**Endurecimiento de seguridad (security hardening)**

El Endurecimiento de seguridad es el proceso de reforzar un sistema para reducir su vulnerabilidad y superficie de ataque. Todas las vulnerabilidades potenciales que un Agente de amenaza podría explotar se denominan superficie de ataque de un sistema. Usemos un ejemplo que compare una red con una casa. La superficie de ataque serían todas las puertas y ventanas que un ladrón podría utilizar para acceder a esa casa. Al igual que poner cerraduras en todas las puertas y ventanas de la casa, el endurecimiento de la seguridad implica minimizar la superficie de ataque o las vulnerabilidades potenciales y mantener una red lo más segura posible.

Como parte del endurecimiento de seguridad, los analistas de seguridad realizan procedimientos regulares de mantenimiento para mantener los dispositivos y sistemas de red funcionando de forma segura y óptima. El endurecimiento de seguridad puede llevarse a cabo en cualquier dispositivo o sistema que pueda verse comprometido, como hardware, sistemas operativos, aplicaciones, redes informáticas y bases de datos. La seguridad física también forma parte del endurecimiento de la seguridad. Puede incluir la protección de un espacio físico con cámaras de seguridad y guardias de seguridad.

Algunos tipos comunes de procedimientos de endurecimiento incluyen actualizaciones de software, también llamadas parches, y cambios en la configuración de aplicaciones de dispositivos. Estas actualizaciones y cambios se realizan para aumentar la seguridad y corregir vulnerabilidades de seguridad en una red. Un ejemplo de cambio en la configuración de seguridad sería exigir contraseñas más largas o cambios de contraseña más frecuentes. Esto dificulta que un actor malicioso obtenga credenciales de inicio de sesión. Un ejemplo de comprobación de la configuración es la actualización de los Estándares de encriptación para los datos que se almacenan en una Base de datos. Mantener la encriptación al día dificulta que actores maliciosos accedan a la base de datos.

Otros ejemplos de endurecimiento de la seguridad incluyen la eliminación o desactivación de aplicaciones y servicios no utilizados, la desactivación de puertos no utilizados y la reducción de los permisos de acceso en los dispositivos y la red. Minimizar el número de aplicaciones, dispositivos, puertos y permisos de acceso hace que la supervisión de la red y los dispositivos sea más eficiente y reduce la superficie de ataque global, que es una de las mejores formas de asegurar una organización.

Otra estrategia importante para endurecer la seguridad es realizar pruebas de penetración periódicas. Una prueba de penetración, también llamada pen test, es un ataque simulado que ayuda a identificar vulnerabilidades en un sistema, red, sitio web, aplicación y proceso. Los encargados de las pruebas de penetración documentan sus hallazgos en un Informe. Dependiendo de dónde falle la prueba, los equipos de seguridad pueden determinar el tipo de vulnerabilidades de seguridad que requieren reparación. Las organizaciones pueden entonces revisar estas vulnerabilidades y elaborar un plan para solucionarlas.

**Prácticas de endurecimiento del OS**

El sistema operativo es la interfaz entre el hardware de la computadora y el usuario. El OS es el primer programa que se carga cuando se enciende una computadora. El OS actúa como intermediario entre las aplicaciones de software y el hardware del ordenador. Es importante asegurar el OS en cada sistema porque un OS inseguro puede llevar a que toda una red se vea comprometida. Hay muchos tipos de sistemas operativos, y todos ellos comparten prácticas de endurecimiento de seguridad similares. Hablemos de algunas de esas prácticas de endurecimiento de seguridad que se recomiendan para asegurar un OS.

