**🧠 1. Nedir?**

**🔹 Vector**

* Open-source bir **log toplama ve yönlendirme aracıdır**.
* Sistem günlüklerini (syslog, journald, nginx logları, vs.) toplayarak bir hedefe iletir (örneğin: Loki, Elasticsearch, Kafka vs.).
* Lightweight (hafif), hızlı ve konfigürasyonu basittir.

**🔹 Loki Stack (Grafana Loki + Promtail + Grafana)**

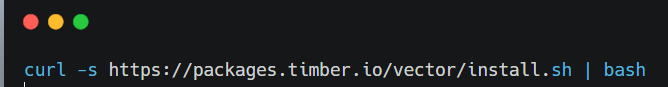
* **Grafana Loki**, log'ları zaman serisi halinde saklayan bir log veritabanıdır (Prometheus'un log versiyonu gibi düşünebilirsin).
* **Promtail**, logları toplar ve Loki’ye iletir.
* **Grafana**, Loki üzerinden log'ları görselleştirir.

**🎯 2. Ne İşe Yarar?**

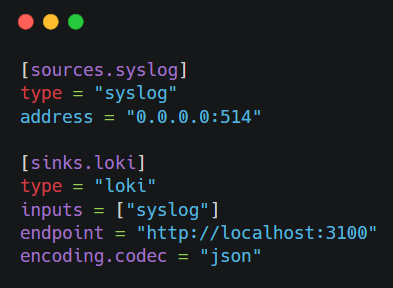
| **Bileşen** | **İşlev** |
| --- | --- |
| 🌀 **Vector** | Log'ları gerçek zamanlı toplar ve yönlendirir |
| 📥 **Loki** | Log'ları zaman serisi olarak saklar |
| 🖼️ **Grafana** | Log’ların analiz ve görselleştirmesini sağlar |
| 🔁 **Promtail** | Alternatif log toplayıcı (Vector yerine de kullanılabilir) |

**⚙️ 3. Kurulum – Vector (Kali/Debian)**

**✅ Vector’i indir ve kur:**



**✅ Konfigürasyon dosyası (örnek: /etc/vector/vector.toml):**



**✅ Vector’i başlat:**

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

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**⚙️ 4. Kurulum – Loki + Grafana (Docker ile)**

**✅ Docker Compose (örnek docker-compose.yml):**

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**✅ Servisleri başlat:**

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

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**🌐 5. Grafana Web Arayüzü**

* Erişim: <http://localhost:3000>
* Kullanıcı adı/şifre: admin / admin
* Veri kaynağı olarak **Loki** eklenir:
  + URL: http://localhost:3100
  + Type: *Loki*

**📋 6. Örnek Log Gösterimi (Grafana)**

{job="vector"} |= "error"

Bu ifade, “vector” kaynaklı tüm hata loglarını filtreler.

**📊 7. Vector vs Promtail**

| **Özellik** | **Vector** | **Promtail** |
| --- | --- | --- |
| Dil | Rust | Go |
| Performans | Çok hızlı (yüksek throughput) | İyi (Loki uyumlu) |
| Destek | Birçok hedef (Kafka, S3, etc.) | Yalnızca Loki |
| Gelişmiş yönlendirme | ✔ | ✖ |

**🧠 8. Kullanım Senaryoları**

* 🛡️ SIEM kurulumu öncesi log toplama çözümü
* 📈 Uygulama ve sunucu loglarının merkezi toplanması
* 🧪 Güvenlik ihlali araştırmalarında log analiz altyapısı
* 🔍 Linux makinelerde hata tespiti (kernel, ssh, nginx logları)
* 🎯 Red/Blue Team çalışmaları için log takibi

**🎯 9. Öğrenim Kazanımları**

* Modern log toplama çözümlerinin nasıl çalıştığını öğrenme
* Vector ile özelleştirilmiş log yönlendirme yapma
* Loki + Grafana ile zaman serisi log analizi yapma
* SIEM öncesi hafif ve esnek log altyapısı oluşturma deneyimi kazanma