GRID-SIEM

SDMAY24-29

Trent Bickford, Westin Chamberlain, Ella Cook, Daniel Ocampo

Client/Advisor: Dr. Gelli Ravikumar

Introduction

Problem: Power grids are prone to cybersecurity attacks which have detrimental effects on public safety.

Solutions:

- Implement NIST cybersecurity framework and use a SIEM tool onto the existing system.
- Leverage machine learning capabilities to assist the detection of cybersecurity attacks.

Context

Users: Power grid companies looking to defend their systems as well as researchers in the field.

Previous Work: A simulated transmission power grid, Power Cyber has been set up by previous research and senior design projects

Design Requirements

Requirements:

- Use a SIEM to detect attacks ran against the Power Cyber testbed.
- The solution will be implemented in a VM environment.

Standards: ISO/IEC 27001, NIST Cyber Framework, MITRE ATT&CK Framework, IEEE P2863, NVD CVSS v3.0, IEEE 1402, IEEE C37.2040

Design

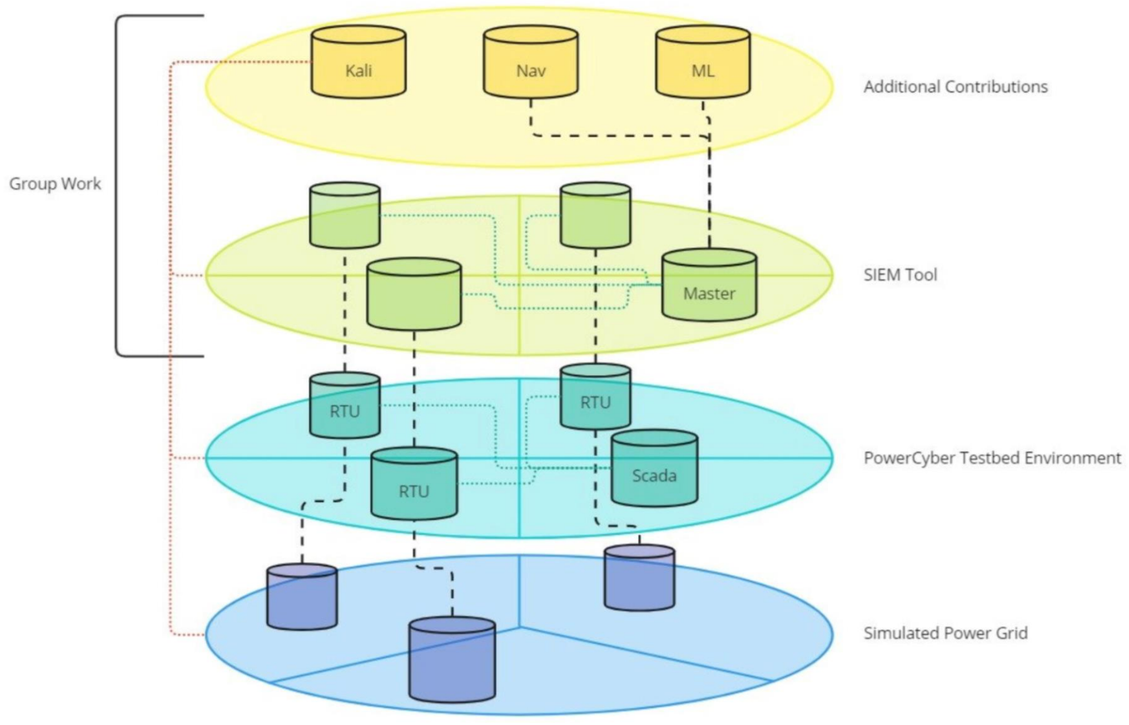

Figure 1: Architecture diagram showcasing Power Cyber Infrastructure, Security Onion, Machine Learning, and Attack Navigator

Attack Modeling

Vulnerable Machines: RTU, Sensors

Protocols: Modbus, dnp3

Potential Attackers:

- Nation state
- Terrorists
- Cyber criminals

Attack Methods

- DDoS
- Phishing
- Brute Force

Attack Components

Kali Machine: where we create and launch our attacks that effect the RTU Machines and Sensors

MITRE Caldera: create operations to infect the RTUs and control the SCADA environment

Types of Attacks Used:

- Nmap
- Ping flood
- Curl injection
- Ssh brute force

Figure 2: Machines Kali and Caldera can attack

Defense Components

Security Onion:

