Cytomic SIEMConnect

Manual de descripción de eventos

Para Cytomic Advanced EPDR y Cytomic EDR

Manual revisado: April 2024

Versión: 4.30.00

Acerca de este manual

El objetivo de este manual es facilitar la explotación de la información de seguridad suministrada porCytomic, y su integración en la infraestructura de almacenamiento implantada en la empresa.

En esta documentación se hace referencia al producto Cytomic EDR de forma genérica, para referirse tanto a Cytomic EDR como a Cytomic Advanced EPDR. Igualmente, se utiliza Cytomic SIEMConnect para referirse no solo a este producto, sino también a Cytomic SIEMConnect for Partners.

La información de este manual puede cambiar sin previo aviso. Las empresas, los nombres, y los datos usados en los ejemplos de este documento son ficticios salvo cuando se indique otra cosa. Ninguna parte de esta guía puede reproducirse ni transmitirse de ninguna forma ni por ningún medio, electrónico o mecánico, con ningún fin, sin el permiso expreso por escrito de WatchGuard Technologies, Inc.

Manual revisado: 4/4/2024

Información sobre copyright, marcas comerciales y patentes

Acerca de WatchGuard

WatchGuard® Technologies, Inc. es un líder mundial en seguridad de la red, que ofrece productos y servicios de Gestión Unificada de Amenazas, Firewall de Última Generación, secure Wi-Fi, e inteligencia de red de la mejor calidad a más de 75.000 clientes en todo el mundo. La misión de la empresa es hacer la seguridad de nivel empresarial accesible a empresas de todo tipo y tamaño mediante la sencillez, lo que convierte a WatchGuard en una solución ideal para Empresas Distribuidas y Pymes. WatchGuard tiene su sede en Seattle, Washington, y oficinas en Norteamérica, Europa, Asia-Pacífico, y Latinoamérica. Para obtener más información, visita WatchGuard.com.

Para obtener información adicional, promociones y actualizaciones, sigue a WatchGuard en Twitter, @WatchGuard en Facebook, o en la página de Empresa de LinkedIn. También puedes visitar nuestro blog sobre InfoSec, Secplicity, para obtener información en tiempo real sobre las amenazas más recientes y sobre cómo enfrentarte a ellas en www.secplicity.org.

Dirección

WatchGuard Technologies
255 S. King St.
Suite 1100
Seattle, WA 98104

Soporte

www.watchguard.com/support
EE. UU. y Canadá: +877.232.3531
Todos los Otros Países: +1.206.521.3575

Ventas

EE. UU. y Canadá: +1.800.734.9905
Todos los Otros Países: +1.206.613.0895

Índice

Recursos de documentación y comentarios

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

https://info.cytomicmodel.com/resources/guides/SIEMConnect/es/SIEMCONNECT-ManualDescripcionEventos-ES.pdf

Guía de infraestructura Cytomic SIEMConnect

La Guía de infraestructura Cytomic SIEMConnect completa el Manual de descripción de eventos Azure mostrando los recursos necesarios en la red del cliente para habilitar la recepción de información generada por el servicio.

https://info.cytomicmodel.com/resources/guides/SIEMConnect/es/SIEMCONNECT-Manual-ES.pdf

Guía de uso de Panda Partner Center

Para configurar el servicioCytomic SIEMConnect for Partners es necesario acceder al producto Panda Partner Center. Para obtener la versión más reciente de esta guía consulta la dirección web:

http://nexus-documents.cytomic.ai/AdvancedGuide/Nexus-Manual-ES.pdf

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

http://nexus-documents.cytomic.ai /Help/v77000//Partners/es-es/index.htm

Cytomic EDR y Cytomic EDPR

Cytomic SIEMConnect es un servicio que requiere los productos de seguridad Cytomic EDR. Consulta las guías en:

- 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 al portal eKnowledge Base consulta la siguiente URL:

https://www.pandasecurity.com/es/support/siemfeeder.htm

Encuesta sobre la Guía para el administrador de la red

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

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

Cómo usar este manual

Esta documentación está dirigida a dos tipos de organizaciones:

- Empresas que tienen contratado el servicio Cytomic SIEMConnect de Cytomic para los productos Cytomic EDR y Cytomic Advanced EPDR.
- Partners que tienen contratado Cytomic SIEMConnect for Partners para ofrecer el servicio de Cytomic SIEMConnect a sus clientes.

Dentro de las organizaciones, la información recogida en este manual está dirigida a:

- El especialista en seguridad informática que necesita una descripción detallada de la información que Cytomic SIEMConnect envía a la plataforma SIEM de su organización.
- El administrador de la solución SIEM adoptada en la empresa, que requiere conocer el formato de la información que recibe para poder incorporarla a su base de datos.

Mienstras no se especifique lo contrario, todos los procedimientos e indicaciones mostradas en este manual son aplicables de forma indistinta a:

- Clientes con licencias de Cytomic EDR contratadas.
- Clientes con licencias de Cytomic Advanced EPDR contratadas.
- Clientes con el servicio Cytomic SIEMConnect contratado.
- Clientes con el servicio Cytomic SIEMConnect for Partners contratado.

Convenciones del documento

Este documento usa estas convenciones de formato para resaltar tipos específicos de información:

Esto es una nota. Resalta información importante o útil.

Esto es una advertencia. Léela atentamente. Existe el riesgo de que pierdas datos, pongas en peligro la integridad del sistema, o afectes al rendimiento del dispositivo si no sigues las instrucciones o las recomendaciones.

Beneficios y arquitectura general

Cytomic SIEMConnect es el servicio de Cytomic que envía a la plataforma SIEM de los clientes la información y el conocimiento generado por los productos Cytomic EDR.

SIEMConnect envía a la plataforma SIEM de sus clientes inteligencia de seguridad sobre los procesos ejecutados en los equipos de los usuarios. Con esta información, el administrador de la seguridad obtiene una mayor visibilidad de lo que ocurre en la infraestructura informática que gestiona.

La información de inteligencia de seguridad suministrada al cliente facilita el descubrimiento de amenazas desconocidas, malware avanzado de tipo APT (Advanced Persistent Threats) y ataques dirigidos específicamente diseñados para extraer información confidencial de las empresas. Para conseguir este objetivo,SIEMConnect obtiene el registro de la actividad de las aplicaciones ejecutadas, gracias a la monitorización permanente del software de seguridad Cytomic EDR instalado en los equipos. Esta información se completa con inteligencia de seguridad generada enCytomic, y se envía a la plataforma SIEM del cliente, donde se integra para su explotación.

Beneficios

Con la inteligencia de seguridad suministrada, el administrador de la seguridad será capaz de:

- **Visualizar la evolución del estado del malware detectado en la red**, indicando si fue ejecutado o no, el vector de infección y las acciones ejecutadas por el proceso, para facilitar la implementación de estrategias de resolución y posterior adaptación de las políticas de seguridad de la empresa.
- **Visualizar las acciones ejecutadas por cada proceso** con el objetivo de centrarse en las actividades sospechosas de los programas desconocidos de muy reciente aparición, y recopilar los indicios que permitan obtener conclusiones acerca de su potencial peligrosidad.
- **Visualizar los accesos de los procesos a la información confidencial de la empresa** para prevenir su extracción o robo. Se muestran los ficheros de ofimática accedidos, bases de datos y otros repositorios de información confidencial.
- **Visualizar las conexiones de red establecidas por los procesos** para identificar destinos sospechosos y susceptibles de estar realizando ex filtración de datos.
- **Localizar 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 y afinar las políticas de seguridad establecidas.

Flujo de información generado por SIEMConnect

Cytomic EDR monitoriza de forma constante las acciones realizadas por los procesos ejecutados en los equipos de los usuarios. Estas acciones se envían a la plataforma Cytomic, donde se analizan y explotan para extraer de forma automatizada inteligencia de seguridad avanzada.

SIEMConnect reúne la información de los eventos monitorizados por Cytomic EDR y la información de seguridad generada para crear un único flujo de datos compatible con el servidor SIEM del cliente.

> Para conocer en detalle el flujo completo de información generado por SIEMConnect consulta la Guía de infraestructura Cytomic SIEMConnect (https://info.cytomicmodel.com/resources/guides/SIEMConnect/es/SIEMCONNECT-Manual-ES.PDF).

Requisitos

SIEMConnect no requiere cambios en los equipos monitorizados, ya que el servicio recibe los datos automáticamente desde cada estación de trabajo o servidor. Sin embargo, dependiendo del tipo de producto contratado, es necesario instalar y configurar varios elementos en la infraestructura informática de las empresas.

SIEMConnect para clientes finales

Se requieren los siguientes recursos en la infraestructura IT del cliente:

- Instalar y configurar el software Panda Importer preferiblemente en un equipo de tipo servidor.
- Si el flujo de eventos recibidos es grande, se recomienda instalar un gestor de colas compatible con Panda Importer.
- Instalar un servidor SIEM compatible con los formatos de log CEF y LEEF.

> Para conocer en detalle el proceso de instalación y configuración de Panda Importer consulta la Guía de infraestructura SIEMConnect (https://www.pandasecurity.com/rfiles/enterprise/solutions/adaptivedefense/SIEMFeeder-Manual-ES.PDF).

Cytomic SIEMConnect para partners

Se requieren los siguientes recursos en la infraestructura IT del partner:

- Instalar y configurar el softwarePanda Importer preferiblemente en un equipo de tipo servidor.
- Instalar un gestor de colas compatible.
- Instalar un servidor SIEM compatible con los formatos de log CEF y LEEF.
- Configurar el servicio Cytomic SIEMConnect for Partners. Consulta http://documents.managedprotection.pandasecurity.com/AdvancedGuide/PARTNERCENTER-Manual-ES.pdf.

El cliente no requiere cambios en su infraestructura informática.

Eventos e información extendida

Cytomic SIEMConnect transforma el flujo de telemetría recibida desde los equipos protegidos con Cytomic EDR en ficheros de texto, que contienen eventos formateados compatibles con servidores SIEM.

La unidad básica de información que recibe el cliente es el evento: cada acción relevante que realizan los procesos ejecutados en el equipo del usuario se transforma en un evento, que se entrega finalmente al servidor SIEM.

Estructura de un evento Cytomic SIEMConnect

Un evento es una acción registrada en el equipo de un cliente y descrita mediante una serie de pares campo-valor. Existen múltiples tipos de eventos, y cada tipo incluye pares campo-valor concretos. A esta colección de pares campo-valor, Cytomic SIEMConnect le agrega un preámbulo o cabecera, que contiene la información necesaria para encapsular la información en un evento compatible con los formatos comúnmente aceptados por los servidores SIEM: CEF o LEEF.

Para conocer en detalle el formato LEEF, consulta el enlace:
https://www.ibm.com/docs/en/dsm?topic=leef-overview

Para conocer en detalle el formato CEF, consulta el enlace:
https://community.microfocus.com/cfs-file/__key/communityserver-wikis-components-files/00-00-00-00-23/3731.CommonEventFormatV25.pdf

Agrupación de eventos

Un fichero de registro, también llamado “log”, es una agrupación de eventos que se entrega al servidor SIEM del cliente. Los logs generados por Cytomic SIEMConnect tienen un tamaño variable y pueden agrupar uno o varios eventos de categorías diferentes. A su vez, el origen de los eventos dentro de un mismo log puede ser uno o más equipos de la red del cliente.

Secuencia y tiempos de entrega de la información

El máximo retardo desde que un proceso realiza una acción en el equipo protegido con Cytomic EDR hasta que Cytomic SIEMConnect formatea el evento asociado y lo completa con inteligencia de seguridad es de 20 minutos.

Los eventos recibidos de los equipos de los clientes se procesan siguiendo una estrategia FIFO.

Los logs enviados al servidor SIEM del cliente no tienen una secuencia predefinida, pero todos los eventos contienen un campo con marca de tiempo (timestap) que permite ubicar el evento de forma precisa en una línea temporal.

Formato de los logs en Cytomic SIEMConnect

Cytomic SIEMConnect entrega la información en uno de los dos formatos disponibles: CEF o LEEF. Dependiendo del tipo de cliente al que va destinado el servicio, el procedimiento para seleccionar el formato varía:

- **Cytomic SIEMConnect**: consulta telefónicamente o por email a tu comercial asignado para cambiar el formato de los logs recibidos (panda.AD_SIEMFeeder@watchguard.com).
- **Cytomic SIEMConnect for Partners**: configura el servicio mediante Panda Partner Center. Consulta http://documents.managedprotection.pandasecurity.com/AdvancedGuide/PARTNERCENTER-Manual-ES.pdf.

Todos los ficheros de registro enviados por Cytomic SIEMConnect siguen la codificación UTF-8.

Formato Common Event Format (CEF)

El formato CEF está constituido por los bloques de datos mostrados a continuación:

- **Bloque Prefijo**: también conocido como “cabecera”. Identifica la categoría del evento y define al log como de tipo CEF. Los campos incluidos en este bloque están separados por pipes “|” y el significado de cada campo viene dado por su posición.
- **Bloque de extensiones del evento**: común a los dos tipos de log (CEF y LEEF). Incluye pares campo=valor separados por espacios.

Cytomic SIEMConnect no incluye la cabecera syslog en los logs CEF.

A continuación se muestra un ejemplo del evento **registryc** (**createExekey**) en formato CEF:

```
CEF:1|Panda Security|paps|02.45.00.0000|registryc|registryc|1|Date=2018-09-27
02:26:52.200188 MachineName=DESKTOP-PC MachineIP=192.168.0.11 User=NT
AUTHORITY\SYSTEM MUID=713FC2B45B429J291EB53467357AC1B7 Op=CreateExeKey
Hash=C86854DF4F3AEC59D523DBAD1F5031FD DriveType=Fixed
Path=SYSTEMX86|\CompatTelRunner.exe ValidSig=true Company=Microsoft Corporation
Broken=true ImageType=EXE 32 ExeType=Unknown Prevalence=Medium PrevLastDay=Low
Cat=Goodware MWName= TargetPath=3|PROGRAM_FILESX86|\Windows Defender\MsMpeng.exe
RegKey=\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows
NT\CurrentVersion\AppCompatFlags\WicaAvPathsExpiredTemp?0
```

Bloque Prefijo

```
CEF:1|Cytomic (Business Unit of Panda Security,
S.L.)|paps|02.45.00.0000|registryc|registryc|1|
```

Los campos dentro del bloque prefijo van separados por pipes “|”.

Campo	Descripción	Valor de ejemplo
Formato:versión	Identificador del formato del log y de la versión.	CEF:1
Device vendor	Nombre del proveedor del servicio.	Cytomic (Business Unit of Panda Security, S.L.)
Device Product	Nombre interno del dispositivo o software.	paps
Signature	Versión de la protección que generó el evento.	2.43.00.0000
Name y Name 2	En los eventos de tipo alerta, el nombre del evento se distribuye en los campos Name y Name 2. Por tanto, para obtener el nombre completo de la alerta es necesario concatenar los campos Name y Name 2. En el resto de tipos de evento, Name 2 tiene una copia del contenido del campo Name.	registryc
Severity	Excepto para los eventos de tipo alerta, el campo Severity siempre contiene en valor 1. Para los eventos de tipo alerta el campo se calcula en función del tipo de alerta y de la acción que tomó el software de seguridad en el equipo del usuario. Esta acción se indica en el segundo enumerado del campo ExecutionStatus del evento. Para conocer los posibles valores del campo Severity consulta la ayuda del evento de tipo alerta.	Numérico

Bloque extensiones del evento

Para obtener información acerca de los eventos soportados, campos existentes y una descripción detallada de los mismos consulta *Estructura de los eventos y sintaxis de los campos*.

Formato Log Event Extended Format (LEEF)

El formato LEEF está constituido por los bloques de datos mostrados a continuación:

- **Bloque Cabecera**: identifica la categoría del evento y define al log como de tipo LEEF. Los campos incluidos en este bloque están separados por pipes “|” y el significado de cada campo viene dado por su posición.

- **Bloque de atributos del evento**: común a los dos tipos de log (CEF y LEEF). Incluyen los campos del evento y sus valores.

> Cytomic SIEMConnect no incluye la cabecera syslog en los logs LEEF.

A continuación se muestra un ejemplo del evento **registryc** (**createExekey**) en formato LEEF:

```
LEEF:1.0|Panda Security|paps|02.43.00.0000|registryc|sev=1 devTime=2016-09-22
15:25:11.000628 devTimeFormat=yyyy-MM-dd HH:mm:ss.SSS usrName=LOCAL SERVICE domain=NT
AUTHORITY src=10.219.202.149 identSrc=10.219.202.149 identHostName=PXE68XXX HostName=
PXE68XXX MUID=1F109BA4E0XXXX37F9995D31FXXXX319 Op=CreateExeKey
Hash=C78655BC80301D76ED4FEF1C1EA40A7D DriveType=Fixed Path=SYSTEM|\svchost.exe
ValidSig= Company=Microsoft Corporation Broken=true ImageType=EXE 64 ExeType=Unknown
Prevalence=High PrevLastDay=Low HeurFI=67108872 Skeptic= AVDets=0 JIDFI=3431993
1NFI=116241 JIDMW=11195630 1NMW=4308325 Class=100 Cat=Goodware MWName=
TargetPath=0|pune.com RegKey=\ REGISTRY\ MACHINE\ SYSTEM\
ControlSet001\services\Tcpip\Parameters?DhcpDomain
```

Bloque Cabecera

```
LEEF:1.0|Cytomic (Business Unit of Panda Security,
S.L.)|paps|02.43.00.0000|registryc|
```

> En el formato LEEF la severidad del evento no se indica en el campo Severity del bloque Cabecera, sino que se especifica en el campo Sev=número en el bloque Atributos. Para conocer los posibles valores del campo Sev consulta la ayuda del evento de tipo alerta.

Campo	Descripción	Valor de ejemplo
Formato:versión	Identificador del formato del log y de la versión	LEEF:1
Vendor	Nombre del proveedor del servicio	Cytomic (Business Unit of Panda Security, S.L.)
Product	Nombre interno del dispositivo o software	paps
Version	Versión de la protección que generó el evento	2.43.00.0000
Event ID Description	Nombre completo del evento enviado	registryc

Bloque Atributos del evento

Para obtener información acerca de los eventos soportados, campos existentes y una descripción detallada de los mismos consulta *Estructura de los eventos y sintaxis de los campos*.

Categorías de eventos

El tipo de evento recibido viene especificado en el campo **Name** y **Name 2** del bloque Preámbulo en el formato CEF o en el campo **Event ID Description** del bloque Cabecera en el formato LEEF. Así mismo, el tipo del evento también se incluye en el campo **op** del bloque de atributos en el formato LEEF, o del bloque de extensiones en el formato CEF, si bien no todos los tipos de evento incluyen este campo.

A continuación se muestran todos los eventos posibles en el campo **Name / Event ID Description** y su significando, agrupados por su tipo.

Despliegue del agente

Campo	Descripción
install	Instalación y desinstalación del agente Cytomic EDR.

Creación de alertas

Campo	Descripción
alertmalware Malware Detected	Detección de malware.
alertpup PUP Detected	Detección de PUP (programa no deseado).
alertrdpattack RDPAttack Detected	Detección de ataque RDP por fuerza bruta.
alertadvpolicy ADVPolicy Detected	Detección realizada por las políticas de seguridad avanzadas. Este evento solo está disponible en Cytomic Advanced EPDR.
alertsecappcontrol SecAppControl Detected	Detección realizada por un nombre de proceso o MD5 definidos por el administrador en las políticas avanzadas de seguridad. Este evento solo está disponible en Cytomic Advanced EPDR

Campo	Descripción
alertprodappcontrol ProdAppControl Detected	Detección realizada por la configuración Bloqueo de programas establecida por el administrador.
alertexploit Exploit Detected	Detección de exploit.
alertdeepinspection DeepInspection Detected	Detección de ataque de red.
thalert	Detecciones de los siguientes tipos: ■ Indicios generados por el Radar de ciber-ataques en Orion. ■ IOCs cargados en la plataforma a través de la API de Orion. ■ IOAs detectados por Cytomic EDR. ■ IOAs avanzados detectados por Cytomic Advanced EPDR.

Modificaciones en el sistema operativo de los usuarios

Campo	Descripción
hostfiles	Modificación del fichero HOSTS.
monitoredregistry	Acceso a ramas del registro sensibles y relacionadas con el intento de ganar persistencia en el equipo tras un reinicio.
registrym	Modificación de rama en el registro del equipo que apunta a un fichero ejecutable.
registryc	Creación de rama en el registro del equipo que apunta a un fichero ejecutable.
openlsass	Acceso al proceso LSASS para intentar comprometer las credenciales de una cuenta de usuario.
modLinuxCfg	Modificación de un fichero de configuración del sistema operativo Linux.
modOSXCfg	Modificación de un fichero de configuración del sistema operativo macOS.
systemops	Modificación del sistema operativo a través de WMI (Windows Management Interface).

Manipulación de procesos

Campo	Descripción
createremotethread	Creación de hilo de ejecución remoto.
exec	Ejecución de proceso.
createprocessbyWMI	Creación de proceso a través del sistema WMI.
scriptcreation	Creación de un script.
scriptlaunch	Ejecución de script.
createpe	Creación de programa ejecutable.
modifype	Modificación de fichero ejecutable.
renamepe	Cambio de nombre de fichero ejecutable.
deletepe	Borrado de programa ejecutable.
loadlib	Carga de librería.
heuhooks	Detección de intento de exploit.

Descarga de ficheros

Campo	Descripción
urldownload	Descarga de fichero.

Acceso a datos

Campo	Descripción
createcmp	Creación de fichero comprimido.
opencmp	Apertura de fichero comprimido.
monitoredopen	Acceso a ficheros de datos monitorizados.
createdir	Creación de directorio en el sistema de ficheros.
socket	Operación de comunicación por red.

Otros

Campo	Descripción
criticalsoft	Detección de aplicación vulnerables instalada en el equipo.
processnetbytes	Consumo de datos de red por proceso.
dnsops	Proceso con peticiones de resolución DNS erróneas.
loginoutsops	Inicio y fin de sesión en el equipo del usuario.
deviceops	Conexión y/o desconexión de dispositivo externo.
notblocked	Evento que Cytomic EDR deja sin analizar debido a situaciones excepcionales.
svcControl	Intento de modificación de los ficheros que pertenecen al producto de seguridad instalado.
block	Bloqueo de ejecución de programa por no estar aun clasificado o ser sospechoso de malware.

Suscripción a categorías de eventos

SIEMConnect puede generar una gran cantidad de eventos en función de la actividad detectada en la infraestructura IT del cliente. Esta situación podría afectar al rendimiento de la red del cliente y a los servicios encargados del almacenamiento y procesamiento de los eventos. Por esta razón, el cliente tiene la opción de suscribirse solo a los grupos de eventos que considere más importantes.

Los tipos de eventos disponibles se agrupan en categorías. Un cliente puede suscribirse a una categoría, a varias categorías o recibir todos los eventos sin filtrar. Por defecto el cliente estará suscrito a la categoría especial 7, a la que pertenecen todos los eventos sin filtrar.

Cambiar la suscripción a eventos

- Si no eres cliente de **Cytomic SIEMConnect for Partners**consulta telefónicamente o por email a tu comercial asignado para cambiar el formato de los logs recibidos (panda.AD_ SIEMFeeder@watchguard.com).
- Si eres cliente de **Cytomic SIEMConnect for Partners** configura el servicio mediante la consola de administración. Consulta http://nexus-documents.cytomic.ai/AdvancedGuide/NEXUS-Manual-ES.pdf.

Categorías de eventos disponibles

Los eventos createcmp, createdir, criticalsoft, hostfiles, install, opencmp, block, urldownload y notblocked no pertenecen a ninguna categoría específica. Para recibirlos, el cliente tiene que estar suscrito a la categoría especial 7, que incorpora todos los eventos sin filtrar.

Campo	Categoría	Descripción
Detecciones de amenazas (Malware, PUPS, Exploits)	1	Alertas de malware / PUP, Exploit, ataques RDP, bloqueo por políticas avanzadas y ataques de red. ▪ alertmalware Malware Detected ▪ alertpup PUP Detected ▪ alertdeepinspection DeepInspection Detected ▪ alertrdpattack RDPAttack Detected ▪ alertadvpolicy ADVPolicy Detected (evento disponible en Cytomic Advanced EPDR) ▪ alertsecappcontrol SecAppControl Detected (evento disponible en Cytomic Advanced EPDR) ▪ alertprodappcontrol ProdAppControl Detected ▪ alertexploit Exploit Detected
Carga y ejecución de ejecutables PE y scripts	2	Carga y ejecución de ficheros ejecutables binarios y no binarios (scripts). ▪ createremotethread ▪ exec ▪ loadlib ▪ scriptlaunch ▪ createprocessbyWMI
Comunicaciones	3	Eventos de apertura y uso de sockets. ▪ sockets ▪ processnetbytes ▪ dnsops
Acceso a datos	4	Acceso a datos contenidos en ficheros y en el registro de Windows. ▪ monitoredopen ▪ monitoredregistry ▪ openlass
Creación y modificación de ejecutables PE y scripts	5	Creación y modificación de ficheros ejecutables binarios y scripts. ▪ createpe

Campo	Categoría	Descripción
		■ modifype ■ renamepe ■ deletepe ■ scriptcreation
Accesos al registro de Windows	6	Eventos relacionados con acceso al registro de Windows. ■ registryc ■ registrym ■ monitoredregistry
Sin filtros	7	Se envían todos los eventos incluyendo createcmp, createdir, criticalsoft, hostfiles, install, opencmp, block, urldownload, notblocked.
Eventos del sistema	8	Eventos relacionados con el acceso a dispositivos, motor WMI e inicios y finales de sesión. ■ deviceops ■ loginoutsops ■ systemops ■ modLinuxCfg ■ modOSXCfg
Indicios de malware	9	Evento THAlert con las generadas por: ■ Las reglas de Threat Hunting en Orion ■ Los IOCs definidos en Orion. ■ El módulo IOA en Cytomic EDR

Estructura de los eventos y sintaxis de los campos

Estructura interna de los eventos

Cytomic SIEMConnect describe cada evento mediante pares campo-valor. Para entender la lógica de la información generada por SIEMConnect, los eventos se pueden dividir en dos tipos: eventos de tipo activo y eventos de tipo pasivo

Eventos de tipo activo

La mayor parte de los eventos recibidos describen situaciones en las que un proceso denominado padre (parent), realiza una acción sobre un elemento hijo (child). El tipo del elemento que recibe la acción varía dependiendo de la categoría del evento. De esta forma el elemento hijo (child) puede ser:

- **Otro proceso**: en eventos de tipo carga y descarga de procesos, carga de librerías etc.
- **Fichero ejecutable**: en eventos de tipo creación, borrado, modificación de programas.
- **Fichero del sistema**: en eventos que reflejan la manipulación del fichero hosts y del registro del equipo de usuario.
- **Fichero de datos**: en eventos que reflejan el acceso a ficheros de ofimática, bases de datos, etc.
- **Fichero de descarga**: en eventos que se generan cuando se detecta la descarga de datos de un proceso.
- **Fichero comprimido**: en eventos que reflejan la creación, modificación y borrado de ficheros comprimidos.
- **Directorio**: en eventos que reflejan la creación, modificación y borrado de carpetas.

Dependiendo del tipo de evento, se incluirán o no ciertos campos que describan las características tanto del elemento padre como del hijo. Por ejemplo, en un evento de tipo creación de directorio, los campos asociados al evento describirán las características del proceso padre (si es o no malware, ruta del proceso, metadatos del proceso, etc) así como las características del hijo. En este caso, al tratarse de un directorio, algunos campos que se incluyen en el evento no llevarán información, como por ejemplo los campos que describen al elemento como malware, o los metadatos del fichero, información que no es posible suministrar al tratarse de un directorio. Otra información, como por ejemplo la ruta del directorio, sí será incluida en el evento.

Eventos de tipo pasivo

Son eventos que en muchos casos no tienen procesos padre o hijo claramente definidos ya que se corresponden al registro pasivo de una situación que se produce en el equipo del usuario. Ejemplos de eventos de tipo registro son los eventos de generación de alertas por malware o la instalación, actualización y modificación del agente Cytomic EDR entre otros.

Prefijos parent y child

En los eventos de tipo activo que involucran a dos ficheros o procesos generalmente se utilizan los prefijos parent y child para diferenciar la información relativa a cada proceso:

- **Parent**: los campos que comienzan con la etiqueta Parent describen un atributo del proceso padre.
- **Child**: los campos que comienzan con la etiqueta Child describen un atributo del elemento hijo.

Otros prefijos y afijos

En muchos campos y valores se utilizan abreviaturas; conocer su significado ayuda a interpretar el campo en cuestión:

- **Sig**: signature (firma digital)
- **Exe y pe**: ejecutable
- **Mw**: malware
- **Sec**: segundos
- **Op**: operación
- **Cat**: categoría
- **PUP**: Potential Unwanted Program (programa potencialmente no deseado)
- **Ver**: versión
- **SP**: service Pack
- **Cfg**: configuración
- **Cmp y comp**: comprimido
- **Dst**: destino

Alertadvpolicy ADVPolicy Detected

Evento de tipo pasivo que describe los parámetros de la alerta que Cytomic Advanced EPDR crea cuando detecta una amenaza mediante las políticas avanzadas de seguridad, definidas por el administrador en la sección Protección avanzada, Políticas avanzadas de seguridad de la configuración Estaciones y servidores.

Este evento solo está disponible en Cytomic Advanced EPDR.

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	Fecha del equipo del usuario cuando se generó el evento.	Fecha
HostIp (CEF)	IP del equipo de usuario o servidor donde se genera el evento.	Dirección IP
sev (LEEF)	Severidad del evento.	9
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
src (LEEF)	IP del equipo de usuario o servidor que genera el evento registrado.	Cadena de caracteres
identSrc (LEEF)	IP del equipo de usuario o servidor que genera el evento registrado.	Cadena de caracteres
identHostName (LEEF)	Nombre del equipo de usuario que genera el evento registrado.	Cadena de caracteres
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
HostName	Nombre del equipo de usuario donde se	Cadena de

Campo	Descripción	Valor
	genera el evento registrado.	caracteres
ThreatType	Tipo de malware detectado.	Cadena de caracteres “ADVPolicy”
ExecutionStatus	Acción realizada por el agente Cytomic EDR. ▪ **Allow** ▪ **Block** ▪ **BlockTimeout**: se mostró un mensaje emergente al usuario pero no contestó a tiempo. ▪ **AllowWL**: elemento permitido por encontrarse en la lista blanca del administrador. ▪ **Disinfect** ▪ **Delete** ▪ **Quarantine** ▪ **AllowByUser**: se mostró un mensaje emergente al usuario y contesto “permitir ejecución”. ▪ **Informed**: se mostró un mensaje emergente al usuario. ▪ **Unquarantine**: el fichero se sacó de la cuarentena. ▪ **Rename**: elemento renombrado por no poderse mover a cuarentena, borrar o desinfectar. ▪ **BlockURL**: se bloqueó el acceso a una URL. ▪ **KillProcess**: cierre de proceso. ▪ **BlockExploit**: intento de explotación de proceso vulnerable detenido. ▪ **ExploitAllowByUser**: el usuario no permitió el cierre del proceso explotado. ▪ **RebootNeeded**: se requiere un reinicio del equipo para bloquear el intento de explotación.	Enumeración

Campo	Descripción	Valor
	▪ **ExploitInformed**: se mostró un mensaje emergente al usuario informando de un intento de explotación de proceso vulnerable. ▪ **AllowSonGWInstaller**: el programa forma parte de un paquete de instalación clasificado como Goodware. ▪ **EmbebedInformed**: el elemento es un script en powershell que ejecuta comandos. ▪ **SuspedProcess**: el elemento intentó suspender alguno de los servicios del software de protección. ▪ **ModifyDiskResource**: el elemento intentó modificar un fichero protegido que pertenece al software de protección. ▪ **ModifyRegistry**: el elemento intentó modificar una clave de registro protegida que pertenece al software de protección. ▪ **RenameRegistry**: el elemento intentó renombrar una clave de registro protegida que pertenece al software de protección. ▪ **ModifyMarkFile**: el elemento intentó renombrar un fichero protegido que pertenece al software de protección. ▪ **UncertainAction**: el elemento intentó una acción sin definir sobre un fichero que pertenece al software de protección. ▪ **AllowGWFilter**: se permite la ejecución del elemento por estar en la caché de goodware. ▪ **AllowSWAuthoriced**: se permite la ejecución del elemento por estar autorizado por el administrador (configuración Software Autorizado). ▪ **NewPE**: aparición de un nuevo programa ejecutable en el equipo que viene del exterior.	

Campo	Descripción	Valor
	▪ **AllowedByAdmin**: se permite la ejecución del elemento porque el administrador excluyó la técnica de explotación detectada. ▪ **Blocked by ip**: se bloqueó la dirección IP de origen por detectarse un ataque de fuerza bruta mediante el protocolo RDP. ▪ **AllowSonMsiGW**: se permite la ejecución del elemento por tratarse de un ejecutable que proviene de un paquete de instalación confiable. ▪ **Allowed by Global Audit**: el elemento se permite porque el software de seguridad está configurado en modo Global Audit.	
DwellTimeSecs	Tiempo transcurrido desde la primera vez que la amenaza fue vista en la red del cliente.	Segundos
MWHash (LEEF) ItemHash (CEF)	Hash del malware.	Cadena de caracteres
MWName (LEEF) ItemName (CEF)	Nombre del malware si está ya catalogado como una amenaza.	Cadena de caracteres
MWPath (LEEF) ItemPath (CEF)	Ruta del malware.	Cadena de caracteres
SourceIP	Si el malware vino desde el exterior indica la dirección IP del equipo remoto.	Dirección IP
SourceMachineName	Si el malware vino desde el exterior indica el nombre del equipo remoto.	Cadena de caracteres
SourceUserName	Si el malware vino desde el exterior 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

Campo	Descripción	Valor
Vulnerable	Indica si la aplicación se considera vulnerable.	Booleano
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres
DriveType	Tipo de unidad donde reside el proceso o fichero que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM ▪ **Ramdisk**: unidad de disco RAM.	Enumeración
ServiceLevel	Modo de ejecución del agente: ▪ **Blocking**: el agente bloquea todos los ejecutables sin clasificar y los clasificados como malware. ▪ **Hardening**: el agente bloquea la ejecución de todos los programas sin clasificar cuyo origen no sea confiable y los clasificados como malware. ▪ **Learning**: el agente no bloquea ningún programa pero monitoriza los procesos ejecutados.	Enumeración

Alertdeepinspection DeepInspection Detected

Evento de tipo pasivo que describe los parámetros de la alerta que Cytomic EDR crea cuando detecta el intento de explotación de una vulnerabilidad a través de la red.

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	Fecha del equipo del usuario cuando se generó el evento.	Fecha
HostIp (CEF)	IP del equipo de usuario o servidor donde se genera el evento.	Dirección IP
sev (LEEF)	Severidad del evento. Consulta *Cálculo del campo Severity / Sev*.	Numérico
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
src (LEEF)	IP del equipo de usuario o servidor que genera el evento registrado.	Cadena de caracteres
identSrc (LEEF)	IP del equipo de usuario o servidor que genera el evento registrado.	Cadena de caracteres
identHostName (LEEF)	Nombre del equipo de usuario que genera el evento registrado.	Cadena de caracteres
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
HostName	Nombre del equipo de usuario donde se genera el evento registrado.	Cadena de caracteres
ThreatType	Tipo de malware detectado.	Cadena de caracteres “DeepInspection”
ExecutionStatus	Acción realizada por el agente Cytomic.	Enumeración

Campo	Descripción	Valor
	▪ **Allow** ▪ **Block** ▪ **BlockTimeout**: se mostró un mensaje emergente al usuario pero no contestó a tiempo. ▪ **AllowWL**: elemento permitido por encontrarse en la lista blanca del administrador. ▪ **Disinfect** ▪ **Delete** ▪ **Quarantine** ▪ **AllowByUser**: se mostró un mensaje emergente al usuario y contesto “permitir ejecución”. ▪ **Informed**: se mostró un mensaje emergente al usuario. ▪ **Unquarantine**: el fichero se sacó de la cuarentena. ▪ **Rename**: elemento renombrado por no poderse mover a cuarentena, borrar o desinfectar. ▪ **BlockURL**: se bloqueó el acceso a una URL. ▪ **KillProcess**: cierre de proceso. ▪ **BlockExploit**: intento de explotación de proceso vulnerable detenido. ▪ **ExploitAllowByUser**: el usuario no permitió el cierre del proceso explotado. ▪ **RebootNeeded**: se requiere un reinicio del equipo para bloquear el intento de explotación. ▪ **ExploitInformed**: se mostró un mensaje emergente al usuario informando de un intento de explotación de proceso vulnerable. ▪ **AllowSonGWInstaller**: el programa forma parte de un paquete de instalación clasificado como Goodware.	

Campo	Descripción	Valor
	▪ **EmbebedInformed**: el elemento es un script en powershell que ejecuta comandos. ▪ **SuspedProcess**: el elemento intentó suspender alguno de los servicios del software de protección. ▪ **ModifyDiskResource**: el elemento intentó modificar un fichero protegido que pertenece al software de protección. ▪ **ModifyRegistry**: el elemento intentó modificar una clave de registro protegida que pertenece al software de protección. ▪ **RenameRegistry**: el elemento intentó renombrar una clave de registro protegida que pertenece al software de protección. ▪ **ModifyMarkFile**: el elemento intentó renombrar un fichero protegido que pertenece al software de protección. ▪ **UncertainAction**: el elemento intentó una acción sin definir sobre un fichero que pertenece al software de protección. ▪ **AllowGWFilter**: se permite la ejecución del elemento por estar en la caché de goodware. ▪ **AllowSWAuthoriced**: se permite la ejecución del elemento por estar autorizado por el administrador (configuración Software Autorizado). ▪ **NewPE**: aparición de un nuevo programa ejecutable en el equipo que viene del exterior. ▪ **AllowedByAdmin**: se permite la ejecución del elemento porque el administrador excluyó la técnica de explotación detectada.	

