Guía esencial de la 3.ª ronda de evaluaciones MITRE ATT&CK

Este libro electrónico ofrece una visión comparativa de los resultados obtenidos por los distintos proveedores en una serie de indicadores y proporciona directrices para seguir analizando los datos. Incluye descripciones clave de la metodología de pruebas de MITRE, describe las herramientas que proporciona MITRE para visualizar y comparar los resultados y señala aspectos concretos que le ayudarán a determinar qué proveedor se ajusta mejor a las necesidades de su organización en materia de seguridad del endpoint.

paloalto® NETWORKS | CORTEX® XDR BY PALO ALTO NETWORKS

Introducción

Si queremos protegernos y evitar las ciberamenazas más sofisticadas e ingeniosas de hoy en día, antes tenemos que conocer a quien se oculta detrás del teclado. Para combatir las amenazas avanzadas persistentes (APT, por sus siglas en inglés), en las que el comportamiento de los ciberdelincuentes cambia constantemente, los proveedores necesitan un formato objetivo que permita poner a prueba sus capacidades frente a las tácticas, técnicas y procedimientos (TTP, por sus siglas en inglés) que se utilizan en el panorama de amenazas actual.

Las evaluaciones MITRE ATT&CK® ofrecen justo eso, pues analizan con eficacia la capacidad de las soluciones de detección y respuesta en el endpoint (EDR, por sus siglas en inglés), así como de los proveedores de detección y respuesta ampliadas (XDR) y de sus productos, de detectar y combatir las secuencias de ataque reales.

Por tercer año consecutivo, Palo Alto Networks ha sido uno de los proveedores con mejores resultados en las evaluaciones MITRE ATT&CK, con una protección contra amenazas del 100 % y una visibilidad de la detección del 97 %, sin necesidad de cambiar la configuración.[1]

En términos generales, estos son los resultados que obtuvo Cortex XDR frente a los TTP utilizados por Carbanak y FIN7:

- Bloqueo del 100 % de los ataques en la prueba de protección, dirigidos a endpoints tanto de Windows® como de Linux.
- Visibilidad del 97 % de las técnicas de ataque.
- Las mejores tasas de detección de entre todas las soluciones con una puntuación de protección perfecta.
- Detección de análisis (que MITRE define como las detecciones que proporcionan contexto adicional más allá de la telemetría) del 86 %, según las técnicas de ataque utilizadas en la prueba.
- 80 % de detecciones a nivel de técnica (el tipo de detección con una valoración más alta en la prueba).
- La tasa global combinada de detección y protección más alta de la prueba.

En la prueba de protección, Cortex XDR bloqueó el

100 %

de los ataques a endpoints tanto de Windows como de Linux

CORTEX XDR BY PALO ALTO NETWORKS

Descripción general de la evaluación

En la tercera ronda de las evaluaciones MITRE ATT&CK, MITRE puso a prueba una mayor cantidad de proveedores que los dos años anteriores, lo que demuestra una vez más la importancia que tienen en el mercado los estudios realizados por terceros para ofrecer orientaciones objetivas útiles a la hora de elegir soluciones de seguridad.

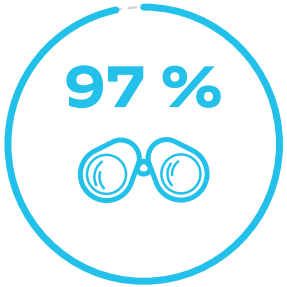
Para los proveedores que participan, las pruebas son una oportunidad de detectar áreas susceptibles de mejora (por ejemplo, les permiten actualizar las reglas de prevención, detección y respuesta en que se basan las políticas de seguridad). Aunque no se establece una clasificación de los proveedores ni se otorgan puntuaciones globales que permitan compararlos entre sí, las pruebas MITRE ATT&CK proporcionan un resumen independiente de las distintas metodologías utilizadas por los profesionales de la seguridad para detectar y prevenir las campañas de ataque más sofisticadas.

En esta ocasión, las pruebas constaron de 20 pasos y 174 pruebas secundarias tanto en sistemas operativos Windows como Linux, y participaron en ellas 29 proveedores, que se sometieron a los TTP utilizados por los grupos de ciberdelincuencia Carbanak y FIN7.

¿Qué ha cambiado este año?

En la tercera ronda, aproximadamente la mitad de los proveedores participaron en una parte de la prueba centrada en funciones de protección que abarcaban tanto Windows como Linux, con 10 pasos que ponían a prueba los distintos productos para ver si bloqueaban activamente los ataques. Sabiendo que contamos con un excelente historial de prevención de amenazas y con una amplia gama de herramientas para endpoints Linux, decidimos participar en las pruebas de protección.

Los resultados son claros: Cortex® XDR™ **bloqueó todos los ataques tanto en Linux como en Windows, además de ofrecer la tasa de detección más alta y las detecciones de mejor calidad** de entre todos los proveedores (véase la figura 3). Al destacar la protección del endpoint con una prueba independiente, MITRE subraya la importancia de ir más allá de las funciones de detección tradicionales y demuestra que conviene combinar una plataforma de protección del endpoint (EPP, por sus siglas en inglés) con la EDR para ofrecer una solución de seguridad del endpoint más completa.



Cortex XDR logró una visibilidad del 97 %
de las técnicas de ataque, las mejores tasas de detección de entre todas las soluciones con una puntuación de protección perfecta

CORTEX XDR BY PALO ALTO NETWORKS

El método de MITRE

MITRE se centra en describir cómo se producen las detecciones, en lugar de asignar puntuaciones a las funciones de los proveedores, y organiza en categorías cada detección y captura.[2] A continuación, las detecciones se organizan según cada técnica. Las técnicas pueden tener más de una detección si la función detecta la técnica de formas diferentes y las detecciones que observan se incluyen en los resultados.

Aunque MITRE hace todo lo posible por capturar las distintas detecciones, podría haber funciones capaces de detectar procesos de formas que MITRE no haya sido capaz de capturar. Para que se tenga en cuenta una detección para una técnica determinada, se debe aplicar a dicha técnica en concreto. Por ejemplo, el hecho de que una detección se corresponda con una técnica determinada en un paso o paso secundario no implica necesariamente que se corresponda con todas las técnicas de dicho paso. Para demostrar la detección en cada categoría, MITRE requiere que se proporcione la prueba de la detección, pero es posible que no se muestren públicamente todos los datos de la detección, en especial si se trata de información confidencial.

