SLS LATAM®

cisco Partner

TEMARIO SESA

SECURING EMAIL WITH CISCO EMAIL SECURITY APPLIANCE v3.2 (SESA)

Este curso Securing Email with Cisco Email Security Appliance (SESA) te enseña cómo implementar y usar el Cisco Email Security Appliance para establecer protección en los sistemas de correo electrónico contra ataques de phishing, compromiso de correo electrónico empresarial y ransomware, además de facilitar la gestión de políticas de seguridad en el correo electrónico.

---

36 CLC | Duración 32 horas | 24 CE

¿CÓMO TE BENEFICIARÁ?

Este curso te prepara para el examen 300-720 SESA v1.1, otorgándote la certificación Cisco Certified Specialist – Email Content Security y cumpliendo con el requisito del examen de concentración para la certificación CCNP Security.

A lo largo de la capacitación, aprenderás a desplegar protección de alta disponibilidad para tus sistemas de correo electrónico frente a amenazas dinámicas como el phishing, el compromiso de correo electrónico empresarial y el ransomware, adquiriendo habilidades clave en seguridad empresarial y preparación para el examen.

¿QUIÉN DEBERÍA INSCRIBIRSE?

Este curso está dirigido a Security Engineers, Security Administrators, Network Engineers, Network Administrators y Cisco Integrators and Partners, brindándoles habilidades para implementar y gestionar soluciones de seguridad avanzadas, protegiendo sistemas de correo electrónico contra amenazas cibernéticas.

DETALLES DEL CURSO

Después de tomar este curso, deberías ser capaz de:

- Describir y administrar el Cisco Email Security Appliance.
- Controlar dominios de remitentes y destinatarios.
- Controlar el spam con Talos SenderBase y anti-spam.
- Usar filtros anti-virus y de brotes.

DETALLES DEL CURSO

Después de tomar este curso, deberías ser capaz de:

- Usar políticas de correo.
- Usar filtros de contenido.
- Usar filtros de mensajes.
- Prevenir la pérdida de datos.
- Realizar consultas de Lightweight Directory Access Protocol (LDAP).
- Autenticar sesiones de Simple Mail Transfer Protocol (SMTP).
- Autenticar el correo electrónico.
- Cifrar el correo electrónico.
- Usar la cuarentena del sistema y métodos de entrega.
- Realizar gestión centralizada utilizando clústeres.
- Pruebas y solución de problemas.

CONOCIMIENTOS RECOMENDADOS

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

- Certificación de Cisco, como Cisco Certified Support Technician (CCST) en Ciberseguridad o superior.
- Certificación relevante de la industria, como (ISC)2, CompTIA Security+, EC-Council, Global Information Assurance Certification (GIAC) e ISACA.
- Certificación CCNA
- Experiencia en Windows, como Microsoft Specialist, Microsoft Certified Solutions Associate (MCSA), Microsoft Certified Systems Engineer (MCSE) y CompTIA (A+, Network+, Server+).

CONTENIDO

- Descripción del Cisco Email Security Appliance.
- Control de dominios de remitentes y destinatarios.
- Control de spam con Talos SenderBase y Anti-Spam.

CONTENIDO

- Uso de Anti-Virus y filtros Outbreak .
- Uso de políticas de correo.
- Uso de filtros de contenido.
- Uso de filtros de mensajes.
- Prevención de pérdida de datos.
- Uso de LDAP.
- Descripción de la autenticación de sesiones SMTP.
- Uso de autenticación de correo electrónico.
- Uso de cifrado de correo electrónico.
- Administración del Cisco Email Security Appliance.
- Uso de la cuarentena del sistema y métodos de entrega.
- Gestión centralizada mediante clústeres.
- Pruebas y resolución de problemas.

ESQUEMA DE LABORATORIOS

- Verificar y probar la configuración de Cisco ESA.
- Detección avanzada de malware en archivos adjuntos (detección de macros).
- Proteger contra URLs maliciosas o indeseables debajo de URLs acortadas.
- Proteger contra URLs maliciosas o indeseables dentro de archivos adjuntos.
- Manejar de manera inteligente los mensajes no escaneables.
- Aprovechar la inteligencia de AMP Cloud mediante la mejora de preclasificación.
- Integrar Cisco ESA con el Consola AMP.
- Prevenir amenazas con protección antivirus.
- Aplicar filtros Outbreak .

ESQUEMA DE LABORATORIOS

- Configurar escaneo de archivos adjuntos.
- Configurar prevención de pérdida de datos en salida.
- Integrar Cisco ESA con LDAP y habilitar la consulta LDAP Accept.
- Domain Keys Identified Mail (DKIM).
- Sender Policy Framework (SPF).
- Detección de correos electrónicos falsificados.
- Realizar administración básica.
- Configurar Cisco Secure Email y Web Manager para seguimiento e informes.