**Respuesta a Incidentes (Incident Response)**

Es el proceso mediante el cual un SOC maneja y mitiga los incidentes de seguridad para minimizar el impacto en la organización.

**Pasos y Componentes:**

* **Unidades de Negocio (Business Units):** Estas unidades de negocio colaboran en la detección temprana de incidentes al informar cualquier actividad sospechosa o inusual dentro de sus operaciones. Aseguran que las políticas de seguridad y los procedimientos establecidos por el equipo de respuesta se implementen correctamente en sus áreas. Participan en la formación de empleados sobre prácticas de seguridad cibernética, promoviendo una cultura de seguridad dentro de la organización. Proporcionan información y soporte al equipo de respuesta durante un incidente, facilitando el acceso a sistemas y datos relevantes.

Adicionalmente, ayudan a evaluar el impacto del incidente en sus operaciones, contribuyendo a la priorización de respuestas y la recuperación. Actúan como un canal de comunicación entre el equipo de respuesta y los empleados, asegurando que la información sobre el incidente y las medidas a tomar se transmitan de manera efectiva. Participan en la revisión post-incidente para identificar lecciones aprendidas y sugerir mejoras en los procesos y procedimientos.

En conclusión, las unidades de negocio son clave para la respuesta a incidentes cibernéticos, ya que aportan conocimientos específicos de su área y colaboran para mitigar el impacto de los incidentes en la organización.

* **Comité de Dirección (Steering Committee):** un grupo de respuesta a incidentes cibernéticos tiene varias funciones clave: Define y revisa las políticas de seguridad cibernética y la estrategia general para la gestión de incidentes. Proporciona supervisión y dirección a las operaciones del equipo de respuesta a incidentes, asegurando que se sigan las mejores prácticas y estándares de la industria. Realiza evaluaciones periódicas de riesgos y vulnerabilidades para identificar áreas de mejora en la seguridad cibernética de la organización. Asegura que el equipo de respuesta tenga acceso a los recursos necesarios, incluyendo personal, tecnología y formación.

Toma decisiones críticas durante un incidente, como la escalación de problemas, la comunicación con las partes interesadas y la implementación de medidas correctivas. Después de un incidente, revisa la respuesta para identificar lecciones aprendidas y mejorar los procesos futuros. Actúa como punto de contacto para la comunicación con la alta dirección y otras partes interesadas, manteniendo a todos informados sobre el estado de los incidentes y las medidas tomadas.

En resumen, el comité de dirección juega un papel vital en la gobernanza y efectividad de la respuesta a incidentes cibernéticos, asegurando que la organización esté bien preparada y pueda reaccionar de manera efectiva ante amenazas.

* **Gestión (Management):** Esta área de gestión dentro de un grupo de respuesta a incidentes cibernéticos tiene funciones cruciales que aseguran una respuesta efectiva y organizada. Algunas de estas funciones incluyen:

la Coordinación de Recursos: Gestiona y coordina los recursos necesarios (personal, tecnología, presupuesto) para responder adecuadamente a los incidentes.

Planificación y Preparación: Desarrolla y mantiene planes de respuesta a incidentes, asegurando que el equipo esté preparado para actuar rápidamente ante cualquier amenaza. Supervisión de Incidentes: Monitorea y supervisa el desarrollo de incidentes, asegurando que se sigan los procedimientos establecidos y se cumplan los plazos.

Comunicación Interna y Externa: Facilita la comunicación entre los diferentes equipos involucrados en la respuesta, así como con las partes interesadas externas, como la alta dirección y, si es necesario, las autoridades. Análisis de Impacto: Evalúa el impacto potencial de los incidentes en la organización, ayudando a priorizar la respuesta y la recuperación.

Documentación y Reportes: Mantiene registros detallados de los incidentes, la respuesta y las decisiones tomadas, lo que es esencial para análisis posteriores y cumplimiento normativo. Revisión y Mejora Continua: Después de cada incidente, lidera la revisión de la respuesta y las lecciones aprendidas, implementando mejoras en los procesos y procedimientos.

Capacitación y Concienciación: Organiza programas de capacitación para el personal sobre la gestión de incidentes y las mejores prácticas de seguridad cibernética. Colaboración con Otros Departamentos: Trabaja en conjunto con áreas como TI, legal, recursos humanos y comunicaciones para garantizar un enfoque integral en la gestión de incidentes.

