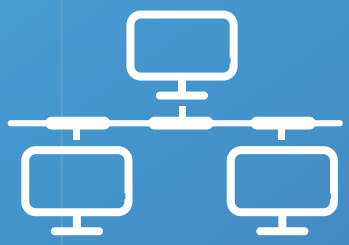
NEXUS ACADEMY

# PROGRAMA DEL CURSO



PROGRAMA DE CERTIFICACIÓN

## CISCO CERTIFIED CYBEROPS ASSOCIATE

Versión 1.1

CISCO

CONTENIDO

PROGRAMA DE CERTIFICACIÓN

# CISCO CERTIFIED CYBEROPS ASSOCIATE

Versión 1.1

# Sumilla

El curso de CYBEROPS ASSOCIATE prepara a los participantes para que comiencen a desarrollar una carrera como analista de ciberseguridad a nivel de asociado, dentro de centros de operaciones de seguridad.

Este curso desarrolla tus habilidades para rendir el examen de certificación CISCO 200-201 CBROPS válido para obtener el grado de asociado de CYBEROPS. Es importante tener en cuenta que, actualmente, las organizaciones afrontan los desafíos de detectar rápidamente las amenazas a la ciberseguridad y responder con eficiencia ante los incidentes de seguridad.

Los equipos de profesionales de los Centros de Operaciones de Seguridad (SOC, Security Operations Centers) vigilan atentamente los sistemas de seguridad para proteger sus organizaciones, detectando y respondiendo antes los exploits y las amenazas de ciberseguridad.

# Objetivos

Al finalizar el curso CYBEROPS ASSOCIATE, los estudiantes estarán en la capacidad de:

- Explicar el rol del analista de las Operaciones de Ciberseguridad en la empresa.
- Explicar las características de los sistemas operativos Windows y Linux desde la perspectiva de la ciberseguridad
- Analizar las operaciones de los protocolos y servicios de red
- Explicar las operaciones de la infraestructura de red
- Clasificar los ataques de red y usar herramientas para monitorear su seguridad
- Prevenir accesos maliciosos a la red, los hosts y los datos
- Explicar el impacto de la criptografía en la seguridad de la red
- Investigar las vulnerabilidades de los endpoints
- Analizar e identificar los sectores comprometidos por una intrusión en la red
- Aplicar modelos de respuesta a los ataques de red

# *Propósito*

El curso CYBEROPS ASSOCIATE de Cisco desarrolla aprendizajes en las siguientes áreas:

**Conceptos de seguridad**
Describe los conceptos y términos básicos de ciberseguridad y establece mecanismos para estimar el impacto derivado de las vulnerabilidades.

**Monitoreo de la seguridad**
Identifica los mecanismos de monitoreo que se pueden desplegar para monitorear la seguridad de la red. Define los distintos tipos de ataques y las formas de evitarlos o controlarlos.

**Análisis de la seguridad a nivel de hosts**
Describe las tecnologías que se usan para reforzar la seguridad de los endpoints y describe los componentes más importantes de dos de los sistemas operativos más comunes para endpoints del tipo desktop: Windows y Linux.

**Análisis de las intrusiones de red**
Desarrolla una metodología para analizar una intrusión de red enfocándose en el análisis de datos recopilados desde los distintos elementos de seguridad instalados.

**Políticas de seguridad y procedimientos**
Define los elementos y métodos que permiten diseñar una política de seguridad y los procedimientos que la complementan para desplegar una red segura.

# Temario

| Módulo / Tópicos | Metas / Objetivos |
|---|---|
| 1. El peligro | Explicar por qué son atacadas las redes y los datos |
| Historias de Guerra | Características destacadas de los incidentes de seguridad |
| Actores de una amenaza | Explicar las motivaciones detrás de los ataques a redes |
| Impacto de la amenaza | Explicar el impacto potencial de los ataques a las redes |
| 2. Luchadores en la guerra contra el ciber-crimen | Explicar por qué son atacadas las redes y los datos |
| El centro de operaciones de seguridad moderno | Explicar la misión del centro de operaciones de seguridad |
| Convertirse en un defensor | Describir los recursos disponibles para formar una carrera profesional en operaciones de ciberseguridad |
| 3. Sistema Operativo Windows | Explicar las características de seguridad Windows |
| Historias de Windows | Narra la historia del Sistema Operativo Windows |
| Arquitectura y operaciones | Explica la arquitectura del OS Windows y su operación |
| Configuración y monitoreo | Explica cómo configurar y monitorear el OS Windows |
| Seguridad Windows | Explica cómo mantener la seguridad del OS Windows |
| 4. Sistema Operativo Linux | Explicar las características de seguridad Linux |
| Fundamentos de Linux | Explicar porque las habilidades en Linux son esenciales para monitorear e investigar la seguridad de la red |

