Fundamentos de ciberseguridad - CIB

GLOSARIO DE TÉRMINOS

Ciberseguridad

ENRIQUE NIETO LORENZO
8-10-2025

GLOSARIO DE TÉRMINOS

1. Amenazas y vulnerabilidades

Las amenazas son peligros potenciales para los sistemas informáticos, mientras que las vulnerabilidades son debilidades explotables; ambos conceptos son cruciales para la protección digital.

En ciberseguridad, una amenaza es cualquier circunstancia o evento capaz de dañar un sistema, ya sea mediante ataques externos como malware, phising, ingeniería social, o por acciones internas como negligencia de usuarios o incumplimiento de políticas de protección. Las vulnerabilidades, por su parte, son fallos o fragilidades en el software, hardware o en los procesos organizativos que facilitan la explotación por parte de amenazas. Estas pueden originarse por errores de diseño, mala configuración, omisión de actualizaciones o simples descuidos en la administración de sistemas, exponiendo los datos a robos, pérdidas o modificaciones. La relación con el módulo es total: el análisis y gestión de amenazas y vulnerabilidades permite abordar los riesgos antes de que ocurran incidentes, diseñando sistemas más seguros y resilientes.

Enlace externo:

- Artículo Amenaza, vulnerabilidad y riesgo: Diferencias en Red Seguridad

2. Principios de confidencialidad, integridad y disponibilidad

La tríada CID asegura que la información de un sistema es privada, precisa y siempre accesible para los usuarios autorizados.

La confidencialidad implica que los datos sólo puedan ser leídos por usuarios autorizados,

implementando mecanismos de acceso restringido, autenticación y cifrado, y evitando la divulgación no deseada. La integridad garantiza la exactitud y la consistencia de la información, protegida contra modificaciones accidentales o maliciosas; para ello se emplean permisos de acceso, copias de seguridad y sistemas de verificación como el hashing. La disponibilidad asegura que los datos y sistemas estén accesibles cuando los necesiten los usuarios autorizados, lo que implica redundancia, recuperación ante desastres y vigilancia constante del sistema. Estos tres principios fundamentan todas las políticas de la seguridad informática, y conocerlos es vital para diseñar y operar sistemas resistentes frente a ataques y fallos.

Enlace externo:

- Artículo: Confidencialidad, integridad y disponibilidad en LinkedIn

3. Malware

El malware es cualquier tipo de software malicioso que perjudica, roba o interrumpe sistemas informáticos y representa un riesgo constante en ciberseguridad.

Malware (malicious software) agrupa diferentes programas creados deliberadamente para causar daño digital. Los tipos principales son virus, gusanos, troyanos, ransomware, spyware y adware. Los virus y gusanos se replican y propagan, infectando archivos y redes. Los troyanos aparentan ser legítimos pero permiten acceso malicioso al sistema. El ransomware cifra los archivos y exige un rescate para su liberación; el spyware sustrae información confidencial sin consentimiento. Estos ataques pueden provocar la pérdida de datos, el robo de contraseñas y la interrupción de operaciones empresariales, lo que subraya su relevancia en el módulo: prevenir y detectar malware es parte esencial del trabajo en ciberseguridad.

Enlace externo:

- Guia de tipos de malware de Kaspersky

4. Ingeniería social

La ingeniería social manipula psicológicamente a las personas para obtener información o acceso a sistemas, usando engaños y técnicas de persuasión.

Esta práctica engloba ataques donde el atacante explota la confianza, curiosidad o miedo de la víctima en vez de vulnerar sistemas tecnológicos. Ejemplos comunes son el phishing (correo falso que simula una entidad legítima para robar credenciales), el vishing (fraudes por teléfono), el smishing (mensajes SMS fraudulentos) y el pretexting (falsificación de identidad para obtener datos privados). La defensa se centra en la educación y la concienciación, la aplicación de controles técnicos como el filtrado de correos o autenticación multifactor y la vigilancia ante comportamientos sospechosos. Este tema es esencial para el módulo, pues muchos incidentes comienzan por errores humanos y mala percepción de los riesgos.

Enlace externo:

- Artículo ingeniería social en hideez.com

5. DoS y DDoS

Los ataques DoS y DDoS buscan dejar fuera de servicio sistemas informáticos o páginas web, saturando los recursos mediante un número desmesurado de peticiones.

