GRID-SIEM
SD GROUP 29
SPRING '24

Trent Bickford

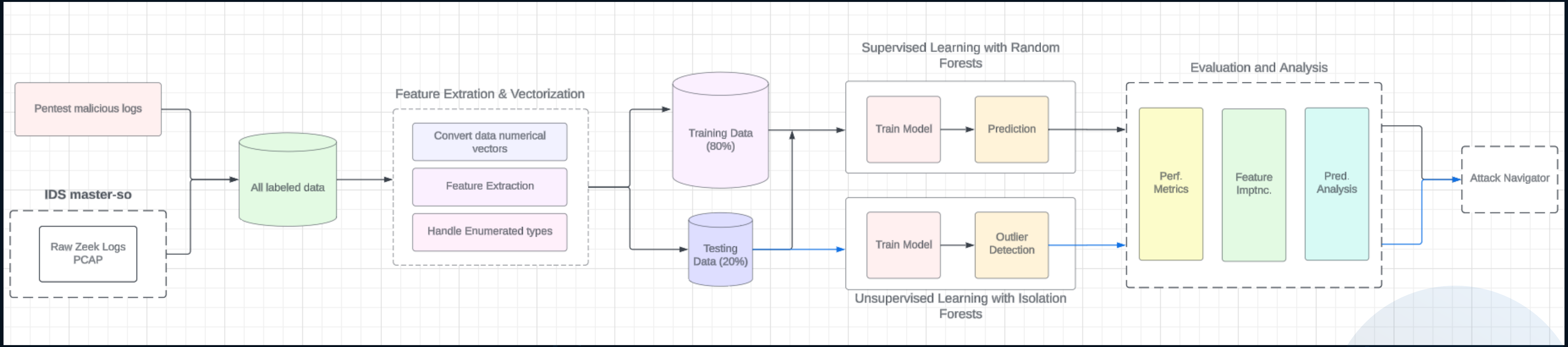
Westin Chamberlain

Ella Cook

Daniel Ocampo

ML Work

- Added a few methods to adapt the script so it can unzip and ingest multiple logs at a time
  - Trent helped with a multi-thread implementation - the logs are now unzipped efficiently
  - Still working to make the ingestion methods more efficient
    - Currently debugging and implementing chunk-based processing because of the large amount of data in each log
- Next steps
  - Finish the ingestion method
  - Check accuracy across multiple logs
  - Eventually integrate output to Navigator if time permits



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

Unsupervised Learning with Isolation Forests

Train Model

Outlier Detection

Evaluation and Analysis

Perf. Metrics

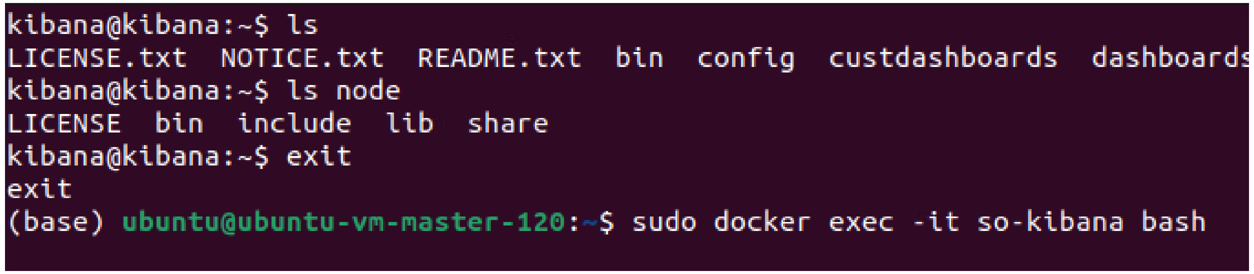
Feature Imptnc.