**Ataques de fuerza bruta**

Un **ataque de fuerza bruta** es un proceso de ensayo y error para descubrir información privada. Existen diferentes tipos de ataques de fuerza bruta que los actores maliciosos utilizan para adivinar contraseñas, entre ellos:

* *Ataques de fuerza bruta simples.* Cuando los atacantes intentan adivinar las credenciales de inicio de sesión de un usuario, se considera un ataque de fuerza bruta simple. Pueden hacerlo introduciendo cualquier combinación de nombres de usuario y contraseñas que se les ocurra hasta encontrar la que funcione.
* *Los ataques de diccionario* utilizan una técnica similar. En los ataques de diccionario, los atacantes utilizan una lista de contraseñas de uso común y credenciales robadas en violaciones anteriores para acceder a un sistema. Se denominan ataques de diccionario porque los atacantes utilizaban originalmente una lista de palabras del diccionario para adivinar las contraseñas, antes de que las reglas de contraseñas complejas se convirtieran en una práctica habitual de Seguridad.

Utilizar la fuerza bruta para acceder a un sistema puede ser un proceso tedioso y lento, sobre todo cuando se hace manualmente. Existe un Rango de herramientas que los atacantes utilizan para llevar a cabo sus ataques.

**Evaluar las vulnerabilidades**

Antes de que se produzca un ataque de fuerza bruta u otro incidente de ciberseguridad, las empresas pueden realizar una serie de pruebas en su red o en sus aplicaciones web para evaluar las vulnerabilidades. Los analistas pueden utilizar máquinas virtuales y cajas de arena para probar archivos sospechosos, comprobar vulnerabilidades antes de que se produzca un evento o simular un incidente de ciberseguridad.

**Máquinas virtuales (VM)**

Las máquinas virtuales (VM) son versiones de software de las computadoras físicas. Las VM proporcionan una capa adicional de Seguridad para una organización porque pueden utilizarse para ejecutar código en un entorno aislado, evitando que el código malicioso afecte al resto de la computadora o del sistema. Las VM también pueden eliminarse y sustituirse por una imagen prístina después de probar software malicioso.

Las VM son útiles cuando se investigan máquinas potencialmente infectadas o se ejecuta software malicioso en un entorno restringido. El uso de una VM puede evitar daños en su sistema en el caso de que sus herramientas se utilicen de forma inadecuada. Las VM también le ofrecen la posibilidad de volver a un estado anterior. Sin embargo, las máquinas virtuales conllevan algunos Riesgos. Todavía existe un pequeño Riesgo de que un programa malicioso pueda escapar a la virtualización y acceder a la máquina anfitriona.

Puede probar y explorar aplicaciones fácilmente con las máquinas virtuales, y es fácil cambiar entre diferentes máquinas virtuales desde su computadora. Esto también puede ayudar a agilizar muchas tareas de Seguridad.

**Espacios aislados**

Un entorno aislado es un tipo de entorno de pruebas que le permite ejecutar software o programas separados de su red. Suelen utilizarse para probar parches, Identificar y solucionar errores o Detectar vulnerabilidades de ciberseguridad. Los espacios aislados también pueden utilizarse para evaluar software sospechoso, evaluar archivos que contienen código malicioso y simular escenarios de ataque.

Los cajones de arena pueden ser ordenadores físicos autónomos que no están conectados a una red; sin embargo, a menudo es más rentable y económico utilizar software o máquinas virtuales basadas en la nube como entornos de cajones de arena. Tenga en cuenta que algunos autores de software malicioso saben cómo escribir código para detectar si el software malicioso se ejecuta en una VM o en un entorno de caja de arena. Los atacantes pueden programar su software malicioso para que se comporte como software inofensivo cuando se ejecuta dentro de este tipo de entornos de pruebas.

**Medidas de prevención**

Algunas medidas comunes que las organizaciones utilizan para evitar que se produzcan ataques de fuerza bruta y ataques similares incluyen:

* **Salting y hash:** El hash convierte la información en un valor único que puede utilizarse para determinar su integridad. Es una función unidireccional, lo que significa que es imposible desencriptar y obtener el texto original. El salting añade caracteres aleatorios a las contraseñas hash. Esto aumenta la Longitud y la complejidad de los valores hash, haciéndolos más seguros.
* **Autenticación de múltiples factores (MFA) y autenticación de dos factores (2FA):** MFA es una medida de seguridad que requiere que un usuario verifique su identidad de dos o más formas para acceder a un sistema o red. Esta autenticación se realiza mediante una combinación de factores de autenticación: un nombre de usuario y una contraseña, huellas dactilares, reconocimiento facial o una contraseña de un solo uso (OTP) enviada a un número de teléfono o a un correo electrónico. la 2FA es similar a la MFA, salvo que sólo utiliza dos formas de verificación.
* **CAPTCHA y reCAPTCHA:** CAPTCHA son las siglas de Completely Automated Public Turing test to tell Computers and Humans Apart (Prueba de Turing pública completamente automatizada para distinguir entre ordenadores y humanos). Pide a los usuarios que completen una sencilla prueba que demuestra que son humanos. Esto ayuda a evitar que el software intente forzar una contraseña. reCAPTCHA es un servicio CAPTCHA gratuito de Google que ayuda a proteger los sitios web de bots y software malicioso.
* **Políticas de contraseñas:** Las organizaciones utilizan políticas de contraseñas para estandarizar las buenas prácticas de contraseñas en toda la empresa. Las políticas pueden incluir directrices sobre lo compleja que debe ser una contraseña, la frecuencia con la que los usuarios deben actualizar las contraseñas, si las contraseñas se pueden reutilizar o no, y si hay límites en el número de veces que un usuario puede intentar iniciar sesión antes de que se suspenda su cuenta.

**Puntos clave**

Los ataques de fuerza bruta son un proceso de ensayo y error para adivinar contraseñas. Los ataques pueden lanzarse manualmente o mediante herramientas de software. Los métodos incluyen ataques de fuerza bruta simples y ataques de diccionario. Para protegerse contra los ataques de fuerza bruta, los analistas de ciberseguridad pueden utilizar sandboxes para probar archivos sospechosos, comprobar vulnerabilidades o simular ataques reales y máquinas virtuales para realizar pruebas de vulnerabilidad. Algunas medidas comunes para prevenir los ataques de fuerza bruta incluyen: hash y salting, MFA y/o 2FA, CAPTCHA y reCAPTCHA, y políticas de contraseña.

**Prácticas de endurecimiento de la red**

Anteriormente, aprendió que el endurecimiento del OS se centra en la seguridad de los dispositivos y utiliza actualizaciones de parches, configuración segura y políticas de acceso a cuentas. Ahora nos centraremos en el endurecimiento de la red. El endurecimiento de la red se centra en el endurecimiento de la seguridad relacionada con la red, como el filtrado de puertos, los privilegios de acceso a la red, y la encriptación a través de redes. Ciertas tareas de endurecimiento de la red se realizan regularmente, mientras que otras se realizan una vez y luego se actualizan según sea necesario.

Algunas tareas que se realizan regularmente son el mantenimiento de las reglas del firewall, el análisis de registros de red, las actualizaciones de parches y las copias de seguridad de servidores. Antes, aprendió que un registro es un registro de eventos que ocurren dentro de los sistemas de una organización. El análisis de registros de red es el proceso de examinar los registros de red para identificar eventos de interés. Los equipos de seguridad utilizan una herramienta de análisis de registros o una herramienta de gestión de eventos e información de seguridad, también conocida como SIEM, para llevar a cabo el análisis de registros de red. Una herramienta SIEM es una aplicación que recopila y analiza datos de registro para supervisar actividades críticas en una organización. Reúne datos de seguridad de una red y presenta esos datos en un único cuadro de mandos. La interfaz del cuadro de mandos se denomina a veces un único panel de cristal. Un SIEM ayuda a los analistas a inspeccionar, analizar, y reaccionar ante eventos de seguridad en toda la red en función de su prioridad. Los informes del SIEM proporcionan una lista de vulnerabilidades de red nuevas o en curso y las enumeran en una escala de prioridad de alta a baja, en la que las vulnerabilidades de alta prioridad tienen un plazo mucho más corto para su mitigación.

