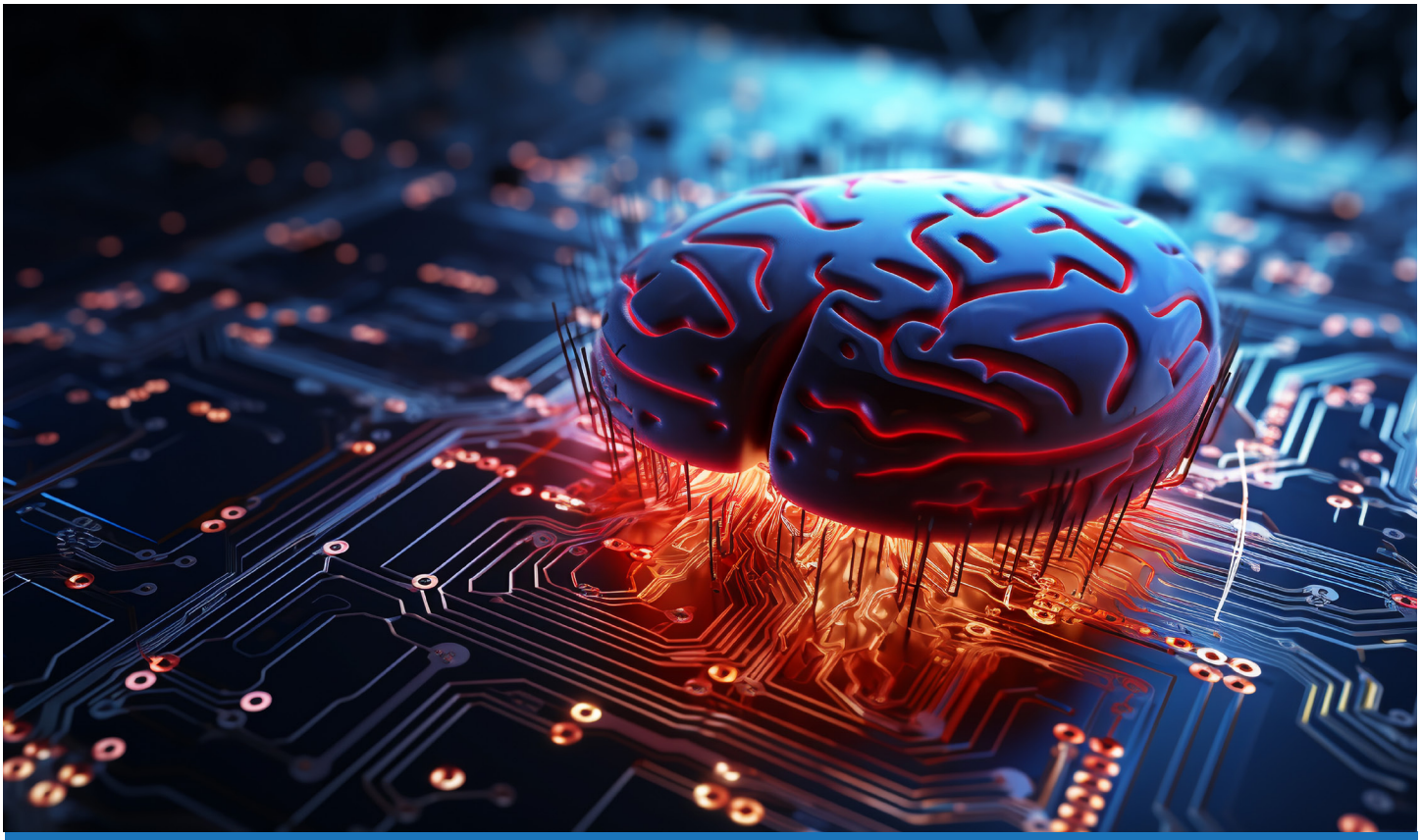


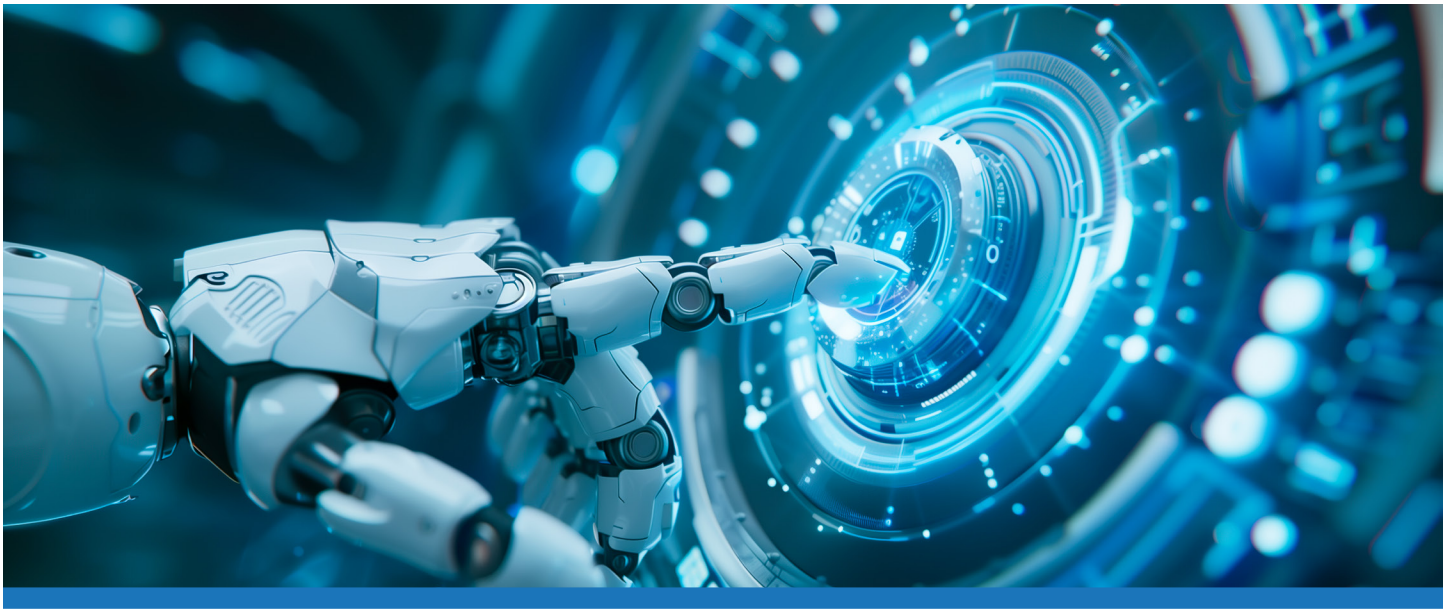
CompTIA SecAI+

Visión General

CompTIA SecAI+ se centra en los aspectos prácticos de la seguridad de los sistemas de IA en entornos de producción. Abarca conceptos fundamentales de IA relevantes para los equipos de seguridad, incluyendo cómo los flujos de trabajo de aprendizaje automático, los procesos de entrenamiento, las canalizaciones de datos y las arquitecturas de implementación afectan al riesgo y al control.

La certificación hace hincapié en la seguridad de los sistemas de IA a lo largo de todo su ciclo de vida: desde la protección de los datos de entrenamiento y los artefactos del modelo hasta la seguridad de los procesos de compilación e implementación, el mantenimiento de la integridad del modelo y la monitorización de los sistemas en funcionamiento para detectar usos indebidos o degradación. También aborda el uso de la IA en las operaciones de seguridad, incluyendo cómo las herramientas de detección, respuesta y automatización basadas en IA introducen nuevos beneficios, así como riesgos como falsos positivos, puntos ciegos y desviaciones del modelo.

Además, SecAI+ abarca amenazas específicas de la IA, como el aprendizaje automático adversario, el envenenamiento de datos, la manipulación de modelos y los ataques basados en avisos, junto con los requisitos de gobernanza, riesgo y cumplimiento necesarios para gestionar los sistemas de IA de forma responsable en entornos empresariales.



