Implementing and Operating Cisco Security Core Technologies v2.0 (350-701)

Exam Description: Implementing and Operating Cisco Security Core Technologies v2.0 (SCOR 350-701) is a 120-minute exam associated with the CCNP and CCIE Security Certifications. This exam tests a candidate's knowledge of implementing and operating core security technologies including network security, cloud security, secure service edge, endpoint protection and detection, network access, visibility, and enforcements. The course, Implementing and Operating Cisco Security Core Technologies, helps candidates to prepare for this exam.

The following topics are general guidelines for the content likely to be included on the exam. However, other related topics may also appear on any specific delivery of the exam. To better reflect the contents of the exam and for clarity purposes, the guidelines below may change at any time without notice.

20% 1.0 Security Concepts

- 1.1 Explain attack threats against on-premises, hybrid, and cloud environments such as viruses, trojans, DoS/DDoS, phishing, rootkits, man-in-the middle, malware, data breaches, insecure APIs, compromised credentials, PQC, and AI
- 1.2 Describe security vulnerabilities and exploits such as software bugs, weak and/or hardcoded passwords, OWASP top ten, missing encryption ciphers, buffer overflow, path traversal, cross-site scripting/forgery, SQL injection, and identification and prioritization using CVEs and CVSS scores
- 1.3 Describe vulnerabilities in AI/LLM models such as prompt injection, system prompt leakage, vector and embedding weaknesses, and supply chain
- 1.4 Describe the controls used to protect against phishing and social engineering attacks
- 1.5 Describe cryptography security components such as hashing, encryption, PKI, SSL, TLS, QUIC, MASQUE, IPsec, NAT-T IPv4 for IPsec, preshared key, certificate-based authorization, and post-quantum cryptography
- 1.6 Describe site-to-site and remote access VPN deployment types such as virtual tunnel interfaces, standards-based IPsec, SSL VPN, DMVPN, FlexVPN, and GETVPN
- 1.7 Describe security intelligence authoring, sharing, and consumption
- 1.8 Describe zero trust architecture
- 1.9 Describe defense in depth strategy such as Secure Architecture for Everyone (SAFE)
- 1.10 Interpret scripts used to call security appliances APIs in a language such as Python

25% 2.0 Network Security

- 2.1 Describe network security solutions and deployment models that provide intrusion prevention and firewall capabilities
- 2.2 Describe security monitoring and telemetry technologies

	2.3	Configure network infrastructure security methods (network segmentation using VLANs or SGTs; Layer 2 and port security; DHCP snooping; Dynamic ARP inspection; storm control; and defenses against MAC, ARP, VLAN hopping, STP, and DHCP rogue attacks)
	2.4	Select management options for network security solutions (single vs. multidevice manager, in-band vs. out-of-band, on-premises vs. cloud with Cisco Security Cloud Control)
	2.5	Describe CIS benchmarks for hardening devices such as Cisco Secure Firewall (FTD) and Cisco IOS XE
	2.6	Troubleshoot AAA for device and network access such as TACACS+ and RADIUS
	2.7	Configure secure network management of perimeter security and infrastructure devices such as SNMPv3, NetConf, RestConf, APIs, secure syslog, and NTP with authentication
	2.8	Implement access control policies, AVC, URL filtering, malware protection, and intrusion prevention using Cisco Secure Firewall (FTD)
	2.9	Configure site-to-site and remote access VPN using Cisco Secure Firewall (FTD) and Cisco Secure Client
	2.10	Troubleshoot VPN tunnel establishment on Cisco Secure Firewall (FTD)
15%	**3.0**	**Cloud Security**
	3.1	Describe security responsibility within common Cloud Shared Responsibility Models
	3.2	Select security capabilities, deployment models, cloud security frameworks, and policy management to secure the cloud
	3.3	Select security solutions for cloud environments (public; private; hybrid; community cloud; NIST 800-145 SaaS, PaaS, and IaaS; and Cloud Access Security Broker)
	3.4	Describe network, application, and data security in cloud environments with solutions such as Cisco Multicloud Defense and Cisco Secure Workload
	3.5	Configure Splunk to ingest cloud logging and monitoring data from other security solutions
	3.6	Describe application and workload security concepts including eBPF
	3.7	Describe DevSecOps (Infrastructure as Code security, CI/CD pipeline, container orchestration, and secure software development)
10%	**4.0**	**Secure Service Edge**
	4.1	Describe Security Service Edge (SSE) and Secure Access Service Edge (SASE)
	4.2	Configure Cisco Secure Access Secure Internet Access
	4.3	Configure Cisco Secure Access Secure Private Access
	4.4	Configure data loss prevention and AI guardrails for secure internet access
	4.5	Interpret Cisco Secure Access Investigate scores and indicators

15% 5.0 Endpoint Protection and Detection

5.1 Describe Endpoint Protection Platforms (EPP) and Endpoint Detection and Response (EDR) solutions

5.2 Describe endpoint device management and asset inventory systems such as MDM

5.3 Describe endpoint posture assessment solutions to ensure endpoint security

5.4 Describe endpoint protection and detection security with solutions such as Cisco Secure Client and Cisco Secure Malware Analytics

5.5 Configure endpoint antimalware protection using Cisco Secure Endpoint

5.6 Interpret Cisco Secure Endpoint malware detection events

5.7 Configure email security features with Cisco Security Email Threat Defense

15% 6.0 Network Access, Visibility, and Enforcement

6.1 Describe identity management and secure network access concepts such as guest services, profiling, posture assessment, and BYOD

6.2 Describe device compliance and application control

6.3 Configure network access control mechanisms such as 802.1X and MAB with Cisco Identity Services Engine

6.4 Configure network access with CoA

6.5 Explain exfiltration techniques such as DNS tunneling, HTTPS, email, FTP/SSH/SCP/SFTP, ICMP, Messenger, IRC, NTP, and cloud storage

6.6 Describe network visibility and enforcement using telemetry and native AI/ML capabilities with XDR and SIEM/SOAR platforms such as Splunk and Cisco XDR

6.7 Describe Cisco Duo in a zero-trust security architecture (Trust Monitor, MFA, Device Trust, health checks, Adaptive Access policies, SSO, and CII)

6.8 Describe managing, orchestrating, and automating security information and events with Splunk