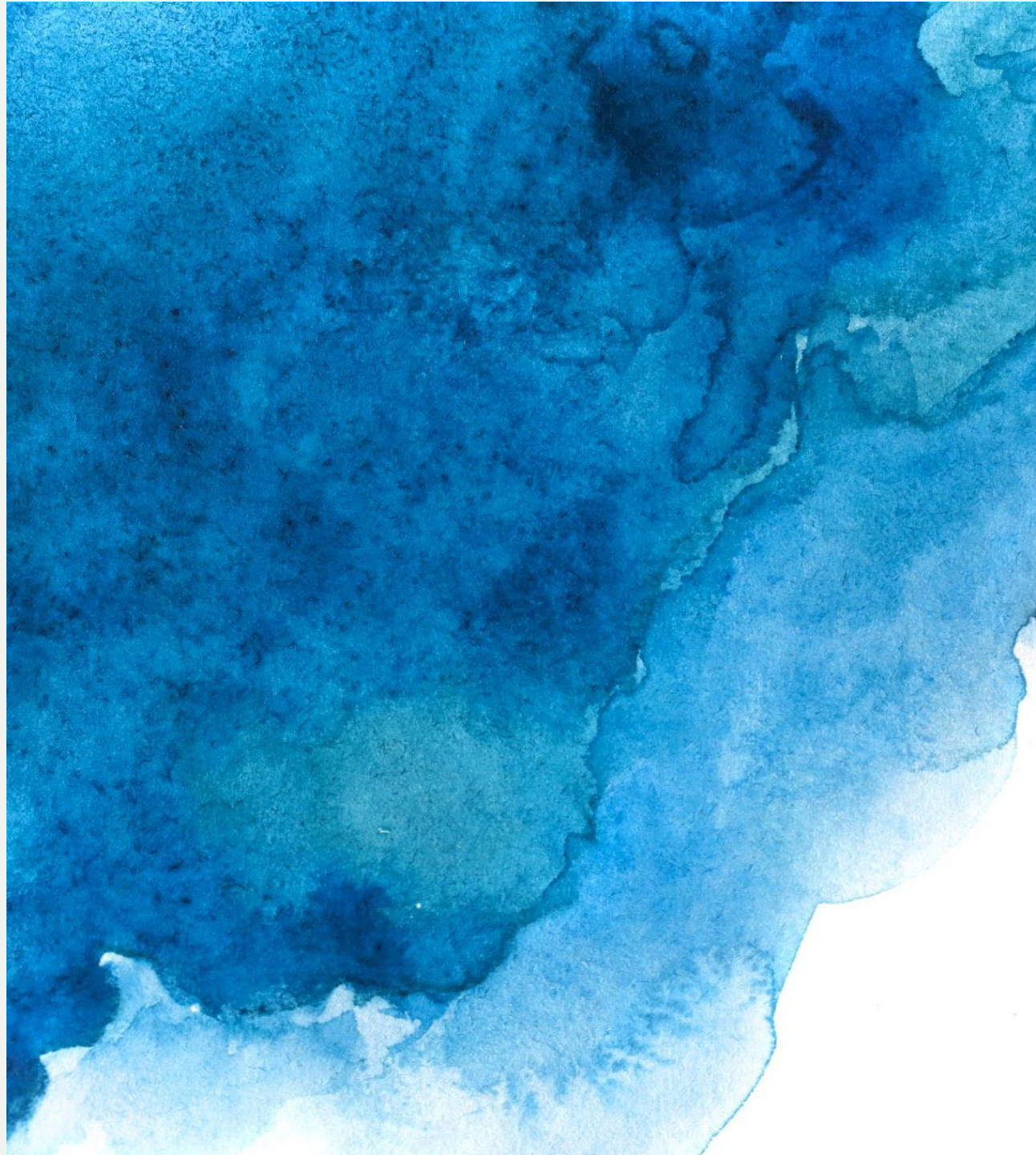


# GRID-SIEM

## SD Group 29

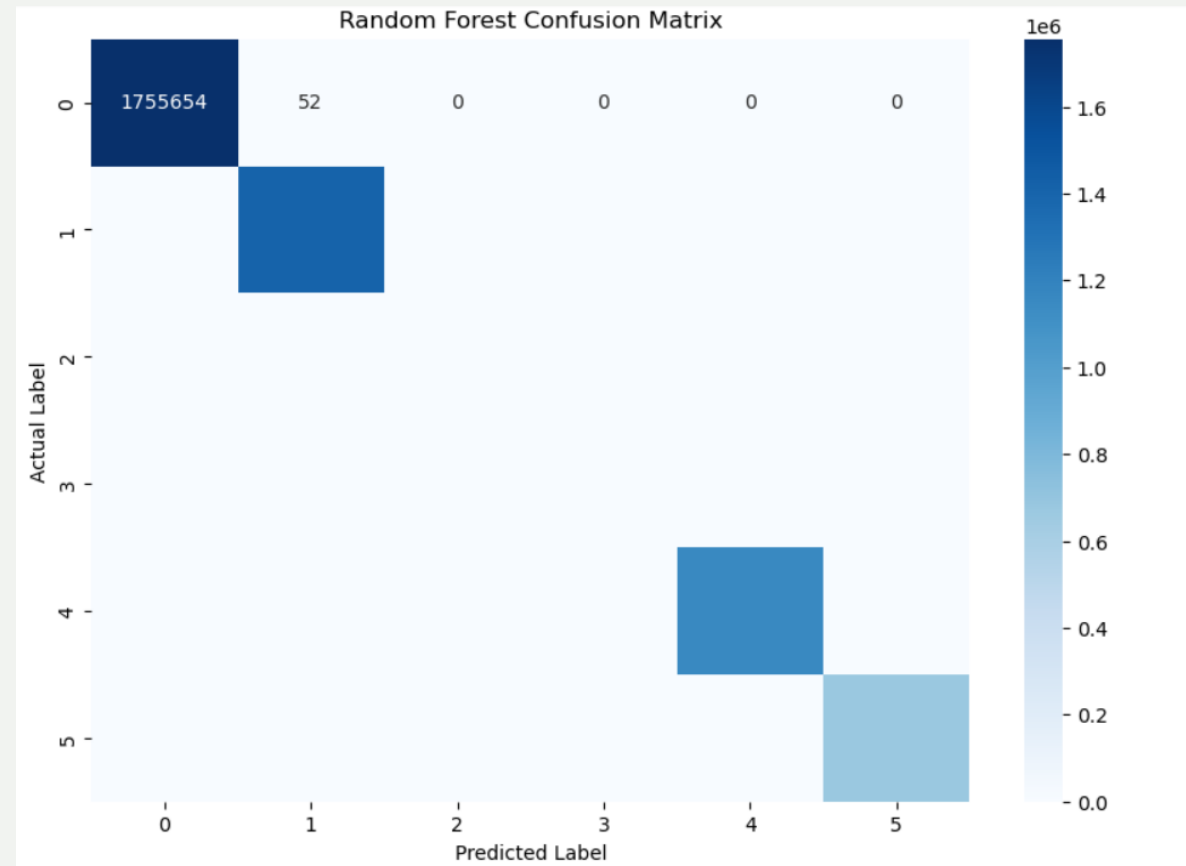


Trent Bickford  
Westin Chamberlain  
Ella Cook  
Daniel Ocampo



# ML

- Jupyter confusion matrix ran but took quite a bit of time
  - Dataset was skewed heavily towards malicious data points which meant the random forest almost always classified as malicious
- Implemented a module to train mainly on the minority, but took too long to run
  - Plan to re-run this week



Random Forest Classifier Results:

	precision	recall	f1-score	support
0	1.00	1.00	1.00	1755706
1	1.00	1.00	1.00	1410821
2	1.00	1.00	1.00	520
3	1.00	1.00	1.00	1692
4	1.00	1.00	1.00	1156283
6	1.00	1.00	1.00	677179
accuracy			1.00	5002201
macro avg	1.00	1.00	1.00	5002201
weighted avg	1.00	1.00	1.00	5002201

