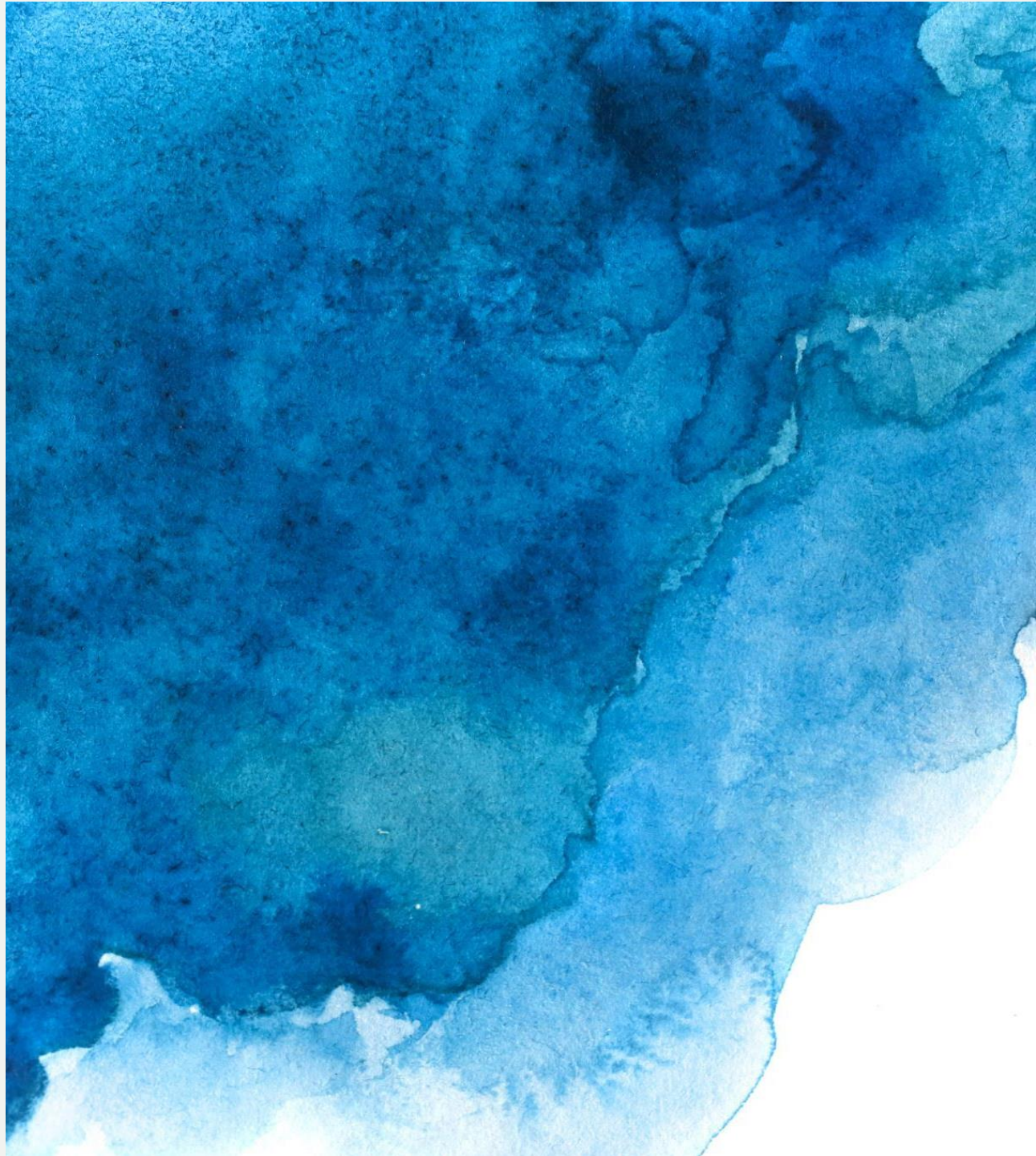
GRID-SIEM
SD Group 29

Trent Bickford
Westin Chamberlain
Ella Cook
Daniel Ocampo

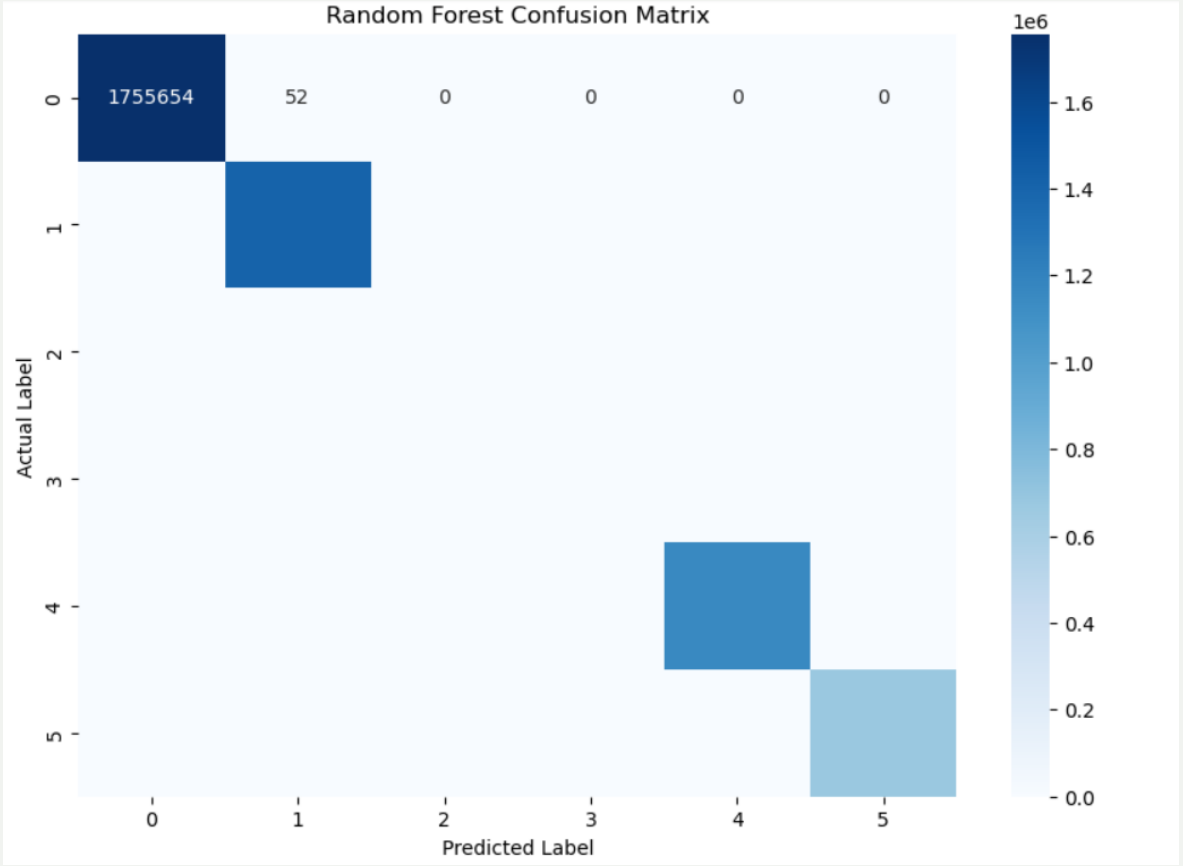


