



**NETWORK GÜVENLİĞİ VE SAVUNMA STRATEJİLERİ
EĞİTİMİ
3 GÜN**



Digital Vizyon
Akademi

www.digitalvizyon.net

Eđitim Hakkında

Network G¼venliđi ve Savunma Stratejileri Eđitimi, son derece ¼nemlidir. Bu eđitim, ađ g¼venliđine kapsamlı bir giriř sađlar. Katılımcılar, siber tehditleri tanıma ve ¼nleme y¼ntemlerini ¼ğrenirler. Aynı zamanda, g¼venlik duvarları, antivir¼s programları gibi savunma aralarını keřfederler. Bu aralar, ađları siber saldırılardan korumak iin gereklidir.

Eđitim, g¼venlik politikalarının oluřturulması ve uygulanmasına odaklanır. Katılımcılar, etkili g¼venlik politikaları nasıl geliřtireceklerini ¼ğrenirler. Bu politikalar, organizasyonların g¼venlik standartlarını belirler. Aynı zamanda, uyum s¼relerini kolaylařtırır. Bu kolaylık, yasal gerekliliklere uyumu sađlar.

Sızma testi ve zafiyet tarama teknikleri de eđitimde yer alır. Katılımcılar, ađ zafiyetlerini tespit etme ve deđerlendirme becerilerini geliřtirirler. Bu beceriler, g¼venlik aıklarını proaktif olarak y¼netmeyi sađlar. Aynı zamanda, risk deđerlendirme s¼relerini iyileřtirir. Bu iyileřtirme, g¼venlik risklerini azaltır.

Eđitim, kriptografi ve řifreleme y¼ntemlerine de yer verir. Katılımcılar, veri gizliliđini ve b¼t¼nl¼đ¼n¼ koruma y¼ntemlerini ¼ğrenirler. Bu y¼ntemler, verilerin yetkisiz eriřime karřı korunmasını sađlar. Aynı zamanda, g¼venli iletiřimi garantiler. Bu garanti, g¼venlik ihlallerinin ¼nlenmesine yardımcı olur.

Network G¼venliđi ve Savunma Stratejileri Eđitimi, katılımcılara pratik beceriler kazandırır. Bu beceriler, onların kendi ađlarını g¼venli bir řekilde y¼netmelerine yardımcı olur. Eđitim, ađ g¼venliđi ve savunma konularında derinlemesine uzmanlık kazandırır. Bu sayede katılımcılar, eđitimle birlikte, g¼venlik tehditlerine karřı etkili ¼nlemler alabilirler.

Sonuç olarak, bu eđitim, ađ g¼venliđi ve savunma stratejileri konusunda kapsamlı bir bilgi sunar. Katılımcılar, ađ g¼venliđini artırmak iin gerekli araları ve teknikleri ¼ğrenirler. Eđitim sonunda, katılımcılar, siber g¼venlik tehditlerine karřı korunaklı ađlar geliřtirebilirler. Bu beceriler, onların profesyonel geliřimlerine b¼y¼k katkı sađlar.

Neler ¼ğreneceksiniz

1. Ađ G¼venliđi Tehditleri ve Zafiyetleri
2. G¼venlik Politikaları ve Standartları
3. Siber G¼venlik Araları ve Teknolojileri
4. Tehdit Tespiti ve Yanıt Stratejileri
5. Olay M¼dahale ve Y¼netimi
6. Veri Koruma ve řifreleme Teknikleri
7. G¼venlik Testleri ve Deđerlendirmeler
8. Gerek D¼nya Senaryoları ve Case Study'ler



Ön Koşullar

1. Temel ağ ve IT güvenliği bilgisi
2. Siber güvenlik ve risk yönetimi konularında genel anlayış
3. Ağ protokolleri ve teknolojileri hakkında temel bilgi

Kimler Katılnmalı

- Ağ güvenliğini ve savunma stratejilerini öğrenmek isteyen IT ve ağ profesyonelleri
- Kurumsal ağ güvenliğini artırmak isteyen sistem yöneticileri ve teknisyenleri
- Siber güvenlik alanında kariyer yapmayı hedefleyen IT uzmanları ve aspiranları
- Ağ güvenliği ve savunma teknikleri konusunda ileri düzey bilgi kazanmak isteyen her seviyeden bireyler

Eğitim İçeriği

1. **Ağ Güvenliği Tehditleri ve Zafiyetleri**
 - Güncel Güvenlik Tehditleri ve Zafiyetler
 - Güvenlik Zafiyetlerinin Analizi
2. **Güvenlik Politikaları ve Standartları**
 - Güvenlik Politika Geliştirme ve Uygulama
 - Uyum ve Standartlar
3. **Siber Güvenlik Araçları ve Teknolojileri**
 - Güvenlik Araçları ve Çözümleri
 - Teknolojik Güvenlik Yaklaşımları
4. **Tehdit Tespiti ve Yanıt Stratejileri**
 - Tehdit Algılama Sistemleri
 - Etkili Yanıt ve Müdahale Yöntemleri
5. **Olay Müdahale ve Yönetimi**
 - Olay Yönetimi Süreçleri
 - Kriz Müdahalesi ve İyileştirme
6. **Veri Koruma ve Şifreleme Teknikleri**
 - Veri Güvenliği ve Şifreleme Yöntemleri
 - Veri Koruma Stratejileri
7. **Güvenlik Testleri ve Değerlendirmeler**
 - Güvenlik Testleri ve Zafiyet Değerlendirmeleri
 - Güvenlik Denetimleri ve Kontrolleri
8. **Gerçek Dünya Senaryoları ve Case Study'ler**
 - Gerçek Dünya Güvenlik Senaryoları
 - Uygulamalı Case Study Analizleri



Digital Vizyon
Akademi