Alcance y secuencia de CyberOps Associate (CA) v1.0

Última actualización: diciembre, 21, 2020

Introducción

Las organizaciones de hoy en día tienen el desafío de detectar rápidamente las intrusiones a la ciberseguridad y de responder eficazmente a los incidentes de seguridad. Los equipos de personal en los centros de operaciones de seguridad (SOC) están atentos a los sistemas de seguridad y protegen a las organizaciones detectando y respondiendo a los ataques y las amenazas de ciberseguridad. CyberOps Associate prepara a los candidatos para que comiencen a trabajar como analistas de ciberseguridad de nivel de asociado dentro de los centros de operaciones de seguridad.

Público al que está destinado

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 de destino incluyen individuos inscritos en programas de grado de tecnología en instituciones de educación superior y profesionales de TI que buscan seguir una carrera en el centro de operaciones de seguridad (SOC). Los estudiantes en este curso están expuestos a todo el conocimiento básico necesario para detectar, analizar y escalar las amenazas básicas de ciberseguridad mediante herramientas comunes de recursos abiertos.

Requisitos previos

Los estudiantes de CyberOps Associate deben tener las siguientes destrezas y conocimientos:

- Destrezas de navegación en Internet y PC
- Conceptos básicos de los sistemas Windows y Linux
- Comprensión básica de las redes informáticas (nivel CCNA ITN)
- Comprensión binaria y hexadecimal
- Familiaridad con Cisco Packet Tracer

Certificaciones a las que se aspira

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. El examen CBROPS evalúa los conocimientos y las destrezas del candidato relacionados con los conceptos de seguridad, el monitoreo de seguridad, el análisis basado en hosts, el análisis de intrusiones en la red, y las políticas y los procedimientos de seguridad.

Descripción del curso

El curso tiene muchas características que ayudan a los estudiantes a comprender estos conceptos:

- El curso consta de veintiocho (28) módulos. Cada módulo se compone de temas.

- Los módulos acentúan el pensamiento crítico, la resolución de problemas, la colaboración y la aplicación práctica de destrezas.
- Cada módulo contiene prácticas y evaluaciones de la comprensión, como prácticas de laboratorio o una actividad de Packet Tracer. Estas actividades a nivel del módulo proporcionan comentarios y están diseñadas para indicar el dominio de las destrezas del estudiante necesarias para el curso. Los estudiantes pueden asegurar su nivel de comprensión mucho antes de tomar un cuestionario o examen calificado.
- Algunos temas pueden contener un cuestionario interactivo de verificación de la comprensión o alguna otra forma de evaluación de la comprensión, como una práctica de laboratorio o Packet Tracer. Las evaluaciones a nivel del tema están diseñadas para indicar a los estudiantes si tienen una buena comprensión del contenido del tema o necesitan revisarlo antes de continuar. Los estudiantes pueden asegurar su nivel de comprensión mucho antes de tomar un cuestionario o examen calificado. Los cuestionarios de verificación de la comprensión no afectan la calificación general del estudiante.
- El contenido multimedia enriquecido, que incluye actividades interactivas, videos y cuestionarios, aborda diversos estilos de aprendizaje, ayuda a estimular la educación e incrementa la retención de conocimientos.
- Los entornos virtuales simulan escenarios de amenazas de ciberseguridad en el mundo real y generan oportunidades de monitoreo, análisis y resolución de la seguridad.
- Las prácticas de laboratorio ayudan a los estudiantes a desarrollar un pensamiento crítico y destrezas de resolución de problemas complejos.
- Los exámenes innovadores proporcionan un panorama inmediato que sirve de apoyo a la evaluación del conocimiento y las destrezas adquiridas.
- Los conceptos técnicos se explican en el idioma adecuado para los estudiantes de todos los niveles y las actividades interactivas integradas dividen la lectura del contenido y ayudan a reforzar la comprensión.
- El currículo incentiva a los estudiantes a considerar la formación adicional en TI y, también, enfatiza las destrezas y la experiencia práctica aplicadas.
- Las actividades de Cisco Packet Tracer están diseñadas para utilizarse con Packet Tracer 7.3.0 o posterior.

