SC-200T00: Microsoft Security Operations Analyst

Microsoft Sentinel, Microsoft Defender for Cloud ve Microsoft 365 Defender kullanarak tehditlerin nasıl araştırıldığını, bu tehditlere nasıl yanıt verildiğini ve çözüldüğünü öğrenin. Bu eğitimde bu teknolojileri kullanarak siber tehditlerin nasıl azaltıldığını öğreneceksiniz. Özellikle de tespit, analiz ve raporlama için Microsoft Sentinel'i yapılandırma ve kullanmanın yanı sıra Kusto Sorgu Dili'ni (KQL) kullanacaksınız. Eğitim, bir Güvenlik Operasyonları rolünde çalışan kişiler için tasarlanmış olup öğrencilerin SC-200: Microsoft Güvenlik Operasyonları Analisti sınavına hazırlanmalarına yardımcı olmaktadır.

Hedefler

- Microsoft Defender for Endpoint'in ortamınızdaki riskleri nasıl giderebileceğini açıklama
- Microsoft Defender for Endpoint ortamını yönetme
- Windows cihazlarında Saldırı Yüzeyini Azaltma kurallarını yapılandırma
- Microsoft Defender for Endpoint kullanarak cihazda ilgili işlemleri gerçekleştirme
- Microsoft Defender for Endpoint'de etki alanlarını ve IP adreslerini araştırma
- Microsoft Defender for Endpoint'de kullanıcı hesaplarını araştırma
- Microsoft 365 Defender'de alarm ayarlarını yapılandırma
- Tehdit ortamının nasıl geliştiğini açıklama
- Microsoft 365 Defender'da gelişmiş avlamayı yürütme
- Microsoft 365 Defender'da vakaları yönetme
- Microsoft Defender for Identity'nin ortamınızdaki riskleri nasıl giderebileceğini açıklama
- Microsoft Defender for Cloud Apps'daki DLP alarmlarını araştırma
- Risk yönetimi vakasında gerçekleştirebileceğiniz eylem türlerini açıklama

- Microsoft Defender for Cloud Apps'daki otomatik karşılamayı yapılandırma
- Microsoft Defender for Cloud Apps'daki alarmları giderme
- KQL ifadelerini oluşturma
- KQL'yi kullanarak aramaları olay zamanı, önem derecesi, etki alanı ve diğer ilgili verilere göre filtreleme
- KQL kullanarak yapılandırılmamış dizi alanlarından verileri çıkartma
- Microsoft Sentinel çalışma alanını yönetme
- Microsoft Sentinel'deki izleme listesine erişmek için KQL'yi kullanma
- Microsoft Sentinel'de tehdit göstergelerini yönetme
- Microsoft Sentinel'de Ortak Olay Formatını ve Syslog konektör farklılıklarını açıklama
- Azure Windows sanal makinelerini Microsoft Sentinel'e bağlama
- Sysmon olaylarını toplamak için Log Analytics ajanını yapılandırma
- Analitik kural sihirbazını kullanarak yeni analitik kuralları ve sorguları oluşturma
- Vaka müdahalesini otomatik hale getirmek için oyun kitabı oluşturma
- Tehditleri avlamak için sorguları kullanma
- Canlı yayın ile tehditleri zaman içinde gözlemleme

Ön Koşullar

- Microsoft 365'i temel düzeyde anlama
- Microsoft'un güvenlik, uyum ve kimlik ürünlerini temel düzeyde anlama
- Windows 10'u anlama
- Özellikle Azure SQL Veritabanı ve Azure Depolama olmak üzere Azure servislerine aşinalık

- Azure sanal makineleri ve sanal ağ kurulumuna aşinalık
- Komut yazma kavramlarını temel düzeyde anlama.

Hedef Kitle

Microsoft Güvenlik Operasyonları Analisti, kuruluş için bilgi teknolojisi sistemlerini güvenli hale getirmek amacıyla kuruluş paydaşları ile işbirliği yapmaktadır. Amacı, ortamdaki aktif saldırıları hızlıca bertaraf ederek, tehditlerden korunma teamüllerine ilişkin tavsiyelerde bulunarak ve kuruluş politikalarının ihlallerini ilgili paydaşlara ileterek organizasyonel riski azaltmaktır. Sorumlulukları arasında ortamdaki çeşitli güvenlik çözümlerini kullanarak tehdit yönetimi, takip ve müdahale yer almaktadır. Bu rol esasen Microsoft Sentinel, Microsoft Defender for Cloud, Microsoft 365 Defender ve üçüncü şahıs güvenlik ürünlerini kullanarak tehditleri araştırmakta ve müdahale etmektedir. Güvenlik Operasyonları Analisti bu araçların operasyonel çıktısını kullandığından bu teknolojilerin yapılandırılmasında ve kurulumunda da kritik bir paydaş konumundadırlar.

Topics

- Mitigate threats using Microsoft Defender for Endpoint
- Mitigate threats using Microsoft 365 Defender
- Mitigate threats using Azure Defender
- Create queries for Azure Sentinel using Kusto Query Language (KQL)
- Configure your Azure Sentinel environment
- Connect logs to Azure Sentinel
- Create detections and perform investigations using Azure Sentinel
- Perform threat hunting in Azure Sentinel