Implementing and Operating Cisco Security Core Technologies (SCOR) v1.0

Lo que aprenderá en este curso

Este curso lo ayuda a prepararse para las certificaciones Cisco® CCNP® Security y CCIE® Security y para roles de seguridad de alto nivel. En este curso, dominará las habilidades y tecnologías que necesita para implementar soluciones de seguridad core de Cisco para brindar protección avanzada contra amenazas y ataques de ciberseguridad. Aprenderá seguridad para redes, nube y contenido, protección de puntos finales, acceso seguro a la red, visibilidad y cumplimiento. Obtendrá una amplia experiencia práctica en la implementación del firewall de Next-Generation Cisco Firepower® y el firewall del Adaptive Security Appliance (ASA) de Cisco; configurar políticas de control de acceso, políticas de correo y autenticación 802.1X; y más. Obtendrá una práctica introductoria sobre las funciones de detección de amenazas de Cisco Stealthwatch® Enterprise y Cisco Stealthwatch Cloud.

Este curso, que incluye el material de autoestudio, que lo prepara para el examen, , **Implementing and Operating Cisco Security Core Technologies (350-701 SCOR**), que conduce a las nuevas certificaciones CCNP Security, CCIE Security y Cisco Certified Specialist - Security Core . Este curso también le otorga 64 créditos de Educación Continua (CE) para la recertificación

Duración del curso

- Capacitación dirigida por un instructor: 5 días en el salón de clases con prácticas de laboratorio, más el equivalente a 3 días de material de autoestudio
- Capacitación virtual dirigida por un instructor: 5 días de clases basadas en la web con prácticas de laboratorio más el equivalente a 3 días de material de autoestudio
- E-learning: Equivalente a 8 días de contenido con videos, práctica y desafíos

Cómo se beneficiará

Este curso te ayudará a:

- Obtener experiencia práctica en la implementación de tecnologías de seguridad core y aprender las mejores prácticas con las soluciones de seguridad de Cisco.
- Prepárarse para el examen Implementing and Operating Cisco Security Core Technologies (350-701 SCOR)
- Calificar para roles de trabajo de seguridad de nivel profesional y experto
- Obtenga 64 créditos CE para la recertificación

Quién debería inscribirse

- Integradores y socios de Cisco
- Ingeniero de sistemas consultor
- Administrador de red
- Diseñador de redes
- Ingeniero de redes
- Gerente de Redes
- Ingeniero de seguridad
- Ingeniero de sistemas
- Arquitecto de soluciones técnicas

Qué esperar en el examen

Este curso lo ayudará a prepararse para tomar el examen **Implementing and Operating Cisco Security Core Technologies (350-701 SCOR)**. Este examen evalúa el conocimiento del candidato sobre la implementación y el funcionamiento de tecnologías de seguridad básicas.

Después de pasar 350-701 SCOR:

•Obtiendrá la certificación **Cisco Certified Specialist - Security Core**

•Cumplirá con los requisitos básicos de CCNP Security y CCIE Security. Para completar su certificación **CCNP Security**, apruebe uno de los exámenes de concentración de seguridad. Para completar su certificación de seguridad CCIE, apruebe el examen de laboratorio **CCIE Security** v6.0

Áreas tecnológicas

- Security

Detalles del curso

Objetivos

Después de tomar este curso, debería ser capaz de:

- Describir conceptos y estrategias de seguridad de la información dentro de la red
- Describir ataques comunes de TCP/IP, aplicaciones de red y puntos finales
- Describir cómo varias tecnologías de seguridad de red funcionan juntas para protegerse contra ataques
- Implementar el control de acceso en el dispositivo Cisco ASA y Cisco Firepower Next-Generation Firewall
- Describir e implementar características y funciones básicas de seguridad de contenido de correo electrónico proporcionadas por Cisco Email Security Appliance
- Describir e implementar características y funciones de seguridad de contenido web proporcionadas por Cisco Web Security Appliance
- Describir las capacidades de seguridad de Cisco Umbrella®, los modelos de implementación, la gestión de políticas y la consola Investigate
- Conocer sobre VPN y describir algoritmos y soluciones criptográficas
- Describir las soluciones de conectividad segura de sitio a sitio de Cisco y explicar cómo implementar Cisco Internetwork Operating System (Cisco IOS®) Virtual Tunnel Interface (VTI) basado en VPN IPsec punto a punto y VPN IPsec punto a punto en Cisco ASA and Cisco Firepower Next-Generation Firewall (NGFW)
- Describir e implementar las soluciones de conectividad de acceso remoto seguro de Cisco y describir cómo configurar la autenticación 802.1X y el Protocolo de autenticación extensible (EAP)

