CYTOMIC

Guía de administración Cytomic Insights_

Aviso legal.

Marcas registradas.

Información de contacto.

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

Versión: 1.02.00-03

Autor: Cytomic

Fecha: 01/08/2021

Acerca de la Guía de administración

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

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

Guía de administración de Cytomic EDR y Cytomic EPDR

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

https://info.cytomicmodel.com/resources/guides/EDR/latest/es/EDR-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.pandasecurity.com/es/support/advanced-reporting-tool.htm

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/feedbackInsightsGuideES

Tabla de contenidos

Parte 3: Información adicional

Parte 1

Introducción a Cytomic Insights

Capítulo 1

Prólogo

Esta guía contiene información y los procedimientos de uso necesarios para obtener el máximo beneficio del servicio Cytomic Insights.

CONTENIDO DEL CAPÍTULO

¿A quién está dirigida esta guía?

Esta documentación está dirigida al personal técnico del departamento de IT de las empresas que tengan contratado el servicio Cytomic Insights para los productos Cytomic EDR y Cytomic EPDR.

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 Insights.

Todos los procedimientos e indicaciones en esa guía técnica se aplican indistintamente tanto si el cliente tiene contratado el producto Cytomic EDR como Cytomic EPDR. 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 Insights.

Consulta en otro capítulo o punto del manual.

Capítulo 2

Introducción al servicio

Cytomic Insights es un servicio de explotación avanzado y en tiempo real de todo el conocimiento generado por los productos Cytomic EDR y Cytomic EPDR.

Su principal objetivo es facilitar el descubrimiento de amenazas desconocidas, ataques dirigidos específicamente diseñados para extraer información confidencial de las empresas y del malware avanzado de tipo APT (Advanced Persistent Threats). Para ello, es capaz de representar los datos de actividad de los procesos ejecutados por los usuarios, poniendo un énfasis especial en los eventos relacionados con la seguridad y la extracción de información del parque informático.

Adicionalmente determina el uso que le dan a sus equipos los usuarios de la red, tanto a nivel de consumo de ancho de banda por aplicación, como de la utilización de las aplicaciones instaladas. Además detecta aquellas aplicaciones que presentan vulnerabilidades aprovechables por el malware de nueva generación.

Cytomic Insights implementa herramientas para realizar búsquedas avanzadas sobre el repositorio de información y desarrollar nuevas configuraciones y representaciones de los datos almacenados. Estas representaciones son flexibles y tienen como requerimiento adaptarse a las necesidades del personal técnico a la hora de generar inteligencia de seguridad para descubrir procesos maliciosos que actúan "por debajo del radar".

Con todos los recursos implementados, Cytomic Insights es la herramienta más completa para determinar de forma precisa el estado de la seguridad de la red.

CONTENIDO DEL CAPÍTULO

Principales beneficios

Los principales beneficios de Cytomic Insights se derivan de la visualización de la actividad de los procesos en la red para generar de forma automática inteligencia de seguridad.

- Muestra la evolución de todo tipo de malware detectado en la red del cliente, indicando si ha sido ejecutado o no, para facilitar los procesos de resolución y adaptación de las políticas de seguridad.
- Lista las acciones ejecutadas por cada proceso, ya sea goodware, malware o desconocido, con el objetivo de recopilar indicios que permitan obtener conclusiones acerca de su potencial peligrosidad.
- Visualiza los accesos a la información confidencial de la empresa para prevenir su extracción o robo.
- Localiza todos los programas ejecutados, y especialmente aquellos instalados en los equipos de los usuarios y que contengan vulnerabilidades conocidas, para ayudar en el diseño de un plan de actualización de software.
- Dimensiona los recursos de red disponibles mostrando las aplicaciones y usuarios que más ancho de banda demandan en la red.

Características del servicio Cytomic Insights

Cytomic Insights transforma la información en bruto recogida por Cytomic EDR en inteligencia de seguridad con diferentes niveles de detalle. Para ello se implementan un conjunto de herramientas y recursos:

- Una amplia variedad de widgets gráficos configurables que facilitan la visualización de los datos de actividad recogidos.
- 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.
- Tablas de conocimiento con información completa de las acciones desencadenadas por todos los procesos ejecutados en los equipos de los usuarios.
- Herramientas avanzadas para la búsqueda y procesamiento de la información almacenada: filtrado, agrupación, operaciones avanzadas con datos, generación de nuevos widgets con información, etc.

Información acumulada

El servicio Cytomic Insights almacena la información suministrada en tiempo real por los equipos de la red que tienen instalado el producto Cytomic EDR.

La mayor parte de la información recogida se genera como resultado de la monitorización activa de los procesos ejecutados en los equipos del cliente. Esta monitorización la realiza Cytomic EDR, y el servicio Cytomic Insights almacena la información en distintas tablas según su tipo, generando al mismo tiempo representaciones gráficas de los datos para facilitar su interpretación.

Algunos tipos de eventos registrados por Cytomic EDR y mostrados por Cytomic Insights son los siguientes:

- Instalación y desinstalación de drivers en el sistema operativo.
- Instalación y modificación de hooks de teclado, ratón y otros dispositivos.
- Modificación del registro en los equipos Windows de la red.
- Modificación de ficheros de sistema (HOSTS).
- Registro del volumen de datos enviado y recibido por cada proceso a través de la red.
- Registro de las comunicaciones establecidas con equipos remotos.
- Software instalado en los equipos con vulnerabilidades conocidas.
- Ejecución y finalización de procesos.
- Carga de librerías.
- Manipulación del sistema de ficheros.
- Apertura de línea de comandos.

Los eventos registrados pueden estar relacionados con la ejecución de código malicioso todavía desconocido, de manera que Cytomic Insights se convierte en una herramienta fundamental para supervisar el funcionamiento de los procesos en busca de comportamientos sospechosos.

Componentes de la arquitectura

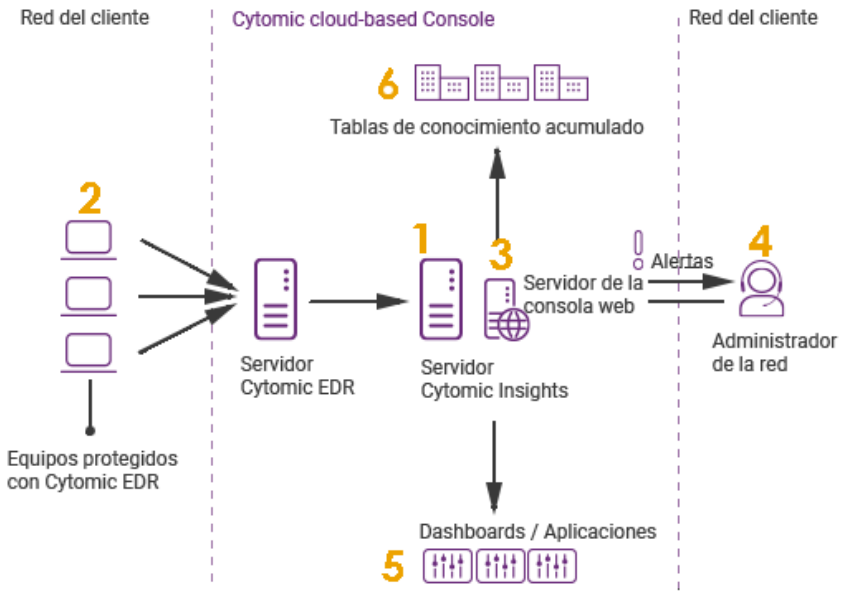

Figura 2.1: arquitectura general de Cytomic Insights

Cytomic Insights está formado por los elementos mostrados a continuación:

- Servidor Cytomic Insights. **(1)**
- Equipos protegidos por Cytomic EDR o Cytomic EPDR. **(2)**
- Servidor de la consola web de administración. **(3)**
- Equipo del administrador de la red para la gestión del servicio. **(4)**
- Aplicaciones / Dashboards. **(5)**
- Tablas de conocimiento acumulado. **(6)**

Infraestructura alojada en la nube

Toda la infraestructura directamente implicada con el servicio (Servidor Cytomic Insights, Servidor Cytomic EDR, Servidor de la consola web) está desplegada en la Nube de Cytomic, ofreciendo los beneficios mostrados a continuación:

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

Al no requerir la instalación de servidores en las oficinas del cliente, todos los costes relacionados con la adquisición de hardware y su mantenimiento (gestión de las garantías, averías y almacenamiento de componentes de recambio, etc.) desaparecen. 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 todos los equipos de la red del cliente, eliminando los problemas de acceso que aparecen en empresas con estructuras distribuidas en varios centros de trabajo.

Por esta razón no son necesarios despliegues específicos de telecomunicaciones como VPNs o configuraciones específicas 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 Insights

Se trata de una granja de servidores configurados en alta disponibilidad, que recoge todos los eventos enviados por los agentes Cytomic EDR instalados en los equipos de los usuarios.

El envío y recolección de datos es continuo y en tiempo real. El servidor almacena todos los datos en tablas de acceso rápido por el administrador, a la vez que genera gráficas de fácil interpretación y alertas configurables que previenen de situaciones potencialmente comprometedoras.

Equipos protegidos por Cytomic EDR y Servidor Cytomic EDR

Los equipos envían de forma continuada las acciones que ejecutan los procesos de usuario al servidor Cytomic EDR, alojado en la nube. Este servidor genera inteligencia de seguridad de forma automática mediante tecnologías Machine Learning trabajando sobre repositorios Big Data. La inteligencia de seguridad es añadida a los eventos recogidos de los equipos protegidos por Cytomic EDR y son enviados directamente al servidor Cytomic Insights Este esquema de funcionamiento presenta las siguientes ventajas:

- La información que recibe el servidor Cytomic Insights ya ha sido previamente procesada por el Servidor Cytomic EDR, de forma que contiene la inteligencia de seguridad que ayudará al administrador en la localización de problemas ocasionados por el 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 de Cytomic Insights.

Servidor Web de la consola de administración y equipo del administrador de la red

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

*Para más información consulta el capítulo "**La consola web**" en la página **19**.*

Aplicaciones / Paneles de control

La información más relevante para el equipo técnico de IT se muestra mediante tres aplicaciones accesibles desde la consola web de administración:

- **Security Incidents**: visualiza la evolución de la actividad del malware en la empresa.
- **Application Control**: muestra información sobre las aplicaciones instaladas en el parque.
- **Data Access Control**: muestra la información accedida por los usuarios y consumos de ancho de banda.

Todas las aplicaciones son interactivas y profundizan en la información haciendo clic en los diversos elementos disponibles.

*Para más información sobre las aplicaciones consulta el capítulo "**Introducción a las aplicaciones**" en la página **25**.*

Tablas de conocimiento acumulado

El sistema almacena los datos recibidos por el servidor de Cytomic EDR en tablas de fácil acceso para el departamento de IT.

Las tablas son una fuente de datos para la generación de gráficas y de operaciones de filtrado y transformación (agrupaciones, ordenación de la información, búsquedas, etc.).

*Consulta el "**Tablas de conocimiento**" en la página **77** para más información sobre las tablas de conocimiento acumulado y el significado de los campos.*

Otros servicios adicionales

Con la contratación del servicio Cytomic SIEMConnect, el administrador de la red podrá incorporar a la solución SIEM de su elección toda la información generada por la actividad de los procesos ejecutados en los equipos del parque informático. Además, esta información se entrega enriquecida con la inteligencia de seguridad desarrollada por Cytomic.

La información tratada por Cytomic Insights y documentada en "**Tablas de conocimiento**" en la página **77**, es un subconjunto del volumen de datos completo que Cytomic pone a disposición del cliente para su explotación a través del servicio Cytomic SIEMConnect.

Para más información sobre Cytomic SIEMConnect y sobre los datos enviados al servidor del cliente, consulta la **Guía del administrador de Cytomic SIEMConnect**.

Perfil de usuario de Cytomic Insights

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

- Monitorización de la actividad de los procesos ejecutados en equipos de usuarios.
- Monitorización del estado de la seguridad general de la red.
- Desarrollo de políticas para la protección de los datos e información confidencial de la empresa.
- Generación de información para procesos de análisis forense en casos de infección por malware.
- Generación de información complementaria para auditoria de equipos.
- Dimensionamiento del ancho de banda necesario para desarrollar la actividad empresarial.
- Generación de información complementaria en auditorias de seguridad.

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. Al tratarse de un servicio Web centralizado, posee una serie de características que influirán de forma positiva en la forma de trabajo del departamento de IT:

- **Única herramienta para la explotación de la información de seguridad**.

Con la consola Web es posible monitorizar el estado de la seguridad de la red y disponer de herramientas preconfiguradas para la representación de toda la información recogida, con el objetivo de facilitar su interpretación.

Todas las funcionalidades se ofrecen 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 la instalación ni mantenimiento de 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 obtener conclusiones de forma más rápida.

CONTENIDO DEL CAPÍTULO

Requisitos de Web Cytomic Insights

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 generar 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 Cytomic Insights

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

Para acceder al entorno Cytomic Insights sigue los pasos mostrados a continuación:

- Haz clic en el menú superior **Estado**.
- En la parte inferior del panel lateral, haz clic en la opción **Advanced Visualization Tool**.

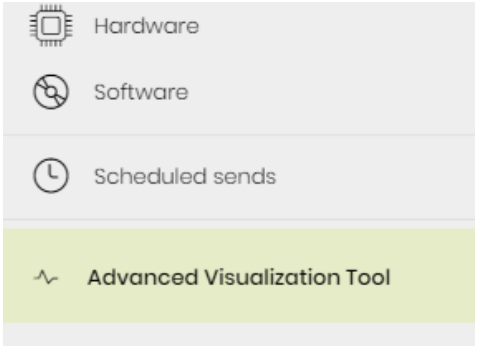

Figura 3.1: acceso a la consola de Cytomic Insights

Estructura de la consola Cytomic Insights

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

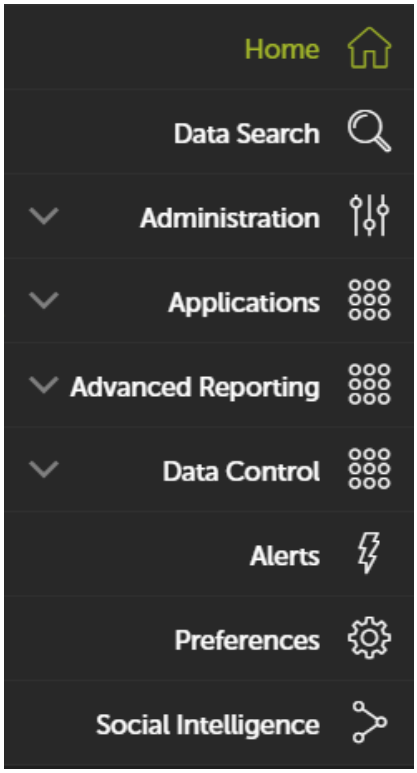

Figura 3.2: menú lateral de la consola Cytomic Insights

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

Accede 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**" en la página **77** para más información acerca de sus campos.*

Figura 3.3: acceso directo a la tabla de conocimiento

Administración 

Configura nuevas alertas.

> *Para más información acerca del funcionamiento de las alertas preconfiguradas consulta el apartado "**Alertas**" en la página **59**. Para más información sobre cómo crear y gestionar alertas nuevas consulta el apartado "**Creación de alertas**" en la página **61**.*

Aplicaciones 

Desplegable con las aplicaciones disponibles para el producto Cytomic Insights.

> *Para más información consulta el capítulo "**Aplicaciones configuradas**" en la página **39***

Alertas 

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

Preferencias 

En esta sección se configuran las preferencias para el usuario que inició la sesión y para todos los usuarios que accedan al servicio.

Salir 

Cierra la sesión de la consola Cytomic Insights y muestra la pantalla de login IDP (Identity Provider).

Parte 2

Recursos de Cytomic Insights

Capítulo 4: Introducción a las aplicaciones

Capítulo 5: Aplicaciones configuradas

Capítulo 6: Alertas

Capítulo 4

Introducción a las aplicaciones

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

Los tres dashboards incluidos en la consola Web de administración son:

- Security Incidents.
- Application Control.
- Data Access Control.

Todos los dashboards están organizados siguiendo un esquema común para facilitar su interpretación, detallado más adelante en el apartado "**Recursos y elementos comunes de los dashboards**".

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 "**Creación de alertas**" en la página 61.*

CONTENIDO DEL CAPÍTULO

Acceso a las aplicaciones y a las alertas

Acceso a los dashboards / aplicaciones:

El acceso a los dashboards se realiza desde el menú lateral, sección **Aplicaciones**.

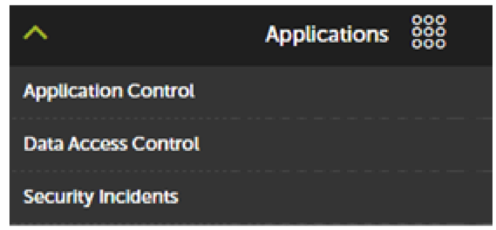

Figura 4.1: menú desplegable Aplicaciones

Acceso a las alertas

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

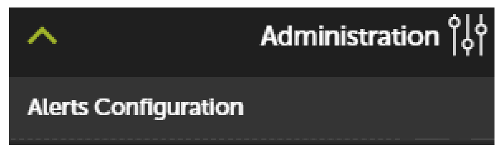

Figura 4.2: entrada del menú Administración para la configuración de alertas existentes

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 para definir el rango de los datos mostrados en pantalla:

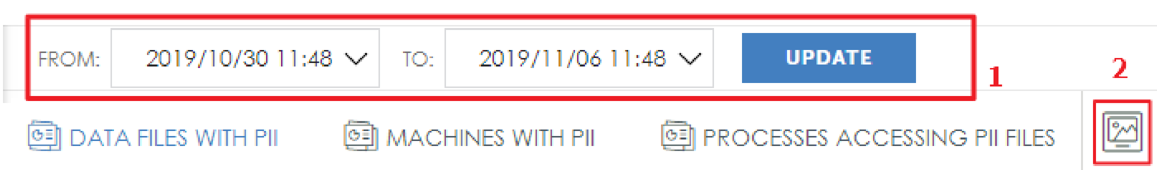

Figura 4.3: controles para configurar los rangos a mostrar

- **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

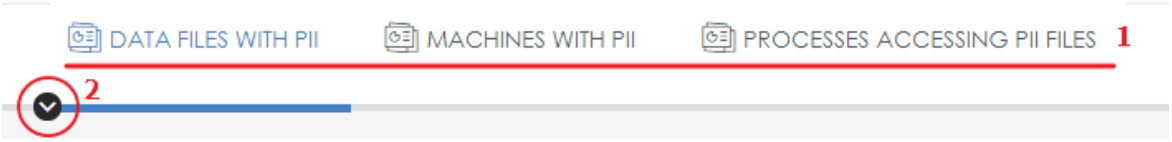

Figura 4.4: ejemplo de pestañas

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 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 te llevará 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 4.5: acceso a las secciones de una pestaña

Widgets

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

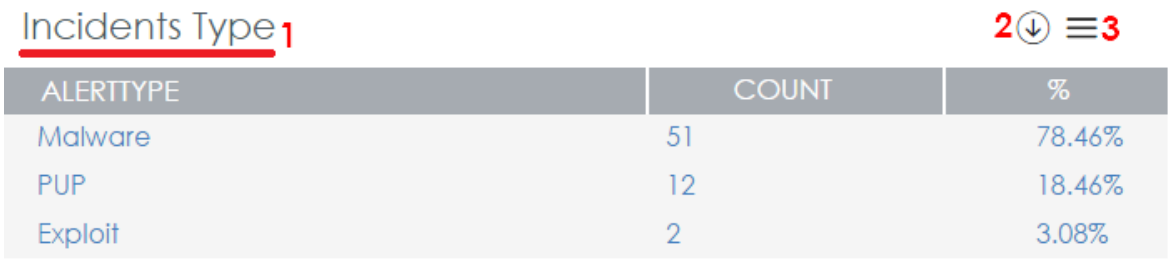

Figura 4.6: ejemplo de widget

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:
  - **Capturar Gráfico**: 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.*

  - Descargar Datos: 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.
  - Ir a la consulta: muestra la tabla de conocimiento que le sirve de fuente de datos al widget, junto con la configuración de filtros, agrupaciones y operaciones aplicadas.

> *En el menú **Ir a la consulta** se visualiza 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.*

- Zoom: amplia el widget a pantalla completa en el navegador.

Herramientas de búsqueda

En algunos widgets de tipo tabla se incorpora la opción de búsqueda para realizar el seguimiento de contenidos en las tablas.

Los datos en las tablas muestran hasta un máximo de 1.000 registros, ordenados de mayor a menor

La herramienta dispone de función de autocompletar, como se puede ver en el ejemplo de esta tabla, donde se buscan los datos correspondientes a "Malware":

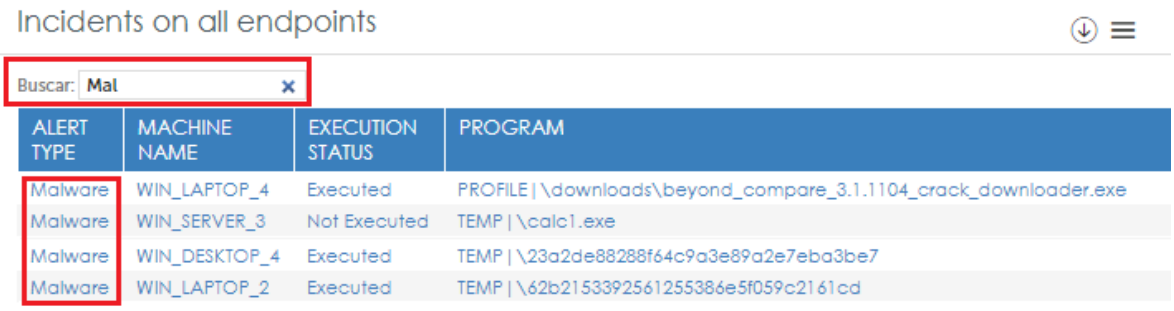

Figura 4.7: tabla de los datos correspondientes a "Malware"

O en esta otra, donde el objetivo de la búsqueda son los programas situados bajo el directorio TEMP:

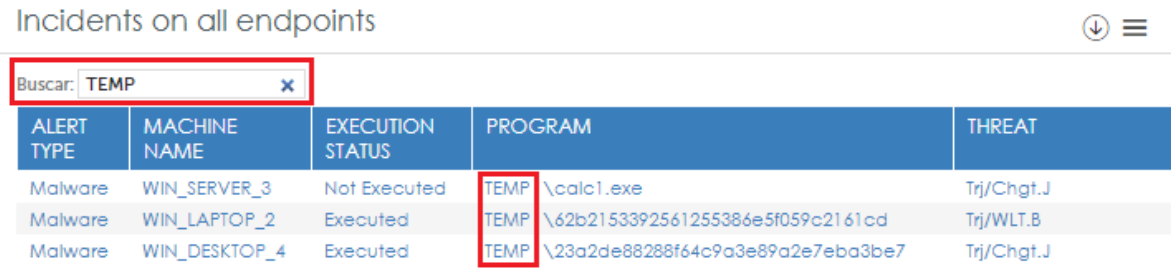

Figura 4.8: programas en el directorio TEMP

> *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.*

Tablas y Gráficos

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.

