

Bordo Takım Siber Güvenlik Eğitimi

Süre: 5 Gün

Bordo Takım Siber Güvenlik Eğitimi Hakkında

Bordo Takım Siber Güvenlik Eğitimi, günlük siber güvenlik operasyonlarında görev alan profesyoneller için saldırı ve savunma konularını birlikte ele alan 5 günlük sanal sınıf / online programdır. Eğitim, saldırı simülasyonu ile saldırı tespiti ve engelleme becerilerini günlük operasyonlarla ilişkilendirmeye odaklanır.

Sparta tarafından geliştirilen program, geleneksel mavi takım / kırmızı takım yaklaşımını birlikte değerlendirir. Yalnızca sızma testi çalışmalarına veya teorik bilgi güvenliği yönetimine odaklanmak yerine, katılımcıların günlük işlerinde kullanabilecekleri becerileri geliştirmeyi amaçlar. Siber güvenlik teorisi, etik hacking ve penetrasyon testleri; paket analizi, log analizi, uyumluluk ve sistem analizi konularıyla birlikte işlenir.

Müfredatta keşif ve tarama, zafiyet tespiti, DoS/DDoS ve web uygulamalarına yönelik saldırılar, siber olaylara müdahale ve adli bilişim yer alır. Wireshark ile trafik inceleme, loglardan saldırı tespiti, Windows ve Linux logları ile komut satırı araçları operasyonel analiz kapsamını oluşturur. Katılım için bilgi güvenliğinde en az iki yıl deneyim ve ileri düzey TCP/IP bilgisi gerekir.

Öğrenme Başlıkları

- Siber Güvenlik Teorisi
- Etik Hacking
- Penetrasyon Testleri
- Paket Analizi
- Log Analizi
- Uyumluluk
- Sistem Analizi

Eğitim İçeriği

Siber Güvenlik Teorisi

- Siber saldırıların tarihsel gelişimi
- Güncel siber tehditler
- Bir saldırının anatomisi

- Bilgi güvenliği teorisi

Etik Hacking

- Siber saldırı türleri
- Siber saldırı döngüsü
- Keşif ve tarama
- Zafiyet tespiti

Penetrasyon Testleri

- Tarayıcıları hedef alan saldırılar
- Bilinen zafiyetleri istismar etmek
- DoS/DDoS saldırıları
- Web uygulamalara yönelik saldırılar
- SOME (Siber Olaylara Müdahale Ekibi)
- Siber olay tespiti
- Siber olaylara müdahale
- Adli bilişim ve Network forensics

Paket Analizi

- Ağ üzerindeki trafiğin yakalanması
- Trafik analizi temelleri
- Wireshark kullanımı
- Ağ sorunlarının tespiti

Log Analizi

- Log kaynaklarının belirlenmesi
- Log toplama ve izleme yöntemleri
- Log analizi teknikleri
- Loglardan saldırı tespiti

Uyumluluk

- ISO 27001
- PCI-DSS
- NIST ve SANS Critical Controls

Sistem Analizi

- Windowslarda log inceleme
- Linux sistemlerde log inceleme

- Temel saldırıların oluşturduğu loglar ve komut satırı araçları

Ön Koşullar

Bilgi güvenliği alanında en az iki yıl deneyim

TCP/IP konusunda ileri düzeyde bilgi sahibi olma