Cybersecurity Foundations Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Overview

Cybersecurity Foundations eğitimi, siber güvenlik alanındaki temel tehditleri, savunma yaklaşımlarını ve kurumsal sorumlulukları kapsamlı biçimde anlamak isteyen katılımcılar için tasarlanmıştır.

Program, güvenli sistemlerin nasıl tasarlanması gerektiğini yalnızca tek bir teknik alan üzerinden değil, siber güvenlik ekosisteminde yer alan farklı rollerin ve kontrol katmanlarının birlikte nasıl çalıştığını göstererek ele alır.

Eğitim boyunca katılımcılar; güncel tehdit eğilimleri, network güvenliği, sistem hardening, malware, social engineering, software vulnerabilities, identity management, data protection, PKI, logging, monitoring, physical security, incident response ve yasal gereksinimler gibi birçok temel konuyu inceler.

Teorik anlatım, laboratuvarlar ve breakout discussion çalışmalarıyla desteklenir. Katılımcılar, güncel saldırı örneklerini ve exploit yöntemlerini değerlendirirken aynı zamanda bu tehditlere karşı uygulanabilecek mitigating controls üzerinde çalışır.

Kontrollü bir laboratuvar ortamında, botnet, worm ve Trojan gibi malware türleri de incelenir. Bu yapı, katılımcıların tehditlerin nasıl davrandığını ve güvenlik kontrollerinin bu tehditleri nasıl sınırladığını daha iyi anlamasını sağlar.

Prerequisites

Katılımcıların aşağıdaki alanlarda temel bilgi sahibi olması önerilir:

- TCP/IP networking
- Network fundamentals
- IP addressing
- Temel network communication
- Ağ cihazları ve servisleri hakkında genel bilgi

TCP/IP Networking veya eşdeğer düzeyde network bilgisi eğitimden daha fazla fayda sağlanmasına yardımcı olur.

Cybersecurity Foundations Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com

Who Should Attend

Bu eğitim özellikle aşağıdaki profiller için uygundur:

- Siber güvenlik alanında uzmanlaşmak isteyen network profesyonelleri
- Güvenlik alanında kariyer hedefleyen teknik çalışanlar
- Güvenlik ekipleriyle daha etkili iletişim kurmak isteyen yöneticiler
- Kurumsal seviyede güvenlik yaklaşımı geliştirmek isteyen executives ve managers
- Cybersecurity fundamentals bilgisini geliştirmek isteyen profesyoneller
- Threats, mitigating controls ve organizational responsibilities konularını daha iyi anlamak isteyen katılımcılar

What You Will Learn

Eğitimin sonunda katılımcılar:

- Güvenlik farkındalığını artırabilir
- Network mapping ve footprinting araçlarından gelen çıktıları yorumlayabilir
- Sistemlerin attack surface alanını azaltabilir
- Networking kavramlarını güvenlik kontrolleri açısından değerlendirebilir
- Data protection prensiplerini açıklayabilir
- PKI ve certificates yapılarını anlayabilir
- Network cihazları arasında güven ilişkilerinin nasıl kurulduğunu açıklayabilir
- Login security ve identity management çözümleri uygulayabilir
- Network cihazlarının attack surface alanını azaltabilir
- Güncel malware tehditlerini ve anti-malware çözümlerini değerlendirebilir
- Social engineering saldırılarını ve kullanılan yöntemleri tanımlayabilir
- Software vulnerabilities ve exploit risklerini analiz edebilir
- Monitoring ve logging gereksinimlerini açıklayabilir
- Monitoring faaliyetlerinin privacy üzerindeki etkilerini değerlendirebilir
- Physical security kontrollerini tanımlayabilir
- Physical ve IT security arasındaki ilişkiyi açıklayabilir
- Incident response süreçlerini tanımlayabilir
- Cybersecurity ile ilgili temel yasal ve düzenleyici konuları değerlendirebilir
- Investigative techniques hakkında temel bilgi geliştirebilir
- Güncel cybersecurity trendlerini araştırabilir

Outline

Modül 1: Cybersecurity Awareness

Bu bölüm, siber güvenliğin temel prensiplerini ve güvenlik yaklaşımının temelini oluşturan kavramları ele alır.

Konular:

- Security nedir?
- Confidentiality

- Integrity
- Availability
- Security baselining
- Human-related security concerns
- Threat types
- Security controls
- Hacking kavramı
- Risk management
- Data in motion
- Data at rest
- Module review

Modül 2: Network Discovery

Bu bölüm saldırganların ve güvenlik uzmanlarının network üzerinde bilgi toplamak için kullandığı temel keşif yöntemlerini inceler.

Konular:

- Networking review
- Discovery
- Footprinting
- Scanning
- Common Vulnerabilities and Exposures
- Security policies
- Vulnerabilities
- Module review

Katılımcılar network görünürlüğünün nasıl oluştuğunu ve bu görünürlüğün saldırı yüzeyine nasıl dönüştüğünü değerlendirir.

Modül 3: Systems Hardening

Bu bölüm sistemlerin saldırılara karşı daha dayanıklı hale getirilmesine odaklanır.

