SİBER OLAY TESPİT VE MÜDAHALE EĞİTİMİ

AMAÇ

Açık ve daha az belirgin olan siber olayların tespit yöntemleri, tehdit avcılığı ve siber olay müdahale metodolojisinin detaylandırılması amaçlanmaktadır.

ODAK NOKTALARI

#Siber Olay #Siber Güvenlik #Tehdit Avcılığı

EĞİTİMDEN BEKLENEN SONUÇLAR

Bilir:Temel siber saldırı yöntemlerini bilir.

Anlar:Siber saldırıların bıraktığı izleri anlar.

Yapar:Siber saldırıları tespit eder ve saldırılara doğru biçimde (saldırıyı çevreleyerek ve kanıtların geçerliliğini bozmadan) müdahale eder.

HEDEF KİTLE

Bilgi güvenliği yönetim, denetim ve operasyon sorumluluğu bulunan uzmanlar ve siber saldırılar hakkında daha fazla bilgi sahibi olmak isteyen bilgi teknolojileri bölüm yöneticileri, sistem yöneticileri ve yazılım uzmanlarının katılımına uygundur.

NOT

İÇERİK

❑ Hazırlık Aşaması
- ▸ Tehdit Yüzeyi Analizi ve Güvenlik Alanlarının (Domain'lerinin) Çıkarılması
- ▸ Sensör Yeterliliklerinin Değerlendirilmesi, Yatırım ve Geliştirme Planlamasının Yapılması
- ▸ Tehdit Yüzeyini Daraltma ve Saldırı İhtimalini Azaltma Amaçlı Erişim Kontrolleri Güçlendirmelerinin Artırılması ve Yetkilerin Sıkılaştırılması

❑ Sıkılaştırma ve Güvenlik Politikaları İzleme
- ▸ Sistem Sıkılaştırma Prosedürleri
- ▸ Envanter ve Güncelleme Takibi
- ▸ Erişim Kontrol Matrisinin Sürekli Gözden Geçirilmesi ve Yüksek Yetkili Kullanıcı Hesaplarının/ Gruplarının Merkezi Olarak İzlenmesi
- ▸ Denetim İzi (Audit Log) Ayarlarının İzlenmesi
- ▸ Öncül veya Yan Belirti Olarak Kapasite Kullanım ve Kesinti Takibi

❑ Saldırı Verisi Toplama
- ▸ Saldırı Tespit Araçları ve Kullandıkları Yöntemler
- ▸ Anti-Virüs Araçları ve Kullandıkları Yöntemler
- ▸ Log Alt Sistemleri ve Temel Log Türleri
- ▸ Temel Log Saklama Formatları ve Erişim Yöntemleri
- ▸ Log Kayıtlarından Faydalanılarak Alarm Kuralları Geliştirme ve Uygulanma Yöntemleri
- ▸ Büyük Veri Kavramları ve Log Yönetimi Arasındaki İlişkiler
- ▸ Gelişmiş Arama Altyapıları ve Log Yönetimine Faydaları
- ▸ Temel Log Yönetim Kavramları ve Güvenlik İzlemesi Açısından Önemleri (Sınıflandırma, Zenginleştirme/ Normalizasyon)
- ▸ Yanal Hareket (Lateral Movement) Metodları ve Tespit Etme Yöntemleri

❑ Saldırı Şüphesi İnceleme Aşaması
- ▸ Zararlı Yazılım İnceleme Yöntem ve Adımları
- ▸ İhlal İşaretleri (IoC – Indicator Of Compromise) Tespiti
- ▸ Kurum Ağının Geri Kalanında Tehdit Arama
- ▸ Adli Bilişim Temel Adımları

EĞİTİM YETKİNLİK İLİŞKİSİ

Davranışsal Yetkinlikler	Merak ve Keşfetme, Analitik Düşünme ve Yaratıcılık
Yönetsel Yetkinlikler	Planlama ve Organizasyon, Koordinasyon, Denetleme
Mesleki/ Bankacılık Teknik Yetkinlikler	Operasyonel Takip ve Bilinç, İç Sistemler ve Denetim, Raporlama ve Sunum
Öz-Gelecek Yetkinlikleri	Değişimi Okuyabilmek ve Geleceği Kurgulamak

Uygulama Yeri	Süre	Eğitim Görevlisi
TBB Eğitim Merkezi	2 gün	Fatih Emiral
Başlangıç Tarihi : 27.5.2020 - Bitiş Tarihi: 28.5.2020 TBB Üyeleri İçin Eğitim Ücreti: ₺700 - Diğer Kurumlar İçin Eğitim Ücreti: ₺820		

- Fiyatlarımıza KDV Dahildir.