Implementing and Operating Cisco Security Core Technologies (SCOR)

En este curso los estudiantes dominarán las habilidades y tecnologías necesarias para implementar las soluciones de seguridad básicas de Cisco para proporcionar protección avanzada contra amenazas contra ataques de ciberseguridad. Los estudiantes aprenderán seguridad para redes, nube y contenido, protección de terminales, acceso seguro a la red, visibilidad y cumplimiento. Obtendrán una amplia experiencia práctica en la implementación del firewall de próxima generación Cisco Firepower y el firewall Cisco ASA; configurar políticas de control de acceso, políticas de correo y autenticación 802.1X; y más. Los estudiantes también obtendrán práctica introductoria sobre las funciones de detección de amenazas de Cisco Stealthwatch Enterprise y Cisco Stealthwatch Cloud.

Este curso lo ayudará a prepararse para tomar el examen Implementación y funcionamiento de las tecnologías básicas de seguridad de Cisco (350-701 SCOR). También lo ayuda a prepararse para las certificaciones CCNP Security y CCIE Security y para los roles de seguridad de nivel superior con soluciones de seguridad de Cisco.

Pre Requisitos

Los conocimientos y habilidades que debe tener un alumno antes de asistir a este curso son los siguientes:

- Habilidades y conocimientos equivalentes a los aprendidos en el curso Implementación y administración de soluciones de Cisco (CCNA) v1.0
- Familiaridad con las redes Ethernet y TCP / IP.
- Conocimientos prácticos del sistema operativo Windows.
- Conocimiento práctico de los conceptos y las redes de Cisco IOS
- Familiaridad con los conceptos básicos de seguridad de redes.

Objetivos del curso

Al completar este curso, el alumno podrá cumplir con estos objetivos generales:

- Describir conceptos y estrategias de seguridad de la información dentro de la red.
- Describir ataques comunes de TCP / IP, aplicaciones de red y terminales.
- Describir cómo funcionan juntas varias tecnologías de seguridad de red para protegerse contra ataques.
- Implementar el control de acceso en el dispositivo Cisco ASA y el firewall de próxima generación Cisco Firepower
- Describir e implementar características y funciones básicas de seguridad del contenido del correo electrónico proporcionadas por Cisco Email Security Appliance.

Implementing and Operating Cisco Security Core Technologies (SCOR)

- 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 administración de políticas y la consola Investigate
- Introducir VPN y describir soluciones y algoritmos de criptografía.
- Describir las soluciones de conectividad segura de sitio a sitio de Cisco y explicar cómo implementar VPN IPsec punto a punto basadas en Cisco IOS VTI y VPN IPsec punto a punto en Cisco ASA y Cisco FirePower NGFW
- Describir e implementar soluciones de conectividad de acceso remoto seguro de Cisco y describir cómo configurar la autenticación 802.1X y EAP
- Proporcionar una comprensión básica de la seguridad de los puntos finales y describir AMP para la arquitectura y las características básicas de los puntos finales.
- Examinar varias defensas en los dispositivos Cisco que protegen el plano de control y administración.
- Configure y verifique los controles del plano de datos de la capa 2 y la capa 3 del software Cisco IOS
- Describir las soluciones Cisco Stealthwatch Enterprise y Stealthwatch Cloud
- Describir los conceptos básicos de la computación en la nube y los ataques comunes a la nube y cómo proteger el entorno de la nube.

Esquema del curso

Descripción de conceptos de seguridad de la información

- Resumen de seguridad de la información
- La gestión del riesgo
- Evaluación de vulnerabilidad
- Entendiendo CVSS

Descripción de ataques comunes de TCP / IP

- Vulnerabilidades heredadas de TCP / IP
- Vulnerabilidades de IP
- Vulnerabilidades de ICMP
- Vulnerabilidades de TCP
- Vulnerabilidades de UDP
- Superficie de ataque y vectores de ataque

Implementing and Operating Cisco Security Core Technologies (SCOR)

- Ataques de reconocimiento
- Ataques de acceso
- Ataques de intermediario
- Ataques de denegación de servicio y denegación de servicio distribuida
- Ataques de reflexión y amplificación
- Ataques de suplantación
- Ataques DHCP

Descripción de ataques comunes a aplicaciones de red

- Ataques de contraseña
- Ataques basados en DNS
- Túnel de DNS
- Ataques basados en web
- Amortiguación HTTP 302
- Inyecciones de comando
- Inyecciones SQL
- Falsificación de solicitudes y secuencias de comandos entre sitios
- Ataques basados en correo electrónico

