Resumen de la solución

Cynet 360 AutoXDR™

La ciberseguridad, más fácil

Introducción

Las capas de seguridad son costosas y complejas, desbordando a los equipos de seguridad de tamaño reducido y dificultando su capacidad para gestionar las operaciones. Mientras tanto, el número de amenazas comunes y avanzadas sigue aumentando y los equipos de seguridad se ven obligados a recurrir a tecnologías diversas para evitar infracciones.

Como resultado, los equipos de seguridad se enfrentan a los siguientes retos:

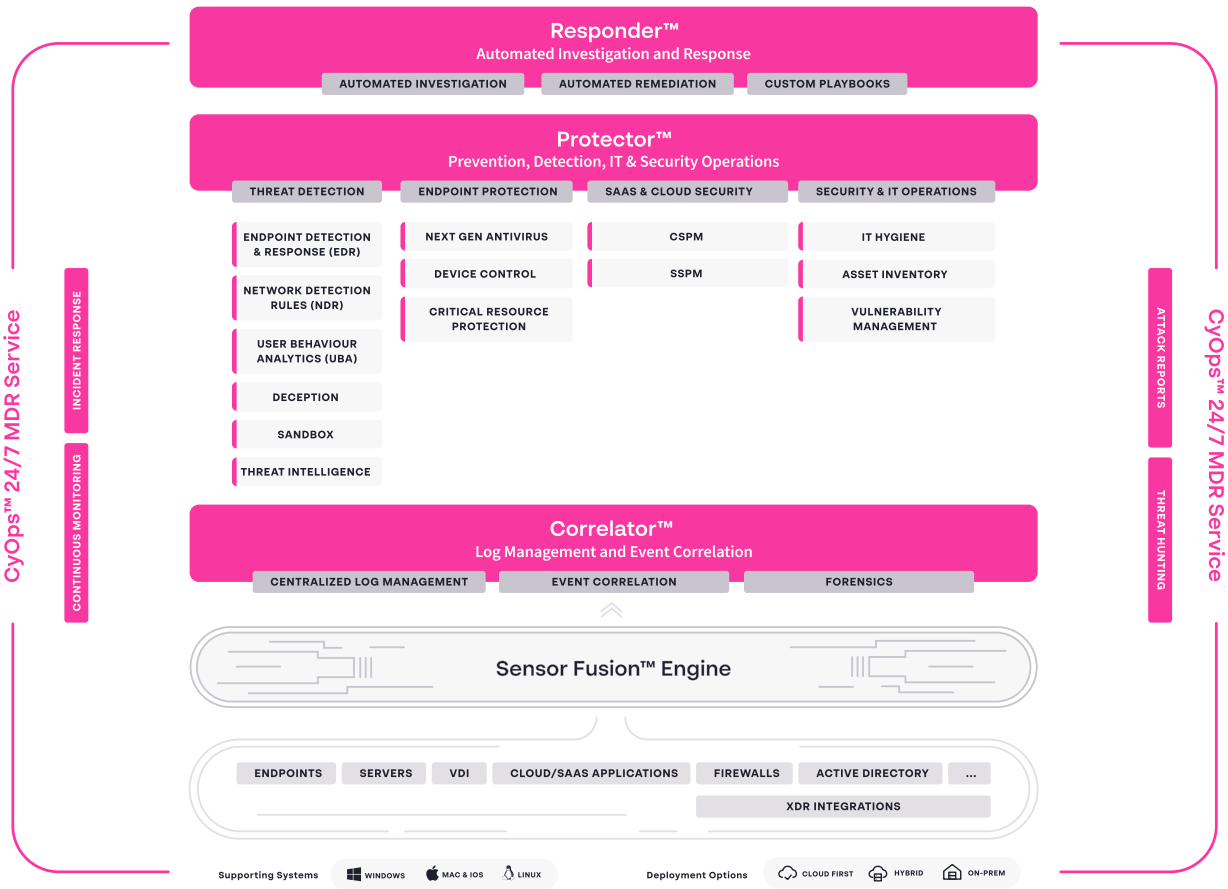
- Complejidad en el despliegue de software: necesidad de unir productos dispares que no fueron diseñados para trabajar juntos.
- Ineficacia e ineficiencia de la seguridad por capas: la disparidad de tecnologías provoca solapamientos y puntos ciegos.
- Flujos de trabajo manuales: las tecnologías de protección contra infracciones introducidas con posterioridad a la detección de una infracción requieren de intervenciones manuales que, por definición, no pueden adaptarse al volumen de alertas generadas.
- Falta de competencias: la escasez de personal preparado y que reúna las competencias requeridas para operar y mantener estas tecnologías de manera eficiente, está colocando la seguridad prácticamente fuera del alcance de la mayoría de las organizaciones.

La ironía que plantea la seguridad por capas es una fuente de desesperación para la mayoría de los equipos de seguridad. Aunque el objetivo de añadir tecnologías es proteger a la organización, la superposición de tecnologías implica que los equipos de seguridad no pueden gestionar eficientemente todas estas capas para garantizar una protección adecuada de la organización.

Acerca de la plataforma de ciberseguridad Cynet 360 AutoXDR™

Cynet facilita la ciberseguridad. La plataforma 360 AutoXDR™ permite que incluso los equipos de seguridad más reducidos alcancen una protección y visibilidad completas y eficaces en todos los puntos de conexión, usuarios, redes y aplicaciones SaaS, independientemente de sus recursos, el tamaño de su equipo o sus habilidades.

Lo hace proporcionando la primera plataforma de detección y respuesta extendidas (XDR) automatizada de forma nativa de extremo a extremo, que se despliega de forma instantánea, es radicalmente sencilla de utilizar y es súper eficiente. La plataforma proporciona visibilidad, prevención, detección, correlación e investigación y respuesta automatizadas a través de una única plataforma.



La plataforma Cynet 360 AutoXDR™ gestiona las operaciones de seguridad del día a día, permitiendo que los equipos de seguridad informática puedan dedicar sus limitados recursos a la gestión de la seguridad, en lugar de centrarse en la gestión de las incidencias.

- **Cynet Protector™** proporciona múltiples tecnologías nativas de detección necesarias para identificar y prevenir las amenazas en todo el entorno, con capacidades EPP, EDR, tecnología de engaño y señuelos, reglas de detección de red, reglas de análisis de comportamiento del usuario, inteligencia de detección de amenazas, entorno de pruebas, y gestión de la postura de seguridad en la nube y en aplicaciones SaaS (SSPM/CSPM).

- **Cynet Correlator™** analiza todos los datos relevantes procedentes de señales de Cynet, sensores de terceros y datos de registro y los correlaciona para crear incidentes procesables, incluyendo la gestión centralizada de los registros.

- **Cynet Responder™** investiga las amenazas existentes y automáticamente orquesta acciones de resolución y reparación en todo el entorno.

- **El servicio complementario de Cynet CyOps™** 24/7 MDR proporciona monitorización, investigación, análisis bajo demanda, respuesta a incidentes y caza de amenazas.

Nuestra visión es permitir a los equipos de seguridad que operen la ciberseguridad en piloto automático para centrar sus recursos en la gestión de la seguridad, en lugar de dedicar su tiempo a la gestión de incidencias.

Devuelva la cordura a la ciberseguridad con un nuevo enfoque que hace que la protección de su organización sea fácil y sin estrés. Con la amplia visibilidad que proporciona a la totalidad del entorno, la completa automatización de la protección y el servicio MDR gratuito las 24 horas del día, 7 días a la semana, Cynet elimina la complejidad, el coste y la preocupación de la ciberseguridad.

MÁS INFORMACIÓN

Cynet Protector™: Prevención, detección, operaciones de TI y seguridad

El componente Protector de Cynet combina de forma nativa varias capacidades de prevención y detección, listas para usar, proporcionando una protección multicapa sin fisuras a los equipos de usuarios. De esta manera, los equipos de trabajo se ahorran el tiempo y el esfuerzo necesarios para comprar, integrar y gestionar múltiples soluciones de terceros.

Vista de alerta 360

Reciba una visión inmediata del estado de actividad de las amenazas existentes en todo el entorno.

Protección de los puntos de conexión

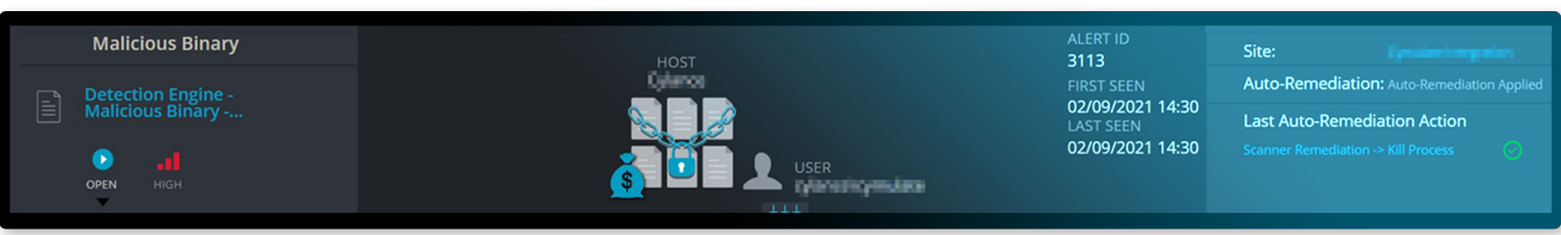
1. Antivirus NGAV

Analiza los archivos en reposo y los archivos no ejecutables para protegerlos contra código malicioso conocido.

- Protección contra código malicioso basada en inteligencia artificial
- Protección contra código malicioso mediante análisis estático basado en IA
- Protección contra la explotación basada en el comportamiento
- Protección de macros y scripts contra los ataques sin archivos basada en el comportamiento.

Alertas - Ejemplo 1: Detección de binario malicioso

La protección de Cynet basada en IA bloquea la ejecución de archivos binarios con código malicioso.

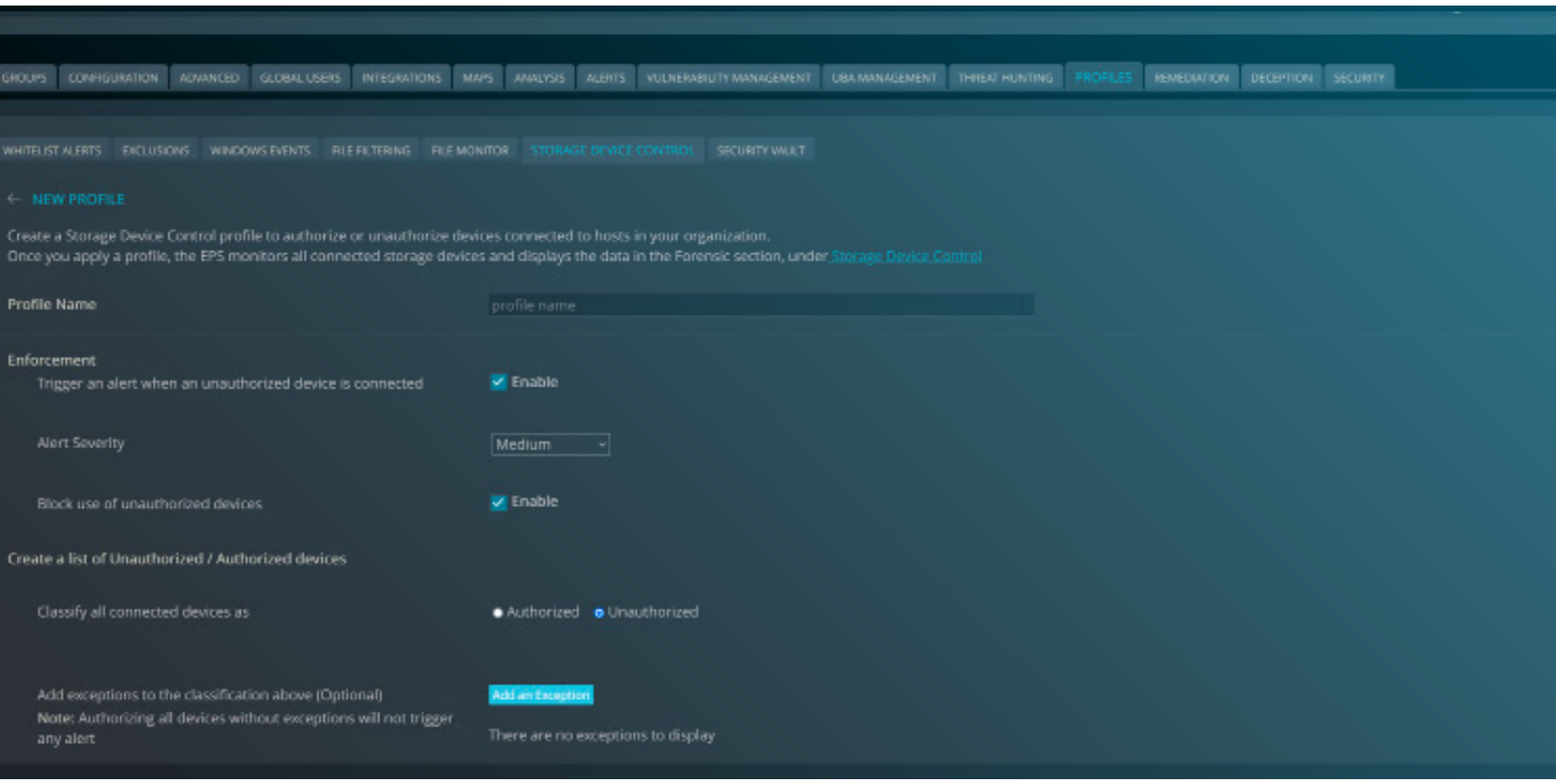


2. Control de dispositivos

Detecta y bloquea los dispositivos de almacenamiento externos que se insertan en el punto de conexión (por ejemplo, un dispositivo USB o una tarjeta SD).

