



CAPÍTULO 4: PROTECCIÓN DE LA ORGANIZACIÓN

ESTE CAPÍTULO ABARCA ALGUNOS DE LOS PROCESOS Y TECNOLOGÍAS UTILIZADOS POR LOS PROFESIONALES DE LA CIBERSEGURIDAD PARA PROTEGER LA RED, EQUIPOS Y LOS DATOS DE UNA ORGANIZACIÓN. PRIMERO, EXPLICA BREVEMENTE LOS TIPOS DE FIREWALLS, DISPOSITIVOS DE SEGURIDAD Y SOFTWARE QUE SE UTILIZAN ACTUALMENTE, INCLUIDAS LAS MEJORES PRÁCTICAS

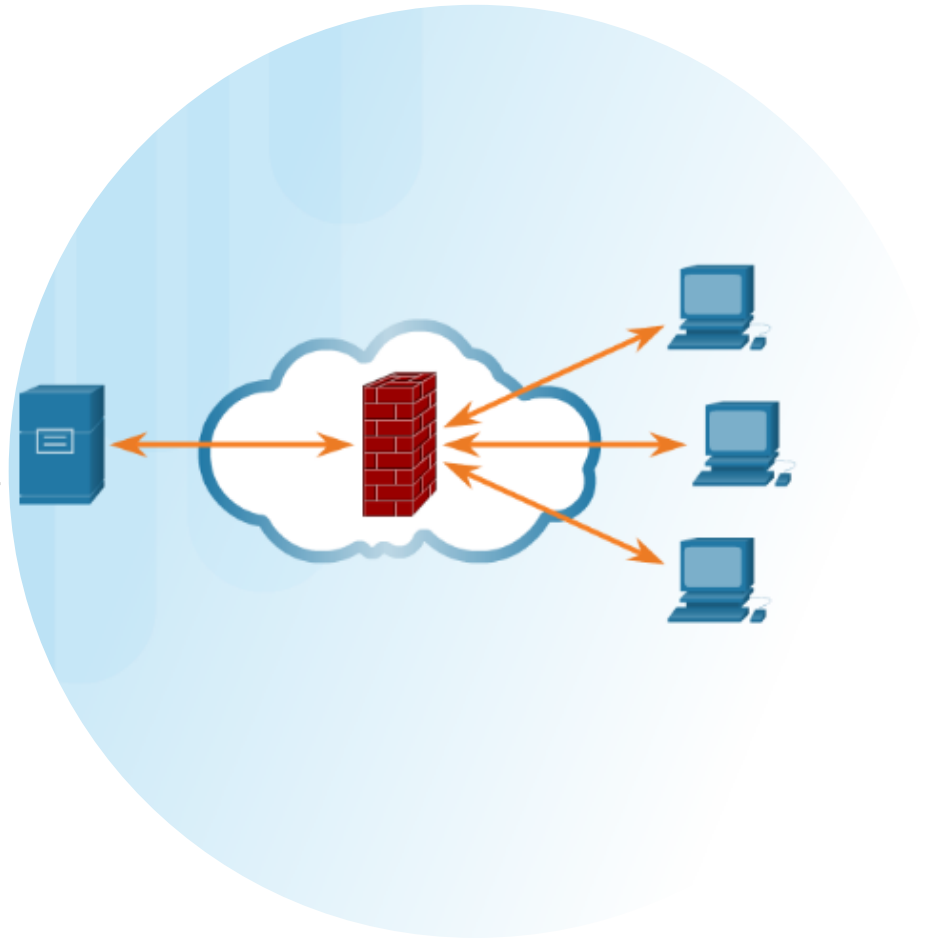
PROTECCIÓN DE LA ORGANIZACIÓN

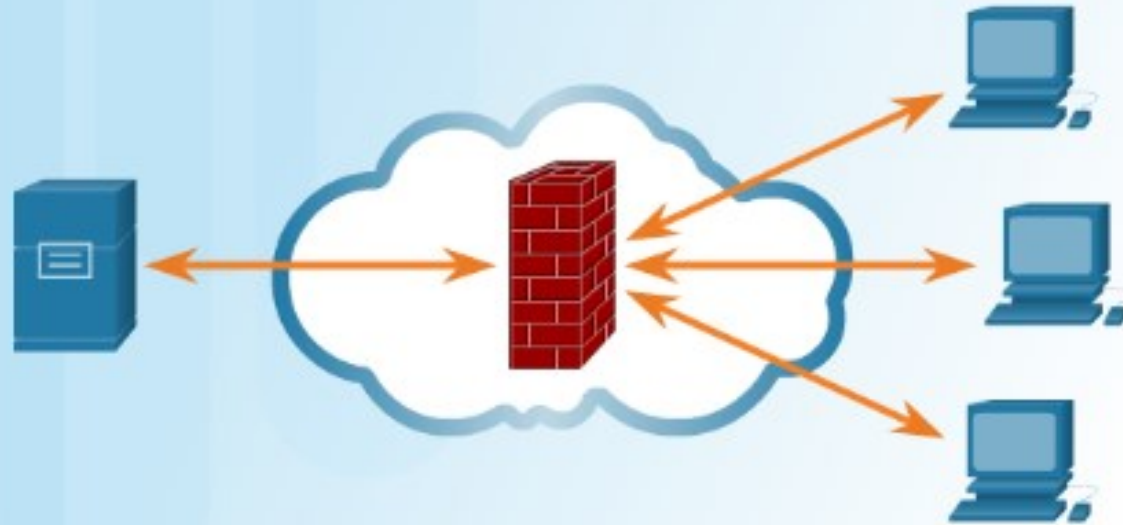
- Luego, este capítulo explica los botnets, the kill chain, la seguridad basada en comportamientos y el uso de NetFlow para monitorear una red.
- Abarca brevemente las herramientas que los profesionales de la ciberseguridad utilizan para detectar y prevenir los ataques a la red.
- Abarca brevemente las herramientas que los profesionales de la ciberseguridad utilizan para detectar y prevenir los ataques a red.



TIPOS DE FIREWALL

- Un firewall (cortafuegos) es un muro o partición diseñada para evitar que el fuego se propague de una parte a otra de un edificio.
- En las redes de computadoras, un firewall está diseñado para controlar o filtrar la entrada o salida de comunicaciones de un dispositivo o una red, como se muestra en la figura.
- Un firewall puede instalarse en una única computadora con el propósito de proteger dicha computadora (firewall ejecutado en un host) o puede ser un dispositivo de red independiente que protege toda una red de computadoras y todos los dispositivos host en dicha red (firewall basado en la red).

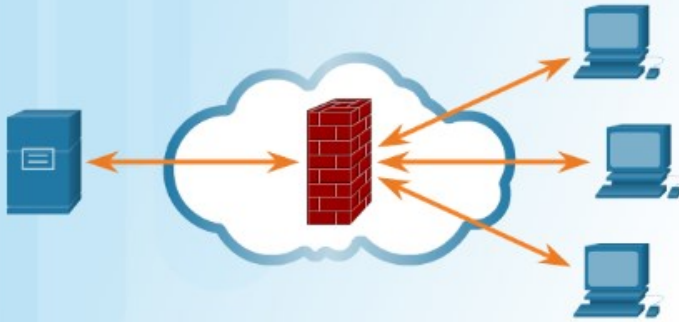




TIPOS DE FIREWALL

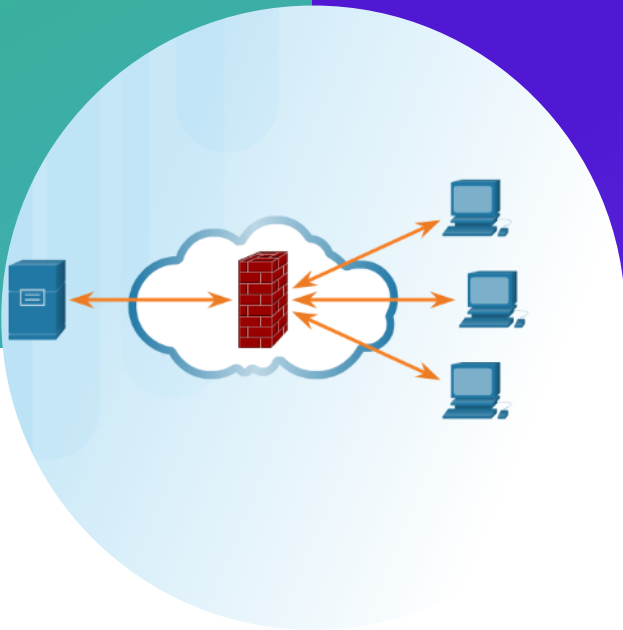
- Durante años, dado que los ataques a la computadora y la red se han vuelto más sofisticados, se han desarrollado nuevos tipos de firewalls que atienden diferentes fines en la protección de la red.

