CyberOPS Associate (CA)
Notas de publicación

Última actualización: diciembre, 21, 2020

Propósito

El curso CyberOps Associate está diseñado para los estudiantes de Cisco Networking Academy® que buscan destrezas de analistas de seguridad de nivel básico orientadas a su carrera. Los estudiantes objetivo de este curso incluyen individuos inscritos en programas de grado tecnológico en instituciones de educación superior y profesionales de TI que buscan aspirar a un puesto profesional en un centro de operaciones de seguridad (Security Operation Center, SOC). Los estudiantes en este curso están expuestos a todo el conocimiento básico necesario para detectar, analizar y descartar las amenazas básicas de ciberseguridad mediante herramientas comunes de código abierto. Este curso se alinea con la certificación Cisco Certified CyberOps Associate (CBROPS). Los candidatos deben aprobar el examen CBROPS 200-201 para lograr la certificación Cisco Certified CyberOps Associate.

Al finalizar este curso, los estudiantes serán capaces de realizar lo siguiente:

- Instalar máquinas virtuales para crear un entorno seguro para la implementación y el análisis de los eventos de amenazas de ciberseguridad.
- Explicar el rol del Analista de operaciones de ciberseguridad en la empresa.
- Explicar las funciones y las características del Sistema operativo Windows necesarias para el análisis de ciberseguridad.
- Explicar las funciones y las características del Sistema operativo Linux.
- Analizar el funcionamiento de los protocolos y servicios de red.
- Explicar el funcionamiento de la infraestructura de red.
- Clasificar los diversos tipos de ataques a la red.
- Emplear herramientas de monitoreo de redes para identificar ataques a servicios y protocolos de red.
- Explicar cómo evitar el acceso malicioso a las redes informáticas, los hosts y los datos.
- Explicar el impacto de la criptografía en el monitoreo de seguridad de red.
- Explicar cómo investigar los ataques y las vulnerabilidades de los terminales.
- Evaluar alertas de seguridad de la red.
- Analizar datos de intrusiones en la red para identificar vulnerabilidades y hosts comprometidos.

- Aplicar modelos de respuesta ante incidentes para gestionar incidentes de seguridad en la red.

Este curso contiene numerosas oportunidades para practicar y evaluar las habilidades de los estudiantes a través de diversos tipos de evaluaciones, prácticas de laboratorio y actividades de Packet Tracer.

En estas notas, se proporciona información detallada sobre esta versión, incluidos el contenido del currículo, los problemas comunes, e información técnica.

Este curso de 70 horas, dirigido por un instructor, incluye videos, Prácticas de Laboratorio, Actividades de Packet Tracer, Cuestionarios del Módulo, Exámenes del Módulo, una Evaluación de Habilidades en Laboratorio y Exámenes finales.

Contenido de la versión

Tabla 1. Contenido incluido en la versión de Cyber Operations Associate

Componente	Descripción
Contenido de educación en línea (online)	28 módulos
Videos	30 videos
Prácticas de laboratorio	46 actividades prácticas de laboratorio y prácticas de laboratorio escritas
Actividades de Packet Tracer	6 actividades de Packet Tracer. Actividades de simulación y modelado diseñadas para la exploración, adquisición, refuerzo y expansión de habilidades, la versión de Packet Tracer debe ser 7.3.0 o superior.
Actividades interactivas	9 actividades interactivas
Verifique su conocimiento	46 Actividades VSC (Verifique su conocimiento) Son cuestionarios por tema en línea (online) de autodiagnóstico para ayudar a los aprendices a medir la comprensión del contenido. Las actividades VSC están diseñadas para permitir a los estudiantes determinar si están comprendiendo el contenido y pueden continuar, o si necesitan repasar. Las actividades VSC ***no afectan*** las calificaciones de los estudiantes.
Cuestionarios de módulo	28 Cuestionarios del Módulo Evaluaciones activadas por el instructor que evalúa el contenido de múltiples módulos. Estas evaluaciones proporcionan a los aprendices la oportunidad de aplicar y validar el conocimiento aprendido.