Objetivos del curso

CyberOps Associate v1.0 abarca las destrezas y los conocimientos necesarios para asumir con éxito las tareas, los deberes y las responsabilidades de los analistas en ciberseguridad de nivel del asociado que trabajan en los centros de operaciones de seguridad (SOC).

Cuando los estudiantes finalicen *CyberOps Associate v1.0*, serán capaces de realizar las siguientes tareas:

- 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 la seguridad de redes.
- Explicar cómo investigar los ataques y las vulnerabilidades de los terminales.
- Evaluar alertas de seguridad de la red.
- Analizar datos de intrusiones en redes para identificar hosts afectados.
- Aplicar modelos de respuesta ante incidentes para administrar los incidentes relacionados con la seguridad de la red.

Requisitos de equipos para laboratorio

Este curso no requiere ningún equipo físico que no sea la PC de laboratorio del estudiante. Utiliza distintas máquinas virtuales (VM) para crear la experiencia de laboratorio.

Paquete de equipos de línea de base:

- PC: requisitos mínimos del sistema
  - CPU: Intel Pentium 4 de 2,53 GHz o equivalente con soporte de virtualización
  - Sistemas operativos: Microsoft Windows, Linux y Mac OS
  - Procesador de 64 bits
  - RAM: 8 GB
  - Almacenamiento: 40 GB de espacio en disco libre
  - Resolución de pantalla: 1024 x 768
  - Fuentes de idioma compatibles con la codificación Unicode (si se ve en otros idiomas que no sean el inglés)
  - Últimos controladores de tarjetas de video y actualizaciones del sistema operativo
- Conexión a Internet para PC de laboratorio y del estudiante

Software de PC para estudiantes:

- Oracle VM VirtualBox Manager (versión 6.1 o posterior)
- VM CyberOps Workstation
  - Descargable desde el curso
  - Requiere 1 GB de RAM, 20 GB de espacio en disco
- VM Security Onion
  - Descargable desde el curso
  - Requiere 4 GB de RAM (mínimo), 8 GB de RAM (muy recomendable), 20 GB de espacio en disco

Esquema de CyberOps Associate

A continuación, se enumeran el conjunto actual de módulos y sus competencias asociadas descritas para este curso. Cada módulo es una unidad de aprendizaje integrada que consta de contenido, actividades y evaluaciones que se dirigen a un conjunto específico de competencias. El tamaño del módulo dependerá de la profundidad de los conocimientos y las destrezas necesarias para dominar la competencia. Algunos módulos se consideran fundacionales debido a que los dispositivos presentados, mientras no se evalúan, activan el aprendizaje de los conceptos cubiertos en el examen de certificación CBROPS.

Tabla 1. Esquema del curso CyberOps Associate v1.0

Módulo/Temas	Metas/Objetivos
Módulo 1. Peligro	**Explique por qué se atacan las redes y los datos.**
1.0 Introducción	Breve introducción al curso y al primer módulo.
1.1 Historias de guerra	Características generales de los incidentes de ciberseguridad.
1.2 Actores maliciosos	Explique las motivaciones de los actores maliciosos detrás de incidentes de seguridad específicos.
1.3 Impacto de la amenaza	Explique el impacto potencial de los ataques de seguridad de la red.
1.4 Resumen del peligro	Breve resumen y cuestionario del módulo.
Módulo 2. Combatientes en la guerra contra la ciberdelincuencia	**Explique cómo prepararse para una carrera profesional en operaciones de ciberseguridad.**
2.0 Introducción	Introducción al módulo.
2.1 El centro de operaciones de seguridad moderno	Explique la misión del centro de operaciones de seguridad.
2.2 Cómo convertirse en defensor	Describa los recursos disponibles para prepararse para una carrera en operaciones de ciberseguridad.
2.3 Resumen de Combatientes en la guerra contra la ciberdelincuencia	Breve resumen y cuestionario del módulo.
Módulo 3. Sistema operativo Windows	**Explique las características de seguridad del sistema operativo Windows.**
3.0 Introducción	Introducción al módulo.
3.1 Historia de Windows	Describa la historia del sistema operativo Windows.
3.2 Arquitectura y operaciones de Windows	Explique la arquitectura de Windows y su funcionamiento.
3.3 Configuración y monitoreo de Windows	Explique cómo configurar y monitorear Windows.
3.4 Seguridad de Windows	Explique cómo puede mantenerse seguro Windows.
3.5 Resumen de Sistema operativo Windows	Breve resumen y cuestionario del módulo.
Módulo 4. Descripción general de Linux	**Implemente la seguridad básica de Linux.**
4.0 Introducción	Introducción al módulo.
4.1 Conceptos básicos de Linux	Explique por qué las destrezas de Linux son esenciales para la supervisión e investigación de la seguridad de la red.
4.2 Uso del shell de Linux	Utilice el shell de Linux para manipular archivos de texto.
4.3 Clientes y servidores de Linux	Explique cómo funcionan las redes cliente-servidor.
4.4 Administración básica del servidor	Explique cómo un administrador de Linux localiza y manipula los archivos de registro de seguridad.

