**Métodos de detección de incidentes de ciberseguridad**

Los analistas de seguridad usan herramientas de detección que los ayudan a descubrir amenazas, pero además, existen otros métodos de detección que pueden ser útiles.

Anteriormente, aprendiste cómo las herramientas de detección pueden identificar ataques como la exfiltración de datos. En esta lección, conocerás diferentes métodos de detección que las organizaciones pueden utilizar para descubrir amenazas.

**Métodos de detección**

Durante la **fase de detección y análisis** del ciclo de vida de respuesta a incidentes, los equipos de seguridad reciben una notificación de un posible incidente y trabajan para investigarlo y verificarlo mediante la recopilación y el análisis de datos. Como recordatorio, la **detección** es el descubrimiento rápido de eventos de seguridad, y el **análisis** implica la investigación y validación de alertas.

Como has aprendido, un sistema de detección de intrusiones (IDS) puede detectar posibles intrusiones y enviar alertas a los analistas de seguridad para que investiguen la actividad sospechosa. Estos, además, pueden utilizar las herramientas de gestión de eventos e información de seguridad (SIEM) para detectar, recopilar y analizar datos de seguridad.

También has aprendido que la detección presenta desafíos. Incluso los mejores equipos de seguridad pueden no detectar amenazas reales por distintas razones. Por ejemplo, las herramientas de detección pueden encontrar únicamente aquello que los equipos de seguridad han configurado para que monitoreen. Si no están configuradas correctamente, es posible que no identifiquen actividades sospechosas, y que los sistemas queden vulnerables a ataques. Por esto, es importante que los equipos de seguridad utilicen métodos adicionales de detección para aumentar su cobertura y precisión.

**Caza de amenazas**

Las amenazas evolucionan y los atacantes avanzan en sus tácticas y técnicas. La detección automatizada y basada en la tecnología puede resultar insuficiente a la hora de mantenerse al día con el panorama de amenazas en constante evolución. La detección impulsada por el ser humano, como la caza de amenazas, combina el poder de la tecnología con un elemento humano para así descubrir amenazas ocultas que las herramientas de detección no logran captar.

**La caza de amenazas** es la búsqueda proactiva de amenazas en una red. Los profesionales de la seguridad la utilizan para descubrir actividades maliciosas que no fueron identificadas por las herramientas de detección y como una forma de llevar a cabo un análisis más detallado de las detecciones. También se utiliza para detectar amenazas antes de que ocasionen daños. Por ejemplo, para las herramientas de detección es difícil identificar el malware sin archivos. Esta es una forma de software malicioso que utiliza técnicas sofisticadas de evasión, como esconderse en la memoria en lugar de usar archivos o aplicaciones, lo que le permite eludir los métodos tradicionales de detección, como el análisis de firmas. La caza de amenazas utiliza la combinación de análisis humano activo y tecnología para identificar amenazas como el malware sin archivos.

**Nota**: Los especialistas en caza de amenazas son conocidos como cazadores de amenazas. Los cazadores de amenazas investigan amenazas y ataques emergentes y luego determinan la probabilidad de que una organización sea vulnerable a un ataque en particular. Para lograrlo, utilizan una combinación de inteligencia sobre amenazas, indicadores de compromiso, indicadores de ataque y aprendizaje automático para buscar amenazas en una organización.

**Inteligencia sobre amenazas**

Las organizaciones pueden mejorar sus capacidades de detección si están al tanto del panorama de amenazas en evolución y comprenden la relación entre su entorno y los agentes de amenaza. Para conocer mejor las amenazas se utiliza la **inteligencia sobre amenazas**, que consiste en información basada en evidencia que proporciona contexto acerca de amenazas existentes o emergentes.

La inteligencia sobre amenazas puede provenir de fuentes privadas o públicas como las siguientes:

* **Informes de la industria**: Estos, a menudo, incluyen detalles sobre las tácticas, técnicas y procedimientos (TTP) del atacante.
* **Avisos gubernamentales:** Al igual que los informes de la industria, los avisos gubernamentales ofrecen información sobre los TTP de los atacantes.
* **Fuentes de datos de amenazas**: Proporcionan información relacionada con amenazas, la cual puede utilizarse como protección contra atacantes sofisticados, como las **amenazas persistentes avanzadas (APT)**. Las APT son instancias en las que un agente de amenaza mantiene acceso no autorizado a un sistema durante un período prolongado de tiempo. Los datos suelen ser una lista de indicadores, como direcciones IP, dominios y hashes de archivos.

**Nota**: Las fuentes de datos de inteligencia de amenazas son importantes para agregar contexto a las detecciones, aunque no deben ser lo único que consideres a la hora de detectar y es necesario evaluarlas antes de ser utilizadas en una organización.

**Ciberengaño**

Se denomina ciberengaño a las técnicas que engañan deliberadamente a los agentes de amenaza con el objetivo de aumentar la detección y mejorar las estrategias defensivas.

Los **honeypots** (sistemas trampa o señuelos) son un ejemplo de un mecanismo activo de defensa cibernética que utiliza tecnología del engaño. Los honeypots son sistemas o recursos que se crean como señuelos vulnerables a ataques con el propósito de atraer posibles intrusos. Por ejemplo, se puede tener un archivo falso con la etiqueta *Información de tarjetas de crédito* *de clientes - 2022* para engañar a los agentes de amenaza y que estos accedan al archivo porque parece legítimo. Una vez que un agente de amenaza intenta acceder a este archivo, los equipos de seguridad son alertados.

**Conclusiones clave**

Se pueden implementar diversos métodos de detección para identificar y localizar eventos de seguridad en un entorno. Es esencial que las organizaciones utilicen una gran variedad de métodos, herramientas y tecnologías de detección para adaptarse a un panorama de amenazas en constante evolución, y proteger mejor los activos.

**Recursos para obtener información adicional**

Si deseas explorar más sobre la caza de amenazas y la inteligencia sobre amenazas, puedes acudir a recursos como los siguientes:

* Un [repositorio informativo sobre la caza de amenazas del](https://www.threathunting.net/) Proyecto ThreatHunting
* Investigación sobre [hackers patrocinados por el estado](https://blog.google/threat-analysis-group/) realizada por el Grupo de Análisis de Amenazas (TAG)

Marcar como completo

Me gusta

No me gusta

Informar de un problema