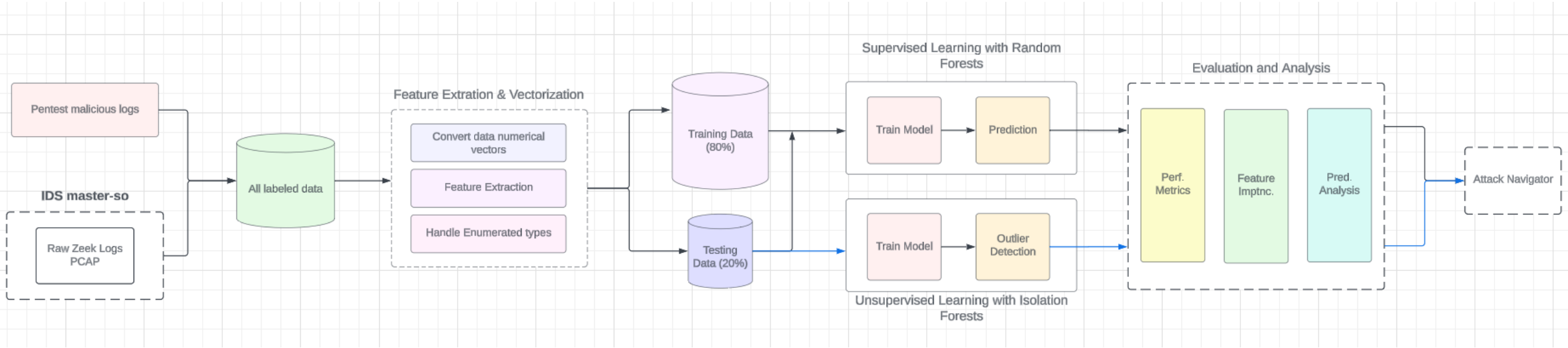
GRID-SIEM
SD GROUP 29
SPRING '24

Trent Bickford

Westin Chamberlain

Ella Cook

Daniel Ocampo


Pentest malicious logs
IDS master-so
Raw Zeek Logs
PCAP
All labeled data
Feature Extration & Vectorization
Convert data numerical vectors
Feature Extraction
Handle Enumerated types
Training Data (80%)
Testing Data (20%)
Supervised Learning with Random Forests
Train Model
Prediction
Train Model
Outlier Detection
Unsupervised Learning with Isolation Forests
Evaluation and Analysis
Perf. Metrics
Feature Imptnc.
Pred. Analysis
Attack Navigator

