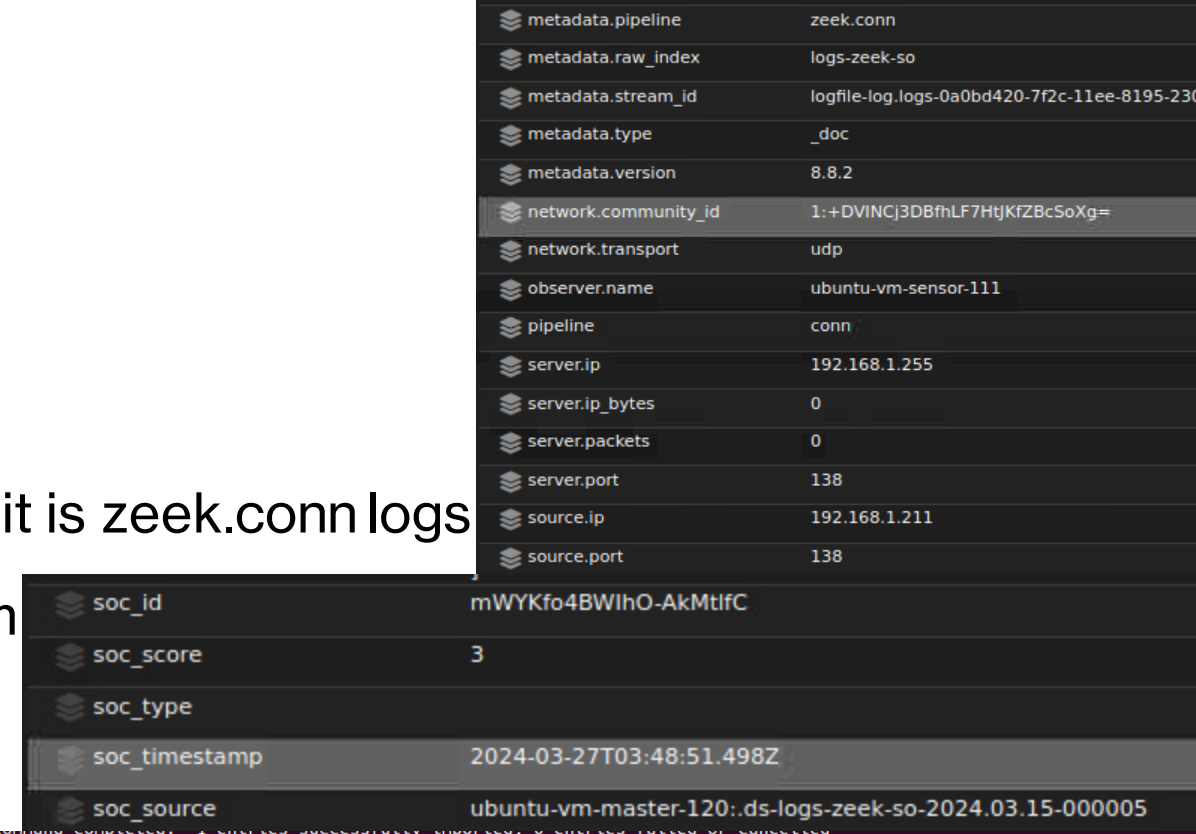
Grid-SIEM SD
Group 29

- Trent Bickford
- Westin Chamberlain
- Ella Cook
- Daniel Ocampo

Security Onion

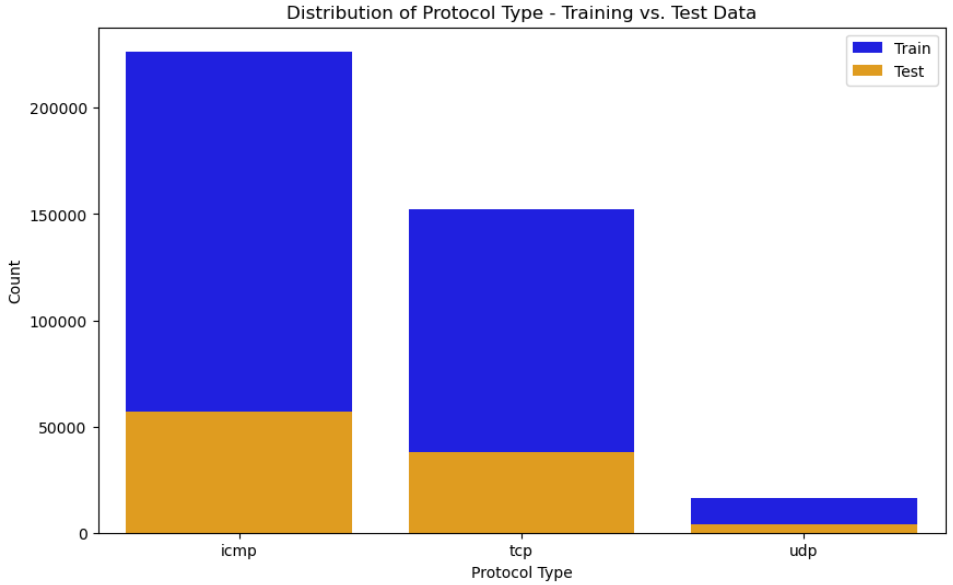
- Finished up the writing for the paper for review
- Found the traffic coming in from the RTU 1 and it is zeek.conn logs
- It is coming from an Elastic Search Data Stream
- Can run commands to see a JSON object

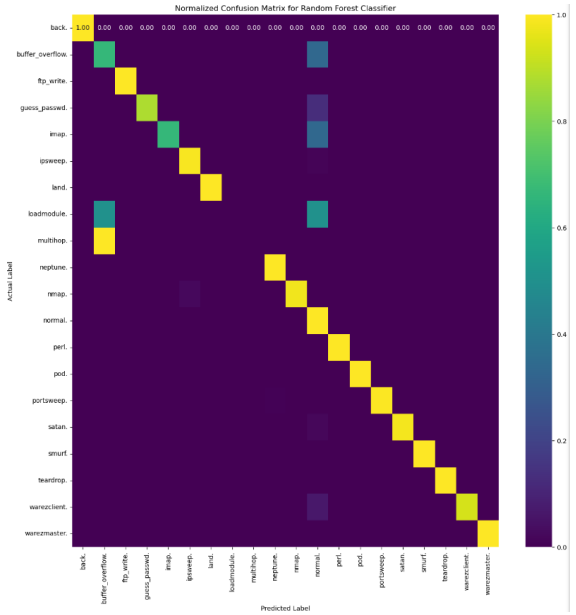



```
(base) ubuntu@ubuntu-vm-master-120:~/Desktop$ sudo so-elasticsearch-query .ds-logs-zeek-so-2024.03.15-000005/_search?pretty
{
  "took" : 4,
  "timed_out" : false,
  "_shards" : {
    "total" : 2,
    "successful" : 2,
    "skipped" : 0,
    "failed" : 0
  },
  "hits" : {
    "total" : {
      "value" : 10000,
      "relation" : "gte"
    },
    "max_score" : 1.0,
    "hits" : [
      {
        "_index" : ".ds-logs-zeek-so-2024.03.15-000005",
        "_id" : "JhxPf44BLzb5M6_YhySe",
        "_score" : 1.0,
        "_source" : {
          "container" : {
            "id" : "ssl.log"
          },
          "server" : {
            "port" : "8086",
            "ip" : "52.135.80.120"
```

