ISTQB - Security Test Engineer Eğitimi

Süre: **3 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

Bu Eğitim Size Ne Kazandırır?

- **Yazılım ve BT sistemlerinin güvenliğini değerlendirmek** için kullanılan test yaklaşımlarını ve tekniklerini öğrenebilirsiniz.
- **Penetrasyon testleri, zafiyet taramaları ve risk odaklı test yöntemleri** hakkında bilgi edinerek güvenlik testlerini daha sistematik şekilde gerçekleştirebilirsiniz.
- **Tehdit modelleme, güvenlik risk analizi ve test tasarımı** süreçlerini kullanarak test çalışmalarını kurumsal risklere göre planlayabilirsiniz.
- **Güvenlik testi araçlarını** ihtiyaçlara uygun şekilde seçebilir ve test sonuçlarını analiz edebilirsiniz.
- **Güvenlik açıklarını raporlama, bulguları paydaşlara aktarma ve zafiyet yönetimi** süreçlerine katkı sağlayabilirsiniz.
- **OWASP, ISO 29119 ve bilgi güvenliği yönetim sistemleri** çerçevesinde güvenlik testlerini yazılım geliştirme yaşam döngüsüne entegre etmeyi öğrenebilirsiniz.

ISTQB – Security Test Engineer Eğitimi, BT tabanlı sistemlerin güvenlik açısından test edilmesinde görev alan profesyoneller için hazırlanmış **3 günlük bir teknik eğitim programıdır**.

Eğitim, güvenlik testlerinin planlanmasından çok**test faaliyetlerinin uygulanmasına, uygun araçların kullanılmasına, sonuçların değerlendirilmesine ve güvenlik bulgularının raporlanmasına** odaklanır. Katılımcılar, farklı yazılım geliştirme ortamlarında güvenlik testlerinin nasıl yürütüldüğünü ve elde edilen sonuçların daha geniş kapsamlı risk yönetimi süreçlerine nasıl dahil edildiğini öğrenir.

Program kapsamında **güvenlik paradigmaları, güvenlik testi teknikleri, test süreçleri, standartlar ve iyi uygulamalar** incelenir. Ayrıca organizasyonların güvenlik politikaları, düzenleyici gereksinimleri ve saldırı senaryolarının test faaliyetleri üzerindeki etkileri değerlendirilir.

Eğitimin devamında güvenlik testlerinin **yazılım geliştirme yaşam döngüsü (SDLC)** boyunca nasıl konumlandırılacağı, operasyon ve bakım aşamalarında nasıl sürdürüleceği ele alınır. **Bilgi Güvenliği Yönetim Sistemi (ISMS)** ile güvenlik testi sonuçları arasındaki ilişki, kabul kriterleri ve süreç iyileştirme yaklaşımları da programın önemli konularındandır.

Katılımcılar ayrıca **güvenlik testi raporları, zafiyet analizi, zafiyet yönetimi ve test araçlarının kullanımı** hakkında bilgi edinir.

Bu eğitim, güvenlik testi uygulamalarındaki yetkinliğini artırmak ve**güvenli yazılım geliştirme süreçlerine** daha etkin katkı sağlamak isteyen profesyoneller için tasarlanmıştır.

Prerequisites

ISTQB - Security Test Engineer Eğitimi

Süre: **3 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Eğitimle ilişkili sınava katılacak adayların **ISTQB Foundation Level** sertifikasına sahip olması gerekir.

Sertifikasyon Ön Koşulu

İlgili **ISTQB Security Test Engineer** sınavına katılabilmek için **ISTQB Foundation Level sertifikası** gereklidir.

Who Should Attend

Bu eğitim, **yazılım ve BT sistemlerinin güvenlik testlerinde** görev alan veya bu alanda uzmanlaşmak isteyen profesyonellere yöneliktir.

Özellikle aşağıdaki roller için uygundur:

- **Yazılım test uzmanları**
- **Güvenlik test mühendisleri**
- **Kalite güvence (QA) uzmanları**
- **Yazılım güvenliği ve uygulama güvenliği uzmanları**
- **Test liderleri ve test yöneticileri**
- **Güvenlik testi süreçlerinde sorumluluk alan BT profesyonelleri**

ISTQB - Security Test Engineer Eğitimi

Süre: **3 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

What You Will Learn

Bu eğitimi tamamladığınızda:

