Cuenta bancaria en el fichero PII.	Booleano
personalID	Indica si se encontraron o no entidades de tipo Tarjetas de identidad (DNI) en el fichero PII.	Booleano
driveLic	Indica si se encontraron o no entidades de tipo Carnet de conducir en el fichero PII.	Booleano
passPort	Indica si se encontraron o no entidades de tipo Pasaporte en el fichero PII.	Booleano
SSId	Indica si se encontraron o no entidades de tipo Número de la seguridad social en el fichero PII.	Booleano
email	Indica si se encontraron o no entidades de tipo mail en el fichero PII.	Booleano
IP	Indica si se encontraron o no entidades de tipo Dirección IP en el fichero PII.	Booleano
name	Indica si se encontraron o no entidades de tipo Nombre y apellidos en el fichero PII.	Booleano
address	Indica si se encontraron o no entidades de tipo Dirección en el fichero PII.	Booleano
phone	Indica si se encontraron o no entidades de tipo Teléfono en el fichero PII.	Booleano
estimatedNumPII	Número estimado de entidades encontradas.	Numérico
Reclassified	• **True**: anteriormente el fichero contenía PII pero en la actualidad no. • **False**: el fichero no ha sido reclasificado y por tanto contiene PII.	Booleano

Tabla 7.1: tabla oem.panda.edp.ops

Tabla oem.paps.edp.usrrules

Almacena toda la información recogida de la monitorización de ficheros que pertenecen a las reglas definidas por el administrador.

Nombre	Descripción	Valores
evendate	Fecha de inserción del evento en el servidor Cytomic Data Watch.	Fecha
serverdate	Fecha del equipo de usuario o servidor cuando se generó el evento.	Fecha
machineName	Nombre del equipo de usuario o servidor.	Cadena de caracteres
machineIP	IP del equipo de usuario o servidor.	Dirección IP
user	Nombre de usuario que inició una sesión interactiva cuando se registro el evento registrado.	Cadena de caracteres
exfiltrationFlag	Indica que el fichero ha sido objeto de una operación clasificada como de entrada de datos, fuga o comunicación de datos o ambas.	• INFILTRATION • EXFILTRATION • BOTH
docSize	Tamaño del fichero en Bytes.	Numérico
op	Operación ejecutada sobre el fichero PII.	• **Create** • **Modify** • **Open** • **Delete** • **Rename** • **Copy-Paste**
fatherHash	MD5 del proceso que opera sobre el fichero.	Cadena de caracteres
fatherPath	Ruta del proceso que opera sobre el fichero.	Cadena de caracteres
fatherCat	Categoría del proceso que opera sobre el fichero.	• **Goodware** • **Malware** • **Monitoring**: proceso desconocido en clasificación • **PUP**: programa no deseado
documentPath	Unidad donde se encuentra el fichero sobre el cual se opera y su ruta, en formato DEVICE TYPE|PATH.	Cadena de caracteres

Tabla 7.2: Tabla oem.paps.edp.usrrules

Nombre	Descripción	Valores
documentName	Nombre del fichero sobre el que se actúa. En las operaciones de renombrado, este campo contiene el **DocumentName** del fichero sin renombrar y el **DocumentName** del fichero renombrado en formato NOMBRE_DESTINO | NOMBRE_ORIGEN.	• Cadena de caracteres • Cadena de caracteres | Cadena de caracteres
documentHash	Hash del fichero sobre el que se ejecuta la operación.	Cadena de caracteres
deviceType	Unidad donde se encuentra el fichero PII sobre el cual se actúa.	• **0**:**UNKNOWN** • **1**:**NO_ROOT_DIR**: ruta invalida o no existente • **2**:**REMOVABLE**: dispositivo portátil (disquetera, lector de tarjetas, dispositivo USB, etc.). • **3**: **FIXED**: disco duro interno • **5**: **CDROM** • **6**: **RAMDISK** • Cadena de caracteres
usrRules	Nombre de las reglas introducidas en la consola de Cytomic EDR separadas por el carácter " | " que están monitorizando el fichero.	Cadena de caracteres | Cadena de caracteres | Cadena de caracteres...

Tabla 7.2: Tabla oem.paps.edp.usrrules

Tabla oem.paps.edp.usrrulesmail

Almacena toda la información de los mensajes de correo que contienen ficheros encontrados y monitorizados en la red del cliente a través de las reglas definidas por el administrador.

