CS-SCOR

CCNP SECURITY SCOR 350-701

DURATION	LEVEL	TECHNOLOGY	DELIVERY METHOD	TRAINING CREDITS
5 Days	Professional	Cisco Security	ILT / VILT	NA

INTRODUCTION

This course covers core security technologies, including cybersecurity fundamentals, network security, cloud security, identity management, secure network access, endpoint protection and detection, and visibility and enforcement.

AUDIENCE PROFILE

This course is primarily intended for:

- Cisco partners and integrators, Network engineers, Technical solutions architect
- Individuals preparing for the CCNP Security Certification

PREREQUISITES

There are no formal prerequisites for CCNP Security. In other words, you do not have to pass the CCNA Security or any other certifications in order to take CCNP-level exams. On the other hand, CCNP candidates often have three to five years of experience in IT and cybersecurity.

The ideal knowledge and skills that a learner should have before attending this course are as follows:

- Knowledge of implementing and operating core security technologies
- Understanding of cloud security
- Hands-on experience with next-generation firewalls, intrusion prevention systems (IPSs), and other network infrastructure devices
- Understanding of content security, endpoint protection and detection, and secure network access, visibility, and enforcement
- Understanding of cybersecurity concepts with hands-on experience in implementing security controls

COURSE OBJECTIVES

On completion of this course, participants should be familiar with:

Monitoring and Reporting:

- Explain common threats against on-premises and cloud environments
- Compare common security vulnerabilities such as software bugs, weak and/or hardcoded passwords, SQL injection, missing encryption, buffer overflow, path traversal, cross-site scripting/forgery
- Describe functions of the cryptography components such as hashing, encryption, PKI, SSL, IPsec, NAT-T IPv4 for IPsec, pre-shared key, and certificate-based authorization
- Compare site-to-site VPN and remote access VPN deployment types such as sVTI, IPsec, Cryptomap, DMVPN, FLEXVPN, including high availability considerations, and AnyConnect
- Describe security intelligence authoring, sharing, and consumption
- Explain the role of the endpoint in protecting humans from phishing and social engineering attacks
- Explain northbound and southbound APIs in the SDN architecture
- Explain DNAC APIs for network provisioning, optimization, monitoring, and troubleshooting
- Interpret basic Python scripts used to call Cisco Security appliances APIs

Network Security:

- Compare network security solutions that provide intrusion prevention and firewall capabilities
- Describe deployment models of network security solutions and architectures that provide intrusion prevention and firewall capabilities
- Describe the components, capabilities, and benefits of NetFlow and Flexible NetFlow records
- Configure and verify network infrastructure security methods (router, switch, wireless)
- Implement segmentation, access control policies, AVC, URL filtering, and malware protection
- Implement management options for network security solutions such as intrusion prevention and perimeter security (single vs. multidevice manager, in-band vs. out-of-band, CDP, DNS, SCP, SFTP, and DHCP security and risks)
- Configure AAA for device and network access (authentication and authorization, TACACS+, RADIUS and RADIUS flows, accounting, and dACL)
- Configure secure network management of perimeter security and infrastructure devices (secure device management, SNMPv3, views, groups, users, authentication, encryption, secure logging, and NTP with authentication)
- Configure and verify site-to-site VPN and remote access VPN

Securing the Cloud:

- Implement traffic redirection and capture methods
- Describe web proxy identity and authentication, including transparent user identification
- Compare the components, capabilities, and benefits of local and cloud-based email and web solutions (ESA, CES, WSA)
- Configure and verify web and email security deployment methods to protect on-premises and remote users (inbound and outbound controls and policy management)
- Configure and verify email security features such as SPAM filtering, antimalware filtering, DLP, blacklisting, and email encryption
- Configure and verify secure Internet gateway and web security features such as blacklisting, URL filtering, malware scanning, URL categorization, web application filtering, and TLS decryption
- Describe the components, capabilities, and benefits of Cisco Umbrella
- Configure and verify web security controls on Cisco Umbrella (identities, URL content settings, destination lists, and reporting)

Endpoint Protection and Detection:

- Compare Endpoint Protection Platforms (EPPs) and Endpoint Detection & Response (EDR) solutions
- Explain antimalware, retrospective security, Indication of Compromise (IOC), antivirus, dynamic file analysis, and endpoint-sourced telemetry
- Configure and verify outbreak control and quarantines to limit infection
- Describe justifications for endpoint-based security
- Describe the value of endpoint device management and asset inventory such as MDM
- Describe the uses and importance of a multifactor authentication (MFA) strategy
- Describe endpoint posture assessment solutions to ensure endpoint security
- Explain the importance of an endpoint patching strategy

Secure Network Access, Visibility, and Enforcement:

- Describe identity management and secure network access concepts such as guest services, profiling, posture assessment, and BYOD
- Configure and verify network access device functionality such as 802.1X, MAB, and WebAuth
- Describe network access with CoA
- Describe the benefits of device compliance and application control
- Explain exfiltration techniques (DNS tunneling, HTTPS, email, FTP/SSH/SCP/FTP, ICMP, Messenger, IRC, and NTP)
- Describe the benefits of network telemetry
- Describe the components, capabilities, and benefits of these security products and solutions:
- Cisco Stealthwatch
- Cisco Stealthwatch Cloud
- Cisco pxGrid
- Cisco Umbrella Investigate
- Cisco Cognitive Threat Analytics
- Cisco Encrypted Traffic Analytics
- Cisco AnyConnect Network Visibility Module (NVM)

COURSE CONTENT

Lesson 1: Cybersecurity Fundamentals

- Introduction to Cybersecurity
- Defining What Are Threats, Vulnerabilities, and Exploits
- Common Software and Hardware Vulnerabilities
- Confidentiality, Integrity, and Availability
- Cloud Security Threats
- IoT Security Threats
- An Introduction to Digital Forensics and Incident Response

Lesson 2: Cryptography

- Introduction to Cryptography
- Fundamentals of PKI

Lesson 3: Software-Defined Networking Security and Network ProgrammabilityFailure

- Introduction to Software-Defined Networking
- Introduction to Network Programmability 132

Lesson 4: Authentication, Authorization, Accounting (AAA) and Identity Management

- Introduction to Authentication, Authorization, and Accounting
- Authentication
- Authorization
- Accounting
- Infrastructure Access Controls
- AAA Protocols
- Cisco Identity Services Engine (ISE)
- Configuring TACACS+ Access
- Configuring RADIUS Authentication
- Sizing a Cisco ISE Distributed Deployment

Lesson 5: Network Visibility and Segmentation

- Introduction to Network Visibility
- NetFlow
- IP Flow Information Export (IPFIX)
- NetFlow Deployment Scenarios
- Cisco Stealthwatch
- Cisco Cognitive Threat Analytics (CTA) and Encrypted Traffic Analytics (ETA)
- NetFlow Collection Considerations and Best Practices
- Configuring NetFlow in Cisco IOS and Cisco IOS-XE
- Configuring NetFlow in NX-OS
- Introduction to Network Segmentation
- Micro-Segmentation with Cisco ACI
- Segmentation with Cisco ISE

Lesson 6: Infrastructure Security

- Securing Layer 2 Technologies
- Common Layer 2 Threats and How to Mitigate Them
- Network Foundation Protection
- Understanding and Securing the Management Plane
- Understanding the Control Plane
- Understanding and Securing the Data Plane
- Securing Management Traffic
- Implementing Logging Features
- Configuring NTP
- Securing the Network Infrastructure Device Image and Configuration Files
- Securing the Data Plane in IPv6
- Securing Routing Protocols and the Control Plane

Lesson 7: Cisco Next-Generation Firewalls and Cisco Next-Generation Intrusion Prevention Systems

- Introduction to NGFW and NGIPS
- Comparing Network Security Solutions that Provide Firewall Capabilities
- Deployment Modes of Network Security Solutions and Architectures That
- Provide Firewall Capabilities
- High Availability and Clustering
- Implementing Access Control
- Cisco Firepower Intrusion Policies
- Cisco Advanced Malware Protection (AMP)
- Security Intelligence, Security Updates, and Keeping Firepower Software up to Date

Lesson 8: Virtual Private Networks (VPNs)

- Virtual Private Network (VPN) Fundamentals
- Deploying and Configuring Site-to-Site VPNs in Cisco Routers
- Configuring Site-to-Site VPNs in Cisco ASA Firewalls
- Configuring Remote Access VPNs in the Cisco ASA
- Configuring Clientless Remote Access SSL VPNs in the Cisco ASA
- Configuring Client-Based Remote-Access SSL VPNs in the Cisco ASA
- Configuring Remote Access VPNs in FTD
- Configuring Site-to-Site VPNs in FTD

Lesson 9: Securing the Cloud

- What Is Cloud and What Are the Cloud Service Models?
- DevOps, Continuous Integration (CI), Continuous Delivery (CD), and DevSecOps
- Describing the Customer vs. Provider Security Responsibility for the Different Cloud Service Models
- Cisco Umbrella
- Cisco Email Security in the Cloud
- Cisco Cloudlock
- Stealthwatch Cloud
- AppDynamics Cloud Monitoring
- Cisco Tetration

Lesson 10: Content Security

- Content Security Fundamentals
- Cisco WSA
- Cisco ESA
- Cisco Content Security Management Appliance (SMA)

Lesson 11: Endpoint Protection and Detection

- Introduction to Endpoint Protection and Detection
- Cisco AMP for Endpoints
- Cisco Threat Response

ASSOCIATED CERTIFICATIONS & EXAM

The Implementing and Operating Cisco Security Core Technologies (SCOR 350-701) exam is the required “core” exam for the CCNP Security and CCIE Security certifications. If you pass the SCOR 350-701 exam, you will also obtain the Cisco Certified Specialist – Security Core Certification.