Desarrollo extenso:
Un ataque DoS (Denial of Service) se realiza desde un único equipo contra un servidor, bombardeándolo hasta que queda inaccesible. Un ataque DDoS (Distributed Denial of Service) multiplica ese efecto usando una red de equipos (botnet), haciendo que el ataque sea más difícil de identificar y detener. Ambos provocan la indisponibilidad de recursos, ralentización de servicios y daños económicos, y suelen aprovechar vulnerabilidades en la infraestructura. Son especialmente relevantes en ciberseguridad porque afectan la disponibilidad de los sistemas, uno de los principios del módulo; detectarlos y mitigarlos es una competencia clave.

Enlace externo:

- Infografía Ataque DoS vs DDoS en Fortinet
- Artículo de Linube sobre DDoS/DoS

6. Man-in-the-Middle

El ataque Man-in-the-Middle consiste en interceptar y manipular la comunicación entre dos partes sin que lo sepan, comprometiendo la confidencialidad y autenticidad de los datos.

Los ataques Man-in-the-Middle (MITM) ocurren cuando un atacante se sitúa entre dos partes que se comunican, como un usuario y un sitio web, interceptando el tráfico en redes Wi-Fi públicas, mediante envenenamiento de ARP o aprovechando vulnerabilidades en los protocolos de seguridad. El agresor puede leer, modificar o suplantar los mensajes, robando contraseñas, datos personales o bancarios y, en ocasiones, alterando transacciones o sessiones. Para prevenirlos, se recomienda usar conexiones seguras (HTTPS), evitar redes abiertas, emplear VPNs y estar atento ante certificaciones digitales dudosas. Este ataque está estrechamente vinculado a la confidencialidad y la integridad, principios fundamentales de ciberseguridad.

Enlace externo recomendado:

- Artículo Man-in-the-Middle Godaddy

7. Exploits

Un exploit es un programa o fragmento de código que aprovecha vulnerabilidades en sistemas o aplicaciones para ejecutar acciones maliciosas sin autorización.

Un exploit consiste en una técnica o software que se utiliza para aprovechar una vulnerabilidad identificada en un sistema, una aplicación o incluso en dispositivos físicos. Estos fallos pueden

ser del tipo conocido (con solución) o de día cero (0-day), cuando aún no se ha hecho público ni existe parche disponible, resultando especialmente peligrosos porque los atacantes tienen ventaja sobre los desarrolladores de la seguridad. Los exploits pueden destinarse a obtener acceso no autorizado, robar información, propagar malware o interrumpir el funcionamiento normal de un sistema.

En ciberseguridad, conocer y entender los exploits es fundamental, ya que permiten a los profesionales anticiparse y proteger los sistemas mediante actualizaciones y corrección de errores. Su relación con el módulo incluye el análisis de vulnerabilidades, la defensa ante ataques y la importancia de mantener un entorno software siempre actualizado.

Enlaces externos:

- Guía completa de Exploits - Universidad Alfonso X
- Bitdefender: Prevención de Exploits

8. Inyección SQL

La inyección SQL es un ataque que introduce código malicioso en consultas a bases de datos, permitiendo el acceso, robo o manipulación de datos sensibles.

La inyección SQL (SQL Injection) explota vulnerabilidades en aplicaciones web que no filtran correctamente las entradas de los usuarios, permitiendo que estos agreguen código malicioso en las consultas SQL. El atacante puede así sortear mecanismos de autenticación, acceder a información confidencial o modificar la base de datos según sus intereses. Los ataques suelen ser simples, como añadir 'OR 1=1--' en un formulario para saltarse un login, pero pueden llegar a comprometer completamente grandes sistemas y datos personales.

La importancia en el módulo es clara: la prevención mediante validación, el uso de consultas preparadas y el control de accesos constituyen pilares esenciales en el diseño de aplicaciones web seguras. Una correcta gestión reduce drásticamente la exposición a este tipo de ataques, crítico en cualquier entorno profesional de desarrollo.

Enlaces externos:

- Microsoft: inyección de código SQL
- Proofpoint: qué es SQL Injection

9. Cross-Site Scripting (XSS)

El Cross-Site Scripting (XSS) es una vulnerabilidad que permite a los atacantes inyectar código malicioso en páginas web vistas por otros usuarios, alterando el comportamiento del sitio o robando datos.

El XSS se produce al aceptar sin validar datos del usuario e insertarlos directamente en el HTML, permitiendo que scripts maliciosos se ejecuten en el navegador de la víctima. Estos scripts aprovechan la confianza del navegador en el sitio web, pudiendo robar cookies, secuestrar sesiones, mostrar contenido falso o redirigir a enlaces peligrosos. Existen variantes como XSS reflejado, almacenado y basado en DOM, cada uno con sus métodos y riesgo potencial.

