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

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

**Inteligencia de Amenazas (Threat Intelligence)**

**Definición:** Proceso de recolección y análisis de información sobre amenazas potenciales para mejorar la capacidad de una organización para prevenir y responder a incidentes de seguridad.

**Pasos y Componentes:**

* **Recursos de Código Abierto (Open-Source Resources):** Fuentes de información disponibles públicamente sobre amenazas.
* **Fuentes de Información Interna (Internal Information Sources):** Información dentro de la organización que puede proporcionar contexto adicional sobre amenazas.
* **Caza de Amenazas Interna (Internal Adversary Hunt):** Proceso de búsqueda proactiva de amenazas dentro de la red.
* **Atributos de Información (Attribution Info):** Información sobre las características y tácticas de los atacantes.
* **Recopilación de Información:** Recoger información sobre características de los atacantes y correlación de eventos para identificar amenazas.