Virtualization Security

Terminus System

About the Course

This course provides a structured and architecture-focused understanding of virtualization security as a critical trust layer in modern IT and cloud-enabled environments. It explains why hypervisors and virtualization platforms remain high-value targets and how failures at this layer can undermine network, endpoint, and cloud security controls simultaneously. The course examines virtualization architectures, management and data planes, attack surfaces, and virtualization-specific attack techniques. It covers VM lifecycle risks, sprawl, data remanence, hardening, segmentation, monitoring, and recovery from a defender's perspective. Emphasis is placed on governance, separation of duties, image integrity, and management plane protection. The course positions virtualization security as a foundational control layer tightly integrated with architecture, ISMS, risk management, and business continuity.

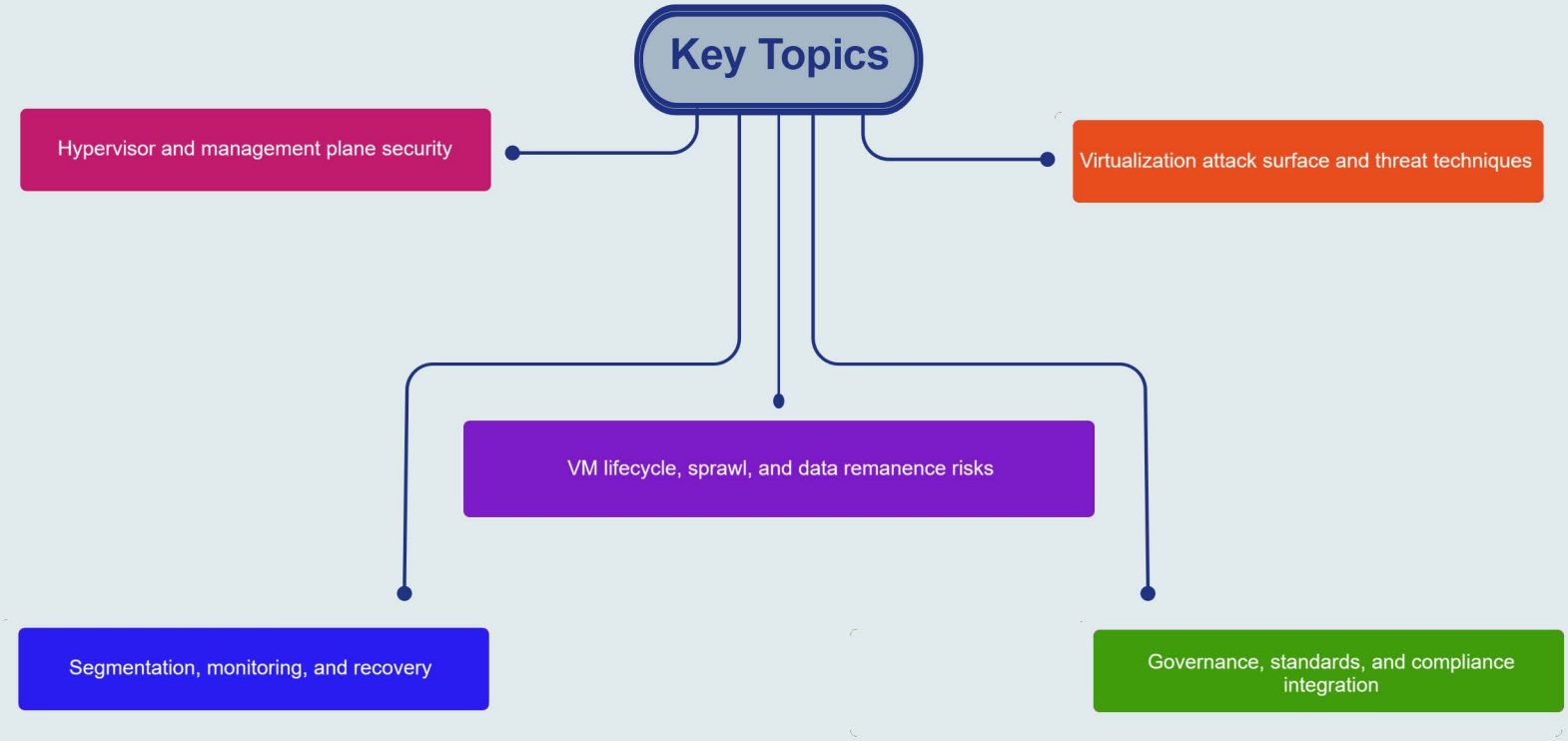
Learning Objectives

1. A clear understanding of virtualization as a critical trust and control layer
2. The ability to identify virtualization-specific attack surfaces and threats
3. A structured view of hypervisor, host, and management plane security
4. A conceptual understanding of segmentation and monitoring in virtualized environments
5. The ability to manage VM lifecycle, sprawl, and residual data risk
6. The ability to integrate virtualization security into ISMS and governance

Virtualization Security

Terminus System

Key Topics



Pre Requisites

- Basic knowledge of networking and operating systems
- Introductory understanding of cybersecurity concepts
  - Information Security Essentials Courses
- Familiarity with virtualization or cloud environments (conceptual level)
  - Cloud Security Course

Virtualization Security

Terminus System

What You Will Receive

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

Who Should Attend

- Virtualization and infrastructure security engineers
- Information Security and ISMS Managers
- Security architects and enterprise architects
- IT operations and platform administrators
- Cloud and hybrid infrastructure specialists
- Professionals preparing for CISSP, CISM, or ISO/IEC 27001 roles

Syllabus

Foundations of Virtualization Security

- Purpose and role of virtualization security
- Hypervisor as a high-value trust layer
- Relationship to cloud, network, endpoint security, and architecture

Virtualization Architecture and Attack Surface

- Hypervisor types, hosts, guests, and clusters
- Management plane, APIs, images, and virtual networking
- Trust boundaries and exposure points

Threat Actors and Virtualization-Specific Attacks

- External attackers, malicious admins, and tenant abuse
- VM escape, hypervisor compromise, and plane takeover
- Snapshot abuse, template poisoning, and side-channel risks

Indicators of Compromise and Sprawl Risks

- Unauthorized changes, snapshots, and accounts
- Configuration drift and resource abuse
- VM sprawl and shadow infrastructure

Hardening and Management Plane Security

- Secure baselines and patch management
- Strong authentication and RBAC
- Separation of duties and admin isolation

Segmentation, Images, and Data Remanence

- Virtual switches and micro-segmentation
- Image, template, and snapshot governance
- Resource reuse and residual data risks

Syllabus

Monitoring, Backup, and Recovery

- Management and lifecycle event logging
- SIEM integration and visibility
- Backup, recovery, and BCDR considerations

Lifecycle Management, Governance, and Limits

- Provisioning, operation, patching, and disposal
- Policies, standards, audit trails, and compliance
- Common failures and limits of virtualization security

Hands-on Training

- Virtualization Architecture Discovery
- Virtual Machine Lifecycle and Sprawl Analysis
- Hypervisor and VM Hardening Review
- Virtual Network Segmentation and Isolation
- Image and Snapshot Security Assessment
- Monitoring and Incident Investigation