CompTIA Security+ Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

CompTIA Security+, dünya çapında kabul gören ve **siber güvenlik kariyeri** hedefleyen profesyoneller için güçlü bir temel oluşturan sertifikalardan biridir. Bu kapsamlı 5 günlük eğitim programı, katılımcıları resmi **CompTIA Security+ SY0-701 sınavına** hazırlamak amacıyla tasarlanmıştır. Eğitim ücretine resmi sınav voucher'ı dahildir.

Program boyunca katılımcılar; **uygulama güvenliği**, **ağ güvenliği**, **cihaz güvenliği** ve **kurumsal sistemlerin korunması** gibi kritik alanlarda bilgi sahibi olur. Ayrıca **tehdit analizi**, **risk azaltma stratejileri**, **olay müdahalesi** ve **uyumluluk süreçleri** gibi günümüz kurumlarının ihtiyaç duyduğu güvenlik becerilerini geliştirir.

Neden CompTIA Security+?

CompTIA Security+ sertifikası, profesyonellerin:

- **Ağları koruma**
- Tehditleri tespit etme
- Verileri güvence altına alma
- Güvenlik olaylarına müdahale etme

becerilerini doğrular.

Bu sertifika, **cyber security career** yolculuğuna başlamak isteyen profesyoneller için güçlü bir referans niteliği taşır ve dünya genelinde işverenler tarafından tanınmaktadır.

Prerequisites

Eğitimden maksimum verim alınabilmesi için aşağıdaki konulara aşinalık önerilir:

- Temel **networking** bilgisi
- **Windows** işletim sistemi deneyimi
- **Linux** işletim sistemi bilgisi
- Temel BT altyapı kavramları

CompTIA Security+ Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Who Should Attend

Bu eğitim aşağıdaki pozisyonlarda çalışan veya çalışmayı hedefleyen profesyoneller için uygundur:

- **Security Administrator**
- **Security Specialist**
- **Systems Administrator**
- **Help Desk Analyst**
- **Security Engineer**
- **Security Analyst**
- Ağ ve sistem uzmanları
- **Siber güvenlik uzmanı** olmak isteyen BT profesyonelleri

What You Will Learn

Bu eğitimi tamamlayan katılımcılar:

- Kurumsal ortamların **güvenlik durumunu değerlendirebilir**
- Uygun **güvenlik çözümlerini** belirleyip uygulayabilir
- **Bulut**, **mobil**, **IoT** ve **operasyonel teknoloji (OT)** ortamlarını güvence altına alabilir
- **Risk yönetimi**, **uyumluluk** ve **güvenlik yönetişimi** süreçlerini anlayabilir
- Güvenlik olaylarını analiz ederek etkili müdahalelerde bulunabilir
- Kimlik ve erişim yönetimi süreçlerini uygulayabilir

Outline

1. Temel Güvenlik Kavramları (%12)

Bu bölüm, modern **siber güvenlik** yaklaşımının temel taşlarını kapsar.

Konular:

- Güvenlik kontrolleri ve türleri
- Temel güvenlik prensipleri
- Değişiklik yönetimi süreçleri
- Güvenlik üzerindeki etkileri
- **Kriptografi** ve şifreleme çözümleri
- Kurumsal güvenlik yaklaşımları

2. Tehditler, Zafiyetler ve Koruma Yöntemleri (%22)

Katılımcılar modern saldırı yöntemlerini ve savunma tekniklerini öğrenir.

Konular:

- Tehdit aktörleri ve motivasyonları
- Saldırı yüzeyleri
- Saldırı vektörleri

- Güvenlik açıkları
- Zararlı aktivite göstergeleri
- Kurumsal koruma stratejileri
- Risk azaltma yöntemleri

3. Güvenlik Mimarisi (%18)

Kurumsal altyapıların güvenli şekilde tasarlanması ve korunması ele alınır.

Konular:

- **Security Architecture** modelleri
- Altyapı güvenliği
- Veri koruma stratejileri
- Güvenlik prensipleri
- İş sürekliliği
- Felaket kurtarma
- Dayanıklılık ve erişilebilirlik

4. Güvenlik Operasyonları (%28)

Modern güvenlik operasyonlarında kullanılan araçlar ve süreçler incelenir.

Konular:

- Sistem güvenliği uygulamaları
- Donanım ve yazılım güvenliği
- Varlık yönetimi
- **Vulnerability Management**
- Güvenlik izleme araçları
- Güvenlik uyarıları ve log yönetimi
- **Identity and Access Management (IAM)**
- Olay müdahalesi süreçleri
- Güvenlik soruşturmaları
- Otomasyon ve orkestrasyon

5. Güvenlik Program Yönetimi ve Yönetişim (%20)

Kurumsal güvenlik programlarının yönetimi üzerinde durulur.

Konular:

- **Security Governance**
- **Risk Management**
- Üçüncü taraf risk değerlendirmeleri
- Güvenlik uyumluluğu
- Denetim ve değerlendirme süreçleri
- Güvenlik farkındalığı çalışmaları
- Kurumsal güvenlik politikaları