REDEFINIR LAS OPERACIONES DE SEGURIDAD CON XDR

No Se Quede en la Detección y Respuesta de Endpoints

Introducción

El objetivo de todo equipo de seguridad es defender la infraestructura y los datos de una organización contra daños, accesos no autorizados y uso indebido. Por lo general, los arquitectos e ingenieros de seguridad adoptan un método de prevención por capas. Como los ataques han aumentado su nivel de automatización y complejidad, este método ahora incluye visibilidad por capas mediante productos de detección y respuesta, como Endpoint Detection and Response (Detección y Respuesta de Endpoints – EDR), Network Traffic Analysis (Análisis de Tráfico de Redes – NTA) y Security Information and Event Management (Gestión de Eventos e Información de la Seguridad – SIEM).

Esta visibilidad por capas tiene costo: tiempo y conocimientos. El uso de distintos productos de detección y respuesta genera alertas adicionales, requiere más habilidades para solucionar los problemas y prolonga los tiempos de un ciclo que parece no tener fin: una serie interminable de eventos, más herramientas e informaciones que analizar y coordinar, mayores tiempos de detección y un equipo de seguridad sobrepasado; todo mientras los gastos en seguridad nunca parecen suficientes. Mientras más reaccionamos, más nos alejamos.

Figura 1: Red, endpoint o nube

Muchas organizaciones como la suya se hacen la misma pregunta: ¿cómo podemos dejar de reaccionar a alertas internas para adoptar una postura de defensa activa capaz de mejorar la prevención de amenazas?

Es tiempo de implementar un método diferente, un método que beneficie a todo el equipo de seguridad en lugar de sobrecargarlo, que simplifique las operaciones y que proporcione los medios necesarios para detectar y responder rápidamente a las amenazas más sofisticadas a través de todo el ecosistema.

Método Actual: Solucionar Un Problema Crear Otros

Los equipos de seguridad trabajan duro para garantizar la seguridad de sus organizaciones, pero les resulta difícil evitar filtraciones de datos. Los cinco desafíos más importantes incluyen:

- Sobrecarga de eventos
- Pocos analistas de seguridad
- Herramientas limitadas, demasiado específicas
- Falta de integración
- Falta de tiempo

Figura 2: Los equipos del SOC enfrentan cinco desafíos principales

Analicemos cada uno en detalle.

1. Sobrecarga de Eventos

Los analistas de seguridad se enfrentan a demasiados eventos para gestionarlos con eficiencia. El 55 % de los equipos de seguridad o Security Operations Centers (Centros de Operaciones de Seguridad – SOCs) reciben en promedio más de 10 000 eventos diarios.[1] Sin embargo, no todos los eventos son iguales: la mayoría se deben priorizar, correlacionar o normalizar, y agregar al conjunto de alertas. Aunque el equipo SOC cuente con la ayuda del SIEM para analizar esta masiva cantidad de datos, los analistas de seguridad aún deben emplear tareas manuales para recopilar datos, realizar análisis y descartar falsos positivos. Y deben hacerlo con rapidez, a menos que quieran pasar por alto las alertas más críticas. Con demasiada frecuencia, los analistas son víctimas de la "fatiga de alertas"; es decir, filtran alertas en base a presuposiciones o la cantidad suprema de datos. Debido al volumen de alertas, el 54 % de los profesionales de seguridad ignoran alertas que deberían investigarse.[2]

2. Falta de Personas Capacitadas

Muchas organizaciones buscan contratar más personas para hacer frente a las altas cargas de trabajo. Pero existe una falta de profesionales de seguridad capacitados a nivel mundial que, según los analistas, llegará a los 1,8 millones en 2022.[3] Incluso, resulta especialmente difícil encontrar especialistas con experiencia forense en redes, endpoints, o ambos. En consecuencia, los equipos de seguridad están sobrecargados en materia de identificación y priorización de alertas, que se suma a las tareas de investigación y respuesta. Pierden demasiado tiempo en tareas tediosas, como recopilación de datos, análisis manuales e incorporación de inteligencia, o en la creación de procesos automatizados, lo que genera aún más estrés. Esto coarta aún más el proceso de aprendizaje y la posibilidad de compartir información ya que el historial de actividades y de inteligencia quedan aislados e inaccesibles a otros grupos.

La combinación de demasiadas alertas, investigaciones complejas y pocos analistas conduce a errores humanos y genera un efecto mariposa en las operaciones subsiguientes. Por falta de información, el nivel de las alertas es disminuido o escalado de forma incorrecta, lo que genera aún más trabajo para los miembros del equipo de investigación de incidentes que requieren la ayuda de equipos de detección de amenazas para manejar la carga de trabajo.

