

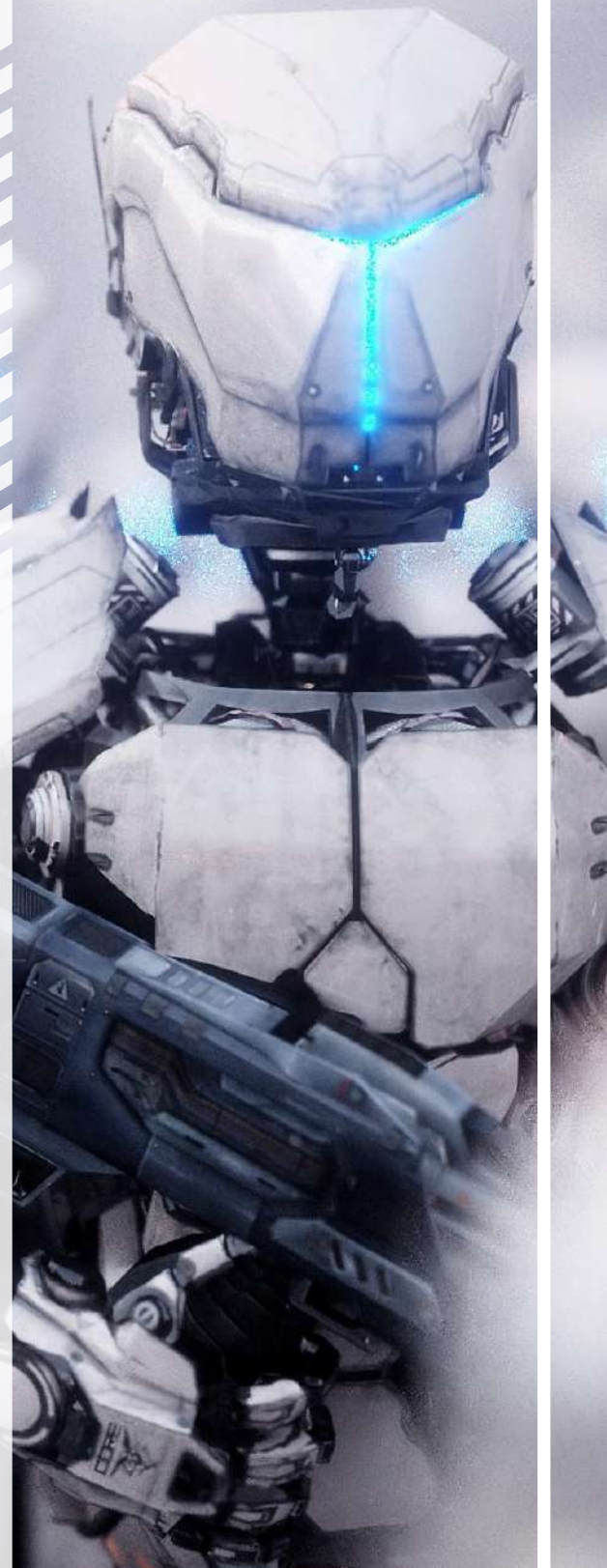
D I G I T A L B U S I N E S S

EC-Council

C | T I A

Certified | Threat Intelligence Analyst

CERTIFIED
THREAT
INTELLIGENCE
ANALYST



DESCRIPCIÓN DEL CURSO

Certified Threat Intelligence Analyst (C|TIA) es un programa de capacitación y acreditación diseñado, desarrollado en colaboración con expertos en ciberseguridad e inteligencia de amenazas de todo el mundo para ayudar a las organizaciones a identificar y mitigar los riesgos comerciales al convertir amenazas internas y externas desconocidas en amenazas conocidas. Es un programa completo de nivel especializado que enseña un enfoque estructurado para construir una inteligencia de amenazas efectiva.

