CÓMO ELEGIR LA MEJOR OPCIÓN EN EDR

El mercado de seguridad de endpoint está lleno de proveedores que afirman tener capacidades superiores. No es sencillo pasar por todos los argumentos de mercadotecnia y de ventas para poder entender cómo funcionan estos productos. Por suerte, The MITRE Corporation llevó a cabo una prueba independiente de las capacidades de detección e investigación de los principales productos de detección y respuesta de endpoint (EDR) contra secuencias de ataques del mundo real. Explicaremos la metodología de MITRE, los resultados y todo lo que esto significa para su organización a medida que evalúe el conjunto de herramientas de seguridad de endpoint actual y futuro.

Conocimientos obtenidos en la Evaluación MITRE ATT&CK

La organización de investigación independiente The MITRE Corporation publicó los resultados finales de la Ronda 1 de sus evaluaciones de seguridad cibernética MITRE ATT&CK™.[1] Estas evaluaciones ponen a prueba las capacidades de detección de las principales herramientas de seguridad de endpoint al emular secuencias de ataques de adversarios del mundo real, con la primera ronda centrada en las técnicas utilizadas por el grupo APT-3 .

En esta evaluación, MITRE evita de manera intencional la comparación directa de los proveedores y, en su lugar, opta por un enfoque científico que captura y categoriza las capacidades de detección e investigación de cada herramienta para diferentes técnicas reales de ataque.

Para obtener información de los resultados de MITRE, Josh Zelonis, analista sénior de Forrester Research, ofrece un marco objetivo de terceros para calificar y evaluar la eficacia de los productos probados. Su informe[2] aplicó una metodología de puntuación pública a la cantidad y calidad de las detecciones para comparar los proveedores y analizar el mercado de EDR.

Al sumar todas las detecciones y aplicar las ponderaciones de Forrester, el marco de Forrester muestra a Cortex XDR™ de Palo Alto Networks como el proveedor que ofrece la mejor visibilidad, por un amplio margen, para la detección e investigación en el mercado EDR. Cortex XDR, junto con Traps™ para la protección y respuesta de endpoints, superó a la competencia en múltiples áreas, entre ellas la cobertura más alta, la menor cantidad de errores y el mejor enriquecimiento de cualquier producto probado.

