Implementing Cisco Cybersecurity Operations (SECOPS)

Eğitim Hakkında

"Implementing Cisco Cybersecurity Operations (SECOPS)" v1.0 kursu, size bir Güvenlik Operasyon Merkezi'nde (SOC) kullanılan güvenlik olayı analizi teknikleri hakkında temel düzeyde bilgi sağlar. Tehditleri ve zararlı faaliyetleri tanımlamayı, olayları ilişkilendirmeyi, güvenlik incelemeleri gerçekleştirmeyi, olay senaryolarını kullanmayı ve SOC operasyonları ile prosedürlerini öğrenmeyi öğreneceksiniz. Bu, sizi Cisco® CCNA® Cyber Ops sertifikası için hazırlayan iki kursun ikincisidir. Bu sertifika, bir SOC ekibinin orta seviye bir üyesi olarak siber güvenlik olaylarını ele almanıza yardımcı olacak bilgi ve uygulamalı becerilerinizi doğrular.

Günümüz siber güvenlik uzmanlarının çok çeşitli güvenlik olaylarını tespit etmesi, araştırması ve yanıtlaması gerekir. Bu kurs, kuruluşunuzun SOC'sinde güvenlik olaylarını tespit edip yanıtlamada rol oynamak için gereken becerileri kazanmanıza yardımcı olacaktır.

Ön Koşullar

- Temel ağ bilgisi
- Temel siber güvenlik kavramlarına aşinalık
- "Introduction to Cybersecurity" veya benzeri bir giriş seviyesi siber güvenlik kursunu tamamlamış olmak

Eğitim Süresi

- **Eğitmen eşliğinde eğitim:** 5 gün, uygulamalı laboratuvar çalışmalarıyla birlikte
- **Sanal eğitmen eşliğinde eğitim:** 5 gün, web tabanlı dersler ve uygulamalı laboratuvar çalışmalarıyla birlikte

Kimler Katılmalı?

- BT profesyonelleri
- Aşağıdaki gibi orta seviye siber güvenlik rollerine girmek isteyen tüm öğrenciler:
    - SOC siber güvenlik analistleri
    - Bilgisayar veya ağ savunma analistleri
    - Bilgisayar ağ savunma altyapı destek personeli
    - Gelecekteki olay müdahale ekipleri ve SOC personeli
    - Cisco entegratörleri veya iş ortakları

Eğitim İçeriği

- **SOC Genel Bakışı**
    - Güvenlik Operasyon Merkezini Tanımlama

    - NSM Araçları ve Verilerini Anlama
    - Tehdit Odaklı bir SOC'da Olay Analizini Anlama
    - Siber Tehditleri Avlamak İçin Kaynakları Belirleme
- **Güvenlik Olayı Araştırmaları**
    - Olay İlişkilendirme ve Normalizasyonu Anlama
    - Ortak Saldırı Vektörlerini Belirleme
    - Zararlı Faaliyetleri Belirleme
    - Şüpheli Davranış Kalıplarını Belirleme
    - Güvenlik Olayı Araştırmaları Yürütme
- **SOC Operasyonları**
    - SOC Senaryosunu Açıklama
    - SOC Metriklerini Anlama
    - SOC WMS ve Otomasyonu Anlama
    - Olay Müdahale Planını Açıklama
    - Ek A - Bilgisayar Güvenlik Olayı Müdahale Ekibini Açıklama
    - Ek B - VERIS kullanımını Anlama

Eğitim Sonunda Kazanacaklarınız

- Üç yaygın SOC türünü, SOC analistleri tarafından kullanılan araçları, SOC içindeki iş rollerini ve tehdit odaklı bir SOC içindeki olay analizini açıklayın.
- Olay ilişkilendirme ve normalizasyon ile ortak saldırı vektörleri dahil olmak üzere güvenlik olayı araştırmalarını açıklayın ve zararlı ve şüpheli faaliyetleri belirleyebilin.
- Araştırmalara yardımcı olmak için bir SOC senaryosunun kullanımını, SOC etkinliğini ölçmek için metriklerin kullanımını, SOC iş akışı yönetim sistemi ve otomasyonun SOC verimliliğini artırmak için kullanımını ve bir olay müdahale planı kavramlarını açıklayın.