Team Name: sdmay24-29
Team Members: Daniel Ocampo, Trent Bickford, Ella Cook, Westin Chamberlain
Report Period: September 17 – October 8

Summary of Progress in this Period

Progress Point	Notes
Team has explored software alternatives which could better serve the project.	Including: • Swimlane for Machine Learning. • Gravwell as a SIEM platform. • Splunk as a SIEM in place of SecurityOnion.
Finalized the requirements and engineering standards presentation.	Identified requirements, constraints and engineering standards for our project. Including: • The uptime and availability of PowerCyber • Building a simple yet informative SIEM dashboard. • Standards such as those outlined by NIST, MITRE and IEEE.
Delved into the inner workings of the PowerCyber infrastructure.	• Had a discussion with the professor going over a high level description of the PowerCyber setup • Better understanding of the specific types of nodes (manager, etc) that we plan to implement within securityOnion on the PowerCyber setup
Researched the Security Onion open source platform and explored what architecture would best suit our project needs.	Decided on the distributed architecture with the following nodes: • Manager Search Node • Forward Nodes at each of the DER Clients
Identified options for the machine learning portion and how we could potentially more data from SecurityOnion into PyTorch.	• Found out that many of the SIEM options have machine learning frameworks imbedded into them
Determined a number of intended use cases for our final project.	Potential use cases and users of our final project would include: • Students and staff that manage the PowerCyber lab in Coover. • Students at Iowa State interested in securing industrial control systems.

	• Project can be used as an official defense system that runs all year long. • A tool to learn more about security best practices by taking the role of a red/blue team.
Anything else...	

Pending Issues

Issue	Description
Explore how the following tools could enhance our project: • SecurityChef • Kibana • Elastic Fleet • ATT&CK Navigator	For the week of October 9th, our team needs to create a slide deck to showcase our understanding of the tools in the issue description. And how they could be useful in our project.
Make use of free online training resources to become comfortable using SecurityOnion.	Since our team will be granted access to virtual resources soon. We need to be able to have a good understanding of how to start configuring and making sense of all the capabilities provided by security onion. We do this by searching for training videos and resources available for free on the internet.

Plans for Upcoming Reporting Period

Pending Item	Notes
Access to virtual resrources in VSphere.	Project adviser has stated that once the group has demonstrated a solid understanding of the PowerCyber infrastructre and which SIEM

	framework will be put to use and why. Then access to the virtual resources will be granted. We have proved our understanding and will be able to work with the project resources the week Oct. 16.
Understand the role of MITRE Caldera to deploy attacks on OT systems.	Since this is one of the portions of the project that will be implemented last, it follows that we have not done enough research to thoroughly understand how testing with MITRE Caldera will be accomplished.
Develop weekly slide deck to showcase progress to our project adviser. Stay prepared for in-class lightning talks.	In order to be prepared to present during the in-class lighting talks our group needs to develop a new slide deck covering project planning. As well as a secondary slide deck to showcase new findings to our project adviser.