

# BÜYÜK ÖLÇEKLİ YAPILARDA MERKEZİ LOG YÖNETİMİ

Onur BAŞKAYA  
Güvenlik Mimarı  
Türk Telekom

# Hakkında

- ❖ Yüksek Elektrik Elektronik Mühendisi
- ❖ Güvenlik Mimarı
- ❖ 8 Yıllık IT ve Bilgi Güvenliği Tecrübesi
  - ❖ T.C.Dışişleri Bakanlığı
  - ❖ Türk Telekom A.Ş.
- ❖ Merkezi Log Yönetimi (KATİP)
  - ❖ Ürün Seçimi
  - ❖ Topoloji
  - ❖ Olay yönetimi süreçlerinin oluşturulması ve kontrolü

baskayaonur@yahoo.com

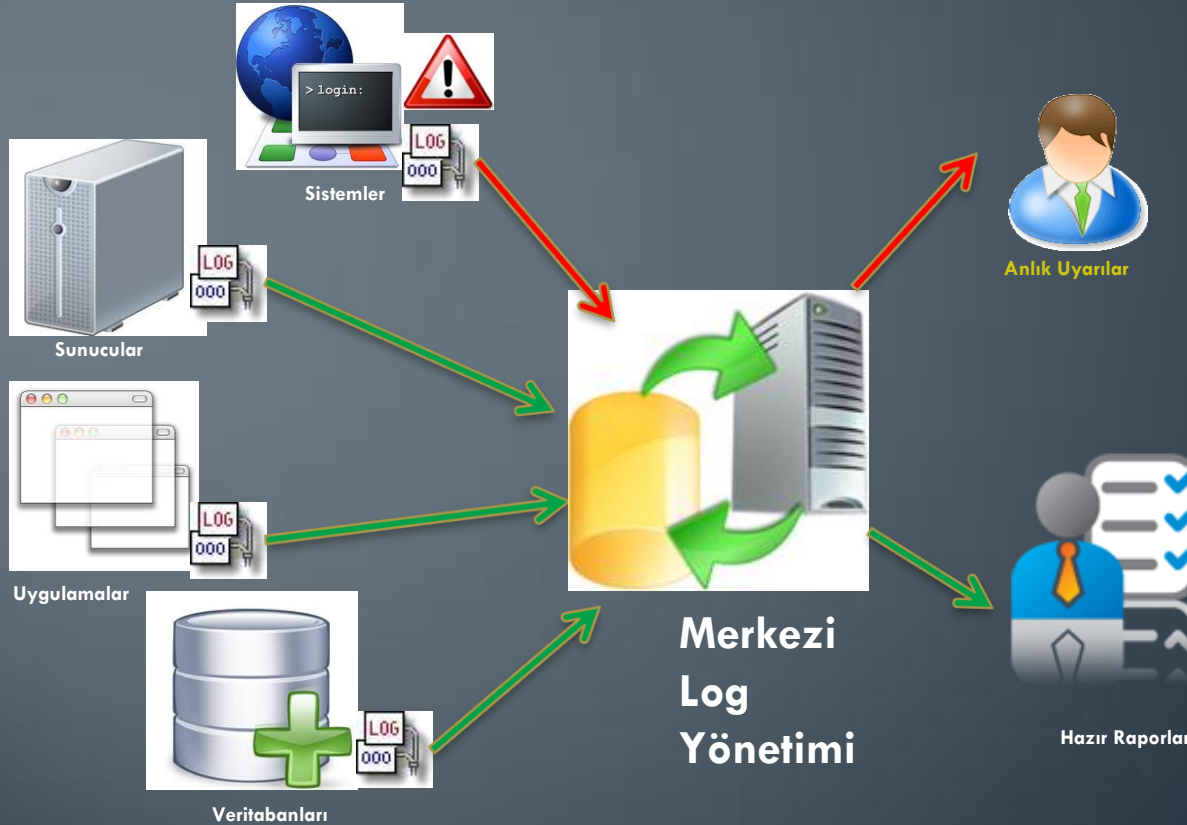
# Büyük Ölçekli Yapılarda Merkezi Log Yönetimi

## ❖ Dağıtık sistemlerdeki LOGLARIN

- ❖ TEK noktada TOPLANması
- ❖ TEK noktadan İZLENmesi
- ❖ TEK noktadan ARŞİVLENMESİ