El programa se basó en un riguroso análisis de tareas laborales (JTA) de los roles laborales involucrados en el campo de la inteligencia de amenazas. Este programa diferencia a los profesionales de inteligencia de amenazas de otros profesionales de seguridad de la información. Es un programa de capacitación intensivo de 3 días altamente interactivo, completo, basado en estándares que enseña a los profesionales de seguridad de la información a desarrollar inteligencia de amenazas profesional.



En el panorama de amenazas en constante cambio, C|TIA es un Programa totalmente esencial para aquellos que se ocupan amenazas cibernéticas en forma diaria. Las organizaciones de hoy en día sondan la demanda de seguridad cibernética de nivel profesional a analistas de inteligencia de amenazas que pueden extraer las estrategias a partir de datos mediante la implementación de varias estrategias avanzadas de inteligencia. Dicho programa de nivel profesional de los planes solo se puede lograr cuando el gobierno de estudios corresponde con los marcos de inteligencia del gobierno central y la industria publican amenazas que cumple con ellos.

C|TIA es un programa basado en métodos que utiliza un enfoque holístico, que cubre conceptos que van desde la planificación del proyecto de inteligencia de amenazas hasta la creación de un informe y la difusión de inteligencia de amenazas. Estos conceptos son muy esenciales a la hora de crear una inteligencia de amenazas eficaz y cuando se utilizan correctamente, pueden proteger a las organizaciones de futuras amenazas o ataques.

Este programa aborda todas las etapas involucradas en el ciclo de vida de Threat Intelligence, con Esta atención a un enfoque realista y futurista hace que C|TIA sea una de las certificaciones de inteligencia de amenazas más completas del mercado actual. Este programa proporciona el conocimiento profesional sólido que se requiere para una carrera en inteligencia de amenazas y mejora sus habilidades como analista de inteligencia de amenazas, lo que aumenta su empleabilidad. Es deseado por la mayoría de los ingenieros, analistas y profesiones de ciberseguridad de todo el mundo y es respetado por las autoridades contratantes.

Por qué las organizaciones necesitan un equipo de inteligencia de amenazas



Solo 1 de cada 10 organizaciones dice que es probable que detecte un ataque.

Los enfoques tradicionales de los ataques maliciosos están desapareciendo lentamente y cada cuatro segundos se forma nuevo malware. Sin embargo, muchas organizaciones todavía siguen los métodos tradicionales básicos para abordar estas técnicas en evolución.

Reaccionar a las amenazas es extremadamente importante, pero reaccionar también significa que el daño ya está hecho. Contar con un analista de inteligencia de amenazas brindará a las organizaciones la oportunidad de librar las batallas imprevistas que surgen constantemente en el mundo cibernético.

Un analista de inteligencia de amenazas capacitado podrá recopilar grandes cantidades de información relevante sobre amenazas de una multitud de fuentes de inteligencia que luego se analizarán para proporcionar inteligencia de amenazas que prediga con precisión las amenazas potenciales que una organización puede encontrar.

El escenario de seguridad de hoy en día requiere la implementación de inteligencia de amenazas cibernéticas, ya que ayuda a las organizaciones a mantenerse al día con las amenazas en evolución y el malware para defender en lugar de reconstruir.



¿Para quién?

Público objetivo

- Hackers éticos
- Profesionales de seguridad, ingenieros, analistas, especialistas, arquitectos, gerentes
- Analistas de inteligencia de amenazas, asociados, investigadores, consultores
- Cazadores de amenazas
- Profesionales SOC
- Analistas forenses digitales y de malware
- Miembros del equipo de respuesta a incidentes
- Cualquier profesional de ciberseguridad de nivel medio a alto con un mínimo de 2 años de experiencia.
- Individuos de la profesión de seguridad de la información y que quieran enriquecer sus habilidades y conocimientos en el campo de la inteligencia de amenazas cibernéticas.
- Personas interesadas en la prevención de amenazas cibernéticas.



Duración sugerida

3 Días (9:00 AM
a 17:00)

24 horas

Certificación:

El examen C|TIA se puede aplicar después de completar el programa de capacitación oficial C|TIA completo. Los candidatos que aprueben con éxito el examen recibirán su certificado C|TIA y privilegios de membresía. Se requiere que los miembros se adhieran a las políticas de la Política de Educación Continua de EC-Council.