Machine Learning

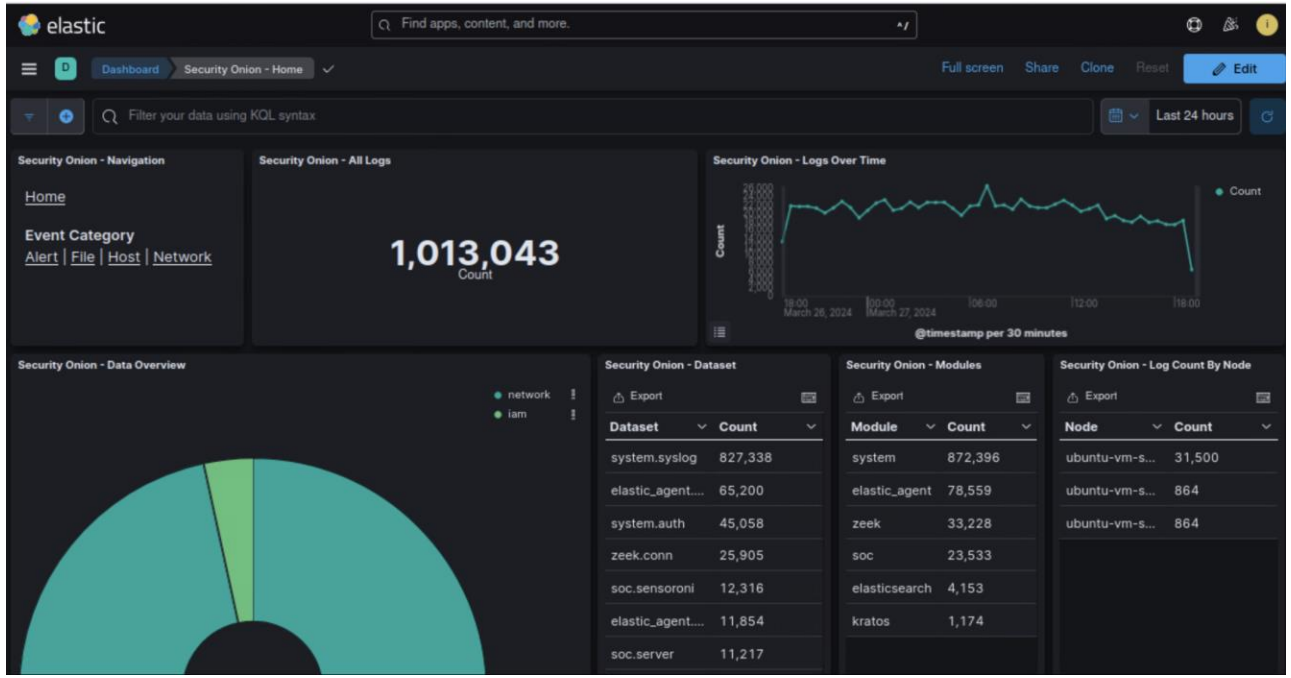
- Updated paper for further review
- New confusion matrix for Random forest classifier with labels
  - New dataset used: KDD Cyberattack dataset from kaggle
- Also included graphs comparing training vs test data for each feature in the dataset





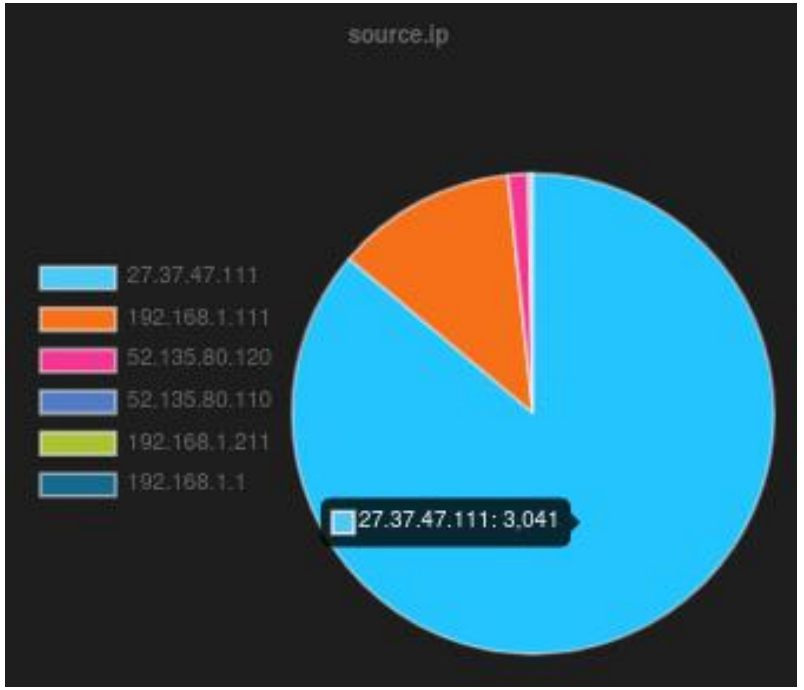
Red Team Testing

- RDP/SSH attacks (Resource Development > Acquire Access)
- Firewall adjustments a possible fix for being able to ssh/rdp machines past the router.
- Remmina remote desktop client, can access Substation 1 IDS. Attack signatures might be detectable with Hunt or Kibana.
- Further attacks pending.
- Trent – successful scan/ping attacks.



Attacking Progress

- Updated and reorganized paper
- Finished attack documentation
- Lauched nmap, ping, curl bash scripts
  - Had to target sensor, RTU stations have trouble getting logs to master node



Future Work

- Revise the paper section if needed
- Finish the final document and slides
- Complete bi-weekly report with peer review feedback.