## ❖ inMemory Correlation

- ❖ Farklı sistem logları ile KORELASYON
- ❖ Anında ALERT



# Merkezi Log Yönetimi Yaşam Döngüsü

❖ Dağıtık sistemlerdeki LOGLARIN

❖ inMemory Correlation

## MERKEZİ LOG YÖNETİMİ YAŞAM DÖNGÜSÜ



# Merkezi Log Yönetimi Kazanımlar

## KAZANIMLAR:

- Gerçek Zamanlı Güvenlik Analizi kabiliyeti sağlandı,
- Kanun ve Standartlara uygun Log Tutuluyor,
  - 5651 sayılı kanun
  - ISO-27001
  - ISO-27002
  - PCI-DSS
- Şüpheli işlemlere karşı **ANINDA uyarı** üretiliyor ve ilgililere Alert e-Mail gönderiliyor
  - Bruteforce
  - Web tarama
  - Separation of duties, Need to know
- KRİTİK UYARILAR için **ANINDA aksiyon** kabiliyeti sağlandı
  - Alarm ilgili birimlere düşürülüyor ve aksiyon alınıyor.

# Merkezi Log Yönetimi



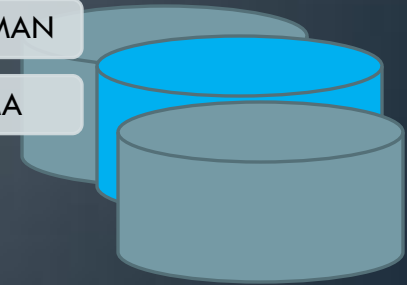
## 1.ADIM

Hangi güvenlik kayıtlarının tutulacağıın analizi ve ilgili sistemlerde bunun sağlanması.

## 2.ADIM

Ölçeklendirme, güvenlik kayıtlarının bütünlüğünün sağlanarak zaman damgası ile tutulması.

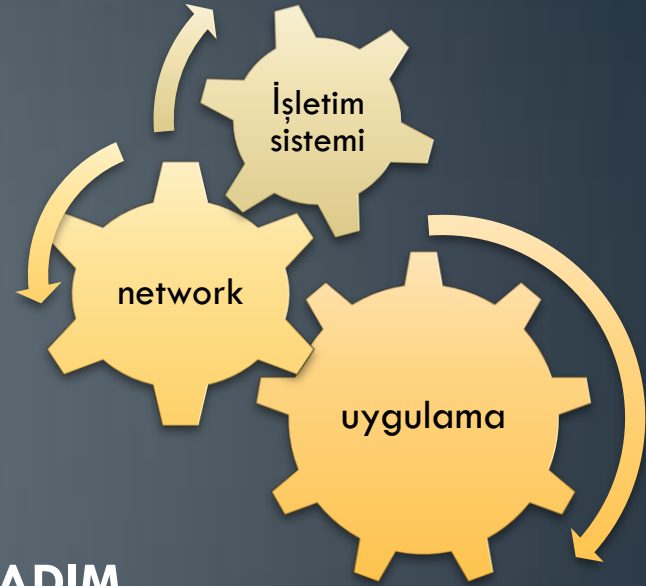
AUDIT LOG	• İZLENEBİLİRLİK
TIMESTAMP	• ORTAK ZAMAN
HASH	• DOĞRULAMA



# Merkezi Log Yönetimi

## 3.ADIM

Güvenlik kayıtlarının birbirleriyle ilişkilendirilmesi ve anlamlandırılması. **KORELASYON**