Gráficos Calendario

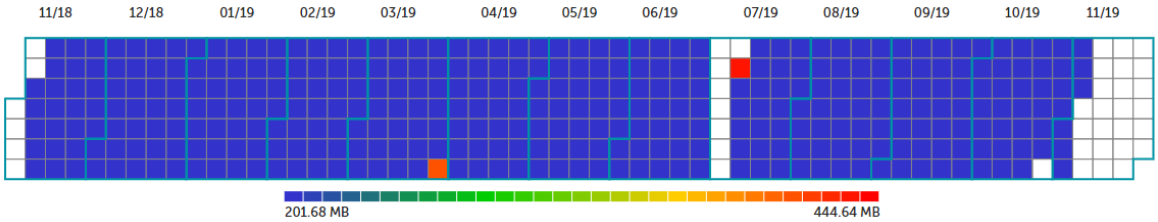

Figura 4.9: gráfica de tipo calendario

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. Con la gama de color utilizada (verde-rojo) se comparan 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.

Gráfica de barras apiladas

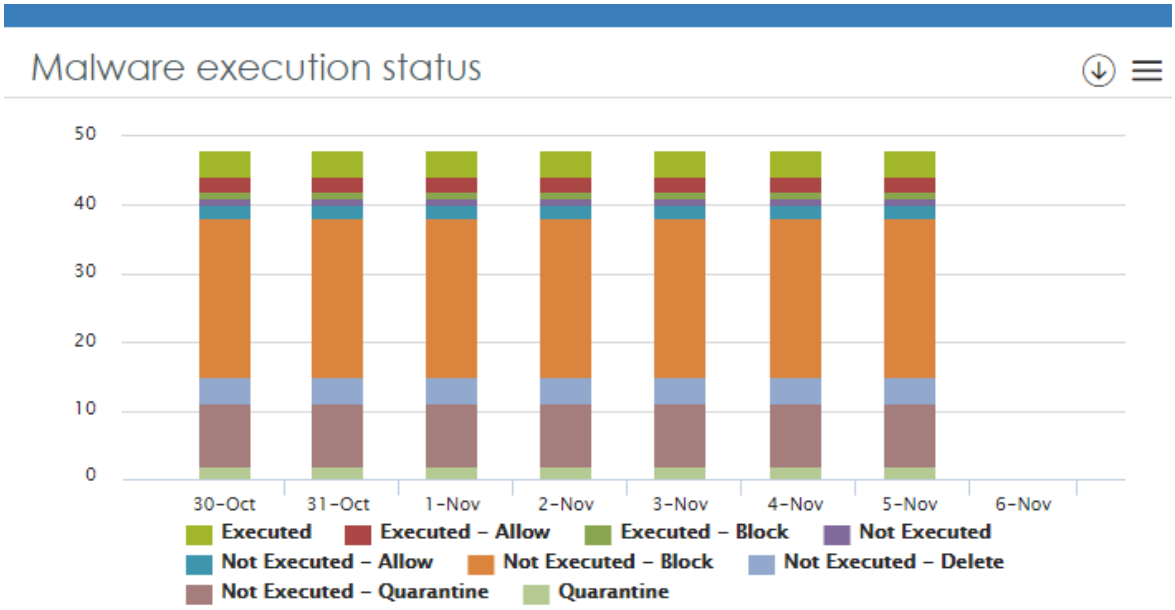

Figura 4.10: gráfica de barras

Los gráficos de barras apilados muestran en un mismo gráfico la evolución de varias series, representadas por distintos colores en la leyenda situada en la parte inferior. Las distintas series se apilan dentro de cada fecha representada para mostrar el total de los datos en esa fecha y cómo se distribuyen según su tipo.

Al pasar el ratón por encima de las series se muestra un tooltip que indica la fecha y el valor de la serie en ese momento.

Gráfico de mapa del mundo

Este tipo de gráfico representa en un mapa los valores recogidos en la tabla de conocimiento, siempre que ésta incluya campos de tipo Latitud y Longitud o datos que permitan inferir coordenadas.

El color y el tamaño de los puntos marcados en el mapa (verde - naranja - rojo) indican de forma relativa el número de ocurrencias que se han registrado en el intervalo de tiempo fijado.

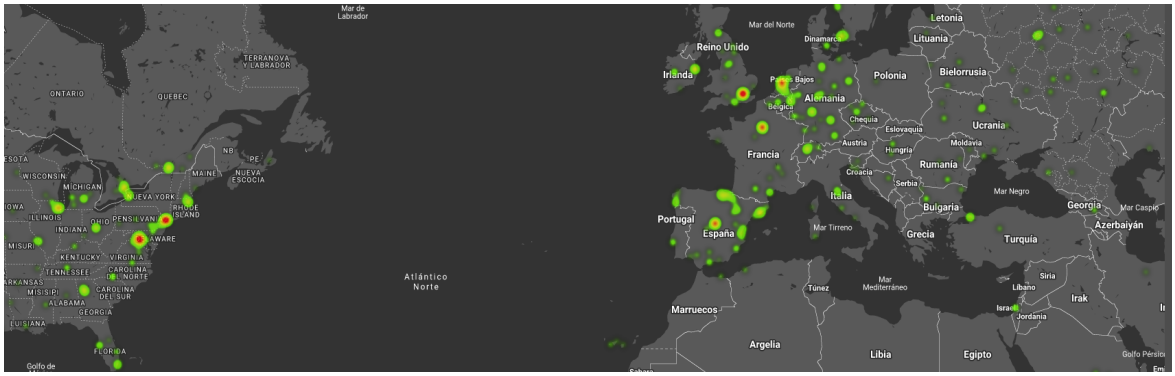

Figura 4.11: Gráfica de tipo mapa del mundo

Gráfico Voronoi

Figura 4.12: gráfica de polígonos de Thiessen o 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 navegan a través de los diferentes niveles de agrupaciones de datos.

Al hacer doble clic con el botón izquierdo del ratón en una agrupación de datos se accede al nivel inferior. Si una vez allí se hace doble clic con el botón derecho del ratón, se regresa a la agrupación del nivel anterior.

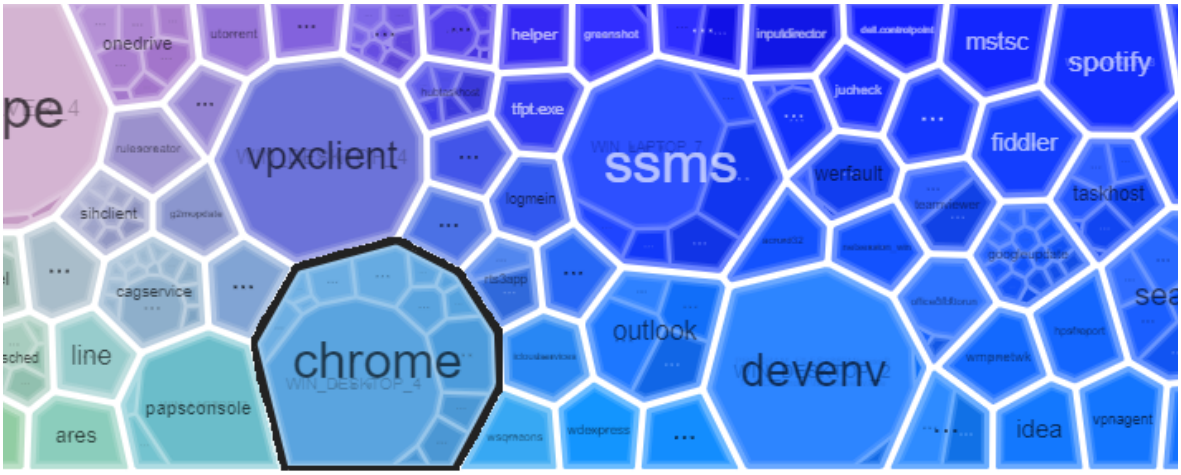

Figura 4.13: zoom in mediante doble clic en un polígono de una gráfica Voronoi

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.

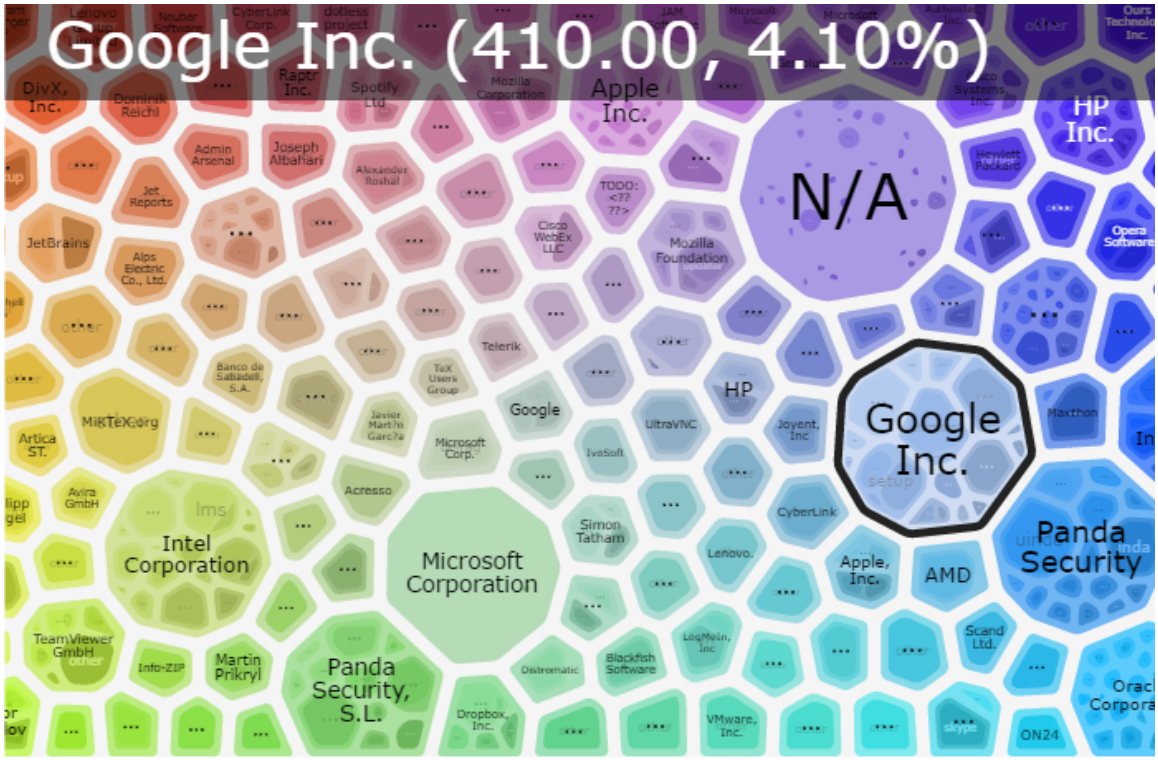

Figura 4.14: información mostrada en los polígonos

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

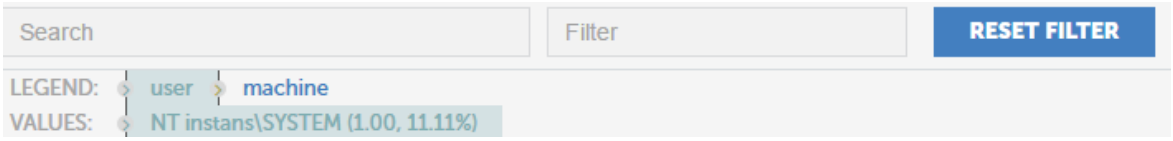

Figura 4.15: controles para configurar los datos mostrados en una gráfica Voronoi

- **Buscar**: 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. Con doble clic del botón derecho del ratón se elimina la búsqueda.
- **Filtro**: muestra solo los polígonos que contienen agrupaciones coincidentes con el filtro establecido.
- **Reiniciar Filtro**: limpia el filtro aplicado. No deshace las búsquedas. Con doble clic del botón derecho del ratón se elimina el filtro.
- **Leyenda**: indica los campos de la tabla de conocimiento que son utilizados para agrupar la información mostrada. 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.
- **Valores**: en combinación con los campos mostrados en el control Legend, indica el valor que toma un determinado campo. Al seleccionar un polígono, bien utilizando la herramienta de búsqueda, bien haciendo doble clic en el mismo, el campo Values tomará el valor de la búsqueda realizada o del polígono seleccionado.

La navegación por niveles se realiza haciendo doble clic con el botón de la izquierda en un polígono del gráfico Voronoi o mediante la herramienta de búsqueda. El campo resaltado en **Leyenda** tomará el valor el polígono seleccionado, mostrando en el Voronoi el siguiente nivel de agrupación indicado en **Leyenda**.

- **Gráfica Voronoi de ejemplo**

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

Según **Leyenda** 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.

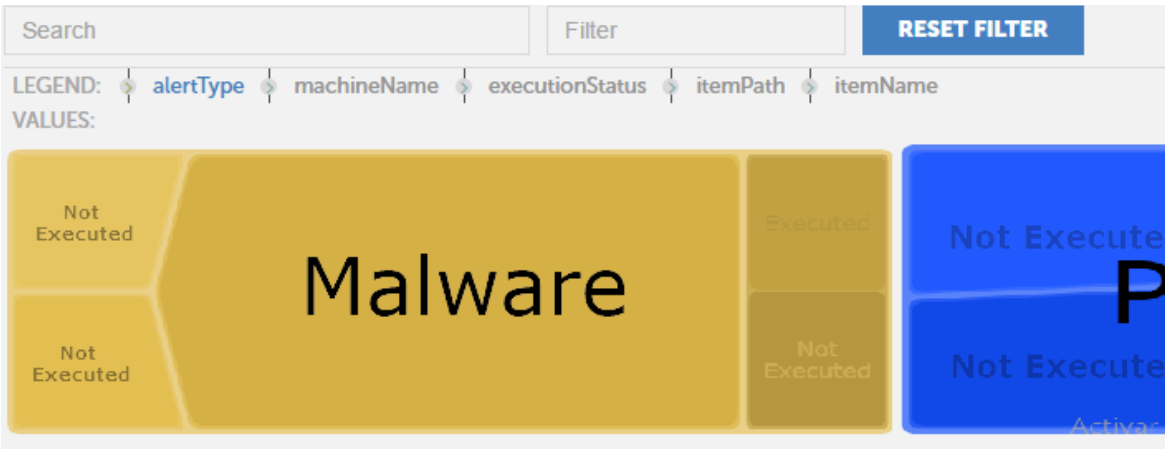

Figura 4.16: ejemplo de la primera capa o agrupación en una gráfica Voronoi

Inicialmente el gráfico muestra el Nivel 1: los datos agrupados por el campo **AlertType**, el primer campo **Leyenda**, 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:

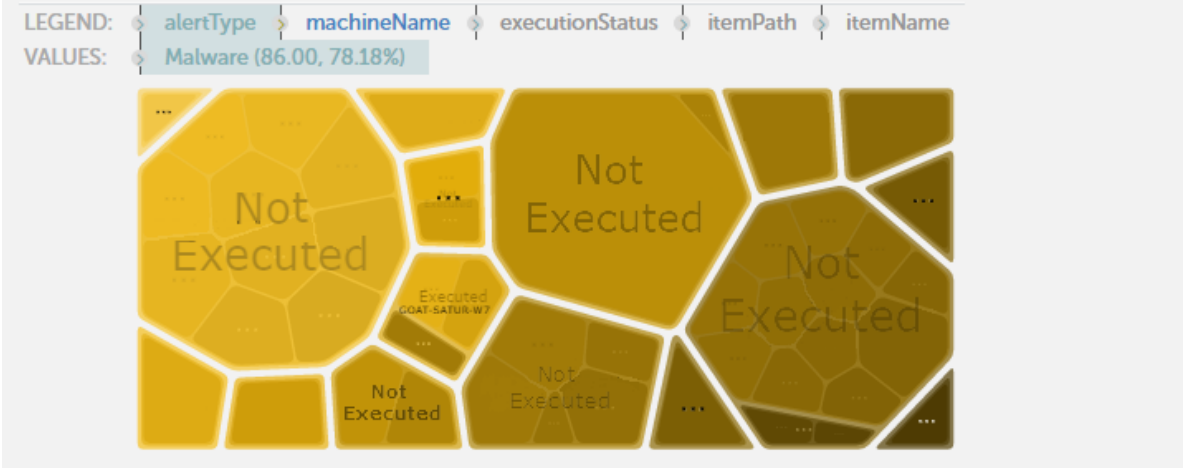

Figura 4.17: ejemplo de la segunda capa de agrupación en una gráfica Voronoi

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 **Leyenda.**

Por ejemplo, para determinar en primer lugar cuales son los equipos que han ejecutado algún tipo de malware, el nombre de la amenaza, y los equipos donde se ejecutó, esto configura el orden de agrupación como se muestra a continuación:

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

Figura 4.18: 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.

Alertas preconfiguradas

Todas las aplicaciones integradas tienen implementadas alertas preconfiguradas para que el administrador conozca en tiempo real las condiciones anómalas que se producen en la red.

*Consulta "**Alertas**" en la página **59** para obtener una descripción de las alertas preconfiguradas*

Acceso a las alertas y modificación de la frecuencia de envío

Las alertas preconfiguradas son accesibles desde el menú lateral **Administración**, **Configuración de alertas**.

El administrador deberá de completar la configuración de las alertas para establecer los parámetros mostrados a continuación:

- **Suscripción a alertas**: accede a la pantalla de **Suscripción de alertas** (menú lateral **Administración**,

Configuración de alertas, **Pestaña Suscripción a alertas**) para activar o desactivar las alertas apropiadas. Por defecto todas las alertas preconfiguradas se entregan activadas.

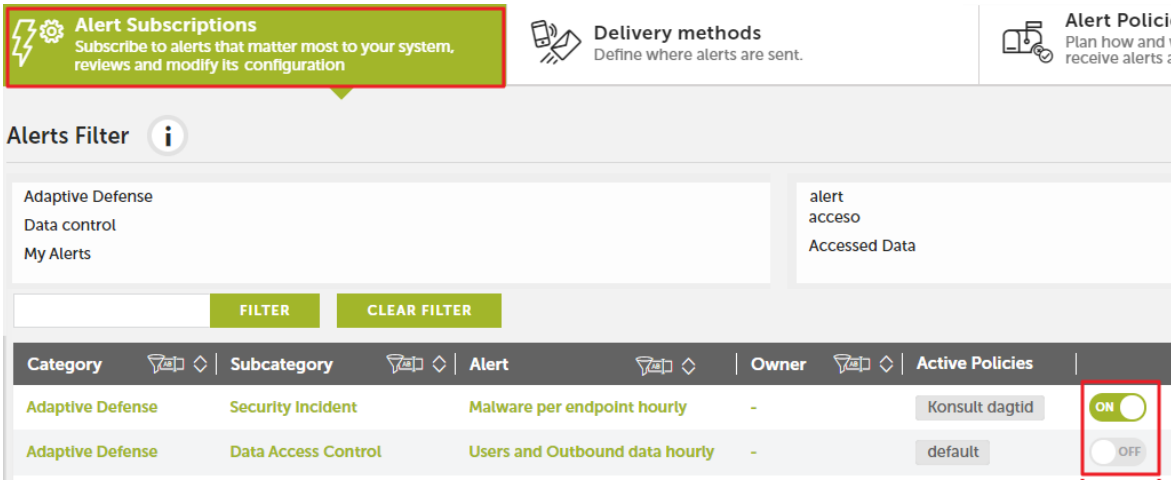

Figura 4.19: pantalla de suscripción de alertas

- **Frecuencia de recepción de las alertas**: el administrador de la red necesitará crear postfiltros (menú lateral **Alertas**, pestaña **Postfiltros**) y políticas antiflooding (menú lateral **Administración**, **Configuración de alertas**, pestaña **Política de alertas**, pestaña **Política antiflooding**) explicadas en el capítulo "**Alertas**" en la página **59** para ajustar la frecuencia de generación de alertas a las necesidades del administrador.
- **Métodos de entrega de las alertas**: el administrador deberá de establecer y configurar los métodos de entrega de las alertas (Email, Json u otros) que se ajusten a la infraestructura ya instalada en la empresa. Para más información consulta el apartado "**Creación de configuraciones de entrega**" en la página **67**. Para acceder a la configuración de entrega haz clic en el menú lateral **Administración**, **Configuración de alertas**, pestaña **Configuración de entrega**.

Cytomic Insights generará todas las alertas creadas sin ningún tipo de límite. Hasta que no se hayan completado los pasos indicados arriba, las alertas solo serán mostradas en la consola web de administración, en el menú lateral Alertas.

Generación de nuevas gráficas basadas en los widgets suministrados

Al hacer clic en el icono ☰ de cada widget y seleccionando la opción **Go to query** se abrirá 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

Una vez 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 la sentencia 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

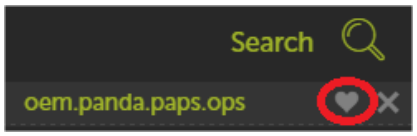

Figura 4.20: Icono para establecer una alerta como favorita

Una vez modificada la sentencia SQL y comprobado que los datos que genera son los correctos, se puede salvar para su acceso posterior, marcándola como **Favorita**. Para ello, al abrir una tabla de conocimiento habrá aparecido 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. Haciendo clic en este icono, la sentencia SQL se marcará como **Favorita** y aparecerá en el listado de consultas favoritas.

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

Capítulo 5

Aplicaciones configuradas

En este capítulo se detalla el funcionamiento de las tres aplicaciones suministradas en Cytomic Insights, tanto en lo relativo a la interpretación de las gráficas y tablas como del funcionamiento de las alertas predefinidas.

CONTENIDO DEL CAPÍTULO

Establecimiento del intervalo de los datos mostrados

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

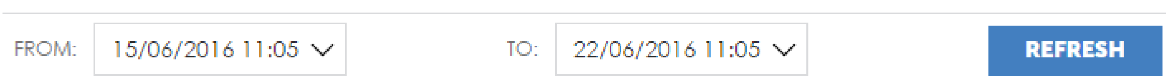

Figura 5.1: herramienta para establecer el rango de datos a mostrar

El administrador deberá de especificar rangos de fechas apropiados para visualizar el estado de la seguridad de la red administrada.

Rangos de fechas amplios

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

- **Ejecución de amenazas desconocidas y aplicaciones vulnerables**

Si el administrador de la red configuró un modo de protección avanzada en Cytomic EDR distinto de **Lock** (**Audit** o **Hardening**) existe la posibilidad de que un usuario ejecute un malware desconocido.