Para determinar la categoría adecuada de una detección, MITRE revisa las capturas de pantalla proporcionadas, los apuntes tomados durante la prueba, los resultados de las preguntas de seguimiento formuladas al proveedor y los comentarios del proveedor sobre los resultados provisionales. Asimismo, evalúan los procesos de forma independiente en un entorno de prueba diferente y revisan las detecciones de las herramientas de código abierto y los artefactos forenses. Estas pruebas determinan qué se considera una detección para cada técnica.

Una vez organizadas las detecciones en categorías, MITRE calibra las categorías entre todos los proveedores para buscar posibles discrepancias y garantizar que se apliquen de forma coherente. En última instancia, la decisión de qué categoría aplicar se basa en el análisis humano y, por lo tanto, está sujeta a la discreción y el sesgo inherentes a todo análisis humano —si bien se hace todo lo posible para evitar el riesgo de sesgo mediante la estructuración del análisis, tal como se describe en esta guía—.

¿Sabía que...?

En 2013, MITRE ATT&CK dio sus primeros pasos con el experimento Fort Meade Experiment (FMX) de MITRE, en el que los investigadores se pusieron en la piel de los adversarios utilizando sus tácticas y técnicas

Cómo utilizar MITRE para evaluar las soluciones EDR

Para las organizaciones que estén valorando distintos proveedores y soluciones EDR, los resultados de MITRE permiten comparar los distintos niveles de seguridad que brindan los proveedores participantes, todo ello con un léxico común para garantizar la paridad y continuidad en toda la evaluación.

¿Cómo ayudan las pruebas de MITRE ATT&CK a los proveedores de soluciones como nosotros a diseñar una estrategia de defensa? Para Palo Alto Networks, participar en las pruebas de MITRE ATT&CK supone la oportunidad de someterse al análisis de un tercero neutral y objetivo para el que se utilizan sofisticadas secuencias de ataque actuales, lo que nos proporciona información constructiva sobre cómo crear soluciones de prevención y detección más eficaces.

Al utilizar los TTP modernos de grupos de ataque como Carbanak y emular la situación de ataque en un entorno controlado —el rango cibernético proporcionado por MITRE Engenuity—, los proveedores de soluciones pueden evaluar su rendimiento y determinar en qué áreas deberían mejorar. Los datos relativos al rendimiento resultantes de las pruebas otorgan información sobre modificaciones de los productos o las soluciones y orientan sobre cómo mejorar los pasos que no hayan obtenido los resultados deseados.

El ciberdelincuente

Los atracos a bancos modernos no son mucho más ingeniosos que las clamorosas campañas de ataque con APT perpetradas por Carbanak contra el sector financiero, que entre 2013 y 2018 se embolsaron en torno a 1000 millones de dólares mediante ataques a casi 100 instituciones financieras de todo el mundo. A veces se usan los nombres FIN7 y Carbanak indistintamente, porque en ambos casos se utiliza el malware Carbanak, pero parece que FIN7 y Carbanak son dos grupos diferentes y, por lo tanto, se analizan por separado.

El malware Carbanak se embolsó un botín de

1000 millones de dólares

en ataques al sector financiero en los que participaron ciberdelincuentes de Rusia, Ucrania, Europa y China

Principalmente mediante el envío de mensajes de correo electrónico de *spear phishing* al personal de los bancos, Carbanak consiguió infectar sistemas, robar credenciales, recopilar información (por ejemplo, mediante la interceptación de las pantallas de los empleados) y hacerse pasar por miembros del personal para robar dinero de distintas formas, como las siguientes:

- Transferencias a cuentas fraudulentas mediante los sistemas de banca online.
- Realización de pagos electrónicos y transferencias a cuentas en Estados Unidos y China.
- Inflado de saldos y transferencia de las diferencias mediante transacciones fraudulentas.
- Control de cajeros automáticos para que dispensen dinero en efectivo a horas determinadas y recogida de dicho dinero mediante cómplices.

Información general: emulación de Carbanak/FIN7 de MITRE

- 2 situaciones de ataque completas (una por atacante)
- 20 fases de ataque
- 174 pasos secundarios con 70 técnicas diferentes
- Evaluación de la protección (10 pasos)

Para ver las técnicas utilizadas en la evaluación de Carbanak+FIN7 en ATT&CK Navigator, MITRE ofrece el archivo de capa aquí.

Credential Access	Discovery	Lateral Movement	Collection
Account Manipulation	Account Discovery	AppleScript	Audio Capture
Bash History	Application Window Discovery	Application Deployment Software	Automated Collection
Brute Force	Browser Bookmark Discovery	Component Object Model and Distributed COM	Clipboard Data
Credential Dumping	Domain Trust Discovery	Exploitation of Remote Services	Data from Information Repositories
Credentials from Web Browsers	File and Directory Discovery	Internal Spearphishing	Data from Local System
Credentials in Files	Network Service Scanning	Logon Scripts	Data from Network Shared Drive
Credentials in Registry	Network Share Discovery	Pass the Hash	Data from Removable Media
Exploitation for Credential Access	Network Sniffing	Pass the Ticket	Data Staged
Forced Authentication	Password Policy Discovery	Remote Desktop Protocol	Email Collection
Hooking	Peripheral Device Discovery	Remote File Copy	Input Capture
Input Capture	Permission Groups Discovery	Remote Services	Man in the Browser
Input Prompt	Process Discovery	Replication Through Removable Media	Screen Capture

Carbanak FIN7 Carbanak+FIN7

Metodología de la 3.ª ronda de evaluaciones MITRE

El entorno

Las pruebas se realizaron en Microsoft Azure Cloud. Se proporcionó a cada proveedor dos entornos idénticos, cada uno de ellos formado por ocho hosts en los que instalar el software de cliente. Estos dos entornos se utilizaron, respectivamente, para las pruebas de protección y las específicas de detección. Los proveedores también tenían la posibilidad de instalar software de servidor en una máquina virtual (MV) ya presente en el entorno o importar una MV de ser necesario. De forma predeterminada, las MV de Azure eran B4MS estándar, cada una de ellas con cuatro vCPU y 16 GB de memoria. Cada proveedor tenía acceso administrativo completo a los hosts instanciados para ellos.

El acceso a la VPN hacía posible la conectividad con el entorno y las contraseñas se compartían mediante métodos fuera de banda. Había un solo servidor VPN por entorno y los proveedores utilizaban RDP o SSH en los demás lugares del entorno. Solo se podía acceder a los hosts dentro de la VPN. No se les asignaban direcciones IP públicas mediante Azure, pero sí que tenían acceso a Internet.