Nombre	Descripción	Valores
evendate	Fecha de inserción del evento en el servidor Cytomic Data Watch.	Fecha
serverdate	Fecha del equipo de usuario o servidor cuando se generó el evento.	Fecha
machineName	Nombre del equipo de usuario o servidor.	Cadena de caracteres
machineIP	IP del equipo de usuario o servidor.	Dirección IP
loggeduser	Nombre de usuario que inició una sesión interactiva cuando se registro el evento registrado.	Cadena de caracteres

Tabla 7.3: Tabla oem.paps.edp.usrrulesmail

Nombre	Descripción	Valores
msgID	Identificador único del mensaje.	Cadena de caracteres
msgTo	Dirección de correo destino del mensaje.	Cadena de caracteres
msgFrom	Dirección de correo origen del mensaje.	Cadena de caracteres
msgSentDate	Fecha de envío del mensaje. En los mensajes recibidos el campo contiene Null.	Fecha
msgSubject	Asunto del mensaje.	Cadena de caracteres
msgReceivedDate	Fecha de recepción del mensaje. En los mensajes enviados el campo contiene Null	Cadena de caracteres
msgElement	Elemento del mensaje procesado.	Cadena de caracteres "Attachment"
msgElementSize	Tamaño del fichero monitorizado.	Numérico
msgElementName	Nombre del fichero monitorizado.	Cadena de caracteres
msgElementHash	MD5 del fichero monitorizado.	Cadena de caracteres
msgExfiltrationFlag	Indica que el fichero ha sido objeto de una operación clasificada como de entrada de datos, fuga o comunicación de datos o ambas.	• INFILTRATION • EXFILTRATION • BOTH
usrRules	Nombre de las reglas introducidas en la consola de Cytomic EDR separadas por el carácter "|" que están monitorizando el fichero.	Cadena de caracteres | Cadena de caracteres | Cadena de caracteres...

Tabla 7.3: Tabla oem.paps.edp.usrrulesmail

Tabla oem.paps.edp.mail

Almacena toda la información de los mensajes de correo que contienen ficheros clasificados como PII, así como las características de los ficheros con información personal que contienen.

Nombre	Descripción	Valores
evendate	Fecha de inserción del evento en el servidor Cytomic Data Watch.	Fecha
serverdate	Fecha del equipo de usuario o servidor cuando se generó el evento.	Fecha
machineName	Nombre del equipo de usuario o servidor.	Cadena de caracteres
machineIP	IP del equipo de usuario o servidor.	Dirección IP
loggeduser	Nombre de usuario que inició una sesión interactiva cuando se registro el evento registrado.	Cadena de caracteres
msgID	Identificador único del mensaje.	Cadena de caracteres

Tabla 7.4: Tabla oem.paps.edp.mail

Nombre	Descripción	Valores
msgTo	Dirección de correo destino del mensaje.	Cadena de caracteres
msgFrom	Dirección de correo origen del mensaje.	Cadena de caracteres
msgSentDate	Fecha de envío del mensaje. En los mensajes recibidos el campo contiene Null.	Fecha
msgSubject	Asunto del mensaje.	Cadena de caracteres
msgReceivedDate	Fecha de recepción del mensaje. En los mensajes enviados el campo contiene Null	Cadena de caracteres
msgElement	Elemento del mensaje procesado.	Cadena de caracteres "Attachment"
msgElementSize	Tamaño del fichero monitorizado.	Numérico
msgElementName	Nombre del fichero monitorizado.	Cadena de caracteres
msgElementHash	MD5 del fichero monitorizado.	Cadena de caracteres
msgExfiltrationFlag	Indica que el fichero ha sido objeto de una operación clasificada como de entrada de datos, fuga o comunicación de datos o ambas.	• INFILTRATION • EXFILTRATION • BOTH
creditCard	Indica si se encontraron o no entidades de tipo Tarjetas de crédito en el fichero PII.	Booleano
bankAccount	Indica si se encontraron o no entidades de tipo Cuenta bancaria en el fichero PII.	Booleano
personalID	Indica si se encontraron o no entidades de tipo Tarjetas de identidad (DNI) en el fichero PII.	Booleano
driveLic	Indica si se encontraron o no entidades de tipo Carnet de conducir en el fichero PII.	Booleano
passPort	Indica si se encontraron o no entidades de tipo Pasaporte en el fichero PII.	Booleano
SSId	Indica si se encontraron o no entidades de tipo Número de la seguridad social en el fichero PII.	Booleano
email	Indica si se encontraron o no entidades de tipo mail en el fichero PII.	Booleano
IP	Indica si se encontraron o no entidades de tipo Dirección IP en el fichero PII.	Booleano
name	Indica si se encontraron o no entidades de tipo Nombre y apellidos en el fichero PII.	Booleano
address	Indica si se encontraron o no entidades de tipo Dirección en el fichero PII.	Booleano
phone	Indica si se encontraron o no entidades de tipo Teléfono en el fichero PII.	Booleano