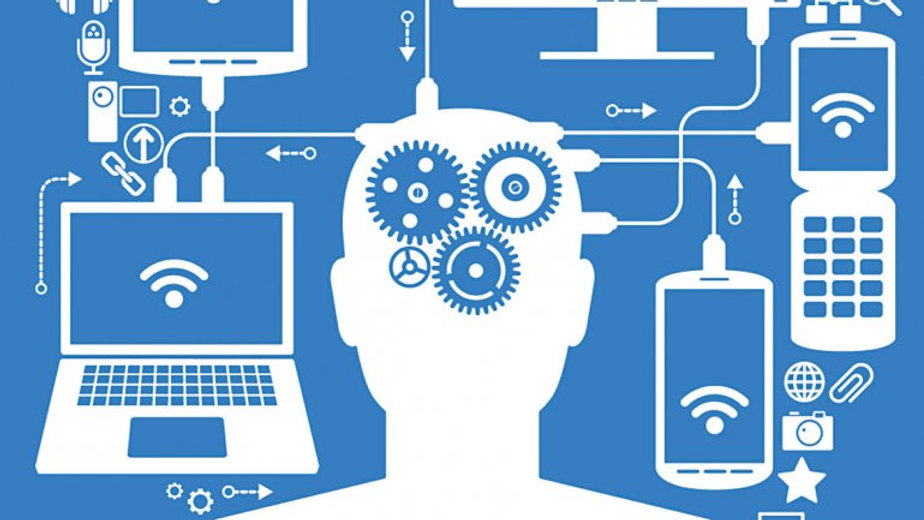
(<https://www.nist.gov/cyberframework>)

(<https://www.sans.org>)

(<https://www.gartner.com/en>)

* **Sistemas Internos (Internal Systems):** Componentes de la infraestructura que pueden ser afectados por un incidente.

Todos los productos y sistemas tecnológicos operados o controlados por una [organización] interna, computadoras, redes informáticas, sistemas telefónicos, sistemas de correo de voz, sistemas de intercomunicación, sistemas de buscapersonas y aplicaciones de software.



* **Sistemas Externos (External Systems):** Elementos fuera de la red interna que podrían estar involucrados en el incidente.

Un sistema o componente de un sistema que se utiliza, pero no forma parte de un sistema organizacional y sobre el cual la organización no tiene control directo en la implementación de los controles de seguridad y privacidad requeridos o en la evaluación de la efectividad del control.



* **Proceso General (Overall Process):** Incluye la identificación, aislamiento y análisis del incidente.

Es el proceso estructurado que utilizan los equipos de TI desde el inicio de una violación hasta garantizar las operaciones normales. Generalmente consta de cuatro etapas: identificar, analizar, mitigar y restaurar.

A person touching a touch screen

Description automatically generated

**Monitoreo de Seguridad de la Red (Network Security Monitoring)**

Se refiere al proceso de supervisión continua de una red para detectar actividades sospechosas que podrían indicar un incidente de seguridad.

**Pasos y Componentes:**

* **Honeypots:** es un sistema diseñado para atraer ataques, un señuelo. El objetivo es simular un objeto atractivo para los hackers y con ello monitorear o detectar posibles ataques para luego aprender de estos y evitarlos en un futuro. El o los honeypots serán los primeros en detectar los posibles ataques antes de infectar a otros en la red. (<https://www.incibe.es/empresas/blog/honeypot-una-trampa-para-los-ciberdelincuentes>)

A diagram of data flow

Description automatically generated

*Tipos de Honeypot*

Existen dos tipos diferentes de Honeypot y que se clasifican de la siguiente manera:

**Production Honeypot (Honeypot de producción)**: son los sistemas que utilizan las empresas para investigar por qué motivo reciben ciberataques de los ciberdelincuentes. La finalidad es averiguar por qué se han fijado en esa empresa, e intentar desviar o mitigar el riesgo de dichos ataques en su red interna.

**Research Honeypot (Investigación de Honeypot)**: estos sistemas son utilizados por organizaciones sin ánimos de lucro e instituciones educativas, donde el único objetivo que persiguen es investigar los motivos y las maneras que usan los ciberdelincuentes para atacar. La diferencia es que, este tipo de sistemas, se utilizan solamente para entender las motivaciones y, en cierta medida, la psicología del atacante.

(<https://www.riial.org/que-es-un-honeypot>)

* **Sistema de detección de intrusiones IDS**

Es una herramienta de seguridad de red que monitorea el tráfico de la red y los dispositivos para detectar actividades maliciosas conocidas, actividades sospechosas o infracciones a las políticas de seguridad.

