

# Siber Olaylara Müdahale

MEHMET KILIÇ  
HACKTRICKCONF

# İçerik

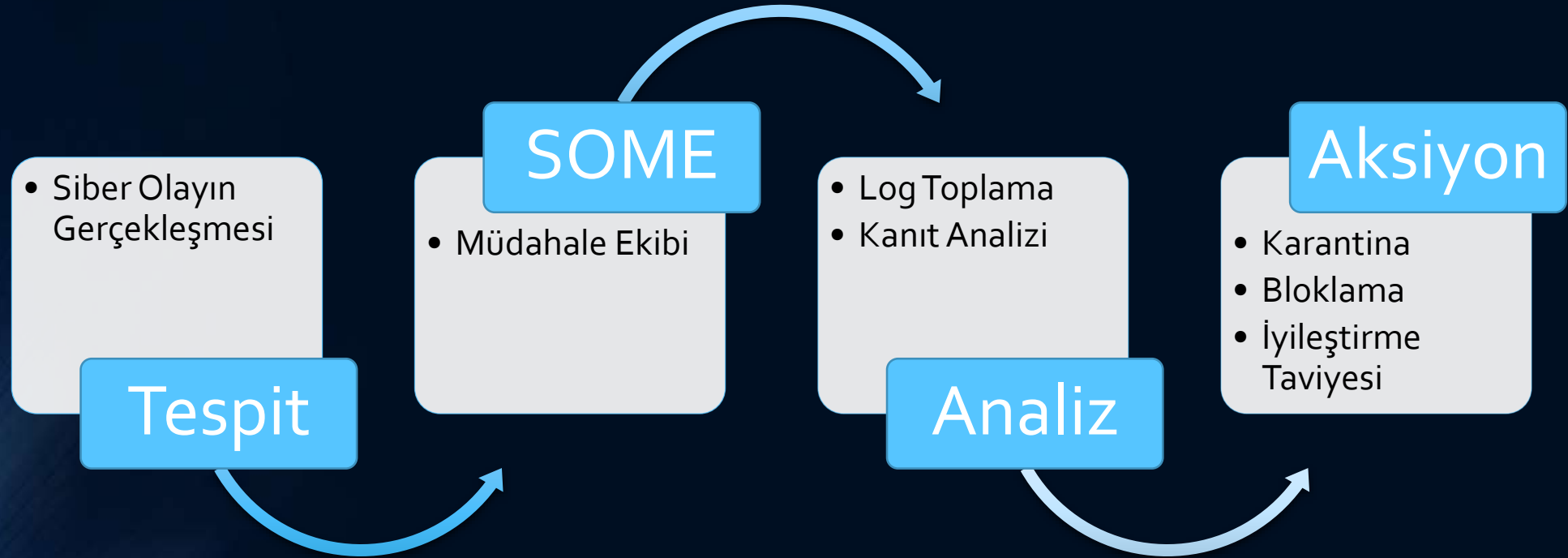
- Siber Olay Nedir? Ne Değildir?
- Siber Olaylara Müdahale Planı
- İstatistikler
- Zararlı Kod Örneği
- Web Sızma Girişimi
- Yetkisiz Erişim

“ Biliřim ve endüstriyel kontrol sistemlerinin veya bu sistemler tarafından işlenen bilginin gizlilik, bütünlük veya erişilebilirliğinin ihlal edilmesini veya ihlal teşebbüsünde bulunulmasıdır. ”

Siber Olay Nedir? Ne Değildir?

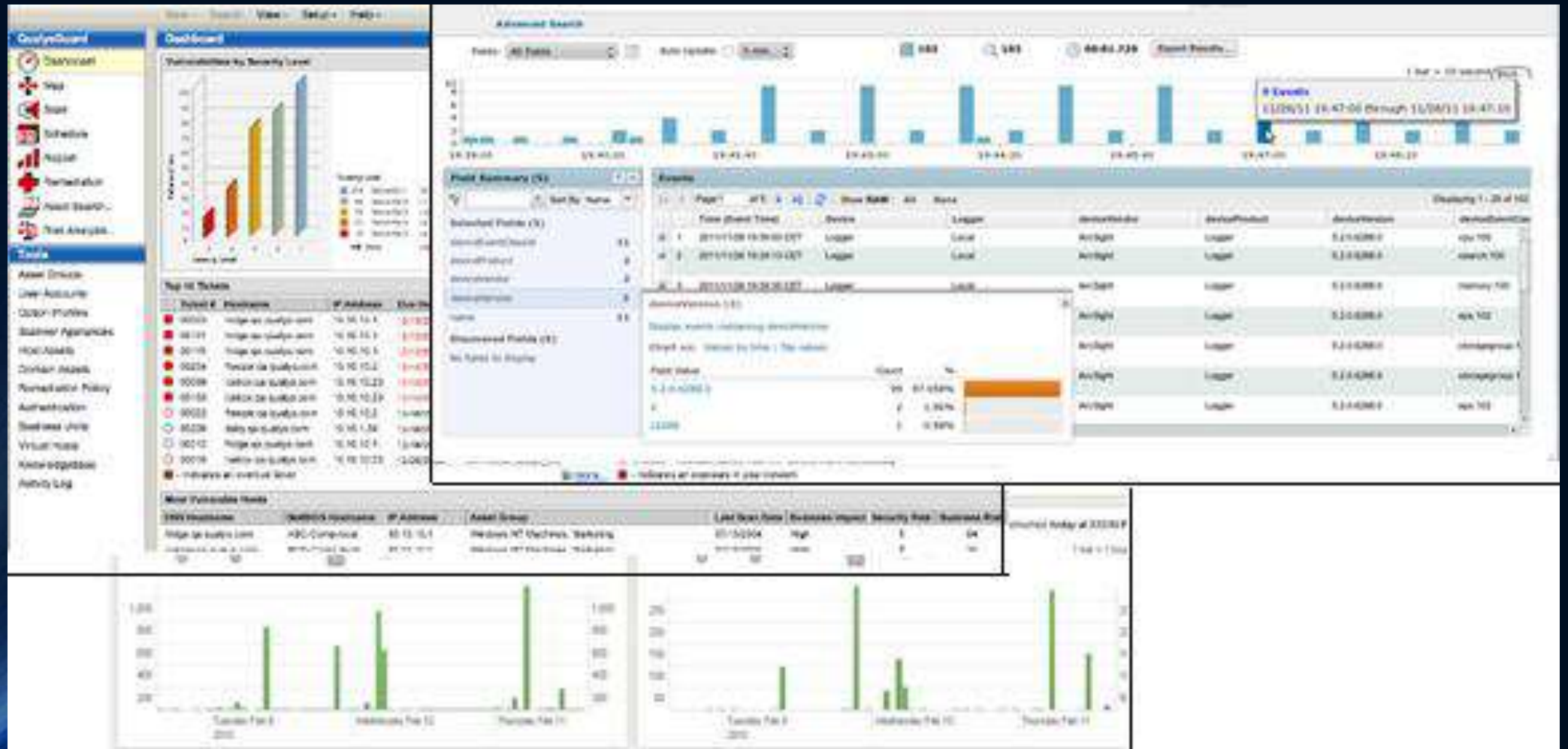
Kaynak : Ulaştırma Bakanlığı Kurumsal SOME Kurulum ve Yönetim Rehberi