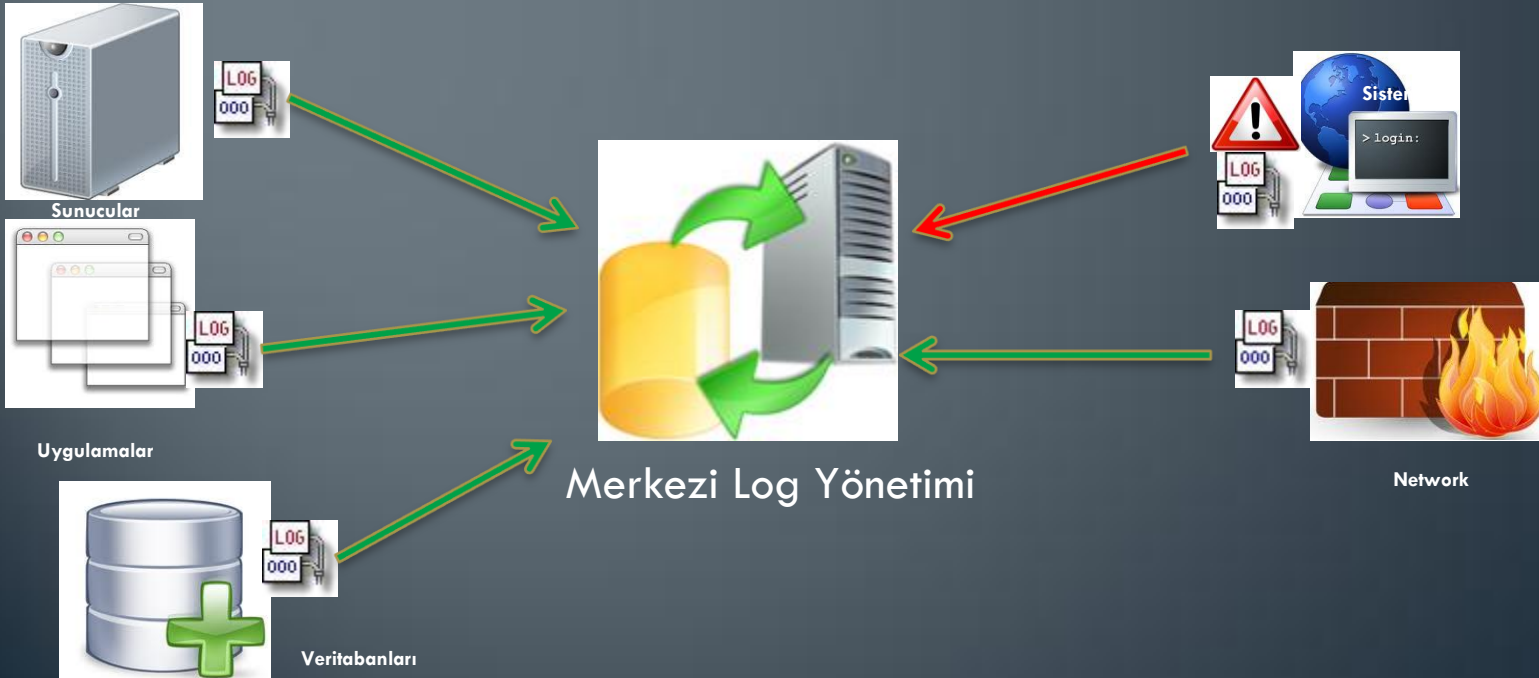
## 4.ADIM

İzlenebilirliği sağlanan güvenlik kayıtlarının ilgili birime alarm üretmesi. Raporların oluşturulması. Sorunla ilgili farkındalığın oluşturulması.



# 1. ADIM – LOG ANALİZİ

- ❖ İşletim Sistemleri Önemli Logları (Login/Logout, Kritik Değişiklikler, Kritik Sistem Çağruları vb.)
- ❖ Network Logları (Firewall, IPS/IDS, Switch vb.)
- ❖ Kapı Geçiş Sistemleri
- ❖ Veritabanı Logları (Erişim, SQL cümleleri vb.)
- ❖ Uygulamalar (Görevler Ayrılığı İlkesi, Need To Know İlkesi)



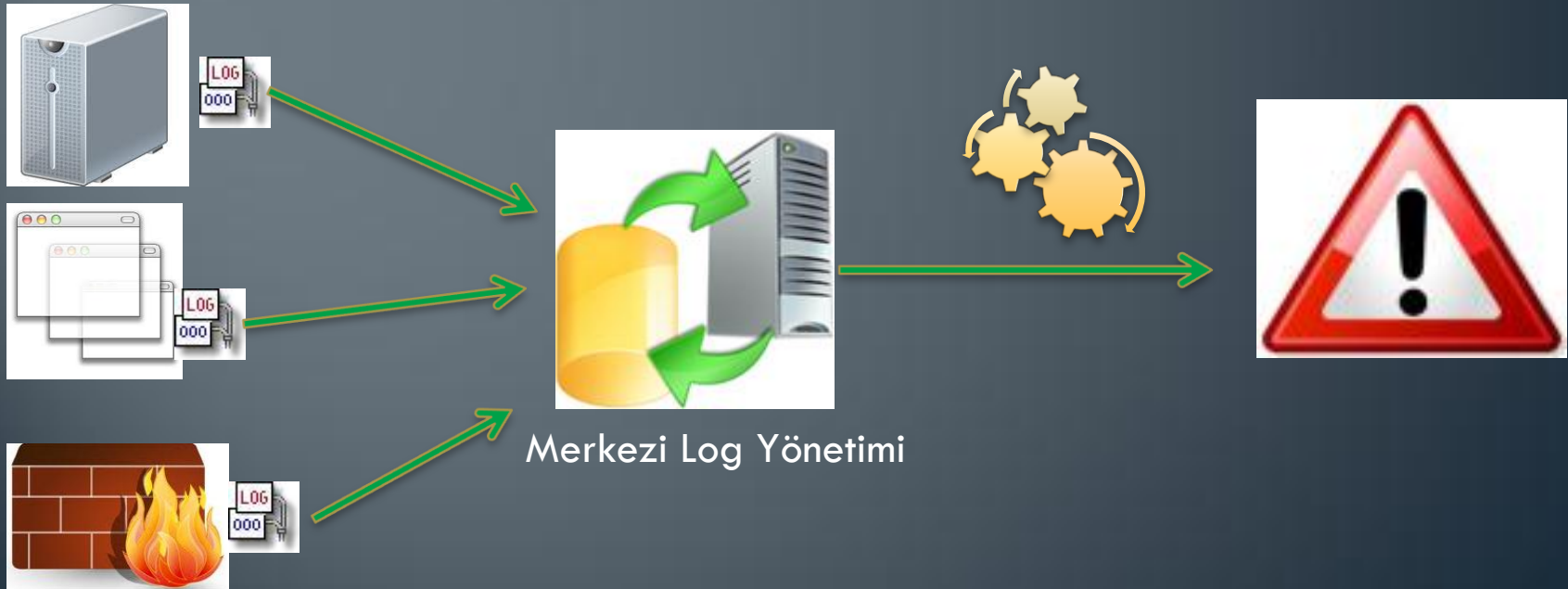
## 2. ADIM – ÖLÇEKLENDİRME VE LOG BÜTÜNLÜĞÜ

