EMA SECURITY

Siber Olay Müdahale 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 Olay Müdahale Eğitimi

Eğitim Açıklaması

Siber Olay Müdahale Eğitimi, bir siber saldırı anında etkin müdahale yapabilme yeteneğini geliştirmeyi amaçlar. Katılımcılar, siber olayları yönetme, olayın yayılmasını engelleme ve hızlıca çözüm üretme becerilerini öğrenirler. Eğitimde, olay müdahale süreçleri, kriz yönetimi, izleme ve raporlama teknikleri gibi önemli konular ele alınır. Katılımcılar, bir saldırı sonrası etkin bir şekilde çözüm sürecine katkı sağlama yeteneği kazanacaklardır.

Eğitim Yeri

- Online
- Fiziksel

Eğitim Süresi

- 5 Gün

Eğitim Seviyesi

- Orta
- İleri

Eğitim İçin Ön Gereksinimler

- Temel ağ, sistem ve güvenlik yönetimi bilgisi
- Olay müdahale süreçlerine aşinalık
- Güvenlik yazılımlarına ve analiz araçlarına hakimiyet

Eğitimi Kimler Katılmalı?

- Olay müdahale ekibi üyeleri
- Güvenlik analistleri ve SOC ekipleri
- Siber güvenlik profesyonelleri ve ağ güvenliği uzmanları

Eğitim Sonunda Katılımcılar Ne Öğrenmiş Olacak?

- Katılımcılar, siber saldırıların ardından etkili müdahale ve kurtarma süreçlerini öğrenir, olaylara hızlı ve etkili yanıt verme becerisi kazanırlar.

Siber Olay Müdahale Eğitimi

Eğitim İçeriği

- Giriş ve Temeller
- Siber olay türleri ve sınıflandırılması
- Olay Müdahale (IR) kavramı, amacı ve kapsamı
- Olay yaşam döngüsü: NIST 800-61 çerçevesi
- IR süreçlerinde yer alan roller (SOC, CERT, CIRT, IR Team)
- Hukuki ve kurumsal sorumluluklar
- Olay Müdahale Süreci
- Hazırlık (Preparation)
- IR planı oluşturma, prosedürler ve yetkilendirme
- İletişim planı ve gizlilik protokolü
- Loglama altyapısının değerlendirilmesi (log retention, centralization)
- Forensik araçlar ve analiz ortamlarının hazır tutulması
- Delil zinciri ve yasal geçerlilik
- Tespit ve Tanımlama (Detection & Analysis)
- Olay alarmı kaynakları: SIEM, EDR, IDS, kullanıcı ihbarları
- IOC ve anomali tabanlı tespit farkları
- İlk analiz: şüpheli dosya, IP, kullanıcı, zaman damgası
- Olayın etki kapsamı ve türünün belirlenmesi
- İlk pivot analizi: lateral hareket, komuta kontrol (C2) izi
- İzolasyon ve İçerme (Containment)
- Host izolasyonu (EDR ile ağdan çıkarma)
- Ağ segmentasyonu
- Uç nokta ve sunucu sistemlerin anlık yedeklenmesi
- Sistem kapatmadan bellek ve disk imajı alma
- Silme ve İyileştirme (Eradication & Recovery)
- Zararlı yazılım ve arka kapıların kaldırılması
- Kalıcılık yöntemlerinin (persistence) tespiti ve temizlenmesi

Siber Olay Müdahale Eğitimi

Eğitim İçeriği

- Şifre sıfırlamaları, servis yeniden yapılandırmaları
- Sistemin güvenli şekilde tekrar devreye alınması
- Öğrenme ve İyileştirme (Lessons Learned)
- Olay sonrası teknik analiz ve kök neden belirleme
- İlgili paydaşlara olay raporlaması
- Güvenlik kontrollerinin güncellenmesi
- Eğitim ve farkındalık süreçlerinin güçlendirilmesi
- Delil Toplama ve Adli Analiz (Forensics)
- Bellek Analizi
- RAM dump alma (DumpIt, Belkasoft RAM Capture)
- Volatility ile analiz: Process, Network, DLL, Hook'lar
- Injected code, credential artefact'ları, C2 iletişimi
- Disk ve Dosya Sistemi Analizi
- Disk imajı alma (dd, FTK Imager, Guymager)
- MFT, $LogFile, $USNJournal, Prefetch, Shellbag analizleri
- Zaman damgaları ile olay zaman çizelgesi oluşturma (timeline)
- Log Analizi
- Windows Event Viewer: 4624, 4688, 7045, 4720 vs.
- Linux logları: auth.log, bash_history, syslog, auditd
- Web sunucu logları (IIS, Apache), DNS logları, firewall kayıtları
- Ağ Trafik Analizi
- PCAP toplama ve Wireshark ile analiz
- C2 bağlantıları, veri sızıntısı, beaconing tespiti
- Zeek ve Suricata ile ağ temelli olay izleme
- 4. Araçlar ve Platformlar
- EDR: CrowdStrike, Carbon Black, Microsoft Defender ATP
- SIEM: Splunk, ELK, QRadar, Sentinel

Siber Olay Müdahale Eğitimi

Eğitim İçeriği

- Forensics: FTK Imager, Autopsy, Volatility, X-Ways
- Network: Wireshark, Zeek, tcpdump, Tshark
- IOC arama: VirusTotal, MISP, ThreatFox, AbuseIPDB
- 5. Gerçek Senaryo Uygulamaları
- Ransomware olayı simülasyonu
- Web shell içeren web sunucusu olayı
- PowerShell ile persistence içeren saldırı analizi
- Active Directory üzerinde lateral movement tespiti
- C2 bağlantısına sahip beaconing davranışı
- Insider threat örneği – hassas veri dışarı çıkarılması
- 6. Raporlama ve Sonuçlandırma
- Olay özet raporu (timeline, etki alanı, zararlı hash, teknik detaylar)
- Teknik ekip için detaylı teknik analiz raporu
- Yönetim için sadeleştirilmiş yönetişim raporu
- Hukuki süreçte kullanılabilir olay kayıtlarının hazırlanması

Sıkça Sorulan Sorular

Saldırı tespit ve analizinde en kritik unsurlar nelerdir?

- Güvenlik araçlarının doğru konfigürasyonu, log yönetimi, anomalilerin tespiti, zaman damgalarının analizi ve güvenlik izleme altyapısı çok önemli unsurlardır.

Eğitimde hangi olay türleri incelenecek?

- Zararlı yazılım analizleri, hacklenmiş sunucu ve sistemlerin analizleri, DDoS saldırıları, veri sızıntıları ve iç tehditler gibi farklı siber olay türleri ele alınacaktır.

Siber olay müdahale ekipleri nasıl organize edilir?

- Eğitim, olay müdahale ekiplerinin nasıl yapılandırılacağı, rollerin ve sorumlulukların nasıl belirleneceği üzerine odaklanacaktır.

Eğitimde kullanılacak araçlar nelerdir?

- SIEM sistemleri, Autopsy, FTK Imager, yeni nesil EDR,XDR, YARA gibi araçlar olay müdahalesinde kullanılacak araçlar arasında yer alır.