Descripción de los ataques comunes a Endpoints

- Desbordamiento de búfer
- Software malicioso
- Ataque de reconocimiento
- Obtener acceso y control
- Obtener acceso a través de la ingeniería social
- Obtener acceso a través de ataques basados en la web
- Exploit Kits y rootkits
- Escalada de privilegios
- Fase posterior a la explotación
- Kit de explotación del pescador

Descripción de tecnologías de seguridad de red

- Estrategia de defensa en profundidad
- Defendiendo a través del continuo de ataque
- Descripción general de virtualización y segmentación de red
- Descripción general de Stateful Firewall
- Descripción general de inteligencia de seguridad
- Estandarización de la información sobre amenazas

Implementing and Operating Cisco Security Core Technologies (SCOR)

- Descripción general de la protección contra malware basada en red
- Descripción general de IPS
- Descripción general del firewall de próxima generación
- Descripción general de la seguridad del contenido del correo electrónico
- Descripción general de la seguridad del contenido web
- Descripción general de Threat Analytic Systems
- Descripción general de la seguridad de DNS
- Descripción general de autenticación, autorización y contabilidad
- Descripción general de la administración de identidades y accesos
- Descripción general de la tecnología de red privada virtual
- Descripción general de los factores de forma del dispositivo de seguridad de red

Implementación del cortafuegos Cisco ASA

- Tipos de implementación de Cisco ASA
- Niveles de seguridad de la interfaz Cisco ASA
- Objetos y grupos de objetos de Cisco ASA
- Traducción de Direcciones de Red
- ACL de interfaz Cisco ASA
- ACL globales de Cisco ASA
- Políticas de acceso avanzado de Cisco ASA
- Descripción general de alta disponibilidad de Cisco ASA

Implementación del firewall de próxima generación Cisco Firepower

- Implementaciones de Cisco Firepower NGFW
- Políticas y procesamiento de paquetes de Cisco Firepower NGFW
- Objetos NGFW de Cisco Firepower
- Cisco Firepower NGFW NAT
- Políticas de prefiltro de Cisco Firepower NGFW
- Políticas de control de acceso de Cisco Firepower NGFW
- Inteligencia de seguridad de Cisco Firepower NGFW
- Políticas de descubrimiento de Cisco Firepower NGFW
- Políticas IPS de Cisco Firepower NGFW
- Políticas de archivos y malware de Cisco Firepower NGFW

Implementación de la seguridad del contenido del correo electrónico

- Descripción general de la seguridad del contenido del correo electrónico de Cisco
- Descripción general de SMTP
- Descripción general de la canalización de correo electrónico

Implementing and Operating Cisco Security Core Technologies (SCOR)

- Oyentes públicos y privados
- Descripción general de la tabla de acceso al host
- Descripción general de la tabla de acceso de destinatarios
- Descripción general de las políticas de correo
- Protección contra correo no deseado y correo gris
- Protección antivirus y antimalware
- Filtros de brotes
- Filtros de contenido
- Prevención de pérdida de datos
- Cifrado de correo electrónico

Implementación de la seguridad del contenido web

- Descripción general de Cisco WSA
- Opciones de implementación
- Autenticación de usuarios de red
- Descifrado de tráfico HTTPS
- Políticas de acceso y perfiles de identificación
- Configuración de controles de uso aceptable
- Protección anti-malware

Implementación de Cisco Umbrella

- Arquitectura Cisco Umbrella
- Implementación de Cisco Umbrella
- Cliente de itinerancia de Cisco Umbrella
- Administrar Cisco Umbrella
- Descripción general de Cisco Umbrella Investigate

Explicando las tecnologías VPN y la criptografía

- Definición de VPN
- Tipos de VPN
- Servicios criptográficos y de comunicación segura
- Claves en criptografía
- Infraestructura de Clave Pública

Presentamos las soluciones VPN de sitio a sitio seguro de Cisco

- Topologías de VPN de sitio a sitio
- Descripción general de IPsec VPN
- Mapas criptográficos estáticos de IPsec
- Interfaz de túnel virtual estático IPsec
- VPN multipunto dinámica
- Cisco IOS FlexVPN

Implementing and Operating Cisco Security Core Technologies (SCOR)

Implementación de punto a punto basado en Cisco IOS VTI
- VTI de Cisco IOS
- Configuración de VPN IPsec IKEv2 punto a punto de VTI estática

Implementación de VPN IPsec punto a punto en Cisco ASA y Cisco Firepower NGFW
- VPN punto a punto en Cisco ASA y Cisco Firepower NGFW
- Configuración de VPN punto a punto de Cisco ASA
- Configuración de VPN punto a punto de Cisco Firepower NGFW

Presentamos las soluciones VPN de acceso remoto seguro de Cisco
- Componentes de VPN de acceso remoto
- Tecnologías VPN de acceso remoto
- Descripción general de SSL

