**Herramientas y técnicas de detección**

En esta lectura, examinarás los diferentes tipos de tecnologías de sistemas de detección de intrusiones (IDS) y las alertas que estos generan. También aprenderás las dos técnicas que más suelen usar los sistemas de detección. Entender las capacidades y limitaciones de las tecnologías IDS y sus técnicas de detección te ayudará a interpretar la información de seguridad para identificar y analizar los eventos de seguridad y responder a ellos.

Como ya sabemos, un **sistema de detección de intrusiones (IDS)** es una aplicación que monitorea la actividad del sistema y alerta sobre posibles intrusiones. Las tecnologías IDS ayudan a las organizaciones a monitorear la actividad que se desarrolla en sus sistemas y redes para poder identificar indicios de actividad maliciosa. Según dónde decidas configurar un IDS, este puede estar basado en host o en red.

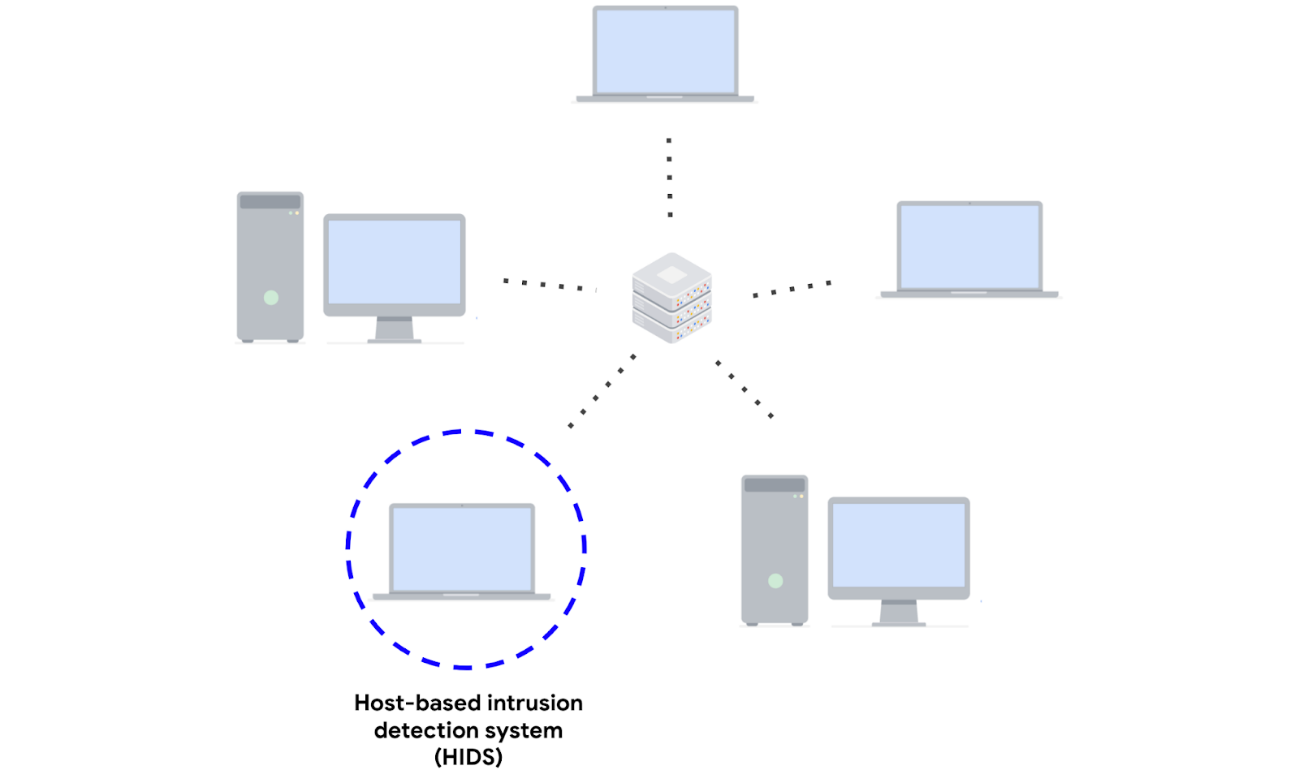
**Sistema de detección de intrusiones basado en host**

El **sistema de detección de intrusiones basado en host (HIDS)** es una aplicación que monitorea la actividad del host en el que está instalado. Se instala como un agente en un host. Al host también se lo conoce como **punto de conexión**,que es cualquier dispositivo conectado a una red, como una computadora o un servidor.

Por lo general, los agentes de HIDS se instalan en todos los puntos de conexión y se utilizan para controlar y detectar amenazas de seguridad. Un HIDS monitorea la actividad interna que ocurre en el host para identificar comportamientos no autorizados o anormales. Si detecta algo inusual, como la instalación de una aplicación no autorizada, el HIDS lo registra y envía una alerta.