Esta amenaza permanecerá en funcionamiento en el equipo del usuario hasta su resolución; por esta razón, la ejecución de una amenaza desconocida se extiende a lo largo del tiempo, si el rango de fechas seleccionado en Cytomic Insights abarca el periodo de ejecución, se mostrará en las gráficas como malware ejecutado, aunque actualmente la situación ya haya sido resuelta con éxito.

- **Bloqueo de amenazas conocidas**

Para los casos de intento de ejecución de malware conocido (bloqueo), las detecciones se producen en un momento puntual en el tiempo. Si el intervalo de fechas seleccionado por el administrador abarca ese momento se mostrarán los datos de la detección.

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.

- **Ejecución de amenazas desconocidas y aplicaciones vulnerables**

Si se ha producido en el pasado una ejecución de malware desconocido y no se han aplicado todavía los procedimientos de resolución, el malware se mostrará en las gráficas como en ejecución. De esta manera el administrador determina rápidamente si tiene pendiente aplicar algún procedimiento de resolución.

- **Bloqueo de amenazas conocidas**

Seleccionando como rangos de fechas el día actual, solo se mostrarán los intentos de infección de amenazas conocidas en el día seleccionado.

Alertas asociadas

Para acceder a las alertas asociadas a las aplicaciones accede desde el panel lateral a la pestaña Administración y haz clic en el menú Configuración de alertas.

Para configurar una alerta asociada en el cuadro de la izquierda selecciona **Adaptive Defense** y en el de la derecha una de las aplicaciones correspondientes (**Application Control**, **Data Access Control** o **Security Incidents**). En el listado inferior aparecerán los diferentes tipos de alertas disponibles:

Las alertas de la aplicación **Security Incidents** informan al administrador de los eventos relacionados con la detección de malware en la red.

Las alertas de la aplicación **Application Control** informan al administrador de la ejecución de aplicaciones vulnerables y consumo de ancho de banda, como parte de la estrategia proactiva del departamento de IT para preservar el buen funcionamiento de la red.

Las alertas generadas en **Data Access Control** informan al administrador del volumen de datos enviados por los usuarios de la red administrada.

Aplicación Security Incidents

Visualiza la actividad del malware en la red del cliente para poder ajustar las políticas de seguridad implantadas en la compañía. También puede contribuir a generar información de partida para el desarrollo de procesos de análisis forense.

Este dashboard muestra las detecciones realizadas en el parque de equipos y su información relacionada:

- **Información de los equipos afectados:** número de detenciones realizadas, evolución de las detecciones a lo largo del tiempo, etc.
- **Información relativa a las amenazas detectadas:** vector de infección utilizado, equipos afectados, estado de la ejecución del virus, tipo de virus, etc.

El dashboard se divide en dos pestañas: **Key Security Indicators** y **Detailed Information**, explicadas en los apartados siguientes.

Key security Indicators

Presenta de forma general los datos más importantes sobre la actividad del malware en la red.

Se divide en dos secciones:

- **Incidents**: muestra información del tipo de malware detectado, equipos afectados, si la amenaza fue ejecutada o no y otra información relevante.
- **Malware, PUPS and Exploits**: contiene la evolución de las detecciones realizadas en el parque informático. Esta información se muestra mediante widgets de tipo calendario.

Alerts summary (daily y weekly)

- **Malware y PUP**: muestran las incidencias detectadas en los procesos ejecutados por los equipos de usuario, así como en sus sistemas de ficheros. Estas incidencias son reportadas tanto por el análisis en tiempo real como por las tareas de análisis bajo demanda.
- **Exploit**: muestra el número de ataques por explotación de vulnerabilidades recibidos en los equipos Windows de la red.

Las alertas indican mediante flecha y porcentaje las variaciones entre las incidencias detectadas el último día con respecto al anterior (daily) y la última semana con respecto a la anterior (weekly).

Malware-PUP-Exploit execution status

- **Objetivo**: muestra la evolución de las amenazas encontradas en la red del cliente según su estado.
- **Tipo de widget**: gráfico de barras apilado.
- **Datos mostrados**: número de detecciones de amenazas según su estado (Not Executed, Blocked, Executed, Allowed by user,...) realizadas en todos los equipos de la red y agrupados por día del mes.

- **Agrupación**: día del mes.

En esta gráfica el administrador visualiza tanto los intentos de infección que han fracasado (not executed y blocked) como los que han prosperado (executed y allowed by user), ya sea por tratarse de malware conocido que el administrador excluyó del análisis, como del malware desconocido que se ejecutó por elección del usuario y que ahora el sistema ha clasificado como peligroso.

Calendar of daily malware detections

- **Objetivo**: Mostrar la evolución de las amenazas de tipo malware encontradas en la red del cliente.
- **Tipo de widget**: gráfico calendario.
- **Datos mostrados**: número de detecciones de malware realizadas en todos los equipos de la red, agrupados por día del mes.
- **Agrupación**: día del mes.

Este widget refleja de forma rápida y mediante códigos de color los días del año que más detecciones se han producido en la red del cliente. De esta forma se localizan los "días negros"

Calendar of daily Potential Unwanted Programs (PUPs) Detection

- **Objetivo**: mostrar la evolución de las amenazas de tipo Programa no deseado (PUP) encontradas en la red del cliente.
- **Tipo de widget**: gráfico calendario.
- **Datos mostrados**: número de detecciones de Programas no deseados (PUP) realizadas en todos los equipos de la red agrupados por día del mes.
- **Agrupación**: día del mes.

Este widget refleja de forma rápida y mediante códigos de color los días del año que más detecciones de Programas no deseados (PUP) se han producido en la red del cliente.Así se localizan los "días negros" para investigar sus causas.

Calendar of daily exploit detections

- **Objetivo**: mostrar la evolución de las amenazas de tipo Exploit encontradas en la red del cliente.
- **Tipo de widget**: gráfico calendario.
- **Datos mostrados**: número de detecciones de Exploit realizadas en todos los equipos de la red agrupados por día del mes.
- **Agrupación**: día del mes.

Este widget refleja de forma rápida y mediante códigos de color los días del año que más detecciones de exploit se han producido en la red del cliente. Así se localizan los "días negros" para investigar sus causas.

Detailled Information

Contiene una única sección **Incidents,** donde se detalla mediante varias tablas las incidencias registradas provocadas por el malware.

Endpoint involved in incidents

- **Objetivo**: ayuda a localizar los equipos de la red con más amenazas detectadas, y su tipo.
- **Campos**:
  - **Alert type**: tipo de amenaza (Malware o PUP).
  - **Machine name**: nombre del equipo donde se detectó la amenaza.
  - **Alert count**: contador con el número de ocurrencias en el plazo indicado.

En esta tabla se localiza de un vistazo los equipos que presentan una mayor probabilidad de problemas en la red.

Incidents on all endpoints

- **Objetivo**: muestra un listado completo de las amenazas detectadas en el periodo de tiempo establecido, con toda la información relevante.
- **Campos**:
  - **Alert type**: tipo de amenaza (Malware, PUP, Exploit).
  - **Machine name**: nombre del equipo donde se detectó la amenaza.
  - **Execution status**: indica si la amenaza llegó a ejecutarse o no (Executed | not Executed).
  - **Program**: ruta completa de la amenaza detectada.
  - **Threat**: nombre de la amenaza.
  - **Threat count**: contador con el número de ocurrencias en el plazo fijado.

Malware per endpoint hourly

- **Objetivo**: muestra el número de detecciones de malware en la última hora por cada equipo de la red.
- **SQL**:

```
from oem.panda.paps.alert where alertType = "Malware" group every 30m by
machineName every 0 select count() as count
```

Malware in the network hourly

- **Objetivo**: muestra el número de detecciones de malware en la última hora para toda la red.

- **SQL**:

```
from oem.panda.paps.alert where alertType = "Malware" group every 30m every 0
select count() as count
```

Malware executed in different endpoints hourly

- **Objetivo**: muestra el número de equipos que han ejecutado un determinado malware en la última hora.
- **SQL:**

```
from oem.panda.paps.alert where alertType = "Malware", executionStatus =
"Executed" group every 30m every 0 select count() as count
```

Consulta el apartado "Alertas asociadas" para más información.

Aplicación Application control

Application Control obtiene información detallada de las aplicaciones instaladas y ejecutadas en los equipos de los usuarios.

El dashboard se divide en cuatro pestañas: **IT Applications**, **Vulnerable applications**, **Bandwidth-consuming applications**, **Special Applications & Tools**.

IT Applications

En esta pestaña el administrador determina las aplicaciones ejecutadas en los equipos de la red, así como establecer un control básico de licencias en uso del paquete de ofimática Microsoft Office.

Executed Applications

- **Objetivo**: muestra los porcentajes de las empresas desarrolladoras del software ejecutado en la red, el nombre del ejecutable, la ruta donde se encuentra dentro del disco duro del equipo del usuario, y el equipo de la red que lo ejecutó.
- **Tipo de widget**: gráfico Voronoi.
- **Datos mostrados**:
  - **Primer nivel**: nombre de la empresa que desarrolló el software ejecutado.
  - **Segundo nivel**: nombre del programa ejecutado.
  - **Tercer nivel**: ruta completa del programa ejecutado referida al disco duro del equipo del usuario.
  - **Cuarto nivel**: nombre del equipo del usuario que ejecutó el programa.

- **Agrupación**: nombre de la empresa, nombre del software, ruta, equipo.

Con esta gráfica el administrador identifica de forma rápida los programas más frecuentemente ejecutados en la red, con el objetivo de detectar el uso de software poco apropiado o sin licencia.

Most frequently executed applications

- **Objetivo**: muestra un listado de las aplicaciones que se han ejecutado con más frecuencia.
- **Campos**:
  - **Childpath**: ruta completa de la aplicación ejecutada.
  - **Executable**: nombre del archivo ejecutable.
  - **Count**: contador con el número de ocurrencias en el plazo fijado.
  - **%**: indica el porcentaje de ejecuciones del programa sobre el total de ejecuciones registradas.

Machines running the most frequently executed applications

- **Objetivo**: muestra un listado de los equipos donde se ejecutaron con más frecuencia las aplicaciones.
- **Campos**:
  - **Childpath**: nombre del equipo en el que se ejecuta la aplicación.
  - **Executable**: nombre del archivo ejecutable.
  - **Count**: contador con el número de veces que se ha ejecutado la aplicación en el equipo en el plazo fijado.
  - **%**: indica el porcentaje de ejecuciones del programa sobre el total de ejecuciones registradas.

Least frequently executed applications

- **Objetivo**: muestra un listado de las aplicaciones que se han ejecutado con menos frecuencia. De esta forma se obtiene visibilidad sobre aplicaciones ejecutadas que puedan estar fuera del control del departamento de IT.
- **Campos**:
  - **Childpath**: ruta completa de la aplicación ejecutada.
  - **Executable**: nombre del archivo ejecutable.
  - **Count**: contador con el número de veces que la aplicación se ha ejecutado en el plazo fijado.
  - **%**: indica el porcentaje de ejecuciones del programa sobre el total de ejecuciones registradas.

Machines running the least frequently executed applications

- **Objetivo**: muestra un listado de los equipos donde se ejecutaron con menos frecuencia las aplicaciones.

- **Campos**:
  - **Machine**: nombre del equipo en el que se ejecuta la aplicación.
  - **Executable**: nombre del archivo ejecutable.
  - **User Count**: contador con el número de usuarios que han ejecutado la aplicación en el equipo en el plazo fijado.
  - **Execution Count**: contador con el número de veces que se ha ejecutado la aplicación en el equipo en el plazo fijado.
  - **%**: indica el porcentaje de ejecuciones del programa, sobre el total de ejecuciones registradas.

Microsoft Office Licenses in use

- **Objetivo**: muestra las aplicaciones del paquete de ofimática Microsoft Office utilizadas en la red y el usuario que las ejecutó.
- **Tipo de widget**: gráfico Voronoi.
- **Datos mostrados**:
  - **Primer nivel**: nombre de la aplicación Microsoft Office ejecutada.
  - **Segundo nivel**: usuario que ejecutó la aplicación.
  - **Agrupación**: nombre de aplicación, usuario.

Microsoft Office Applications in use

- **Objetivo**: muestra un listado que detalla las aplicaciones del paquete de ofimática Microsoft Office utilizadas en la red y el número de usuarios que la ejecutaron.
- **Campos**:
  - **Office Application**: nombre de la aplicación Microsoft Office ejecutada.
  - **User Count**: contador con el número de usuarios que han ejecutado la aplicación en el plazo fijado.
  - **%**: indica el porcentaje de ejecuciones del programa sobre el total de ejecuciones registradas.

Microsoft Office Applications by user

- **Objetivo**: muestra un listado de los usuarios que han ejecutado aplicaciones del paquete de ofimática Microsoft Office y las veces que lo han hecho.
- **Campos**:
  - **User**: nombre del usuario que ha ejecutado la aplicación de Microsoft Office.
  - **Office Application in Use Count**: contador con el número de veces que el usuario ha ejecutado una aplicación de Microsoft Office.
  - **%**: indica el porcentaje de ejecuciones del programa sobre el total de ejecuciones registradas.

Vulnerable Applications

Con esta pestaña el administrador determina las aplicaciones vulnerables instaladas y / o ejecutadas en los equipos de la red. El objetivo de las gráficas es poder determinar las prioridades del departamento de IT a la hora de actualizar el software con vulnerabilidades conocidas.

Vulnerable applications installed

- **Objetivo**: muestra las aplicaciones de software consideradas vulnerables instaladas en la red.
- **Campos**:
  - **Vulnerable application**: nombre de la aplicación de software considerada vulnerable.
  - **Machine count**: número de equipos en los que se ha instalado/ejecutado la aplicación considerada vulnerable.
  - **%**: indica el porcentaje de instalaciones/ejecuciones del programa sobre el total de instalaciones/ejecuciones registradas.

Vulnerable applications installed by machine

- **Objetivo**: muestra las aplicaciones de software consideradas vulnerables instaladas en la red y el equipo en el que están instaladas.
- **Campos**:
  - **Vulnerable application**: nombre de la aplicación de software considerada vulnerable.
  - **Company**: nombre de la compañía propietaria de la aplicación de software instalada.
  - **Machine**: nombre del equipo en el que se ha instalado la aplicación considerada vulnerable.
  - **%**: indica el porcentaje de instalaciones/ejecuciones del programa en el equipo sobre el total de instalaciones/ejecuciones registradas.

Vulnerable applications executed

- **Objetivo**: muestra las aplicaciones de software consideradas vulnerables ejecutadas en la red.
- **Campos**:
  - **Vulnerable application**: nombre de la aplicación de software considerada vulnerable.
  - **Machine count**: número de equipos en los que se ha ejecutado la aplicación considerada vulnerable.
  - **%**: indica el porcentaje de ejecuciones del programa sobre el total de ejecuciones registradas.

Vulnerable applications executed by machine

- **Objetivo**: muestra las aplicaciones de software consideradas vulnerables ejecutadas en la red, la compañía propietaria de la aplicación y el equipo en el que ha sido ejecutada la aplicación.
- **Campos**:

- **Company**: nombre de la compañía propietaria de la apllicación de software ejecutada.
- **Machine**: nombre del equipo en el que se ha ejecutado la aplicación considerada vulnerable.
- **Count**: número de veces que la aplicación considerada vulnerable ha sido ejecutada en el equipo.
- **%**: indica el porcentaje de ejecuciones del programa en el equipo, sobre el total de ejecuciones registradas.

Bandwidth-consuming applications

Esta pestaña muestra el volumen y porcentaje de ancho de banda consumido por las aplicaciones ejecutadas en el parque informático. El objetivo es dar una perspectiva del consumo de ancho de banda que producen las aplicaciones ejecutadas por los usuarios con un doble objetivo: para detectar aplicaciones con consumos por encima de la media, y para ayudar al correcto dimensionamiento del ancho de banda a provisionar en la empresa.

Data Volume Received by applications

- **Objetivo**: muestra los porcentajes y volúmenes de consumo de ancho de banda recibido por las aplicaciones ejecutadas en los equipos de la red, la ruta de la aplicación y el equipo que la ejecutó.
- **Tipo de widget**: grafico Voronoi.
- **Datos mostrados**:
  - **Primer nivel**: ejecutable que recibe los datos.
  - **Segundo nivel**: nombre del equipo que recibió los datos.
  - **Tercer nivel**: ruta completa del ejecutable en el equipo del cliente.
  - **Agrupación**: ejecutable, nombre de equipo, ruta.

Una agrupación alternativa que ayude a visualizar los equipos que reciben más tráfico de la red sería la siguiente: **machineName**, **executable**, **path**.

Data volume Sent by applications

- **Objetivo**: muestra los porcentajes y volúmenes de consumo de ancho de banda enviados por las aplicaciones ejecutadas en los equipos de la red, la ruta de la aplicación y el equipo que la ejecutó.
- **Tipo de widget**: gráfico Voronoi.
- **Datos mostrados**:
  - **Primer nivel**: ejecutable que envía los datos.
  - **Segundo nivel**: nombre del equipo que envió los datos.
  - **Tercer nivel**: ruta completa del ejecutable en el equipo del cliente.

- **Agrupación**: ejecutable, nombre de equipo, ruta.

Una agrupación alternativa que ayude a visualizar los equipos que envían más tráfico de la red sería la siguiente: **machineName**, **executable**, **path.**

Special Applications & Tools

Esta pestaña detalla las aplicaciones de scripting, de acceso remoto, herramientas de administrador y de sistema así como no deseadas de software libre que se ejecutan en la red. Además, se especifican cuáles de estas aplicaciones y herramientas se han ejecutado por equipo/usuario y el número de veces que ha esto ha sucedido.

Consulta **https://www.pandasecurity.com/spain/support/card?id=700065** *para ver la lista de programas detectados por Cytomic Insights.*

Scripting Applications Executed

- **Objetivo**: muestra los motores o intérpretes de aplicaciones de script ejecutados en los equipos.
- **Campos**:
  - **Scripting Application**: nombre de la aplicación de script ejecutada.
  - **Machine count**: número de equipos en los que se ha ejecutado la aplicación de script.
  - **%**: indica el porcentaje de ejecuciones de la aplicación sobre el total de ejecuciones registradas.

Scripting Applications Executed by machine and user

- **Objetivo**: muestra las aplicaciones de script ejecutadas en los equipos por los usuarios.
- **Campos**:
  - **Machine**: nombre del equipo en el que se ejecuta la aplicación script.
  - **User**: nombre del usuario que ejecuta la aplicación script en el equipo.
  - **Scripting application**: nombre de la aplicación de script ejecutada.
  - **Scripting application count**: número de veces que la aplicación de script ha sido ejecutada en el equipo.
  - **%**: indica el porcentaje de ejecuciones de la aplicación en el equipo sobre el total de ejecuciones registradas.

Remote Access Applications Executed

- **Objetivo**: muestra las aplicaciones de acceso remoto ejecutadas en la red.
- **Campos**:
- **Remote Access Application**: nombre de la aplicación de acceso remoto ejecutada.

- **Machine count**: número de equipos en los que se ha ejecutado la aplicación de acceso remoto.
- **%**: indica el porcentaje de ejecuciones de la aplicación de acceso remoto, sobre el total de ejecuciones registradas.

Remote Access Applications Executed by machine and user

- **Objetivo**: muestra las aplicaciones de acceso remoto ejecutadas en los equipos por los usuarios.
- **Campos**:
  - **Machine**: nombre del equipo en el que se ejecuta la aplicación de acceso remoto.
  - **User**: nombre del usuario que ejecuta la aplicación de acceso remoto.
  - **Remote Access application**: nombre de la aplicación de acceso remoto ejecutada.
  - **Remote application count**: número de veces que la aplicación de acceso remoto ha sido ejecutada en el equipo por el usuario.
  - **%**: indica el porcentaje de ejecuciones de la aplicación de acceso remoto, en el equipo sobre el total de ejecuciones registradas.

Admin Tools Executed

- **Objetivo**: muestra las herramientas de administración ejecutadas en la red.
- **Campos**:
  - **Admin Tools Executed**: nombre de la herramienta de administración ejecutada.
  - **Machine count**: número de equipos en los que se ha ejecutado la herramienta de administración.
  - **%**: indica el porcentaje de ejecuciones de la herramienta de administración sobre el total de ejecuciones registradas.

Admin Tools Executed by machine and user

- **Objetivo**: muestra las herramientas de administración ejecutadas en los equipos por los usuarios.
- **Campos**:
  - **Machine**: nombre del equipo en el que se ejecuta la herramienta de administración.
  - **User**: nombre del usuario que ejecuta la herramienta de administración.
  - **Admin Tools Executed**: nombre de la herramienta de administración ejecutada.
  - **Admin Tools Count**: número de veces que la herramienta de administración ha sido ejecutada en el equipo por el usuario.
  - **%**: indica el porcentaje de ejecuciones de la herramienta de administración en el equipo, sobre el total de ejecuciones registradas.

System Tools Executed

- **Objetivo**: muestra las herramientas de sistema ejecutadas en los equipos.

- **Campos**:
  - **System Tools Executed**: nombre de la herramienta de sistema ejecutada.
  - **Machine count**: número de equipos en los que se ha ejecutado la herramienta de sistema.
  - **%**: indica el porcentaje de ejecuciones de la herramienta de sistema, sobre el total de ejecuciones registradas.

System Tools Executed by machine and user

- **Objetivo**: muestra las herramientas de sistema ejecutadas en los equipos por los usuarios.
- **Campos**:
  - **Machine**: nombre del equipo en el que se ejecuta la herramienta de sistema.
  - **User**: nombre del usuario que ejecuta la herramienta de sistema.
  - **System Tools Executed**: nombre de la herramienta de sistema ejecutada.
  - **System Tools Count**: número de veces que la herramienta de sistema ha sido ejecutada en el equipo por el usuario.
  - **%**: indica el porcentaje de ejecuciones de la herramienta de sistema en el equipo, sobre el total de ejecuciones registradas.

System Internal Tools Executed

- **Objetivo**: muestra las herramientas de sistema internas ejecutadas en los equipos.
- **Campos**:
  - **System Internal Tools**: nombre de la herramienta de sistema interna ejecutada.
  - **Machine count**: número de equipos en los que se ha ejecutado la herramienta de sistema interna.
  - **%**: indica el porcentaje de ejecuciones de la herramienta de sistema interna, sobre el total de ejecuciones registradas.

System Internal Tools Executed by machine and user

- **Objetivo**: muestra las herramientas de sistema internas ejecutadas en los equipos por los usuarios.
- **Campos**:
  - **Machine**: nombre del equipo en el que se ejecuta la herramienta de sistema interna.
  - **User**: nombre del usuario que ejecuta la herramienta de sistema interna.
  - **System Internal Tools**: nombre de la herramienta de sistema interna ejecutada.
  - **System Internal Tool Count**: número de veces que la herramienta de sistema interna ha sido ejecutada en el equipo por el usuario.
  - **%**: indica el porcentaje de ejecuciones de la herramienta de sistema interna en el equipo, sobre el total de ejecuciones registradas.

