SİSTEM GÜVENLİĞİ VE SİBER SAVUNMA EĞİTİMİ
4 GÜN

Digital Vizyon
Akademi

www.digitalvizyon.net

Eğitim Hakkında

Sistem Güvenliği ve Siber Savunma Eğitimi, dijital dünyayı korur. Bu eğitim, sistem güvenliği temelleri ve siber savunma stratejilerine odaklanır. Katılımcılar, siber tehditleri tanıma, önleme ve müdahale etme yöntemlerini öğrenirler. Aynı zamanda, güvenlik duvarları, antivirüs sistemleri ve şifreleme teknolojileri gibi güvenlik araçlarının kullanımını keşfederler. Bu keşif, bilgi sistemlerinin ve ağların güvende tutulmasını sağlar.

Eğitim, siber tehdit analizi ve risk değerlendirme üzerine yoğunlaşır. Katılımcılar, potansiyel güvenlik zafiyetlerini nasıl belirleyeceklerini ve riskleri nasıl azaltacaklarını öğrenirler. Bu öğrenim, proaktif güvenlik önlemlerinin alınmasını sağlar. Aynı zamanda, sistemlerin ve verilerin korunmasına yardımcı olur.

Olay yanıtı ve kriz yönetimi de eğitimde yer alır. Katılımcılar, siber saldırılar sonrasında olay yanıt süreçlerini ve kriz yönetimi tekniklerini öğrenirler. Bu bilgi, siber saldırıların etkilerini minimize etmeyi ve hızlı bir şekilde iyileşmeyi sağlar.

Eğitim, ayrıca, kullanıcı eğitimi ve farkındalık programlarının önemine de odaklanır. Katılımcılar, kullanıcıları siber güvenlik tehditleri konusunda nasıl eğiteceklerini ve bilinçlendireceklerini öğrenirler. Bu eğitim ve farkındalık, güvenlik ihlallerinin önlenmesinde kritik bir rol oynar.

Sistem Güvenliği ve Siber Savunma Eğitimi, katılımcılara pratik beceriler kazandırır. Bu beceriler, onların bilgi sistemlerini ve ağları etkili bir şekilde korumalarına yardımcı olur. Eğitim, siber güvenlik ve savunma konularında derinlemesine uzmanlık kazandırır. Katılımcılar, eğitimle birlikte, güvenli ve güvenilir bilgi sistemleri oluşturabilirler.

Sonuç olarak, bu eğitim, sistem güvenliği ve siber savunma konusunda kapsamlı bir bilgi sunar. Katılımcılar, tehdit analizi, risk değerlendirme, olay yanıtı ve kullanıcı eğitimi konusunda uzmanlaşır. Eğitim sonunda, katılımcılar, siber güvenlik tehditlerine karşı korunma ve müdahale etme becerilerine sahip olurlar. Bu beceriler, onların profesyonel gelişimlerine büyük katkı sağlar.

Neler Öğreneceksiniz

1. **Siber Tehditlerin Tanınması:** Farklı siber saldırı türlerini ve tehditlerini tanıma.
2. **Güvenlik Mekanizmaları:** Şifreleme, güvenlik duvarları, saldırı tespit sistemleri gibi güvenlik mekanizmalarını anlama.
3. **Ağ Güvenliği:** Ağ güvenliği yöntemleri ve siber saldırılara karşı koruma stratejileri.
4. **Siber Savunma Planlaması:** Siber saldırılara karşı hazırlık ve olay müdahalesi planlaması.
5. **Veri Koruma ve Gizlilik:** Hassas verilerin korunması ve gizliliğin sağlanması.
6. **Etik Hackerlık (Ethical Hacking):** Sistemlerin güvenlik açıklarını tespit etme ve düzeltme.

Ön Koşullar

- Temel bilgisayar ve ağ konularında bilgi.
- Temel bilgisayar güvenliği konularına aşina olma.
- Temel programlama ve sistem yönetimi becerileri.

Kimler Katılmalı

- Bilgi güvenliği uzmanları ve siber güvenlik profesyonelleri.
- Ağ yöneticileri ve sistem mühendisleri.
- Yazılım geliştiricileri ve siber güvenlikle ilgilenen herkes.
- İşletmelerin güvenlik departmanlarında çalışanlar.
- Siber güvenlik kariyeri yapmak isteyen kişiler.

Eğitim İçeriği

1. **Siber Tehditler ve Saldırı Türleri:**
    - Malware, phishing, DDoS gibi temel siber saldırı türleri.
    - Sosyal mühendislik ve kimlik avı saldırıları.
2. **Güvenlik Mekanizmaları:**
    - Şifreleme ve güvenli iletişim.
    - Güvenlik duvarları ve saldırı tespit sistemleri.
3. **Ağ Güvenliği ve Savunma:**
    - Ağ güvenliği stratejileri.
    - Ağ güvenliği cihazları ve yöntemleri.
4. **Siber Savunma ve Olay Müdahalesi:**
    - Siber olayların tespiti ve yanıt verme.
    - Siber savunma planlaması.
5. **Veri Güvenliği ve Gizlilik:**
    - Veri şifreleme ve koruma yöntemleri.
    - Kişisel verilerin korunması.
6. **Etik Hackerlık (Ethical Hacking):**
    - Güvenlik açıklarının tespiti ve düzeltme.
    - Penetrasyon testleri ve zafiyet analizi.