TIPOS DE FIREWALL



- **Servidor proxy:** filtrado de solicitudes de contenido web, como URL, dominio, medios, etcétera.
- **Servidor de proxy inverso:** ubicados frente a los servidores web, los servidores de proxy inversos protegen, ocultan, descargan y distribuyen el acceso a los servidores web.
- **Firewall de traducción de direcciones de red (NAT):** ocultan o enmascaran las direcciones privadas de los hosts de red.
- **Firewall basado en host:** filtrado de puertos y llamadas de servicio del sistema en el sistema operativo de una computadora.
- **Firewall de capa de red:** filtrado basado en las direcciones IP de origen y destino.
- **Firewall de capa de transporte:** filtrado basado en puertos de origen y datos de destino y filtrado basado en los estados de conexión.
- **Firewall de capa de aplicación:** filtrado basado en la aplicación, el programa o el servicio.
- **Firewall de aplicación consciente del contexto:** filtrado basada en el usuario, el dispositivo, la función, el tipo de aplicación y el perfil de amenazas.

TIPOS DE FIREWALL

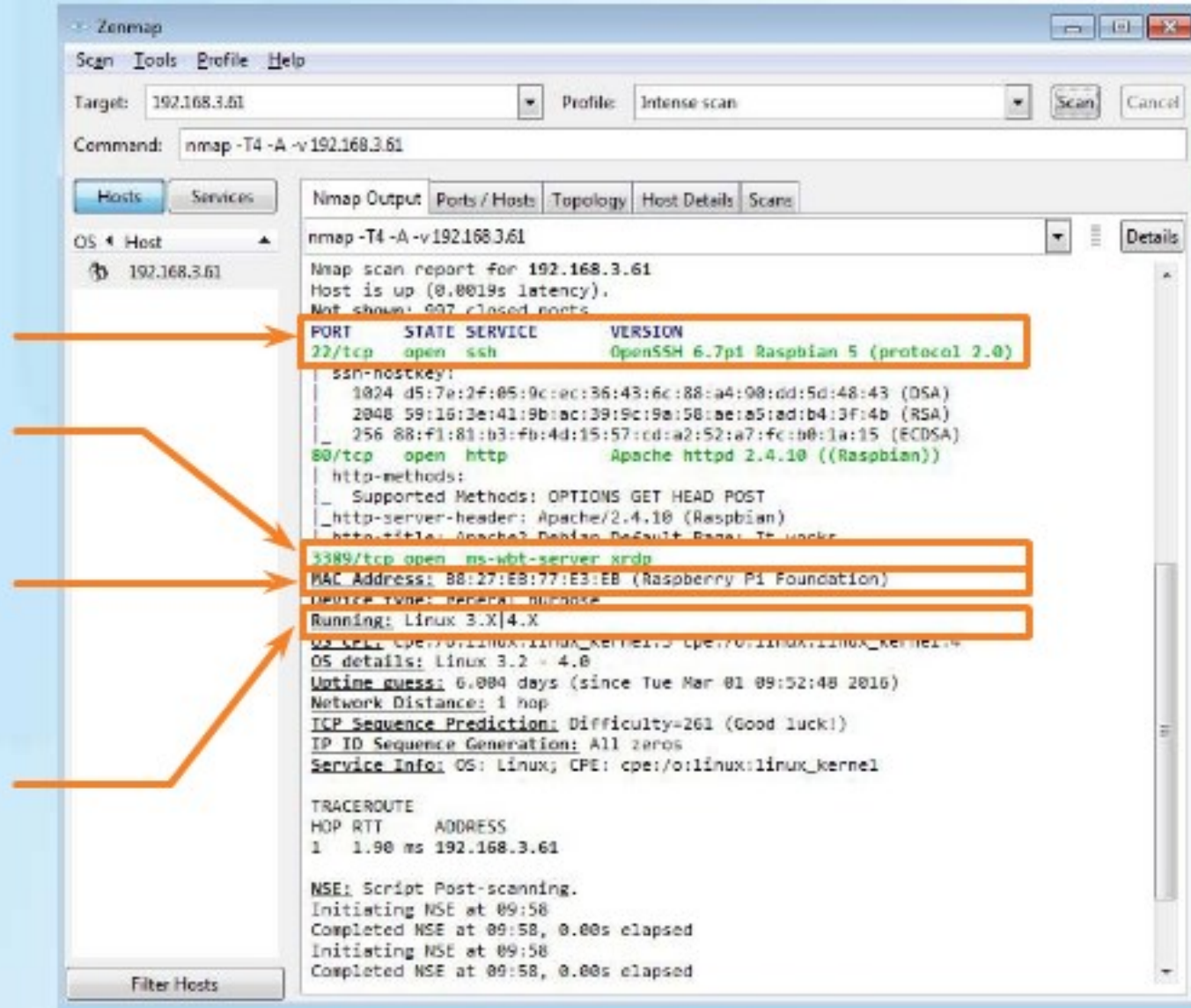


Tipo de firewall	
Descripción	
	Ocultar o enmascarar las direcciones privadas de los hosts de la red.
	Filtrado de las solicitudes de contenido web.
	Filtrado de puertos y llamadas de servicio al sistema en un sistema operativo.
	Filtrado basado en el usuario, el dispositivo, la función y el perfil de la aplicación.
	Filtrado basado en los puertos de datos de origen y destino, y estados de conexión.
	Se coloca por encima de los servidores web para proteger, ocultar, y controlar el acceso a los servidores web.
	Filtrado basado en el programa o el servicio.
	Filtrado basado en las direcciones IP de origen y destino.

ESCA NEO DE PUERTOS

- El escaneo de puertos es un proceso de comprobación de una computadora, un servidor u otro host de red para conocer los puertos abiertos.
 - En redes, a cada aplicación que se ejecuta en un dispositivo se le asigna un identificador llamado número de puerto.
 - Este número de puerto se utiliza en ambos extremos de la transmisión para asegurar que los datos estén llegando a la aplicación correcta.
 - El escaneo de puertos se puede utilizar con fines maliciosos como una herramienta de reconocimiento, para identificar el sistema operativo y los servicios que se ejecutan en una computadora o un host, o se puede utilizar inofensivamente por parte de un administrador de red para verificar las políticas de seguridad en la red.
- Con el propósito de evaluar el firewall de la red de computadoras y la seguridad de los puertos, puede utilizar una herramienta de escaneo de puertos, como Nmap, para encontrar todos los puertos abiertos en su red. El escaneo de puertos se puede considerar como precursor para un ataque a la red y, por lo tanto, no debe realizarse en servidores públicos en Internet o en la red de una empresa sin permiso.

ESCANEOD E PUERTOS



- Con el propósito de evaluar el firewall de la red de computadoras y la seguridad de los puertos, puede utilizar una herramienta de escaneo de puertos, como Nmap, para encontrar todos los puertos abiertos en su red. El escaneo de puertos se puede considerar como precursor para un ataque a la red y, por lo tanto, no debe realizarse en servidores públicos en Internet o en la red de una empresa sin permiso.



ESCANEOD E PUERTOS

- Para ejecutar el escaneo de puertos Nmap de una computadora en la red doméstica local, descargue y ejecute un programa como Zenmap, proporcione la dirección IP de destino de la computadora que desea analizar, elija un perfil de escaneo predeterminado y presione Escanear.
- El escaneo de Nmap reportará cualquier servicio que se esté ejecutando (como servicios web, servicios de correo, etc.) y los números de puerto. El escaneo de puertos generalmente provoca alguna de estas tres respuestas:
- **Abierto o aceptado:** el host respondió e indicó que hay un servicio activo en el puerto.
- **Cerrado, denegado o no escucha:** el host respondió e indicó que se denegarán las conexiones en el puerto.
- **Filtrado, caído o bloqueado:** no hubo respuesta del host.

ESCA NEO DE PUERTOS

- Para ejecutar escaneo del puerto desde fuera de la red, deberá iniciar el escaneo desde fuera de la red.
 - Esto implicará la ejecución de un escaneo de puertos de Nmap con la dirección IP pública del firewall o router.
 - Para obtener su dirección IP pública, utilice un motor de búsqueda, como Google, con la consulta “cuál es mi dirección IP”.
 - El motor de búsqueda le devolverá su dirección IP pública.

Starting Nmap 7.40 (<https://nmap.org>) at 2021-11-11

20:28 UTC

Nmap scan report for scanme.nmap.org (45.33.32.156)

Host is up (0.070s latency).

