Training Course on API Security and API Incident Response

Professional Development Training Course Outline

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

Course Introduction

In today’s cloud-native and microservices-driven digital ecosystem, APIs have become the backbone of modern software architecture. However, with their increased use comes heightened vulnerability. Organizations must adopt robust API security practices and develop an agile incident response framework to defend against cyberattacks, data breaches, and malicious exploits. Training Course on API Security and API Incident Response equips professionals with the essential tools to protect APIs, detect anomalies, and respond to security incidents swiftly and efficiently.

This hands-on course leverages industry-leading frameworks, real-world case studies, and trending tools to guide participants in mastering OAuth2.0, JWT validation, rate limiting, WAF integration, and zero-trust security models. Learners will explore attack surfaces unique to REST and GraphQL APIs and will build resilient systems with threat modeling, secure API gateways, and compliance-focused monitoring solutions.

Programme Curriculum

Training Course on API Security and API Incident Response

Introduction

In today’s cloud-native and microservices-driven digital ecosystem, APIs have become the backbone of modern software architecture. However, with their increased use comes heightened vulnerability. Organizations must adopt robust API security practices and develop an agile incident response framework to defend against cyberattacks, data breaches, and malicious exploits. Training Course on API Security and API Incident Response equips professionals with the essential tools to protect APIs, detect anomalies, and respond to security incidents swiftly and efficiently.

This hands-on course leverages industry-leading frameworks, real-world case studies, and trending tools to guide participants in mastering OAuth2.0, JWT validation, rate limiting, WAF integration, and zero-trust security models. Learners will explore attack surfaces unique to REST and GraphQL APIs and will build resilient systems with threat

modeling, secure API gateways, and compliance-focused monitoring solutions.

Learning Objectives

1. Understand API architectures including REST, GraphQL, SOAP, and gRPC.
2. Identify and mitigate common API vulnerabilities (OWASP API Top 10).
3. Apply OAuth2.0, JWT, and OpenID Connect for secure authentication and authorization.
4. Implement rate limiting, throttling, and API gateway controls.
5. Detect API abuse using behavioral analytics and anomaly detection.
6. Secure API integrations with cloud-native environments (AWS, Azure, GCP).
7. Establish secure DevSecOps pipelines for API development and deployment.
8. Design zero-trust architecture models for API ecosystems.
9. Build real-time API monitoring and logging systems for rapid detection.
10. Develop a comprehensive API incident response playbook.
11. Perform post-incident forensic analysis on compromised APIs.
12. Align API security with regulatory compliance (GDPR, HIPAA, PCI-DSS).
13. Leverage machine learning for predictive threat intelligence and response automation.

Target Audiences

1. API Developers
2. Cloud Security Engineers
3. DevOps and DevSecOps Professionals
4. Network Security Architects
5. SOC Analysts and Incident Responders
6. Cybersecurity Consultants
7. IT Risk and Compliance Officers
8. Security Product Managers

Course Duration: 5 days

Course Modules

Module 1: API Security Fundamentals

- API types: REST, GraphQL, SOAP
- OWASP API Top 10 overview
- API threat landscape
- API trust boundaries
- Role of API gateways
- **Case Study: API misconfiguration breach at Facebook**

Module 2: Authentication and Authorization

- OAuth2.0 flows
- OpenID Connect integration
- JWT validation and revocation
- Secure session management
- Token expiration best practices
- **Case Study: Misused tokens in Uber API incident**

Module 3: Secure API Design Principles

- Principle of least privilege
- Input/output validation

- Error handling and logging
- Schema-based validation (OpenAPI/Swagger)
- HTTPS and TLS enforcement
- **Case Study: Capital One’s API design flaws**

Module 4: API Gateway and Proxy Security

- Role of API gateways in access control
- Rate limiting and throttling
- IP filtering and geo-fencing
- Logging and request transformations
- WAF integration strategies
- **Case Study: T-Mobile’s exposed API via unfiltered gateway**

Module 5: Zero Trust for APIs

- Identity-aware proxies
- Trust but verify model
- Microsegmentation strategies
- Dynamic policy enforcement
- Mutual TLS (mTLS)
- **Case Study: Google BeyondCorp API model**

Module 6: API Monitoring and Logging

- Centralized logging tools
- Log correlation techniques
- Real-time dashboards
- SIEM integrations (Splunk, ELK)
- Alert tuning and thresholds
- **Case Study: Log-based detection in Shopify breach**

Module 7: Threat Modeling APIs

- STRIDE framework for APIs
- Attack trees and risk scoring
- Threat simulation tools
- API asset inventory creation
- Security posture scoring
- **Case Study: Azure API threat modeling workshop**

Module 8: API Vulnerability Scanning Tools

- Dynamic and static analysis tools
- Open-source vs commercial scanners
- CI/CD pipeline integration
- API-specific scanners (e.g., OWASP ZAP, Burp Suite)
- Reporting and remediation workflows
- **Case Study: Zoom’s security via automated scanning**

Module 9: Cloud API Security

- IAM policies in AWS/GCP/Azure
- API key management
- Cross-account access auditing
- Secure API exposure in cloud

- KMS and secrets management
- **Case Study: Misconfigured AWS API Gateway**

Module 10: Incident Detection & Response Planning

- API incident classification
- Indicators of compromise (IOCs)
- API traffic pattern anomalies
- Role of SOAR platforms
- Stakeholder communication protocols
- **Case Study: Twilio API phishing attack response**

Module 11: API Forensics & Post-Incident Analysis

- Log aggregation for analysis
- Timeline reconstruction
- Identifying lateral movement
- Recovery and root cause
- Lessons learned documentation
- **Case Study: SolarWinds API breach forensic timeline**

Module 12: Regulatory Compliance for APIs

- GDPR and API data processing rules
- HIPAA-compliant API development
- PCI-DSS and tokenization
- Audit logging for compliance
- Privacy-by-design APIs
- **Case Study: API privacy failure in Marriott data breach**

Module 13: DevSecOps for API Security

- Secure CI/CD integration
- Shift-left security testing
- Code linting and security plugins
- Security gates in pipelines
- Continuous monitoring
- **Case Study: Netflix’s DevSecOps for API resilience**

Module 14: Machine Learning in API Security

- Behavioral modeling of API usage
- Detecting anomalies with ML
- Clustering and classification models
- Training models on logs
- Risk scoring via AI
- **Case Study: ML-based API threat detection at Akamai**

Module 15: Future Trends in API Security

- API security in Web3 and blockchain
- Quantum-safe APIs
- API-as-a-product security models
- API security marketplaces
- Autonomous security orchestration
- **Case Study: API security trends in Apple’s developer API ecosystem**

Training Methodology

- Instructor-led live sessions (online/offline)
- Real-world simulations and hands-on labs
- Interactive threat modeling and red team scenarios
- Group discussions and table-top exercises
- Access to cloud-based sandbox environments

Register as a group from 3 participants for a Discount

Send us an email: info@fineskilltrainingcenter.com 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	$2,200
14 Sep 2026	25 Sep 2026	Online	$2,200
21 Sep 2026	02 Oct 2026	Online	$2,200
28 Sep 2026	09 Oct 2026	Online	$2,200
05 Oct 2026	16 Oct 2026	Online	$2,200
12 Oct 2026	23 Oct 2026	Online	$2,200

Start Date	End Date	Location	Price
19 Oct 2026	30 Oct 2026	Online	$2,200
26 Oct 2026	06 Nov 2026	Online	$2,200

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

Register Online Now

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