ML

- 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

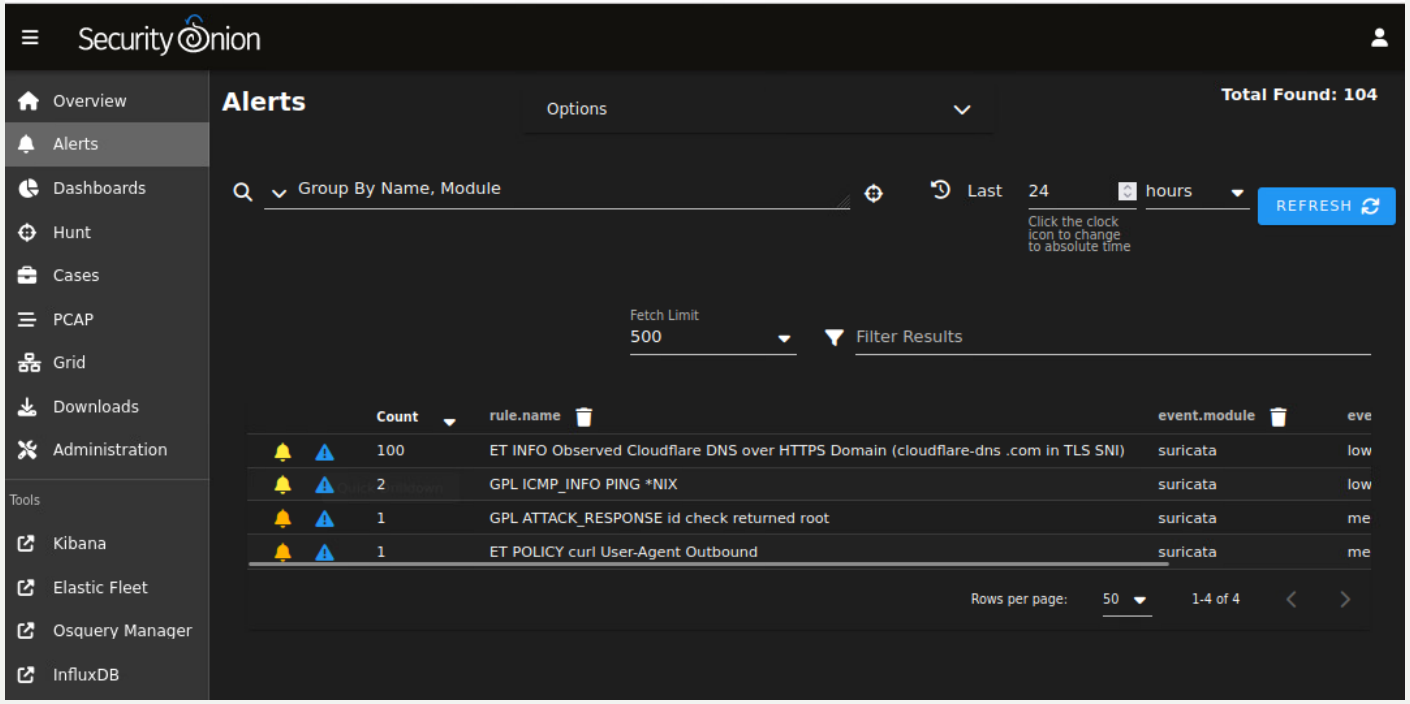
Precision: 1.00
Recall: 1.00
F1 Score: 1.00