Protegerse contra XSS implica validar y limpiar todas las entradas del usuario, aplicar políticas de seguridad de contenido (CSP) y emplear frameworks y bibliotecas que mitiguen la ejecución de scripts no confiables. El módulo exige comprender estas técnicas para desarrollar aplicaciones robustas y confiables, evitando daños reputacionales y legales.

Enlaces externos:

- Artículo CDmon sobre XSS
- Xygeni: cómo mantenerse seguro frente a XSS

10. Cifrar

Cifrar es convertir información en un formato ilegible salvo para quienes posean la clave correcta, protegiendo la confidencialidad y la integridad de los datos.

El cifrado es un proceso clave en la protección de la información. Utiliza algoritmos y claves para convertir datos claros (plaintext) en datos cifrados (ciphertext), de modo que solo quienes tengan la clave puedan acceder a la información original. Existen dos grandes tipos: el cifrado simétrico (misma clave para cifrar y descifrar) y el asimétrico (un par de claves, pública y privada). El cifrado garantiza privacidad, ayuda a demostrar la autenticidad y evita alteraciones no autorizadas en archivos o transmisiones.

El uso de la criptografía es esencial en el módulo: protege mensajes, archivos, comunicaciones y procesos críticos; es además obligatorio por diversas normativas y leyes de protección de datos. La elección de buenas herramientas y su correcta implementación marcan la diferencia en cualquier entorno profesional.

Enlaces externos:

- Aplicaciones criptográficas y cifrado

11. Ransomware

El ransomware es un malware que cifra los archivos de la víctima, exigiendo un rescate por la recuperación de los datos, y supone una de las amenazas más graves para particulares y empresas.

El término ransomware proviene de “ransom” (rescate). Este malware accede a un sistema, cifra los datos o bloquea el acceso, y luego solicita un pago, normalmente en criptomonedas, a cambio de la clave de descifrado. Los métodos más frecuentes de infección incluyen emails maliciosos, enlaces fraudulentos y vulnerabilidades sin actualizar. Los atacantes pueden utilizar ransomware de cifrado (encripta archivos) o ransomware bloqueador (impide el uso del sistema mostrando una pantalla de bloqueo).

En los últimos años, ha crecido el riesgo para organizaciones que dependen de la disponibilidad operativa de sus datos. Este tipo de ataque subraya la importancia de la ciberseguridad, las copias de seguridad regulares y la concienciación de los usuarios, cuestiones que son pilares en el contenido del módulo.

Enlaces externos:

- Proofpoint: ransomware y prevención
- Checkpoint: Qué es un ataque ransomware

12. Autenticación Multifactor (MFA)

La autenticación multifactor (MFA) exige más de una prueba de identidad, como contraseña más un código enviado al móvil o biometría, reforzando la seguridad de accesos y datos.

MFA significa emplear dos o más métodos independientes para verificar la identidad de un usuario. Estos métodos suelen dividirse en algo que el usuario conoce (contraseña), algo que posee (un teléfono o token de hardware) y algo que es (biometría, como huella digital). Este enfoque dificulta el acceso no autorizado, ya que aunque uno de los factores sea robado (por ejemplo, la contraseña) el atacante necesitaría los otros para acceder.

La MFA es cada vez más obligatoria para servicios online, banca, redes corporativas e infraestructuras críticas. Su integración y correcta configuración es fundamental en el módulo de ciberseguridad, enseñando cómo implementar barreras efectivas frente al robo de credenciales.

Enlaces externos:

- IBM: ¿qué es MFA?
- Splashtop: MFA métodos y ventajas

13. Roles y permisos

Los roles y permisos son controles de acceso fundamentales en ciberseguridad que gestionan quién puede hacer qué dentro de un sistema o red. Los roles agrupan a los usuarios con

responsabilidades similares, mientras que los permisos definen las acciones específicas que pueden realizar, garantizando así el principio de mínimo privilegio.

En el ámbito de la seguridad informática, la gestión de acceso es crucial para proteger la información y los recursos. El "control de acceso basado en roles" (RBAC) es un enfoque en el que los permisos se asignan a roles específicos dentro de una organización en lugar de a usuarios individuales. Los usuarios son luego asignados a estos roles, heredando los permisos correspondientes.

Esta metodología simplifica la administración, ya que en lugar de gestionar los permisos de cada usuario por separado, se administran los roles. Por ejemplo, en una empresa, se pueden definir roles como "Administrador de TI", "Analista de seguridad" o "Usuario estándar". Cada uno de estos roles tendrá asociados permisos específicos. El administrador de TI tendrá amplios permisos para configurar sistemas, mientras que un usuario estándar solo podrá acceder a las aplicaciones necesarias para su trabajo diario.

