SLS LATAM®

cisco Partner

TEMARIO SCAZT

DESIGNING AND IMPLEMENTING SECURE CLOUD ACCESS FOR USERS AND ENDPOINTS v1.0 (SCAZT)

El curso Designing and Implementing Secure Cloud Access for Users and Endpoints te enseña las habilidades necesarias para diseñar e implementar una arquitectura de seguridad en la nube, seguridad de usuarios y dispositivos, seguridad de redes, aplicaciones, datos, visibilidad y assurance y cómo responder a amenazas en la nube.

---

44 CLC | Duración 40 horas | 40 CE

¿CÓMO TE BENEFICIARÁ?

Este curso te prepara para el examen 300-740 SCAZT v1.0, otorgándote la certificación Cisco Certified Specialist – Security Secure Cloud Access y satisfaciendo el requisito del examen de concentración para la certificación Cisco Certified Network Professional (CCNP) Security.

A través de esta formación, adquirirás habilidades para diseñar e implementar arquitecturas de seguridad en la nube, proteger usuarios y dispositivos, asegurar redes y aplicaciones en la nube, garantizar visibilidad y respuesta ante amenazas y desarrollar competencias avanzadas para roles profesionales y expertos en el diseño e implementación de soluciones de seguridad en la nube.

¿QUIÉN DEBERÍA INSCRIBIRSE?

Dirigido a ingenieros de redes y arquitectos de seguridad, les permite desarrollar competencias avanzadas en protocolos y soluciones para roles de diseño e implementación en el ámbito de la seguridad en la nube.

DETALLES DEL CURSO

Después de tomar este curso, deberías ser capaz de:

- Comparar y contrastar los marcos de seguridad del National Institute of Standards and Technology (Instituto Nacional de Estándares y Tecnología, NIST), la Cybersecurity and Infrastructure Security Agency (Agencia de Seguridad Cibernética e Infraestructura, CISA) y la Defense Information Systems Agency (Agencia de Sistemas de Información de Defensa, DISA) y comprender la importancia de adoptar marcos estandarizados para mejorar la postura de seguridad cibernética de una organización.

DETALLES DEL CURSO

Después de tomar este curso, deberías ser capaz de:

- Describir la Arquitectura de Referencia de Seguridad de Cisco y sus cinco componentes principales.
- Describir los casos de uso comúnmente implementados y recomendar las funcionalidades necesarias dentro de una arquitectura de seguridad integrada para abordarlos eficazmente.
- Describir la arquitectura Cisco Secure Architecture for Everyone (SAFE).
- Revisar los beneficios, componentes y proceso de autenticación basada en certificados para usuarios y dispositivos.
- Habilitar la autenticación multifactor (MFA) de Duo para proteger una aplicación desde el Portal de Administración de Duo y luego configurar la aplicación para usar Duo MFA para la autenticación de inicio de sesión de usuarios.
- Instalar Cisco Duo e implementar su autenticación multifactor en una red privada virtual (VPN) de acceso remoto.
- Configurar el cumplimiento de los puntos finales.
- Revisar y demostrar la capacidad de comprender el Stateful Switchover (SSO) utilizando Security Assertion Markup Language (SAML) o OpenID Connect junto con Cisco Duo.
- Describir los servicios de prevención de amenazas integrados y en el dispositivo de Cisco software-defined wide-area network (SD-WAN).
- Describir los servicios de filtrado de contenido integrados y en el dispositivo de Cisco SD-WAN.
- Describir las características y capacidades de Cisco Umbrella Secure Internet Gateway (SIG), como DNS Security, Cloud-Delivered Firewall (CDFW), sistemas de prevención de intrusiones (IPS) e interacción con Cisco SD-WAN.
- Presentación de Reverse Proxy para la protección de aplicaciones expuestas a internet.
- Explorar el caso de uso de Cisco Umbrella SIG para asegurar el acceso a aplicaciones en la nube, las limitaciones y beneficios de la solución y las características disponibles para descubrir y controlar el acceso a aplicaciones entregadas por la nube.
- Explorar las capacidades de Cisco ThousandEyes para monitorear la implementación de Cisco SD-WAN.
- Describir los desafíos de acceder a aplicaciones SaaS en entornos empresariales modernos y explorar la solución Cisco SD-WAN Cloud OnRamp para SaaS con acceso a internet directo o centralizado.