Continúa en la página siguiente >

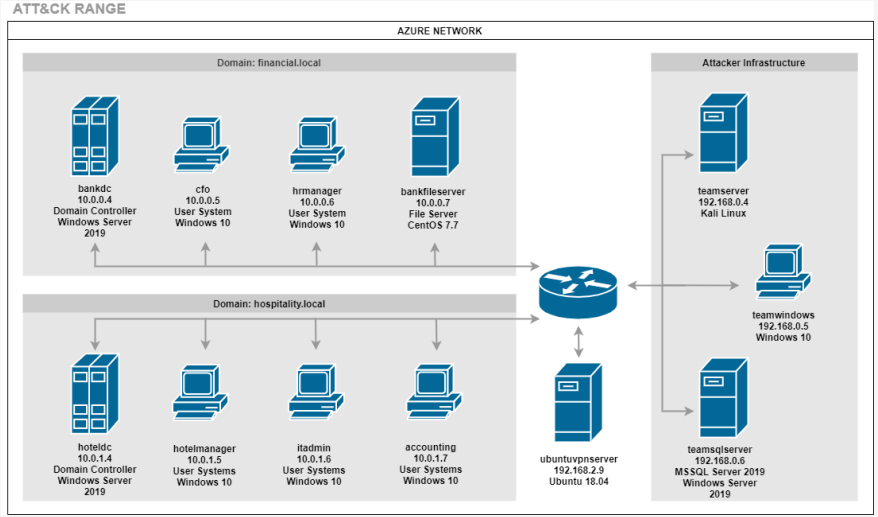


Figura 1: Rango de ATT&CK - Red de Azure

Entorno de prueba de Carbanak/FIN7

Hosts objetivo:

- Windows Server 2019
- Windows 10
- CentOS 7.7

Aunque cada participante puede utilizar su propio método y su propia terminología para detectar el comportamiento del atacante y protegerse de este, MITRE resume los respectivos datos en dos grandes categorías para evaluar los productos con términos similares: «Principal» y «Modificador».

Con relación a la cantidad de información contextual que se proporciona al usuario, cada detección o protección recibe una sola designación de la categoría «Principal», mientras que es posible proporcionar una o varias designaciones de la categoría «Modificador» para describir el evento más a fondo.

En la evaluación de Carbanak+FIN7, hay *seis categorías principales de detección*, que representan la cantidad de información contextual proporcionada al analista, y *tres categorías principales de protección*.

Continúa en la página siguiente >

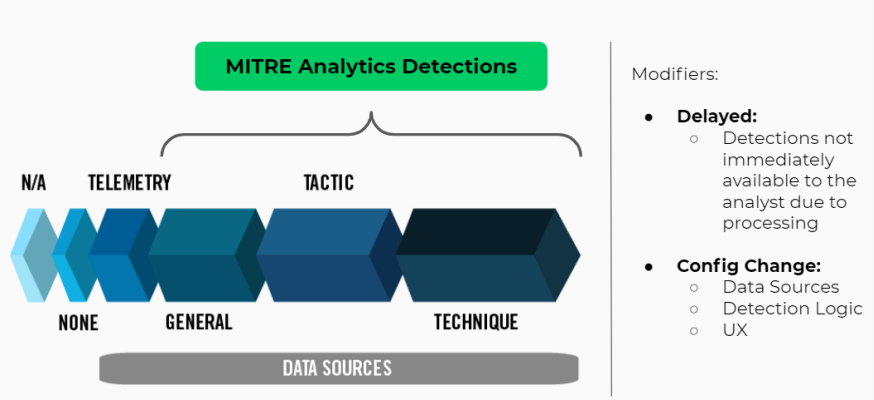


Figura 2: Categorías de detección de Carbanak/FIN7

Categorías de detección

No procede: el proveedor no tenía visibilidad del sistema sometido a las pruebas. Antes de la evaluación, el proveedor debe especificar en qué sistemas no ha implementado un sensor para poder aplicar la categoría «No procede» a los pasos pertinentes.

Ninguna: no se han proporcionado datos dentro de la función relacionados con el comportamiento analizado que satisfagan los criterios de detección asignados. No se han incluido modificadores, notas ni capturas de pantalla.

Telemetría: la función ha recopilado datos mínimamente procesados que demuestran que se han producido eventos específicos del comportamiento analizado y satisfacen los criterios de detección asignados. Debe haber pruebas que demuestren sin lugar a dudas que el comportamiento tuvo lugar y deben estar relacionadas con el mecanismo de ejecución. Estos datos deben ser visibles de forma nativa dentro de la herramienta y pueden incluir información extraída del endpoint.

General: hay datos procesados que especifican que se han producido uno o varios eventos maliciosos/anómalos relacionados con el comportamiento analizado. Apenas se proporcionan datos sobre por qué tuvo lugar la acción (táctica) o cómo se llevó a cabo (técnica).

Táctica: hay datos procesados que especifican la táctica de ATT&CK o proporcionan un nivel de información equivalente a los datos recopilados por la función. Se proporciona al analista información sobre la posible intención de la actividad o se ayuda a conocer el motivo que podría llevar a realizar la actividad. Para que se considere una detección, tiene que haber más de una etiqueta sobre el evento que identifique la táctica de ATT&CK y debe haber una conexión clara entre la descripción de la táctica y la técnica observada en la prueba.

Continúa en la página siguiente >

Técnica: hay datos procesados que especifican la técnica o técnica secundaria de ATT&CK o proporcionan un nivel de información equivalente a los datos recopilados por la función. Se proporciona al analista información sobre cómo se llevó a cabo la acción o se ayuda a saber qué se hizo exactamente (p. ej., funciones de accesibilidad o vaciado de credenciales). Para que se considere una detección, tiene que haber más de una etiqueta sobre el evento que identifique la ID de la técnica de ATT&CK (TID, por sus siglas en inglés) y debe haber una conexión clara entre la descripción de la técnica y la técnica observada en la prueba.

Categorías de protección

Se han utilizado categorías de protección para especificar si se ha observado una protección en la emulación del ataque y si ha sido necesario un mensaje de usuario para confirmar la actividad de bloqueo. Las categorías pueden cambiar, según las conclusiones que se saquen en la prueba.

No procede: el proveedor no ha implantado funciones de protección en el sistema sometido a las pruebas. Antes de la evaluación, el proveedor debe especificar en qué sistemas no ha implementado un sensor para poder aplicar la categoría «No procede» a los pasos pertinentes.

Ninguna: la técnica observada en la prueba no se bloqueó o la técnica no tuvo éxito y el usuario no tiene pruebas de que la función haya bloqueado la actividad.