Ahora que hemos cubierto las tareas que se realizan con regularidad, examinemos las tareas que se realizan una vez. Estas tareas incluyen el filtrado de puertos en cortafuegos, los privilegios de acceso a la red y la encriptación para la comunicación, entre otras muchas cosas. Comencemos con el filtrado de puertos. El filtrado de puertos puede formarse a través de la Red. El filtrado de puertos es una función del cortafuegos que bloquea o permite ciertos números de puerto para limitar la comunicación no deseada. Un principio básico es que los únicos puertos que son necesarios son los que están permitidos. Cualquier puerto que no esté siendo utilizado por las operaciones normales de la red debe ser desautorizado. Esto protege contra las vulnerabilidades de los puertos. Las redes deberían configurarse con los protocolos inalámbricos más actualizados disponibles y los protocolos inalámbricos más antiguos deberían desactivarse. Los analistas de seguridad también utilizan la segmentación de red para crear subredes aisladas para diferentes departamentos de una organización. Por ejemplo, podrían hacer una para el departamento de marketing y una para el departamento financiero. Esto se hace para que los problemas de cada subred no se extiendan por toda la empresa y sólo los usuarios especificados tengan acceso a la parte de la red que necesitan para su función. La segmentación de red también puede utilizarse para separar diferentes zonas de seguridad. Cualquier zona restringida de una red que contenga datos altamente clasificados o confidenciales debería estar separada del resto de la red. Por último, todas las comunicaciones de red deberían cifrarse utilizando los últimos estándares de cifrado. Los Estándares de encriptación son reglas o métodos utilizados para ocultar los datos salientes y descubrir o desencriptar los datos entrantes. Los datos en zonas restringidas deben tener unos Estándares de encriptación mucho más altos, lo que hace que sea más difícil acceder a ellos.

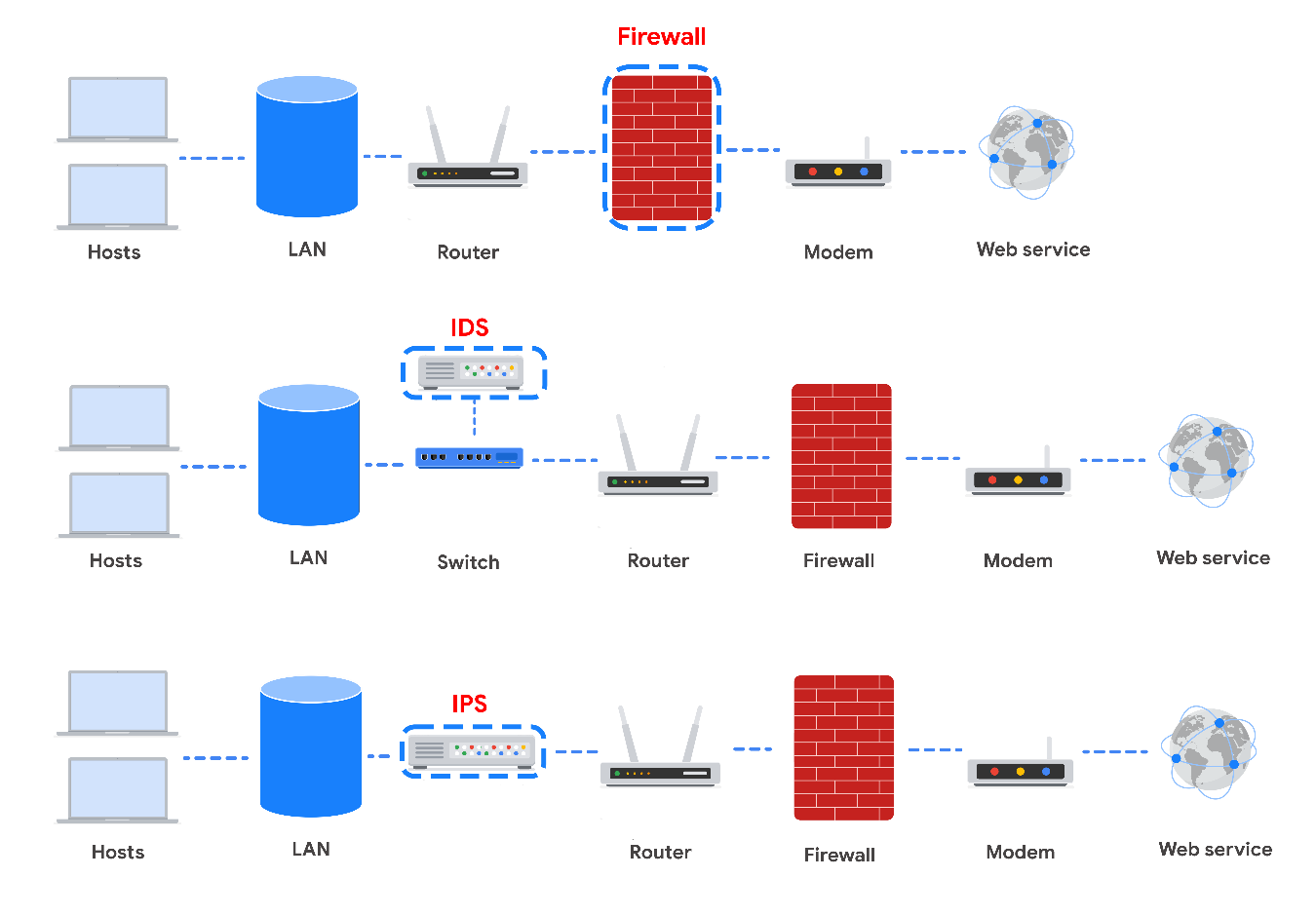
Ha aprendido las prácticas de endurecimiento más comunes. Estos conocimientos le serán útiles a medida que complete el programa de certificación y son esenciales para su carrera como analista de seguridad.

