Eğitim İçeriği

Cybersecurity Fundamentals Training

Tüm Siber Güvenlik EğitimleriTemel Güvenlik EğitimleriVeri ve Erişim GüvenliğiTehdit Yönetim ve İstihbarat 9 modül

Siber Güvenlik Temelleri Nedir?

Siber Güvenlik Temelleri, dijital sistemleri koruma, veri güvenliğini sağlama ve siber tehditlere karşı önlem alma süreçlerini kapsayan bir alandır. Ağ güvenliği, veri şifreleme, erişim kontrolü ve saldırı önleme yöntemlerini içerir.

Siber Güvenlik Temelleri Eğitiminin Amacı Nedir?

Eğitim, temel siber güvenlik kavramlarını öğretmeyi ve katılımcılara işletmelerin dijital varlıklarını koruma becerisi kazandırmayı hedefler. Katılımcılar, tehdit analizi yaparak güvenlik açıklarını belirleme ve önlem alma konularında uzmanlaşır.

Siber Güvenlik Temelleri Eğitimini Neden Almalısınız?

Bu eğitim, dijital ortamda güvenliği artırmak, veri ihlallerini önlemek ve işletmelerin siber saldırılara karşı dayanıklılığını artırmak isteyen profesyoneller için tasarlanmıştır. Siber güvenlik bilgisi, işletmelere stratejik koruma ve operasyonel verimlilik kazandırır.

Kimler Siber Güvenlik Temelleri Eğitimini Alabilir?

- IT uzmanları ve sistem yöneticileri
- Veri güvenliği alanında kariyer yapmak isteyen profesyoneller
- Şirketlerin dijital güvenlik süreçlerini yöneten bireyler
- Kendi sistemlerinin güvenliğini sağlamak isteyen kişiler

Eğitim, dijital dünyada güvenlik süreçlerini etkin bir şekilde yönetmek isteyen herkes için uygundur.

Siber Güvenlik Temelleri Eğitiminin Kariyere Yararları Nelerdir?

- Temel siber güvenlik alanında uzmanlık kazandırır.
- Veri güvenliği ve sistem koruma alanlarında yetkinlik sağlar.
- Şirketlerin siber tehditlere karşı dayanıklılığını artırır.
- İş dünyasında artan siber güvenlik talebine yanıt verme fırsatı sunar.
- Daha geniş iş olanakları ve profesyonel statü elde etme imkânı sağlar.

Eğitim Sonunda Hangi Beceriler Kazanılır?

- Siber tehditleri tespit etme ve analiz etme
- Güvenlik duvarları ve saldırı önleme sistemlerini yönetme
- Veri şifreleme ve güvenlik politikaları oluşturma
- Ağ güvenliğini sağlama ve güvenlik açıklarını kapatma

Eğitim Programı

1. Siber Güvenliğe Giriş

1. Siber Güvenliğe Giriş

- Siber güvenliğin tanımı ve önemi
- Bilgi güvenliği temel ilkeleri: Gizlilik, bütünlük, erişilebilirlik
- Siber güvenlik terminolojisi

2. Siber Tehditler ve Saldırı Türleri

2. Siber Tehditler ve Saldırı Türleri

- Kötü amaçlı yazılımlar: Virüsler, solucanlar, truva atları
- Sosyal mühendislik saldırıları: Phishing (oltalama), pretexting
- Dağıtılmış Hizmet Reddi (DDoS) saldırıları
- Gelişmiş Kalıcı Tehditler (APT)

3. Ağ Güvenliği

3. Ağ Güvenliği

- Ağ protokolleri ve güvenliği
- Güvenlik duvarları ve Intrusion Detection Systems (IDS)
- Sanal Özel Ağlar (VPN) ve güvenliği
- Kablosuz ağ güvenliği

4. Kriptografi ve Veri Şifreleme

4. Kriptografi ve Veri Şifreleme

- Simetrik ve asimetrik şifreleme yöntemleri
- Dijital imzalar ve sertifikalar
- Kriptografik protokoller ve uygulamaları

5. Siber Güvenlik Politikaları ve Yönetişim

5. Siber Güvenlik Politikaları ve Yönetişim

- Güvenlik politikalarının oluşturulması ve uygulanması
- Risk yönetimi ve uyumluluk süreçleri
- İş sürekliliği ve felaket kurtarma planları

6. Siber Olay Yönetimi ve Adli Bilişim

6. Siber Olay Yönetimi ve Adli Bilişim

- Siber olayların tespiti ve müdahale yöntemleri
- Adli bilişim süreçleri ve delil toplama
- Olay sonrası analiz ve raporlama

7. Güvenlik Açığı Yönetimi ve Sızma Testleri

7. Güvenlik Açığı Yönetimi ve Sızma Testleri

- Güvenlik açıklarının tespiti ve değerlendirilmesi
- Sızma testleri ve penetrasyon yöntemleri
- Zafiyet tarama araçlarının kullanımı

8. Bulut ve Uygulama Güvenliği

8. Bulut ve Uygulama Güvenliği

- Bulut bilişim güvenliği prensipleri
- Web uygulama güvenliği ve yaygın zafiyetler
- Güvenli yazılım geliştirme yaşam döngüsü

9. Siber Güvenlikte Yasal ve Etik Konular

9. Siber Güvenlikte Yasal ve Etik Konular

- Siber güvenlik ile ilgili yasal düzenlemeler
- Etik hacking ve beyaz şapkalı hacker kavramı
- Kişisel verilerin korunması ve mahremiyet

Bu eğitimi kurumunuza özel planlayalım. İçerik, süre ve uygulama senaryoları ekiplerinizin rolüne ve seviyesine göre uyarlanabilir. www.impress.com.tr/iletisim