Módulo/Temas	Metas/Objetivos
4.5 Sistema de archivos de Linux	Administre los permisos y el sistema de archivos de Linux.
4.6 Trabajo con la GUI de Linux	Explique los componentes básicos de la GUI de Linux.
4.7 Trabajo con el host de Linux	Utilice herramientas para detectar malware en un host de Linux.
4.8 Resumen de Nociones básicas de Linux	Breve resumen y cuestionario del módulo.
Módulo 5. Protocolos de red	**Explique cómo los protocolos habilitan las operaciones de red.**
5.0 Introducción	Introducción al módulo.
5.1 Proceso de comunicación en red	Explique las operaciones básicas de las comunicaciones en red de datos.
5.2 Protocolos de comunicación	Explique cómo los protocolos habilitan las operaciones de red.
5.3 Encapsulación de datos	Explique la forma en que la encapsulación de datos permite que se transporten a través de la red.
5.4 Resumen de Protocolos de red	Breve resumen y cuestionario del módulo.
Módulo 6. Protocolo de Internet (IP) y Ethernet	**Explique cómo los protocolos de Internet (IP) y Ethernet permiten la comunicación en red.**
6.0 Introducción	Introducción al módulo.
6.1 Ethernet	Explique cómo Ethernet permite la comunicación en red.
6.2 IPv4	Explique cómo el IPv4 permite la comunicación en red.
6.3 Fundamentos de las direcciones IP	Explique cómo las direcciones IP permiten la comunicación en red.
6.4 Tipos de direcciones IPv4	Explique el tipo de dirección IPv4 que permite la comunicación en red.
6.5 Gateway predeterminado	Explique cómo el gateway predeterminado permite la comunicación en red.
6.6 Longitud de prefijo IPv6	Explique cómo el IPv6 permite la comunicación en red.
6.7 Resumen de Ethernet y protocolo de IP	Breve resumen y cuestionario del módulo.
Módulo 7. Principios de la seguridad de red	**Verificación de la conectividad.**
7.0 Introducción	Introducción al módulo.
7.1 ICMP	Explique la forma en que se usa ICMP para probar la conectividad de red.
7.2 Utilidades Ping y Traceroute	Utilice las herramientas de Windows, Ping y Traceroute para verificar la conectividad de la red.
7.3 Resumen de Verificación de conectividad	Breve resumen y cuestionario del módulo.
Módulo 8. Protocolo de resolución de direcciones	**Analice las PDU del protocolo de resolución de direcciones en la red.**

