

Days: 5

Prerequisites: No formal prerequisites. Recommended preparation includes Ethernet and TCP/IP, Windows, Cisco IOS, and basic network security knowledge. CCNA training provides relevant foundational skills.

Audience: Security and networking professionals, systems engineers, architects, Cisco partners, and network, program, and project managers.

Description: Implementing and Operating Cisco Security Core Technologies v3 develops practical skills for protecting enterprise environments with Cisco solutions. Instruction and labs address network and cloud protection, identity-based access, endpoint defense, and security operations.

The course prepares participants for the 350-701 SCOR v2.0 exam. Passing earns Cisco Certified Specialist - Security Core and fulfills the core exam requirement for CCNP Security and CCIE Security. Additional requirements apply to those certifications.

This training earns 30 Cisco Continuing Education credits toward recertification.

Course Objectives: Participants will learn to:

- Assess threat actors, vulnerabilities, AI risks, and identity abuse.
- Explain cryptography, Zero Trust, SAFE, and Layer 2 defenses.
- Harden infrastructure and troubleshoot administrative AAA.
- Configure Cisco Secure Firewall, security policies, and VPN connectivity.
- Evaluate cloud protection, workload segmentation, eBPF, and DevSecOps.
- Explain SASE and SSE and configure private and internet access.
- Apply Cisco ISE access controls and explain Duo identity protection.
- Explain email protection, endpoint trust, EDR, and malware analysis.
- Explore Splunk analytics, SOAR automation, and Cisco XDR response

OUTLINE:

LESSON 1. THREAT INTELLIGENCE AND CYBER ADVERSARIES

LESSON 2. VULNERABILITY ASSESSMENT AND AI EXPOSURE

LESSON 3. PHISHING AND ABUSE OF IDENTITIES

LESSON 4. CRYPTOGRAPHY AND TRUST

LESSON 5. SECURING LAYER 2 NETWORKS

LESSON 6. ZERO TRUST ARCHITECTURE AND CISCO SAFE

LESSON 7. HARDENING DEVICES AND ADMINISTRATIVE ACCESS

LESSON 8. TROUBLESHOOTING AAA ADMINISTRATION

LESSON 9. DEPLOYING CISCO SECURE FIREWALL THREAT DEFENSE

LESSON 10. FIREWALL ACCESS AND THREAT POLICIES

LESSON 11. VPN CONNECTIONS BETWEEN SITES

LESSON 12. VPN CONNECTIONS FOR REMOTE USERS

LESSON 13. CLOUD FRAMEWORKS AND RESPONSIBILITY MODELS

LESSON 14. WORKLOAD SEGMENTATION AND EBPF PROTECTION

LESSON 15. DEVSECOPS PRACTICES AND API AUTOMATION

LESSON 16. CISCO DUO IDENTITY VERIFICATION

LESSON 17. ARCHITECTURES FOR SASE AND SSE

LESSON 18. DEPLOYING PRIVATE APPLICATION ACCESS
LESSON 19. DEPLOYING INTERNET AND SAAS ACCESS
LESSON 20. IDENTITY AND ACCESS CONTROL FUNDAMENTALS
LESSON 21. CISCO ISE CONTROLS USING 802.1X MAB AND COA
LESSON 22. EMAIL DEFENSE WITH CISCO ETD
LESSON 23. ENDPOINT COMPLIANCE AND DEVICE TRUST
LESSON 24. EDR CAPABILITIES AND MALWARE INVESTIGATION
LESSON 25. SECURITY DATA ANALYSIS WITH SPLUNK
LESSON 26. SOC ORCHESTRATION THROUGH SOAR
LESSON 27. DETECTION AND RESPONSE THROUGH XDR

HANDS-ON LABS:

- HARDEN CISCO IOS XE DEVICES
- AUTHENTICATE OSPFV3 ROUTING
- ADMINISTER DEVICES THROUGH TACACS+
- SET UP CISCO SECURE FIREWALL
- MANAGE FIREWALL SECURITY POLICIES
- CONFIGURE SITE VPN CONNECTIVITY
- CONFIGURE REMOTE USER VPN ACCESS
- DEPLOY PRIVATE ACCESS CONTROLS
- DEPLOY INTERNET ACCESS CONTROLS
- CONFIGURE ISE MAB AND WIRED 802.1X
- EXPLORE CISCO EMAIL THREAT DEFENSE
- EXPLORE CISCO ENDPOINT PROTECTION
- CONNECT FIREWALL TELEMETRY TO SPLUNK
- EXPLORE CISCO XDR