

# CISC-21 - SCOR - IMPLEMENTING AND OPERATING CISCO SECURITY CORE TECHNOLOGIES (SCOR) V1.0

Categoria: Cisco

## INFORMAZIONI SUL CORSO



Durata:  
5 Giorni



Categoria:  
Cisco



Qualifica Istruttore:  
Cisco Certified  
Instructor



Dedicato a:  
Professionista IT



Produttore:  
Cisco

## OBIETTIVI

After taking 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 Internetwork Operating System (Cisco IOS®) Virtual Tunnel Interface (VTI)-based point-to-point IPsec VPNs, and point-to-point IPsec VPN on the Cisco ASA and Cisco Firepower Next-Generation Firewall (NGFW)
- Describe and deploy Cisco secure remote access connectivity solutions and describe how to configure 802.1X and Extensible Authentication Protocol (EAP) authentication
- Provide basic understanding of endpoint security and describe Advanced Malware Protection (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

To fully benefit from this course, you should have the following knowledge and skills:

- Skills and knowledge equivalent to those learned in Implementing and Administering Cisco Solutions (CCNA®) v1.0 course
- 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

These Cisco courses are recommended to help you meet these prerequisites:

- Implementing and Administering Cisco Solutions (CCNA)

## CONTENUTI

### **Describing Information Security Concepts\***

- Information Security Overview
- Assets, Vulnerabilities, and Countermeasures
- Managing Risk
- Vulnerability Assessment
- Understanding Common Vulnerability Scoring System (CVSS)

### **Describing Common TCP/IP Attacks\***

- Legacy TCP/IP Vulnerabilities
- IP Vulnerabilities
- Internet Control Message Protocol (ICMP) Vulnerabilities
- TCP Vulnerabilities
- User Datagram Protocol (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
- Dynamic Host Configuration Protocol (DHCP) Attacks

### **Describing Common Network Application Attacks\***

- Password Attacks
- Domain Name System (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\***

- 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
- Intrusion Prevention System (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 Access Control Lists (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 Network Address Translation (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
- Simple Mail Transfer Protocol (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 Web Security Appliance (WSA) Overview
- Deployment Options
- Network Users Authentication
- Secure HTTP (HTTPS) Traffic Decryption
- Access Policies and Identification Profiles
- Acceptable Use Controls Settings
- Anti-Malware Protection

### **Deploying Cisco Umbrella\***

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

### **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 IPsec VPNs**

- Cisco IOS VTIs
- Static VTI Point-to-Point IPsec Internet Key Exchange (IKE) v2 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
- Secure Sockets Layer (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 Extensible Authentication Protocol (EAP)
- EAP Methods
- Role of Remote Authentication Dial-in User Service (RADIUS) in 802.1X Communications
- RADIUS Change of Authorization

### **Configuring 802.1X Authentication**

- Cisco Catalyst® Switch 802.1X Configuration
- Cisco Wireless LAN Controller (WLC) 802.1X Configuration
- Cisco Identity Services Engine (ISE) 802.1X Configuration
- Supplicant 802.1x Configuration
- Cisco Central Web Authentication

### **Describing Endpoint Security Technologies\***

- 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 Advanced Malware Protection (AMP) for Endpoints\***

- 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\***

- 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\***

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

### **Deploying Layer 2 Data Plane Security Controls\***

- Overview of Layer 2 Data Plane Security Controls
- Virtual LAN (VLAN)-Based Attacks Mitigation
- Spanning Tree Protocol (STP) Attacks Mitigation
- Port Security
- Private VLANs
- Dynamic Host Configuration Protocol (DHCP) Snooping
- Address Resolution Protocol (ARP) Inspection
- Storm Control
- MACsec Encryption

### **Deploying Layer 3 Data Plane Security Controls\***

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

### **Deploying Management Plane Security Controls\***

- Cisco Secure Management Access
- Simple Network Management Protocol Version 3
- Secure Access to Cisco Devices
- AAA for Management Access

### **Deploying Traffic Telemetry Methods\***

- Network Time Protocol
- Device and Network Events Logging and Export
- Network Traffic Monitoring Using NetFlow

### **Deploying Cisco Stealthwatch Enterprise\***

- Cisco Stealthwatch Offerings Overview
- Cisco Stealthwatch Enterprise Required Components
- Flow Stitching and Deduplication
- Stealthwatch Enterprise Optional Components
- Stealthwatch Enterprise and ISE Integration

- Cisco Stealthwatch with Cognitive Analytics
- Cisco Encrypted Traffic Analytics
- Host Groups
- Security Events and Alarms
- Host, Role, and Default Policies

### **Describing Cloud and Common Cloud Attacks\***

- Evolution of Cloud Computing
- Cloud Service Models
- Security Responsibilities in Cloud
- Cloud Deployment Models
- Common Security Threats in Cloud
- Patch Management in the Cloud
- Security Assessment in the Cloud

### **Securing the Cloud\***

- Cisco Threat-Centric Approach to Network Security
- Cloud Physical Environment Security
- Application and Workload Security
- Cloud Management and API Security
- Network Function Virtualization (NFV) and Virtual Network Functions (VNF)
- Cisco NFV Examples
- Reporting and Threat Visibility in Cloud
- Cloud Access Security Broker
- Cisco CloudLock®
- OAuth and OAuth Attacks

### **Deploying Cisco Stealthwatch Cloud\***

- Cisco Stealthwatch Cloud for Public Cloud Monitoring
- Cisco Stealthwatch Cloud for Private Network Monitoring
- Cisco Stealthwatch Cloud Operations

### **Describing Software-Defined Networking (SDN\*)**

- Software-Defined Networking Concepts
- Network Programmability and Automation
- Cisco Platforms and APIs
- Basic Python Scripts for Automation

\* This section is self-study material that can be done at your own pace if you are taking the instructor-led version of this course.

### **Lab outline**

- 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, Host Access Table (HAT), and Recipient Access Table (RAT) on Cisco Email Security

- Appliance (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 Cognitive Threat Analytics (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)