**🧠 INTELMQ – TEHDİT İSTİHBARATI OTOMASYON ARACI**

**🔍 1. Intelmq Nedir?**

**Intelmq**, tehdit istihbarat verilerini **toplamak, sınıflandırmak, filtrelemek ve dağıtmak** için geliştirilen **modüler ve otomatik bir sistemdir**.

* CERT/CSIRT ekiplerinin daha hızlı ve verimli olay yanıtı vermesini sağlar
* Python ile yazılmıştır, modüler **"bot"** yapısı sayesinde özelleştirilebilir
* IOC (Indicator of Compromise) akışlarını işler: IP, domain, hash, saldırı logları...

**🔧 2. Temel Bileşenler (Bot Türleri)**

| **Bot Türü** | **Görevi** |
| --- | --- |
| 📨 **Collector** | Tehdit verilerini dış kaynaklardan alır (feeds, logs vs.) |
| 🧠 **Parser** | Alınan verileri ayrıştırır, IOC’leri çıkarır |
| 🧹 **Expert** | Kurallar uygular, veriyi filtreler/sınıflandırır |
| 🚚 **Output** | İşlenmiş verileri SIEM, Elasticsearch, E-Mail gibi hedefe gönderir |

Her bot kendi görevini yapar ve veriler sırayla geçer.

**📦 3. Kullanım Amaçları**

| **Amaç** | **Açıklama** |
| --- | --- |
| 📡 Otomatik feed çekme | Abuse.ch, CIRCL, MISP gibi kaynaklardan tehdit verisi almak |
| 🧪 IOC (IP, domain, hash) işleme | Her bir feed içeriğinden zararlı göstergeleri ayıklamak |
| 📬 Raporlama | Anlık, günlük ya da anomali temelli uyarılar göndermek |
| 🔁 SIEM/Log entegrasyonu | Olayları SIEM’e göndermek (Elastic, Splunk, Graylog...) |

**⚙️ 4. Kurulum (Debian/Kali Linux)**

**✅ 1. Bağımlılıkları yükle**

sudo apt update

sudo apt install intelmq intelmq-manager intelmq-api redis-server

**✅ 2. Hizmetleri başlat**

sudo systemctl start redis-server

sudo systemctl enable redis-server

**✅ 3. Intelmq konfigürasyon dizinine geç**

cd /opt/intelmq/

sudo intelmqctl setup

**🌐 5. Intelmq Manager (Web Arayüzü)**

**Web arayüzü üzerinden bot yönetimi yapılabilir:**

* Arayüz: <http://localhost:8000>
* Özellikler:
  + Bot ekleme/kaldırma
  + Akış diyagramı (pipeline) oluşturma
  + Log görüntüleme
  + Test ve simülasyon

**⚙️ 6. Komut Satırından Kullanım Örnekleri**

**🔍 Bot listesi:**

intelmqctl list bots

**🚀 Bot çalıştırma:**

intelmqctl start collector-abusech

**⏹️ Bot durdurma:**

intelmqctl stop all

**📤 Queue izleme:**

intelmqctl status

**📋 7. Örnek Çalışma Akışı**

1. **collector-abusech** → Abuse.ch feed’inden zararlı IP'leri alır
2. **parser-abusech** → Bu feed’i ayrıştırır, IOC’leri çıkarır
3. **expert-ipfilter** → Gereksiz IP'leri filtreler
4. **output-elastic** → Sonuçları Elasticsearch’e gönderir

**🖥️ 8. Örnek Terminal Çıktısı**

metin, ekran görüntüsü, yazı tipi içeren bir resim

Yapay zeka tarafından oluşturulmuş içerik yanlış olabilir.

**🎯 9. Öğrenim Kazanımları**

* Tehdit istihbaratının otomasyonu hakkında pratik bilgi edinme
* IOC akışlarını tanıma ve filtreleme mantığını öğrenme
* CSIRT süreçlerinin otomasyona nasıl bağlandığını anlama
* Feed toplama, analiz ve loglama konularında teknik tecrübe kazanma