Kayıt (LOG) Toplama ve Yönetimi Eğitimi

Açıklama

Kuruluş ağında ve sistemlerinden alınabilecek kayıtlar (log) kullanılarak siber olay tespiti ve olay sonrası inceleme becerisi kazandırmak.

Bu eğitimde neler öğreneceksiniz?

- Ağ Üzerinde Üretilen Kayıt Türleri
- Kayıt Toplama ve Tutma Yapısının Kurulması
- Kayıtların İşlenmesi
- Kayıtların Kullanılması

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.