**Aplicaciones de Seguridad de red**

Esta sección del curso trata el tema del endurecimiento de la red y su supervisión. Cada dispositivo, herramienta o estrategia de seguridad puesta en marcha por los analistas de seguridad protege -o endurece- aún más la red hasta que el propietario de la red está satisfecho con el nivel de seguridad. Este enfoque de añadir capas de seguridad a una red se conoce como defensa en profundidad.

En esta lectura, va a conocer la Función de cuatro dispositivos utilizados para proteger una red: cortafuegos, sistemas de detección de intrusiones, sistemas de prevención de intrusiones y herramientas de gestión de incidentes y eventos de seguridad. Los profesionales de la Seguridad de red tienen la opción de utilizar cualquiera de estos dispositivos y herramientas, o todos ellos, en función del nivel de seguridad que esperen alcanzar.

En esta lectura se analizarán los beneficios de la Seguridad por capas. Cada herramienta mencionada es una capa adicional de defensa que puede endurecer una red de forma incremental, empezando por el nivel mínimo de seguridad (proporcionado sólo por un cortafuegos), hasta el nivel más alto de seguridad (proporcionado por la combinación de un cortafuegos, un dispositivo de detección y prevención de intrusiones y el monitoreo de eventos de seguridad).

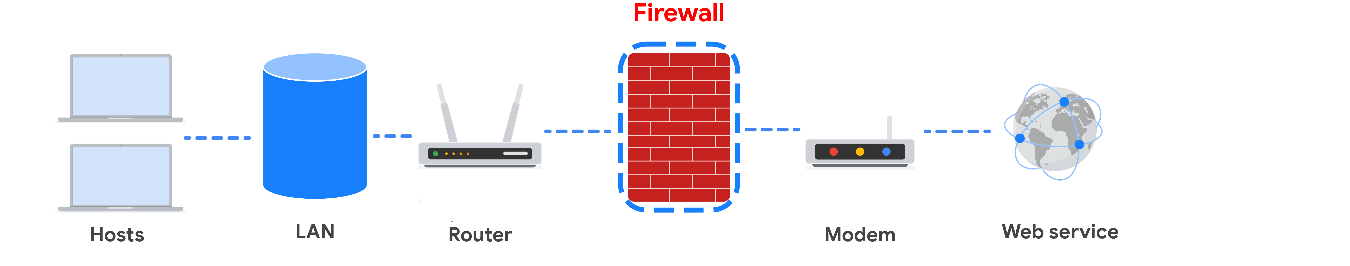


Tome nota de dónde se encuentra cada herramienta en la red. Cada herramienta tiene su propio lugar en la arquitectura de la red. Los analistas de seguridad deben comprender las topologías de red que se muestran en los diagramas a lo largo de esta lectura.

