Syft Aracı - Eğitim Materyali

# 🧠 Syft Nedir?

Syft, yazılım bileşenlerinin envanterini (Software Bill of Materials - SBOM) oluşturmak için kullanılan açık kaynaklı bir araçtır. Konteyner görüntüleri, dosya sistemleri veya kaynak kodlar üzerinde çalışarak bileşenleri listeler. Güvenlik, uyumluluk ve yazılım izlenebilirliği açısından kritik bir rol oynar.

# 🚀 Özellikleri

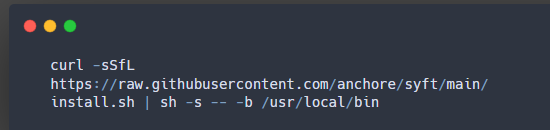
- Docker/OCI container image analizleri  
- Yerel dosya sisteminden SBOM oluşturma  
- CycloneDX, SPDX, JSON, Table gibi çıktı formatları  
- Paket yöneticilerini (apt, yum, pip, npm vb.) otomatik tanıma  
- CLI ile entegre çalışabilme

# 🎯 Kullanım Alanları

- Yazılım bileşenlerini listeleyerek güvenlik denetimi yapmak  
- Açık kaynak lisans kontrolleri ve uyumluluk  
- CI/CD hatlarında SBOM üretimi  
- Konteyner içeriği şeffaflığı ve güvenlik açığı tespiti

# 🛠️ Kurulum

1. Syft'i yüklemek için terminalde şu komutu çalıştırın:

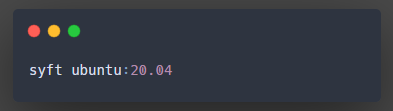
******

2. Kurulumun başarılı olduğunu doğrulamak için:

# 

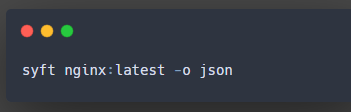
# 🧪 Örnek Komutlar ve Açıklamaları

✅ Docker Görüntüsünden SBOM Oluşturma:

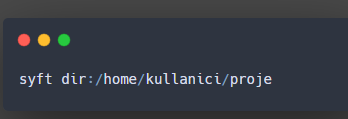
******

→ ubuntu:20.04 imajı içindeki paketleri listeler.

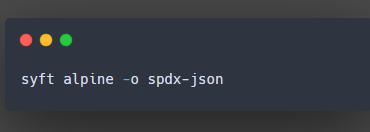
✅ Çıktıyı JSON Formatında Alma:

******

✅ Yerel Dosya Sistemini Tara:

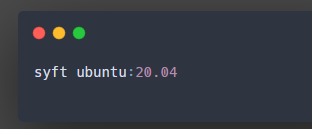
******

✅ SPDX Formatında SBOM:

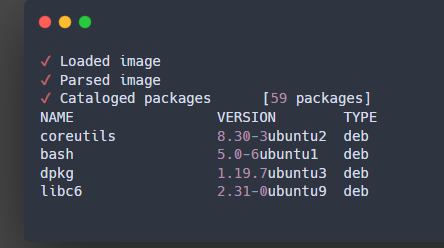
**

**✅ 1. Docker İmajı Taraması**

**Komut:**



Örnek Çıktı:

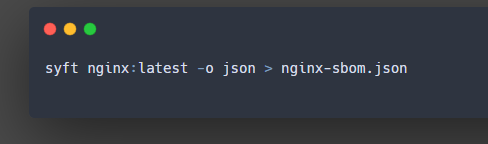


📌 Açıklama:

* ubuntu:20.04 imajındaki tüm sistem paketleri listelenmiştir.
* TYPE kısmı, paketin hangi türden (örneğin debian paketi) olduğunu gösterir.

**✅ 2. JSON Formatında SBOM Üretmek**

**Komut:**



Örnek JSON Çıktıdan Parça:

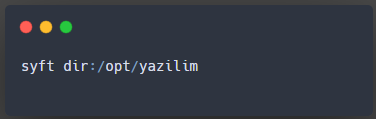


📌 Açıklama:

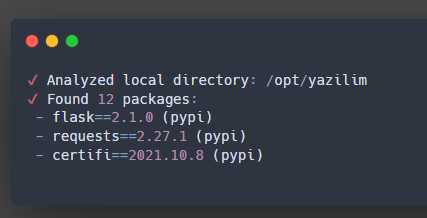
* JSON formatında SBOM çıktısı alınır.
* CI/CD hatlarında veya SBOM doğrulama sistemlerinde kullanılabilir.

**✅ 3. Yerel Dosya Sisteminde Paket Taraması**

**Komut:**



Örnek Çıktı:

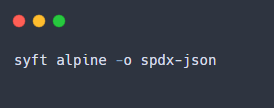


📌 Açıklama:

* Belirtilen dizinde Python modülleri taranmıştır.
* Özellikle sanal ortamlar (venv) veya proje kök dizinleri için kullanılır.

**✅ 4. SPDX JSON Formatında Rapor Alma**

**Komut:**



Çıktıdan Parça:



📌 Açıklama:

* SPDX standardına uygun bir SBOM çıktısıdır.
* Uyumluluk, lisans analizi ve denetimler için kullanılır.

# 📎 Notlar

- Syft, Anchore ekibi tarafından geliştirilmiştir.  
- SBOM çıktısı diğer araçlar (Grype, Trivy, vs.) ile birlikte kullanılabilir.  
- CI/CD süreçlerine kolayca entegre edilebilir.  
- SBOM çıktısı lisans denetimi ve güvenlik açığı taraması için kullanılabilir.