**Descripción general de las herramientas de detección**

Anteriormente, exploraste las tecnologías de **sistema de detección de intrusiones** (**IDS**) y **sistemas de prevención de intrusiones** (**IPS**). En esta lectura, compararás y contrastarás estas herramientas y aprenderás sobre la **detección y respuesta de puntos de conexión** (**EDR**). Como analista de seguridad, es probable que trabajes con estas herramientas, por lo que te será de utilidad conocer sus funciones.

**Por qué necesitas herramientas de detección**

Las herramientas de detección funcionan de forma similar a los sistemas de seguridad para el hogar. Mientras que estos últimos monitorean y protegen las viviendas contra intrusiones, las herramientas de detección de ciberseguridad ayudan a las organizaciones a resguardar sus redes y sistemas contra accesos no deseados ni autorizados. Para que las organizaciones puedan proteger sus sistemas contra amenazas o ataques de seguridad, es fundamental que sean notificadas ante cualquier indicio de intrusión. Estas herramientas de detección mantienen a los profesionales de seguridad al tanto de la actividad que se desarrolla en una red o sistema. Para ello, monitorean de forma continua las redes y los sistemas en busca de cualquier actividad sospechosa. Una vez que se detecta algo inusual o sospechoso, la herramienta activa una alerta que notifica al profesional de seguridad, permitiéndole investigar y detener la posible intrusión.

**Herramientas de detección**

Como analista de seguridad, es probable que en algún momento te encuentres con herramientas de detección **IDS**, **IPS** y **EDR**. Por lo tanto, es importante que conozcas las diferencias que hay entre ellas. Aquí tienes una tabla comparativa que puede servirte como referencia:

| **Capacidad** | **IDS** | **IPS** | **EDR** |
| --- | --- | --- | --- |
| Detecta actividad maliciosa | ✓ | ✓ | ✓ |
| Previene las intrusiones | N/A | ✓ | ✓ |
| Registra la actividad | ✓ | ✓ | ✓ |
| Genera alertas | ✓ | ✓ | ✓ |
| Realiza análisis de comportamiento | N/A | N/A | ✓ |

**Descripción general de las herramientas IDS**

Un **sistema de detección de intrusiones** (**IDS**) es una aplicación que monitorea la actividad del sistema y emite alertas sobre posibles accesos no autorizados. Un IDS proporciona un seguimiento continuo de eventos de red para ayudar a protegerse contra amenazas o ataques de seguridad. El objetivo de un IDS es detectar actividades potencialmente maliciosas y generar una alerta. Un IDS *no* detiene ni previene la actividad. En su lugar, los profesionales de la seguridad investigarán la alerta y actuarán para detenerla, si es necesario.

Por ejemplo, un IDS puede enviar una alerta cuando identifica un inicio de sesión de usuario sospechoso, como una dirección IP desconocida que inicia sesión en una aplicación o un dispositivo a una hora inusual. Sin embargo, un IDS no detendrá ni impedirá acciones adicionales, como bloquear el inicio de sesión del usuario sospechoso.

Algunos ejemplos de herramientas de IDS incluyen Zeek, Suricata, Snort® y Sagan.

**Categorías de detección**

Como analista de seguridad, investigarás las alertas que genera un IDS. Existen cuatro tipos de categorías de detección que deberías conocer:

1. **Un verdadero positivo** es el resultado de un análisis o una detección en el que un sistema de seguridad identifica correctamente un incidente real.
2. **Un verdadero negativo** es el resultado de un análisis o una detección en el que un sistema de seguridad identifica correctamente la inexistencia de incidentes. Esto ocurre cuando no existe actividad maliciosa y no se dispara ninguna alerta.
3. **Un falso positivo** es el resultado de un análisis que detecta erróneamente una amenaza y dispara una alerta. Esto ocurre cuando un IDS identifica una actividad como maliciosa, pero no lo es. Los falsos positivos son una molestia para los equipos de seguridad, porque pierden tiempo y recursos investigando una alerta ilegítima.
4. **Un falso negativo** es el resultado de un análisis que no detecta una amenaza existente y, por lo tanto, no activa una alerta. Esto ocurre cuando sucede una actividad maliciosa pero un IDS no la detecta. Los falsos negativos son peligrosos porque dejan a los equipos de seguridad sin saber de ataques legítimos a los que pueden ser vulnerables.

**Descripción general de las herramientas IPS**

Un **sistema de prevención de intrusiones** (**IPS**) es una aplicación que monitorea la actividad del sistema en busca de actividades intrusivas y toma medidas para detenerlas. Un IPS funciona de manera similar a un IDS. Sin embargo, el IPS monitorea la actividad del sistema para detectar y alertar sobre intrusiones, *y* también toma medidas para *prevenir* la actividad y minimizar sus efectos. Por ejemplo, un IPS puede enviar una alerta y modificar una lista de control de acceso en un router, para bloquear tráfico específico en un servidor.

**Nota:** Muchas herramientas IDS también pueden funcionar como IPS. Herramientas como Suricata, Snort y Sagan tienen capacidades tanto de IDS como de IPS.

**Descripción general de las herramientas EDR**

La **detección y respuesta de puntos de conexión** (**EDR**) es una aplicación que monitorea la actividad maliciosa en un punto de conexión. Las herramientas de EDR se instalan en los **puntos de conexión,** es decir, cualquier dispositivo conectado a una red. Algunos ejemplos incluyen los dispositivos de usuario final, como computadoras, teléfonos y tabletas, entre otros.

Las herramientas EDR monitorean, registran y analizan la actividad del sistema del punto de conexión para identificar, alertar y responder a actividades sospechosas. A diferencia de las herramientas de IDS o IPS, las de EDR recopilan datos de actividad del punto de conexión y realizan *análisis de comportamiento* para identificar patrones de amenazas. El análisis de comportamiento utiliza la potencia del aprendizaje automático y la inteligencia artificial para analizar el comportamiento del sistema e identificar actividades maliciosas o inusuales. Las herramientas de EDR también utilizan la *automatización* para detener los ataques sin la intervención manual de los profesionales de seguridad. Por ejemplo, si una herramienta de EDR detecta un proceso inusual que se inicia en la estación de trabajo de un usuario y que normalmente no se utiliza, puede bloquear automáticamente la ejecución del proceso.

Open EDR®, Bitdefender™ Endpoint Detection and Response y FortiEDR™ son ejemplos de herramientas de EDR.

**Nota**: La gestión de eventos e información de seguridad (SIEM) también tiene capacidades de detección, que verás más adelante.

**Conclusiones clave**

Las organizaciones implementan herramientas de detección para obtener información acerca de la actividad que ocurre en sus entornos. IDS, IPS y EDR son diferentes tipos de herramientas de detección. Su valor radica en su capacidad para detectar, registrar, alertar y detener posibles actividades maliciosas.