



CBROPS - CyberOps

Duración: 70 hrs

Descripción general

El nuevo curso de CyberOps Associate se enmarca en el programa oficial Cisco Networking Academy. A lo largo de los módulos que conforman este currículum, se introducen conceptos de seguridad fundamentales y se enseñan las habilidades necesarias para monitorear, detectar, analizar y dar respuesta a la ciberdelincuencia, el ciberespionaje, las amenazas internas, las amenazas persistentes avanzadas, los requisitos normativos y otros problemas de ciberseguridad a los que se enfrentan las organizaciones a diario.

Así mismo, este curso pone énfasis en la aplicación práctica de las habilidades necesarias para mantener y garantizar la disponibilidad de seguridad operativa de los sistemas en red.

Como valor añadido del presente curso, se dará acceso a todo el material disponible en NetAcad asociado al presente curso, así como a los escenarios prácticos del curso, basados en las distribuciones Kali Linux y Security Onion, que incorporan herramientas especializadas en pruebas de penetración y auditoría, así como herramientas de análisis, clasificación y monitorización de alertas.

Objetivos

- Comprender los principios, roles y responsabilidades involucrados en las operaciones de ciberseguridad, así como las tecnologías, herramientas, regulaciones y estándares disponibles.
 - Describir las vulnerabilidades y amenazas comunes en los dispositivos de usuario y en las infraestructuras de red.
 - Demostrar habilidades fundamentales aplicadas a la monitorización, detección, investigación, análisis y respuesta a incidentes de seguridad.
 - Clasificar eventos intrusivos según categorías definidas por modelos de seguridad y establecer acciones defensivas.
 - Explicar cómo investigar las vulnerabilidades y ataques de punto final.
 - Evaluar alertas de seguridad y analizar los datos de intrusión en la red para identificar vulnerabilidades y hosts comprometidos.
 - Aplicar modelos de respuesta a incidentes para gestionar incidentes de seguridad de red
-
-



-
- Llevar a cabo con éxito las tareas, deberes y responsabilidades de un Analista de Seguridad de nivel asociado en un Centro de Operaciones de Seguridad (SOC).

Prerrequisitos del curso

Para un mayor aprovechamiento del curso, es recomendable que el alumno tenga conocimientos básicos de sistemas operativos Windows y/o Linux, conceptos básicos de programación y un nivel de conocimientos previos en redes equivalente a haber realizado CCNA v7.

Dirigido a:

El curso está dirigido de manera específica a profesionales IT (ingenieros de Networking, administradores de redes, etc.) que quieren iniciarse en la temática de la ciberseguridad, aumentando su conocimiento y experiencia en esta área de demanda creciente y en los procedimientos empleados en un Centro de Operaciones de Seguridad - SOC.

Esquema del curso

Módulo 1. Introducción – Amenazas, actores e impacto

Módulo 2. Ciberseguridad: el Centro de Operaciones de Seguridad – SOC

Módulo 3. Sistema operativo Windows

Módulo 4. Sistema operativo Linux

Módulo 5. Protocolos de red

Módulo 6. Protocolos Ethernet e IP

Módulo 7. Principios de seguridad en red

Módulo 8. Protocolo de resolución de direcciones

Módulo 9. Capa de transporte

Módulo 10. Servicios de red

Módulo 11. Dispositivos de comunicación de red



Módulo 12. Infraestructura de seguridad de red

Módulo 13. Atacantes y sus herramientas

Módulo 14. Amenazas y ataques comunes

Módulo 15. Monitorización de las operaciones de red

Módulo 16. Ataques a los fundamentos

Módulo 17. Ataques a los servicios

Módulo 18. Comprensión de la defensa

Módulo 19. Control de acceso

Módulo 20. Inteligencia de amenazas

Módulo 21. Criptografía de clave pública - PKI

Módulo 22. Protección de puntos finales

Módulo 23. Evaluación de vulnerabilidades en puntos finales

Módulo 24. Tecnologías de seguridad y protocolos

Módulo 25. Monitorización de la seguridad y tipos de datos

Módulo 26. Evaluación de alertas

Módulo 27. Interpretación de los datos de monitorización

Módulo 28. Análisis forense. Respuesta y gestión de incidencias