Conocimientos y formación recomendadas

Para beneficiarse plenamente de este curso, debe tener los siguientes conocimientos y habilidades:

- Habilidades y conocimientos equivalentes a los aprendidos en el curso Implementing and Administering Cisco Solutions (CCNA®) v1.0
- Familiarizado con las redes Ethernet y TCP/IP
- Conocimiento práctico del sistema operativo Windows
- Conocimiento práctico de redes y los conceptos de Cisco IOS
- Familiarizarse con los conceptos básicos de seguridad de redes

Se recomienda este curso de Cisco para ayudarlo a cumplir con estos requisitos previos:

- **Implementing and Administering Cisco Solutions (CCNA)**

Esquema

- Describing Information Security Concepts*
  - Information Security Overview
  - Assets, Vulnerabilities, and Countermeasures
  - Managing Risk
- Describing Common TCP/IP Attacks*
  - Legacy TCP/IP Vulnerabilities
  - IP Vulnerabilities
  - Internet Control Message Protocol (ICMP) Vulnerabilities
- Describing Common Network Application Attacks*
  - Password Attacks
  - Domain Name System (DNS)-Based Attacks
  - DNS Tunneling
- Describing Common Endpoint Attacks*
  - Buffer Overflow
  - Malware
  - Reconnaissance Attack

- Describing Network Security Technologies
  - Defense-in-Depth Strategy
  - Defending Across the Attack Continuum
  - Network Segmentation and Virtualization Overview
- Deploying Cisco ASA Firewall
  - Cisco ASA Deployment Types
  - Cisco ASA Interface Security Levels
  - Cisco ASA Objects and Object Groups
- Deploying Cisco Firepower Next-Generation Firewall
  - Cisco Firepower NGFW Deployments
  - Cisco Firepower NGFW Packet Processing and Policies
  - Cisco Firepower NGFW Objects
- Deploying Email Content Security
  - Cisco Email Content Security Overview
  - Simple Mail Transfer Protocol (SMTP) Overview
  - Email Pipeline Overview
- Deploying Web Content Security
  - Cisco Web Security Appliance (WSA) Overview
  - Deployment Options
  - Network Users Authentication
- Deploying Cisco Umbrella*
  - Cisco Umbrella Architecture
  - Deploying Cisco Umbrella
  - Cisco Umbrella Roaming Client
- Explaining VPN Technologies and Cryptography
  - VPN Definition
  - VPN Types
  - Secure Communication and Cryptographic Services
- Introducing Cisco Secure Site-to-Site VPN Solutions
  - Site-to-Site VPN Topologies
  - IPsec VPN Overview
  - IPsec Static Crypto Maps
- Deploying Cisco IOS VTI-Based Point-to-Point IPsec VPNs
  - Cisco IOS VTIs
  - Static VTI Point-to-Point IPsec Internet Key Exchange (IKE) v2 VPN Configuration

- Deploying Point-to-Point IPsec VPNs on the Cisco ASA and Cisco Firepower NGFW
  - Point-to-Point VPNs on the Cisco ASA and Cisco Firepower NGFW
  - Cisco ASA Point-to-Point VPN Configuration
  - Cisco Firepower NGFW Point-to-Point VPN Configuration
- Introducing Cisco Secure Remote Access VPN Solutions
  - Remote Access VPN Components
  - Remote Access VPN Technologies
  - Secure Sockets Layer (SSL) Overview
- Deploying Remote Access SSL VPNs on the Cisco ASA and Cisco Firepower NGFW
  - Remote Access Configuration Concepts
  - Connection Profiles
  - Group Policies
- Explaining Cisco Secure Network Access Solutions
  - Cisco Secure Network Access
  - Cisco Secure Network Access Components
  - AAA Role in Cisco Secure Network Access Solution
- Describing 802.1X Authentication
  - 802.1X and Extensible Authentication Protocol (EAP)
  - EAP Methods
  - Role of Remote Authentication Dial-in User Service (RADIUS) in 802.1X Communications
- Configuring 802.1X Authentication
  - Cisco Catalyst® Switch 802.1X Configuration
  - Cisco Wireless LAN Controller (WLC) 802.1X Configuration
  - Cisco Identity Services Engine (ISE) 802.1X Configuration
- Describing Endpoint Security Technologies*
  - Host-Based Personal Firewall
  - Host-Based Anti-Virus
  - Host-Based Intrusion Prevention System
- Deploying Cisco Advanced Malware Protection (AMP) for Endpoints*
  - Cisco AMP for Endpoints Architecture
  - Cisco AMP for Endpoints Engines
  - Retrospective Security with Cisco AMP
- Introducing Network Infrastructure Protection*
  - Identifying Network Device Planes
  - Control Plane Security Controls
  - Management Plane Security Controls
- Deploying Control Plane Security Controls*
  - Infrastructure ACLs
  - Control Plane Policing
  - Control Plane Protection