DETALLES DEL CURSO

Después de tomar este curso, deberías ser capaz de:

- Presentación de las plataformas Cisco Secure Firewall, casos de uso y capacidades de seguridad.
- Demostrar un conocimiento completo de los firewalls de aplicaciones web.
- Demostrar un conocimiento integral de las capacidades de Cisco Secure Workload, opciones de implementación, agentes y conectores.
- Demostrar un conocimiento completo sobre el mapeo de dependencias de aplicaciones y el descubrimiento de políticas de Cisco Secure Workload.
- Demostrar un conocimiento integral de las tácticas comunes de ataques en la nube y estrategias de mitigación.
- Demostrar un conocimiento completo de los requisitos de seguridad en multicloud y capacidades de políticas.
- Presentación de los problemas de seguridad con la adopción de nubes públicas y las capacidades comunes de las herramientas de visibilidad y aseguramiento de la nube para mitigar estos problemas.
- Presentación de Cisco Secure Network Analytics y Cisco Security Analytics and Logging.
- Describir Cisco Attack Surface Management.
- Describir cómo las Application Program Intercaces (API) y la automatización pueden ayudar a resolver problemas de políticas en la nube, especialmente en el contexto de configuraciones incorrectas.
- Demostrar un conocimiento integral de las respuestas apropiadas a amenazas en la nube en escenarios específicos.
- Demostrar el conocimiento integral necesario para usar la automatización en la detección y respuesta ante amenazas en la nube.

CONOCIMIENTOS RECOMENDADOS

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

- Comprensión básica del ruteo empresarial.
- Comprensión básica de redes WAN.
- Comprensión básica de Cisco SD-WAN.
- Comprensión básica de los servicios de Nube Pública.

CONOCIMIENTOS RECOMENDADOS

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

- Estas habilidades se pueden encontrar en los siguientes cursos:
- Implementing and Administering Cisco Solutions 2.0
- Implementing Cisco SD-WAN Solutions 3.0
- Cisco SD-WAN Operation and Deployment 2.0

CONTENIDO

- Marcos de seguridad de la industria.
- Fundamentos de la arquitectura de seguridad de Cisco.
- Casos de uso comunes de la arquitectura de seguridad de Cisco.
- Arquitectura Cisco SAFE.
- Autenticación basada en certificados para usuarios y dispositivos.
- Autenticación Multi-factor Cisco Duo para protección de aplicaciones.
- Cisco Duo con VPN AnyConnect para acceso remoto.
- Introducción a los servicios de cumplimiento de endpoints con Cisco ISE.
- SSO utilizando SAML o OpenID Connect.
- Configuración de prevención de amenazas locales.
- Examinando el filtrado de contenido.
- Explorando Cisco Umbrella SIG.
- Reverse Proxy
- Asegurando aplicaciones en la nube con Cisco Umbrella SIG.
- Explorando Cisco SD-WAN ThousandEyes.
- Optimización de aplicaciones SaaS.
- Políticas de seguridad para VPN de acceso remoto.
- Cisco Secure Access.
- Cisco Secure Firewall.
- Firewall de aplicaciones web.

CONTENIDO

- Implementación, agentes y conectores de Cisco Secure Workload.
- Estructura y políticas de Cisco Secure Workload.
- Ataques a la seguridad en la nube y estrategias de mitigación.
- Políticas de seguridad multicloud.
- Visibilidad y aseguramiento en la nube.
- Cisco Secure Network Analytics y Cisco Secure Analytics y Logging.
- Cisco XDR.
- Gestión de la superficie de ataque de Cisco.
- Verificaciones de acceso a aplicaciones y datos en la nube.
- Automatización de políticas en la nube.
- Respuesta ante amenazas en la nube.
- Automatización de la detección y respuestas ante amenazas en la nube.

ESQUEMA DE LABORATORIOS

- Explorar Cisco SecureX.
- Actividad interactiva de incorporación de BYOD Windows.
- Usar Cisco Duo MFA para proteger la aplicación Splunk.
- Integrar Cisco Duo Authentication Proxy implementar MFA en Cisco Security Secure Firewall AnyConnect Remote Access VPN.
- Configurar Cisco ISE Compliance Services.
- Configurar la prevención de amenazas.
- Implementar seguridad web.
- Desplegar seguridad DIA con políticas de seguridad unificadas.
- Configurar políticas de DNS de Cisco Umbrella.
- Instalar Cisco Umbrella Secure Internet Gateway.
- Implementar seguridad CASB.

ESQUEMA DE LABORATORIOS

- Probar Microsoft 365 SaaS usando Cisco ThousandEyes.
- Configurar VPN de acceso remoto en Cisco Secure Firewall Threat Defense.
- Configurar políticas de Cisco Secure Firewall.
- Explorar Cisco Secure Workload.
- Explorar las técnicas basadas en la nube de la matriz ATT&CK.
- Explorar Cisco Secure Network Analytics.
- Explorar tareas de respuesta ante incidentes de Cisco XDR.