PORT	STATE	SERVICE
21/tcp	closed	ftp
22/tcp	open	ssh
23/tcp	closed	telnet
80/tcp	open	http
110/tcp	closed	pop3
143/tcp	closed	imap
443/tcp	closed	https
3389/tcp	closed	ms-wbt-server

Nmap done: 1 IP address (1 host up) scanned in 0.38

ESCANEOD E PUERTOS

- Para ejecutar un escaneo de los seis puertos más comunes de un router o firewall doméstico, vaya al escáner de puertos en línea de Nmap en <https://hackertarget.com/nmap-online-port-scanner/> e ingrese la dirección IP pública de [Go ahead and ScanMe! \(nmap.org\)](https://nmap.org) en el cuadro del formulario: *dirección IP para escanear...* y presione *Escaneo rápido de Nmap*.
 - Si la respuesta es *Abierta* para cualquiera de los puertos: 21, 22, 25, 80, 443 o 3389, lo más probable es que esté habilitado el reenvío de puertos en el router o firewall y que ejecute servidores en su red privada, como se muestra en la figura.

ACTIVIDAD

Actividad: Identificar la respuesta de un escaneo de puertos

Elija la respuesta correcta:	▼	Descartada
Un host respondió indicando que un servicio está siendo utilizado en un puerto		
Un host respondió indicando negando la conexión al puerto		
El host no respondió		
Elija la respuesta correcta:	▼	Cerrado
Elija la respuesta correcta:	▼	Ablerta
Elija la respuesta correcta:	▼	Filtrado
Elija la respuesta correcta:	▼	Denegado
Elija la respuesta correcta:	▼	Aceptado

DISPOSITIVOS DE SEGURIDAD

- Hoy no existe un dispositivo de seguridad o una tecnología que resuelva todas las necesidades de seguridad de la red por sí solo.
 - Debido a que hay una variedad de dispositivos de seguridad y herramientas que deben implementarse, es importante que trabajen en conjunto.
 - Los dispositivos de seguridad son más efectivos cuando forman parte de un sistema.
- Los dispositivos de seguridad pueden ser dispositivos independientes, como un router o firewall, una tarjeta que puede instalarse en un dispositivo de red o un módulo con su propio procesador y memoria en caché.
 - Los dispositivos de seguridad también pueden ser herramientas de software que se ejecutan en un dispositivo de red.

DISPOSITIVOS DE SEGURIDAD



Routers: los routers de servicios integrados (ISR) Cisco, como se muestra en la Figura 1, tienen muchas capacidades similares a las de un firewall además de las funciones de ruteo, entre ellas, el filtrado de tráfico, la capacidad de ejecutar un sistema de prevención de intrusiones (IPS), el cifrado y las capacidades de VPN para las conexiones de cifrado seguro.



Firewalls: los firewalls de nueva generación de Cisco tienen todas las capacidades de un router ISR además de análisis y administración de redes avanzadas. El dispositivo de seguridad adaptable (ASA, por sus siglas en inglés) de Cisco con funcionalidades de firewall se muestra en la Figura 2.



IPS: los dispositivos IPS de nueva generación, que se muestran en la Figura 3, están dedicados a la prevención de intrusiones.

DISPOSITIVOS DE SEGURIDAD



VPN: los dispositivos de seguridad de Cisco cuentan con tecnologías de redes virtuales privadas (VPN) tanto de cliente como servidor. Están diseñados para conexiones de cifrado seguro.



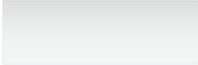

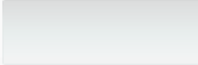
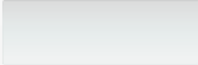

Malware/antivirus: Cisco Advanced Malware Protection (AMP) viene en los routers de nueva generación de Cisco, como también en los firewalls, los dispositivos IPS y los dispositivos de seguridad web y de correo electrónico y además puede instalarse como software en los equipos host.



Otros dispositivos de seguridad: esta categoría incluye dispositivos de seguridad web y de correo electrónico, dispositivos de descifrado, servidores de control de acceso del cliente y sistemas de administración de seguridad.

ACTIVIDAD: IDENTIFICAR DISPOSITIVOS DE SEGURIDAD

Actividad: identificar los dispositivos de seguridad

Dispositivo de seguridad	Descripción
	Dedicado a la prevención de intrusiones.
	Se ofrece en los dispositivos de nueva generación y también puede instalarse como software en los equipos host.
	Están diseñados para túneles de cifrado seguro.
	Tiene muchas capacidades además de las funciones de routing, entre ellas, filtrado de tráfico, cifrado y capacidades para túneles de cifrado seguro.
	Cuenta con todas las capacidades de un ISR, además de administración y análisis avanzados de red.

Dispositivos de seguridad

VPN

Firewall

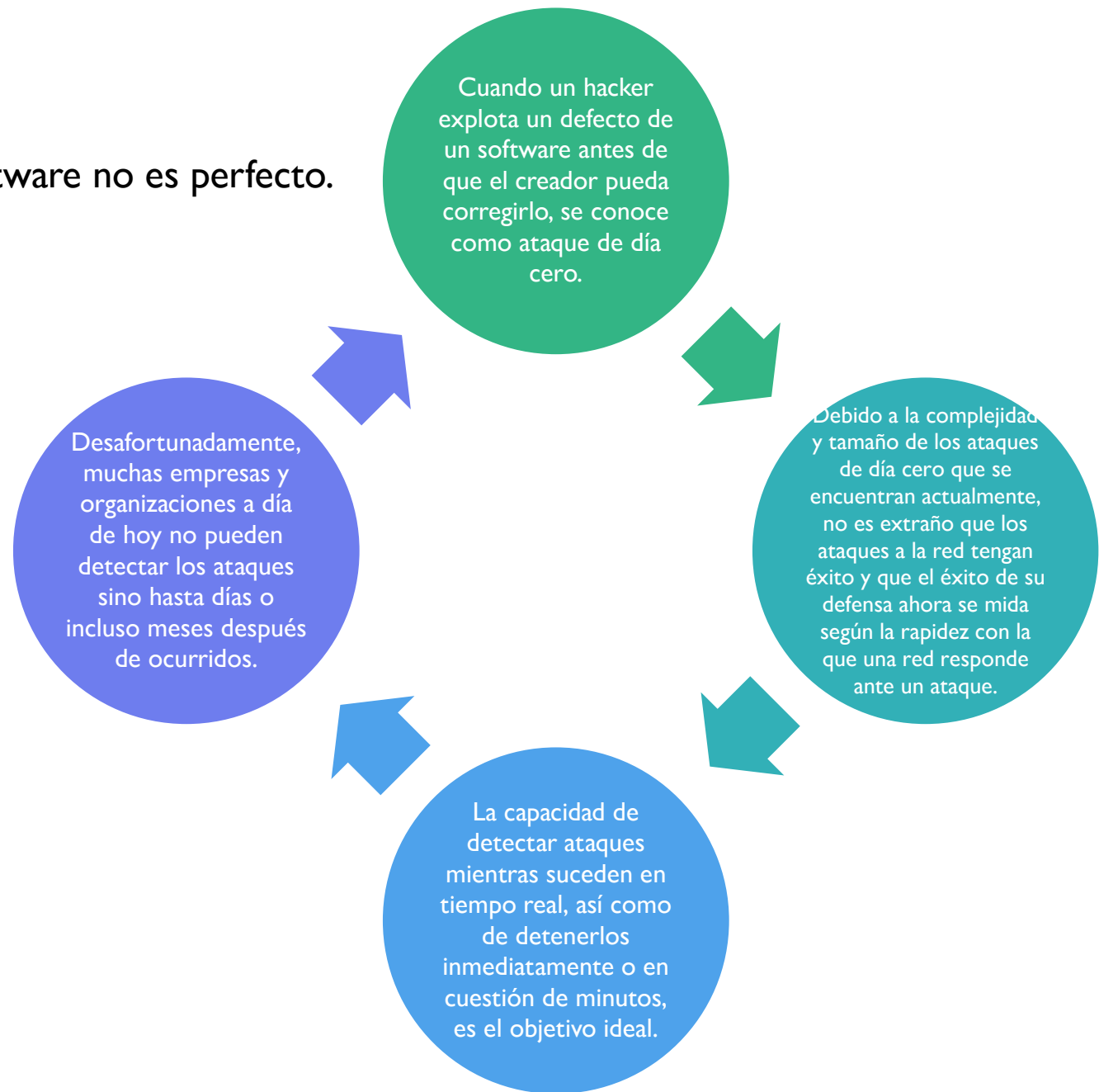
IPS

AMP

Router

DETECCIÓN DE ATAQUES EN TIEMPO REAL

- El software no es perfecto.