- Deploying Layer 2 Data Plane Security Controls*
  - Overview of Layer 2 Data Plane Security Controls
  - Virtual LAN (VLAN)-Based Attacks Mitigation
  - Spanning Tree Protocol (STP) Attacks Mitigation
- Deploying Layer 3 Data Plane Security Controls*
  - Infrastructure Antispoofing ACLs
  - Unicast Reverse Path Forwarding
  - IP Source Guard
- Deploying Management Plane Security Controls*
  - Cisco Secure Management Access
  - Simple Network Management Protocol Version 3
  - Secure Access to Cisco Devices
- Deploying Traffic Telemetry Methods*
  - Network Time Protocol
  - Device and Network Events Logging and Export
  - Network Traffic Monitoring Using NetFlow
- Deploying Cisco Stealthwatch Enterprise*
  - Cisco Stealthwatch Offerings Overview
  - Cisco Stealthwatch Enterprise Required Components
  - Flow Stitching and Deduplication
- Describing Cloud and Common Cloud Attacks*
  - Evolution of Cloud Computing
  - Cloud Service Models
  - Security Responsibilities in Cloud
- Securing the Cloud*
  - Cisco Threat-Centric Approach to Network Security
  - Cloud Physical Environment Security
  - Application and Workload Security
- Deploying Cisco Stealthwatch Cloud*
  - Cisco Stealthwatch Cloud for Public Cloud Monitoring
  - Cisco Stealthwatch Cloud for Private Network Monitoring
  - Cisco Stealthwatch Cloud Operations
- Describing Software-Defined Networking (SDN*)
  - Software-Defined Networking Concepts
  - Network Programmability and Automation
  - Cisco Platforms and APIs

* This section is self-study material that you can complete at your own pace if you are taking the instructor-led version of this course.

Cómo inscribirse

Para inscribirse al curso SCOR o explorar nuestro catálogo completo de cursos sobre Cisco Digital Learning, contáctenos en:

info@slslatam.com

O bien visite nuestra página en:

www.slslatam.com

Esquema de los laboratorios

- Configure Network Settings and NAT on Cisco ASA
- Configure Cisco ASA Access Control Policies
- Configure Cisco Firepower NGFW NAT
- Configure Cisco Firepower NGFW Access Control Policy
- Configure Cisco Firepower NGFW Discovery and IPS Policy
- Configure Cisco NGFW Malware and File Policy
- Configure Listener, Host Access Table (HAT), and Recipient Access Table (RAT) on Cisco Email Security Appliance (ESA)
- Configure Mail Policies
- Configure Proxy Services, Authentication, and HTTPS Decryption
- Enforce Acceptable Use Control and Malware Protection
- Examine the Umbrella Dashboard
- Examine Cisco Umbrella Investigate
- Explore DNS Ransomware Protection by Cisco Umbrella
- Configure Static VTI Point-to-Point IPsec IKEv2 Tunnel
- Configure Point-to-Point VPN between the Cisco ASA and Cisco Firepower NGFW
- Configure Remote Access VPN on the Cisco Firepower NGFW
- Explore Cisco AMP for Endpoints
- Perform Endpoint Analysis Using AMP for Endpoints Console
- Explore File Ransomware Protection by Cisco AMP for Endpoints Console
- Explore Cisco Stealthwatch Enterprise v6.9.3
- Explore Cognitive Threat Analytics (CTA) in Stealthwatch Enterprise v7.0
- Explore the Cisco Cloudlock Dashboard and User Security
- Explore Cisco Cloudlock Application and Data Security
- Explore Cisco Stealthwatch Cloud
- Explore Stealthwatch Cloud Alert Settings, Watchlists, and Sensors

SLS LATAM®

CISCO Partner

SCOR_v1.0 C22-743407-04 03/22