## **AIEngine Nedir?**

**AIEngine**, gerçek zamanlı ağ trafiğini analiz eden, özelleştirilebilir, yüksek performanslı bir **yapay zekâ destekli ağ analiz ve saldırı tespit (IDS) aracıdır**.  
Açık kaynaklıdır ve C++ dilinde yazılmıştır. Hem **ağ trafiğini analiz etmek**, hem de **anormal davranışları** ve **potansiyel saldırıları** tespit etmek için kullanılır.

AIEngine, klasik imza tabanlı IDS çözümlerinin aksine, **istatistiksel öğrenme ve örüntü tanıma** teknikleri kullanarak bilinmeyen saldırıları da tespit etmeye çalışır.

## **Neden Kullanılır?**

* Gerçek zamanlı ağ trafiğini **izlemek** ve analiz etmek için,
* **Kötü amaçlı paketleri**, bilinmeyen tehditleri veya anormal davranışları fark etmek için,
* Kendi **kural tabanını oluşturmak** ve sistemin öğrenmesini sağlamak için,
* Özellikle düşük kaynakla çalışan sistemlerde **hafif bir IDS alternatifi** olarak.

AIEngine, siber güvenlik uzmanlarına, ağ güvenliği mühendislerine ve araştırmacılara ağ trafiği üzerinde daha fazla kontrol ve görünürlük sağlar.

**Kurmak için:**

* git clone https://github.com/campuscodi/AIEngine.git
* cd AIEngine
* mkdir build
* cd build
* cmake ..
* make -j4

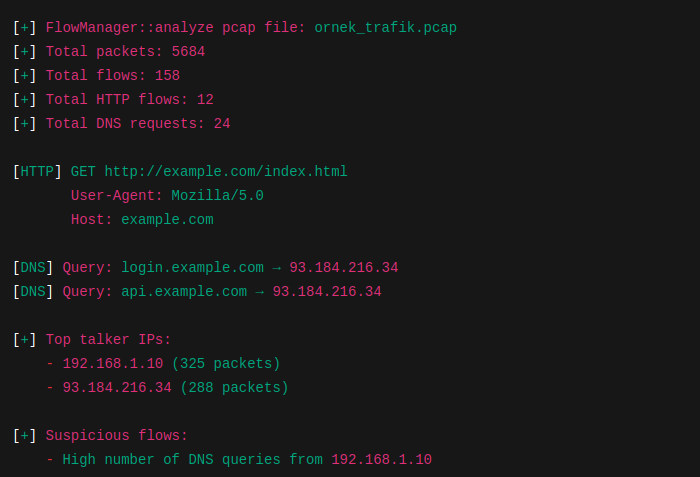
## Örnek Giriş (Input)

Bir ağ kaydı içeren .pcap dosyasını analiz etmek istiyoruz. Diyelim ki elimizde ornek\_trafik.pcap adlı bir dosya var.

* ./aiengine -r ornek\_trafik.pcap -s --http –dns

Bu komut:

* ornek\_trafik.pcap dosyasını analiz eder,
* HTTP ve DNS trafiğini inceler,
* Sonuçları ekrana (stdout) yazdırır.



## Başlıca Parametreler

* -i <interface>:  
  Canlı trafik izlemek için kullanılacak ağ arayüzünü belirtir.
* -r <file.pcap>:  
  Daha önce kaydedilmiş bir .pcap dosyasını analiz eder.
* -w:  
  Analiz sırasında hangi içeriklerin yazılacağını (örneğin DNS istekleri, IP'ler) gösterir.
* -s:  
  Sonuçları ekrana yazdırır (stdout).
* -k:  
  Kullanılan kuralları gösterir.
* --http, --dns, --ssl, --smtp:  
  Belirli protokollere özel analiz modlarını etkinleştirir.

**AIEngine**, klasik IDS sistemlerine göre daha esnek ve daha hafiftir.  
Geliştiriciler ve güvenlik analistleri için gerçek zamanlı trafik analizinde oldukça faydalıdır. Yapay zekâ ile desteklenen örüntü tanıma özellikleri sayesinde hem bilinen hem de bilinmeyen tehditleri saptamada etkilidir.