Guía de la profesión

Especialista en Ciberseguridad

Plan de estudios →

Descripción de proyecto →

Contenido técnico →

tripleten

Especialista en Ciberseguridad

Plan de estudios

12 proyectos

12 sprints

20–40 horas de estudio

tripleten

Acerca del Programa

Este programa completo de 7 meses te proporcionará el conocimiento, las habilidades y la experiencia práctica que necesitas para iniciar una carrera en ciberseguridad. Cada sprint dura entre dos y seis semanas, con una carga aproximada de 20–40 horas de estudio.

A través de clases en vivo, laboratorios interactivos, proyectos prácticos y preparación profesional, dominarás desde los fundamentos de seguridad hasta la respuesta a incidentes y la gestión de vulnerabilidades.

1

Fundamentos: Cómo se comunican los hosts y las redes

+1 proyecto | 2 semanas | 20-25 horas

Capítulos:

1. Cómo se comunican realmente las computadoras
2. Paquetes, movimientos y rastros
3. Arquitectura, observabilidad y puntos de entrada
4. Las redes desde una perspectiva de seguridad
5. Proyecto del Sprint

2 Descubrimiento de activos y servicios expuestos

+1 proyecto | 2 semanas | 20-25 horas

Capítulos:

1. Por qué la visibilidad precede a la seguridad
2. Escaneo, enumeración y exposición
3. Exposición interna vs. externa
4. Contexto y criticidad de los activos
5. Proyecto del Sprint

3 Aplicando marcos de seguridad a entornos reales

+1 proyecto | 2 semanas | 20-25 horas

Capítulos:

1. De la actividad a la evidencia
2. Logs en diferentes capas
3. Alertas, ruido y contexto
4. Correlación y pensamiento de investigación
5. Lección del Proyecto

4 Telemetría de seguridad: Logs, evidencia y límites de visibilidad

+1 proyecto | 2 semanas | 20-25 horas

Capítulos:

1. La arquitectura como una decisión de seguridad
2. Error de configuración vs. Ataque
3. Exposición de credenciales en redes
4. Logs, brechas y falsa confianza
5. Pensamiento de Seguro-por-Defecto
6. Lección del Proyecto

5 Fundamentos de Ingeniería de Detección: De eventos a alertas

+1 proyecto | 2 semanas | 20-25 horas

Capítulos:

1. Cómo nacen las alertas
2. Señal vs. Ruido
3. Investigando bajo presión
4. Correlación y narrativa
5. Escalamiento, severidad y respuesta
6. Proyecto del Sprint

6 Operaciones SIEM: Consultas, pivoteo y flujo de casos (SOC L1)

+1 proyecto | 2 semanas | 20-25 horas

Capítulos:

1. Qué convierte una alerta en un incidente
2. Contención y control
3. Erradicación y recuperación
4. Comunicación durante incidentes
5. Aprendiendo de los incidentes
6. Proyecto del Sprint

7 Triaje y escalamiento de alertas: Tomando decisiones defendibles rápido

+1 proyecto | 2 semanas | 20-25 horas

Capítulos:

1. Por qué ocurren los ataques
2. Del acceso inicial al impacto
3. Técnicas de ataque comunes (Sin obsesión por las herramientas)
4. "Living off the Land" y ataques combinados
5. Usando el contexto de amenazas en el SOC
6. Proyecto del Sprint

8 Investigación y reconstrucción de amenazas (Núcleo SOC L2)

+1 proyecto | 2 semanas | 20-25 horas

Capítulos:

1. Cómo cambia la nube el modelo de seguridad
2. La identidad es el nuevo perímetro
3. Malas configuraciones comunes en la nube
4. Abuso de identidad y ataques en la nube
5. Visibilidad en la nube y límites de registros
6. Proyecto del Sprint

9 Detección y respuesta en endpoint (Operaciones EDR/XDR)

+1 proyecto | 2 semanas | 20-25 horas

Capítulos:

1. Por qué existen las detecciones
2. Qué hace que una detección sea buena
3. De los registros a la lógica de detección
4. Ajuste, validación y cobertura
5. Automatización, SOAR y seguridad en IA
6. Proyecto del Sprint

10 Arquitectura de seguridad en la nube

+1 proyecto | 2 semanas | 20-25 horas

Capítulos:

1. Qué convierte un incidente en una crisis
2. El Ransomware como incidente de negocio
3. Detectando e investigando Ransomware
4. Respuesta, contención y decisiones
5. Secuelas, recuperación y lecciones aprendidas
6. Proyecto del Sprint

11

GRC, Cumplimiento y Gobernanza

+1 proyecto | 2 semanas | 20-25 horasa

Capítulos:

1. Por qué la gobernanza define la seguridad
2. ISO 27001 y SOC 2 en la práctica
3. Derecho Digital en el contexto de LATAM
4. Traduciendo hallazgos técnicos a lenguaje de gobernanza
5. Simulación de auditoría y mapeo de evidencia
6. Proyecto del Sprint

12

Capstone: Evaluación de seguridad empresarial integral

+ 1 proyecto | 3 semanas | 25-30 horas

Capítulos:

1. Contexto empresarial y marco de amenazas
2. Investigación técnica y correlación
3. Riesgo, cumplimiento e impacto al negocio
4. Reporteo Profesional
5. Defensa y simulación de entrevista
6. Proyecto del Sprint

Especialista en Ciberseguridad

Contenido técnico

7 meses | Online | A tiempo parcial

tripleten

El Bootcamp de Ciberseguridad de TripleTen está diseñado para preparar a los estudiantes para roles de nivel junior en un área de alta demanda.

Habilidades Desarrolladas

- Fundamentos de ciberseguridad y redes seguras
- Gestión de riesgos y cumplimiento (ISO, NIST, GDPR)
- Análisis y escaneo de vulnerabilidades
- Respuesta a incidentes y defensa
- Seguridad en la nube (AWS, Azure, GCP)

Tecnologías y herramientas clave

- Sigma Rules
- Wazuh
- Nmap
- ELK
- Kali Linux
- n8n
- Figma
- Cloudshare
- The Hive
- Obsidian
- Splunk (SIEM)
- MITRE ATT&CK
- sqlmap

Preparación para la profesión

- Auditor de TI
- Analista SOC
- Especialista en Ciberseguridad
- Pentester / Hacker Ético
- Especialista en Seguridad en la Nube

Habilidades Sociales

- Trabajo en equipo
- Manejo del tiempo
- Adaptabilidad
- Resolución de problemas
- Pensamiento lógico
- Ética profesional