Unwanted Freeware Executed Applications

- **Objetivo**: muestra las aplicaciones de software libre no deseadas ejecutadas en la red.
- **Campos**:
  - **Freeware Application**: nombre de la aplicación de software libre no deseada ejecutada.
  - **Machine count**: número de equipos en los que se ha ejecutado la aplicación de software libre no deseada.
  - **%**: indica el porcentaje de ejecuciones de la aplicación de software libre no deseada, sobre el total de ejecuciones registradas.

Unwanted Freeware Executed Applications by machine and user

- **Objetivo**: muestra las aplicaciones de software libre no deseadas ejecutadas en los equipos por los usuarios.
- **Campos**:
  - **Freeware Application**: nombre de la aplicación de software libre no deseada ejecutada.
  - **Machine**: nombre del equipo en el que se ejecuta la aplicación de software libre no deseada.
  - **User**: nombre del usuario que ejecuta la aplicación de software libre no deseada en el equipo.
  - **Freeware application count**: número de veces que la aplicación de software libre no deseada ha sido ejecutada en el equipo por el usuario.
  - **%**: indica el porcentaje de ejecuciones de la aplicación de software libre no deseada en el equipo, sobre el total de ejecuciones registradas.

Executions of Vulnerable apps per endpoint today

- **Objetivo**: muestra el número de aplicaciones vulnerables ejecutadas en las últimas 24 horas por cada equipo de la red.
- **SQL**:

```
from oem.panda.paps.ops where isnotnull(ocsVer) group every 30m by machine every
1d select count(childPath) as childPath
```

Bandwidth consumption to endpoint hourly

- **Objetivo**: ancho de banda recibido en la última hora por cada equipo en la red.
- **SQL**:

```
from oem.panda.paps.processnetbytes group every 30m by machineName every 0
select sum(bytesReceived) as sum_bytes_received
```

Bandwidth consumption from endpoint hourly

- **Objetivo**: ancho de banda enviado en la última hora por cada equipo en la red.
- **SQL**:

```
from oem.panda.paps.processnetbytes group every 30m by machineName every 0
select sum(bytesSent) as sum_bytes_sent
```

Bandwidth consumption per Apps. hourly

- **Objetivo**: ancho de banda recibido y enviado por cada aplicación en la última hora.
- **SQL**:

```
from oem.panda.paps.processnetbytes select subs(path,
re("(.*\\\\)(?=.*(\\.\\w*)$|(\\w+)$)"), template("")) as executablename select
lower(executablename) as executable where endswith(executable, "exe") group
every 15s by executable every 15s select sum(bytesReceived) as
sum_bytes_consumption
```

*Consulta el apartado "**Alertas asociadas**" para más información.*

Aplicación Data Access Control

Data Access Control muestra la información que sale de la red del cliente para detectar fugas de datos y robos de información confidencial.

El dashboard se divide en cuatro pestañas: **Outbound network traffic**, **Users activity**, **Bandwidth consumers** y **Data file accessed**.

Outbound network traffic

Esta pestaña muestra información sobre el volumen de datos enviado fuera de la red del cliente. Se divide en dos secciones:

- **Data**: muestra valores absolutos y relativos de transferencias de datos.
- **Map**: geolocaliza sobre un mapa del mundo los destinos hacia los que un mayor porcentaje de datos es enviado.

Annual Calendar of outbound network traffic

- **Objetivo**: muestra la evolución de los datos enviados desde la red del cliente.

- **Tipo de widget**: gráfico calendario.
- **Datos mostrados**: volumen de datos medido en Megabytes o Gigabytes de todos los equipos que componen la red del cliente, agrupados por día del mes.
- **Agrupación**: día del mes.

En esta gráfica el administrador visualiza los días del mes donde los equipos de la red han enviado un volumen de datos anormalmente alto.

Countries with outbound connections

- **Objetivo**: localiza los países que reciben mayor número de conexiones desde la red del cliente.
- **Campos**:
  - **CC**: código del país destino de la conexión.
  - **Count**: número de conexiones.
  - **%**: porcentaje del volumen de conexiones de cada país.

Este gráfico muestra cuales son los países que más conexiones han recibido desde la red gestionada por el administrador. En estos casos suelen ser un indicio de problemas el hecho de mostrar en este listado países que, en principio, no tienen relación con la provisión de servicios contratada por la empresa.

Outbound network traffic destination

- **Objetivo**: geolocaliza en un mapa del mundo el destino del tráfico de la red del cliente.
- **Tipo de widget**: gráfico mapa.
- **Datos mostrados**: representación del volumen de datos enviados desde la red del cliente a los países indicados en el mapa mediante puntos de diferente intensidad. El color y diámetro de los puntos representan el volumen de datos enviado.
- **Agrupación**: país.

Como complemento a la tabla **Countries with outbound connections** se muestran en un mapa los países que han recibido datos de la red del cliente, mostrando el volumen de forma relativa.

User activity

Muestra información de acceso de las cuentas de usuario a las máquinas de la red.

Logged-in users

- **Objetivo**: muestra las máquinas accedidas por cada cuenta de usuario dada de alta en la red.
- **Tipo de widget**: grafico Voronoi.
- **Datos mostrados**:

- **Primer nivel**: cuentas de usuario.
- **Segundo nivel**: máquinas accedidas por la cuenta de usuario seleccionada en el primer nivel.
- **Agrupación**: usuario, máquina.

Una posible variación de este gráfico se obtiene cambiando el orden del campo **Legend** a **machineuser**, si lo que queremos es determinar qué cuentas de usuario han accedido a cada máquina.

Bandwidth consumers

Localiza los procesos y usuarios que más volumen de datos consumen en la red. Los datos en las tablas muestran hasta un máximo de 1.000 registros, ordenados de mayor a menor.

Applications with Inbound network traffic

- **Objetivo**: localiza las aplicaciones que reciben mayor volumen de tráfico de la red del cliente.
- **Campos**:
  - **Executable**: nombre del fichero ejecutable que recibe datos.
  - **Volume received**: suma del volumen de datos recibido.
  - **%**: porcentaje del volumen de datos recibido sobre el total.

Applications with Outbound network traffic

- **Objetivo**: localiza las aplicaciones que envían mayor volumen de tráfico de la red del cliente.
- **Campos**:
  - **Executable**: nombre del fichero ejecutable que envía datos.
  - **Sum_sent_sum**: suma del volumen de datos enviado por programa.
  - **%**: porcentaje del volumen de datos recibido sobre el total.

Machine-User pairs with most outbound network traffic

- **Objetivo**: localiza los pares usuario-máquina que envían mayor volumen de tráfico de la red del cliente.
- **Campos**:
  - **User**: usuario logeado en la máquina que envía el tráfico.
  - **Machinename**: nombre del equipo que envía el tráfico.
  - **Volume Sent**: volumen de datos enviados.
  - **%**: porcentaje del volumen de datos enviados sobre el total.

Machine-User pairs with most inbound network traffic

- **Objetivo**: localiza los pares usuario-máquina que reciben mayor volumen de tráfico de la red del cliente.
- **Campos**:
  - **User**: usuario logeado en la máquina que recibe el tráfico.
  - **Machinename**: nombre del equipo que recibe el tráfico.
  - **Volume Recived**: volumen de datos recibidos.
  - **%**: porcentaje del volumen de datos recibidos sobre el total.

Data file Accessed

Localiza los ficheros accedidos por los usuarios de la red del cliente. Con los datos de esta sección el administrador podrá acceder a algunas funciones de tipo DLD (Data Leak Detection).

Se presentan las siguientes secciones:

- **Endpoints**: muestra estadísticas de acceso a ficheros por usuario y extensión.
- **Users & extensions**: muestra estadísticas de acceso según el tipo de fichero extensión.

Files most accesed from endpoints

- **Objetivo**: mostrar los ficheros más accedidos por los usuarios de la red.
- **Campos**:
  - **Machine**: nombre de la máquina utilizado para acceder al fichero.
  - **Childpath**: ruta y nombre del fichero accedido.
  - **Count**: número de veces que el equipo accedió al fichero.
  - **%**: porcentaje de accesos respecto al número total de accesos.

Most accessed files by user

- **Objetivo**: mostrar los ficheros más accedidos por los usuarios de la red.
- **Campos**:
  - **Childpath**: ruta y nombre del fichero accedido.
  - **Loggeduser**: usuario logeado que accede al fichero.
  - **Count**: número de veces que el usuario accede al fichero.
  - **%**: porcentaje de accesos respecto al número total de accesos.

Most executed extensions

- **Objetivo**: mostrar las extensiones más utilizadas en la red, bien de forma individual (extensiones de

ficheros ejecutables), bien de ficheros de datos abiertos por programas (archivos de ofimática, archivos comprimidos, etc.).

- **Campos**:
  - **File Extension**: extensión del fichero accedido.
  - **Count**: número de veces que se accedió a un fichero con la extensión indicada.
  - **%**: porcentaje de accesos respecto al número total de accesos.

Users and Outbound data hourly

- **Objetivo**: muestra el volumen de datos enviado por cada usuario en la ultima hora.
- **SQL**:

```
from oem.panda.paps.processnetbytes select yesterday("") asyest_date where eventdate >= yest_date and not startswith(user, "NTAUTHORITY") and not startswith(user, "<unknown>\\<unknown>") groupevery 30m by user every 1d select sum(bytesSent) as total_tx
```

*Consulta el apartado "**Alertas asociadas**" para más información.*

Capítulo 6

Alertas

El sistema de alertas de Cytomic Insights 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

Arquitectura del sistema de alertas

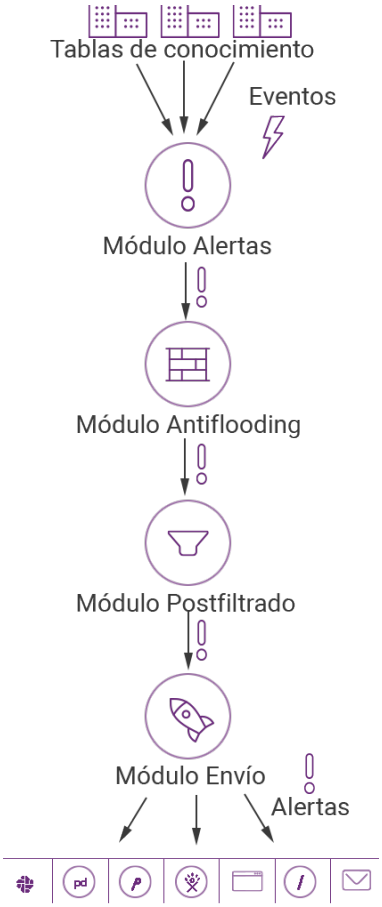

Figura 6.1: Módulos implementados en el flujo de generación de alertas

El sistema de alertas de Cytomic Insights 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 antifllooding** (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:

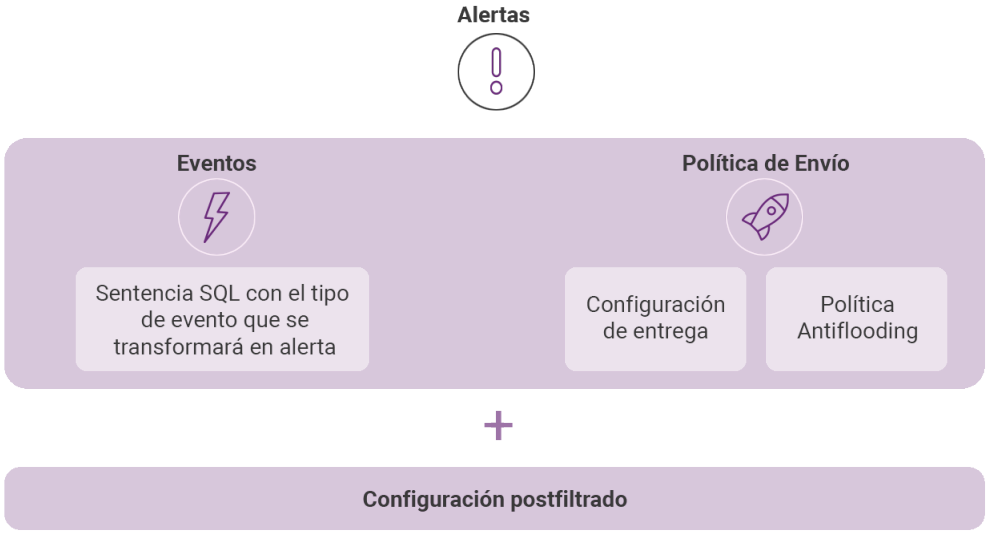

Figura 6.2: componentes lógicos que forman una alerta

Creación de alertas

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

1. Selecciona la tabla apropiada en el menú lateral, **Búsqueda**.

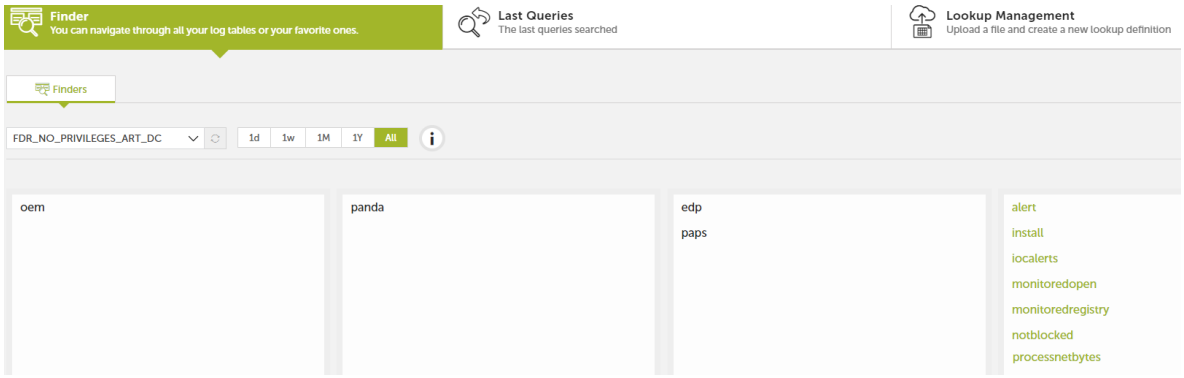

Figura 6.3: ventana de administración de alertas

2. Aplica 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.

- **Message**: asunto de la alerta.
- **Description**: contenido de la alerta.
- **Subcategory**: etiqueta para clasificar la alerta y facilitar su búsqueda o filtrado posteriores.
- **Alert name**: Sección nueva

4. Ritmo de generación de alertas.

- **Each**: genera una alerta por cada evento de inserción en la tabla.
- **Several**: genera una única alerta por cada grupo de eventos de inserción en la tabla producidos durante un tiempo determinado.
  - **Period**: intervalo de tiempo.
  - **Threshold**: número de eventos recibidos en el intervalo definido.
- **Low**: genera una única alerta si se producen menos eventos que los indicados en el período de tiempo configurado.
  - **Period**: intervalo de tiempo.
  - **Threshold**: número de eventos recibidos en el intervalo definido.
- **Rolling**: comprueba en intervalos regulares los eventos productos en el periodo de tiempo especificado.
  - **Run every:** indica cada cuantos minutos se comprobará la existencia de eventos.
  - **Check last:** establece el intervalo de comprobación.

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 generará 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 más información consulta el apartado "**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.

Para acceder a las alertas en el menú lateral haz clic en **Alertas** y en el menú superior en la pestaña **Panel de Alertas**.

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 mes.
- 1 año.

- **Filtrado por estado de la alerta** (4):
  - **Abierta**: solo se muestran las alertas en estado Abierta.
  - **Todas las alertas**: se muestran todas las alertas.

*Consulta "**Tablas y Gráficos**" en la página **29** 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 realizada por el administrador en el momento de creación de la alerta:

- **Estado**: vista, no leída.
- **Tipo**: tipo de la alerta, tomado del campo **Message** en la configuración de la alerta, consulta "**Creación de alertas**" para más información.
- **Información detallada**: extracto del cuerpo de la alerta tomada del campo **Description,** consulta "**Creación de alertas**" para más información. Al hacer clic en el campo **Información detallada** la alerta se desplegará mostrando su contenido.
- **Categoría**: categoría de la alerta tomada del campo **Subcategory** y **Context,** consulta "**Creación de alertas**" para más información.
- **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 "**Gestión de postfiltros**" para más información.
- **Creada**: fecha, hora y tiempo transcurrido desde la generación de la alerta.
- **Menú**: la última columna de la tabla de **Historial de alertas** despliega un menú de opciones para cada alerta:
  - **Ver detalles de alerta**: muestra toda la información asociada a la alerta en una ventana independiente.
  - **Ir a la consulta**: accede a la tabla con los datos.
  - **Crear anotación**: añade 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. También es posible convertir una anotación en una tarea si la alerta requiere de una intervención alargada en el tiempo.

- **Nuevo filtro**: crea postfiltros, descritos apartado "**Creación de postfiltros**".
- **Marcar como cerrada**: marca una alerta como cerrada.
- **Borrar**: borra la 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.

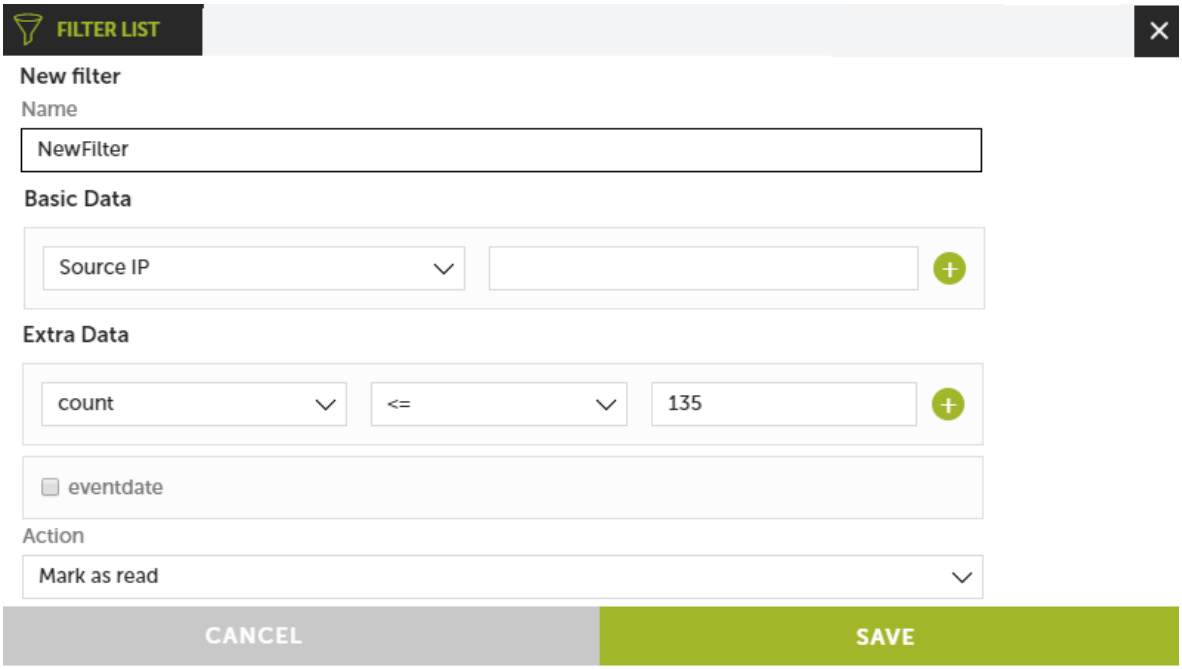

Figura 6.5: Ventana de creación de un nuevo post filtro

La pantalla de posfiltros está formada por cinco secciones:

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.

- **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.

Sección 2: Contenido base

Esta sección no tiene uso.

Sección 3: Contenido extra

En esta sección se establecen las condiciones basadas en el contenido del evento y que la alerta tendrá que cumplir para que el postfiltro se aplique.

En el proceso de configuración de una alerta se podían establecer una serie de columnas en el campo **Counter**. El contenido de estas columnas se accede desde el cuerpo de la alerta en el momento de su generación mediante el símbolo $, y en la sección **Contenido extra** se elige del desplegable los contadores a 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.

Haz clic en el botón de **Guardar** cuando toda la información esté incluida. Esta operación generará el código de filtro en una ventana emergente, haz clic en **Añadir** para agregarlo en la pestaña de postfiltros.

Gestión de postfiltros

La gestión de postfiltros se realiza desde el menú lateral **Alertas** haciendo clic en la pestaña **Post filtros**.

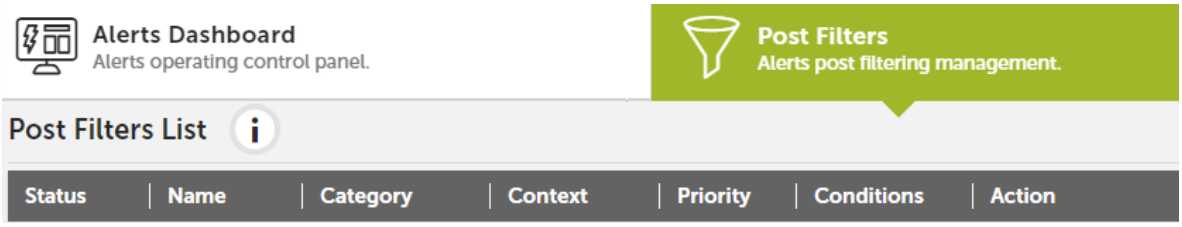

Figura 6.6: pestaña de gestión de postfiltros

En esta ventana se muestra un listado de los postfiltros configurados con la información mostrada a continuación:

- **Estado**: activo o inactivo.
- **Nombre**: nombre del postfiltro elegido por el administrador en la 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.

Creación de configuraciones de entrega

Las configuraciones de entrega se crean en el menú lateral **Administración**, **Configuración de alertas**, en la pestaña **Configuración entrega**.

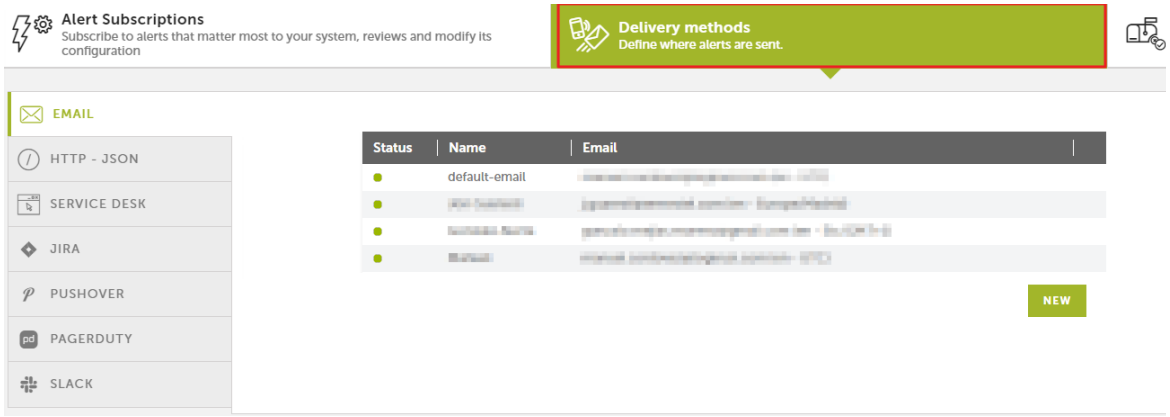

Figura 6.7: ventana de creación de métodos de entrega

En el panel de la izquierda se 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

Envío en tiempo real de alertas a cuentas de correo.