Campo	Descripción	Valor
	▪ **Blocked by ip**: se bloqueó la dirección IP de origen por detectarse un ataque de fuerza bruta mediante el protocolo RDP. ▪ **AllowSonMsiGW**: se permite la ejecución del elemento por tratarse de un ejecutable que proviene de un paquete de instalación confiable. ▪ **Allowed by Global Audit**: el elemento se permite porque el software de seguridad está configurado en modo Global Audit.	
DwellTimeSecs	Tiempo transcurrido desde la primera vez que la amenaza fue vista en la red del cliente.	Segundos
MWHash (LEEF) ItemHash (CEF)	Hash del malware.	Cadena de caracteres
MWPath (LEEF) ItemPath (CEF)	Ruta del malware.	Cadena de caracteres
MWName (LEEF) ItemName (CEF)	Nombre del malware si está ya catalogado como una amenaza.	Cadena de caracteres
SourceIP	Si el malware vino desde el exterior indica la dirección IP del equipo remoto.	Dirección IP
SourceMachineName	Si el malware vino desde el exterior indica el nombre del equipo remoto.	Cadena de caracteres
SourceUserName	Si el malware vino desde el exterior 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

Campo	Descripción	Valor
Vulnerable	Indica si la aplicación se considera vulnerable.	Booleano
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres
DriveType	Tipo de unidad donde reside el proceso o fichero que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM ▪ **Ramdisk**: unidad de disco RAM.	Enumeración
ServiceLevel	Modo de ejecución del agente: ▪ **Blocking**: el agente bloquea todos los ejecutables sin clasificar y los clasificados como malware. ▪ **Hardening**: el agente bloquea la ejecución de todos los programas sin clasificar cuyo origen no sea confiable y los clasificados como malware. ▪ **Learning**: el agente no bloquea ningún programa pero monitoriza los procesos ejecutados.	Enumeración

Cálculo del campo Severity / Sev

Dependiendo del valor del campo ExecutionStatus - Action, el valor de Severity / Sev varía según la tabla mostrada a continuación:

ExecutionStatus - Action	Severity
■ Allow ■ AllowWL ■ AllowByUser ■ Informed ■ Unquarantine ■ Rename ■ BlockURL ■ BlockExploit ■ RebootNeeded ■ AllowSonGwInstaller ■ InformNewPE ■ SonMSIGW ■ RDPOff	8
■ Block ■ BlockBL ■ BlockTimeout ■ Delete ■ Disinfect ■ Quarantine ■ KillProcess ■ EmbebedBlocked ■ SuspendProcess ■ BlockedIp ■ RenameRegistry ■ AllowSWAutoriced	7
■ ExploitAllowByUser ■ ExploitInformed ■ EmbebedInformed ■ ModifyMarkFile ■ UncertainAction	10

ExecutionStatus - Action	Severity
■ ResponseLast ■ IsolateHost	
■ ModifyRegistry ■ AllowFGW	6
■ ExploitAllowByAdmin	5

Alertexploit Exploit Detected

Evento de tipo pasivo que describe los parámetros de la alerta que Cytomic EDR crea cuando detecta el intento de explotación de una vulnerabilidad en un programa instalado en un equipo de la red.

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	Fecha del equipo del usuario cuando se generó el evento.	Fecha
HostIp (CEF)	IP del equipo de usuario o servidor donde se genera el evento.	Dirección IP
sev (LEEF)	Severidad del evento.	9
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
src (LEEF)	IP del equipo de usuario o servidor que genera el evento registrado.	Cadena de caracteres
identSrc (LEEF)	IP del equipo de usuario o servidor que genera el evento registrado.	Cadena de caracteres
identHostName (LEEF)	Nombre del equipo de usuario que genera el evento registrado.	Cadena de caracteres
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
HostName	Nombre del equipo de usuario donde se genera el evento registrado.	Cadena de caracteres
ThreatType	Tipo de malware detectado.	Cadena de caracteres “Exploit”
ExecutionStatus	Acción realizada por el agente Cytomic.	Enumeración

Campo	Descripción	Valor
	▪ **Allow** ▪ **Block** ▪ **BlockTimeout**: se mostró un mensaje emergente al usuario pero no contestó a tiempo. ▪ **AllowWL**: elemento permitido por encontrarse en la lista blanca del administrador. ▪ **Disinfect** ▪ **Delete** ▪ **Quarantine** ▪ **AllowByUser**: se mostró un mensaje emergente al usuario y contesto “permitir ejecución”. ▪ **Informed**: se mostró un mensaje emergente al usuario. ▪ **Unquarantine**: el fichero se sacó de la cuarentena. ▪ **Rename**: elemento renombrado por no poderse mover a cuarentena, borrar o desinfectar. ▪ **BlockURL**: se bloqueó el acceso a una URL. ▪ **KillProcess**: cierre de proceso. ▪ **BlockExploit**: intento de explotación de proceso vulnerable detenido. ▪ **ExploitAllowByUser**: el usuario no permitió el cierre del proceso explotado. ▪ **RebootNeeded**: se requiere un reinicio del equipo para bloquear el intento de explotación. ▪ **ExploitInformed**: se mostró un mensaje emergente al usuario informando de un intento de explotación de proceso vulnerable. ▪ **AllowSonGWInstaller**: el programa forma parte de un paquete de instalación clasificado como Goodware.	

Campo	Descripción	Valor
	▪ **EmbebedInformed**: el elemento es un script en powershell que ejecuta comandos. ▪ **SuspedProcess**: el elemento intentó suspender alguno de los servicios del software de protección. ▪ **ModifyDiskResource**: el elemento intentó modificar un fichero protegido que pertenece al software de protección. ▪ **ModifyRegistry**: el elemento intentó modificar una clave de registro protegida que pertenece al software de protección. ▪ **RenameRegistry**: el elemento intentó renombrar una clave de registro protegida que pertenece al software de protección. ▪ **ModifyMarkFile**: el elemento intentó renombrar un fichero protegido que pertenece al software de protección. ▪ **UncertainAction**: el elemento intentó una acción sin definir sobre un fichero que pertenece al software de protección. ▪ **AllowGWFilter**: se permite la ejecución del elemento por estar en la caché de goodware. ▪ **AllowSWAuthoriced**: se permite la ejecución del elemento por estar autorizado por el administrador (configuración Software Autorizado). ▪ **NewPE**: aparición de un nuevo programa ejecutable en el equipo que viene del exterior. ▪ **AllowedByAdmin**: se permite la ejecución del elemento porque el administrador excluyó la técnica de explotación detectada.	

Campo	Descripción	Valor
	▪ **Blocked by ip**: se bloqueó la dirección IP de origen por detectarse un ataque de fuerza bruta mediante el protocolo RDP. ▪ **AllowSonMsiGW**: se permite la ejecución del elemento por tratarse de un ejecutable que proviene de un paquete de instalación confiable. ▪ **Allowed by Global Audit**: el elemento se permite porque el software de seguridad está configurado en modo Global Audit.	
DwellTimeSecs	Tiempo transcurrido desde la primera vez que la amenaza fue vista en la red del cliente.	Segundos
MWHash (LEEF) ItemHash (CEF)	Hash del malware.	Cadena de caracteres
MWPath (LEEF) ItemPath (CEF)	Ruta del malware.	Cadena de caracteres
MWName (LEEF) ItemName (CEF)	Nombre del malware si está ya catalogado como una amenaza.	Cadena de caracteres
SourceIP	Si el malware vino desde el exterior indica la dirección IP del equipo remoto.	Dirección IP
SourceMachineName	Si el malware vino desde el exterior indica el nombre del equipo remoto.	Cadena de caracteres
SourceUserName	Si el malware vino desde el exterior 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

Campo	Descripción	Valor
Vulnerable	Indica si la aplicación se considera vulnerable.	Booleano
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres
DriveType	Tipo de unidad donde reside el proceso o fichero que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM ▪ **Ramdisk**: unidad de disco RAM.	Enumeración
ServiceLevel	Modo de ejecución del agente: ▪ **Blocking**: el agente bloquea todos los ejecutables sin clasificar y los clasificados como malware. ▪ **Hardening**: el agente bloquea la ejecución de todos los programas sin clasificar cuyo origen no sea confiable y los clasificados como malware. ▪ **Learning**: el agente no bloquea ningún programa pero monitoriza los procesos ejecutados.	Enumeración

Alertmalware Malware Detected

Evento de tipo pasivo que describe los parámetros de la alerta que Cytomic EDR crea cuando detecta un elemento clasificado como malware.

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	Fecha del equipo del usuario cuando se generó el evento.	Fecha
HostIp (CEF)	IP del equipo de usuario o servidor donde se genera el evento.	Dirección IP
sev (LEEF)	Severidad del evento. Consulta *Cálculo del campo Severity / Sev*.	Numérico
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
src (LEEF)	IP del equipo de usuario o servidor que genera el evento registrado.	Cadena de caracteres
identSrc (LEEF)	IP del equipo de usuario o servidor que genera el evento registrado.	Cadena de caracteres
identHostName (LEEF)	Nombre del equipo de usuario que genera el evento registrado.	Cadena de caracteres
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
HostName	Nombre del equipo de usuario donde se genera el evento registrado.	Cadena de caracteres
ThreatType	Tipo de malware detectado.	Cadena de caracteres “Malware”
ExecutionStatus	La amenaza detectada se llegó a ejecutar o	Enumeración -

Campo	Descripción	Valor
	no: ▪ **Executed** ▪ **Not executed** Acción realizada por el agente Cytomic: ▪ **Allow** ▪ **Block** ▪ **BlockTimeout**: se mostró un mensaje emergente al usuario pero no contestó a tiempo. ▪ **AllowWL**: elemento permitido por encontrarse en la lista blanca del administrador. ▪ **Disinfect** ▪ **Delete** ▪ **Quarantine** ▪ **AllowByUser**: se mostró un mensaje emergente al usuario y contesto “permitir ejecución”. ▪ **Informed**: se mostró un mensaje emergente al usuario. ▪ **Unquarantine**: el fichero se sacó de la cuarentena. ▪ **Rename**: elemento renombrado por no poderse mover a cuarentena, borrar o desinfectar. ▪ **BlockURL**: se bloqueó el acceso a una URL. ▪ **KillProcess**: cierre de proceso. ▪ **BlockExploit**: intento de explotación de proceso vulnerable detenido. ▪ **ExploitAllowByUser**: el usuario no permitió el cierre del proceso explotado. ▪ **RebootNeeded**: se requiere un reinicio del equipo para bloquear el intento de explotación. ▪ **ExploitInformed**: se mostró un mensaje emergente al usuario informando de un intento de explotación de proceso vulnerable.	Enumeración

Campo	Descripción	Valor
	▪ **AllowSonGWInstaller**: el programa forma parte de un paquete de instalación clasificado como Goodware. ▪ **EmbebedInformed**: el elemento es un script en powershell que ejecuta comandos. ▪ **SuspedProcess**: el elemento intentó suspender alguno de los servicios del software de protección. ▪ **ModifyDiskResource**: el elemento intentó modificar un fichero protegido que pertenece al software de protección. ▪ **ModifyRegistry**: el elemento intentó modificar una clave de registro protegida que pertenece al software de protección. ▪ **RenameRegistry**: el elemento intentó renombrar una clave de registro protegida que pertenece al software de protección. ▪ **ModifyMarkFile**: el elemento intentó renombrar un fichero protegido que pertenece al software de protección. ▪ **UncertainAction**: el elemento intentó una acción sin definir sobre un fichero que pertenece al software de protección. ▪ **AllowGWFilter**: se permite la ejecución del elemento por estar en la caché de goodware. ▪ **AllowSWAuthoriced**: se permite la ejecución del elemento por estar autorizado por el administrador (configuración Software Autorizado). ▪ **NewPE**: aparición de un nuevo programa ejecutable en el equipo que viene del exterior. ▪ **AllowedByAdmin**: se permite la ejecución del elemento porque el administrador excluyó la técnica de explotación detectada.	

Campo	Descripción	Valor
	▪ **Blocked by ip**: se bloqueó la dirección IP de origen por detectarse un ataque de fuerza bruta mediante el protocolo RDP. ▪ **AllowSonMsiGW**: se permite la ejecución del elemento por tratarse de un ejecutable que proviene de un paquete de instalación confiable. ▪ **Allowed by Global Audit**: el elemento se permite porque el software de seguridad está configurado en modo Global Audit.	
DwellTimeSecs	Tiempo transcurrido desde la primera vez que la amenaza fue vista en la red del cliente.	Segundos
MWHash (LEEF) ItemHash (CEF)	Hash del malware.	Cadena de caracteres
MWPath (LEEF) ItemPath (CEF)	Ruta del malware.	Cadena de caracteres
MWName (LEEF) ItemName (CEF)	Nombre del malware si está ya catalogado como una amenaza.	Cadena de caracteres
SourceIP	Si el malware vino desde el exterior indica la dirección IP del equipo remoto.	Dirección IP
SourceMachineName	Si el malware vino desde el exterior indica el nombre del equipo remoto.	Cadena de caracteres
SourceUserName	Si el malware vino desde el exterior 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

Campo	Descripción	Valor
Vulnerable	Indica si la aplicación se considera vulnerable.	Booleano
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres
DriveType	Tipo de unidad donde reside el proceso o fichero que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM ▪ **Ramdisk**: unidad de disco RAM.	Enumeración
ServiceLevel	Modo de ejecución del agente: ▪ **Blocking**: el agente bloquea todos los ejecutables sin clasificar y los clasificados como malware. ▪ **Hardening**: el agente bloquea la ejecución de todos los programas sin clasificar cuyo origen no sea confiable y los clasificados como malware. ▪ **Learning**: el agente no bloquea ningún programa pero monitoriza los procesos ejecutados.	Enumeración

Cálculo del campo Severity / Sev

Dependiendo del valor del campo ExecutionStatus - Action, el valor de Severity / Sev varía según la tabla mostrada a continuación:

ExecutionStatus - Action	Severity
■ Allow ■ AllowWL ■ AllowByUser ■ Informed ■ Unquarantine ■ Rename ■ BlockURL ■ BlockExploit ■ RebootNeeded ■ AllowSonGwInstaller ■ InformNewPE ■ SonMSIGW ■ RDPOff	8
■ Block ■ BlockBL ■ BlockTimeout ■ Delete ■ Disinfect ■ Quarantine ■ KillProcess ■ EmbebedBlocked ■ SuspendProcess ■ BlockedIp ■ RenameRegistry ■ AllowSWAutoriced	7
■ ExploitAllowByUser ■ ExploitInformed ■ EmbebedInformed ■ ModifyMarkFile ■ UncertainAction	10

ExecutionStatus - Action	Severity
■ ResponseLast ■ IsolateHost	
■ ModifyRegistry ■ AllowFGW	6
■ ExploitAllowByAdmin	5

Alertprodappcontrol ProdAppControl Detected

Evento de tipo pasivo que describe los parámetros de la alerta que Cytomic EDR crea cuando bloquea elementos según un nombre o MD5, definidos por el administrador en la configuración **Bloqueo de programas**.

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	Fecha del equipo del usuario cuando se generó el evento.	Fecha
HostIp (CEF)	IP del equipo de usuario o servidor donde se genera el evento.	Dirección IP
sev (LEEF)	Severidad del evento.	9
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
src (LEEF)	IP del equipo de usuario o servidor que genera el evento registrado.	Cadena de caracteres
identSrc (LEEF)	IP del equipo de usuario o servidor que genera el evento registrado.	Cadena de caracteres
identHostName (LEEF)	Nombre del equipo de usuario que genera el evento registrado.	Cadena de caracteres
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
HostName	Nombre del equipo de usuario donde se genera el evento registrado.	Cadena de caracteres
ThreatType	Tipo de malware detectado.	Cadena de caracteres “ProdAppControl”
ExecutionStatus	Acción realizada por el agente Cytomic EDR.	Enumeración

Campo	Descripción	Valor
	▪ **Allow** ▪ **Block** ▪ **BlockTimeout**: se mostró un mensaje emergente al usuario pero no contestó a tiempo. ▪ **AllowWL**: elemento permitido por encontrarse en la lista blanca del administrador. ▪ **Disinfect** ▪ **Delete** ▪ **Quarantine** ▪ **AllowByUser**: se mostró un mensaje emergente al usuario y contesto “permitir ejecución”. ▪ **Informed**: se mostró un mensaje emergente al usuario. ▪ **Unquarantine**: el fichero se sacó de la cuarentena. ▪ **Rename**: elemento renombrado por no poderse mover a cuarentena, borrar o desinfectar. ▪ **BlockURL**: se bloqueó el acceso a una URL. ▪ **KillProcess**: cierre de proceso. ▪ **BlockExploit**: intento de explotación de proceso vulnerable detenido. ▪ **ExploitAllowByUser**: el usuario no permitió el cierre del proceso explotado. ▪ **RebootNeeded**: se requiere un reinicio del equipo para bloquear el intento de explotación. ▪ **ExploitInformed**: se mostró un mensaje emergente al usuario informando de un intento de explotación de proceso vulnerable. ▪ **AllowSonGWInstaller**: el programa forma parte de un paquete de instalación clasificado como Goodware.	

Campo	Descripción	Valor
	▪ **EmbebedInformed**: el elemento es un script en powershell que ejecuta comandos. ▪ **SuspedProcess**: el elemento intentó suspender alguno de los servicios del software de protección. ▪ **ModifyDiskResource**: el elemento intentó modificar un fichero protegido que pertenece al software de protección. ▪ **ModifyRegistry**: el elemento intentó modificar una clave de registro protegida que pertenece al software de protección. ▪ **RenameRegistry**: el elemento intentó renombrar una clave de registro protegida que pertenece al software de protección. ▪ **ModifyMarkFile**: el elemento intentó renombrar un fichero protegido que pertenece al software de protección. ▪ **UncertainAction**: el elemento intentó una acción sin definir sobre un fichero que pertenece al software de protección. ▪ **AllowGWFilter**: se permite la ejecución del elemento por estar en la caché de goodware. ▪ **AllowSWAuthoriced**: se permite la ejecución del elemento por estar autorizado por el administrador (configuración Software Autorizado). ▪ **NewPE**: aparición de un nuevo programa ejecutable en el equipo que viene del exterior. ▪ **AllowedByAdmin**: se permite la ejecución del elemento porque el administrador excluyó la técnica de explotación detectada.	

Campo	Descripción	Valor
	▪ **Blocked by ip**: se bloqueó la dirección IP de origen por detectarse un ataque de fuerza bruta mediante el protocolo RDP. ▪ **AllowSonMsiGW**: se permite la ejecución del elemento por tratarse de un ejecutable que proviene de un paquete de instalación confiable. ▪ **Allowed by Global Audit**: el elemento se permite porque el software de seguridad está configurado en modo Global Audit.	
DwellTimeSecs	Tiempo transcurrido desde la primera vez que la amenaza fue vista en la red del cliente.	Segundos
MWHash (LEEF) ItemHash (CEF)	Hash del malware.	Cadena de caracteres
MWName (LEEF) ItemName (CEF)	Nombre del malware si está ya catalogado como una amenaza.	Cadena de caracteres
MWPath (LEEF) ItemPath (CEF)	Ruta del malware.	Cadena de caracteres
SourceIP	Si el malware vino desde el exterior indica la dirección IP del equipo remoto.	Dirección IP
SourceMachineName	Si el malware vino desde el exterior indica el nombre del equipo remoto.	Cadena de caracteres
SourceUserName	Si el malware vino desde el exterior 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

Campo	Descripción	Valor
Vulnerable	Indica si la aplicación se considera vulnerable.	Booleano
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres
DriveType	Tipo de unidad donde reside el proceso o fichero que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM ▪ **Ramdisk**: unidad de disco RAM.	Enumeración
ServiceLevel	Modo de ejecución del agente: ▪ **Blocking**: el agente bloquea todos los ejecutables sin clasificar y los clasificados como malware. ▪ **Hardening**: el agente bloquea la ejecución de todos los programas sin clasificar cuyo origen no sea confiable y los clasificados como malware. ▪ **Learning**: el agente no bloquea ningún programa pero monitoriza los procesos ejecutados.	Enumeración

Alertpup PUP Detected

Evento de tipo pasivo que describe los parámetros de la alerta que Cytomic EDR crea cuando detecta un elemento clasificado como programa no deseado (PUP).

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	Fecha del equipo del usuario cuando se generó el evento.	Fecha
HostIp (CEF)	IP del equipo de usuario o servidor donde se genera el evento.	Dirección IP
sev (LEEF)	Severidad del evento. Consulta *Cálculo del campo Severity / Sev*.	Numérico
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
src (LEEF)	IP del equipo de usuario o servidor que genera el evento registrado.	Cadena de caracteres
identSrc (LEEF)	IP del equipo de usuario o servidor que genera el evento registrado.	Cadena de caracteres
identHostName (LEEF)	Nombre del equipo de usuario que genera el evento registrado.	Cadena de caracteres
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
HostName	Nombre del equipo de usuario donde se genera el evento registrado.	Cadena de caracteres
ThreatType	Tipo de malware detectado.	Cadena de caracteres “PUP”
ExecutionStatus	La amenaza detectada se llegó a ejecutar o no:	Enumeración - Enumeración

Campo	Descripción	Valor
	▪ **Executed** ▪ **Not executed** Acción realizada por el agente Cytomic EDR. ▪ **Allow** ▪ **Block** ▪ **BlockTimeout**: se mostró un mensaje emergente al usuario pero no contestó a tiempo. ▪ **AllowWL**: elemento permitido por encontrarse en la lista blanca del administrador. ▪ **Disinfect** ▪ **Delete** ▪ **Quarantine** ▪ **AllowByUser**: se mostró un mensaje emergente al usuario y contesto “permitir ejecución”. ▪ **Informed**: se mostró un mensaje emergente al usuario. ▪ **Unquarantine**: el fichero se sacó de la cuarentena. ▪ **Rename**: elemento renombrado por no poderse mover a cuarentena, borrar o desinfectar. ▪ **BlockURL**: se bloqueó el acceso a una URL. ▪ **KillProcess**: cierre de proceso. ▪ **BlockExploit**: intento de explotación de proceso vulnerable detenido. ▪ **ExploitAllowByUser**: el usuario no permitió el cierre del proceso explotado. ▪ **RebootNeeded**: se requiere un reinicio del equipo para bloquear el intento de explotación. ▪ **ExploitInformed**: se mostró un mensaje emergente al usuario informando de un intento de explotación de proceso vulnerable.	

Campo	Descripción	Valor
	▪ **AllowSonGWInstaller**: el programa forma parte de un paquete de instalación clasificado como Goodware. ▪ **EmbebedInformed**: el elemento es un script en powershell que ejecuta comandos. ▪ **SuspedProcess**: el elemento intentó suspender alguno de los servicios del software de protección. ▪ **ModifyDiskResource**: el elemento intentó modificar un fichero protegido que pertenece al software de protección. ▪ **ModifyRegistry**: el elemento intentó modificar una clave de registro protegida que pertenece al software de protección. ▪ **RenameRegistry**: el elemento intentó renombrar una clave de registro protegida que pertenece al software de protección. ▪ **ModifyMarkFile:** el elemento intentó renombrar un fichero protegido que pertenece al software de protección. ▪ **UncertainAction**: el elemento intentó una acción sin definir sobre un fichero que pertenece al software de protección. ▪ **AllowGWFilter**: se permite la ejecución del elemento por estar en la caché de goodware. ▪ **AllowSWAuthoriced**: se permite la ejecución del elemento por estar autorizado por el administrador (configuración Software Autorizado). ▪ **NewPE**: aparición de un nuevo programa ejecutable en el equipo que viene del exterior. ▪ **AllowedByAdmin**: se permite la ejecución del elemento porque el administrador excluyó la técnica de explotación detectada.	

Campo	Descripción	Valor
	▪ **Blocked by ip**: se bloqueó la dirección IP de origen por detectarse un ataque de fuerza bruta mediante el protocolo RDP. ▪ **AllowSonMsiGW**: se permite la ejecución del elemento por tratarse de un ejecutable que proviene de un paquete de instalación confiable. ▪ **Allowed by Global Audit**: el elemento se permite porque el software de seguridad está configurado en modo Global Audit.	
DwellTimeSecs	Tiempo transcurrido desde la primera vez que la amenaza fue vista en la red del cliente.	Segundos
MWHash (LEEF) ItemHash (CEF)	Hash del malware.	Cadena de caracteres
MWPath (LEEF) ItemPath (CEF)	Ruta del malware.	Cadena de caracteres
MWName (LEEF) ItemName (CEF)	Nombre del malware si está ya catalogado como una amenaza.	Cadena de caracteres
SourceIP	Si el malware vino desde el exterior indica la dirección IP del equipo remoto.	Dirección IP
SourceMachineName	Si el malware vino desde el exterior indica el nombre del equipo remoto.	Cadena de caracteres
SourceUserName	Si el malware vino desde el exterior 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

Campo	Descripción	Valor
Vulnerable	Indica si la aplicación se considera vulnerable.	Booleano
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres
DriveType	Tipo de unidad donde reside el proceso o fichero que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM ▪ **Ramdisk**: unidad de disco RAM.	Enumeración
ServiceLevel	Modo de ejecución del agente: ▪ **Blocking**: el agente bloquea todos los ejecutables sin clasificar y los clasificados como malware. ▪ **Hardening**: el agente bloquea la ejecución de todos los programas sin clasificar cuyo origen no sea confiable y los clasificados como malware. ▪ **Learning**: el agente no bloquea ningún programa pero monitoriza los procesos ejecutados.	Enumeración

Cálculo del campo Severity / Sev

Dependiendo del valor del campo ExecutionStatus - Action, el valor de Severity / Sev varía según la tabla mostrada a continuación:

ExecutionStatus - Action	Severity
■ Allow ■ AllowWL ■ AllowByUser ■ Informed ■ Unquarantine ■ Rename ■ BlockURL ■ BlockExploit ■ RebootNeeded ■ AllowSonGwInstaller ■ InformNewPE ■ SonMSIGW ■ RDPOff	6
■ Block ■ BlockBL ■ BlockTimeout ■ Delete ■ Disinfect ■ Quarantine ■ KillProcess ■ EmbebedBlocked ■ SuspendProcess ■ BlockedIp ■ RenameRegistry ■ AllowSWAutoriced	5
■ ExploitAllowByUser ■ ExploitInformed ■ EmbebedInformed ■ ModifyMarkFile ■ UncertainAction	8

ExecutionStatus - Action	Severity
■ ResponseLast ■ IsolateHost	
■ ModifyRegistry ■ AllowFGW	4
■ ExploitAllowByAdmin	3

Alertrdpattack RDPAttack Detected

Evento de tipo pasivo que describe los parámetros de la alerta que Cytomic EDR crea cuando detecta un ataque por fuerza bruta a través del protocolo RDP (Remote Desktop Protocol).

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	Fecha del equipo del usuario cuando se generó el evento.	Fecha
HostIp (CEF)	IP del equipo de usuario o servidor donde se genera el evento.	Dirección IP
sev (LEEF)	Severidad del evento.	9
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
src (LEEF)	IP del equipo de usuario o servidor que genera el evento registrado.	Cadena de caracteres
identSrc (LEEF)	IP del equipo de usuario o servidor que genera el evento registrado.	Cadena de caracteres
identHostName (LEEF)	Nombre del equipo de usuario que genera el evento registrado.	Cadena de caracteres
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
HostName	Nombre del equipo de usuario donde se genera el evento registrado.	Cadena de caracteres
ThreatType	Tipo de ataque detectado.	Cadena de caracteres “RDPAttack”
ExecutionStatus	Tipo de acción ejecutada.	Cadena de

Campo	Descripción	Valor
		caracteres “Blocked by ip”
DwellTimeSecs	Sin uso.	Segundos
MWHash (LEEF) ItemHash (CEF)	Sin uso	
MWName (LEEF) ItemName (CEF)	Nombre del ataque registrado: ▪ **Exploit/BruteForce_RDP**: intento de intrusión por fuerza bruta utilizando el protocolo RDP. ▪ **Exploit/RemoteDesktopIntrusion**: intrusión detectada mediante el protocolo RDP.	Cadena de caracteres
MWPath (LEEF) ItemPath (CEF)	Nombre del ataque empleado.	Cadena de caracteres “Malicious Network Rdp Attack”
SourceIP	Dirección IP del equipo atacante.	Dirección IP
SourceMachineName	Nombre del equipo atacante.	Cadena de caracteres
SourceUserName	Nombre de la cuenta de usuario utilizado en el ataque.	Cadena de caracteres
UrlList	Sin uso.	Cadena de caracteres
DocList	Sin uso.	Cadena de caracteres
Version	Sin uso.	Cadena de caracteres

Campo	Descripción	Valor
Vulnerable	Sin uso.	Booleano
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres
DriveType	Tipo de unidad donde reside el proceso o fichero que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM ▪ **Ramdisk**: unidad de disco RAM.	Enumeración
ServiceLevel	Modo de ejecución del agente: ▪ **Blocking**: el agente bloquea todos los ejecutables sin clasificar y los clasificados como malware. ▪ **Hardening**: el agente bloquea la ejecución de todos los programas sin clasificar cuyo origen no sea confiable y los clasificados como malware. ▪ **Learning**: el agente no bloquea ningún programa pero monitoriza los procesos ejecutados.	Enumeración

Alertsecappcontrol SecAppControl Detected

Evento de tipo pasivo que describe los parámetros de la alerta que Cytomic Advanced EPDR crea cuando bloquea elementos según un nombre o MD5, definido por el administrador en la sección Protección avanzada, Políticas avanzadas, Bloquear programas de la configuración Estaciones y servidores.

Este evento solo está disponible en Cytomic Advanced EPDR.

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	Fecha del equipo del usuario cuando se generó el evento.	Fecha
HostIp (CEF)	IP del equipo de usuario o servidor donde se genera el evento.	Dirección IP
sev (LEEF)	Severidad del evento.	9
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
src (LEEF)	IP del equipo de usuario o servidor que genera el evento registrado.	Cadena de caracteres
identSrc (LEEF)	IP del equipo de usuario o servidor que genera el evento registrado.	Cadena de caracteres
identHostName (LEEF)	Nombre del equipo de usuario que genera el evento registrado.	Cadena de caracteres
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
HostName	Nombre del equipo de usuario donde se	Cadena de

Campo	Descripción	Valor
	genera el evento registrado.	caracteres
ThreatType	Tipo de malware detectado.	Cadena de caracteres “SecAppControl”
ExecutionStatus	Acción realizada por el agente Cytomic EDR. ▪ **Allow** ▪ **Block** ▪ **BlockTimeout**: se mostró un mensaje emergente al usuario pero no contestó a tiempo. ▪ **AllowWL**: elemento permitido por encontrarse en la lista blanca del administrador. ▪ **Disinfect** ▪ **Delete** ▪ **Quarantine** ▪ **AllowByUser**: se mostró un mensaje emergente al usuario y contesto “permitir ejecución”. ▪ **Informed**: se mostró un mensaje emergente al usuario. ▪ **Unquarantine**: el fichero se sacó de la cuarentena. ▪ **Rename**: elemento renombrado por no poderse mover a cuarentena, borrar o desinfectar. ▪ **BlockURL**: se bloqueó el acceso a una URL. ▪ **KillProcess**: cierre de proceso. ▪ **BlockExploit**: intento de explotación de proceso vulnerable detenido. ▪ **ExploitAllowByUser**: el usuario no permitió el cierre del proceso explotado. ▪ **RebootNeeded**: se requiere un reinicio del equipo para bloquear el intento de explotación.	Enumeración

Campo	Descripción	Valor
	▪ **ExploitInformed**: se mostró un mensaje emergente al usuario informando de un intento de explotación de proceso vulnerable. ▪ **AllowSonGWInstaller**: el programa forma parte de un paquete de instalación clasificado como Goodware. ▪ **EmbebedInformed**: el elemento es un script en powershell que ejecuta comandos. ▪ **SuspedProcess**: el elemento intentó suspender alguno de los servicios del software de protección. ▪ **ModifyDiskResource**: el elemento intentó modificar un fichero protegido que pertenece al software de protección. ▪ **ModifyRegistry**: el elemento intentó modificar una clave de registro protegida que pertenece al software de protección. ▪ **RenameRegistry**: el elemento intentó renombrar una clave de registro protegida que pertenece al software de protección. ▪ **ModifyMarkFile**: el elemento intentó renombrar un fichero protegido que pertenece al software de protección. ▪ **UncertainAction**: el elemento intentó una acción sin definir sobre un fichero que pertenece al software de protección. ▪ **AllowGWFilter**: se permite la ejecución del elemento por estar en la caché de goodware. ▪ **AllowSWAuthoriced**: se permite la ejecución del elemento por estar autorizado por el administrador (configuración Software Autorizado). ▪ **NewPE**: aparición de un nuevo programa ejecutable en el equipo que viene del exterior.	

Campo	Descripción	Valor
	▪ **AllowedByAdmin**: se permite la ejecución del elemento porque el administrador excluyó la técnica de explotación detectada. ▪ **Blocked by ip**: se bloqueó la dirección IP de origen por detectarse un ataque de fuerza bruta mediante el protocolo RDP. ▪ **AllowSonMsiGW**: se permite la ejecución del elemento por tratarse de un ejecutable que proviene de un paquete de instalación confiable. ▪ **Allowed by Global Audit**: el elemento se permite porque el software de seguridad está configurado en modo Global Audit.	
DwellTimeSecs	Tiempo transcurrido desde la primera vez que la amenaza fue vista en la red del cliente.	Segundos
MWHash (LEEF) ItemHash (CEF)	Hash del malware.	Cadena de caracteres
MWName (LEEF) ItemName (CEF)	Nombre del malware si está ya catalogado como una amenaza.	Cadena de caracteres
MWPath (LEEF) ItemPath (CEF)	Ruta del malware.	Cadena de caracteres
SourceIP	Si el malware vino desde el exterior indica la dirección IP del equipo remoto.	Dirección IP
SourceMachineName	Si el malware vino desde el exterior indica el nombre del equipo remoto.	Cadena de caracteres
SourceUserName	Si el malware vino desde el exterior 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

Campo	Descripción	Valor
Vulnerable	Indica si la aplicación se considera vulnerable.	Booleano
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres
DriveType	Tipo de unidad donde reside el proceso o fichero que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM ▪ **Ramdisk**: unidad de disco RAM.	Enumeración
ServiceLevel	Modo de ejecución del agente: ▪ **Blocking**: el agente bloquea todos los ejecutables sin clasificar y los clasificados como malware. ▪ **Hardening**: el agente bloquea la ejecución de todos los programas sin clasificar cuyo origen no sea confiable y los clasificados como malware. ▪ **Learning**: el agente no bloquea ningún programa pero monitoriza los procesos ejecutados.	Enumeración

Block

Evento de tipo activo que describe el mensaje emergente que Cytomic EDR muestra al usuario cuando bloquea un ejecutable que no ha sido clasificado todavía.

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
User (CEF)	Nombre de la cuenta de usuario y dominio al que pertenece utilizada para ejecutar el proceso que genero el evento registrado.	Cadena de caracteres
MachineIP (CEF)	Nombre del equipo que desencadena el evento registrado.	Dirección IP
MachineName (CEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
sev (LEEF)	Severidad del evento.	8
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
usrName (LEEF)	Cuenta de usuario utilizada por el proceso que realizó la operación registrada.	Cadena de caracteres
domain (LEEF)	Dominio de la cuenta de usuario utilizado por el proceso que realizó la operación registrada.	Cadena de caracteres
src (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identSrc (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identHostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres

Campo	Descripción	Valor
HostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
LocalDateTime	Fecha en formato UTC que tenía el equipo en el momento en que se produjo el evento registrado. Esta fecha depende de la configuración del equipo y por lo tanto puede ser errónea	Fecha
PandaTimeStatus	Contenido de los campos DateTime, Date y LocalDateTime	**0**: fecha real no soportada por tratarse de un evento antiguo. **1**: fecha real no disponible el servidor Cytomic y obtenida mediante un cálculo. **2**: fecha real proporcionada por el servidor Cytomic.
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
LocalCat	Categoría del elemento calculada por el agente Cytomic: ▪ **NotClassified**: fichero en proceso de clasificación. ▪ **Goodware** ▪ **Malware** ▪ **Suspect**: fichero en proceso de clasificación con alta probabilidad de resultar malware. ▪ **Compromised**: proceso comprometido por un ataque de tipo exploit. ▪ **GoodwareNotConfirmed**: fichero en apariencia goodware pero pendiente de clasificar. ▪ **PUP** ▪ **GoodwareUnwanted**: equivalente a PUP.	Enumeración

Campo	Descripción	Valor
	▪ **GoodwareRanked**: proceso clasificado como goodware.	
cloudAcces	Indica si hay acceso a la nube.	Booleano
DetId	Identificador de la detección.	Numérico
FirstSeen	Fecha en la que se vio por primera vez el fichero.	Fecha
LastQueryDate	Fecha de la última consulta del agente Cytomic a la nube.	Fecha
ToastBlockReason	Motivo de la aparición del mensaje emergente en el puesto de usuario o servidor. **0**: bloqueo por fichero desconocido en modo bloqueo. **1**: Bloqueo por reglas locales. **2**: Bloqueo por regla de origen del fichero no fiable. **3**: Bloqueo por regla de contexto. **4**: Bloqueo por exploit. **5**: Bloqueo por pregunta al usuario de cerrar el proceso.	Enumeración
ToastResult	Respuesta del usuario ante el mensaje emergente mostrado por Cytomic EDR. ▪ **Ok**: el cliente acepta el mensaje. ▪ **Timeout**: el mensaje emergente desaparece por la no acción del usuario. ▪ **Angry**: el usuario rechaza el bloqueo desde el mensaje emergente. ▪ **Block** ▪ **Allow**	Enumeración
WinningTech	Tecnología que provocó el evento. ▪ **Blockmode**: el agente estaba en modo Lock en el momento del bloqueo. ▪ **Cache**: clasificación cacheada en local. ▪ **Cloud**: clasificación descargada de la nube. ▪ **Context**: regla de contexto local.	Enumeración

Campo	Descripción	Valor
	▪ **ContextMinerva**: regla de contexto en la nube. ▪ **Digital Signature**: fichero firmado digitalmente. ▪ **Exploit**: tecnología de identificación de intento de explotación de proceso vulnerable. ▪ **ExploitLegacy** ▪ **GWFilter**: tecnologías de identificación de ficheros GW desconocidos. ▪ **LegacyUser**: permiso solicitado al usuario. ▪ **Local Signature**: firma local. ▪ **MetaEsploit:** ataque generado con el framework metaExploit. ▪ **NetNative**: tipo de binario. ▪ **Serializer**: tipo de binario. ▪ **User**: permiso solicitado al usuario. ▪ **RDP**: ataque de fuerza bruta por el protocolo RDP. ▪ **AMSI**: detección encontrada mediante Antimalware Scan Interface.	
ServiceLevel	Modo de ejecución del agente: ▪ **Blocking**: el agente bloquea todos los ejecutables sin clasificar y los clasificados como malware. ▪ **Hardening**: el agente bloquea la ejecución de todos los programas sin clasificar cuyo origen no sea confiable y los clasificados como malware. ▪ **Learning**: el agente no bloquea ningún programa pero monitoriza los procesos ejecutados.	Enumeración
Hash	Hash / digest del fichero.	MD5
Path	Ruta del elemento que desencadenó la operación registrada.	Cadena de caracteres (Ruta)

Campo	Descripción	Valor
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres
DriveType	Tipo de unidad donde reside el proceso o fichero que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM ▪ **Ramdisk**: unidad de disco RAM.	Enumeración

Createcmp

Evento de tipo activo que se genera cuando un proceso (parent) crea un nuevo fichero comprimido (child).

