kaspersky BRING ON THE FUTURE

EDR: ¿qué y cómo?

Se habla mucho en el mercado sobre de que la detección y la respuesta en endpoints (EDR, por sus siglas en inglés) es la gran novedad. Según Gartner1, por ejemplo: "Las herramientas de EDR proporcionan un método para que los profesionales técnicos en materia de seguridad y gestión del riesgo respondan dos preguntas claves sobre la seguridad del entorno:

- ¿Qué sucedió aquí?
- ¿ Qué sucede en este momento?"

Pero ¿qué significa esto en la práctica y por qué es tan importante para las organizaciones complementar sus plataformas de protección de endpoints (EPP, por sus siglas en inglés) con herramientas de EDR o con detección y respuesta administradas (MDR, por sus siglas en inglés)?

¿Qué?

En los últimos años, la tendencia de la ciberseguridad ha sido que, en lugar de las amenazas de productos, que son relativamente fáciles de detectar y prevenir con la EPP, los cibercriminales se enfoquen más y más en las amenazas "evasivas" diseñadas específicamente para eludir las medidas existentes de protección de endpoints.

Una de las razones es que es cada vez más fácil (y más barato) para los cibercriminales encontrar, combinar y probar herramientas y métodos preparados (incluidas campañas de "rentar un malware" con asistencia técnica ininterrumpida), y que los ataques de este tipo prometen mayores posibilidades de éxito que los métodos tradicionales.

Sumado a esto, está el aumento del trabajo remoto que está disolviendo el perímetro corporativo de muchas organizaciones. Y es fácil ver por qué los endpoints se mantendrán en la primera línea de batalla contra cibercriminales en el futuro cercano.

Entonces, ¿qué sucede cuando la EPP se enfrenta a una amenaza cibernética evasiva? Estas amenazas no solo son difíciles de detectar debido al la variedad de técnicas de evasión adoptadas, sino, en especial, al uso de herramientas legítimas y nativas del sistema. Como permanecen sin ser detectadas por más tiempo, estas amenazas también tienen el tiempo necesario para explorar y atrincherarse en la infraestructura de la empresa y hacer un daño mayor, por ejemplo, una vulneración de datos, un ataque de ransomware o spyware, o la anulación directa de las operaciones.

¿El resultado? El impacto financiero promedio de una filtración de datos2 es de 101 000 dólares para las pymes y de 1 090 000 dólares para las grandes empresas. Además, mientras más lenta sea la respuesta, más grande será el impacto promedio, que se eleva a 118 000 y 1 340 000 dólres, respectivamente, para respuestas que requieren más de una semana. Con impactos como estos, en lugar de preguntar "¿por qué debemos invertir en EDR?", un mejor interrogante para muchas empresas es "¿por qué aún no hemos invertido?"

¿Cómo?

Entonces, ¿en qué (y cuándo) lo ayudará la inversión en EDR? En términos simples, cada vez que reciba una alerta, EDR le ayudará a entender de dónde proviene la amenaza, cómo se desarrolló, cuál es la causa raíz, si ha afectado a otro host y, por lo tanto, qué dimensiones tiene.

---

[1] Gartner: Solution Comparison for Endpoint Detection and Response Technologies and Solutions, enero del 2020

[2] Kaspersky, Economía de la seguridad de TI, 2020)

Si desea fortalecer sus defensas internas o luchar contra las últimas amenazas con orientación externa experta, Kaspersky puede ayudarlo. Nuestro Kaspersky Optimum Security habilitado para la nube le permite actualizar la protección contra amenazas nuevas, desconocidas y evasivas a través de una detección y respuesta de amenazas efectivas y un monitoreo de seguridad 24/7 sin costos ni complejidad prohibitivos.

También debe guiarlo a través de un sencillo proceso de manejo de incidentes, que incluya pasos como la identificación, la contención, la erradicación, la recuperación y el análisis de las lecciones aprendidas con el fin de prepararse para futuros ataques. Por ejemplo:

- **Identificación.** ¿Qué encontró la herramienta de EDR? ¿Es una amenaza común o grave? ¿Se requiere una respuesta acorde al contexto y los detalles sobre la amenaza y el incidente que esta creó?
- **Contención.** ¿Qué se debe hacer con la amenaza? Por ejemplo, ¿aislar el host, impedir la ejecución o poner en cuarentena los archivos sospechosos?
- **Erradicación.** Usar un análisis de indicadores de compromiso (IoC) para buscar y eliminar archivos relacionados, junto con cualquier otro proceso necesario para erradicar la amenaza.
- **Recuperación**. Devolver la red a la normalidad. Por ejemplo, si se aisló un host infectado para evitar la propagación de la infección, se lo puede sacar del aislamiento.
- **Analizar las lecciones aprendidas.** Por ejemplo, integrar los datos de IoC en las herramientas de seguridad existentes, revisar el acceso y los controles web, bloquear el acceso a determinadas direcciones IP o cuentas de correo electrónico, o introducir capacitación de concientización en seguridad para ayudar a los empleados a comprender y detectar mejor las amenazas de seguridad modernas.

En resumen, tanto si usa una herramienta de EDR interna o una MDR, la solución debe trabajar junto con la EPP para bloquear una gran cantidad de amenazas de forma automática y, cuando se produzcan incidentes, permitirle investigarlos de forma más eficiente. Esto significa obtener más información sobre lo que sucede detrás de escena para comprender mejor las amenazas que ve; además, ser capaz de responder de manera rápida y sencilla y buscar otros dispositivos que también puedan estar en riesgo y, así, fortalecer sus medidas de seguridad, sobre todo las relativas a amenazas nuevas, desconocidas y evasivas.

Ya sea que quiera fortalecer las defensas internas o combatir las amenazas más recientes con una orientación de expertos externos, Kaspersky puede ayudarle. Nuestra solución Kaspersky Optimum Security basada en la nube le permite actualizar la protección contra amenazas nuevas, desconocidas y evasivas mediante la detección y respuesta eficaces contra amenazas y la supervisión de seguridad ininterrumpida, sin que los costos ni la complejidad se hagan prohibitivos.

Obtenga más información en go.kaspersky.com/es_mx_optimum

saber más acerca de go.kaspersky.com/optimum

Kaspersky Optimum Security

Noticias sobre amenazas cibernéticas: www.securelist.com
Noticias de seguridad de TI: business.kaspersky.com
Seguridad de TI para pequeñas y medianas empresas: kaspersky.com/business
Seguridad de TI para empresas: kaspersky.com/enterprise
Portal de inteligencia sobre amenazas: opentip.kaspersky.com
Herramienta de cartera interactiva: kaspersky.com/int_portfolio

www.kaspersky.com

Estamos probados. Somos independientes.
Somos transparentes. Estamos comprometidos con la construcción de una entorno más seguro del mundo, donde la tecnología mejora nuestras vidas. Por eso te protegemos, para que todos en todas partes tiene un sinfín de oportunidades que trae. traer seguridad cibernética para un mañana más seguro.

Obtenga más información en kaspersky.com/transparency

Proven. Transparent. Independent.