**Falco Nedir?**

**Falco**, CNCF (Cloud Native Computing Foundation) tarafından desteklenen, açık kaynak kodlu bir **Linux run-time security** (çalışma zamanı güvenliği) aracıdır. Sistem çağrılarını izleyerek (syscall), güvenlik politikalarına aykırı davranışları tespit eder ve uyarı üretir.

**📌 Kısaca:**

* **Gerçek zamanlı** olarak sistem olaylarını dinler
* Davranış temelli saldırıları veya beklenmedik hareketleri algılar
* Linux sistem çağrılarını (syscalls) denetler
* Kubernetes, Docker ve konteyner ortamlarında özellikle güçlüdür
* **Falco Özellikleri**

| **Özellik** | **Açıklama** |
| --- | --- |
| 🕵️ Gerçek Zamanlı İzleme | Çalışan işlemleri ve sistem çağrılarını canlı izler |
| 🔒 Güvenlik Politikaları | Kendi yazabileceğin veya hazır kurallar ile ihlalleri tanımlar |
| 🐳 Konteyner Uyumlu | Docker/Kubernetes sistemleri için optimize edilmiştir |
| 📢 Uyarı Üretme | Syslog, stdout, HTTP, JSON, webhook gibi birçok kanaldan log üretir |
| 🔧 Özelleştirilebilir Kurallar | YAML tabanlı kurallar kolayca düzenlenebilir |

**Falco Ne Zaman Kullanılır?**

* Bir saldırganın root yetkisiyle sistemde işlem yaptığını tespit etmek
* Konteyner içinde şüpheli komutların çalıştırıldığını izlemek
* Dosya sistemi, ağ ve kullanıcı hareketlerini denetlemek
* Anormal davranışların (örn. bash içinde exec komutu, ssh key ekleme vb.) algılanması

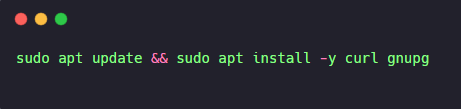
**Falco’nun İzlediği Bazı Davranış Örnekleri:**

* /etc/shadow dosyasının okunması
* Kabuk (bash, zsh) açılması
* chmod veya chown gibi komutların kullanılması
* Root yetkisi ile çalıştırılan beklenmedik komutlar
* Konteyner içinde paket yüklenmesi (apt, apk vb.)

Falco Kurulumu

**1. Gerekli Paketleri Kur**

Komut: sudo apt update && sudo apt install -y curl gnupg



2. Falco GPG Anahtarını ve Reposunu Ekle

Komut: curl -fsSL https://falco.org/repo/falcosecurity-packages.asc | sudo gpg --dearmor -o /usr/share/keyrings/falco-archive-keyring.gpg

echo "deb [signed-by=/usr/share/keyrings/falco-archive-keyring.gpg] https://download.falco.org/packages/deb stable main" | sudo tee /etc/apt/sources.list.d/falcosecurity.list

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

3. Falco'yu Yükle

Komut: sudo apt update && sudo apt install -y falco

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

4. Hizmeti Başlat

Komut: sudo systemctl start falco

sudo systemctl enable falco

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

5. Falco’yu Test Et

Komut: cat /etc/shadow

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

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**📁 Falco Log Dosyası:**

Falco log'ları genellikle şurada bulunur:

/var/log/falco.log

**⚙️ Falco Kurallarını Düzenleme**

Kurallar /etc/falco/falco\_rules.yaml dosyasında tanımlıdır.

Örnek bir kural:

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

Falco Aracı Nasıl Kullanılır?

Temel Kullanım Komutları

Servisin Başlatılması – Komut: sudo systemctl start falco

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

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

Servisin Durumunu Kontrol Etme - Komut: sudo systemctl status falco

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

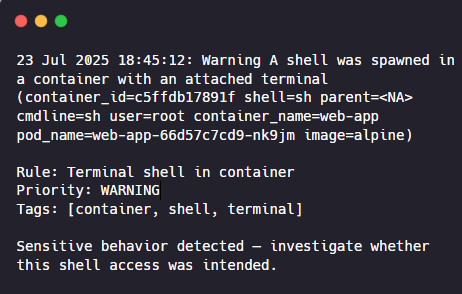
Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

Logları Görüntüleme – Komut: sudo tail -f /var/log/falco.log

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

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**Falco Örnek Log Çıktısı**

****