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
User (CEF)	Nombre de la cuenta de usuario y dominio al que pertenece utilizada para ejecutar el proceso que genero el evento registrado.	Cadena de caracteres
MachineIP (CEF)	Nombre del equipo de usuario que desencadena el evento registrado.	Dirección IP
MachineName (CEF)	Nombre del equipo de usuario que desencadena el evento registrado.	Cadena de caracteres
sev (LEEF)	Severidad del evento.	1
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
usrName (LEEF)	Cuenta de usuario utilizada por el proceso que realizó la operación registrada.	Cadena de caracteres
domain (LEEF)	Dominio de la cuenta de usuario utilizado por el proceso que realizó la operación registrada.	Cadena de caracteres
src (LEEF)	IP del equipo de usuario o servidor que desencadena el evento registrado.	Cadena de caracteres
identSrc (LEEF)	IP del equipo de usuario o servidor que desencadena el evento registrado.	Cadena de caracteres
identHostName (LEEF)	Nombre del equipo de usuario que desencadena el evento registrado.	Cadena de caracteres

Campo	Descripción	Valor
HostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
LocalDateTime	Fecha en formato UTC que tenía el equipo en el momento en que se produjo el evento registrado. Esta fecha depende de la configuración del equipo y por lo tanto puede ser errónea	Fecha
PandaTimeStatus	Contenido de los campos DateTime, Date y LocalDateTime	**0**: fecha real no soportada por tratarse de un evento antiguo. **1**: fecha real no disponible el servidor Cytomic y obtenida mediante un cálculo. **2**: fecha real proporcionada por el servidor Cytomic.
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
Op	Operación registrada.	Cadena de caracteres: “createcmp”
ParentHash	Hash del proceso que actúa como padre.	Cadena de caracteres
ParentDriveType	Tipo de unidad donde reside el proceso o fichero padre que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM ▪ **Ramdisk**: unidad de disco RAM.	Enumeración

Campo	Descripción	Valor
ParentPath	Ruta del fichero padre que realizó la operación registrada.	Cadena de caracteres
ParentPID	Identificador del proceso padre.	Numérico
ParentValidSig	El proceso padre está firmado digitalmente.	Booleano
ParentCompany	Contenido del atributo Company de los metadatos del proceso padre.	Cadena de caracteres
ParentBroken	El proceso padre está corrupto o defectuoso.	Booleano
ParentImageType	Arquitectura interna del proceso padre: ▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DDLx64	Enumeración
ParentExeType	Estructura interna / tipo del proceso padre. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
ParentPrevalence	Prevalencia histórica del proceso padre en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ParentPrevLastDay	Prevalencia del proceso padre en el día anterior en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración

Campo	Descripción	Valor
ParentCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración
ParentMWName	Nombre del malware en el proceso padre si ya está catalogado como una amenaza. Si es Null el elemento no es malware.	Cadena de caracteres
ChildHash	Hash del proceso que actúa como hijo.	Cadena de caracteres
ChildDriveType	Tipo de unidad donde reside el proceso o fichero padre que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM ▪ **Ramdisk**: unidad de disco RAM.	Enumeración
ChildPath	Ruta del fichero hijo que realizó la operación registrada.	Cadena de caracteres (Ruta)
ChildPID	Identificador del proceso hijo.	Numérico
ChildValidSig	El proceso hijo está firmado digitalmente.	Booleano
ChildCompany	Contenido del atributo Company de los metadatos del proceso hijo.	Cadena de caracteres
ChildBroken	El proceso hijo está corrupto o defectuoso.	Booleano
ChildImageType	Arquitectura interna del proceso hijo: ▪ EXEx32 ▪ EXEx64	Enumeración

Campo	Descripción	Valor
	▪ DLLx32 ▪ DLLx64	
ChildExeType	Estructura interna / tipo del proceso hijo. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
ChildPrevalence	Prevalencia histórica del proceso hijo en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ChildPrevLastDay	Prevalencia histórica del proceso hijo en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ChildCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración
ChildMWName	Nombre del malware en el proceso hijo si ya está catalogado como una amenaza. Si es Null el elemento no es malware.	Cadena de caracteres
OCS_Exec	Se ejecutó en el equipo software considerado	Booleano

Campo	Descripción	Valor
	como vulnerable.	
OCS_Name	Nombre del software vulnerable ejecutado.	Cadena de caracteres
OCS_Version	Versión del sistema operativo del equipo donde se ejecutó el software vulnerable.	Cadena de caracteres
Params	Parámetros de ejecución del proceso en la linea de comandos.	Cadena de caracteres
ToastResult	Respuesta del usuario ante el mensaje emergente mostrado por Cytomic EDR. ▪ **Ok**: el cliente acepta el mensaje. ▪ **Timeout**: el mensaje emergente desaparece por la no acción del usuario. ▪ **Angry**: el usuario rechaza el bloqueo desde el mensaje emergente. ▪ **Block** ▪ **Allow**	Enumeración
Action	Acción realizada por el agente Cytomic. ▪ **Allow** ▪ **Block** ▪ **BlockTimeout**: se mostró un mensaje emergente al usuario pero no contestó a tiempo. ▪ **AllowWL**: elemento permitido por encontrarse en la lista blanca del administrador. ▪ **Disinfect** ▪ **Delete** ▪ **Quarantine** ▪ **AllowByUser**: se mostró un mensaje emergente al usuario y contesto “permitir ejecución”. ▪ **Informed**: se mostró un mensaje emergente al usuario. ▪ **Unquarantine**: el fichero se sacó de la cuarentena.	Enumeración - Enumeración

Campo	Descripción	Valor
	▪ **Rename**: elemento renombrado por no poderse mover a cuarentena, borrar o desinfectar. ▪ **BlockURL**: se bloqueó el acceso a una URL. ▪ **KillProcess**: cierre de proceso. ▪ **BlockExploit**: intento de explotación de proceso vulnerable detenido. ▪ **ExploitAllowByUser**: el usuario no permitió el cierre del proceso explotado. ▪ **RebootNeeded**: se requiere un reinicio del equipo para bloquear el intento de explotación. ▪ **ExploitInformed**: se mostró un mensaje emergente al usuario informando de un intento de explotación de proceso vulnerable. ▪ **AllowSonGWInstaller**: el programa forma parte de un paquete de instalación clasificado como Goodware. ▪ **EmbebedInformed**: el elemento es un script en powershell que ejecuta comandos. ▪ **SuspedProcess**: el elemento intentó suspender alguno de los servicios del software de protección. ▪ **ModifyDiskResource:** el elemento intentó modificar un fichero protegido que pertenece al software de protección. ▪ **ModifyRegistry**: el elemento intentó modificar una clave de registro protegida que pertenece al software de protección. ▪ **RenameRegistry**: el elemento intentó renombrar una clave de registro protegida que pertenece al software de protección. ▪ **ModifyMarkFile**: el elemento intentó renombrar un fichero protegido que pertenece al software de protección.	

Campo	Descripción	Valor
	▪ **UncertainAction**: el elemento intentó una acción sin definir sobre un fichero que pertenece al software de protección. ▪ **AllowGWFilter**: se permite la ejecución del elemento por estar en la caché de goodware. ▪ **AllowSWAuthoriced**: se permite la ejecución del elemento por estar autorizado por el administrador (configuración Software Autorizado). ▪ **NewPE**: aparición de un nuevo programa ejecutable en el equipo que viene del exterior. ▪ **AllowedByAdmin**: se permite la ejecución del elemento porque el administrador excluyó la técnica de explotación detectada. ▪ **Blocked by ip**: se bloqueó la dirección IP de origen por detectarse un ataque de fuerza bruta mediante el protocolo RDP. ▪ **AllowSonMsiGW**: se permite la ejecución del elemento por tratarse de un ejecutable que proviene de un paquete de instalación confiable. ▪ **Allowed by Global Audit**: el elemento se permite porque el software de seguridad está configurado en modo Global Audit.	
ServiceLevel	Modo de ejecución del agente: ▪ **Blocking**: el agente bloquea todos los ejecutables sin clasificar y los clasificados como malware. ▪ **Hardening**: el agente bloquea la ejecución de todos los programas sin clasificar cuyo origen no sea confiable y los clasificados como malware. ▪ **Learning**: el agente no bloquea ningún programa pero monitoriza los procesos ejecutados.	Enumeración

Campo	Descripción	Valor
WinningTech	Tecnología que provocó el evento. ▪ **Blockmode**: el agente estaba en modo Lock en el momento del bloqueo. ▪ **Cache**: clasificación cacheada en local. ▪ **Cloud**: clasificación descargada de la nube. ▪ **Context**: regla de contexto local. ▪ **ContextMinerva**: regla de contexto en la nube. ▪ **Digital Signature**: fichero firmado digitalmente. ▪ **Exploit**: tecnología de identificación de intento de explotación de proceso vulnerable. ▪ **ExploitLegacy** ▪ **GWFilter**: tecnologías de identificación de ficheros GW desconocidos. ▪ **LegacyUser**: permiso solicitado al usuario. ▪ **Local Signature**: firma local. ▪ **MetaEsploit**: ataque generado con el framework metaExploit. ▪ **NetNative**: tipo de binario. ▪ **Serializer**: tipo de binario. ▪ **User**: permiso solicitado al usuario. ▪ **RDP**: ataque de fuerza bruta por el protocolo RDP. ▪ **AMSI**: detección encontrada mediante Antimalware Scan Interface.	Enumeración
DetId	Identificador de la detección.	Cadena de caracteres
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres
TTPs	Lista de las técnicas, tácticas y subtécnicas asociadas al evento MITRE.	Cadena de caracteres

Campo	Descripción	Valor
IOAIds	Cuando una secuencia de eventos sigue un patrón descrito en la matriz MITRE, el producto de seguridad crea un indicio (IOA) y añade su identificador a todos los eventos que lo forman.	Numérico
TelemetryType	▪ **0: telemetría normal**. El evento no pertenece a un indicio que siga un patrón descrito en la matriz MITRE. ▪ **1: evento reenviado**. El evento se envió inicialmente como tipo 0 (telemetría normal), pero tiempo después se ha detectado que pertenece a un patrón de ataque escrito en la matriz MITRE. El evento se vuelve a enviar con los campos TTPs e IOAIds completados. ▪ **2: evento acumulado**. Para ahorrar recursos, parte de la telemetría generada en el cliente se retiene hasta que el software de seguridad detecta un patrón de ataque MITRE. En ese momento se envían todos los eventos acumulados.	Enumeración

Createdir

Evento de tipo activo que se genera cuando un proceso (parent) crea un directorio (child).

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
User (CEF)	Nombre de la cuenta de usuario y dominio al que pertenece utilizada para ejecutar el proceso que genero el evento registrado.	Cadena de caracteres
MachineIP (CEF)	Nombre del equipo que desencadena el evento registrado.	Dirección IP
MachineName (CEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
sev (LEEF)	Severidad del evento	1
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
usrName (LEEF)	Cuenta de usuario utilizada por el proceso que realizó la operación registrada.	Cadena de caracteres
domain (LEEF)	Dominio de la cuenta de usuario utilizado por el proceso que realizó la operación registrada.	Cadena de caracteres
src (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identSrc (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identHostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres

Campo	Descripción	Valor
HostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
LocalDateTime	Fecha en formato UTC que tenía el equipo en el momento en que se produjo el evento registrado. Esta fecha depende de la configuración del equipo y por lo tanto puede ser errónea	Fecha
PandaTimeStatus	Contenido de los campos DateTime, Date y LocalDateTime	**0**: fecha real no soportada por tratarse de un evento antiguo. **1**: fecha real no disponible el servidor Cytomic y obtenida mediante un cálculo. **2**: fecha real proporcionada por el servidor Cytomic.
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
Op	Operación registrada.	Cadena de caracteres: “Createdir”
ParentHash	Hash del proceso que actúa como padre.	Cadena de caracteres
ParentDriveType	Tipo de unidad donde reside el proceso o fichero padre que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM	Enumeración

Campo	Descripción	Valor
	▪ **Ramdisk**: unidad de disco RAM.	
ParentPath	Ruta del fichero padre que realizó la operación registrada.	Cadena de caracteres
ParentPID	Identificador del proceso padre.	Numérico
ParentValidSig	El proceso padre está firmado digitalmente.	Booleano
ParentCompany	Contenido del atributo Company de los metadatos del proceso padre.	Cadena de caracteres
ParentBroken	El proceso padre está corrupto o defectuoso.	Booleano
ParentImageType	Arquitectura interna del proceso padre: ▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	Enumeración
ParentExeType	Estructura interna / tipo del proceso padre. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
ParentPrevalence	Prevalencia histórica del proceso padre en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ParentPrevLastDay	Prevalencia del proceso padre en el día anterior en los sistemas de Cytomic. ▪ High ▪ Medium	Enumeración

Campo	Descripción	Valor
	▪ Low	
ParentCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración
ParentMWName	Nombre del malware en el proceso padre si ya está catalogado como una amenaza. Si es Null el elemento no es malware.	Cadena de caracteres
ChildHash	Hash del proceso que actúa como hijo.	Cadena de caracteres
ChildDriveType	Tipo de unidad donde reside el proceso o fichero padre que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM ▪ **Ramdisk**: unidad de disco RAM.	Enumeración
ChildPath	Ruta del fichero hijo que realizó la operación registrada.	Cadena de caracteres (Ruta)
ChildPID	Identificador del proceso hijo.	Numérico
ChildValidSig	El proceso hijo está firmado digitalmente.	Booleano
ChildCompany	Contenido del atributo Company de los metadatos del proceso hijo.	Cadena de caracteres
ChildBroken	El proceso hijo está corrupto o defectuoso.	Booleano
ChildImageType	Arquitectura interna del proceso hijo:	Enumeración

Campo	Descripción	Valor
	▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	
ChildExeType	Estructura interna / tipo del proceso hijo. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
ChildPrevalence	Prevalencia histórica del proceso hijo en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ChildPrevLastDay	Prevalencia histórica del proceso hijo en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ChildCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración
ChildMWName	Nombre del malware en el proceso hijo si ya está catalogado como una amenaza. Si es	Cadena de caracteres

Campo	Descripción	Valor
	Null el elemento no es malware.	
OCS_Exec	Se ejecutó en el equipo software considerado como vulnerable.	Booleano
OCS_Name	Nombre del software vulnerable ejecutado.	Cadena de caracteres
OCS_Version	Versión del sistema operativo del equipo donde se ejecutó el software vulnerable.	Cadena de caracteres
Params	Parámetros de ejecución del proceso en la linea de comandos.	Cadena de caracteres
ToastResult	Respuesta del usuario ante el mensaje emergente mostrado por Cytomic. ▪ **Ok**: el cliente acepta el mensaje. ▪ **Timeout**: el mensaje emergente desaparece por la no acción del usuario. ▪ **Angry**: el usuario rechaza el bloqueo desde el mensaje emergente. ▪ **Block** ▪ **Allow**	Enumeración
Action	Acción realizada por el agente Cytomic EDR. ▪ **Allow** ▪ **Block** ▪ **BlockTimeout**: se mostró un mensaje emergente al usuario pero no contestó a tiempo. ▪ **AllowWL**: elemento permitido por encontrarse en la lista blanca del administrador. ▪ **Disinfect** ▪ **Delete** ▪ **Quarantine** ▪ **AllowByUser**: se mostró un mensaje emergente al usuario y contesto “permitir ejecución”. ▪ **Informed**: se mostró un mensaje emergente al usuario. ▪ **Unquarantine**: el fichero se sacó de la cuarentena.	Enumeración

Campo	Descripción	Valor
	▪ **Rename**: elemento renombrado por no poderse mover a cuarentena, borrar o desinfectar. ▪ **BlockURL**: se bloqueó el acceso a una URL. ▪ **KillProcess**: cierre de proceso. ▪ **BlockExploit**: intento de explotación de proceso vulnerable detenido. ▪ **ExploitAllowByUser**: el usuario no permitió el cierre del proceso explotado. ▪ **RebootNeeded**: se requiere un reinicio del equipo para bloquear el intento de explotación. ▪ **ExploitInformed**: se mostró un mensaje emergente al usuario informando de un intento de explotación de proceso vulnerable. ▪ **AllowSonGWInstaller**: el programa forma parte de un paquete de instalación clasificado como Goodware. ▪ **EmbebedInformed**: el elemento es un script en powershell que ejecuta comandos. ▪ **SuspedProcess**: el elemento intentó suspender alguno de los servicios del software de protección. ▪ **ModifyDiskResource**: el elemento intentó modificar un fichero protegido que pertenece al software de protección. ▪ **ModifyRegistry**: el elemento intentó modificar una clave de registro protegida que pertenece al software de protección. ▪ **RenameRegistry**: el elemento intentó renombrar una clave de registro protegida que pertenece al software de protección.	

Campo	Descripción	Valor
	▪ **ModifyMarkFile**: el elemento intentó renombrar un fichero protegido que pertenece al software de protección. ▪ **UncertainAction**: el elemento intentó una acción sin definir sobre un fichero que pertenece al software de protección. ▪ **AllowGWFilter**: se permite la ejecución del elemento por estar en la caché de goodware. ▪ **AllowSWAuthoriced**: se permite la ejecución del elemento por estar autorizado por el administrador (configuración Software Autorizado). ▪ **NewPE**: aparición de un nuevo programa ejecutable en el equipo que viene del exterior. ▪ **AllowedByAdmin**: se permite la ejecución del elemento porque el administrador excluyó la técnica de explotación detectada. ▪ **Blocked by ip**: se bloqueó la dirección IP de origen por detectarse un ataque de fuerza bruta mediante el protocolo RDP. ▪ **AllowSonMsiGW**: se permite la ejecución del elemento por tratarse de un ejecutable que proviene de un paquete de instalación confiable. ▪ **Allowed by Global Audit**: el elemento se permite porque el software de seguridad está configurado en modo Global Audit.	
ServiceLevel	Modo de ejecución del agente: ▪ **Blocking**: el agente bloquea todos los ejecutables sin clasificar y los clasificados como malware. ▪ **Hardening**: el agente bloquea la ejecución de todos los programas sin clasificar cuyo origen no sea confiable y los clasificados como malware.	Enumeración

Campo	Descripción	Valor
	▪ **Learning**: el agente no bloquea ningún programa pero monitoriza los procesos ejecutados.	
WinningTech	Tecnología que provocó el evento. ▪ **Blockmode**: el agente estaba en modo Lock en el momento del bloqueo. ▪ **Cache**: clasificación cacheada en local. ▪ **Cloud**: clasificación descargada de la nube. ▪ **Context**: regla de contexto local. ▪ **ContextMinerva**: regla de contexto en la nube. ▪ **Digital Signature**: fichero firmado digitalmente. ▪ **Exploit**: tecnología de identificación de intento de explotación de proceso vulnerable. ▪ **ExploitLegacy** ▪ **GWFilter**: tecnologías de identificación de ficheros GW desconocidos. ▪ **LegacyUser**: permiso solicitado al usuario. ▪ **Local Signature**: firma local. ▪ **MetaEsploit**: ataque generado con el framework metaExploit. ▪ **NetNative**: tipo de binario. ▪ **Serializer**: tipo de binario. ▪ **User**: permiso solicitado al usuario. ▪ **RDP**: ataque de fuerza bruta por el protocolo RDP. ▪ **AMSI**: detección encontrada mediante Antimalware Scan Interface.	Enumeración
DetId	Identificador de la detección.	Cadena de caracteres
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres

Campo	Descripción	Valor
TTPs	Lista de las técnicas, tácticas y subtécnicas asociadas al evento MITRE.	Cadena de caracteres
IOAIds	Cuando una secuencia de eventos sigue un patrón descrito en la matriz MITRE, el producto de seguridad crea un indicio (IOA) y añade su identificador a todos los eventos que lo forman.	Numérico
TelemetryType	▪ **0: telemetría normal**. El evento no pertenece a un indicio que siga un patrón descrito en la matriz MITRE. ▪ **1: evento reenviado**. El evento se envió inicialmente como tipo 0 (telemetría normal), pero tiempo después se ha detectado que pertenece a un patrón de ataque escrito en la matriz MITRE. El evento se vuelve a enviar con los campos TTPs e IOAIds completados. ▪ **2: evento acumulado**. Para ahorrar recursos, parte de la telemetría generada en el cliente se retiene hasta que el software de seguridad detecta un patrón de ataque MITRE. En ese momento se envían todos los eventos acumulados.	Enumeración

CreatePE

Evento de tipo activo que se genera cuando un proceso (parent) crea un nuevo fichero ejecutable (child).

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
User (CEF)	Nombre de la cuenta de usuario y dominio al que pertenece utilizada para ejecutar el proceso que genero el evento registrado.	Cadena de caracteres
MachineIP (CEF)	Nombre del equipo que desencadena el evento registrado.	Dirección IP
MachineName (CEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
sev (LEEF)	Severidad del evento.	1
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
usrName (LEEF)	Cuenta de usuario utilizada por el proceso que realizó la operación registrada.	Cadena de caracteres
domain (LEEF)	Dominio de la cuenta de usuario utilizado por el proceso que realizó la operación registrada.	Cadena de caracteres
src (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identSrc (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identHostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres

Campo	Descripción	Valor
HostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
LocalDateTime	Fecha en formato UTC que tenía el equipo en el momento en que se produjo el evento registrado. Esta fecha depende de la configuración del equipo y por lo tanto puede ser errónea	Fecha
PandaTimeStatus	Contenido de los campos DateTime, Date y LocalDateTime	**0**: fecha real no soportada por tratarse de un evento antiguo. **1**: fecha real no disponible el servidor Cytomic y obtenida mediante un cálculo. **2**: fecha real proporcionada por el servidor Cytomic.
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
Op	Operación registrada.	Cadena de caracteres: “CreatePE”
ParentHash	Hash del proceso que actúa como padre.	Cadena de caracteres
ParentDriveType	Tipo de unidad donde reside el proceso o fichero padre que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM	Enumeración

Campo	Descripción	Valor
	▪ **Ramdisk**: unidad de disco RAM.	
ParentPath	Ruta del fichero padre que realizó la operación registrada.	Cadena de caracteres
ParentPID	Identificador del proceso padre.	Numérico
ParentValidSig	El proceso padre está firmado digitalmente.	Booleano
ParentCompany	Contenido del atributo Company de los metadatos del proceso padre.	Cadena de caracteres
ParentBroken	El proceso padre está corrupto o defectuoso.	Booleano
ParentImageType	Arquitectura interna del proceso padre: ▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	Enumeración
ParentExeType	Estructura interna / tipo del proceso padre. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
ParentPrevalence	Prevalencia histórica del proceso padre en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ParentPrevLastDay	Prevalencia del proceso padre en el día anterior en los sistemas de Cytomic. ▪ High ▪ Medium	Enumeración

Campo	Descripción	Valor
	▪ Low	
ParentCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración
ParentMWName	Nombre del malware en el proceso padre si ya está catalogado como una amenaza. Si es Null el elemento no es malware.	Cadena de caracteres
ChildHash	Hash del proceso que actúa como hijo.	Cadena de caracteres
ChildDriveType	Tipo de unidad donde reside el proceso o fichero padre que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM ▪ **Ramdisk**: unidad de disco RAM.	Enumeración
ChildPath	Ruta del fichero hijo que realizó la operación registrada.	Cadena de caracteres (Ruta)
ChildPID	Identificador del proceso hijo.	Numérico
ChildValidSig	El proceso hijo está firmado digitalmente.	Booleano
ChildCompany	Contenido del atributo Company de los metadatos del proceso hijo.	Cadena de caracteres
ChildBroken	El proceso hijo está corrupto o defectuoso.	Booleano
ChildImageType	Arquitectura interna del proceso hijo:	Enumeración

Campo	Descripción	Valor
	▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	
ChildExeType	Estructura interna / tipo del proceso hijo. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
ChildPrevalence	Prevalencia histórica del proceso hijo en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ChildPrevLastDay	Prevalencia histórica del proceso hijo en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ChildCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración
ChildMWName	Nombre del malware en el proceso hijo si ya está catalogado como una amenaza. Si es	Cadena de caracteres

Campo	Descripción	Valor
	Null el elemento no es malware.	
OCS_Exec	Se ejecutó en el equipo software considerado como vulnerable.	Booleano
OCS_Name	Nombre del software vulnerable ejecutado.	Cadena de caracteres
OCS_Version	Versión del sistema operativo del equipo donde se ejecutó el software vulnerable.	Cadena de caracteres
Params	Parámetros de ejecución del proceso en la linea de comandos.	Cadena de caracteres
ToastResult	Respuesta del usuario ante el mensaje emergente mostrado por Cytomic EDR. ▪ **Ok**: el cliente acepta el mensaje. ▪ **Timeout**: el mensaje emergente desaparece por la no acción del usuario. ▪ **Angry**: el usuario rechaza el bloqueo desde el mensaje emergente. ▪ **Block** ▪ **Allow**	Enumeración
Action	Acción realizada por el agente Cytomic. ▪ **Allow** ▪ **Block** ▪ **BlockTimeout**: se mostró un mensaje emergente al usuario pero no contestó a tiempo. ▪ **AllowWL**: elemento permitido por encontrarse en la lista blanca del administrador. ▪ **Disinfect** ▪ **Delete** ▪ **Quarantine** ▪ **AllowByUser**: se mostró un mensaje emergente al usuario y contesto “permitir ejecución”. ▪ **Informed**: se mostró un mensaje emergente al usuario. ▪ **Unquarantine**: el fichero se sacó de la cuarentena.	Enumeración

Campo	Descripción	Valor
	▪ **Rename**: elemento renombrado por no poderse mover a cuarentena, borrar o desinfectar. ▪ **BlockURL**: se bloqueó el acceso a una URL. ▪ **KillProcess**: cierre de proceso. ▪ **BlockExploit**: intento de explotación de proceso vulnerable detenido. ▪ **ExploitAllowByUser**: el usuario no permitió el cierre del proceso explotado. ▪ **RebootNeeded**: se requiere un reinicio del equipo para bloquear el intento de explotación. ▪ **ExploitInformed**: se mostró un mensaje emergente al usuario informando de un intento de explotación de proceso vulnerable. ▪ **AllowSonGWInstaller**: el programa forma parte de un paquete de instalación clasificado como Goodware. ▪ **EmbebedInformed**: el elemento es un script en powershell que ejecuta comandos. ▪ **SuspedProcess**: el elemento intentó suspender alguno de los servicios del software de protección. ▪ **ModifyDiskResource**: el elemento intentó modificar un fichero protegido que pertenece al software de protección. ▪ **ModifyRegistry**: el elemento intentó modificar una clave de registro protegida que pertenece al software de protección. ▪ **RenameRegistry**: el elemento intentó renombrar una clave de registro protegida que pertenece al software de protección.	

Campo	Descripción	Valor
	▪ **ModifyMarkFile**: el elemento intentó renombrar un fichero protegido que pertenece al software de protección. ▪ **UncertainAction**: el elemento intentó una acción sin definir sobre un fichero que pertenece al software de protección. ▪ **AllowGWFilter**: se permite la ejecución del elemento por estar en la caché de goodware. ▪ **AllowSWAuthoriced**: se permite la ejecución del elemento por estar autorizado por el administrador (configuración Software Autorizado). ▪ **NewPE**: aparición de un nuevo programa ejecutable en el equipo que viene del exterior. ▪ **AllowedByAdmin**: se permite la ejecución del elemento porque el administrador excluyó la técnica de explotación detectada. ▪ **Blocked by ip**: se bloqueó la dirección IP de origen por detectarse un ataque de fuerza bruta mediante el protocolo RDP. ▪ **AllowSonMsiGW**: se permite la ejecución del elemento por tratarse de un ejecutable que proviene de un paquete de instalación confiable. ▪ **Allowed by Global Audit**: el elemento se permite porque el software de seguridad está configurado en modo Global Audit.	
ServiceLevel	Modo de ejecución del agente: ▪ **Blocking**: el agente bloquea todos los ejecutables sin clasificar y los clasificados como malware. ▪ **Hardening**: el agente bloquea la ejecución de todos los programas sin clasificar cuyo origen no sea confiable y los clasificados como malware.	Enumeración

Campo	Descripción	Valor
	▪ **Learning**: el agente no bloquea ningún programa pero monitoriza los procesos ejecutados.	
WinningTech	Tecnología que provocó el evento. ▪ **Blockmode**: el agente estaba en modo Lock en el momento del bloqueo. ▪ **Cache**: clasificación cacheada en local. ▪ **Cloud**: clasificación descargada de la nube. ▪ **Context**: regla de contexto local. ▪ **ContextMinerva**: regla de contexto en la nube. ▪ **Digital Signature**: fichero firmado digitalmente. ▪ **Exploit**: tecnología de identificación de intento de explotación de proceso vulnerable. ▪ **ExploitLegacy** ▪ **GWFilter**: tecnologías de identificación de ficheros GW desconocidos. ▪ **LegacyUser**: permiso solicitado al usuario. ▪ **Local Signature**: firma local. ▪ **MetaEsploit**: ataque generado con el framework metaExploit. ▪ **NetNative**: tipo de binario. ▪ **Serializer**: tipo de binario. ▪ **User**: permiso solicitado al usuario. ▪ **RDP**: ataque de fuerza bruta por el protocolo RDP. ▪ **AMSI**: detección encontrada mediante Antimalware Scan Interface.	Enumeración
DetId	Identificador de la detección.	Cadena de caracteres
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres

Campo	Descripción	Valor
TTPs	Lista de las técnicas, tácticas y subtécnicas asociadas al evento MITRE.	Cadena de caracteres
IOAIds	Cuando una secuencia de eventos sigue un patrón descrito en la matriz MITRE, el producto de seguridad crea un indicio (IOA) y añade su identificador a todos los eventos que lo forman.	Numérico
TelemetryType	▪ **0: telemetría normal**. El evento no pertenece a un indicio que siga un patrón descrito en la matriz MITRE. ▪ **1: evento reenviado**. El evento se envió inicialmente como tipo 0 (telemetría normal), pero tiempo después se ha detectado que pertenece a un patrón de ataque escrito en la matriz MITRE. El evento se vuelve a enviar con los campos TTPs e IOAIds completados. ▪ **2: evento acumulado**. Para ahorrar recursos, parte de la telemetría generada en el cliente se retiene hasta que el software de seguridad detecta un patrón de ataque MITRE. En ese momento se envían todos los eventos acumulados.	Enumeración

CreateprocessbyWMI

Evento de tipo activo que se genera cuando un proceso (parent) crea un proceso (child) a través del sistema WMI.

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
User (CEF)	Nombre de la cuenta de usuario y dominio al que pertenece utilizada para ejecutar el proceso que genero el evento registrado.	Cadena de caracteres
MachineIP (CEF)	Nombre del equipo que desencadena el evento registrado.	Dirección IP
MachineName (CEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
sev (LEEF)	Severidad del evento.	1
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
usrName (LEEF)	Cuenta de usuario utilizada por el proceso que realizó la operación registrada.	Cadena de caracteres
domain (LEEF)	Dominio de la cuenta de usuario utilizado por el proceso que realizó la operación registrada.	Cadena de caracteres
src (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identSrc (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identHostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres

Campo	Descripción	Valor
HostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
LocalDateTime	Fecha en formato UTC que tenía el equipo en el momento en que se produjo el evento registrado. Esta fecha depende de la configuración del equipo y por lo tanto puede ser errónea	Fecha
PandaTimeStatus	Contenido de los campos DateTime, Date y LocalDateTime	**0**: fecha real no soportada por tratarse de un evento antiguo. **1**: fecha real no disponible el servidor Cytomic y obtenida mediante un cálculo. **2**: fecha real proporcionada por el servidor Cytomic.
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
Op	Operación registrada.	Cadena de caracteres: “CreateprocessbyWMI”
ParentHash	Hash del proceso que actúa como padre.	Cadena de caracteres
ParentDriveType	Tipo de unidad donde reside el proceso o fichero padre que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada.	Enumeración

Campo	Descripción	Valor
	▪ **Cdrom**: unidad de CD-ROM ▪ **Ramdisk**: unidad de disco RAM.	
ParentPath	Ruta del fichero padre que realizó la operación registrada.	Cadena de caracteres
ParentPID	Identificador del proceso padre.	Numérico
ParentValidSig	El proceso padre está firmado digitalmente.	Booleano
ParentCompany	Contenido del atributo Company de los metadatos del proceso padre.	Cadena de caracteres
ParentBroken	El proceso padre está corrupto o defectuoso.	Booleano
ParentImageType	Arquitectura interna del proceso padre: ▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	Enumeración
ParentExeType	Estructura interna / tipo del proceso padre. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
ParentPrevalence	Prevalencia histórica del proceso padre en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ParentPrevLastDay	Prevalencia del proceso padre en el día anterior en los sistemas de Cytomic.	Enumeración

Campo	Descripción	Valor
	▪ High ▪ Medium ▪ Low	
ParentCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración
ParentMWName	Nombre del malware en el proceso padre si ya está catalogado como una amenaza. Si es Null el elemento no es malware.	Cadena de caracteres
ChildHash	Hash del proceso que actúa como hijo.	Cadena de caracteres
ChildDriveType	Tipo de unidad donde reside el proceso o fichero padre que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM ▪ **Ramdisk**: unidad de disco RAM.	Enumeración
ChildPath	Ruta del fichero hijo que realizó la operación registrada.	Cadena de caracteres (Ruta)
ChildPID	Identificador del proceso hijo.	Numérico
ChildValidSig	El proceso hijo está firmado digitalmente.	Booleano
ChildCompany	Contenido del atributo Company de los metadatos del proceso hijo.	Cadena de caracteres
ChildBroken	El proceso hijo está corrupto o defectuoso.	Booleano

Campo	Descripción	Valor
ChildImageType	Arquitectura interna del proceso hijo: ▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	Enumeración
ChildExeType	Estructura interna / tipo del proceso hijo. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
ChildPrevalence	Prevalencia histórica del proceso hijo en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ChildPrevLastDay	Prevalencia histórica del proceso hijo en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ChildCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración

Campo	Descripción	Valor
ChildMWName	Nombre del malware en el proceso hijo si ya está catalogado como una amenaza. Si es Null el elemento no es malware.	Cadena de caracteres
OCS_Exec	Se ejecutó en el equipo software considerado como vulnerable.	Booleano
OCS_Name	Nombre del software vulnerable ejecutado.	Cadena de caracteres
OCS_Version	Versión del sistema operativo del equipo donde se ejecutó el software vulnerable.	Cadena de caracteres
Params	Parámetros de ejecución del proceso en la linea de comandos.	Cadena de caracteres
ToastResult	Respuesta del usuario ante el mensaje emergente mostrado por Cytomic. ▪ **Ok**: el cliente acepta el mensaje. ▪ **Timeout**: el mensaje emergente desaparece por la no acción del usuario. ▪ **Angry**: el usuario rechaza el bloqueo desde el mensaje emergente. ▪ **Block** ▪ **Allow**	Enumeración
Action	Acción realizada por el agente Cytomic. ▪ **Allow** ▪ **Block** ▪ **BlockTimeout**: se mostró un mensaje emergente al usuario pero no contestó a tiempo. ▪ **AllowWL**: elemento permitido por encontrarse en la lista blanca del administrador. ▪ **Disinfect** ▪ **Delete** ▪ **Quarantine** ▪ **AllowByUser**: se mostró un mensaje emergente al usuario y contesto “permitir ejecución”. ▪ **Informed**: se mostró un mensaje emergente al usuario.	Enumeración

Campo	Descripción	Valor
	▪ **Unquarantine**: el fichero se sacó de la cuarentena. ▪ **Rename**: elemento renombrado por no poderse mover a cuarentena, borrar o desinfectar. ▪ **BlockURL**: se bloqueó el acceso a una URL. ▪ **KillProcess**: cierre de proceso. ▪ **BlockExploit**: intento de explotación de proceso vulnerable detenido. ▪ **ExploitAllowByUser**: el usuario no permitió el cierre del proceso explotado. ▪ **RebootNeeded**: se requiere un reinicio del equipo para bloquear el intento de explotación. ▪ **ExploitInformed**: se mostró un mensaje emergente al usuario informando de un intento de explotación de proceso vulnerable. ▪ **AllowSonGWInstaller**: el programa forma parte de un paquete de instalación clasificado como Goodware. ▪ **EmbebedInformed**: el elemento es un script en powershell que ejecuta comandos. ▪ **SuspedProcess**: el elemento intentó suspender alguno de los servicios del software de protección. ▪ **ModifyDiskResource:** el elemento intentó modificar un fichero protegido que pertenece al software de protección. ▪ **ModifyRegistry**: el elemento intentó modificar una clave de registro protegida que pertenece al software de protección.	