Implementación de VPN SSL de acceso remoto en Cisco ASA y Cisco Firepower NGFW
- Conceptos de configuración de acceso remoto
- Perfiles de conexión
- Políticas de grupo
- Configuración de VPN de acceso remoto de Cisco ASA
- Configuración de VPN de acceso remoto de Cisco Firepower NGFW

Explicación de las soluciones de acceso a redes seguras de Cisco
- Acceso seguro a la red de Cisco
- Componentes de acceso seguro a la red de Cisco
- Rol de AAA en la solución de acceso seguro a la red de Cisco
- Motor de servicios de identidad de Cisco
- Cisco TrustSec

Descripción de la autenticación 802.1X
- 802.1X y EAP
- Métodos EAP
- Papel de RADIUS en comunicaciones 802.1X
- Cambio de autorización de RADIUS

Configuración de la autenticación 802.1X
- Configuración del Cisco Catalyst Switch 802.1X
- Configuración de Cisco WLC 802.1X
- Configuración de Cisco ISE 802.1X
- Configuración del solicitante 802.1x
- Autenticación web de Cisco Central

Implementing and Operating Cisco Security Core Technologies (SCOR)

Descripción de tecnologías de seguridad de terminales

- Cortafuegos personal basado en host
- Antivirus basado en host
- Sistema de prevención de intrusiones basado en host
- Listas blancas y listas negras de aplicaciones
- Protección contra malware basada en host
- Descripción general de la zona de pruebas
- Comprobación de la integridad de los archivos

Implementación de Cisco AMP para terminales

- Arquitectura de Cisco AMP para terminales
- Cisco AMP para motores de terminales
- Seguridad retrospectiva con Cisco AMP
- Trayectoria de archivos y dispositivos Cisco AMP
- Administración de Cisco AMP para terminales

Introducción a la protección de infraestructura de red

- Identificación de planos de dispositivos de red
- Controles de seguridad del plano de control
- Controles de seguridad del plano de gestión
- Telemetría de red
- Controles de seguridad del plano de datos de capa 2
- Controles de seguridad del plano de datos de capa 3

Implementación de controles de seguridad del plano de control

- ACL de infraestructura
- Vigilancia del plano de control
- Protección del plano de control
- Seguridad del protocolo de enrutamiento

Implementación de controles de seguridad del plano de datos de capa 2

- Descripción general de los controles de seguridad del plano de datos de capa 2
- Mitigación de ataques basados en VLAN
- Mitigación de ataques STP
- Seguridad Portuaria
- VLAN privadas

- Indagación DHCP
- Inspección ARP
- Control de tormentas
- Cifrado MACsec
-

Implementación de controles de seguridad del plano de datos de capa 3

- Infraestructura ACL antisupervisión
- Reenvío de ruta inversa de unidifusión
- Guardia de fuente de IP

Esquema del laboratorio

Los laboratorios están diseñados para asegurar a los alumnos una experiencia práctica completa, a través de las siguientes actividades prácticas:

- Configure las configuraciones de red y NAT en Cisco ASA
- Configure las políticas de control de acceso de Cisco ASA
- Configure Cisco Firepower NGFW NAT
- Configurar la política de control de acceso de Cisco Firepower NGFW
- Configurar la política IPS y de descubrimiento de Cisco Firepower NGFW
- Configurar la política de archivos y malware de Cisco NGFW
- Configure Listener, HAT y RAT en Cisco ESA
- Configurar políticas de correo
- Configurar servicios de proxy, autenticación y descifrado HTTPS
- Hacer cumplir el control de uso aceptable y la protección contra malware
- Examinar el panel de Umbrella
- Examinar Cisco Umbrella Investigar
- Explore la protección contra ransomware de DNS de Cisco Umbrella
- Configure el túnel IPsec IKEv2 punto a punto de VTI estático
- Configure la VPN punto a punto entre Cisco ASA y Cisco Firepower NGFW
- Configure la VPN de acceso remoto en Cisco Firepower NGFW
- Explore Cisco AMP para terminales
- Realizar análisis de endpoints con AMP para la consola de endpoints

Implementing and Operating Cisco Security Core Technologies (SCOR)

- Explore la protección contra ransomware de archivos de Cisco AMP para la consola de endpoints
- Explore Cisco Stealthwatch Enterprise v6.9.3
- Explore CTA en Stealthwatch Enterprise v7.0
- Explore el panel de Cisco Cloudlock y la seguridad del usuario
- Explore la seguridad de datos y aplicaciones de Cisco Cloudlock
- Explore Cisco Stealthwatch Cloud
- Explore la configuración de alertas en la nube, las listas de seguimiento y los sensores de Stealthwatch