Accuracy: 0.9999872056320808

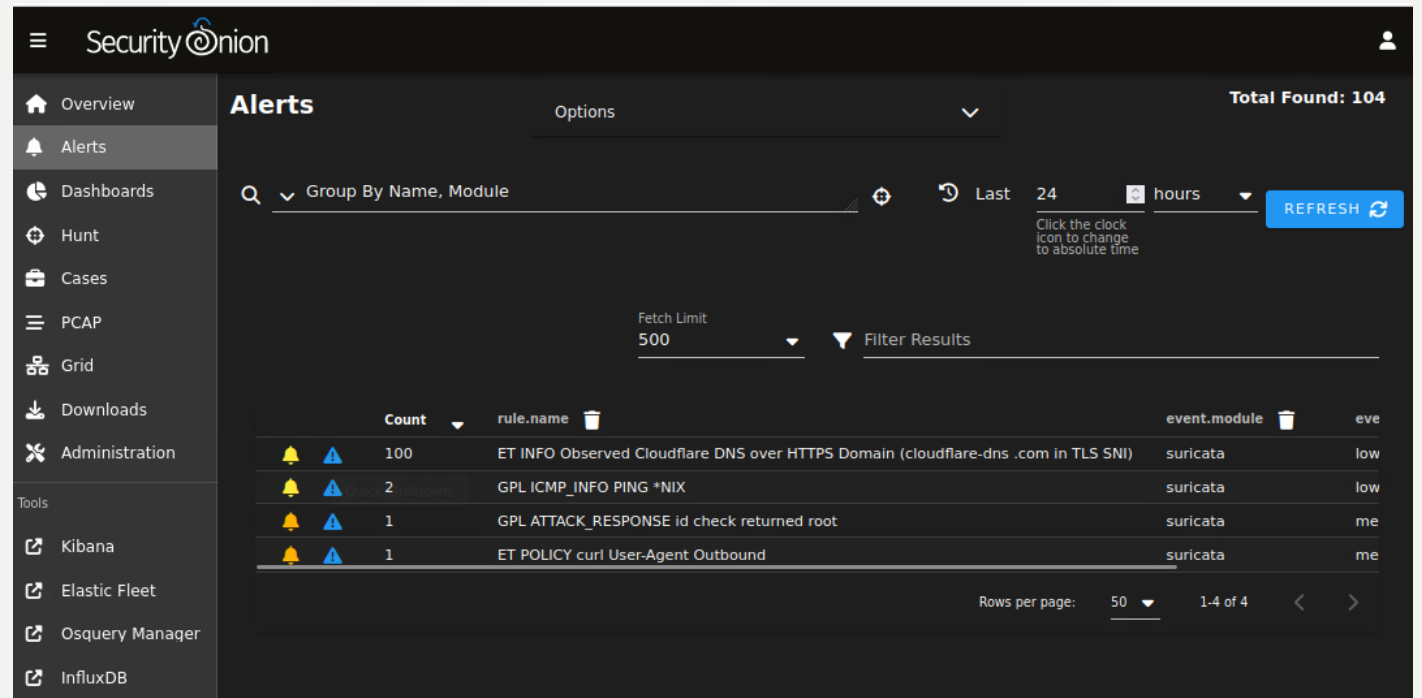
Precision: 1.00  
Recall: 1.00  
F1 Score: 1.00

# Attack updates

- Finished documentation
  - Put documentation in paper for attack section
- Daniel found a program like Caldera Called atomic red team
  - Going to be looking into it this week
  - It can interact with playbook
  - Unsure if it will run into the same compatibility issues as caldera

# Security Onion

- Team launched and detected a ping attack on sensor 1 and launched a curl command from sensor that were both caught in SOC



The screenshot displays the Security Onion Alerts interface. The left sidebar contains navigation options: Overview, Alerts, Dashboards, Hunt, Cases, PCAP, Grid, Downloads, Administration, and Tools (Kibana, Elastic Fleet, Osquery Manager, InfluxDB). The main area is titled 'Alerts' and shows a table of detected events. The table has columns for Count, rule.name, event.module, and eve. The first row shows 100 alerts for 'ET INFO Observed Cloudflare DNS over HTTPS Domain (cloudflare-dns .com in TLS SNI)' from the 'suricata' module. The second row shows 2 alerts for 'GPL ICMP\_INFO PING \*NIX'. The third row shows 1 alert for 'GPL ATTACK\_RESPONSE id check returned root'. The fourth row shows 1 alert for 'ET POLICY curl User-Agent Outbound'. The interface also includes search filters, a 'Group By Name, Module' dropdown, a 'Fetch Limit' of 500, and a 'Filter Results' button. A 'REFRESH' button is visible in the top right corner of the alert list area.

Count	rule.name	event.module	eve
100	ET INFO Observed Cloudflare DNS over HTTPS Domain (cloudflare-dns .com in TLS SNI)	suricata	low
2	GPL ICMP_INFO PING *NIX	suricata	low
1	GPL ATTACK_RESPONSE id check returned root	suricata	me
1	ET POLICY curl User-Agent Outbound	suricata	me



# Upcoming Work

- Finish the presentation and receive feedback from other groups
- Finish the document by the end of March
- Test new attack framework Atomic Red Team which works directly off MITRE matrix techniques.
- Utilize Playbook to implement detection capabilities and mitigations. Prove their effectiveness with the Hunt tool. Update Navigator APT heat map with all of the areas that are then being defended.

# Worked on the Paper-IEEE-TCPS

- [https://iowastate-my.sharepoint.com/:w:/r/personal/docompo\\_iastate\\_edu/\\_layouts/15/Doc.aspx?sourcedoc=%7BE0ADF599-08CF-4CEC-95F3-DA4B1A387424%7D&file=Paper-IEEE-TCPS.docx&action=default&mobileredirect=true](https://iowastate-my.sharepoint.com/:w:/r/personal/docompo_iastate_edu/_layouts/15/Doc.aspx?sourcedoc=%7BE0ADF599-08CF-4CEC-95F3-DA4B1A387424%7D&file=Paper-IEEE-TCPS.docx&action=default&mobileredirect=true)