Cyber Threat Intelligence for Banks Training Course

Professional Development Training Course Outline

Category	Banking Institute	**Duration**	10 Days
Base Fee	$3,000 USD	**Delivery Mode**	Online / On-site Hybrid

Course Introduction

In today’s hyper-connected financial ecosystem, Cyber Threat Intelligence (CTI) has become a mission-critical capability for banks aiming to combat advanced persistent threats (APTs), ransomware attacks, phishing campaigns, and financial fraud schemes. With the rapid evolution of AI-driven cyberattacks, zero-day vulnerabilities, and dark web threats, financial institutions must leverage real-time threat intelligence, predictive analytics, and cyber risk management frameworks to proactively defend their digital assets. This course equips banking professionals with cutting-edge knowledge in threat intelligence lifecycle management, cybersecurity analytics, and threat hunting techniques aligned with global standards such as MITRE ATT&CK, NIST, and ISO 27001.

Cyber Threat Intelligence for Banks Training Course is designed to provide a comprehensive understanding of how to collect, analyze, and operationalize threat intelligence to enhance security operations centers (SOC), incident response strategies, and fraud detection systems. Participants will gain hands-on experience in threat intelligence platforms (TIPs), open-source intelligence (OSINT), and machine learning-driven cybersecurity tools, enabling them to strengthen cyber resilience, improve decision-making, and protect customer trust in an increasingly volatile digital banking landscape.

Programme Curriculum

Cyber Threat Intelligence for Banks Training Course

Introduction

In today’s hyper-connected financial ecosystem, Cyber Threat Intelligence (CTI) has become a mission-critical capability for banks aiming to combat advanced persistent threats (APTs), ransomware attacks, phishing campaigns, and financial fraud schemes. With the rapid evolution of AI-driven cyberattacks, zero-day vulnerabilities, and dark web threats, financial institutions must leverage real-time threat intelligence, predictive

analytics, and cyber risk management frameworks to proactively defend their digital assets. This course equips banking professionals with cutting-edge knowledge in threat intelligence lifecycle management, cybersecurity analytics, and threat hunting techniques aligned with global standards such as MITRE ATT&CK, NIST, and ISO 27001.

Cyber Threat Intelligence for Banks Training Course is designed to provide a comprehensive understanding of how to collect, analyze, and operationalize threat intelligence to enhance security operations centers (SOC), incident response strategies, and fraud detection systems. Participants will gain hands-on experience in threat intelligence platforms (TIPs), open-source intelligence (OSINT), and machine learning-driven cybersecurity tools, enabling them to strengthen cyber resilience, improve decision-making, and protect customer trust in an increasingly volatile digital banking landscape.

Course Duration

10 days

Course Objectives

1. Master Cyber Threat Intelligence lifecycle management and frameworks
2. Identify and analyze emerging cyber threats in banking ecosystems
3. Implement AI-powered threat detection and predictive analytics
4. Strengthen SOC operations with real-time intelligence integration
5. Apply MITRE ATT&CK framework for threat mapping and defense strategies
6. Enhance fraud detection using behavioral analytics and anomaly detection
7. Conduct advanced threat hunting and digital forensics investigations
8. Utilize OSINT and dark web intelligence for proactive risk mitigation
9. Improve incident response and cyber crisis management capabilities
10. Integrate threat intelligence with SIEM and SOAR platforms
11. Assess cyber risk exposure using data-driven intelligence models
12. Develop cyber resilience and business continuity strategies
13. Ensure compliance with global cybersecurity regulations and standards

Target Audience

1. Cybersecurity Analysts and Threat Intelligence Specialists
2. Banking IT Security Professionals
3. Risk Management and Compliance Officers
4. Fraud Detection and Prevention Teams
5. SOC Analysts and Incident Response Teams
6. Digital Banking and FinTech Professionals
7. Internal Audit and Cyber Risk Consultants
8. Senior Management and Decision Makers in Banking Security