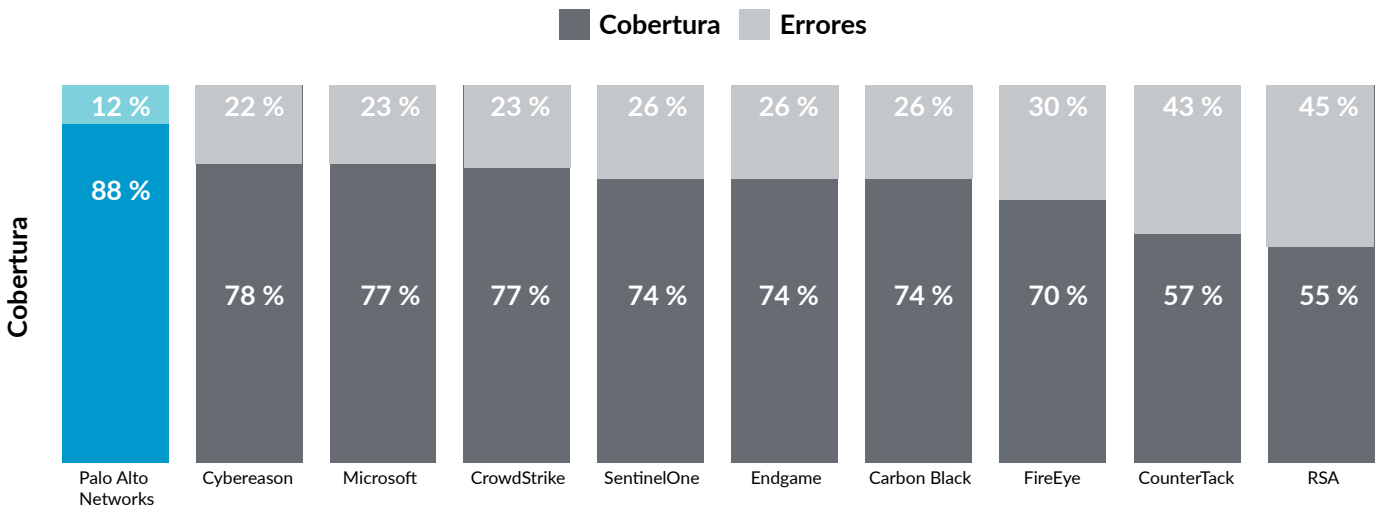

Figura 1: Cobertura y pérdidas en todo el mercado

La evaluación de las nuevas tecnologías requiere una evaluación integral y personalizada. En este artículo, profundizaremos en la metodología de evaluación de MITRE ATT&CK y en el análisis de Forrester para evaluar qué capacidades son importantes para estas organizaciones independientes. A continuación, proporcionaremos un análisis más detallado de las capacidades probadas por MITRE para ayudarle a evaluar qué herramienta de EDR es adecuada para sus necesidades.

Principales conclusiones

- **MITRE y Forrester ofrecen una plantilla inicial para la evaluación de la seguridad.** Es igualmente difícil mantenerse al día con la evolución del panorama de las amenazas como lo es leer las afirmaciones contradictorias de los proveedores acerca de por qué sus productos son los mejores. Aunque las distintas organizaciones ponderan los diversos criterios de forma diferente, MITRE y Forrester establecieron bases objetivas para ayudar a las organizaciones a comprender las fortalezas y las debilidades de su seguridad de endpoint actual, así como toda inversión potencial.
- **Los equipos de SecOps requieren algo más que solo datos de endpoint.** Como si los equipos de seguridad no estuvieran lo suficientemente dispersos, también están sujetos a un conjunto de herramientas increíblemente fragmentado. La consolidación de las capacidades en una plataforma sólida significa una respuesta más rápida, una mejor seguridad y mucho menos tiempo perdido. Los equipos expertos de SecOps adoptarán herramientas que pueden correlacionar varias fuentes de datos para encontrar amenazas que las herramientas aisladas pueden pasar por alto, incluidas las vulnerabilidades en endpoints no administrados.
- **Cortex XDR entrega una visibilidad inigualable.** Cortex XDR, combinado con Traps para la protección de endpoints (incluido), entrega la mayor cobertura a lo largo del ciclo de vida de los ataques, con la menor cantidad de técnicas fallidas, alta correlación y cero alertas con retraso. Además, MITRE solo probó las capacidades de EDR, pero Cortex XDR entrega una serie de capacidades adicionales críticas, como la prevención superior y la capacidad de sincronizar los datos de red, de nube y de endpoint.

1. «Evaluaciones MITRE ATT&CK», The MITRE Corporation, consultado el 17 de junio de 2019, https://attackevals.mitre.org/evaluations.html.
2. «Guía de Evaluaciones MITRE ATT&CK de Forrester», Josh Zelonis y otros., 21 de mayo de 2019, https://www.forrester.com/report/The+Forrester+MITRE+ATTCK+Evaluation+Guide/-/E-RES147475.

Explicación de la Ronda 1 de la Evaluación MITRE ATT&CK

MITRE ATT&CK es una «base de conocimiento de acceso global sobre tácticas y técnicas adversarias basadas en observaciones del mundo real». La matriz de MITRE ATT&CK abarca cientos de técnicas diferentes en 12 categorías diferentes (ver la Figura 2). En un escenario de ataque real, el atacante une una secuencia lógica de técnicas en estas categorías para obtener acceso, ejecutar comandos, extraer información y realizar otras acciones. Para emular el mundo real, MITRE dividió sus evaluaciones en rondas, de las cuales cada una utiliza estrategias y técnicas comunes de un adversario conocido del mundo real.

