CURSO DE CIBERSEGURIDAD DEFENSIVA

DESCRIPCIÓN

El curso sobre Ciberseguridad Defensiva está diseñado para profesionales interesados en aprender a defenderse de los ciberataques y proteger los activos digitales de su organización. Este curso cubre conceptos clave y habilidades prácticas en seguridad de redes, modelado y análisis de amenazas, respuesta a incidentes y operaciones de seguridad.
Al final del programa, los estudiantes estarán equipados con los conocimientos y habilidades necesarios para asegurar las redes, sistemas y aplicaciones de su organización contra las últimas amenazas cibernéticas. Este curso es adecuado para profesionales de diversos campos, incluyendo TI, ciberseguridad, y carreras de tecnología en general.

REQUISITOS DE INGRESO

- Conocimientos básicos de conceptos de redes informáticas
- Familiaridad con los principios y la terminología de la ciberseguridad
- Conocimientos básicos de sistemas operativos y lenguajes de programación
- Acceso a un ordenador con conexión a Internet.
- El candidato debe tener acceso a un equipo computacional con al menos 16 GB de RAM y 50 GB de capacidad de almacenamiento disponible, junto con la capacidad de virtualizar máquinas.

DIRIGIDO A

El curso sobre técnicas de ciberseguridad defensiva está diseñado para profesionales interesados en mejorar sus conocimientos y habilidades en ciberseguridad defensiva. Es adecuado para personas que deseen seguir una carrera en ciberseguridad, así como para profesionales que deseen ampliar sus conocimientos en este campo. El curso también es ideal para quienes se dedican a la gestión de la seguridad de la información, la gestión de riesgos y la gestión de operaciones informáticas.

MODALIDAD

Online – sincrónico (vía zoom)* con apoyo de plataforma U-Cursos para gestión académica.
*Las clases son grabadas y están disponibles para ser visualizadas hasta dos semanas después de finalizado el curso.

OBJETIVOS GENERALES

Proporcionar a los participantes una comprensión completa de las tácticas, técnicas y estrategias de ciberseguridad defensiva para proteger los sistemas informáticos y las redes contra las ciberamenazas.
Al final del curso, los participantes deben estar equipados con los conocimientos y habilidades para desarrollar e implementar defensas eficaces de ciberseguridad, incluyendo el modelado de amenazas, análisis de vulnerabilidades, gestión de riesgos, respuesta a incidentes y operaciones de seguridad.

CONTENIDOS | 30 horas cronológicas

MÓDULOS / TEMARIO

- Introducción a la ciberseguridad y a la modelización de amenazas basado en MITRE ATT&CK
- Técnicas de análisis y gestión de vulnerabilidades
- Seguridad de redes y estrategias de defensa perimetral
- Respuesta y gestión de incidentes
- Técnicas de supervisión de la seguridad y detección de amenazas

METODOLOGÍA

El curso será fundamentalmente práctico, en base a sesiones de trabajo directo en el computador. Todas las sesiones contemplan instrucción del profesor en los contenidos y técnicas de uso de las herramientas y luego aplicación en ejercicios crecientes en complejidad por parte de los estudiantes. Los ejercicios y/o proyectos personales están orientados de manera que los estudiantes puedan aplicar los contenidos en sus contextos profesionales, disciplinares, laborales o personales. Las clases se complementan con exposiciones teóricas de los fundamentos conceptuales necesarios para comprender el alcance y potencial de la herramienta. El trabajo del estudiante es principalmente individual.

EVALUACIÓN

El curso se aprueba con nota mínima promedio 4.0 en escala de 1.0 a 7.0 en trabajo/prueba final, asistencia 75% y participación en clases.
Al finalizar el curso se enviará a los participantes Certificado Digital (Diploma) acreditado por la Facultad de Ciencias Físicas y Matemáticas de la Universidad de Chile.

RELATOR

Sebastián **Vargas**
Presidente de Fundación Sochisi, es Ingeniero Civil en informática e Ingeniero en Ciberseguridad. Máster en Ciberseguridad Industrial, Centro de Ciberseguridad Industrial España. Máster en Gestión de Tecnologías de la información y Máster en Ciberseguridad, Ciberterrorismo y Ciberguerra, Universidad Pegaso de Italia.

[□] Profesional con más de 15 años de experiencia en el ámbito de la ciberseguridad, desarrollándose en diversos cargos como OSI, CISO o CSO en el sector Público, financiero y empresas relacionadas a la infraestructura crítica del país.

Posee las certificaciones:

[[□□]] Certified Ethical Hacker (Practical)
[[□]] eLearnSecurity Certified Incident Responder (eCIR)
[[□♂]] eLearnSecurity Certified Digital Forensics Professional (eCDFP)
[[□]] eLearnSecurity Junior Penetration Tester (eJPT)
[[□]] ATT&CK Fundamentals [[□]]
[[□]] ATT&CK PurpleTeam [[□]]
[[□]] ATT&CK for Cyber Threat Intelligence [[□]]
[[□]] ATT&CK for Security Operations Center Assessments [[□]]
[[□]] ATT&CK for Adversary Emulation Methodology [[□]]
[[□]] ATT&CK for Threat Hunting Detection Engineering
[[□]] Implementador y auditor de ISO 27.001

Puedes conocer su trayectoria en:
https://www.linkedin.com/in/mgsebastianvargasyanez/

FECHA Y HORARIO

Fecha Inicio: 06 de mayo de 2024.
Fecha de Término: 05 de junio de 2024.
Días y horario de clases: 06, 08, 13, 15, 20, 22, 27 y 29 mayo, 03 y 05 junio 2024.
Lugar de clases: Modalidad a distancia (vía streaming)
Duración total: 30 horas cronológicas.