Cloud API Gateway Security 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 rapid adoption of Cloud-Native Architecture and Microservices has made APIs the foundational fabric of modern digital business. Consequently, the API Gateway, which acts as the crucial single entry point to backend services, has become a high-value, highly-targeted attack surface. Traditional security measures are insufficient against sophisticated, API-specific threats like those outlined in the OWASP API Security Top 10. This course is designed to equip security professionals and developers with the advanced, hands-on skills required to design, implement, and maintain robust API Gateway security across leading cloud platforms.

Cloud API Gateway Security Training Course focuses on proactive defense strategies, moving beyond simple rate limiting to master Zero Trust principles, advanced authentication and authorization, input validation, and real-time API threat monitoring. By blending theoretical knowledge with practical, lab-based exercises and real-world case studies, participants will learn to effectively mitigate risks such as BOLA, Excessive Data Exposure, and Business Logic Abuse. Successfully completing this training ensures you can secure your organization's digital assets, maintain regulatory compliance, and drive a secure DevSecOps pipeline in the era of pervasive cloud APIs.

Programme Curriculum

Cloud API Gateway Security Training Course

Introduction

The rapid adoption of Cloud-Native Architecture and Microservices has made APIs the foundational fabric of modern digital business. Consequently, the API Gateway, which acts as the crucial single entry point to backend services, has become a high-value, highly-targeted attack surface. Traditional security measures are insufficient against sophisticated, API-specific threats like those outlined in the OWASP API Security Top 10. This course is designed to equip security professionals and developers with the advanced, hands-on skills

required to design, implement, and maintain robust API Gateway security across leading cloud platforms.

Cloud API Gateway Security Training Course focuses on proactive defense strategies, moving beyond simple rate limiting to master Zero Trust principles, advanced authentication and authorization, input validation, and real-time API threat monitoring. By blending theoretical knowledge with practical, lab-based exercises and real-world case studies, participants will learn to effectively mitigate risks such as BOLA, Excessive Data Exposure, and Business Logic Abuse. Successfully completing this training ensures you can secure your organization's digital assets, maintain regulatory compliance, and drive a secure DevSecOps pipeline in the era of pervasive cloud APIs.

Course Duration

5 days

Course Objectives

Upon completion, participants will be able to:

1. Harden and Configure major Cloud API Gateways to industry Best Practices.
2. Implement advanced Authentication and Authorization mechanisms, including OAuth 2.1 and secure JWT validation.
3. Apply effective Rate Limiting and Throttling strategies to mitigate DDoS and API Abuse.
4. Defend against the OWASP API Security Top 10 vulnerabilities using gateway controls.
5. Design and enforce a Zero Trust Architecture for all API access flows.
6. Master granular Input Validation and Schema Enforcement to prevent Injection Attacks.
7. Deploy and manage Web Application Firewalls for API Gateway protection.
8. Implement mTLS for secure, encrypted communication between services.
9. Establish robust Logging, Monitoring, and Auditing strategies for Real-Time Threat Detection.
10. Integrate API security testing into a seamless DevSecOps and CI/CD Pipeline.
11. Secure Serverless and Containerized backend services exposed via the API Gateway.
12. Analyze and respond to API Security Incidents and perform effective Risk Assessment.
13. Ensure Regulatory Compliance through secure API practices.

Target Audience

1. Cloud Security Engineers/Architects
2. API Developers/Engineers
3. DevSecOps Engineers
4. Application Security Specialists
5. Penetration Testers/Red Teamers
6. Cloud Architects
7. Security Operations Center Analysts
8. Technical Security Managers/Team Leads

Course Modules

Module 1: Foundations of Cloud API Gateway Security

- API Gateway Architecture and its role in Microservices and Cloud-Native environments.
- Shared Responsibility Model in API Gateway Security across major Cloud Providers
- Understanding the expanded Attack Surface introduced by APIs and the shift from perimeter defense.
- In-depth review of the current Threat Landscape and common API attack vectors.

- Case Study: Analysis of a major Broken Access Control breach due to a misconfigured API Gateway proxy.

Module 2: Authentication and Authorization Mastery

- Implementing OAuth 2.1 and OpenID Connect for secure client and user authentication.
- Deep dive into JWT structure, validation, and common security pitfalls.
- Enforcing Granular Access Control and Role-Based Access Control policies at the gateway.
- Practical implementation of API Keys and Client Credentials with proper rotation and secret management.
- Case Study: Securing a partner API endpoint by migrating from insecure API keys to signed JWTs and resource-based authorization.

Module 3: OWASP API Top 10 Defense

- Mitigating Broken Object Level Authorization and Broken Function Level Authorization using gateway policies.
- Preventing Excessive Data Exposure and proper payload filtering.
- Implementing controls against Mass Assignment and ensuring safe request processing.
- Defense against Unrestricted Resource Consumption via advanced Rate Limiting and Throttling.
- Case Study: Simulating and remediating an attack where a user exploited BOLA to access data of other users on a multi-tenant cloud application.

Module 4: Network and Transport Layer Security

- Mandatory use and advanced configuration of TLS/SSL with strong cipher suites and protocols.
- Implementing mTLS for service-to-service authentication and encryption.
- Utilizing API Gateways to enforce CORS policies and prevent Cross-Site Request Forgery.
- DNS and Subdomain Takeover prevention for API endpoints.
- Case Study: Implementing mTLS on an API Gateway to secure communication with a sensitive internal microservice, demonstrating a key Zero Trust principle.

Module 5: Traffic Management and Attack Mitigation

- Designing an effective Rate Limiting strategy based on users, IP addresses, and request headers.
- Deploying and configuring a Web Application Firewall specifically for API traffic
- Implementing advanced Bot Mitigation and analyzing traffic patterns for Business Logic Abuse.
- Utilizing Input Validation and Schema Enforcement for all request and response payloads.
- Case Study: Configuring WAF rules to block common SQL Injection and XSS attempts targeting API input parameters.

Module 6: DevSecOps and API Security Testing

- Integrating API Security Testing into the CI/CD pipeline.
- Using Infrastructure as Code tools to secure gateway deployments.
- Automated Vulnerability Scanning and configuration auditing of the API Gateway.
- Shift-Left Security: Establishing a secure API Design-First approach with security requirements.
- Case Study: Setting up a GitOps workflow where API Gateway configuration changes are automatically audited and tested for security misconfigurations before deployment.

Module 7: Monitoring, Logging, and Incident Response

- Establishing comprehensive API Gateway Logging for security-relevant events.
- Integrating logs with Security Information and Event Management and Cloud Monitoring services.
- Creating Real-Time Alerts for suspicious activities
- Developing an effective API Security Incident Response Plan and forensic readiness.
- Case Study: Tracing an attempted data scraping attack using aggregated logs and creating a custom alert to prevent future occurrences.

Module 8: Platform-Specific Hardening and Advanced Topics

- Deep-dive into platform-specific security features
- Securing Serverless Functions exposed via the gateway.
- Advanced Secret Management and secure handling of backend service credentials.
- Understanding and mitigating risks associated with GraphQL API Security.
- Case Study: Hardening an AWS API Gateway deployment, including the use of a Lambda Authorizer and resource policies to control access to S3 buckets.

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