EMA SECURITY

Siber Tehdit İstihbaratı 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

Siber Tehdit İstihbaratı Eğitimi

Eğitim Açıklaması

Siber Tehdit İstihbaratı Eğitimi, organizasyonları hedefleyen potansiyel tehditlerin analiz edilmesi ve bunlara karşı önceden önlem alınması için gereken bilgileri sağlar. Katılımcılar, siber tehdit istihbaratı toplama yöntemleri, tehdit aktörlerinin analiz edilmesi ve güvenlik açıklarının tespiti konusunda derinlemesine bilgi edinirler. Bu eğitim, tehditleri anlamak ve onlara karşı proaktif savunmalar geliştirmek isteyen profesyonellere yöneliktir.

Eğitim Yeri

- Online
- Fiziksel

Eğitim Süresi

- 3 Gün

Eğitim Seviyesi

- Başlangıç
- Orta

Eğitim İçin Ön Gereksinimler

- Temel siber güvenlik ve ağ bilgisi
- Siber tehdit analiz ve bilgi toplama becerisi
- Malware analizi ve saldırı vektörlerini anlamak

Eğitimi Kimler Katılmalı?

- Tehdit istihbaratı analistleri
- SOC ve güvenlik ekipleri
- Siber güvenlik uzmanları ve araştırmacıları

Eğitim Sonunda Katılımcılar Ne Öğrenmiş Olacak?

- Katılımcılar, siber tehditleri önceden tespit etmek için istihbarat toplama, analiz etme ve tehditlere karşı strateji geliştirme yeteneği kazanırlar.

Eğitim İçeriği

- Giriş ve Teorik Temeller
- CTI nedir? Tehdit İstihbaratı Türleri: Stratejik, Taktiksel, Operasyonel, Teknik
- Tehdit İstihbaratı Yaşam Döngüsü (Intelligence Lifecycle)
- Tehdit modeli: Diamond Model of Intrusion Analysis
- MITRE ATT&CK Framework ile saldırgan davranışı analizi
- Cyber Kill Chain modeli ile tehdit ilerleyişinin evrelenmesi
- CTI & SOC, IR, Red/Blue/Purple Team entegrasyonu
- Tehdit Kaynakları ve Toplama Yöntemleri
- Açık Kaynak (OSINT) Toplama
- Domain, IP, DNS, SSL analizleri (crt.sh, VirusTotal, RiskIQ)
- Paste siteleri, açık forumlar, social media, GitHub aramaları
- IOC kaynakları: AlienVault OTX, ThreatFox, AbuseIPDB, MISP feedleri
- CVE ve Exploit analiz kaynakları: NVD, ExploitDB, GitHub exploits
- Arama motorları: Shodan, Censys, ZoomEye, BinaryEdge
- Kapalı Kaynaklar ve Dark Web
- Deep/Dark Web forumlarında tehdit aktörü takibi
- Chat platformları ve sızıntı kaynakları
- Breach veri setlerinin analizi
- TOR ağı üzerinde arama yöntemleri
- Makine Kaynaklı Toplama
- SIEM, EDR, NDR platformlarından IOC ve TTP çıkarımı
- Honeypot sistemleri ile saldırgan takibi
- Sandbox analizlerinden veri çıkartımı
- Malware analizinden IOC üretimi (Yara, Sigma, static/dynamic analysis)
- Tehdit Aktörü ve APT Analizi
- Tehdit aktör sınıflandırması (hacktivist, cybercriminal, state-sponsored)
- APT grup profilleme (TA505, APT28, Lazarus, FIN7 vb.)
- TTP haritalandırma (ATT&CK Navigator ile analiz)
- Threat Group Matrix & TTP correlasyonları

Eğitim İçeriği

- Teknik izler üzerinden tehdit aktörü belirleme (toolset, infrastructure, lingo)
- Örnek Case Study: APT29 saldırı kampanyası analizi
- IOC ve TTP Analizi
- IOC türleri: IP, domain, URL, hash, yara, email artefact'ları
- IOC doğrulama, yaşlandırma (decay), önem derecesi
- TTP çıkarımı ve teknik özet oluşturma
- Sigma, Yara, Snort kuralı üretimi
- IOC yayılımı ve paylaşımı: STIX, TAXII, MISP
- IOC takibi için otomatizasyon: TheHive, OpenCTI, MISP senkronizasyonu
- CTI Platformları ve Araçları
- CTI Platformları:
- MISP (Malware Information Sharing Platform)
- OpenCTI
- ThreatConnect, Recorded Future, Anomali, Intel 471
- Analiz Araçları:
- Yara, Sigma, IOC Parser, IOC Extractor
- VirusTotal, AnyRun, Maltego, Spiderfoot
- ATT&CK Navigator, Caldera, YETI
- Harita/bağlantı çıkarımı için: MISP Galaxy, IntelMQ, Kusto, Greynoise
- İleri Seviye Analiz Teknikleri
- Taktik - teknik eşleşmesi: TTP to IOC eşleşmesi
- Log korelasyonu üzerinden IOC match'leme
- Malware campaign analizi (makro, droppers, C2)
- Domain ve altyapı ilişkileri (Passive DNS, subdomain enumeration)
- Saldırgan altyapısı haritalama: hosting, whois, sertifika, ASN korelasyonu
- CTI Raporlama ve Paylaşım
- Taktik raporlama: IOC ve TTP'ye dayalı kısa notlar
- Teknik raporlama: Analiz, zincirleme, davranış, malware ilişkisi
- Stratejik raporlama: Yönetim seviyesi karar destek

Eğitim İçeriği

- CTI rapor şablonları ve stil rehberleri
- Rapor paylaşımı: e-posta, MISP, STIX/TAXII entegrasyon
- Senaryolar ve Uygulamalı Laboratuvarlar
- APT saldırı kampanyası analizi (TTP, IOC, yapı haritalama)
- OSINT kullanarak domain/SSL/C2 ağı haritası çıkarımı
- IOC'den log eşleşmesi ve tehdit avı
- Dark web üzerinden sızdırılmış veri tespiti
- VirusTotal + Yara + AnyRun ile malware davranış analizi
- MISP ve OpenCTI üzerinden IOC yönetimi ve paylaşımı

Sıkça Sorulan Sorular

Siber tehdit istihbaratı nedir ve neden önemlidir?

- Siber tehdit istihbaratı, potansiyel siber tehditleri tanımlayarak, organizasyonları bu tehditlere karşı önceden hazırlıklı hale getirir. Tehditlerin izlenmesi ve analiz edilmesi ile güvenlik stratejileri oluşturulur.

Tehdit istihbaratını toplamak için hangi kaynaklar kullanılır?

- Açık kaynaklar (OSINT), kapalı kaynaklar, Dark Web izleme ve siber güvenlik tehdit raporları gibi kaynaklar kullanılarak bilgi toplanır.

Eğitim sonunda ne tür beceriler kazanılır?

- Katılımcılar, tehdit istihbaratını toplama, analiz etme ve siber tehditlerin organizasyonları nasıl etkileyebileceğini anlamada beceri kazanacaklardır.