Además de controlar los flujos de tráfico entrante y saliente, el HIDS puede tener otras capacidades, como supervisar los sistemas de archivos, el uso de los recursos del sistema, la actividad del usuario y más.

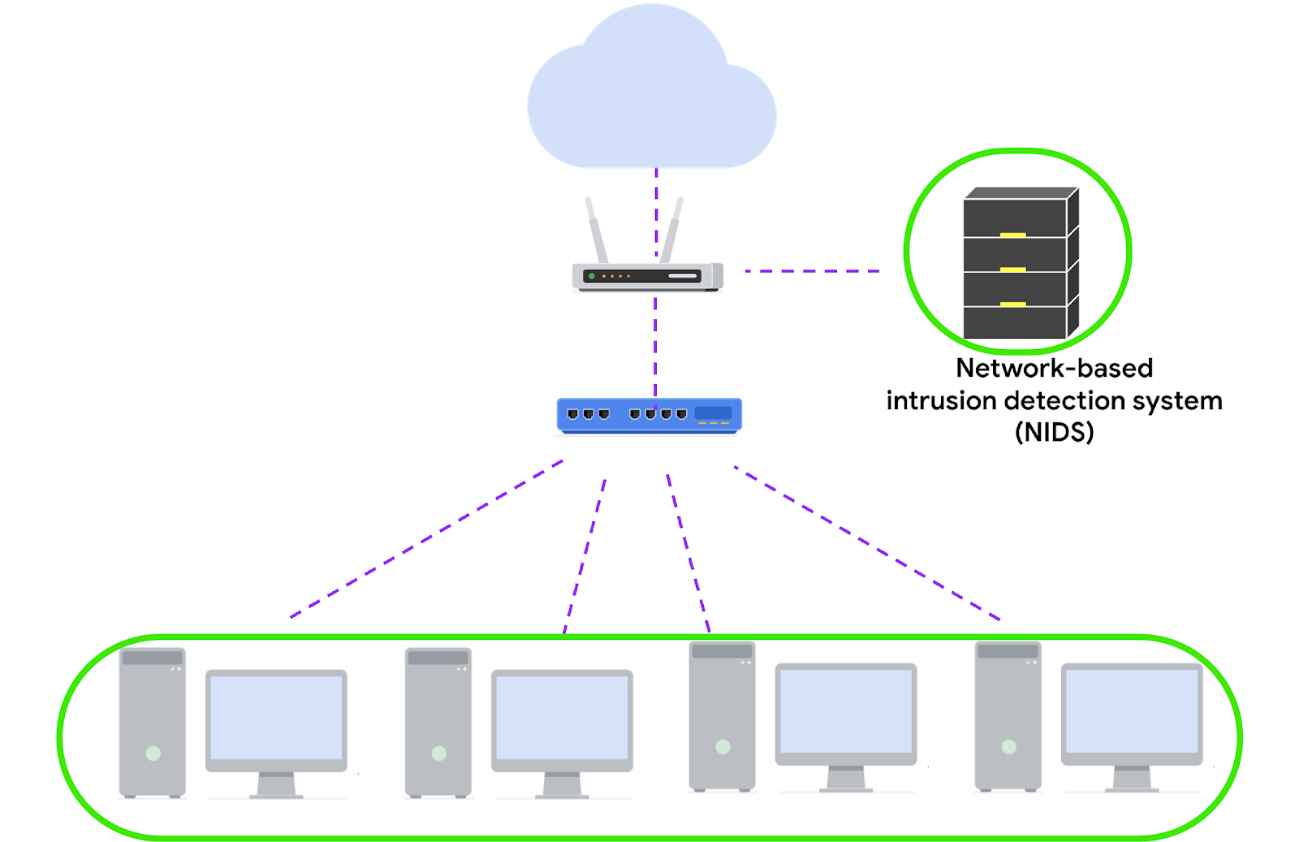
Este diagrama muestra una herramienta HIDS instalada en una computadora. El círculo punteado alrededor del host indica que solo está controlando la actividad local en esa computadora en la que está instalado.



**Sistema de detección de intrusiones basado en la red**

Un **sistema de detección de intrusiones basado en la red** **(NIDS)** es una aplicación que recopila y monitorea el tráfico de la red y sus datos. El software NIDS se instala en dispositivos ubicados en aquellas partes específicas de la red que se quiere monitorear. La aplicación NIDS inspecciona el tráfico de red desde diferentes dispositivos. Si detecta algún tráfico malicioso, lo registra y genera una alerta.