Figura 2: Categorías de la matriz MITRE ATT&CK

La Ronda 1 fue diseñada para emular el grupo APT-3, un grupo adversario sofisticado asociado con la actividad del estado nación, que tiene un historial de uso de exploits basados en navegadores para obtener credenciales. Los ataques APT-3 suelen emitir comandos en el teclado, tomar el control de programas de confianza y moverse lateralmente a servidores adicionales. En esta ronda, MITRE eligió una serie de 56 técnicas de Enterprise ATT&CK para representar varios escenarios de ataque APT-3.

MITRE utilizó herramientas públicas de emulación de amenazas como Cobalt Strike™ y Empire para llevar a cabo ataques contra cada proveedor evaluado. Para cada técnica, MITRE documentó si se produjo una detección y, en caso afirmativo, el tipo de detección, en una escala desde la más baja (sin detección) hasta la más alta (una alerta con información sobre la amenaza específica). Las herramientas que recopilan los datos de telemetría con fines de la búsqueda de amenazas pero que no generan alertas se encuentran calificadas en el medio de la escala (ver la Figura 3).

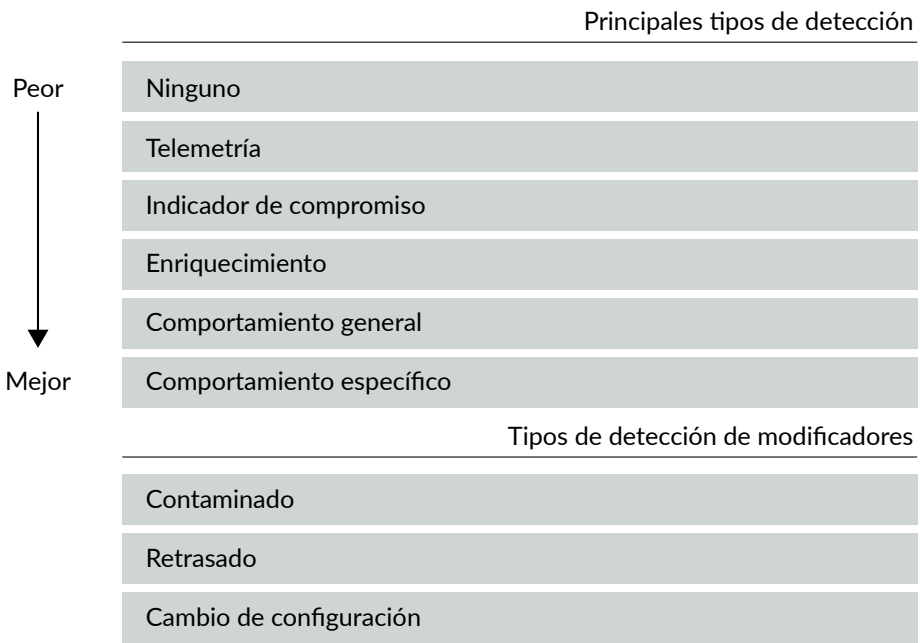

Figura 3: Escala de detección de MITRE

Además de estas categorizaciones, MITRE aplicó los modificadores necesarios:

- **Contaminado:** Si la detección se lleva a cabo inmediatamente debido a una asociación con un comportamiento malicioso previamente descubierto, se marca como «contaminado». Esto es lo ideal.
- **Retrasado:**La detección no ocurrió en tiempo real, pero a la larga se produjo.
- **Cambio en la configuración:** Cualquier detección se hizo posible solo porque el proveedor cambió la configuración inicial.

Capas en el Análisis de Forrester

De acuerdo con los criterios antes mencionados, Forrester ha aplicado puntuaciones a cada detección (ver la Figura 4) y también ha asignado cero puntos a todas las detecciones que solo se han producido a través de un cambio de configuración.

