aulamentor

Área formativa
Informática y Comunicac.

CiberOps Associate

80h

Los usuarios finales y empresas necesitan saber cómo proteger sus datos. Diariamente nos encontramos, al navegar, con que tenemos que aceptar las "cookies" que posteriormente se utilizan como moneda de cambio para ofertarnos productos sobre los artículos que hemos buscado.

Cada día se hace más necesario en las empresas un perfil de experto que atienda los incidentes de seguridad, cada vez más frecuentes. Desde correos donde se suplanta la identidad de otra persona, hasta que nos encontramos con que toda la información crítica de la empresa está cifrada y no podemos acceder a ella, salvo que hagamos un pago.

El curso de "Cybersecurity Operations", formará a los alumnos en destrezas para: Conocer las vulnerabilidades que se producen en Ciberseguridad, los sistemas operativos que utilizan; Detectar los tipos de ataque, los métodos que utilizan; Proteger los datos personales, los corporativos, todas las infraestructuras; Analizar todos estos riesgos y tomar medidas al respecto; Al superar el curso podrán adquirir con éxito las responsabilidades de un analista de seguridad que trabaja en un Centro de Operaciones de Seguridad (SOC).

Destinatarios

Todas aquellas personas interesadas en iniciarse o perfeccionar en los conceptos y la práctica de la ciberseguridad.

Contenidos

- **Tema 1.** The Danger
- **Tema 2.** Fighters in the War Against Cybercrime
- **Tema 3.** The Windows Operating System
- **Tema 4.** Linux Overviw
- **Tema 5.** Network Protocols
- **Tema 6.** Ethernet and Internet Protocol (IP)
- **Tema 7.** Connectivity Verification
- **Tema 8.** Address Resolution Protocols
- **Tema 9.** - The transport Layer
- **Tema 10.** Network Services
- **Tema 11.** Network Communication Devices
- **Tema 12.** Network Security Infraestructure
- **Tema 13.** Atttackers and Their Tools
- **Tema 14.** Common Threats and Attacks
- **Tema 15.** Network Monitoring and Tools
- **Tema 16.** Attacking the Foundation
- **Tema 17.** Attacking What We Do
- **Tema 18.** Understanding Defense
- **Tema 19.** Acces Control
- **Tema 20.** Threat Intelligence
- **Tema 21.** Cryptography
- **Tema 22.** Endpoint Protection
- **Tema 23.** Endpoint Vulnerability Assessment
- **Tema 24.** Technologies and Protocols
- **Tema 25.** Network Security Data
- **Tema 26.** Avaluating Alerts
- **Tema 27.** Working with Network Security Data
- **Tema 28.** Digital Forensics and Incident Analysis and Response

Observaciones: Es recomendable que el alumno tenga conocimientos básicos de los sistemas operativos Linux y Windows, conocimiento de redes equivalente a los módulos 1 y 2 del CCNA R&S. No es necesario un amplio conocimiento de idioma inglés, ya que la documentación se encuentra totalmente traducida al castellano. En este curso se van a usar máquinas virtuales (VM) y el simulador de redes Packet Tracer de Cisco. Requerimientos del ordenador personal para poder ejecutar el programa de virtualización (VirtualBox de Oracle): Mínimo 4GB de RAM, recomendable 4 GB de RAM y 30 GB de espacio libre en disco. El tutor seleccionará algunas prácticas obligatorias de todas las del curso. Se realizarán exámenes por grupos módulos de la misma temática. Al finalizar es obligatorio superar un examen final de todo el curso.

GOBIERNO DE ESPAÑA
MINISTERIO DE EDUCACIÓN Y FORMACIÓN PROFESIONAL
UNIÓN EUROPEA
NextGenerationEU