# Siber Olaylara Müdahale Planı



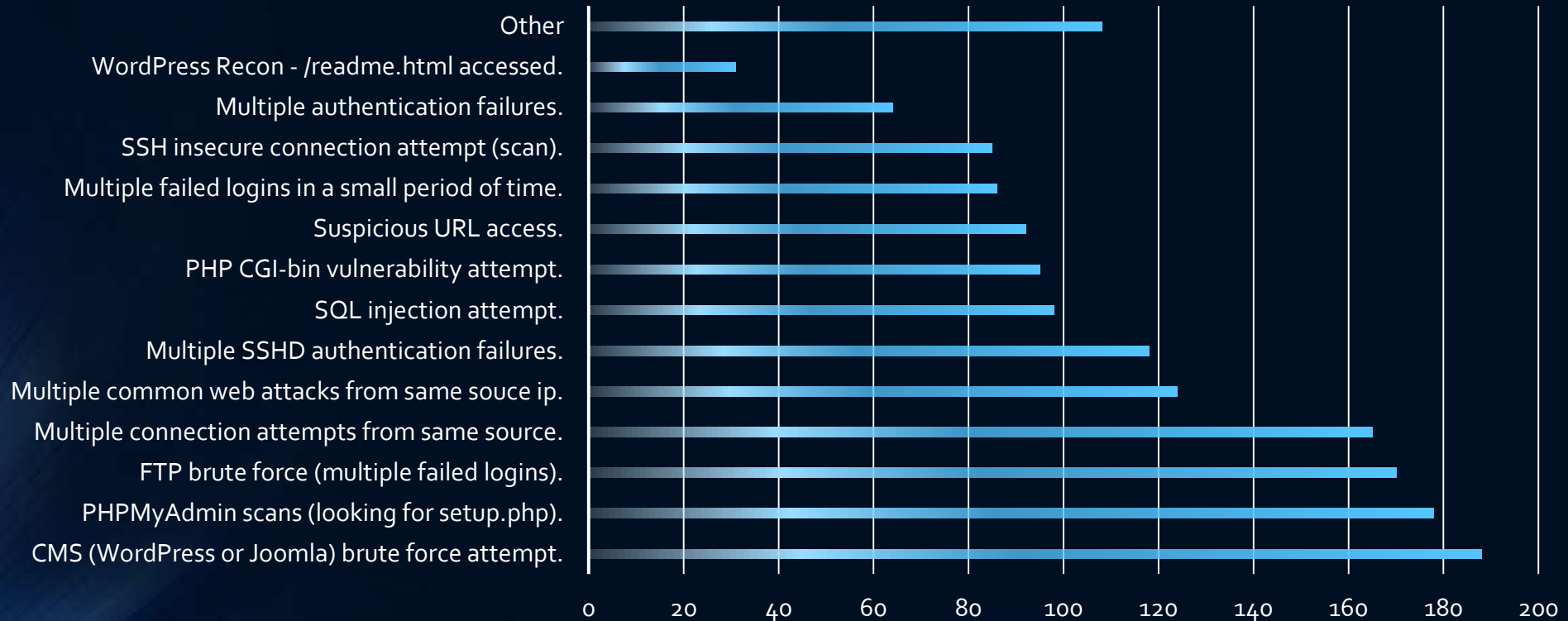


# Analiz



# GERÇEK SUNUCU SALDIRI İSTATİSTİKLERİ

## SUNUCU SALDIRI İSTATİSTİKLERİ



# Zararlı Kod

- Virus Bulaşımı (Tek/Çoklu)
- Trojan İçeren Program
- Zararlı Script

Aksiyon :

?



# Web Sızma Girişimi

- IPS/IDS Alarmı
- Web Uygulamasına Çok Sayıda İstek
- Şüpheli Metod Kullanımı

Aksiyon :

?





# Yetkisiz Erişim

- Kaba Kuvvet Saldırıları
- Oturum Açma Denemeleri
- ...

Aksiyon :

?



Teşekkürler

???