¿Quien debería asistir?

- **Ingeniero de Ciberseguridad**
- **Gerente de Ciberseguridad**
- **Arquitecto de Ciberseguridad**
- **Analista/Ingeniero de Ciberseguridad**
- **Gerente de TI**
- **Consultor de seguridad**

Agenda del curso

Duración: 5 días /40 horas

Día 1

- Tipos de IA (machine learning, deep learning, NLP, IA generativa)
- Entrenamiento de modelos (supervisado, no supervisado, reforzado, federado)
- Prompt engineering y diseño de prompts
- Seguridad de los datos utilizados por modelos de IA
- Modelado de amenazas para sistemas de IA
- Uso de marcos y recursos de threat modeling

Día 2

- Implementación de controles de seguridad
- Protección de modelos y uso de guardrails, gateways y límites de uso
- Controles de acceso a modelos, datos, agentes, APIs y redes
- Cifrado, anonimización y sanitización de datos
- Monitoreo de prompts, rendimiento y costos
- Auditoría de calidad, cumplimiento y registros (logs)

Día 3

- Seguridad en todas las fases del ciclo de vida de la IA
- Ética y rol humano en la seguridad de la IA
- Ataques
- Diseño e implementación de controles compensatorios
- Herramientas de seguridad habilitadas por IA
- Uso de IA en detección, análisis e incident response

