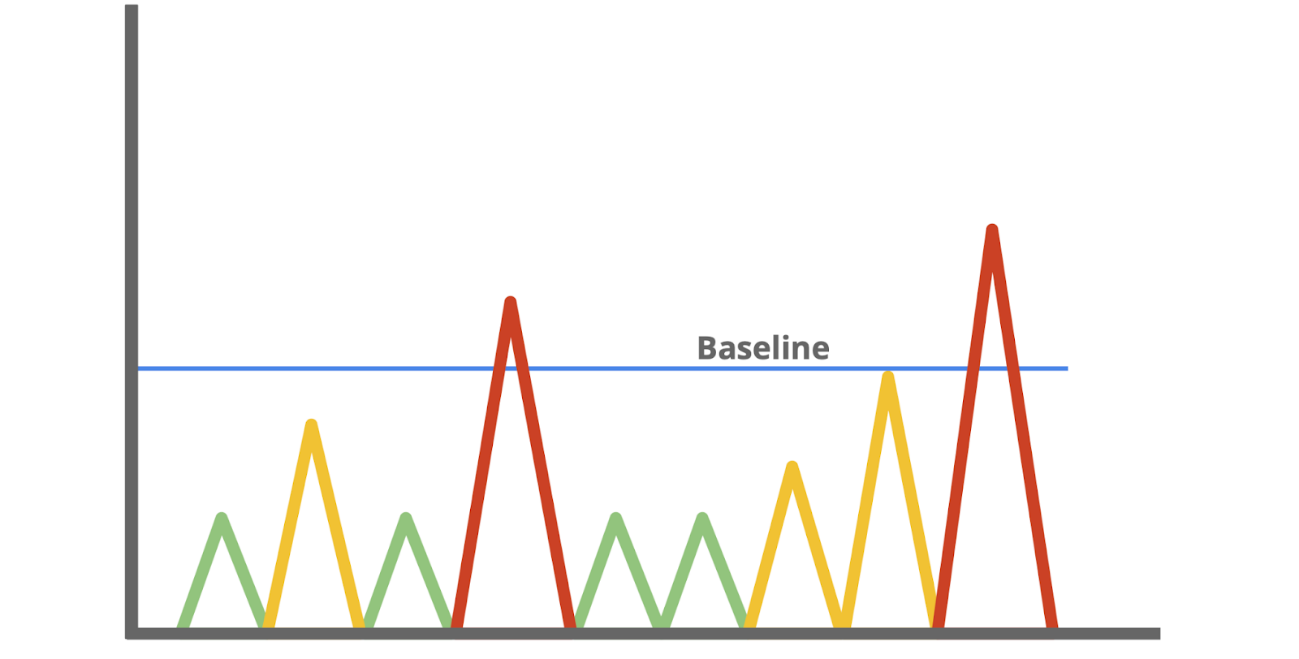
**Mantener la conciencia con el monitoreo de la red**

La comunicación en red puede ser ruidosa. Actividades como enviar un correo electrónico, reproducir un video o visitar un sitio web generan flujos de comunicación en forma de tráfico y datos en la red. Repasemos, el **tráfico de red** es la cantidad de información que se mueve a través de una red, e incluye el tipo de datos que se está transfiriendo, como por ejemplo HTTP. Por otro lado, los **datos** **de red** son la información que se intercambia entre dispositivos en una red.

El monitoreo de la red resulta fundamental para mantener una perspectiva actualizada de cualquier actividad que tenga lugar en la red. Al recopilar y analizar el tráfico de red, las organizaciones pueden identificar actividades inusuales o sospechosas. Sin embargo, antes de proceder con el monitoreo de las redes, debes saber qué aspectos se deben vigilar de manera específica. A lo largo de esta lectura, profundizarás en la importancia de la supervisión de la red, las metodologías para llevarla a cabo y las herramientas destinadas a tal fin.

**Conoce tu red**

Como ya aprendiste, las redes conectan dispositivos y luego estos se comunican e intercambian datos utilizando protocolos de red. Las comunicaciones en red ofrecen información sobre conexiones, como direcciones IP de origen y destino, cantidad de datos transferidos, la fecha y la hora, y más. Esta información puede resultar valiosa para los profesionales de la seguridad al establecer **valores de referencia** de comportamiento normal o esperado.



Los valores de referencia son un punto de partida que se utiliza para la comparación. Es probable que en algún momento hayas encontrado o utilizado valores de referencia. Por ejemplo, un monto destinado a compras de alimentos en un presupuesto personal es un ejemplo que puede usarse para identificar cualquier patrón o cambio en los hábitos de gasto. En el ámbito de la seguridad, los valores de referencia ayudan a establecer un estándar de comportamiento esperado o normal para sistemas, dispositivos y redes. En esencia, al conocer los valores de referencia del comportamiento *normal* de una red, estarás en mejor posición para identificar un comportamiento de red *anormal*.

**Monitorea tu red**

Una vez que hayas establecido los valores de referencia, podrás monitorear una red para identificar cualquier desviación. El monitoreo implica examinar los componentes de la red para detectar actividades atípicas, como transferencias de datos grandes e inusuales. Aquí te brindamos algunos ejemplos de componentes de la red que se pueden monitorear para detectar actividad maliciosa:

**Análisis de flujos**

El flujo se refiere al movimiento de las comunicaciones en la red e incluye información relacionada con paquetes, protocolos y puertos. Los paquetes pueden dirigirse a puertos que reciben y transmiten comunicaciones. Con frecuencia, los puertos están asociados con los protocolos de red. Por ejemplo, el puerto 443 es comúnmente utilizado por HTTPS, que es un protocolo que proporciona cifrado de tráfico web.

