Protecting Data in Transit and at Rest Masterclass Training Course

Professional Development Training Course Outline

Category	Data Security	**Duration**	5 Days
Base Fee	$1,500 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

Protecting Data in Transit and at Rest Masterclass Training Course addresses the most critical challenge in modern cybersecurity: safeguarding sensitive information across its entire lifecycle from the moment it's stored on a disk to the millisecond it traverses a network. In today's landscape of escalating Ransomware-as-a-Service attacks, sophisticated Advanced Persistent Threats, and tightening regulatory compliance like GDPR and CCPA, traditional perimeter defenses are obsolete. Organizations must adopt a Data-Centric Security model, ensuring data itself, not just the network it resides in, is intrinsically protected. This course provides the architectural, procedural, and technical expertise required to implement Zero Trust principles for data protection.

This intensive program moves beyond foundational theory to equip participants with hands-on proficiency in cutting-edge encryption, Cloud Security Posture Management (CSPM), and tokenization strategies. We'll demystify complex topics like Post-Quantum Cryptography readiness and the practical application of Homomorphic Encryption to meet emerging challenges. Mastering the art of securing data at rest through Full Disk Encryption and Transparent Data Encryption, coupled with securing data in transit via TLS/SSL and Secure File Transfer (MFT), is essential for mitigating insider threats and preventing catastrophic data breaches. This Masterclass is your blueprint for building an immutable data protection framework that not only achieves cyber resilience but transforms security into a core business enabler.

Programme Curriculum

Protecting Data in Transit and at Rest Masterclass Training Course

Introduction

Protecting Data in Transit and at Rest Masterclass Training Course addresses the most critical challenge in modern cybersecurity: safeguarding sensitive information across its entire lifecycle from the moment it's stored

on a disk to the millisecond it traverses a network. In today's landscape of escalating Ransomware-as-a-Service attacks, sophisticated Advanced Persistent Threats, and tightening regulatory compliance like GDPR and CCPA, traditional perimeter defenses are obsolete. Organizations must adopt a Data-Centric Security model, ensuring data itself, not just the network it resides in, is intrinsically protected. This course provides the architectural, procedural, and technical expertise required to implement Zero Trust principles for data protection.

This intensive program moves beyond foundational theory to equip participants with hands-on proficiency in cutting-edge encryption, Cloud Security Posture Management (CSPM), and tokenization strategies. We'll demystify complex topics like Post-Quantum Cryptography readiness and the practical application of Homomorphic Encryption to meet emerging challenges. Mastering the art of securing data at rest through Full Disk Encryption and Transparent Data Encryption, coupled with securing data in transit via TLS/SSL and Secure File Transfer (MFT), is essential for mitigating insider threats and preventing catastrophic data breaches. This Masterclass is your blueprint for building an immutable data protection framework that not only achieves cyber resilience but transforms security into a core business enabler.

Course Duration

5 days

Course Objectives

1. Architect and implement a comprehensive Data-Centric Security strategy that aligns with Zero Trust Architecture (ZTA).
2. Master the practical application of AES-256 and Post-Quantum Cryptography (PQC) for future-proofing data assets.
3. Design and deploy robust Key Management Systems (KMS) and Hardware Security Modules (HSM) for key lifecycle control.
4. Differentiate, select, and implement Full Disk Encryption (FDE) and Transparent Data Encryption (TDE) for Data at Rest.
5. Implement and audit TLS 1.3 and other VPN/tunneling protocols to ensure secure Data in Transit.
6. Utilize Data Loss Prevention (DLP) and Cloud Access Security Brokers (CASB) to monitor and control data movement across hybrid and multi-cloud environments.
7. Conduct a thorough Data Classification and Data Mapping exercise as a foundation for protection policies.
8. Formulate a Data Protection Impact Assessment (DPIA) and align security controls with GDPR, HIPAA, and CCPA compliance.
9. Mitigate Supply Chain Risk and Third-Party Risk through secure data-sharing protocols and security audits.
10. Implement secure DevSecOps practices for encrypting and protecting data within CI/CD pipelines.
11. Apply Data Masking, Tokenization, and Format-Preserving Encryption (FPE) for protecting data in non-production environments.
12. Develop and practice an Incident Response Plan focused on data breach containment and forensic analysis of encrypted systems.
13. Integrate Security Orchestration, Automation, and Response (SOAR) tools for automated data protection workflow management.

Target Audience

1. Chief Information Security Officers (CISOs) and Security Directors.

2. Security Architects and Cloud Security Engineers.
3. Data Protection Officers (DPOs) and Compliance Managers.
4. Security Operations Center (SOC) Analysts and Incident Responders.
5. DevSecOps and Cloud/DevOps Engineers responsible for production systems.
6. IT/System Administrators managing database and file server infrastructure.
7. Risk Management and Audit Professionals focusing on data control.
8. Senior Data Scientists and Software Developers handling sensitive data.

