



SOC: GUÍA PRÁCTICA

Como iniciar en Security Operations Center

Autor: Zahira Marano Leguiza

Contenido

Introducción.....	2
¿Qué es un SOC y por qué es importante?	2
Definiciones Importantes	2
Roadmap de Crecimiento en el SOC	3
Nivel 1 - Analista SOC Junior	3
Nivel 2 - Analista SOC Intermedio	4
Nivel 3 - Analista Avanzado / Threat Hunter (<i>a futuro</i>)	5
Glosario Básico SOC	5
Tips para Aprender Mejor	5

INTRODUCCIÓN

¿Qué es un SOC y por qué es importante?

Un **SOC (Security Operations Center)** es el corazón de la defensa cibernética de una organización. Es un equipo especializado que se encarga de:

- ✓ **Monitorear continuamente** los sistemas de la empresa.
- ✓ **Detectar** amenazas de seguridad en tiempo real.
- ✓ **Responder** de forma rápida y eficiente ante incidentes.
- ✓ **Prevenir y minimizar daños** causados por ciberataques.

Dentro del SOC hay diferentes niveles de analistas (L1, L2, L3), cada uno con responsabilidades crecientes. A medida que ganas experiencia, vas pasando de tareas de monitoreo y clasificación, a análisis más complejos e incluso cacería de amenazas.

Objetivo del SOC: proteger la confidencialidad, integridad y disponibilidad de la información de la empresa.

Definiciones Importantes

Ciberseguridad: Conjunto de medidas y prácticas diseñadas para proteger sistemas informáticos, redes y datos contra ataques, daños o accesos no autorizados.

Incidente de seguridad: Evento que compromete o tiene el potencial de comprometer la confidencialidad, integridad o disponibilidad de la información o los sistemas.

Alerta: Notificación generada por un sistema de seguridad indicando una posible amenaza o evento anómalo.

Eventos: Registros de actividades generadas por los sistemas, como inicios de sesión, accesos, errores, etc.

Logs: Archivos que almacenan eventos generados por sistemas y aplicaciones, fundamentales para el análisis forense.

Firewall: Dispositivo o software que controla el tráfico de red entrante y saliente según políticas de seguridad.

Antivirus: Software diseñado para detectar y eliminar software malicioso (malware).

Phishing: Técnica de engaño que busca obtener información confidencial (como contraseñas o tarjetas) haciéndose pasar por una entidad confiable.

APT (Amenaza Persistente Avanzada): Ataque dirigido y prolongado llevado a cabo por actores sofisticados con fines específicos.

Roadmap de Crecimiento en el SOC

Fase	Enfoque principal	Objetivo	Nivel
Fase 1	Aprendizaje y observación	Conocer el entorno SOC, herramientas y tipos de alertas	SOC L1
Fase 2	Ejecución supervisada	Clasificar, documentar y escalar eventos correctamente	SOC L1
Fase 3	Investigación inicial	Correlacionar eventos y responder alertas simples	SOC L2
Fase 4	Contención y mejora	Responder incidentes y optimizar procesos	SOC L2
Fase 5	Caza y análisis avanzado	Buscar amenazas y crear defensas personalizadas	SOC L3

Nivel 1 - Analista SOC Junior

Objetivo: Detectar y reportar eventos sospechosos. Aprender a clasificar, documentar y escalar.

Tareas principales:

- ✓ Monitorear alertas de seguridad desde el SIEM.
- ✓ Clasificar alertas (falso positivo / verdadero positivo).
- ✓ Documentar alertas y eventos con claridad.
- ✓ Escalar incidentes según criticidad.

- ✓ Ejecutar pasos definidos en playbooks simples (procedimientos).
- ✓ Verificar el estado de las herramientas de seguridad (antivirus, EDR, firewall).
- ✓ Soporte básico a usuarios ante casos como correos sospechosos o bloqueos de acceso.

Herramientas que usarás: SIEM, EDR, consola de antivirus, analizador de correos, VirusTotal.