Pred. Analysis

Attack Navigator

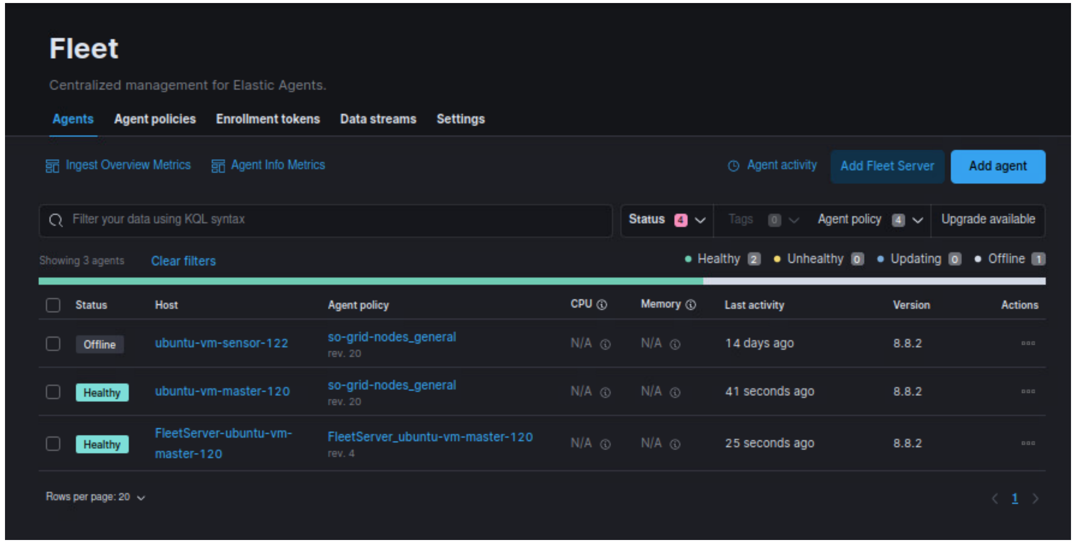
Security Onion Work

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



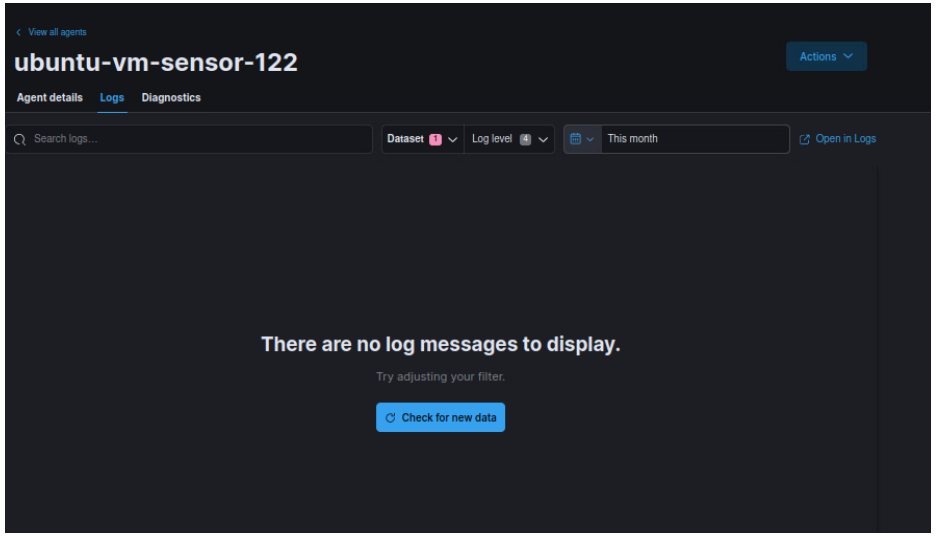
Fleet

Centralized management for Elastic Agents.