Konular:

- Hardening nedir?
- Hangi sistemler harden edilebilir?
- Security baselines
- Hardening methods
- Role-based hardening
- Mobile devices
- Network-based hardening
- Analysis tools
- Authentication
- Authorization
- Accounting
- Physical security
- Module review

Modül 4: Security Architecture

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

Bu bölüm güvenli network ve sistem mimarilerinin temel yapı taşlarını ele alır.

Konular:

- Security architecture
- Network devices
- Network zones
- Network segmentation
- Network Address Translation
- Network Access Control
- Module review

Katılımcılar farklı güvenlik katmanlarının mimari tasarım içerisinde nasıl birlikte çalıştığını inceler.

Modül 5: Data Security

Bu bölüm verilerin korunmasına yönelik temel teknikleri kapsar.

Konular:

- Cryptography
- Permission principles
- Access control
- Steganography
- Module review

Modül 6: Public Key Infrastructure

Bu bölüm dijital güven ilişkilerinin oluşturulmasında PKI yapısının rolünü ele alır.

Konular:

- Public Key Infrastructure
- Certification Authorities
- Establishing trust
- Certificates
- CA management
- Module review

Modül 7: Identity Management

Bu bölüm kullanıcı ve servis kimliklerinin güvenli şekilde yönetilmesine odaklanır.

Konular:

- Identity management nedir?
- Personally Identifiable Information
- Authentication factors
- Directory services
- Kerberos
- Windows NT LAN Manager
- Password policies
- Password cracking

- Password assessment tools
- Password managers
- Group accounts
- Service accounts
- Federated identities
- Identity as a Service
- Module review

Modül 8: Network Hardening

Bu bölüm network cihazlarının ve yönetim erişimlerinin güvenli hâle getirilmesine odaklanır.

Konular:

- Remote admin access'i sınırlandırma
- AAA for administrative access
- Simple Network Management Protocol
- Network segmentation
- Physical access restriction
- Secure access
- Network devices
- Fundamental device protection
- Traffic filtering best practices
- Module review

Modül 9: Malware

Bu bölüm yaygın malware türlerini ve bunlara karşı kullanılan savunma yöntemlerini ele alır.

Konular:

- Malware nedir?
- Infection methods
- Malware types
- Botnets
- Worms
- Trojans
- Backdoors
- Countermeasures
- Protection tools
- Module review

Kontrollü laboratuvar ortamında malware davranışları incelenir.

Modül 10: Social Engineering

Bu bölüm insan faktörünü hedefleyen saldırıları ele alır.

Konular:

- Social engineering nedir?
- Target profiles
- Social engineering attacks

- Statistical data
- Information harvesting
- Social engineering prevention
- Cyber awareness policies
- Procedures
- Social media risks
- Module review

Modül 11: Software Security

Bu bölüm yazılım geliştirme süreçlerindeki güvenlik risklerine odaklanır.

Konular:

- Software engineering
- Security guidelines
- Software vulnerabilities
- Exploitation riskleri
- Security solutions
- Module review

Modül 12: Environment Monitoring

Bu bölüm güvenlik açısından monitoring ve logging süreçlerini ele alır.

Konular:

- Monitoring
- Monitoring vs. logging
- Monitoring benefits
- Logging benefits
- Logging
- Metrics
- Privacy considerations
- Module review

Modül 13: Physical Security

Bu bölüm fiziksel güvenlik kontrollerinin IT security üzerindeki etkisini inceler.

Konular:

- Physical security nedir?
- Defense in depth
- Physical security controls
- Device security
- Human security
- Security policies
- Equipment tracking
- Module review

Modül 14: Incident Response

BİLGİNÇ IT Academy

info@bilginc.com

bilginc.com

Bu bölüm güvenlik olaylarına hazırlık ve müdahale süreçlerini kapsar.

Konular:

- Disaster types
- Incident investigation
- Investigation tips
- Business Continuity Planning
- Disaster Recovery Plan
- Forensic Incident Response
- Module review

Katılımcılar bir güvenlik olayının belirlenmesi, araştırılması, sınırlandırılması ve sonrasında yapılması gerekenleri değerlendirir.

Modül 15: Legal Considerations

Bu bölüm cybersecurity çalışmalarının yasal ve düzenleyici boyutunu ele alır.

Konular:

- Regulatory compliance
- Cybercrime
- Legal responsibilities
- Investigative considerations
- Module review

Modül 16: Trends in Cybersecurity

Bu bölüm değişen tehdit ortamını ve gelecekteki güvenlik gereksinimlerini inceler.

Konular:

- Cybersecurity design constraints
- Cyber driving forces
- Connectivity level
- Dependency on connectivity
- Identity management trends
- Cybersecurity standards
- Cybersecurity training
- Emerging security considerations

Modül 17: Course Look Around

Eğitimin son bölümü, katılımcıların öğrendiklerini değerlendirmesine ve gelişim planı oluşturmasına odaklanır.

Konular:

- Looking back
- Looking forward
- Planning your cybersecurity journey
- Sonraki gelişim alanlarının belirlenmesi

Cybersecurity Foundations Eğitimi

Süre: **5 Gün**

BİLGİNÇ IT Academy
info@bilginc.com
bilginc.com