**Helk (Hunting ELK) Nedir?**

**HELK (Hunting ELK)**, tehdit avcılığı (threat hunting), güvenlik analizi ve olay müdahalesi süreçlerini kolaylaştırmak için tasarlanmış açık kaynaklı bir siber güvenlik platformudur. Temel olarak Elastic Stack (Elasticsearch, Logstash, Kibana) altyapısını kullanır, fakat siber güvenlik uzmanları için özel olarak yapılandırılmış, özelleştirilmiş ve genişletilmiştir. Sızma testi ve tehdit avı faaliyetlerinde oldukça faydalıdır.

HELK, verilerin toplanması, analiz edilmesi, korelasyonu ve görselleştirilmesi için kapsamlı bir çerçeve sunar. Bu yönüyle hem mavi takım (savunma) hem de kırmızı takım (saldırı) faaliyetlerinde kullanılabilir.

**HELK’in Temel Özellikleri**

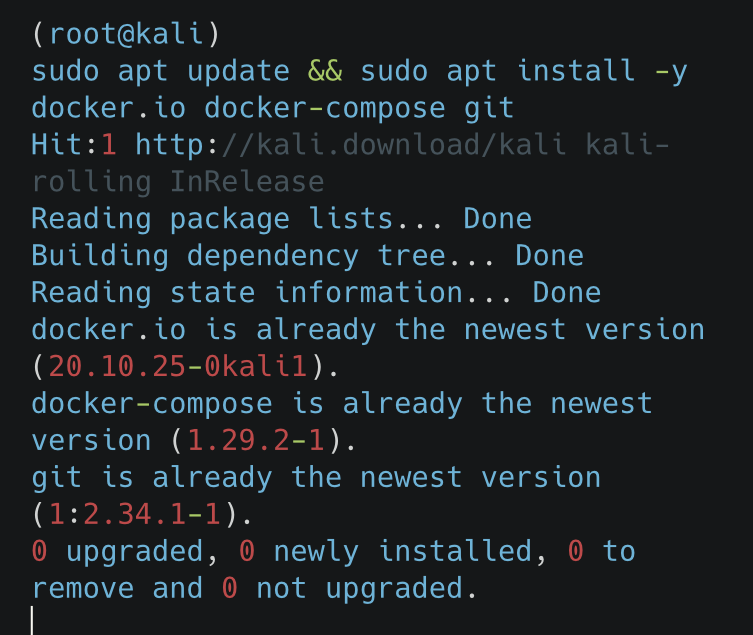
1. **Elastic Stack Entegrasyonu**: Elasticsearch, Logstash ve Kibana gibi bileşenleri temel alır.
2. **Sigma Kural Desteği**: Açık kaynaklı tehdit algılama kural dili olan Sigma ile entegrasyonu sayesinde olayları anlamlı hale getirir.
3. **Kafka Entegrasyonu**: Yüksek hacimli veri akışları için Kafka desteği sunar.
4. **Jupyter Notebook Desteği**: Analitik ve tehdit avcılığı için Python tabanlı veri analizine olanak tanır.
5. **Kolay Kurulum**: Docker ve Docker-Compose ile kolayca kurulabilir.
6. **Sysmon Desteği**: Windows sistemlerinden gelen detaylı olayları analiz etmek için Sysmon verilerini işler.
7. **MITRE ATT&CK Entegrasyonu**: Tehdit aktörlerinin davranışlarını analiz etmek için ATT&CK çerçevesi ile eşleşme yapar.

**HELK Kullanım Alanları**

* Tehdit Avcılığı (Threat Hunting)
* Güvenlik Bilgi ve Olay Yönetimi (SIEM)
* Sızma Testi ve Olay Müdahalesi
* Anomali Tespiti ve Davranış Analizi
* Siber Güvenlik Eğitimi ve Simülasyonlar

**HELK Nasıl Kurulur? (Örnek Komutlar)**

Helk’in kurulumu Docker üzerinde gerçekleştirilir. Aşağıdaki adımlar ile temel kurulumu yapabilirsiniz:



metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.Bu çıktı, gerekli paketlerin zaten sistemde yüklü olduğunu gösterir. Eğer yüklü değilse, sistem onları indirip kuracaktır.

Ardından cd HELK komutu ile dizin içine giriyoruz.

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

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

Son Olarak Kurulumu Başlatıyoruz:

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

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**Avantajları**

* ✅ **Açık kaynaklı ve ücretsizdir.**
* ✅ **Tehdit avcılığı için özel olarak yapılandırılmıştır.**
* ✅ **Kapsamlı log toplama ve analiz altyapısı sunar.**
* ✅ **Sigma ve MITRE ATT&CK gibi endüstri standartları ile entegredir.**
* ✅ **Geniş kullanıcı topluluğu ve destek dökümantasyonuna sahiptir.**
* ✅ **Docker tabanlı yapısı sayesinde esnek ve taşınabilirdir.**
* ✅ **Jupyter Notebook desteği ile ileri düzey veri analizi yapılabilir.**

**Dezavantajları / Zorluklar**

* ❌ İlk kurulum ve yapılandırma yeni başlayanlar için karmaşık olabilir.
* ❌ Yüksek kaynak tüketimi nedeniyle güçlü donanımlarda daha verimli çalışır.
* ❌ Öğrenme eğrisi dik olabilir (özellikle ELK ve Kafka’ya yabancı kullanıcılar için).

**Kimler Kullanmalı?**

* Siber güvenlik analistleri
* Tehdit avcıları (threat hunters)
* Mavi takım ve sızma testi ekipleri
* Güvenlik operasyon merkezi (SOC) çalışanları
* Siber güvenlik eğitmenleri ve öğrenciler