- **ISTQB güvenlik testi** yaklaşımında kullanılan temel kavramları, ilkeleri ve terminolojiyi açıklayabileceksiniz.
- **Penetrasyon testi (Penetration Testing)** ve **zafiyet taraması (Vulnerability Scanning)** dahil olmak üzere güvenlik testi tekniklerini değerlendirebilecek ve uygun durumlarda uygulayabileceksiniz.
- **Tehdit modelleme (Threat Modeling)** ve **risk odaklı test (Risk-Based Testing)** yaklaşımlarıyla güvenlik risklerini analiz edebileceksiniz.
- Kurumsal **risk yönetimi ve uyumluluk gereksinimleriyle** uyumlu güvenlik testi planları hazırlayabileceksiniz.
- Farklı yazılım geliştirme ortamlarında kullanılabilecek **güvenlik testi araçlarını** seçebilecek ve uygulayabileceksiniz.
- **Güvenlik testi sonuçlarını** yorumlayabilecek, bulguları raporlayabilecek ve ilgili paydaşlara anlaşılır biçimde aktarabileceksiniz.
- **OWASP ve ISO 29119** gibi güvenlik testiyle ilişkili standart ve iyi uygulamalardan yararlanabileceksiniz.
- Güvenlik testi faaliyetlerini farklı **yazılım geliştirme yaşam döngüsü (SDLC)** aşamalarına entegre edebileceksiniz.
- **Zero Trust, güvenlik denetimleri ve varlık güvenliği** gibi temel güvenlik yaklaşımlarını test süreçleriyle ilişkilendirebileceksiniz.
- **Saldırı senaryolarını** analiz ederek güvenlik testi tasarımına katkı sağlayabileceksiniz.
- **Bilgi Güvenliği Yönetim Sistemi (ISMS)** kapsamında test sonuçlarının risk yönetimi süreçlerinde nasıl kullanılacağını açıklayabileceksiniz.
- **Güvenlik açıklarının analizi ve yönetimi** süreçlerine destek olabileceksiniz.
- Kurumunuzdaki **güvenlik testi süreçlerinin sürekli iyileştirilmesine** yönelik fırsatları belirleyebileceksiniz.

Outline

1. Güvenlik Paradigmaları

- **Varlık güvenlik seviyelerinin (Asset Security Levels)** belirlenmesi ve değerlendirilmesi
- **Güvenlik denetimlerinin (Security Audits)** amacı ve güvenlik testleriyle ilişkisinin incelenmesi

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- **Zero Trust (Sıfır Güven)** yaklaşımının temel kavramlarının açıklanması
- **Açık kaynak yazılımların (Open-Source Software)** güvenlik açısından değerlendirilmesi

2. Güvenlik Testi Teknikleri

- Farklı **güvenlik testi türlerinin** ve kullanım amaçlarının incelenmesi
- **Güvenlik testi tekniklerinin** uygun senaryolarda uygulanması
- **Güvenlik testlerinin tasarlanması** ve test yaklaşımının belirlenmesi

3. Güvenlik Testi Süreci

- **Güvenlik testi sürecini** oluşturan temel faaliyetlerin açıklanması
- Güvenlik gereksinimlerine uygun **test senaryolarının ve testlerin tasarlanması**
- **Test yürütme (Test Execution)** aşamasında dikkate alınması gereken koşulların değerlendirilmesi

4. Standartlar ve İyi Uygulamalar

- **Güvenlik testi standartlarının** ve kullanım alanlarının incelenmesi
- Güvenlik testlerinde **iyi uygulamaların (Best Practices)** kullanılması
- **Standartlardan yararlanarak** test faaliyetlerinin planlanması ve yürütülmesi

5. Organizasyonel Bağlam

- **Organizasyon yapılarının** güvenlik testi süreçleri üzerindeki etkilerinin değerlendirilmesi
- **Güvenlik politikalarının ve yasal/düzenleyici gereksinimlerin** incelenmesi
- **Saldırı senaryolarının (Attack Scenarios)** analiz edilmesi

6. Yazılım Geliştirme Yaşam Döngüsü

- Farklı **yazılım geliştirme yaşam döngüsü modellerinin** değerlendirilmesi
- **Operasyon süreçlerinde güvenlik testlerinin** uygulanması
- Yazılımın **bakım faaliyetleri** sırasında güvenlik testlerinin sürdürülmesi

7. Bilgi Güvenliği Yönetimi

- **Bilgi Güvenliği Yönetim Sistemlerinin (ISMS)** temel yapısının ve güvenlik testleriyle ilişkisinin açıklanması
- Güvenlik testleri için **kabul kriterlerinin (Acceptance Criteria)** belirlenmesi
- **Güvenlik testi süreçlerinin iyileştirilmesine** yönelik yaklaşımların değerlendirilmesi

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

8. Raporlama ve Güvenlik Açıkları

- **Güvenlik testi sonuçlarının raporlanması** ve bulguların sunulması
- **Güvenlik açıklarının (Vulnerabilities)** analiz edilmesi
- **Zafiyet yönetimi (Vulnerability Management)** süreçlerinin incelenmesi

9. Güvenlik Testi Araçları

- **Güvenlik testi araç kategorilerinin** ve kullanım amaçlarının tanıtılması
- Farklı test gereksinimlerine uygun **güvenlik testi araçlarının seçilmesi ve uygulanması**