DETECCIÓN DE ATAQUES EN TIEMPO REAL

- **Análisis en tiempo real de principio a fin:**

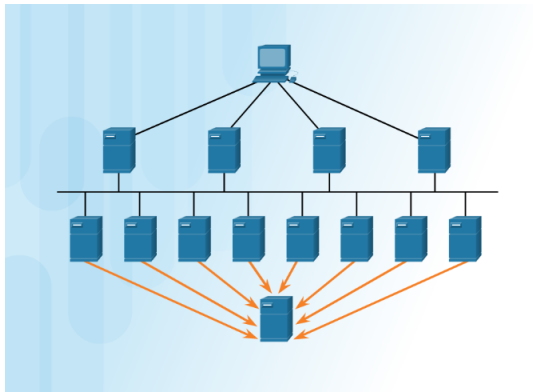
Detectar ataques en tiempo real requiere el análisis activo mediante el firewall y los dispositivos de red IDS/IPS.

También debe usarse la detección de malware de cliente/servidor de nueva generación con conexiones a los centros de amenazas globales en línea.

En la actualidad, el software y los dispositivos de análisis activos deben detectar anomalías de red mediante la detección de comportamientos y el análisis basado en el comportamiento.

DETECCIÓN DE ATAQUES EN TIEMPO REAL

- Ataques DDoS y respuesta en tiempo real:



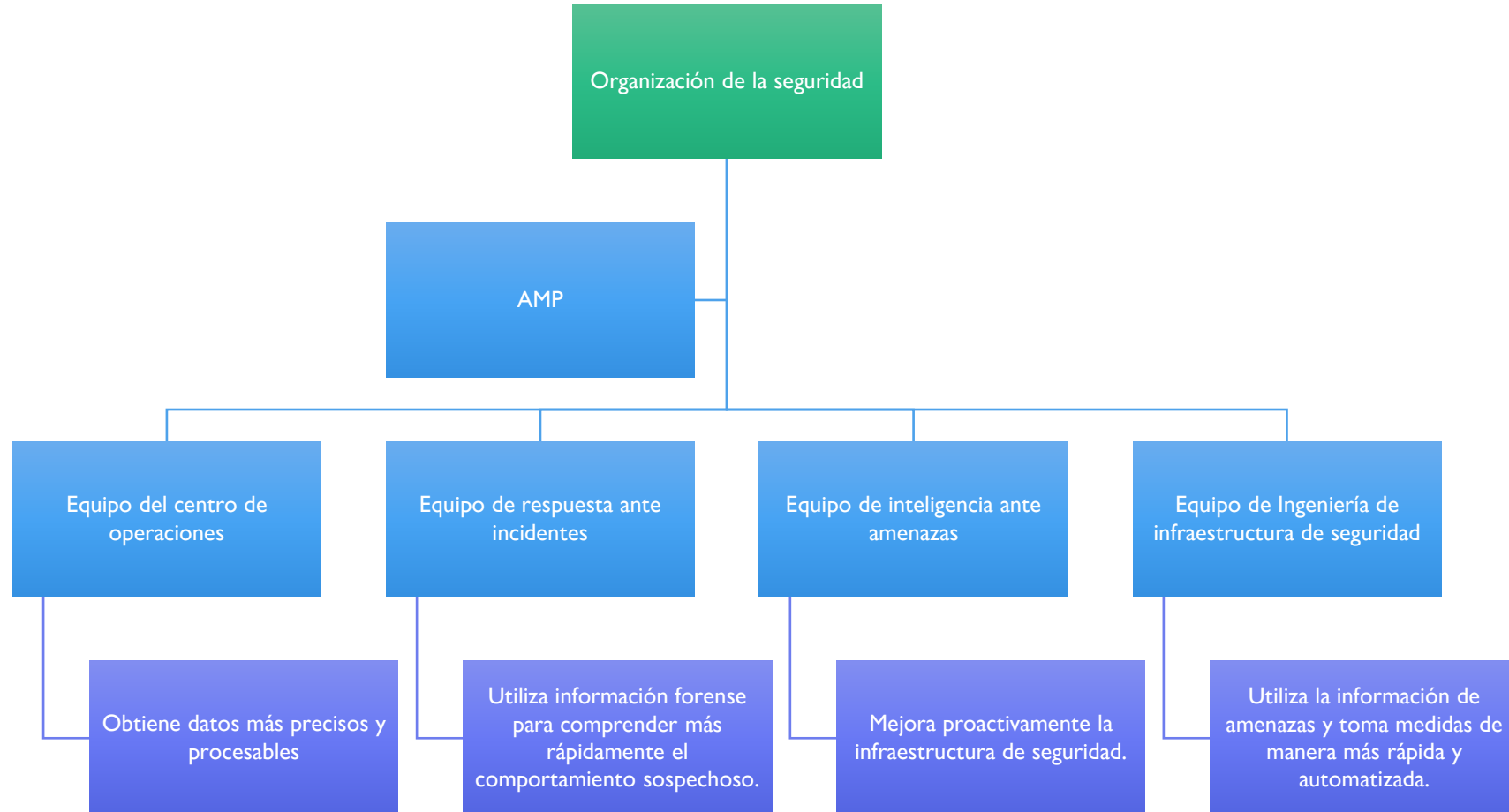
El ataque DDoS es una de las mayores amenazas que requiere la detección y respuesta en tiempo real.

La capacidad para detectar y responder a los ataques DDoS en tiempo real es crucial.

Para muchas empresas y organizaciones, los ataques DDoS ocurren de forma regular y paralizan los servidores de Internet y la disponibilidad de la red.

Es extremadamente difícil defenderse contra los ataques de DDoS porque los ataques se originan en cientos o miles de hosts zombis y aparecen como tráfico legítimo, como se muestra en la figura.

ADVANCED MALWARE PROTECTION (AMP) THREAT GRID BENEFICIA LAS FUNCIONES DE SEGURIDAD DE TODA LA ORGANIZACIÓN



PROTECCIÓN CONTRA EL MALWARE

¿Cómo proporciona la defensa contra la presencia constante de ataques de día cero y las amenazas persistentes avanzadas (APT, por sus siglas en inglés) que roban datos durante largos períodos de tiempo?

- Una solución es utilizar una aplicación de detección de malware avanzada de nivel empresarial que ofrezca detección de malware en tiempo real.

Los administradores de red deben monitorear constantemente la red para detectar signos de malware o comportamientos que revelan la presencia de una APT.

