Secure by Design Eğitimi

Süre: **2 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

Siber tehditler, kurumların yazılım ve sistem geliştirme süreçlerinde **güvenliği en baştan tasarlama** gerekliliğini her geçen gün artırıyor.
“Secure by Design” prensibiyle geliştirilen sistemler, saldırı yüzeyini minimize eder ve saldırganların yaygın zafiyetlerden faydalanmasını engeller.

Bu {*eğitim}, **OWASP Top 10 (2021)** ve en güncel **OWASP Top 10 for LLM Applications** (Prompt Injection, Data Leakage, Unauthorized Code Execution vb.) içeriğiyle güncellenmiştir.
Katılımcılar, güvenli geliştirme yaşam döngüsünü (SDLC) tasarımdan üretime kadar nasıl güvenli hale getireceklerini öğreneceklerdir.
Ayrıca **yapay zekâ destekli yazılım (AI-generated code)** güvenliği ve **GitHub Copilot** gibi araçların güvenlik riskleri de uygulamalı olarak ele alınır.

Regülasyon Uyumu (BDDK)

Bu eğitim içeriği,
“Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik” kapsamında **tam uyumludur**.
İlgili maddeler:

- **Madde 20 – Güvenli Yazılım Geliştirme:** Eğitimdeki *Secure SDLC, Threat Modeling, OWASP Top 10* modülleri birebir uyumludur.
- **Madde 22 – Değişiklik Yönetimi:** Konfigürasyon, kaynak kod yönetimi ve sürüm güvenliği eğitim içinde yer alır.
- **Madde 23 – Güvenlik Testleri:** OWASP temelli zafiyet analizi ve güvenlik test stratejileri bölümleri kapsar.
- **Madde 25 – Bilgi Güvenliği Yönetimi:** Eğitim boyunca kurum içi güvenli tasarım ve izlenebilir geliştirme süreçleri vurgulanır.

Bu nedenle **bankalar, sigorta kurumları ve finansal kuruluşlar** için bu eğitimi almak **regülasyon uyumluluğu açısından önerilmektedir**.

Who Should Attend

- Yazılım geliştiriciler
- DevOps / DevSecOps mühendisleri
- BT Güvenlik yöneticileri
- **Bankalar, FinTech ve regülasyona tabi kurumlarda** görev alan teknik uzmanlar

Secure by Design Eğitimi

Süre: **2 Gün**

BİLGİNÇ
IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

Bu {*eğitim} sonunda aşağıdaki konularda bilgi ve beceri kazanmış olacaksınız:

- Secure SDLC modellerini tanır ve doğru model seçimini yapar.
- Yazılım yaşam döngüsünün her aşamasında güvenliği dahil etmeyi öğrenir.
- OWASP Top 10 (2021) ve**LLM Top 10** risklerini anlar, önlem tekniklerini uygular.
- Tehdit modelleme, STRIDE, Attack Tree gibi güvenlik analiz yöntemlerini kullanır.
- API güvenliği, şifreleme, kod gözden geçirme (Code Review) süreçlerinde en iyi uygulamaları uygular.
- AI tabanlı yazılımlarda prompt injection ve model zehirlenmesi (data poisoning) gibi tehditleri tanımlar.

Bu eğitimi tamamlayan katılımcılar, yazılım geliştirme süreçlerine güvenliği tasarımdan itibaren dahil ederek:

- Güvenli kodlama kültürü oluşturabilir,
- AI tabanlı sistemlerde güvenlik farkındalığı kazanır,
- **BDDK Bilgi Sistemleri Yönetmeliği**'ne tam uyumlu süreçler kurabilir.

Secure by Design Eğitimi

Süre: **2 Gün**

BİLGİNÇ
IT Academy
info@bilginc.com
bilginc.com

Outline

Modül 1 – Secure Development Lifecycle (SDLC)

- SDLC modellerine genel bakış
- DevOps, DevSecOps ve güvenli kaynak kod yönetimi
- API güvenliği, yapılandırma yönetimi
- Risk analiz araçları ve güvenli sürümleme

Modül 2 – Secure by Design

- Güvenli geliştirme süreçleri
- Tehdit modelleme (STRIDE, Attack Trees)
- Tedarik zinciri güvenliği ve güven sınırları (Trust Boundaries)
- Geliştirme aşamasında “Defense in Depth” prensipleri
- En az ayrıcalık (Least Privilege) ve giriş doğrulama stratejileri

Modül 3 – Application Security & OWASP 2021

- OWASP Top 10 (2021) zafiyetleri ve vaka çalışmaları
- Broken Access Control, Injection, XSS, Misconfiguration
- Data Exposure, Insecure Deserialization, SSRF
- Güvenlik testleri, loglama, kriptografi yönetimi

Modül 4 – Modern Uygulama Güvenliği ve AI

- Kod inceleme (Code Review) ve CI/CD entegrasyonu
- Şifreleme, hashleme, metadata koruma
- **AI Security for Secure by Design**
- OWASP Top 10 for LLM (Prompt Injection, Data Leakage, Insecure Plugins vb.)
- Geleceğin AI güvenliği tehditleri