INFOSECTRAIN

Security Architecture

Hands-on Training

Course Highlights

32-Hour LIVE Instructor-led Training

Practical Approach

Real-World Case Studies

Core Security Domains

TOGAF & **SABSA** Frameworks

SDLC Integration

Post Training Support

Career Guidance & Mentorship

Access to Recorded Sessions

About Course

This training offers in-depth knowledge and hands-on experience with the tools required to design, evaluate, and implement security architecture within complex enterprise ecosystems. It has a balanced perspective on how security and business objectives can co-exist, empowering professionals to make architecture decisions that are both technically sound and strategically aligned. With a stronghold and emphasis on frameworks, compliance, threat modeling, and secure design templates, this training ensures learners are well-versed in both theory and application.

Course Objectives

- Understand the role and significance of security architecture in enterprise environments
- Explore the integration of architecture within secure SDLC models
- Evaluate and apply global frameworks like TOGAF, SABSA, and OSA
- Map business requirements to security policies and regulatory obligations
- Apply secure design strategies, including threat modeling and surface analysis
- Design and document system architectures with contextual, logical, and physical views
- Address domain-specific security challenges across IAM, network, applications, and platforms
- Learn strategies for multi-cloud, SaaS, and on-prem hosting environments
- Improve communication and documentation of risk within architectural processes

Target Audience

- Security Architects
- Solutions Architects
- Cybersecurity Engineers
- Enterprise Architects
- Mid to Senior-Level Security Professionals

Pre-requisites

- This is an advanced-level training; at least **7 years of experience** in the security domain is required
- Fundamental knowledge of networks, cloud computing, and security concepts and terminology

Course Content

Introduction

- Significance of Design
- Architecture in SDLC
- Enterprise Architecture
- Onboarding System Challenges
- What is Security Architecture?

Common Frameworks

- Common Frameworks for Security Architecture
- TOGAF
- SABSA
- Open Security Architecture (OSA)

Business & Regulatory Requirements

- Mapping business & security requirements
- What business/industry are you in?
- Business Use Cases
- Business should supersede security requirements - Debatable
- Find a middle ground
- Security Policy should be aligned with regulatory requirements
- Mapping business requirements with security policies
- Regulatory requirement
- GDPR
- GLBA
- HIPAA
- DPDP Act

Security by Design

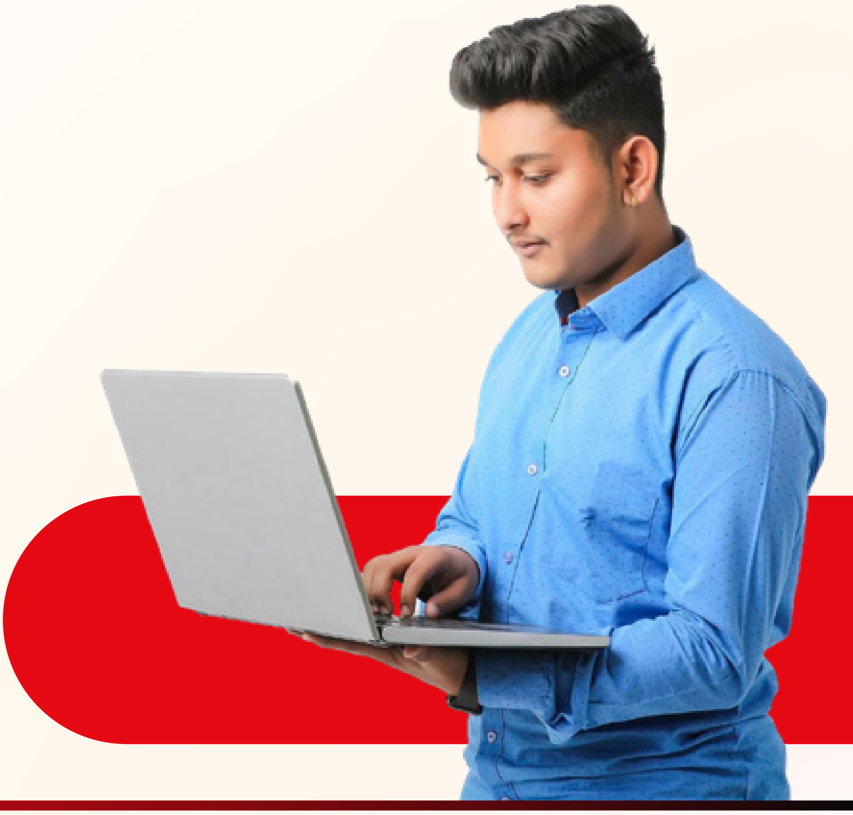
- Attack Surface Analysis
- Secure Technical Components
- Threat Modeling
- Fail Secure
- Defense in Depth
- Privacy By Design
- Secure Default
- Keep it Simple

Security Architecture Fundamentals

- Data Life Cycle
- Authentication and authorization (IAM & UER)
- Encryption
- Network Communication
- Business Resiliency
- Secure Data Integration Patterns
- Logging & Monitoring

Hosting Scenarios

- Hosting details
- On-Prem Data Center
- Private Cloud
- SaaS
- Multi-cloud strategy



Secure Design Template

- What is an architecture design?
- Design Interpretation (templates/references)
- System Contextual
- Logical Contextual
- Data flow design
- HLD
- LLD
- Physical Design
- Sample Designs

Elements of Security Architecture

- IAM Lifecycle (RBAM architecture, separate domains for employees/customers/vendors, etc.), UER
- GRC (Policy requirements and feedback, regulatory and legal updates)
- Application Security Architecture (DevOps, DevSecOps, CICD pipeline, container images, K8s, SCA, shift left, etc.) Microservice
- Network Security (SDN, SD-WAN, firewall rules, audits and management, EOL of network appliance, remote authentication protocols, using voice communication, wireless security)
- Security Operations (Incident response, SIEM, DLP capabilities, SOAR)
- PKI Infrastructure
- Emerging Technologies (AI/ML, Blockchain)
- Zero Trust Architecture
- Enterprise Data Warehouse, DB management architecture
- Platform Security
- Physical Security

Documenting & Communicating Risk

Case Study

Sample case study with artefacts

Solutions Architect 1

Solutions Architect 2

Solutions Architect 3

Solutions Architect 4

INFOSECTRAIN

Educate. Excel. Empower.

Contact us

www.infosectrain.com
sales@infosectrain.com

Follow us on