Bloqueada: la técnica observada en la prueba ha sido bloqueada y se ha informado explícitamente al usuario de que la función ha bloqueado la actividad.

Continúa en la página siguiente >

Tipos de detección de la categoría «Modificador»

MITRE diferencia entre varios tipos de detección para ofrecer más información contextual en cuanto a las funciones que ofrece un proveedor, de modo que los usuarios puedan sopesar, puntuar o clasificar los tipos de detección según sus necesidades y decidir qué opción les resulta más ventajosa.

Cambio de configuración: la configuración de la función se ha modificado desde el comienzo de la evaluación. Se puede hacer para demostrar que es posible recopilar o procesar más datos. El modificador «Cambio de configuración» se puede aplicar junto con más modificadores que describan la naturaleza del cambio, como los siguientes:

- **Fuentes de datos:** cambios realizados en la recopilación de información por parte del sensor.
- **Lógica de detección:** cambios realizados en la lógica de procesamiento de datos.
- **UX (experiencia del usuario):** cambios relacionados con la visualización de datos que ya se recopilaban pero no eran visibles para el usuario.

Retrasada: el analista no tiene acceso de inmediato a la detección porque el procesamiento adicional no está disponible debido a algún factor que ralentiza o retrasa su presentación al usuario (por ejemplo, el procesamiento adicional o sucesivo produce una detección para la actividad). La categoría «Retrasada» no se aplica para el procesamiento de datos automatizado normal ni para el procesamiento rutinario que conlleva una espera mínima para que el usuario visualice los datos, ni se aplica por problemas de conectividad o rango que no guarden relación con la función en sí. Este modificador siempre se aplicará con otros que describan más a fondo la naturaleza del retraso.

Cortex XDR frente a Carbanak+FIN7: nuestros resultados

MITRE se centra en analizar cómo se producen las detecciones, en lugar de asignar puntuaciones a las funciones de los proveedores. Además, organiza en categorías cada detección y captura y, a continuación, organiza las detecciones según cada técnica de ataque. Cada técnica puede tener más de una detección si una solución de seguridad detecta una técnica de varias formas diferentes. Todas las detecciones observadas se incluyen en los resultados de la prueba.

MITRE combinó las técnicas de ataque detectadas por telemetría (lo que significa que se necesitó poco procesamiento para detectar la técnica) y las detecciones que exigían un procesamiento analítico para determinar la visibilidad para llegar a la tasa de detección global de las 174 técnicas de ataque a las que se sometieron los proveedores que participaron en las pruebas.

El valor añadido de Cortex XDR: los datos no mienten

Cortex XDR, la primera plataforma XDR del sector, integra los datos de los endpoints, la red, la nube y de terceros para detener los ataques sofisticados. Tal como demuestran los excelentes resultados que hemos obtenido en las evaluaciones MITRE ATT&CK durante tres años consecutivos, Cortex XDR garantiza un alto rendimiento en protección, detección y visibilidad, los tres pilares de una solución de seguridad del endpoint holística y de primera.

Cortex XDR aplica técnicas de análisis de comportamiento y aprendizaje automático para proporcionar detecciones más fiables. Recopila y agrupa un amplio conjunto de datos, como logs de los endpoints Cortex XDR, cortafuegos de nueva generación, Prisma® Access, proveedores de identidad y un largo etcétera. Cortex XDR crea un perfil con el comportamiento previsto del usuario para señalar las anomalías que apunten a un posible ataque. El análisis de comportamiento aplica el aprendizaje automático y los análisis estadísticos a datos enriquecidos para destapar técnicas y tácticas de ataque con menos falsos positivos de los que generan las reglas de detección tradicionales.

Cortex XDR: resultados extraordinarios durante tres años seguidos

- **2018:** la mayor cobertura de técnicas de ataque
- **2019:** cobertura general de las técnicas de ataque sin rival en el mercado
- **2020:** mejor combinación de detección y prevención

CORTEX XDR BY PALO ALTO NETWORKS

Como Cortex XDR combina protección, detección analítica y visibilidad, se identifica con precisión el comportamiento anómalo, lo cual acelera el proceso de clasificación y reduce el tiempo de permanencia y, por consiguiente, el movimiento lateral dentro de una red.

La protección es la clave

Cortex XDR no solo bloqueó todos los ataques en las primeras pruebas de protección de MITRE ATT&CK de la historia, sino que además integró los datos de los logs proporcionados por los cortafuegos de nueva generación de Palo Alto Networks para aumentar la fiabilidad de la detección. Y como protección equivale a prevención, el adversario no consiguió llevar a cabo el ataque, con lo que el tiempo de permanencia fue nulo. Además, al detener la amenaza, se reduce el mal de alertas, pues los pasos de seguimiento no tienen lugar y se interrumpe la secuencia del ciclo de vida del ataque.

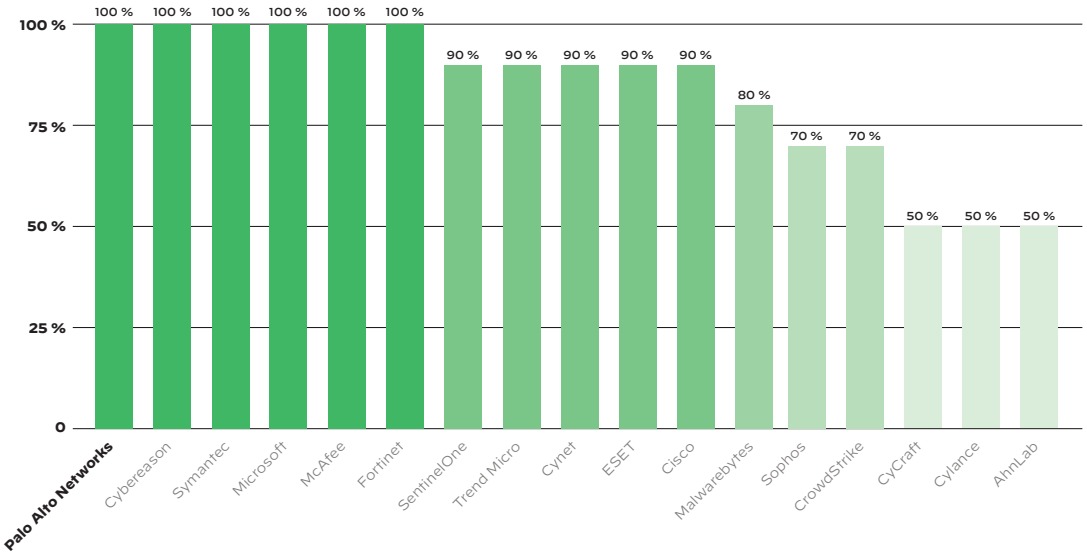


Figura 3: En la fase de protección, Cortex XDR bloqueó el 100 % de los ataques a sistemas tanto de Linux como de Windows

