FUTURE PATH
INFOCAMPUS

www.teaminfocampus.com

CCIE SECURITY V6

About Infocampus

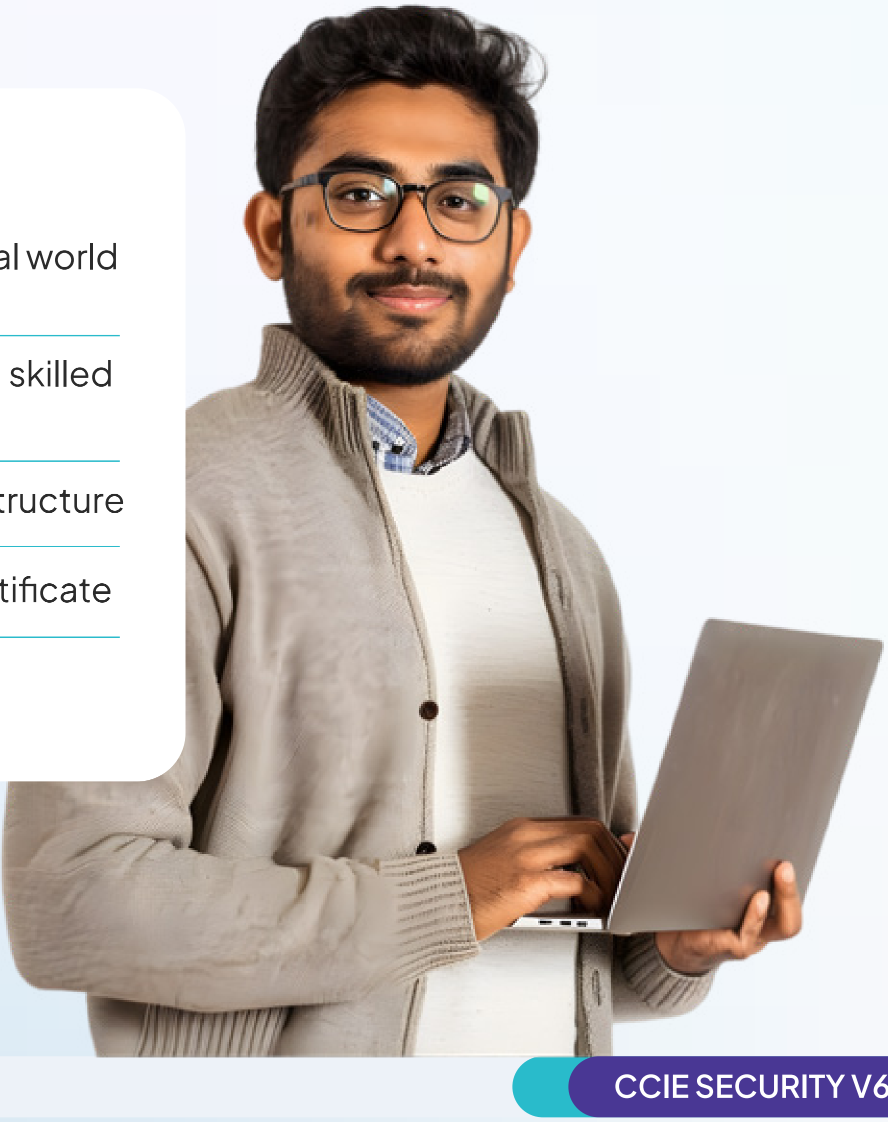
Infocampus is a community of learners, educators, and industry professionals dedicated to creating a supportive and dynamic learning environment. Since 2009, we have specialized in IT and networking courses for both beginners and professionals, bridging the gap between theory and practice. Our mission is to prepare students for the evolving tech industry, making us a trusted choice for career advancement in technology.

15+ Years of Expertise

5K+ Successful Graduates

Key Features

- Hands on training for real world application
- Highly experienced and skilled faculties
- State-of-the-Art Infrastructure
- Course completion certificate
- Job Assistance



Duration
5
Months

CCIE Security V6

Cisco Certified Internetwork Expert

The CCIE Security Version 6.0 (CCIE Security V6) course is a premier certification program offered by Cisco Systems, designed to equip network professionals with the highest level of expertise in network security. Recognized globally for its prestige and rigor, this certification is highly sought after by employers and provides exceptional career growth opportunities. The CCIE Security V6 course is an extensive and integrated program that combines advanced Cisco Routing & Switching with cutting-edge Cisco Network Security technologies. It aims to develop comprehensive skills in designing, implementing, and managing secure network infrastructures. Participants will gain deep knowledge and hands-on experience in areas such as threat defense, advanced malware protection, next-generation firewall capabilities, secure network access, and virtualization security. This course is ideal for experienced network engineers and security professionals who aspire to achieve the highest level of technical proficiency in network security. By completing the CCIE Security V6 course, candidates will be well-prepared to tackle the challenges of modern network security and will stand out as experts in their field.