La correcta definición de roles y la asignación de permisos son esenciales para implementar el "principio de mínimo privilegio", que establece que un usuario solo debe tener los permisos estrictamente necesarios para realizar sus tareas. Esto minimiza el riesgo de exposición o uso indebido de información sensible. La relación con el módulo de ciberseguridad es total, ya que una gestión de roles y permisos deficiente puede dar lugar a brechas de seguridad, ya sea por errores humanos o por actores malintencionados que explotan permisos excesivos.

Enlace externo:

- Artículo sobre Control de acceso basado en roles: https://ciberseguridad.vip/control-de-acceso/por-roles/

14. Reglas de firewall

Las reglas de firewall son un conjunto de condiciones que determinan qué tráfico de red se permite o se bloquea. Actúan como un filtro de seguridad, controlando las comunicaciones entre una red interna y una externa para proteger los sistemas de accesos no autorizados y otras amenazas.

Un firewall es una barrera de seguridad que monitorea y controla el tráfico de red entrante y saliente basándose en un conjunto de reglas de seguridad predefinidas. Estas reglas especifican los criterios que debe cumplir el tráfico para ser permitido o denegado. Los criterios pueden incluir la dirección IP de origen y destino, el puerto de origen y destino, y el protocolo de red utilizado (como TCP o UDP).

La función principal de un firewall es determinar qué tipos de tráfico pueden entrar y salir de una red protegida. Por ejemplo, una regla de firewall podría permitir el tráfico web entrante en el puerto 80 (HTTP), pero bloquear el acceso a otros puertos para prevenir ataques. Las reglas se evalúan en un orden de prioridad, y cuando el tráfico coincide con una regla, se aplica la acción correspondiente (permitir o bloquear) y no se evalúan más reglas.

Una configuración adecuada de las reglas del firewall es fundamental para la seguridad de la red. Una base de reglas optimizada y actualizada ayuda a restringir el tráfico no deseado y a supervisar el acceso a los dispositivos. La relación con el módulo de ciberseguridad es directa, ya que los firewalls son una de las primeras líneas de defensa contra ciberataques, y la correcta definición de sus reglas es esencial para proteger la integridad y confidencialidad de la información de una organización.

15. Filtrado de puertos y protocolos

El filtrado de puertos y protocolos es una función de seguridad de red que controla el flujo de datos basándose en los números de puerto y los protocolos de red. Permite a los administradores de red especificar qué servicios y aplicaciones pueden ser accedidos desde el exterior, bloqueando el tráfico no deseado.

En las redes informáticas, los puertos son puntos finales de comunicación que permiten a los ordenadores distinguir entre diferentes tipos de tráfico. Cada servicio de red (como la navegación web o el correo electrónico) utiliza un puerto específico. El filtrado de puertos y protocolos implica la configuración de dispositivos de red, como routers o firewalls, para permitir o denegar el tráfico a puertos y protocolos específicos.

Por ejemplo, el tráfico web normalmente utiliza el puerto 80 para HTTP y el 443 para HTTPS. Un administrador de red puede configurar un firewall para permitir el tráfico en estos puertos, pero bloquear el acceso a otros puertos que podrían ser utilizados para ataques, como el puerto 23 para Telnet (un protocolo de texto no seguro). El filtrado también puede basarse en protocolos como TCP (Protocolo de Control de Transmisión) o UDP (Protocolo de Datagramas de Usuario).

El filtrado de paquetes en los routers puede basarse en criterios como los protocolos utilizados, la dirección IP de origen y destino, y el puerto TCP/UDP de origen y destino. Esto proporciona una gran flexibilidad para gestionar el tráfico de la red. La relación con el módulo de ciberseguridad es fundamental, ya que el filtrado de puertos y protocolos es una técnica esencial para hacer segura una red, limitando la superficie de ataque y previniendo que los atacantes exploten servicios vulnerables.

Enlace externo recomendado:

- Artículo sobre filtrado de paquetes: https://www.segu-info.com.ar/firewall/fw_paquetes.htm[8]

16. Routers

Los routers son dispositivos de hardware que conectan redes y dirigen el tráfico de datos entre ellas. En ciberseguridad, son un componente crítico ya que pueden ser un punto de entrada para los atacantes si no se configuran y mantienen adecuadamente.

