Performing CyberOps Using Cisco Security Technologies (CBRCOR)

Eğitim Hakkında

Performing CyberOps Using Cisco Security Technologies (CBRCOR) eğitimi, siber güvenlik operasyonlarının temelleri, yöntemleri ve otomasyon teknikleri hakkında bilgi sağlar. Bu kurs, bir **Güvenlik Operasyonları Merkezi (SOC)** ekibinde **Bilgi Güvenliği Analisti** rolüne hazırlanmanıza yardımcı olur. Eğitim süresince, olay müdahale (IR) süreçlerinde kullanılabilecek playbook'ları oluşturma, bulut platformları üzerinden güvenlik otomasyonu sağlama ve **SecDevOps** metodolojisini öğrenirsiniz. Ayrıca, siber saldırıları tespit etme, tehditleri analiz etme ve siber güvenliği iyileştirmek için uygun önerilerde bulunma tekniklerini öğreneceksiniz.

Ön Koşullar

Zorunlu ön koşullar bulunmamakla birlikte, aşağıdaki bilgi ve becerilere sahip olmanız önerilir:

- **UNIX/Linux** shell'lerine (bash, csh) ve shell komutlarına aşinalık
- **Splunk** arama ve gezinme işlevlerine aşinalık
- Python, JavaScript, PHP veya benzeri bir dil ile temel düzeyde betik yazımı bilgisi

Cisco'nun aşağıdaki kursları bu eğitime hazırlanmanıza yardımcı olabilir:

- **Understanding Cisco Cybersecurity Operations Fundamentals (CBROPS)**
- **Implementing and Administering Cisco Solutions (CCNA)**

Üçüncü parti kaynaklar:

- **Splunk Fundamentals 1**
- **Blue Team Handbook: Incident Response Edition** - Don Murdoch
- **Threat Modeling: Designing for Security** - Adam Shostack
- **Red Team Field Manual** - Ben Clark
- **Blue Team Field Manual** - Alan J. White
- **Purple Team Field Manual** - Tim Bryant
- **Applied Network Security and Monitoring** - Chris Sanders, Jason Smith

---

Eğitim Süresi

- **Eğitmen eşliğinde sınıf eğitimi:** 5 gün (pratik laboratuvar çalışmalarıyla)

- **Sanal eğitmen eşliğinde eğitim:** 5 gün (çevrim içi sınıflar ve pratik laboratuvar çalışmalarıyla)

Kimler Katılmalı?

Bu eğitim özellikle aşağıdaki pozisyonlarda çalışan kişiler için uygundur:

- **Siber güvenlik mühendisleri**
- **Siber güvenlik araştırmacıları**
- **Olay yöneticileri**
- **Olay müdahale ekipleri**
- **Ağ mühendisleri**
- SOC analistleri (en az 1 yıl deneyime sahip giriş seviyesi profesyoneller)

Eğitim İçeriği

1. Risk Yönetimi ve SOC Operasyonlarını Anlama
2. Analitik Süreçler ve Playbook'lar Hakkında Bilgi Edinme
3. Paket Yakalamaları, Günlükler ve Trafik Analizi İnceleme
4. Uç Nokta ve Cihaz Günlüklerini İnceleme
5. Bulut Hizmet Modellerindeki Güvenlik Sorumluluklarını Anlama
6. Kurumsal Çevre Varlıklarını Anlama
7. Tehdit Ayarlarını Uygulama
8. Tehdit Araştırma ve Tehdit İstihbaratı Uygulamaları
9. API'leri Anlama
10. SOC Geliştirme ve Dağıtım Modellerini Anlama
11. SOC'de Güvenlik Analitiği ve Raporlama Yapma
12. Kötü Amaçlı Yazılım Adli Analiz Temelleri
13. Tehdit Avcılığı Temelleri
14. Olay Araştırması ve Müdahalesi Gerçekleştirme

Eğitim Sonunda Kazanacaklarınız

Eğitim sonunda:

- SOC ortamlarında güvenlik analitiği ve olay müdahale süreçlerini uygulayabileceksiniz.
- Siber saldırı ve tehditleri tespit ederek analiz yapabilecek, raporlama ve iyileştirme önerileri sunabileceksiniz.
- SecDevOps metodolojisini kullanarak güvenlik otomasyon çözümlerini etkin bir şekilde uygulayabileceksiniz.