CORTEX XDR BY PALO ALTO NETWORKS

Cortex XDR: el mejor rendimiento global

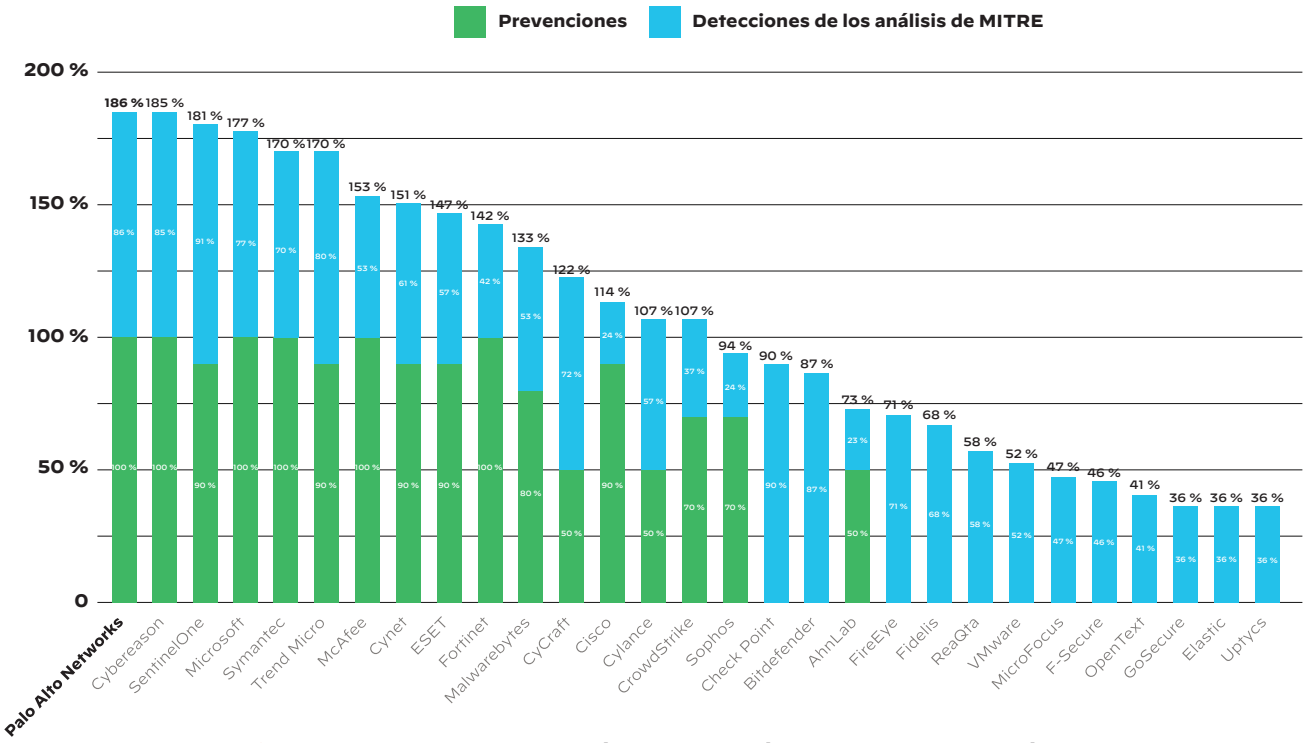


Figura 4: La mejor combinación de detección analítica y protección

CORTEX XDR BY PALO ALTO NETWORKS

En una solución EDR, la eficacia de la protección o prevención es clave, pues reduce de forma considerable el trabajo de los analistas de seguridad para que dispongan de más tiempo para la investigación y la búsqueda de amenazas. Una buena detección garantiza la visibilidad de la secuencia de ataque y ofrece los análisis adecuados para filtrar y señalar las anomalías que requieren una investigación más a fondo. La visibilidad es la base de la prevención y la detección, pero por sí sola muchas veces solo genera ruido. Cuando se utilizan los análisis para establecer correlaciones y dar sentido a la telemetría procedente de distintas fuentes, las campañas de ataque se ven con más claridad.

Los cambios de configuración

MITRE da a los proveedores de soluciones una «segunda oportunidad» si un paso de la prueba no ha generado la detección deseada. Estas segundas oportunidades se denominan «cambios de configuración». De este modo, los proveedores de seguridad pueden mejorar su detección de una técnica que no habían detectado con su configuración inicial. Por lo tanto, un cambio de configuración no es más que una detección que ha sido posible gracias a un cambio realizado para conseguir un resultado mejor. MITRE brinda esta oportunidad a los proveedores para que estos puedan validar el modo en que los cambios realizados en una solución mejoran la seguridad.

En el mundo real, cuando un ciberdelincuente ejecuta un paso de su cadena de ataque sin que se lo detecte, no existe una segunda oportunidad para cambiar la configuración y capturar al adversario. Por este motivo, pensamos que, a la hora de comparar los resultados, es mejor excluir las detecciones (véase la figura 5) que sean consecuencia directa de un cambio de configuración.

Veamos varios ejemplos de cambios de configuración[3]:

- Se crea una nueva regla, se habilita una regla preexistente o se modifican los niveles de sensibilidad (por ejemplo, las listas de bloqueados) para que se activen correctamente en una nueva prueba. Estos cambios se etiquetarían con el modificador «Cambio de configuración-Lógica de detección».
- Se recopilan en el back-end datos sobre la creación de cuentas, pero no se muestran al usuario de forma predeterminada. El proveedor modifica una configuración interna para permitir que la telemetría sobre la creación de cuentas se muestre en la interfaz de usuario, así que se daría a la técnica de creación de cuentas una detección de telemetría y el modificador «Cambio de configuración-Experiencia del usuario».

