SOME Kurulumu

Açıklama

Kamu kurumları ve kritik sektörlerde kurulması gereken SOME (Siber Olaylara Müdahale Ekibi) yapısının başarılı bir proje dahilinde etkili ve sürdürülebilir şekilde kurulması için gerekli bilgiler aktarılacaktır.

Bu eğitimde neler öğreneceksiniz?

- SOME Temelleri
- SOME Personeli
- SOME Süreçleri
- Siber Olayların Tespiti
- SOME Teknolojileri

Eğitim İçeriği

SOME Temelleri

- SOME kurulumunun temelleri
- Türkiye'de SOME'ler
- Uluslarası SOME standartları

SOME Personeli

- Personel seçimi kriterleri
- Personelin alması gereken eğitimler
- SOME'ye destek olacak görevler
- SOME'nin iletişim kanalları

SOME Süreçleri

- Temel SOME süreçleri
- SOME süreçlerinin detaylandırılması
- Kuruluşa özel SOME süreçlerinin belirlenmesi
- SOME süreçlerinin kontrolü
- Örnek SOME politikaları ve süreçleri

Siber Olayların Tespiti

- IOC (Indicators of Compromise olay göstergeleri)
- Teknik olmayan siber olay göstergeleri
- Teknik olay göstergeleri
- Olay göstergelerinin teyidi ve yanlış alarmların ayıklanması

SOME Teknolojileri

- Etkili bir SOME için gerekli teknolojileri
- Siber olay tespiti için kullanılabilecek teknolojiler
- SOME teknolojilerinin entegrasyonu
- Olay sonrası takip

Ön Koşullar

Herhangi bir ön koşul bulunmamaktadır.