3. Herramientas Diferentes con Foco Limitado

Añadir más herramientas es una forma de sortear otros obstáculos para poder tomar decisiones más informadas con mayor rapidez. Sin embargo, la incorporación de demasiadas herramientas puede ser problemático. La mayoría de las herramientas de seguridad se desarrollaron para hacer frente a cuestiones tecnológicas específicas, pero sin tener en cuenta la forma en que deben funcionar en un entorno operativo y, muchas veces, trabajan en contra del objetivo del equipo de seguridad de proporcionar prevención y visibilidad holísticas. Estas herramientas funcionan de forma aislada, se caracterizan por su falta de integración y recopilan datos de una sola fuente. Es decir, son valiosas solo para los miembros del equipo específico con ese conjunto de habilidades especializadas, pero no proporcionan valor alguno, o incluso sobrecargan, al resto.

Algunas herramientas usadas normalmente en la detección y respuesta son valiosas, pero limitadas:

- **EDR** puede disminuir los tiempos de respuesta para equipos experimentados de respuesta a incidentes, pero se limita a datos de endpoints donde se pueden instalar agentes. EDR también puede aumentar demasiado el volumen de las alertas y requiere desarrollos personalizados para habilitar automatizaciones básicas; así, se convierte a la vez en una carga para otras partes del equipo.
- **NTA** requiere la instalación de sensores adecuados para evitar pasar por alto grandes volúmenes de tráfico; por lo general no incluye respuestas y no incorpora datos de endpoints como factor en la detección de anomalías o la investigación de amenazas.
- **User and Entity Behavior Analytics (Analítica de Comportamiento de Usuarios y Entidades – UEBA)** se centra principalmente en datos de registros y pasa por alto aspectos clave del análisis profundo de las redes, sin mencionar endpoints y nubes. Además, UEBA tiene una alta tasa de falsos positivos, que aumenta aún más la carga laboral de los analistas.

Todas estas herramientas contribuyen a la visibilidad, pero como introducen nuevos problemas, aún requieren habilidades especializadas para poder generar resultados accionables.

4. Investigaciones con Síndrome de la Puerta Giratoria

Para detectar ataques sofisticados, es necesario correlacionar datos de algún punto del entorno digital. Como la mayoría de las herramientas que ayudan a la detección y respuesta se basan en una sola fuente de datos, como el endpoint, no tienen en cuenta información importante de otras fuentes cruciales por lo que sobrecargan a los equipos de seguridad para validar las amenazas. En una típica gran organización, el SOC utiliza más de 40 herramientas que funcionan de forma independiente. En consecuencia, los analistas del SOC deben pasar de una pantalla a otra para unificar conclusiones con información relevante y mitigar las amenazas reales. Si los datos estuviesen correlacionados, podrían proporcionar una visión holística del entorno. Pero esto requeriría normalización, coordinación de fecha/hora/evento y conocimientos de técnicas de investigación en múltiples áreas como las redes y los endpoints. No es una propuesta simple y, en la actualidad, debe hacerse manualmente.

1. Estudio: "27 % de los profesionales de TI reciben más de 1 millón de alertas de seguridad diarias", Imperva, 28 de mayo de 2018, https://www.imperva.com/blog/2018/05/27-percent-of-it-professionals-receive-more-than-1-million-security-alerts-daily/.
2. "2017: Security Operations Challenges, Priorities, and Strategies", ESG, marzo de 2017, http://resources.siemplify.co/hubfs/PDF%20Downloads/ESG-Research-Insights-Report-Siemplify.pdf?hsCtaTracking=4303efc5-9f7b-4a8a-9438-263c0588b898%7C6043fb9a-2881-4940-9a0e-6239a8686b81.
3. "2017 Global Information Security Workforce Study", Frost & Sullivan, consultado el 8 de enero 2019, https://iamcybersafe.org/wp-content/uploads/2017/06/Europe-GISWS-Report.pdf.