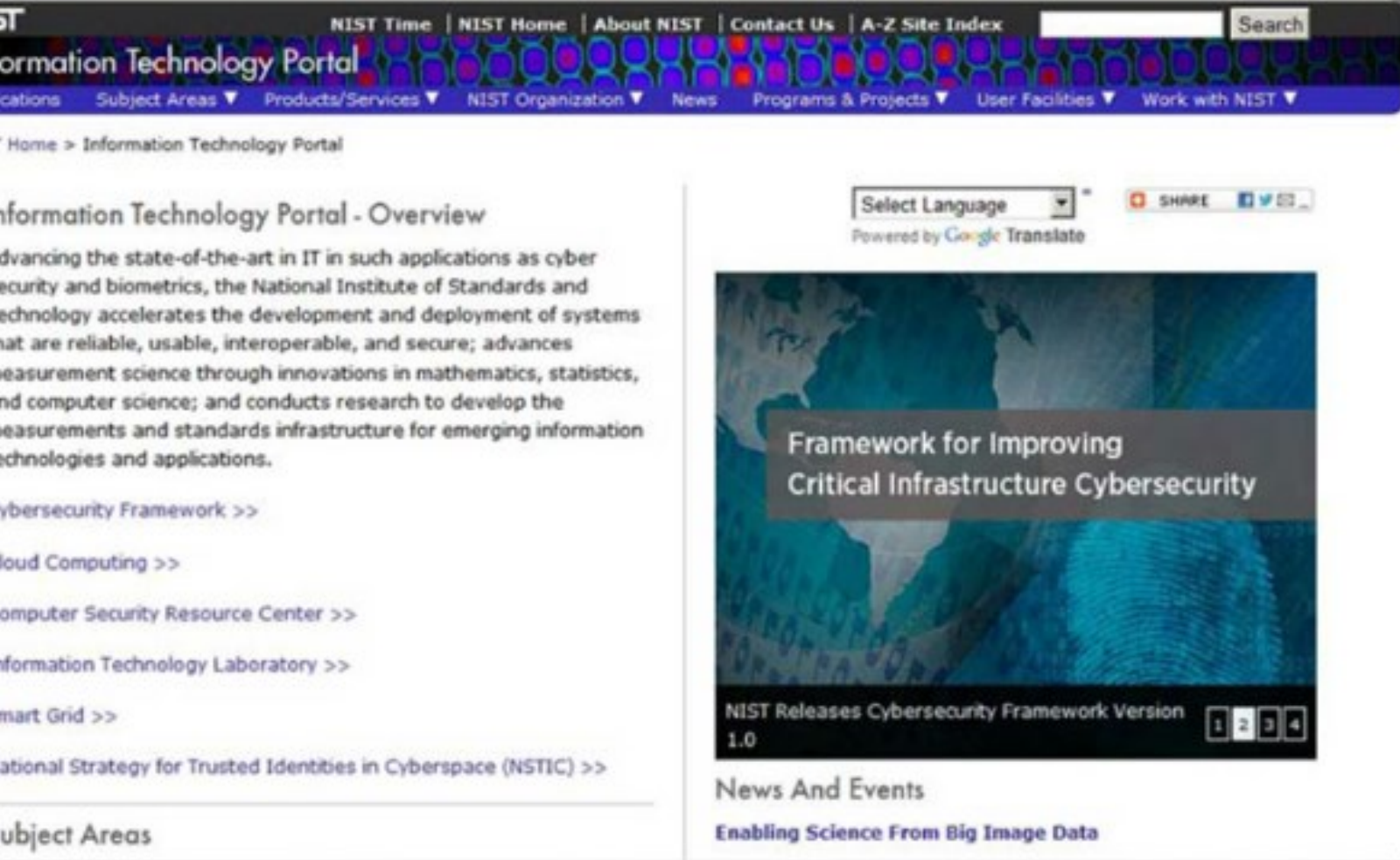
- Cisco cuenta con Advanced Malware Protection (AMP) Threat Grid, que analiza millones de archivos y los correlaciona con cientos de millones de otros objetos de malware analizados.
- Esto brinda a los clientes una vista global de las campañas, la distribución y los ataques de malware.
- AMP es un software de Cliente/Servidor implementado en terminales de host, como servidor independiente, o en otros dispositivos de seguridad de la red. La figura muestra los beneficios de AMP Threat Grid.

BUENAS PRÁCTICAS DE SEGURIDAD

- Muchas organizaciones nacionales y profesionales han publicado listas de buenas prácticas de seguridad. La siguiente es una lista de algunas de las buenas prácticas de seguridad:
- **Realizar una evaluación de riesgos:** conocer el valor de lo que protege ayuda a justificar los gastos de seguridad.
- **Crear una política de seguridad:** cree una política que delimite claramente las reglas de la empresa, las tareas y las expectativas.
- **Medidas de seguridad física:** restringen el acceso a los centros de datos, a las ubicaciones de servidores y a los extintores.
- **Medidas de seguridad de recursos humanos:** los empleados deben ser correctamente investigados con comprobaciones de antecedentes.
- **Efectuar y probar las copias de respaldo:** realice copias de respaldo periódicas y pruebe los datos recuperados de las copias de respaldo.
- **Mantener parches y actualizaciones de seguridad:** actualice periódicamente los servidores, computadoras, los programas y sistemas operativos de los dispositivos de red.
- **Implementar controles de acceso:** configure los roles de usuario y los niveles de privilegio, así como una autenticación de usuario sólida.

BUENAS PRÁCTICAS DE SEGURIDAD

- **Revisar periódicamente la respuesta ante incidentes:** utilice un equipo de respuesta ante incidentes y pruebe los escenarios de respuesta ante emergencias.
- **Implementar una herramienta de administración, análisis y supervisión de red:** seleccione una solución de monitoreo de seguridad que se integre con otras tecnologías.
- **Implementar dispositivos de seguridad de la red:** utilice routers de nueva generación, firewalls y otros dispositivos de seguridad.
- **Implementar una solución de seguridad integral para terminales:** utilice software antivirus y antimalware de nivel empresarial.
- **Informar a los usuarios:** educar a los usuarios y a los empleados sobre los procedimientos seguros.
- **Cifrar los datos:** cifrar todos los datos confidenciales de la empresa, incluido el correo electrónico.



BUENAS PRÁCTICAS DE SEGURIDAD

- Algunas de las pautas más útiles se encuentran en los depósitos organizacionales, como el Centro de Recursos de Seguridad Informática del Instituto Nacional de Normas y Tecnología (NIST, por sus siglas en inglés), según se muestra en la figura.

BUENAS PRÁCTICAS DE SEGURIDAD

About SANS Institute

Launched in 1989 as a cooperative for information security thought leadership, it is SANS' ongoing mission to empower cyber security professionals with the practical skills and knowledge they need to make our world a safer place.

We fuel this effort with high quality training, certifications, scholarship academies, degree programs, cyber ranges, and resources to meet the needs of every cyber professional. Our research, and the top minds in cybersecurity collectively ensure that individuals and organizations have the actionable education and support they need.

- Una de las organizaciones más conocidas y respetadas para la capacitación en ciberseguridad es el SANS Institute.
 - Haga clic [aquí](#) para obtener más información sobre SANS y los tipos de capacitación y certificaciones que ofrece.

Botnet Traffic Filter de ASA



BOTNET

- Un botnet es un grupo de bots conectados a través de Internet con la capacidad de ser controlados por un individuo o grupo malicioso.
 - Una computadora bot se infecta generalmente por visitar un sitio web, abrir un elemento adjunto de correo electrónico o abrir un archivo de medios infectado.
- Un botnet puede tener decenas de miles o incluso cientos de miles de bots.
 - Estos bots se pueden activar para distribuir malware, lanzar ataques DDoS, distribuir correo electrónico no deseado o ejecutar ataques de contraseña por fuerza bruta.
 - Los botnets por lo general se controlan a través de un servidor de comando y control.
- Los delincuentes cibernéticos alquilan a menudo los botnets, por un monto, a otros proveedores para fines infames.
- La figura muestra cómo un filtro de tráfico de botnet se utiliza para informar a la comunidad de seguridad mundial las ubicaciones de los botnets.



BOTNET

- Paso 1
 - Los clientes infectados intentan comunicarse con un host de comando y control dentro de internet.
- Paso 2
 - Cisco SIO actualiza la lista de Botnet Filter de Cisco ASA; el destino es un sitio de ataque conocido..
- Paso 3
 - Se emiten alertas a los equipos de seguridad con fines de prevención, mitigación y corrección.