Los campos requeridos son:

- **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.

HTTP-JSON

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

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

Los campos requeridos son:

- **Nombre**: nombre de la configuración de envío.
- **Huso horario**: ajusta la fecha y hora de envío del mail.
- **URL**: URL del servidor destino indicando el protocolo (http o https) y el puerto (p.ej. **http://localhost:8080/index.php**).
- **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.

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). 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.

Service desk

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

Los campos requeridos son:

- **Nombre**: nombre de la configuración de envío.
- **URL**: URL del servidor destino.
- **Huso horario**: ajusta la fecha y hora de envío del mail.
- **Idioma**: idioma en el que se recibe la alerta.
- **Método de envío**: REST o SERVLET.
- **REST**: **http://[SERVER]:[PORT]/sdpapi/request/**
- **SERVLET**: **http://[SERVER]:[PORT]/servlets/RequestServlet**
- **Usuario**: nombre del técnico asignado.
- **Technician Key**: llave del técnico generado en el panel de administración de 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). 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.

JIRA

Envío en tiempo real de alertas a servidores Jira.

Los campos requeridos son:

- **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.
- **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.

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 JIRA 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.

Pushover

Envío en tiempo real de alertas a cuentas PushOver.

Los campos requeridos son:

- **Usuario**: 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.

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 Pushover 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.

Pagerduty

Envío en tiempo real de alertas a cuentas PagerDuty.

Los campos requeridos son:

- **Usuario**: 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 (opcional)**: 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.

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 Pagerduty 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.

SLACK

Envío en tiempo real de alertas por medio de SLACK.

Los campos requeridos son:

- 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 destino.
- Idioma: Idioma en el que se recibe la alerta.

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**.

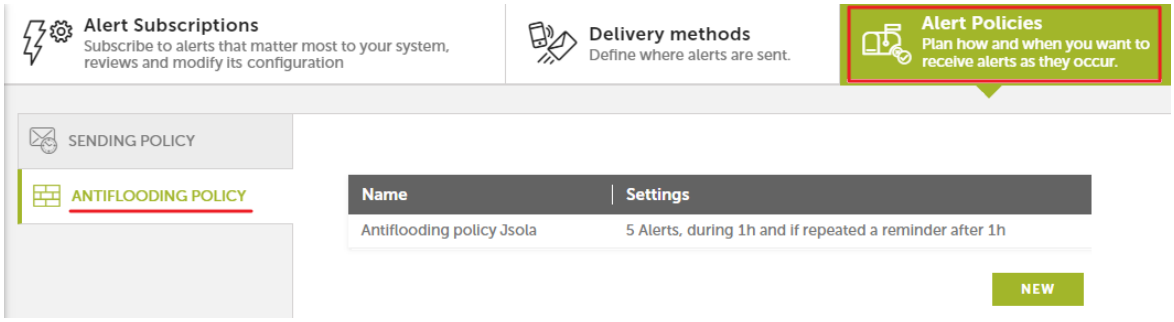

Figura 6.8: ventana de creación de políticas antiflooding

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

En esta ventana se define:

- Número máximo de alertas a recibir.
- Intervalo de tiempo durante el cual se recibirán el número de alertas especificado en el punto anterior.
- Recordatorio si la alerta se repite después de un intervalo de tiempo configurable.

Edición de políticas antiflooding

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

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

Creación de políticas de alertas o políticas de envío

Las políticas de alertas, también llamadas políticas de envío definen el comportamiento de envío de las alertas generadas.

Una política de envío es el nexo de unión de las políticas definidas en los puntos anteriores (política antiflooding y configuración de entrega).

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

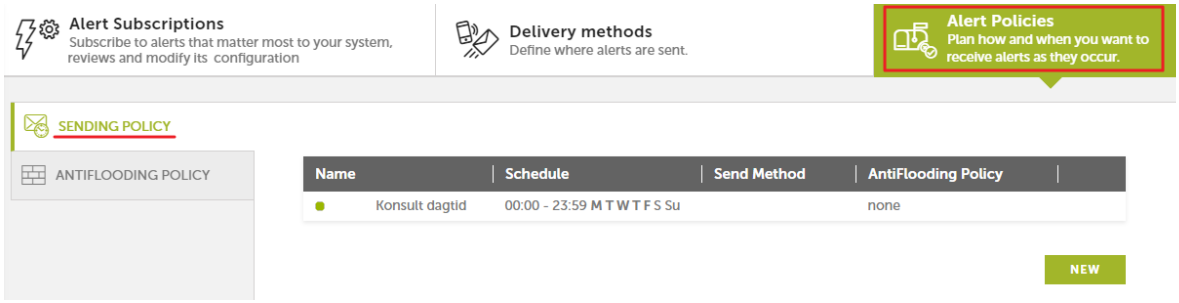

Figura 6.9: ventana de creación de políticas de envío

Al hacer clic en el botón **Nuevo** se abrirá una ventana donde podremos especificar todos los parámetros de la política de envío:

- **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 envío asignada se aplicara ésta por defecto.
- **Política antiflooding**: indicar 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 varias formas de envío configuradas previamente, que se utilizaran para despachar la alerta.

Edición de políticas de envío

Cada una de las políticas de envío creadas tiene asociado un menú para 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**.

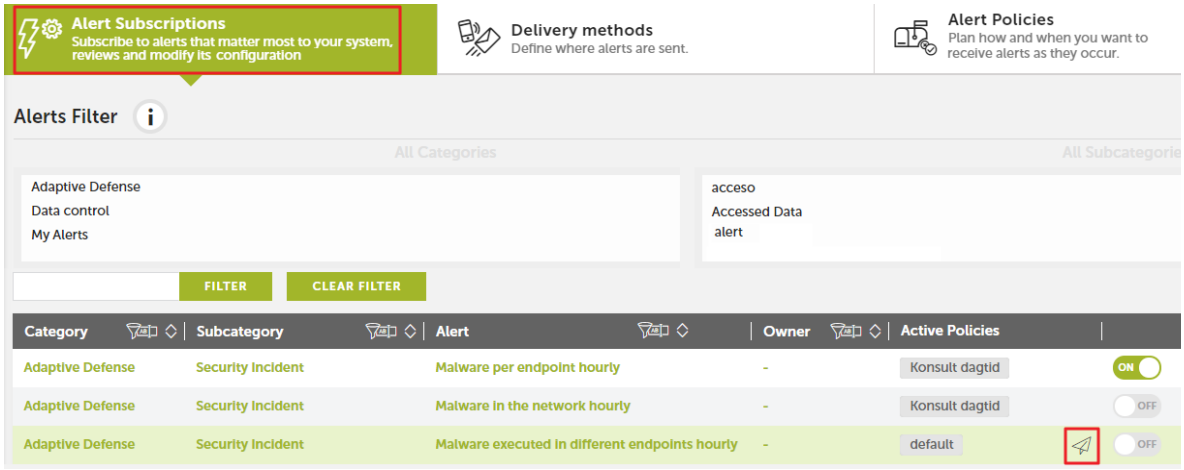

Figura 6.10: ventana de administración de alertas

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

Capítulo 8: Requisitos de hardware, software y red

Capítulo 7

Tablas de conocimiento

Cytomic EDR envía toda la información recogida por Cytomic EDR al servicio Cytomic Insights, que se encargará de organizarla en tablas de fácil lectura.

Cada línea de una tabla se corresponde a un evento supervisado por Cytomic EDR. Las tablas contienen una serie de campos específicos, además de campos comunes que aparecen en todas y que ofrecen información, tal y como el momento en que ocurrió el evento, la máquina donde se registró, su dirección IP, etc.

Notación utilizada en los campos

Muchos campos de las tablas utilizan prefijos que ayudan a referir la información mostrada. Los dos prefijos más usados son:

- **Parent**: los campos que comienzan con la etiqueta Parent (parentPath, parentHash, parentCompany…) reflejan el contenido de una característica o atributo del proceso padre.
- **Child**: los campos que comienzan con la etiqueta Child (childPath, childHash, childCompany…) reflejan el contenido de una característica o atributo de un proceso hijo creado por el proceso padre.

Además de estos prefijos en muchos campos y valores se utilizan abreviaturas; conocer su significado ayuda a interpretar el campo en cuestión:

- **Cat**: categoría.
- **Cfg**: configuración.
- **Cmp** y **comp**: comprimido.
- **Dst**: destino.
- **Exe**: executable (ejecutable).
- **Mw**: malware.
- **Op**: operación.
- **PE**: programa ejecutable.
- **Prev**: prevalencia.
- **PUP**: Potential Unwanted Program (programa potencialmente no deseado).
- **Sec**: seconds (segundos).
- **Sig**: signature (firma digital).
- **SP**: Service Pack.
- **Svc**: servicio.
- **Ver**: versión.

A continuación, se listan las tablas disponibles indicando el tipo de información que contienen y sus campos específicos.

Alert

Esta tabla es una correspondencia de las incidencias mostradas en la sección **Actividad** del panel de control de la consola de Cytomic EDR.

Contiene una línea por cada amenaza detectada en la red del cliente con información sobre el equipo involucrado, tipo de alerta, timestamp y resultado de la alerta:

Nombre	Descripción	Valores
evendate	Fecha de inserción del evento en el servidor Cytomic Insights.	Fecha
machineIP	IP de la máquina del cliente que desencadenó la alerta.	Dirección IP
date	Fecha del equipo del usuario cuando se generó el evento.	Fecha
alertType	Categoría de la amenaza que disparó la alerta.	• Malware • PUP
machineName	Nombre de la máquina del cliente.	Cadena de caracteres
executionStatus	La amenaza se llegó a ejecutar o no.	• Executed • Not Executed
dwellTimeSecs	Tiempo transcurrido en segundos desde la primera vez que la amenaza fue vista en la red del cliente.	Segundos
itemHash	Hash de la amenaza encontrada.	Cadena de caracteres
itemName	Nombre de la amenaza detectada.	Cadena de caracteres
itemPath	Ruta completa del fichero que contiene la amenaza.	Cadena de caracteres
sourceIP	Si el malware vino del exterior de la red del cliente indica la ip del equipo remoto.	Dirección IP
sourceMachineName	Si el malware vino del exterior de la red del cliente indica el nombre del equipo remoto.	Cadena de caracteres
sourceUserName	Si el malware vino del exterior de la red del cliente indica el usuario del equipo remoto.	Cadena de caracteres
urlList	Lista de URLs accedidas en el momento de detectar un exploit desde el navegador.	Cadena de caracteres
docList	Lista de documentos accedidos en el momento de detectar un exploit de fichero.	Cadena de caracteres
version	Contenido del atributo Version de los metadatos del proceso.	Cadena de caracteres
vulnerable	Indica si la aplicación se considera vulnerable.	Booleano

Tabla 7.1: descripción de los eventos de tipo alerta generados

Puesto que la tabla **Alerts** es una transposición de la sección **Actividad** del panel de control de Cytomic EDR es pueden obtener estadísticas de los equipos más infectados:

10 equipos más atacados e infectados

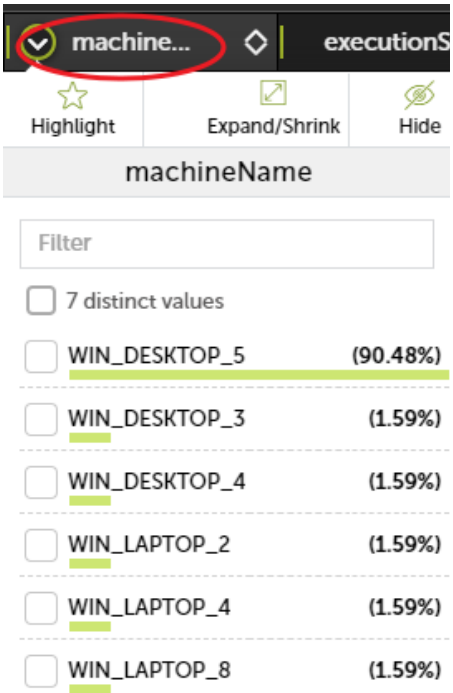

Figura 7.1: desplegable con los valores más frecuentemente encontrados

Para obtener un listado simple de los 10 equipos más atacados haz clic en la cabecera de la columna **machineName** o **machineIP**.

Este listado abarca desde el primer momento en que Cytomic EDR comenzó a funcionar en el cliente; para reducir el rango de fechas acota el intervalo con los controles **Apply interval**.

Figura 7.2: herramienta para definir los datos a mostrar

Estos listados incluyen tanto bloqueos como ejecuciones de malware, para mostrar únicamente los equipos infectados añade un filtro haciendo clic en el icono de la barra de herramientas.

Figura 7.3: acceso a la herramienta para crear un nuevo filtro de datos

Configura un filtro de datos utilizando el campo **executionStatus** e igualando a **Executed**, tal y como se muestra en la imagen.

Figura 7.4: herramienta para crear un nuevo filtro de datos

10 amenazas más vistas

Haz clic en las columnas **itemHash** o **ítemName** para visualizar estadísticas rápidas sobre las 10 amenazas más vistas en la red del cliente.

Otra forma de obtener información de forma mucho más visual es utilizar una gráfica del malware más visto. En el eje de las coordenadas se muestra el nombre del malware y en el eje de abscisas el número de ocurrencias.

Para generar una gráfica sigue los pasos:

1. Añade una agrupación sobre el campo **itemName** sin límite temporal (**No temporal aggrupation**).

Figura 7.5: acceso a la herramienta para crear una nueva agrupación de datos

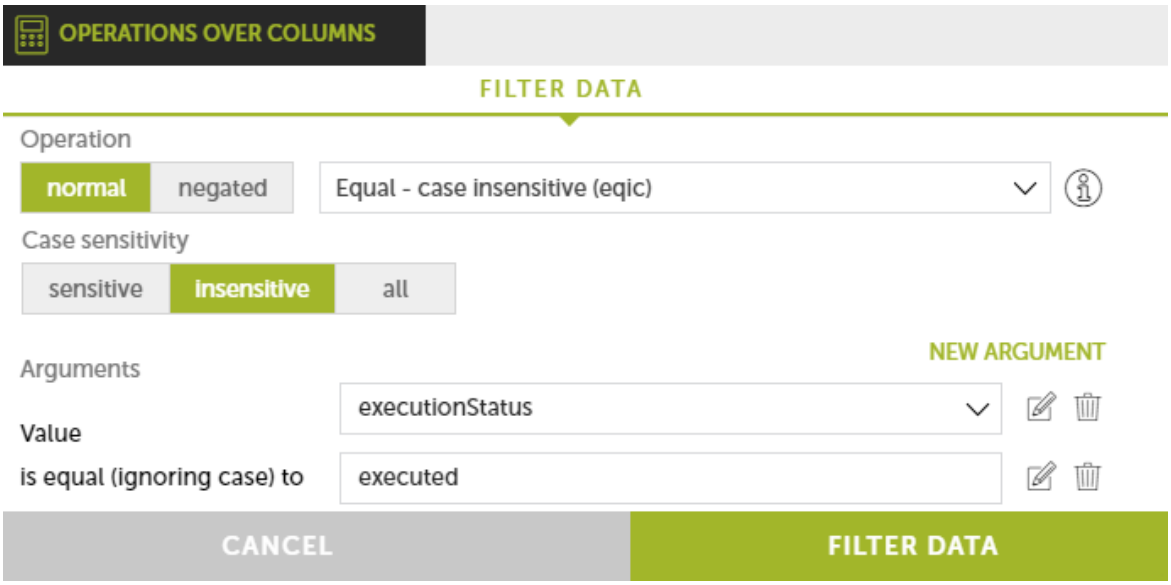

Figura 7.6: herramienta para crear una agrupación de datos

2. Agrega una función **Contador** para determinar cuántas ocurrencias hay en cada grupo **itemName**.

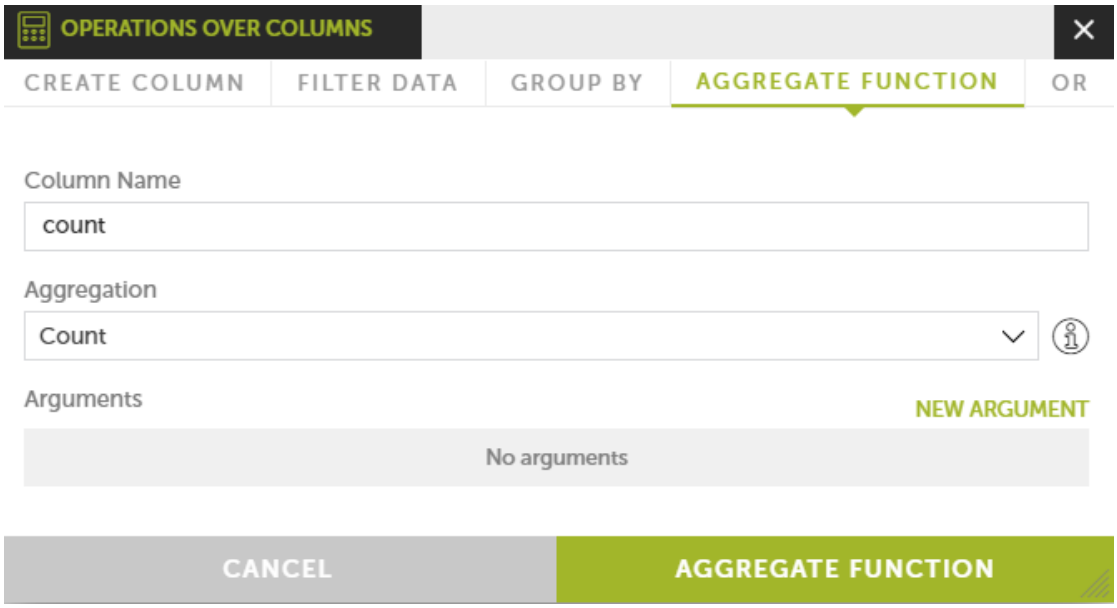

Figura 7.7: herramienta para crear operaciones sobre columnas

3. Utiliza un filtro para discriminar las agrupaciones de 2 o menos ocurrencias. De esta forma se limpia

la gráfica de aquellas amenazas que solo hayan sido vistas 2 veces.

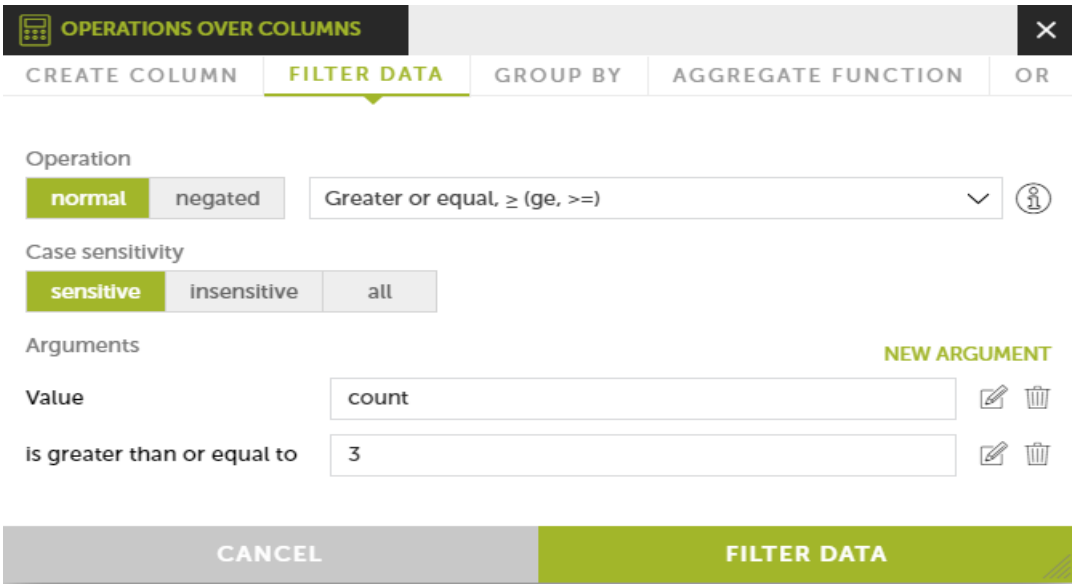

Figura 7.8: herramienta para crear operaciones sobre columnas

4. Crea un gráfico de tipo **Chart Aggregation** y coloca la columna **Count** como parámetro.

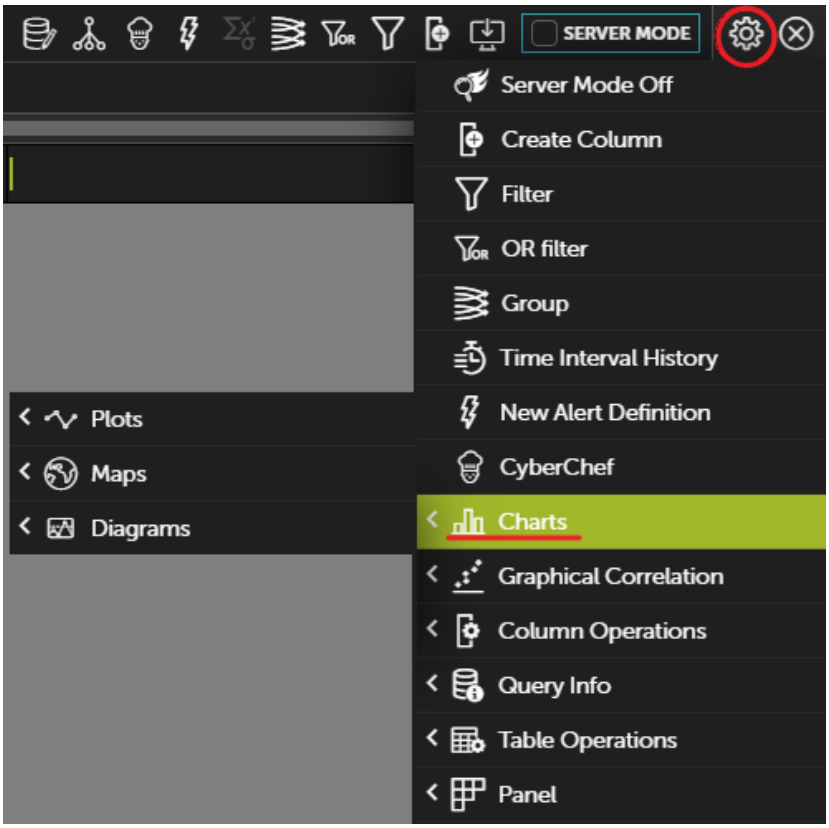

Figura 7.9: menú de acceso a la creación de gráficas

En este punto ya se dispone de un listado alertas agrupadas por amenaza y con el número de ocurrencias por cada amenaza. Con estos datos se puede construir una gráfica simple:

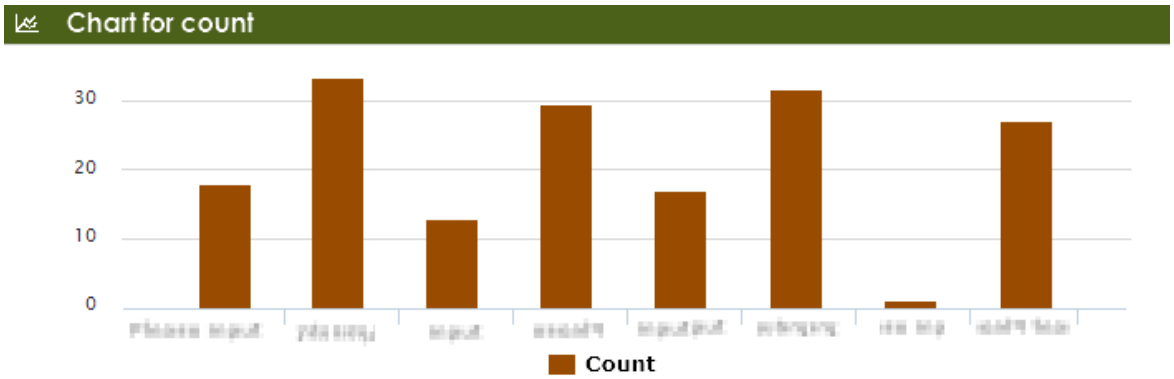

Figura 7.10: gráfica de barras generada

Otra información útil

Hay varios campos en la tabla **Alerts** que se utilizan para extraer información valiosa acerca de los ataques recibidos en la red del cliente:

- **Eventdate**: agrupa por este campo para visualizar el número de ataques diarios y así determinar si hay una epidemia en curso.
- **dwellTimeSecs**: campo que obtiene la ventana de detección de las amenazas recibidas, es decir, el tiempo desde que la amenaza fue vista por primera vez en la red del cliente hasta su clasificación.
- **itemHash**: dado que el nombre de la amenaza varía entre proveedores de seguridad utiliza el campo hash para agrupar amenazas en vez del **itemName**. Así se discrimina además el malware que se etiqueta con el mismo nombre.