5. El Tiempo es el Enemigo

El tiempo es la mercancía más valiosa. Mientras más rápido se pueda identificar una amenaza, mayores serán las probabilidades de contenerla. A medida que los equipos se enfrenten a sobrecargas de eventos, problemas de recursos y falta de correlación, aumentan el riesgo a pasar por alto alertas no descritas capaces de convertirse en incidentes mayores y tampoco dispongan del tiempo necesario para encontrar amenazas desconocidas. En promedio, el intervalo de tiempo entre una filtración de datos y su identificación es de seis meses[4], pero todo indica que continuará aumentando. El Mean Time To Identify (Tiempo Medio de Identificación – MTTI) aumentó de 190 días en 2017 a 197 días con respecto a 2018. Y el tiempo de respuesta, que se mide como Mean Time To Contain (Tiempo Medio de Contención – MTTC), aumentó de 66 días a 69 días de 2017 a 2018.[5]

Todo esto ocurre en una época en el que las organizaciones utilizan EDR, NTA y UEBA, mientras revalúan el SIEM y gastan casi el 60 % del presupuesto de TI en seguridad.[6] Incluso con estas herramientas, los analistas pasan demasiado tiempo en tareas manuales: redacción de consultas, correlación de alertas con datos de registros, combinación de información de distintas fuentes independientes y más. Con una carga de trabajo constante, no es de extrañarse que solo algunos equipos de seguridad tengan tiempo para enfocarse en tareas críticas como buscar amenazas sofisticadas, realizar análisis más profundos y solucionar problemas de seguridad más complejos que superen la capacidad de programas inteligentes y procesos automatizados.

El SOC Merece un Método Más Optimizado

El equipo del SOC necesita un método que aborde con eficacia todos estos problemas. Por lo tanto, necesitamos un método capaz de asistir al SOC en todas las etapas de las operaciones (identificación de alertas, investigación de incidentes y búsqueda de amenazas) y ayudar a cerrar investigaciones con rapidez, independientemente del tipo de amenaza. En términos prácticos, el método ideal debe ser capaz de:

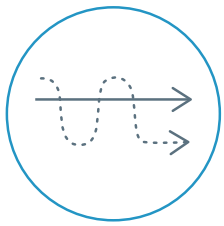
- Realizar el seguimiento de las actividades de detección, identificación y priorización de alertas, investigaciones y respuestas a través de redes, endpoints y nubes.
- Integrarse con herramientas que generen alertas o proporcionen inteligencia automáticamente para obtener información, formar conclusiones e incluso tomar medidas cuando sea posible.
- Aprovechar analítica a gran escala para correlacionar datos de todas las fuentes y detectar de forma manual o automática amenazas difíciles de encontrar en múltiples fuentes de datos con pocos falsos positivos.
- Simplificar investigaciones para ayudar a los analistas menos experimentados y reducir la carga del personal especializado para mejorar radicalmente los tiempos a través de todas las etapas de las operaciones del SOC.
- Garantizar que la inteligencia obtenida de todas las investigaciones se pueda convertir rápidamente en defensas mejoradas (p. ej., para añadir contexto a futuras investigaciones, disminuir la cantidad de alertas y corregir vulnerabilidades nuevas o conocidas).

Esto permitirá disminuir el dwell time o tiempo de espera medio necesario para la detección y respuesta de amenazas); además de ayudar a que los equipos de seguridad dejen su postura reactiva con respecto a las alertas de seguridad para defender la red de forma proactiva.

XDR Lleva la Detección y Respuesta a Otro Nivel

Palo Alto Networks presenta un método revolucionario para las operaciones de seguridad al aumentar la visibilidad, así como la velocidad de detección, investigación y resolución de amenazas. Se llama XDR, una evolución de la categoría de detección y respuesta. La "X" hace referencia a cualquier fuente de dato, ya sea una red, un endpoint o la nube, y hace hincapié en multiplicar la productividad del SOC a través de la automatización. La visibilidad total provee un panorama holístico de las actividades de la organización al vincular los datos de múltiples fuentes: ya no se correlacionan los datos de forma manual y las amenazas no tienen dónde ocultarse. A través de la integración, se obtienen datos de distintas fuentes, como alertas de seguridad e inteligencia de amenazas globales, para incorporar información valiosa.

Encontrar más rápido amenazas ocultas con analítica de todas las redes, nubes y endpoints.



Simplificar la investigación y respuesta ante amenazas conocidas y desconocidas.

Mejorar radicalmente las operaciones de seguridad y el rendimiento de las inversiones de seguridad.

Figura 3: Tres beneficios clave de XDR

4. "2018 Cost of a Data Breach Study", Ponemon Institute, mayo de 2018, https://www-01.ibm.com/common/ssi/cgi-bin/ssialias?htmlfid=55017055USEN&.
5. Ídem.
6. Infografía: "2018 IT budgets are up slightly; spending focus is on security, hardware, and cloud", ZDNet, 2 de octubre de 2017, https://www.zdnet.com/article/infographic-2018-it-budgets-are-up-slightly-spending-focus-is-on-security-hardware-and-cloud.

