**FALCO**

**1. Nedir?**

**Falco**, **bulut sistemlerinde ve Linux tabanlı sunucularda çalışan bir davranış izleme (behavior monitoring) ve tehdit algılama sistemidir.**

Kubernetes, Docker gibi modern sistemlerde şüpheli olayları tespit etmek için kullanılır.  
CNCF (Cloud Native Computing Foundation) tarafından desteklenen açık kaynak bir projedir.

Basitçe: **Bilgisayarda neler olup bittiğini takip eder ve “şüpheli hareket” gördüğünde seni uyarır.**

**2. Ne İşe Yarar?**

Falco’nun başlıca görevleri:

* Dosya, ağ veya sistem çağrısı (syscall) gibi davranışları izler.
* Şüpheli veya anormal hareketleri (örn. passwd dosyasını izinsiz değiştirme) tespit eder.
* Gerçek zamanlı uyarılar üretir (log, e-posta, webhook vs.).

**Örnek:** Bir saldırgan root dizinine garip bir betik koymaya çalışırsa, Falco seni uyarır! 🚨

**3. Neden Önemlidir?**

* **Canlı İzleme:** Sunucularda olan biteni anlık takip eder.
* **Konteyner Desteği:** Docker, Kubernetes gibi modern sistemlerle uyumludur.
* **Geliştirilebilir Kurallar:** Ne zaman uyarı vermesi gerektiğini sen tanımlayabilirsin.
* **Açık Kaynak ve Ücretsiz:** İsteyen herkes indirip kullanabilir.

**Sistemine biri dışardan erişmeye çalışırsa, Falco seni hemen uyarır.**

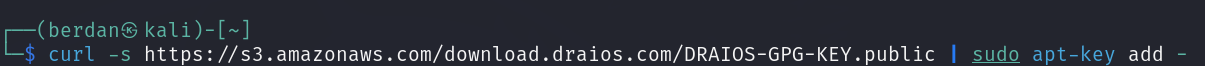
**4. Nasıl Kurulur? (Linux Üzerinden Kullanım)**

Falco, çoğunlukla Ubuntu, Debian ve CentOS gibi Linux sistemlere kolayca kurulabilir.

**Temel Kurulum (Ubuntu Örneği):**

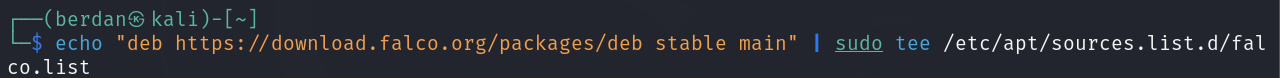
1. Falco’nun GPG anahtarını ve depolarını ekle:

**curl -s https://s3.amazonaws.com/download.draios.com/DRAIOS-GPG-KEY.public | sudo apt-key add –**

****

1. Repo'yu ekle:

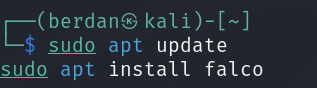
**echo "deb https://download.falco.org/packages/deb stable main" | sudo tee /etc/apt/sources.list.d/falco.list**

****

1. Kurulum:

**sudo apt update**

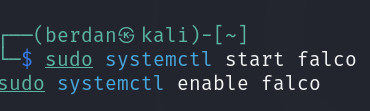
**sudo apt install falco**

****

1. Falco’yu başlat:

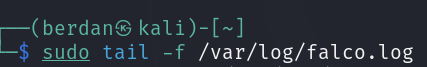
**sudo systemctl start falco**

**sudo systemctl enable falco**

****

1. Falco artık çalışıyor!   
   Logları şuradan görebilirsin:

**sudo tail -f /var/log/falco.log**



**5. Örnek Bir Anlatım (Senaryo):**

**Senaryo: Güvenlik Kulübü'nün Linux Sunucusu Tehlikede!**

Yusuf, lisede bilişim laboratuvarında Linux sunucularını kurmuş ve herkese SSH ile erişim vermiştir. Bir gün CPU kullanımı artar, sistem yavaşlar.

Yusuf, sisteme **Falco** kurar.

* Falco loglara bakar ve “root yetkisi ile kabuk açma girişimi” olduğunu bildirir.
* Ayrıca /etc/passwd dosyasına gece 3’te izinsiz erişildiğini fark eder.
* Yusuf hemen kullanıcıları kontrol eder ve yetkisiz giriş yapan kişiyi tespit eder.
* Bu kişi sistemden uzaklaştırılır ve sistem tekrar güvenli hale gelir.

**Sonuç:** Falco sayesinde Yusuf, saldırıyı erken tespit eder ve sistemi kurtarır. 🛡️