ESPE Innovativa

DESARROLLA
ESPECIALIZA
TRANSFIERE

Presentación del Curso

CCNA Cyber Ops

Unidad de
Capacitación y Certificación

Tabla de contenido

Campus Universitario-ESPE / Sangolquí - Ecuador
www.espe-innovativa.edu.ec
(02) 382-0800 Ext. 112 - 113 - 115 -116 - 126 -129 - 134
capacitacion-matriz@espe-innovativa.edu.ec

CCNA CYBER OPS

Descripción general

El presente curso se desarrollará en la modalidad online, el cual les permitirá a los participantes prepararse para detectar la ciberdelincuencia, el ciberespionaje y otras amenazas a la integridad de las redes

Este curso se encuentra organizado en trece capítulos, el cual ofrece una cobertura integral y completa de los temas de ciberseguridad en la red, y en los que aprenderá sobre:

- Criptografía
- Análisis de seguridad basado en host
- Monitoreo de seguridad
- Análisis forense de computadoras
- Métodos de ataque
- Informes y manejo de incidentes

El curso es apropiado para el público en general de muchos niveles de educación y tipos de instituciones, como escuelas secundarias, institutos de enseñanza superior, universidades, escuelas técnicas y de formación profesional, y centros comunitarios, que brindará numerosos aportes de experiencia práctica y desarrollo de destrezas profesionales.

También usted podrá desarrollar un pensamiento crítico y habilidades para resolver problemas mediante programas de monitoreo y detección de intrusión a la red.

Con esta capacitación le permitirá ser una de las pocas personas que conoce **cómo monitorear, detectar y responder a las amenazas de ciberseguridad.**

Público Objetivo

El curso de CCNA CYBER OPS está dirigido a todas las personas que estén interesadas en fortalecer sus conocimientos, habilidades y destrezas relacionadas con Tecnologías de la Información, Ingeniería Electrónica, Ingeniería en Sistemas o afines.

Objetivos de aprendizaje

Objetivo general:

- Comprender el rol de un centro de operaciones de seguridad (SOC) así como los lineamientos, herramientas y procedimientos para monitorear, detectar y contener ataques que se efectúen en una red.

Objetivos específicos:

- Describir las características de los delincuentes y héroes del ámbito de la ciberseguridad.
- Detallar los principios de confidencialidad, integridad y disponibilidad que se relacionan con los estados de datos y las contramedidas de ciberseguridad.
- Aprender las tácticas, las técnicas y los procedimientos utilizados por los delincuentes cibernéticos.
- Conocer cómo las tecnologías, los productos y los procedimientos se utilizan para proteger la confidencialidad, garantizar la integridad y proporcionar alta disponibilidad
- Entender la forma en que los profesionales de la ciberseguridad utilizan las tecnologías, los procesos y los procedimientos para defender todos los componentes de la red.
- Analizar el propósito de las leyes relacionadas con la ciberseguridad.

Duración

El curso tiene una duración de 70 horas.

Contenidos

CAPÍTULO 1: LA CIBERSEGURIDAD Y EL CENTRO DE OPERACIONES DE SEGURIDAD

1.1. El peligro
1.2. Soldados en la guerra contra la ciberdelincuencia

CAPÍTULO 2: SISTEMA OPERATIVO WINDOWS

2.1. Descripción General de Windows
2.2. Administración de Windows

CAPÍTULO 3: SISTEMA OPERATIVO LINUX

3.1. Descripción general de Linux
3.2. Administración de Linux
3.3. Hosts de Linux

CAPÍTULO 4: PROTOCOLOS Y SERVICIOS DE RED

4.1. Protocolos de red
4.2. Protocolo de Ethernet y protocolo de Internet IP

CAPÍTULO 11: MONITOREO DE LA SEGURIDAD

11.1. Tecnologías y protocolos
11.2. Archivos de registro

CAPÍTULO 12: ANÁLISIS DE DATOS DE INTRUSIONES

12.1. Evaluar alertas
12.2. Trabajar con datos de seguridad de la red
12.3. Informática forense digital

CAPÍTULO 13: RESPUESTA Y MANEJO ANTE INCIDENTES

13.1. Modelos de respuesta ante los incidentes
13.2. Manejo de incidentes

Competencias previas

Conocimientos: Es recomendable que los participantes de este curso, tengan conocimientos básicos de redes y sistemas operativos Windows y Linux

Habilidades o destrezas: Los participantes deben tener uno o más años de experiencia implementando y administrando soluciones de seguridad, una buena comprensión binaria y hexadecimal.

Valores: Los participantes deben establecer criterios éticos respecto al manejo y evaluación de los comportamientos observables de las personas.

Recursos

- Habilidades de navegación de PC y de Internet
- Tiempo para el desarrollo de las actividades de aprendizaje planificadas, así como para las actividades que realice de manera autónoma
- Disponer de una computadora, con sus periféricos bien configurados y funcionales (micrófono, parlantes y cámara).
- Disponer de una buena conexión a internet.
- Tener una cuenta de correo electrónico.

Aspectos metodológicos

- La capacitación se desarrollará en la modalidad online, para lo cual, se realizará un control de asistencia de los participantes en el horario establecido.
- Los contenidos del curso están a su disposición las 24 horas del día y los 7 días de la semana dentro del tiempo establecido para la duración del curso, por lo que, todos los participantes pueden organizar su propio horario de estudio.
- El curso es teórico – práctico, por cuanto el estudiante se apoyará en la plataforma de NetAcad, para lo cual se creará un nombre de usuario y contraseña para el acceso.
- Cada día se presentan contenidos que son estructurados con actividades individuales y colaborativas, recursos complementarios y herramientas que estarán disponibles en formatos para navegar.
- El seguimiento tutorial efectuado es constante y proactivo, lo que garantiza el éxito del proceso de aprendizaje.

Criterios de aprobación

El Programa de Capacitación CISCO que administra ESPE INNOVATIVA EP es de aprobación, para lo cual se aplican las siguientes evaluaciones académicas por cada uno de los módulos:

Exámenes electrónicos, estos exámenes pueden presentarlos en base a la planificación académica del instructor en el horario de las clases online o fuera de ellas.

Prácticas de laboratorio por cada capítulo y práctica final (skills).

- Examen Final Teórico
- Examen Final Práctico
- Examen Feedback (Satisfacción del Cliente)

Todas las evaluaciones son calificadas sobre 100 puntos, por lo que para aprobar cada uno de los módulos el participante debe obtener una nota promedio de todas las evaluaciones descritas de 80/100 puntos y registrar una asistencia mínima del 80% a las sesiones online.

Certificado

El participante que cumpla con los criterios de aprobación, recibirá un certificado digital con el aval de la Academy Networking CISCO.

Perfil del Facilitador

Formación académica

Pregrado:

Título de grado de tercer nivel en carreras como Ingeniería Electrónica, Sistemas, Tecnologías de la Información o afines.

Posgrado (De preferencia):

- Redes y Telecomunicaciones
- Gerencia de Sistemas y Tecnología Empresarial
- Gestión de la Seguridad de la Información
- Seguridad Informática y Hacking Ético

Otros:

- Certificación activa de CCNA CYBER OPS.

Experiencia relacionada:

- Desempeño profesional en el área de su especialidad
- Docencia en áreas relacionadas a su especialidad
- Instructor de cursos CCNA en la Academy Networking Cisco