EC-COUNCIL



EC-COUNCIL · PROGRAMA DE INTELIGENCIA DE AMENAZAS

Certified Threat Intelligence Analyst (C|TIA) v2

Domine la inteligencia de amenazas predictiva para una defensa proactiva: planificar, recolectar, analizar y difundir

¿Por qué debería asistir?

El Certified Threat Intelligence Analyst (C|TIA) de EC-Council es un programa integral de nivel especialista, dirigido a quienes recolectan, analizan y difunden inteligencia de amenazas. Cubre los fundamentos de la inteligencia de amenazas, el uso de sus herramientas y técnicas, y el desarrollo de un programa de inteligencia, con un enfoque estructurado en todas las etapas del ciclo de vida de la inteligencia de amenazas cibernéticas (CTI).

El curso convierte datos e información en inteligencia accionable para prevenir, detectar y monitorear ciberataques. Según Gartner Peer Insights, el 73 % de los profesionales señala la falta de habilidades como su mayor desafío en inteligencia de amenazas.

3 días	8	27	40 %	4
DURACIÓN	MÓDULOS	LABORATORIOS	TIEMPO EN LABORATORIO	TIPOS DE INTELIGENCIA



¿Quién debería participar?

Analistas de inteligencia
Analistas, investigadores y consultores de inteligencia de amenazas cibernéticas.

SOC y cacería de amenazas
Analistas de inteligencia en el SOC y cazadores de amenazas (threat hunters).

Ingeniería y liderazgo
Ingenieros, especialistas, líderes y gerentes de inteligencia de amenazas, y directores del área.

Seguridad e incidentes
Profesionales de seguridad de la información, seguridad de redes y respuesta a incidentes.

Objetivos de aprendizaje

- Comprender los tipos, el ciclo de vida, la estrategia, los marcos y las plataformas de inteligencia de amenazas
- Analizar amenazas y marcos de ataque: APT, Cyber Kill Chain, MITRE ATT&CK y el Modelo Diamante
- Planificar un programa de inteligencia de amenazas: requisitos, planificación, dirección y revisión
- Recolectar datos mediante OSINT, HUMINT, contrainteligencia, indicadores de compromiso (IoC), análisis de malware y Python
- Aplicar técnicas de análisis como el análisis estadístico y el análisis de hipótesis en competencia (ACH y SACH)
- Elaborar reportes y compartir inteligencia con las plataformas, leyes y regulaciones aplicables
- Realizar inteligencia de amenazas en la nube y automatizar la cacería de amenazas con Python
- Integrar la inteligencia de amenazas en las operaciones del SOC, la respuesta a incidentes y la gestión de riesgos

Ciclo de vida de la inteligencia de amenazas (CTI)

Planificación y dirección | Recolección | Procesamiento y explotación | Análisis y producción | Difusión e integración

Estratégica · Operativa · Táctica · Técnica

Programa del curso

Duración: 3 días

Módulo	Contenido
Módulos 1–3 Día 1	01 **Introducción a la inteligencia de amenazas:** tipos de inteligencia, ciclo de vida, estrategia, capacidades, modelo de madurez, marcos y plataformas. 02 **Ciberamenazas y marcos de ataque:** amenazas persistentes avanzadas (APT), Cyber Kill Chain, MITRE ATT&CK y Modelo Diamante de análisis de intrusiones. 03 **Requisitos, planificación, dirección y revisión:** pasos para planificar un programa de inteligencia de amenazas.
Módulos 4–6 Día 2	04 **Recolección y procesamiento de datos:** fuentes y feeds; OSINT, HUMINT, contrainteligencia, IoC, análisis de malware y Python; procesamiento y explotación de datos. 05 **Análisis de datos:** análisis estadístico, ACH y SACH; modelado de amenazas, ajuste, evaluación, runbooks y base de conocimiento. 06 **Reportes y difusión de inteligencia:** reportes, intercambio y colaboración con Python; plataformas, leyes y regulaciones para compartir inteligencia.
Módulos 7–8 Día 3	07 **Cacería y detección de amenazas:** tipos, proceso, ciclo y metodología de threat hunting, y automatización con Python. 08 **Inteligencia de amenazas en las operaciones del SOC, la respuesta a incidentes y la gestión de riesgos:** integración de la inteligencia en la operación, incluida la inteligencia de amenazas en entornos de nube.

Los cuatro tipos de Inteligencia			
Tipo	Pregunta que responde	Quién la usa	Horizonte
Estratégica	¿Qué riesgos enfrenta el negocio y cómo evolucionan?	Junta directiva, CISO	Meses o años
Operativa	¿Qué campaña viene contra nosotros y cuándo?	Gerencia de seguridad, respuesta a incidentes	Semanas
Táctica	¿Cómo ataca el adversario (técnicas y procedimientos)?	SOC, arquitectos, cazadores de amenazas	Días o semanas

Examen

Duración: 2 horas

Título	EC-Council Certified Threat Intelligence Analyst (C|TIA) – Versión 2		
Código	312-85	**N.º de preguntas**	50
Formato	Opción múltiple	**Duración**	2 horas
Plataforma	EC-Council Exam Portal		

¿Quién puede aplicar?

- **Experiencia:** profesionales de ciberseguridad de nivel medio a alto, con un mínimo de tres años de experiencia.
- **Certificaciones previas:** quienes poseen las certificaciones C|EH y C|ND de EC-Council pueden inscribirse en este curso.

Roles profesionales asociados a C|TIA

Analista de inteligencia de amenazas cibernéticas, cazador de amenazas, investigador o consultor de inteligencia, ingeniero, especialista, líder o gerente de inteligencia de amenazas, analista de inteligencia en el SOC, analista principal de amenazas de cibercrimen, director asociado de gestión de amenazas y director de inteligencia de amenazas. El salario promedio de un analista de inteligencia de amenazas en EE. UU. es de US$120.150 al año.

Información general

- Programa intensivo en laboratorios: 40 % del tiempo de formación dedicado a 27 laboratorios prácticos en redes y plataformas reales
- Alineado al 100 % con el marco NICE 800-181 y con CREST Certified Threat Intelligence Manager (CCTIM)
- Basado en un análisis de tareas del puesto (JTA) de toda la industria