La automatización combina datos críticos en un único tablero mientras genera conclusiones para los analistas de seguridad: en solo unos segundos realiza lo que normalmente toma horas con años de experiencia. ¿El resultado? Investigaciones simplificadas en las operaciones de seguridad que permiten reducir el tiempo utilizado para descubrir, cazar, investigar y responder a cualquier tipo de amenaza.

XDR anuncia una nueva era de heurística, analítica y modelado gracias a la aplicación de inteligencia artificial y aprendizaje automático para detectar y detener rápidamente las amenazas más sofisticadas. A medida que realiza el seguimiento de amenazas a través de todas las fuentes y ubicaciones de la estructura de la organización, XDR puede automatizar la contención, reconstruir cada paso de un ataque para proveer una clara secuencia de eventos, implementar inteligencia de amenazas y cerrar brechas para la futura prevención. Esto acelera el tiempo de resolución y libera a los analistas de arduas investigaciones. Cabe destacar que XDR se debería instalarse como una solución de nube completa para facilitar la implementación.

Beneficios para la Detección y Respuesta con XDR

XDR está diseñado para trabajar con el SOC y para el SOC. Proporciona tres beneficios significativos: visibilidad ilimitada, operaciones de seguridad simplificadas y un aumento radical en el rendimiento de las inversiones de seguridad.

Visibilidad Ilimitada para Encontrar Amenazas Ocultas con Mayor Velocidad

XDR descubre actividades anómalas al correlacionar el comportamiento de usuarios, entidades y acciones de todas las fuentes de datos. Reduce la complejidad de búsqueda de amenazas ya que proporciona poderosas capacidades de búsqueda, atribuciones enriquecidas y correlación de datos. XDR automatiza el descubrimiento de amenazas activas o pasadas al utilizar analítica de big data con inteligencia de redes, nubes, endpoints y de terceros, y ofrecer un único lugar donde consultar los descubrimientos de amenazas desconocidas para el SOC.

Simplifique las Operaciones de Seguridad para la Identificación, Investigación y Respuesta

XDR acelera y simplifica las investigaciones: visualiza las secuencias de actividades para detectar eventos que revelen automáticamente la causa raíz y proveer información forense útil para todos los analistas de seguridad. Elimina la “fatiga de alertas” al correlacionar los resultados de investigaciones con todas las alertas de seguridad de todo tipo de tecnología; de esta forma, los analistas menos experimentados pueden hacer más, más rápidamente. XDR responde a amenazas activas e impide ataques futuros mediante la coordinación de normativas de cumplimiento a través de redes, nubes y endpoints, para liberar a los analistas de trabajos manuales permitiéndoles tener más tiempo para detectar amenazas.

Aumento Radical en el Rendimiento de las Inversiones de Seguridad

XDR actúa como multiplicador de fuerza para el equipo de análisis de seguridad al optimizar flujos de trabajo y reducir el tiempo y la complejidad en los procesos de identificación de eventos, investigación de incidentes, respuestas y búsqueda. Permite que las herramientas de seguridad trabajen en conjunto para abordar los problemas de forma automática a través del uso de datos enriquecidos e inteligencia de amenazas. XDR fortalece la prevención al aplicar los conocimientos adquiridos en cada investigación para mejorar las defensas y evitar que aparezcan alertas adicionales o amenazas similares en el futuro.

¿Cuáles son los beneficios que XDR ofrece al SOC?

XDR complementa su método que prioriza la prevención con tecnologías de detección y respuesta que contribuyen a transformar sus operaciones de seguridad reactivas en proactivas. La total de todas las fuentes de datos y centrarse en los procesos adecuados, desde identificación de alertas hasta caza de amenazas, le permitirá mejorar sus operaciones de seguridad radicalmente.

Podrá dejar atrás la “fatiga de alertas”, permitir que sus analistas de seguridad filtren los falsos positivos y tomen decisiones en tiempo récord, liberar a sus analistas especializados de investigaciones y soluciones manuales, otorgar a los encargados de buscar amenazas la capacidad de encontrar amenazas desconocidas y estar preparados para las amenazas conocidas en el futuro.

Al otorgarle automatización y un panorama general de la seguridad, XDR cumple con la promesa de multiplicar todo el potencial de su SOC. Si busca tecnologías de detección y respuesta, consulte a su proveedor sobre la “X”, porque una vista de su entorno ya no es suficiente.

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

redefine-security-operations-with-xdr-wp-012219