EC-COUNCIL



EC-COUNCIL · PROGRAMA DE OPERACIONES DE SEGURIDAD

Certified SOC Analyst (C|SA) v2

Domine las habilidades del SOC con experiencia práctica e inteligencia artificial, del analista L1 al L3

¿Por qué debería asistir?

El programa Certified SOC Analyst (C|SA) es el punto de partida para quienes aspiran a integrarse o avanzar en un Centro de Operaciones de Seguridad (SOC). Brinda formación en los principios y prácticas de las operaciones de seguridad, la inteligencia de amenazas y la respuesta a incidentes: vectores de ataque comunes, herramientas, SIEM, gestión centralizada de logs (CLM), triaje de incidentes, indicadores de compromiso (IoC) y la cyber kill chain.

La versión 2 eleva la cobertura hasta el nivel de analista L3 e incorpora la detección activa y proactiva de amenazas, la detección en la nube, la investigación forense y el uso de IA en el SOC con herramientas como Splunk AI, Elastic AI, Copilot, ChatGPT y PowerShell AI para crear reglas, priorizar alertas y automatizar la cacería de amenazas.

3 días	8	50+	120+	L1 – L3
DURACIÓN	MÓDULOS	LABORATORIOS	HERRAMIENTAS	NIVEL SOC

SIEM SECURITY INFORMATION AND EVENT MANAGEMENT

¿Quién debería participar?

Analistas SOC L1
Analistas SOC junior y profesionales que se inician en el monitoreo, el triaje de alertas y el escalamiento de incidentes.

Analistas SOC L2 y L3
Analistas SOC y de amenazas que investigan incidentes, desarrollan casos de uso y realizan cacería de amenazas.

Respuesta a incidentes
Analistas de respuesta a incidentes y de seguridad de la información que colaboran con el SOC.

Redes y TI
Administradores de red y de seguridad que desean dar el paso a las operaciones de seguridad.

Objetivos de aprendizaje

- Conocer a fondo los procesos, procedimientos, tecnologías y flujos de trabajo del SOC
- Comprender amenazas, ataques, vulnerabilidades, el comportamiento del atacante y la cyber kill chain, e identificar sus IoC
- Monitorear y analizar logs y alertas de IDS/IPS, protección de endpoints, servidores y estaciones de trabajo
- Administrar soluciones SIEM como Splunk, AlienVault OSSIM y ELK Stack, y desarrollar casos de uso y reglas de correlación
- Realizar el triaje de alertas, escalar incidentes y documentarlos con sistemas de tickets y reportes
- Integrar inteligencia de amenazas en el SIEM y participar en ejercicios de cacería de amenazas
- Apoyar la respuesta a incidentes con técnicas forenses y de análisis de malware, incluida la detección en la nube
- Aprovechar la IA y el aprendizaje automático para mejorar la detección y la respuesta en el SOC

Novedades de C|SA v2

Detección activa de amenazas | Detección proactiva | Detección en la nube | IA y ML en el SOC | SOC habilitado con IA | Investigación forense | Cobertura hasta L3

Programa del curso

Duración: 3 días

Módulo	Contenido
Módulos 1–3 Día 1	01 **Operaciones y gestión de la seguridad:** cómo un SOC fortalece la gestión de la seguridad y la postura de la organización, y el papel de las personas, la tecnología y los procesos en su operación. 02 **Amenazas cibernéticas, IoC y metodología de ataque:** tipos de ciberataques, sus indicadores de compromiso y las tácticas, técnicas y procedimientos (TTP) de los atacantes. 03 **Gestión de logs:** cómo se generan, almacenan, recolectan de forma centralizada, normalizan y correlacionan los logs en el SIEM.
Módulos 4–6 Día 2	04 **Detección y triaje de incidentes:** fundamentos del SIEM, capacidades y estrategias de despliegue, desarrollo de casos de uso, detección de anomalías, triaje de alertas y reporte de incidentes. 05 **Detección proactiva de amenazas:** inteligencia de amenazas y threat hunting, y su integración con el SIEM para reducir falsos positivos y acelerar el triaje. 06 **Respuesta a incidentes:** etapas de la respuesta a incidentes y colaboración del equipo de respuesta (IRT) con el SOC ante incidentes escalados.
Módulos 7–8 Día 3	07 **Investigación forense y análisis de malware:** su importancia en las operaciones del SOC para entender los métodos de ataque, identificar IoC y fortalecer las defensas futuras. 08 **SOC para entornos en la nube:** monitoreo, detección de incidentes, respuesta automatizada y seguridad en AWS, Azure y GCP con herramientas nativas de la nube.

Novedades de la versión 2

- Contenido que llega hasta el nivel L3; antes cubría niveles más básicos de analista.
- Mayor foco en detección activa y en enfoques de detección proactiva.
- Detección de amenazas en la nube.
- Uso de IA y aprendizaje automático en el SOC.
- Investigación forense dentro del SOC.

Uso de la IA

- Generar reglas de SIEM con lenguaje natural.
- Clasificar y priorizar alertas de forma automática.
- Crear scripts de PowerShell para cacería de amenazas con Copilot, ChatGPT y el módulo de IA de PowerShell.
- Análisis de comportamiento con herramientas de IA.
- Integrar Splunk AI y Elasticsearch AI con el SIEM.



Examen

Duración: 3 horas

Título	EC-Council Certified SOC Analyst (C|SA) – Versión 2		
Código	312-39	**N.º de preguntas**	100
Formato	Opción múltiple	**Duración**	3 horas
Aprobación	70 %	**Plataforma**	EC-Council Exam Portal

Requisitos de elegibilidad

- **Con capacitación oficial de EC-Council:** puede presentar el examen sin proceso de elegibilidad.
- **Sin capacitación oficial:** al menos dos años de experiencia en administración o seguridad de redes, solicitud de elegibilidad aprobada y una cuota de US$100.

IA aplicada al SOC

Aprenderá cómo la IA transforma el SOC tradicional y potencia el SIEM: generar reglas de detección con lenguaje natural, priorizar y categorizar alertas, crear scripts de PowerShell para cacería de amenazas con **Copilot**, **ChatGPT** y **PowerShell AI**, e integrar **Splunk AI** y **Elasticsearch AI** con el SIEM.

Información general

- Más de 50 laboratorios y 120 herramientas, con más del 50 % del tiempo de formación dedicado a prácticas
- 350 casos de uso para ArcSight, QRadar, LogRhythm y Splunk, y 65 casos de uso aplicables a cualquier SIEM
- Mapeado al marco NICE 2.0 (Cyber Defense Analyst); EC-Council está acreditada por ANAB (ISO/IEC 17024) y reconocida por el DoD 8140/8570