Módulo/Temas	Metas/Objetivos
8.0 Introducción	Introducción al módulo.
8.1 MAC e IP	Compare las funciones de la dirección MAC y la dirección IP.
8.2 ARP	Analice la ARP examinando las tramas de Ethernet.
8.3 Problemas de la ARP	Explique cómo las solicitudes de ARP afectan el rendimiento de la red y el host.
8.4 Resumen de Protocolo de resolución de direcciones	Breve resumen y cuestionario del módulo.
Módulo 9. Capa de transporte	**Explique cómo los protocolos de capa de transporte habilitan la funcionalidad de la red.**
9.0 Introducción	Introducción al módulo.
9.1 Características de la capa de transporte	Explique cómo permiten las comunicaciones en red los protocolos de la capa de transporte.
9.2 Establecimiento de la sesión de capa de transporte	Explique cómo la capa de transporte establece sesiones de comunicación.
9.3 Confiabilidad de la capa de transporte	Explique cómo la capa de transporte establece comunicaciones confiables.
9.4 Resumen de Capa de transporte	Breve resumen y cuestionario del módulo.
Módulo 10. Servicios de red	**Explique cómo los servicios de red habilitan la funcionalidad de la red.**
10.0 Introducción	Introducción al módulo.
10.1 DHCP	Explique cómo los servicios de DHCP habilitan la funcionalidad de la red.
10.2 DNS	Explique cómo los servicios de DNS habilitan la funcionalidad de la red.
10.3 NAT	Explique cómo los servicios de NAT habilitan la funcionalidad de la red.
10.4 Servicios de uso compartido y transferencia de archivos	Explique cómo los servicios de transferencia de archivos habilitan la funcionalidad de la red.
10.5 Correo electrónico	Explique cómo los servicios de correo electrónico habilitan la funcionalidad de la red.
10.6 HTTP	Explique cómo los servicios de HTTP habilitan la funcionalidad de la red.
10.7 Resumen de Servicios de red	Breve resumen y cuestionario del módulo.
Módulo 11. Dispositivos de comunicación por redes	**Explique cómo los dispositivos de red permiten la comunicación por redes cableadas e inalámbricas.**
11.0 Introducción	Introducción al módulo.

Módulo/Temas	Metas/Objetivos
11.1 Dispositivos de red	Explique cómo los dispositivos de red permiten la comunicación por redes.
11.2 Comunicaciones inalámbricas	Explique cómo los dispositivos de red inalámbrica permiten la comunicación por redes.
11.3 Resumen de Dispositivos de comunicación por redes	Breve resumen y cuestionario del módulo.
Módulo 12. Infraestructura de seguridad de la red	**Explique cómo se utilizan los dispositivos y los servicios de red para mejorar la seguridad de la red.**
12.0 Introducción	Introducción al módulo.
12.1 Topologías de red	Explique cómo los diseños de red influyen en el flujo de tráfico a través de la red.
12.2 Dispositivos de seguridad	Explique cómo se emplean los dispositivos para reforzar la seguridad de las redes.
12.3 Servicios de seguridad	Explique cómo los servicios de red mejoran la seguridad de las redes.
12.4 Resumen de Infraestructura de seguridad de la red	Breve resumen de este módulo.
Módulo 13. Los atacantes y sus herramientas	**Explique cómo se atacan las redes.**
13.0 Introducción	Introducción al módulo.
13.1 ¿Quién está atacando nuestra red?	Explique cómo han evolucionado las amenazas de la red.
13.2 Herramientas de los actores maliciosos	Describa los diferentes tipos de herramientas de ataque utilizadas por los actores maliciosos.
13.3 Resumen de Los atacantes y sus herramientas	Breve resumen y cuestionario del módulo.
Módulo 14. Amenazas y ataques comunes	**Explique los diferentes tipos de amenazas y ataques.**
14.0 Introducción	Introducción al módulo.
14.1 Malware	Describa los tipos de malware.
14.2 Ataques de red comunes: reconocimiento, acceso e ingeniería social	Explique los ataques de reconocimiento, acceso e ingeniería social.
14.3 Ataques de red: denegación de servicio, desbordamientos del búfer y evasión	Explique la denegación de servicio, el desbordamiento del búfer y los ataques de evasión.
14.4 Resumen de Amenazas y ataques comunes	Breve resumen y cuestionario del módulo.
Módulo 15. Observación de la operación de red	**Explique el monitoreo del tráfico de red.**
15.0 Introducción	Introducción al módulo.
15.1 Introducción al monitoreo de la red	Explique la importancia del monitoreo de la red.
15.2 Introducción a las herramientas de monitoreo de la	Explique cómo se realiza el monitoreo de la red.

