HELK (The Hunting ELK) - Kurulum ve Kullanım Rehberi

# 📊 HELK (Hunting ELK) Nedir?

HELK (The Hunting ELK), siber güvenlik analistleri için geliştirilmiş açık kaynaklı bir tehdit avcılığı ve log analiz platformudur. Elasticsearch, Logstash, Kibana, Kafka, Spark ve Jupyter gibi bileşenleri birleştirerek güçlü bir SIEM ve tehdit tespit ortamı sunar.

# 🔍 HELK Ne İşe Yarar?

Temel kullanım amaçları şunlardır:

* • Log toplama ve korelasyon
* • Tehdit avcılığı (Threat Hunting)
* • Siber güvenlik olaylarının analizi
* • IOC ve anomali tespiti
* • Görselleştirme ile saldırı izlerinin takibi

# 🧱 HELK Mimarisi

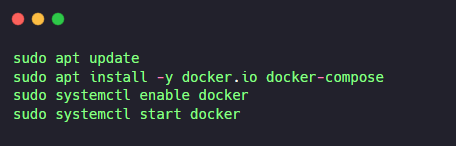
HELK; log kaynaklarından gelen verileri Kafka üzerinden alır, Logstash ile işler, Elasticsearch’e kaydeder ve Kibana ile görselleştirir. Ek olarak Jupyter Notebook üzerinden analiz yapılabilir.

# 🖥️ Kali Linux Üzerinde HELK Kurulumu

💡 Minimum sistem gereksinimleri: 4 CPU, 16 GB RAM, 50+ GB disk alanı.

## 1. Docker ve Docker Compose Kurulumu

sudo apt update  
sudo apt install -y docker.io docker-compose  
sudo systemctl enable docker  
sudo systemctl start docker



## 2. HELK Kaynak Kodunu İndirin

git clone https://github.com/Cyb3rWard0g/HELK.git  
cd HELK

ekran görüntüsü, metin, yazı tipi, grafik içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

## 3. HELK’i Başlatın

sudo ./helk\_install.sh

ekran görüntüsü, grafik, yazı tipi, grafik tasarım içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

## 4. Portlar ve Erişim Bilgileri

Kibana: http://localhost:5601  
Elasticsearch: http://localhost:9200  
Kafka: localhost:9092

## 5. Sysmon Logları Gönderme (Opsiyonel)

Windows üzerinden Sysmon + Winlogbeat kullanarak Kafka’ya log gönderilebilir. Örnek Çıktı:

metin, ekran görüntüsü içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

# 🧠 Kullanım Senaryoları

HELK ile yapılabilecek bazı işlemler:

* • Sysmon loglarını analiz etme
* • Anormal davranışları tespit etme
* • MITRE ATT&CK haritalaması yapma
* • Jupyter üzerinden log sorguları gerçekleştirme

# 🎯 Avantajları

* • Tamamen açık kaynak
* • MITRE ATT&CK uyumlu tehdit analizi
* • Sysmon ve Winlogbeat ile uyumlu
* • Gelişmiş görselleştirme ve log sorgulama