Showing 3 agents

● Healthy 2 ● Unhealthy 0 ● Updating 0 ● Offline 1

☐	Status	Host	Agent policy	CPU	Memory	Last activity	Version	Actions
☐	Offline	ubuntu-vm-sensor-122	so-grid-nodes_general rev. 20	N/A	N/A	14 days ago	8.8.2	···
☐	Healthy	ubuntu-vm-master-120	so-grid-nodes_general rev. 20	N/A	N/A	41 seconds ago	8.8.2	···
☐	Healthy	FleetServer-ubuntu-vm-master-120	FleetServer_ubuntu-vm-master-120 rev. 4	N/A	N/A	25 seconds ago	8.8.2	···



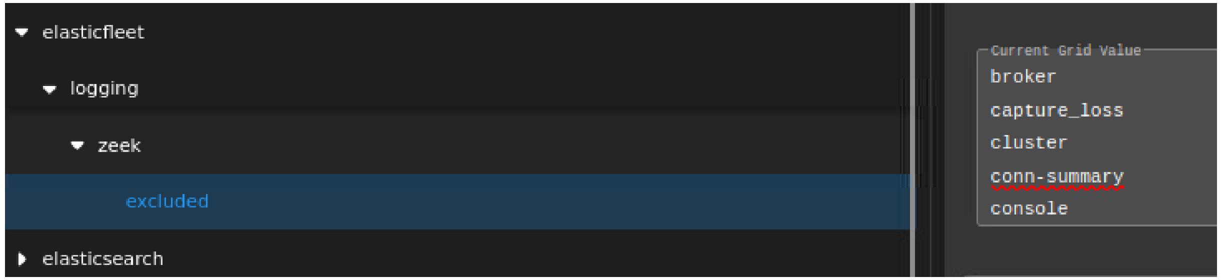
ubuntu-vm-sensor-122

There are no log messages to display.

Try adjusting your filter.

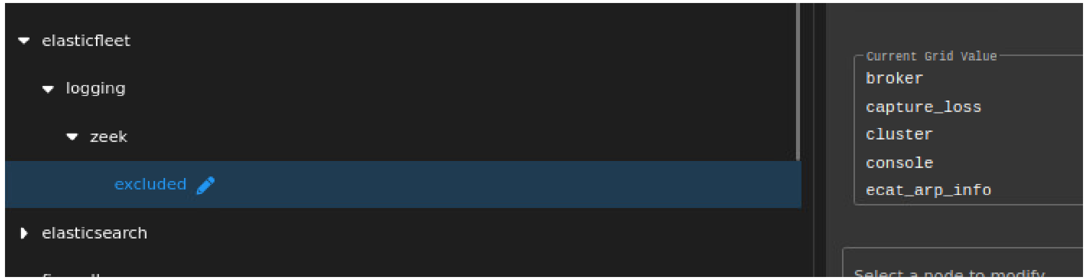
Security Onion Work

ElasticFleet removed exclusions known_hosts, known_services, conn-summary



Current Grid Value

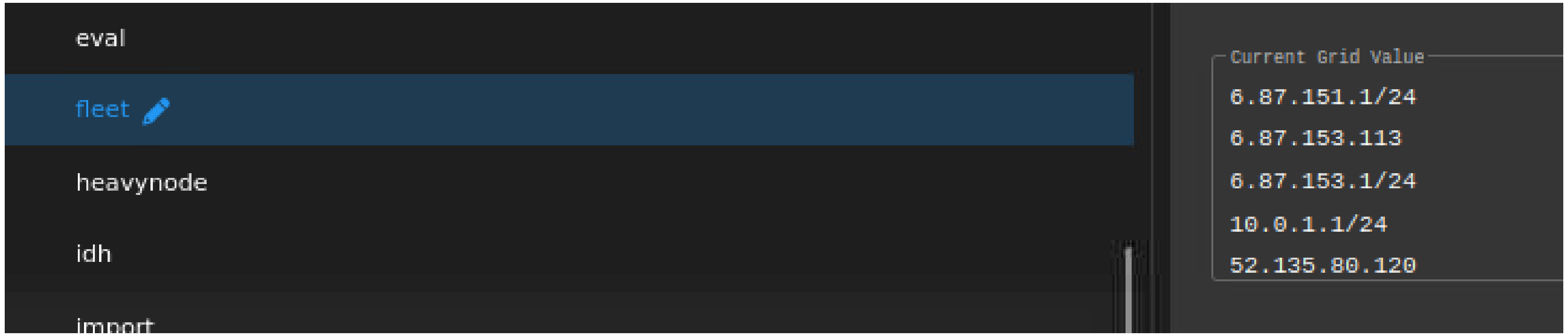
```
broker
capture_loss
cluster
conn-summary
console
```