El IDS puede ayudar a acelerar y automatizar la detección de amenazas en la red alertando a los administradores de seguridad.

(<https://www.ibm.com/mx-es/topics/intrusion-detection-system>)

* **Sistema de detección de intrusiones de Red:** los NIDS son un tipo de IDS que se instala directamente en la red, con el fin de analizar y filtrar el tráfico que recibe. De esta manera se detectan anomalías y comportamientos maliciosos, tal como son:
  1. Acceso a sitios web maliciosos.
  2. Ciberataques de hacking web.
  3. Ataques de intermediario (man in the middle)

(<https://keepcoding.io/blog/que-son-los-nids/>)

* **Sistema de detección de intrusiones de WIFI):** WIDS es una tecnología desarrollada para proteger y getionar las infraestructuras WIFI de ataques y accesos no autorizados.

WIDS ofrece protección a la red y los dispositivos móviles conectados, identificando:

* + 1. Vulnerabilidades
    2. Accesos no autorizados
    3. Niveles de trazabilidad

(<https://www.teknei.com/soluciones/wids/>)

* **Sistema de detección de intrusiones de Host:** HIDS son software que se instalan directamente en el equipo de cómputo del usuario conectado a la red. Escanean las actividades del equipo para ser procesados y enviados a una ubicación central.

Como los HIDS monitorean datos individuales, es buena idea combinar su uso con los NIDS, con el fin de obtener información general de la red.

(<https://keepcoding.io/blog/que-son-los-nids/>)

* **Malware detonation:** Es una herramienta de análisis de malware que implica abrir archivos y enlaces sospechosos en una máquina virtual (VM) para el control de actividades maliciosas y realizar acciones adicionales en un entorno controlado o modo seguro. La plataforma de detonación de ayuda a comprender la naturaleza del malware y sus actividades en caso de infección.

(<https://www.group-ib.com/resources/knowledge-hub/malware-detonation-platform/>)

* **Logs de Red (Network Logs):** Registros que contienen información sobre el tráfico de red, es decir pueden incluir información de las solicitudes entre el navegador web y el sitio que se está consultando o de una aplicación a la que se está intentando ingresar.

(<https://help.testim.io/docs/network-logs>)

* **Logs de Aplicaciones (Application Logs):** Los registros de aplicaciones (logs) son archivos o entradas que contienen información detallada sobre el comportamiento y las actividades de una aplicación o appliance. Estos son generados por sí mismos y pueden incluir información útil para los administradores y desarrolladores en el análisis de rendimiento, resolución de problemas y mejora de la seguridad.



Elasticsearch es un motor de búsqueda y analítica de RESTful distribuido, un almacén de datos escalable y una base de datos de vectores capaz de abordar un número creciente de casos de uso. Como núcleo del Elastic Stack, almacena de forma central tus datos para una búsqueda a la velocidad de la luz, relevancia refinada y analíticas poderosas que escalan con facilidad.

**Elastic Stack (ELK Stack)**

1. Elasticsearch: Es un motor de búsqueda y análisis de texto completo que indexa y permite buscar grandes volúmenes de datos rápidamente.
2. Logstash: Un pipeline de procesamiento de datos que recoge, transforma y envía logs desde diversas fuentes a Elasticsearch.
3. Kibana: Una interfaz de visualización y análisis para consultar los datos almacenados en Elasticsearch.

Elastic Stack se utiliza no solo para almacenar registros de aplicaciones, sino también para generar insights visuales a partir de los logs, ayudando a los equipos de TI a monitorear sistemas y detectar problemas en tiempo real.

Tipos de Información Contenida en los registros:

1. Eventos de la aplicación: Incluyen eventos importantes en el ciclo de vida de una aplicación, como el inicio, la finalización, errores, advertencias o excepciones manejadas.

2. Mensajes de error: Descripciones de los errores que se producen, a menudo con detalles sobre la ubicación y la causa del error.

3. Advertencias: Indican problemas potenciales que no han causado un fallo, pero que podrían hacerlo si no se corrigen.

4. Mensajes informativos: Información sobre el funcionamiento normal de la aplicación, como actualizaciones de estado o la ejecución de ciertas funciones.

5. Acceso a servicios o recursos: Logs que muestran cuándo una aplicación accede a un recurso o servicio, como bases de datos, API externas, servidores web, etc.

6. Actividad del usuario: Detalles sobre las acciones realizadas por los usuarios dentro de la aplicación (inicio de sesión, transacciones, cambios de configuración).

7. Tiempos de respuesta y rendimiento: Datos sobre el rendimiento de la aplicación, como tiempos de respuesta a solicitudes o carga del servidor.

