SLS LATAM®

cisco Partner

TEMARIO SCOR

IMPLEMENTING AND OPERATING CISCO SECURITY CORE TECHNOLOGIES v2.0 (SCOR)

El curso Implementing and Operating Cisco Security Core Technologies (SCOR) te ayuda a adquirir las habilidades y tecnologías necesarias para implementar soluciones de seguridad básicas de Cisco. Este entrenamiento te preparará para ofrecer protección avanzada contra ataques cibernéticos y te pondrá en camino para roles de seguridad de nivel senior.

---

43 CLC

Duración
40 horas

64 CE

¿CÓMO TE BENEFICIARÁ?

En este curso aprenderás a implementar tecnologías de seguridad fundamentales y mejores prácticas utilizando soluciones de seguridad de Cisco, lo que te permitirá prepararte para roles profesionales y de nivel experto en seguridad.

Además, te ayudará a obtener experiencia práctica en la implementación de soluciones de protección contra amenazas avanzadas, y te preparará para el examen 350-701 SCOR v1.1, obteniendo la certificación Cisco Certified Specialist - Security Core, que también satisface los requisitos para las certificaciones CCNP y CCIE Security.

¿QUIÉN DEBERÍA INSCRIBIRSE?

Dirigido a ingenieros de seguridad, ingenieros de redes, diseñadores de redes, administradores de redes, ingenieros de sistemas, arquitectos de soluciones técnicas, integradores y socios de Cisco, gerentes de redes, gerentes de programas y gerentes de proyectos.

DETALLES DEL CURSO

Después de tomar este curso, deberías ser capaz de:

- Describir conceptos y estrategias de seguridad de la información en la red.
- Explicar vulnerabilidades en el protocolo TCP/IP y cómo pueden ser usadas para atacar redes y dispositivos.
- Identificar ataques basados en aplicaciones de red.

DETALLES DEL CURSO

Después de tomar este curso, deberías ser capaz de:

- Explicar cómo diversas tecnologías de seguridad trabajan juntas para defenderse de ataques.
- Implementar control de acceso en Cisco Secure Firewall ASA.
- Configurar Cisco Secure Firewall Threat Defense en su nivel básico.
- Implementar políticas de IPS, malware y firewall en Cisco Secure Firewall Threat Defense.
- Configurar Cisco Secure Email Gateway en su nivel básico.
- Implementar políticas en Cisco Secure Email Gateway.
- Explicar y configurar funciones básicas de seguridad de contenido web en Cisco Secure Web Appliance.
- Identificar diversas técnicas de ataque contra endpoints.
- Describir las capacidades de seguridad, modelos de despliegue y gestión de políticas en Cisco Umbrella.
- Explicar conceptos básicos de seguridad en endpoints y tecnologías comunes de protección.
- Describir la arquitectura y funciones básicas de Cisco Secure Endpoint.
- Explicar soluciones de acceso seguro a la red de Cisco.
- Describir la autenticación 802.1X y el protocolo EAP.
- Configurar dispositivos para operaciones 802.1X.
- Introducir VPNs y explicar soluciones criptográficas y algoritmos.
- Describir soluciones de conectividad segura de sitio a sitio en Cisco.
- Implementar VPNs IPsec punto a punto con Cisco IOS VTI.
- Configurar VPNs IPsec en Cisco Secure Firewall ASA y Cisco Secure Firewall Threat Defense.
- Explicar soluciones de conectividad remota segura de Cisco.
- Implementar soluciones de conectividad remota segura de Cisco.
- Presentar controles de protección de infraestructura de red.
- Examinar defensas en dispositivos Cisco para proteger el plano de control.
- Configurar y verificar controles del plano de datos en capa 2 en Cisco IOS.

DETALLES DEL CURSO

Después de tomar este curso, deberías ser capaz de:

- Configurar y verificar controles del plano de datos en capa 3 en Cisco IOS y Cisco ASA.
- Examinar defensas en dispositivos Cisco para proteger el plano de gestión.
- Describir formas básicas de telemetría recomendadas para infraestructura y dispositivos de seguridad.
- Explicar el despliegue de Cisco Secure Network Analytics.
- Describir fundamentos de computación en la nube y ataques comunes en la nube.
- Explicar cómo proteger entornos en la nube.
- Describir la implementación de Cisco Secure Cloud Analytics.
- Explicar fundamentos de redes definidas por software y programabilidad de redes.