Current Grid Value

```
broker
capture_loss
cluster
console
ecat_arp_info
```

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

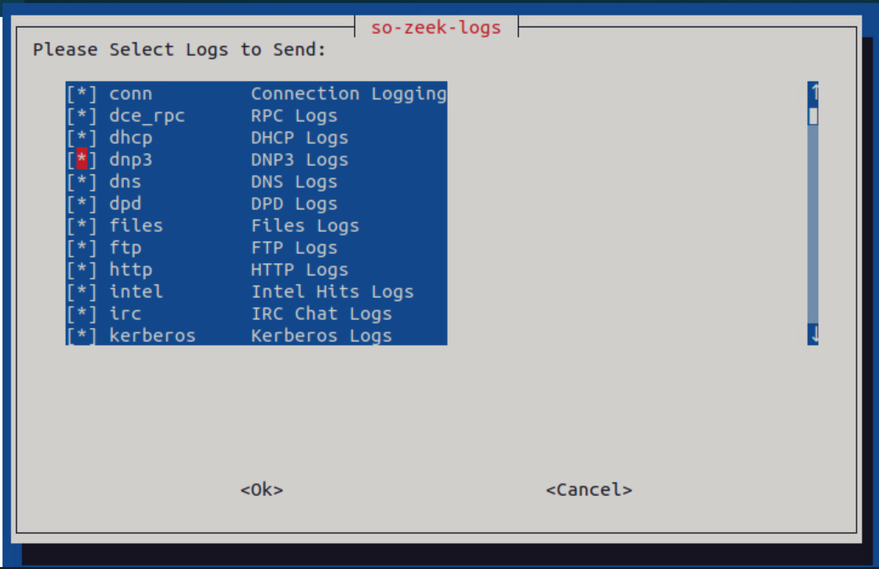


Current Grid Value

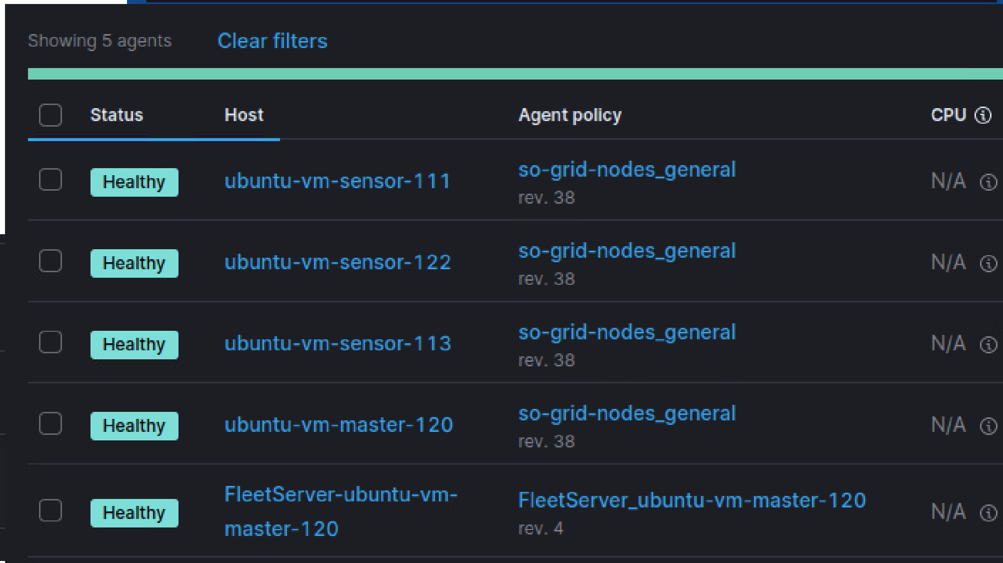
```
6.87.151.1/24
6.87.153.113
6.87.153.1/24
10.0.1.1/24
52.135.80.120
```

