Endpoint Security

Terminus System

About the Course

This course provides a structured and operationally grounded understanding of endpoint security as one of the most critical and most targeted layers of information security. It explains what constitutes an endpoint in modern environments and why endpoints remain the primary entry point for attacks despite advances in network and cloud security.

The course examines endpoint attack surfaces, threat actors, entry vectors, and indicators of compromise from a defender's perspective. It covers secure baselines, hardening, patching, malware prevention, detection, containment, and lifecycle management. Emphasis is placed on the relationship between endpoint security and network security, identity and access management, data protection, and incident response.

The course positions endpoint security as both a first line and last line of defense and highlights its limits when governance, architecture, or identity foundations are weak.

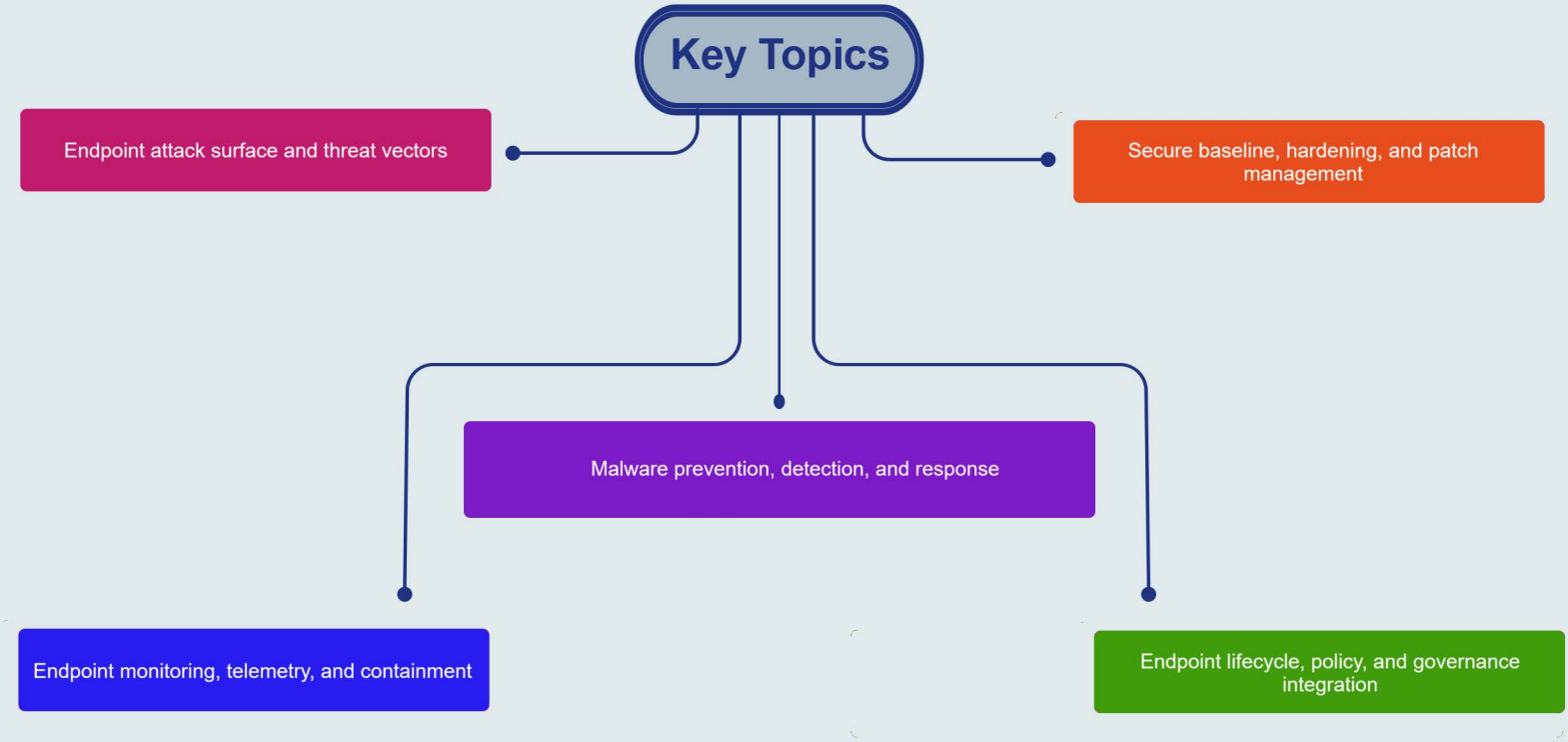
Learning Objectives

1. The ability to identify endpoint attack surfaces and entry vectors
2. A clear understanding of the role of endpoint security within ISMS
3. The ability to recognize indicators of endpoint compromise
4. A structured understanding of endpoint hardening and patching practices
5. A conceptual understanding of EDR, XDR, and behavioral analytics
6. The ability to integrate endpoint security into incident response and governance

Endpoint Security

Terminus System

Key Topics



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

Endpoint Security

Terminus System

What You Will Receive

- Course Presentation File
- Complementary Files & Toolkit
- Information Security Tactics eBook

Who Should Attend

- Endpoint, desktop, and infrastructure security engineers
- Information Security and ISMS Managers
- SOC, detection, and incident response professionals
- IT operations and system administrators
- Security architects responsible for endpoint strategy
- Professionals preparing for CISSP, CISM, or ISO/IEC 27001 roles

Terminus System

Syllabus

Foundations of Endpoint Security

- Purpose and role of endpoint security
- Definition of endpoints and workloads
- Relationship to network security, IAM, data security, and IR

Endpoint Threat Actors and Attack Surface

- Phishing, email-borne, web, removable media, and insider threats
- Operating systems, applications, browsers, and firmware exposure
- Privileges, local admin risk, and hidden trust

Indicators of Compromise and Secure Baselines

- Behavioral and performance anomalies
- Persistence mechanisms and tampering indicators
- Secure configuration baselines and hardening principles

Patch, Vulnerability, and Application Control

- OS, application, and firmware patching
- Third-party software exposure
- Allowlisting, scripting controls, sandboxing, and isolation

Malware Prevention and Host-Based Controls

- Traditional AV vs next-generation protection
- HIDS, HIPS, and integrity monitoring concepts
- Strengths, limitations, and operational tradeoffs

Endpoint Detection, Telemetry, and Analytics

- EDR and XDR concepts
- Telemetry collection and correlation
- UEBA, false positives, and SOC integration

Syllabus

Email as an Endpoint Attack Vector

- Phishing, malicious attachments, and links
- Business email compromise patterns
- Email protection controls and user reporting

Containment, Lifecycle, and Governance

- Endpoint isolation and remediation strategies
- Reimaging vs cleaning tradeoffs
- Endpoint lifecycle management, policies, standards, and limits

Hands-on Training

- Endpoint Hardening and Secure Baseline Implementation
- Patch and Vulnerability Management Process
- Endpoint Monitoring and Threat Detection (EDR Concepts)
- Endpoint Incident Response and Containment