Course Curriculum

Perimeter Security and Intrusion Prevention (20%)

Deployment modes on Cisco ASA & Cisco FTD

- Routed
- Transparent
- Single
- Multi-instance
- Multi-context

Firewall features on Cisco ASA & FTD

- NAT
- Application inspection
- Traffic zones
- Policy-based routing
- Traffic redirection to service modules
- Identity firewall

Security features on Cisco IOS/IOS XE

- Application awareness
- Zone-based firewall
- NAT

Cisco FMC features

- Alerting
- Logging
- Reporting
- Dynamic objects

Cisco NGIPS deployment modes

- In-line
- passive
- TAP

Cisco NGFW features

- SSL inspection
- Geolocation
- User identity
- AVC

Detect and mitigate common types of attacks

- Spoofing
- Evasion techniques
- DoS/DDoS
- Man-in-the-middle
- Botnet

Policies and rules for traffic control on Cisco ASA and Cisco FTD

Routing protocols security on Cisco IOS, Cisco ASA, and Cisco FTD

Clustering and high availability features on Cisco ASA and Cisco FTD

Network connectivity through Cisco ASA and Cisco FTD

Correlation and remediation rules on Cisco FMC

Secure Connectivity and Segmentation (20%)

Cisco AnyConnect client-based, remote-access VPN technologies on Cisco ASA, Cisco FTD, and Cisco routers

Firewall features on Cisco ASA & FTD

FlexVPN, DMVPN, and IPsec L2L tunnels

VPN high availability methods

- Cisco ASA VPN clustering
- Dual-hub DMVPN deployments

Infrastructure segmentation methods

- VLAN
- PVLAN
- GRE
- VRF-Lite
- Microsegmentation with Cisco TrustSec using SFT and SXP

Security Infrastructure (15%)

Device hardening techniques & control plane protection methods

- CoPP
- IP source routing
- iACLs

Management plane protection techniques

- CPU
- Memory thresholding
- Securing device access

Data plane protection techniques

- uRPF
- QoS
- RTBH

Layer 2 security techniques

- DAI
- STP security
- Port security
- DHCP snooping
- RA Guard
- IPDT
- VACL

Wireless security technologies

- WPA
- WPA2
- WPA3
- AES
- TKIP

Monitoring protocols

- NetFlow/IPFIX/NSEL
- SNMP
- SYSLOG

Security features to comply with organizational security policies, procedures, and standards BCP 38

- ISO 27001
- RFC 2827
- PCI-DSS

Cisco SAFE model to validate network security design and to identify threats to different PINs

Interaction with network devices through APIs using basic Python scripts

- REST API requests and responses
- Data encoding formats

Cisco DNAC Northbound APIs use cases

- Authentication and authorization
- Network discovery
- Network device
- Network host

Identity Management, Information Exchange, & Access Control (25%)

Cisco ISE scalability using multiple nodes and personas

Cisco switches and Cisco Wireless LAN Controllers for network access AAA with Cisco ISE

Cisco devices for administrative access with Cisco ISE

AAA for network access with 802.1X and MAB using Cisco ISE

Guest lifecycle management using Cisco ISE and Cisco WLC

BYOD on-boarding and network access flows

Cisco ISE integration with external identity sources

- LDAP
- AD
- External RADIUS

Provisioning Cisco AnyConnect with Cisco ISE and Cisco ASA

Posture assessment with Cisco ISE

Endpoint profiling using Cisco ISE and Cisco network infrastructure including device sensor

Integration of MDM with Cisco ISE

Certification-based authentication using Cisco ISE

Authentication methods

- EAP Chaining and TEAP
- MAR

Identity mapping on Cisco ASA, Cisco ISE, Cisco WSA, and Cisco FTD

pxGrid integration between security devices Cisco WSA, Cisco ISE, and Cisco FMC

Integration of Cisco ISE with multifactor authentication

Access control and single sign-on using Cisco DUO security technology

Cisco IBNS 2.0 (C3PL) for authentication, access control, and user policy enforcement

Advanced Threat Protection & Content Security (20%)

Cisco AMP for networks, Cisco AMP for endpoints, and Cisco AMP for content security (Cisco ESA, and Cisco WSA)

Detect, analyze, and mitigate malware incidents

Perform packet capture and analysis using Wireshark, tcpdump, SPAN, ERSPAN, and RSPAN

Cloud security

- DNS proxy through Cisco Umbrella virtual appliance
- DNS security policies in Cisco Umbrella
- RBI policies in Cisco Umbrella
- CASB policies in Cisco Umbrella
- DLP policies in Cisco Umbrella

Web filtering, user identification, and Application Visibility and Control (AVC) on Cisco FTD and CiscoWSA

WCCP redirection on Cisco devices

Email security features

- Mail policies
- DLP
- Quarantine
- Authentication
- Encryption

HTTP decryption and inspection on Cisco FTD, Cisco WSA, and Cisco Umbrella

Cisco SMA for centralized content security management

Cisco advanced threat solutions and their integration: Cisco Stealthwatch, Cisco FMC, Cisco AMP, Cisco CTA, Threat Grid, ETA, Cisco WSA, Cisco SMA, Cisco Threat Response, and Cisco Umbrella

FUTURE PATH
INFOCAMPUS

KERALA

6th Floor, Markaz Complex,
Mavoor Road,
Opp.Private Bus Stand,
Kozhikode, Kerala – 673004

BENGALURU

No.50, 1st Floor, JKN Arcade,
1st Cross Road, 27th Main,
Old Madiwala, BTM 1st stage,
Bengaluru-560068

Call +91 9037555777 | +91 62821 25456

Email: hello@teaminfocampus.com

www.teaminfocampus.com