Módulo/Temas	Metas/Objetivos
red	
15.3 Resumen de Monitoreo de red y herramientas	Breve resumen y cuestionario del módulo.
Módulo 16. Ataque a las bases	**Explique cómo las vulnerabilidades de TCP/IP permiten los ataques a las redes.**
16.0 Introducción	Introducción al módulo.
16.1 Detalles de la PDU del IP	Explique la estructura de encabezado IPv4 e IPv6.
16.2 Vulnerabilidades del IP	Explique cómo las vulnerabilidades del IP permiten los ataques a las redes.
16.3 Vulnerabilidades del TCP y el UDP	Explique cómo las vulnerabilidades del TCP y el UDP permiten los ataques a las redes.
16.4 Resumen de Ataque a las bases	Breve resumen y cuestionario del módulo.
Módulo 17. Un ataque a lo que hacemos	**Explique cómo las aplicaciones y los servicios de red comunes son vulnerables a los ataques.**
17.0 Introducción	Introducción al módulo.
17.1 Servicios IP	Explique las vulnerabilidades del servicio IP.
17.2 Servicios de la empresa	Explique cómo las vulnerabilidades de las aplicaciones de red permiten los ataques a las redes.
17.3 Resumen de Un ataque a lo que hacemos	Breve resumen y cuestionario del módulo.
Módulo 18. ¿Qué es la defensa?	**Explique los enfoques para la defensa de la seguridad de la red.**
18.0 Introducción	Introducción al módulo.
18.1 Defensa en profundidad	Explique cómo se utiliza la estrategia de defensa en profundidad para proteger las redes.
18.2 Políticas, regulaciones y estándares de seguridad	Explique las políticas, las regulaciones y los estándares de seguridad.
18.3 Resumen de ¿Qué es la defensa?	Breve resumen y cuestionario del módulo.
Módulo 19. Control de acceso	**Explique el control de acceso como método de protección de la red.**
19.0 Introducción	Introducción al módulo.
19.1 Conceptos del control de acceso	Explique cómo el control de acceso protege los datos de la red.
19.2 Uso y funcionamiento de AAA	Explique cómo se utiliza AAA para controlar el acceso a la red.
19.3 Resumen de Control de acceso	Breve resumen y cuestionario del módulo.
Módulo 20. Inteligencia de amenazas	**Utilice varias fuentes de inteligencia para localizar las amenazas de seguridad actuales.**
20.0 Introducción	Introducción al módulo.

Módulo/Temas	Metas/Objetivos
20.1 Fuentes de información	Describa las fuentes de información utilizadas para comunicar las amenazas emergentes de seguridad de la red.
20.2 Servicios de inteligencia de amenazas	Describa varios servicios de inteligencia de amenazas.
20.3 Resumen de Inteligencia de amenazas	Breve resumen y cuestionario del módulo.
Módulo 21. Criptografía	**Explique cómo la infraestructura de clave pública admite la seguridad de la red.**
21.0 Introducción	Introducción al módulo.
21.1 Integridad y autenticidad	Explique el rol de la criptografía para garantizar los datos de integridad y autenticidad.
21.2 Confidencialidad	Explique cómo los enfoques criptográficos mejoran la confidencialidad de los datos.
21.3 Criptografía de clave pública	Explique la criptografía de clave pública.
21.4 Autoridades y sistema de confianza de la PKI	Explique cómo funciona la infraestructura de clave pública.
21.5 Aplicaciones e impacto de la criptografía	Explique cómo el uso de la criptografía afecta las operaciones de ciberseguridad.
21.6 Resumen de Criptografía	Breve resumen de este módulo.
Módulo 22. Protección de terminales	**Explique cómo un sitio web de análisis de malware genera un informe de análisis de malware.**
22.0 Introducción	Introducción al módulo.
22.1 Protección antimalware	Explique los métodos para mitigar el malware.
22.2 Prevención de intrusiones basada en hosts	Explique las entradas de registro de IPS/IDS basadas en hosts.
22.3 Seguridad de las aplicaciones	Explique cómo se usa el entorno de ejecución seguro (sandbox) para analizar el malware.
22.4 Resumen de Protección de terminales	Breve resumen y cuestionario del módulo.
Módulo 23. Evaluación de vulnerabilidades en terminales	**Explique cómo se evalúan y administran las vulnerabilidades de los terminales.**
23.0 Introducción	Introducción al módulo.
23.1 Perfiles de redes y servidores	Explique el valor de la generación de perfiles de redes y servidores.
23.2 Sistema de puntuación de vulnerabilidades comunes (CVSS)	Explique cómo se utilizan los informes del CVSS para describir las vulnerabilidades de seguridad.
23.3 Administrador de dispositivos de seguridad	Explique cómo se utilizan las técnicas de administración segura de dispositivos para proteger los datos y los recursos.
23.4 Sistemas de administración de seguridad de la información	Explique cómo se utilizan los sistemas de administración de seguridad de la información para proteger los recursos.