Campo	Descripción	Valor
	▪ **RenameRegistry**: el elemento intentó renombrar una clave de registro protegida que pertenece al software de protección. ▪ **ModifyMarkFile:** el elemento intentó renombrar un fichero protegido que pertenece al software de protección. ▪ **UncertainAction**: el elemento intentó una acción sin definir sobre un fichero que pertenece al software de protección. ▪ **AllowGWFilter**: se permite la ejecución del elemento por estar en la caché de goodware. ▪ **AllowSWAuthoriced**: se permite la ejecución del elemento por estar autorizado por el administrador (configuración Software Autorizado). ▪ **NewPE**: aparición de un nuevo programa ejecutable en el equipo que viene del exterior. ▪ **AllowedByAdmin**: se permite la ejecución del elemento porque el administrador excluyó la técnica de explotación detectada. ▪ **Blocked by ip**: se bloqueó la dirección IP de origen por detectarse un ataque de fuerza bruta mediante el protocolo RDP. ▪ **AllowSonMsiGW**: se permite la ejecución del elemento por tratarse de un ejecutable que proviene de un paquete de instalación confiable. ▪ **Allowed by Global Audit**: el elemento se permite porque el software de seguridad está configurado en modo Global Audit.	
ServiceLevel	Modo de ejecución del agente: ▪ **Blocking**: el agente bloquea todos los ejecutables sin clasificar y los clasificados como malware.	Enumeración

Campo	Descripción	Valor
	▪ **Hardening**: el agente bloquea la ejecución de todos los programas sin clasificar cuyo origen no sea confiable y los clasificados como malware. ▪ **Learning**: el agente no bloquea ningún programa pero monitoriza los procesos ejecutados.	
WinningTech	Tecnología que provocó el evento. ▪ **Blockmode**: el agente estaba en modo Lock en el momento del bloqueo. ▪ **Cache**: clasificación cacheada en local. ▪ **Cloud**: clasificación descargada de la nube. ▪ **Context**: regla de contexto local. ▪ **ContextMinerva**: regla de contexto en la nube. ▪ **Digital Signature**: fichero firmado digitalmente. ▪ **Exploit**: tecnología de identificación de intento de explotación de proceso vulnerable. ▪ **ExploitLegacy** ▪ **GWFilter**: tecnologías de identificación de ficheros GW desconocidos. ▪ **LegacyUser**: permiso solicitado al usuario. ▪ **Local Signature**: firma local. ▪ **MetaEsploit**: ataque generado con el framework metaExploit. ▪ **NetNative**: tipo de binario. ▪ **Serializer**: tipo de binario. ▪ **User**: permiso solicitado al usuario. ▪ **RDP**: ataque de fuerza bruta por el protocolo RDP.	Enumeración

Campo	Descripción	Valor
	▪ **AMSI**: detección encontrada mediante Antimalware Scan Interface.	
DetId	Identificador de la detección.	Cadena de caracteres
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres

Createremotethread

Evento de tipo activo que se genera cuando un proceso (parent) crea un hilo de ejecución remoto.

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
User (CEF)	Nombre de la cuenta de usuario y dominio al que pertenece utilizada para ejecutar el proceso que genero el evento registrado.	Cadena de caracteres
MachineIP (CEF)	Nombre del equipo que desencadena el evento registrado.	Dirección IP
MachineName (CEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
sev (LEEF)	Severidad del evento.	1
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
usrName (LEEF)	Cuenta de usuario utilizada por el proceso que realizó la operación registrada.	Cadena de caracteres
domain (LEEF)	Dominio de la cuenta de usuario utilizado por el proceso que realizó la operación registrada.	Cadena de caracteres
src (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identSrc (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identHostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres

Campo	Descripción	Valor
HostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
LocalDateTime	Fecha en formato UTC que tenía el equipo en el momento en que se produjo el evento registrado. Esta fecha depende de la configuración del equipo y por lo tanto puede ser errónea	Fecha
PandaTimeStatus	Contenido de los campos DateTime, Date y LocalDateTime	**0**: fecha real no soportada por tratarse de un evento antiguo. **1**: fecha real no disponible el servidor Cytomic y obtenida mediante un cálculo. **2**: fecha real proporcionada por el servidor Cytomic.
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
Op	Operación registrada.	Cadena de caracteres: “Createremotethread”
ParentHash	Hash del proceso que actúa como padre.	Cadena de caracteres
ParentDriveType	Tipo de unidad donde reside el proceso o fichero padre que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM	Enumeración

Campo	Descripción	Valor
	▪ **Ramdisk**: unidad de disco RAM.	
ParentPath	Ruta del fichero padre que realizó la operación registrada.	Cadena de caracteres
ParentPID	Identificador del proceso padre.	Numérico
ParentValidSig	El proceso padre está firmado digitalmente.	Booleano
ParentCompany	Contenido del atributo Company de los metadatos del proceso padre.	Cadena de caracteres
ParentBroken	El proceso padre está corrupto o defectuoso.	Booleano
ParentImageType	Arquitectura interna del proceso padre: ▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	Enumeración
ParentExeType	Estructura interna / tipo del proceso padre. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
ParentPrevalence	Prevalencia histórica del proceso padre en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ParentPrevLastDay	Prevalencia del proceso padre en el día anterior en los sistemas de Cytomic. ▪ High ▪ Medium	Enumeración

Campo	Descripción	Valor
	▪ Low	
ParentCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración
ParentMWName	Nombre del malware en el proceso padre si ya está catalogado como una amenaza. Si es Null el elemento no es malware.	Cadena de caracteres
ChildHash	Hash del proceso que actúa como hijo.	Cadena de caracteres
ChildDriveType	Tipo de unidad donde reside el proceso o fichero padre que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM ▪ **Ramdisk**: unidad de disco RAM.	Enumeración
ChildPath	Ruta del fichero hijo que realizó la operación registrada.	Cadena de caracteres (Ruta)
ChildPID	Identificador del proceso hijo.	Numérico
ChildValidSig	El proceso hijo está firmado digitalmente.	Booleano
ChildCompany	Contenido del atributo Company de los metadatos del proceso hijo.	Cadena de caracteres
ChildBroken	El proceso hijo está corrupto o defectuoso.	Booleano
ChildImageType	Arquitectura interna del proceso hijo:	Enumeración

Campo	Descripción	Valor
	▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	
ChildExeType	Estructura interna / tipo del proceso hijo. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
ChildPrevalence	Prevalencia histórica del proceso hijo en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ChildPrevLastDay	Prevalencia histórica del proceso hijo en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ChildCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración
ChildMWName	Nombre del malware en el proceso hijo si ya está catalogado como una amenaza. Si es	Cadena de caracteres

Campo	Descripción	Valor
	Null el elemento no es malware.	
OCS_Exec	Se ejecutó en el equipo software considerado como vulnerable.	Booleano
OCS_Name	Nombre del software vulnerable ejecutado.	Cadena de caracteres
OCS_Version	Versión del sistema operativo del equipo donde se ejecutó el software vulnerable.	Cadena de caracteres
Params	Parámetros de ejecución del proceso en la linea de comandos.	Cadena de caracteres
ToastResult	Respuesta del usuario ante el mensaje emergente mostrado por Cytomic EDR. ▪ **Ok**: el cliente acepta el mensaje. ▪ **Timeout**: el mensaje emergente desaparece por la no acción del usuario. ▪ **Angry**: el usuario rechaza el bloqueo desde el mensaje emergente. ▪ **Block** ▪ **Allow**	Enumeración
Action	Acción realizada por el agente Cytomic EDR. ▪ **Allow** ▪ **Block** ▪ **BlockTimeout**: se mostró un mensaje emergente al usuario pero no contestó a tiempo. ▪ **AllowWL**: elemento permitido por encontrarse en la lista blanca del administrador. ▪ **Disinfect** ▪ **Delete** ▪ **Quarantine** ▪ **AllowByUser**: se mostró un mensaje emergente al usuario y contesto “permitir ejecución”. ▪ **Informed**: se mostró un mensaje emergente al usuario. ▪ **Unquarantine**: el fichero se sacó de la cuarentena.	Enumeración

Campo	Descripción	Valor
	▪ **Rename**: elemento renombrado por no poderse mover a cuarentena, borrar o desinfectar. ▪ **BlockURL**: se bloqueó el acceso a una URL. ▪ **KillProcess**: cierre de proceso. ▪ **BlockExploit**: intento de explotación de proceso vulnerable detenido. ▪ **ExploitAllowByUser**: el usuario no permitió el cierre del proceso explotado. ▪ **RebootNeeded**: se requiere un reinicio del equipo para bloquear el intento de explotación. ▪ **ExploitInformed**: se mostró un mensaje emergente al usuario informando de un intento de explotación de proceso vulnerable. ▪ **AllowSonGWInstaller**: el programa forma parte de un paquete de instalación clasificado como Goodware. ▪ **EmbebedInformed**: el elemento es un script en powershell que ejecuta comandos. ▪ **SuspedProcess**: el elemento intentó suspender alguno de los servicios del software de protección. ▪ **ModifyDiskResource**: el elemento intentó modificar un fichero protegido que pertenece al software de protección. ▪ **ModifyRegistry**: el elemento intentó modificar una clave de registro protegida que pertenece al software de protección. ▪ **RenameRegistry**: el elemento intentó renombrar una clave de registro protegida que pertenece al software de protección.	

Campo	Descripción	Valor
	▪ **ModifyMarkFile**: el elemento intentó renombrar un fichero protegido que pertenece al software de protección. ▪ **UncertainAction**: el elemento intentó una acción sin definir sobre un fichero que pertenece al software de protección. ▪ **AllowGWFilter**: se permite la ejecución del elemento por estar en la caché de goodware. ▪ **AllowSWAuthoriced**: se permite la ejecución del elemento por estar autorizado por el administrador (configuración Software Autorizado). ▪ **NewPE**: aparición de un nuevo programa ejecutable en el equipo que viene del exterior. ▪ **AllowedByAdmin**: se permite la ejecución del elemento porque el administrador excluyó la técnica de explotación detectada. ▪ **Blocked by ip**: se bloqueó la dirección IP de origen por detectarse un ataque de fuerza bruta mediante el protocolo RDP. ▪ **AllowSonMsiGW**: se permite la ejecución del elemento por tratarse de un ejecutable que proviene de un paquete de instalación confiable. ▪ **Allowed by Global Audit**: el elemento se permite porque el software de seguridad está configurado en modo Global Audit.	
ServiceLevel	Modo de ejecución del agente: ▪ **Blocking**: el agente bloquea todos los ejecutables sin clasificar y los clasificados como malware. ▪ **Hardening**: el agente bloquea la ejecución de todos los programas sin clasificar cuyo origen no sea confiable y los clasificados como malware.	Enumeración

Campo	Descripción	Valor
	▪ **Learning**: el agente no bloquea ningún programa pero monitoriza los procesos ejecutados.	
WinningTech	Tecnología que provocó el evento. ▪ **Blockmode**: el agente estaba en modo Lock en el momento del bloqueo. ▪ **Cache**: clasificación cacheada en local. ▪ **Cloud**: clasificación descargada de la nube. ▪ **Context**: regla de contexto local. ▪ **ContextMinerva**: regla de contexto en la nube. ▪ **Digital Signature**: fichero firmado digitalmente. ▪ **Exploit**: tecnología de identificación de intento de explotación de proceso vulnerable. ▪ **ExploitLegacy** ▪ **GWFilter**: tecnologías de identificación de ficheros GW desconocidos. ▪ **LegacyUser**: permiso solicitado al usuario. ▪ **Local Signature**: firma local. ▪ **MetaEsploit**: ataque generado con el framework metaExploit. ▪ **NetNative**: tipo de binario. ▪ **Serializer**: tipo de binario. ▪ **User**: permiso solicitado al usuario. ▪ **RDP**: ataque de fuerza bruta por el protocolo RDP. ▪ **AMSI**: detección encontrada mediante Antimalware Scan Interface.	Enumeración
DetId	Identificador de la detección.	Cadena de caracteres
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres
TTPs	Lista de las técnicas, tácticas y subtécnicas	Cadena de caracteres

Campo	Descripción	Valor
	asociadas al evento MITRE.	
IOAIds	Cuando una secuencia de eventos sigue un patrón descrito en la matriz MITRE, el producto de seguridad crea un indicio (IOA) y añade su identificador a todos los eventos que lo forman.	Numérico
TelemetryType	▪ **0: telemetría normal**. El evento no pertenece a un indicio que siga un patrón descrito en la matriz MITRE. ▪ **1: evento reenviado**. El evento se envió inicialmente como tipo 0 (telemetría normal), pero tiempo después se ha detectado que pertenece a un patrón de ataque escrito en la matriz MITRE. El evento se vuelve a enviar con los campos TTPs e IOAIds completados. ▪ **2: evento acumulado**. Para ahorrar recursos, parte de la telemetría generada en el cliente se retiene hasta que el software de seguridad detecta un patrón de ataque MITRE. En ese momento se envían todos los eventos acumulados.	Enumeración

Criticalsoft

Evento de tipo pasivo que se genera cuando se ejecuta una aplicación vulnerable.

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
User (CEF)	Nombre de la cuenta de usuario y dominio al que pertenece utilizada para ejecutar el proceso que genero el evento registrado.	Cadena de caracteres
MachineIP (CEF)	Nombre del equipo que desencadena el evento registrado.	Dirección IP
MachineName (CEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
sev (LEEF)	Severidad del evento.	1
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
usrName (LEEF)	Cuenta de usuario utilizada por el proceso que realizó la operación registrada.	Cadena de caracteres
domain (LEEF)	Dominio de la cuenta de usuario utilizado por el proceso que realizó la operación registrada.	Cadena de caracteres
src (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identSrc (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identHostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres

Campo	Descripción	Valor
HostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
LocalDateTime	Fecha en formato UTC que tenía el equipo en el momento en que se produjo el evento registrado. Esta fecha depende de la configuración del equipo y por lo tanto puede ser errónea	Fecha
PandaTimeStatus	Contenido de los campos DateTime, Date y LocalDateTime	**0**: fecha real no soportada por tratarse de un evento antiguo. **1**: fecha real no disponible el servidor Cytomic y obtenida mediante un cálculo. **2**: fecha real proporcionada por el servidor Cytomic.
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
CriticalSoftEventType	▪ **True**: el software vulnerable se ejecuto en el equipo. ▪ **False**: el software vulnerable fue visto en el equipo pero no se ejecutó.	Booleano
ItemHash	Hash / digest de la amenaza o programa vulnerable encontrada.	Cadena de caracteres
Filename	Nombre del fichero vulnerable.	Cadena de caracteres
FilePath	Ruta completa donde se encuentra el fichero vulnerable.	Cadena de caracteres
Size	Tamaño del fichero vulnerable.	Numérico
InternalName	Contenido del atributo Name de los metadatos del fichero vulnerable.	Numérico
CompanyName	Contenido del atributo Company de los metadatos del fichero vulnerable.	Cadena de caracteres

Campo	Descripción	Valor
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
FilePlatform	Arquitectura interna del fichero ▪ Win32NT ▪ Win64NT	Enumeración
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres

DeletePE

Evento de tipo activo que se genera cuando un proceso (parent) borra un programa ejecutable (child).

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
User (CEF)	Nombre de la cuenta de usuario y dominio al que pertenece utilizada para ejecutar el proceso que genero el evento registrado.	Cadena de caracteres
MachineIP (CEF)	Nombre del equipo que desencadena el evento registrado.	Dirección IP
MachineName (CEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
sev (LEEF)	Severidad del evento.	1
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
usrName (LEEF)	Cuenta de usuario utilizada por el proceso que realizó la operación registrada.	Cadena de caracteres
domain (LEEF)	Dominio de la cuenta de usuario utilizado por el proceso que realizó la operación registrada.	Cadena de caracteres
src (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identSrc (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identHostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres

Campo	Descripción	Valor
HostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
LocalDateTime	Fecha en formato UTC que tenía el equipo en el momento en que se produjo el evento registrado. Esta fecha depende de la configuración del equipo y por lo tanto puede ser errónea	Fecha
PandaTimeStatus	Contenido de los campos DateTime, Date y LocalDateTime	**0**: fecha real no soportada por tratarse de un evento antiguo. **1**: fecha real no disponible el servidor Cytomic y obtenida mediante un cálculo. **2**: fecha real proporcionada por el servidor Cytomic.
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
Op	Operación registrada.	Cadena de caracteres: “DeletePE”
ParentHash	Hash del proceso que actúa como padre.	Cadena de caracteres
ParentDriveType	Tipo de unidad donde reside el proceso o fichero padre que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM ▪ **Ramdisk**: unidad de disco RAM.	Enumeración

Campo	Descripción	Valor
ParentPath	Ruta del fichero padre que realizó la operación registrada.	Cadena de caracteres
ParentPID	Identificador del proceso padre.	Numérico
ParentValidSig	El proceso padre está firmado digitalmente.	Booleano
ParentCompany	Contenido del atributo Company de los metadatos del proceso padre.	Cadena de caracteres
ParentBroken	El proceso padre está corrupto o defectuoso.	Booleano
ParentImageType	Arquitectura interna del proceso padre: ▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	Enumeración
ParentExeType	Estructura interna / tipo del proceso padre. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
ParentPrevalence	Prevalencia histórica del proceso padre en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ParentPrevLastDay	Prevalencia del proceso padre en el día anterior en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración

Campo	Descripción	Valor
ParentCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración
ParentMWName	Nombre del malware en el proceso padre si ya está catalogado como una amenaza. Si es Null el elemento no es malware.	Cadena de caracteres
ChildHash	Hash del proceso que actúa como hijo.	Cadena de caracteres
ChildDriveType	Tipo de unidad donde reside el proceso o fichero padre que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM ▪ **Ramdisk**: unidad de disco RAM.	Enumeración
ChildPath	Ruta del fichero hijo que realizó la operación registrada.	Cadena de caracteres (Ruta)
ChildPID	Identificador del proceso hijo.	Numérico
ChildValidSig	El proceso hijo está firmado digitalmente.	Booleano
ChildCompany	Contenido del atributo Company de los metadatos del proceso hijo.	Cadena de caracteres
ChildBroken	El proceso hijo está corrupto o defectuoso.	Booleano
ChildImageType	Arquitectura interna del proceso hijo: ▪ EXEx32 ▪ EXEx64	Enumeración

Campo	Descripción	Valor
	▪ DLLx32 ▪ DLLx64	
ChildExeType	Estructura interna / tipo del proceso hijo. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
ChildPrevalence	Prevalencia histórica del proceso hijo en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ChildPrevLastDay	Prevalencia histórica del proceso hijo en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ChildCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración
ChildMWName	Nombre del malware en el proceso hijo si ya está catalogado como una amenaza. Si es Null el elemento no es malware.	Cadena de caracteres
OCS_Exec	Se ejecutó en el equipo software considerado	Booleano

Campo	Descripción	Valor
	como vulnerable.	
OCS_Name	Nombre del software vulnerable ejecutado.	Cadena de caracteres
OCS_Version	Versión del sistema operativo del equipo donde se ejecutó el software vulnerable.	Cadena de caracteres
Params	Parámetros de ejecución del proceso en la linea de comandos.	Cadena de caracteres
ToastResult	Respuesta del usuario ante el mensaje emergente mostrado por Cytomic EDR. ▪ **Ok**: el cliente acepta el mensaje. ▪ **Timeout**: el mensaje emergente desaparece por la no acción del usuario. ▪ **Angry**: el usuario rechaza el bloqueo desde el mensaje emergente. ▪ **Block** ▪ **Allow**	Enumeración
Action	Acción realizada por el agente Cytomic EDR. ▪ **Allow** ▪ **Block** ▪ **BlockTimeout**: se mostró un mensaje emergente al usuario pero no contestó a tiempo. ▪ **AllowWL**: elemento permitido por encontrarse en la lista blanca del administrador. ▪ **Disinfect** ▪ **Delete** ▪ **Quarantine** ▪ **AllowByUser**: se mostró un mensaje emergente al usuario y contesto “permitir ejecución”. ▪ **Informed**: se mostró un mensaje emergente al usuario. ▪ **Unquarantine**: el fichero se sacó de la cuarentena.	Enumeración

Campo	Descripción	Valor
	▪ **Rename**: elemento renombrado por no poderse mover a cuarentena, borrar o desinfectar. ▪ **BlockURL**: se bloqueó el acceso a una URL. ▪ **KillProcess**: cierre de proceso. ▪ **BlockExploit**: intento de explotación de proceso vulnerable detenido. ▪ **ExploitAllowByUser**: el usuario no permitió el cierre del proceso explotado. ▪ **RebootNeeded**: se requiere un reinicio del equipo para bloquear el intento de explotación. ▪ **ExploitInformed**: se mostró un mensaje emergente al usuario informando de un intento de explotación de proceso vulnerable. ▪ **AllowSonGWInstaller**: el programa forma parte de un paquete de instalación clasificado como Goodware. ▪ **EmbebedInformed**: el elemento es un script en powershell que ejecuta comandos. ▪ **SuspedProcess**: el elemento intentó suspender alguno de los servicios del software de protección. ▪ **ModifyDiskResource**: el elemento intentó modificar un fichero protegido que pertenece al software de protección. ▪ **ModifyRegistry**: el elemento intentó modificar una clave de registro protegida que pertenece al software de protección. ▪ **RenameRegistry**: el elemento intentó renombrar una clave de registro protegida que pertenece al software de protección. ▪ **ModifyMarkFile**: el elemento intentó renombrar un fichero protegido que pertenece al software de protección.	

Campo	Descripción	Valor
	▪ **UncertainAction**: el elemento intentó una acción sin definir sobre un fichero que pertenece al software de protección. ▪ **AllowGWFilter**: se permite la ejecución del elemento por estar en la caché de goodware. ▪ **AllowSWAuthoriced**: se permite la ejecución del elemento por estar autorizado por el administrador (configuración Software Autorizado). ▪ **NewPE**: aparición de un nuevo programa ejecutable en el equipo que viene del exterior. ▪ **AllowedByAdmin**: se permite la ejecución del elemento porque el administrador excluyó la técnica de explotación detectada. ▪ **Blocked by ip**: se bloqueó la dirección IP de origen por detectarse un ataque de fuerza bruta mediante el protocolo RDP. ▪ **AllowSonMsiGW**: se permite la ejecución del elemento por tratarse de un ejecutable que proviene de un paquete de instalación confiable. ▪ **Allowed by Global Audit**: el elemento se permite porque el software de seguridad está configurado en modo Global Audit.	
ServiceLevel	Modo de ejecución del agente: ▪ **Blocking**: el agente bloquea todos los ejecutables sin clasificar y los clasificados como malware. ▪ **Hardening**: el agente bloquea la ejecución de todos los programas sin clasificar cuyo origen no sea confiable y los clasificados como malware. ▪ **Learning**: el agente no bloquea ningún programa pero monitoriza los procesos ejecutados.	Enumeración

Campo	Descripción	Valor
WinningTech	Tecnología que provocó el evento. ▪ **Blockmode**: el agente estaba en modo Lock en el momento del bloqueo. ▪ **Cache**: clasificación cacheada en local. ▪ **Cloud**: clasificación descargada de la nube. ▪ **Context**: regla de contexto local. ▪ **ContextMinerva**: regla de contexto en la nube. ▪ **Digital Signature**: fichero firmado digitalmente. ▪ **Exploit**: tecnología de identificación de intento de explotación de proceso vulnerable. ▪ **ExploitLegacy** ▪ **GWFilter**: tecnologías de identificación de ficheros GW desconocidos. ▪ **LegacyUser**: permiso solicitado al usuario. ▪ **Local Signature**: firma local. ▪ **MetaEsploit**: ataque generado con el framework metaExploit. ▪ **NetNative**: tipo de binario. ▪ **Serializer**: tipo de binario. ▪ **User**: permiso solicitado al usuario. ▪ **RDP**: ataque de fuerza bruta por el protocolo RDP. ▪ **AMSI**: detección encontrada mediante Antimalware Scan Interface.	Enumeración
DetId	Identificador de la detección.	Cadena de caracteres
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres
TTPs	Lista de las técnicas, tácticas y subtécnicas asociadas al evento MITRE.	Cadena de caracteres

Campo	Descripción	Valor
IOAIds	Cuando una secuencia de eventos sigue un patrón descrito en la matriz MITRE, el producto de seguridad crea un indicio (IOA) y añade su identificador a todos los eventos que lo forman.	Numérico
TelemetryType	▪ **0: telemetría normal**. El evento no pertenece a un indicio que siga un patrón descrito en la matriz MITRE. ▪ **1: evento reenviado**. El evento se envió inicialmente como tipo 0 (telemetría normal), pero tiempo después se ha detectado que pertenece a un patrón de ataque escrito en la matriz MITRE. El evento se vuelve a enviar con los campos TTPs e IOAIds completados. ▪ **2: evento acumulado**. Para ahorrar recursos, parte de la telemetría generada en el cliente se retiene hasta que el software de seguridad detecta un patrón de ataque MITRE. En ese momento se envían todos los eventos acumulados.	Enumeración

Deviceops

Evento de tipo activo que se genera cuando se ejecuta una operación sobre un dispositivo externo por parte de un proceso.

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
User (CEF)	Nombre de la cuenta de usuario y dominio al que pertenece utilizada para ejecutar el proceso que genero el evento registrado.	Cadena de caracteres
MachineIP (CEF)	Nombre del equipo que desencadena el evento registrado.	Dirección IP
MachineName (CEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
sev (LEEF)	Severidad del evento.	1
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
usrName (LEEF)	Cuenta de usuario utilizada por el proceso que realizó la operación registrada.	Cadena de caracteres
domain (LEEF)	Dominio de la cuenta de usuario utilizado por el proceso que realizó la operación registrada.	Cadena de caracteres
src (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identSrc (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identHostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres

Campo	Descripción	Valor
HostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
LocalDateTime	Fecha en formato UTC que tenía el equipo en el momento en que se produjo el evento registrado. Esta fecha depende de la configuración del equipo y por lo tanto puede ser errónea	Fecha
PandaTimeStatus	Contenido de los campos DateTime, Date y LocalDateTime	**0**: fecha real no soportada por tratarse de un evento antiguo. **1**: fecha real no disponible el servidor Cytomic y obtenida mediante un cálculo. **2**: fecha real proporcionada por el servidor Cytomic.
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
NotificationType	Tipo de operación realizada. ▪ **40067**: conexión del dispositivo. ▪ **40068**: desconexión correcta del dispositivo. ▪ **40070**: desconexión del dispositivo sin desmontarlo previamente.	Enumeración
DeviceType	Tipo de unidad donde reside el proceso o fichero que desencadenó la operación registrada. ▪ **0**: desconocido. ▪ **1**: unidad de CD o DVD. ▪ **2**: dispositivo de almacenamiento SB. ▪ **3**: fichero imagen. ▪ **4**: dispositivo bluetooth.	Enumeración

Campo	Descripción	Valor
	▪ **5**: modem. ▪ **6**: impresora USB. ▪ **7**: teléfono móvil. ▪ **8**: teclado. ▪ **9**: teclado y ratón. ▪ **10**: ratón.	
UniqueId	Identificador único del dispositivo.	Cadena de caracteres
IsDenied	Indica si se ha denegado la acción reportada sobre el dispositivo.	Booleano
IdName	Nombre del dispositivo.	Cadena de caracteres
ClassName	Clase del dispositivo. Se corresponde con la clase indicada en el fichero .inf asociado al dispositivo.	Cadena de caracteres
FriendlyName	Nombre comprensible del dispositivo.	Cadena de caracteres
Description	Descripción del dispositivo.	Cadena de caracteres
Manufacturer	Fabricante del dispositivo.	Cadena de caracteres
PhoneDescription	Descripción del teléfono si la operación involucró a un dispositivo de este tipo.	Cadena de caracteres

Campo	Descripción	Valor
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres
TTPs	Lista de las técnicas, tácticas y subtécnicas asociadas al evento MITRE.	Cadena de caracteres
IOAIds	Cuando una secuencia de eventos sigue un patrón descrito en la matriz MITRE, el producto de seguridad crea un indicio (IOA) y añade su identificador a todos los eventos que lo forman.	Numérico
TelemetryType	▪ **0: telemetría normal**. El evento no pertenece a un indicio que siga un patrón descrito en la matriz MITRE. ▪ **1: evento reenviado**. El evento se envió inicialmente como tipo 0 (telemetría normal), pero tiempo después se ha detectado que pertenece a un patrón de ataque escrito en la matriz MITRE. El evento se vuelve a enviar con los campos TTPs e IOAIds completados. ▪ **2: evento acumulado**. Para ahorrar recursos, parte de la telemetría generada en el cliente se retiene hasta que el software de seguridad detecta un patrón de ataque MITRE. En ese momento se envían todos los eventos acumulados.	Enumeración

Dnsops

Evento de tipo pasivo que se genera con cada petición de una resolución dns por parte de un proceso.

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
User (CEF)	Nombre de la cuenta de usuario y dominio al que pertenece utilizada para ejecutar el proceso que genero el evento registrado.	Cadena de caracteres
MachineIP (CEF)	Nombre del equipo que desencadena el evento registrado.	Dirección IP
MachineName (CEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
sev (LEEF)	Severidad del evento.	1
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
usrName (LEEF)	Cuenta de usuario utilizada por el proceso que realizó la operación registrada.	Cadena de caracteres
domain (LEEF)	Dominio de la cuenta de usuario utilizado por el proceso que realizó la operación registrada.	Cadena de caracteres
src (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identSrc (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identHostName	Nombre del equipo que desencadena	Cadena de caracteres

Campo	Descripción	Valor
(LEEF)	el evento registrado.	
HostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
LocalDateTime	Fecha en formato UTC que tenía el equipo en el momento en que se produjo el evento registrado. Esta fecha depende de la configuración del equipo y por lo tanto puede ser errónea	Fecha
PandaTimeStatus	Contenido de los campos DateTime, Date y LocalDateTime	**0**: fecha real no soportada por tratarse de un evento antiguo. **1**: fecha real no disponible el servidor Cytomic y obtenida mediante un cálculo. **2**: fecha real proporcionada por el servidor Cytomic.
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
ProcessCount	Número de procesos en el equipo con fallos de resolución dns en la última hora.	Numérico
ProcessMD5	MD5 del proceso con operaciones de DNS fallidas.	Cadena de caracteres
ProcessPid	Identificador del proceso con operaciones de DNS fallidas.	Numérico
ProcessPath	Ruta del proceso con operaciones de DNS fallidas.	Cadena de caracteres
FailedQueries	Número de peticiones de resolución DNS fallidas producidas por el proceso en la última hora.	Numérico
QueriedDomainCount	Número de dominios diferentes con resolución fallida del proceso en la última hora.	Numérico

Campo	Descripción	Valor
DomainList	Lista de dominios enviados por el proceso al servidor DNS para su resolución y número de resoluciones por cada dominio.	{nombre_ dominio,numero#nombre_ dominio,numero}
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres
TTPs	Lista de las técnicas, tácticas y subtécnicas asociadas al evento MITRE.	Cadena de caracteres
IOAIds	Cuando una secuencia de eventos sigue un patrón descrito en la matriz MITRE, el producto de seguridad crea un indicio (IOA) y añade su identificador a todos los eventos que lo forman.	Numérico
TelemetryType	▪ **0: telemetría normal**. El evento no pertenece a un indicio que siga un patrón descrito en la matriz MITRE. ▪ **1: evento reenviado**. El evento se envió inicialmente como tipo 0 (telemetría normal), pero tiempo después se ha detectado que pertenece a un patrón de ataque escrito en la matriz MITRE. El evento se vuelve a enviar con los campos TTPs e IOAIds completados. ▪ **2: evento acumulado**. Para ahorrar recursos, parte de la telemetría generada en el cliente se retiene hasta que el software de seguridad detecta un patrón de ataque MITRE. En ese momento se envían todos los eventos acumulados.	Enumeración

Exec

Evento de tipo activo que se genera cada vez que un proceso (parent) ejecuta un nuevo proceso (child).

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
User (CEF)	Nombre de la cuenta de usuario y dominio al que pertenece utilizada para ejecutar el proceso que genero el evento registrado.	Cadena de caracteres
MachineIP (CEF)	Nombre del equipo que desencadena el evento registrado.	Dirección IP
MachineName (CEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
sev (LEEF)	Severidad del evento.	1
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
usrName (LEEF)	Cuenta de usuario utilizada por el proceso que realizó la operación registrada.	Cadena de caracteres
domain (LEEF)	Dominio de la cuenta de usuario utilizado por el proceso que realizó la operación registrada.	Cadena de caracteres
src (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identSrc (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identHostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres

Campo	Descripción	Valor
HostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
LocalDateTime	Fecha en formato UTC que tenía el equipo en el momento en que se produjo el evento registrado. Esta fecha depende de la configuración del equipo y por lo tanto puede ser errónea	Fecha
PandaTimeStatus	Contenido de los campos DateTime, Date y LocalDateTime	**0**: fecha real no soportada por tratarse de un evento antiguo. **1**: fecha real no disponible el servidor Cytomic y obtenida mediante un cálculo. **2**: fecha real proporcionada por el servidor Cytomic.
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
Op	Operación registrada.	Cadena de caracteres: “Exec”
ParentHash	Hash del proceso que actúa como padre.	Cadena de caracteres
ParentDriveType	Tipo de unidad donde reside el proceso o fichero padre que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM	Enumeración

Campo	Descripción	Valor
	▪ **Ramdisk**: unidad de disco RAM.	
ParentPath	Ruta del fichero padre que realizó la operación registrada.	Cadena de caracteres
ParentPID	Identificador del proceso padre.	Numérico
ParentValidSig	El proceso padre está firmado digitalmente.	Booleano
ParentCompany	Contenido del atributo Company de los metadatos del proceso padre.	Cadena de caracteres
ParentBroken	El proceso padre está corrupto o defectuoso.	Booleano
ParentImageType	Arquitectura interna del proceso padre: ▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	Enumeración
ParentExeType	Estructura interna / tipo del proceso padre. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
ParentPrevalence	Prevalencia histórica del proceso padre en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ParentPrevLastDay	Prevalencia del proceso padre en el día anterior en los sistemas de Cytomic. ▪ High ▪ Medium	Enumeración

Campo	Descripción	Valor
	▪ Low	
ParentCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración
ParentMWName	Nombre del malware en el proceso padre si ya está catalogado como una amenaza. Si es Null el elemento no es malware.	Cadena de caracteres
ChildHash	Hash del proceso que actúa como hijo.	Cadena de caracteres
ChildDriveType	Tipo de unidad donde reside el proceso o fichero padre que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM ▪ **Ramdisk**: unidad de disco RAM.	Enumeración
ChildPath	Ruta del fichero hijo que realizó la operación registrada.	Cadena de caracteres (Ruta)
ChildPID	Identificador del proceso hijo.	Numérico
ChildValidSig	El proceso hijo está firmado digitalmente.	Booleano
ChildCompany	Contenido del atributo Company de los metadatos del proceso hijo.	Cadena de caracteres
ChildBroken	El proceso hijo está corrupto o defectuoso.	Booleano
ChildImageType	Arquitectura interna del proceso hijo:	Enumeración

Campo	Descripción	Valor
	▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	
ChildExeType	Estructura interna / tipo del proceso hijo. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
ChildPrevalence	Prevalencia histórica del proceso hijo en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ChildPrevLastDay	Prevalencia histórica del proceso hijo en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ChildCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración
ChildMWName	Nombre del malware en el proceso hijo si ya está catalogado como una amenaza. Si es	Cadena de caracteres

Campo	Descripción	Valor
	Null el elemento no es malware.	
OCS_Exec	Se ejecutó en el equipo software considerado como vulnerable.	Booleano
OCS_Name	Nombre del software vulnerable ejecutado.	Cadena de caracteres
OCS_Version	Versión del sistema operativo del equipo donde se ejecutó el software vulnerable.	Cadena de caracteres
Params	Parámetros de ejecución del proceso en la linea de comandos.	Cadena de caracteres
ToastResult	Respuesta del usuario ante el mensaje emergente mostrado por Cytomic. ▪ **Ok**: el cliente acepta el mensaje. ▪ **Timeout**: el mensaje emergente desaparece por la no acción del usuario. ▪ **Angry**: el usuario rechaza el bloqueo desde el mensaje emergente. ▪ **Block** ▪ **Allow**	Enumeración
Action	Acción realizada por el agente Cytomic. ▪ **Allow** ▪ **Block** ▪ **BlockTimeout**: se mostró un mensaje emergente al usuario pero no contestó a tiempo. ▪ **AllowWL**: elemento permitido por encontrarse en la lista blanca del administrador. ▪ **Disinfect** ▪ **Delete** ▪ **Quarantine** ▪ **AllowByUser**: se mostró un mensaje emergente al usuario y contesto “permitir ejecución”. ▪ **Informed**: se mostró un mensaje emergente al usuario. ▪ **Unquarantine**: el fichero se sacó de la cuarentena.	Enumeración

Campo	Descripción	Valor
	▪ **Rename**: elemento renombrado por no poderse mover a cuarentena, borrar o desinfectar. ▪ **BlockURL**: se bloqueó el acceso a una URL. ▪ **KillProcess**: cierre de proceso. ▪ **BlockExploit**: intento de explotación de proceso vulnerable detenido. ▪ **ExploitAllowByUser**: el usuario no permitió el cierre del proceso explotado. ▪ **RebootNeeded**: se requiere un reinicio del equipo para bloquear el intento de explotación. ▪ **ExploitInformed**: se mostró un mensaje emergente al usuario informando de un intento de explotación de proceso vulnerable. ▪ **AllowSonGWInstaller**: el programa forma parte de un paquete de instalación clasificado como Goodware. ▪ **EmbebedInformed**: el elemento es un script en powershell que ejecuta comandos. ▪ **SuspedProcess**: el elemento intentó suspender alguno de los servicios del software de protección. ▪ **ModifyDiskResource**: el elemento intentó modificar un fichero protegido que pertenece al software de protección. ▪ **ModifyRegistry**: el elemento intentó modificar una clave de registro protegida que pertenece al software de protección. ▪ **RenameRegistry**: el elemento intentó renombrar una clave de registro protegida que pertenece al software de protección.	