Security Onion Work

- Checked that Zeek.conn logs are included in the logs to be sent over in the rules on the manager
- Added all the sensors to Elastic Fleet and made them all Elastic Agents

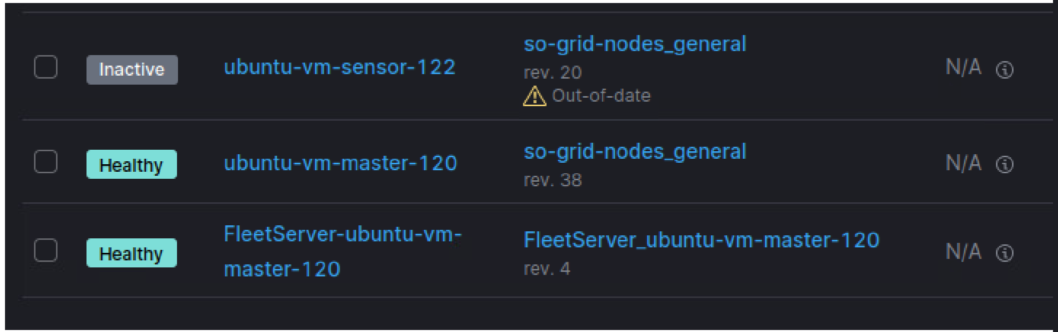


```
so-zeek-logs
Please Select Logs to Send:

[*] conn         Connection Logging
[*] dce_rpc      RPC Logs
[*] dhcp         DHCP Logs
[*] dnp3         DNP3 Logs
[*] dns          DNS Logs
[*] dpd          DPD Logs
[*] files        Files Logs
[*] ftp          FTP Logs
[*] http         HTTP Logs
[*] intel        Intel Hits Logs
[*] irc          IRC Chat Logs
[*] kerberos     Kerberos Logs

        <Ok>                <Cancel>
```

