Criterios de Evaluación

Unidad 2: Auditoría de Incidentes

- CA2.1 Clasificación y taxonomía de incidentes
- CA2.2 Monitorización, detección y alertas
- CA2.3 Incidentes de seguridad física
- CA2.4 Investigación en fuentes abiertas (OSINT)
- CA2.5 Documentación y seguimiento inicial

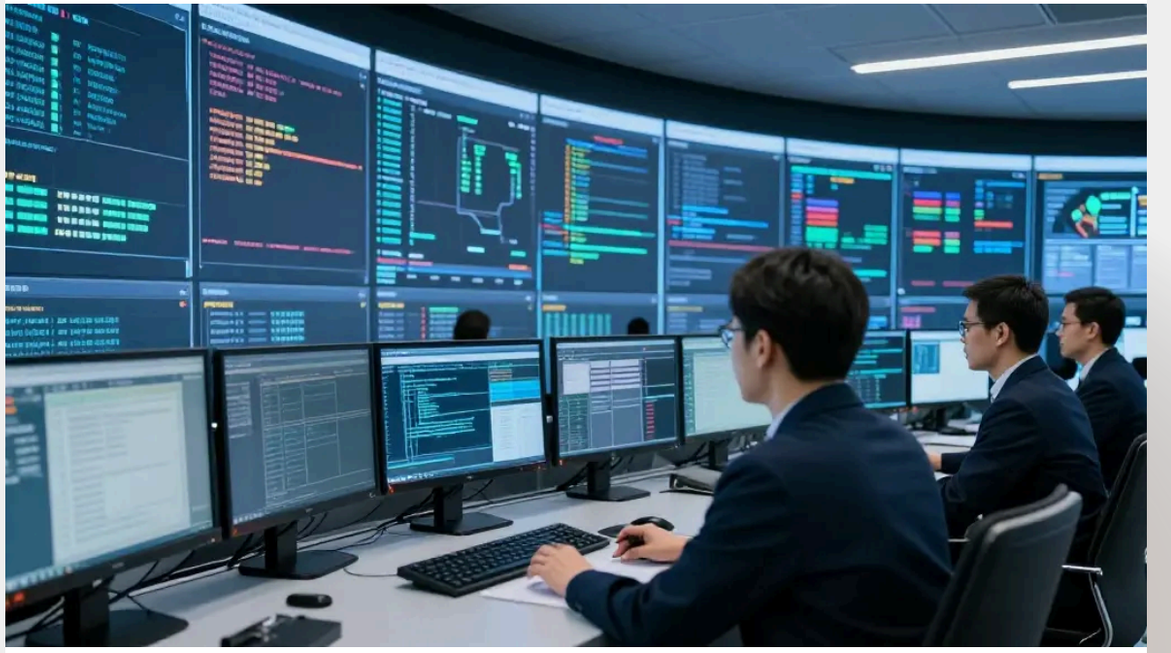
Unidad 2. Auditoría de incidentes ciberseguridad

Sección	Contenido Principal
2.1 Taxonomía	Clasificación y definición de incidentes
2.2 Monitorización	Identificación y alerta → SIEM + IDS
2.3 Seguridad Física	Controles y mecanismos de detección física
2.4 OSINT	Investigación en fuentes abiertas para alertas

Ciclo de Vida de Respuesta a Incidentes

Proceso continuo y estructurado para fortalecer la postura de seguridad.

- **Preparación:** Equipos, herramientas y procedimientos.
- **Detección y Análisis:** Identificar la naturaleza del evento.
- **Contención y Recuperación:** Minimizar impacto y restaurar.
- **Lecciones Aprendidas:** Mejora continua post-incidente.



Recopilación de Información

Footprinting + Proceso OSINT

Footprinting Activo

Carácter interno: escaneos de red y comandos como traceroute/tracert.

Footprinting Pasivo

Uso de motores de búsqueda y redes sociales sin interacción directa.

¿Qué es OSINT?

- **Open Source Intelligence:** Recopilación y análisis de información pública.
- **Legalidad:** Trabaja exclusivamente con datos accesibles sin vulnerar sistemas.
- **Fuentes:** Redes sociales, registros públicos, foros y dispositivos en Shodan.
- **Objetivo:** Ver lo que el enemigo ve para anticiparse a sus movimientos.

Utilidad de OSINT

En Defensa

Descubrir la propia huella digital: contraseñas filtradas o documentos expuestos.

En Investigación

Contextualizar alertas relacionando IPs maliciosas con campañas de malware.