Un router es un dispositivo que sirve de punto de conexión entre una red local e Internet, gestionando el tráfico y los datos entre diferentes redes.[9] Permiten que varios dispositivos compartan la misma conexión a Internet. Sin embargo, los routers también presentan riesgos para la ciberseguridad.

Muchos usuarios no cambian la contraseña predeterminada del router, lo que facilita a los hackers el acceso al dispositivo y el control de la red. Además, la falta de actualizaciones de firmware puede dejar a los routers vulnerables a ataques conocidos. Es crucial cambiar la contraseña predeterminada, utilizar una contraseña segura para la red Wi-Fi, actualizar el firmware regularmente y desactivar el acceso remoto si no es necesario para minimizar los riesgos.

La relación con el módulo de ciberseguridad es muy importante. Un router mal configurado puede ser una puerta de entrada para malware y otros ataques a la red de una casa o una oficina. La seguridad del router es un paso fundamental para proteger todos los dispositivos conectados a la red.

Enlace externo:

- Artículo sobre los peligros de los routers para la ciberseguridad: https://onwork.es/blog/los-routers-y-sus-peligros-para-la-ciberseguridad/

17. Monitoreo y auditoría

El monitoreo y la auditoría en ciberseguridad son procesos continuos de supervisión y evaluación de los sistemas informáticos para detectar y responder a amenazas de seguridad. El monitoreo busca actividades sospechosas en tiempo real, mientras que la auditoría revisa periódicamente los controles de seguridad para asegurar su eficacia y cumplimiento.

El monitoreo constante de los sistemas es crucial para detectar posibles amenazas y tomar medidas preventivas a tiempo. Implica la revisión de registros de eventos (logs), el análisis del tráfico de red y el uso de herramientas de detección de intrusiones para identificar patrones de comportamiento anómalos. La falta de un monitoreo y registro suficientes puede permitir a los atacantes persistir en sus ataques, moverse a otros sistemas y manipular o robar datos.

Por otro lado, la auditoría de ciberseguridad es una evaluación exhaustiva de los sistemas, políticas y procedimientos de una organización para garantizar que cumplen con los estándares de seguridad y las mejores prácticas. Las auditorías ayudan a identificar vulnerabilidades y brechas de seguridad que podrían ser explotadas por ciberamenazas. También verifican el cumplimiento de leyes y regulaciones relevantes.

La relación con el módulo de ciberseguridad es esencial. El monitoreo y la auditoría permiten a las organizaciones adoptar un enfoque proactivo de la seguridad, identificando y mitigando los riesgos antes de que se conviertan en incidentes graves. Son prácticas fundamentales para la mejora continua de la postura de seguridad de una organización.

Enlace externo:

- Artículo sobre la auditoría de ciberseguridad: https://www.piranirisk.com/es/blog/auditoria-de-ciberseguridad-todo-lo-que-necesitas-saber

18. Incidentes de seguridad.

Un incidente de seguridad es cualquier evento que compromete la confidencialidad, integridad o disponibilidad de la información de una organización. Estos eventos pueden variar desde ataques de malware y phishing hasta accesos no autorizados y fugas de datos.

Un incidente de seguridad informática es la ocurrencia de uno o más eventos que atentan contra la seguridad de la información. Estos incidentes pueden ser causados por debilidades o vulnerabilidades en los sistemas que son explotadas de forma intencionada o no. Ejemplos comunes de incidentes de seguridad incluyen ataques de ransomware, ataques de denegación de servicio (DDoS), phishing, acceso no autorizado a sistemas y pérdida de datos.

La gestión de incidentes de seguridad es un proceso que incluye varias etapas: identificación y análisis del incidente, contención, erradicación, recuperación y lecciones aprendidas. La falta de preparación ante un incidente puede amplificar sus consecuencias, llevando a la pérdida irreversible de datos, interrupción de las operaciones, sanciones legales y daños a la reputación.

La relación con el módulo de ciberseguridad es directa. La prevención y gestión de incidentes de seguridad son aspectos centrales de la ciberseguridad. La capacidad de una organización para responder de manera rápida y efectiva a un incidente es crucial para mitigar su impacto y restaurar la normalidad de las operaciones lo antes posible.

Enlace externo:

- Artículo sobre incidentes de seguridad de la información: https://blog.hackmetrix.com/incidentes-de-seguridad-que-son-y-como-protegerte/

19. Ciclo de vida de un incidente: detección, análisis, contención, erradicación, recuperación y aprendizaje

El ciclo de vida de un incidente de seguridad es un modelo estructurado que guía a las organizaciones a través de las fases necesarias para gestionar una brecha de seguridad de manera efectiva. Este proceso abarca desde la identificación inicial de una amenaza hasta la restauración de las operaciones normales y la implementación de mejoras para prevenir futuros incidentes.

