Meeting date – 18th July 2020

Agenda

1. CoDR Review Meeting
2. Survey of algorithm discussion
3. Contribution of Everyone in group
4. Kali linux set up ?
5. Install and Understand Wireshark, SNORT
6. ICS CERT courses ? do Mapping Defence-In-Depth IT security solution to ICS Part I and Part II

* Outline of our work

1. What is Critical Infrastucture?
2. What is ICS/SCADA?
3. What is IT/OT network (Purdue Model diagram)? From ICS CERT Course
4. Identify the Testbed architecture
5. We will be creating one Malware and inserting into
6. Objectives of Problems(Extension of work with Mayuri and Akshay)
   1. To study Components of SCADA Architecture
   2. Identify traffic characterization of SCADA Components.
   3. Literature survey and Find out the best fit algorithm for our work
   4. The system includes each components of SCADA operation is to be monitored using AI/ML algorithm for reconnaissance process.
   5. Collect and analyse data coming from SCADA operations.
   6. If data is found malicious/suspicious then keep watch and sends to incident response team for further forensic examination and then investigate report to law enforcement agency.

Reference

DFIR webs , NIST Webs, find out Blogs, find out Transaction PPrs , find out authors