Módulo/Temas	Metas/Objetivos
23.5 Resumen de Evaluación de vulnerabilidades en terminales	Breve resumen y cuestionario del módulo.
Módulo 24. Tecnologías y protocolos	**Explique cómo las tecnologías de seguridad afectan el monitoreo de la seguridad.**
24.0 Introducción	Introducción al módulo.
24.1 Protocolos comunes de monitoreo	Explique el comportamiento de los protocolos de red comunes en el contexto del monitoreo de la seguridad.
24.2 Tecnologías de seguridad	Explique cómo las tecnologías de seguridad afectan la capacidad de supervisar los protocolos de red comunes.
24.3 Resumen de Tecnologías y protocolos	Breve resumen y cuestionario del módulo.
Módulo 25. Datos de seguridad de la red	**Explique los tipos de datos de seguridad de la red utilizados en el monitoreo de la seguridad.**
25.0 Introducción	Introducción al módulo.
25.1 Tipos de datos de seguridad	Describa los tipos de datos utilizados en el monitoreo de la seguridad.
25.2 Registros de terminales	Describa los elementos del archivo de registro de un terminal.
25.3 Registros de red	Describa los elementos del archivo de registro de un dispositivo de red.
25.4 Resumen de Datos de seguridad de la red	Breve resumen y cuestionario del módulo.
Módulo 26. Evaluación de alertas	**Explique el proceso de evaluación de alertas.**
26.0 Introducción	Introducción al módulo.
26.1 Fuente de alertas	Identifique la estructura de alertas.
26.2 Descripción general de la evaluación de alertas	Explique cómo se clasifican las alertas.
26.3 Resumen de evaluación de alertas	Breve resumen y cuestionario del módulo.
Módulo 27. Trabajo con datos de seguridad de la red	**Interprete los datos para determinar el origen de una alerta.**
27.0 Introducción	Introducción al módulo.
27.1 Plataforma de datos común	Explique cómo se preparan los datos para el uso en el sistema de monitoreo de seguridad de la red (NSM).
27.2 Investigación de datos de la red	Utilice herramientas de seguridad de Onion para investigar los eventos de seguridad de la red.
27.3 Cómo mejorar el trabajo del analista de ciberseguridad	Describa las herramientas de monitoreo de red que mejoran la administración del flujo de trabajo.
27.4 Resumen de Trabajo con datos de seguridad de la red	Breve resumen y cuestionario del módulo.

Módulo/Temas	Metas/Objetivos
Módulo 28. Análisis y respuesta de incidentes e informática forense digital	**Explique cómo CyberOps Associate responde a los incidentes de ciberseguridad.**
28.0 Introducción	Introducción al módulo.
28.1 Manejo de evidencia y atribución del ataque	Explique el rol de los procesos forenses digitales.
28.2 Cyber Kill Chain	Identifique los pasos en Cyber Kill Chain.
28.3 Análisis del modelo de diamante de las intrusiones	Clasifique un evento de intrusión mediante el modelo de diamante.
28.4 Respuesta ante incidentes	Aplique los procedimientos de manejo de incidentes NIST 800-61r2 para una situación de incidentes determinada.
28.5 Resumen de Análisis y respuesta de incidentes e informática forense digital	Breve resumen de este módulo.
28.6 ¡Prepárese para el examen e inicie su carrera profesional!	Preparación para la certificación, vales de descuento y otros recursos profesionales.

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV Amsterdam,
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**