Puede crear perfiles de control de dispositivos de almacenamiento. Cada perfil puede asignarse a un grupo de escaneo diferente y puede incluir normas como:

- Dispositivo de conexión autorizado o no autorizado según el ID del dispositivo
- Dispositivo de conexión autorizado o no autorizado según el tipo de dispositivo
- Dispositivo de conexión autorizado o no autorizado según las reglas de combinación de ID de producto o de proveedor



Alertas - Ejemplo 2: Alerta sobre un dispositivo de almacenamiento insertado

Detección y bloqueo de un dispositivo de almacenamiento insertado en contra de la política de seguridad.

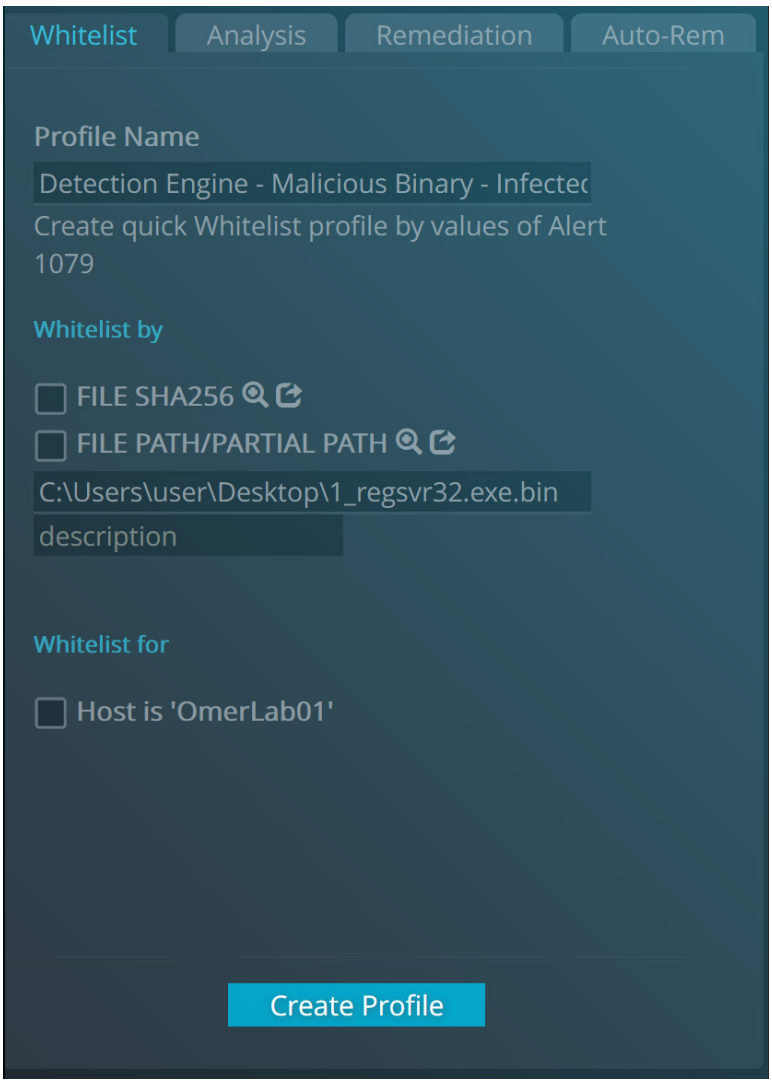
3. Protección de recursos críticos

Cynet protege a los usuarios, las redes, los servidores (físicos y virtuales), los archivos, los procesos, los componentes de la nube y las configuraciones del cliente gracias a su amplia visión de la superficie de ataque. Funciona conectando diversos sensores ligeros a diferentes recursos, alimentando los datos a un agregador centralizado.

El objetivo de Cynet es reducir el número de falsos positivos, facilitando que el cliente pueda centrarse en lo que es importante.

Cynet desarrolló dos mecanismos:

- Reglas dinámicas: Las reglas de Cynet son dinámicas y pueden ser modificadas en tiempo real por el equipo de CyOps de Cyent.
- Reglas de inclusión en lista blanca: Los clientes de Cynet pueden marcar un componente (archivos, servidores, configuraciones, etc.) para incluirlo en la lista blanca e identificarlo como no malicioso.



Detección extendida de amenazas

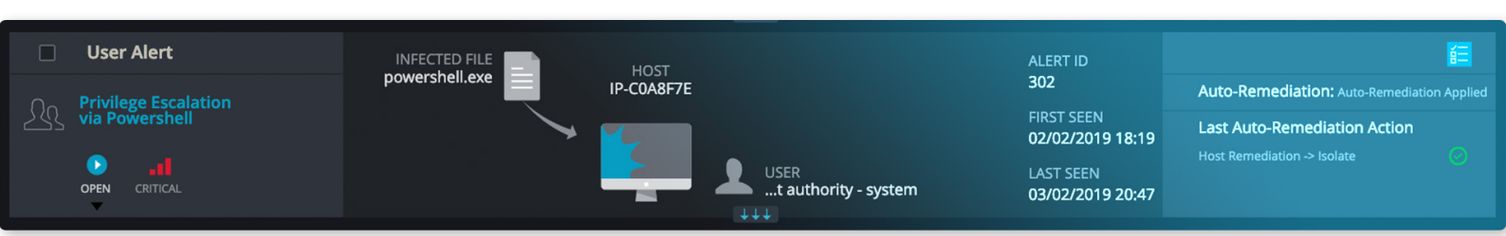
1. EDR

Analiza el comportamiento de los procesos para detectar procesos y aplicaciones fraudulentas a través de varios mecanismos, entre ellos

- **SSDEEP Scan**: utiliza un algoritmo de compresión que busca similitudes con un código malicioso (conocido como Fuzzy fingerprints), usado comúnmente para reutilizar herramientas existentes a través de soluciones tradicionales basadas en firmas.
- **Patrones de memoria**: analiza la memoria cargada de un host en busca de procesos para identificar patrones de actividad, estructura y comportamiento de datos, datos con cadenas sospechosas y similitudes con código malicioso conocido, actividad de código malicioso, procesos de carga de DLLs sospechosas o maliciosas a la memoria para obtener acceso a áreas sensibles del sistema operativo o ser inyectadas en otros procesos.
- **Tecnología de detección avanzada (ADT)**: herramientas heurísticas para la inspección de sistemas operativos en busca de comportamientos dañinos originados por código malicioso y ataques con o sin archivos. Esto detecta actividades maliciosas en procesos legítimos como PowerShell o cmd. ADT analiza la estructura de un comando, sus resultados y la conexión entre el comando y el proceso primario, buscando patrones maliciosos como por ejemplo un archivo WinWord que ejecuta un comando PowerShell.
- **Controlador en modo kernel**: logre una mayor visibilidad de las amenazas existentes a nivel del kernel. Este mecanismo también evita que el Cynet Endpoint Protection Scanner (EPS) sea terminado. Los sistemas de protección incluyen los mecanismos antimanipulación, que protegen los procesos de Cynet evitando que puedan ser terminados o manipulados, la protección contra escritura en áreas sensibles del sistema operativo en el disco duro, y redirección de proxy para recursos críticos del sistema como Lsass.

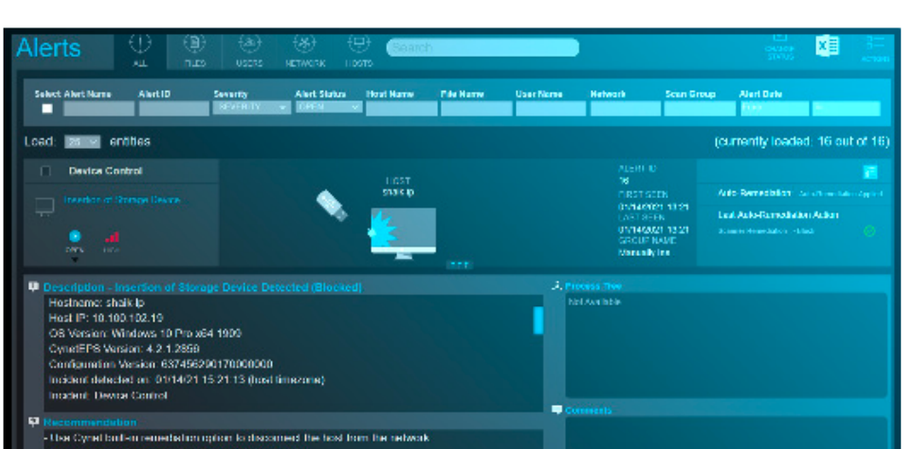
Alertas - Ejemplo 3: Escalada de privilegios

Cynet bloquea PowerShell, un proceso de administración legítimo, si detecta un intento de escalada de privilegios para un usuario.



Alertas - Ejemplo 4: Protección contra exploits

Cynet detecta y bloquea un documento de Word manipulado que contiene un exploit.



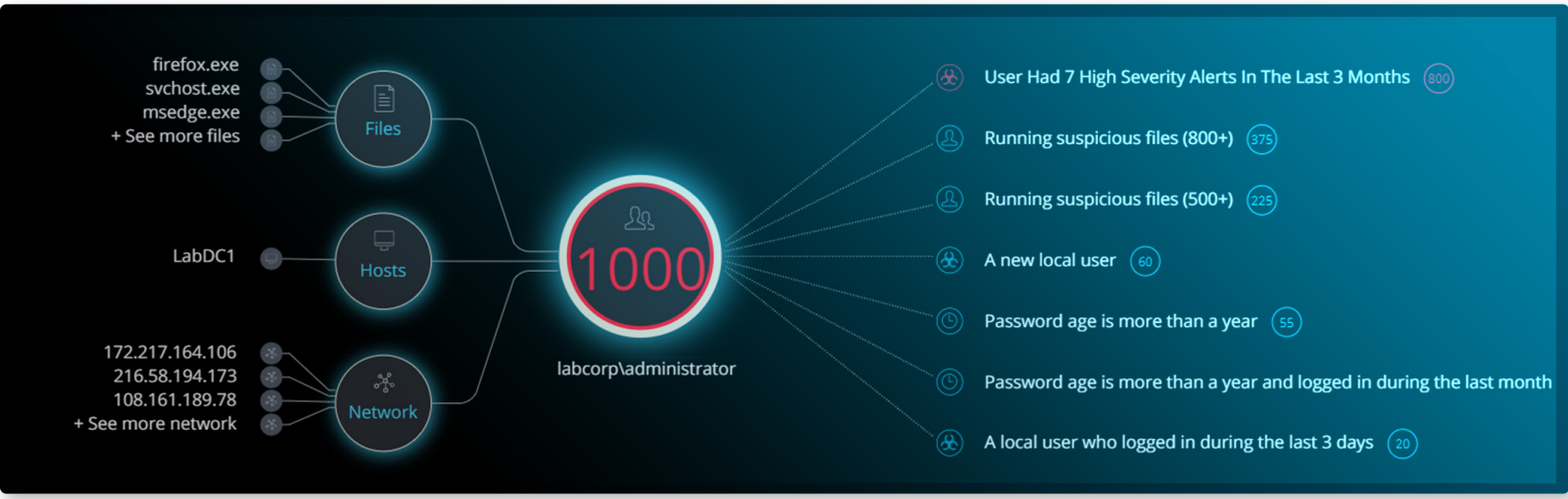
2. Reglas de análisis del comportamiento del usuario (reglas UBA)

Aprende el comportamiento de usuarios y entidades para alertar sobre la detección de actividades inusuales, incluyendo:

- Seguimiento en tiempo real de todas las interacciones que inician los usuarios
- Hosts en los que los usuarios inician sesión, número de hosts, ubicación y frecuencia
- Comunicación en red interna y externa
- Archivos de datos que han sido abiertos por usuarios
- Procesos ejecutados

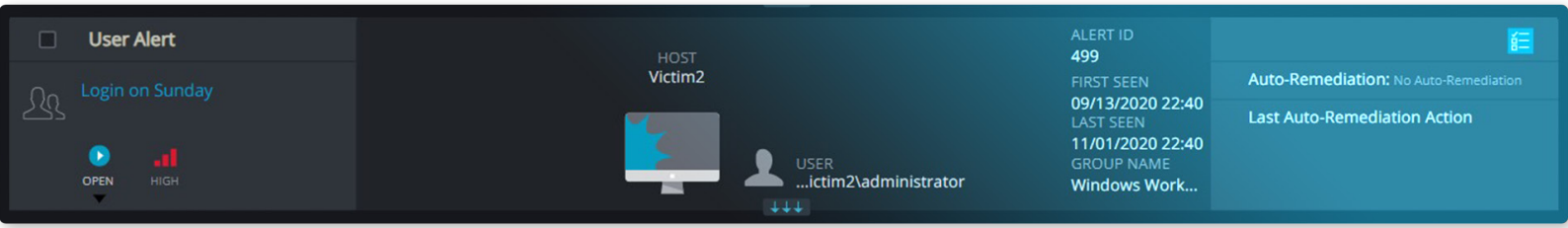
Ejemplo forense 5: Comportamiento del usuario

El análisis forense de Cynet muestra un comportamiento de usuario altamente sospechoso mediante la correlación de varias actividades anormales.



Alertas - Ejemplo 6: Acceso en domingo

El componente UEBA de Cynet detecta actividad anormal de inicio de sesión durante el fin de semana.



