Senior Design Bi-Weekly Status Report; Fall 2023

Team Name: sdmay24-29
Team Members: Daniel Ocampo, Trent Bickford, Ella Cook, Westin Chamberlain
Report Period: Aug 28-Sept 17

Summary of Progress in this Period

Progress Point	**Notes**
Outlined project resource requirements to our project adviser. This includes a table of basic computational requirements we need to get started.	For example RAM and storage. Each Node in a distributed architecture requires: • 12GB RAM • 4 CPU Cores • 200GB Storage The manager search node in an distributed architecture requires: • 16-128GB RAM • 8 CPU Cores • 1TB Storage
Reviewed SecurityOnion Documentation	Security Onion provides multiple network monitoring tools to improve threat detection. It includes signature-based NIDS alerts created by Suricata and network metadata logging for protocols like HTTP, DNS, and SSH. The platform also does a full packet capture using Stenographer, which allows it to record all network activity. Additionally, Security Onion analyzes files transferred over the network with Strelka. It also has an Intrusion Detection Honeypot functionality that imitates FTP and HTTP to initiate automatic alerts. Security Onion can also take in log data from routers and firewalls that don't support installation.
Reviewed PowerCyber Documentation	At the base of the cyber-physical system there are Distributed energy resources (DER), which are generally consumer side energy generation units such as solar panels, wind turbine, or batteries. The DER clients are where we will be including our IDS Sensors and IPS for SecurityOnion Monitoring. Past that is the third party access through the internet and our own Wide area network which can also transmit data and connect to our IDS master (SecurityOnion) and the DER control center. Our IDS Sensors will consist of basic IDS Rules, IT-Based rules, and Modbus-specific rules to detect intrusions. The Modbus rules are based on physics thresholds, this means that if there is a certain

	amount of “power” being sent or recieved, our IDS will be notified.

Pending Issues

Issue	Description
SecurityOnion Architectures	Understand the different architectures offered by security onion. And identify a potential best option for future implementation. Four Types: • Import • Evaluation • Standalone • Distributed
SecurityOnion Distributed Architecture (Node Types)	There are different types of nodes with different capabilities and the team will have to identify which nodes fit the need of the project. Manager Nodes: This is the central component for managing and disecting data and will be the primary interface for the SIEM. Manager Search Nodes: This node is the same as a manager node, but does not require separate search nodes to search data in the sensors and may instead do it itself. Forward Node: These nodes act as the sensors to record logs and other security instances.
Figure out how to take the data out of security onion and feed into PyTorch.	• Export specific logs from Security Onion via CSV file • Use Pandas and Jupyter notebook to clean the data • Convert Pandas to PyTorch tensors • Implement a predefined PyTorch model • Train model and evaluate

Plans for Upcoming Reporting Period

Pending Item	Notes
Obtain access to the VMs and understand the purpose of each individual virtual machine.	testbed.ece.istate.edu
Team needs diagrams that outline the topology of the power cyber system within VSphere.	

Develop slide deck to showcase progress to our project adviser. Be prepared for lightning talks.	As a team and individually.
Explore machine/deeplearning packages on github.	Options include: PyTorch. Tensorflow. Keras.
Understand the role of MITRE Caldera to deploy attacks on OT systems.	