La gestión de incidentes de seguridad sigue un ciclo de vida bien definido para garantizar una respuesta organizada y eficaz. Las fases son las siguientes:

- **Detección:** Es el punto de partida, donde se identifica que ha ocurrido un incidente de seguridad. Esto puede ser a través de alertas de sistemas de monitoreo, informes de usuarios o análisis de registros del sistema.
- **Análisis:** Una vez detectado, se analiza el incidente para comprender su alcance, impacto y origen. Se busca determinar qué sistemas están afectados, qué tipo de ataque se ha producido y cuál es la gravedad de la situación.

- **Contención:** En esta fase, el objetivo es limitar el daño y evitar que el incidente se propague. Esto puede implicar aislar los sistemas afectados de la red o desactivar ciertas funcionalidades temporalmente.
- **Erradicación:** Una vez contenido, se procede a eliminar la causa raíz del incidente. Esto puede significar eliminar malware, parchear vulnerabilidades o cambiar contraseñas comprometidas.
- **Recuperación:** Se restauran los sistemas y datos afectados a su estado normal de funcionamiento. Esto puede incluir la restauración de copias de seguridad y la verificación de que los sistemas están limpios y seguros.
- **Aprendizaje (o lecciones aprendidas):** Después de que el incidente se ha resuelto, se realiza un análisis post-incidente para identificar qué salió bien, qué se podría haber hecho mejor y qué cambios se deben implementar para prevenir incidentes similares en el futuro. Esta fase es crucial para la mejora continua de la seguridad.

20. Indicadores de compromiso (IoC)

Los Indicadores de Compromiso (IoC) son piezas de evidencia o datos forenses que señalan que la seguridad de una red o sistema ha sido potencialmente vulnerada. Estos indicadores actúan como pistas que los equipos de ciberseguridad utilizan para detectar actividades maliciosas, investigar incidentes y fortalecer las defensas.

En el campo de la ciberseguridad, los IoC son las "huellas dactilares" que dejan los atacantes. Identificar estos indicadores permite a las organizaciones detectar ataques en sus primeras etapas y responder de manera proactiva. Algunos ejemplos comunes de Indicadores de Compromiso incluyen:

- **Tráfico de red inusual:** Patrones de tráfico extraños, como grandes volúmenes de datos saliendo de la red en horarios no habituales o conexiones a direcciones IP sospechosas.
- **Anomalías en cuentas de usuario:** Actividad inusual en cuentas con privilegios elevados, múltiples intentos fallidos de inicio de sesión o inicios de sesión desde ubicaciones geográficas extrañas.
- **Cambios en archivos o registros del sistema:** Modificaciones no autorizadas en archivos críticos del sistema o en el registro de Windows pueden ser un signo de malware.
- **Solicitudes de DNS anómalas:** Peticiones a dominios maliciosos conocidos o patrones de solicitud de DNS extraños.

La monitorización y el análisis de IoC son componentes clave de la inteligencia de amenazas. Permiten a los equipos de seguridad no solo responder a los incidentes actuales, sino también aprender de ellos para mejorar las defensas y prevenir futuros ataques. La relación con el

módulo es total, ya que el uso de IoC es una práctica fundamental en la detección y respuesta a incidentes.

21. Estrategias proactivas

Las estrategias proactivas en ciberseguridad se centran en anticipar y prevenir los ataques antes de que ocurran, en lugar de simplemente reaccionar a ellos. Este enfoque implica una monitorización constante, la búsqueda activa de amenazas y la implementación de defensas robustas para minimizar la superficie de ataque.

A diferencia de la ciberseguridad reactiva, que se activa después de que un incidente ha ocurrido, la seguridad proactiva busca identificar y mitigar las vulnerabilidades antes de que puedan ser explotadas. Algunas de las prácticas clave en una estrategia proactiva incluyen:

- **Caza de amenazas (Threat Hunting):** Búsqueda activa de amenazas y actores maliciosos dentro de la red, sin esperar a que se disparen las alertas.
- **Análisis de vulnerabilidades y pruebas de penetración:** Evaluaciones periódicas de los sistemas para identificar y corregir debilidades de seguridad.
- **Inteligencia de amenazas:** Recopilación y análisis de información sobre amenazas emergentes para anticipar posibles ataques.
- **Monitorización continua de la seguridad:** Supervisión constante de la red y los sistemas para detectar actividades sospechosas en tiempo real.
- **Formación y concienciación de los empleados:** Educar a los usuarios sobre las mejores prácticas de seguridad para reducir el riesgo de errores humanos.