Este diagrama muestra un NIDS que está instalado en una red. El círculo resaltado alrededor del servidor y las computadoras indica que el NIDS está instalado en el servidor y está monitoreando la actividad de las computadoras.



Combinar un HIDS y un NIDS para monitorear un entorno puede ofrecer un enfoque multicapa para detectar intrusiones y darles respuesta. Ambas herramientas proporcionan una perspectiva diferente sobre la actividad que ocurre en una red y cada uno de los hosts que están conectados a ella. Esto aporta una visión integral de la actividad que se está desarrollando en un entorno.

**Técnicas de detección**

Los sistemas de detección pueden utilizar diferentes técnicas para detectar amenazas y ataques. Los dos tipos de técnicas de detección más utilizados por las tecnologías IDS son el análisis basado en firmas y el análisis basado en anomalías.

**Análisis basado en firmas**

**El análisis de firmas**, o análisis basado en firmas, es un método de detección que se utiliza para encontrar eventos de interés. Una **firma** es un patrón asociado con actividad maliciosa. Las firmas pueden contener patrones específicos, como una secuencia de números binarios, bytes o incluso datos específicos (como una dirección IP).

Anteriormente, exploraste la pirámide del dolor, un concepto que prioriza los diferentes tipos de **indicadores de compromiso** (IoC) asociados con un ataque o amenaza, como direcciones IP, herramientas, tácticas, técnicas y demás. Los IoC y otros indicadores de ataque pueden ser útiles para crear firmas dirigidas para detectar y bloquear ataques.

Se pueden usar diferentes tipos de firmas según el tipo de amenaza o ataque que quieras detectar. Por ejemplo, una firma antimalware contiene patrones asociados con el malware. Esto puede incluir los scripts maliciosos que suele utilizar el malware. Las herramientas de IDS revisarán un entorno en busca de eventos que coincidan con los patrones definidos en esta firma de malware. Si un evento coincide con la firma, este se registra y se genera una alerta.

**Ventajas**

* **Baja tasa de falsos positivos:** El análisis basado en firmas es muy eficiente para detectar amenazas conocidas porque simplemente compara la actividad con las firmas y esto arroja menos falsos positivos. Recuerda que un **falso positivo** es una alerta que detecta incorrectamente la presencia de una amenaza, ya que esta no existe.

**Desventajas**

* **Las firmas se pueden eludir:** Al ser únicas, los atacantes pueden modificar sus comportamientos de ataque para evitarlas. Por ejemplo, pueden hacer pequeñas modificaciones en el código de malware para alterar su firma y evitar su detección.
* **Las firmas requieren actualizaciones:** El análisis basado en firmas depende de una base de datos de firmas para detectar amenazas. Cada vez que se descubre un nuevo exploit o ataque, es necesario crear nuevas firmas y agregarlas a la base de datos de firmas.
* **Es incapaz de detectar amenazas desconocidas:** El análisis basado en firmas se basa en la detección de amenazas conocidas a través de firmas. No es posible detectar amenazas desconocidas, como familias de malware nuevas o ataques de **día cero**, que son vulnerabilidades recién descubiertas.

**Análisis basado en anomalías**

El **análisis basado en anomalías** es un método de detección que identifica comportamiento anormal. En este tipo de análisis hay dos fases: aprendizaje y detección. Durante la fase de aprendizaje, es necesario crear un valor de referencia de lo que sería un comportamiento normal o esperado. Estos valores de referencia se desarrollan recopilando datos que corresponden al comportamiento normal del sistema. Durante la fase de detección, la actividad actual del sistema se compara con este valor de referencia. La actividad que está por fuera de ese valor se registra, y se genera una alerta.

**Ventajas**

* **Capacidad para detectar amenazas nuevas y en evolución:** A diferencia del análisis basado en firmas, que utiliza patrones conocidos para detectar amenazas, el análisis basado en anomalías *puede* detectar amenazas desconocidas.

**Desventajas**

* **Alta tasa de falsos positivos:** Cualquier comportamiento que se desvíe del valor de referencia se puede marcar como anormal, incluidos los comportamientos no maliciosos. Esto arroja una alta tasa de falsos positivos.
* **Compromiso preexistente:** La existencia de un atacante durante la fase de aprendizaje incluirá un comportamiento malicioso en el valor de referencia. Esto puede llevar a pasar por alto a un atacante preexistente.

**Conclusiones clave**

Las tecnologías IDS son herramientas de seguridad esenciales con las que te encontrarás en tu trayectoria en el campo de la ciberseguridad. En resumen, un NIDS monitorea toda una red, mientras que un HIDS monitorea cada uno de los puntos de conexión. Las tecnologías IDS generan diferentes tipos de alertas y utilizan distintas técnicas de detección, como el análisis basado en firmas o en anomalías, para identificar actividades maliciosas.