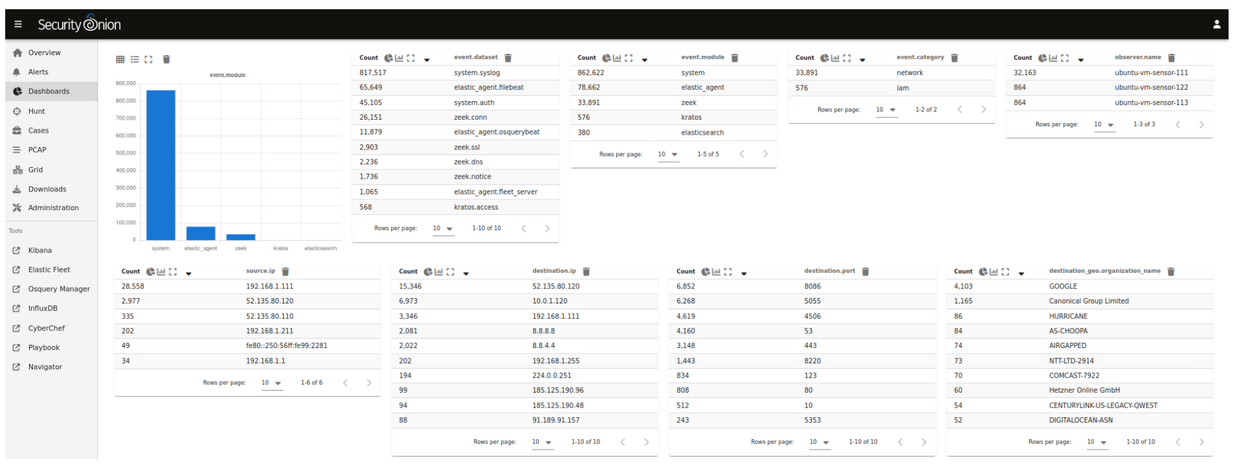

Figure 3: Security Onion Dashboard with attack detected on the Alert tab

Navigator

- Blue teams can explore and understand the relationships between defensive tactics and techniques.
- Defenders can then use the framework resources to understand attacks and the rules and methods for detection

Figure 4: Mitre Attack Navigator Heatmap of attacks

Machine Learning:

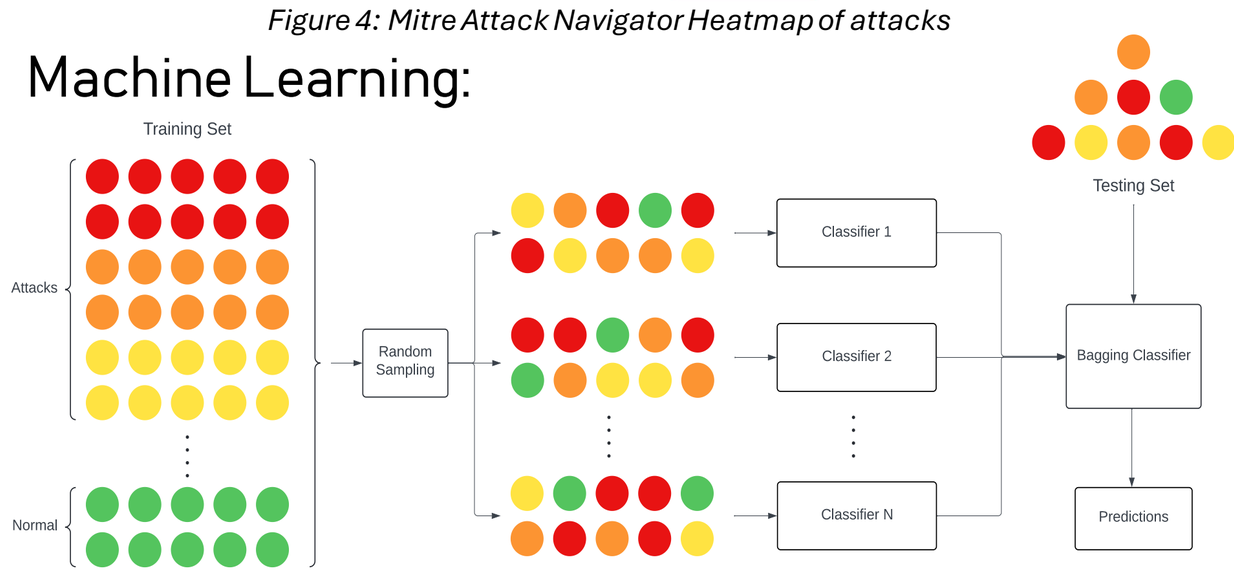

Figure 5: Machine learning bagging classifier

Testing & Results

- The integrated SIEM was tested by running attacks launched from a Kali VM. These attacks were picked up and caused alerts in the system.
- We also measured connectivity of the system using existing tools in Security Onion.