Detalles del examen

 Título del examen Analista de inteligencia de amenazas certificado	 Código de examen 312-85
 numero de preguntas 50	 Duración 2 horas
 Disponibilidad Portal de exámenes del EC-Council	 Formato de prueba Opción multiple
 Puntaje de aprobación 70%	

Criterio de elegibilidad

Para ser elegible para desafiar el examen C|TIA, el candidato debe:

- Asistir a la capacitación oficial de EC-Council C|TIA a través de un socio acreditado de EC-Council (Centro de capacitación acreditado, iWeek, iLearn) (Todos los candidatos deben pagar la tarifa de solicitud de USD 100 a menos que su tarifa de capacitación ya lo incluya) o
- Presentar una solicitud que muestre un mínimo de 2 años de experiencia laboral en seguridad de la información (Todos los candidatos deben pagar USD 100 como tarifa de solicitud no reembolsable)



Los 10 principales componentes críticos de C|TIA

1. Cumplimiento al 100 % de los marcos NICE 2.0 y CREST

C|TIA asigna el 100 por ciento a la Iniciativa Nacional para la Educación en Seguridad Cibernética (NICE) en la categoría "Analizar" y el área de especialidad "Analista de amenazas/advertencias (TWA)", así como al "Administrador de inteligencia de amenazas certificado por CREST (CC TIM)."

2. Concéntrese en desarrollar habilidades para realizar varios tipos de inteligencia de amenazas

Se enfoca en desarrollar las habilidades para realizar diferentes tipos de inteligencia de amenazas, incluida la inteligencia de amenazas estratégica, operativa, táctica y técnica para una organización en particular.

3. Énfasis en varias técnicas de recopilación de datos de múltiples fuentes y mecanismos de alimentación.

Enfatiza varias técnicas de recopilación de datos de varias fuentes y mecanismos de alimentación. Permite a los estudiantes emplear diferentes estrategias de recopilación de datos para tener información relevante sobre amenazas.

4. Énfasis en la recopilación, creación y difusión de Indicadores de Compromiso (IoC) en varios formatos

C|TIA analiza los indicadores de compromiso (IoC) en detalle, incluidos los IoC internos y externos. Ilustra cómo adquirir estos IoC de varias fuentes. Los IoC son una buena fuente de información sobre amenazas cibernéticas y una organización puede detectar fácilmente ataques cibernéticos y responder a tiempo al monitorear los IoC. C|TIA explica detalladamente cómo crear y difundir estos IoC.

5. Concéntrese en un análisis intenso de malware para recopilar datos de adversarios y desviarse de ellos.

Explica en detalle cómo aplicar ingeniería inversa al malware y desviarse de él para determinar el origen, la funcionalidad y el impacto potencial del malware, así como también determinar el actor de la amenaza. Esta es una habilidad crucial requerida para el analista de inteligencia de amenazas.

6. Centrarse en un enfoque estructurado para realizar análisis de amenazas y evaluación de inteligencia de amenazas

Analizar los datos de amenazas recopilados y evaluar la inteligencia de amenazas requerida del proceso de análisis es uno de los pasos cruciales para extraer la inteligencia de amenazas. C|TIA analiza un enfoque estructurado que puede ser empleado por un analista para realizar análisis de amenazas y también modelado de amenazas. Este programa también ilustra cómo afinar el proceso de análisis para filtrar información innecesaria y extraer inteligencia efectiva. C|TIA también discute diferentes tipos de técnicas de evaluación de inteligencia de amenazas para adquirir la inteligencia deseada.

7. Centrarse en diversas técnicas para informar y difundir información sobre amenazas

C|TIA enfatiza la creación de informes de inteligencia de amenazas eficientes. Describe los componentes básicos para el intercambio de inteligencia sobre amenazas junto con diferentes reglas y modelos de intercambio. Explica las mejores prácticas para compartir TI y también discute diferentes leyes y regulaciones de intercambio de inteligencia.

