CISC-21 - SCOR - IMPLEMENTING AND OPERATING CISCO SECURITY CORE TECHNOLOGIES V2.0

Categoria: **Cisco**

INFORMAZIONI SUL CORSO

Durata:	Categoria:	Qualifica Istruttore:	Dedicato a:	Produttore:
5 Giorni	Cisco	Cisco Certified Instructor	Professionista IT	Cisco

OBIETTIVI

After completing this course you should be able to:

- -Describe information security concepts and strategies within the network
- -Describe common TCP/IP, network application, and endpoint attacks
- -Describe how various network security technologies work together to guard against attacks
- -Implement access control on Cisco ASA appliance and Cisco Firepower Next-Generation Firewall
- -Describe and implement basic email content security features and functions provided by Cisco Email Security Appliance
- -Describe and implement web content security features and functions provided by Cisco Web Security Appliance
- -Describe Cisco Umbrella security capabilities, deployment models, policy management, and Investigate console
- -Introduce VPNs and describe cryptography solutions and algorithms
- -Describe Cisco secure site-to-site connectivity solutions and explain how to deploy Cisco IOS VTI-based point-to-point IPsec VPNs, and point-to-point IPsec VPN on the Cisco ASA and Cisco FirePower NGFW
- -Describe and deploy Cisco secure remote access connectivity solutions and describe how to configure 802.1X and EAP authentication
- -Provide basic understanding of endpoint security and describe AMP for Endpoints architecture and basic features
- -Examine various defenses on Cisco devices that protect the control and management plane
- -Configure and verify Cisco IOS Software Layer 2 and Layer 3 Data Plane Controls
- -Describe Cisco Stealthwatch Enterprise and Stealthwatch Cloud solutions
- -Describe basics of cloud computing and common cloud attacks and how to secure cloud environment

PREREQUISITI

Attendees should meet the following prerequisites:

- -Familiarity with Ethernet and TCP/IP networking
- -Working Knowledge of the Windows operating system
- -Working Knowledge of Cisco IOS networking and concepts
- -Familiarity with basics of networking security concepts

Recommended prerequisites:

- -CCNA - Implementing and Administering Cisco Solutions

CONTENUTI

Describing Information Security Concepts (Self-Study)

- -Information Security Overview
- -Managing Risk
- -Vulnerability Assessment
- -Understanding CVSS

Describing Common TCP/IP Attacks (Self-Study)

- -Legacy TCP/IP Vulnerabilities
- -IP Vulnerabilities
- -ICMP Vulnerabilities
- -TCP Vulnerabilities
- -UDP Vulnerabilities
- -Attack Surface and Attack Vectors
- -Reconnaissance Attacks
- -Access Attacks
- -Man-In-The-Middle Attacks
- -Denial of Service and Distributed Denial of Service Attacks
- -Reflection and Amplification Attacks
- -Spoofing Attacks
- -DHCP Attacks

Describing Common Network Application Attacks (Self-Study)

- -Password Attacks
- -DNS-Based Attacks
- -DNS Tunneling
- -Web-Based Attacks
- -HTTP 302 Cushioning
- -Command Injections
- -SQL Injections
- -Cross-Site Scripting and Request Forgery
- -Email-Based Attacks

Describing Common Endpoint Attacks (Self-Study)

- -Buffer Overflow
- -Malware
- -Reconnaissance Attack
- -Gaining Access and Control
- -Gaining Access via Social Engineering
- -Gaining Access via Web-Based Attacks
- -Exploit Kits and Rootkits
- -Privilege Escalation
- -Post-Exploitation Phase
- -Angler Exploit Kit

Describing Network Security Technologies

- -Defense-in-Depth Strategy

-Defending Across the Attack Continuum
-Network Segmentation and Virtualization Overview
-Stateful Firewall Overview
-Security Intelligence Overview
-Threat Information Standardization
-Network-Based Malware Protection Overview
-IPS Overview
-Next Generation Firewall Overview
-Email Content Security Overview
-Web Content Security Overview
-Threat Analytic Systems Overview
-DNS Security Overview
-Authentication, Authorization, and Accounting Overview
-Identity and Access Management Overview
-Virtual Private Network Technology Overview
-Network Security Device Form Factors Overview

Deploying Cisco ASA Firewall

-Cisco ASA Deployment Types
-Cisco ASA Interface Security Levels
-Cisco ASA Objects and Object Groups
-Network Address Translation
-Cisco ASA Interface ACLs
-Cisco ASA Global ACLs
-Cisco ASA Advanced Access Policies
-Cisco ASA High Availability Overview