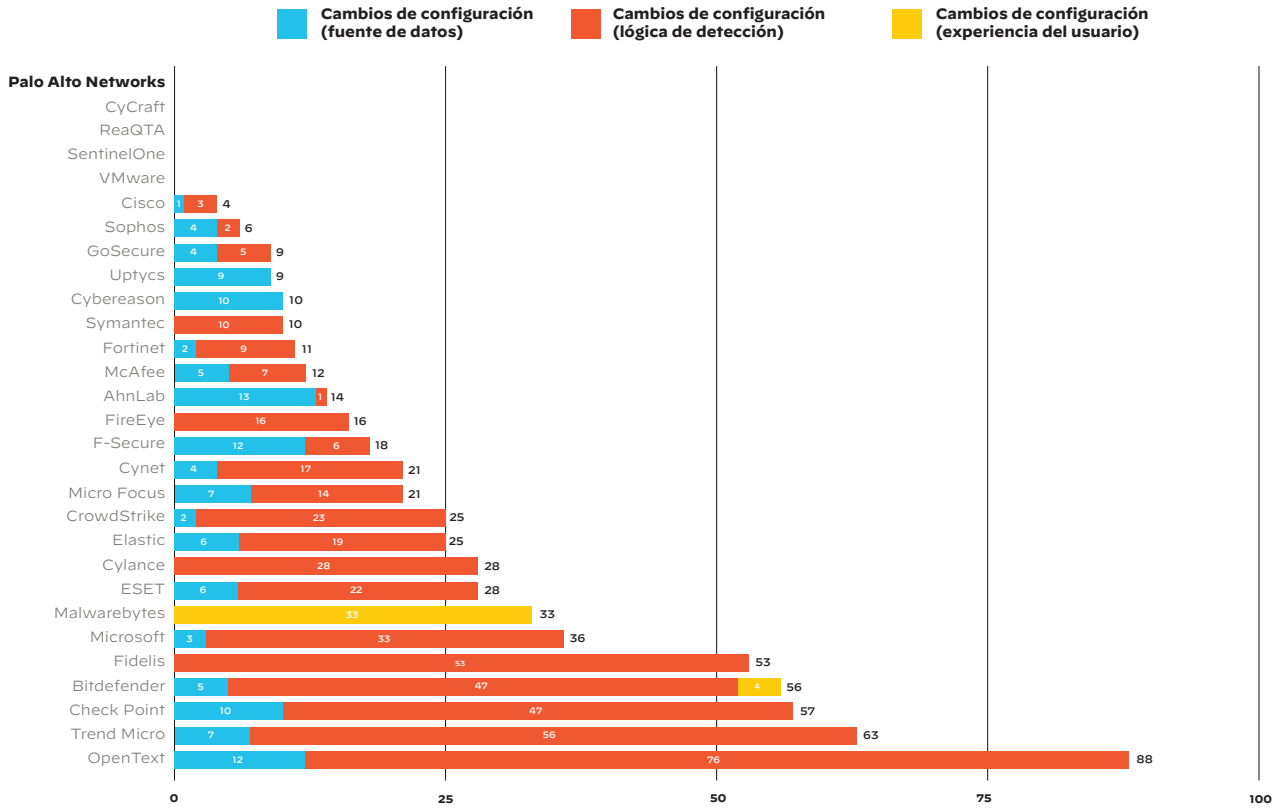


Figura 5: Número de cambios de configuración por proveedor en la tercera ronda de evaluaciones

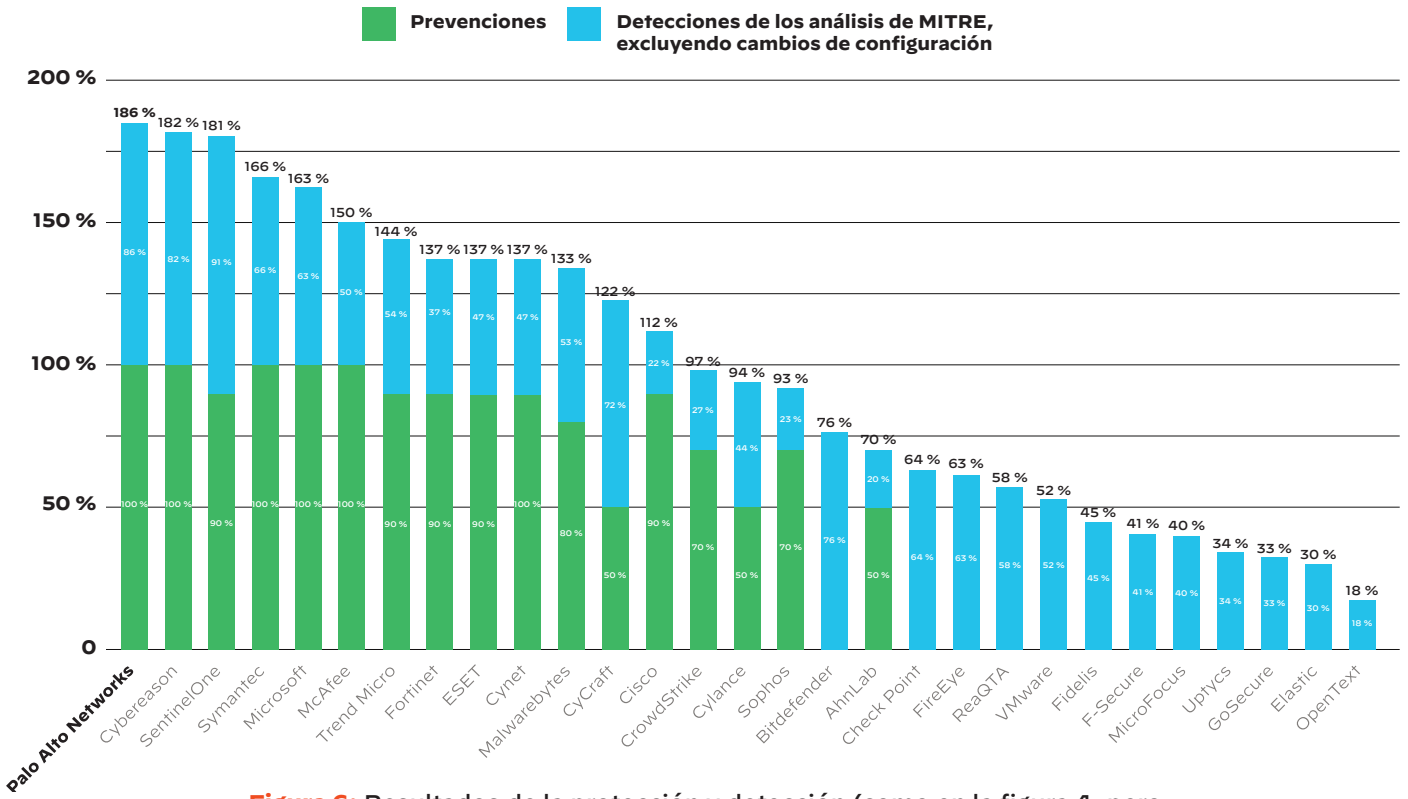


Figura 6: Resultados de la protección y detección (como en la figura 4, pero se excluyen los resultados de detección logrados con un cambio de configuración)

Las cifras por sí solas no bastan

Al examinar los resultados de MITRE, es importante observar las capturas de pantalla del producto para tener una idea más clara de la información que recibe el analista de seguridad.