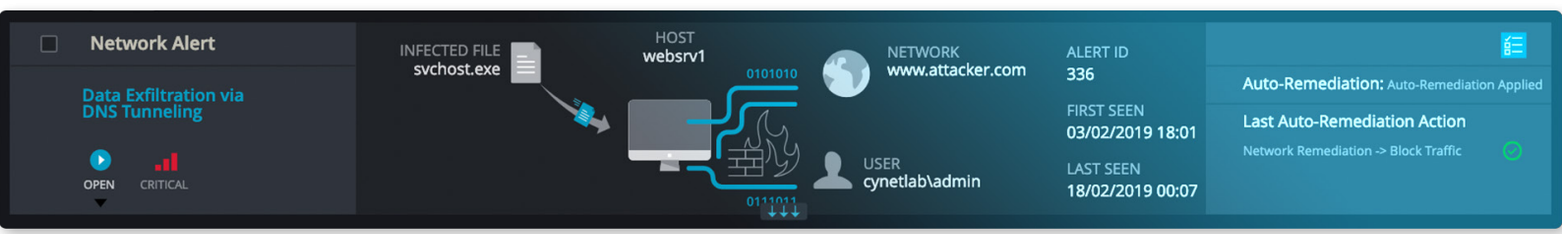
3. Detección y respuesta de red

Analiza la actividad para detectar ataques en la red, incluyendo:

- Robo de credenciales basado en la red (suplantación de ARP, respondedor DNS)
- Movimiento lateral en la red
- Comunicación saliente maliciosa (C2C, suplantación de identidad o phishing)
- Reconocimiento basado en la red (ataques de escaneo)
- Exfiltración de datos basada en la red (tunelización a través de varios protocolos)

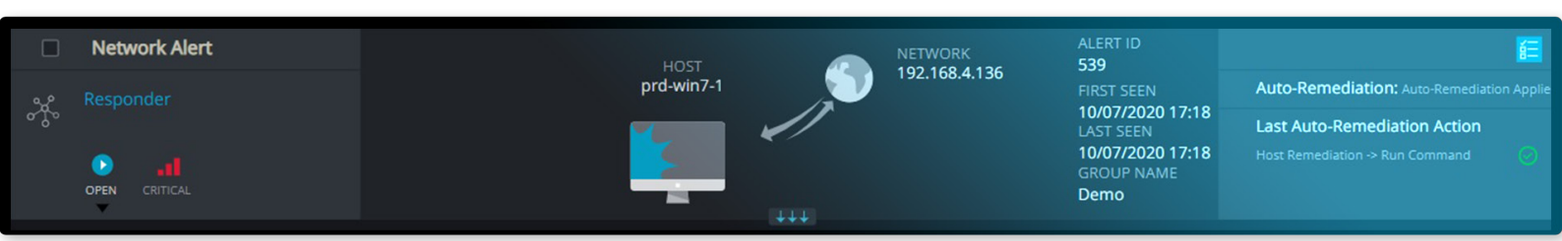
Alertas - Ejemplo 7: Exfiltración o robo de datos

Esta alerta detecta una etapa avanzada en la cadena de destrucción del ataque, en la que el atacante ha obtenido acceso a los datos e intenta filtrarlos al exterior, disfrazando los datos robados como tráfico DNS legítimo.



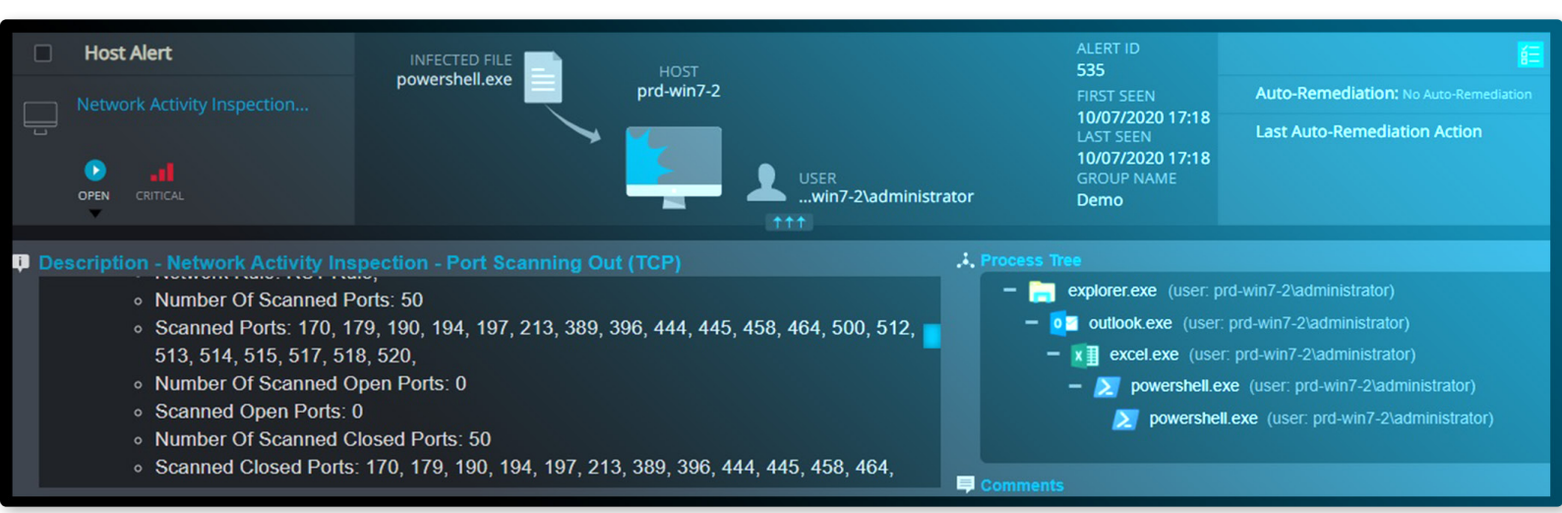
Alertas - Ejemplo 8: Software malicioso Responder

Cynet detecta y bloquea el software malicioso Responder, que explota las vulnerabilidades de los protocolos de red.



Alertas - Ejemplo 9: Escaneo de puertos

Cynet detecta que un servidor ha iniciado un escaneo de puertos en la red.



4. Tecnología de engaño y señuelos

Utilizando tácticas de señuelo o *honeypot*, Cynet coloca sistemas trampa en el entorno y los monitoriza con el objetivo de atraer y detectar intentos de ataque, y alertar acerca de los mismos.

Las alertas se generan al detectar:

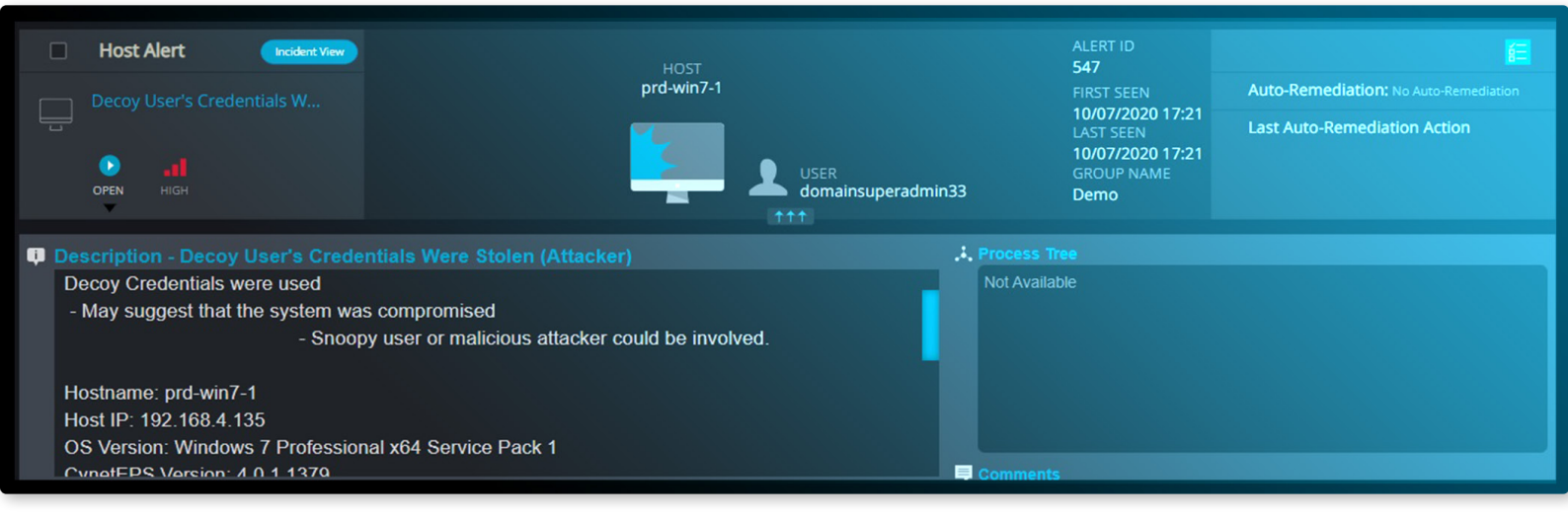
- Señuelos de secuestro de datos o ransomware
- Ficheros sospechosos
- Señuelos de usuario
- Señuelos de red

Alertas - Ejemplo 10: Tecnología de engaño y señuelos (Archivos)

Con la finalidad de revelar su presencia, se atrajo al atacante a través de un archivo de Word plantado como señuelo.

Alertas - Ejemplo 11: Tecnología de engaño y señuelos (Usuarios)

El atacante fue atraído a revelar su presencia al intentar utilizar las credenciales de un usuario señuelo.

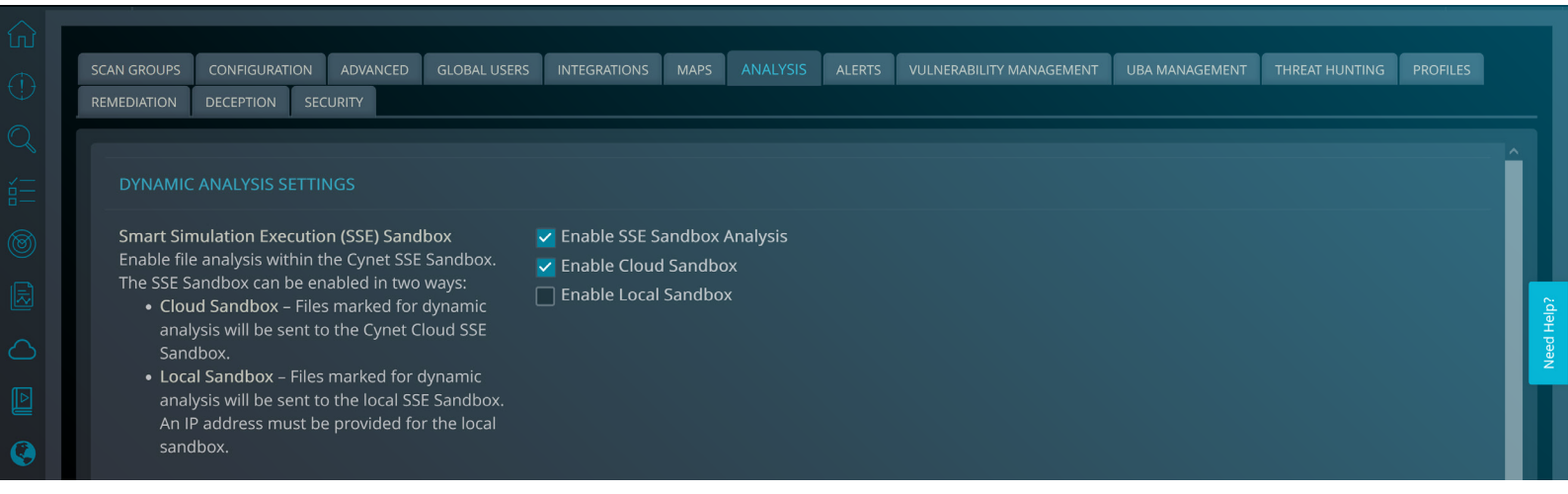


5. Entorno de pruebas

La plataforma de Cynet envía archivos para su inspección a través del entorno de pruebas Smart Simulation Execution (SSE) Sandbox.

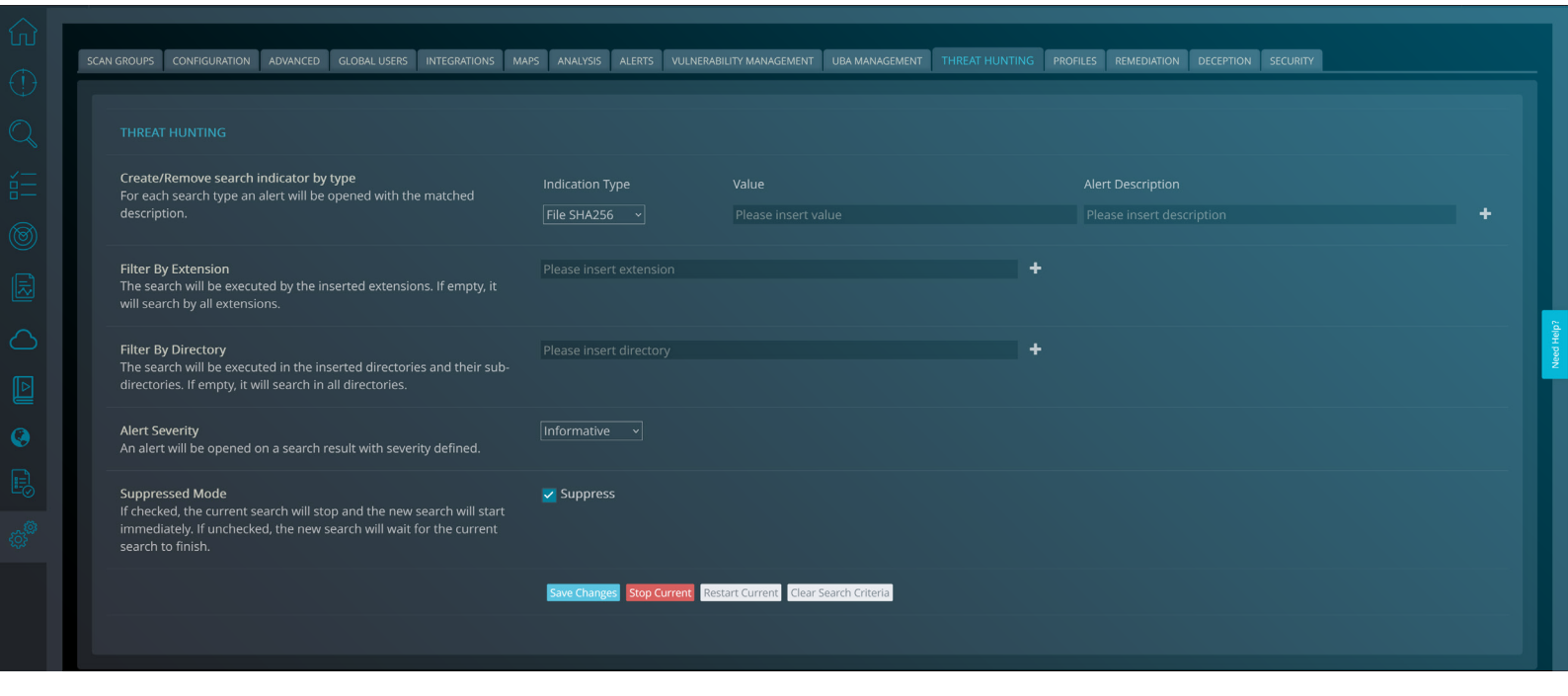
SSE Sandbox puede ser activado de dos maneras:

- **Entorno de pruebas en la nube**: los archivos marcados para su análisis dinámico serán enviados a Cynet Cloud SSE Sandbox.
- **Entorno de pruebas en local**: los archivos marcados para su análisis dinámico serán enviados al SSE Sandbox local. Para el entorno de pruebas en local es necesario proporcionar una dirección IP.



