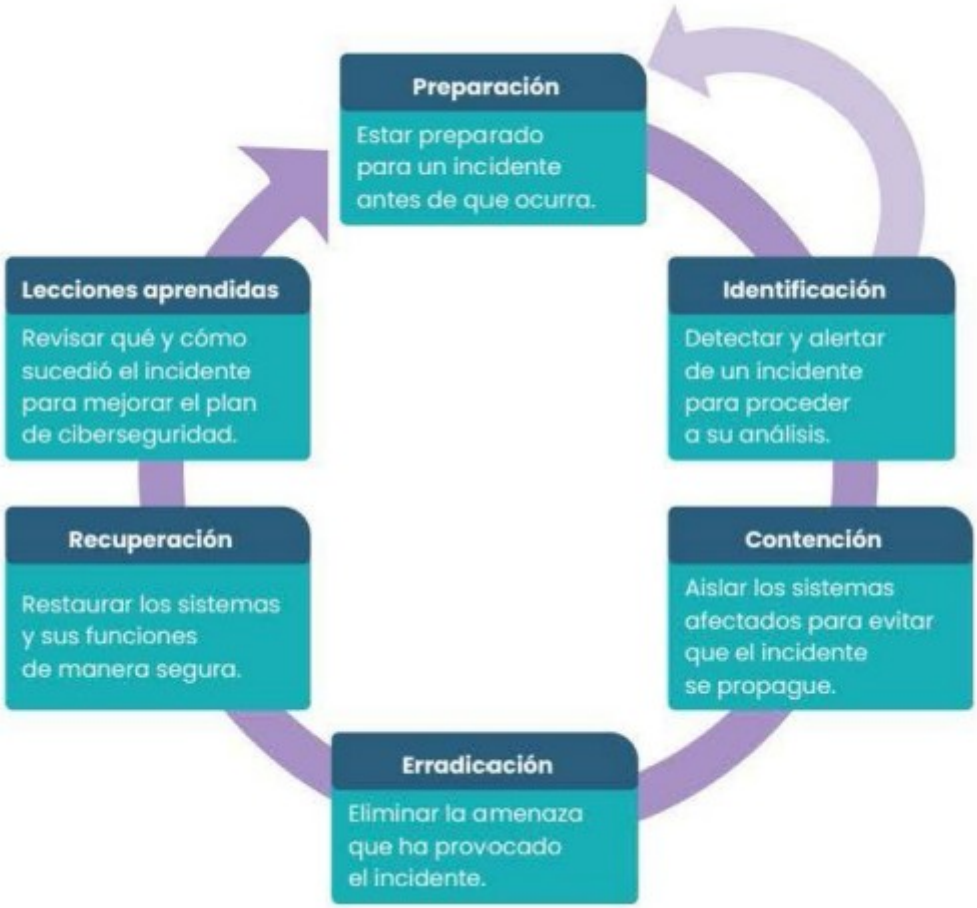
Preparación
Estar preparado para un incidente antes de que ocurra.
Identificación
Detectar y alertar de un incidente para proceder a su análisis.
Contención
Aislar los sistemas afectados para evitar que el incidente se propague.
Erradicación
Eliminar la amenaza que ha provocado el incidente.
Recuperación
Restaurar los sistemas y sus funciones de manera segura.
Lecciones aprendidas
Revisar qué y cómo sucedió el incidente para mejorar el plan de ciberseguridad.

En el ciclo de vida de respuesta a incidentes, OSINT actúa como el proveedor de inteligencia contextual en varias fases:

Identificación: Enriquece las alertas del SIEM. Una IP sospechosa en un log se convierte en una amenaza conocida al verificarla en Shodan o en bases OSINT, validando si es un falso positivo o un ataque real.

Contención/Erradicación: Ayuda a localizar toda la infraestructura del atacante (dominios, servidores C2) mediante búsquedas relacionadas.

Lecciones aprendidas: Investiga si la información filtrada (credenciales, documentos) ya estaba expuesta públicamente antes del incidente, identificando el vector de entrada inicial.

EJEMPLOS EXPLICADOS

El SIEM genera una alerta porque detecta una IP sospechosa, pero solo es un dato bruto. Ahí entra OSINT para darle contexto y convertirlo en inteligencia. Tomas esa IP y la consultas en bases de datos OSINT como Shodan, VirusTotal o listas de reputación. Si OSINT revela que la IP es un nodo de Tor, está reportada en múltiples listas negras o aloja malware, confirmas que es una amenaza real y debes actuar. Si, por el contrario, OSINT muestra que pertenece a un proveedor de confianza o no tiene historial malicioso, puedes descartarla como un falso positivo, ahorrando tiempo al equipo.

En la fase de Contención y Erradicación, el objetivo es expulsar al atacante y asegurarse de que no pueda volver a entrar. OSINT actúa como un radar que mapea todo el ecosistema del adversario para no dejar cabos sueltos. Cuando encuentras un servidor de Comando y Control (C2) o un dominio malicioso en tus logs, OSINT permite "tirar del hilo". Los analistas utilizan técnicas de inteligencia para buscar relaciones: consultan historiales de DNS para ver a qué otras IPs ha estado vinculado ese dominio, buscan certificados SSL compartidos que revelen más servidores del atacante, o rastrean huellas digitales como el registro WHOIS. Si el atacante reutilizó la misma infraestructura en otros ataques, OSINT los descubre. También permite encontrar dominios similares recién registrados que podrían usar para reagruparse. Con esta información, puedes bloquear no solo lo que ya viste, sino todo su entramado, asegurando una erradicación completa y evitando que el incidente se repita minutos después con un nuevo dominio.

OSINT en Lecciones Aprendidas: Investigación del vector de entrada
Tras un incidente de seguridad, la fase de lecciones aprendidas busca entender cómo ocurrió la intrusión. Aquí, OSINT juega un papel clave para determinar el vector de entrada inicial. ¿Qué se investiga? Se analiza si la información comprometida durante el incidente (como credenciales o documentos internos) ya estaba expuesta públicamente con anterioridad. Para ello, se consultan filtraciones históricas, foros oscuros, repositorios públicos y brechas de datos conocidas. ¿Por qué es importante? Si las credenciales afectadas ya circulaban en Internet antes del incidente, el vector de entrada probablemente fue un ataque de relleno de credenciales (credential stuffing). El atacante simplemente utilizó credenciales que otro había filtrado previamente. Si no hay rastros de exposición previa, el vector de entrada fue otro: campañas de phishing, explotación de vulnerabilidades, o ataques de fuerza bruta. En conclusión, esta técnica permite conectar filtraciones pasadas con incidentes presentes, identificando con precisión cómo el atacante obtuvo su acceso inicial.