Campo	Descripción	Valor
	▪ **ModifyMarkFile**: el elemento intentó renombrar un fichero protegido que pertenece al software de protección. ▪ **UncertainAction**: el elemento intentó una acción sin definir sobre un fichero que pertenece al software de protección. ▪ **AllowGWFilter**: se permite la ejecución del elemento por estar en la caché de goodware. ▪ **AllowSWAuthoriced**: se permite la ejecución del elemento por estar autorizado por el administrador (configuración Software Autorizado). ▪ **NewPE**: aparición de un nuevo programa ejecutable en el equipo que viene del exterior. ▪ **AllowedByAdmin**: se permite la ejecución del elemento porque el administrador excluyó la técnica de explotación detectada. ▪ **Blocked by ip**: se bloqueó la dirección IP de origen por detectarse un ataque de fuerza bruta mediante el protocolo RDP. ▪ **AllowSonMsiGW**: se permite la ejecución del elemento por tratarse de un ejecutable que proviene de un paquete de instalación confiable. ▪ **Allowed by Global Audit**: el elemento se permite porque el software de seguridad está configurado en modo Global Audit.	
ServiceLevel	Modo de ejecución del agente: ▪ **Blocking**: el agente bloquea todos los ejecutables sin clasificar y los clasificados como malware. ▪ **Hardening**: el agente bloquea la ejecución de todos los programas sin clasificar cuyo origen no sea confiable y los clasificados como malware.	Enumeración

Campo	Descripción	Valor
	▪ **Learning**: el agente no bloquea ningún programa pero monitoriza los procesos ejecutados.	
WinningTech	Tecnología que provocó el evento. ▪ **Blockmode**: el agente estaba en modo Lock en el momento del bloqueo. ▪ **Cache**: clasificación cacheada en local. ▪ **Cloud**: clasificación descargada de la nube. ▪ **Context**: regla de contexto local. ▪ **ContextMinerva**: regla de contexto en la nube. ▪ **Digital Signature**: fichero firmado digitalmente. ▪ **Exploit**: tecnología de identificación de intento de explotación de proceso vulnerable. ▪ **ExploitLegacy** ▪ **GWFilter**: tecnologías de identificación de ficheros GW desconocidos. ▪ **LegacyUser**: permiso solicitado al usuario. ▪ **Local Signature**: firma local. ▪ **MetaEsploit**: ataque generado con el framework metaExploit. ▪ **NetNative**: tipo de binario. ▪ **Serializer**: tipo de binario. ▪ **User**: permiso solicitado al usuario. ▪ **RDP**: ataque de fuerza bruta por el protocolo RDP. ▪ **AMSI**: detección encontrada mediante Antimalware Scan Interface.	Enumeración
DetId	Identificador de la detección.	Cadena de caracteres
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres

Campo	Descripción	Valor
TTPs	Lista de las técnicas, tácticas y subtécnicas asociadas al evento MITRE.	Cadena de caracteres
IOAIds	Cuando una secuencia de eventos sigue un patrón descrito en la matriz MITRE, el producto de seguridad crea un indicio (IOA) y añade su identificador a todos los eventos que lo forman.	Numérico
TelemetryType	▪ **0: telemetría normal**. El evento no pertenece a un indicio que siga un patrón descrito en la matriz MITRE. ▪ **1: evento reenviado**. El evento se envió inicialmente como tipo 0 (telemetría normal), pero tiempo después se ha detectado que pertenece a un patrón de ataque escrito en la matriz MITRE. El evento se vuelve a enviar con los campos TTPs e IOAIds completados. ▪ **2: evento acumulado**: para ahorrar recursos, parte de la telemetría generada en el cliente se retiene hasta que el software de seguridad detecta un patrón de ataque MITRE. En ese momento se envían todos los eventos acumulados.	Enumeración

HeuHooks

Evento de tipo activo que se genera cuando una función de una dll interceptada es analizada y se considera que podría estar implicada en la ejecución de un ataque al equipo. Dependiendo de la configuración del módulo antiexploit del producto de seguridad instalado en el equipo protegido, la operación se bloqueará o se notificará al usuario.

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
User (CEF)	Nombre de la cuenta de usuario y dominio al que pertenece utilizada para ejecutar el proceso que genero el evento registrado.	Cadena de caracteres
MachineIP (CEF)	Nombre del equipo que desencadena el evento registrado.	Dirección IP
MachineName (CEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
sev (LEEF)	Severidad del evento.	1
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
usrName (LEEF)	Cuenta de usuario utilizada por el proceso que realizó la operación registrada.	Cadena de caracteres
domain (LEEF)	Dominio de la cuenta de usuario utilizado por el proceso que realizó la operación registrada.	Cadena de caracteres
src (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identSrc (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres

Campo	Descripción	Valor
identHostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
HostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
LocalDateTime	Fecha en formato UTC que tenía el equipo en el momento en que se produjo el evento registrado. Esta fecha depende de la configuración del equipo y por lo tanto puede ser errónea	Fecha
PandaTimeStatus	Contenido de los campos DateTime, Date y LocalDateTime	**0**: fecha real no soportada por tratarse de un evento antiguo. **1**: fecha real no disponible el servidor Cytomic y obtenida mediante un cálculo. **2**: fecha real proporcionada por el servidor Cytomic.
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
Op	Operación registrada.	Cadena de caracteres: “DeletePE”
ParentHash	Hash del proceso que actúa como padre.	Cadena de caracteres
ParentDriveType	Tipo de unidad donde reside el proceso o fichero padre que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido.	Enumeración

Campo	Descripción	Valor
	▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM ▪ **Ramdisk**: unidad de disco RAM.	
ParentPath	Ruta del fichero padre que realizó la operación registrada.	Cadena de caracteres
ParentPID	Identificador del proceso padre.	Numérico
ParentValidSig	El proceso padre está firmado digitalmente.	Booleano
ParentCompany	Contenido del atributo Company de los metadatos del proceso padre.	Cadena de caracteres
ParentBroken	El proceso padre está corrupto o defectuoso.	Booleano
ParentImageType	Arquitectura interna del proceso padre: ▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	Enumeración
ParentExeType	Estructura interna / tipo del proceso padre. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
ParentPrevalence	Prevalencia histórica del proceso padre en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ParentPrevLastDay	Prevalencia del proceso padre en el día	Enumeración

Campo	Descripción	Valor
	anterior en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	
ParentCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración
ParentMWName	Nombre del malware en el proceso padre si ya está catalogado como una amenaza. Si es Null el elemento no es malware.	Cadena de caracteres
ChildHash	Hash del proceso que actúa como hijo.	Cadena de caracteres
ChildDriveType	Tipo de unidad donde reside el proceso o fichero padre que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM ▪ **Ramdisk**: unidad de disco RAM.	Enumeración
ChildPath	Ruta del fichero hijo que realizó la operación registrada.	Cadena de caracteres (Ruta)
ChildPID	Identificador del proceso hijo.	Numérico
ChildValidSig	El proceso hijo está firmado digitalmente.	Booleano
ChildCompany	Contenido del atributo Company de los metadatos del proceso hijo.	Cadena de caracteres

Campo	Descripción	Valor
ChildBroken	El proceso hijo está corrupto o defectuoso.	Booleano
ChildImageType	Arquitectura interna del proceso hijo: ▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	Enumeración
ChildExeType	Estructura interna / tipo del proceso hijo. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
ChildPrevalence	Prevalencia histórica del proceso hijo en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ChildPrevLastDay	Prevalencia histórica del proceso hijo en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ChildCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown	Enumeración

Campo	Descripción	Valor
	▪ Monitoring	
ChildMWName	Nombre del malware en el proceso hijo si ya está catalogado como una amenaza. Si es Null el elemento no es malware.	Cadena de caracteres
OCS_Exec	Se ejecutó en el equipo software considerado como vulnerable.	Booleano
OCS_Name	Nombre del software vulnerable ejecutado.	Cadena de caracteres
OCS_Version	Versión del sistema operativo del equipo donde se ejecutó el software vulnerable.	Cadena de caracteres
Params	Parámetros de ejecución del proceso en la linea de comandos.	Cadena de caracteres
ToastResult	Respuesta del usuario ante el mensaje emergente mostrado por Cytomic EDR. ▪ **Ok**: el cliente acepta el mensaje. ▪ **Timeout**: el mensaje emergente desaparece por la no acción del usuario. ▪ **Angry**: el usuario rechaza el bloqueo desde el mensaje emergente. ▪ **Block** ▪ **Allow**	Enumeración
Action	Acción realizada por el agente Cytomic EDR. ▪ **Allow** ▪ **Block** ▪ **BlockTimeout**: se mostró un mensaje emergente al usuario pero no contestó a tiempo. ▪ **AllowWL**: elemento permitido por encontrarse en la lista blanca del administrador. ▪ **Disinfect** ▪ **Delete** ▪ **Quarantine** ▪ **AllowByUser**: se mostró un mensaje emergente al usuario y contesto “permitir ejecución”.	Enumeración

Campo	Descripción	Valor
	▪ **Informed**: se mostró un mensaje emergente al usuario. ▪ **Unquarantine**: el fichero se sacó de la cuarentena. ▪ **Rename**: elemento renombrado por no poderse mover a cuarentena, borrar o desinfectar. ▪ **BlockURL**: se bloqueó el acceso a una URL. ▪ **KillProcess**: cierre de proceso. ▪ **BlockExploit**: intento de explotación de proceso vulnerable detenido. ▪ **ExploitAllowByUser**: el usuario no permitió el cierre del proceso explotado. ▪ **RebootNeeded**: se requiere un reinicio del equipo para bloquear el intento de explotación. ▪ **ExploitInformed**: se mostró un mensaje emergente al usuario informando de un intento de explotación de proceso vulnerable. ▪ **AllowSonGWInstaller**: el programa forma parte de un paquete de instalación clasificado como Goodware. ▪ **EmbebedInformed**: el elemento es un script en powershell que ejecuta comandos. ▪ **SuspedProcess**: el elemento intentó suspender alguno de los servicios del software de protección. ▪ **ModifyDiskResource**: el elemento intentó modificar un fichero protegido que pertenece al software de protección. ▪ **ModifyRegistry**: el elemento intentó modificar una clave de registro protegida que pertenece al software de protección.	

Campo	Descripción	Valor
	▪ **RenameRegistry**: el elemento intentó renombrar una clave de registro protegida que pertenece al software de protección. ▪ **ModifyMarkFile**: el elemento intentó renombrar un fichero protegido que pertenece al software de protección. ▪ **UncertainAction**: el elemento intentó una acción sin definir sobre un fichero que pertenece al software de protección. ▪ **AllowGWFilter**: se permite la ejecución del elemento por estar en la caché de goodware. ▪ **AllowSWAuthoriced**: se permite la ejecución del elemento por estar autorizado por el administrador (configuración Software Autorizado). ▪ **NewPE**: aparición de un nuevo programa ejecutable en el equipo que viene del exterior. ▪ **AllowedByAdmin**: se permite la ejecución del elemento porque el administrador excluyó la técnica de explotación detectada. ▪ **Blocked by ip**: se bloqueó la dirección IP de origen por detectarse un ataque de fuerza bruta mediante el protocolo RDP. ▪ **AllowSonMsiGW**: se permite la ejecución del elemento por tratarse de un ejecutable que proviene de un paquete de instalación confiable. ▪ **Allowed by Global Audit**: el elemento se permite porque el software de seguridad está configurado en modo Global Audit.	
ServiceLevel	Modo de ejecución del agente: ▪ **Blocking**: el agente bloquea todos los ejecutables sin clasificar y los clasificados como malware.	Enumeración

Campo	Descripción	Valor
	▪ **Hardening**: el agente bloquea la ejecución de todos los programas sin clasificar cuyo origen no sea confiable y los clasificados como malware. ▪ **Learning**: el agente no bloquea ningún programa pero monitoriza los procesos ejecutados.	
WinningTech	Tecnología que provocó el evento. ▪ **Blockmode**: el agente estaba en modo Lock en el momento del bloqueo. ▪ **Cache**: clasificación cacheada en local. ▪ **Cloud**: clasificación descargada de la nube. ▪ **Context**: regla de contexto local. ▪ **ContextMinerva**: regla de contexto en la nube. ▪ **Digital Signature**: fichero firmado digitalmente. ▪ **Exploit**: tecnología de identificación de intento de explotación de proceso vulnerable. ▪ **ExploitLegacy** ▪ **GWFilter**: tecnologías de identificación de ficheros GW desconocidos. ▪ **LegacyUser**: permiso solicitado al usuario. ▪ **Local Signature**: firma local. ▪ **MetaEsploit**: ataque generado con el framework metaExploit. ▪ **NetNative**: tipo de binario. ▪ **Serializer**: tipo de binario. ▪ **User**: permiso solicitado al usuario. ▪ **RDP**: ataque de fuerza bruta por el protocolo RDP. ▪ **AMSI**: detección encontrada mediante Antimalware Scan Interface.	Enumeración
DetId	Identificador de la detección.	Cadena de caracteres
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres

Hostfiles

Evento de tipo activo que se genera cuando un proceso (parent) detecta una modificación del fichero hosts.

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
User (CEF)	Nombre de la cuenta de usuario y dominio al que pertenece utilizada para ejecutar el proceso que genero el evento registrado.	Cadena de caracteres
MachineIP (CEF)	Nombre del equipo que desencadena el evento registrado.	Dirección IP
MachineName (CEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
sev (LEEF)	Severidad del evento.	1
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
usrName (LEEF)	Cuenta de usuario utilizada por el proceso que realizó la operación registrada.	Cadena de caracteres
domain (LEEF)	Dominio de la cuenta de usuario utilizado por el proceso que realizó la operación registrada.	Cadena de caracteres
src (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identSrc (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identHostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres

Campo	Descripción	Valor
HostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
LocalDateTime	Fecha en formato UTC que tenía el equipo en el momento en que se produjo el evento registrado. Esta fecha depende de la configuración del equipo y por lo tanto puede ser errónea	Fecha
PandaTimeStatus	Contenido de los campos DateTime, Date y LocalDateTime	**0**: fecha real no soportada por tratarse de un evento antiguo. **1**: fecha real no disponible el servidor Cytomic y obtenida mediante un cálculo. **2**: fecha real proporcionada por el servidor Cytomic.
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
HostName	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
Hash	Hash / digest del fichero.	Cadena de caracteres
Drivetype	Tipo de unidad donde reside el proceso o fichero que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM ▪ **Ramdisk**: unidad de disco RAM.	Enumeración

Campo	Descripción	Valor
Path	Ruta del elemento que desencadenó la operación registrada.	Cadena de caracteres
ValidSig	Proceso firmado digitalmente.	Booleano
Company	Contenido del atributo Company de los metadatos del proceso.	Cadena de caracteres
Broken	El fichero esta corrupto o defectuoso.	Cadena de caracteres
ImageType	Arquitectura interna del proceso. ▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	Enumeración
ExeType	Estructura interna / tipo del proceso. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
Prevalence	Prevalencia histórica del proceso en los sistemas de Cytomic (Business Unit of Panda Security, S.L.). ▪ High ▪ Medium ▪ Low	Enumeración
PrevLastDay	Prevalencia del proceso en el día anterior en los sistemas de Cytomic (Business Unit of Panda Security, S.L.). ▪ High ▪ Medium ▪ Low	Enumeración

Campo	Descripción	Valor
Cat	Categoría del fichero que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración
MWName	Nombre del malware si está ya catalogado como una amenaza.	Cadena de caracteres
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres
TTPs	Lista de las técnicas, tácticas y subtécnicas asociadas al evento MITRE.	Cadena de caracteres
IOAIds	Cuando una secuencia de eventos sigue un patrón descrito en la matriz MITRE, el producto de seguridad crea un indicio (IOA) y añade su identificador a todos los eventos que lo forman.	Numérico
TelemetryType	▪ **0: telemetría normal**. El evento no pertenece a un indicio que siga un patrón descrito en la matriz MITRE. ▪ **1: evento reenviado**. El evento se envió inicialmente como tipo 0 (telemetría normal), pero tiempo después se ha detectado que pertenece a un patrón de ataque escrito en la matriz MITRE. El evento se vuelve a enviar con los campos TTPs e IOAIds completados. ▪ **2: evento acumulado**: para ahorrar recursos, parte de la telemetría generada en el cliente se retiene hasta que el software de seguridad detecta un patrón de ataque MITRE. En ese momento se envían todos los eventos acumulados.	Enumeración

Install

Evento de tipo pasivo que se genera cuando se instala el software de protección Cytomic EDR.

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
User (CEF)	Nombre de la cuenta de usuario y dominio al que pertenece utilizada para ejecutar el proceso que genero el evento registrado.	Cadena de caracteres
MachineIP (CEF)	Nombre del equipo que desencadena el evento registrado.	Dirección IP
MachineName (CEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
sev (LEEF)	Severidad del evento.	1
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
usrName (LEEF)	Cuenta de usuario utilizada por el proceso que realizó la operación registrada.	Cadena de caracteres
domain (LEEF)	Dominio de la cuenta de usuario utilizado por el proceso que realizó la operación registrada.	Cadena de caracteres
src (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identSrc (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identHostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres

Campo	Descripción	Valor
HostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
LocalDateTime	Fecha en formato UTC que tenía el equipo en el momento en que se produjo el evento registrado. Esta fecha depende de la configuración del equipo y por lo tanto puede ser errónea	Fecha
PandaTimeStatus	Contenido de los campos DateTime, Date y LocalDateTime	**0**: fecha real no soportada por tratarse de un evento antiguo. **1**: fecha real no disponible el servidor Cytomic y obtenida mediante un cálculo. **2**: fecha real proporcionada por el servidor Cytomic.
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
Operation	Tipo de operación: ▪ Install ▪ Uninstall	Enumeración
Result	Resultado de la operación: ▪ OK ▪ No ok	Enumeración
OSVersion	Versión del sistema operativo instalado en el equipo del usuario.	Cadena de caracteres

Campo	Descripción	Valor
OSServicePack	Service Pack del sistema operativo del equipo de usuario.	Cadena de caracteres
OSPlatform	Plataforma del sistema operativo del equipo de usuario. ▪ WIN32 ▪ WIN64	Enumeración
MachineIP0	IP del equipo donde se registró el evento.	Dirección IP
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres

Loadlib

Evento de tipo activo que se genera cuando un proceso (parent) carga una librería (child).

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
User (CEF)	Nombre de la cuenta de usuario y dominio al que pertenece utilizada para ejecutar el proceso que genero el evento registrado.	Cadena de caracteres
MachineIP (CEF)	Nombre del equipo que desencadena el evento registrado.	Dirección IP
MachineName (CEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
sev (LEEF)	Severidad del evento.	1
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
usrName (LEEF)	Cuenta de usuario utilizada por el proceso que realizó la operación registrada.	Cadena de caracteres
domain (LEEF)	Dominio de la cuenta de usuario utilizado por el proceso que realizó la operación registrada.	Cadena de caracteres
src (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identSrc (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identHostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres

Campo	Descripción	Valor
HostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
LocalDateTime	Fecha en formato UTC que tenía el equipo en el momento en que se produjo el evento registrado. Esta fecha depende de la configuración del equipo y por lo tanto puede ser errónea	Fecha
PandaTimeStatus	Contenido de los campos DateTime, Date y LocalDateTime	**0**: fecha real no soportada por tratarse de un evento antiguo. **1**: fecha real no disponible el servidor Cytomic y obtenida mediante un cálculo. **2**: fecha real proporcionada por el servidor Cytomic.
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
Op	Operación registrada.	Cadena de caracteres: “Loadlib”
ParentHash	Hash del proceso que actúa como padre.	Cadena de caracteres
ParentDriveType	Tipo de unidad donde reside el proceso o fichero padre que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM	Enumeración

Campo	Descripción	Valor
	▪ **Ramdisk**: unidad de disco RAM.	
ParentPath	Ruta del fichero padre que realizó la operación registrada.	Cadena de caracteres
ParentPID	Identificador del proceso padre.	Numérico
ParentValidSig	El proceso padre está firmado digitalmente.	Booleano
ParentCompany	Contenido del atributo Company de los metadatos del proceso padre.	Cadena de caracteres
ParentBroken	El proceso padre está corrupto o defectuoso.	Booleano
ParentImageType	Arquitectura interna del proceso padre: ▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	Enumeración
ParentExeType	Estructura interna / tipo del proceso padre. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
ParentPrevalence	Prevalencia histórica del proceso padre en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ParentPrevLastDay	Prevalencia del proceso padre en el día anterior en los sistemas de Cytomic. ▪ High ▪ Medium	Enumeración

Campo	Descripción	Valor
	▪ Low	
ParentCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración
ParentMWName	Nombre del malware en el proceso padre si ya está catalogado como una amenaza. Si es Null el elemento no es malware.	Cadena de caracteres
ChildHash	Hash del proceso que actúa como hijo.	Cadena de caracteres
ChildDriveType	Tipo de unidad donde reside el proceso o fichero padre que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM ▪ **Ramdisk**: unidad de disco RAM.	Enumeración
ChildPath	Ruta del fichero hijo que realizó la operación registrada.	Cadena de caracteres (Ruta)
ChildPID	Identificador del proceso hijo.	Numérico
ChildValidSig	El proceso hijo está firmado digitalmente.	Booleano
ChildCompany	Contenido del atributo Company de los metadatos del proceso hijo.	Cadena de caracteres
ChildBroken	El proceso hijo está corrupto o defectuoso.	Booleano
ChildImageType	Arquitectura interna del proceso hijo:	Enumeración

Campo	Descripción	Valor
	▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	
ChildExeType	Estructura interna / tipo del proceso hijo. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
ChildPrevalence	Prevalencia histórica del proceso hijo en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ChildPrevLastDay	Prevalencia histórica del proceso hijo en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ChildCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración
ChildMWName	Nombre del malware en el proceso hijo si ya está catalogado como una amenaza. Si es	Cadena de caracteres

Campo	Descripción	Valor
	Null el elemento no es malware.	
OCS_Exec	Se ejecutó en el equipo software considerado como vulnerable.	Booleano
OCS_Name	Nombre del software vulnerable ejecutado.	Cadena de caracteres
OCS_Version	Versión del sistema operativo del equipo donde se ejecutó el software vulnerable.	Cadena de caracteres
Params	Parámetros de ejecución del proceso en la linea de comandos.	Cadena de caracteres
ToastResult	Respuesta del usuario ante el mensaje emergente mostrado por Cytomic EDR. ▪ **Ok**: el cliente acepta el mensaje. ▪ **Timeout**: el mensaje emergente desaparece por la no acción del usuario. ▪ **Angry**: el usuario rechaza el bloqueo desde el mensaje emergente. ▪ **Block** ▪ **Allow**	Enumeración
Action	Acción realizada por el agente Cytomic EDR. ▪ **Allow** ▪ **Block** ▪ **BlockTimeout**: se mostró un mensaje emergente al usuario pero no contestó a tiempo. ▪ **AllowWL**: elemento permitido por encontrarse en la lista blanca del administrador. ▪ **Disinfect** ▪ **Delete** ▪ **Quarantine** ▪ **AllowByUser**: se mostró un mensaje emergente al usuario y contesto “permitir ejecución”. ▪ **Informed**: se mostró un mensaje emergente al usuario. ▪ **Unquarantine**: el fichero se sacó de la cuarentena.	Enumeración

Campo	Descripción	Valor
	▪ **Rename**: elemento renombrado por no poderse mover a cuarentena, borrar o desinfectar. ▪ **BlockURL**: se bloqueó el acceso a una URL. ▪ **KillProcess**: cierre de proceso. ▪ **BlockExploit**: intento de explotación de proceso vulnerable detenido. ▪ **ExploitAllowByUser**: el usuario no permitió el cierre del proceso explotado. ▪ **RebootNeeded**: se requiere un reinicio del equipo para bloquear el intento de explotación. ▪ **ExploitInformed**: se mostró un mensaje emergente al usuario informando de un intento de explotación de proceso vulnerable. ▪ **AllowSonGWInstaller**: el programa forma parte de un paquete de instalación clasificado como Goodware. ▪ **EmbebedInformed**: el elemento es un script en powershell que ejecuta comandos. ▪ **SuspedProcess**: el elemento intentó suspender alguno de los servicios del software de protección. ▪ **ModifyDiskResource**: el elemento intentó modificar un fichero protegido que pertenece al software de protección. ▪ **ModifyRegistry**: el elemento intentó modificar una clave de registro protegida que pertenece al software de protección. ▪ **RenameRegistry**: el elemento intentó renombrar una clave de registro protegida que pertenece al software de protección.	

Campo	Descripción	Valor
	▪ **ModifyMarkFile**: el elemento intentó renombrar un fichero protegido que pertenece al software de protección. ▪ **UncertainAction**: el elemento intentó una acción sin definir sobre un fichero que pertenece al software de protección. ▪ **AllowGWFilter**: se permite la ejecución del elemento por estar en la caché de goodware. ▪ **AllowSWAuthoriced**: se permite la ejecución del elemento por estar autorizado por el administrador (configuración Software Autorizado). ▪ **NewPE**: aparición de un nuevo programa ejecutable en el equipo que viene del exterior. ▪ **AllowedByAdmin**: se permite la ejecución del elemento porque el administrador excluyó la técnica de explotación detectada. ▪ **Blocked by ip**: se bloqueó la dirección IP de origen por detectarse un ataque de fuerza bruta mediante el protocolo RDP. ▪ **AllowSonMsiGW**: se permite la ejecución del elemento por tratarse de un ejecutable que proviene de un paquete de instalación confiable. ▪ **Allowed by Global Audit**: el elemento se permite porque el software de seguridad está configurado en modo Global Audit.	
ServiceLevel	Modo de ejecución del agente: ▪ **Blocking**: el agente bloquea todos los ejecutables sin clasificar y los clasificados como malware. ▪ **Hardening**: el agente bloquea la ejecución de todos los programas sin clasificar cuyo origen no sea confiable y los clasificados como malware.	Enumeración

Campo	Descripción	Valor
	▪ **Learning**: el agente no bloquea ningún programa pero monitoriza los procesos ejecutados.	
WinningTech	Tecnología que provocó el evento. ▪ **Blockmode**: el agente estaba en modo Lock en el momento del bloqueo. ▪ **Cache**: clasificación cacheada en local. ▪ **Cloud**: clasificación descargada de la nube. ▪ **Context**: regla de contexto local. ▪ **ContextMinerva**: regla de contexto en la nube. ▪ **Digital Signature**: fichero firmado digitalmente. ▪ **Exploit**: tecnología de identificación de intento de explotación de proceso vulnerable. ▪ **ExploitLegacy** ▪ **GWFilter**: tecnologías de identificación de ficheros GW desconocidos. ▪ **LegacyUser**: permiso solicitado al usuario. ▪ **Local Signature**: firma local. ▪ **MetaEsploit**: ataque generado con el framework metaExploit. ▪ **NetNative**: tipo de binario. ▪ **Serializer**: tipo de binario. ▪ **User**: permiso solicitado al usuario. ▪ **RDP**: ataque de fuerza bruta por el protocolo RDP. ▪ **AMSI**: detección encontrada mediante Antimalware Scan Interface.	Enumeración
DetId	Identificador de la detección.	Cadena de caracteres
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres

Campo	Descripción	Valor
TTPs	Lista de las técnicas, tácticas y subtécnicas asociadas al evento MITRE.	Cadena de caracteres
IOAIds	Cuando una secuencia de eventos sigue un patrón descrito en la matriz MITRE, el producto de seguridad crea un indicio (IOA) y añade su identificador a todos los eventos que lo forman.	Numérico
TelemetryType	▪ **0: telemetría normal**. El evento no pertenece a un indicio que siga un patrón descrito en la matriz MITRE. ▪ **1: evento reenviado**. El evento se envió inicialmente como tipo 0 (telemetría normal), pero tiempo después se ha detectado que pertenece a un patrón de ataque escrito en la matriz MITRE. El evento se vuelve a enviar con los campos TTPs e IOAIds completados. ▪ **2: evento acumulado**: para ahorrar recursos, parte de la telemetría generada en el cliente se retiene hasta que el software de seguridad detecta un patrón de ataque MITRE. En ese momento se envían todos los eventos acumulados.	Enumeración

Loginoutops

Evento de tipo activo que se genera cuando se detecta un inicio de sesión en el equipo.

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
User (CEF)	Nombre de la cuenta de usuario y dominio al que pertenece utilizada para ejecutar el proceso que generó el evento registrado.	Cadena de caracteres
MachineIP (CEF)	Nombre del equipo que desencadena el evento registrado.	Dirección IP
MachineName (CEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
sev (LEEF)	Severidad del evento.	1
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
usrName (LEEF)	Cuenta de usuario utilizada por el proceso que realizó la operación registrada.	Cadena de caracteres
domain (LEEF)	Dominio de la cuenta de usuario utilizado por el proceso que realizó la operación registrada.	Cadena de caracteres
src (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identSrc (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identHostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres

Campo	Descripción	Valor
HostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
LocalDateTime	Fecha en formato UTC que tenía el equipo en el momento en que se produjo el evento registrado. Esta fecha depende de la configuración del equipo y por lo tanto puede ser errónea	Fecha
PandaTimeStatus	Contenido de los campos DateTime, Date y LocalDateTime	**0**: fecha real no soportada por tratarse de un evento antiguo. **1**: fecha real no disponible el servidor Cytomic y obtenida mediante un cálculo. **2**: fecha real proporcionada por el servidor Cytomic.
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
ActionType	▪ **0**: inicio de sesión. ▪ **1**: fin de sesión.	Enumeración
SessionType	Tipo de inicio de sesión: ▪ **2**: sesión creada físicamente mediante un teclado o a través de KVM sobre IP. ▪ **3**: sesión creada remotamente en carpetas o impresoras compartidas. Este tipo de inicio de sesión tiene autenticación segura. ▪ **4**: sesión creada por el programador de tareas de Windows. ▪ **5**: sesión creada cuando arranca un servicio que requiere ejecutarse en la sesión de usuario. La sesión es eliminada cuando el servicio se detiene.	Numérico

Campo	Descripción	Valor
	▪ **7**: sesión creada cuando un usuario intenta entrar en una sesión que ya está creada y ha sido bloqueada. ▪ **8**: idéntico al tipo 3 pero la contraseña viaja en texto plano. ▪ **9**: sesión creada cuando se usa el comando “RunAs” bajo una cuenta diferente a la utilizada para iniciar la sesión, y especificando el parámetro “/netonly”. Sin el parámetro “/netonly” se genera un tipo de sesión 2. ▪ **10**: sesión creada cuando se accede mediante “Terminal Service”, “Remote desktop” o “Remote Assistance”. Identifica una conexión de usuario remota. ▪ **11**: sesión de usuario creada con credenciales de dominio cacheadas en el equipo, pero sin conexión con el controlador de dominio.	
ErrorCode	▪ **0xC0000064**: el nombre de usuario no existe. ▪ **0XC000005E**: el servidor necesario para validar el inicio de sesión no está disponible. ▪ **0xC000006A**: el usuario es correcto pero la contraseña es incorrecta. ▪ **0XC000006D**: el usuario o la información de autenticación es errónea. ▪ **0XC000006E**: nombre desconocido o contraseña errónea. ▪ **0xC0000234**: acceso bloqueado. ▪ **0xC0000072**: cuenta deshabilitada. ▪ **0xC000006F**: intento de inicio de sesión en horario restringido. ▪ **0xC0000070**: intento de inicio de sesión desde un equipo no autorizado.	Numérico (hexadecimal)

Campo	Descripción	Valor
	▪ **0xC00000DC**: error en el servidor de validación. No se puede realizar la operación. ▪ **0xC0000193**: cuenta caducada. ▪ **0xC0000071**: contraseña caducada. ▪ **0xC0000133:** el reloj de los equipos conectados tienen un desfase demasiado grande. ▪ **0xC0000224**: se requiere que el usuario cambie la contraseña en el siguiente reinicio. ▪ **0xC0000225:** error de Windows que no implica riesgo. ▪ **0xc000018c**: la solicitud de inicio de sesión falló porque la relación de confianza entre el dominio primario y el dominio confiable falló. ▪ **0XC0000192**: se intentó iniciar sesión, pero el servicio Netlogon no se inició. ▪ **0XC00002EE**: se produjo un error durante el inicio de sesión. ▪ **0XC0000413**: el equipo en la que se está iniciando sesión está protegida por un firewall de autenticación. La cuenta especificada no puede autenticarse en el equipo. ▪ **0xc000015b**: el usuario no tiene permisos para ese tipo de inicio de sesión.	
User	Dominio\usuario con el que se ha creado la sesión.	Cadena de caracteres
Interactive	Indica si es un inicio de sesión de usuario interactiva.	Booleano
RemoteMachineName	Si el evento es un inicio de sesión remoto indica el nombre del equipo remoto.	Cadena de caracteres
RemoteIP	Si el evento es un inicio de sesión remoto indica la IP del equipo remoto.	Dirección IP
RemotePort	Si el evento es un inicio de sesión remoto	Numérico

Campo	Descripción	Valor
	indica el puerto del equipo remoto.	
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres
TTPs	Lista de las técnicas, tácticas y subtécnicas asociadas al evento MITRE.	Cadena de caracteres
IOAIds	Cuando una secuencia de eventos sigue un patrón descrito en la matriz MITRE, el producto de seguridad crea un indicio (IOA) y añade su identificador a todos los eventos que lo forman.	Numérico
TelemetryType	▪ **0: telemetría normal**. El evento no pertenece a un indicio que siga un patrón descrito en la matriz MITRE. ▪ **1: evento reenviado**. El evento se envió inicialmente como tipo 0 (telemetría normal), pero tiempo después se ha detectado que pertenece a un patrón de ataque escrito en la matriz MITRE. El evento se vuelve a enviar con los campos TTPs e IOAIds completados. ▪ **2: evento acumulado**: para ahorrar recursos, parte de la telemetría generada en el cliente se retiene hasta que el software de seguridad detecta un patrón de ataque MITRE. En ese momento se envían todos los eventos acumulados.	Enumeración

Modifype

Evento de tipo activo que se genera cuando un proceso (parent) modifica un programa ejecutable (child).

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
User (CEF)	Nombre de la cuenta de usuario y dominio al que pertenece utilizada para ejecutar el proceso que genero el evento registrado.	Cadena de caracteres
MachineIP (CEF)	Nombre del equipo que desencadena el evento registrado.	Dirección IP
MachineName (CEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
sev (LEEF)	Severidad del evento.	1
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
usrName (LEEF)	Cuenta de usuario utilizada por el proceso que realizó la operación registrada.	Cadena de caracteres
domain (LEEF)	Dominio de la cuenta de usuario utilizado por el proceso que realizó la operación registrada.	Cadena de caracteres
src (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identSrc (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identHostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres

Campo	Descripción	Valor
HostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
LocalDateTime	Fecha en formato UTC que tenía el equipo en el momento en que se produjo el evento registrado. Esta fecha depende de la configuración del equipo y por lo tanto puede ser errónea	Fecha
PandaTimeStatus	Contenido de los campos DateTime, Date y LocalDateTime	**0**: fecha real no soportada por tratarse de un evento antiguo. **1**: fecha real no disponible el servidor Cytomic y obtenida mediante un cálculo. **2**: fecha real proporcionada por el servidor Cytomic.
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
Op	Operación registrada.	Cadena de caracteres: “Modifype”
ParentHash	Hash del proceso que actúa como padre.	Cadena de caracteres
ParentDriveType	Tipo de unidad donde reside el proceso o fichero padre que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM	Enumeración

Campo	Descripción	Valor
	▪ **Ramdisk**: unidad de disco RAM.	
ParentPath	Ruta del fichero padre que realizó la operación registrada.	Cadena de caracteres
ParentPID	Identificador del proceso padre.	Numérico
ParentValidSig	El proceso padre está firmado digitalmente.	Booleano
ParentCompany	Contenido del atributo Company de los metadatos del proceso padre.	Cadena de caracteres
ParentBroken	El proceso padre está corrupto o defectuoso.	Booleano
ParentImageType	Arquitectura interna del proceso padre: ▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	Enumeración
ParentExeType	Estructura interna / tipo del proceso padre. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
ParentPrevalence	Prevalencia histórica del proceso padre en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ParentPrevLastDay	Prevalencia del proceso padre en el día anterior en los sistemas de Cytomic. ▪ High ▪ Medium	Enumeración

Campo	Descripción	Valor
	▪ Low	
ParentCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración
ParentMWName	Nombre del malware en el proceso padre si ya está catalogado como una amenaza. Si es Null el elemento no es malware.	Cadena de caracteres
ChildHash	Hash del proceso que actúa como hijo.	Cadena de caracteres
ChildDriveType	Tipo de unidad donde reside el proceso o fichero padre que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM ▪ **Ramdisk**: unidad de disco RAM.	Enumeración
ChildPath	Ruta del fichero hijo que realizó la operación registrada.	Cadena de caracteres (Ruta)
ChildPID	Identificador del proceso hijo.	Numérico
ChildValidSig	El proceso hijo está firmado digitalmente.	Booleano
ChildCompany	Contenido del atributo Company de los metadatos del proceso hijo.	Cadena de caracteres
ChildBroken	El proceso hijo está corrupto o defectuoso.	Booleano
ChildImageType	Arquitectura interna del proceso hijo:	Enumeración

Campo	Descripción	Valor
	▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	
ChildExeType	Estructura interna / tipo del proceso hijo. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
ChildPrevalence	Prevalencia histórica del proceso hijo en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ChildPrevLastDay	Prevalencia histórica del proceso hijo en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ChildCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración
ChildMWName	Nombre del malware en el proceso hijo si ya está catalogado como una amenaza. Si es	Cadena de caracteres

Campo	Descripción	Valor
	Null el elemento no es malware.	
OCS_Exec	Se ejecutó en el equipo software considerado como vulnerable.	Booleano
OCS_Name	Nombre del software vulnerable ejecutado.	Cadena de caracteres
OCS_Version	Versión del sistema operativo del equipo donde se ejecutó el software vulnerable.	Cadena de caracteres
Params	Parámetros de ejecución del proceso en la linea de comandos.	Cadena de caracteres
ToastResult	Respuesta del usuario ante el mensaje emergente mostrado por Cytomic EDR. ▪ **Ok**: el cliente acepta el mensaje. ▪ **Timeout**: el mensaje emergente desaparece por la no acción del usuario. ▪ **Angry**: el usuario rechaza el bloqueo desde el mensaje emergente. ▪ **Block** ▪ **Allow**	Enumeración
Action	Acción realizada por el agente Cytomic EDR. ▪ **Allow** ▪ **Block** ▪ **BlockTimeout**: se mostró un mensaje emergente al usuario pero no contestó a tiempo. ▪ **AllowWL**: elemento permitido por encontrarse en la lista blanca del administrador. ▪ **Disinfect** ▪ **Delete** ▪ **Quarantine** ▪ **AllowByUser**: se mostró un mensaje emergente al usuario y contesto “permitir ejecución”. ▪ **Informed**: se mostró un mensaje emergente al usuario. ▪ **Unquarantine**: el fichero se sacó de la cuarentena.	Enumeración

Campo	Descripción	Valor
	▪ **Rename**: elemento renombrado por no poderse mover a cuarentena, borrar o desinfectar. ▪ **BlockURL**: se bloqueó el acceso a una URL. ▪ **KillProcess**: cierre de proceso. ▪ **BlockExploit**: intento de explotación de proceso vulnerable detenido. ▪ **ExploitAllowByUser**: el usuario no permitió el cierre del proceso explotado. ▪ **RebootNeeded**: se requiere un reinicio del equipo para bloquear el intento de explotación. ▪ **ExploitInformed**: se mostró un mensaje emergente al usuario informando de un intento de explotación de proceso vulnerable. ▪ **AllowSonGWInstaller**: el programa forma parte de un paquete de instalación clasificado como Goodware. ▪ **EmbebedInformed**: el elemento es un script en powershell que ejecuta comandos. ▪ **SuspedProcess**: el elemento intentó suspender alguno de los servicios del software de protección. ▪ **ModifyDiskResource**: el elemento intentó modificar un fichero protegido que pertenece al software de protección. ▪ **ModifyRegistry**: el elemento intentó modificar una clave de registro protegida que pertenece al software de protección. ▪ **RenameRegistry**: el elemento intentó renombrar una clave de registro protegida que pertenece al software de protección.	