Tabla 7.4: Tabla oem.paps.edp.mail

Nombre	Descripción	Valores
estimatedNumPII	Número estimado de entidades encontradas.	Numérico

Tabla 7.4: Tabla oem.paps.edp.mail

Capítulo 8

Listado de extensiones

A continuación, se muestra un listado de las extensiones de ficheros donde Cytomic Data Watch busca información personal de los usuarios y clientes de la empresa:

Extensiones soportadas

Nombre de la suite	Producto	Extensiones
Office	Word	• DOC • DOT • DOCX • DOCM • RTF
	Excel	• XLS • XLSM • XLSX • XLSB • CSV
	PowerPoint	• PPT • PPS • PPSX • PPSM • SLDX • SLDM • POTX • PPTM • PPTX • POTM

Tabla 8.1: Ficheros en los que Cytomic Data Watch busca PII

Nombre de la suite	Producto	Extensiones
OpenOffice	Writer	• ODM • ODT • OTT • OXT • STW • SXG • SXW
	Draw	• ODG • OTG • STD
	Math	• ODF • SXM
	Base	• ODB
	Impress	• OTP • ODP • STI • SXI
	Calc	• OTS • ODS • SXC
Texto plano		TXT
Navegadores web	• Internet Explorer • Chrome • Opera • Otros	• HTM • HTML • MHT • OTH
Cliente de correo	• Outlook • Outlook Express	EML
Otros	Adobe Acrobat Reader	PDF
	Extensible Markup Language	XML
	Contribute	STC
	ArcGIS Desktop	SXD

Tabla 8.1: Ficheros en los que Cytomic Data Watch busca PII

Capítulo 9

Listado de procesos

Cytomic EDR monitoriza todos los procesos que se ejecutan en los puestos de usuario o servidores en busca de operaciones sobre ficheros con información personal. Esta monitorización es siempre representada por Cytomic Data Watch mediante las aplicaciones de Advanced Visualization Tool y la Tabla de conocimiento PII. Sin embargo, a la hora de valorar si una operación forma parte de un incidente catalogado como comunicación no autorizada de datos personales (Exfiltration) o recepción de los mismos (Infiltration), los algoritmos de Machine Learning consideran el subconjunto de procesos mostrado a continuación:

Procesos de extracción de datos

Tipo	Nombre del programa	Nombre del binario
Navegador web	Microsoft Edge	• browser_broker.exe • microsoftedge.exe • microsoftedgecp.exe
	Google Chrome	chrome.exe
	Comodo Dragon	dragon.exe
	Mozilla Firefox	firefox.exe
	Microsoft Internet Explorer	• iexplore.exe • msimn.exe
	Opera	opera.exe
	Yandex	yandex.exe
	Mozilla Prism	zdclient.exe
	Torch	torch.exe
	Apple Safari	safari.exe

Tabla 9.1: procesos monitorizados en busca de operaciones de extracción de datos, nombre comercial del programa y tipo de software

Tipo	Nombre del programa	Nombre del binario
Mensajería de correo	Microsoft Outlook	outlook.exe
	Mozilla Thunderbird	thunderbird.exe
	Windows Live Mail	wlmail.exe
	Yahoo Zimbra Desktop	zdesktop.exe
Mensajería de chat	Microsoft Skype	skype.exe
	Facebook Whatsapp	• whatsapp.exe • winuapentry.exe
	Fleep	• fleep.exe • fleep.browsersubprocess.exe
	Pidgin	• pidgin.exe
	Line	line.exe
	Telegram	telegram.exe
	Rocket chat	rocket.chat.exe
Videoconferencia y colaboración	Spark	ciscocollabhost.exe
	Moxtra	moxtra.exe
	Ring Central	rincentral.exe
	Samepage	samepage.exe
	Yammer	yammer.exe
	Microsoft Teams	teams.exe
	Microsoft Lync	lync.exe
Almacenamiento de ficheros	Dropbox	dropbox.exe
Reproductor de medios	Line media player	linemediaplayer.exe
Transferencia de ficheros	PuTTY SFTP	psftp.exe
	WinSCP	winscp.exe
Administración de Windows	Putty	• pscp.exe • putty.exe
	Netcat	nc.exe
	Microsoft BITSAdmin Tool	bitsadmin.exe
Intérprete / compilador	Microsoft Scripting Host	mshta.exe
	Java	• java.exe • javaw.exe
Base de datos	Firebird SQL Server	fbserver.exe

Tabla 9.1: procesos monitorizados en busca de operaciones de extracción de datos, nombre comercial del programa y tipo de software

Tipo	Nombre del programa	Nombre del binario
Varios	Varios	• browser.exe • stride.exe • wechatstore.exe

Tabla 9.1: procesos monitorizados en busca de operaciones de extracción de datos, nombre comercial del programa y tipo de software