| | |
|---|---|
| El Shell de Linux | Usar el Shell de Linux ara manipular archivos de texto |
| Servidores y clientes Linux | Explicar cómo funcionan los servidores y clientes Linux |
| Administración básica de un servidor | Explicar cómo se localizan y manipula los archivos LOG |
| Sistema de archivos Linux | Administrar el sistema de archivos Linux y los permisos |
| Trabajar con la interfaz GUI | Explicar los componentes base de la GUI Linux |
| Trabajar en un Host Linux | Usar herramientas para detectar malware en Linux |
| 5. Protocolos de Red | Explicar el rol de los protocolos en las operaciones de red |
| Proceso de comunicación | Explicar la operación básica de la comunicación en red |
| Protocolos de Red | Cómo los protocolos permiten las operaciones de red |
| Encapsulamiento de datos | Cómo el encapsulamiento permite que los datos sean transportados a través de la red |
| 6. Ethernet y el protocolo IP | Cómo Ethernet e IP soportan las comunicaciones de red |
| Ethernet | Cómo Ethernet soporta las comunicaciones de red |
| IPv4 | Cómo IPv4 soporta las comunicaciones de red, la dirección IPv4, puerta de enlace por defecto y tipos de direcciones |
| IPv6 | Cómo IPv6 soporta las comunicaciones de red |
| 7. Principios de seguridad de Red | Verificación de la conectividad |
| ICMP | Cómo usar ICMP para diagnostica la conectividad |
| Utilitarios Ping y Traceroute | Usar las herramientas Windows ping y traceroute para verificar la conectividad de red |
| 8. Protocolos de resolución | Analizar PDU de los protocolos de resolución |
| ARP e IP | Comparar el rol de las direcciones MAC e IP |

| | |
|---|---|
| ARP | Analizar el protocolo ARP y las tramas ARP |
| Debilidades ARP | Explicar cómo las solicitudes ARP pueden afectar el performance de la red y los HOST |
| 9. La capa de transporte | Explicar la funcionalidad del protocolo de transporte |
| Características de la capa de transporte | Explicar cómo los protocolos de transporte soportan las comunicaciones de Red |
| Establecimiento de conexión | Cómo se establece la conexión en capa de transporte |
| Confiabilidad de la capa | Cómo la capa de transporta permite comunicaciones confiables |
| 10. Servicios de Red | Explicar cómo los servicios de red permiten la funcionalidad de la red |
| ICMP | Cómo usar ICMP para diagnostica la conectividad |
| DHCP | Explica la funcionalidad del servicio DHCP |
| DNS | Explica la funcionalidad del servicio DNS |
| NAT | Explica cómo NAT provee soporte a la comunicación en red |
| FTP | Explica la funcionalidad del servicio de transferencia FTP |
| EMAIL | Explica la funcionalidad del servicio de correo electrónico |
| HTTP | Explica la funcionalidad del servicio Web |
| 11. Dispositivos de Red | Explicar cómo los dispositivos de red proveen comunicaciones de red cablead y wireless |
| Dispositivos de Red | |
| Comunicaciones Wireless | |
| 12. Infraestructura de seguridad de Red | Explicar cómo se usan los dispositivos y servicios para reforzar la seguridad de la red |
| Topologías de Red | Cómo influye los diseños de red en el flujo de tráfico |
| Dispositivos de seguridad | Cómo se usan dispositivos especiales de seguridad |