- ❖ Ölçeklendirme (Log Sayısı, Log Uzunluğu, Log Tutma Süresi, Donanım Özellikleri, Band Genişliği, Topoloji)
- ❖ Logların timestamp ile tutulması.
- ❖ Logların hash alınarak, raw datası ile tutulması.
- ❖ Logların doğrulamasının yapılması. (hash karşılaştırması)



### 3. ADIM - KORELASYON

- ❖ KORELASYON içinde kullanılacak senaryoların belirlenmesi.
- ❖ Senaryo içinde kullanılacak korelasyon deęişkenlerinin sistem için uygunluk kontrolü.
- ❖ Senaryolarda kullanılacak logların ve log içindeki parametrelerin tespiti.
- ❖ İlgili korelasyon kuralının oluşturulması.
- ❖ Korelasyon kuralının testi ve devreye alınması.



### 3. ADIM - SENARYOLAR

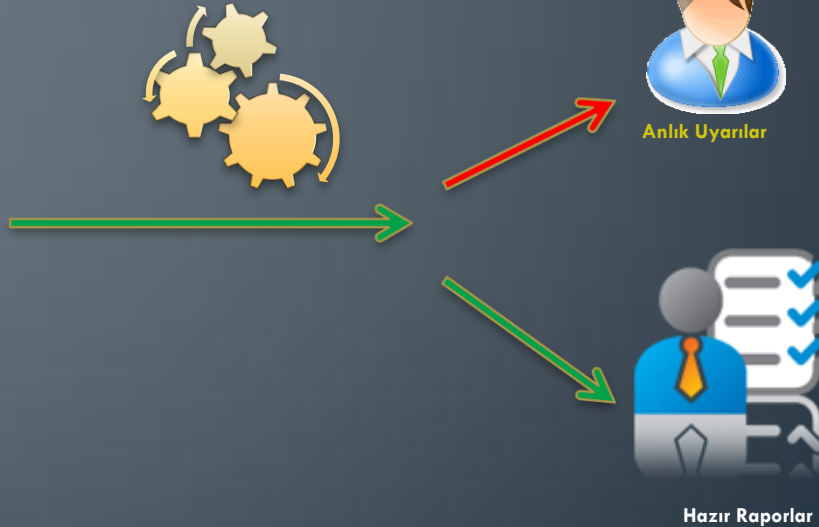
- ❖ Kapıdan girmeyen sistem yöneticilerinin konsoldan bağlantı kurmasının tespiti (Kapı Geçiş Sistemi ve İşletim Sistemi Logları)
- ❖ VPN erişimi ile bağlanan firma kullanıcısının veritabanı yöneticisi hakkı ile sistemlere erişiminin tespiti (Network ve Veritabanı Logları)
- ❖ Uygulamalarda işlemi kontrol eden ve işi yapan kullanıcının aynı kullanıcı olmasının tespiti (Uygulama Logları)
- ❖ Herhangi bir sisteme bruteforce atağının tespiti
- ❖ Firewall ve IDS/IPS sistemlerinde tespit edilen DoS atakları

## 4. ADIM – ALARM ve RAPOLAMA

- ❖ Korelasyon sonucunda etkilenen sistem sahiplerinin belirlenmesi.
- ❖ Alarmın iletilmesi sonrası alınacak aksiyonun belirlenmesi.
- ❖ Korelasyon kurallarına alarm yollanacak personel listesinin girilmesi.
- ❖ Alarm raporlarının periyodik olarak ilgili yöneticilere iletilmesi.



Merkezi Log Yönetimi



TEŞEKKÜRLER..