Procesos de infiltración de datos

Tipo	Nombre del programa	Nombre del binario
Navegador web	Microsoft Edge	• browser_broker.exe • microsoftedge.exe • microsoftedgecp.exe
	Google Chrome	chrome.exe
	Comodo Dragon	dragon.exe
	Mozilla Firefox	firefox.exe
	Microsoft Internet Explorer	• iexplore.exe • msimn.exe
	Opera	opera.exe
	Yandex	yandex.exe
	Mozilla Prism	zdclient.exe
	Torch	torch.exe
	Apple Safari	safari.exe
	Brave	brave.exe
	Vivaldi	vivaldi.exe
Servidores web	Apache HTTP	httpd.exe
Ofimática	Microsoft Excel	excel.exe
	Microsoft PowerPoint	powerpnt.exe
	Microsoft Word	winword.exe
	OpenOffice	• soffice.bin • soffice.exe
Lector de ficheros	Adobe Reader	acrord32.exe
Reproductor de medios	Line media player	linemediaplayer.exe

Tabla 9.2: procesos monitorizados en busca de operaciones de infiltración de datos, nombre comercial del programa y tipo de software

Tipo	Nombre del programa	Nombre del binario
Mensajería de correo	Microsoft Outlook	outlook.exe
	Mozilla Thunderbird	thunderbird.exe
	Windows Live Mail	wlmail.exe
	Yahoo Zimbra Desktop	zdesktop.exe
	Lotus Notes	nlnotes.exe
	Remark	mark5.exe
Mensajería de chat	Microsoft Skype	skype.exe
	Facebook Whatsapp	• whatsapp.exe • winuapentry.exe
	Telegram	telegram.exe
	Pidgin	pidgin.exe
	Line	line.exe
	Fleep	• fleep.exe • fleep.browsersubprocess.exe
	Pidgin	pidgin.exe
Videoconferencia y herramientas de colaboración	Spark	ciscocollabhost.exe
	Microsoft Lync	lync.exe
	Moxtra	moxtra.exe
	Ring Central	rincentral.exe
	Samepage	samepage.exe
	Slack	slack.exe
	Microsoft Teams	teams.exe
	Yammer	yammer.exe
Transferencia de ficheros	PuTTY SFTP	psftp.exe
	WinSCP	winscp.exe
	Internet Download Manager	idman.exe
	IceCast	icecast2.exe
	uTorrent	utorrent.exe

Tabla 9.2: procesos monitorizados en busca de operaciones de infiltración de datos, nombre comercial del programa y tipo de software

Tipo	Nombre del programa	Nombre del binario
Administración de Windows	Putty	• pscp.exe • putty.exe
	Netcat	nc.exe
	Microsoft BITSAdmin Tool	bitsadmin.exe
Componente de Windows	Linea de comandos	conhost.exe
	Runtime Broker	runtimeBroker.exe
	WMI linea de comandos	wmic.exe
Intérprete / compilador	Microsoft Scripting Host	mshta.exe
	Java	• java.exe • javaw.exe
Base de datos	Firebird SQL Server	fbserver.exe
Seguridad	Picus Security	picus.agent.service.exe
Varios	Varios	• browser.exe • bvs.exe • stride.exe • wechatstore.exe
	David InfoCenter	dvwin32.exe
	Ezvit Intellectservice	ezvit.exe

Tabla 9.2: procesos monitorizados en busca de operaciones de infiltración de datos, nombre comercial del programa y tipo de software

Capítulo 10

Requisitos de hardware, software y red

Cytomic Data Watch es un servicio cloud y como tal, Cytomic mantiene en sus instalaciones toda la infraestructura necesaria para prestar el servicio a sus clientes sin necesidad de desplegar software o hardware adicional en las redes de las organizaciones. No obstante, es necesario cumplir con ciertos requisitos mínimos para garantizar un correcto funcionamiento del producto.

CONTENIDO DEL CAPÍTULO

Requisitos de acceso a la consola de administración

Para acceder a la consola Web es necesario cumplir con el siguiente listado de requisitos:

- Un navegador compatible certificado (otros navegadores pueden funcionar).
  - Mozilla Firefox
  - Google Chrome

Los navegadores no listados pueden funcionar, pero es posible que no se soporten todas las versiones. Por esta razón se recomienda el uso de los navegadores indicados anteriormente.

- Conexión a Internet y comunicación por el puerto 443.
- Resolución mínima 1280x1024, recomendada 1920x1080.

Requisitos hardware

- Equipo con capacidad de proceso adecuada para la generación de los gráficos y listados en tiempo real.

- Ancho de banda suficiente para poder mostrar en tiempo real toda la información recogida en los equipos de los usuarios.