6. Inteligencia de detección de amenazas

Las ciberamenazas en constante evolución, lo que significa que debe haber un mecanismo continuo y dinámico que permita crear y actualizar el mapa de amenazas. La inteligencia de detección de amenazas de Cynet permite a sus clientes ampliar, configurar, crear y actualizar los indicadores de búsqueda mediante el uso de SHA256, MD5, FileName o Full File Path.



Seguridad en la nube y en aplicaciones SaaS

1. Gestión de la postura de seguridad de SaaS (SSPM)

Cynet SSPM permite visualizar la configuración de seguridad de todas las aplicaciones SaaS en una única plataforma, incluyendo:

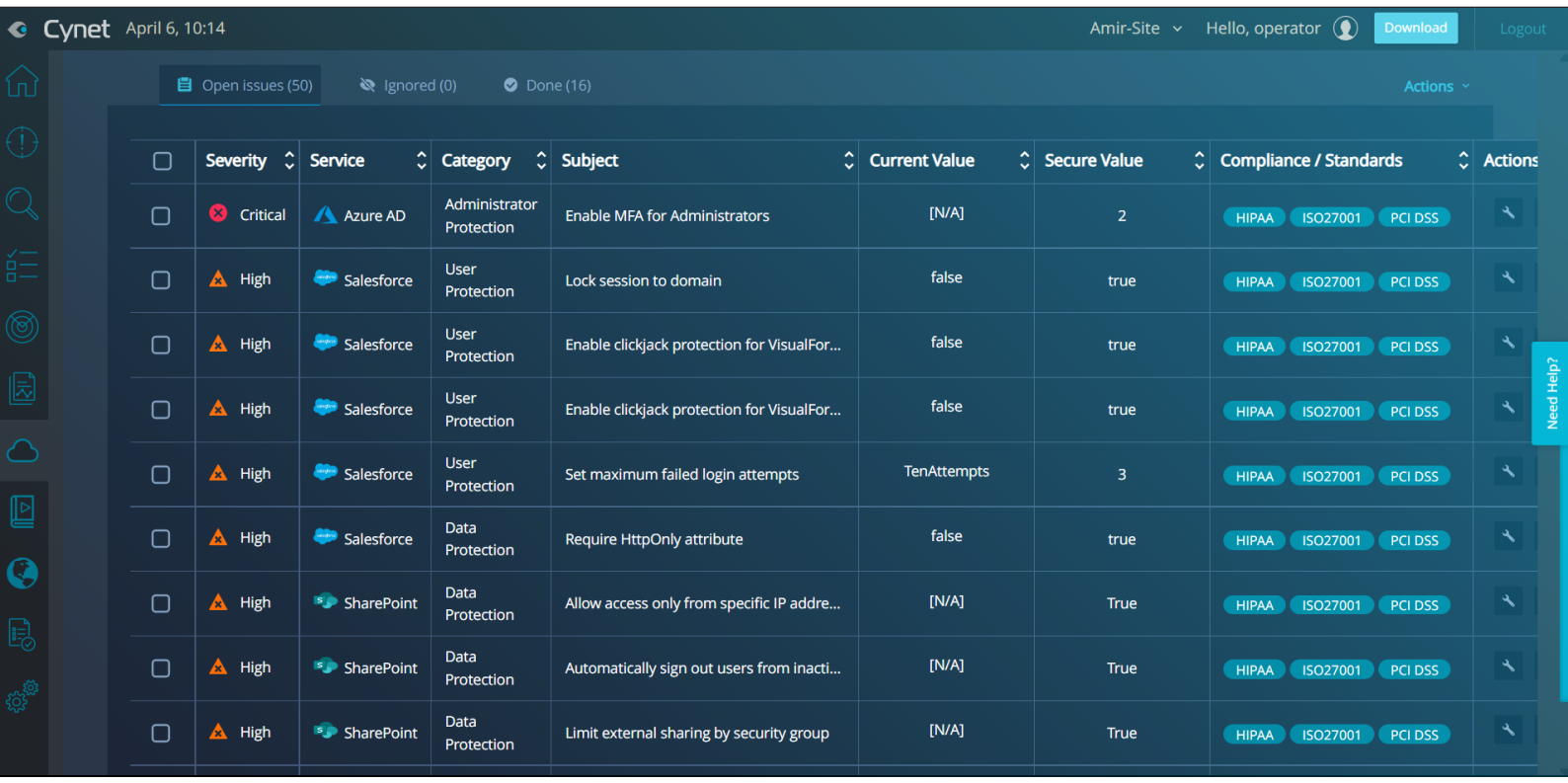
- Información sobre la configuración de los parámetros de seguridad nativos de una aplicación SaaS
- Sugerencias para mejorar las configuraciones y reducir el nivel de riesgo
- Corrección automática de errores de configuración mediante un solo clic
- Comparación con los marcos de la industria con ajustes y reconfiguración automáticos

Detección automática de los riesgos de una aplicación SaaS

Identificación automática de los riesgos de seguridad en todas sus aplicaciones SaaS, priorización de los riesgos por categoría y monitorización de todas las incidencias, por estado, directamente desde su panel de control de Cynet. Mejore sus capacidades integrales de detección y corrección de riesgos de seguridad de SaaS en su panel de control de Cynet. Supervise de forma proactiva los ajustes de configuración de todas sus aplicaciones SaaS y busque problemas de seguridad sin necesidad de acceder a paneles adicionales. La intuitiva interfaz de usuario de Cynet le permite identificar y priorizar inmediatamente los problemas de seguridad de SaaS.

Analice y solucione el problema con un solo clic

Profundice en los detalles exactos y acceda a toda la información de cada riesgo identificado, vea las acciones de resolución recomendadas y solucione los problemas con un solo clic. Cynet elimina las conjeturas, sugiriendo ajustes de configuración basados en mejores prácticas y capacidades de corrección automática para que usted pueda adoptar medidas rápidamente y corregir los problemas antes de que se conviertan en eventos de seguridad.



2. CSPM

Cynet amplía su oferta de SSPM con la gestión de la postura de seguridad en la nube (CSPM) para Amazon Web Services (AWS), que supervisa y remedia continuamente los riesgos, mientras comprueba si los servicios en la nube están mal configurados.

Cynet CSPM incluye:

- Análisis de la configuración IaaS desplegada en AWS
  - Regiones
  - VMs
  - Almacenamiento
  - Bases de Datos
  - Redes
  - Usuarios
- Potenciación de las capacidades mediante políticas personalizables que permiten una configuración sencilla y fácil de las reglas.

Severity	Service	Category	Subject	Current Value	Secure Value	Compliance / Standards	Actions
Critical	AWS	Prowler	Prowler. Ensure the S3 bucket CloudTrail logs to is not publicly ...	FAIL! us-east-1: No Cl...	not FAIL		
Critical	AWS	Prowler	Prowler. Ensure MFA is enabled for the root account - iam	FAIL! us-east-1: MFA i...	not FAIL		
Critical	AWS	Prowler	Prowler. Ensure hardware MFA is enabled for the root account -...	FAIL! us-east-1: MFA i...	not FAIL		
High	AWS	Prowler	Prowler. Ensure no security groups allow ingress from 0.0.0.0/...	PASS! eu-north-1: No ...	not FAIL		
High	AWS	Prowler	Prowler. Ensure no security groups allow ingress from 0.0.0.0/...	PASS! eu-north-1: No ...	not FAIL		
High	AWS	Prowler	Prowler. Ensure the default security group of every VPC restrict...	FAIL! eu-north-1: Defa...	not FAIL		
High	AWS	Prowler	Prowler. Check if GuardDuty is enabled - guardduty	FAIL! eu-north-1: Guar...	not FAIL		
High	AWS	Prowler	Prowler. Ensure CloudTrail is enabled in all regions - cloudtrail	FAIL! us-west-2: No Cl...	not FAIL		
High	AWS	Prowler	Prowler. Ensure there are no Security Groups without ingress fil...	INFO! eu-central-1: sg...	not FAIL		
High	AWS	Prowler	Prowler. Ensure no Network ACLs allow ingress from 0.0.0.0/0 ...	INFO! eu-north-1: Fou...	not FAIL		

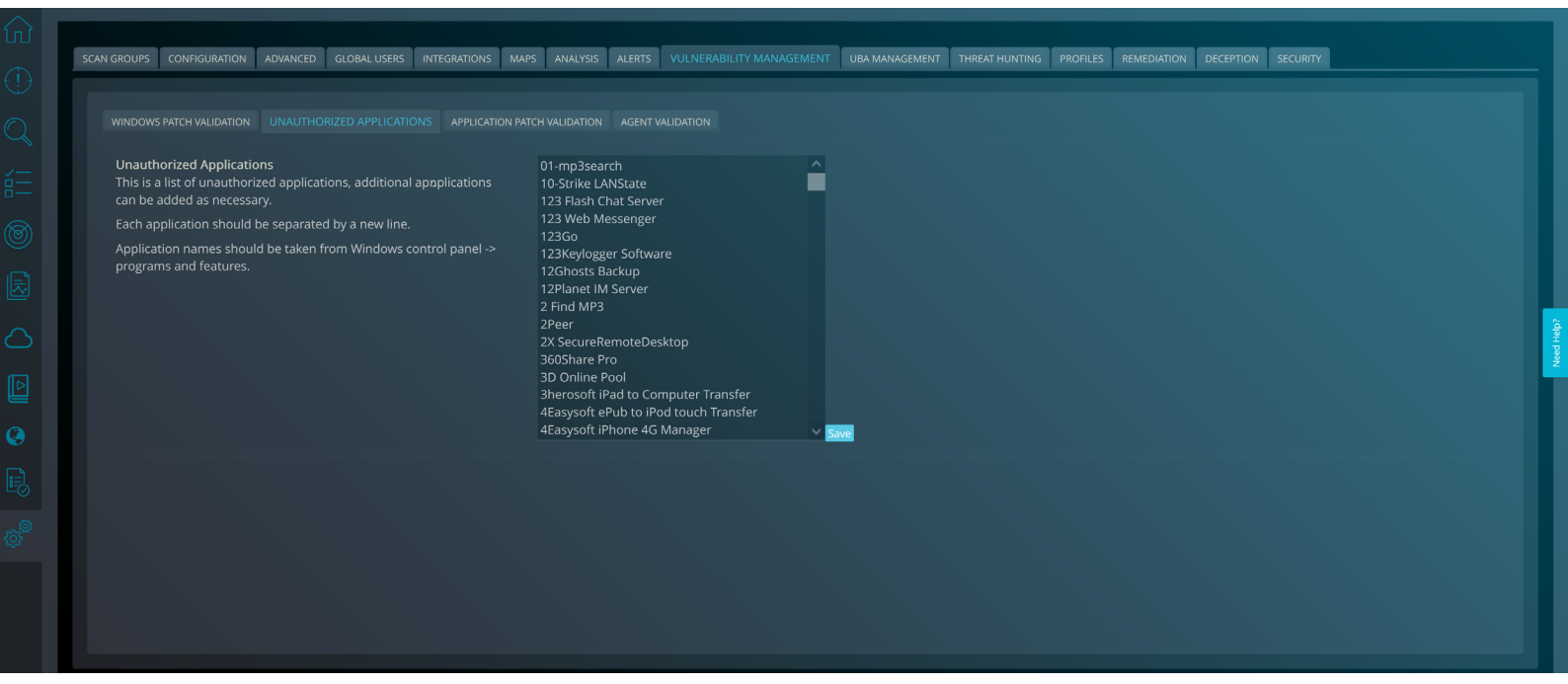
Rows per page: 10 1–10 of 48

Operaciones de TI y seguridad

1. Gestión de la vulnerabilidad

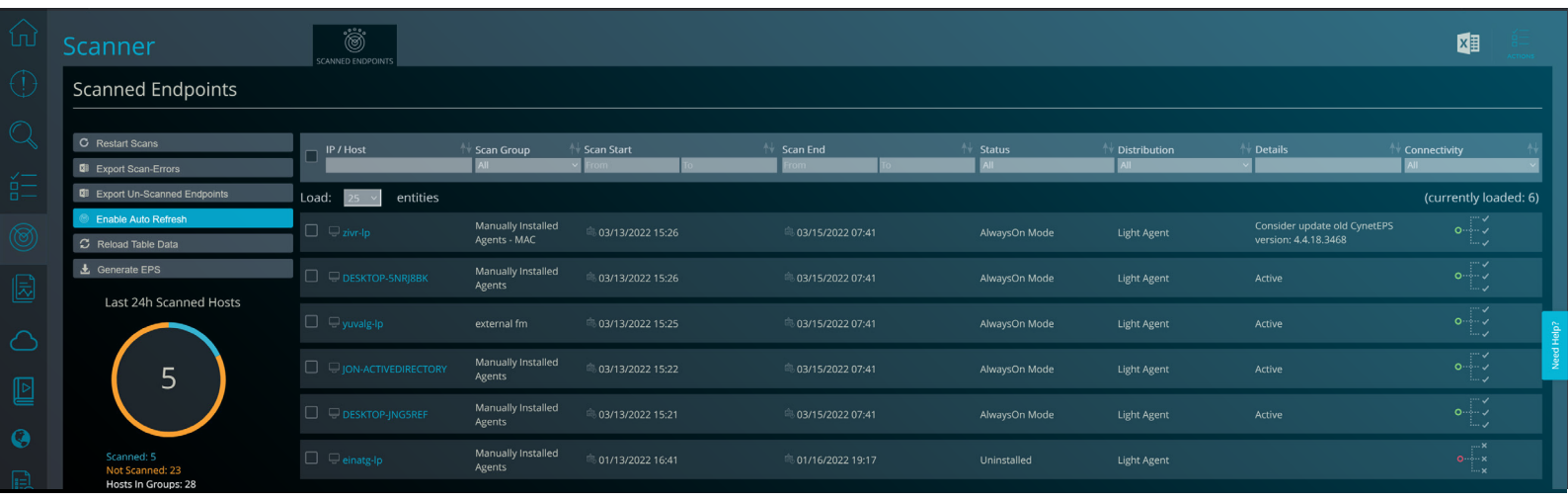
Cynet recoge las vulnerabilidades del host y la información avanzada del sistema y se los muestra al usuario en forma de indicadores forenses procesables, como por ejemplo:

- Aplicaciones no autorizadas
- Validación de agentes



2. Inventario de activos

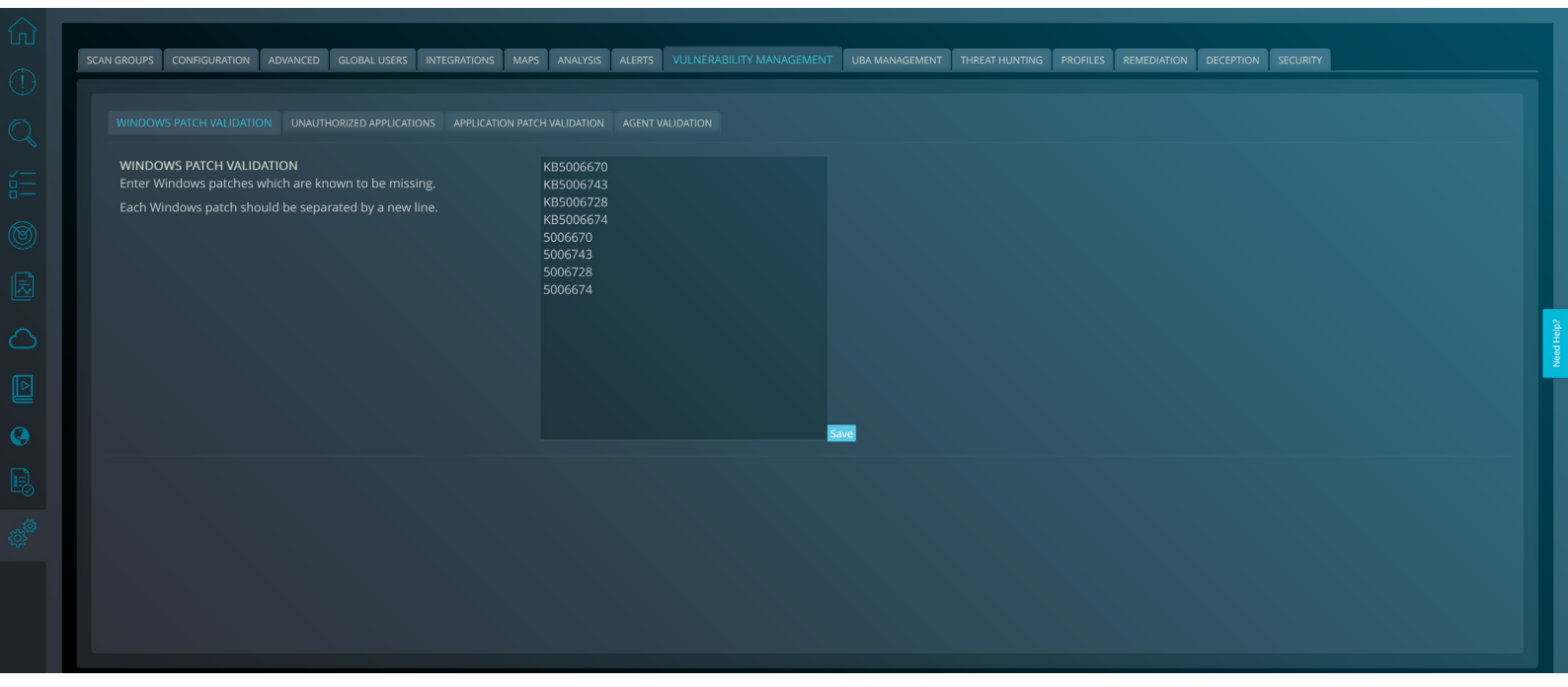
Puede revisar y gestionar los activos conectados, como los usuarios de aplicaciones en la nube o en la propia empresa, los archivos, las configuraciones y los certificados, desde la plataforma de Cynet. El uso de esta opción permite a los usuarios de Cynet revisar el estado de los activos y la cobertura contra las amenazas, así como adoptar medidas de protección específicas para cada activo.

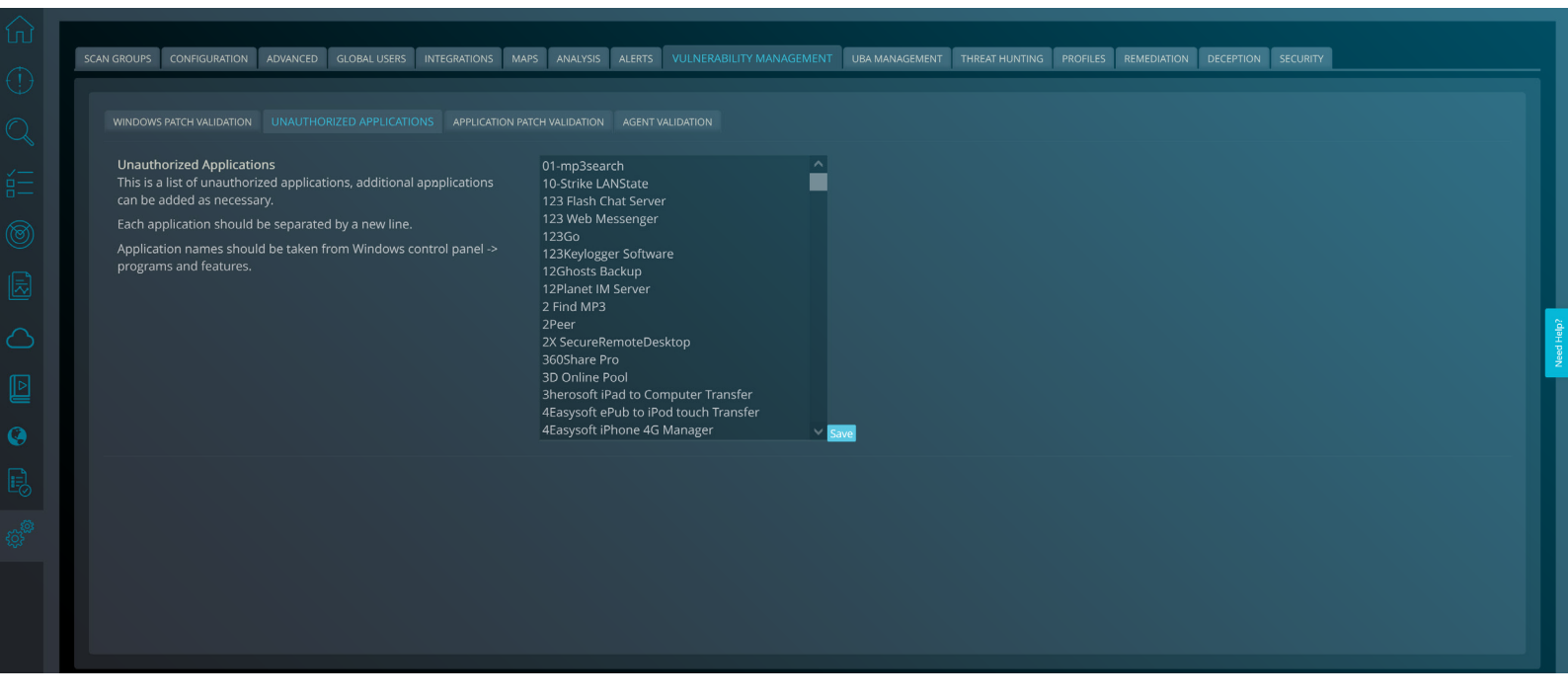


3. Higiene informática

Cynet permite a nuestros clientes recopilar y supervisar información avanzada del sistema, y la muestra al usuario en forma de indicadores forenses procesables, como por ejemplo:

- Validación de parches de Windows
- Validación de parches de aplicaciones





Cynet Responder™: Investigación y respuesta automatizadas

Cynet automatiza completamente todo el flujo de trabajo de respuesta, eliminando los esfuerzos manuales y garantizando que se completan todos los detalles y acciones de respuesta importantes.

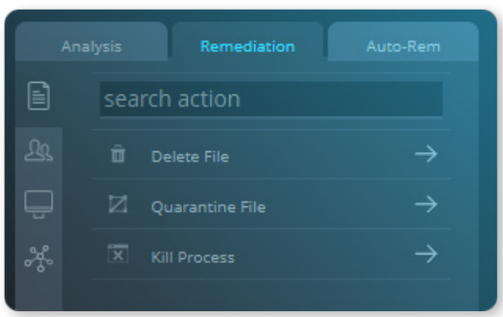
Las alertas se agrupan de forma lógica en incidentes, lo que reduce la fatiga causada por el exceso de alertas y proporciona información sobre el contexto de la amenaza. Esto incluye:

- **Investigación:** Análisis automatizados de la causa raíz y el impacto
- **Hallazgos:** Conclusiones procesables sobre el origen del ataque y las entidades afectadas
- **Acciones correctivas:** Eliminación de presencia, actividad e infraestructura maliciosas en ataques a usuarios, redes y puntos de conexión.

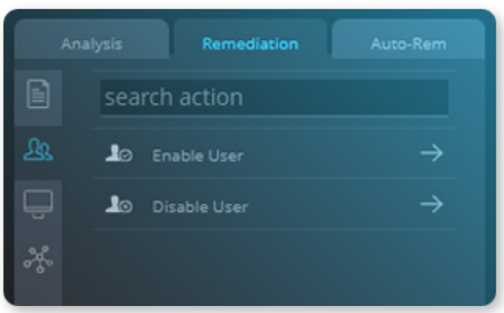
Acciones de resolución predefinidas

Cynet proporciona el más amplio conjunto de herramientas de resolución disponibles para servidores infectados, archivos maliciosos, cuentas de usuario en riesgo y tráfico controlado por atacantes.

