CompTIA SecAI+

La inteligencia artificial está transformando la ciberseguridad, pero también está creando nuevas amenazas y vulnerabilidades. ¿Estás preparado para proteger los sistemas de IA y aprovechar su potencial para mejorar la seguridad de tu organización?

Con el **Curso CompTIA SecAI+ de DIGNITAE** aprenderás a identificar y mitigar riesgos específicos de la inteligencia artificial, proteger modelos y aplicaciones de IA, automatizar operaciones de seguridad y aplicar buenas prácticas de gobernanza y cumplimiento normativo. Una formación especializada que te ayudará a desarrollar las competencias necesarias para afrontar los nuevos desafíos de la ciberseguridad y **prepararte para obtener la certificación oficial CompTIA SecAI+ (CY0-001)**.

Objetivos Didácticos

Al finalizar el curso, habrás adquirido los conocimientos necesarios para comprender los riesgos asociados a la inteligencia artificial, proteger los sistemas que la utilizan y aprovechar sus capacidades para reforzar la seguridad de las organizaciones.

En concreto, aprenderás a:

- **Comprender los fundamentos de la inteligencia artificial aplicada a la ciberseguridad**, incluyendo aprendizaje automático, aprendizaje profundo, IA generativa y modelos de lenguaje.
- **Identificar las amenazas y vulnerabilidades específicas de los sistemas de IA**, utilizando marcos de referencia como OWASP y MITRE ATLAS.
- **Proteger modelos, aplicaciones y datos utilizados por sistemas de inteligencia artificial**, mediante controles de seguridad, acceso y protección de la información.
- **Detectar y mitigar ataques contra sistemas de IA**, como la inyección de instrucciones maliciosas, el envenenamiento de datos, el robo de modelos y las fugas de información.
- **Utilizar herramientas de inteligencia artificial para mejorar las operaciones de ciberseguridad**, automatizando el análisis de vulnerabilidades, la detección de amenazas y determinadas tareas de respuesta.
- **Reconocer nuevas amenazas potenciadas por la IA**, como las falsificaciones digitales, la suplantación de identidad y la ingeniería social automatizada.
- **Aplicar principios de gobernanza, gestión de riesgos y cumplimiento normativo** relacionados con la inteligencia artificial, considerando el Reglamento Europeo de IA, el RGPD y el marco NIST AI RMF.
- **Prepararte para el examen oficial CompTIA SecAI+ (CY0-001)**, familiarizándote con las áreas de conocimiento evaluadas en la certificación.

Audiencia

Este curso está dirigido a profesionales de tecnologías de la información y ciberseguridad que desean ampliar sus conocimientos sobre la protección de sistemas de inteligencia artificial y su aplicación a las operaciones de seguridad.

Especialmente recomendado para:

- **Analistas de ciberseguridad y profesionales de centros de operaciones de seguridad (SOC)** que necesitan identificar nuevas amenazas y utilizar herramientas de IA para mejorar la detección y respuesta ante incidentes.
- **Ingenieros y arquitectos de seguridad** interesados en incorporar controles de protección en infraestructuras, aplicaciones y modelos de inteligencia artificial.
- **Especialistas en pruebas de penetración y análisis de vulnerabilidades** que desean comprender las técnicas de ataque específicas contra sistemas de IA.
- **Profesionales de inteligencia artificial y aprendizaje automático** que necesitan integrar medidas de seguridad durante el desarrollo, despliegue y mantenimiento de modelos.
- **Responsables de seguridad de la información y gestión de riesgos** que buscan comprender las implicaciones de la IA para la protección de los activos de su organización.
- **Consultores y especialistas en cumplimiento normativo** interesados en la gobernanza de la inteligencia artificial y los requisitos regulatorios relacionados con su seguridad.

También resulta adecuado para profesionales con experiencia en seguridad informática que desean evolucionar hacia perfiles especializados en ciberseguridad e inteligencia artificial.

Requisitos previos

Para aprovechar adecuadamente la formación, CompTIA recomienda contar con:

- Entre 3 y 4 años de experiencia profesional en tecnologías de la información.
- Al menos 2 años de experiencia práctica en ciberseguridad.
- Conocimientos de seguridad informática equivalentes a los que proporcionan certificaciones como CompTIA Security+, CySA+ o PenTest+.

Estos conocimientos constituyen recomendaciones de preparación, no requisitos obligatorios de certificación según la documentación aportada.

Modalidad

Aula virtual en directo.

Duración

3 días

Temario del curso

1. **Fundamentos de inteligencia artificial relacionados con la ciberseguridad**
   - Tipos y técnicas de inteligencia artificial.
   - Aprendizaje automático, aprendizaje profundo y modelos de lenguaje.
   - Técnicas de entrenamiento y optimización de modelos.
   - Ingeniería de instrucciones para modelos de IA.
   - Seguridad de los datos, recuperación aumentada por generación (RAG) y bases de datos vectoriales.
   - Ciclo de vida seguro de los sistemas de inteligencia artificial.

2. **Protección y aseguramiento de sistemas de IA**
   - Modelado de amenazas con OWASP y MITRE ATLAS.
   - Controles técnicos, de acceso y protección de datos.
   - Prevención de inyección de instrucciones maliciosas.
   - Mitigación del envenenamiento de datos y robo de modelos.
   - Detección de fugas de información.
   - Supervisión, auditoría y análisis de incidentes en sistemas de IA.

3. **3. Ciberseguridad asistida por inteligencia artificial**
   - Herramientas de seguridad basadas en inteligencia artificial.
   - Automatización del análisis de vulnerabilidades.
   - Aplicación de IA en pruebas de penetración.
   - Detección de falsificaciones digitales y suplantación.
   - Amenazas de ingeniería social automatizada.
   - Correlación de datos y automatización de operaciones de seguridad.

4. **4. Gobernanza, riesgo y cumplimiento de la IA**
   - Modelos organizativos de gobernanza de inteligencia artificial.
   - Reglamento Europeo de Inteligencia Artificial.
   - Marco de gestión de riesgos NIST AI RMF.
   - Protección de datos y RGPD.
   - Riesgos éticos, privacidad y explicabilidad de los modelos.