CompTIA Cybersecurity Analyst (CySA+) Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

Bu **{*eğitim}**, güvenlik olaylarını tespit etmek, analiz etmek ve müdahale etmekle görevli **Siber Güvenlik Uzmanları** için tasarlanmış uluslararası geçerliliğe sahip bir sertifikasyon eğitimidir. Program, sürekli **Güvenlik İzleme (Security Monitoring)** süreçleri kapsamında tehditlerin belirlenmesi, güvenlik açıklarının yönetilmesi ve olay müdahalesi konularına odaklanmaktadır.

Katılımcılar eğitim süresince **Tehdit İstihbaratı (Threat Intelligence)**, **Threat Hunting**, **Zafiyet Yönetimi**, **SOC Operasyonları**, **Olay Müdahalesi (Incident Response)** ve modern güvenlik analiz yöntemleri hakkında kapsamlı bilgi edinirler. Eğitim sonunda katılımcılar, gerçek dünya senaryolarında güvenlik olaylarını analiz etme ve uygun aksiyonları alma becerisine sahip olurlar.

Prerequisites

Katılımcıların aşağıdaki bilgi ve deneyimlere sahip olması tavsiye edilir:

- **CompTIA Network+** seviyesinde ağ bilgisi
- **CompTIA Security+** seviyesinde güvenlik bilgisi
- Temel veya orta düzey **Siber Güvenlik Operasyonları** deneyimi

Who Should Attend

Bu eğitim aşağıdaki profesyoneller için uygundur:

- **Security Analyst**
- **SOC Analyst**
- **Incident Response Analyst**
- **Vulnerability Management Analyst**
- **Security Engineer**
- Güvenlik operasyon merkezlerinde çalışan uzmanlar
- Siber güvenlik kariyerini geliştirmek isteyen BT profesyonelleri

What You Will Learn

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

- Zararlı aktivitelerin göstergelerini tespit edip analiz edebilir.
- **Threat Hunting** ve **Threat Intelligence** süreçlerini uygulayabilir.
- Güvenlik açıklarını önceliklendirebilir ve yönetebilir.
- **Incident Response** süreçlerini etkin şekilde yürütebilir.
- Güvenlik raporlaması ve iletişim süreçlerini yönetebilir.
- Modern siber tehditleri analiz ederek uygun güvenlik kontrolleri önerebilir.

CompTIA Cybersecurity Analyst (CySA+) Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Outline

Modül 1: Zafiyet Yönetimi ve Güvenlik İyileştirme Süreçleri

- **Cybersecurity Leadership** kavramları
- Güvenlik kontrolleri ve kontrol türleri
- **Patch Management** süreçleri
- Güvenlik iyileştirme stratejileri

Modül 2: Tehdit İstihbaratı ve Threat Hunting

- Tehdit aktörlerinin analizi
- Aktif tehditlerin belirlenmesi
- **Threat Hunting** metodolojileri
- Güvenlik istihbaratının kullanımı

Modül 3: Sistem ve Ağ Mimarisi Temelleri

- Sistem mimarisi kavramları
- Ağ altyapılarının değerlendirilmesi
- **Identity and Access Management (IAM)**
- Operasyonel görünürlük ve izleme

Modül 4: Güvenlik Operasyonlarında Sürekli İyileştirme

- Güvenlik operasyonlarında liderlik
- Operasyonel verimlilik
- Güvenlik teknolojilerinin etkin kullanımı

Modül 5: Zafiyet Tarama Süreçleri

- Uyumluluk gereksinimleri
- **Vulnerability Scanning** yöntemleri
- Zafiyet taramalarında özel senaryolar
- Güvenlik değerlendirme araçları

Modül 6: Zafiyet Analizi

- **CVSS** ve zafiyet puanlama sistemleri
- Risk önceliklendirme yöntemleri
- Zafiyet bağlamı ve etki değerlendirmeleri

Modül 7: Zafiyet Bilgilerinin Raporlanması

- Etkili güvenlik iletişimi
- Teknik raporlama yöntemleri
- Aksiyon planlarının hazırlanması
- Güvenlik yöneticileri için raporlama süreçleri

Modül 8: Olay Müdahalesi Süreçleri

- **Incident Response Planning**

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

- Olay müdahale yaşam döngüsü
- Güvenlik olaylarının yönetimi
- Müdahale prosedürleri

Modül 9: Olay Müdahalesi İletişimi

- Olay iletişim planları
- Paydaş yönetimi
- Güvenlik olaylarının analizi
- Olay sonrası değerlendirme süreçleri

Modül 10: Zararlı Aktivitelerin Tespiti

- Zararlı faaliyetlerin belirlenmesi
- **MITRE ATT&CK** ve saldırı metodolojileri
- Tehdit tespit teknikleri
- Güvenlik analizi araçları

Modül 11: Şüpheli Aktivitelerin Analizi

- Ağ saldırısı göstergeleri
- Host tabanlı saldırı göstergeleri
- **Vulnerability Assessment Tools**
- Tehdit göstergelerinin değerlendirilmesi

Modül 12: Uygulama Güvenliği ve Zafiyet Analizi

- Web uygulaması güvenlik açıkları
- **Cloud Security Vulnerabilities**
- Uygulama güvenliği değerlendirmeleri
- Modern saldırı senaryoları

Modül 13: Script ve Analiz Araçları

- Temel script dilleri
- Güvenlik otomasyonu
- Analiz araçlarının kullanımı
- Şüpheli aktivitelerin incelenmesi

Modül 14: Uygulama Güvenliği ve Saldırı Önleme

- **Secure Software Development**
- Güvenli yazılım geliştirme yaşam döngüsü
- Uygulama saldırılarını önleme yöntemleri
- Güvenlik kontrollerinin uygulanması
- Savunma katmanlarının güçlendirilmesi