



ACTIVE DIRECTORY ŞİFRELEME VE GÜVENLİK YÖNETİMİ EĞİTİMİ

3 GÜN



Digital Vizyon
Akademi

www.digitalvizyon.net

Eđitim Hakkında

Active Directory Şifreleme ve Güvenlik Yönetimi Eğitimi, kurumsal bilgi varlıklarının korunmasında kritik bir rol oynuyor. Bu kapsamlı eğitim programı, sistem yöneticilerine Active Directory ortamında şifreleme ve güvenlik yönetimi konusunda derin bir uzmanlık kazandırmayı hedefliyor. Günümüzde siber tehditlerin sürekli evrim geçirmesi nedeniyle, güçlü güvenlik politikalarının oluşturulması ve uygulanması her zamankinden daha önemli hale geliyor.

Eđitim süresince, temel şifreleme kavramlarından başlayarak ileri düzey güvenlik yapılandırmalarına kadar geniş bir yelpazede bilgi edineceksiniz. Özellikle, modern şifreleme protokolleri ve güvenlik mekanizmalarının Active Directory entegrasyonu konularında derinlemesine bilgi sahibi olacaksınız. Bunun yanı sıra, güvenlik açıklarının tespiti ve giderilmesi konusunda pratik beceriler kazanacaksınız.

Laboratuvar ortamında gerçekleştireceğimiz uygulamalar, gerçek dünya saldırı senaryolarını temel alıyor. Bu sayede, öğrendiğiniz teorik bilgileri hemen pratiğe dökme fırsatı bulacaksınız. Ayrıca, kurumsal ortamlarda sıkça karşılaşılan güvenlik sorunlarını çözme teknikleri üzerinde yoğunlaşacağız.

Active Directory Şifreleme ve Güvenlik Yönetimi Eğitimi içeriğinde, Kerberos ve NTLM protokollerini derinlemesine ele alacağız. Özellikle, Pass-the-Hash ve Pass-the-Ticket gibi modern saldırı tekniklerine karşı koruma yöntemlerine odaklanacağız. Buna ek olarak, kimlik hırsızlığı ve yetkisiz erişim girişimlerinin tespiti konularında uzmanlaşacaksınız.

Zero Trust güvenlik modeli çerçevesinde Active Directory güvenliğinin nasıl sağlanacağını öğreneceksiniz. Bu kapsamda, en iyi güvenlik uygulamalarını ve modern tehdit koruma yöntemlerini detaylı şekilde inceleyeceğiz. Üstelik, Microsoft'un en güncel güvenlik araçları ve çözümleri hakkında bilgi sahibi olacaksınız.

Eđitmenlerimiz, siber güvenlik ve Active Directory konularında uzmanlaşmış, sertifikalı profesyonellerden oluşuyor. Her biri, yıllara dayanan kurumsal deneyimlerini size aktaracak. Dolayısıyla, teorik bilginin ötesinde, sahada karşılaşılan gerçek saldırı senaryolarına dayalı çözümler öğreneceksiniz.

Neler Öğreneceksiniz

- Active Directory şifreleme protokolleri
- Kerberos ve NTLM güvenliği
- Şifre politikaları yönetimi
- Güvenlik duvarı yapılandırması
- Saldırı tespit ve önleme
- Security baseline oluşturma
- Privileged Access Management
- Multi-Factor Authentication
- Zero Trust implementasyonu
- Güvenlik izleme ve denetim



Kimler Katılmalı

- Sistem güvenlik yöneticileri
- Network güvenlik uzmanları
- Active Directory yöneticileri
- IT altyapı sorumluları
- Güvenlik mimarları
- Sistem denetçileri
- Identity yöneticileri

Ön Koşullar

- Active Directory temel bilgisi
- Windows Server yönetim deneyimi
- Temel network güvenliği bilgisi
- PowerShell scripting deneyimi
- Kriptografi temel anlayışı

Eğitim İçeriği

1. Gün: Temel Güvenlik ve Şifreleme

- Active Directory Güvenlik Temelleri
 - Güvenlik mimarisi
 - Şifreleme protokolleri
 - Kerberos authentication
 - NTLM güvenliği
 - TLS/SSL yapılandırması
- Şifre Politikaları
 - Password policy yönetimi
 - Fine-grained password policies
 - Password complexity
 - Account lockout
 - Password history

2. Gün: Tehdit Koruması

- Saldırı Tespit ve Önleme
 - Common attack vectors
 - Pass-the-Hash koruması
 - Golden Ticket önleme
 - Lateral movement tespiti



- Privilege escalation koruması
- Güvenlik izleme
 - Security log yönetimi
 - Event forwarding
 - Audit politikaları
 - SIEM entegrasyonu
 - Alerting yapılandırması

3. Gün: Modern Güvenlik Yaklaşımları

- Zero Trust ve PAM
 - Zero Trust prensipleri
 - Just-In-Time access
 - Privileged Access Workstations
 - ESAE mimarisi
 - Red Forest yapılandırması
- İleri Düzey Güvenlik
 - MFA implementasyonu
 - Conditional Access
 - Device compliance
 - Security score iyileştirme
 - Best practices