Team 38

Project Title: ADSICS Anomaly Detection System for Industrial Control Systems

Date: October 17th, 2021

Members:

- Alex Nicolellis – Organizing
- Jung Ho Suh – Communicating to the client
- Muhamed Stilic – Controlling
- Pallavi Santhosh – Planning

What we've accomplished in the past week/what we've been researching:

- Alex Nicolellis – Studying alert correlation algorithms, their strengths, and their weaknesses.
- Jung Ho Suh – Installing SNORT/SecurityOnion on the VMs
- Muhamed Stilic – Understanding SNORT and how the design process works for our project
- Pallavi Santhosh – Learning about zero-day attacks and presenting to clients about research so far.

What we're planning to do in the coming week:

- Alex Nicolellis – Detecting intrusions using SNORT.
- Jung Ho Suh – Establishing the connection between sensor and IDS master and set up the rules.
- Muhamed Stilic – Work on implementation of tests and test documentation
- Pallavi Santhosh – Installing Security Onion from scratch.

Issues we had in the previous week:

- Alex Nicolellis – Difficulty with SNORT installation.
- Jung Ho Suh – Installing SNORT on the system is confusing at first.
- Muhamed Stilic – Uses with understanding SNORT and the overall design of the project
- Pallavi Santhosh – Issues connecting to the testbed platform.