Grid-SIEM

SDMAY24-29

Implementing the SIEM

Findings this week:

- Security Onion requires different hardware requirements depending on the amount of information being sent.
- Sensors require hardware requirements depending on traffic.

Team asks:

- A network diagram of the PowerCyber network or access so that we may construct one.
- Information of the devices in the network such as CPUs, RAM, and storage.

For next week:

- Team will utilize the information received to match whether the devices and sensors meet the requirements for Security Onion.

Machine Learning in the SIEM

Findings this week:

- Security Onion has a beta machine learning component in it that exclusively monitors logs but requires CPUs with AVX support.

Team asks:

For next week:

- Further research on the current beta machine learning component of Security Onion.
- Research on Elastic and X-Pack.