Advanced Security for Services & SOA

OEM: Arcitura • Duration: 5 Days (40 hrs) • Code: S90.19B

COURSE MODULES & TOPICS

Module 1: Fundamental SOA, Services & Microservices

- Business and Technology Drivers for SOA, Services and Microservices
- Strategic Goals and Benefits of Service-Oriented Computing
- Plain English Introduction to Services and Microservices
- Fundamental Characteristics of a Service-Oriented Architecture
- Understanding Service-Orientation as a Design Paradigm, including coverage of the Four Pillars of Service-Orientation
- Introduction to Service Layers, Service Models and Service Compositions
- Service Inventories, Service Layers and Service API Governance and Management
- Introduction to Common Service Technologies, including API Gateways, Virtualization, Containerization
- Introduction to Cloud Computing and Cloud Services
- Adoption Impacts and Requirements, including considerations for Governance, Infrastructure, Performance and Standardization

Module 2: Microservice Technology Concepts

- Comparing Service Implementation Mediums
- Service Roles and Service Agents
- Message Exchange Patterns and Service Activities
- Basic XML, XML Schema, JSON and JSON Schema Concepts
- HTTP Methods, Response Codes and Headers
- Basic REST Service Concepts, including Properties and Constraints
- REST Services, Contracts, Resources and Messaging
- Hypermedia and Late Binding
- Basic WSDL and SOAP Concepts
- WS-* Technologies
- Web Service Contracts, Messaging and Registries
- Cloud Computing Concepts
- Vertical and Horizontal Scaling
- Multitenancy, Elasticity and Resiliency
- On-Demand Usage, Ubiquitous Access and Measured Usage
- Public, Private and Hybrid Clouds
- IaaS, PaaS and SaaS

Module 18: Fundamental Security for Services, Microservices & SOA

- Security and the Service-Oriented Architectural Model
- SOA Security Considerations for Service and Composition Architectures
- Security Implications of Service-Orientation Principles
- Trust, Claims, Tokens, Identity, Authentication, Authorization, Transport and Message Layer Security
- Encryption, Hashing, Digital Signatures, Identity and Access Management (IAM)
- Public Key Infrastructure (PKI), Digital Certificates, Certificate Authorities, Single Sign-On (SSO)
- REST Services and JSON Industry Standards
- JavaScript Object Signing and Encryption (JOSE) Framework, OAuth2
- HTTP Basic and Digest Authentication, API Key, JWT with X.509 certificates
- Service Interaction Security Patterns (Data Confidentiality, Data Origin Authentication, Direct Authentication, Brokered Authentication)
- Web Services and XML Industry Standards
- XML Encryption, XML Signature, WS-Security, Token Profiles, SAML
- Microservice Security Considerations
- Implementing SOA Security and Service-Orientation Security

Module 19: Advanced Security for Services, Microservices & SOA

- Understanding SOA Security Threats
- STRIDE (Spoofing, Tampering, Repudiation, Information Disclosure, Denial-of-Service, Elevation of Privilege)
- SOA Security Patterns for Internal Service Architecture (Exception Shielding, Message Screening, Trusted Subsystem, Service Perimeter Guard)
- Security Token Structures and Issuance (JWT, Username, X.509, SAML)
- Authentication Sessions and Secure Conversations
- Federation and Trust Brokering Security
- Policy Design and Governance
- REST Security Controls and Designs
- Open API Specification (OAS v 3.0), Open ID Connect
- Web service Security Controls and Designs
- WS-Policy, WS-SecurityPolicy, WS-Trust and WS-Secure Conversation with SAML
- Microservices and Containerization Security Considerations
- Security Extensions and Controls for API Gateways and ESBs
- Security Risks and Considerations for Cloud-based Services and Service Compositions
- Preparing for Common SOA Security Threats

Module 20: Security Lab for Services, Microservices & SOA

- Reading Exercise 20.1: Cutit Saws Mini Case Study Background
- Lab Exercise 20.2: Ordering Service Security Architecture Redesign
- Lab Exercise 20.3: Ordering Service Security Architecture Hardening for Threat Protection
- Lab Exercise 20.4: Aggregate Report Service Security Architecture
- Lab Exercise 20.5: REST Inventory Service Security Architecture
- Lab Exercise 20.6: Three-Party Permit Service Security Architecture

- Lab Exercise 20.7: Auction Solution Security Architecture
- Reading Exercise 20.8: YouSave Automotive Parts Mini Case Study Background
- Lab Exercise 20.9: ProcessOrder Service Security Architecture
- Lab Exercise 20.10: ProcessOrder Service Security Architecture Redesign
- is authored by a dedicated courseware development team
- has a self-test, accreditation exam and professional certification
- is available via two different eLearning platforms
- undergo a common development process
- are authored to be consistent in quality, structure and style
- share a common vocabulary and symbol notation
- are authored in collaboration with subject matter experts
- About Arcitura
- Instructor-Led Training & Coaching
- eLearning with Arcitura
- Course & Certification Tracks
- Exams & Proctoring
- Digital Accreditations
- Trainer Development
- Partner Program
- Partner Portal
- Privacy Policy
- Candidate Agreement
- Logo Guidelines
- Contact
- Help
- Arcitura on LinkedIn