**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):** Interactúan con el SOC para reportar incidentes y coordinar acciones. ANDRES
* **Comité de Dirección (Steering Committee):** Proporciona orientación y apoyo en la toma de decisiones críticas durante un incidente. ANDRES
* **Gestión (Management):** Asegura que los incidentes sean manejados de acuerdo con las políticas de la organización y proporciona los recursos necesarios. ANDRES
* **Sistemas Internos (Internal Systems):** Componentes de la infraestructura que pueden ser afectados por un incidente. OSCAR
* **Sistemas Externos (External Systems):** Elementos fuera de la red interna que podrían estar involucrados en el incidente.OSCAR
* **Proceso General (Overall Process):** Incluye la identificación, aislamiento y análisis del incidente.OSCAR

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

**Definición:** 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:** Sistemas diseñados para atraer ataques y recopilar datos sobre actividades maliciosas. RAUL
* **Dispositivos Internos (Internal Devices):** Componentes de hardware dentro de la red que se monitorean.RAUL
* **Dispositivos Externos (External Devices):** Elementos fuera de la red interna que también se monitorean.RAUL
* **Logs de Red (Network Logs):** Registros que contienen información sobre el tráfico de red.RAUL
* **Logs de Aplicaciones (Application Logs):** Registros que contienen información sobre el comportamiento de las aplicaciones. PEDRO
* **PCAP Completo (Full PCAP):** Captura completa de paquetes para un análisis detallado.PEDRO
* **Evaluación Histórica (Historical Assessment):** Evaluación de logs históricos para detectar patrones y anomalías. PEDRO
* **SIEM (Security Information and Event Management):** Sistema que recopila y analiza logs de diferentes fuentes para identificar y responder a incidentes de seguridad. ENRIQUE

**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>