Course Modules

Module 1: Foundational Data States and Risk Modeling

- Defining and differentiating Data at Rest, Data in Transit, and Data in Use and the unique risks each state presents.
- Conducting Data Classification and Data Flow Mapping to identify critical protection points.
- The CIA Triad applied specifically to data protection across the data lifecycle.
- Case Study: Target Data Breach analysis how unsegmented network access and lack of strong access control led to compromise.
- Introduction to the Data-Centric Security model and its alignment with NIST CSF

Module 2: Data at Rest Encryption Deep Dive

- Implementing Full Disk Encryption for endpoints and non-database servers.
- Mastering Transparent Data Encryption in major database systems and its performance considerations.
- Understanding the risks of storing keys with data.
- Case Study: Analysis of a lost laptop scenario; how mandatory FDE rendered the data useless to unauthorized parties.
- Securing object storage and filesystems with Server-Side Encryption and Client-Side Encryption in cloud environments.

Module 3: Key Management and Cryptographic Controls

- Designing and operating a secure Key Management System using Hardware Security Modules.
- Implementing Key Rotation, key revocation, and robust access controls for cryptographic keys.
- Exploring modern algorithms.
- Case Study: The significance of the Heartbleed vulnerability in TLS a failure of cryptographic implementation and integrity.
- Practical guide to implementing Digital Signatures and Hashing for data integrity and non-repudiation.

Module 4: Securing Data in Transit (Network & Cloud)

- Advanced configuration of TLS/SSL protocols, focusing on TLS 1.3 and perfect forward secrecy.
- Deployment of enterprise-grade Virtual Private Networks and IPsec tunnels for secure site-to-site communication.
- Implementing Secure File Transfer solutions as an alternative to unmanaged FTP/SFTP.
- Case Study: Man-in-the-Middle attacks on a Wi-Fi network; students implement packet analysis to identify non-TLS traffic.
- Securing API Endpoints and service-to-service communication with mutual TLS in a microservices architecture.

Module 5: Cloud and Hybrid Data Protection

- Leveraging Cloud Access Security Brokers to enforce policies on shadow IT and cloud data movement.
- Using Cloud Security Posture Management tools to detect and remediate Cloud Misconfigurations.
- Implementing Zero Trust principles for data access in IaaS and PaaS.
- Case Study: Capital One Breach demonstrating the danger of server-side misconfigurations in cloud WAF/IAM that led to data theft.
- Data protection in serverless and containerized environments

Module 6: Data Loss Prevention (DLP) and Data Masking

- Establishing an effective DLP program.
- Techniques for Data Masking, Tokenization, and Format-Preserving Encryption for testing/development.
- Mitigating Insider Threats by monitoring data exfiltration attempts and abnormal user behavior.
- Case Study: An employee attempts to email a large file of customer PII; students configure a DLP rule to block the transfer and alert the SOC.
- Integrating DLP with Data Classification tools for automated policy enforcement.

Module 7: Compliance, Governance, and Risk Management

- Mapping technical controls to major regulations.
- The role of the Data Protection Impact Assessment and its mandatory triggers.
- Developing and maintaining Data Retention and Data Disposal policies for encrypted and unencrypted data.
- Case Study: A company's regulatory fine due to failure to implement Privacy by Design focusing on data minimization and encryption.
- Managing Third-Party Risk by ensuring vendors meet minimum data protection standards and security auditing requirements.

Module 8: Incident Response and Advanced Topics

- Developing an Incident Response Plan specifically for a data breach involving encrypted data.
- Performing Digital Forensics and eDiscovery on compromised, encrypted systems for evidence collection.
- Introduction to Post-Quantum Cryptography and the migration strategy for future-proofing encryption.
- Case Study: A successful Ransomware attack on a production database; participants simulate the triage, containment, and recovery process.
- The security implications of Homomorphic Encryption and Confidential Computing for data-in-use protection.

Training Methodology

This course employs a participatory and hands-on approach to ensure practical learning, including:

- Interactive lectures and presentations.
- Group discussions and brainstorming sessions.
- Hands-on exercises using real-world datasets.
- Role-playing and scenario-based simulations.
- Analysis of case studies to bridge theory and practice.
- Peer-to-peer learning and networking.
- Expert-led Q&A sessions.
- Continuous feedback and personalized guidance.

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.org or call +254769199797

Certification

Upon successful completion of this training, participants will be issued with a globally- recognized certificate.

Tailor-Made Course

We also offer tailor-made courses based on your needs.

Key Notes

a. The participant must be conversant with English.

b. Upon completion of training the participant will be issued with an Authorized Training Certificate

c. Course duration is flexible and the contents can be modified to fit any number of days.

d. The course fee includes facilitation training materials, 2 coffee breaks, buffet lunch and A Certificate upon successful completion of Training.

e. One-year post-training support Consultation and Coaching provided after the course.

f. Payment should be done at least a week before commence of the training, to Fineskill Training Center account, as indicated in the invoice so as to enable us prepare better for you.

Upcoming Scheduled Sessions

Start Date	End Date	Location	Price
21 Sep 2026	25 Sep 2026	Online	$1,000
21 Sep 2026	25 Sep 2026	Physical	$1,500
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0
21 Sep 2026	25 Sep 2026	Physical	$0

Ready to enroll or request a customized program? Book online or contact us:

Register Online Now

Email: info@fineskilltrainingcenter.com | Website: www.fineskilltrainingcenter.com