Cloud Security

Terminus System

About the Course

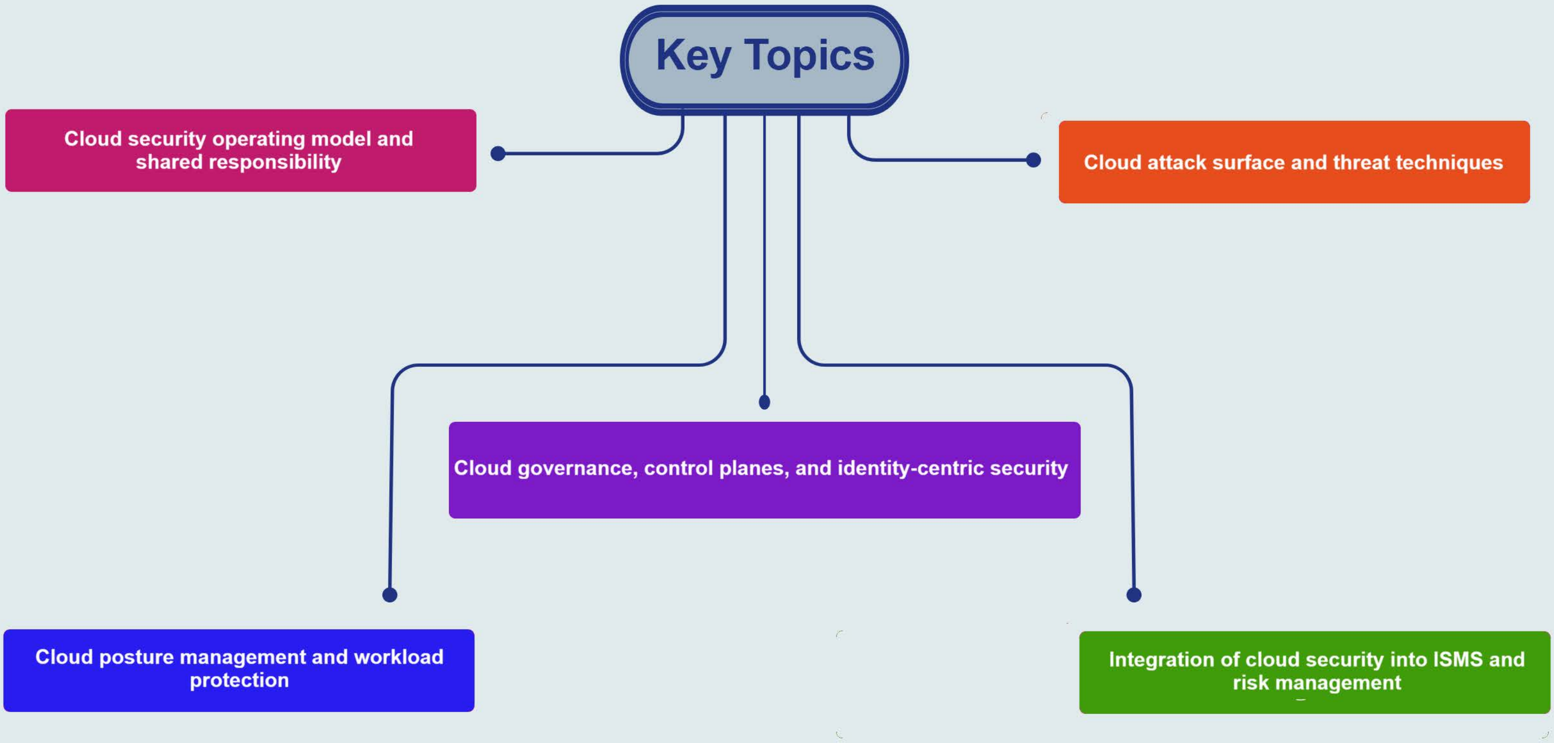
This course provides a structured, governance-driven understanding of cloud security as a fundamental shift in the security operating model rather than a simple extension of traditional infrastructure security. It explains why cloud environments move security away from perimeter-centric controls toward identity, control planes, and automation-driven enforcement. The course examines shared responsibility, cloud governance models, attack surfaces, and cloud-specific threat techniques across IaaS, PaaS, and SaaS environments. It covers identity-centric security, cloud networking, data protection, workload security, posture management, and detection from a defender's perspective. Emphasis is placed on cloud governance, policy-as-code, DevSecOps, and lifecycle-based security integration. The course positions cloud security as an architectural, risk, and operating discipline tightly integrated with ISMS, GRC, and enterprise risk management.

Learning Objectives

1. A clear understanding of why cloud fundamentally changes the security model
2. The ability to apply the shared responsibility model correctly
3. A structured understanding of cloud attack surfaces and threat techniques
4. The ability to design governance and control frameworks for cloud environments
5. A conceptual understanding of cloud-native security controls and platforms
6. The ability to integrate cloud security into ISMS, risk management, and incident response

Cloud Security

Key Topics



Key Topics

Cloud security operating model and shared responsibility

Cloud attack surface and threat techniques

Cloud governance, control planes, and identity-centric security

Cloud posture management and workload protection

Integration of cloud security into ISMS and risk management

Pre Requisites

- Basic knowledge of networking and operating systems
- Introductory understanding of cybersecurity concepts
  - Information Security Essentials Course
- Familiarity with cloud computing concepts (IaaS, PaaS, SaaS)

What You Will Receive

Course Presentation File

Complementary Files & Toolkit

Information Security Tactics eBook

Who Should Attend

- Cloud security and infrastructure security engineers
- Information Security and ISMS Managers
- Security architects and enterprise architects
- GRC, risk, and compliance professionals
- DevOps and platform engineering leaders
- Professionals preparing for CISSP, CISM, CCSP, or ISO/IEC 27001 roles

Syllabus

Foundations of Cloud Security

- Why cloud changes the security model
- From perimeter security to identity and control planes
- Cloud as an operating model

Cloud Models, Concepts, and Shared Responsibility

- IaaS, PaaS, SaaS and deployment models
- Responsibility boundaries and trust assumptions
- Common causes of cloud security failures

Cloud Governance and Attack Surface

- Landing zones, guardrails, and policy as code
- Management interfaces, APIs, identities, and storage
- CI/CD pipelines and automation exposure

Cloud Threats and Attack Techniques

- Account takeover and API abuse
- Metadata service and supply-chain attacks
- Lateral movement in cloud environments

Identity, Network, and Data Security in Cloud

- Cloud IAM as the primary perimeter
- Virtual networks, segmentation, and private endpoints
- Storage security, encryption, backup, and exfiltration controls

Workload Security and Posture Management

- VM, container, and platform hardening concepts
- CSPM and CWPP capabilities
- Continuous assessment and drift detection

Syllabus

DevSecOps, IaC, and Hybrid / Multi-Cloud Security

- IaC security and pre-deployment enforcement
- CI/CD pipeline and secrets management
- Hybrid and multi-cloud governance challenges

Monitoring, Incident Response, and Risk Management

- Cloud logging, audit trails, and SIEM integration
- Cloud incident response and containment limits
- Cloud risk patterns, compliance, and security limits

Hands-on Training

- Cloud Architecture and Shared Responsibility Mapping
- Cloud Identity and Access Security Configuration
- Cloud Storage Security and Data Protection
- Cloud Network Segmentation and Security Controls
- Cloud Posture Assessment and Misconfiguration Detection
- Cloud Logging and Incident Investigation