CONOCIMIENTOS RECOMENDADOS

La base de conocimientos y habilidades que se espera tengas antes de asistir a esta capacitación son:

- Familiaridad con redes Ethernet y TCP/IP.
- Conocimiento práctico del sistema operativo Windows.
- Conocimiento práctico de redes y conceptos de Cisco IOS.
- Familiaridad con conceptos básicos de seguridad en redes.

CONTENIDO

- Tecnologías de seguridad en redes.
- Implementación de Cisco Secure Firewall ASA.
- Fundamentos de Cisco Secure Firewall Threat Defense.
- Cisco Secure Firewall Threat Defense IPS, malware y políticas de archivos.
- Fundamentos de Cisco Secure Email Gateway.

CONTENIDO

- Configuración de políticas en Cisco Secure Email.
- Implementación de Cisco Secure Web Appliance.
- Tecnologías VPN y conceptos de criptografía.
- Soluciones de Cisco Secure Site-to-Site VPN.
- VPN IPsec punto a punto con Cisco IOS VTI.
- VPN IPsec punto a punto en Cisco Secure Firewall ASA y Threat Defense.
- Soluciones de Cisco Secure Remote-Access VPN.
- VPN SSL de acceso remoto en Cisco Secure Firewall ASA y Threat Defense.
- Conceptos de seguridad de la información.
- Ataques comunes en TCP/IP.
- Ataques comunes a aplicaciones de red.
- Ataques comunes a endpoints.
- Implementación de Cisco Umbrella.
- Tecnologías de seguridad para endpoints.
- Cisco Secure Endpoint.
- Soluciones de acceso seguro a la red de Cisco.
- Autenticación 802.1X.
- Configuración de autenticación 802.1X.
- Protección de infraestructura de red.
- Soluciones de seguridad en el plano de control.
- Controles de seguridad en el plano de datos de capa 2.
- Controles de seguridad en el plano de datos de capa 3.
- Controles de seguridad en el plano de gestión.
- Métodos de telemetría de tráfico.
- Implementación de Cisco Secure Network Analytics.
- Computación en la nube y seguridad en la nube.

CONTENIDO

- Seguridad en la nube.
- Implementación de Cisco Secure Cloud Analytics.
- Redes definidas por software.

ESQUEMA DE LABORATORIOS

- Configurar ajustes de red y NAT en Cisco Secure Firewall ASA.
- Configurar políticas de control de acceso en Cisco Secure Firewall ASA.
- Configurar NAT en Cisco Secure Firewall Threat Defense.
- Configurar política de control de acceso en Cisco Secure Firewall Threat Defense.
- Configurar descubrimiento y política IPS en Cisco Secure Firewall Threat Defense.
- Configurar política de malware y archivos en Cisco Secure Firewall Threat Defense.
- Configurar Listener, HAT y RAT en Cisco Secure Email Gateway.
- Configurar políticas en Cisco Secure Email.
- Configurar servicios proxy, autenticación y descifrado HTTPS.
- Aplicar control de uso aceptable y protección contra malware.
- Configurar túnel IPsec IKEv2 punto a punto con VTI estático.
- Configurar VPN punto a punto entre dispositivos Cisco Secure Firewall Threat Defense.
- Configurar VPN de acceso remoto en Cisco Secure Firewall Threat Defense.
- Examinar el panel de control de Cisco Umbrella y la seguridad DNS.
- Examinar Cisco Umbrella Secure Web Gateway y Cloud-Delivered Firewall.
- Explorar las funcionalidades CASB de Cisco Umbrella.
- Explorar Cisco Secure Endpoint.
- Realizar análisis de endpoints con Cisco Secure Endpoint Console.
- Explorar la protección contra ransomware en Cisco Secure Endpoint Console.

ESQUEMA DE LABORATORIOS

- Explorar Secure Network Analytics v7.4.2.
- Explorar la integración de Global Threat Alerts y la auditoría criptográfica ETA.
- Explorar el panel de análisis en la nube y sus operaciones.
- Explorar la monitorización de nubes privadas y públicas con Secure Cloud.