Secure by Design Training

Duration: **2 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

With the rise of cybercrime and exploitation of software vulnerabilities, organizations must integrate security **from the design phase**.
This {*training} teaches how to design, implement, and maintain security throughout the software development lifecycle (SDLC).

Updated with the **OWASP Top 10 (2021)** and **OWASP Top 10 for LLM Applications**, it covers the latest AI-related security threats, including prompt injection, data leakage, and unauthorized code execution. Learners gain deep understanding of **Secure by Design** principles and how to implement them in DevOps and AI-driven environments.

Regulatory Compliance (BDDK)

This course **fully complies** with the
Regulation on Banks' Information Systems and Electronic Banking Services (Articles 20, 22, 23, and 25).

Covered articles include:

- **Article 20:** Secure software development lifecycle and process management
- **Article 22:** Change management and configuration control
- **Article 23:** Security testing and vulnerability management
- **Article 25:** Information security management and traceability

Hence, this training is **recommended for banks and regulated financial institutions** to maintain compliance and resilience.

Who Should Attend

Developers, DevOps engineers, cybersecurity professionals,
and **IT leaders in financial institutions or regulated industries**.

Secure by Design Training

Duration: **2 Day**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

By the end of this {*training}, you will have gained knowledge and skills in the following areas:

- Understand Secure SDLC models and choose the appropriate approach.
- Apply secure design principles throughout the lifecycle.
- Identify and mitigate OWASP Top 10 vulnerabilities.
- Implement threat modeling (STRIDE, Attack Trees).
- Apply encryption, access control, and code review best practices.
- Address AI-generated software risks (prompt injections, data poisoning).
- Understand OWASP Top 10 for Large Language Models.

Upon completion, participants will be able to:

- Embed security in design and development workflows,
- Create BDDK-compliant secure SDLC pipelines,
- Strengthen software resilience against modern and AI-based threats.

Secure by Design Training

Duration: **2 Day**

BILGINÇ IT Academy
info@bilginc.com
bilginc.com

Outline

Module 1 – Secure Development Lifecycle (SDLC)

- Overview of SDLC models and DevSecOps integration
- Source control and configuration management
- API security and risk analysis tools

Module 2 – Secure by Design

- Threat modeling and secure architecture
- Supply chain and trust boundary risk mitigation
- Defense in Depth, Least Privilege, and input validation

Module 3 – Application Security (OWASP 2021)

- Vulnerabilities and mitigation strategies
- Case studies and attack vectors
- Logging, cryptography, and security configuration

Module 4 – Securing AI and Modern Apps

- Code review and CI/CD testing
- Encryption and hashing strategies
- AI security and LLM-specific vulnerabilities
- Future of Secure by Design in AI