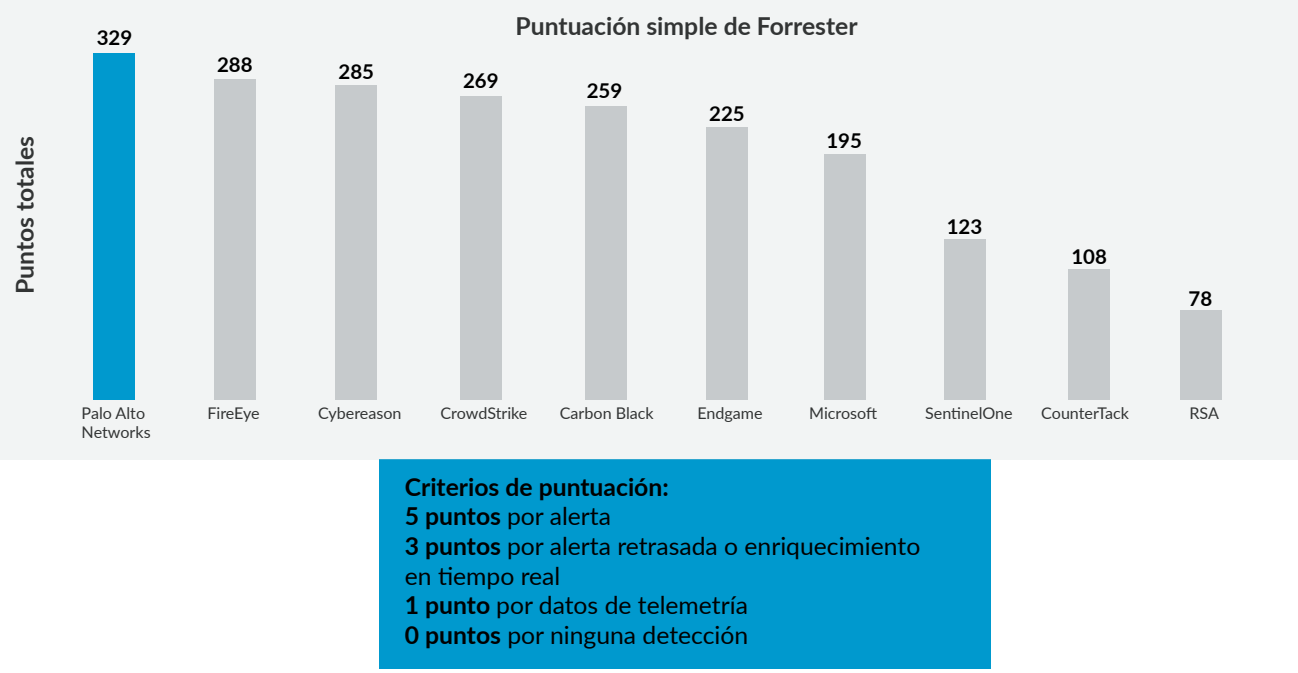

Figura 4: Puntuaciones por proveedor

La evaluación de Forrester profundiza más, evaluando las herramientas y estrategias de EDR sobre la base de tres métricas clave:

- **¿Qué porcentaje de técnicas se detectaron?**Independientemente del tipo de detección, la conclusión es que una técnica debe ser detectada para que un analista tenga la oportunidad de investigarla y remediarla.
- **¿Qué porcentaje de detecciones estaban contaminadas?** El término «contaminado» es positivo en el contexto de la detección. Los datos se consideran contaminados si están correlacionados con otros eventos maliciosos o sospechosos. Casi ninguna acción es intrínsecamente «mala» por sí sola: la forma en cómo se unen las técnicas es lo que indica que un adversario puede estar operando en el sistema.
- **¿Cómo funciona el producto en la cadena de ataque?** La cadena de ataque, a la que Palo Alto Networks llama ciclo de vida del ataque, describe el conjunto completo de objetivos que un adversario debe lograr en el transcurso de un ataque exitoso. Detectar y detener una técnica de acceso inicial es excelente, pero si un adversario llega a un obstáculo, lo más probable es que busque una ruta alternativa. La evaluación de un producto a lo largo del ciclo de vida del ataque muestra su capacidad de proporcionar defensa en profundidad e indica la existencia de una herramienta más desarrollada e integral.

