# EDS (Ensemble Defense System – Hybrid IDS with SIEM)

The Ensemble Defense System (EDS) is a hybrid security framework that integrates multiple Intrusion Detection Systems (IDS) with a Security Information and Event Management (SIEM) solution.  
  
The goal is to provide a more efficient defense against cyber threats by combining:  
- Signature-based IDS tools such as Zeek and Suricata  
- Behavior-based IDS tools such as Slips  
- Open-source SIEM (Elasticsearch & Kibana) for log management, analysis, and visualization  
  
This hybrid approach leverages the strengths of each system to achieve better accuracy, reduce false positives, and improve detection capabilities.

## Steps to Evaluate EDS

Clone this repository and unzip the files.  
Tested on Ubuntu, but feel free to experiment on other environments since the system runs in Docker containers.

cd eds -> cd EDS

Update environment variables as needed:

nano .env

After proper configuration, start the containers one by one.

### Elasticsearch

docker-compose up -d elasticsearch

docker logs -f eds-elasticsearch-1

curl -X POST --user elastic:changeme 0.0.0.0:9200/\_security/service/elastic/kibana/credential/token/token1?pretty

nano docker-compose.yml # Add the generated key in the kibana section

### Kibana

docker-compose up -d kibana

docker logs -f eds-kibana-1

### Filebeat

docker-compose build --no-cache filebeat

docker-compose up -d filebeat

docker logs -f eds-filebeat-1

### Zeek

docker-compose build --no-cache zeek

docker-compose up -d zeek

docker logs -f eds-zeek-1

### Suricata

docker-compose build --no-cache suricata

docker-compose up -d suricata

docker logs -f eds-suricata-1

Note: Custom rules have been added in the suricata folder for detecting DoS attacks, SQL injections, and privilege escalation attempts. You can also create your own rules for detecting custom attacks.

### Slips

docker-compose build --no-cache slips

docker-compose up -d slips

docker logs -f eds-slips-1