**Firewall**

Hasta ahora en este curso, ha aprendido sobre los firewalls sin estado, los firewalls con estado y los firewalls de nueva generación (NGFW), así como las ventajas de seguridad de cada uno de ellos.

La mayoría de los firewalls son similares en sus funciones básicas. Los firewalls permiten o bloquean el tráfico basándose en un conjunto de reglas. Cuando los paquetes de datos entran en una red, se inspecciona el encabezado del paquete y se permite o deniega en función de su número de puerto. Los NGFW también pueden inspeccionar la carga útil de los paquetes. Cada sistema debe tener su propio firewall, independientemente del cortafuegos de la red.

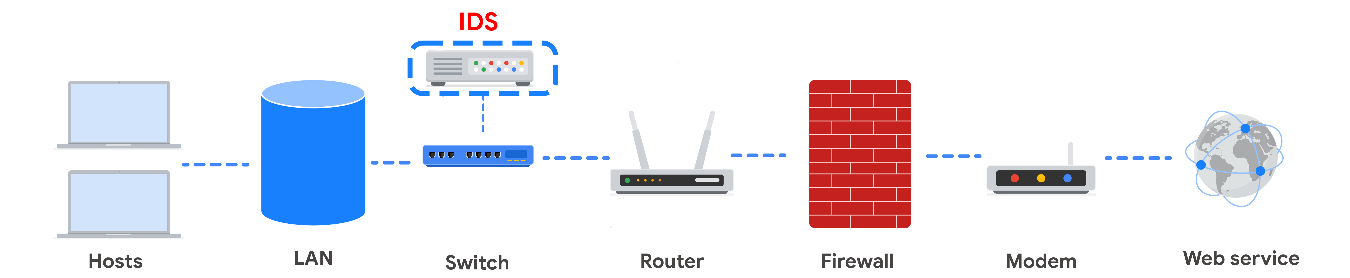


**Sistema de detección de intrusiones**

Un **Sistema de detección de intrusiones** (IDS) es una aplicación que monitoriza la actividad del sistema y alerta sobre posibles intrusiones. Un IDS alerta a los administradores basándose en la firma del tráfico malicioso.

El IDS está configurado para detectar ataques conocidos. Los sistemas IDS suelen olfatear los paquetes de datos mientras se desplazan por la red y los analizan en busca de las características de ataques conocidos. Algunos sistemas IDS revisan no sólo en busca de firmas de ataques conocidos, sino también de anomalías que podrían ser el signo de una actividad maliciosa. Cuando el IDS descubre una anomalía, envía una alerta al administrador de la red, que puede investigar más a fondo.

Las limitaciones de los sistemas IDS son que sólo pueden buscar ataques conocidos o anomalías evidentes. Los ataques nuevos y sofisticados podrían no ser detectados. La otra limitación es que el IDS no detiene realmente el tráfico entrante si detecta algo raro. Depende del administrador de la red detectar la actividad maliciosa antes de que cause algún daño a la red.

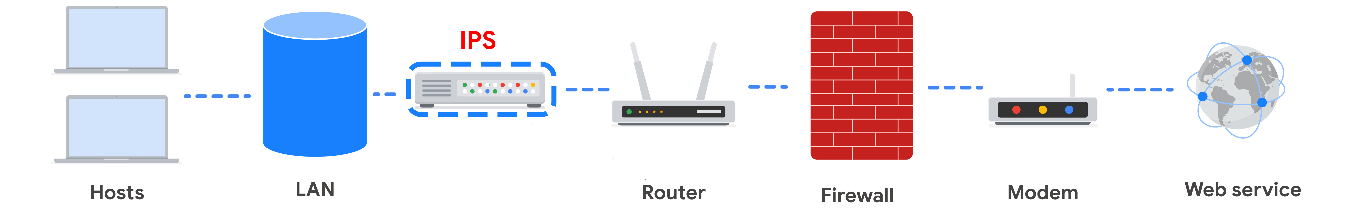


Cuando se combina con un firewall, un IDS añade otra capa de defensa. El IDS se coloca detrás del firewall y antes de entrar en la LAN, lo que permite al IDS analizar los flujos de Datos después de que el Tráfico de red no permitido por el firewall haya sido filtrado. Esto se hace para reducir el ruido en las alertas del IDS, también denominadas falsos positivos.