Cómo funcionan Cortex XDR y Traps

Cortex XDR descubrió el 88.9 % de las técnicas (ver Figura 5), pasando por alto solo el 11.1 % de 136 amenazas. El segundo mejor proveedor pasó por alto el 21 %, lo que equivale a dejar sin visibilidad a los equipos de seguridad casi el doble de veces. La mayoría de las técnicas se correlacionaron y enriquecieron con otros puntos de datos, lo que significa que los analistas recibieron alertas contextualizadas y accionables en lugar de puntos de datos independientes que pueden no representar amenazas reales. Cortex XDR mostró su capacidad de detectar durante todo el ciclo de vida del ataque sin que se pasara por alto un solo objetivo. En general, la evaluación MITRE y el análisis de Forrester destacaron que Cortex XDR es una herramienta de élite entre las herramientas de EDR, que proporciona una detección sin igual.

Figura 5: Cobertura de Cortex XDR

De Todas las Formas en las que lo Vea

Naturalmente, hay muchas otras formas de analizar los datos. Es importante analizar en profundidad la forma en que varias herramientas pueden adaptarse a las necesidades y estrategias particulares de su organización. Su equipo de seguridad puede valorar ciertos tipos de detección sobre otros o priorizar la cobertura en una parte determinada del ciclo de vida del ataque. Es posible que desee considerar algunos puntos de análisis adicionales.

Alertas Retrasadas Frente a Alertas en Tiempo Real

El análisis de Forrester combina alertas retrasadas y enriquecimientos en una sola categoría. Sin embargo, estas detecciones no son las mismas, lo que puede suponer una diferencia para el equipo de operaciones de seguridad. En muchos casos, las alertas retrasadas indican que la herramienta en sí pasó por alto la alerta, pero un servicio administrado supervisó los datos de telemetría y generó de manera manual una alerta después del hecho. El riesgo con alertas retrasadas es que, en el caso de detener a un adversario real antes de que pueda hacer daño, las horas, los minutos e incluso los segundos importan.

Los proveedores sin alertas retrasadas muestran una mayor confianza en la tecnología para realizar la detección, en lugar de en un analista. Cortex XDR no tenía alertas retrasadas, lo que resalta nuestra decisión estratégica de desarrollar herramientas que utilicen una inteligencia de amenazas sólida, reglas listas para usar y aprendizaje automático para automatizar la detección y la correlación. Como resultado, Cortex XDR puede reducir el tiempo medio de respuesta (ver la Figura 6).

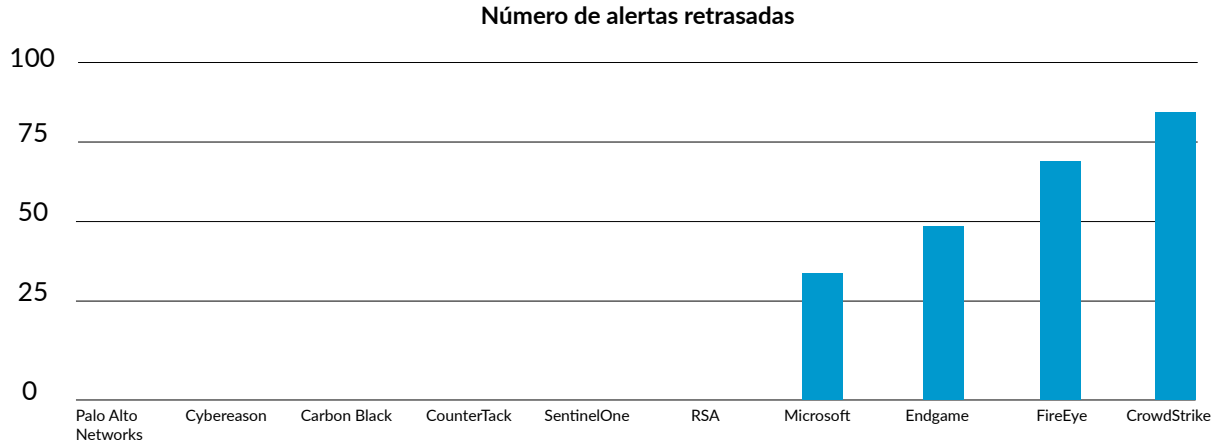

Figura 6: Cantidad de alertas retrasadas por el proveedor

Alertas Frente a la Telemetría

No todas las alertas se crean de la misma forma. Según las estimaciones del sector, las herramientas pueden generar más de 100 alertas por cada amenaza real, una tasa de falsos positivos que puede llevar fácilmente a que se pasen por alto o se ignoren amenazas reales (tenga en cuenta que la evaluación MITRE ATT&CK no examinó los falsos positivos). Al mismo tiempo, una herramienta EDR que no genera alertas solo es útil para los buscadores de amenazas que ya tienen una buena idea de lo que están buscando.

