kaspersky BRING ON THE FUTURE

¡Larga vida a XDR con la evolución de EDR!

XDR (Extended Detection and Response) generalmente se describe como una evolución natural del EDR (Endpoint Detection and Response), con capacidades de defensa de alto nivel que se extienden más allá del endpoint de comunicación para incluir la red, la nube, el servidor y otras capas. Algunos entusiastas de XDR han llegado tan lejos como a declarar la muerte de EDR con el ascenso de XDR como rey de la ciberseguridad. Sin embargo, la realidad es mucho más compleja.

Con la entrada de XDR en el ciclo Gartner Hype Cycle por primera vez, decidimos profundizar en la relación entre EDR y XDR. Revelaremos por qué las fuentes del mundo real (como MITRE ATT&CK) demuestran que la función de EDR como sensor de comunicación de punto final (entre otras cosas) dentro de una solución XDR seguirá siendo esencial dentro de cualquier solución de seguridad empresarial integrada, unificada y eficaz.

Primero, saquemos algunas definiciones del camino:

Endpoint Detection and Response (EDR) se refiere a soluciones que registran y almacenan comportamientos a nivel del sistema de comunicación de endpoint, utilizan diversas técnicas de análisis de datos para detectar comportamientos sospechosos del sistema, proporcionar información contextual, bloquear actividad maliciosa y brindar sugerencias de corrección para restaurar los sistemas afectados. Fuente: Gartner

Extended Detection and Response (XDR) describe una plataforma unificada de respuesta y detección de incidentes de seguridad que recopila y correlaciona automáticamente los datos de varios componentes de seguridad propios. Fuente: Gartner

La clave para comprender la relación entre EDR y XDR es la palabra "unificado". En lugar de reemplazar a EDR, XDR unifica múltiples formas de telemetría en una sola plataforma. Y claramente, la detección (y la respuesta) a nivel de la comunicación del endpoint debe seguir siendo el núcleo de cualquier solución XDR. Para decirlo sin rodeos, es imposible tener un buen XDR sin un EDR óptimo.

Tácticas, técnicas y mitigaciones de MITRE ATT&CK: la comunicación del endpoint sigue dominando

La mayoría de las tácticas en la matriz empresarial de Mitre ATT&CK provienen de la comunicación del endpoint, con ejemplos obvios que incluyen el acceso inicial (TA0001) y la ejecución (TA0002). En términos de técnicas, el abuso de secuencias de comando de PowerShell para la ejecución depende del compromiso de la comunicación del endpoint, al igual que la explotación de aplicaciones orientadas al público, y la ejecución desencadenada por evento, por nombrar solo tres. Por razones obvias, la pertinencia de EDR para las tácticas y técnicas móviles es aún más perdurable.

En lo que respecta al acceso inicial en particular, incluso las amenazas modernas más avanzadas todavía suelen depender de vectores de ataque algo básicos, como los mensajes de correo electrónico empresarial comprometido (que aumentaron casi un 100 % en 2019). Sofacy (APT28) utilizó vínculos y archivos adjuntos de spearphishing, incluso con miembros de la campaña Clinton en 2016.

La centralidad de la comunicación del endpoint para los actores de APT se resume sucintamente en las palabras del Tribunal de Distrito de EE. UU. en la acusación contra presuntos miembros de APT28:

- se explicó que estaban "dedicados a atacar organizaciones militares, políticas, gubernamentales y no gubernamentales con correos electrónicos de spearphishing y otra actividad de intrusión de **equipos**".
- agregaron que ellos "monitorearon de manera encubierta los **equipos** de decenas de empleados del DCCC y DNC".
- indicaron que todo el objetivo de la conspiración del grupo era "hackear los equipos de las personas y entidades estadounidenses involucradas en las elecciones presidenciales estadounidenses de 2016, robar documentos de esos **equipos** y poner en escena los documentos robados para interferir con las elecciones presidenciales de EE. UU. de 2016".

Si bien XDR puede ser una evolución natural de EDR, no eclipsa a EDR ni elimina su necesidad. En algunos sentidos, podría ser más exacto decir que XDR es realmente el resultado de la propia evolución de EDR hacia el trabajo con formas de telemetría que van más allá del nivel de comunicación del endpoint, como parte de una plataforma unificada. Visto de esta manera, EDR sigue siendo el núcleo de cualquier plataforma XDR eficaz.

Un comentario sobre Unified Enterprise Security (UES)

UES se unió a XDR para ingresar al Gartner's Hype Cycle para el Endpoint Security por primera vez en 2020. Según Gartner, UES "implica asegurar estaciones de trabajo, así como teléfonos inteligentes y tabletas, con un solo producto", y "combina elementos de EDR, EPP (Endpoint Protection Platform) y MTD (Mobile Threat Defense)". UES no es una clase de herramientas o soluciones, sino más bien un enfoque, uno que busca asegurar todo tipo de endpoint (computadora, tableta, teléfono) con un solo producto.

Incluso la integración de soluciones heterogéneas en una herramienta de gestión de eventos e información de seguridad (SIEM) no resuelve por completo el problema. Idealmente, los flujos de trabajo de seguridad deberían conectarse de forma nativa a las herramientas de detección (como en XDR), en lugar de administrarse mediante una herramienta separada.