CADENA DE ELIMINACIÓN O PROCESO DE ATAQUE (KILL CHAIN) EN LA CIBERDEFENSA

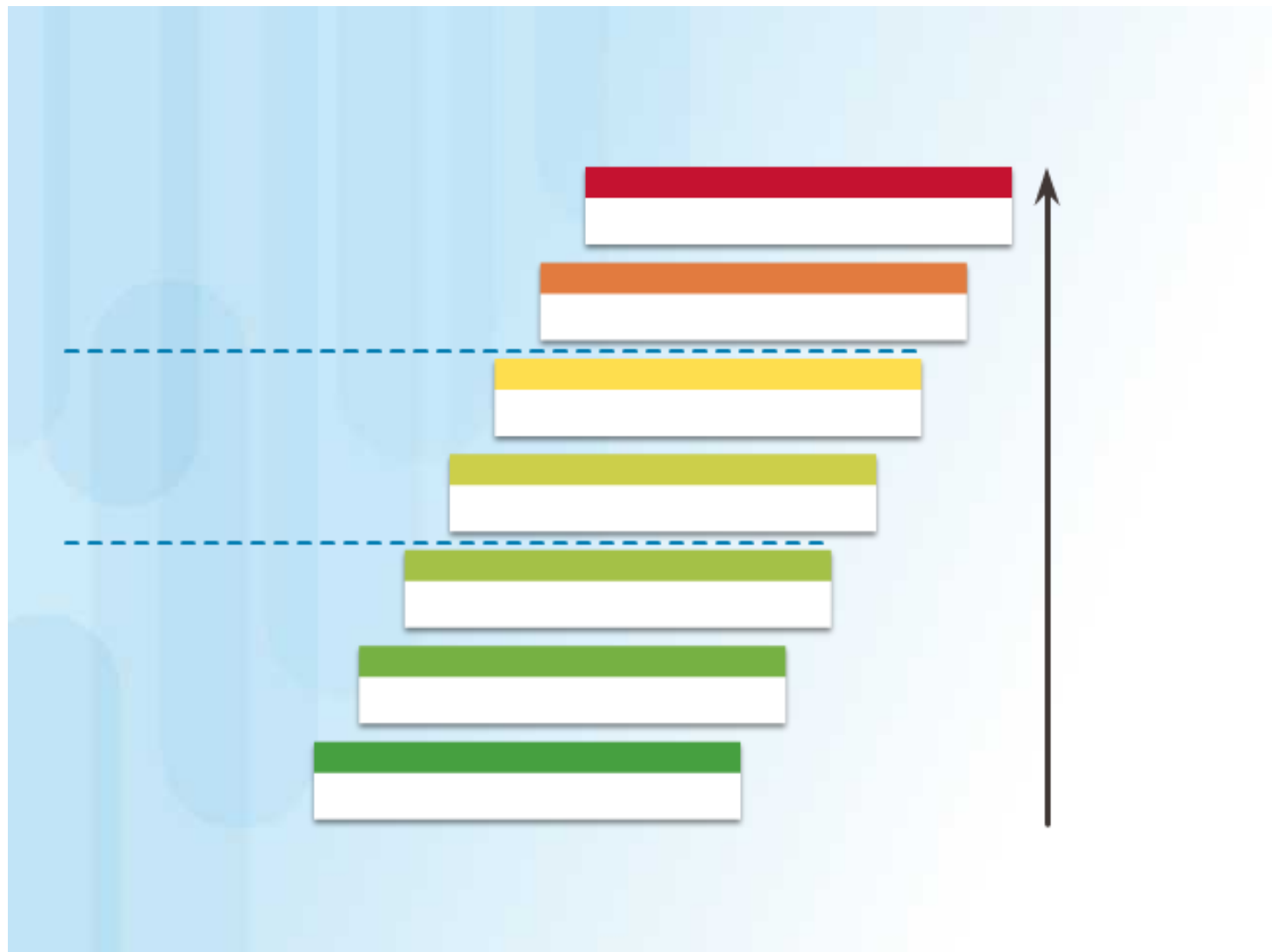
- En la ciberseguridad, la cadena de eliminación o proceso de ataque (Kill Chain) representa las etapas de un ataque a los sistemas de información. Desarrollada por Lockheed Martin como marco de seguridad para la respuesta y la detección de incidentes, la cadena de eliminación consta de los siguientes pasos:
- **Etapas 1. Reconocimiento:** el atacante recopila información sobre el objetivo.
- **Etapas 2. Armamentización:** el atacante crea un ataque y contenido malicioso para enviar al objetivo.
- **Etapas 3. Entrega:** el atacante envía el ataque y la carga maliciosa al objetivo por correo electrónico u otros métodos.
- **Etapas 4. Explotación:** se ejecuta el ataque.
- **Etapas 5. Instalación:** el malware y las puertas traseras se instalan en el objetivo.
- **Etapas 6. Mando y control:** se obtiene el control remoto del objetivo mediante un servidor o canal de comando y control.
- **Etapas 7. Acción:** el atacante realiza acciones maliciosas, como el robo de información, o ejecuta ataques adicionales en otros dispositivos desde dentro de la red a través de las etapas de la cadena de eliminación nuevamente.

CADENA DE ELIMINACIÓN O PROCESO DE ATAQUE (KILL CHAIN) EN LA CIBERDEFENSA

- Para defendernos de la cadena de eliminación, existen acciones de seguridad diseñadas en torno a las etapas de la cadena de eliminación.
 - Estas son algunas preguntas sobre las defensas de seguridad de una empresa en función de la cadena de eliminación:
 - ¿Cuáles son los indicadores de ataque en cada etapa de la cadena de eliminación?
 - ¿Qué herramientas de seguridad son necesarias para detectar los indicadores de ataque en cada una de las etapas?
 - ¿Hay brechas en la capacidad de la empresa para detectar un ataque?

Según Lockheed Martin, comprender las etapas de la cadena de eliminación permite poner obstáculos defensivos, demorar el ataque y, finalmente, evitar la pérdida de datos.

LA FIGURA
MUESTRA CÓMO
CADA ETAPA DE
LA CADENA DE
ELIMINACIÓN
EQUIVALE A UN
AUMENTO EN LA
CANTIDAD DE
ESFUERZO Y
COSTOS PARA
IMPEDIR Y
CORREGIR
ATAQUES.



Actividad: Ordenar las etapas de la cadena de destrucción

Instrucciones

Una cada número de la etapa con el nombre de la etapa correcto.

Etapa 5

Etapa 3

Etapa 2

Etapa 1

Etapa 6

Etapa 7

Etapa 4

Término

Descripción

Entrega

Acción

Comando y control

Reconocimiento

Instalación

Ataque

Armamentización



SEGURIDAD BASADA EN EL COMPORTAMIENTO

La seguridad basada en el comportamiento es una forma de detección de amenazas que no depende de las firmas malintencionadas conocidas, pero que utiliza el contexto informativo para detectar anomalías en la red.

La detección basada en el comportamiento implica la captura y el análisis del flujo de comunicación entre un usuario de la red local y un destino local o remoto.

- Estas comunicaciones, cuando se detectan y analizan, revelan el contexto y los patrones de comportamiento que se pueden usar para detectar anomalías.

La detección basada en el comportamiento puede detectar la presencia de un ataque mediante un cambio en el comportamiento normal.

SEGURIDAD BASADA EN EL COMPORTAMIENTO

- **Honeypot:**
- Una honeypot es una herramienta de detección basada en el comportamiento que primero atrae al atacante apelando al patrón previsto de comportamiento malicioso del atacante;
 - una vez dentro de la honeypot, el administrador de la red puede capturar, registrar y analizar el comportamiento del atacante.
 - Esto permite que un administrador gane más conocimiento y construya una mejor defensa.

- **Arquitectura de Cyber Threat Defense Solution de Cisco:**
- Esta es una arquitectura de seguridad que utiliza la detección basada en el comportamiento e indicadores para proporcionar mayor visibilidad, contexto y control.
 - El objetivo es definir quién, qué, dónde, cuándo y cómo se produce un ataque.
 - Esta arquitectura de seguridad utiliza muchas tecnologías de seguridad para lograr este objetivo.

**SEGURIDAD
BASADA EN EL
COMPORTAMIENTO**

La evolución de las amenazas cibernéticas

Virus (*década de 1990*)
Defensa: antivirus, firewalls

ILOVEYOU
Melissa
Anna Kournikova

Gusanos (*década del 2000*)
Defensa: detección y prevención de intrusiones

Nimda
SQL Slammer
Conficker

Botnets (*fines de 2000 al presente*)
Defensa: reputación, DLP, firewalls con reconocimiento de aplicaciones

Tedroo
Rustock
Conficker

Ataques dirigidos (APT) (*actualmente*)
Estrategia: visibilidad y contexto

Aurora
Shady Rat
Duqu

SEGURIDAD BASADA EN EL COMPORTAMIENTO

NETFLOW



- La tecnología NetFlow se usa para recopilar información sobre los datos que atraviesan la red.
 - La información de NetFlow se puede comparar con una factura telefónica por el tráfico de la red.
 - Muestra quién y qué dispositivos están en la red también como y cuando los usuarios y dispositivos tuvieron acceso a la red.
 - NetFlow es un componente importante del análisis y la detección basados en el comportamiento.
 - Los switches, routers y firewalls equipados con NetFlow pueden comunicar información sobre los datos que ingresan, egresan y viajan por la red.
 - La información se envía a los recopiladores de NetFlow que recopilan, almacenan y analiza los registros de NetFlow.
- NetFlow puede recopilar información sobre el uso a través de muchas características diferentes de cómo se transportan los datos por la red, como se muestra en la figura.
 - Mediante la recopilación de la información sobre los flujos de datos de la red, NetFlow puede establecer comportamientos de línea base en más de 90 atributos diferentes.

NETFLOW

Creación de un flujo de NetFlow



Cree un flujo basado en los atributos del paquete.

CSIRT

- Muchas organizaciones grandes tienen un Equipo de respuesta a incidentes de seguridad informática (CSIRT, por sus siglas en inglés) para recibir, revisar y responder a informes de incidentes de seguridad informática, como se muestra en la Figura 1. La función principal del CSIRT es ayudar a proteger la empresa, el sistema y la preservación de datos realizando investigaciones integrales de los incidentes de seguridad informática. Para evitar incidentes de seguridad, el CSIRT de Cisco proporciona una evaluación de amenazas proactiva, planificación de la mitigación, análisis de tendencias de incidentes y revisión de la arquitectura de seguridad, como se muestra en la Figura 2.
- El CSIRT de Cisco colabora con el Foro de respuesta ante los incidentes y los equipos de seguridad (FIRST), el Intercambio de información de seguridad nacional (NSIE), el Intercambio de información de seguridad de defensa (DSIE) y el Centro de Investigación y Análisis de operaciones DNS (DNS-OARC).
- Hay organizaciones de CSIRT nacionales y públicas, como la División CERT del Instituto de Ingeniería de Software de la Universidad Carnegie Mellon, que están dispuestos a ayudar a las organizaciones, y a los CSIRT nacionales, a desarrollar, utilizar y mejorar sus capacidades de administración de incidentes.



