

A vertical watercolor-style background on the left side of the slide, featuring various shades of blue and teal with soft, blended edges.

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

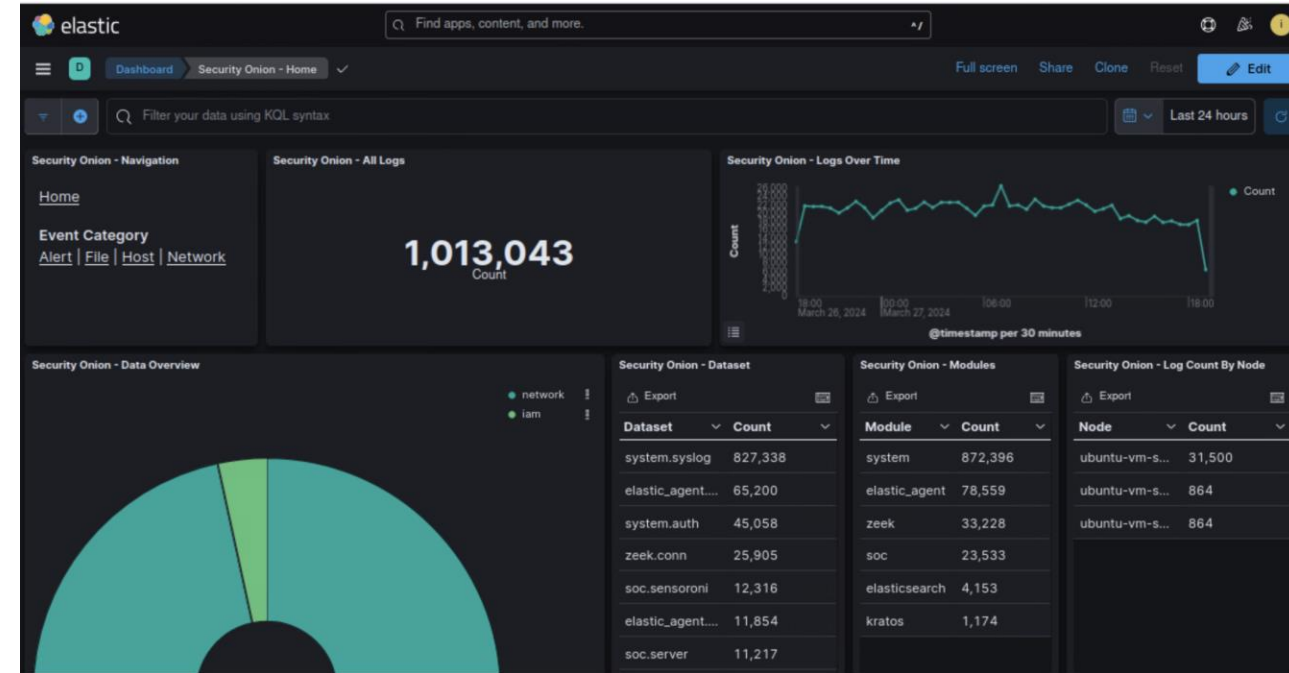
metadata.pipeline	zeek.conn
metadata.raw_index	logs-zeek-so
metadata.stream_id	logfile-log.logs-0a0bd420-7f2c-11ee-8195-230
metadata.type	_doc
metadata.version	8.8.2
network.community_id	1:+DVINCj3DBfhLF7HtjKfZBcSoXg=
network.transport	udp
observer.name	ubuntu-vm-sensor-111
pipeline	conn
server.ip	192.168.1.255
server.ip_bytes	0
server.packets	0
server.port	138
source.ip	192.168.1.211
source.port	138

soc_id	mWYkfo4BWlhO-AkMtifC
soc_score	3
soc_type	
soc_timestamp	2024-03-27T03:48:51.498Z
soc_source	ubuntu-vm-master-120:.ds-logs-zeek-so-2024.03.15-000005

```
(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"
          }
        }
      }
    ]
  }
}
```

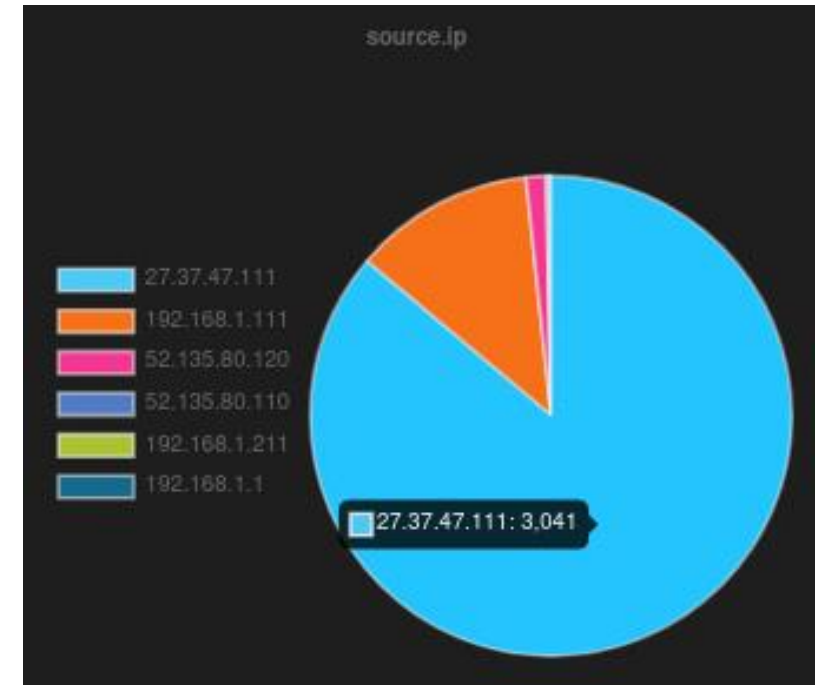

Red Team Testing

- 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
- Launched 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.