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

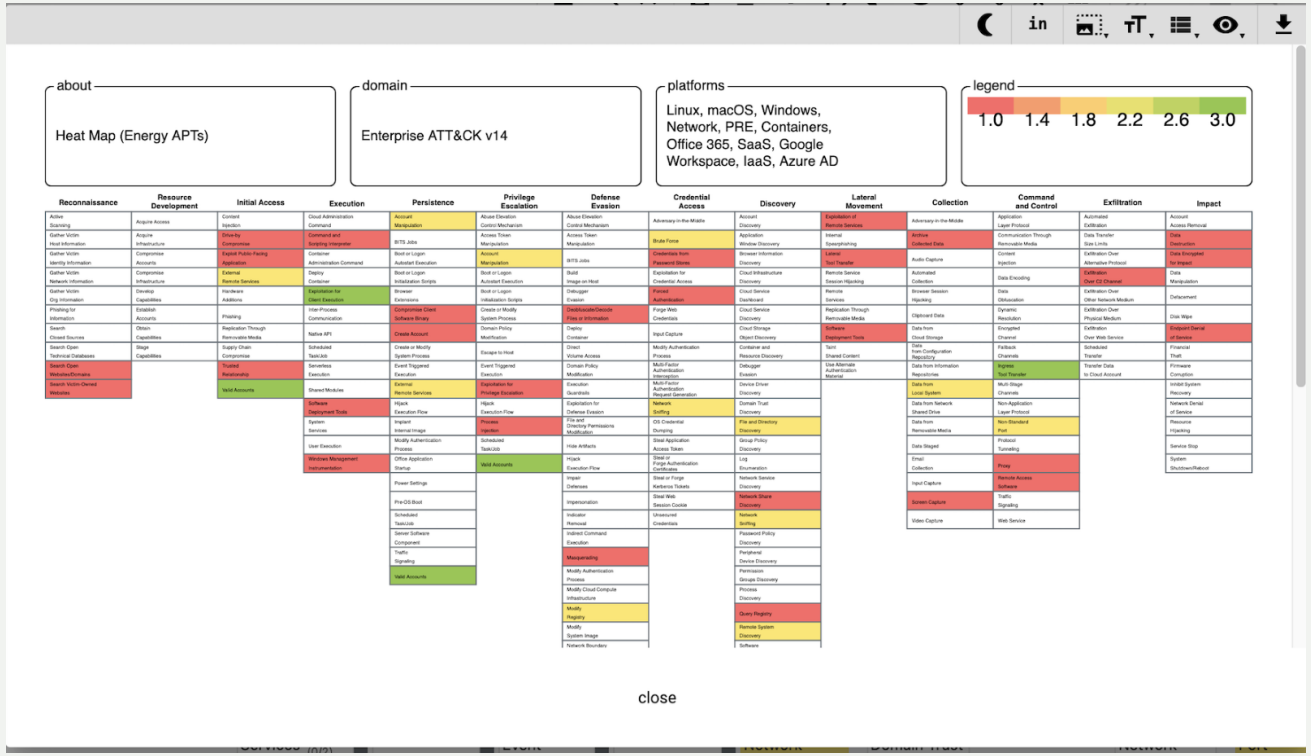
Security Onion

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



ATT&CK Navigator

- Built a heat map using the TTPs three energy infrastructure attacking APTs would use.
- Use the results from this to deploy focused plays within security onion. Check their effectiveness with hunt.
- Test the security of defense measures using a tool called Atomic Red Team by RedCanary.



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