8. Detalles de configuración: Información sobre cómo se configuró la aplicación en un momento específico, lo cual es útil para rastrear problemas relacionados con cambios en la configuración. <https://www.elastic.co/es/elasticsearch>

**PCAP Completo (Full PCAP):** El pcap es una interfaz de una aplicación de programación para captura de paquetes. La implementación del pcap para sistemas basados en Unix se conoce como libpcap; el port para Windows del libpcap recibe el nombre de WinPcap.

El libpcap y WinPcap pueden ser utilizados por un programa para capturar los paquetes que viajan por toda la red y, en las versiones más recientes, para transmitir los paquetes en la capa de enlace de una red, así como para conseguir una lista de las interfaces de red que se pueden utilizar con el libpcap o WinPcap.

El libpcap y WinPcap son la captura del paquete y los motores de filtración de muchas herramientas de código abierto y comerciales de la red, incluyendo analizadores de protocolo, monitores de la red, sistemas de detección de intrusos en la red, programas de captura de las tramas de red (packet sniffers), generadores de tráfico y puesta a punto de la red. (<https://es.wikipedia.org/wiki/Pcap_(interfaz)>

A black shark fin on a blue background

Description automatically generated

A screenshot of a computer

Description automatically generated

* **Evaluación Histórica (Historical Assessment):** Evaluación de logs históricos para detectar patrones y anomalías.

A pink logo with white text

Description automatically generated

Análisis de patrones:

CloudWatch Logs Insights utiliza algoritmos de aprendizaje automático para encontrar patrones cuando consultas tus registros. Un patrón es una estructura de texto compartida que se repite en los campos de registro. Al ver los resultados de una consulta, puede seleccionar la pestaña Patrones para ver los patrones que los CloudWatch registros encontraron a partir de una muestra de sus resultados. Como alternativa, puede añadir el pattern comando a la consulta para analizar los patrones de todo el conjunto de eventos de registro coincidentes.

Los patrones son útiles para analizar conjuntos de registros grandes porque, a menudo, una gran cantidad de eventos de registro se pueden comprimir en unos pocos patrones.

Considere el siguiente ejemplo de tres eventos de registro.

2023-01-01 19:00:01 [INFO] Calling DynamoDB to store for resource id 12342342k124-12345

2023-01-01 19:00:02 [INFO] Calling DynamoDB to store for resource id 324892398123-12345

2023-01-01 19:00:03 [INFO] Calling DynamoDB to store for resource id 3ff231242342-12345

En el ejemplo anterior, los tres eventos de registro siguen un patrón:

<\*> <\*> [INFO] Calling DynamoDB to store for resource id <\*>

Los campos dentro de un patrón se denominan fichas. Los campos que varían dentro de un patrón, como un identificador de solicitud o una marca de tiempo, son símbolos dinámicos. Cada token dinámico se representa <\*> cuando CloudWatch Logs lo muestra.

Algunos ejemplos comunes de tokens dinámicos son los códigos de error, las marcas de tiempo y las solicitudes. IDs El valor de un token representa un valor concreto de un token dinámico. Por ejemplo, si un token dinámico representa un código de HTTP error, el valor del token podría serlo501.

La detección de patrones también se utiliza en el detector de anomalías de CloudWatch Logs y en las funciones de comparación. (<https://docs.aws.amazon.com/es_es/AmazonCloudWatch/latest/logs/CWL_AnalyzeLogData_Patterns.html>)

* **SIEM (Security Information and Event Management):** Sistema que recopila y analiza logs de diferentes fuentes para identificar y responder a incidentes de seguridad.

La gestión de eventos e información de seguridad, o SIEM, es una solución de seguridad que ayuda a las organizaciones a reconocer y abordar posibles amenazas y vulnerabilidades de seguridad antes de tener la oportunidad de interrumpir las operaciones comerciales. Los sistemas SIEM ayudan a los equipos de seguridad empresarial a detectar anomalías de comportamiento de los usuarios y utilizan [inteligencia artificial (IA)](https://www.ibm.com/mx-es/topics/artificial-intelligence) para automatizar muchos de los procesos manuales asociados con la detección de amenazas y la [respuesta ante incidentes](https://www.ibm.com/mx-es/topics/incident-response).

SIEM captura datos de eventos de una amplia gama de fuentes en toda la red de una organización. Los registros y datos de flujo de usuarios, aplicaciones, activos, entornos de nube y redes se recopilan, almacenan y analizan en tiempo real, lo que brinda a los equipos de TI y seguridad la capacidad de **administrar automáticamente el registro de eventos y los datos de flujo de red** de su red en una ubicación centralizada.