Campo	Descripción	Valor
	▪ **ModifyMarkFile**: el elemento intentó renombrar un fichero protegido que pertenece al software de protección. ▪ **UncertainAction**: el elemento intentó una acción sin definir sobre un fichero que pertenece al software de protección. ▪ **AllowGWFilter**: se permite la ejecución del elemento por estar en la caché de goodware. ▪ **AllowSWAuthoriced**: se permite la ejecución del elemento por estar autorizado por el administrador (configuración Software Autorizado). ▪ **NewPE**: aparición de un nuevo programa ejecutable en el equipo que viene del exterior. ▪ **AllowedByAdmin**: se permite la ejecución del elemento porque el administrador excluyó la técnica de explotación detectada. ▪ **Blocked by ip**: se bloqueó la dirección IP de origen por detectarse un ataque de fuerza bruta mediante el protocolo RDP. ▪ **AllowSonMsiGW**: se permite la ejecución del elemento por tratarse de un ejecutable que proviene de un paquete de instalación confiable. ▪ **Allowed by Global Audit**: el elemento se permite porque el software de seguridad está configurado en modo Global Audit.	
ServiceLevel	Modo de ejecución del agente: ▪ **Blocking**: el agente bloquea todos los ejecutables sin clasificar y los clasificados como malware. ▪ **Hardening**: el agente bloquea la ejecución de todos los programas sin clasificar cuyo origen no sea confiable y los clasificados como malware.	Enumeración

Campo	Descripción	Valor
	▪ **Learning**: el agente no bloquea ningún programa pero monitoriza los procesos ejecutados.	
WinningTech	Tecnología que provocó el evento. ▪ **Blockmode**: el agente estaba en modo Lock en el momento del bloqueo. ▪ **Cache**: clasificación cacheada en local. ▪ **Cloud**: clasificación descargada de la nube. ▪ **Context**: regla de contexto local. ▪ **ContextMinerva**: regla de contexto en la nube. ▪ **Digital Signature**: fichero firmado digitalmente. ▪ **Exploit**: tecnología de identificación de intento de explotación de proceso vulnerable. ▪ **ExploitLegacy** ▪ **GWFilter**: tecnologías de identificación de ficheros GW desconocidos. ▪ **LegacyUser**: permiso solicitado al usuario. ▪ **Local Signature**: firma local. ▪ **MetaEsploit**: ataque generado con el framework metaExploit. ▪ **NetNative**: tipo de binario. ▪ **Serializer**: tipo de binario. ▪ **User**: permiso solicitado al usuario. ▪ **RDP**: ataque de fuerza bruta por el protocolo RDP. ▪ **AMSI**: detección encontrada mediante Antimalware Scan Interface.	Enumeración
DetId	Identificador de la detección.	Cadena de caracteres
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres

Campo	Descripción	Valor
TTPs	Lista de las técnicas, tácticas y subtécnicas asociadas al evento MITRE.	Cadena de caracteres
IOAIds	Cuando una secuencia de eventos sigue un patrón descrito en la matriz MITRE, el producto de seguridad crea un indicio (IOA) y añade su identificador a todos los eventos que lo forman.	Numérico
TelemetryType	▪ **0: telemetría normal**. El evento no pertenece a un indicio que siga un patrón descrito en la matriz MITRE. ▪ **1: evento reenviado**. El evento se envió inicialmente como tipo 0 (telemetría normal), pero tiempo después se ha detectado que pertenece a un patrón de ataque escrito en la matriz MITRE. El evento se vuelve a enviar con los campos TTPs e IOAIds completados. ▪ **2: evento acumulado**: para ahorrar recursos, parte de la telemetría generada en el cliente se retiene hasta que el software de seguridad detecta un patrón de ataque MITRE. En ese momento se envían todos los eventos acumulados.	Enumeración

ModLinuxCfg

Evento de tipo activo que se genera cuando se detecta una modificación de un fichero de configuración en un sistema operativo Linux.

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
User (CEF)	Nombre de la cuenta de usuario y dominio al que pertenece utilizada para ejecutar el proceso que genero el evento registrado.	Cadena de caracteres
MachineIP (CEF)	Nombre del equipo que desencadena el evento registrado.	Dirección IP
MachineName (CEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
sev (LEEF)	Severidad del evento.	1
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
usrName (LEEF)	Cuenta de usuario utilizada por el proceso que realizó la operación registrada.	Cadena de caracteres
domain (LEEF)	Dominio de la cuenta de usuario utilizado por el proceso que realizó la operación registrada.	Cadena de caracteres
src (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identSrc (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identHostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres

Campo	Descripción	Valor
HostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
LocalDateTime	Fecha en formato UTC que tenía el equipo en el momento en que se produjo el evento registrado. Esta fecha depende de la configuración del equipo y por lo tanto puede ser errónea	Fecha
PandaTimeStatus	Contenido de los campos DateTime, Date y LocalDateTime	**0**: fecha real no soportada por tratarse de un evento antiguo. **1**: fecha real no disponible el servidor Cytomic y obtenida mediante un cálculo. **2**: fecha real proporcionada por el servidor Cytomic.
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
Op	Operación registrada.	Cadena de caracteres: “ModLinuxCfg”
ParentHash	Hash del proceso que actúa como padre.	Cadena de caracteres
ParentDriveType	Tipo de unidad donde reside el proceso o fichero padre que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM	Enumeración

Campo	Descripción	Valor
	▪ **Ramdisk**: unidad de disco RAM.	
ParentPath	Ruta del fichero padre que realizó la operación registrada.	Cadena de caracteres
ParentPID	Identificador del proceso padre.	Numérico
ParentValidSig	El proceso padre está firmado digitalmente.	Booleano
ParentCompany	Contenido del atributo Company de los metadatos del proceso padre.	Cadena de caracteres
ParentBroken	El proceso padre está corrupto o defectuoso.	Booleano
ParentImageType	Arquitectura interna del proceso padre: ▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	Enumeración
ParentExeType	Estructura interna / tipo del proceso padre. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
ParentPrevalence	Prevalencia histórica del proceso padre en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ParentPrevLastDay	Prevalencia del proceso padre en el día anterior en los sistemas de Cytomic. ▪ High ▪ Medium	Enumeración

Campo	Descripción	Valor
	▪ Low	
ParentCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración
ParentMWName	Nombre del malware en el proceso padre si ya está catalogado como una amenaza. Si es Null el elemento no es malware.	Cadena de caracteres
ChildHash	Hash del proceso que actúa como hijo.	Cadena de caracteres
ChildDriveType	Tipo de unidad donde reside el proceso o fichero padre que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM ▪ **Ramdisk**: unidad de disco RAM.	Enumeración
ChildPath	Ruta del fichero hijo que realizó la operación registrada.	Cadena de caracteres (Ruta)
ChildPID	Identificador del proceso hijo.	Numérico
ChildValidSig	El proceso hijo está firmado digitalmente.	Booleano
ChildCompany	Contenido del atributo Company de los metadatos del proceso hijo.	Cadena de caracteres
ChildBroken	El proceso hijo está corrupto o defectuoso.	Booleano
ChildImageType	Arquitectura interna del proceso hijo:	Enumeración

Campo	Descripción	Valor
	▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	
ChildExeType	Estructura interna / tipo del proceso hijo. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
ChildPrevalence	Prevalencia histórica del proceso hijo en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ChildPrevLastDay	Prevalencia histórica del proceso hijo en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ChildCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración
ChildMWName	Nombre del malware en el proceso hijo si ya está catalogado como una amenaza. Si es	Cadena de caracteres

Campo	Descripción	Valor
	Null el elemento no es malware.	
OCS_Exec	Se ejecutó en el equipo software considerado como vulnerable.	Booleano
OCS_Name	Nombre del software vulnerable ejecutado.	Cadena de caracteres
OCS_Version	Versión del sistema operativo del equipo donde se ejecutó el software vulnerable.	Cadena de caracteres
Params	Parámetros de ejecución del proceso en la linea de comandos.	Cadena de caracteres
ToastResult	Respuesta del usuario ante el mensaje emergente mostrado por Cytomic EDR. ▪ **Ok**: el cliente acepta el mensaje. ▪ **Timeout**: el mensaje emergente desaparece por la no acción del usuario. ▪ **Angry**: el usuario rechaza el bloqueo desde el mensaje emergente. ▪ **Block** ▪ **Allow**	Enumeración
Action	Acción realizada por el Cytomic EDR. ▪ **Allow** ▪ **Block** ▪ **BlockTimeout**: se mostró un mensaje emergente al usuario pero no contestó a tiempo. ▪ **AllowWL**: elemento permitido por encontrarse en la lista blanca del administrador. ▪ **Disinfect** ▪ **Delete** ▪ **Quarantine** ▪ **AllowByUser**: se mostró un mensaje emergente al usuario y contesto “permitir ejecución”. ▪ **Informed**: se mostró un mensaje emergente al usuario. ▪ **Unquarantine**: el fichero se sacó de la cuarentena.	Enumeración

Campo	Descripción	Valor
	▪ **Rename**: elemento renombrado por no poderse mover a cuarentena, borrar o desinfectar. ▪ **BlockURL**: se bloqueó el acceso a una URL. ▪ **KillProcess**: cierre de proceso. ▪ **BlockExploit**: intento de explotación de proceso vulnerable detenido. ▪ **ExploitAllowByUser**: el usuario no permitió el cierre del proceso explotado. ▪ **RebootNeeded**: se requiere un reinicio del equipo para bloquear el intento de explotación. ▪ **ExploitInformed**: se mostró un mensaje emergente al usuario informando de un intento de explotación de proceso vulnerable. ▪ **AllowSonGWInstaller**: el programa forma parte de un paquete de instalación clasificado como Goodware. ▪ **EmbebedInformed**: el elemento es un script en powershell que ejecuta comandos. ▪ **SuspedProcess**: el elemento intentó suspender alguno de los servicios del software de protección. ▪ **ModifyDiskResource**: el elemento intentó modificar un fichero protegido que pertenece al software de protección. ▪ **ModifyRegistry**: el elemento intentó modificar una clave de registro protegida que pertenece al software de protección. ▪ **RenameRegistry**: el elemento intentó renombrar una clave de registro protegida que pertenece al software de protección.	

Campo	Descripción	Valor
	▪ **ModifyMarkFile:** el elemento intentó renombrar un fichero protegido que pertenece al software de protección. ▪ **UncertainAction**: el elemento intentó una acción sin definir sobre un fichero que pertenece al software de protección. ▪ **AllowGWFilter**: se permite la ejecución del elemento por estar en la caché de goodware. ▪ **AllowSWAuthoriced**: se permite la ejecución del elemento por estar autorizado por el administrador (configuración Software Autorizado). ▪ **NewPE**: aparición de un nuevo programa ejecutable en el equipo que viene del exterior. ▪ **AllowedByAdmin**: se permite la ejecución del elemento porque el administrador excluyó la técnica de explotación detectada. ▪ **Blocked by ip**: se bloqueó la dirección IP de origen por detectarse un ataque de fuerza bruta mediante el protocolo RDP. ▪ **AllowSonMsiGW**: se permite la ejecución del elemento por tratarse de un ejecutable que proviene de un paquete de instalación confiable. ▪ **Allowed by Global Audit**: el elemento se permite porque el software de seguridad está configurado en modo Global Audit.	
ServiceLevel	Modo de ejecución del agente: ▪ **Blocking**: el agente bloquea todos los ejecutables sin clasificar y los clasificados como malware. ▪ **Hardening**: el agente bloquea la ejecución de todos los programas sin clasificar cuyo origen no sea confiable y los clasificados como malware.	Enumeración

Campo	Descripción	Valor
	▪ **Learning**: el agente no bloquea ningún programa pero monitoriza los procesos ejecutados.	
WinningTech	Tecnología que provocó el evento. ▪ **Blockmode**: el agente estaba en modo Lock en el momento del bloqueo. ▪ **Cache**: clasificación cacheada en local. ▪ **Cloud**: clasificación descargada de la nube. ▪ **Context**: regla de contexto local. ▪ **ContextMinerva**: regla de contexto en la nube. ▪ **Digital Signature**: fichero firmado digitalmente. ▪ **Exploit**: tecnología de identificación de intento de explotación de proceso vulnerable. ▪ **ExploitLegacy** ▪ **GWFilter**: tecnologías de identificación de ficheros GW desconocidos. ▪ **LegacyUser**: permiso solicitado al usuario. ▪ **Local Signature**: firma local. ▪ **MetaEsploit**: ataque generado con el framework metaExploit. ▪ **NetNative**: tipo de binario. ▪ **Serializer**: tipo de binario. ▪ **User**: permiso solicitado al usuario. ▪ **RDP**: ataque de fuerza bruta por el protocolo RDP. ▪ **AMSI**: detección encontrada mediante Antimalware Scan Interface.	Enumeración
DetId	Identificador de la detección.	Cadena de caracteres
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres

ModOSXCfg

Evento de tipo activo que se genera cuando se detecta una modificación de un fichero de configuración en un sistema operativo macOS.

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
User (CEF)	Nombre de la cuenta de usuario y dominio al que pertenece utilizada para ejecutar el proceso que genero el evento registrado.	Cadena de caracteres
MachineIP (CEF)	Nombre del equipo que desencadena el evento registrado.	Dirección IP
MachineName (CEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
sev (LEEF)	Severidad del evento.	1
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
usrName (LEEF)	Cuenta de usuario utilizada por el proceso que realizó la operación registrada.	Cadena de caracteres
domain (LEEF)	Dominio de la cuenta de usuario utilizado por el proceso que realizó la operación registrada.	Cadena de caracteres
src (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identSrc (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identHostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres

Campo	Descripción	Valor
HostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
LocalDateTime	Fecha en formato UTC que tenía el equipo en el momento en que se produjo el evento registrado. Esta fecha depende de la configuración del equipo y por lo tanto puede ser errónea	Fecha
PandaTimeStatus	Contenido de los campos DateTime, Date y LocalDateTime	**0**: fecha real no soportada por tratarse de un evento antiguo. **1**: fecha real no disponible el servidor Cytomic y obtenida mediante un cálculo. **2**: fecha real proporcionada por el servidor Cytomic.
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
Op	Operación registrada.	Cadena de caracteres: “ModOSXCfg”
ParentHash	Hash del proceso que actúa como padre.	Cadena de caracteres
ParentDriveType	Tipo de unidad donde reside el proceso o fichero padre que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM	Enumeración

Campo	Descripción	Valor
	▪ **Ramdisk**: unidad de disco RAM.	
ParentPath	Ruta del fichero padre que realizó la operación registrada.	Cadena de caracteres
ParentPID	Identificador del proceso padre.	Numérico
ParentValidSig	El proceso padre está firmado digitalmente.	Booleano
ParentCompany	Contenido del atributo Company de los metadatos del proceso padre.	Cadena de caracteres
ParentBroken	El proceso padre está corrupto o defectuoso.	Booleano
ParentImageType	Arquitectura interna del proceso padre: ▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	Enumeración
ParentExeType	Estructura interna / tipo del proceso padre. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
ParentPrevalence	Prevalencia histórica del proceso padre en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ParentPrevLastDay	Prevalencia del proceso padre en el día anterior en los sistemas de Cytomic. ▪ High ▪ Medium	Enumeración

Campo	Descripción	Valor
	▪ Low	
ParentCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración
ParentMWName	Nombre del malware en el proceso padre si ya está catalogado como una amenaza. Si es Null el elemento no es malware.	Cadena de caracteres
ChildHash	Hash del proceso que actúa como hijo.	Cadena de caracteres
ChildDriveType	Tipo de unidad donde reside el proceso o fichero padre que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM ▪ **Ramdisk**: unidad de disco RAM.	Enumeración
ChildPath	Ruta del fichero hijo que realizó la operación registrada.	Cadena de caracteres (Ruta)
ChildPID	Identificador del proceso hijo.	Numérico
ChildValidSig	El proceso hijo está firmado digitalmente.	Booleano
ChildCompany	Contenido del atributo Company de los metadatos del proceso hijo.	Cadena de caracteres
ChildBroken	El proceso hijo está corrupto o defectuoso.	Booleano
ChildImageType	Arquitectura interna del proceso hijo:	Enumeración

Campo	Descripción	Valor
	▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	
ChildExeType	Estructura interna / tipo del proceso hijo. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
ChildPrevalence	Prevalencia histórica del proceso hijo en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ChildPrevLastDay	Prevalencia histórica del proceso hijo en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ChildCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración
ChildMWName	Nombre del malware en el proceso hijo si ya está catalogado como una amenaza. Si es	Cadena de caracteres

Campo	Descripción	Valor
	Null el elemento no es malware.	
OCS_Exec	Se ejecutó en el equipo software considerado como vulnerable.	Booleano
OCS_Name	Nombre del software vulnerable ejecutado.	Cadena de caracteres
OCS_Version	Versión del sistema operativo del equipo donde se ejecutó el software vulnerable.	Cadena de caracteres
Params	Parámetros de ejecución del proceso en la linea de comandos.	Cadena de caracteres
ToastResult	Respuesta del usuario ante el mensaje emergente mostrado por Cytomic EDR. ▪ **Ok**: el cliente acepta el mensaje. ▪ **Timeout**: el mensaje emergente desaparece por la no acción del usuario. ▪ **Angry**: el usuario rechaza el bloqueo desde el mensaje emergente. ▪ **Block** ▪ **Allow**	Enumeración
Action	Acción realizada por el agente Cytomic EDR. ▪ **Allow** ▪ **Block** ▪ **BlockTimeout**: se mostró un mensaje emergente al usuario pero no contestó a tiempo. ▪ **AllowWL**: elemento permitido por encontrarse en la lista blanca del administrador. ▪ **Disinfect** ▪ **Delete** ▪ **Quarantine** ▪ **AllowByUser**: se mostró un mensaje emergente al usuario y contesto “permitir ejecución”. ▪ **Informed**: se mostró un mensaje emergente al usuario. ▪ **Unquarantine**: el fichero se sacó de la cuarentena.	Enumeración

Campo	Descripción	Valor
	▪ **Rename**: elemento renombrado por no poderse mover a cuarentena, borrar o desinfectar. ▪ **BlockURL**: se bloqueó el acceso a una URL. ▪ **KillProcess**: cierre de proceso. ▪ **BlockExploit**: intento de explotación de proceso vulnerable detenido. ▪ **ExploitAllowByUser**: el usuario no permitió el cierre del proceso explotado. ▪ **RebootNeeded**: se requiere un reinicio del equipo para bloquear el intento de explotación. ▪ **ExploitInformed**: se mostró un mensaje emergente al usuario informando de un intento de explotación de proceso vulnerable. ▪ **AllowSonGWInstaller**: el programa forma parte de un paquete de instalación clasificado como Goodware. ▪ **EmbebedInformed**: el elemento es un script en powershell que ejecuta comandos. ▪ **SuspedProcess**: el elemento intentó suspender alguno de los servicios del software de protección. ▪ **ModifyDiskResource**: el elemento intentó modificar un fichero protegido que pertenece al software de protección. ▪ **ModifyRegistry**: el elemento intentó modificar una clave de registro protegida que pertenece al software de protección. ▪ **RenameRegistry**: el elemento intentó renombrar una clave de registro protegida que pertenece al software de protección.	

Campo	Descripción	Valor
	▪ **ModifyMarkFile**: el elemento intentó renombrar un fichero protegido que pertenece al software de protección. ▪ **UncertainAction**: el elemento intentó una acción sin definir sobre un fichero que pertenece al software de protección. ▪ **AllowGWFilter**: se permite la ejecución del elemento por estar en la caché de goodware. ▪ **AllowSWAuthoriced**: se permite la ejecución del elemento por estar autorizado por el administrador (configuración Software Autorizado). ▪ **NewPE**: aparición de un nuevo programa ejecutable en el equipo que viene del exterior. ▪ **AllowedByAdmin**: se permite la ejecución del elemento porque el administrador excluyó la técnica de explotación detectada. ▪ **Blocked by ip**: se bloqueó la dirección IP de origen por detectarse un ataque de fuerza bruta mediante el protocolo RDP. ▪ **AllowSonMsiGW**: se permite la ejecución del elemento por tratarse de un ejecutable que proviene de un paquete de instalación confiable. ▪ **Allowed by Global Audit**: el elemento se permite porque el software de seguridad está configurado en modo Global Audit.	
ServiceLevel	Modo de ejecución del agente: ▪ **Blocking**: el agente bloquea todos los ejecutables sin clasificar y los clasificados como malware. ▪ **Hardening**: el agente bloquea la ejecución de todos los programas sin clasificar cuyo origen no sea confiable y los clasificados como malware.	Enumeración

Campo	Descripción	Valor
	▪ **Learning**: el agente no bloquea ningún programa pero monitoriza los procesos ejecutados.	
WinningTech	Tecnología que provocó el evento. ▪ **Blockmode**: el agente estaba en modo Lock en el momento del bloqueo. ▪ **Cache**: clasificación cacheada en local. ▪ **Cloud**: clasificación descargada de la nube. ▪ **Context**: regla de contexto local. ▪ **ContextMinerva**: regla de contexto en la nube. ▪ **Digital Signature**: fichero firmado digitalmente. ▪ **Exploit**: tecnología de identificación de intento de explotación de proceso vulnerable. ▪ **ExploitLegacy** ▪ **GWFilter**: tecnologías de identificación de ficheros GW desconocidos. ▪ **LegacyUser**: permiso solicitado al usuario. ▪ **Local Signature**: firma local. ▪ **MetaEsploit**: ataque generado con el framework metaExploit. ▪ **NetNative**: tipo de binario. ▪ **Serializer**: tipo de binario. ▪ **User**: permiso solicitado al usuario. ▪ **RDP**: ataque de fuerza bruta por el protocolo RDP. ▪ **AMSI**: detección encontrada mediante Antimalware Scan Interface.	Enumeración
DetId	Identificador de la detección.	Cadena de caracteres
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres

Monitoredopen

Evento de tipo activo que se genera cuando se detecta que un proceso (parent) accede a un fichero de datos (child).

El campo childpath solo contiene la extensión del fichero accedido para preservar la privacidad de los datos del cliente. Para incluir la ruta y nombre concreto del fichero accedido, consulta la guía avanzada del administrador de Cytomic EDR.

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
User (CEF)	Nombre de la cuenta de usuario y dominio al que pertenece utilizada para ejecutar el proceso que genero el evento registrado.	Cadena de caracteres
MachineIP (CEF)	Nombre del equipo que desencadena el evento registrado.	Dirección IP
MachineName (CEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
sev (LEEF)	Severidad del evento.	1
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
usrName (LEEF)	Cuenta de usuario utilizada por el proceso que realizó la operación registrada.	Cadena de caracteres
domain (LEEF)	Dominio de la cuenta de usuario utilizado por el proceso que realizó la operación registrada.	Cadena de caracteres
src (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres

Campo	Descripción	Valor
identSrc (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identHostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
HostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
LocalDateTime	Fecha en formato UTC que tenía el equipo en el momento en que se produjo el evento registrado. Esta fecha depende de la configuración del equipo y por lo tanto puede ser errónea	Fecha
PandaTimeStatus	Contenido de los campos DateTime, Date y LocalDateTime	**0**: fecha real no soportada por tratarse de un evento antiguo. **1**: fecha real no disponible el servidor Cytomic y obtenida mediante un cálculo. **2**: fecha real proporcionada por el servidor Cytomic.
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
ParentPid	Identificador del proceso padre.	Numérico
ParentHash	Hash del proceso que actúa como padre.	Cadena de caracteres
ParentPath	Ruta del fichero padre que realizó la operación registrada.	Cadena de caracteres
ParentValidSig	El proceso padre está firmado digitalmente.	Booleano
ParentCompany	Contenido del atributo Company de los metadatos del proceso padre.	Cadena de caracteres
ParentBroken	El proceso padre está corrupto o defectuoso.	Booleano
ParentImageType	Arquitectura interna del proceso padre: ▪ EXEx32	Enumeración

Campo	Descripción	Valor
	▪ EXEx64 ▪ DLLx32 ▪ DLLx64	
ParentExeType	Estructura interna / tipo del proceso padre. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
ParentPrevalence	Prevalencia histórica del proceso padre en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ParentPrevLastDay	Prevalencia del proceso padre en el día anterior en los sistemCytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ParentCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración
ParentMWName	Nombre del malware en el proceso padre si ya está catalogado como una amenaza. Si es Null el elemento no es malware.	Cadena de caracteres

Campo	Descripción	Valor
ChildPath	Ruta del fichero hijo que realizó la operación registrada.	Cadena de caracteres
LoggedUser	Usuario logeado en el equipo en el momento de la generación del evento.	Cadena de caracteres
ConfigString	Indica la versión del juego de reglas que estaban activas cuando se registró el evento. Utilizado para tareas de diagnóstico por parte del departamento de soporte de Cytomic.	Cadena de caracteres “Mx” (M0, M1, M2 etc.)
ParentAttibutes	Flags de atributos del proceso padre. ▪ **0x0000**: nivel de integridad del proceso Untrusted. ▪ **0x1000**: nivel de integridad del proceso Low integrity. ▪ **0x2000**: nivel de integridad del proceso Medium integrity. ▪ **0x3000**: nivel de integridad del proceso High integrity. ▪ **0x4000**: nivel de integridad del proceso System integrity. ▪ **0x5000**: nivel de integridad del proceso Protected. ▪ **0x00000100**: evento acumulativo. ▪ **0x00000200**: Indica si el proceso ha sido creado local o remotamente. ▪ **0x00000400**: Indica que la operación se ha producido antes del arranque del servicio.	Numérico
ChildAttributes	Flags de atributos del proceso hijo. ▪ **0x0000**: nivel de integridad del proceso Untrusted. ▪ **0x1000**: nivel de integridad del proceso Low integrity. ▪ **0x2000**: nivel de integridad del proceso Medium integrity. ▪ **0x3000**: nivel de integridad del proceso High integrity. ▪ **0x4000**: nivel de integridad del proceso System integrity.	Numérico

Campo	Descripción	Valor
	▪ **0x5000**: nivel de integridad del proceso Protected. ▪ **0x00000100**: evento acumulativo. ▪ **0x00000200**: Indica si el proceso ha sido creado local o remotamente. ▪ **0x00000400**: Indica que la operación se ha producido antes del arranque del servicio.	
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres
TTPs	Lista de las técnicas, tácticas y subtécnicas asociadas al evento MITRE.	Cadena de caracteres
IOAIds	Cuando una secuencia de eventos sigue un patrón descrito en la matriz MITRE, el producto de seguridad crea un indicio (IOA) y añade su identificador a todos los eventos que lo forman.	Numérico
TelemetryType	▪ **0: telemetría normal**. El evento no pertenece a un indicio que siga un patrón descrito en la matriz MITRE. ▪ **1: evento reenviado**. El evento se envió inicialmente como tipo 0 (telemetría normal), pero tiempo después se ha detectado que pertenece a un patrón de ataque escrito en la matriz MITRE. El evento se vuelve a enviar con los campos TTPs e IOAIds completados. ▪ **2: evento acumulado**: para ahorrar recursos, parte de la telemetría generada en el cliente se retiene hasta que el software de seguridad detecta un patrón de ataque MITRE. En ese momento se envían todos los eventos acumulados.	Enumeración

Monitoredregistry

Evento de tipo activo que se genera cuando se detecta un proceso (parent) que accede al registro del equipo del usuario para leer una rama.

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
User (CEF)	Nombre de la cuenta de usuario y dominio al que pertenece utilizada para ejecutar el proceso que genero el evento registrado.	Cadena de caracteres
MachineIP (CEF)	Nombre del equipo que desencadena el evento registrado.	Dirección IP
MachineName (CEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
sev (LEEF)	Severidad del evento.	1
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
usrName (LEEF)	Cuenta de usuario utilizada por el proceso que realizó la operación registrada.	Cadena de caracteres
domain (LEEF)	Dominio de la cuenta de usuario utilizado por el proceso que realizó la operación registrada.	Cadena de caracteres
src (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identSrc (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identHostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres

Campo	Descripción	Valor
HostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
LocalDateTime	Fecha en formato UTC que tenía el equipo en el momento en que se produjo el evento registrado. Esta fecha depende de la configuración del equipo y por lo tanto puede ser errónea	Fecha
PandaTimeStatus	Contenido de los campos DateTime, Date y LocalDateTime	**0**: fecha real no soportada por tratarse de un evento antiguo. **1**: fecha real no disponible el servidor Cytomic y obtenida mediante un cálculo. **2**: fecha real proporcionada por el servidor Cytomic.
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
ParentPid	Identificador del proceso padre.	Numérico
ParentHash	Hash del proceso que actúa como padre.	Cadena de caracteres
ParentPath	Ruta del fichero padre que realizó la operación registrada.	Cadena de caracteres
ParentValidSig	El proceso padre está firmado digitalmente.	Booleano
ParentCompany	Contenido del atributo Company de los metadatos del proceso padre.	Cadena de caracteres
ParentBroken	El proceso padre está corrupto o defectuoso.	Booleano
ParentImageType	Arquitectura interna del proceso padre: ▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	Enumeración
ParentExeType	Estructura interna / tipo del proceso padre.	Enumeración

Campo	Descripción	Valor
	▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	
ParentPrevalence	Prevalencia histórica del proceso padre en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ParentPrevLastDay	Prevalencia del proceso padre en el día anterior en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ParentCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración
ParentMWName	Nombre del malware en el proceso padre si ya está catalogado como una amenaza. Si es Null el elemento no es malware.	Cadena de caracteres
RegAction	Tipo de operación realizada en el registro del equipo. ▪ CreateKey ▪ CreateValue	Enumeración

Campo	Descripción	Valor
	▪ ModifyValue	
Key	Rama o clave del registro afectado.	Cadena de caracteres
Value	Nombre del valor afectado dentro de la clave del registro.	Cadena de caracteres
ValueData	Contenido del valor de la clave del registro.	Cadena de caracteres
LoggedUser	Usuario logeado en el equipo en el momento de la generación del evento.	Cadena de caracteres
ConfigString	Indica la versión del juego de reglas que estaban activas cuando se registró el evento. Utilizado para tareas de diagnóstico por parte del departamento de soporte de Cytomic.	Cadena de caracteres “Mx” (M0, M1, M2 etc.)
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres
TTPs	Lista de las técnicas, tácticas y subtécnicas asociadas al evento MITRE.	Cadena de caracteres
IOAIds	Cuando una secuencia de eventos sigue un patrón descrito en la matriz MITRE, el producto de seguridad crea un indicio (IOA) y añade su identificador a todos los eventos que lo forman.	Numérico
TelemetryType	▪ **0: telemetría normal**. El evento no pertenece a un indicio que siga un patrón descrito en la matriz MITRE. ▪ **1: evento reenviado**. El evento se envió inicialmente como tipo 0 (telemetría normal), pero tiempo después se ha detectado que pertenece a un patrón de ataque escrito en la matriz MITRE. El evento se vuelve a enviar con los campos TTPs e IOAIds completados. ▪ **2: evento acumulado**: para ahorrar recursos, parte de la telemetría generada en el cliente se retiene hasta que el software de seguridad detecta un patrón de ataque MITRE. En ese momento se envían todos los eventos acumulados.	Enumeración

Notblocked

Evento de tipo activo que se genera con cada acción que Cytomic EDPR deja sin analizar debido a situaciones excepcionales (durante el tiempo de arranque del servicio en la protección, cambios de configuración etc.).

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
User (CEF)	Nombre de la cuenta de usuario y dominio al que pertenece utilizada para ejecutar el proceso que genero el evento registrado.	Cadena de caracteres
MachineIP (CEF)	Nombre del equipo que desencadena el evento registrado.	Dirección IP
MachineName (CEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
sev (LEEF)	Severidad del evento.	1
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
usrName (LEEF)	Cuenta de usuario utilizada por el proceso que realizó la operación registrada.	Cadena de caracteres
domain (LEEF)	Dominio de la cuenta de usuario utilizado por el proceso que realizó la operación registrada.	Cadena de caracteres
src (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identSrc (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres

Campo	Descripción	Valor
identHostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
HostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
LocalDateTime	Fecha en formato UTC que tenía el equipo en el momento en que se produjo el evento registrado. Esta fecha depende de la configuración del equipo y por lo tanto puede ser errónea	Fecha
PandaTimeStatus	Contenido de los campos DateTime, Date y LocalDateTime	**0**: fecha real no soportada por tratarse de un evento antiguo. **1**: fecha real no disponible el servidor Cytomic y obtenida mediante un cálculo. **2**: fecha real proporcionada por el servidor Cytomic.
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
ParentHash	Digest / hash del fichero padre.	Cadena de caracteres
ParentPath	Ruta del proceso padre.	Cadena de caracteres
ParentValidSig	Proceso padre firmado digitalmente.	Booleano
ParentCompany	Contenido del atributo Company de los metadatos del proceso padre	Cadena de caracteres
ParentBroken	El proceso padre está corrupto o defectuoso.	Booleano
ParentImageType	Arquitectura interna del proceso	Enumeración

Campo	Descripción	Valor
	padre: ▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	
ParentExeType	Estructura interna / tipo del proceso padre. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
ParentPrevalence	Prevalencia histórica del proceso padre en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ParentPrevLastDay	Prevalencia del proceso padre en el día anterior en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ParentCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP	Enumeración

Campo	Descripción	Valor
	▪ Unknown ▪ Monitoring	
ParentMWName	Nombre del malware en el proceso padre si ya está catalogado como una amenaza. Si es Null el elemento no es malware.	Cadena de caracteres
ChildHash	Hash del proceso que actúa como hijo.	Cadena de caracteres
ChildPath	Ruta del fichero hijo que realizó la operación registrada.	Cadena de caracteres (Ruta)
ChildValidSig	El proceso hijo está firmado digitalmente.	Booleano
ChildCompany	Contenido del atributo Company de los metadatos del proceso hijo.	Cadena de caracteres
ChildBroken	El proceso hijo está corrupto o defectuoso.	Booleano
ChildImageType	Arquitectura interna del proceso hijo: ▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	Enumeración
ChildExeType	Estructura interna / tipo del proceso hijo. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración

Campo	Descripción	Valor
ChildPrevalence	Prevalencia histórica del proceso hijo en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ChildPrevLastDay	Prevalencia histórica del proceso hijo en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ChildCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración
ChildMWName	Nombre del malware en el proceso hijo si ya está catalogado como una amenaza. Si es Null el elemento no es malware.	Cadena de caracteres
ResponseCat	Categoría del fichero asignada según las tecnologías locales implementadas en del software de protección. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración
NumCacheClassifiedElements	Numero de identificadores cacheados en el equipo del usuario en el momento en que se generó el evento.	Numérico
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres

Opencmp

Evento de tipo activo que se genera cuando se detecta un proceso (parent) que abre un fichero comprimido (child).

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
User (CEF)	Nombre de la cuenta de usuario y dominio al que pertenece utilizada para ejecutar el proceso que genero el evento registrado.	Cadena de caracteres
MachineIP (CEF)	Nombre del equipo que desencadena el evento registrado.	Dirección IP
MachineName (CEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
sev (LEEF)	Severidad del evento.	1
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
usrName (LEEF)	Cuenta de usuario utilizada por el proceso que realizó la operación registrada.	Cadena de caracteres
domain (LEEF)	Dominio de la cuenta de usuario utilizado por el proceso que realizó la operación registrada.	Cadena de caracteres
src (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identSrc (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identHostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres

Campo	Descripción	Valor
HostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
LocalDateTime	Fecha en formato UTC que tenía el equipo en el momento en que se produjo el evento registrado. Esta fecha depende de la configuración del equipo y por lo tanto puede ser errónea	Fecha
PandaTimeStatus	Contenido de los campos DateTime, Date y LocalDateTime	**0**: fecha real no soportada por tratarse de un evento antiguo. **1**: fecha real no disponible el servidor Cytomic y obtenida mediante un cálculo. **2**: fecha real proporcionada por el servidor Cytomic.
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
Op	Operación registrada.	Cadena de caracteres: “Opencmp”
ParentHash	Hash del proceso que actúa como padre.	Cadena de caracteres
ParentDriveType	Tipo de unidad donde reside el proceso o fichero padre que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM	Enumeración

Campo	Descripción	Valor
	▪ **Ramdisk**: unidad de disco RAM.	
ParentPath	Ruta del fichero padre que realizó la operación registrada.	Cadena de caracteres
ParentPID	Identificador del proceso padre.	Numérico
ParentValidSig	El proceso padre está firmado digitalmente.	Booleano
ParentCompany	Contenido del atributo Company de los metadatos del proceso padre.	Cadena de caracteres
ParentBroken	El proceso padre está corrupto o defectuoso.	Booleano
ParentImageType	Arquitectura interna del proceso padre: ▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	Enumeración
ParentExeType	Estructura interna / tipo del proceso padre. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
ParentPrevalence	Prevalencia histórica del proceso padre en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ParentPrevLastDay	Prevalencia del proceso padre en el día anterior en los sistemas de Cytomic. ▪ High ▪ Medium	Enumeración

Campo	Descripción	Valor
	▪ Low	
ParentCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración
Parent MWName	Nombre del malware en el proceso padre si ya está catalogado como una amenaza. Si es Null el elemento no es malware.	Cadena de caracteres
ChildHash	Hash del proceso que actúa como hijo.	Cadena de caracteres
ChildDriveType	Tipo de unidad donde reside el proceso o fichero padre que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM ▪ **Ramdisk**: unidad de disco RAM.	Enumeración
ChildPath	Ruta del fichero hijo que realizó la operación registrada.	Cadena de caracteres (Ruta)
ChildPID	Identificador del proceso hijo.	Numérico
ChildValidSig	El proceso hijo está firmado digitalmente.	Booleano
ChildCompany	Contenido del atributo Company de los metadatos del proceso hijo.	Cadena de caracteres
ChildBroken	El proceso hijo está corrupto o defectuoso.	Booleano
ChildImageType	Arquitectura interna del proceso hijo:	Enumeración

Campo	Descripción	Valor
	▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	
ChildExeType	Estructura interna / tipo del proceso hijo. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
ChildPrevalence	Prevalencia histórica del proceso hijo en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ChildPrevLastDay	Prevalencia histórica del proceso hijo en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ChildCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración
ChildMWName	Nombre del malware en el proceso hijo si ya está catalogado como una amenaza. Si es	Cadena de caracteres

Campo	Descripción	Valor
	Null el elemento no es malware.	
OCS_Exec	Se ejecutó en el equipo software considerado como vulnerable.	Booleano
OCS_Name	Nombre del software vulnerable ejecutado.	Cadena de caracteres
OCS_Version	Versión del sistema operativo del equipo donde se ejecutó el software vulnerable.	Cadena de caracteres
Params	Parámetros de ejecución del proceso en la linea de comandos.	Cadena de caracteres
ToastResult	Respuesta del usuario ante el mensaje emergente mostrado por Cytomic EDR. ▪ **Ok**: el cliente acepta el mensaje. ▪ **Timeout**: el mensaje emergente desaparece por la no acción del usuario. ▪ **Angry**: el usuario rechaza el bloqueo desde el mensaje emergente. ▪ **Block** ▪ **Allow**	Enumeración
Action	Acción realizada por el agente Cytomic. ▪ **Allow** ▪ **Block** ▪ **BlockTimeout**: se mostró un mensaje emergente al usuario pero no contestó a tiempo. ▪ **AllowWL**: elemento permitido por encontrarse en la lista blanca del administrador. ▪ **Disinfect** ▪ **Delete** ▪ **Quarantine** ▪ **AllowByUser**: se mostró un mensaje emergente al usuario y contesto “permitir ejecución”. ▪ **Informed**: se mostró un mensaje emergente al usuario. ▪ **Unquarantine**: el fichero se sacó de la cuarentena.	Enumeración

Campo	Descripción	Valor
	▪ **Rename**: elemento renombrado por no poderse mover a cuarentena, borrar o desinfectar. ▪ **BlockURL**: se bloqueó el acceso a una URL. ▪ **KillProcess**: cierre de proceso. ▪ **BlockExploit**: intento de explotación de proceso vulnerable detenido. ▪ **ExploitAllowByUser**: el usuario no permitió el cierre del proceso explotado. ▪ **RebootNeeded**: se requiere un reinicio del equipo para bloquear el intento de explotación. ▪ **ExploitInformed**: se mostró un mensaje emergente al usuario informando de un intento de explotación de proceso vulnerable. ▪ **AllowSonGWInstaller**: el programa forma parte de un paquete de instalación clasificado como Goodware. ▪ **EmbebedInformed**: el elemento es un script en powershell que ejecuta comandos. ▪ **SuspedProcess**: el elemento intentó suspender alguno de los servicios del software de protección. ▪ **ModifyDiskResource**: el elemento intentó modificar un fichero protegido que pertenece al software de protección. ▪ **ModifyRegistry**: el elemento intentó modificar una clave de registro protegida que pertenece al software de protección. ▪ **RenameRegistry**: el elemento intentó renombrar una clave de registro protegida que pertenece al software de protección.	