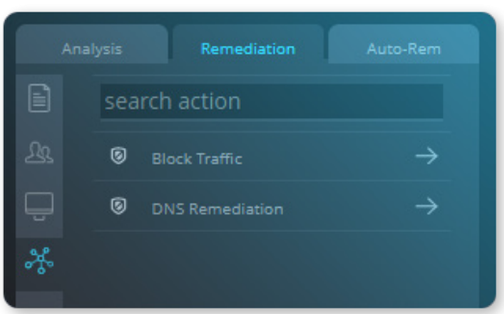
Archivo



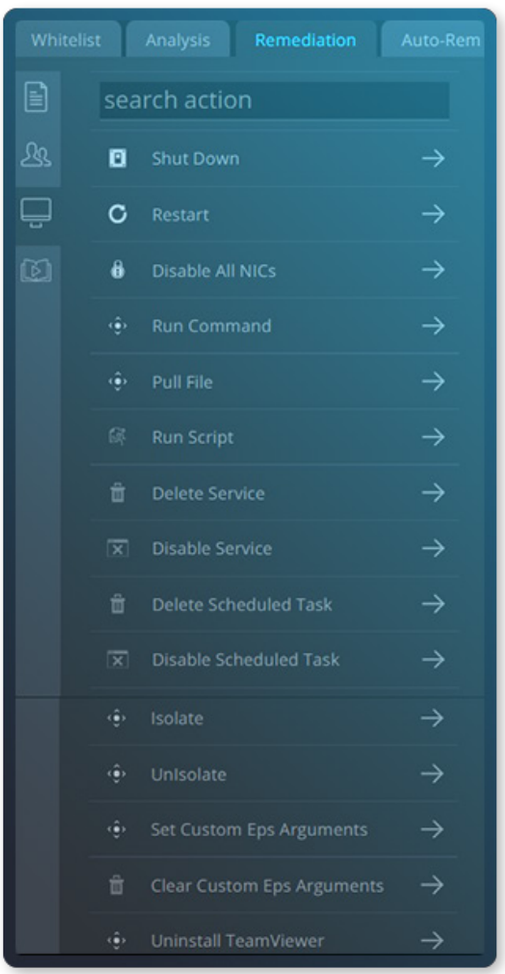
Usuario



Red



Servidor

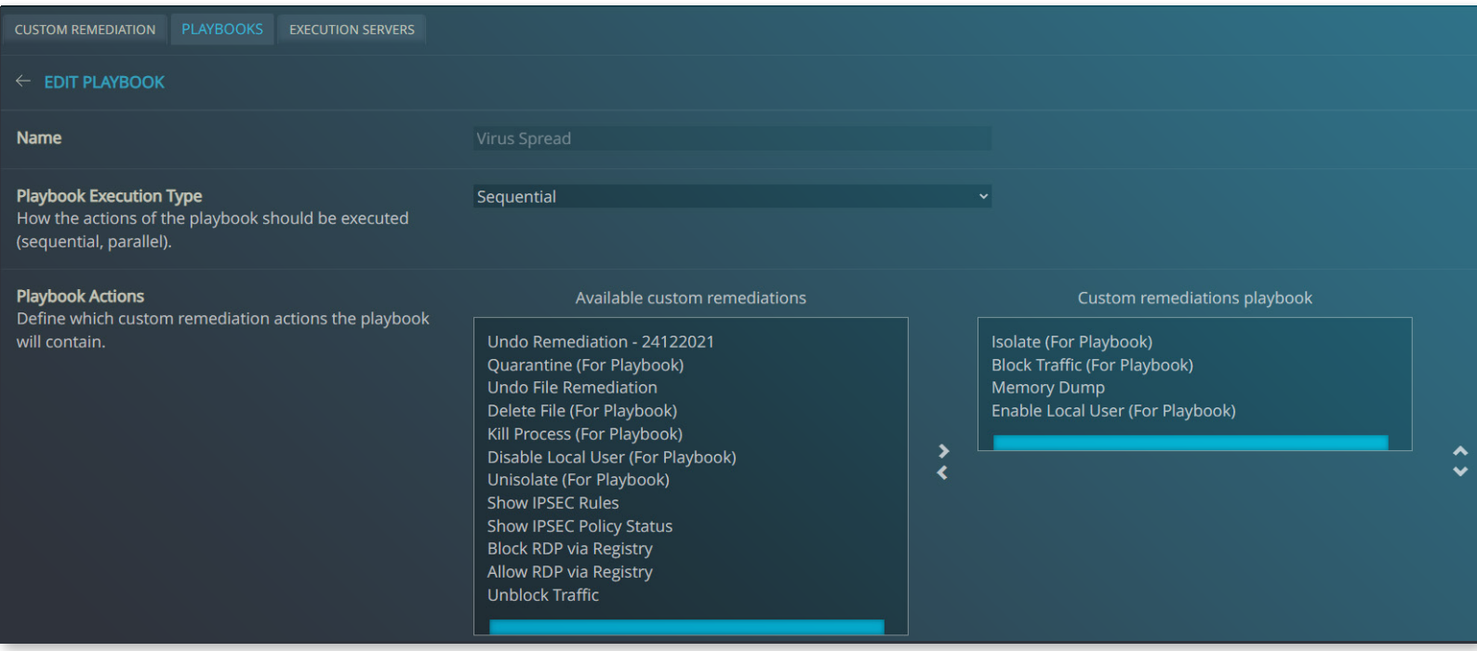


Protocolos de resolución

Los protocolos encadenan múltiples acciones de resolución asociadas. Esto permite a su equipo de seguridad escalar su capacidad de gestión de alertas, eliminando las tareas repetitivas y aumentando radicalmente la proporción de ataques que son abordados y resueltos de forma autónoma por la plataforma Cynet 360 AutoXDR™ sin necesidad de intervención humana.

Cynet 360 AutoXDR™ proporciona un amplio número de acciones de resolución listas para usar y le permite crear o editar su propio protocolo.

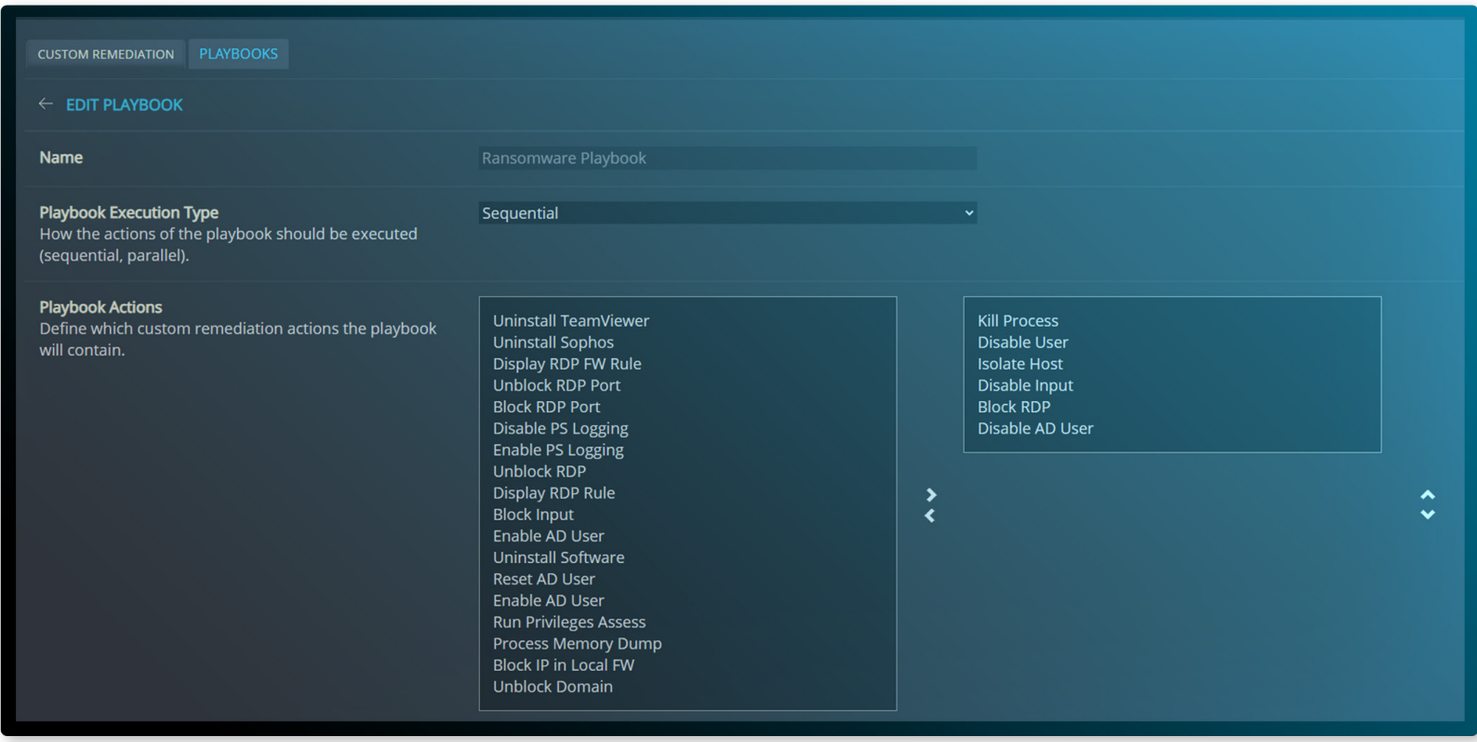
Protocolo de resolución - Ejemplo 1: Propagación de virus



En este protocolo personalizado, las acciones de resolución mostradas se ejecutan automáticamente en paralelo para impedir que el código malicioso salte de una máquina a otra.

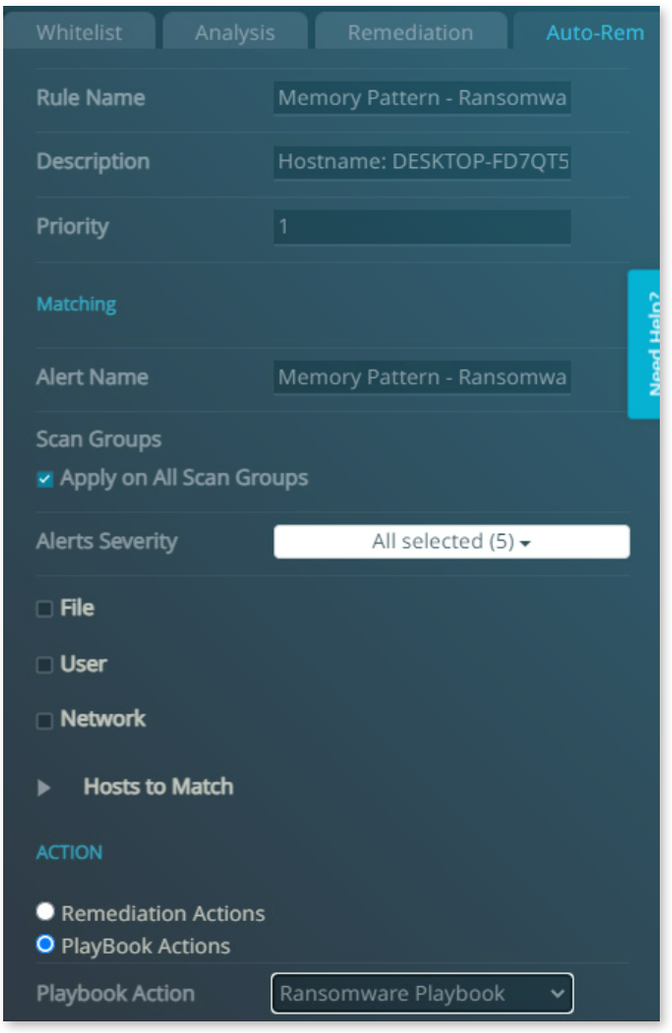
Protocolo de resolución - Ejemplo 2: Editar un protocolo de resolución

Editar su propio protocolo es fácil: puede añadir o cambiar el flujo de acciones a través de un simple menú de arrastrar y soltar.



Resolución automatizada

Cynet 360 AutoXDR™ le permite ejecutar automáticamente un protocolo de resolución listo para usar, o uno personalizado, para responder a una alerta específica.



Motor de Incidentes

Exclusivo de Cynet, el Motor de Incidentes proporciona acciones automatizadas de respuesta a incidentes, dispuestas de manera visual en una línea de tiempo que facilita la comprensión inmediata del ataque, incluyendo la causa raíz, su alcance y su resolución.

El Motor de Incidentes comienza formulando una serie de preguntas para determinar la causa raíz y el alcance del ataque. Cuando obtiene hallazgos, puede llevar a cabo acciones automatizadas para remediar la amenaza. La línea de tiempo visual le muestra todas las acciones de resolución necesarias realizadas para resolver la amenaza.

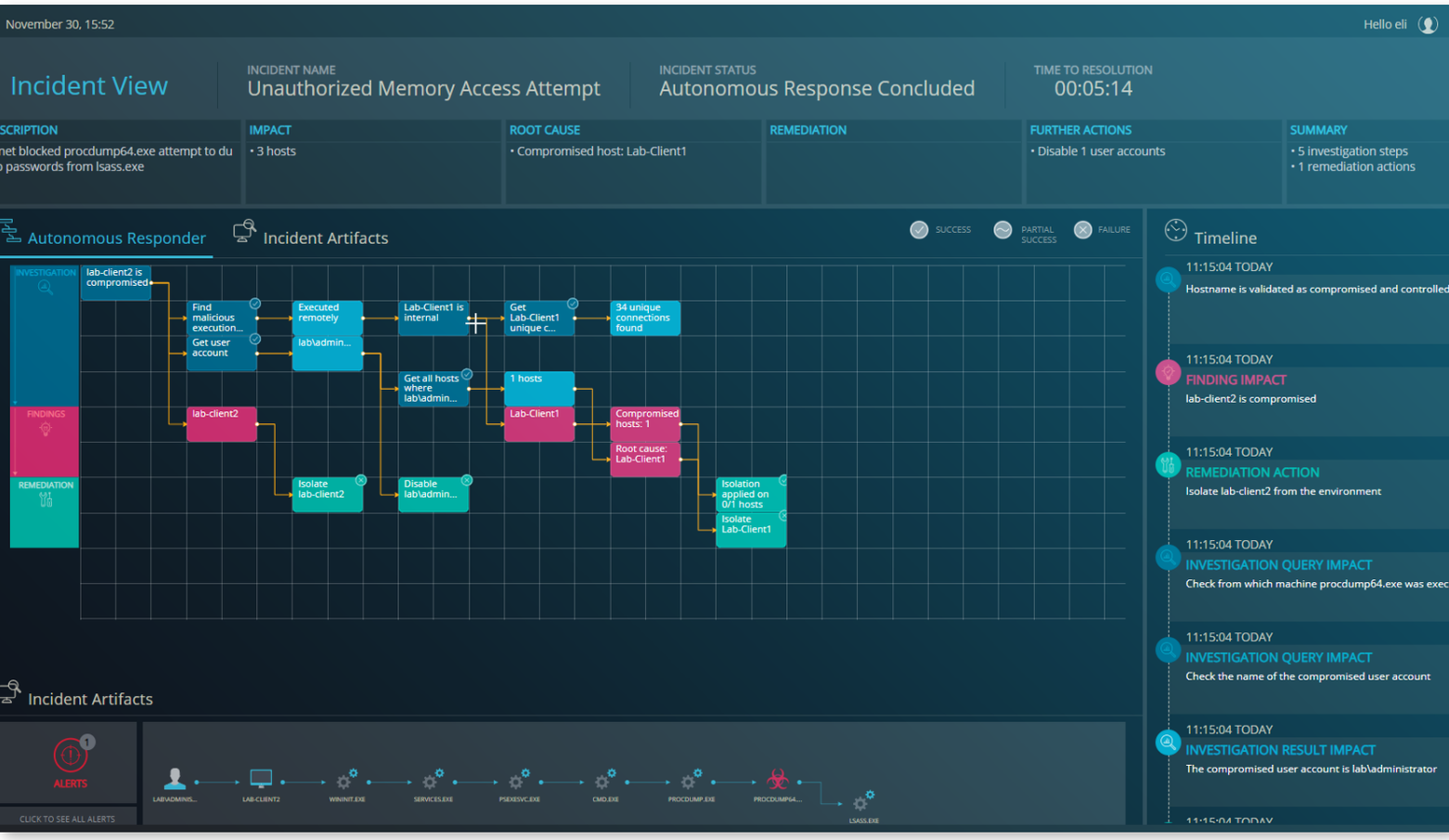
El Motor de Incidentes le ahorra un tiempo y un esfuerzo inmensos. La investigación completa hasta la resolución suele durar de unos segundos a unos pocos minutos.