El hecho de que UES haya ingresado al Hype Cycle al mismo tiempo que XDR no es una coincidencia. Ambos abordan el problema de la complejidad y reflejan una necesidad urgente de integración y consolidación. No es de extrañar que en la Encuesta de tendencias de adopción de soluciones de seguridad de IAM (Identity and Access Management) de Gartner, 2020, se descubrió que el 25 % de las organizaciones de usuarios finales seguían una estrategia de consolidación de proveedores.

Heterogeneidad y los límites de la integración de SIEM

Uno de los beneficios clave de XDR es que elimina el problema causado por la compra tradicional de los mejores productos: la falta de integración entre las soluciones. Esta falta de integración causa una serie de problemas, que incluyen alertas excesivas e inmanejables, actualizaciones retrasadas (o perdidas) y configuraciones no óptimas.

EDR se encuentra en el corazón de XDR

Es tentador leer la X en XDR no como "Extendida" sino como "Cruzada", como en "Detección y respuesta entre capas". Después de todo, XDR representa una extensión de las capacidades de detección y respuesta en las capas de red, datos y nube, así como en la comunicación del endpoint. Las herramientas de Endpoint Detection and Response seguirán siendo el núcleo de cualquier solución XDR.

Echando un vistazo a la actividad del grupo de APT más reciente detectada por nuestro Equipo de Investigación y Análisis Global (GReAT), los siguientes ataques y técnicas requieren mitigación de EDR:

- El uso de un paquete ZIP malicioso que contiene un paquete ejecutable RAR malicioso de varias capas por un cibercriminal desconocido. En uno de los incidentes, el paquete tenía como tema la contención del COVID-19.
- DeathStalker: uso de intérpretes nativos de Windows para lenguajes de secuencias de comandos, como powershell.exe y cscript.exe

Estos son solo algunos ejemplos de atacantes que utilizan programas de utilidades comunes para lanzar ataques dirigidos. La visibilidad proporcionada por EDR, en particular (en este caso) del software, las aplicaciones y los controles, protegería contra este elemento del ciclo de ataque.

En Kaspersky, comprendemos los desafíos que presenta la defensa contra las APT y amenazas similares. Por eso, hemos construido un concepto unificado que cumple los tres pilares de una estrategia de seguridad anti-APT exitosa. **Kaspersky Expert Security** le permite a su equipo reducir el trabajo de amenazas sofisticadas y ataques del tipo APT, al enfrentar los desafíos del sigilo, la persistencia, los silos y el talento de frente. Está diseñado y construido alrededor de una plataforma XDR con organizaciones maduras en seguridad de TI en mente. Está repleto de características que aumentan los superpoderes internos de su equipo de seguridad de TI, incluidas la inteligencia integral de amenazas, la capacitación y la orientación de expertos.

Los tres pilares de cualquier estrategia de protección de APT exitosa

Alentamos a todos nuestros clientes empresariales desarrollados en TI a que se aseguren de abordar con cuidado lo que consideramos los tres pilares de cualquier estrategia exitosa de seguridad anti-APT. Es decir, los equipos de seguridad deben ser los siguientes:

- **Equipados:**
  la ciberseguridad es un área de experiencia en la que incluso los trabajadores más hábiles pueden culpar válidamente a sus herramientas. Protección contra ataques multivectoriales y APT requiere una plataforma unificada consolidada que brinde visibilidad total, al eliminar núcleos obstructivos y prevenir la "fatiga de alerta" y otras tareas rutinarias dentro del proceso de respuesta a incidentes.
- **Informados:**
  la experiencia avanzada existente de las organizaciones con una TI madura nunca debe darse por sentada. Después de todo, el horizonte de la ciberdelincuencia cambia y se expande constantemente. La educación continua y la poderosa inteligencia de amenazas de un socio confiable de ciberseguridad son absolutamente cruciales.
- **Reforzado:**
  si se descubre una APT, incluso los analistas de seguridad de TI más avanzados deberían poder recurrir a soporte externo para obtener la opinión, la evaluación de seguridad, la búsqueda de amenazas gestionada o la respuesta a incidentes por parte de un tercero. Si bien las APT suelen ser muy específicas, rara vez se dirigen a una sola víctima. La experiencia externa puede arrojar una luz global multisectorial sobre los posibles caminos de una APT y brindar consejos prácticos sobre la forma más decisiva de eliminarla del sistema.

Obtén más información sobre Kaspersky Expert Security

Kaspersky Expert Security

Noticias sobre ciberamenazas: www.securelist.es
Noticias sobre seguridad de TI: business.kaspersky.com
Seguridad de TI para pequeñas y medianas empresas: kaspersky.com/business
Seguridad de IT para grandes empresas: kaspersky.es/enterprise-security
Threat Intelligence Portal: opentip.kaspersky.com
Herramienta de cartera interactiva: kaspersky.com/int_portfolio

latam.kaspersky.com

Hemos pasado pruebas. Somos independientes. Somos transparentes. Estamos comprometidos con la construcción de un mundo más seguro, en el que la tecnología mejore nuestras vidas. Por eso la protegemos, para que todas las personas del mundo puedan beneficiarse de las oportunidades que ofrece la tecnología. Incorpore ciberseguridad para disfrutar un futuro más seguro.

Más información en kaspersky.es/transparency

Proven. Transparent. Independent.