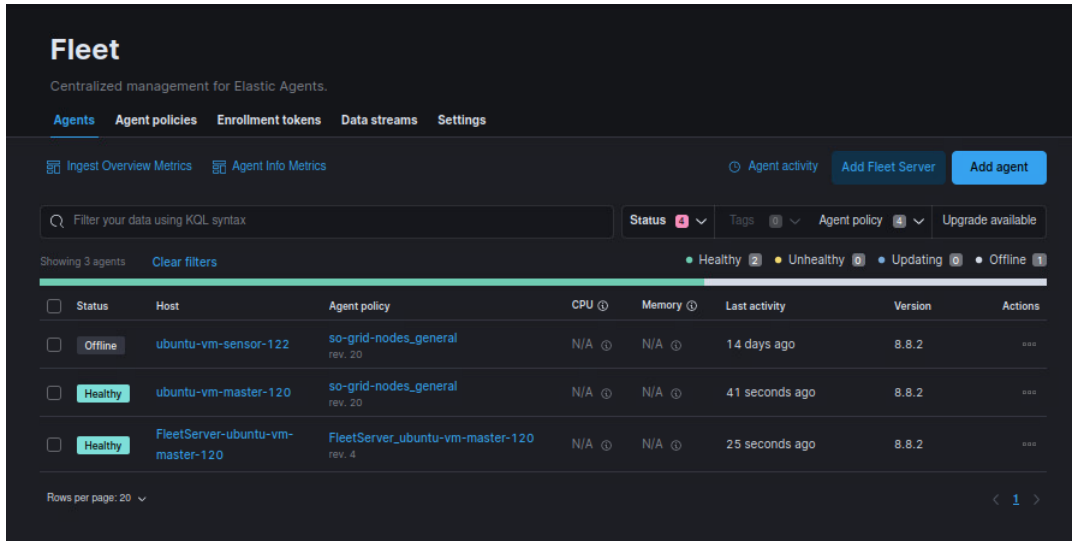
ML Graphic

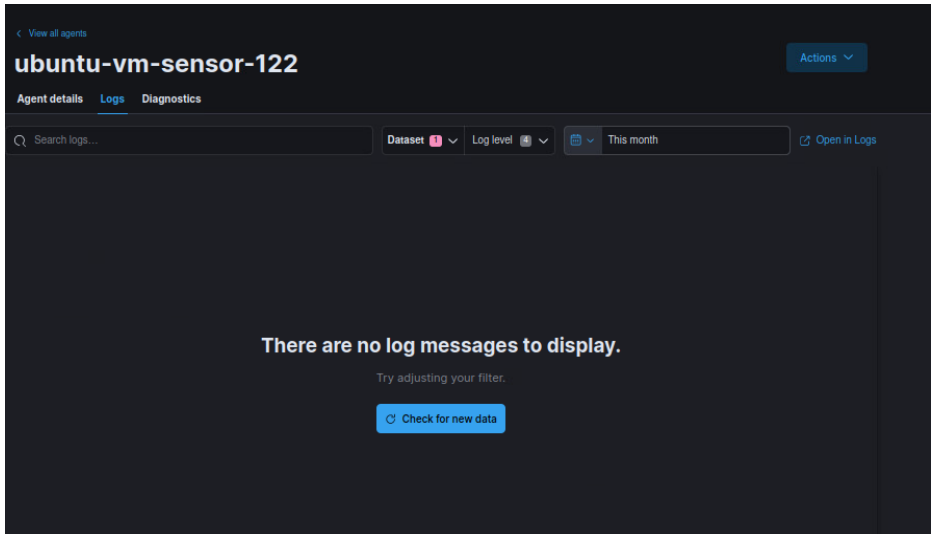
Security Onion Work

Got into the Kibana docker, but no Suricata or Zeek docker that I could find

```
kibana@kibana:~$ ls
LICENSE.txt  NOTICE.txt  README.txt  bin  config  custdashboards  dashboards
kibana@kibana:~$ ls node
LICENSE  bin  include  lib  share
kibana@kibana:~$ exit
exit
(base) ubuntu@ubuntu-vm-master-120:~$ sudo docker exec -it so-kibana bash
```

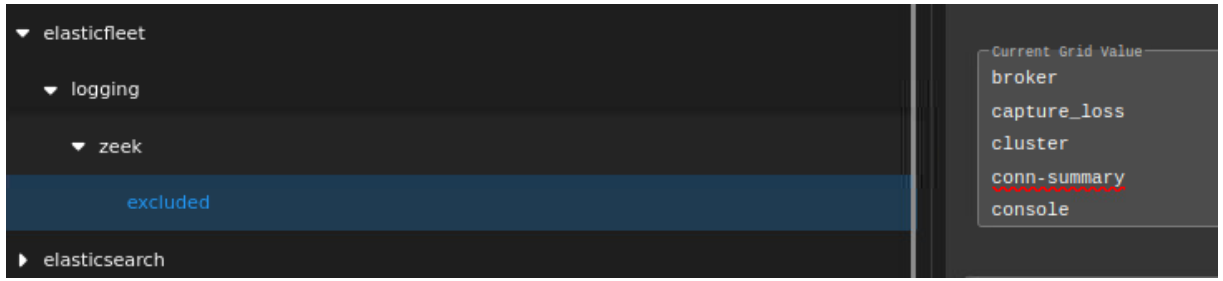
Think Elastic Fleet may be the problem, so in Kibana looked at the fleet for our environment