La relación con el módulo de ciberseguridad es intrínseca, ya que un enfoque proactivo es esencial para construir una defensa en profundidad y resiliente. Permite a las organizaciones pasar de una postura defensiva a una de anticipación, reduciendo significativamente la probabilidad y el impacto de los ciberataques.

22. Análisis forense

El análisis forense informático es la disciplina que aplica técnicas de investigación para recopilar, examinar y preservar evidencia digital de un dispositivo informático de manera que sea admisible en un proceso legal. Su objetivo es reconstruir eventos pasados para determinar el origen y el alcance de un incidente de seguridad o un delito cibernético.

El proceso de análisis forense digital se lleva a cabo siguiendo una metodología estricta para garantizar la integridad de la evidencia. Las fases principales incluyen:

- **Identificación:** Reconocer y localizar las posibles fuentes de evidencia digital, como ordenadores, servidores o dispositivos móviles.

- **Preservación:** Asegurar que la evidencia digital no sea alterada. Esto generalmente implica crear una copia exacta (imagen forense) del dispositivo original para trabajar sobre ella.
- **Análisis:** Utilizar herramientas y técnicas especializadas para examinar la copia de la evidencia en busca de datos relevantes, incluidos archivos eliminados o fragmentos de información.
- **Documentación:** Registrar detalladamente todos los pasos seguidos durante la investigación, desde la recopilación de la evidencia hasta las conclusiones obtenidas.
- **Presentación:** Exponer los hallazgos de manera clara y concisa, a menudo en forma de un informe pericial que puede ser utilizado en un tribunal.

La relación con el módulo de ciberseguridad es crucial, especialmente en la respuesta a incidentes. El análisis forense permite a las organizaciones entender cómo ocurrió un ataque, qué datos fueron comprometidos y quién fue el responsable, proporcionando información valiosa para la recuperación y para fortalecer las defensas futuras.

23. Cortafuegos, IDS/IPS

Los cortafuegos (Firewalls), los Sistemas de Detección de Intrusiones (IDS) y los Sistemas de Prevención de Intrusiones (IPS) son componentes fundamentales de la seguridad de una red. Mientras que los cortafuegos actúan como una barrera que filtra el tráfico basándose en reglas predefinidas, los IDS monitorizan la red en busca de actividades sospechosas y los IPS pueden además tomar medidas para bloquear dichas actividades.

Estos tres elementos, aunque a menudo trabajan juntos, tienen funciones distintas:

- **Cortafuegos (Firewall):** Es la primera línea de defensa. Funciona como un filtro que controla el tráfico de red entrante y saliente basándose en un conjunto de reglas, como permitir o bloquear el tráfico según direcciones IP, puertos o protocolos.
- **Sistema de Detección de Intrusiones (IDS):** Es un sistema pasivo que monitoriza el tráfico de la red o las actividades de un sistema en busca de patrones maliciosos o anómalos. Cuando detecta una posible amenaza, genera una alerta para que un administrador la investigue. No bloquea el tráfico por sí mismo.
- **Sistema de Prevención de Intrusiones (IPS):** Es un sistema activo que no solo detecta actividades maliciosas como un IDS, sino que también puede tomar medidas para prevenirlas en tiempo real. Por ejemplo, puede bloquear el tráfico de una dirección IP sospechosa o terminar una conexión maliciosa.

La relación con el módulo de ciberseguridad es total, ya que la combinación de estas tecnologías crea una defensa en capas (defensa en profundidad). El cortafuegos establece el perímetro de seguridad, el IDS proporciona visibilidad sobre las posibles amenazas que lo atraviesan y el IPS actúa como una barrera adicional para detener los ataques conocidos.

24. Antivirus

El software antivirus es un programa diseñado para detectar, prevenir y eliminar software malicioso (malware) de los dispositivos informáticos. Actúa como una defensa esencial para proteger los sistemas contra una amplia gama de amenazas como virus, troyanos, gusanos y spyware.

El funcionamiento de un antivirus se basa principalmente en dos métodos:

- **Detección basada en firmas:** El antivirus mantiene una base de datos de "firmas" de malware conocido. Escanea los archivos del sistema y los compara con esta base de datos. Si encuentra una coincidencia, identifica el archivo como malicioso. Por esta razón, es crucial mantener la base de datos del antivirus actualizada.
- **Detección heurística o basada en el comportamiento:** Para detectar malware nuevo y desconocido (amenazas de día cero), los antivirus modernos utilizan análisis heurístico. Monitorizan el comportamiento de los programas en tiempo real y buscan acciones sospechosas, como la modificación de archivos del sistema o el intento de replicarse. Si un programa exhibe un comportamiento considerado malicioso, el antivirus lo bloquea.