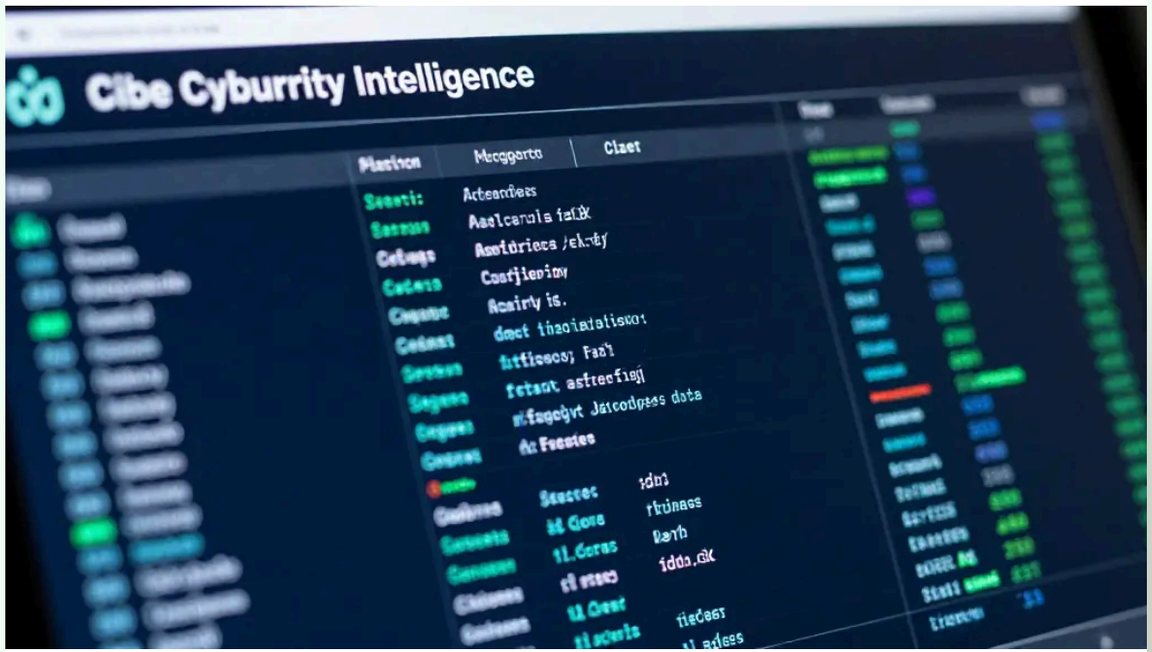
Herramientas

Maltego para relaciones, SpiderFoot para automatización y Google Dorks.

OSINT en Identificación

Enriquece las alertas del SIEM convirtiendo datos brutos en inteligencia.

- **Validación:** Verifica si una IP es un nodo Tor o amenaza real.
- **Eficiencia:** Descarta falsos positivos rápidamente.
- **Fuentes:** Consulta VirusTotal, Shodan o listas de reputación.



Contención y Erradicación

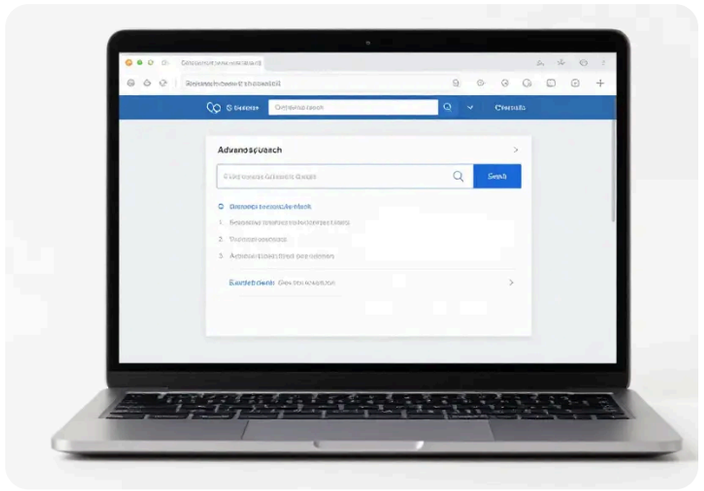
Actúa como un radar para mapear el ecosistema del adversario.

- **Tirar del hilo:** Busca relaciones mediante historiales DNS y WHOIS.
- **Infraestructura:** Localiza servidores C2 y certificados compartidos.
- **Bloqueo Total:** Asegura que el atacante no pueda reagruparse.

OSINT en Lecciones Aprendidas

Investigación	Hallazgo OSINT	Conclusión del Vector
Credenciales	Expuestas en foros/brechas previas	Credential Stuffing
Documentos	Filtrados en repositorios públicos	Fuga de información previa
Sin rastro	No hay exposición pública previa	Phishing o Exploit directo

Herramientas OSINT

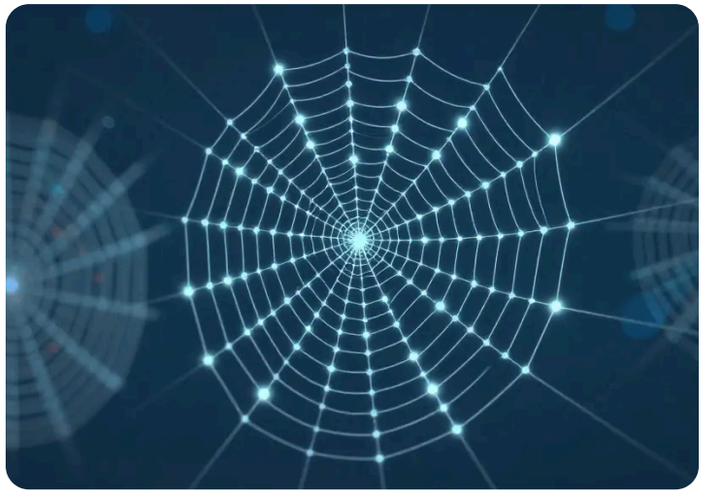


Buscadores

Google Dorks y buscadores de imágenes especializados.

Shodan

El buscador de dispositivos conectados a Internet.



SpiderFoot

Automatización de la recopilación de inteligencia.