Course Modules

Module 1: Introduction to Cyber Threat Intelligence

- CTI fundamentals and importance in banking
- Threat landscape overview in financial services
- Types of threat intelligence
- Intelligence lifecycle stages

- **Case Study:** Global bank phishing attack analysis

Module 2: Cyber Threat Landscape in Banking

- Financial malware and ransomware trends
- Insider threats and social engineering attacks
- Mobile banking vulnerabilities
- Payment system threats
- **Case Study:** SWIFT banking cyberattack

Module 3: Threat Intelligence Lifecycle

- Planning and direction
- Data collection and processing
- Analysis and dissemination
- Feedback and improvement
- **Case Study:** Intelligence lifecycle implementation in a bank

Module 4: Threat Intelligence Sources

- Open Source Intelligence (OSINT)
- Dark web and deep web monitoring
- Commercial threat feeds
- Government and industry intelligence sharing
- **Case Study:** Dark web data breach detection

Module 5: Threat Intelligence Platforms (TIPs)

- Overview of TIP tools
- Integration with banking systems
- Automation and orchestration
- Data visualization techniques
- **Case Study:** TIP deployment in a financial institution

Module 6: MITRE ATT&CK Framework

- Framework overview
- Mapping threats to tactics and techniques
- Threat detection strategies
- Use cases in banking
- **Case Study:** Mapping ransomware attack using MITRE

Module 7: Security Operations Center (SOC) Integration

- Role of CTI in SOC
- SIEM integration
- Alert prioritization and triage
- Incident correlation
- **Case Study:** SOC optimization using CTI

Module 8: Threat Hunting Techniques

- Proactive threat detection strategies

- Hypothesis-driven threat hunting
- Behavioral analytics
- Tools and methodologies
- **Case Study:** Detecting insider threats

Module 9: Cyber Threat Analytics

- Data-driven threat analysis
- Machine learning in cybersecurity
- Predictive threat modeling
- Risk scoring
- **Case Study:** AI-based fraud detection

Module 10: Incident Response and Crisis Management

- Incident response frameworks
- Cyberattack containment strategies
- Communication during cyber crises
- Post-incident analysis
- **Case Study:** Banking ransomware response

Module 11: Fraud Detection and Prevention

- Digital fraud trends
- Behavioral biometrics
- Transaction monitoring systems
- Anti-money laundering (AML) integration
- **Case Study:** Real-time fraud detection system

Module 12: Cyber Risk Management

- Risk identification and assessment
- Risk mitigation strategies
- Cyber insurance considerations
- Governance frameworks
- **Case Study:** Enterprise cyber risk assessment

Module 13: Regulatory Compliance and Standards

- NIST Cybersecurity Framework
- ISO 27001 and ISO 22301
- GDPR and data protection
- Banking compliance requirements
- **Case Study:** Compliance failure impact

Module 14: Emerging Technologies in Cybersecurity

- AI and automation in CTI
- Blockchain security
- Cloud security threats
- IoT risks in banking
- **Case Study:** Cloud breach in financial sector

Module 15: Building Cyber Resilience

- Business continuity planning
- Disaster recovery strategies
- Cyber resilience frameworks
- Continuous monitoring and improvement
- **Case Study:** Bank recovery after cyberattack

Training Methodology

- 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

07 Sep 2026	18 Sep 2026	Online	$2,000
07 Sep 2026	18 Sep 2026	Physical	$3,000
14 Sep 2026	25 Sep 2026	Online	$2,000
14 Sep 2026	25 Sep 2026	Physical	$3,000
21 Sep 2026	02 Oct 2026	Online	$2,000
21 Sep 2026	02 Oct 2026	Physical	$3,000
28 Sep 2026	09 Oct 2026	Online	$2,000
28 Sep 2026	09 Oct 2026	Physical	$3,000

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

Register Online Now

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