E E 491 Weekly Report #5

Team 38

Project Title: ADSICS Anomaly Detection System for Industrial Control Systems

Date: October 31st, 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 – Visualized data on the testbed environment
- Jung Ho Suh – Installed Securityonion in the testbed environment.
- Muhamed Stilic – Worked on the testbed environment more and used nmap and sent packets to visualize in kibana
- Pallavi Santhosh – Worked in testbed environment with nmap

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

- Alex Nicolellis – Compare algorithms for anomaly detection in the context of our project
- Jung Ho Suh – Configure Snort to find out how to use rule based IDS
- Muhamed Stilic – Work with snort and apply files we already have to the website
- Pallavi Santhosh – Use snort in testbed environment

Issues we had in the previous week:

- Alex Nicolellis – Kibana version on the testbed is different from what I’m used to so it’s hard to find tools.
- Jung Ho Suh – Testbed could not be configured due to the administrator privilege issue.
- Muhamed Stilic – Testbed admin issues, installation process of sec onion on local machine
- Pallavi Santhosh – Trouble using boot camp to install windows on mac