Campo	Descripción	Valor
	▪ **ModifyMarkFile**: el elemento intentó renombrar un fichero protegido que pertenece al software de protección. ▪ **UncertainAction**: el elemento intentó una acción sin definir sobre un fichero que pertenece al software de protección. ▪ **AllowGWFilter**: se permite la ejecución del elemento por estar en la caché de goodware. ▪ **AllowSWAuthoriced**: se permite la ejecución del elemento por estar autorizado por el administrador (configuración Software Autorizado). ▪ **NewPE**: aparición de un nuevo programa ejecutable en el equipo que viene del exterior. ▪ **AllowedByAdmin**: se permite la ejecución del elemento porque el administrador excluyó la técnica de explotación detectada. ▪ **Blocked by ip**: se bloqueó la dirección IP de origen por detectarse un ataque de fuerza bruta mediante el protocolo RDP. ▪ **AllowSonMsiGW**: se permite la ejecución del elemento por tratarse de un ejecutable que proviene de un paquete de instalación confiable. ▪ **Allowed by Global Audit**: el elemento se permite porque el software de seguridad está configurado en modo Global Audit.	
ServiceLevel	Modo de ejecución del agente: ▪ **Blocking**: el agente bloquea todos los ejecutables sin clasificar y los clasificados como malware. ▪ **Hardening**: el agente bloquea la ejecución de todos los programas sin clasificar cuyo origen no sea confiable y los clasificados como malware.	Enumeración

Campo	Descripción	Valor
	▪ **Learning**: el agente no bloquea ningún programa pero monitoriza los procesos ejecutados.	
WinningTech	Tecnología que provocó el evento. ▪ **Blockmode**: el agente estaba en modo Lock en el momento del bloqueo. ▪ **Cache**: clasificación cacheada en local. ▪ **Cloud**: clasificación descargada de la nube. ▪ **Context**: regla de contexto local. ▪ **ContextMinerva**: regla de contexto en la nube. ▪ **Digital Signature**: fichero firmado digitalmente. ▪ **Exploit**: tecnología de identificación de intento de explotación de proceso vulnerable. ▪ **ExploitLegacy** ▪ **GWFilter**: tecnologías de identificación de ficheros GW desconocidos. ▪ **LegacyUser**: permiso solicitado al usuario. ▪ **Local Signature**: firma local. ▪ **MetaEsploit**: ataque generado con el framework metaExploit. ▪ **NetNative**: tipo de binario. ▪ **Serializer**: tipo de binario. ▪ **User**: permiso solicitado al usuario. ▪ **RDP**: ataque de fuerza bruta por el protocolo RDP. ▪ **AMSI**: detección encontrada mediante Antimalware Scan Interface.	Enumeración
DetId	Identificador de la detección.	Cadena de caracteres
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres

Campo	Descripción	Valor
TTPs	Lista de las técnicas, tácticas y subtécnicas asociadas al evento MITRE.	Cadena de caracteres
IOAIds	Cuando una secuencia de eventos sigue un patrón descrito en la matriz MITRE, el producto de seguridad crea un indicio (IOA) y añade su identificador a todos los eventos que lo forman.	Numérico
TelemetryType	▪ **0: telemetría normal**. El evento no pertenece a un indicio que siga un patrón descrito en la matriz MITRE. ▪ **1: evento reenviado**. El evento se envió inicialmente como tipo 0 (telemetría normal), pero tiempo después se ha detectado que pertenece a un patrón de ataque escrito en la matriz MITRE. El evento se vuelve a enviar con los campos TTPs e IOAIds completados. ▪ **2: evento acumulado**: para ahorrar recursos, parte de la telemetría generada en el cliente se retiene hasta que el software de seguridad detecta un patrón de ataque MITRE. En ese momento se envían todos los eventos acumulados.	Enumeración

OpenIsass

Evento de tipo activo que se genera cuando se detecta un proceso (parent) que acede al proceso LSASS para intentar comprometer las credenciales de una cuenta de usuario.

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
User (CEF)	Nombre de la cuenta de usuario y dominio al que pertenece utilizada para ejecutar el proceso que genero el evento registrado.	Cadena de caracteres
MachineIP (CEF)	Nombre del equipo que desencadena el evento registrado.	Dirección IP
MachineName (CEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
sev (LEEF)	Severidad del evento.	1
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
usrName (LEEF)	Cuenta de usuario utilizada por el proceso que realizó la operación registrada.	Cadena de caracteres
domain (LEEF)	Dominio de la cuenta de usuario utilizado por el proceso que realizó la operación registrada.	Cadena de caracteres
src (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identSrc (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identHostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres

Campo	Descripción	Valor
HostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
LocalDateTime	Fecha en formato UTC que tenía el equipo en el momento en que se produjo el evento registrado. Esta fecha depende de la configuración del equipo y por lo tanto puede ser errónea	Fecha
PandaTimeStatus	Contenido de los campos DateTime, Date y LocalDateTime	**0**: fecha real no soportada por tratarse de un evento antiguo. **1**: fecha real no disponible el servidor Cytomic y obtenida mediante un cálculo. **2**: fecha real proporcionada por el servidor Cytomic.
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
Op	Operación registrada.	Cadena de caracteres: “OpenIsass”
ParentHash	Hash del proceso que actúa como padre.	Cadena de caracteres
ParentDriveType	Tipo de unidad donde reside el proceso o fichero padre que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM	Enumeración

Campo	Descripción	Valor
	▪ **Ramdisk**: unidad de disco RAM.	
ParentPath	Ruta del fichero padre que realizó la operación registrada.	Cadena de caracteres
ParentPID	Identificador del proceso padre.	Numérico
ParentValidSig	El proceso padre está firmado digitalmente.	Booleano
ParentCompany	Contenido del atributo Company de los metadatos del proceso padre.	Cadena de caracteres
ParentBroken	El proceso padre está corrupto o defectuoso.	Booleano
ParentImageType	Arquitectura interna del proceso padre: ▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	Enumeración
ParentExeType	Estructura interna / tipo del proceso padre. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
ParentPrevalence	Prevalencia histórica del proceso padre en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ParentPrevLastDay	Prevalencia del proceso padre en el día anterior en los sistemas de Cytomic. ▪ High ▪ Medium	Enumeración

Campo	Descripción	Valor
	▪ Low	
ParentCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración
ParentMWName	Nombre del malware en el proceso padre si ya está catalogado como una amenaza. Si es Null el elemento no es malware.	Cadena de caracteres
ChildHash	Hash del proceso que actúa como hijo.	Cadena de caracteres
ChildDriveType	Tipo de unidad donde reside el proceso o fichero padre que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM ▪ **Ramdisk**: unidad de disco RAM.	Enumeración
ChildPath	Ruta del fichero hijo que realizó la operación registrada.	Cadena de caracteres (Ruta)
ChildPID	Identificador del proceso hijo.	Numérico
ChildValidSig	El proceso hijo está firmado digitalmente.	Booleano
ChildCompany	Contenido del atributo Company de los metadatos del proceso hijo.	Cadena de caracteres
ChildBroken	El proceso hijo está corrupto o defectuoso.	Booleano
ChildImageType	Arquitectura interna del proceso hijo:	Enumeración

Campo	Descripción	Valor
	▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	
ChildExeType	Estructura interna / tipo del proceso hijo. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
ChildPrevalence	Prevalencia histórica del proceso hijo en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ChildPrevLastDay	Prevalencia histórica del proceso hijo en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ChildCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración
ChildMWName	Nombre del malware en el proceso hijo si ya está catalogado como una amenaza. Si es	Cadena de caracteres

Campo	Descripción	Valor
	Null el elemento no es malware.	
OCS_Exec	Se ejecutó en el equipo software considerado como vulnerable.	Booleano
OCS_Name	Nombre del software vulnerable ejecutado.	Cadena de caracteres
OCS_Version	Versión del sistema operativo del equipo donde se ejecutó el software vulnerable.	Cadena de caracteres
Params	Parámetros de ejecución del proceso en la linea de comandos.	Cadena de caracteres
ToastResult	Respuesta del usuario ante el mensaje emergente mostrado por Cytomic EDR. ▪ **Ok**: el cliente acepta el mensaje. ▪ **Timeout**: el mensaje emergente desaparece por la no acción del usuario. ▪ **Angry**: el usuario rechaza el bloqueo desde el mensaje emergente. ▪ **Block** ▪ **Allow**	Enumeración
Action	Acción realizada por el agente Cytomic. ▪ **Allow** ▪ **Block** ▪ **BlockTimeout**: se mostró un mensaje emergente al usuario pero no contestó a tiempo. ▪ **AllowWL**: elemento permitido por encontrarse en la lista blanca del administrador. ▪ **Disinfect** ▪ **Delete** ▪ **Quarantine** ▪ **AllowByUser**: se mostró un mensaje emergente al usuario y contesto “permitir ejecución”. ▪ **Informed**: se mostró un mensaje emergente al usuario. ▪ **Unquarantine**: el fichero se sacó de la cuarentena.	Enumeración

Campo	Descripción	Valor
	▪ **Rename**: elemento renombrado por no poderse mover a cuarentena, borrar o desinfectar. ▪ **BlockURL**: se bloqueó el acceso a una URL. ▪ **KillProcess**: cierre de proceso. ▪ **BlockExploit**: intento de explotación de proceso vulnerable detenido. ▪ **ExploitAllowByUser**: el usuario no permitió el cierre del proceso explotado. ▪ **RebootNeeded**: se requiere un reinicio del equipo para bloquear el intento de explotación. ▪ **ExploitInformed**: se mostró un mensaje emergente al usuario informando de un intento de explotación de proceso vulnerable. ▪ **AllowSonGWInstaller**: el programa forma parte de un paquete de instalación clasificado como Goodware. ▪ **EmbebedInformed**: el elemento es un script en powershell que ejecuta comandos. ▪ **SuspedProcess**: el elemento intentó suspender alguno de los servicios del software de protección. ▪ **ModifyDiskResource**: el elemento intentó modificar un fichero protegido que pertenece al software de protección. ▪ **ModifyRegistry**: el elemento intentó modificar una clave de registro protegida que pertenece al software de protección. ▪ **RenameRegistry**: el elemento intentó renombrar una clave de registro protegida que pertenece al software de protección.	

Campo	Descripción	Valor
	▪ **ModifyMarkFile**: el elemento intentó renombrar un fichero protegido que pertenece al software de protección. ▪ **UncertainAction**: el elemento intentó una acción sin definir sobre un fichero que pertenece al software de protección. ▪ **AllowGWFilter**: se permite la ejecución del elemento por estar en la caché de goodware. ▪ **AllowSWAuthoriced**: se permite la ejecución del elemento por estar autorizado por el administrador (configuración Software Autorizado). ▪ **NewPE**: aparición de un nuevo programa ejecutable en el equipo que viene del exterior. ▪ **AllowedByAdmin**: se permite la ejecución del elemento porque el administrador excluyó la técnica de explotación detectada. ▪ **Blocked by ip**: se bloqueó la dirección IP de origen por detectarse un ataque de fuerza bruta mediante el protocolo RDP. ▪ **AllowSonMsiGW**: se permite la ejecución del elemento por tratarse de un ejecutable que proviene de un paquete de instalación confiable. ▪ **Allowed by Global Audit**: el elemento se permite porque el software de seguridad está configurado en modo Global Audit.	
ServiceLevel	Modo de ejecución del agente: ▪ **Blocking**: el agente bloquea todos los ejecutables sin clasificar y los clasificados como malware. ▪ **Hardening**: el agente bloquea la ejecución de todos los programas sin clasificar cuyo origen no sea confiable y los clasificados como malware.	Enumeración

Campo	Descripción	Valor
	▪ **Learning**: el agente no bloquea ningún programa pero monitoriza los procesos ejecutados.	
WinningTech	Tecnología que provocó el evento. ▪ **Blockmode**: el agente estaba en modo Lock en el momento del bloqueo. ▪ **Cache**: clasificación cacheada en local. ▪ **Cloud**: clasificación descargada de la nube. ▪ **Context**: regla de contexto local. ▪ **ContextMinerva**: regla de contexto en la nube. ▪ **Digital Signature**: fichero firmado digitalmente. ▪ **Exploit**: tecnología de identificación de intento de explotación de proceso vulnerable. ▪ **ExploitLegacy** ▪ **GWFilter**: tecnologías de identificación de ficheros GW desconocidos. ▪ **LegacyUser**: permiso solicitado al usuario. ▪ **Local Signature**: firma local. ▪ **MetaEsploit**: ataque generado con el framework metaExploit. ▪ **NetNative**: tipo de binario. ▪ **Serializer**: tipo de binario. ▪ **User**: permiso solicitado al usuario. ▪ **RDP**: ataque de fuerza bruta por el protocolo RDP. ▪ **AMSI**: detección encontrada mediante Antimalware Scan Interface.	Enumeración
DetId	Identificador de la detección.	Cadena de caracteres
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres

Campo	Descripción	Valor
TTPs	Lista de las técnicas, tácticas y subtécnicas asociadas al evento MITRE.	Cadena de caracteres
IOAIds	Cuando una secuencia de eventos sigue un patrón descrito en la matriz MITRE, el producto de seguridad crea un indicio (IOA) y añade su identificador a todos los eventos que lo forman.	Numérico
TelemetryType	▪ **0: telemetría normal**. El evento no pertenece a un indicio que siga un patrón descrito en la matriz MITRE. ▪ **1: evento reenviado**. El evento se envió inicialmente como tipo 0 (telemetría normal), pero tiempo después se ha detectado que pertenece a un patrón de ataque escrito en la matriz MITRE. El evento se vuelve a enviar con los campos TTPs e IOAIds completados. ▪ **2: evento acumulado**: para ahorrar recursos, parte de la telemetría generada en el cliente se retiene hasta que el software de seguridad detecta un patrón de ataque MITRE. En ese momento se envían todos los eventos acumulados.	Enumeración

ProcessNetBytes

Evento de tipo activo que se genera cuando un proceso consume datos de red. Se envía un evento 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 es la suma de todas las cantidades registradas.

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
User (CEF)	Nombre de la cuenta de usuario y dominio al que pertenece utilizada para ejecutar el proceso que genero el evento registrado.	Cadena de caracteres
MachineIP (CEF)	Nombre del equipo que desencadena el evento registrado.	Dirección IP
MachineName (CEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
sev (LEEF)	Severidad del evento.	1
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
usrName (LEEF)	Cuenta de usuario utilizada por el proceso que realizó la operación registrada.	Cadena de caracteres
domain (LEEF)	Dominio de la cuenta de usuario utilizado por el proceso que realizó la operación registrada.	Cadena de caracteres
src (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identSrc (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identHostName	Nombre del equipo que desencadena el evento	Cadena de caracteres

Campo	Descripción	Valor
(LEEF)	registrado.	
HostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
LocalDateTime	Fecha en formato UTC que tenía el equipo en el momento en que se produjo el evento registrado. Esta fecha depende de la configuración del equipo y por lo tanto puede ser errónea	Fecha
PandaTimeStatus	Contenido de los campos DateTime, Date y LocalDateTime	**0**: fecha real no soportada por tratarse de un evento antiguo. **1**: fecha real no disponible el servidor Cytomic y obtenida mediante un cálculo. **2**: fecha real proporcionada por el servidor Cytomic.
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
Hash	Hash / digest del fichero.	Cadena de caracteres
Path	Ruta del elemento que desencadenó la operación registrada.	Cadena de caracteres
PID	Identificador del proceso.	Numérico
BytesSent	Acumulado de bytes enviados por el proceso desde la generación del ultimo evento ProcessNetBytes.	Numérico
BytesReceived	Acumulado de bytes recibidos por el proceso desde la generación del ultimo evento ProcessNetBytes.	Numérico
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres

Registryc

Evento de tipo activo que se genera cuando un proceso (parent) crea una rama del registro que apunta a un fichero ejecutable (child).

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
User (CEF)	Nombre de la cuenta de usuario y dominio al que pertenece utilizada para ejecutar el proceso que genero el evento registrado.	Cadena de caracteres
MachineIP (CEF)	Nombre del equipo que desencadena el evento registrado.	Dirección IP
MachineName (CEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
sev (LEEF)	Severidad del evento.	1
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
usrName (LEEF)	Cuenta de usuario utilizada por el proceso que realizó la operación registrada.	Cadena de caracteres
domain (LEEF)	Dominio de la cuenta de usuario utilizado por el proceso que realizó la operación registrada.	Cadena de caracteres
src (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identSrc (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identHostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres

Campo	Descripción	Valor
HostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
LocalDateTime	Fecha en formato UTC que tenía el equipo en el momento en que se produjo el evento registrado. Esta fecha depende de la configuración del equipo y por lo tanto puede ser errónea	Fecha
PandaTimeStatus	Contenido de los campos DateTime, Date y LocalDateTime	**0**: fecha real no soportada por tratarse de un evento antiguo. **1**: fecha real no disponible el servidor Cytomic y obtenida mediante un cálculo. **2**: fecha real proporcionada por el servidor Cytomic.
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
op	Operación registrada.	CreateExeKey
Hash	Hash del proceso que actúa como padre.	Cadena de caracteres
DriveType	Tipo de unidad donde reside el proceso o fichero padre que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM ▪ **Ramdisk**: unidad de disco RAM.	Enumeración

Campo	Descripción	Valor
Path	Ruta del fichero padre que realizó la operación registrada.	Cadena de caracteres
ValidSig	El proceso padre está firmado digitalmente.	Booleano
Company	Contenido del atributo Company de los metadatos del proceso padre.	Cadena de caracteres
Broken	El proceso padre está corrupto o defectuoso.	Booleano
ImageType	Arquitectura interna del proceso padre: ▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	Enumeración
ExeType	Estructura interna / tipo del proceso padre. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
Prevalence	Prevalencia histórica del proceso padre en los sistemas de Cytomic EDR. ▪ High ▪ Medium ▪ Low	Enumeración
PrevLastDay	Prevalencia del proceso padre en el día anterior en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
Cat	Categoría del fichero padre que realizó la	Enumeración

Campo	Descripción	Valor
	operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	
MWName	Nombre del malware en el proceso padre si ya está catalogado como una amenaza. Si es Null el elemento no es malware.	Cadena de caracteres
TargetPath	Ruta del ejecutable apuntado en el registro.	Cadena de caracteres
Regkey	Clave de registro.	Cadena de caracteres
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres
TTPs	Lista de las técnicas, tácticas y subtécnicas asociadas al evento MITRE.	Cadena de caracteres
IOAIds	Cuando una secuencia de eventos sigue un patrón descrito en la matriz MITRE, el producto de seguridad crea un indicio (IOA) y añade su identificador a todos los eventos que lo forman.	Numérico
TelemetryType	▪ **0: telemetría normal**. El evento no pertenece a un indicio que siga un patrón descrito en la matriz MITRE. ▪ **1: evento reenviado**. El evento se envió inicialmente como tipo 0 (telemetría normal), pero tiempo después se ha detectado que pertenece a un patrón de ataque escrito en la matriz MITRE. El evento se vuelve a enviar con los campos TTPs e IOAIds completados. ▪ **2: evento acumulado**: para ahorrar recursos, parte de la telemetría generada en el cliente se retiene hasta que el software de seguridad detecta un patrón de ataque MITRE. En ese momento se envían todos los eventos acumulados.	Enumeración

Registrym

Evento de tipo activo que se genera cuando se detecta un proceso (parent) que modifica una rama del registro que apunta a un fichero ejecutable (child).

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
User (CEF)	Nombre de la cuenta de usuario y dominio al que pertenece utilizada para ejecutar el proceso que genero el evento registrado.	Cadena de caracteres
MachineIP (CEF)	Nombre del equipo que desencadena el evento registrado.	Dirección IP
MachineName (CEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
sev (LEEF)	Severidad del evento.	1
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
usrName (LEEF)	Cuenta de usuario utilizada por el proceso que realizó la operación registrada.	Cadena de caracteres
domain (LEEF)	Dominio de la cuenta de usuario utilizado por el proceso que realizó la operación registrada.	Cadena de caracteres
src (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identSrc (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identHostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres

Campo	Descripción	Valor
HostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
LocalDateTime	Fecha en formato UTC que tenía el equipo en el momento en que se produjo el evento registrado. Esta fecha depende de la configuración del equipo y por lo tanto puede ser errónea	Fecha
PandaTimeStatus	Contenido de los campos DateTime, Date y LocalDateTime	**0**: fecha real no soportada por tratarse de un evento antiguo. **1**: fecha real no disponible el servidor Cytomic y obtenida mediante un cálculo. **2**: fecha real proporcionada por el servidor Cytomic.
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
Op	Operación registrada.	Cadena de caracteres: “ModifyExeKey”
Hash	Hash del proceso que actúa como padre.	Cadena de caracteres
DriveType	Tipo de unidad donde reside el proceso o fichero padre que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM ▪ **Ramdisk**: unidad de disco RAM.	Enumeración

Campo	Descripción	Valor
Path	Ruta del fichero padre que realizó la operación registrada.	Cadena de caracteres
ValidSig	El proceso padre está firmado digitalmente.	Booleano
Company	Contenido del atributo Company de los metadatos del proceso padre.	Cadena de caracteres
Broken	El proceso padre está corrupto o defectuoso.	Booleano
ImageType	Arquitectura interna del proceso padre: ▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	Enumeración
ExeType	Estructura interna / tipo del proceso padre. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
Prevalence	Prevalencia histórica del proceso padre en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
PrevLastDay	Prevalencia del proceso padre en el día anterior en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
Cat	Categoría del fichero padre que realizó la	Enumeración

Campo	Descripción	Valor
	operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	
MWName	Nombre del malware en el proceso padre si ya está catalogado como una amenaza. Si es Null el elemento no es malware.	Cadena de caracteres
TargetPath	Ruta del ejecutable apuntado en el registro.	Cadena de caracteres
Regkey	Clave de registro.	Cadena de caracteres
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres
TTPs	Lista de las técnicas, tácticas y subtécnicas asociadas al evento MITRE.	Cadena de caracteres
IOAIds	Cuando una secuencia de eventos sigue un patrón descrito en la matriz MITRE, el producto de seguridad crea un indicio (IOA) y añade su identificador a todos los eventos que lo forman.	Numérico
TelemetryType	▪ **0: telemetría normal**. El evento no pertenece a un indicio que siga un patrón descrito en la matriz MITRE. ▪ **1: evento reenviado**. El evento se envió inicialmente como tipo 0 (telemetría normal), pero tiempo después se ha detectado que pertenece a un patrón de ataque escrito en la matriz MITRE. El evento se vuelve a enviar con los campos TTPs e IOAIds completados. ▪ **2: evento acumulado**: para ahorrar recursos, parte de la telemetría generada en el cliente se retiene hasta que el software de seguridad detecta un patrón de ataque MITRE. En ese momento se envían todos los eventos acumulados.	Enumeración

Renamepe

Evento de tipo activo que se genera cuando se detecta un proceso (parent) que cambia el nombre de un programa ejecutable (child).

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
User (CEF)	Nombre de la cuenta de usuario y dominio al que pertenece utilizada para ejecutar el proceso que genero el evento registrado.	Cadena de caracteres
MachineIP (CEF)	Nombre del equipo que desencadena el evento registrado.	Dirección IP
MachineName (CEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
sev (LEEF)	Severidad del evento.	1
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
usrName (LEEF)	Cuenta de usuario utilizada por el proceso que realizó la operación registrada.	Cadena de caracteres
domain (LEEF)	Dominio de la cuenta de usuario utilizado por el proceso que realizó la operación registrada.	Cadena de caracteres
src (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identSrc (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identHostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres

Campo	Descripción	Valor
HostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
LocalDateTime	Fecha en formato UTC que tenía el equipo en el momento en que se produjo el evento registrado. Esta fecha depende de la configuración del equipo y por lo tanto puede ser errónea	Fecha
PandaTimeStatus	Contenido de los campos DateTime, Date y LocalDateTime	**0**: fecha real no soportada por tratarse de un evento antiguo. **1**: fecha real no disponible el servidor Cytomic y obtenida mediante un cálculo. **2**: fecha real proporcionada por el servidor Cytomic.
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
Op	Operación registrada.	Cadena de caracteres: “Renamepe”
ParentHash	Hash del proceso que actúa como padre.	Cadena de caracteres
ParentDriveType	Tipo de unidad donde reside el proceso o fichero padre que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM	Enumeración

Campo	Descripción	Valor
	▪ **Ramdisk**: unidad de disco RAM.	
ParentPath	Ruta del fichero padre que realizó la operación registrada.	Cadena de caracteres
ParentPID	Identificador del proceso padre.	Numérico
ParentValidSig	El proceso padre está firmado digitalmente.	Booleano
ParentCompany	Contenido del atributo Company de los metadatos del proceso padre.	Cadena de caracteres
ParentBroken	El proceso padre está corrupto o defectuoso.	Booleano
ParentImageType	Arquitectura interna del proceso padre: ▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	Enumeración
ParentExeType	Estructura interna / tipo del proceso padre. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
ParentPrevalence	Prevalencia histórica del proceso padre en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ParentPrevLastDay	Prevalencia del proceso padre en el día anterior en los sistemas de Cytomic. ▪ High ▪ Medium	Enumeración

Campo	Descripción	Valor
	▪ Low	
ParentCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración
ParentMWName	Nombre del malware en el proceso padre si ya está catalogado como una amenaza. Si es Null el elemento no es malware.	Cadena de caracteres
ChildHash	Hash del proceso que actúa como hijo.	Cadena de caracteres
ChildDriveType	Tipo de unidad donde reside el proceso o fichero padre que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM ▪ **Ramdisk**: unidad de disco RAM.	Enumeración
ChildPath	Ruta del fichero hijo que realizó la operación registrada.	Cadena de caracteres (Ruta)
ChildPID	Identificador del proceso hijo.	Numérico
ChildValidSig	El proceso hijo está firmado digitalmente.	Booleano
ChildCompany	Contenido del atributo Company de los metadatos del proceso hijo.	Cadena de caracteres
ChildBroken	El proceso hijo está corrupto o defectuoso.	Booleano
ChildImageType	Arquitectura interna del proceso hijo:	Enumeración

Campo	Descripción	Valor
	▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	
ChildExeType	Estructura interna / tipo del proceso hijo. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
ChildPrevalence	Prevalencia histórica del proceso hijo en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ChildPrevLastDay	Prevalencia histórica del proceso hijo en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ChildCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración
ChildMWName	Nombre del malware en el proceso hijo si ya está catalogado como una amenaza. Si es	Cadena de caracteres

Campo	Descripción	Valor
	Null el elemento no es malware.	
OCS_Exec	Se ejecutó en el equipo software considerado como vulnerable.	Booleano
OCS_Name	Nombre del software vulnerable ejecutado.	Cadena de caracteres
OCS_Version	Versión del sistema operativo del equipo donde se ejecutó el software vulnerable.	Cadena de caracteres
Params	Parámetros de ejecución del proceso en la linea de comandos.	Cadena de caracteres
ToastResult	Respuesta del usuario ante el mensaje emergente mostrado por Cytomic EDR. ▪ **Ok**: el cliente acepta el mensaje. ▪ **Timeout**: el mensaje emergente desaparece por la no acción del usuario. ▪ **Angry**: el usuario rechaza el bloqueo desde el mensaje emergente. ▪ **Block** ▪ **Allow**	Enumeración
Action	Acción realizada por el agente Cytomic. ▪ **Allow** ▪ **Block** ▪ **BlockTimeout**: se mostró un mensaje emergente al usuario pero no contestó a tiempo. ▪ **AllowWL**: elemento permitido por encontrarse en la lista blanca del administrador. ▪ **Disinfect** ▪ **Delete** ▪ **Quarantine** ▪ **AllowByUser**: se mostró un mensaje emergente al usuario y contesto “permitir ejecución”. ▪ **Informed**: se mostró un mensaje emergente al usuario. ▪ **Unquarantine**: el fichero se sacó de la cuarentena.	Enumeración

Campo	Descripción	Valor
	▪ **Rename**: elemento renombrado por no poderse mover a cuarentena, borrar o desinfectar. ▪ **BlockURL**: se bloqueó el acceso a una URL. ▪ **KillProcess**: cierre de proceso. ▪ **BlockExploit**: intento de explotación de proceso vulnerable detenido. ▪ **ExploitAllowByUser**: el usuario no permitió el cierre del proceso explotado. ▪ **RebootNeeded**: se requiere un reinicio del equipo para bloquear el intento de explotación. ▪ **ExploitInformed**: se mostró un mensaje emergente al usuario informando de un intento de explotación de proceso vulnerable. ▪ **AllowSonGWInstaller**: el programa forma parte de un paquete de instalación clasificado como Goodware. ▪ **EmbebedInformed**: el elemento es un script en powershell que ejecuta comandos. ▪ **SuspedProcess**: el elemento intentó suspender alguno de los servicios del software de protección. ▪ **ModifyDiskResource**: el elemento intentó modificar un fichero protegido que pertenece al software de protección. ▪ **ModifyRegistry**: el elemento intentó modificar una clave de registro protegida que pertenece al software de protección. ▪ **RenameRegistry**: el elemento intentó renombrar una clave de registro protegida que pertenece al software de protección.	

Campo	Descripción	Valor
	▪ **ModifyMarkFile**: el elemento intentó renombrar un fichero protegido que pertenece al software de protección. ▪ **UncertainAction**: el elemento intentó una acción sin definir sobre un fichero que pertenece al software de protección. ▪ **AllowGWFilter**: se permite la ejecución del elemento por estar en la caché de goodware. ▪ **AllowSWAuthoriced**: se permite la ejecución del elemento por estar autorizado por el administrador (configuración Software Autorizado). ▪ **NewPE**: aparición de un nuevo programa ejecutable en el equipo que viene del exterior. ▪ **AllowedByAdmin**: se permite la ejecución del elemento porque el administrador excluyó la técnica de explotación detectada. ▪ **Blocked by ip**: se bloqueó la dirección IP de origen por detectarse un ataque de fuerza bruta mediante el protocolo RDP. ▪ **AllowSonMsiGW**: se permite la ejecución del elemento por tratarse de un ejecutable que proviene de un paquete de instalación confiable. ▪ **Allowed by Global Audit**: el elemento se permite porque el software de seguridad está configurado en modo Global Audit.	
ServiceLevel	Modo de ejecución del agente: ▪ **Blocking**: el agente bloquea todos los ejecutables sin clasificar y los clasificados como malware. ▪ **Hardening**: el agente bloquea la ejecución de todos los programas sin clasificar cuyo origen no sea confiable y los clasificados como malware.	Enumeración

Campo	Descripción	Valor
	▪ **Learning**: el agente no bloquea ningún programa pero monitoriza los procesos ejecutados.	
WinningTech	Tecnología que provocó el evento. ▪ **Blockmode**: el agente estaba en modo Lock en el momento del bloqueo. ▪ **Cache**: clasificación cacheada en local. ▪ **Cloud**: clasificación descargada de la nube. ▪ **Context**: regla de contexto local. ▪ **ContextMinerva**: regla de contexto en la nube. ▪ **Digital Signature**: fichero firmado digitalmente. ▪ **Exploit**: tecnología de identificación de intento de explotación de proceso vulnerable. ▪ **ExploitLegacy** ▪ **GWFilter**: tecnologías de identificación de ficheros GW desconocidos. ▪ **LegacyUser**: permiso solicitado al usuario. ▪ **Local Signature**: firma local. ▪ **MetaEsploit**: ataque generado con el framework metaExploit. ▪ **NetNative**: tipo de binario. ▪ **Serializer**: tipo de binario. ▪ **User**: permiso solicitado al usuario. ▪ **RDP**: ataque de fuerza bruta por el protocolo RDP. ▪ **AMSI**: detección encontrada mediante Antimalware Scan Interface.	Enumeración
DetId	Identificador de la detección.	Cadena de caracteres
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres

Campo	Descripción	Valor
TTPs	Lista de las técnicas, tácticas y subtécnicas asociadas al evento MITRE.	Cadena de caracteres
IOAIds	Cuando una secuencia de eventos sigue un patrón descrito en la matriz MITRE, el producto de seguridad crea un indicio (IOA) y añade su identificador a todos los eventos que lo forman.	Numérico
TelemetryType	▪ **0: telemetría normal**. El evento no pertenece a un indicio que siga un patrón descrito en la matriz MITRE. ▪ **1: evento reenviado**. El evento se envió inicialmente como tipo 0 (telemetría normal), pero tiempo después se ha detectado que pertenece a un patrón de ataque escrito en la matriz MITRE. El evento se vuelve a enviar con los campos TTPs e IOAIds completados. ▪ **2: evento acumulado**: para ahorrar recursos, parte de la telemetría generada en el cliente se retiene hasta que el software de seguridad detecta un patrón de ataque MITRE. En ese momento se envían todos los eventos acumulados.	Enumeración

Scriptcreation

Evento de tipo activo que se genera cuando un proceso (parent) crea un proceso (child) de tipo script.

Descripción de los campo del evento

Campo	Descripción	Valor
Date (CEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
User (CEF)	Nombre de la cuenta de usuario y dominio al que pertenece utilizada para ejecutar el proceso que genero el evento registrado.	Cadena de caracteres
MachineIP (CEF)	Nombre del equipo que desencadena el evento registrado.	Dirección IP
MachineName (CEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
sev (LEEF)	Severidad del evento.	1
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
usrName (LEEF)	Cuenta de usuario utilizada por el proceso que realizó la operación registrada.	Cadena de caracteres
domain (LEEF)	Dominio de la cuenta de usuario utilizado por el proceso que realizó la operación registrada.	Cadena de caracteres
src (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identSrc (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identHostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres

Campo	Descripción	Valor
HostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
LocalDateTime	Fecha en formato UTC que tenía el equipo en el momento en que se produjo el evento registrado. Esta fecha depende de la configuración del equipo y por lo tanto puede ser errónea	Fecha
PandaTimeStatus	Contenido de los campos DateTime, Date y LocalDateTime	**0**: fecha real no soportada por tratarse de un evento antiguo. **1**: fecha real no disponible el servidor Cytomic y obtenida mediante un cálculo. **2**: fecha real proporcionada por el servidor Cytomic.
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
Op	Operación registrada.	Cadena de caracteres: “scriptcreation”
ParentHash	Hash del proceso que actúa como padre.	Cadena de caracteres
ParentDriveType	Tipo de unidad donde reside el proceso o fichero padre que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM	Enumeración

Campo	Descripción	Valor
	▪ **Ramdisk**: unidad de disco RAM.	
ParentPath	Ruta del fichero padre que realizó la operación registrada.	Cadena de caracteres
ParentFlags	Flags de uso interno al servicio.	Cadena de caracteres
ParentValidSig	El proceso padre está firmado digitalmente.	Booleano
ParentCompany	Contenido del atributo Company de los metadatos del proceso padre.	Cadena de caracteres
ParentBroken	El proceso padre está corrupto o defectuoso.	Booelano
ParentImageType	Arquitectura interna del proceso padre: ▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	Enumeración
ParentExeType	Estructura interna / tipo del proceso padre. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
ParentPrevalence	Prevalencia histórica del proceso padre en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ParentPrevLastDay	Prevalencia del proceso padre en el día anterior en los sistemas de Cytomic. ▪ High ▪ Medium	Enumeración

Campo	Descripción	Valor
	▪ Low	
ParentCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración
ParentMWName	Nombre del malware en el proceso padre si ya está catalogado como una amenaza. Si es Null el elemento no es malware.	Cadena de caracteres
ChildHash	Hash del proceso que actúa como hijo.	Cadena de caracteres
ChildDriveType	Tipo de unidad donde reside el proceso o fichero padre que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM ▪ **Ramdisk**: unidad de disco RAM.	Enumeración
ChildPath	Ruta del fichero hijo que realizó la operación registrada.	Cadena de caracteres
ChildFlags	Flags de uso interno al servicio.	Cadena de caracteres
ChildValidSig	El proceso hijo está firmado digitalmente.	Booleano
ChildCompany	Contenido del atributo Company de los metadatos del proceso hijo.	Cadena de caracteres
ChildBroken	El proceso hijo está corrupto o defectuoso.	Booleano
ChildImageType	Arquitectura interna del proceso hijo:	Enumeración

Campo	Descripción	Valor
	▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	
ChildExeType	Estructura interna / tipo del proceso padre. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
ChildPrevalence	Prevalencia histórica del proceso hijo en los sistemas de Cytomic ▪ High ▪ Medium ▪ Low	Enumeración
ChildPrevLastDay	Prevalencia histórica del proceso hijo en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ChildCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración
ChildMWName	Nombre del malware en el proceso hijo si ya está catalogado como una amenaza. Si es	Cadena de caracteres

Campo	Descripción	Valor
	Null el elemento no es malware.	
ServiceLevel	Modo de ejecución del agente: ▪ **Blocking**: el agente bloquea todos los ejecutables sin clasificar y los clasificados como malware. ▪ **Hardening**: el agente bloquea la ejecución de todos los programas sin clasificar cuyo origen no sea confiable y los clasificados como malware. ▪ **Learning**: el agente no bloquea ningún programa pero monitoriza los procesos ejecutados.	Enumeración
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres
TTPs	Lista de las técnicas, tácticas y subtécnicas asociadas al evento MITRE.	Cadena de caracteres
IOAIds	Cuando una secuencia de eventos sigue un patrón descrito en la matriz MITRE, el producto de seguridad crea un indicio (IOA) y añade su identificador a todos los eventos que lo forman.	Numérico
TelemetryType	▪ **0: telemetría normal**. El evento no pertenece a un indicio que siga un patrón descrito en la matriz MITRE. ▪ **1: evento reenviado**. El evento se envió inicialmente como tipo 0 (telemetría normal), pero tiempo después se ha detectado que pertenece a un patrón de ataque escrito en la matriz MITRE. El evento se vuelve a enviar con los campos TTPs e IOAIds completados. ▪ **2: evento acumulado**: para ahorrar recursos, parte de la telemetría generada en el cliente se retiene hasta que el software de seguridad detecta un patrón de ataque MITRE. En ese momento se envían todos los eventos acumulados.	Enumeración

Scriptlaunch

Evento de tipo activo que se genera cuando se un proceso (parent) ejecuta un proceso (child) de tipo script.