8. Programa práctico

Más del 40 por ciento del tiempo de clase se dedica al aprendizaje de habilidades prácticas, y esto se logra a través de los laboratorios del EC-Council. La relación entre la teoría y la práctica del programa C|TIA es de 60:40, lo que brinda a los estudiantes una experiencia práctica de las últimas herramientas, técnicas, metodologías, marcos, scripts, etc. de inteligencia de amenazas. C|TIA viene integrado con laboratorios para enfatizar el aprendizaje objetivos

9. El entorno de laboratorio simula un entorno en tiempo real

El entorno de laboratorio de C|TIA consta de los últimos sistemas operativos, incluidos Windows 10 y Kali Linux, para planificar, recopilar, analizar, evaluar y difundir inteligencia sobre amenazas.

10. Cubre las últimas herramientas, plataformas y marcos de inteligencia de amenazas

El curso C|TIA incluye una biblioteca de herramientas, plataformas y marcos en diferentes plataformas operativas que los profesionales de seguridad requieren para extraer inteligencia de amenazas organizacional efectiva. Esto proporciona una opción más amplia para los estudiantes que cualquier otro programa en el mercado.



Esquema del curso

- 01** Introducción a la inteligencia de amenazas
- 02** Amenazas cibernéticas y metodología Kill Chain
- 03** Requisitos, planificación, dirección y revisión
- 04** Recopilación y procesamiento de datos
- 05** Análisis de los datos
- 06** Informes y difusión de inteligencia

OBJETIVOS DE APRENDIZAJE DEL PROGRAMA C|TIA

Problemas clave que plagan la información mundo de la seguridad

Importancia de inteligencia de amenazas en gestión de riesgos, SIEM e incidencia respuesta

Varios tipos de amenazas cibernéticas, actores de amenazas y sus motivos, metas y objetivos de los ataques de seguridad cibernética.

Fundamentos de la inteligencia de amenazas (incluidos los tipos de inteligencia de amenazas, el ciclo de vida, la estrategia, las capacidades, el modelo de madurez, frameworks, etc.)

Metodología de cadena cibernética, ciclo de vida de amenazas persistentes avanzadas (APT), tácticas, técnicas y procedimientos (TTP), indicadores de compromiso (IoC) y pirámide de dolor

Varios pasos involucrados en la planificación de un programa de inteligencia de amenazas (Requisitos, Planificación, Dirección y Revisión)

Diferentes tipos de fuentes de datos, fuentes, y recopilación de datos métodos

Inteligencia de amenazas recopilación de datos y adquisición a través de Fuente abierta Inteligencia (OSINT), Inteligencia humana (HUMINT), Cibernético Contraespionaje (ICC), Indicadores de compromiso (IoC) y malware análisis

Datos voluminosos colección y gestión (procesamiento de datos, estructuración, normalización, muestreo, almacenamiento, y visualización)

Datos diferentes tipos de análisis y técnicas incluido Datos estadísticos Análisis, Análisis de competir Hipótesis (ACH), Análisis estructurado de competir Hipótesis (SACH), etc.)

Proceso completo de análisis de amenazas que incluye modelado de amenazas, ajuste fino, evaluación, runbook y creación de base del conocimiento.

Datos diferentes análisis, amenaza

Protocolo de difusión e intercambio de inteligencia de amenazas, incluidas las preferencias de difusión, colaboración de inteligencia, reglas y modelos de intercambio, tipos y arquitecturas de intercambio de TI, participación en relaciones de intercambio, estándares y formatos para compartir inteligencia de amenazas.

modelado, y inteligencia de amenazas herramientas

Creando efectivo inteligencia de amenazas informes

Diferentes plataformas de intercambio de inteligencia de amenazas, leyes y regulaciones para compartir inteligencia estratégica, táctica, operativa y técnica.



EC-Council

Envia un Correo a:
academiacyber@tgk.com.mx
Siguenos en nuestras redes