Cuando un antivirus detecta una amenaza, generalmente ofrece opciones como poner el archivo en cuarentena (aislarlo para que no pueda causar daño) o eliminarlo por completo. La relación con el módulo de ciberseguridad es fundamental, ya que los antivirus son una herramienta de protección de endpoints indispensable tanto para usuarios individuales como para organizaciones.

25. Cortafuegos: basados en red y cortafuegos basados en host

Los cortafuegos, una herramienta esencial de seguridad, se pueden clasificar en dos tipos principales según su ubicación y alcance: los basados en red, que protegen a toda una red, y los basados en host, que protegen a un dispositivo individual.

La principal diferencia entre estos dos tipos de cortafuegos radica en dónde operan y qué protegen:

- **Cortafuegos basados en red:** Son dispositivos de hardware o software que se sitúan en el perímetro de una red (por ejemplo, entre la red interna de una empresa e Internet). Inspeccionan todo el tráfico que entra y sale de la red y aplican un conjunto de reglas para permitir o bloquear el tráfico para todos los dispositivos dentro de esa red. Son ideales para establecer una primera línea de defensa general para una organización.
- **Cortafuegos basados en host:** Son aplicaciones de software que se instalan directamente en un dispositivo individual (un "host"), como un ordenador portátil o un servidor. Monitorizan el tráfico que entra y sale de ese dispositivo específico. Ofrecen una protección más granular, permitiendo establecer reglas específicas para diferentes

aplicaciones en el mismo dispositivo. Un ejemplo común es el Firewall de Windows Defender.

La relación con el módulo de ciberseguridad es muy relevante. A menudo, se utiliza una combinación de ambos tipos de cortafuegos para crear una defensa en profundidad. El cortafuegos de red protege el perímetro, mientras que los cortafuegos de host proporcionan una capa adicional de seguridad para los dispositivos individuales, protegiéndolos incluso de amenazas que puedan originarse dentro de la propia red local.

26. IDS y IPS

Los Sistemas de Detección de Intrusiones (IDS) y los Sistemas de Prevención de Intrusiones (IPS) son tecnologías de seguridad de red que monitorizan el tráfico en busca de actividades maliciosas. La diferencia fundamental es que un IDS es un sistema de monitorización pasivo que genera alertas, mientras que un IPS es un sistema activo que puede tomar medidas para bloquear las amenazas detectadas.

Aunque ambos sistemas a menudo se utilizan conjuntamente, sus roles son distintos:

- **Sistema de Detección de Intrusiones (IDS):** Este sistema se coloca fuera del flujo de tráfico real, analizando una copia del mismo. Su función es similar a la de un vigilante de seguridad que observa las cámaras y avisa si ve algo sospechoso. Detecta posibles intrusiones basándose en firmas de ataques conocidos o en desviaciones del comportamiento normal de la red (anomalías). Cuando identifica una amenaza, registra la información y envía una alerta a un administrador, pero no interviene para detenerla.
- **Sistema de Prevención de Intrusiones (IPS):** A diferencia del IDS, el IPS se sitúa en línea, directamente en la ruta del tráfico de red. Esto le permite no solo detectar amenazas, sino también actuar para prevenirlas en tiempo real. Siguiendo la analogía, sería como un guardia de seguridad en la puerta que puede impedir físicamente la entrada a alguien no autorizado. Un IPS puede descartar paquetes maliciosos, bloquear el tráfico de una fuente peligrosa o restablecer conexiones.

La relación con el módulo de ciberseguridad es muy estrecha. Muchas soluciones de seguridad modernas integran ambas funcionalidades en un solo dispositivo, a menudo denominado Sistema de Detección y Prevención de Intrusiones (IDPS). La elección entre un IDS, un IPS o una solución combinada dependerá de las necesidades específicas de seguridad y de la arquitectura de red de una organización.

27. Antivirus y antimalware
28. Reglamento General de Protección de Datos (RGPD). ISO/IEC 27001
29. Esquema Nacional de Seguridad (ENS).
30. Datos sensibles
31. Políticas de acceso
32. Ciclo de vida de la información
33. Diagnóstico de fallos
34. Propuestas de mejora
35. Registro de incidencias