CORE CONCEPT

API Management and API Security: Design, Gateways, Testing and Lifecycle

API Management and API Security: Design, Gateways, Testing and Lifecycle

Introduction:

API management decides whether an organisation's APIs behave as reliable products or as an unmanaged sprawl of undocumented endpoints, shadow versions and inconsistent access rules. Partners and internal teams then integrate against contracts that change without notice, and attackers exploit broken object level authorization or forgotten endpoints. This Core Concept course trains practitioners to design APIs contract first with the OpenAPI Specification, publish them through a gateway with enforced policies, secure them with OAuth 2.0 and JWT, test them and govern their lifecycle. Participants produce an API Product Management and Security Blueprint.

Course Objectives:

- Define API products, consumers and an API-first operating model with an inventory of existing endpoints and owners
- Write an OpenAPI description for a REST API that applies resource naming, status code, pagination and error model conventions
- Configure gateway policies for rate limiting, quotas, caching, request transformation and token validation on a published API
- Apply OAuth 2.0 grant selection, PKCE, scopes and JWT validation to protect API operations against the OWASP API Security Top 10 risks
- Build functional, contract and performance test suites for an API and wire them into a release pipeline
- Produce an API Product Management and Security Blueprint covering portal, versioning, deprecation, monitoring and governance rules

Target Audience:

- Developers who build and maintain REST services and the integrations that consume them
- Solution and integration architects responsible for interface design across applications and partners
- API product owners accountable for API consumers, onboarding and roadmap
- Platform and middleware engineers who run API gateways and developer portals
- Application security staff who review and test API authorisation and exposure

Course Outline:

Day 1: API-First Strategy, API Products and the Current API Estate

- API Management Components: Gateway, Developer Portal, Analytics, Lifecycle and Monetisation
- API-First Operating Model and Contract-Before-Code Workflow
- API Product Canvas: Consumers, Value, Service Levels and Access Tiers
- Private, Partner and Public API Exposure Models
- API Inventory and Ownership Register for the Participant Estate

Day 2: REST Design, the OpenAPI Specification and API Style Choices

- REST Resource Modelling, HTTP Methods, Status Codes and Idempotency
- OpenAPI Specification Structure: Info, Servers, Paths, Components and Security Schemes
- Pagination, Filtering, Error Payload and Naming Conventions in an API Style Guide
- GraphQL, gRPC and Event-Driven APIs at Overview: When REST Is Not the Fit
- Lab: Authoring and Linting an OpenAPI Description for a Sample Service

Day 3: API Gateway Policies, OAuth 2.0 and JWT in Practice

- API Gateway Request Pipeline: Routing, Policy Order and Backend Mediation
- Lab: Rate Limiting, Quota and Spike Arrest Policies per Consumer Tier
- Lab: Response Caching, Header Rewriting and Payload Transformation Policies
- OAuth 2.0 Grant Types, Scopes and PKCE per RFC 9700 Security Best Current Practice
- Lab: JWT Signature, Issuer, Audience and Expiry Validation at the Gateway

Day 4: OWASP API Security Top 10, API Testing and Contract Control

- Broken Object Level and Function Level Authorization: Attack Paths and Controls
- Unrestricted Resource Consumption, Server Side Request Forgery and Security Misconfiguration Controls
- Improper Inventory Management and Unsafe Consumption of Third-Party APIs
- Lab: Functional and Negative Test Collections with Common API Testing Tools
- Consumer-Driven Contract Tests and Load Tests in a Release Pipeline

Day 5: Developer Portal, Versioning, Monitoring, Governance and the Blueprint

- Developer Portal Onboarding Flow: Documentation, Sandbox, Keys and Support
- Versioning Scheme, Breaking Change Rules and Deprecation Notice Plan
- API Analytics Dashboard: Traffic, Latency, Error Rate and Consumer Adoption Metrics
- API Governance Review Board, Design Linting Rules and Publication Checklist
- API Product Management and Security Blueprint Build and Peer Review

Skills You Will Gain:

- API Product Definition
- OpenAPI Contract Authoring
- Gateway Policy Configuration
- Token-Based API Authorisation
- API Threat Assessment
- Contract and Load Testing
- API Version Lifecycle Control
- API Design Governance

Why Attend This Course:

- Return with an API Product Management and Security Blueprint built around APIs your own teams publish or consume
- Stop breaking consumers by moving to contract-first design, tested contracts and planned deprecation
- Close the authorisation and inventory gaps behind the most common API breaches before an attacker finds them
- Configure gateway, token and test settings hands on in labs and compare API practice with peers from banking, telecoms, retail, logistics and public services

Conclusion:

APIs now carry the transactions, data and partner integrations that organisations depend on, so they need the discipline of a product and the controls of a security boundary. The course moves from API products and the current estate, through REST design and the OpenAPI Specification, to gateway policies, OAuth 2.0 and JWT, then to the OWASP API Security Top 10 risks and functional, contract and performance testing. The final day covers the portal, versioning, monitoring and governance and produces an API Product Management and Security Blueprint.