Motor de Incidentes - Ejemplo 1: Comando de proceso malicioso

Como parte de la investigación automatizada, el Motor de Incidentes revela que el proceso fue terminado con suficiente antelación, evitando la ejecución de archivos maliciosos. A continuación, identifica que este comando malicioso fue ejecutado en primer lugar por una tarea programada, una utilidad común aprovechada por los atacantes para eludir los controles de seguridad. Muchos atacantes plantan una tarea programada que puede permanecer inactiva durante un tiempo y luego comenzar a ejecutar un archivo malicioso. En este caso, es el archivo wmic.exe, lo que nos lleva al primer hallazgo: la causa raíz es la Tarea Programada.

El Motor de Incidentes actúa inmediatamente y elimina la Tarea Programada del servidor. Es importante tener en cuenta que si nos basáramos sólo en el nivel de prevención, esa Tarea Programada podría haber seguido ejecutando archivos maliciosos, o tal vez varios, esperando que uno de ellos no fuera detectado. Sin embargo, el Motor de Incidentes eliminó la causa raíz antes de que tuviera la oportunidad de producirse.

Como parte de la investigación, el Motor de Incidentes comprueba si la tarea maliciosa llegó a otros servidores y, efectivamente, descubre que esta tarea ha sido programada en otros dos equipos. El Motor de Incidentes elimina automáticamente la tarea programada de estos servidores. Finalmente, el Motor de Incidentes encuentra el primer servidor infectado: Yiftach-pc4. Esta máquina se comunicaba con los otros dos hosts infectados, por lo que es aislada automáticamente antes de que se produzcan más daños.



Cynet Correlator™: Gestión de registros y correlación de eventos

Cynet Correlator™ recopila y correlaciona los datos de actividad y alertas, agrupándolos en incidentes procesables, proporcionando capacidades similares a las de SIEM.

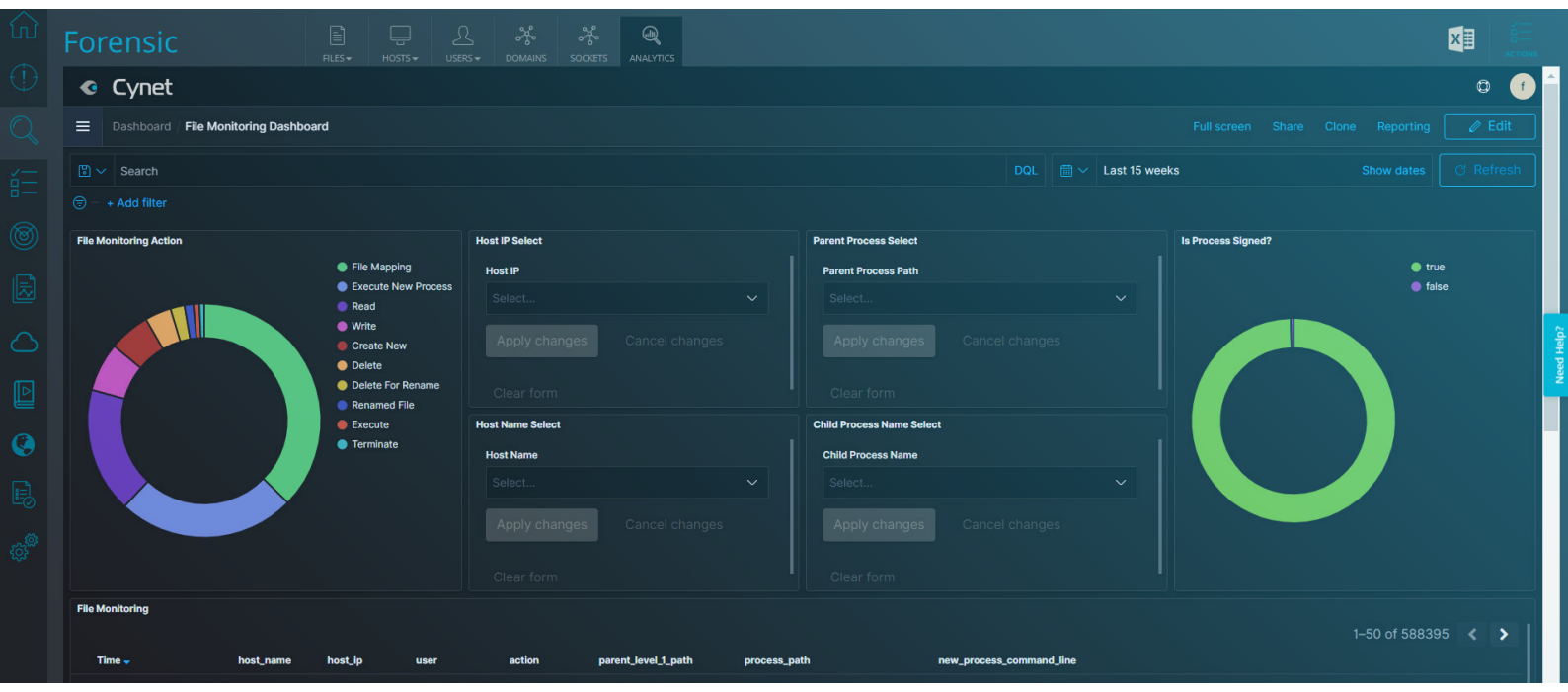
1. Gestión centralizada de registros (CLM)

La gestión centralizada de registros de Cynet recopila automáticamente los datos de registro prioritarios necesarios para descubrir rápidamente y con precisión las amenazas presentes en todo el entorno.

- Identifique las amenazas y las anomalías con herramientas intuitivas de análisis y visualización
- Simplifique los análisis forenses para investigar y descubrir los componentes ocultos de los ataques
- Ejecute informes personalizados que le ayudarán a evaluar y demostrar el cumplimiento de las normas del sector
- Aproveche las potentes filtros de búsqueda y consultas para obtener un análisis detallado y minucioso
- Conserve los datos de registro en Cynet CLM para facilitar la conformidad con los requisitos de cumplimiento

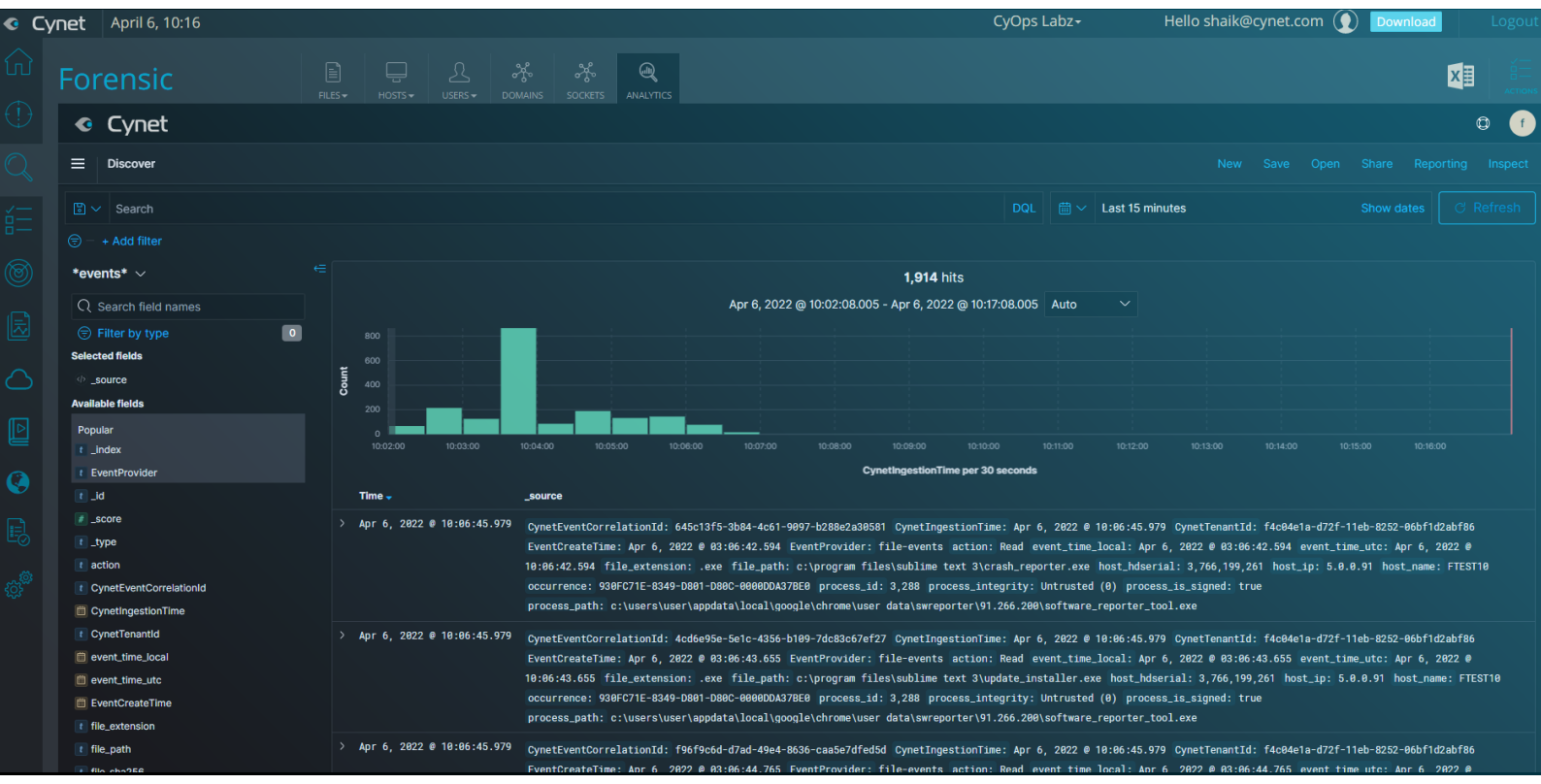
Analice visualmente los datos de registro con gráficos y cuadros de mando intuitivos

Cree gráficos y cuadros de mando fácilmente para elaborar la información de sus datos de registro. Los gráficos avanzados le permiten ver inmediatamente las anomalías y tendencias para que pueda localizar y resolver los problemas de manera rápida.



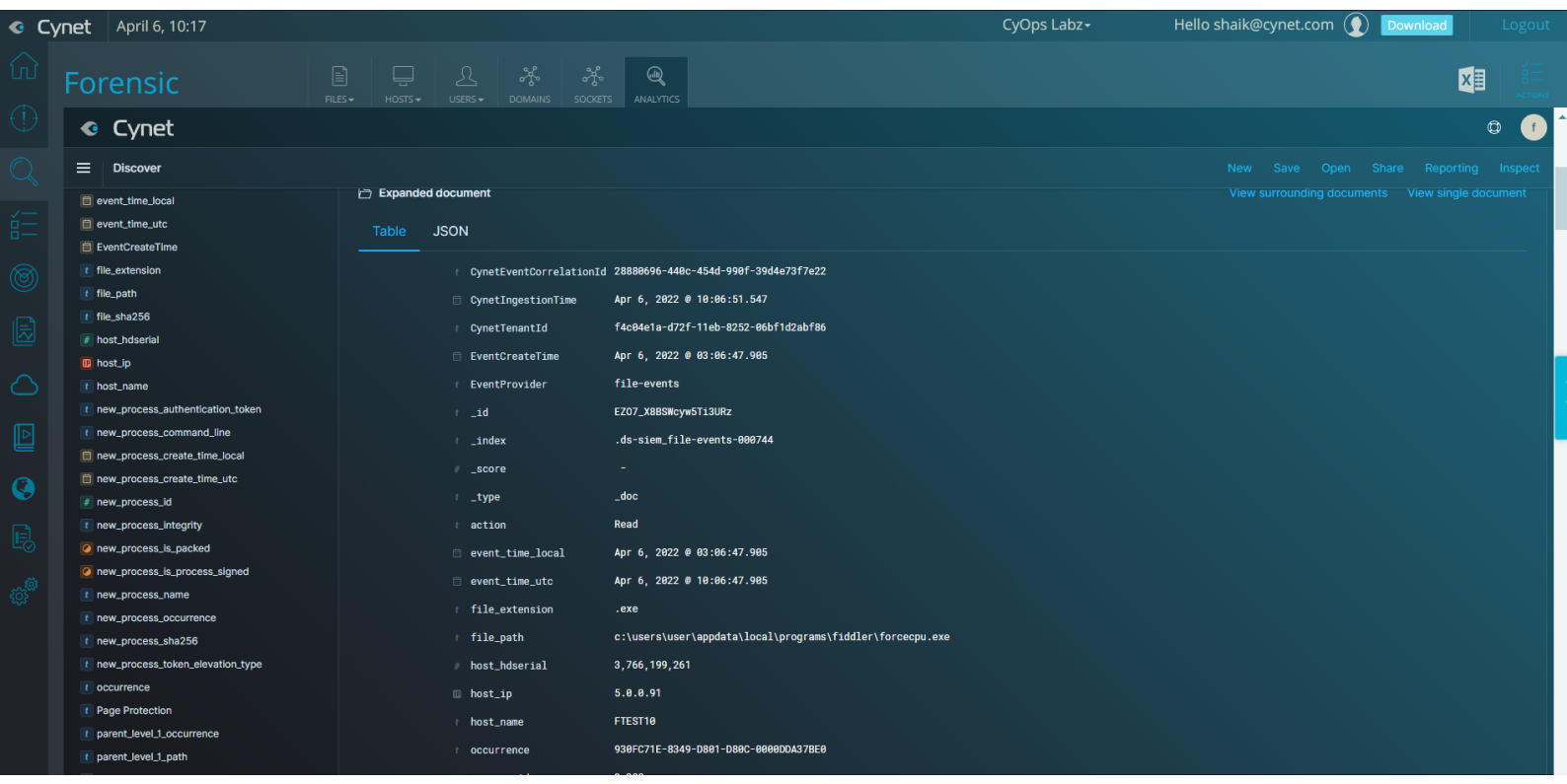
Analice los datos de registro mediante una interfaz de usuario intuitiva y coherente

Visualice, ordene, consulte, filtre y correlacione los eventos detectados en cortafuegos, Active Directory (AD), puntos de conexión y otros, utilizando un único panel de control que le permitirá conectar toda esta información y descubrir las amenazas sigilosas. Elimine el tiempo necesario para examinar múltiples registros no interconectados y para recopilar y correlacionar manualmente los hallazgos. Disponer de todos los datos de registro necesarios en un solo panel de control proporciona el acceso y la visibilidad que necesita, sin pasar por alto los datos críticos.