CSIRT

- Muchas organizaciones grandes tienen un Equipo de respuesta a incidentes de seguridad informática (CSIRT, por sus siglas en inglés) para recibir, revisar y responder a informes de incidentes de seguridad informática, como se muestra en la Figura 1.
- La función principal del CSIRT es ayudar a proteger la empresa, el sistema y la preservación de datos realizando investigaciones integrales de los incidentes de seguridad informática.

CSIRT

- Para evitar incidentes de seguridad, el CSIRT de Cisco proporciona una evaluación de amenazas proactiva, planificación de la mitigación, análisis de tendencias de incidentes y revisión de la arquitectura de seguridad, como se muestra en la Figura:



Respuesta del CSIRT de Cisco contra el Heartbleed

Preparación

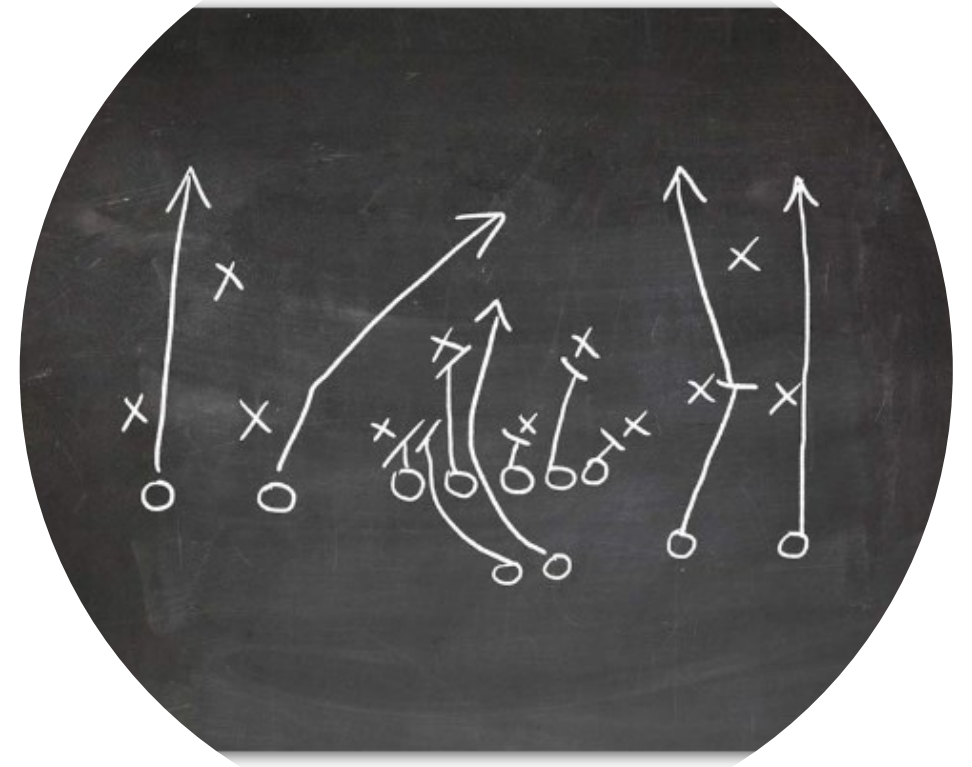
- Se escanearon 1,2 millones de servidores vulnerables; 300 necesitaron reparación.
- Ayudó a desarrollar firmas para Sourcefire y los IDS de Cisco.
- Firmas implementadas en los IDS.

Supervisión y respuesta

- Se descubrieron 25 ataques: 21 benignos, 4 maliciosos.
- Ataque investigado vía NetFlow para determinar las conexiones normales de las anómalas v maliciosas.

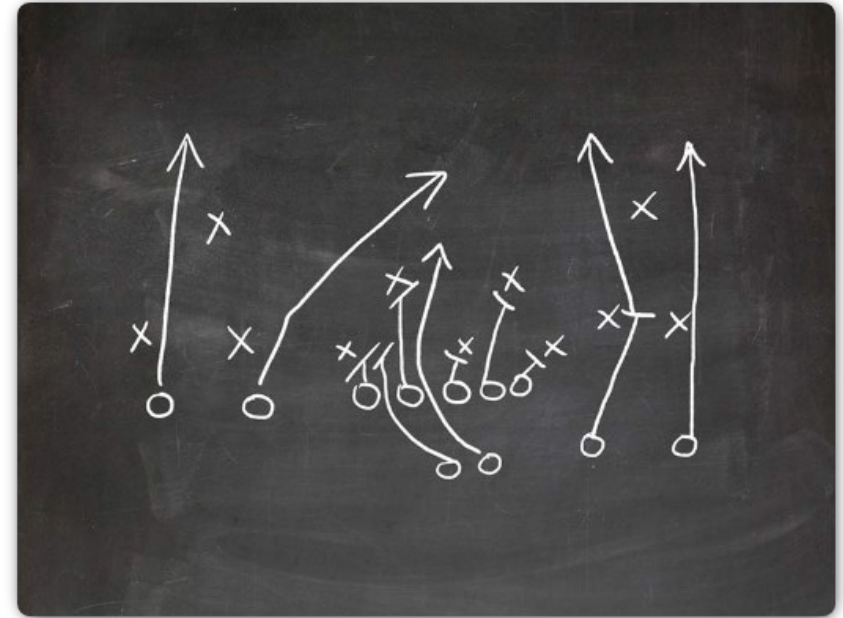
LIBRO DE ESTRATEGIAS DE SEGURIDAD

- La tecnología cambia constantemente.
 - Esto significa que los ciberataques también evolucionan.
 - Continuamente se descubren nuevas vulnerabilidades y métodos de ataque.
 - La seguridad se ha convertido en una preocupación importante para las empresas debido a la reputación y el impacto financiero resultantes de las violaciones a la seguridad.
 - Los ataques están dirigidos a redes críticas y datos confidenciales.
 - Las organizaciones deben tener planes para prepararse, para tratar las violaciones a la seguridad y recuperarse de estas.



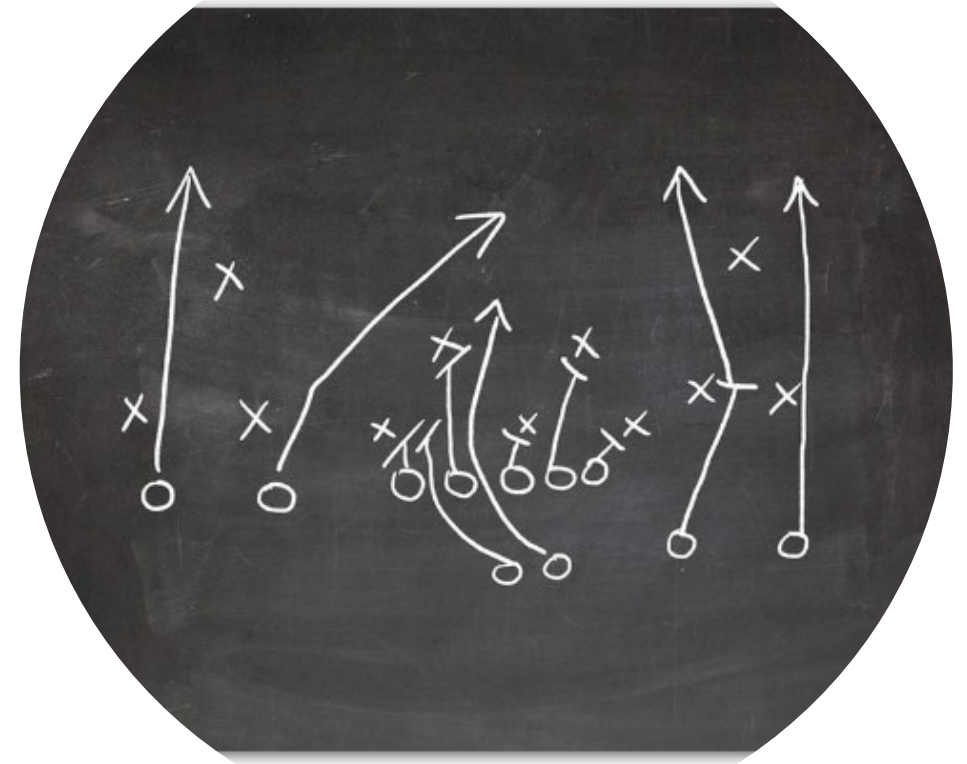
LIBRO DE ESTRATEGIAS DE SEGURIDAD

- Una de las mejores maneras de prepararse para una violación a la seguridad es prevenirla.
 - Se deben tener pautas sobre cómo identificar el riesgo de la ciberseguridad en los sistemas, los activos, los datos y las funcionalidades, proteger el sistema mediante la implementación de protecciones y capacitaciones del personal, y detectar el evento de ciberseguridad lo más rápidamente posible.
 - Cuando se detecta una violación a la seguridad, deben adoptarse las acciones adecuadas para minimizar el impacto y los daños.
 - El plan de respuesta debe ser flexible con múltiples opciones de acción durante la violación.
 - Una vez contenida la violación y restaurados los sistemas y servicios comprometidos, las medidas de seguridad y los procesos deben actualizarse para incluir las lecciones aprendidas durante la violación.