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
User (CEF)	Nombre de la cuenta de usuario y dominio al que pertenece utilizada para ejecutar el proceso que genero el evento registrado.	Cadena de caracteres
MachineIP (CEF)	Nombre del equipo que desencadena el evento registrado.	Dirección IP
MachineName (CEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
sev (LEEF)	Severidad del evento.	1
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
usrName (LEEF)	Cuenta de usuario utilizada por el proceso que realizó la operación registrada.	Cadena de caracteres
domain (LEEF)	Dominio de la cuenta de usuario utilizado por el proceso que realizó la operación registrada.	Cadena de caracteres
src (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identSrc (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identHostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres

Campo	Descripción	Valor
HostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
LocalDateTime	Fecha en formato UTC que tenía el equipo en el momento en que se produjo el evento registrado. Esta fecha depende de la configuración del equipo y por lo tanto puede ser errónea	Fecha
PandaTimeStatus	Contenido de los campos DateTime, Date y LocalDateTime	**0**: fecha real no soportada por tratarse de un evento antiguo. **1**: fecha real no disponible el servidor Cytomic y obtenida mediante un cálculo. **2**: fecha real proporcionada por el servidor Cytomic.
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
Op	Operación registrada.	Cadena de caracteres: “scriptlauch”
ParentHash	Hash del proceso que actúa como padre.	Cadena de caracteres
ParentDriveType	Tipo de unidad donde reside el proceso o fichero padre que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM.	Enumeración

Campo	Descripción	Valor
	▪ **Ramdisk**: unidad de disco RAM.	
ParentPath	Ruta del fichero padre que realizó la operación registrada.	Cadena de caracteres
ParentFlags	Flags de uso interno al servicio.	Cadena de caracteres
ParentValidSig	El proceso padre está firmado digitalmente.	Booleano
ParentCompany	Contenido del atributo Company de los metadatos del proceso padre.	Cadena de caracteres
ParentBroken	El proceso padre está corrupto o defectuoso.	Booleano
ParentImageType	Arquitectura interna del proceso padre: ▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	Enumeración
ParentExeType	Estructura interna / tipo del proceso padre. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
ParentPrevalence	Prevalencia histórica del proceso padre en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ParentPrevLastDay	Prevalencia del proceso padre en el día anterior en los sistemas de Cytomic. ▪ High ▪ Medium	Enumeración

Campo	Descripción	Valor
	▪ Low	
ParentCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración
ParentMWName	Nombre del malware en el proceso padre si ya está catalogado como una amenaza. Si es Null el elemento no es malware.	Cadena de caracteres
ChildHash	Hash del proceso que actúa como hijo.	Cadena de caracteres
ChildDriveType	Tipo de unidad donde reside el proceso o fichero padre que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM ▪ **Ramdisk**: unidad de disco RAM.	Enumeración
ChildPath	Ruta del fichero hijo que realizó la operación registrada.	Cadena de caracteres
ChildFlags	Flags de uso interno al servicio.	Cadena de caracteres
ChildValidSig	El proceso hijo está firmado digitalmente.	Booleano
ChildCompany	Contenido del atributo Company de los metadatos del proceso hijo.	Cadena de caracteres
ChildBroken	El proceso hijo está corrupto o defectuoso.	Booleano
ChildImageType	Arquitectura interna del proceso hijo:	Enumeración

Campo	Descripción	Valor
	▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	
ChildExeType	Estructura interna / tipo del proceso padre. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
ChildPrevalence	Prevalencia histórica del proceso hijo en los sistemas de Cytomic (Business Unit of Panda Security, S.L.). ▪ High ▪ Medium ▪ Low	Enumeración
ChildPrevLastDay	Prevalencia histórica del proceso hijo en los sistemas de Cytomic (Business Unit of Panda Security, S.L.). ▪ High ▪ Medium ▪ Low	Enumeración
ChildCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración

Campo	Descripción	Valor
ChildMWName	Nombre del malware en el proceso hijo si ya está catalogado como una amenaza. Si es Null el elemento no es malware.	Cadena de caracteres
ServiceLevel	Modo de ejecución del agente: ▪ **Blocking**: el agente bloquea todos los ejecutables sin clasificar y los clasificados como malware. ▪ **Hardening**: el agente bloquea la ejecución de todos los programas sin clasificar cuyo origen no sea confiable y los clasificados como malware. ▪ **Learning**: el agente no bloquea ningún programa pero monitoriza los procesos ejecutados.	Enumeración
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres
TTPs	Lista de las técnicas, tácticas y subtécnicas asociadas al evento MITRE.	Cadena de caracteres
IOAIds	Cuando una secuencia de eventos sigue un patrón descrito en la matriz MITRE, el producto de seguridad crea un indicio (IOA) y añade su identificador a todos los eventos que lo forman.	Numérico
TelemetryType	▪ **0: telemetría normal**. El evento no pertenece a un indicio que siga un patrón descrito en la matriz MITRE. ▪ **1: evento reenviado**. El evento se envió inicialmente como tipo 0 (telemetría normal), pero tiempo después se ha detectado que pertenece a un patrón de ataque escrito en la matriz MITRE. El evento se vuelve a enviar con los campos TTPs e IOAIds completados. ▪ **2: evento acumulado**: para ahorrar recursos, parte de la telemetría generada en el cliente se retiene hasta que el software de seguridad detecta un patrón de ataque MITRE. En ese momento se envían todos los eventos acumulados.	Enumeración

Socket

Evento de tipo activo que se genera cuando se detecta un proceso (parent) que abre un socket.

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
User (CEF)	Nombre de la cuenta de usuario y dominio al que pertenece utilizada para ejecutar el proceso que genero el evento registrado.	Cadena de caracteres
MachineIP (CEF)	Nombre del equipo que desencadena el evento registrado.	Dirección IP
MachineName (CEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
sev (LEEF)	Severidad del evento.	1
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
usrName (LEEF)	Cuenta de usuario utilizada por el proceso que realizó la operación registrada.	Cadena de caracteres
domain (LEEF)	Dominio de la cuenta de usuario utilizado por el proceso que realizó la operación registrada.	Cadena de caracteres
src (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identSrc (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identHostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres

Campo	Descripción	Valor
HostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
LocalDateTime	Fecha en formato UTC que tenía el equipo en el momento en que se produjo el evento registrado. Esta fecha depende de la configuración del equipo y por lo tanto puede ser errónea	Fecha
PandaTimeStatus	Contenido de los campos DateTime, Date y LocalDateTime	**0**: fecha real no soportada por tratarse de un evento antiguo. **1**: fecha real no disponible el servidor Cytomic y obtenida mediante un cálculo. **2**: fecha real proporcionada por el servidor Cytomic.
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
Protocol	Protocolo de comunicaciones utilizado por el proceso. ▪ TCP ▪ UDP ▪ RDP	Enumeración
Localport	Puerto local del proceso.	Numérico
Direction	Sentido de la conexión de red. ▪ Up ▪ Down ▪ Both	Enumeración
LocalIP	Dirección IP local del proceso.	Dirección IP
Hash	Hash / digest del fichero.	Cadena de caracteres
DriveType	Tipo de unidad donde reside el proceso o fichero que desencadenó la operación registrada.	Enumeración

Campo	Descripción	Valor
	▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM ▪ **Ramdisk**: unidad de disco RAM.	
Path	Ruta del elemento que desencadenó la operación registrada.	Cadena de caracteres
Hostname	Nombre del equipo remoto que inició la conexión.	Cadena de caracteres
IP	Dirección IP de la comunicación.	Dirección IP
Port	Puerto de comunicaciones utilizado por el proceso.	Numérico
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. 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	Numérico

Campo	Descripción	Valor
	registrado.	
Pid	Identificador del proceso.	Numérico
ValidSig	El proceso padre está firmado digitalmente.	Booleano
Company	Contenido del atributo Company de los metadatos del proceso padre.	Cadena de caracteres
Broken	El proceso padre está corrupto o defectuoso.	Cadena de caracteres
ImageType	Arquitectura interna del proceso. ▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	Enumeración
ExeType	Estructura interna / tipo del proceso padre. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
Prevalence	Prevalencia histórica del proceso en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
PrevLastDay	Prevalencia del proceso en el día anterior en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración

Campo	Descripción	Valor
Cat	Categoría del fichero que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración
MWName	Nombre del malware si está ya catalogado como una amenaza.	Cadena de caracteres
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres
TTPs	Lista de las técnicas, tácticas y subtécnicas asociadas al evento MITRE.	Cadena de caracteres
IOAIds	Cuando una secuencia de eventos sigue un patrón descrito en la matriz MITRE, el producto de seguridad crea un indicio (IOA) y añade su identificador a todos los eventos que lo forman.	Numérico
TelemetryType	▪ **0: telemetría normal**. El evento no pertenece a un indicio que siga un patrón descrito en la matriz MITRE. ▪ **1: evento reenviado**. El evento se envió inicialmente como tipo 0 (telemetría normal), pero tiempo después se ha detectado que pertenece a un patrón de ataque escrito en la matriz MITRE. El evento se vuelve a enviar con los campos TTPs e IOAIds completados. ▪ **2: evento acumulado**: para ahorrar recursos, parte de la telemetría generada en el cliente se retiene hasta que el software de seguridad detecta un patrón de ataque MITRE. En ese momento se envían todos los eventos acumulados.	Enumeración

SvcControl

Evento correspondiente a un intento de modificación de los ficheros del producto de seguridad instalado.

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
User (CEF)	Nombre de la cuenta de usuario y dominio al que pertenece utilizada para ejecutar el proceso que genero el evento registrado.	Cadena de caracteres
MachineIP (CEF)	Nombre del equipo que desencadena el evento registrado.	Dirección IP
MachineName (CEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
sev (LEEF)	Severidad del evento.	1
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
usrName (LEEF)	Cuenta de usuario utilizada por el proceso que realizó la operación registrada.	Cadena de caracteres
domain (LEEF)	Dominio de la cuenta de usuario utilizado por el proceso que realizó la operación registrada.	Cadena de caracteres
src (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identSrc (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identHostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres

Campo	Descripción	Valor
HostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
LocalDateTime	Fecha en formato UTC que tenía el equipo en el momento en que se produjo el evento registrado. Esta fecha depende de la configuración del equipo y por lo tanto puede ser errónea	Fecha
PandaTimeStatus	Contenido de los campos DateTime, Date y LocalDateTime	**0**: fecha real no soportada por tratarse de un evento antiguo. **1**: fecha real no disponible el servidor Cytomic y obtenida mediante un cálculo. **2**: fecha real proporcionada por el servidor Cytomic.
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
HostName	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
Op	Operación registrada.	Cadena de caracteres: “Loadlib”
ParentHash	Hash del proceso que actúa como padre.	Cadena de caracteres
ParentDriveType	Tipo de unidad donde reside el proceso o fichero padre que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido.	Enumeración

Campo	Descripción	Valor
	▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM ▪ **Ramdisk**: unidad de disco RAM.	
ParentPath	Ruta del fichero padre que realizó la operación registrada.	Cadena de caracteres
ParentPID	Identificador del proceso padre.	Numérico
ParentValidSig	El proceso padre está firmado digitalmente.	Booleano
ParentCompany	Contenido del atributo Company de los metadatos del proceso padre.	Cadena de caracteres
ParentBroken	El proceso padre está corrupto o defectuoso.	Booleano
ParentImageType	Arquitectura interna del proceso padre: ▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	Enumeración
ParentExeType	Estructura interna / tipo del proceso padre. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
ParentPrevalence	Prevalencia histórica del proceso padre en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ParentPrevLastDay	Prevalencia del proceso padre en el día	Enumeración

Campo	Descripción	Valor
	anterior en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	
ParentCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración
ParentMWName	Nombre del malware en el proceso padre si ya está catalogado como una amenaza. Si es Null el elemento no es malware.	Cadena de caracteres
ChildHash	Hash del proceso que actúa como hijo.	Cadena de caracteres
ChildDriveType	Tipo de unidad donde reside el proceso o fichero padre que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM ▪ **Ramdisk**: unidad de disco RAM.	Enumeración
ChildPath	Ruta del fichero hijo que realizó la operación registrada.	Cadena de caracteres (Ruta)
ChildPID	Identificador del proceso hijo.	Numérico
ChildValidSig	El proceso hijo está firmado digitalmente.	Booleano
ChildCompany	Contenido del atributo Company de los metadatos del proceso hijo.	Cadena de caracteres

Campo	Descripción	Valor
ChildBroken	El proceso hijo está corrupto o defectuoso.	Booleano
ChildImageType	Arquitectura interna del proceso hijo: ▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	Enumeración
ChildExeType	Estructura interna / tipo del proceso hijo. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
ChildPrevalence	Prevalencia histórica del proceso hijo en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ChildPrevLastDay	Prevalencia histórica del proceso hijo en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ChildCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown	Enumeración

Campo	Descripción	Valor
	▪ Monitoring	
ChildMWName	Nombre del malware en el proceso hijo si ya está catalogado como una amenaza. Si es Null el elemento no es malware.	Cadena de caracteres
OCS_Exec	Se ejecutó en el equipo software considerado como vulnerable.	Booleano
OCS_Name	Nombre del software vulnerable ejecutado.	Cadena de caracteres
OCS_Version	Versión del sistema operativo del equipo donde se ejecutó el software vulnerable.	Cadena de caracteres
Params	Parámetros de ejecución del proceso en la linea de comandos.	Cadena de caracteres
ToastResult	Respuesta del usuario ante el mensaje emergente mostrado por Cytomic EDR. ▪ **Ok**: el cliente acepta el mensaje. ▪ **Timeout**: el mensaje emergente desaparece por la no acción del usuario. ▪ **Angry**: el usuario rechaza el bloqueo desde el mensaje emergente. ▪ **Block** ▪ **Allow**	Enumeración
Action	Acción realizada por el agente Cytomic. ▪ **Allow** ▪ **Block** ▪ **BlockTimeout**: se mostró un mensaje emergente al usuario pero no contestó a tiempo. ▪ **AllowWL**: elemento permitido por encontrarse en la lista blanca del administrador. ▪ **Disinfect** ▪ **Delete** ▪ **Quarantine** ▪ **AllowByUser**: se mostró un mensaje emergente al usuario y contesto “permitir ejecución”.	Enumeración

Campo	Descripción	Valor
	▪ **Informed**: se mostró un mensaje emergente al usuario. ▪ **Unquarantine**: el fichero se sacó de la cuarentena. ▪ **Rename**: elemento renombrado por no poderse mover a cuarentena, borrar o desinfectar. ▪ **BlockURL**: se bloqueó el acceso a una URL. ▪ **KillProcess**: cierre de proceso. ▪ **BlockExploit**: intento de explotación de proceso vulnerable detenido. ▪ **ExploitAllowByUser**: el usuario no permitió el cierre del proceso explotado. ▪ **RebootNeeded**: se requiere un reinicio del equipo para bloquear el intento de explotación. ▪ **ExploitInformed**: se mostró un mensaje emergente al usuario informando de un intento de explotación de proceso vulnerable. ▪ **AllowSonGWInstaller**: el programa forma parte de un paquete de instalación clasificado como Goodware. ▪ **EmbebedInformed**: el elemento es un script en powershell que ejecuta comandos. ▪ **SuspedProcess**: el elemento intentó suspender alguno de los servicios del software de protección. ▪ **ModifyDiskResource**: el elemento intentó modificar un fichero protegido que pertenece al software de protección. ▪ **ModifyRegistry**: el elemento intentó modificar una clave de registro protegida que pertenece al software de protección.	

Campo	Descripción	Valor
	▪ **RenameRegistry**: el elemento intentó renombrar una clave de registro protegida que pertenece al software de protección. ▪ **ModifyMarkFile**: el elemento intentó renombrar un fichero protegido que pertenece al software de protección. ▪ **UncertainAction**: el elemento intentó una acción sin definir sobre un fichero que pertenece al software de protección. ▪ **AllowGWFilter**: se permite la ejecución del elemento por estar en la caché de goodware. ▪ **AllowSWAuthoriced**: se permite la ejecución del elemento por estar autorizado por el administrador (configuración Software Autorizado). ▪ **NewPE**: aparición de un nuevo programa ejecutable en el equipo que viene del exterior. ▪ **AllowedByAdmin**: se permite la ejecución del elemento porque el administrador excluyó la técnica de explotación detectada. ▪ **Blocked by ip**: se bloqueó la dirección IP de origen por detectarse un ataque de fuerza bruta mediante el protocolo RDP. ▪ **AllowSonMsiGW**: se permite la ejecución del elemento por tratarse de un ejecutable que proviene de un paquete de instalación confiable. ▪ **Allowed by Global Audit**: el elemento se permite porque el software de seguridad está configurado en modo Global Audit.	
ServiceLevel	Modo de ejecución del agente: ▪ **Blocking**: el agente bloquea todos los ejecutables sin clasificar y los clasificados como malware.	Enumeración

Campo	Descripción	Valor
	▪ **Hardening**: el agente bloquea la ejecución de todos los programas sin clasificar cuyo origen no sea confiable y los clasificados como malware. ▪ **Learning**: el agente no bloquea ningún programa pero monitoriza los procesos ejecutados.	
WinningTech	Tecnología que provocó el evento. ▪ **Blockmode**: el agente estaba en modo Lock en el momento del bloqueo. ▪ **Cache**: clasificación cacheada en local. ▪ **Cloud**: clasificación descargada de la nube. ▪ **Context**: regla de contexto local. ▪ **ContextMinerva**: regla de contexto en la nube. ▪ **Digital Signature**: fichero firmado digitalmente. ▪ **Exploit**: tecnología de identificación de intento de explotación de proceso vulnerable. ▪ **ExploitLegacy** ▪ **GWFilter**: tecnologías de identificación de ficheros GW desconocidos. ▪ **LegacyUser**: permiso solicitado al usuario. ▪ **Local Signature**: firma local. ▪ **MetaEsploit**: ataque generado con el framework metaExploit. ▪ **NetNative**: tipo de binario. ▪ **Serializer**: tipo de binario. ▪ **User**: permiso solicitado al usuario. ▪ **RDP**: ataque de fuerza bruta por el protocolo RDP. ▪ **AMSI**: detección encontrada mediante Antimalware Scan Interface.	Enumeración
DetId	Identificador de la detección.	Cadena de caracteres
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres

Systemops

Evento de tipo activo que se genera cuando se detecta la ejecución de acciones que afectan o modifican procesos y ficheros del sistema operativo a través del sistema WMI (Windows Management Interface).

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
User (CEF)	Nombre de la cuenta de usuario y dominio al que pertenece utilizada para ejecutar el proceso que genero el evento registrado.	Cadena de caracteres
MachineIP (CEF)	Nombre del equipo que desencadena el evento registrado.	Dirección IP
MachineName (CEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
sev (LEEF)	Severidad del evento.	1
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
usrName (LEEF)	Cuenta de usuario utilizada por el proceso que realizó la operación registrada.	Cadena de caracteres
domain (LEEF)	Dominio de la cuenta de usuario utilizado por el proceso que realizó la operación registrada.	Cadena de caracteres
src (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identSrc (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identHostName	Nombre del equipo que desencadena el	Cadena de

Campo	Descripción	Valor
(LEEF)	evento registrado.	caracteres
HostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
LocalDateTime	Fecha en formato UTC que tenía el equipo en el momento en que se produjo el evento registrado. Esta fecha depende de la configuración del equipo y por lo tanto puede ser errónea	Fecha
PandaTimeStatus	Contenido de los campos DateTime, Date y LocalDateTime	**0**: fecha real no soportada por tratarse de un evento antiguo. **1**: fecha real no disponible el servidor Cytomic y obtenida mediante un cálculo. **2**: fecha real proporcionada por el servidor Cytomic.
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
HostName	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
Type	Tipo de operación realizada por el proceso: ▪ **0 (WMI_COMMAND_LINE_EVENT_CREATION)**: evento que se genera cada vez que se crea un "CommandLineEventConsumer", que es una línea de comandos que va a lanzar WMI al producirse un evento en la base de datos. ▪ **1 (WMI_ACTIVE_SCRIPT_EVENT_CREATION)**: se ha creado una consulta que lanzará un script.	Enumeración

Campo	Descripción	Valor
	▪ **2 (CREATE_WMI_EVENT_ CONSUMER_TO_FILTER_ CONSUMER)**: se va a ejecutar una consulta registrada para lanzar en el equipo un proceso, un fichero JS/VBS o un script de JS/VBS embebido dentro de la propia BBDD (sin fichero en disco). ▪ **3 (CREATE_WMI_EVENT_ CONSUMER_TO_FILTER_QUERY)**: se ha registrado un filtro que es una consulta. ▪ **4 (WMI_EVENT_CREATE_USER)**: se ha creado una cuenta de usuario. ▪ **5 (WMI_EVENT_DELETE_USER)**: se ha borrado una cuenta de usuario. ▪ **6 (WMI_EVENT_ADD_USER_ GROUP)**: se ha añadido una cuenta a un grupo de usuarios. ▪ **7 (WMI_EVENT_DELETE_USER_ GROUP)**: se ha borrado una cuenta de un grupo de usuarios. ▪ **8 (WMI_EVENT_USER_GROUP_ ADMIN)**: se ha añadido un usuario a un grupo de usuarios administradores. ▪ **9 (WMI_EVENT_USER_GROUP_ RDP)**: se ha añadido un usuario a un grupo de usuarios con acceso al equipo por RDP. ▪ **10 (WMI_EVENT_CREATE_ SERVICE)**: se instaló un nuevo servicio en el sistema. ▪ **11 (WMI_EVENT_USER_ACCOUNT_ CHANGED**: se modificó una cuenta de usuario. ▪ **12 (WMI_EVENT_USER_ PASSWORD_RESET_ATTEMPT)**: se intentó borrar la contraseña de una cuenta de usuario. ▪ **13 WMI_QUERY**: consulta realizada en el equipo al sistema WMI. El campo **CommandLine** contiene la consulta.	

Campo	Descripción	Valor
	▪ **14 WMI_LOGIN_ATTEMP**: el equipo intentó iniciar una sesión en otro equipo. ▪ **15 WMI_SCHEDULER_TASKS**: el equipo realizó una operación con el programador de tareas. ▪ **16 WMI_LOGIN_SPECIAL_ PRIVILEGES**: un proceso escaló privilegios. ▪ **17 NOTIFICATION_ID_ INTERCEPTION_AMSI_BUFFER_ SCAN_REQUEST**: intento de ejecución de un script. Se logea el comando que provocó la ejecución del script y si se ha detectado malware o no.	
ObjectName	Nombre único del objeto dentro de la jerarquía WMI.	Cadena de caracteres
CommandLine	Línea de comandos configurada como tarea para ser ejecutada a través de WMI.	Cadena de caracteres
MachineName	Nombre del equipo que ejecutó el proceso.	Cadena de caracteres
User	Usuario con el que se lanza.	Cadena de caracteres
IsLocal	Indica si la tarea se crea local o remotamente.	Booleano
ExtendedInfo	Información extendida. Depende de la operación.	Cadena de caracteres
ChildMD5	Hash del fichero cuando proceda.	Cadena de caracteres
ParentPid	PID del proceso padre.	Numérico
RemoteMachineName	Nombre del equipo remoto que genera el evento.	Cadena de caracteres
RemoteIP	IP remota que genera el evento.	Cadena de caracteres
SessionInteractive	Indica si la sesión es interactiva o no.	Booleano

Campo	Descripción	Valor
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres
TTPs	Lista de las técnicas, tácticas y subtécnicas asociadas al evento MITRE.	Cadena de caracteres
IOAIds	Cuando una secuencia de eventos sigue un patrón descrito en la matriz MITRE, el producto de seguridad crea un indicio (IOA) y añade su identificador a todos los eventos que lo forman.	Numérico
TelemetryType	▪ **0: telemetría normal**. El evento no pertenece a un indicio que siga un patrón descrito en la matriz MITRE. ▪ **1: evento reenviado**. El evento se envió inicialmente como tipo 0 (telemetría normal), pero tiempo después se ha detectado que pertenece a un patrón de ataque escrito en la matriz MITRE. El evento se vuelve a enviar con los campos TTPs e IOAIds completados. ▪ **2: evento acumulado**: para ahorrar recursos, parte de la telemetría generada en el cliente se retiene hasta que el software de seguridad detecta un patrón de ataque MITRE. En ese momento se envían todos los eventos acumulados.	Enumeración

Thalert

Evento de tipo pasivo. Describe los indicios generados por las siguientes tecnologías de detección:

- **HRs (Hunting Rules)**: implementadas en Orion y utilizadas por el Radar de ciber-ataques para generar indicios de ataque o infección.
- **IOCs (Indicartor Of Compromise)**: implementadas en Orion. Son reglas creadas por el cliente que buscan indicios de equipos comprometidos en la red administrada.
- **IOAs (Indicator of Attack)**: implementadas en Cytomic EDR y vinculadas a MITRE, son reglas que buscan indicios de ataque recibidos en la red administrada.

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
MachineIP (CEF)	IP del equipo de usuario que desencadena el evento registrado.	Dirección IP
MachineName (CEF)	Nombre del equipo de usuario que desencadena el evento registrado.	Cadena de caracteres
sev (LEEF)	Severidad del evento. Consulta *Cálculo del campo Severity / Sev*.	Numérico
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
usrName (LEEF)	Cuenta de usuario utilizada por el proceso que realizó la operación registrada.	Cadena de caracteres
domain (LEEF)	Dominio de la cuenta de usuario utilizado por el proceso que realizó la operación registrada.	Cadena de caracteres
src (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identSrc (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres

Campo	Descripción	Valor
identHostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
AlertDate	Fecha en la que se registró la alerta en la plataforma asociada.	Fecha
THRuleName	Nombre de la regla de Hunting que generó el indicio.	Cadena de caracteres
Mitre	Técnica y Táctica Mitre asociada a la regla de Hunting que generó el indicio.	Lista de pares Técnica/ Táctica
Severity	Gravedad del indicio. Cuanto menor es el número, el indicio es más grave.	Numérico
TimeStamp	Marca de tiempo de la acción registrada en el equipo del cliente que generó el indicio.	Fecha
EvidenceData	Datos relevantes relacionados con el indicio y dependientes de la regla de hunting activada. Contiene varios campos separados por espacios con el formato “NombreCampo: valor”.	Cadena de caracteres
LastHourEvidenceCount	Nº de veces que ha ocurrido el mismo indicio en el equipo del cliente en la última hora.	Numérico
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres
Times	Número de repeticiones de la alerta. Consulta *Agrupación de alertas*.	Numérico

Cálculo del campo Severity / Sev

Dependiendo del valor del campo ExecutionStatus - Action, el valor de Severity / Sev varía según la tabla mostrada a continuación:

ExecutionStatus - Action	Severity
■ Allow ■ AllowWL ■ AllowByUser ■ Informed ■ Unquarantine ■ Rename ■ BlockURL ■ BlockExploit ■ RebootNeeded ■ AllowSonGwInstaller ■ InformNewPE ■ SonMSIGW ■ RDPOff	8
■ Block ■ BlockBL ■ BlockTimeout ■ Delete ■ Disinfect ■ Quarantine ■ KillProcess ■ EmbebedBlocked ■ SuspendProcess ■ BlockedIp ■ RenameRegistry ■ AllowSWAutoriced	7
■ ExploitAllowByUser ■ ExploitInformed ■ EmbebedInformed ■ ModifyMarkFile ■ UncertainAction	10

ExecutionStatus - Action	Severity
▪ ResponseLast ▪ IsolateHost	
▪ ModifyRegistry ▪ AllowFGW	6
▪ ExploitAllowByAdmin	5

Agrupación de alertas

Para minimizar el consumo de ancho de banda y evitar la saturación de la infraestructura IT que gestiona y almacena los eventos en el cliente, SIEMConnect implementa un algoritmo para agrupar alertas de características similares.

Se considera que dos o más alertas son iguales si cumplen todas las condiciones siguientes:

- Son de un mismo tipo.
- Se han registrado en un intervalo de tiempo próximo.
- Se han registrado en el mismo equipo de usuario o servidor.

Agrupación de IOAs avanzados de Cytomic EDR

Los IOAs avanzados no se agrupan si el equipo se encuentra en modo auditoría. Cada IOA recibido en este modo lleva el campo Times a 1. Para obtener más información consulta la guía de tu producto de seguridad Cytomic EDR.

- El primer IOA registrado genera una alerta THAlert con el campo Times a 1.
- Se agrupan todos los IOAs repetidos en intervalos de 6 horas. Se envía una alerta THAlert al final de cada intervalo y se indica en el campo Times el acumulado de IOAs registrados hasta el momento.
- Si no se registran IOAs iguales en un intervalo de 6 horas no se envía la alerta THAlert para ese intervalo.
- Pasados 4 intervalos (24 horas) se vuelve a iniciar el proceso.

Agrupación de IOAs de Cytomic EDR

- El primer IOA registrado genera una alerta THAlert con el campo Times a 1.
- Se agrupan todos los IOAs repetidos en intervalos de 1 hora. Se envía una alerta THAlert al final de cada intervalo y se indica en el campo Times el acumulado de IOAs registrados hasta el momento.

- Si no se registran IOAs iguales en un intervalo de 1 hora no se envía la alerta THAlert para ese intervalo.
- Pasados 24 horas se vuelve a iniciar el proceso.

Agrupación de IOCs en búsquedas retrospectivas de Orion

Los IOCs se cargan en la plataforma a través de la API de Orion. Para obtener más información consulta el manual del producto.

Esta búsqueda examina una única vez el flujo de eventos generado por los equipos del cliente y acumulado durante el último año desde el momento de la importación y genera una única alerta por cada equipo / IOC encontrado.

Agrupación de IOCs en búsquedas en streaming de Orion

Los IOCs se cargan en la plataforma a través de la API de Orion. Para obtener más información consulta el manual del producto.

Esta búsqueda examina en tiempo real la información generada por los procesos en ejecución de los equipos del cliente y genera una alerta por cada equipo / IOC / hora.

Agrupación de Indicios de Orion

- El primer Indicio registrado genera una alerta THAlert con el campo Times a 1.
- Se agrupan todos los Indicios repetidos en intervalos de 1 hora. Se envía una alerta THAlert al final de cada intervalo y se indica en el campo Times el acumulado de Indicios registrados hasta el momento.
- Si no se registran Indicios iguales en un intervalo de 1 hora no se envía la alerta THAlert para ese intervalo.
- Pasados 24 horas se vuelve a iniciar el proceso.

Urldownload

Evento de tipo activo que se genera cuando un proceso realiza una petición / descarga de un fichero de datos por HTTP.

Descripción de los campos del evento

Campo	Descripción	Valor
Date (CEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
User (CEF)	Nombre de la cuenta de usuario y dominio al que pertenece utilizada para ejecutar el proceso que genero el evento registrado.	Cadena de caracteres
MachineIP (CEF)	Nombre del equipo que desencadena el evento registrado.	Dirección IP
MachineName (CEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
sev (LEEF)	Severidad del evento.	1
devTime (LEEF)	TimeStamp de la creación del evento en el equipo del usuario.	Fecha
devTimeFormat (LEEF)	Formato del timestamp enviado.	Cadena de caracteres “yyyy-MM-dd”
usrName (LEEF)	Cuenta de usuario utilizada por el proceso que realizó la operación registrada.	Cadena de caracteres
domain (LEEF)	Dominio de la cuenta de usuario utilizado por el proceso que realizó la operación registrada.	Cadena de caracteres
src (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identSrc (LEEF)	IP del equipo donde se registró el evento.	Cadena de caracteres
identHostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres

Campo	Descripción	Valor
HostName (LEEF)	Nombre del equipo que desencadena el evento registrado.	Cadena de caracteres
LocalDateTime	Fecha en formato UTC que tenía el equipo en el momento en que se produjo el evento registrado. Esta fecha depende de la configuración del equipo y por lo tanto puede ser errónea	Fecha
PandaTimeStatus	Contenido de los campos DateTime, Date y LocalDateTime	**0**: fecha real no soportada por tratarse de un evento antiguo. **1**: fecha real no disponible el servidor Cytomic y obtenida mediante un cálculo. **2**: fecha real proporcionada por el servidor Cytomic.
Client	Identificador utilizado para distinguir los eventos recibidos de cada cliente del partner. Este campo únicamente se utiliza en el producto Cytomic SIEMConnect for Partners.	Numérico
ParentHash	Hash del proceso que actúa como padre.	Cadena de caracteres
ParentDriveType	Tipo de unidad donde reside el proceso o fichero padre que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM ▪ **Ramdisk**: unidad de disco RAM.	Enumeración

Campo	Descripción	Valor
ParentPath	Ruta del fichero padre que realizó la operación registrada.	Cadena de caracteres
ParentValidSig	El proceso padre está firmado digitalmente.	Booleano
ParentCompany	Contenido del atributo Company de los metadatos del proceso padre.	Cadena de caracteres
ParentBroken	El proceso padre está corrupto o defectuoso.	Booleano
ParentImageType	Arquitectura interna del proceso padre: ▪ EXEx32 ▪ EXEx64 ▪ DLLx32 ▪ DLLx64	Enumeración
ParentExeType	Estructura interna / tipo del proceso padre. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
ParentPrevalence	Prevalencia histórica del proceso padre en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ParentPrevLastDay	Prevalencia del proceso padre en el día anterior en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ParentCat	Categoría del fichero padre que realizó la	Enumeración

Campo	Descripción	Valor
	operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	
ParentMWName	Nombre del malware en el proceso padre si ya está catalogado como una amenaza. Si es Null el elemento no es malware.	Cadena de caracteres
URL	Url de descarga lanzada por el proceso que generó el evento registrado.	Cadena de caracteres
ChildHash	Hash del proceso que actúa como hijo.	Cadena de caracteres
ChildDriveType	Tipo de unidad donde reside el proceso o fichero padre que desencadenó la operación registrada. ▪ **Fixed**: dispositivo no extraible, como por ejemplo un disco duro interno. ▪ **Remote**: unidad de red. ▪ **Removable**: dispositivo extraible, como por ejemplo un pen drive o un diskette. ▪ **Unknown**: dispositivo de tipo desconocido. ▪ **NoRootDir**: dispositivo no disponible en la ruta indicada. ▪ **Cdrom**: unidad de CD-ROM ▪ **Ramdisk**: unidad de disco RAM.	Enumeración
ChildPath	Ruta del fichero hijo que realizó la operación registrada.	Cadena de caracteres (Ruta)
ChildValidSig	El proceso hijo está firmado digitalmente.	Booleano
ChildCompany	Contenido del atributo Company de los metadatos del proceso hijo.	Cadena de caracteres
ChildBroken	El proceso hijo está corrupto o defectuoso.	Booleano
ChildImageType	Arquitectura interna del proceso hijo: ▪ EXEx32	Enumeración

Campo	Descripción	Valor
	▪ EXEx64 ▪ DLLx32 ▪ DLLx64	
ChildExeType	Estructura interna / tipo del proceso padre. ▪ Delphi ▪ DOTNET ▪ VisualC ▪ VB ▪ CBuilder ▪ Mingw ▪ Mssetup ▪ Setupfactory ▪ Lcc32 ▪ Vc7setupproject ▪ Unknown	Enumeración
ChildPrevalence	Prevalencia histórica del proceso hijo en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ChildPrevLastDay	Prevalencia histórica del proceso hijo en los sistemas de Cytomic. ▪ High ▪ Medium ▪ Low	Enumeración
ChildCat	Categoría del fichero padre que realizó la operación registrada. ▪ Goodware ▪ Malware ▪ PUP ▪ Unknown ▪ Monitoring	Enumeración
ChildMWName	Nombre del malware en el proceso hijo si ya está catalogado como una amenaza. Si es Null el elemento no es malware.	Cadena de caracteres

Campo	Descripción	Valor
ParentPid	Pid del proceso padre que realiza la descarga del fichero.	Numérico
MUID	Identificador interno del equipo del cliente.	Cadena de caracteres
TTPs	Lista de las técnicas, tácticas y subtécnicas asociadas al evento MITRE.	Cadena de caracteres
IOAIds	Cuando una secuencia de eventos sigue un patrón descrito en la matriz MITRE, el producto de seguridad crea un indicio (IOA) y añade su identificador a todos los eventos que lo forman.	Numérico
TelemetryType	▪ **0: telemetría normal**. El evento no pertenece a un indicio que siga un patrón descrito en la matriz MITRE. ▪ **1: evento reenviado**. El evento se envió inicialmente como tipo 0 (telemetría normal), pero tiempo después se ha detectado que pertenece a un patrón de ataque escrito en la matriz MITRE. El evento se vuelve a enviar con los campos TTPs e IOAIds completados. ▪ **2: evento acumulado**: para ahorrar recursos, parte de la telemetría generada en el cliente se retiene hasta que el software de seguridad detecta un patrón de ataque MITRE. En ese momento se envían todos los eventos acumulados.	Enumeración