Falco Aracı - Eğitim Materyali

# 🧠 Falco Nedir?

**Falco**, konteyner (örneğin Docker) ve Linux sistemlerinde çalışan davranışları gerçek zamanlı olarak izleyen bir **açık kaynaklı tehdit tespit aracıdır**. CNCF (Cloud Native Computing Foundation) desteklidir.

# 🚀 Özellikleri

🔍 Gerçek zamanlı sistem çağrısı denetimi yapar.

🐳 Kubernetes ve Docker ortamlarıyla uyumludur.

📜 Özel kurallarla şüpheli davranışları tanımlayabilir.

🧠 Anormal davranışları loglar veya uyarı verir.

# 🎯 Kullanım Alanları

Linux sistem güvenliği izleme,

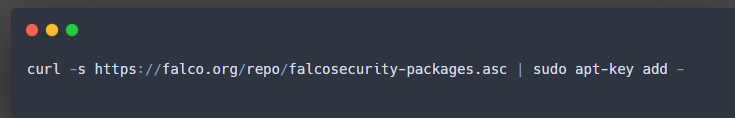
Bulut ortamlarında tehdit tespiti,

Siber güvenlik eğitimlerinde davranış analiz çalışmaları.

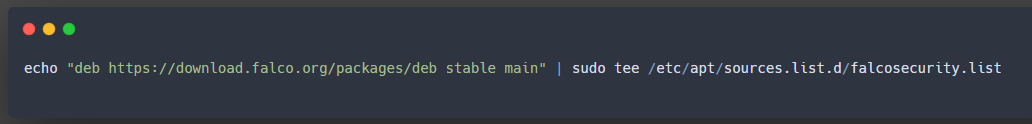
# 🛠️ Kurulum

Falco genellikle bulut ve sunucu ortamlarında tercih edilir. Kali'de temel kurulum şöyledir:

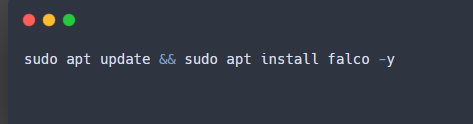
1.Kurulum için GPG anahtarı ve depo ekle:



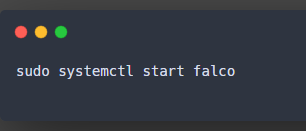
2. Paket deposunu ekleyin:



# 3. Güncelle ve kur:



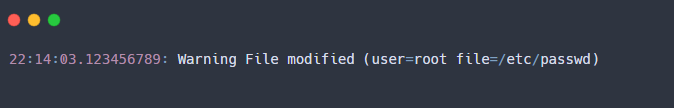
4. Başlat:



# 🧪 Örnek Kullanım

Falco çalışırken sistem çağrılarını izler. Örneğin, biri /etc/passwd dosyasını düzenlemeye çalışırsa uyarı verir:

Log Örneği:



# 📎 Notlar

Gerçek zamanlı tespit sistemi sayesinde olayları anında bildirir.

Sunucu güvenliğinde ve siber savunma eğitimlerinde çok değerlidir.

Etik amaçlı izleme sistemidir; casusluk için değil.