<https://www.ibm.com/mx-es/topics/siem>

**Inteligencia de Amenazas (Threat Intelligence)**

**Definición:** La inteligencia de amenazas es el proceso de recopilación y análisis de información clave sobre amenazas cibernéticas, con el objetivo de mejorar la capacidad de una organización para identificar, prevenir y responder a incidentes de seguridad. Este enfoque permite a las empresas anticiparse a ataques dirigidos, reducir su superficie de ataque y tomar decisiones basadas en datos de ciberinteligencia. El objetivo final es proporcionar una visión más amplia del panorama de amenazas y facilitar respuestas rápidas y eficaces.

**Pasos y Componentes:**

* **Recursos de Código Abierto (Open-Source Resources):** Fuentes de información disponibles públicamente sobre amenazas.ENRIQUE
* **Fuentes de Información Interna (Internal Information Sources):** Información dentro de la organización que puede proporcionar contexto adicional sobre amenazas.ENRIQUE
* **Caza de Amenazas Interna (Internal Adversary Hunt):** Es un proceso en el que un equipo especializado busca proactivamente amenazas dentro de la red de una organización, antes de que se conviertan en incidentes graves. Esta caza utiliza análisis avanzados y herramientas forenses para identificar comportamientos inusuales o indicios de intrusiones. Al realizar búsquedas constantes, las organizaciones pueden detectar y mitigar ataques persistentes avanzados (APT) antes de que causen daño significativo. (<https://www.crowdstrike.com/epp-101/threat-hunting/>)

**Ejemplo**: CrowdStrike Falcon  
CrowdStrike Falcon es una plataforma líder de caza de amenazas. Utiliza análisis de comportamiento y análisis forense para identificar actividades maliciosas dentro de una red. A través de la detección proactiva de amenazas persistentes avanzadas (APT), los equipos de seguridad pueden localizar intrusiones antes de que causen daño. Esta herramienta es muy utilizada para la búsqueda activa de amenazas que ya han evadido las defensas iniciales.  
URL: <https://www.crowdstrike.com/endpoint-security-products/falcon-threat-hunting/>



* **Atributos de Información (Attribution Info):** La atribución en ciberseguridad implica identificar las características clave, tácticas, técnicas y procedimientos (TTPs) de los atacantes. Esto incluye la identificación de grupos de amenazas, su motivación y localización geográfica. Atribuir adecuadamente los ataques permite a las organizaciones responder de manera más efectiva y coordinar esfuerzos con otras entidades globales para mitigar ataques cibernéticos masivos. (<https://www.fireeye.com/current-threats/what-is-threat-intelligence.html>)

**Ejemplo**: Mandiant Threat Intelligence  
Mandiant, una subsidiaria de FireEye, ofrece una de las mejores soluciones de atribución de amenazas. Su equipo de inteligencia proporciona informes detallados sobre actores de amenazas, incluidas sus tácticas, técnicas y procedimientos (TTPs). Esto ayuda a las organizaciones a identificar quién está detrás de los ataques y sus motivaciones. Además, la plataforma permite obtener datos sobre el comportamiento de los atacantes en tiempo real.  
URL: <https://www.mandiant.com/resources/mandiant-advantage-threat-intelligence>



* **Recopilación de Información:** Recoger información sobre los atacantes y correlacionar eventos de seguridad es una de las tareas principales en la inteligencia de amenazas. Se utiliza para identificar patrones de ataque y potenciales vulnerabilidades dentro del entorno de la organización. Al combinar fuentes de datos internas y externas, las organizaciones pueden fortalecer su postura de seguridad, desarrollando medidas proactivas que se adapten a las últimas tendencias en amenazas cibernéticas. (<https://www.trendmicro.com/en_us/security-intelligence/threat-intelligence-101.html>)

**Ejemplo**: Recorded Future  
Recorded Future es una herramienta de inteligencia de amenazas que recopila grandes volúmenes de datos de diversas fuentes, incluidos foros clandestinos, redes sociales, y otras fuentes de amenazas. La plataforma utiliza inteligencia artificial para analizar y correlacionar eventos en tiempo real, ayudando a las organizaciones a descubrir patrones y posibles ataques antes de que ocurran. Es ideal para identificar nuevas amenazas y correlacionar eventos en grandes redes.  
URL: <https://www.recordedfuture.com/threat-intelligence>

