EMA SECURITY

# SOC ve MDR Analist Eğitimi

## AI-Powered Defense Service


### İletişim

www.emasecurity.com

info@emasecurity.com

Bostancı Mah, Ali Nihat Tarhan Cd, Kahraman Sk,
No:2/D:11, Hoffman Plaza, Kadıkoy/İstanbul

+90 (850) 244 49 26

# SOC ve MDR Analist Eğitimi



**Eğitim Açıklaması**

SOC ve MDR Analist Eğitimi, Güvenlik Operasyon Merkezleri (SOC) ve Yönetilen Tespit ve Yanıt (MDR) hizmetleri veren analistlerin, saldırıları tespit etme ve müdahale etme becerilerini geliştirmeyi hedefler. Katılımcılar, ağ trafiği analizi, tehdit avcılığı ve otomatik güvenlik sistemlerini kullanma konusunda derinlemesine bilgi edinir. Ayrıca, SOC ve MDR süreçlerini etkin bir şekilde yönetmek için gerekli bilgi ve beceriler kazandırılır.

**Eğitim Yeri**

- Online
- Fiziksel

**Eğitim Süresi**

- 5 Gün

**Eğitim Seviyesi**

- Orta
- İleri

**Eğitim İçin Ön Gereksinimler**

- Temel ağ ve güvenlik bilgisi
- SIEM, IDS/IPS ve ağ izleme araçları bilgisi
- Güvenlik olaylarının analizi ve raporlama bilgisi

**Eğitimi Kimler Katılmalı?**

- SOC analistleri ve güvenlik ekipleri
- MDR analistleri ve hizmet sağlayıcıları
- Siber güvenlik uzmanları ve ağ güvenliği analistleri

**Eğitim Sonunda Katılımcılar Ne Öğrenmiş Olacak?**

- Katılımcılar, güvenlik operasyon merkezlerinde (SOC) ve yönetilen tespit ve yanıt (MDR) hizmetlerinde görev alabilecek, tehditleri izleme, analiz etme ve müdahale etme becerisi kazanırlar.

**Eğitim İçeriği**

- SOC ve MDR Nedir?
- SOC katmanları (Tier 1, Tier 2, Tier 3) görev tanımları
- MDR nedir? Farkı ve avantajları
- SOC operasyon süreçleri ve olay döngüsü
- Kullanılan ürünler: SIEM, EDR, SOAR, NDR, Threat Intelligence
- Alert → Investigation → Response döngüsü
- SLA yönetimi, önceliklendirme ve vaka kapanış süreçleri
- Temel ve İleri Seviye Tehditlerin Tanınması
- Malware türleri, exploit teknikleri, persistence yöntemleri
- Phishing, C2, beaconing, data exfiltration, privilege escalation
- TTP analizi ile saldırı evresi tanımlama
- Saldırgan davranışlarının loglarda izi (Logon, process, registry, network, DNS)
- MITRE ATT&CK ile analiz modelleme
- Örnek: APT, ransomware, insider threat senaryoları
- SIEM Kullanımı ve Olay Analizi
- SIEM nedir? SIEM mimarisi ve veri akışı
- Log türleri ve log normalizasyonu (Windows, Linux, FW, Proxy, AV, EDR vs.)
- Kuralların yazımı: correlation, anomaly, threshold
- SIEM platformları:
- Spluk, QRadar, Elastic, Microsoft Sentinel, Logpoint
- Use Case örnekleri ve rule geliştirme
- Olay triyajı, alarm araştırması, pivot teknikleri
- Zaman çizelgesi oluşturma ve log korelasyonu
- IOC ve TTP üzerinden alert zenginleştirme
- EDR ve NDR Kullanımı
- EDR nedir? EDR ile endpoint davranış analizi
- Popüler EDR çözümleri: CrowdStrike, SentinelOne, Defender, Carbon Black
-

**Eğitim İçeriği**

- Suspicious process tree analizi
- PowerShell abuse, LOLBin, persistence tespiti
- NDR kavramı ve anomalous network detection
- DNS Tunneling, beaconing, C2 davranışı izleme
- Netflow, packet analysis, protocol behavior analizi
- Tehdit Avı (Threat Hunting)
- Hypothesis-based ve IOC-based threat hunting farkı
- Sigma, Yara, KQL kullanarak hunt senaryoları
- MITRE ATT&CK üzerinden davranış bazlı arama
- Normal dışı davranışların tespiti (süre, sıklık, pattern)
- Hunt loop: hypothesis → query → match → context → escalation
- Senaryo: İçeriden veri sızdırma – DNS exfiltration analizi
- Olay Müdahale Süreci (IR)
- Vaka yaşam döngüsü: Identification → Containment → Eradication → Recovery
- Önceliklendirme ve olay sınıflandırma (alert severity & risk context)
- Temizleme ve forensic preservation dengesini kurma
- Karantina, komuta kontrol kesme, hesap devre dışı bırakma uygulamaları
- Örnek senaryo: Ransomware vakası müdahalesi
- Olay kayıt altına alma, timeline çıkarımı, artefact analizi
- Uygulamalı Vaka Senaryoları
- Windows Log'larında başarılı oturum açma sonrası şüpheli PowerShell
- Web proxy log'larında C2 iletişimi belirleme
- EDR üzerinden credential dumping ve persistence analizi
- SIEM'de failed logon burst + account lockout kombinasyonu
- DNS log'larında veri sızdırma davranışının yakalanması
- MITRE T1059, T1003, T1547 örnekleriyle saldırgan davranışı tespiti

**Eğitim İçeriği**

- Threat intelligence IOC ile korelasyon ve yayılım takibi
- CTI ve SOC Entegrasyonu
- IOC & TTP aktarımı: CTI'dan SOC'a bilgi akışı
- MISP, OpenCTI, ThreatFox entegrasyonu
- Threat actor mapping ve kampanya takibi
- IOC yaşlandırma (decay), enrichment
- Olaylara CTI perspektifinden yaklaşım ve false positive filtreleme
- Raporlama, Dökümantasyon ve Sunum
- Olay raporu formatları
- Yönetim ve teknik ekip için ayrı raporlama yapısı
- Timeline çıkarımı ve yorumlama
- SLA, KPI, olay istatistikleri, dashboard raporlaması
- SOC performans ölçümü ve Continuous Improvement döngüsü

**Sıkça Sorulan Sorular**

**SOC (Security Operations Center) nedir ve ne iş yapar?**

- SOC, organizasyonların güvenliğini izlemek, tehditleri tespit etmek ve yanıt vermek için oluşturulmuş bir birimdir. Eğitim, SOC süreçlerini yönetmek ve optimize etmek üzerine odaklanacaktır.

**MDR (Managed Detection and Response) nedir?**

- MDR, dış kaynaklı bir hizmet olarak, organizasyonların siber güvenlik olaylarını tespit etme, yanıt verme ve analiz etme süreçlerini yönetir.

**SOC ve MDR analistinin temel görevleri nelerdir?**

- Analist, güvenlik uyarılarını izler, tehditleri tespit eder, analiz eder ve gerektiğinde müdahalelerde bulunur.

**Eğitim sonunda hangi beceriler kazanılacak?**

- Katılımcılar, SOC ve MDR altyapısında çalışabilecek, olayları analiz etme ve önceliklendirme becerileri kazanacaklardır.