IOT CİHAZ GÜVENLİĞİ VE SALDIRI SENARYOLARI EĞİTİMİ
3 GÜN

Digital Vizyon
Akademi

www.digitalvizyon.net

Eğitim Hakkında

IoT Cihaz Güvenliği ve Saldırı Senaryoları Eğitimi, hayati öneme sahiptir. Bu eğitim, IoT güvenlik zafiyetlerine dikkat çeker. Katılımcılar, IoT cihazlarının güvenlik açıklarını öğrenirler. Aynı zamanda, bu açıkları nasıl tespit edeceklerini ve önleyeceklerini keşfederler. Bu önlemler, IoT ekosistemini güvenli hale getirir.

Eğitim, güvenlik duvarları, şifreleme ve güvenli protokoller üzerine odaklanır. Katılımcılar, IoT cihazlarını korumak için bu teknikleri uygulamayı öğrenirler. Bu uygulama, veri sızıntılarını ve yetkisiz erişimi engeller. Aynı zamanda, cihazlar arası güvenli iletişimi sağlar. Bu sağlama, IoT ağlarının bütünlüğünü korur.

Saldırı senaryoları ve gerçek dünya vakaları da eğitimde yer alır. Katılımcılar, yaygın IoT saldırı türlerini ve bunlara karşı savunma stratejilerini öğrenirler. Bu öğrenim, tehditleri anlama ve bunlara proaktif olarak yanıt verme yeteneğini geliştirir. Aynı zamanda, risk değerlendirme ve yönetim becerilerini artırır. Bu artış, güvenlik önlemlerinin etkinliğini maksimize eder.

Eğitim, güvenlik politikalarının oluşturulması ve uygulanmasına da değinir. Katılımcılar, IoT projeleri için etkili güvenlik politikaları nasıl geliştireceklerini öğrenirler. Bu politikalar, organizasyonların güvenlik standartlarını belirler. Aynı zamanda, uyum ve yasal gerekliliklere uyumu kolaylaştırır. Bu kolaylık, işletmelerin güvenliğini ve itibarını korur.

IoT Cihaz Güvenliği ve Saldırı Senaryoları Eğitimi, katılımcılara pratik beceriler kazandırır. Bu beceriler, onların kendi IoT projelerinde güvenlik önlemlerini etkili bir şekilde uygulamalarına yardımcı olur. Eğitim, IoT güvenliği konusunda derinlemesine uzmanlık kazandırır. Bu sayede katılımcılar, eğitimle birlikte, IoT cihazlarını ve ağlarını güvenli bir şekilde yönetebilirler.

Sonuç olarak, bu eğitim, IoT güvenliği ve saldırı senaryoları konusunda kapsamlı bir bilgi sunar. Katılımcılar, IoT cihazlarını ve ağlarını güvenli bir şekilde koruma konusunda uzmanlaşır. Eğitim sonunda, katılımcılar, IoT güvenlik tehditlerine karşı korunaklı çözümler geliştirebilirler. Bu beceriler, onların profesyonel gelişimlerine büyük katkı sağlar.

Neler Öğreneceksiniz

1. IoT Cihazlarının Güvenlik Zafiyetleri
2. IoT Güvenlik Protokolleri ve Standartları
3. Saldırı Tespiti ve Yanıt Verme Mekanizmaları
4. IoT Güvenlik Mimarileri ve Çözümleri
5. Gerçek Dünya IoT Saldırı Senaryoları
6. Güvenlik Testleri ve Zafiyet Değerlendirmeleri
7. IoT Güvenlik Yönetimi ve Politikaları
8. Etik Hacking ve Savunma Stratejileri

Ön Koşullar

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

Kimler Katılmalı

- IoT cihaz güvenliği konusunda bilgi edinmek isteyen siber güvenlik uzmanları
- Güvenli IoT çözümleri geliştirmek isteyen IoT geliştiriciler ve mühendisler
- IoT ekosisteminin güvenliğini artırmak isteyen sistem yöneticileri ve teknisyenler
- IoT güvenliği ve siber saldırılar konusunda ileri düzey bilgi kazanmak isteyen her seviyeden bireyler

Eğitim İçeriği

1. Giriş ve Temel Kavramlar

- IoT nedir?
- IoT'nin temel bileşenleri.
- IoT cihazlarının yaygın kullanım alanları.
- IoT cihazlarının karşılaştığı güvenlik zorlukları.

2. IoT Cihazlarına Yönelik Güvenlik Tehditleri

- Fiziksel erişim tehditleri.
- Ağ üzerinden yapılan saldırılar.
- Yazılım ve donanım güvenlik açıkları.
- Uçtan uca veri iletimindeki güvenlik zaafları.

3. IoT Güvenlik Mekanizmaları ve Protokolleri

- Şifreleme ve kimlik doğrulama yöntemleri.
- Güvenli veri iletimi için protokoller (MQTT, CoAP, HTTPS).
- Yazılım güncellemeleri ve yama yönetimi.

4. IoT Saldırı Senaryoları ve Gerçek Dünya Örnekleri

- DDoS (Dağıtık Hizmet Reddi) saldırıları.
- Man-in-the-Middle (Ortadaki Adam) saldırıları.
- Kimlik avı ve sosyal mühendislik saldırıları.
- Firmware/hardware bazlı saldırılar.

5. Güvenlik İncelemesi ve Zafiyet Analizi

- IoT cihazlarının güvenlik incelemesi.
- Zafiyet tespiti ve risk değerlendirme yöntemleri.
- Güvenlik duvarları ve sızma testi uygulamaları.

6. Savunma Stratejileri ve En İyi Uygulamalar

- Güçlü kimlik doğrulama sistemleri.
- Güvenlik katmanlarının oluşturulması.
- Sürekli izleme ve olaya müdahale planları.
- Kullanıcı eğitimi ve farkındalık programları.

7. Uygulamalı Atölye Çalışmaları

- Gerçek zamanlı IoT güvenlik senaryoları üzerinde çalışma.
- Saldırı tespit ve müdahale simülasyonları.
- Güvenlik politikaları ve prosedürlerinin oluşturulması.

8. Sonuç ve Değerlendirme

- Öğrenilenlerin değerlendirilmesi.
- Katılımcıların geri bildirimleri.
- Sürekli eğitim ve kaynakların paylaşımı.