Por ejemplo, Cortex XDR es la única solución unificada capaz de establecer correlaciones entre los datos de la red, los endpoints y de terceros, agruparlos en un mismo lugar mostrando las causalidades y, a continuación, aplicar análisis para detectar anomalías en la información que se desprende de esos datos agrupados. Podemos ver un ejemplo en la captura de pantalla de Cortex XDR que muestra el paso 5.C.2 de la evaluación (figura 7). En este paso, observamos un ataque en cadena detallado con una visualización que abarca varios hosts y muestra cuándo realizó el atacante un movimiento lateral de Linux a Windows mediante el bloque de mensajes del servidor (SMB, por sus siglas en inglés). Se muestran agrupados los datos procedentes de los endpoints y de las redes. Cortex XDR detectó la técnica utilizando nuestro motor de análisis en todo el conjunto de datos.

Otro ejemplo muestra el paso 17.A.6 de la evaluación (figura 8), donde podemos observar una inyección de código mediante llamada a procedimiento remoto (RPC, por sus siglas en inglés) en una sesión HTTPS cifrada. Este resultado se logra a pesar del canal cifrado mediante la supervisión de la llamada RPC como fuente de datos, aunque se enmascare mediante un cambio de puerto. El resultado es la visibilidad de la conexión de comando y control. Este nivel de transparencia fue posible gracias a la supervisión detallada de la llamada RPC mediante el agente de Cortex XDR.

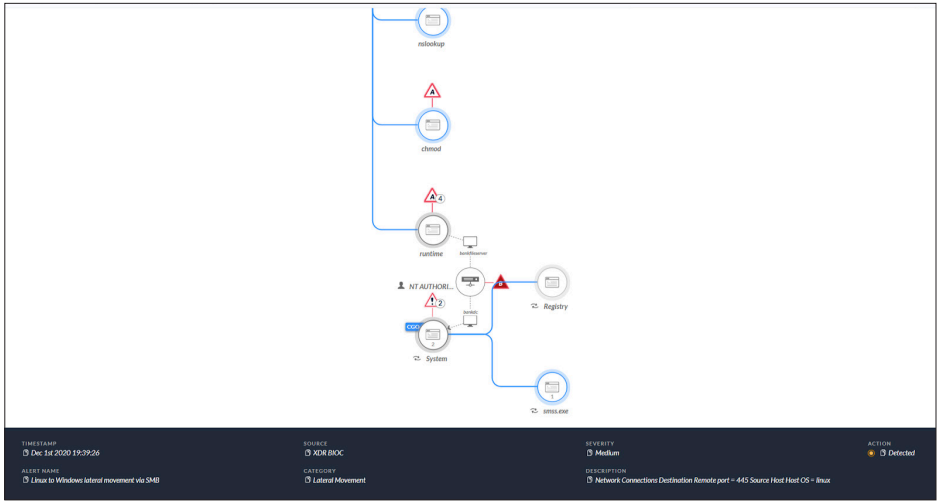


Figura 7: En el paso 5.C.2, un ataque en cadena detallado con una visualización que abarca los distintos hosts

CORTEX XDR BY PALO ALTO NETWORKS

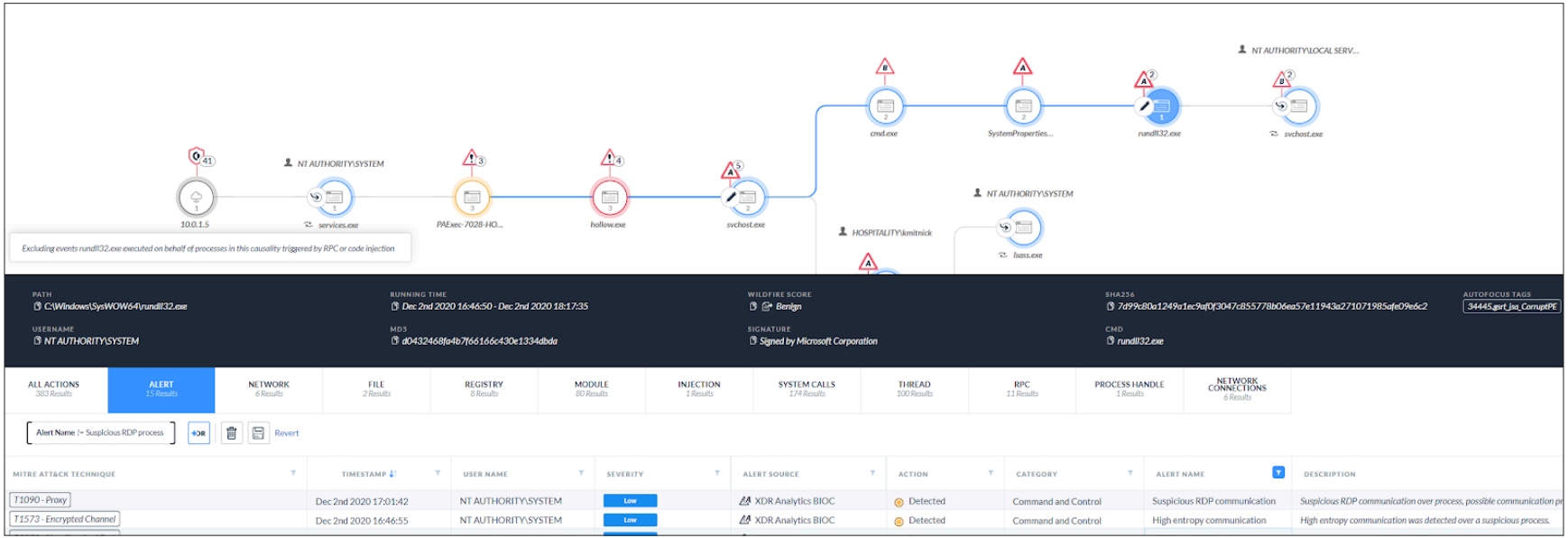


Figura 8: En el paso 17.A.6, Cortex XDR hace un seguimiento de las llamadas RPC en la sesión HTTPS a pesar del enmascaramiento

CORTEX XDR
BY PALO ALTO NETWORKS

Como Cortex XDR integraba datos del endpoint con datos de la red que contenían información de App-ID™, logró detectar el movimiento lateral del equipo rojo de MITRE realizado con SSH entre los hosts Windows y Linux. Esto se puede observar en el paso 5.B.1 de la evaluación (figura 9), donde Cortex XDR permitió ver el movimiento lateral del atacante y reveló qué protocolos se utilizaron.