| | |
|---|---|
| Servicios de seguridad | Cómo se usan los servicios para mejorar la seguridad |
| 13. Atacantes y sus herramientas | Explicar cómo son atacadas las redes |
| ICMP | Cómo usar ICMP para diagnostica la conectividad |
| Quién está atacando la red | Explicar cómo han evolucionado las amenazas |
| Herramientas de lo atacantes | Describe las herramientas para ataques a la red |
| 14. Amenazas y ataques comunes | Explicar los diversos tipos de ataques y amenazas |
| Malware | Describe los tipos de malware |
| Ataques más comunes | Describe los diversos tipos de ataques de reconocimiento, acceso e ingeniería social |
| Ataques de Red | Ataques DoS, Desbordamiento de buffers, Evasión |
| 15. Observar las operaciones | Explicar el monitoreo de las operaciones de red |
| Introducción al monitoreo | Explicar la importancia del monitoreo de la red |
| Introducción a las herramientas de monitoreo | Cómo se despliega el monitoreo de la red |
| 16. Ataques a la tecnología base | Cómo las vulnerabilidades TCP/IP permiten ataques de red |
| Vulnerabilidades IP | Explica cómo las vulnerabilidades IP afectan la seguridad |
| Vulnerabilidades TCP y UDP | Explica cómo las vulnerabilidades TCP afectan la seguridad |
| 17. Ataques a los servicios | Explicar las vulnerabilidades de los servicios de red |
| ICMP | Cómo usar ICMP para diagnosticar la conectividad |
| Servicios IP | Explicar cómo se comprometen a los servicios IP |
| Servicios Enterprise | Explicar cómo las vulnerabilidades de aplicaciones de red permiten los ataques a la red |
| 18. Comprendiendo la defensa | Explicar los enfoques de defensa de seguridad de red |

| | |
|---|---|
| Defense-in-Depth | Explicar cómo el enfoque Defense-in-Depth (defensa profunda) se usa para proteger la red |
| Políticas de seguridad, regulaciones y estándares | Explicar las políticas de seguridad, las regulaciones y los estándares de seguridad |
| 19. Control de acceso | Explicar el uso del control de acceso como método para proteger la red |
| Conceptos de control de acceso | Explicar cómo el control de acceso protege la red |
| Uso y operación de AAA | Explicar cómo usar AAA para controlar el acceso a la red |
| 20. Inteligencia de la amenaza | Usar varias fuentes de inteligencia para localizar amenazas de seguridad presentes en la red |
| Orígenes de información | Describir las fuentes de información para detectar amenazas emergentes |
| Servicios de inteligencia | Describe varios servicios para obtener información de amenazas emergentes en la red |
| 21. Criptografía | Explicar el uso de la infraestructura de clave pública para soportar la seguridad de la red |
| ICMP | Cómo usar ICMP para diagnostica la conectividad |
| Integridad y autenticidad | El rol de la criptografía en el aseguramiento de la integridad y autenticidad de los datos |
| Confidencialidad | El rol de la criptografía para asegurar la confidencialidad de los datos |
| Criptografía de clave pública | Explicar la criptografía de clave pública |
| Autoridades y el sistema PKI | Explica las funciones de la infraestructura de clave pública |
| Aplicaciones e impactos | Efectos de la criptografía en las operaciones de seguridad |
| 22. Protección del endpoint | Explicar como generar un reporte de análisis de malware |
| Protección anti malware | Explicar los métodos para mitigar el malware |
| Prevenir intrusiones en el Host | Explicar los registros de los IPS/IDS basados en Host |

| | |
|---|---|
| Aplicación de seguridad | Como se usa un sandbox para analizar el malware |
| 23. Evaluar la vulnerabilidad del Host | Explicar la funcionalidad del protocolo de transporte |
| Perfilar la red y servidores | Explicar el valor del perfilamiento de la red y servidores |
| Common Vulnerability Scoring System (CVSS) | Explicar cómo usar el CVSS para describir las vulnerabilidades de seguridad |
| Gestión de dispositivos seguros | Explicar cómo se usan las técnicas de gestión de dispositivos para proteger datos y los activos de la red |
| Sistemas de gestión de la seguridad de la información | Explicar cómo se usan los sistemas de gestión de la seguridad de la información para proteger los activos |
| 24. Tecnologías y protocolos | Explicar cómo las tecnologías de seguridad afectan el monitoreo de la seguridad |
| Monitorear protocolos comunes | Explicar el comportamiento de protocolos de red comunes en el contexto de monitoreo de la seguridad |
| Tecnologías de seguridad | Cómo afectan las tecnologías de seguridad, la habilidad de monitorear protocolos de red comunes |
| 25. La capa de transporte | Explicar la funcionalidad del protocolo de transporte |
| Características de la capa de transporte | Explicar cómo los protocolos de transporte soportan las comunicaciones de Red |
| Establecimiento de conexión | Cómo se establece la conexión en capa de transporte |
| Confiabilidad de la capa | Cómo la capa de transporta permite comunicaciones confiables |

NEXUS
ACADEMY

**Contáctanos**

(01) 617 0400
academy@nexus.com.pe
Av. Ricardo Palma 693 - Miraflores
Lima 18 - Perú