

# Kayıt (LOG) Toplama ve Yönetimi Eğitimi

Süre: 3 Gün

## Kayıt (LOG) Toplama ve Yönetimi Eğitimi Hakkında

Kayıt (LOG) Toplama ve Yönetimi Eğitimi, kuruluşun ağ ve sistemlerinden alınan kayıtlarla siber olay tespiti ve olay sonrası inceleme becerilerini geliştirmeye yöneliktir. 3 günlük sanal sınıf / online program; kayıt türleri, toplama ve tutma yapısının kurulması, kayıtların işlenmesi ve güvenlik incelemelerinde kullanılması konularını kapsar.

Sunucular, Windows ve Linux istemciler, ağ cihazları ve güvenlik cihazlarının ürettiği kayıtlar birlikte ele alınır. Kayıt üreten sistemlerin belirlenmesi, toplama yöntemlerinin değerlendirilmesi ve kayıtların önemlerine göre sınıflandırılması üzerinde durulur.

Kayıt işleme ve inceleme araçları ile yöntemler, ham kayıt verilerinin işe yarar bilgiye dönüştürülmesi kapsamında incelenir. Siber saldırıların, ağ içindeki saldırganların ve zararlı yazılımların kayıtlar üzerinden tespiti ile olay sonrası inceleme, programın güvenlik odağını oluşturur.

## Eğitim İçeriği

### Ağ Üzerinde Üretilen Kayıt Türleri

- Kayıtların dünyasına giriş
- Sunucuların ürettiği kayıtlar
- İstemci (Windows ve Linux) kayıtları
- Ağ cihazlarının kayıtları
- Güvenlik cihazlarının kayıtları

### Kayıt Toplama ve Tutma Yapısının Kurulması

- Ağ üzerinde kayıt üreten sistemlerin belirlenmesi
- Kayıt toplamak için kullanılabilecek yöntemler
- Kayıtların önemlerine göre sınıflandırılması
- Kayıt toplama yapısı kurulumu
- Toplanan kayıtların tutulması

## Kayıtların İşlenmesi

- Kayıt işleme araçları
- Kayıt işlemek için kullanılabilecek teknikler
- Kayıt verilerinin işe yarar bilgiye dönüştürülmesi
- Kayıt inceleme araçları
- Kayıt inceleme yöntemleri

## Kayıtların Kullanılması

- Siber olaylarda ortaya çıkan kayıtlar
- Kayıtlar üzerinden siber saldırı tespiti
- Kayıtlarla ağ içinde saldırgan tespiti
- Kayıtlar ile zararlı yazılım tespiti
- Siber olay sonrası kayıtların kullanımı

## Ön Koşullar

---

Herhangi bir ön koşul bulunmamaktadır.