

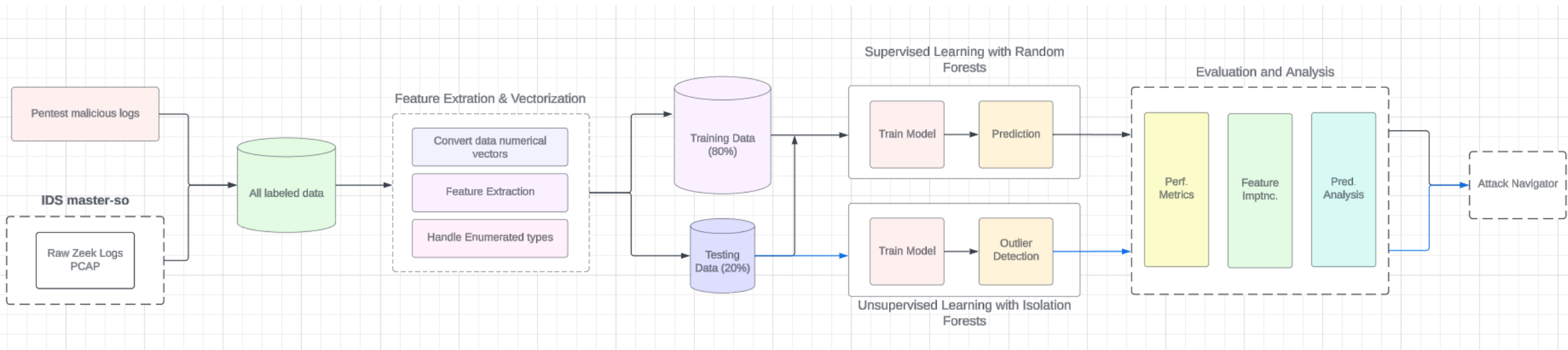
# **GRID-SIEM SD GROUP 29 SPRING '24**

Trent Bickford

Westin Chamberlain

Ella Cook

Daniel Ocampo



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

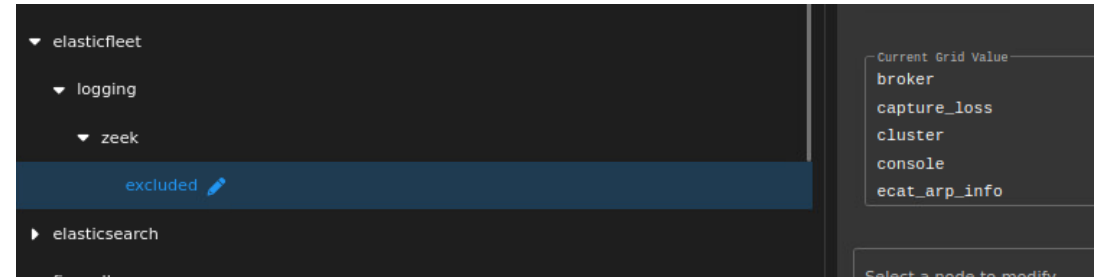
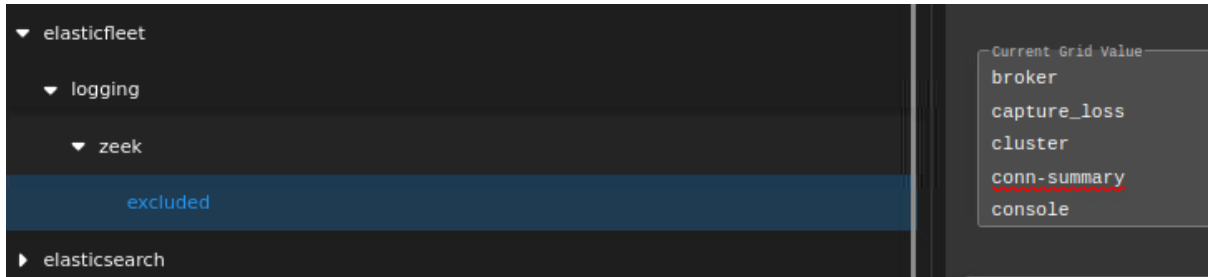
The screenshot shows the Elastic Fleet management interface. At the top, it says "Fleet" and "Centralized management for Elastic Agents." Below this are tabs for "Agents", "Agent policies", "Enrollment tokens", "Data streams", and "Settings". There are also buttons for "Add Fleet Server" and "Add agent". A search bar is present with the text "Filter your data using KQL syntax". Below the search bar, there are filters for "Status" (Healthy, Unhealthy, Updating, Offline) and "Upgrade available". The main content is a table with 3 agents listed:

| 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   | ...     |

The screenshot shows the Elastic Agent details page for "ubuntu-vm-sensor-122". The page has tabs for "Agent details", "Logs", and "Diagnostics". The "Logs" tab is selected. There is a search bar for logs and filters for "Dataset", "Log level", and "This month". The main content area displays the message: "There are no log messages to display. Try adjusting your filter." Below this message is a button labeled "Check for new data".

# 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