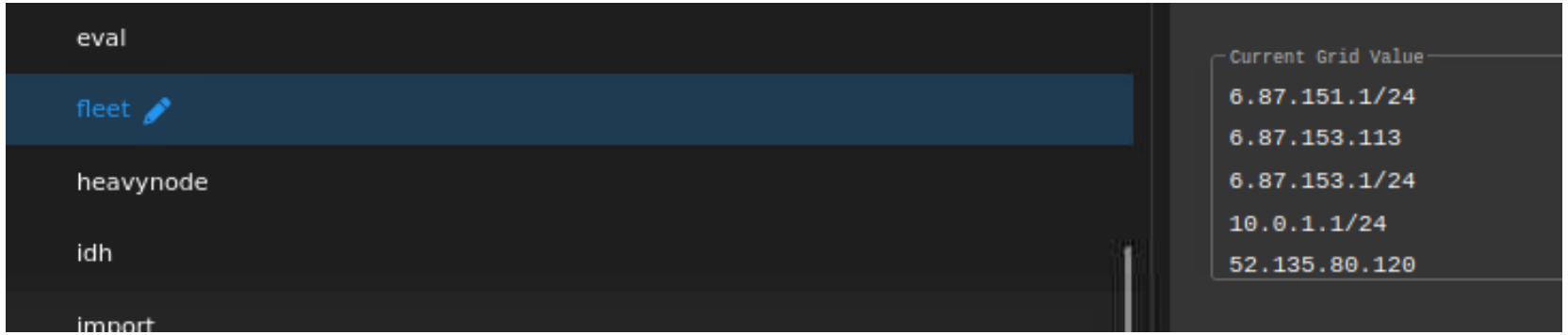


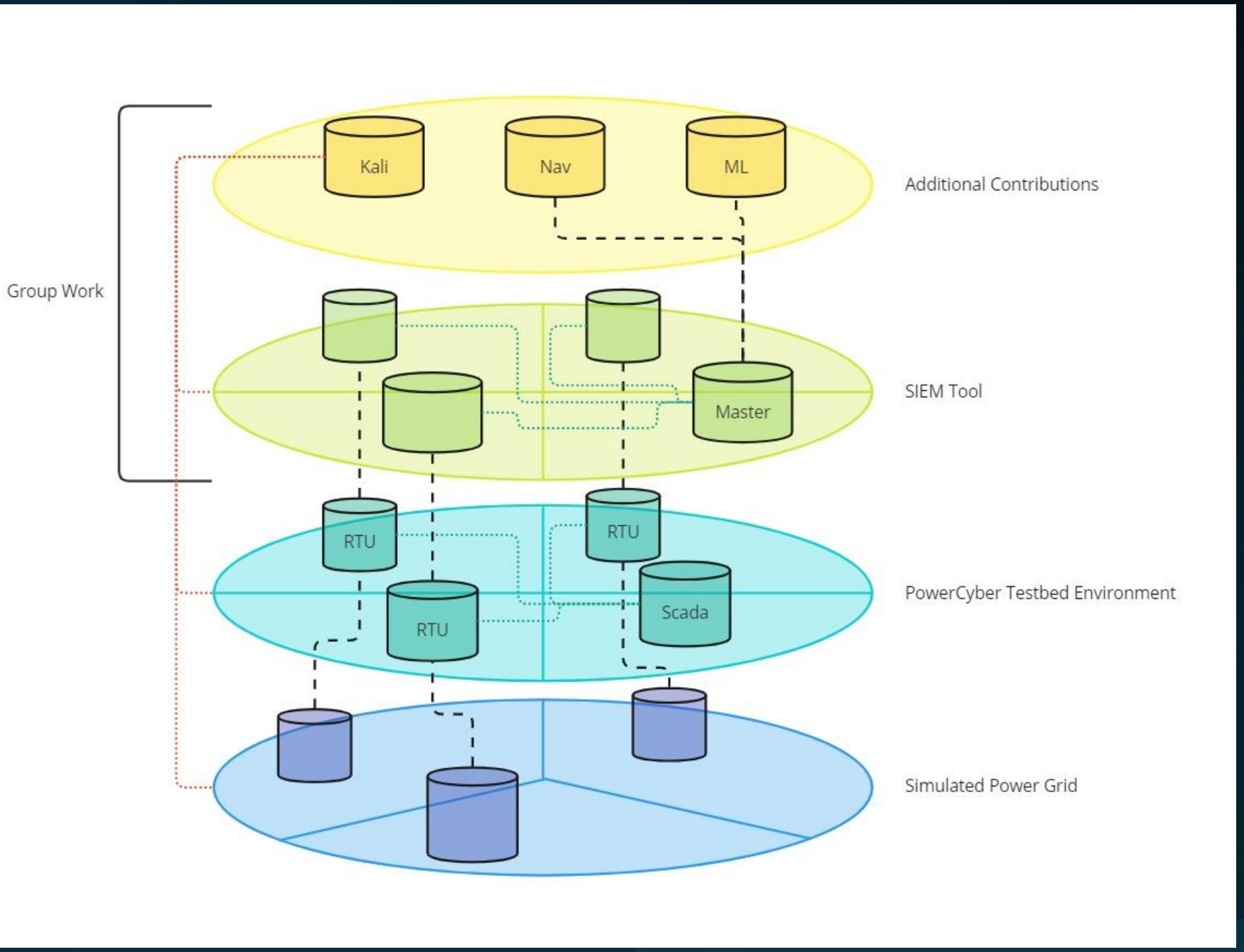
Security Onion Work

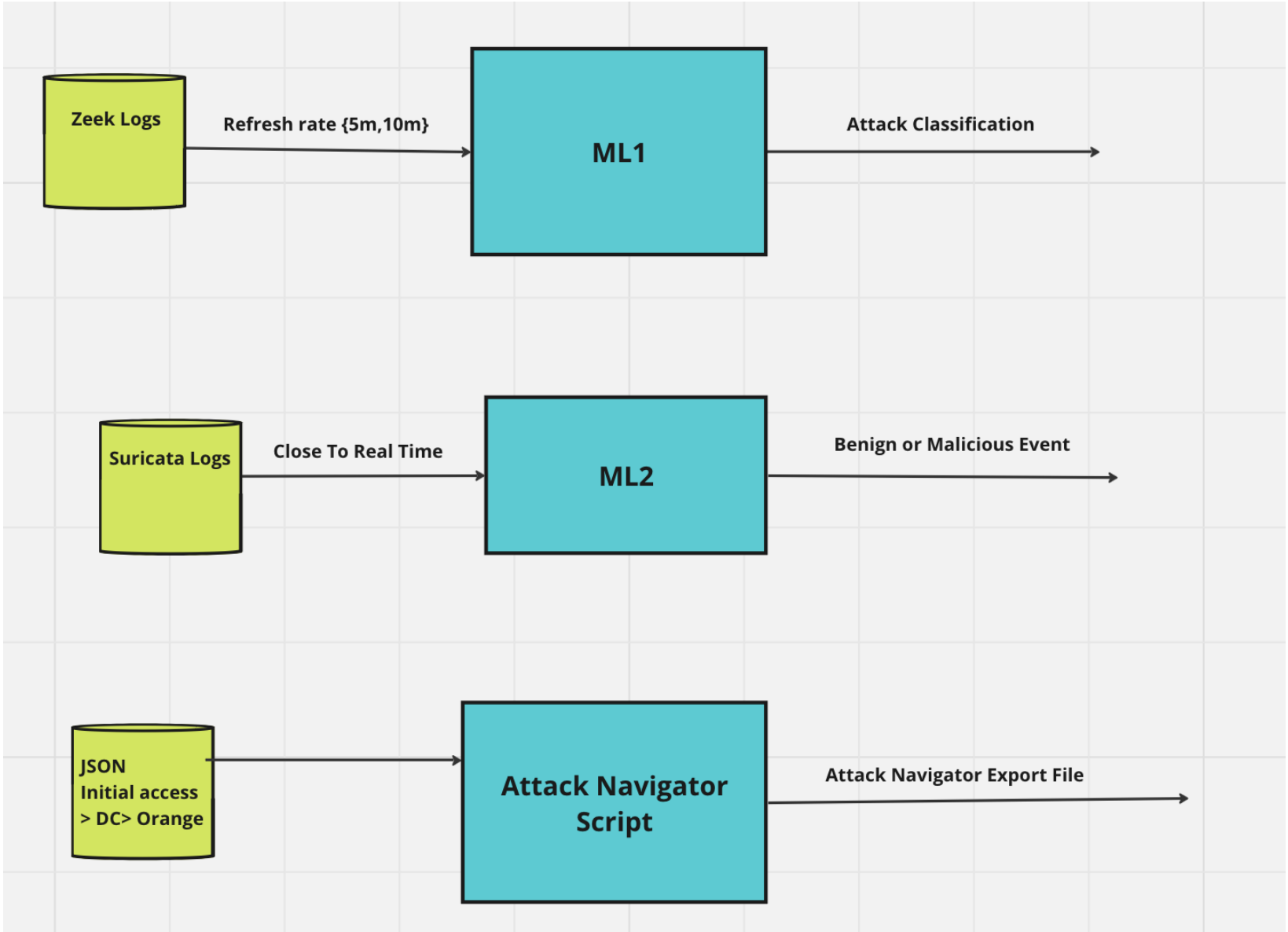
ElasticFleet removed exclusions known_hosts, known_services, conn-summary



Also added the IPs to fleet since they were not already in there




Group Work
Kali
Nav
ML
Additional Contributions
Master
SIEM Tool
RTU
RTU
RTU
Scada
PowerCyber Testbed Environment
Simulated Power Grid


Zeek Logs
Refresh rate {5m,10m}
ML1
Attack Classification
Suricata Logs
Close To Real Time
ML2
Benign or Malicious Event
JSON
Initial access
> DC> Orange
Attack Navigator
Script
Attack Navigator Export File