LIBRO DE ESTRATEGIAS DE SEGURIDAD

- Toda esta información se debe recopilar en un libro de estrategias de seguridad.
 - Un libro de estrategias de seguridad es un conjunto de consultas repetidas (informes) de fuentes de datos de eventos de seguridad que conducen a la detección y la respuesta ante los incidentes. Idealmente, el libro de estrategias de seguridad debe cumplir las siguientes acciones:
 - Detectar equipos infectados con malware.
 - Detectar actividad de red sospechosa.
 - Detectar intentos de autenticación irregulares.
 - Describir y entender el tráfico entrante y saliente.
 - Proporcionar información de resumen que incluya tendencias, estadísticas y recuentos.
 - Proporcionar acceso rápido y utilizable a estadísticas y métricas.
 - Establecer una correspondencia de eventos en todas las fuentes de datos relevantes.



- **Herramientas para prevención y detección de incidentes**

- Estas son algunas de las herramientas utilizadas para detectar y evitar incidentes de seguridad:

- **SIEM:** un sistema de administración de información y eventos de seguridad (SIEM) es un software que recopila y analiza las alertas de seguridad, los registros y otros datos históricos y en tiempo real de los dispositivos de seguridad de la red.

- **DLP:** el software Data Loss Prevention (DLP) es un sistema de hardware o software diseñado para evitar el robo o la fuga de datos confidenciales de la red. El sistema DLP puede concentrarse en la autorización de acceso a los archivos, el intercambio de datos, la copia de datos, la supervisión de la actividad del usuario y más. Los sistemas DLP están diseñados para supervisar y proteger los datos en tres diferentes estados: datos en uso, datos en movimiento y datos almacenados. Los datos en uso se centran en el cliente, los datos en movimiento se refieren a los datos mientras viajan a través de la red y los datos almacenados se refieren al almacenamiento de datos.



- **Cisco ISE y TrustSec:** Cisco Identity Services Engine (Cisco ISE) y Cisco TrustSec aplican el acceso a los recursos de red mediante la creación de políticas de control de acceso basado en roles que segmenta el acceso a la red (usuarios temporales, usuarios móviles, empleados) sin complejidad agregada. La clasificación del tráfico se basa en la identidad del usuario o el dispositivo. Haga clic en Reproducir en la figura para obtener más información sobre el ISE.

- Haga clic [aquí](#) para leer la transcripción de este video.

Fundamentals of ISE

HERRAMIENTAS PARA PREVENCIÓN Y DETECCIÓN DE INCIDENTES

Estas son algunas de las herramientas utilizadas para detectar y evitar incidentes de seguridad:



• Haga clic [aquí](#) para leer la transcripción de este video.

- **SIEM:**

- Un sistema de administración de información y eventos de seguridad (SIEM) es un software que recopila y analiza las alertas de seguridad, los registros y otros datos históricos y en tiempo real de los dispositivos de seguridad de la red.

- **DLP:**

- El software Data Loss Prevention (DLP) es un sistema de hardware o software diseñado para evitar el robo o la fuga de datos confidenciales de la red.
- El sistema DLP puede concentrarse en la autorización de acceso a los archivos, el intercambio de datos, la copia de datos, la supervisión de la actividad del usuario y más.
- Los sistemas DLP están diseñados para supervisar y proteger los datos en tres diferentes estados: datos en uso, datos en movimiento y datos almacenados.
- Los datos en uso se centran en el cliente, los datos en movimiento se refieren a los datos mientras viajan a través de la red y los datos almacenados se refieren al almacenamiento de datos.

- **Cisco ISE y TrustSec:**

- Cisco Identity Services Engine (Cisco ISE) y Cisco TrustSec aplican el acceso a los recursos de red mediante la creación de políticas de control de acceso basado en roles que segmenta el acceso a la red (usuarios temporales, usuarios móviles, empleados) sin complejidad agregada.
- La clasificación del tráfico se basa en la identidad del usuario o el dispositivo.

IDS E IPS

- Un sistema de detección de intrusiones (IDS), que se muestra en la figura, es un dispositivo de red exclusivo, o una de varias herramientas en un servidor o firewall que analiza los datos de una base de datos de reglas o firmas de ataque, que busca tráfico malicioso.
 - Si se detecta una coincidencia, el IDS registrará la detección y creará una alerta para el administrador de la red.
 - El sistema de detección de intrusiones no adopta medidas cuando se detecta una coincidencia, por lo que no evita que se produzcan los ataques.
 - El trabajo del IDS es simplemente detectar, registrar y generar informes.
- El análisis que realiza el IDS ralentiza la red (esto se denomina latencia).
 - Para evitar el retraso de la red, el IDS generalmente se configura sin conexión, separado del tráfico de red común.
 - Los datos se copian o duplican mediante un switch y luego se reenvían a los IDS para la detección sin conexión.
 - También existen herramientas del IDS que pueden instalarse sobre un sistema operativo de la computadora host, como Linux o Windows.
- Un sistema de prevención de intrusiones (IPS) tiene la capacidad de bloquear o denegar el tráfico en función de las coincidencias positivas de la regla o la firma.
 - Uno de los IPS/IDS más reconocidos es **Snort**.
 - La versión comercial de Snort es Sourcefire de Cisco. Sourcefire tiene la capacidad de realizar el análisis de tráfico y puerto en tiempo real, registrar, buscar y comparar contenido; puede detectar sondas, ataques y escaneos de puertos. También se combina con otras herramientas de terceros para informar y analizar el rendimiento y los registros.

Actividad: identificar la terminología del enfoque en ciberseguridad

Instrucciones

Una cada término con su descripción.

Libro de estrategias de
seguridad

IDS

SIEM

IPS

DLP

CSIRT

ISE y TrustSec

Término

Descripción

Un sistema de hardware o software diseñado para evitar el robo o la fuga de datos confidenciales en la red.

Un conjunto de consultas repetitivas contra fuentes de datos de eventos de seguridad que conduce a la detección y respuesta ante incidentes.

Refuerza el acceso a los recursos de red mediante la creación de políticas de control de acceso basadas en roles que segmentan el acceso a la red.

Ayuda a garantizar la preservación de la empresa, el sistema y los datos mediante extensas investigaciones de los incidentes en seguridad informática.

Analiza la información dentro de la base de datos de reglas o firmas de ataque, registra lo encontrado y crea una alerta para el administrador de red.

Software que recopila y analiza alertas de seguridad, registros y otros datos históricos en tiempo real de dispositivos de seguridad en la red

Bloquea o niega el tráfico de acuerdo a una regla positiva o una coincidencia de firmas.

CAPÍTULO 4: PROTECCIÓN DE LA ORGANIZACIÓN

- Este capítulo comenzó analizando algunos procesos y tecnologías utilizados por los profesionales de la ciberseguridad para proteger la red, los equipos y los datos de una organización. Incluyó tipos de firewalls, dispositivos de seguridad y software.
- Se abarcaron los botnets, la cadena de eliminación (Kill chain), la seguridad basada en el comportamiento y el uso de NetFlow para monitorear una red.
- Por último, se explicó el enfoque de Cisco para la ciberseguridad, incluidos los equipos de CSIRT y el libro de estrategias de seguridad. Abarca brevemente las herramientas que los profesionales de la ciberseguridad utilizan para detectar y prevenir los ataques a la red, incluidas SIEM, DLP, Cisco ISE y TrustSec, así como IDS e IPS.
- Si desea explorar más a fondo los conceptos de este capítulo, consulte la página [Actividades y recursos adicionales](#) en Recursos para los estudiantes.