# Comprehensive API Security and Microservices Defense Training Course



16 - 20 Nov 2026

Boston

7500 € (Per Person)

Ref: #CYB1510_88007

## Course Introduction / Overview:

In today's distributed computing landscape, the shift from monolithic applications to microservices architectures has revolutionized software development, offering unparalleled scalability and agility. However, this architectural evolution introduces a complex and expanded attack surface, making robust API security and microservices defense non-negotiable. This course provides a comprehensive, A-to-Z exploration of the principles, protocols, and practices required to secure modern applications. Drawing on foundational concepts discussed by industry leaders like Sam Newman in his seminal work "Building Microservices," we will delve into the specific security challenges inherent in distributed systems. Participants will move beyond theoretical knowledge to gain practical, hands-on experience in identifying vulnerabilities and implementing multi-layered defense strategies. BIG BEN Training Center has designed this program to empower professionals to build, deploy, and maintain resilient and secure systems, ensuring that security is an integral part of the development lifecycle, not an afterthought. This training is essential for safeguarding sensitive data and maintaining operational integrity in a world increasingly reliant on interconnected services.

## Target Audience / This training course is suitable for:

- Software Developers and Engineers.
- DevOps and DevSecOps Professionals.
- Cybersecurity Analysts and Architects.
- Penetration Testers and Ethical Hackers.
- System and Network Administrators.
- IT Managers and Team Leaders.
- Quality Assurance Engineers.
- Cloud Security Engineers.

## Target Sectors and Industries:

- Financial Services and Banking.
- Healthcare and Medical Technology.
- E-commerce and Retail.
- Information Technology and Software Services.
- Telecommunications.
- Government and Public Sector Agencies.
- Energy and Utilities.
- Consulting and Professional Services.

## Target Organizations Departments:

- Information Technology.
- Software Development and Engineering.
- Cybersecurity and Information Security.
- DevOps and Platform Engineering.
- Infrastructure and Operations.
- Quality Assurance and Testing.
- Research and Development.
- Architecture and Strategy.

## Course Offerings:

By the end of this course, the participants will have able to:

- Master the fundamentals of microservices architecture and its unique security threat landscape.
- Implement robust authentication and authorization mechanisms using OAuth 2.0, OIDC, and JWTs.
- Apply the OWASP API Security Top 10 to identify and mitigate common vulnerabilities.
- Secure containerized environments using Docker and Kubernetes best practices.
- Configure and manage service mesh technologies like Istio for secure inter-service communication.
- Develop and execute effective API security testing and penetration testing strategies.
- Integrate security practices into CI/CD pipelines to foster a DevSecOps culture.
- Design and enforce comprehensive API security governance and lifecycle management policies.
- Implement advanced defense tactics such as rate limiting, throttling, and input validation.
- Conduct threat modeling for microservices-based applications to proactively identify risks.

## Course Methodology:

The training methodology at BIG BEN Training Center is designed to be highly interactive, immersive, and practical, ensuring participants can apply learned concepts directly to their professional roles. This course moves beyond traditional lectures by integrating hands-on labs, real-world case studies, and collaborative group exercises. Each module is structured to build knowledge incrementally, starting with foundational theories and progressing to advanced implementation techniques. Participants will engage in simulated scenarios that mirror the challenges of securing complex microservices architectures, allowing them to practice threat modeling, configure security protocols, and respond to mock security incidents in a controlled environment. Our expert instructors facilitate dynamic discussions, encouraging peer-to-peer learning and knowledge sharing. Continuous feedback is provided throughout the sessions to reinforce understanding and address individual queries. The program emphasizes a problem-solving approach, equipping attendees not just with answers, but with the critical thinking skills needed to architect and maintain secure systems in an ever-evolving technological landscape.

## Course Agenda (Course Units):

### Unit One: Foundations of Microservices and API Security

- Introduction to Microservices Architecture.
- The Evolving Threat Landscape for APIs.
- Understanding the OWASP API Security Top 10.
- Principles of Secure API Design.
- Deconstructing RESTful and GraphQL API Security.
- Security Considerations in Synchronous vs. Asynchronous Communication.
- Introduction to Threat Modeling for Distributed Systems.

### Unit Two: Identity, Authentication, and Access Control

- Deep Dive into API Authentication Patterns.
- Implementing OAuth 2.0 and OpenID Connect (OIDC).
- Securing Applications with JSON Web Tokens (JWTs).
- Best Practices for API Key Management and Security.
- Role-Based Access Control (RBAC) in Microservices.
- Attribute-Based Access Control (ABAC) Strategies.
- Managing Secrets in Distributed Environments (e.g., Vault).

### Unit Three: Securing the Microservices Infrastructure

- Container Security Fundamentals for Docker.
- Hardening Kubernetes Clusters and Pod Security Policies.
- Introduction to Service Mesh Concepts (e.g., Istio, Linkerd).
- Implementing Mutual TLS (mTLS) for Secure Service-to-Service Communication.
- Securing CI/CD Pipelines for DevSecOps.
- Infrastructure as Code (IaC) Security Best Practices.
- Network Policies and Segmentation in Kubernetes.

## Unit Four: Advanced API Defense and Mitigation Techniques

- The Role of API Gateways in Security Enforcement.
- Implementing Rate Limiting and Throttling to Prevent Abuse.
- Advanced Input Validation and Output Encoding.
- Comprehensive Logging, Monitoring, and Alerting for Security Events.
- Using Web Application Firewalls (WAFs) for API Protection.
- Defending Against Injection, Broken Object Level Authorization, and Mass Assignment.
- Strategies for Data Encryption in Transit and at Rest.

## Unit Five: Security Testing, Governance, and Future Trends

- API Security Testing and Vulnerability Assessment Methodologies.
- Automating Security Tests in the Development Lifecycle.
- API Penetration Testing Techniques and Tools.
- Establishing an API Security Governance Framework.
- Managing Security Across the Full API Lifecycle.
- Security Challenges in Serverless Architectures and Function-as-a-Service (FaaS).
- Emerging Trends in API Security and Zero Trust Architecture.

# FAQ:

### Qualifications required for registering to this course?

There are no requirements.

### How long is each daily session, and what is the total number of training hours for the course?

This training course spans five days, with daily sessions ranging between 4 to 5 hours, including breaks and interactive activities, bringing the total duration to 20 - 25 training hours.

## Something to think about:

As microservices become increasingly ephemeral and dynamic, how can traditional perimeter-based security models evolve to effectively implement a zero-trust architecture without hindering development velocity?

## What unique qualities does this course offer compared to other courses?

This course distinguishes itself by offering a holistic and deeply practical perspective that bridges the critical gap between software development and cybersecurity. Unlike programs that treat API security as an isolated topic, our curriculum integrates it directly into the context of modern microservices architectures and DevSecOps cultures. We move beyond a simple checklist of vulnerabilities by focusing on the architectural decisions and design patterns that create inherently resilient systems. The content is meticulously curated to reflect the realities of cloud-native environments, addressing the security of containers, Kubernetes, and service mesh technologies in detail. Participants will not only learn the "what" and "why" of API security threats but also the "how" of implementing robust defenses through extensive hands-on labs. The emphasis is on building a security-first mindset, enabling attendees to conduct meaningful threat modeling and embed security into every stage of the software development lifecycle, rather than treating it as a final, separate step.