Deploying Cisco Firepower Next-Generation Firewall

-Cisco Firepower NGFW Deployments
-Cisco Firepower NGFW Packet Processing and Policies
-Cisco Firepower NGFW Objects
-Cisco Firepower NGFW NAT
-Cisco Firepower NGFW Prefilter Policies
-Cisco Firepower NGFW Access Control Policies
-Cisco Firepower NGFW Security Intelligence
-Cisco Firepower NGFW Discovery Policies
-Cisco Firepower NGFW IPS Policies
-Cisco Firepower NGFW Malware and File Policies

Deploying Email Content Security

-Cisco Email Content Security Overview
-SMTP Overview
-Email Pipeline Overview
-Public and Private Listeners
-Host Access Table Overview
-Recipient Access Table Overview
-Mail Policies Overview
-Protection Against Spam and Graymail

- -Anti-virus and Anti-malware Protection
- -Outbreak Filters
- -Content Filters
- -Data Loss Prevention
- -Email Encryption

Deploying Web Content Security

- -Cisco WSA Overview
- -Deployment Options
- -Network Users Authentication
- -HTTPS Traffic Decryption
- -Access Policies and Identification Profiles
- -Acceptable Use Controls Settings
- -Anti-Malware Protection

Deploying Cisco Umbrella (Self-Study)

- -Cisco Umbrella Architecture
- -Deploying Cisco Umbrella
- -Cisco Umbrella Roaming Client
- -Managing Cisco Umbrella
- -Cisco Umbrella Investigate Overview

Explaining VPN Technologies and Cryptography

- -VPN Definition
- -VPN Types
- -Secure Communication and Cryptographic Services
- -Keys in Cryptography
- -Public Key Infrastructure

Introducing Cisco Secure Site-to-Site VPN Solutions

- -Site-to-Site VPN Topologies
- -IPsec VPN Overview
- -IPsec Static Crypto Maps
- -IPsec Static Virtual Tunnel Interface
- -Dynamic Multipoint VPN
- -Cisco IOS FlexVPN

Deploying Cisco IOS VTI-Based Point-to-Point

- -Cisco IOS VTIs
- -Static VTI Point-to-Point IPsec IKEv2 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

-SSL Overview

Deploying Remote Access SSL VPNs on the Cisco ASA and Cisco Firepower NGFW

-Remote Access Configuration Concepts
-Connection Profiles
-Group Policies
-Cisco ASA Remote Access VPN Configuration
-Cisco Firepower NGFW Remote Access VPN Configuration

Explaining Cisco Secure Network Access Solutions

-Cisco Secure Network Access
-Cisco Secure Network Access Components
-AAA Role in Cisco Secure Network Access Solution
-Cisco Identity Services Engine
-Cisco TrustSec

Describing 802.1X Authentication

-802.1X and EAP
-EAP Methods
-Role of RADIUS in 802.1X Communications
-RADIUS Change of Authorization

Configuring 802.1X Authentication

-Cisco Catalyst Switch 802.1X Configuration
-Cisco WLC 802.1X Configuration
-Cisco ISE 802.1X Configuration
-Supplicant 802.1x Configuration
-Cisco Central Web Authentication

Describing Endpoint Security Technologies (Self-Study)

-Host-Based Personal Firewall
-Host-Based Anti-Virus
-Host-Based Intrusion Prevention System
-Application Whitelists and Blacklists
-Host-Based Malware Protection
-Sandboxing Overview
-File Integrity Checking

Deploying Cisco AMP for Endpoints (Self-study)

-Cisco AMP for Endpoints Architecture
-Cisco AMP for Endpoints Engines
-Retrospective Security with Cisco AMP
-Cisco AMP Device and File Trajectory
-Managing Cisco AMP for Endpoints

Introducing Network Infrastructure Protection (Self-Study)

-Identifying Network Device Planes
-Control Plane Security Controls
-Management Plane Security Controls

-Network Telemetry
-Layer 2 Data Plane Security Controls
-Layer 3 Data Plane Security Controls

Deploying Control Plane Security Controls (Self-Study)

-Infrastructure ACLs
-Control Plane Policing
-Control Plane Protection
-Routing Protocol Security

Deploying Layer 2 Data Plane Security Controls (Self-Study)

-Overview of Layer 2 Data Plane Security Controls
-VLAN-Based Attacks Mitigation
-STP Attacks Mitigation
-Port Security
-Private VLANs
-DHCP Snooping
-ARP Inspection
-Storm Control
-MACsec Encryption

Deploying Layer 3 Data Plane Security Controls (Self-Study)

-Infrastructure Antispoofing ACLs
-Unicast Reverse Path Forwarding
-IP Source Guard

Labs

-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, HAT, and RAT on Cisco 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 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

INFO

Esame: 350-701 - Implementing and Operating Cisco Security Core Technologies
Materiale didattico: Materiale didattico ufficiale Cisco in formato digitale
Costo materiale didattico: incluso nel prezzo del corso a Calendario
Natura del corso: Operativo (previsti lab su PC)