Data Security for FinTech and Financial Services 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

The global financial sector is undergoing a massive transformation, driven by FinTech innovation, which necessitates an aggressive and proactive approach to cyber defense and data governance. The convergence of traditional financial services with disruptive technologies like cloud computing, APIs, and Decentralized Finance (DeFi) has dramatically expanded the attack surface, making organizations vulnerable to sophisticated threats like ransomware and API vulnerabilities. Protecting high-value assets specifically Personally Identifiable Information (PII) and transaction data is no longer a mere IT task; it is a business-critical imperative directly impacting customer trust, brand reputation, and bottom-line viability. This course provides the strategic knowledge and practical skills required to build a robust, Zero-Trust security posture in this high-stakes environment.

Data Security for FinTech and Financial Services Training Course is engineered to equip professionals with the advanced knowledge needed to master the complex landscape of financial regulation and implement next-generation security frameworks. We move beyond foundational cybersecurity to focus on real-time fraud detection, AI-driven threat intelligence, and managing the unique risks of third-party vendor relationships and supply chain attacks prevalent in the modern FinTech ecosystem. By integrating theoretical concepts with hands-on labs and real-world case studies, participants will gain the confidence to lead incident response efforts, ensure regulatory compliance, and drive their organizations toward achieving cyber resilience in the age of digital finance.

Programme Curriculum

Data Security for FinTech and Financial Services Training Course

Introduction

The global financial sector is undergoing a massive transformation, driven by FinTech innovation, which necessitates an aggressive and proactive approach to cyber defense and data governance. The convergence of traditional financial services with disruptive technologies like cloud computing, APIs, and Decentralized Finance (DeFi) has dramatically expanded the attack surface, making organizations vulnerable to sophisticated threats like ransomware and API vulnerabilities. Protecting high-value assets specifically Personally Identifiable Information (PII) and transaction data is no longer a mere IT task; it is a business-critical imperative directly impacting customer trust, brand reputation, and bottom-line viability. This course provides the strategic knowledge and practical skills required to build a robust, Zero-Trust security posture in this high-stakes environment.

Data Security for FinTech and Financial Services Training Course is engineered to equip professionals with the advanced knowledge needed to master the complex landscape of financial regulation and implement next-generation security frameworks. We move beyond foundational cybersecurity to focus on real-time fraud detection, AI-driven threat intelligence, and managing the unique risks of third-party vendor relationships and supply chain attacks prevalent in the modern FinTech ecosystem. By integrating theoretical concepts with hands-on labs and real-world case studies, participants will gain the confidence to lead incident response efforts, ensure regulatory compliance, and drive their organizations toward achieving cyber resilience in the age of digital finance.

Course Duration

5 days

Course Objectives

Upon completion of this course, participants will be able to:

1. Analyze the expanded attack surface unique to the FinTech and digital banking landscape.
2. Design and implement a comprehensive Zero-Trust architecture across cloud-native financial platforms.
3. Master the application of End-to-End Encryption and Tokenization for sensitive PII and payment data.
4. Evaluate and mitigate risks associated with API security vulnerabilities and Open Banking protocols.
5. Develop robust strategies for Real-time Fraud Detection using AI and Machine Learning (ML) models.
6. Navigate the complex global regulatory environment, including GDPR, CCPA, and Basel IV requirements for data protection.
7. Identify and defend against prevalent cyber threats in FinTech, such as Ransomware-as-a-Service (RaaS) and advanced Social Engineering attacks.
8. Implement and manage a robust Third-Party Risk Management (TPRM) program to secure the supply chain.
9. Formulate an effective, legally sound Incident Response (IR) plan for major data breaches and financial system compromise.
10. Assess the security implications of emerging technologies like Decentralized Finance (DeFi) and Central Bank Digital Currencies (CBDCs).
11. Utilize Security Information and Event Management (SIEM) and Security Orchestration, Automation, and Response (SOAR) tools for automated defense.
12. Establish an organizational culture focused on minimizing Insider Threats and human error through training and access control.
13. Justify the business case for security investments by calculating the cost of a breach and demonstrating improved cyber resilience.