**Sistema de prevención de intrusiones**

Un **Sistema de prevención de intrusiones (IPS** ) es una aplicación que monitoriza la actividad del sistema en busca de actividades intrusivas y toma medidas para detenerlas. Ofrece incluso más protección que un IDS porque detiene activamente las anomalías cuando las detecta, a diferencia del IDS que simplemente informa de la anomalía a un administrador de red.

Un IPS busca firmas de ataques conocidos y anomalías en los Datos. Un IPS informa de la anomalía a los analistas de seguridad y bloquea un remitente específico o elimina los paquetes de red que parecen sospechosos.



El IPS (como un IDS) se sitúa detrás del firewall en la arquitectura de red. Esto ofrece un alto nivel de seguridad porque los flujos de datos arriesgados se interrumpen incluso antes de que lleguen a las partes sensibles de la red. Sin embargo, una limitación potencial es que está en línea: Si se rompe, se interrumpe la conexión entre la red privada e Internet. Otra limitación de los IPS es la posibilidad de que se produzcan falsos positivos, lo que puede hacer que se interrumpa el tráfico legítimo.

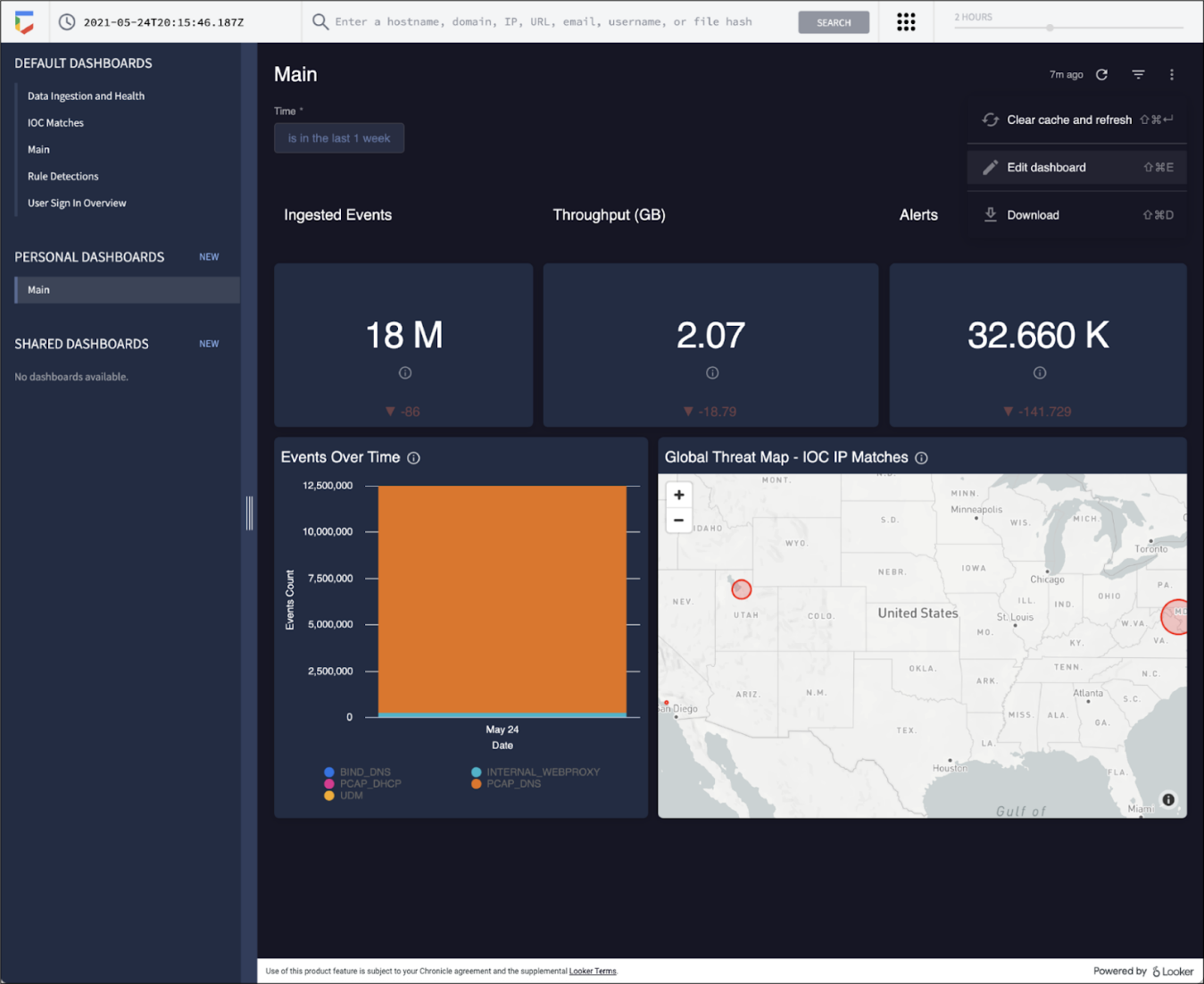
**Dispositivos de captura de paquetes completos**