Ejemplos de alertas comunes:

Correo con archivo adjunto malicioso detectado por el antivirus.

Usuario que recibe un enlace sospechoso por correo electrónico.

Conexión entrante desde IP externa no autorizada.

Usuario que intenta múltiples accesos fallidos.

Cómo documentarlas:

- ✓ Título: tipo de alerta.
- ✓ Fuente: qué sistema la generó.
- ✓ Usuario afectado / IP.
- ✓ Acciones realizadas (clasificación, escalamiento, bloqueo, etc).
- ✓ Resultado (contenida, escalada, pendiente).

Nivel 2 - Analista SOC Intermedio

Objetivo: Investigar incidentes y comenzar a tomar decisiones iniciales de contención.

Tareas principales:

- ✓ Investigar alertas escaladas por el Nivel 1.
- ✓ Correlacionar eventos de distintos sistemas (correo, red, firewall, etc).
- ✓ Realizar análisis básico de malware (usando hashes, sandbox, etc).
- ✓ Redactar informes de incidentes.
- ✓ Ejecutar acciones de contención como aislar equipos o bloquear IPs.
- ✓ Proponer mejoras a procedimientos existentes.

Herramientas que usarás: Sandbox, herramientas de red, VirusTotal, MITRE ATT&CK.

Ejemplos de casos:

Malware detectado en estación de trabajo con múltiples conexiones a dominios sospechosos.

IP externa identificada en listas negras que interactúa con sistemas internos.

Análisis de archivos usando SHA256 y comparación en VirusTotal / Any.Run.

Nivel 3 - Analista Avanzado / Threat Hunter (a futuro)

Objetivo: Buscar amenazas de forma proactiva y realizar análisis avanzados.

Tareas principales:

- ✓ Realizar búsqueda activa de amenazas (Threat Hunting).
- ✓ Analizar cadenas de ataque completas (kill chain).
- ✓ Crear reglas personalizadas para el SIEM.
- ✓ Detectar campañas dirigidas (APT).
- ✓ Apoyar en análisis forense digital.

Ejemplos de hunting:

Buscar conexiones persistentes a dominios raros o sin reputación.

Detectar actividad fuera del horario laboral con patrones sospechosos.

Investigar credenciales utilizadas desde múltiples ubicaciones geográficas en poco tiempo.

Glosario Básico SOC

SIEM: Sistema que centraliza y correlaciona logs de distintos dispositivos para detectar amenazas.

EDR: Endpoint Detection and Response, permite monitorear y responder en endpoints.

IOC: Indicador de compromiso (IP maliciosa, hash de malware, dominio sospechoso).

Falso Positivo: Alerta que parece maliciosa pero no lo es.

True Positive: Alerta que indica una amenaza real.

Playbook: Procedimiento paso a paso para responder a un tipo de alerta.

Hash: Identificador único de un archivo, útil para detectar malware.

Sandbox: Entorno seguro donde se ejecuta un archivo sospechoso para ver su comportamiento.

Threat Hunting: Proceso proactivo para detectar amenazas que no han sido alertadas por herramientas.


Tips para Aprender Mejor

- No tengas miedo de preguntar. Nadie nació sabiendo.

- Documentá todo lo que hagas, incluso lo que no entiendas.
- Hacé tus propios apuntes, screenshots y guías.
- Leé sobre casos reales y practicá con ejemplos.
- Aprendé a pensar como un atacante: eso te hará una gran defensora.

Cierre

Este documento no solo es una guía de entrenamiento, sino también una puerta de entrada a una carrera llena de desafíos y aprendizaje constante. Ser parte de un SOC significa estar en la primera línea de defensa de la ciberseguridad, y cada alerta que analizás, cada incidente que contenés, te convierte en una pieza clave en la protección de toda la organización.

- ✓  *"Cada alerta es una historia esperando ser entendida. Cada incidente, una oportunidad para aprender y mejorar."*