Grupo de exámenes de módulo	9 grupos de exámenes de módulo Estas evaluaciones proporcionan a los alumnos la oportunidad de aplicar y validar el conocimiento aprendido a lo largo del curso.
Examen Final de Práctica	1 examen final de práctica No asegurado. No dinámico.
Examen final dinámico asegurado	1 Examen final dinámico con Activación asegurada Las variables en el diseño del examen permiten a un instructor administrar exámenes únicos a cada estudiante y evaluar el aprendizaje de cada estudiante individualmente. Con activación asegurada, la vista previa y revisión de elementos de evaluación individuales se deshabilita para mejorar la validez y la seguridad de esta evaluación sumativa. Se proporciona a los instructores un resumen visual de cómo los estudiantes se desempeñaron frente a las aptitudes descritas para el curso.
Examen de práctica de certificación 200-201	1 Examen de práctica de certificación No asegurado. Dinámico.
Actividad de laboratorio de evaluación de habilidades	1
Comentarios finales del curso	1 encuesta de fin de curso para brindar comentarios sobre el curso.
Accesibilidad	La nueva interfaz de usuario (User Interface) cumple con las pautas WCAG 2.1 Nivel AA. Todas las páginas contienen texto con opciones de accesibilidad y transcripciones muy descriptivas del material multimedia. Todos los archivos PDF del currículo ofrecen opciones de accesibilidad. Los videos tienen la opción de activar subtítulos (CC). La interfaz de usuario tiene la funcionalidad de lectura por voz que se puede activar con el teclado.
Certificado de finalización	Se requiere completar exitosamente la evaluación final del curso y la encuesta final del curso para recibir el Certificado de finalización.

Lista de equipos (herramientas)

Este curso utiliza dos máquinas virtuales (VM) para la mayoría de prácticas de laboratorio. Solo se requiere una VM a la vez en cualquier práctica de laboratorio que utilice una VM. Las computadoras del estudiante o del laboratorio deben cumplir con los siguientes requisitos:

- Computadora (host) con procesador de 64 bits, al menos 8 GB de RAM y 45 GB de espacio libre en disco (consulte este enlace para determinar si la computadora (host) tiene un procesador de 64 bits: https://www.computerhope.com/issues/ch001121.htm)
- Versión más reciente de Oracle VirtualBox: http://www.oracle.com/technetwork/server-storage/virtualbox/downloads/index.html
- Conexión a Internet
- Las dos máquinas virtuales mencionadas en la siguiente tabla:

Tabla 2. Requisitos de las máquinas virtuales

Máquina virtual	RAM	Espacio en disco	Usuario	Contraseña
VM CyberOps Workstation	1 GB	20 GB	analyst	cyberops
VM Security Onion	Mínimo 4 GB (Se recomiendan 8 GB)	20 GB	analyst	cyberops

Problemas comunes

Tabla 3. Problemas comunes

Problemas y avisos comunes	Descripción
Texto en inglés	En los módulos, hay texto en inglés estadounidense intercalado.
Subtítulos (CC)	Use el enlace de video externo si experimenta problemas con los videos adjuntos en el material.
Programa Packet Tracer	Debe usar Packet Tracer versión 7.3.0 para cargar las actividades de Packet Tracer contenidas en este curso y en las evaluaciones.
Desafío de habilidades de CyberOps v1.1	Este curso también contiene las VM (máquinas virtuales) y guías de instalación para ejecutar el juego opcional "Desafío de habilidades de CyberOps" desarrollado con el curso CCNA CyberOps v1.1. El juego y las VM no se alinean completamente con el curso o certificación de CyberOps Associate, pero ofrecen oportunidades para divertirse y practicar con las habilidades y conocimientos fundamentales de ciberseguridad. Los archivos se utilizan tal y como están y no se han actualizado. Consulte la "Respuesta a preguntas frecuentes" proporcionada en los Recursos del instructor para obtener más información sobre el juego.

Resumen del curso

Tabla 4. Resumen del curso

Módulo	Título
1	Introducción al curso/ El peligro
2	Combatientes en la guerra contra el cibercrimen
3	El Sistema operativo Windows
4	Descripción general de Linux
5	Protocolos de red
6	Ethernet y Protocolo de Internet (IP)
7	Principios de la seguridad de red
8	Protocolo de resolución de direcciones
9	Capa de transporte
10	Servicios de red
11	Dispositivos de comunicación de red
12	Infraestructura de seguridad de redes
13	Los atacantes y sus herramientas
14	Amenazas y ataques comunes
15	Observación de la operación de red
16	Ataque a los fundamentos
17	Atacando lo que hacemos
18	Comprendiendo qué es defensa
19	Control de acceso
20	Inteligencia contra amenazas
21	Criptografía
22	Protección de terminales
23	Evaluación de vulnerabilidades en terminales
24	Tecnologías y protocolos
25	Datos de seguridad de la red
26	Evaluación de alertas
27	Trabajo con datos de seguridad de la red
28	Análisis y respuesta de incidentes e informática forense digital

Actualizaciones en CyberOps Associate

Esta es la primera versión del curso CyberOps Associate; por lo tanto, no hay actualizaciones.

Asistencia técnica

Para obtener asistencia general con problemas del currículo, el aula o el programa, por favor comunicarse con Networking Academy™ Support Desk, iniciando sesión en netacad.com ™ y haciendo clic en el signo de interrogación de asistencia ténica (?)..