E E 491 Weekly Report #4

Team 38

Project Title: ADSICS Anomaly Detection System for Industrial Control Systems

Date: October 24h, 2021

Members:

- Alex Nicolellis – Organizing -	7 hrs
- Jung Ho Suh – Communicating to the client	10 hrs
- Muhamed Stilic – Controlling	10 hrs
- Pallavi Santhosh – Planning	8 hrs

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

- Alex Nicolellis – Used Kibana to analyze anomalous datasets and understand what information would be valuable to our own project.
- Jung Ho Suh – Installed SecurityOnion on a local computer, created alerts and signals.
- Muhamed Stilic – Worked on figuring out Kibana. Tried to use Security Onion.
- Pallavi Santhosh – Used on ElasticSearch to set up TLS.

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

- Alex Nicolellis – Explore Kibana more and test SecurityOnion on the testbed.
- Jung Ho Suh – Set up the Testbed environment perfectly, IADS Master- SecurityOnion, IADS Sensors - Snort to create meaningful alerts.
- Muhamed Stilic – Testing our current test bed and learning more on how security onion and elastic search work together.
- Pallavi Santhosh – Begin to test SecurityOnion within the testbed environment.

Issues we had in the previous week:

- Alex Nicolellis – SecurityOnion does not work for the most current version of Ubuntu.
- Jung Ho Suh – The testbed environment configuration was unable to install SecurityOnion.
- Muhamed Stilic – Installing elastic search/kibana on a virtual machine. Issues with security onion os version.
- Pallavi Santhosh – Downloading windows onto macbook