Hay un punto óptimo en algún lugar en el medio. La herramienta ideal solo genera alertas de alta calidad, específicas y priorizadas. Para otros comportamientos potencialmente maliciosos, aunque probablemente no lo sean, la herramienta EDR debe capturar y correlacionar datos de telemetría para la investigación y la búsqueda de amenazas, aunque es posible que no desee que la herramienta genere una alerta que tenga una alta probabilidad de ser un falso positivo. Además, desea que su herramienta EDR enriquezca los datos de telemetría con un contexto adicional, lo que facilita y agiliza la tarea de un analista de obtener significado de ellos.

Con la configuración predeterminada durante la prueba MITRE, Cortex XDR generó 20 alertas específicas en tiempo real y 82 registros de telemetría enriquecidos (ver Figura 7). En una implementación real, los clientes que conectan sensores adicionales de red y nube en Cortex Data Lake brindan a Cortex XDR aún más visibilidad y contexto en el comportamiento de los posibles actores de amenazas, lo cual reduce aún más los falsos positivos y mejora la identificación de comportamientos maliciosos que de otro modo podrían parecer benignos.

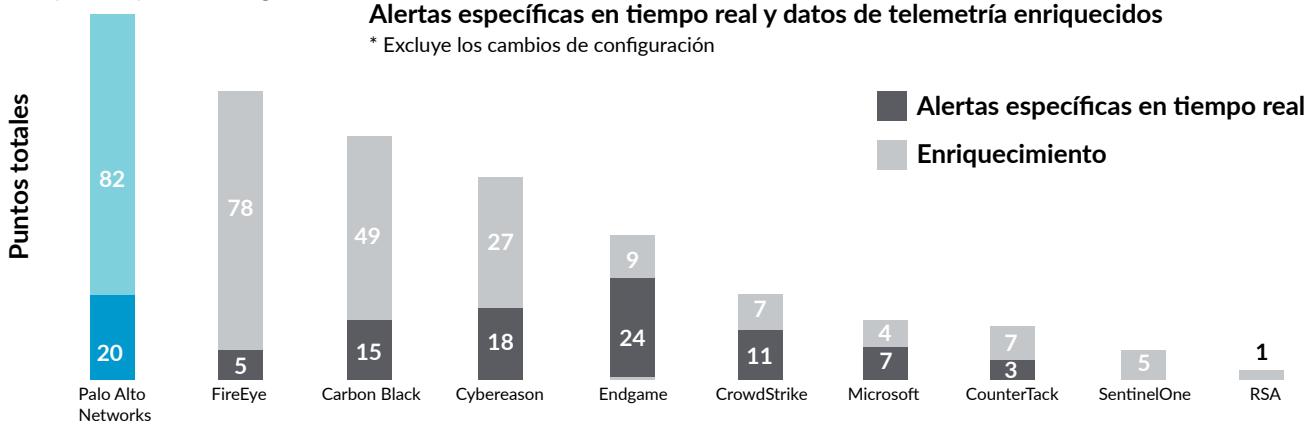

Figura 7: Alertas específicas en tiempo real y datos de telemetría enriquecidos

EDR No Es Suficiente

Los equipos de seguridad tienen dificultades con la ineficiencia, con un **tiempo medio para identificar (MTTI) de 197 días** y un **tiempo medio para contener (MTTC) de 69 días.**[3] El Ponemon Institute descubrió que, desde el surgimiento de EDR, esta ineficiencia no ha hecho más que empeorar. Agregar más herramientas aisladas no es la respuesta. La evolución de EDR como un programa eficaz de seguridad de endpoint requiere un enfoque más holístico e integral.