Target Audience

1. Chief Information Security Officers and Security Directors in FinTech and Banks.
2. Compliance Officers and Risk Managers responsible for financial regulation
3. Security Architects and Engineers who design and implement security solutions.
4. IT Auditors and Penetration Testers focused on financial applications.
5. FinTech Product Managers overseeing the development of new financial services.
6. Chief Technology Officers and Heads of Infrastructure dealing with cloud adoption.
7. Data Governance Specialists managing PII and sensitive data lifecycle.
8. Legal and Regulatory Affairs professionals who handle data breach notifications and litigation.

Course Modules

Module 1: The FinTech & Financial Services Threat Landscape

- The Digital Transformation.
- Analyzing the Expanded Attack Surface.
- The Financial Value Chain
- Ransomware-as-a-Service (RaaS), Credential Stuffing, and Account Takeover.
- Case Study: Analysis of unpatched software vulnerability, massive PII theft, and subsequent leadership/regulatory fallout.

Module 2: Security Architecture and Zero Trust Frameworks

- Designing a Zero-Trust Model for distributed FinTech applications and remote workforces.
- Implementing Micro-segmentation and network isolation in a hybrid/multi-cloud environment.
- Advanced Identity and Access Management.
- Securing API Gateways and implementing OAuth 2.0/OpenID Connect for secure data sharing.
- Case Study: Examination of lateral movement and privilege escalation due to weak authentication and network segmentation.

Module 3: Data Protection, Cryptography, and Privacy

- Data Classification and Lifecycle Management.
- Mastering Encryption and Key Management Systems in the cloud.
- Practical application of Tokenization and Data Masking for regulatory compliance
- Data Privacy Regulations.
- Case Study: Focus on the compromise of cardholder data and the necessity of robust data segregation and encryption in payment processing.

Module 4: Regulatory Compliance and Governance

- Basel IV and operational resilience.
- Implementing Anti-Money Laundering and Know Your Customer compliance through automated RegTech solutions.
- Audit and Reporting.
- Securing Cloud Deployments.
- Case Study: Analyzing failures in transaction monitoring and data retention that led to massive regulatory penalties.

Module 5: Real-time Threat and Fraud Detection

- Leveraging AI/ML for Real-time Fraud Detection, behavioral analytics, and anomaly scoring.
- Deployment of SIEM/UEBA for detecting insider threats and ATO.

- Threat Intelligence.
- Advanced Phishing and Social Engineering defense techniques for employees and customers.
- Case Study: Examination of successful layered security implementation, including behavioral biometrics to counter mobile fraud.

Module 6: Third-Party Risk and Supply Chain Security

- Developing a comprehensive Third-Party Risk Management framework for FinTech vendors.
- Vendor Onboarding and Continuous Monitoring.
- Addressing Supply Chain Attacks
- Contractual Security Requirements: Enforcing strong SLAs and right-to-audit clauses.
- Case Study: Analysis of major data leaks originating from compromised third-party service providers

Module 7: Cloud and DevOps Security

- DevSecOps integration.
- Securing serverless functions, containers, and infrastructure-as-code.
- Identifying and mitigating Cloud Security Misconfigurations
- Implementing Cloud Workload Protection Platforms and Cloud Security Posture Management.
- Case Study: Deep dive into the consequences of a WAF misconfiguration on a cloud platform leading to the exfiltration of 100 million customer records.

Module 8: Incident Response and Cyber Resilience

- Building a resilient Business Continuity Plan and Disaster Recovery strategy.
- The six phases of Incident Response.
- Legal and PR Crisis Management.
- Conducting Post-Incident Digital Forensics and evidence preservation.
- Case Study: Simulating a critical infrastructure or supply chain ransomware event and the necessary containment and recovery steps.

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
23 Nov 2026	27 Nov 2026	Online	$1,000
23 Nov 2026	27 Nov 2026	Physical	$1,500
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$3,000
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$4,500
23 Nov 2026	27 Nov 2026	Physical	$6,000
23 Nov 2026	27 Nov 2026	Physical	$6,000

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

Register Online Now

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