Network Security

Terminus
System

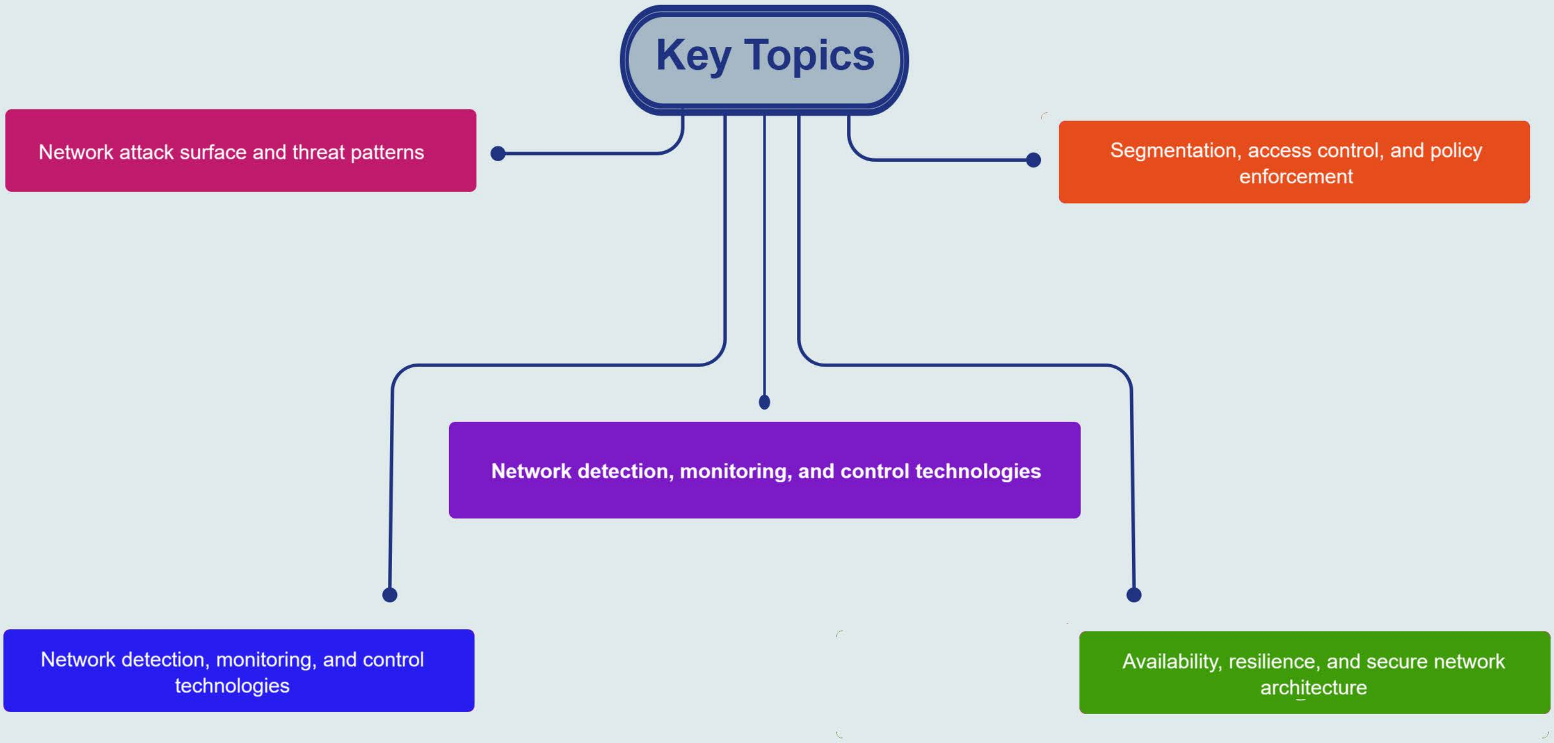
About the Course

This course presents network security as a core component of an organization’s information infrastructure and a foundational layer of information security. It provides a structured, risk-driven, and architectural perspective on securing modern LAN environments by explaining how networks establish trust boundaries, expose attack surfaces, and enforce security controls across on-premises, cloud, and hybrid systems. Participants will develop practical skills to secure firewalls, routers, and switches, implement segmentation and access control strategies, and monitor network activities to detect and prevent attacks. From a defender’s perspective, the course examines network threats, attack patterns, secure communications, and monitoring mechanisms, with strong emphasis on zoning, least exposure, policy enforcement, and resilience. It also highlights the integration of network security practices into organizational risk management, governance, and broader information security frameworks, enabling learners to design and manage secure, resilient network infrastructures.

Learning Objectives

1. **Explain fundamental network security concepts, principles, and their role within information security.**
2. Assess network vulnerabilities and apply appropriate mitigation and remediation techniques
3. **Identify and analyze network threats, risks, attack surfaces, trust boundaries, and common attack patterns.**
4. Implement and configure network security controls and policies using firewalls, IDS/IPS, NAC, and network gateways.
5. Design secure network architectures, including segmentation, access control strategies, and secure communication mechanisms
6. Evaluate and integrate network security controls within organizational risk management, governance, and ISMS processes

Key Topics



Key Topics

Network attack surface and threat patterns

Segmentation, access control, and policy enforcement

Network detection, monitoring, and control technologies

Network detection, monitoring, and control technologies

Availability, resilience, and secure network architecture

Pre Requisites

A powerful knowledge about network concepts and understanding of information security topics is necessary for students attending this class.

- Information Security Fundamentals Course

What You Will Receive

Course Presentation File

Complementary Files & Toolkit

Information Security Tactics eBook

Who Should Attend

- Network Security and Infrastructure Security Engineers
- Information Security and ISMS Managers
- Security architects and enterprise architects
- SOC, detection, and incident response professionals
- IT managers responsible for networked environments
- Professionals preparing for CISSP, CISM, ISO/IEC 27001, or network-focused security roles

Syllabus

Foundations of Network Security

- OSI model
- Network zoning
- Trust boundaries
- DMZ
- Secure network design

Network Threats, Attacks, and Reconnaissance

- Malware
- Social engineering
- Scanning, spoofing
- MITM
- DNS attacks
- DoS/DDoS
- Network attack techniques

Network Segmentation and Access Control

- VLANs
- Least-privilege networking
- Ingress/egress control
- Port security
- Authentication mechanisms (802.1X)

Secure Communication

- VPNs
- IPsec
- TLS
- Secure Remote Access

Syllabus

Network Security Controls and Defense Technologies

- Firewalls
- IDS/IPS
- NAC
- Proxies
- Gateways
- Bastion hosts
- Honeypots, and policy enforcement

Secure Network Device Configuration and Management

- Router and switch security
- ACLs
- SSH
- NAT
- Device hardening
- Configuration management

Network Monitoring, Detection, and Incident Response

- Log monitoring
- SNMP
- Traffic Analysis
- Anomaly Detection
- Attack response

System and Network Hardening

- Patch management
- Configuration baselines
- OS and service hardening
- Misconfiguration management

Syllabus

Resilience and Continuous Improvement

- Availability
- Redundancy
- Failover strategies
- Security monitoring and improvement

Hands-on Training

- Network Segmentation and Security Zoning Design
- Firewall Policy and Access Control Implementation
- Secure Network Device Configuration and Hardening
- Network Monitoring and Threat Detection