Aun así, los agentes de amenaza pueden utilizar protocolos y puertos que no están comúnmente asociados, para mantener comunicaciones entre el sistema comprometido y su propia máquina. Estas comunicaciones son lo que se conoce como **comando y control (C2)**,que son las técnicas utilizadas por agentes de amenaza para mantener las comunicaciones con sistemas comprometidos.

Por ejemplo, los agentes de amenaza pueden utilizar el protocolo HTTPS sobre el puerto 8088 en lugar de su puerto comúnmente asociado, el 443, para comunicarse con sistemas comprometidos. Las organizaciones deben saber qué puertos tienen que estar abiertos y aprobados para conexiones, y estar en alerta ante cualquier desajuste entre los puertos y sus protocolos asociados.

**Información de la carga útil del paquete**

Los paquetes de red contienen componentes relacionados con la transmisión del paquete. Esto incluye detalles como la dirección IP de origen y destino, y la información de su carga útil, que son los datos reales que se transmiten. Con frecuencia, estos datos se cifran y requieren ser descifrados para poder ser legibles. Las organizaciones pueden monitorear la información de la carga útil de los paquetes para identificar actividades inusuales, como la transmisión de datos confidenciales fuera de la red, lo que podría indicar un posible ataque de exfiltración de datos.

**Patrones temporales**

Los paquetes de red contienen información relacionada con el tiempo. Esta información es útil para comprender los patrones temporales. Por ejemplo, una empresa que opera en América del Norte experimenta flujos de tráfico masivo entre las 9 am y las 5 pm, que es el valor de referencia de la actividad normal en la red. Si de pronto se observan volúmenes grandes de tráfico fuera de los horarios normales de actividad de la red, esto se considera *fuera del valor de referencia* y debe investigarse.

A través del monitoreo de la red, las organizaciones pueden detectar rápidamente intrusiones y trabajar para prevenirlas, asegurando los componentes de la red.

**Protege tu red**

En este programa, aprendiste sobre los **centros de operaciones de seguridad** (**SOC**) y su papel en el monitoreo de sistemas contra amenazas y ataques de seguridad. Las organizaciones pueden implementar un **centro de operaciones de red** (**NOC**), que es una unidad organizativa encargada de supervisar el rendimiento de una red y responder a cualquier interrupción, como un fallo de red. Mientras que un SOC se centra en mantener la seguridad de una organización a través de la detección y la respuesta, un NOC es responsable de mantener el rendimiento, la disponibilidad y el tiempo de actividad de la red.



Los analistas de seguridad monitorean las redes para identificar cualquier signo de posibles incidentes de seguridad, conocidos como **indicadores de compromiso** (**IoC**), y protegerlas contra los ataques o amenazas. Para hacerlo, deben comprender el entorno por el que viajan las comunicaciones de red y así poder identificar las desviaciones en el tráfico de red.

**Herramientas de monitoreo de red**

El monitoreo de la red se puede automatizar o realizar de forma manual. Algunas herramientas comúnmente utilizadas pueden incluir:

* **Sistemas de detección de intrusiones** (**IDS**), que monitorean la actividad del sistema y alertan sobre posibles intrusiones. Un IDS identifica y alerta sobre las desviaciones que le hayas configurado para que detecte. Lo más habitual es que las herramientas IDS monitoreen el contenido de la carga útil del paquete para detectar los patrones asociados con amenazas como malware o intentos de phishing.
* **Analizadores de protocolo de red**, también conocidos como rastreadores de paquetes, que son herramientas diseñadas para capturar y analizar el tráfico de datos dentro de una red. Se pueden utilizar para analizar las comunicaciones de red manualmente en detalle. Los ejemplos incluyen herramientas como tcpdump y Wireshark, que pueden utilizar los profesionales de seguridad para registrar comunicaciones de red a través de capturas de paquetes. Estas se pueden investigar para identificar las actividades potencialmente maliciosas.

**Conclusiones clave**

Monitorear y proteger las redes de intrusiones y ataques son responsabilidades fundamentales de los profesionales de seguridad. No se puede proteger lo que no se conoce. Como analista de seguridad, necesitarás comprender los componentes de una red y las comunicaciones que ocurren en ella, para así poder protegerla de manera más efectiva. Los valores de referencia proporcionan una forma de comprender el tráfico de red al revelar patrones comunes que ayudan a identificar cualquier desviación de los patrones de tráfico esperados. Herramientas como los sistemas de detección de intrusiones y los analizadores de protocolos de red apoyan los esfuerzos para monitorear las actividades de la red.

**Recursos**

* Si deseas obtener más información sobre los componentes de red que las organizaciones pueden monitorear, consulta [tráfico de red: MITRE ATT&CK®](https://attack.mitre.org/datasources/DS0029/)
* Los atacantes pueden aprovechar diferentes técnicas para exfiltrar datos. Si deseas obtener más información, consulta [técnicas de exfiltración de datos: MITRE ATT&CK®](https://attack.mitre.org/tactics/TA0010/)