En primer lugar, se encuentra la prevención con una potente protección de endpoint, algo en lo que Traps funciona excepcionalmente bien (aunque la prevención se desactivó para la prueba MITRE). Siempre es mejor evitar que un adversario entre en su entorno a detectarlo después del hecho. Cuanto más prevenga por adelantado, menos incidentes tendrán que remediar sus analistas.

Luego se encuentra la amplia visibilidad de su infraestructura, incluido del 10 % al 20 % de los endpoints que no están bajo gestión, como la mayoría de los dispositivos del Internet de las cosas (IoT). Aquí es donde EDR, estrechamente integrada con las capacidades de análisis de comportamiento de usuario y entidad (UEBA) y análisis de tráfico de red (NTA), es más útil. Una plataforma integrada debe detectar a los actores amenazantes que evaden la primera línea de defensa y siguen sus acciones a lo largo de toda la infraestructura. Debe reconocer cuándo una cadena de comportamientos es maliciosa o benigna. A continuación, debe compartir esas conclusiones y coordinar la respuesta con las tecnologías de protección de endpoint y de las redes, asegurándose de que todos los sistemas se actualicen y trabajen juntos.

Una plataforma simplificada, integrada y completa es la estrategia adecuada para optimizar la seguridad en la actualidad, así como para crear operaciones de seguridad escalables para hacerle frente a las amenazas del futuro. Esto debería facultar a sus analistas de seguridad, sobrecargados de manera rutinaria con eventos, frecuentemente obligados a priorizar e ignorar amenazas legítimas, y que pierden constantemente el tiempo probando distintas herramientas, para centrarse en lo que importa.

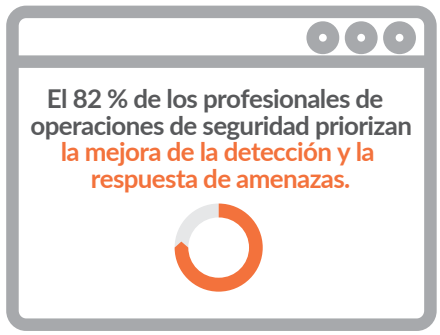

Figura 8: Prioridad EDR por investigación ESG [4]

La Diferencia de Cortex XDR

Cortex XDR es la primera aplicación de detección y respuesta basada en la nube en el mundo que integra de forma nativa datos de red, endpoints y datos de la nube para detener ataques sofisticados. Diseñamos Cortex XDR desde cero para ayudar a las organizaciones a proteger sus activos digitales y sus usuarios, a la vez que se simplifican las operaciones. Los modelos de aprendizaje automático y de AI descubren amenazas de cualquier origen de datos, incluidos los dispositivos administrados y no administrados, con una precisión inigualable.

Cortex XDR ayuda a acelerar las investigaciones proporcionando la visión completa de cualquier alerta o amenaza. Este sistema une automáticamente diferentes tipos de datos y revela la causa principal, lo que permite a los analistas de todos los niveles de experiencia realizar una selección de análisis de alerta e investigación de incidentes en una sola consola. La estrecha integración con los puntos de aplicación les permite a los equipos de seguridad responder rápidamente a las amenazas y aplicar los conocimientos adquiridos en las investigaciones para detectar ataques similares en el futuro.

Para obtener más información, visite nuestro sitio web o lea la ficha técnica de Cortex XDR.

3. «2018 Costo de un Estudio de Filtración de Datos: Descripción General», Ponemon Institute, julio de 2018, https://public.dhe.ibm.com/common/ssi/ecm/55/en/55017055usen/2018-global-codb-report_06271811_55017055USEN.pdf.
4. «Un Capítulo Nuevo y Prometedor en Herramientas de Detección y Respuesta», Enterprise Strategy Group, 28 de mayo de 2019, https://www.esg-global.com/blog/a-promising-new-chapter-in-detection-and-response-tools.

CORTEX BY PALO ALTO NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Línea principal: +1.408.753.4000
Ventas: +1.866.320.4788
Soporte técnico: +1.866.898.9087

www.paloaltonetworks.com