Estos ejemplos demuestran que los beneficios de Cortex XDR van mucho más allá de las cifras relativas a la detección proporcionadas en los resultados de las pruebas. Cortex XDR proporciona una representación completa y detallada de los entresijos del ataque, mediante la extracción de datos de distintas fuentes y el uso de nuestro motor de análisis para mostrar al administrador una visión completa de causalidades sin necesidad de investigar ni de establecer correlaciones de forma manual.

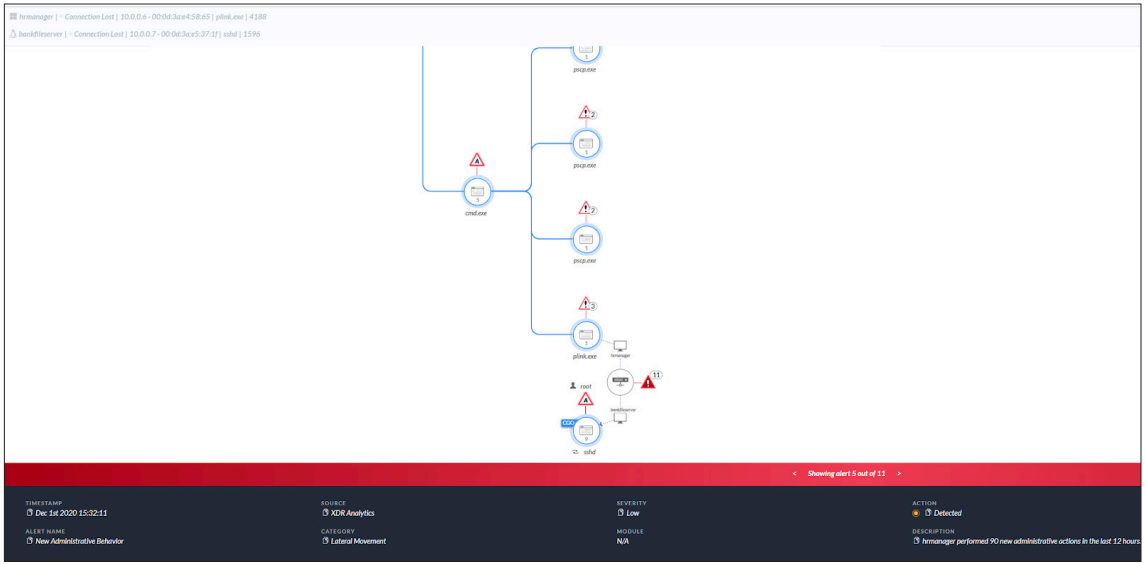


Figura 9: En el paso 5.B.1, movimiento lateral de Windows a Linux por SSH

CORTEX XDR BY PALO ALTO NETWORKS

¿Le ha sabido a poco esta guía? ¡Aún hay más!

Sabemos que, para los equipos de seguridad que intentan estudiar los resultados de MITRE ATT&CK, no es nada fácil descifrar las interpretaciones de los distintos proveedores. Además de esta guía, recomendamos leer la siguiente publicación del blog (en inglés), escrito por Josh Zelonis, director tecnológico sobre el terreno de Palo Alto Networks: *Don't Let Vendor Exuberance Distract from the Value of the MITRE ATT&CK Evaluation*. Explica más a fondo los parámetros de visibilidad y análisis, y le ayudará a comprender algunas de las cuestiones más complejas.

Si le interesa saber más sobre los casos de ataque emulados en esta evaluación y las tecnologías que mejor detectaron estas técnicas y protegieron de ellas, inscríbase en nuestro seminario web a petición Carbanak+FIN7: resultados de MITRE ATT&CK al descubierto.

Las soluciones EDR avanzan a marchas forzadas hacia la tecnología XDR: mejor prepararse cuanto antes

¿Quiere saber más sobre las soluciones de detección y respuesta ampliadas (XDR) ahora que están ganando protagonismo en el mercado? Descargue nuestro libro electrónico *XDR: detección y respuesta ampliadas* para ampliar la información y descubrir:

- las carencias de las tecnologías de detección y respuesta actuales;
- cómo mejorar las operaciones de seguridad con XDR;
- qué es la tecnología XDR y qué requisitos debe cumplir.

Más información sobre MITRE

Para obtener más información sobre el marco ATT&CK, visite MITRE.org. No se pierda la herramienta ATT&CK Navigator, que le ayudará a recorrer y visualizar las técnicas de ATT&CK, así como a tomar notas.

Acerca de MITRE Engenuity

Las evaluaciones ATT&CK de MITRE Engenuity, financiadas por los proveedores, persiguen el objetivo de ayudar a los proveedores y usuarios a comprender mejor las funciones de un producto con respecto al marco ATT&CK® de MITRE, que es accesible públicamente. MITRE ha desarrollado la base de conocimientos de ATT&CK, creada a partir de informes reales sobre las técnicas y tácticas de los ciberdelincuentes, y se ocupa de su mantenimiento. Numerosos responsables de la seguridad del sector y de instituciones gubernamentales utilizan ATT&CK, que es de acceso gratuito, para detectar lagunas en la visibilidad, herramientas de defensa y procesos a la hora de evaluar y elegir soluciones para mejorar la protección de las redes. MITRE Engenuity pone a disposición del público su metodología y los datos resultantes para que otras organizaciones puedan aprovecharlos, realizar sus propios análisis y sacar sus propias conclusiones. Las pruebas no dan lugar a clasificaciones ni avalan ninguna opción en concreto.

MITRE ENGENUITY™

A Foundation for Public Good

Referencias

1. «Detection and Protection Categories» (Categorías de detección y protección, disponible en inglés), Evaluaciones ATT&CK, MITRE Engenuity, último acceso el 21 de mayo de 2021, https://attackevals.mitre-engenuity.org/enterprise/carbanak_fin7/#detection-categories.
2. *Ibidem*.
3. *Ibidem*.

paloalto® NETWORKS

Oval Tower, De Entrée 99 - 197
1101HE Ámsterdam
Países Bajos

Tel.: +31 20 888 1883

www.paloaltonetworks.es