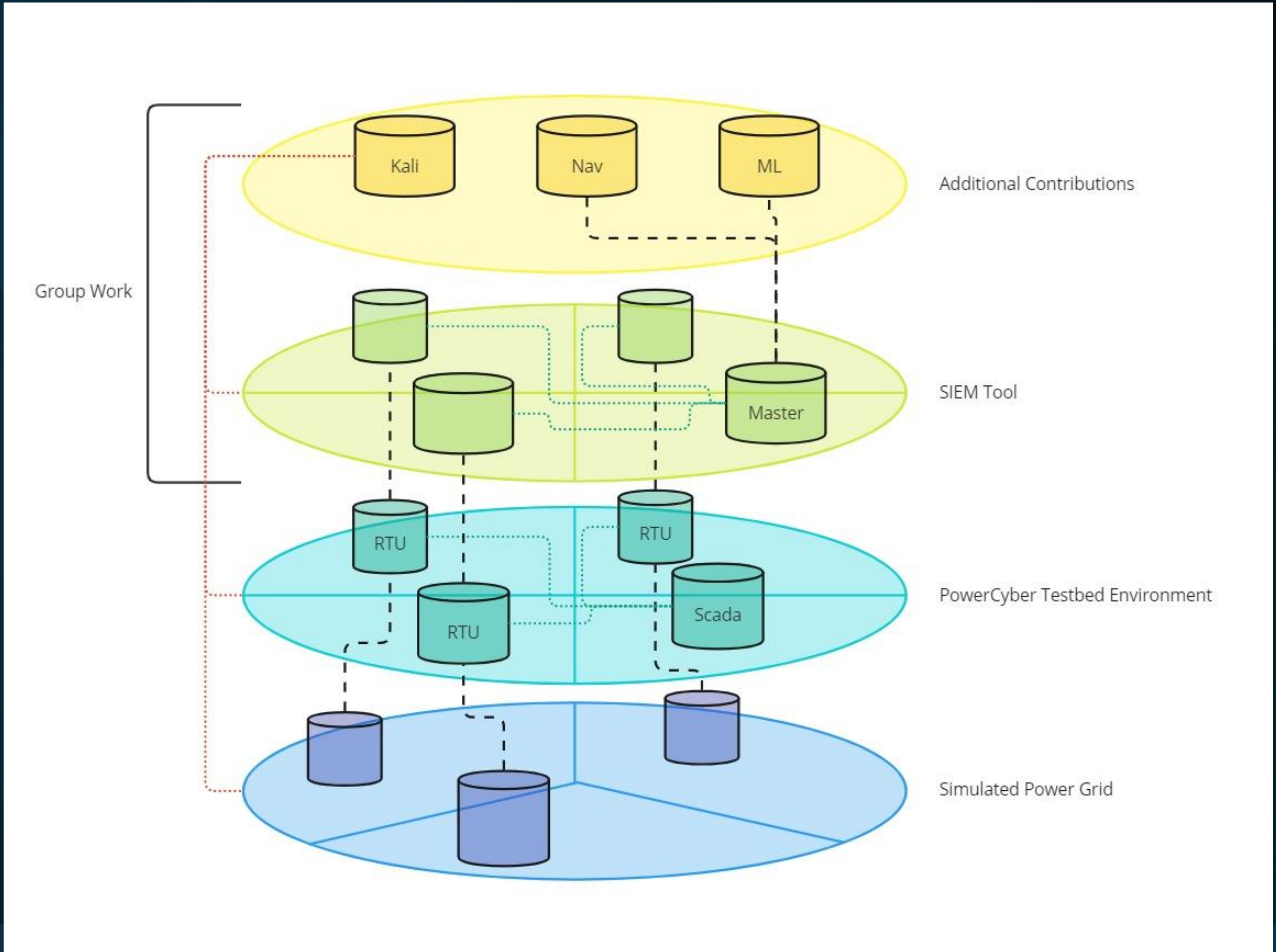


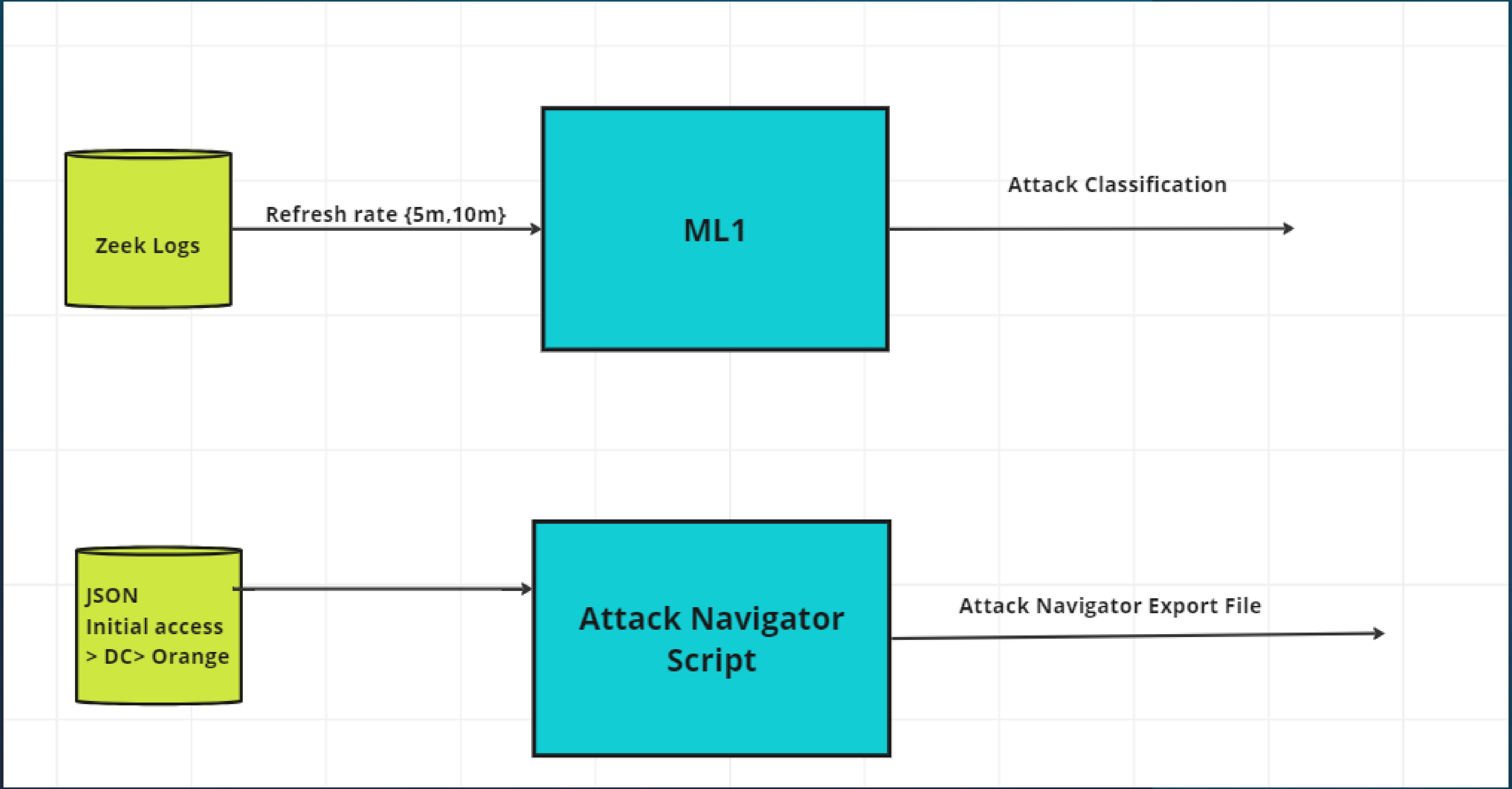
Showing 5 agents Clear filters

□	Status	Host	Agent policy	CPU ⓘ
□	Healthy	ubuntu-vm-sensor-111	so-grid-nodes_general rev. 38	N/A ⓘ
□	Healthy	ubuntu-vm-sensor-122	so-grid-nodes_general rev. 38	N/A ⓘ
□	Healthy	ubuntu-vm-sensor-113	so-grid-nodes_general rev. 38	N/A ⓘ
□	Healthy	ubuntu-vm-master-120	so-grid-nodes_general rev. 38	N/A ⓘ
□	Healthy	FleetServer-ubuntu-vm-master-120	FleetServer_ubuntu-vm-master-120 rev. 4	N/A ⓘ



□	Inactive	ubuntu-vm-sensor-122	so-grid-nodes_general rev. 20 ⚠ Out-of-date	N/A ⓘ
□	Healthy	ubuntu-vm-master-120	so-grid-nodes_general rev. 38	N/A ⓘ
□	Healthy	FleetServer-ubuntu-vm-master-120	FleetServer_ubuntu-vm-master-120 rev. 4	N/A ⓘ


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



Zeek Logs

Refresh rate {5m,10m}

ML1

Attack Classification

JSON
Initial access
> DC> Orange

Attack Navigator Script

Attack Navigator Export File

Attack Progress

- Created a Document for detailing the attacks I do
    - So far have ping attack and internal scripting attack
- Getting ready to attempt pre-made scripts on the RTU stations to affect the power grid