Profundice en los detalles de los datos de registro con un solo clic

Con sus datos de registro críticos integrados en Cynet CLM, puede ver información detallada de cada evento del registro con un solo clic. Con Cynet CLM no es necesario moverse entre múltiples fuentes de registro e interfaces. Acceda rápidamente a los datos de registro que necesita para su investigación, todo ello dentro de la consola de Cynet.



CyOps: Equipo de detección y respuesta gestionadas (MDR) 24/7

Cynet complementa su tecnología de protección autónoma contra vulneraciones con servicios de seguridad integrados, sin coste adicional. CyOps es un equipo de analistas de amenazas e investigadores de seguridad que aprovechan su experiencia y la ingente información sobre amenazas de que dispone Cynet para proporcionar diversos servicios a los clientes de Cynet, según las necesidades específicas de cada cliente y sus preferencias de seguridad, las 24 horas del día.

Control de alertas

El equipo de CyOps supervisa continuamente su entorno, todas las horas del día y a lo largo de todo el año. El equipo gestiona eventos, alertas, consultas de clientes e incidentes, y proporciona asimismo análisis de alertas y correlaciones con otros eventos que han activado una alerta de Cynet 360 AutoXDR™.

El equipo de CyOps se pondrá en contacto con usted de forma proactiva cuando se detecten determinadas alertas o eventos, y le indicará las acciones específicas que deben llevarse a cabo.

Caza de amenazas

CyOps busca continuamente nuevas amenazas emergentes para implementar Indicadores de Compromiso (IOC) y patrones en los mecanismos de Cynet 360 AutoXDR™. Estas acciones proactivas permiten a Cynet 36 AutoXDR™ 0 recopilar y analizar los eventos y alertar sobre ellos, al tiempo que dotan a la función forense de capacidad para evaluar el nivel de riesgo de una entidad.

Respuesta remota a incidentes (IR)

Los expertos en IR de CyOps trabajan en estrecha colaboración con la empresa afectada para resolver los incidentes lo más rápido posible. Este proceso incluye la creación de políticas personalizadas dentro de la plataforma Cynet 360 AutoXDR™ para alcanzar y analizar la amenaza, así como recomendaciones y soluciones para mitigar el impacto en el punto de conexión y en todo el entorno de TI y seguridad.

Informes sobre ataques

Los equipos de CyOps generan informes completos en respuesta a las preguntas de los clientes.

Informes sobre ataques. Ejemplo 1: Ataque de 13 segundos

El informe de investigación de amenazas de Cynet contiene un resumen a nivel ejecutivo, una descripción del análisis, incluyendo los procesos implicados, y los indicadores de compromiso asociados, sobre el “Ataque de los 13 segundos” en el que el malware compromete a un único servidor en 13 segundos.

EXECUTIVE SUMMARY

In this article, the Cynet Research team reveals a highly complex attack that runs for only 13 seconds by using several malwares and different tactics. From our analysis, the threat that we discovered within our investigation is name the **“ClipBanker” trojan.**

The attack flow contains several stages of LOLBins (Living Off the Land) abuse, masquerading, persistency, enumeration techniques, credential thieving, fileless attacks, and finally banking trojan activities.

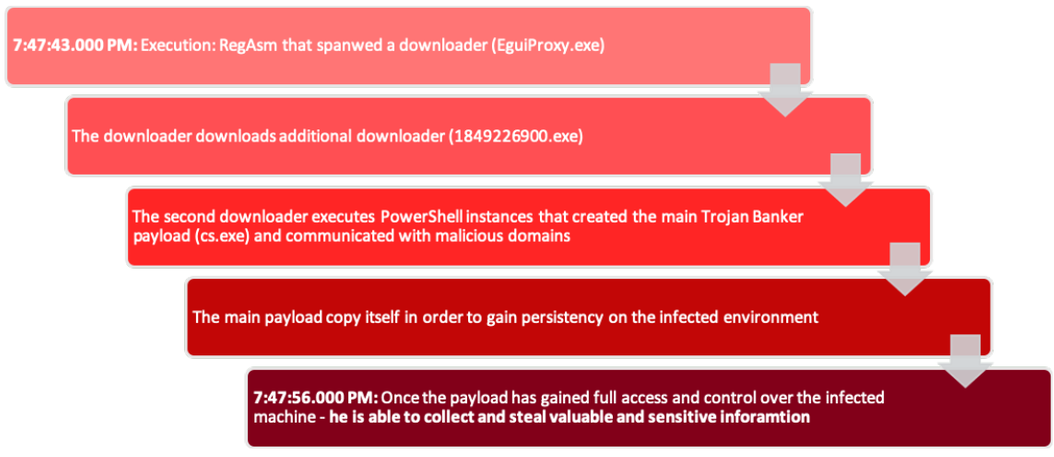
This attack is also using Fileless techniques in order to evade from security detections. Fileless attack has been a growing threat since 2017 and require highly sophisticated detection and prevention tools to detect and block. The most common Windows tools used in “Fileless” attacks are PowerShell, JS, VBA and WMI. PowerShell is a highly popular tool used for Fileless attack, because PowerShell commands can be executed natively on Windows without writing data to disk.

The ClipBanker Trojan is known as an information stealer and spy trojan, it aims to steal and record any type of sensitive information from the infected environment such as browser history, cookies, Outlook data, Skype, Telegram, or cryptocurrency wallet account addresses. The main goal of this threat is to steal confidential information.

The ClipBanker uses PowerShell commands for executing malicious activities. The thing that made the ClipBanker unique is its ability to record various banking actions of the user and manipulate them for its own benefit.

The distribution method of the ClipBanker is through phishing emails or through social media posts that lure users to download malicious content.

Cynet 360 is protecting your assets against this type of exploit.



Servicios avanzados de CyOps

Informe mensual de inteligencia sobre amenazas

Informe detallado sobre las amenazas de mayor gravedad detectadas por los agentes de Cynet360 desplegados en los entornos de nuestros clientes en todo el mundo. El informe completo incluye un resumen de las tendencias y los aspectos más destacados, así como actividades y recomendaciones de buenas prácticas para mejorar sus conocimientos informáticos.

Analista dedicado a CyOps

Un analista de CyOps con experiencia, asignado para supervisar personalmente su cuenta y servicios y ser su único punto de contacto con Cynet. Más allá de la supervisión proactiva 24/7 que recibe automáticamente del equipo de CyOps, el analista dedicado se centra en su entorno y sus necesidades.

Contrato de servicio de respuesta ante incidentes avanzado

Cobertura con capacidad de respuesta avanzada que se extiende más allá del entorno protegido por la plataforma Cynet AutoXDR™. Con el contrato de servicio de respuesta ante incidentes avanzado de Cynet, el equipo de respuesta ante incidentes de esta entidad está preparado para actuar las 24 horas del día, 7 días a la semana, en caso de que se produzca una vulneración en cualquier lugar de su entorno, para eliminar rápidamente las amenazas y volver a poner en marcha su negocio.

Integraciones de terceros

La integración de Cynet con sus tecnologías de seguridad actuales y su infraestructura es una tarea fácil. Los ingenieros de integración de Cynet pueden desarrollar integraciones para la mayoría de las tecnologías con la plataforma Cynet 360 AutoXDR™ utilizando lenguajes de programación comunes y una API RESTful, e incluyendo tecnologías como SIEM (gestión de eventos e información de seguridad), *ticketing* (gestión de incidencias y reclamaciones**)**, gestión de casos, cortafuegos, y mucho más.

SOPORTE DE SO

WINDOWS (32/64 BITS)

- Windows XP SP3
- Windows Vista
- Windows 7
- Windows 8 y 8.1
- Windows 10
- Windows Server 2003 SP2
- Windows Server 2008 / 2008 R2
- Windows Server 2012 / 2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

LINUX (32/64 BITS)

- Red Hat 6.4+
- Fedora 21+
- Ubuntu 14.04+
- CentOS 6.7+
- SUSE 12.0+
- Debian 6.0+

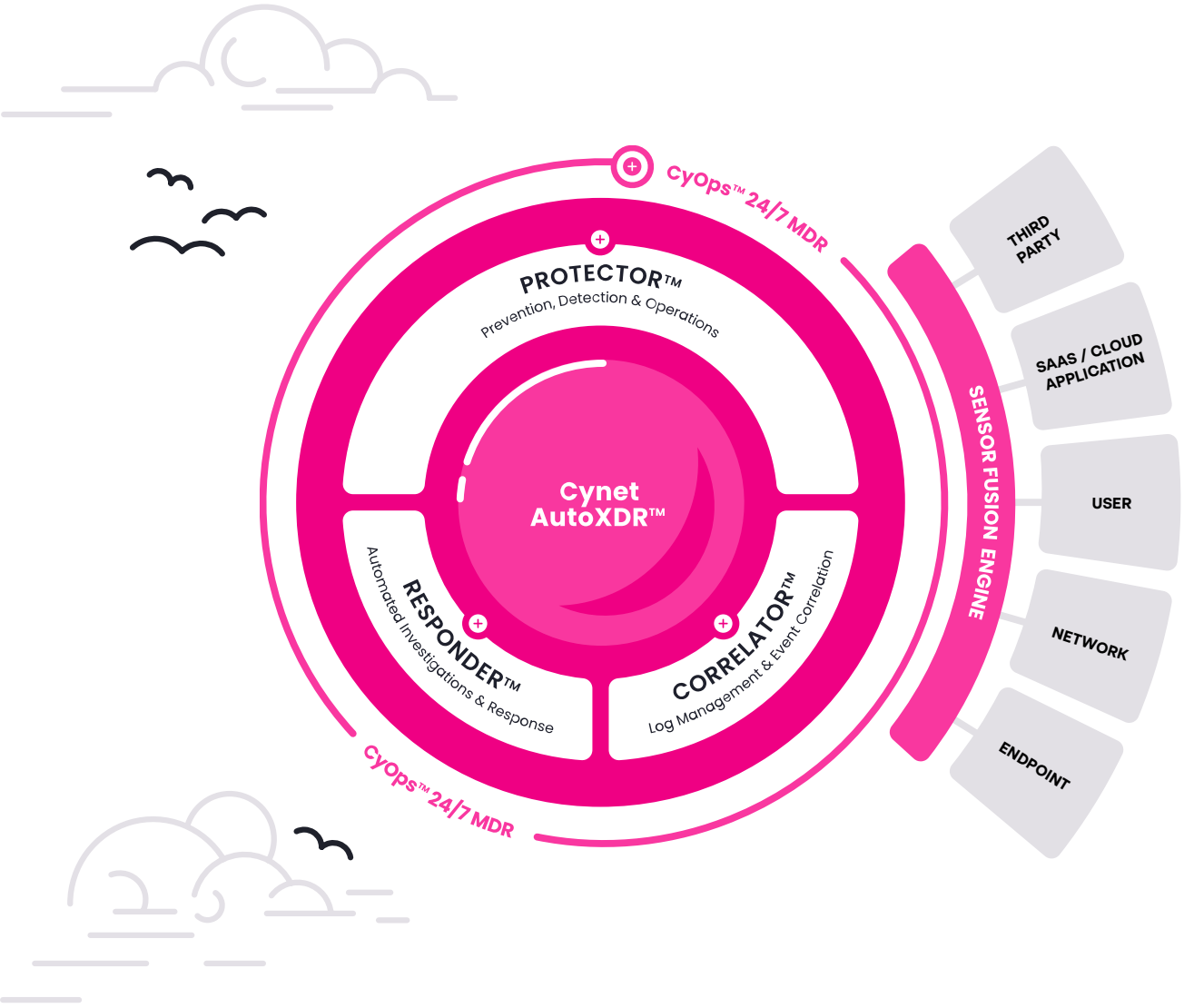
MAC (64 BITS)

- OS X Mavericks
- OS X Yosemite
- OS X El Capitan
- MacOS Sierra
- MacOS High Sierra
- MacOS Mojave
- MacOS Catalina

ACERCA DE NOSOTROS

La plataforma XDR de Cynet, automatizada de forma nativa de extremo a extremo y respaldada por un servicio MDR las 24 horas del día, ha sido diseñada para permitir a los equipos de seguridad de TI lograr una protección completa y eficaz, independientemente de sus recursos, del tamaño del equipo y de su capacidad técnica.

Cynet ofrece las siguientes capacidades de prevención y detección: EPP (plataformas de protección de puntos de conexión), EDR (detección y respuesta en puntos de conexión), NDR (detección y respuesta de red), tecnología de engaño, reglas de UBA (análisis del comportamiento del usuario) y CSPM (postura de seguridad en la nube), junto con la correlación de alertas y actividades y amplias capacidades de automatización de respuestas.



Nuestra visión es permitir a los equipos de seguridad que operen la ciberseguridad en piloto automático para centrar sus recursos en la gestión de la seguridad, en lugar de dedicar su tiempo a la gestión de incidencias.

Devuelva la cordura a la ciberseguridad con un nuevo enfoque que hace que la protección de su organización sea fácil y sin estrés.