Día 4

- Automatización de tareas de seguridad con IA
- IA para scripting, DevSecOps y flujos de trabajo
- Análisis de vectores de ataque potenciados por IA (deepfakes, ingeniería social, ataques automatizados)

Día 5

- Estructuras de gobernanza de IA
- Roles y responsabilidades organizacionales
- Riesgos específicos y principios de IA responsable
- Cumplimiento normativo y marcos regulatorios de IA
- Impacto del cumplimiento en el desarrollo y uso empresarial de la IA

Resumen de los objetivos del examen SecAI+ (V1)

Conceptos básicos de IA relacionados con la ciberseguridad (17%)

- Explicar los principios y la terminología básicos de la IA : aprendizaje automático, aprendizaje profundo, procesamiento del lenguaje natural y automatización.
- Identificar aplicaciones de IA en seguridad : Casos de uso de la IA en la detección de amenazas, la defensa y las operaciones de seguridad.
- Reconocer las amenazas impulsadas por IA : phishing automatizado, malware polimórfico, aprendizaje automático adversario y uso malicioso de IA generativa.

Garantizar la seguridad de los sistemas de IA (40%)

- Implementar controles de seguridad : Proteja los sistemas, datos y modelos de IA mediante sólidas medidas de seguridad técnicas.
- Entornos de implementación de IA seguros : Aplique las mejores prácticas en infraestructuras locales, en la nube e híbridas.
- Mitigar los riesgos de ataques : Protegerse contra los ataques dirigidos a los modelos de IA, las canalizaciones de datos y las capas de inferencia.

Seguridad asistida por IA (24%)

- Mejorar la detección y la respuesta : utilice herramientas basadas en inteligencia artificial para identificar anomalías, detectar amenazas y acelerar la resolución de incidentes.
- Automatice los flujos de trabajo de seguridad : integre la IA para la clasificación de eventos, la correlación de alertas y la orquestación de respuestas.
- Aplicar técnicas de IA en las operaciones : Incorporar la IA en el modelado de amenazas, el análisis del comportamiento y la monitorización continua.

Gobernanza, riesgo y cumplimiento de la IA (19%)

- Comprender los marcos regulatorios : Identificar los requisitos de gobernanza global y sus implicaciones para la adopción de la IA.
- Integrar GRC en los proyectos de IA : Incorporar prácticas de gobernanza, gestión de riesgos y cumplimiento a lo largo de todo el ciclo de vida de la IA.
- Garantizar un uso responsable de la IA : Aplicar directrices éticas, normas legales y marcos de referencia del sector, como el RGPD y el Marco de Gestión de Riesgos de IA del NIST.

Características generales del curso

Recursos incluidos

- 17 laboratorios prácticos
- 18 videos
- 19 actividades interactivas
- 75 lecciones teóricas
- 27 evaluaciones

Más de 500 preguntas en banco de exámenes

Este plan de lecciones proporciona una formación integral en seguridad de IA, combinando conceptos técnicos, prácticas defensivas, análisis de amenazas, automatización, gobernanza y cumplimiento. Está orientado a profesionales de ciberseguridad que buscan entender, proteger y operar sistemas de IA de forma segura, así como a quienes desean obtener la certificación CompTIA SecAI+.
Si quieres, puedo:

Examen

Nombre del examen: CY0-001
Cantidad de preguntas: 60
Formato: Selección múltiple interactiva y desempeño
Disponibilidad: Pearson / VUE
Puntuación mínima para aprobar: 600 (en una escala de 100 a 900)
Duración del examen: 60minutos

Certificación

Después de completar con éxito el examen, recibirá el certificado digital de Comptia que le acredita como un profesional certificado

Información general

- Somos el único Centro de Entrenamiento Autorizado en el país
- Los honorarios del curso incluye el costo del examen
- Cada estudiante tendrá acceso a un entorno personalizado de aprendizaje con todos los contenidos necesarios para el curso
- Se incluye el acceso a los laboratorios virtuales para la realización de los ejercicios y aumentar así la comprensión y dominio de los objetivos del curso
- Como material para la preparación cada estudiante tendrá acceso a su propio entorno de preguntas de práctica para simular un ambiente de examen y mejorar las posibilidades de éxito
- Precio sugerido, USD 2,000 o su equivalente en pesos dominicanos
- Los participantes a nuestros cursos pueden asistir más de una vez ya sea para reforzar conocimientos o como preparación para el examen de esa versión del curso

CompTIA Authorized Partner DELIVERY PARTNER

CompTIA SecAI+ CERTIFICATION Expansion Series

SAVANT CONSULTORES

CompTIA