SECURING WINDOWS SERVER 2016

Eğitim Hakkında

Windows Server 2016 ortamlarında güvenliği sağlama becerilerini kazandırmayı amaçlayan bu eğitim, katılımcılara sistemlerinizi güvenli hale getirmek, tehditleri tespit etmek ve etkili bir şekilde yanıt vermek için gerekli araç ve teknikleri öğretir. Eğitimde **Windows Defender**, **BitLocker**, **AppLocker**, **Dynamic Access Control**, **Just Enough Administration (JEA)** gibi modern güvenlik araçları ve özellikler ele alınır.

Ön Koşullar

Bu eğitime katılmadan önce aşağıdaki bilgi ve becerilere sahip olunması önerilir:

- Temel ağ ve güvenlik bilgisi
- Windows Server yönetimi konusunda deneyim
- Active Directory Domain Services (AD DS) yapılandırma bilgisi
- PowerShell kullanımı hakkında temel bilgi

Eğitim Süresi

- **Eğitmen liderliğinde eğitim:** 5 gün (uygulamalı laboratuvar çalışmalarıyla)
- **Sanal eğitmen liderliğinde eğitim:** 5 gün (web tabanlı dersler ve uygulamalı laboratuvar çalışmalarıyla)

Kimler Katılmalı?

- Sistem yöneticileri
- Güvenlik uzmanları
- Windows Server altyapısını yöneten IT profesyonelleri
- Windows Server güvenliğini optimize etmek isteyen ağ mühendisleri

---

Eğitim İçeriği ve Laboratuvar Detayları

Modül 1: Saldırıları Anlama, İhlalleri Tespit Etme ve Sysinternals Araçları

Konular:

- Saldırı türleri ve vektörlerini anlama
- Güvenlik ihlallerini tespit etme
- Sysinternals araçları ile etkinliklerin incelenmesi

Lab:

1. Saldırı türlerini tanımlama
2. Sysinternals araçlarını keşfetme

Modül 2: Kimlik Bilgileri ve Ayrıcalıklı Erişim Koruması

Konular:

- Kullanıcı hakları ve hesap güvenliği
- Ayrıcalıklı Erişim Çalışma İstasyonları (PAWs)
- Yerel Yönetici Parola Çözümü (LAPS)

Lab:

1. Kullanıcı haklarını yapılandırma
2. LAPS dağıtımı ve test edilmesi

Modül 3: Just Enough Administration (JEA) ile Yöneticileri Sınırlama

Konular:

- JEA'nin temelleri
- JEA yapılandırması ve dağıtımı

Lab:

1. JEA uç noktası oluşturma ve test etme

Modül 4: Ayrıcalıklı Erişim Yönetimi (PAM) ve Yönetim Ormanları

Konular:

- ESAE ormanları
- Microsoft Identity Manager (MIM)
- Zamanında Ayrıcalık Yönetimi (JIT)

Lab:

1. PAM rollerinin yapılandırılması ve yönetimi

Modül 5: Zararlı Yazılım ve Tehditleri Azaltma

Konular:

- Windows Defender ve AppLocker yapılandırması
- Device Guard kullanımı

Lab:

1. Windows Defender ve AppLocker ile uygulama güvenliği

Modül 6: İleri Düzey Denetim ve Günlük Analitiği

Konular:

- Gelişmiş denetim yapılandırması
- PowerShell günlük kaydı

Lab:

1. Dosya sistemi erişim denetimi yapılandırması
2. PowerShell günlük kaydı ve denetimi

Modül 7: İleri Tehdit Analitiği ve Yönetim Araçları

Konular:

- Advanced Threat Analytics (ATA) yapılandırması
- Microsoft Operations Management Suite (OMS) kullanımı

Lab:

1. ATA ve OMS'in uygulanması ve yapılandırılması

Modül 8: Sanallaştırma Altyapısının Güvenliği

Konular:

- Korunan kumaşlar ve Shielded VMs

Lab:

1. Yönetici tarafından güvenilen doğrulama ile Guarded Fabric dağıtımı

Modül 9: Uygulama Geliştirme ve Sunucu İş Yükü Güvenliği

Konular:

- Security Compliance Toolkit (SCT) kullanımı
- Windows ve Hyper-V konteynerlarının yapılandırılması

Lab:

1. SCT ile güvenlik temel çizgilerinin yapılandırılması
2. Windows konteynerlarının dağıtımı

Modül 10: Veriyi Planlama ve Koruma

Konular:

- Şifreleme ve BitLocker uygulamaları
- Azure Information Protection kullanımı

Lab:

1. Şifreleme ve BitLocker kullanarak veri koruma

Modül 11: Dosya Hizmetlerini Optimize Etme ve Güvenli Hale Getirme

Konular:

- File Server Resource Manager (FSRM) kullanımı
- Dynamic Access Control (DAC) uygulamaları

Lab:

1. FSRM kotalarının ve dosya tarama ayarlarının yapılandırılması

Modül 12: Güvenlik Duvarları ve Şifreleme ile Ağ Trafiğini Güvenli Hale Getirme

Konular:

- Windows Güvenlik Duvarı ve IPsec yapılandırmaları

Lab:

1. Giden ve gelen kuralların yapılandırılması
2. Bağlantı güvenliği kuralları oluşturma

Modül 13: Ağ Trafiğini Güvenli Hale Getirme

Konular:

- DNSSEC ve SMB güvenliği

Lab:

1. DNSSEC yapılandırması ve test edilmesi
2. SMB şifrelemesinin doğrulanması

Eğitim Sonunda Kazanacaklarınız

Bu eğitimi tamamlayan katılımcılar:

- Windows Server 2016 güvenlik özelliklerini kullanabilir.
- Zararlı yazılım tehditlerini tespit edip yönetebilir.
- Kimlik bilgileri ve ayrıcalıklı erişim yönetimi uygulamalarını yapılandırabilir.
- Dinamik erişim kontrolü ve şifreleme yöntemlerini uygulayabilir.
- İleri düzey tehdit analitiği araçlarını dağıtıp yönetebilir.