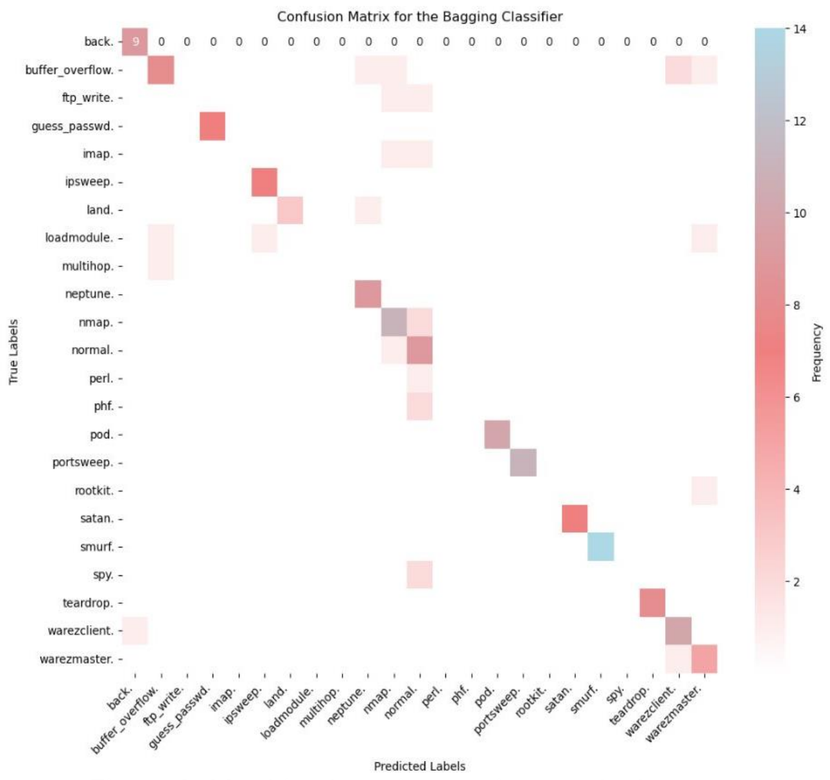

Figure 6: Machine learning testing results heatmap

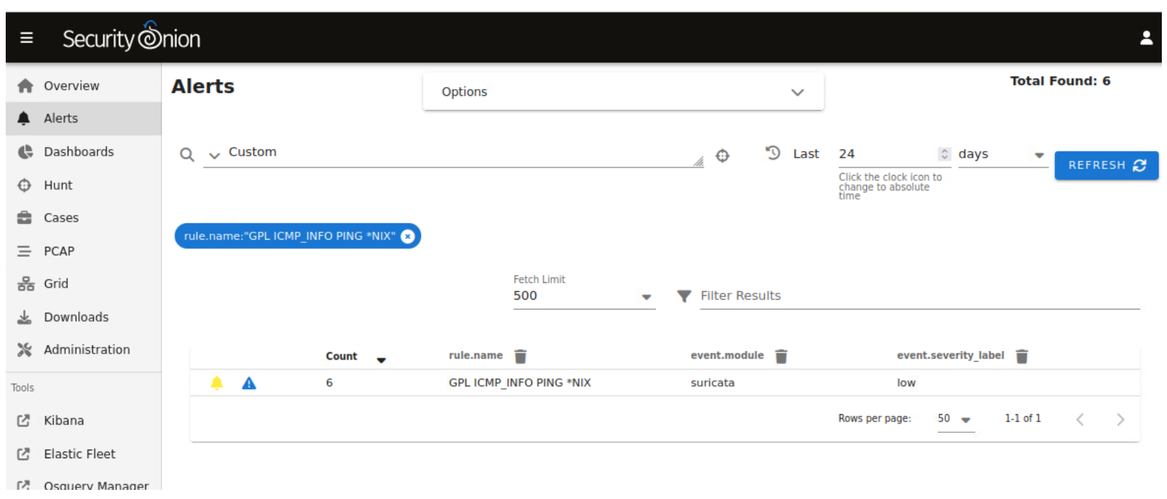

Figure 7: Security Onion Dashboard with attack detected on the Alert tab