Install

Esta tabla contiene toda la información generada en la instalación de los agentes de Cytomic EDR en las equipos del cliente.

Nombre	Descripción	Valores
eventDate	Fecha de inserción del evento en el servidor Cytomic Insights.	Fecha
serverdate	Fecha del equipo del usuario cuando se generó el evento.	Fecha
machine	Nombre de la máquina del cliente.	Cadena de caracteres
machineIP	IP de la máquina del cliente.	Dirección IP

Tabla 7.2: descripción de los eventos generados en el proceso de instalación

Nombre	Descripción	Valores
machineIP1	IP de una tarjeta de red adicional si está instalada.	Dirección IP
machineIP2	IP de una tarjeta de red adicional si está instalada.	Dirección IP
op	Operación realizada.	• Install • Uninstall • Upgrade
osVersion	Versión del Sistema Operativo.	Cadena de caracteres
osServicePack	Versión del Service Pack.	Cadena de caracteres
osPlatform	Plataforma del sistema operativo instalado. • **Darwin_x86_64**: macOS 64 bits • **Win64NT**: Windows 64 bits • **Win32NT**: Windows 32 bits • **Linux_i686**: Linux 32 bits • **Linux_x86_64**: Linux 64 bits • **Win64ARM**: Windows para procesadores ARM	Enumeración

Tabla 7.2: descripción de los eventos generados en el proceso de instalación

Desinstalación de agentes

Para localizar los equipos que han desinstalado su agente en un periodo de tiempo dado acota la fecha y añade un filtro sobre el campo **op** para seleccionar todas las filas que tengan el string "Uninstall". Con esta operación se obtiene un listado de máquinas desinstaladas y por lo tanto vulnerables a las amenazas.

Monitoredopen

Esta tabla contiene los ficheros de datos accedidos por las aplicaciones ejecutadas en el equipo del usuario junto con los procesos que accedieron a los datos.

Nombre	Descripción	Valores
eventdate	Fecha de inserción del evento en el servidor Cytomic Insights.	Fecha
serverdate	Fecha del equipo del usuario cuando se generó el evento.	Fecha
date	Fecha del equipo del usuario cuando se generó el evento.	Fecha
machine	Nombre de la máquina del cliente.	Cadena de caracteres

Tabla 7.3: descripción de los eventos generados por los procesos monitorizados al acceder a ficheros de datos

Nombre	Descripción	Valores
machineIP	IP de la máquina del cliente.	Dirección IP
user	Nombre del usuario del proceso.	Cadena de caracteres
muid	Identificador interno del equipo del cliente.	Cadena de caracteres en formato: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
parentsHash	Digest / hash del fichero que accede a datos.	Cadena de caracteres.
parentPath	Ruta del proceso que accede a datos.	Cadena de caracteres
parentValidSig	Proceso que accede a datos firmado digitalmente.	Booleano
parentCompany	Contenido del atributo Company de los metadatos del fichero que accede a datos.	Cadena de caracteres
parentCat	Categoría del fichero que accede a datos.	• Goodware • Malware • PUP • Unknown • Monitoring
parentMWName	Nombre del malware si el fichero que accede a datos está catalogado como una amenaza.	Cadena de caracteres (Null si el elemento no es Malware)
childPath	Nombre del fichero de datos accedido por el proceso. Por defecto solo se indica la extensión del fichero para preservar la privacidad de datos del cliente.	Cadena de caracteres
loggedUser	Usuario logueado en el equipo en el momento del acceso del fichero.	Cadena de caracteres
firstParentCat	Primera clasificación emitida del fichero padre que realizó la operación registrada.	• Goodware • Malware • PUP • Unknown • Monitoring • Null

Tabla 7.3: descripción de los eventos generados por los procesos monitorizados al acceder a ficheros de datos

Acceso a documentos de usuario

Esta tabla muestra el acceso a ficheros de todos los procesos que se ejecutan en el equipo del usuario por lo que permite localizar una fuga de información en caso de infección.

Filtra por el campo **parentCat** para discriminar el goodware del resto de posibilidades para obtener un listado de accesos a ficheros de datos por parte de procesos sin clasificar o clasificados como malware, con lo que se visualiza el impacto de la fuga de datos.

MonitoredRegistry

Esta tabla contiene todos los eventos de monitorización del registro relativos a cambios o accesos relacionados con permisos, contraseñas, almacenes de certificados y otros.

Nombre	Descripción	Valores
eventdate	Fecha de inserción del evento en el servidor Cytomic Insights.	Fecha
date	Fecha del equipo del usuario cuando se generó el evento.	Fecha
machine	Nombre de la máquina del cliente.	Cadena de caracteres
machineIP	IP de la máquina del cliente.	Dirección IP
user	Nombre de usuario del proceso que accedió o modificó el registro.	Cadena de caracteres
muid	Identificador interno del equipo del cliente.	Cadena de caracteres en formato: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxx
parentHash	Digest / hash del proceso que accedió o modificó el registro.	Cadena de caracteres
parentPath	Ruta del ejecutable que accedió o modificó el registro.	Cadena de caracteres
parentValidSig	Proceso que accede al registro firmado digitalmente.	Booleano
parentCompany	Contenido del atributo Company de los metadatos del proceso que accede al registro.	Cadena de caracteres
parentCat	Categoría del proceso.	• Goodware • Malware • PUP • Unknown • Monitoring
parentMwName	Nombre del malware si el proceso está catalogado como una amenaza.	Cadena de caracteres (Null si el elemento no es Malware)
regAction	Operación realizada sobre el registro del equipo.	• CreateKey • CreateValue • ModifyValue
key	Rama o clave del registro afectada.	Cadena de caracteres

Tabla 7.4: descripción de los eventos generados por los procesos monitorizados al acceder al registro

Nombre	Descripción	Valores
Value	Nombre del valor afectado dentro de la clave.	Cadena de caracteres
valueData	Contenido del valor.	Cadena de caracteres
loggedUser	Usuario logueado en el equipo en el momento del acceso al registro.	Cadena de caracteres
firstParentCat	Primera clasificación emitida del fichero padre que realizó la operación registrada.	• Goodware • Malware • PUP • Unknown • Monitoring • Null

Tabla 7.4: descripción de los eventos generados por los procesos monitorizados al acceder al registro

Notblocked

Esta tabla incluye un registro por cada elemento que Cytomic EDR ha dejado pasar sin analizar debido a situaciones excepcionales como tiempo de arranque del servicio en el agente, cambios de configuración, etc.

Nombre	Descripción	Valores
eventdate	Fecha de inserción del evento en el servidor Cytomic Insights.	Fecha
date	Fecha del equipo del usuario cuando se generó el evento.	Fecha
machine	Nombre de la máquina del cliente.	Cadena de caracteres
machineIP	IP de la máquina del cliente.	Dirección IP
user	Nombre de usuario del proceso.	Cadena de caracteres
muid	Identificador interno del equipo del cliente.	Cadena de caracteres en formato: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
parentHash	Digest / hash del fichero padre.	Cadena de caracteres
parentPath	Ruta del proceso padre.	Cadena de caracteres

Tabla 7.5: descripción de los eventos generados por los elementos no monitorizados

Nombre	Descripción	Valores
parentValidSig	Proceso padre firmado digitalmente.	Booleano
parentCompany	Contenido del atributo Company de los metadatos del proceso padre.	Cadena de caracteres
parentCat	Categoría del fichero padre.	• Goodware • Malware • PUP • Unknown • Monitoring
ParentMwName	Nombre del Malware si el fichero padre está catalogado como una amenaza.	Cadena de caracteres (Null si el elemento no es Malware)
childHash	Digest / hash del fichero hijo.	Cadena de caracteres
childPath	Ruta del proceso hijo.	Cadena de caracteres
childValidSig	Proceso hijo firmado digitalmente.	Booleano
childCompany	Contenido del atributo Company de los metadatos del proceso hijo.	Cadena de caracteres
childCat	Categoría del proceso hijo.	• Goodware • Malware • PUP • Unknown • Monitoring
childMwName	Nombre del malware si el fichero hijo está catalogado como una amenaza.	Cadena de caracteres (Null si el elemento no es Malware)
firstParentCat	Primera clasificación emitida del fichero padre que realizó la operación registrada.	• Goodware • Malware • PUP • Unknown • Monitoring • Null
firstChildCat	Primera clasificación emitida del fichero hijo que realizó la operación registrada.	• Goodware • Malware • PUP • Unknown • Monitoring • Null

Tabla 7.5: descripción de los eventos generados por los elementos no monitorizados

Ops

Esta tabla contiene un registro de todas las operaciones realizadas por los procesos vistos en la red del cliente.

Nombre	Descripción	Valores
eventdate	Fecha de inserción del evento en el servidor Cytomic Insights.	Fecha
serverdate	Fecha del equipo del usuario cuando se generó el evento.	Fecha
machine	Nombre de la máquina del cliente.	Cadena de caracteres
machineIP	IP de la máquina del cliente.	Dirección IP
user	Nombre de usuario del proceso.	Cadena de caracteres
op	Operación realizada.	• CreateDir • Exec • CreatePE • DeletePE • LoadLib • OpenCmp • RenamePE • CreateCmp
muid	Identificador único del equipo.	Cadena de caracteres en formato: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
parentHash	Digest / hash del fichero padre.	Cadena de caracteres
parentDriveType	Tipo de unidad donde reside el proceso padre.	• Fixed • Remote • Removable
parentPath	Ruta del proceso padre.	Cadena de caracteres
parentValidSig	Proceso padre firmado digitalmente.	Booleano
parentCompany	Contenido del atributo Company de los metadatos del fichero padre.	Cadena de caracteres

Tabla 7.6: descripción de los eventos generados por los procesos monitorizados

Nombre	Descripción	Valores
parentCat	Categoría de fichero padre.	• Goodware • Malware • PUP • Unknown • Monitoring
parentMwName	Nombre del malware encontrado en el fichero padre.	Cadena de caracteres (Null si el elemento no es Malware)
childHash	Digest / hash del fichero hijo.	Cadena de caracteres
childDrive Type	Tipo de unidad donde reside el proceso hijo.	• Fixed • Remote • Removable
childPath	Ruta del proceso hijo.	Cadena de caracteres
childValidSig	Proceso hijo firmado digitalmente.	Booleano
childCompany	Contenido del atributo Company de los metadatos del fichero hijo.	Cadena de caracteres
childCat	Categoría del fichero hijo.	• Goodware • Malware • PUP • Unknown • Monitoring
childMwName	Nombre del malware encontrado en el fichero hijo.	Cadena de caracteres (Null si el elemento no es Malware)
OcsExec	Se ejecutó o no software considerado como vulnerable.	Booleano
OcsName	Nombre del software considerado vulnerable.	Cadena de caracteres
OcsVer	Versión del software considerado vulnerable.	Cadena de caracteres
action	Acción realizada.	• Allow • Block • BlockTimeout • BlockIP

Tabla 7.6: descripción de los eventos generados por los procesos monitorizados

Nombre	Descripción	Valores
serviceLevel	Modo del agente. • **Learning**: el agente permite la ejecución de los procesos no conocidos. • **Hardening**: el agente impide la ejecución de los procesos clasificados como amenazas. • **Block**: el agente impide la ejecución de los procesos clasificados como amenazas y de los procesos desconocidos.	Enumeración
params	Parámetros de ejecución del proceso en la linea de comandos.	Cadena de caracteres.
firstParenCat	Primera clasificación emitida del fichero padre que realizó la operación registrada.	• Goodware • Malware • PUP • Unknown • Monitoring • Null
firstChildCat	Primera clasificación emitida del fichero hijo que realizó la operación registrada.	• Goodware • Malware • PUP • Unknown • Monitoring • Null

Tabla 7.6: descripción de los eventos generados por los procesos monitorizados

ProcessNetBytes

Esta tabla contiene un registro de los consumos de datos realizados por los procesos vistos en la red del cliente. Se envía un registro por proceso cada cuatro horas aproximadamente con la suma de datos transferida desde el último envío del registro. El total de bytes enviados y recibidos por proceso será la suma de todas las cantidades recibidas.

Nombre	Descripción	Valores
eventdate	Fecha de inserción del evento en el servidor Cytomic Insights.	Fecha
serverdate	Fecha del equipo del usuario cuando se generó el evento.	Fecha
machineName	Nombre de la máquina del cliente.	Cadena de caracteres

Tabla 7.7: descripción de los eventos generados por el tráfico de red generado los procesos

Nombre	Descripción	Valores
machineIP	IP de la máquina del cliente.	Dirección IP
user	Nombre del usuario del proceso.	Cadena de caracteres
muid	Identificador único del equipo.	Cadena de caracteres en formato: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
hash	Digest / hash del proceso.	Cadena de caracteres
path	Ruta y nombre del programa.	Cadena de caracteres
bytesSent	Número de bytes enviados por el proceso desde el ultimo evento generado.	Numérico
bytesReceived	Número de bytes recibidos por el proceso desde el ultimo evento generado.	Numérico

Tabla 7.7: descripción de los eventos generados por el tráfico de red generado los procesos

Representación gráfica de las aplicaciones con mayor uso de datos

El uso más habitual de esta tabla es el de localizar aquellos programas dentro de los equipos de la red del cliente que producen un mayor consumo de datos. Es importante resaltar que en esta tabla no se distingue el consumo de datos interno del externo, de esta forma el consumo total de los procesos podrá ser una mezcla de datos pedidos al exterior vía internet, y datos consumidos de servidores internos a la empresa (servidores de correo, servidores web de una intranet, compartición de ficheros entre puestos de trabajo, etc.).

Para poder determinar de forma fácil las aplicaciones de la red con mayor consumo de datos se va a pintar un gráfico de tipo Voronoi con los datos de consumo (recepción) de datos por aplicación ejecutada en el parque informático del cliente.

1. Extracción del nombre del programa ejecutado.

Dado que el nombre de las aplicaciones ejecutadas se registra en el campo Path con su ruta completa extrae el nombre de la aplicación. Para ello crea una nueva columna de nombre **PreNombrePrograma** con la función **Substitute All** añadiendo los parámetros siguientes:

- **String to scan**: columna Path.
- **Regular Expresion**: (.*\\)

- **Template**: (vacio).

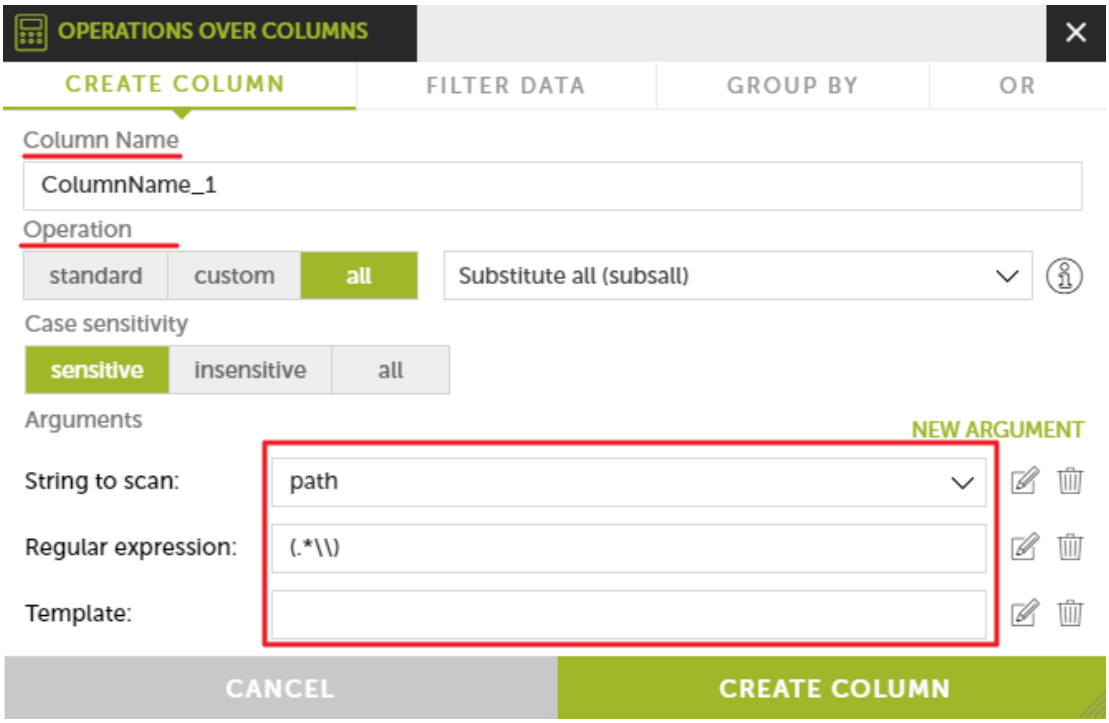

Figura 7.11: herramienta para crear una nueva columna

Acto seguido filtra por **null** para evitar el procesado de entradas erróneas y crea otra columna **NombrePrograma** con la función **Lower Case** sobre la columna creada anteriormente **PreNombrePrograma**. De esta forma obtendremos los nombres de los programas ejecutados en minúsculas y sin errores.

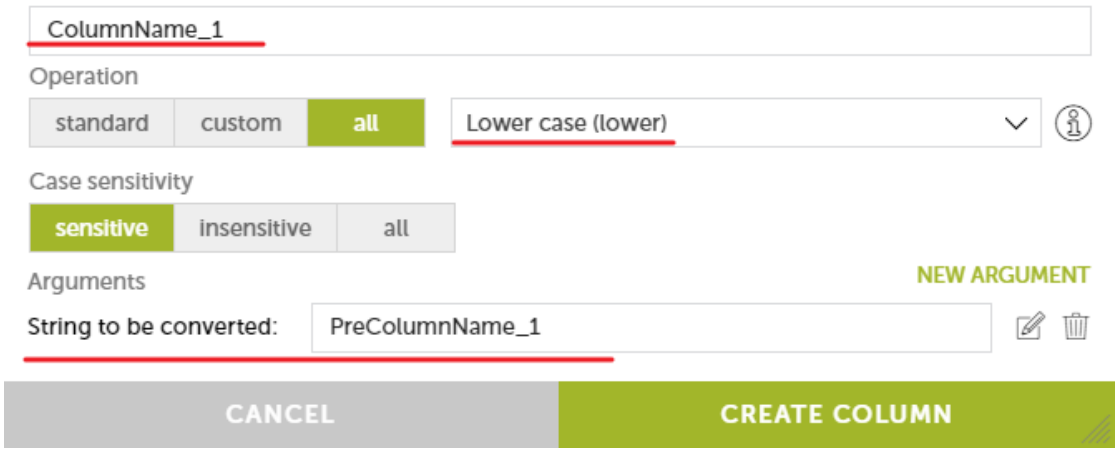

Figura 7.12: herramienta para crear una nueva columna

Otro enfoque sería utilizar el campo **hash** de la tabla para identificar los procesos en ejecución. Este enfoque sin embargo puede resultar en un número de procesos únicos mayor ya que diferentes versiones de un mismo programa tienen hashes distintos, dificultando la lectura del gráfico presentado en el último paso.

2. Agregar una agrupación diaria.

Dependiendo del número de días a tratar añade una agrupación (en el ejemplo es diaria) junto con el campo **NombrePrograma**.

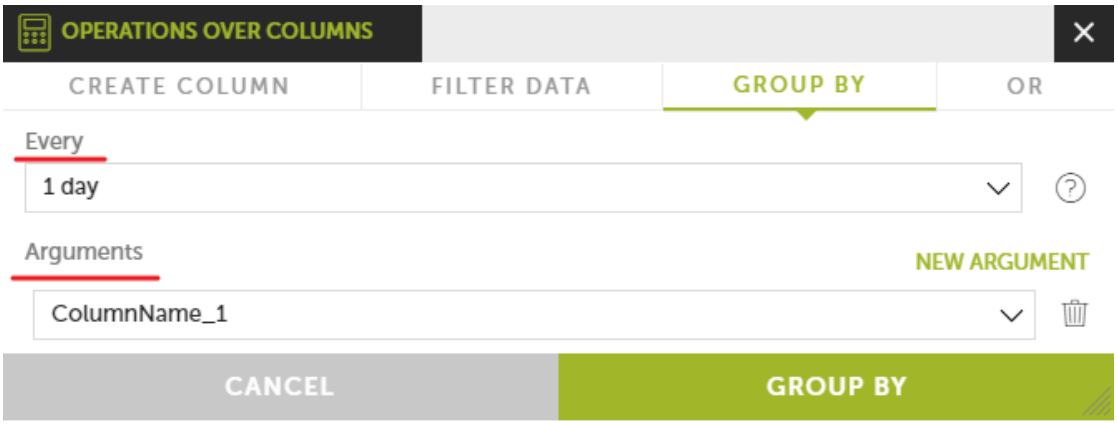

Figura 7.13: herramienta para crear una nueva agrupación

3. Agregar función de suma.

Añade el total de cada proceso añadiendo una función de suma sobre el campo **bytesReceived**.