Los dispositivos de captura de paquetes completos pueden ser increíblemente útiles para los administradores de redes y los profesionales de la Seguridad. Estos dispositivos le permiten registrar y analizar todos los Datos que se transmiten a través de su red. También ayudan a investigar las alertas creadas por un IDS.

**Administración de información y eventos de seguridad**

Un **sistema de administración de información y eventos de seguridad (SIEM** ) es una aplicación que recopila y analiza los datos de registro para supervisar las actividades críticas de una organización. Las herramientas SIEM trabajan en tiempo real para informar de las actividades sospechosas en un panel centralizado. Las herramientas SIEM analizan además los datos de registro de red procedentes de IDS, IPS, cortafuegos, VPN, proxies y registros DNS. Las herramientas SIEM son una forma de agregar los datos de los eventos de seguridad para que aparezcan todos en un mismo lugar y puedan ser analizados por los analistas de seguridad. Esto se conoce como un panel único de cristal.

A continuación, puede revisar un ejemplo de un panel de control de la herramienta SIEM de Google Nube, Chronicle. **Chronicle** es una herramienta nativa de la nube diseñada para retener, analizar y buscar datos.



**Splunk** es otra herramienta SIEM común. Splunk ofrece diferentes opciones de herramientas SIEM: Splunk Enterprise y Splunk Cloud. Ambas opciones incluyen cuadros de mando detallados que ayudan a los profesionales de la Seguridad a revisar y analizar los datos de una organización. También hay otras herramientas SIEM similares disponibles, y es importante que los profesionales de la Seguridad investiguen las diferentes herramientas para determinar cuál es la más beneficiosa para la organización.

Una herramienta SIEM no sustituye a los conocimientos de los analistas de seguridad ni a las actividades de refuerzo de redes y sistemas que se tratan en este curso, pero se utilizan en combinación con otros métodos de seguridad. Los analistas de seguridad suelen trabajar en un Centro de Operaciones de Seguridad (SOC) donde pueden supervisar la actividad en toda la red. A continuación, pueden utilizar sus conocimientos y experiencia para determinar cómo responder a la información del cuadro de mandos y decidir cuándo los eventos cumplen los criterios para ser escalados a supervisión.

Tabla

Descripción generada automáticamente**Puntos Clave**

La compra, instalación y mantenimiento de cada uno de estos dispositivos o herramientas cuesta dinero. Es posible que una organización necesite contratar personal adicional para monitorizar las herramientas de Seguridad, como en el caso de un SIEM. Los responsables de la toma de decisiones tienen la tarea de seleccionar el nivel apropiado de Seguridad basándose en el coste y el Riesgo para la organización. Más adelante aprenderá más sobre la elección de los niveles de Seguridad.