

CCNA CyberOps Associate

Descrición

CCNA Cybersecurity Operations - CYBER OPS introduce os coñecementos e habilidades necesarias para asumir con éxito as tarefas, deberes e responsabilidades dos analistas de seguridade de nivel asociado que traballan en centros de operacións de seguridade (SOC). Este curso introduce os conceptos de seguridade fundamentais e habilidades necesarias para supervisar, detectar, analizar e dar resposta á ciberdelincuencia, ciberespionaxe, ameazas internas, ameazas persistentes avanzadas, requisitos normativos e outros problemas de ciberseguridade aos que se enfrontan as organizacións. Así mesmo, fai fincapé na aplicación práctica das habilidades necesarias para manter e garantir a dispoñibilidade de seguridade operativa dos sistemas en rede.

O curso será en aula virtual e a proba de selección realizarase en liña, polo que tanto para a proba como para o seguimento do curso é necesario que as persoas interesadas en participar teñan:

- Correo electrónico
- Ordenador (preferentemente Windows ou MacOS) con conexión a internet.
- Para seguir o curso é necesario que o equipo conte con altofalantes ou auriculares, micrófono e cámara web.

Os días lectivos serán de luns a xoves, e serán non lectivos o 7 e 8 de decembro e do 23 de decembro ao 10 de xaneiro incluídos.

Obxectivos

Unha vez rematado o curso, o alumno adquirirá os coñecementos necesarios para:

- Comprender os principios, roles e responsabilidades involucrados nas operacións de ciberseguridade, así como as tecnoloxías, ferramentas, regulacións e estándares dispoñibles.
 - Describir vulnerabilidades e ameazas comúns en dispositivos de usuario e infraestruturas de rede.
 - Demostrar habilidades fundamentais aplicadas ao seguimento, detección, investigación, análise e resposta a incidentes de seguridade.
 - Clasificar eventos intrusivos segundo categorías definidas por modelos de seguridade e establecer accións defensivas.
 - Realizar con éxito as tarefas, deberes e responsabilidades dun analista de seguridade de nivel asociado nun Centro de Operacións de Seguridade (SOC).

Dirixido a

Dirixido a profesionais de IT (enxeñeiros de Networking, administradores de rede, etc.) que queiran iniciarse no tema da ciberseguridade, aumentando o seu coñecemento e experiencia nesta área de demanda crecente e nos procedementos empregados nun Centro de Operacións de Seguridade -SOC. Débense destacar os escenarios prácticos do curso baseados nas distribucións de Kali Linux e Security Onion, que incorporan ferramentas especializadas en probas de penetración e auditoría, así como ferramentas de análise, clasificación e monitorización de alertas.

Para un maior aproveitamento do curso, recoméndase que o alumno teña coñecementos básicos de sistemas operativos Windows e / ou Linux, e un nivel de coñecementos previos en redes equivalente a ter completados os módulos 1 e 2 do curso CCNA R&S (conceptos básicos de redes, coñecemento de sistemas binarios e hexadecimais, conceptos básicos de programación e coñecemento de consultas básicas de SQL).

Perfil do docente

Instrutor/a acreditado/a polo programa CISCO NETACAD con máis de 5 anos de experiencia e certificado nesta especialidade.

DURACIÓN	80 horas
PROGRAMA	Programación 2020/21
MATRÍCULA	Gratuíta
METODOLOXÍA	Virtual
TIPO	CURSO
CERTIFICACIÓN OFICIAL	Sí
EXAME CERTIFICACIÓN	200-201 CBROPS

BENEFICIOS

CCNA CyberOps Associate

HORARIO	De luns a xoves de 16:30 a 20:30 horas.
PERIODO INSCRICIÓN	03/11/2020 - 04/11/2020
PROBA DE SELECCIÓN	17/11/2020, 16:30
LUGAR DE DOCENCIA	
Nº PRAZAS	16 (Mínimo 10)

Temario

- Módulo 1. Ciberseguridade: o Centro de Operacións de Seguridade - SOC
- Módulo 2. Sistema operativo Windows
- Módulo 3. Sistema operativo Linux
- Módulo 4. Protocolos e servizos de rede
- Módulo 5. Infraestrutura de rede
- Módulo 6. Principios de seguridade en rede
- Módulo 7. Ataques de rede: Unha inspección detallada
- Módulo 8. Protección da rede
- Módulo 9. Infraestrutura e Criptografía de clave pública
- Módulo 10. Análise e seguridade de dispositivos finais
- Módulo 11. Monitorización de seguridade
- Módulo 12. Análise de datos de intrusións
- Módulo 13. Resposta e xestión de incidencias