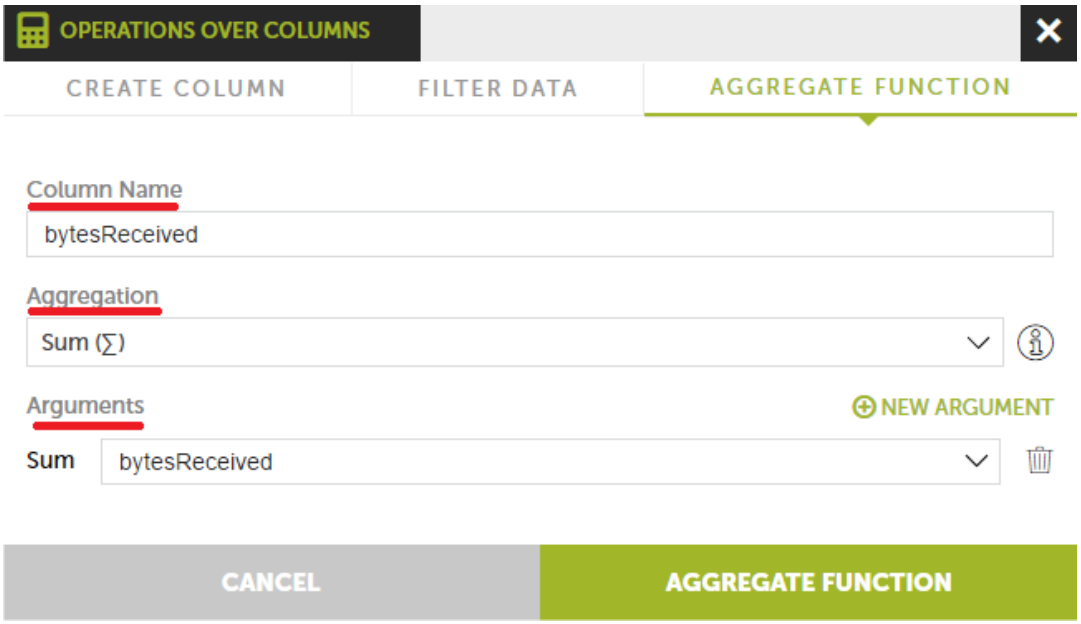

Figura 7.14: herramienta para crear operaciones sobre columnas

4. Filtro de corte.

Con el objetivo de mostrar solo los procesos que han consumido más de una determinada cantidad y simplificar el gráfico filtra los resultados por una cantidad, 100 Mbytes en el ejemplo (104857600 bytes).

5. Creación del grafico Voronoi.

En el apartado **Signals** arrastra el campo **NombrePrograma** y en el campo **Value** el campo **bytesReceived**.

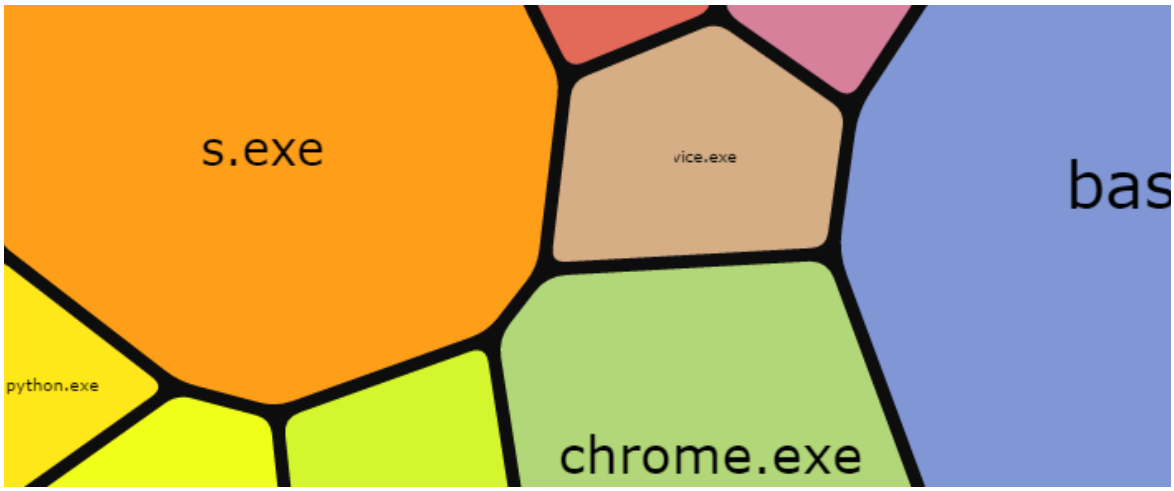

Figura 7.15: gráfico Voronoi resultante

Registry

Esta tabla contiene una lista de todas las operaciones realizadas sobre las ramas del registro utilizadas por los programas para ganar persistencia y sobrevivir a un reinicio del equipo.

Nombre	Descripción	Valores
eventdate	Fecha de inserción del evento en el servidor Cytomic Insights.	Fecha
serverdate	Fecha del equipo del usuario cuando se generó el evento.	Fecha
machine	Nombre de la máquina del cliente.	Cadena de caracteres
machineIP	IP de la máquina del cliente.	Dirección IP
user	Nombre de usuario del proceso que modificó el registro.	Cadena de caracteres
op	Operación realizada sobre el registro del equipo.	• ModifyExeKey • CreateExeKey
hash	Digest / hash del proceso que realiza la modificación en registro.	Cadena de caracteres
muid	Identificador único del equipo.	Cadena de caracteres en formato: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

Tabla 7.8: descripción de los eventos generados por los procesos que modifican las ramas del registro para ganar persistencia

Nombre	Descripción	Valores
targetPath	Ruta del ejecutable apuntado en el registro.	Tipo de unidad donde reside el proceso que realiza el hook
regKey	Clave de registro.	Cadena de caracteres
driveType	Tipo de unidad donde reside el proceso que accede al registro.	Cadena de caracteres
path	Ruta del proceso que modifica el registro.	Cadena de caracteres
validSig	Clave de registro.	Booleano
company	Clave de registro.	Cadena de caracteres
cat	Categoría del proceso.	• Goodware • Malware • PUP • Unknown • Monitoring
mwName	Nombre del malware si el proceso está catalogado como una amenaza.	Cadena de caracteres (Null si el elemento no es Malware)
firstCat	Categoría del proceso la primera vez que se clasificó.	• Goodware • Malware • PUP • Unknown • Monitoring

Tabla 7.8: descripción de los eventos generados por los procesos que modifican las ramas del registro para ganar persistencia

Persistencia de las amenazas instaladas

En esta tabla se muestra el acceso al registro de todos los procesos que se ejecutan en el equipo del usuario cuando afectan a las ramas que son leídas en el inicio del sistema como parte del proceso de carga del sistema operativo. Modificando estas ramas el malware se garantiza la ejecución aunque la maquina se reinicie.

Las ramas del registro que invocan a un programa en el arranque son múltiples pero las más utilizadas por troyanos y otros tipos de amenazas son:

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run

HKLM\Software\Microsoft\Windows\CurrentVersion\Run

HKCU\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run

HKLM\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\Run

HKCU\Software\Microsoft\Windows\CurrentVersion\RunOnceEx

HKLM\Software\Microsoft\Windows\CurrentVersion\RunOnceEx
```

Socket

Esta tabla contiene un registro de todas las operaciones de red realizadas por los procesos vistos en la red del cliente.

Nombre	Descripción	Valores
eventdate	Fecha de inserción del evento en el servidor Cytomic Insights.	Fecha
serverdate	Fecha del equipo del usuario cuando se generó el evento.	Fecha
machine	Nombre de la máquina del cliente.	Cadena de caracteres
machineIP	Ip de la máquina del cliente.	Dirección IP
user	Nombre del usuario del proceso.	Cadena de caracteres
hash	Digest / hash del proceso que realiza la conexión.	Cadena de caracteres
driveType	Tipo de unidad donde reside el proceso que realiza la conexión.	• Fixed • Remote • Removable
path	Ruta del proceso que realiza la conexión.	Cadena de caracteres
protocol	Protocolo de comunicaciones utilizado por el proceso.	• TCP • UDP • ICMP • ICMPv6 • IGMP • RF

Tabla 7.9: descripción de los eventos generados por los procesos que utilizan la red

Nombre	Descripción	Valores
remotePort	Puerto destino al que se comunica el proceso.	0-65535
direction	Sentido de la comunicación.	• Upload • Download • Bidirectional • Unknown
remoteIP	Ip destino.	Dirección IP
localPort	Puerto origen.	0-65535
localIP	Ip origen.	Dirección IP
validSig	Fichero que realiza la conexión firmado digitalemente.	Booleano
company	Contenido.	Cadena de caracteres
category	Categoría actual del proceso que realiza la conexión.	• Goodware • Malware • PUP • Unknown • Monitoring
mwName	Nombre del malware si el proceso que realiza la conexión está catalogado como una amenaza.	Cadena de caracteres (Null si el elemento no es Malware)
firstCategory	Categoría del proceso la primera vez que se clasificó.	• Goodware • Malware • PUP • Unknown • Monitoring
times	Número de veces que se ha producido el mismo evento de comunicación en la última hora. Para que dos eventos de comunicación se consideren iguales es necesario que coincidan los siguientes parámetros, teniendo en cuenta la dirección de la comunicación: • El nombre del proceso. • La dirección IP local del proceso. • La ruta del proceso. • La dirección IP de destino de la comunicación. • El puerto destino de la comunicación.	Numérico

Tabla 7.9: descripción de los eventos generados por los procesos que utilizan la red

Nombre	Descripción	Valores
	Con cada primera comunicación diferente registrada se envía un evento con el campo times a 1. Posteriormente, por cada hora transcurrida desde el primer evento, el campo times indicará el numero de eventos de comunicación iguales menos 1 producidos en ese intervalo, con la fecha del último evento registrado.	

Tabla 7.9: descripción de los eventos generados por los procesos que utilizan la red

Programas que más se conectan al exterior

Se puede obtener una gráfica con los destinos más conectados por el software lícito que se ejecuta en los equipos. Para ello hay que seguir los siguientes pasos:

1. Añade un filtro que elimine todos los programas que no sean considerados lícitos. Para ello iguala el campo Cat a la cadena "Goodware".
2. Añade un filtro que elimine todas las conexiones de destino a direcciones IP privadas. Para ello crea una columna con la función Is Public IPv4 sobre el campo dstIp, tal y como se muestra en la figura.

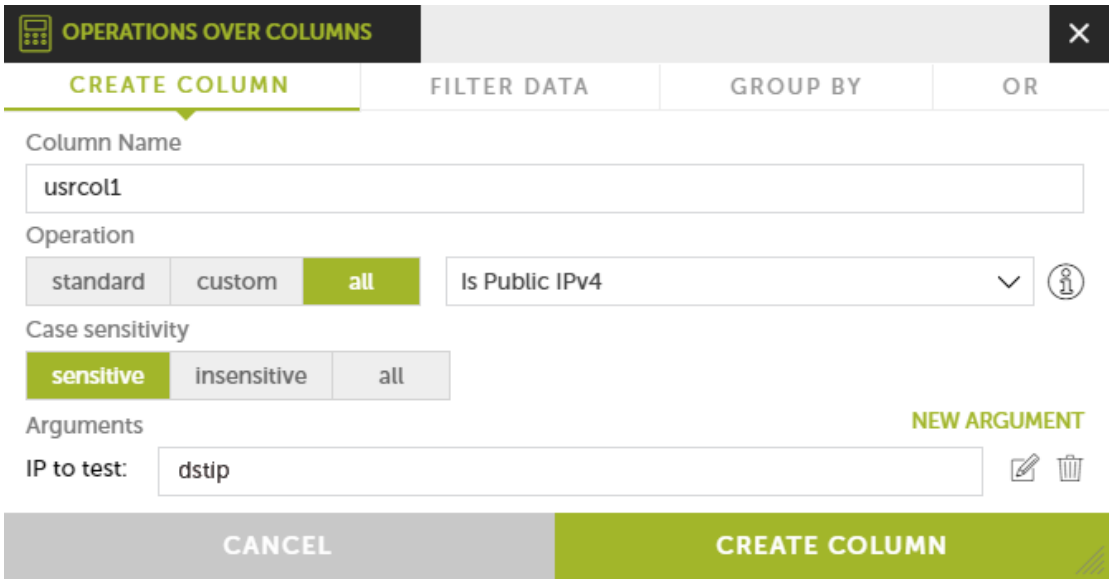

Figura 7.16: herramienta para añadir un filtro de datos

3. Añade columnas **latitude** y **longitude** que extraigan del campo **dstIP** la longitud y la latitud con las

funciones **Geolocated Latitude / Longitude**.

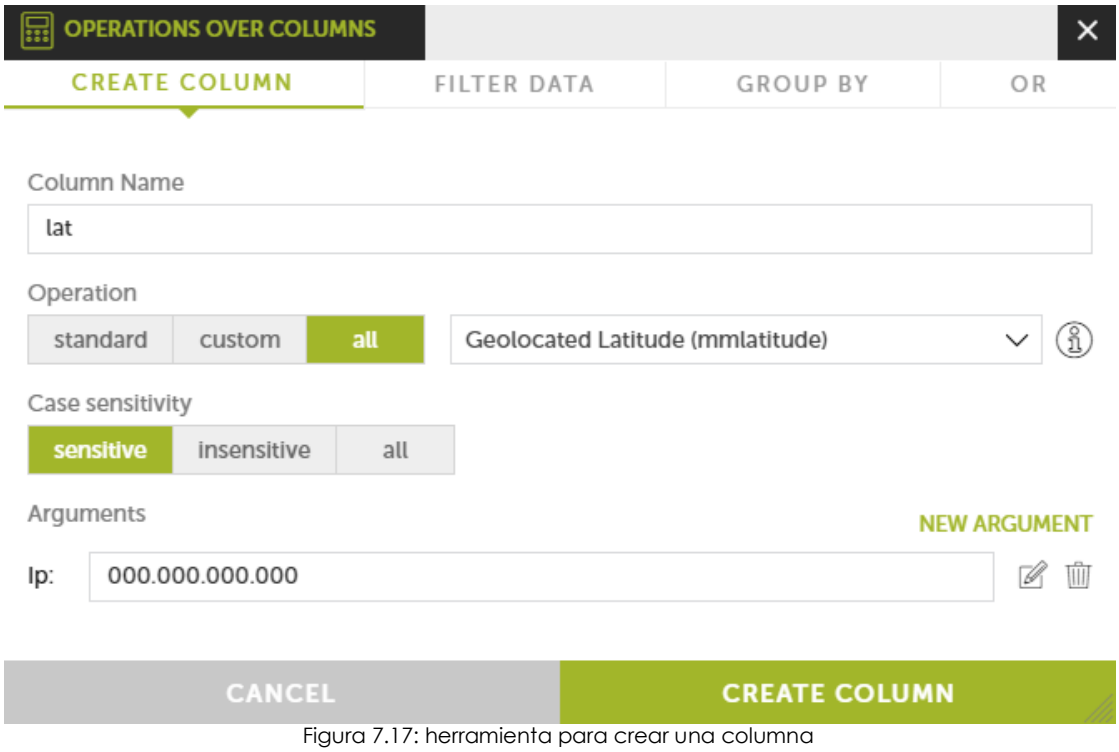

Figura 7.17: herramienta para crear una columna

En este punto del procedimiento tendras un listado de conexiones desde software legítimo hacia direcciones IP públicas y la latitud y longitud de cada IP. Las coordenadas obtenidas se representaran en la gráfica de tipo mapa como puntos.

Puesto que se quiere representar el número de conexiones a una misma dirección IP será necesario realizar una agrupación y añadir un contador para obtener el número de direcciones IP repetidas en una agrupación.

4. Añade una agrupación por el campo de la tabla dstIP y los campos de nueva creación **latitude** y

longitude, sin límite temporal.

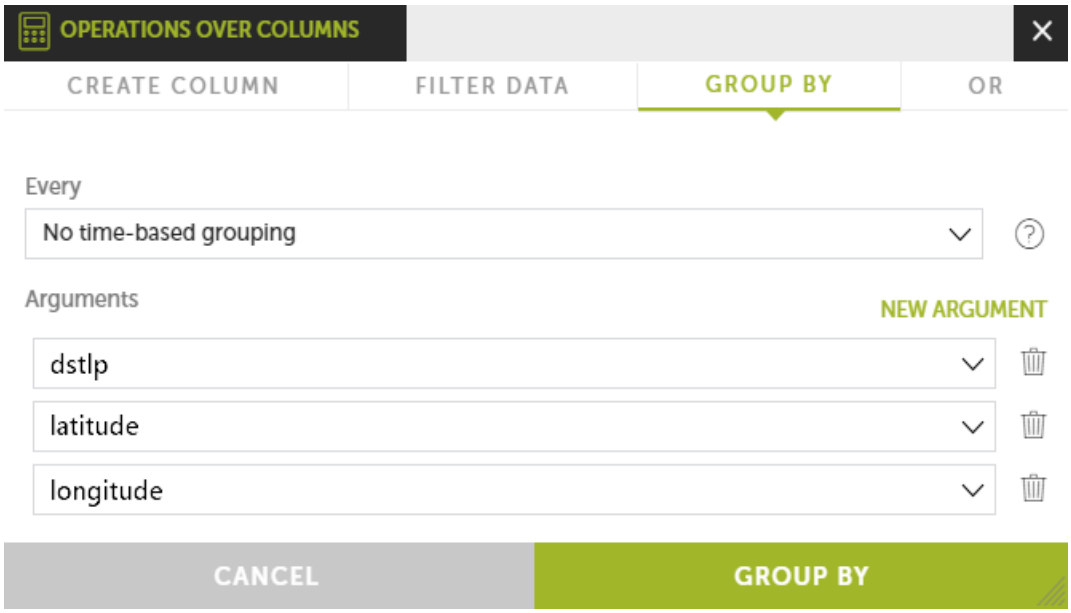

Figura 7.18: herramienta para crear una agrupación de datos

5. Agrega una función de tipo contador.
6. Añade una gráfica de tipo **Flat world map by coordinates** o **Google heat map** utilizando como datos las columnas count, latitude y longitude.

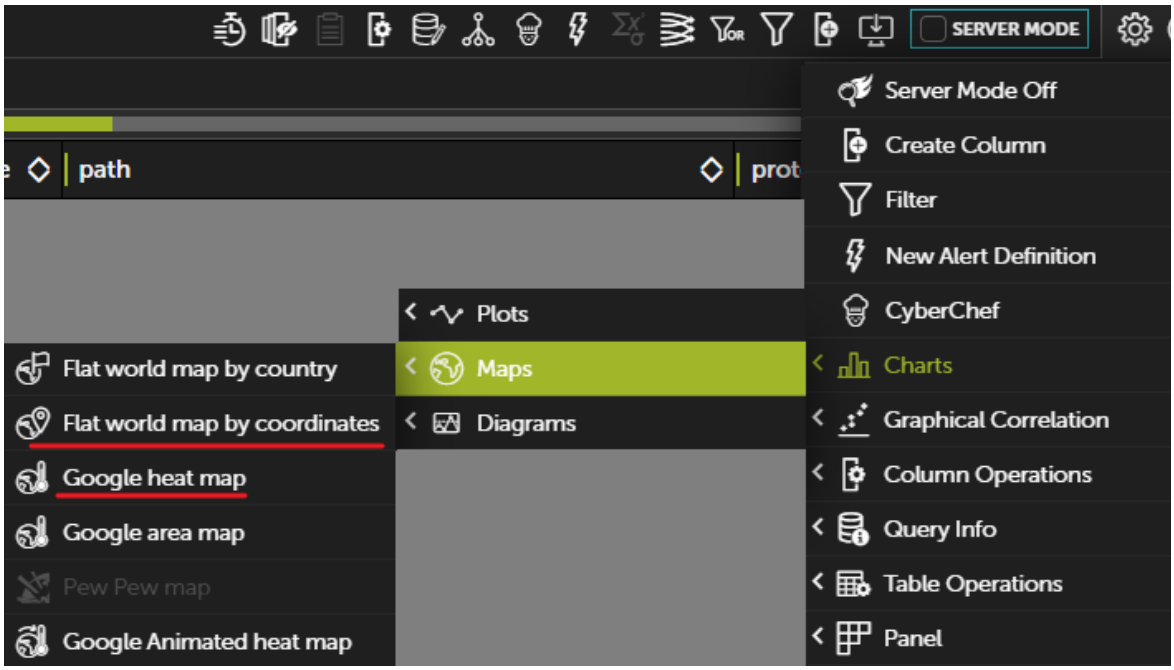

Figura 7.19: acceso a la creación de gráficas

Al arrastrar las columnas a las casillas indicadas se mostrará el mapa elegido con los datos representados por puntos de diversos colores y tamaños.

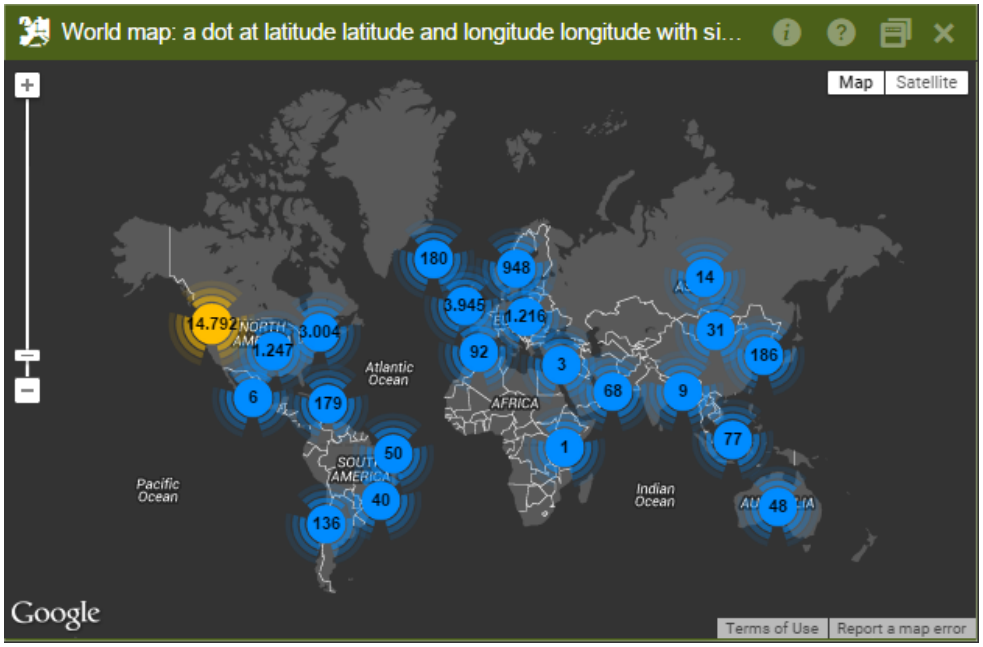

Figura 7.20: gráfica mapa del mundo resultante

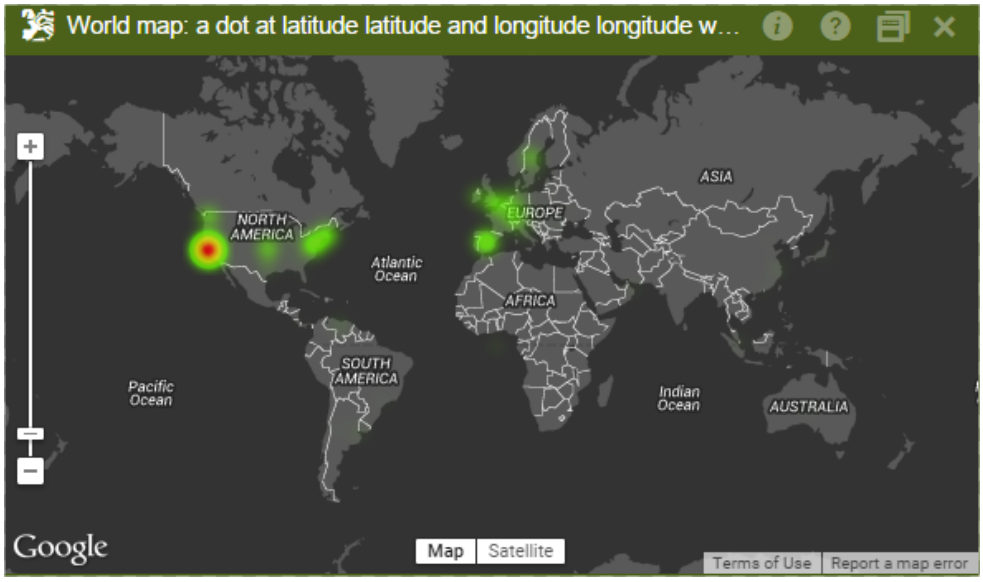

Figura 7.21: gráfica mapa del mundo resultante

ToastBlocked

Esta tabla contiene un registro por cada proceso bloqueado debido a que Cytomic EDR todavía no ha emitido una clasificación del mismo.

Nombre	Descripción	Valores
eventdate	Fecha de inserción del evento en el servidor Cytomic Insights.	Fecha
severdate	Fecha del equipo del usuario cuando se generó el evento.	Fecha
machineName	Nombre de la máquina del cliente.	Cadena de caracteres
machineIP	Ip de la máquina del cliente.	Dirección IP
user	Nombre del usuario del proceso.	Cadena de caracteres
muid	Identificador único del equipo.	Cadena de caracteres en formato: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
hash	Digest / hash del proceso que generó el mensaje emergente.	Cadena de caracteres
path	Ruta del proceso que generó el mensaje emergente.	Cadena de caracteres
toastBlockReason	Motivo de bloqueo: • **0**: Bloqueo por unk en modo bloqueo • **1**: Bloqueo por regla de blockunk • **2**: Bloqueo por regla de "vino del exterior" • **3**: Bloqueo por regla de contexto • **4**: Bloqueo por exploit • **5**: Bloqueo por pregunta de kill de proceso	Enumeración
toastResult	Resultado del mensaje emergente: • **0 Ok**: el cliente acepta el mensaje • **1 Timeout**: la tostada desaparece por la no acción del usuario • **2 Angry**: el usuario rechaza el bloqueo • **3 Block**. • **4 Allow**. • **5 BadCall**	Enumeración

Tabla 7.10: descripción de los eventos de bloqueo por resultar desconocido el proceso ejecutado

URLdownload

Esta tabla contiene información sobre las operaciones de descarga de datos por HTTP realizadas por los procesos vistos en la red del cliente (URL, datos de los ficheros descargados, equipos que las realizaron, etc.).

Nombre	Descripción	Valores
eventdate	Fecha de inserción del evento en el servidor Cytomic Insights.	Fecha
severdate	Fecha del equipo del usuario cuando se generó el evento.	Fecha
machine	Nombre de la máquina del cliente.	Cadena de caracteres
machineIP	Ip de la máquina del cliente.	Dirección IP
user	Nombre del usuario del proceso.	Cadena de caracteres
url	URL de descarga.	Recurso URL
parentHash	Digest / hash del proceso que descarga el fichero.	Cadena de caracteres
muid	Identificador interno del equipo del cliente.	Cadena de caracteres en formato: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
parentDriveType	Tipo de unidad donde reside el proceso que descarga el fichero.	• Fixed • Remote • Removable
parentPath	Ruta del proceso que descarga el fichero.	Cadena de caracteres
parentValidSig	Proceso que descarga el fichero firmado digitalmente.	Booleano
parentCompany	Contenido del atributo Company de los metadatos del proceso que descarga el fichero.	Cadena de caracteres
parentCat	Categoría del proceso que descarga el fichero.	• Goodware • Malware • PUP • Unknown • Monitoring
parentMwName	Nombre del Malware si el proceso que descarga el fichero está catalogado como una amenaza.	Cadena de caracteres (Null si el elemento no es Malware)

Tabla 7.11: descripción de los ficheros descargados por los procesos mediante HTTP

Nombre	Descripción	Valores
childHash	Digest / hash del fichero descargado.	Cadena de caracteres
childDriveType	Tipo de unidad donde reside el proceso que realiza la conexión.	• Fixed • Remote. • Removable
childPath	Ruta del fichero descargado.	Cadena de caracteres
childValidSig	Fichero descargado firmado digitalmente.	Booleano
childCompany	Contenido del atributo Company de los metadatos del fichero descargado.	Cadena de caracteres
childCat	Categoría del fichero descargado.	• Goodware • Malware • PUP. • Unknown • Monitoring
chilMwName	Nombre del Malware si el fichero descargado está catalogado como una amenaza.	Cadena de caracteres (Null si el elemento no es Malware)
firstParentCat	Primera clasificación emitida del fichero padre que realizó la operación registrada.	• Goodware • Malware • PUP • Unknown • Monitoring • Null
firstChildCat	Primera clasificación emitida del fichero hijo que realizó la operación registrada.	• Goodware • Malware • PUP • Unknown • Monitoring • Null

Tabla 7.11: descripción de los ficheros descargados por los procesos mediante HTTP

Esta tabla muestra todas las descargas de los usuarios de la red independientemente de que sean malware o goodware. Además de filtrar la información de la descarga, también es posible visualizar de forma gráfica los dominios que reciben más descargas.

Dominios que reciben más descargas

Para mostrar este tipo de información es necesario manipular el contenido del campo url para limpiar la parte del string que no nos interesa y conservar la parte del dominio.

1. Crea una columna nueva con la operación **Split** sobre el campo url.

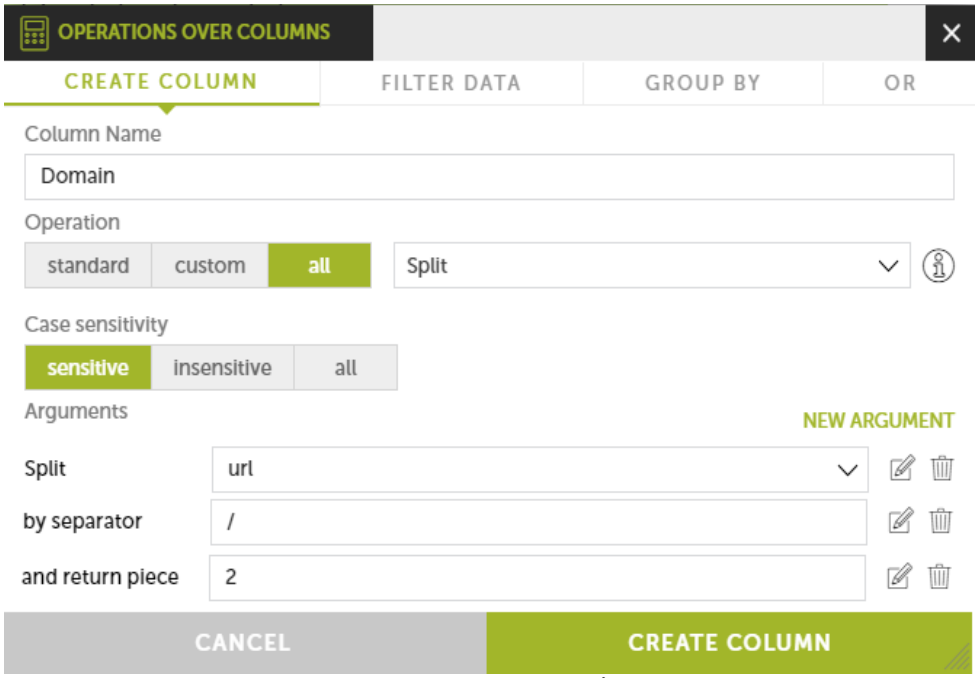

Figura 7.22: herramienta para la creación de una columna

2. Agrupa por **url** diferente sin marcar agrupación temporal.

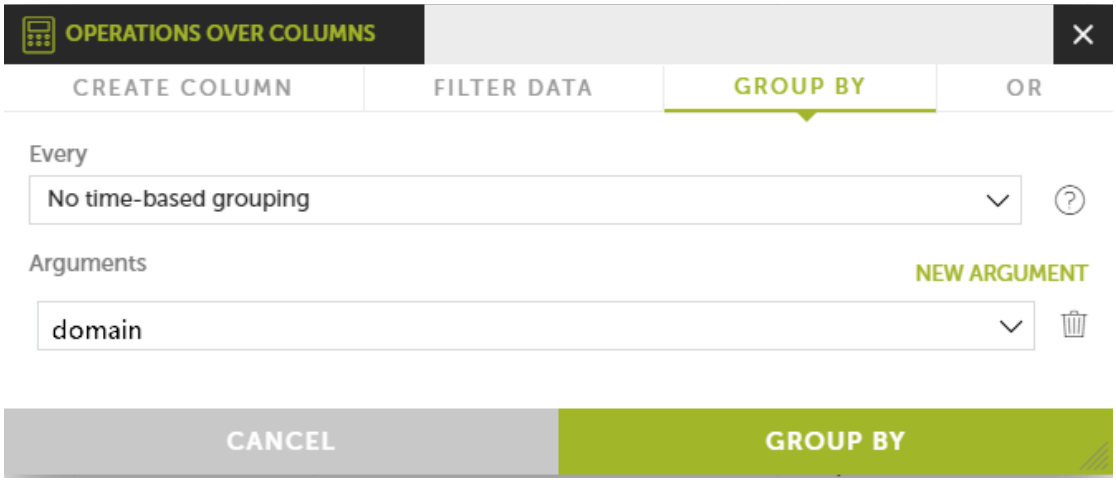

Figura 7.23: herramienta para creación de una agrupación de datos

3. Añade una columna agregación de tipo contador.

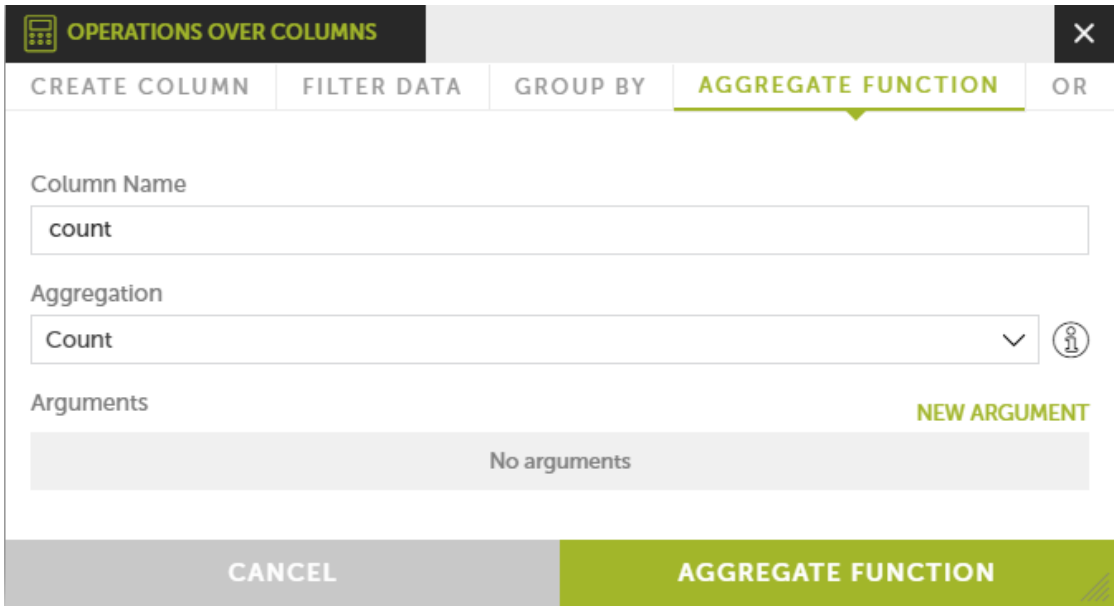

Figura 7.24: herramienta para agregar una operación sobre columnas

De esta forma se obtiene un listado por dominio agrupado y el número de ocurrencias de cada dominio dentro de cada grupo. Con esta información se obtiene una gráfica con los dominios más visitados para descarga.

Los datos se muestran, en este caso, con una gráfica de tarta. Filtra las agrupaciones de o menos ocurrencias para poder fijar con más detalle en el resto de dominios.

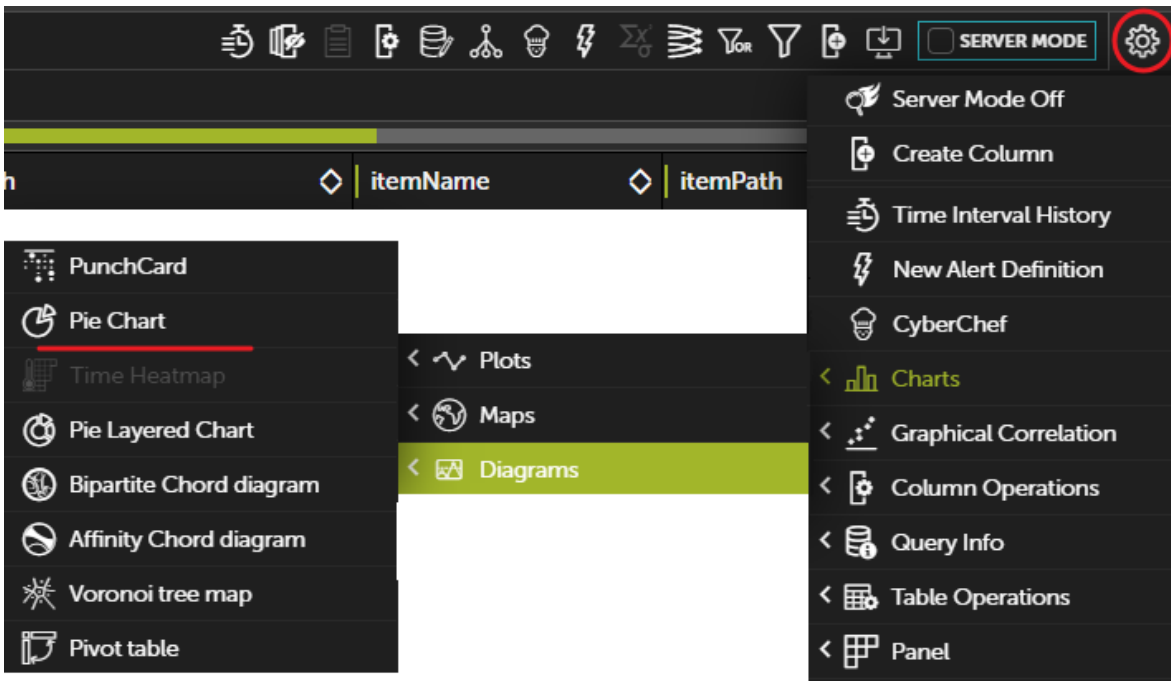

Figura 7.25: acceso a la creación de gráficas

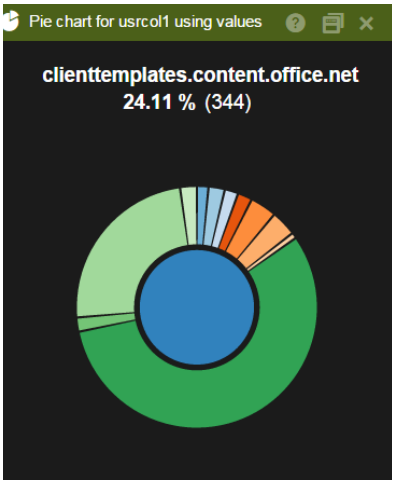

Figura 7.26: gráfica resultante

En las gráficas de tipo tarta las diferentes secciones son activas y al pasar el ratón por encima muestran los porcentajes y el nombre de la serie representada.

- **Otra información útil**

De la misma manera se pueden conjugar otros campos para enriquecer o filtrar los listados y conseguir unas tablas más afinadas. De esta forma se puede utilizar:

• **Machine** o **machineIP**: agrupando por estos campos se pueden ver los equipos de la red del cliente que más descargas inician.

• **ParentCat** y **ChildCat**: filtrando por este campo se puede despejar la tabla y mostrar únicamente lo que está catalogado como malware. De esta forma se pueden obtener dominios considerados como emisores de malware para bloquearlos en un cortafuegos que permita análisis en la capa 7.

VulnerableAppsFound

Esta tabla contiene un registro de todas las aplicaciones vulnerables detectadas en cada equipo de la red del cliente. A diferencia de la tabla Ops donde se muestra la ejecución de aplicaciones vulnerables mediante los campos ocsExec, ocsName y ocsVer, en esta tabla aparecen todas las aplicaciones vulnerables que residen en el equipo.

Una vez al día se envía un registro por cada aplicación detectada. Si la aplicación se borra el evento dejará de enviarse.

Nombre	Descripción	Valores
eventdate	Fecha de inserción del evento en el servidor Cytomic Insights.	Fecha
serverdate	Fecha del equipo del usuario cuando se generó el evento.	Fecha
muid	Identificador interno del equipo del cliente.	Cadena de caracteres en formato: xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx
machineName	Nombre de la máquina del cliente	Cadena de caracteres
machineIP	Ip de la máquina del cliente.	Dirección IP
criticalSoftEventType	Indica la presencia de software vulnerable.	Present

Tabla 7.12: descripción de las aplicaciones vulnerables encontradas

Nombre	Descripción	Valores
itemHash	Digest del programa vulnerable encontrado en el equipo.	Cadena de caracteres
fileName	Nombre del fichero vulnerable.	Cadena de caracteres
filePath	Ruta completa done se encuentra el fichero vulnerable.	Cadena de caracteres
internalName	Contenido del atributo Name de los metadatos del fichero vulnerable.	Cadena de caracteres
companyName	Contenido del atributo Company de los metadatos del fichero vulnerable.	Cadena de caracteres
fileVersion	Contenido del atributo Version de los metadatos del fichero vulnerable.	Cadena de caracteres
productVersion	Contenido del atributo ProductVersion de los metadatos del fichero vulnerable.	Cadena de caracteres

Tabla 7.12: descripción de las aplicaciones vulnerables encontradas

Equipos con mayor número de aplicaciones vulnerables

Un ejemplo típico de esta tabla es determinar los equipos de la red que tienen un mayor número de aplicaciones vulnerables.

En este ejemplo no se distingue si la aplicación está instalada o simplemente está copiada en el disco duro del equipo. También hay que tener en cuenta que una misma aplicación copiada 'n' veces en un mismo equipo no contará únicamente como uno, sino como 'n'.

1. Agregar una agrupación con periodo 1 día.

Como los eventos de software vulnerable se generan diariamente, agrupa todas las filas con un intervalo de un día añadiendo el campo **machineName** de la tabla como argumento. Sin embargo

hay que tener en cuenta que los equipos que no hayan sido conectados ese día no habrán generado eventos.

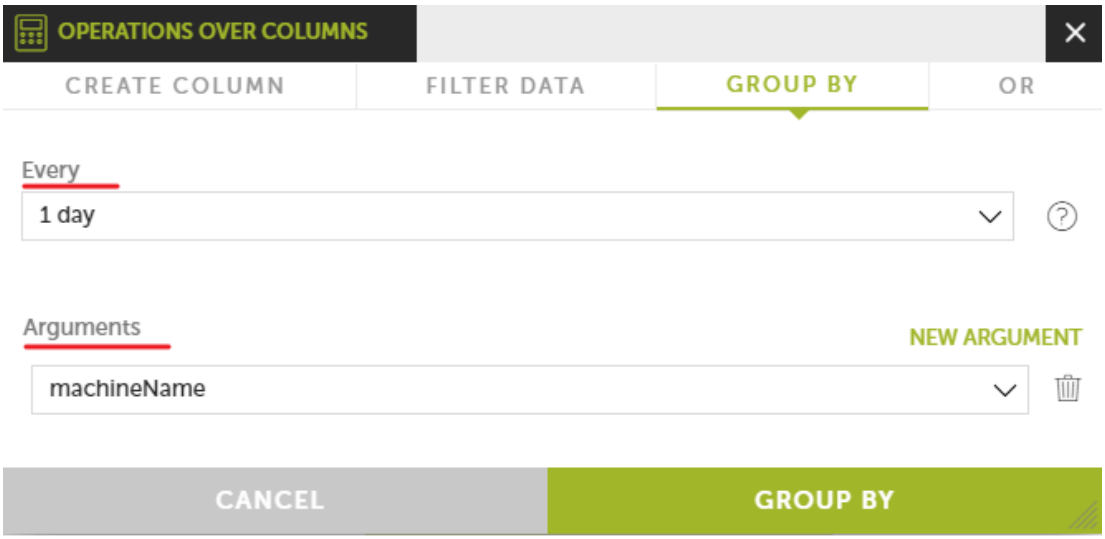

Figura 7.27: herramienta para la creación de una nueva agrupación

2. Agregar una función Count.

Como cada programa vulnerable detectado en un equipo genera un único evento diario, será necesario contar el número de veces que aparece cada equipo en la agrupación.

3. Agregar un filtro.

Si la dispersión de valores resultantes es muy grande es posible que interese establecer un filtro que deje fuera todos aquellos equipos que no lleguen a un cierto umbral de corte. Para lograr esto añade un filtro de tipo **Greater or equal** con el valor que consideremos oportuno. Por debajo de ese valor no aparecerán equipos en el listado.

4. Generar un gráfico Voronoi.

Utilizando el campo **MachineName** como **Signal** y **Count** como **Value** genera un gráfico con los equipos más vulnerables de la red.

Capítulo 8

Requisitos de hardware, software y red

Cytomic Insights 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.