CISC-21 - SCOR - IMPLEMENTING AND OPERATING CISCO SECURITY CORE TECHNOLOGIES V3.0

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:

- Explain how different threat actors operate by describing their motivations, common attack vectors, typical breach and credential-abuse patterns, and the role of the cyber threat intelligence lifecycle in helping organizations understand and track these evolving threats
- Describe how structural weaknesses in software and web applications are identified, classified, and prioritized using concepts such as vulnerability classes, OWASP, CVE, and CVSS, and explain how AI/LLM systems extend this landscape with new vulnerability patterns
- Explain why humans and identity remain a primary attack vector by describing social-engineering and credential-theft lifecycles and by outlining the key conceptual defense layers that organizations apply to reduce, but not completely remove, identity-driven risk
- Describe the main cryptographic building blocks, hashing, symmetric and asymmetric encryption, key exchange, digital signatures, PKI, and encrypted transport protocols, and explain the specific security guarantees and trust assumptions each introduces into an enterprise design
- Explain how Zero Trust, defense in depth, and the Cisco SAFE Blueprint framework together turn threat, vulnerability, identity, and cryptographic insights into a coherent security architecture that assumes failure, limits blast radius, and guides technology placement across the environment
- Describe why the Layer 2 access network is a foundational security boundary by explaining how segmentation, topology, addressing, neighbor discovery, and edge-port controls work together to prevent local attacks from undermining higher-layer security
- Describe how to secure network infrastructure devices by reducing their attack surface, protecting management and control planes as privileged authority channels, and choosing management-plane architectures that create clear, defensible trust boundaries
- Explain how to design and operate AAA for infrastructure administration by choosing appropriate protocols, defining AAA and fallback behavior, and systematically troubleshooting AAA failures to restore secure administrative access
- Perform Cisco Secure Firewall Threat Defense Basic Setup
- Configure access control policy with intrusion policy, file and malware policy to meet given security requirements
- Configure secure site-to-site VPN solutions to establish connectivity between remote sites using Cisco Secure Firewall Threat Defense
- Configure remote access VPN solutions on Cisco Secure Firewall Threat Defense to provide secure connectivity to the corporate network for remote users

- Evaluate cloud security strategies using NIST 800-145 shared responsibility models, security frameworks, and CASB solutions for multicloud environments
- Describe cloud workload security strategies encompassing microsegmentation principles, Cisco Secure Workload, Multicloud Defense platforms, and eBPF-based security approaches
- Describe DevSecOps and Infrastructure as Code principles and interpret Python scripts to call security appliances API
- Describe SASE and SSE architectures and Cisco Secure Access capabilities providing unified, cloud-delivered protection of private applications and the internet across remote and branch environments
- Configure cloud-delivered connectivity, identity-aware authentication, and granular access policies to provide secure access to private applications for remote and branch users
- Configure connectivity identity, and security controls to provide secure access to the internet and SaaS applications for remote and branch users
- Explain how identity, device context, and policy-driven access control work together in secure network access solutions, and describe how Cisco ISE supports differentiated access through AAA, guest access, profiling, and BYOD
- Configure wired and wireless network access control with Cisco ISE by implementing 802.1X and MAB, applying Cisco ISE authentication and authorization policy, selecting appropriate EAP and supplicant approaches, and using RADIUS and CoA to enforce the change access state
- Explain how Cisco Duo supports zero-trust principles through strong user verification, device trust, adaptive access policy, and identity-risk visibility with Cisco Identity Intelligence
- Explain how Cisco Secure Email Threat Defense is integrated and configured in Microsoft 365-based email environments to provide message visibility, threat analysis, and remediation against phishing, business email compromise, and account takeover
- Explain how organizations build, validate, and enforce endpoint trust through device management, asset visibility, compliance and posture assessment, and application control to reduce endpoint security risk
- Explain how modern endpoint security, such as Cisco Secure Endpoint with Cisco Secure Malware Analytics, combines prevention, continuous detection, malware analysis, and event-driven investigation by using Endpoint Protection Platform (EPP) and Endpoint Detection and Response (EDR) concepts
- Describe how Splunk Enterprise and Splunk Cloud function as data analytics platforms for security operations, explain how Splunk platform components and deployment models support scalable data processing and analytics, construct queries using Splunk Processing Language to search and analyze the ingested data, explain how Cisco security products are integrated into Splunk, and describe how Splunk Enterprise extends the platform with SIEM capabilities
- Explain how Splunk SOAR supports SOC operations through orchestration, playbook automation, and case-driven response, and describe how it works with Splunk Enterprise Security and Cisco XDR to automate investigation and response workflows
- Explain how XDR unifies threat detection, investigation, and response across multiple security domains, and describe how Cisco XDR provides cross-domain visibility, correlation, prioritization, investigation, and coordinated and automated response across integrated security controls

PREREQUISITI

There are no prerequisites for this training. However, the knowledge and skills you are recommended to have before attending this training are:

- 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

Course Outline

-Modern Cyber Threat Analysis and Intelligence
-Vulnerabilities, Exploits, and AI Risks
-Social Engineering, Identity Abuse, and Phishing Controls
-Cryptographic Foundations
-Layer 2 Security
-Design Principles: Zero Trust and SAFE
-Device Hardening and Secure Management
-AAA Troubleshooting for Device Admin Access
-Cisco Secure Firewall Threat Defense Deployment
-Cisco Secure Firewall Security Policies
-Site-to-Site VPN Solutions
-Remote Access VPN Solutions
-Cloud Security Models and Frameworks
-Secure Cloud Workloads and eBPF
-DevSecOps and Security Automation
-Zero Trust Identity with Cisco Duo
-SASE and SSE Architecture
-Secure Private Access Implementation
-Secure Internet Access Implementation
-Identity and Access Management Foundations
-Configuring 802.1X, MAB, and CoA with Cisco ISE
-Cisco Secure Email Threat Defense (ETD)
-Endpoint Trust, Compliance, and Device Management
-Modern EDR and Malware Analytics
-Splunk and Security Analytics
-SOC Automation and SOAR
-Extended Detection and Response (XDR)

Lab Outline

-Cisco IOS XE Device Hardening
-OSPFv3 Routing Protocol Authentication
-TACACS+ Network Device Administration
-Cisco Secure Firewall Initial Setup
-Cisco Secure Firewall Policy Management
-Cisco Secure Firewall Site-to-Site VPN
-Cisco Secure Firewall Remote Access VPN
-Implement Secure Private Access
-Implement Secure Internet Access
-Cisco ISE MAB and Wired 802.1X
-Cisco Secure Email Threat Defense

-Cisco Secure Endpoint
-Cisco Secure Firewall Integration with Splunk
-Cisco XDR

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)