Lightning Talk II - Project Planning

Team 29: Ella C. Daniel M. Westin C. Trent B.

Grid-SIEM: Defending the PowerCyber Infrastructure

CPR E 491- Fall 2023

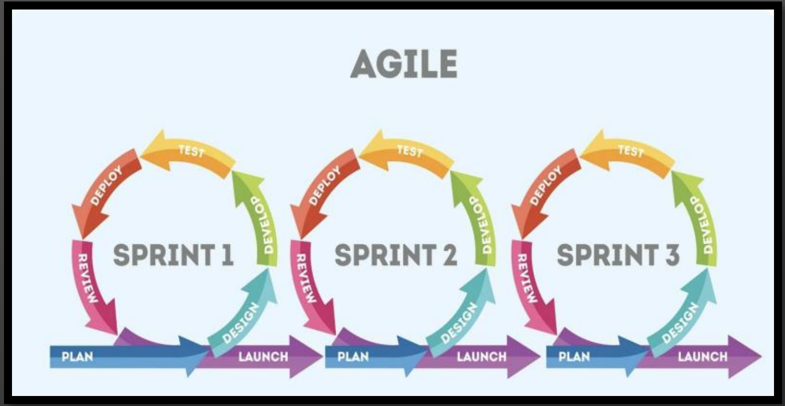
Overview

- ❖ Task Decomposition
- ❖ Project Management – Tracking Procedures
- ❖ Proposed Milestones, Metrics and Evaluation Criteria
- ❖ Timeline and Schedule
- ❖ Risks Management and Mitigation Strategies
- ❖ Personnel Effort Requirements

Task Decomposition

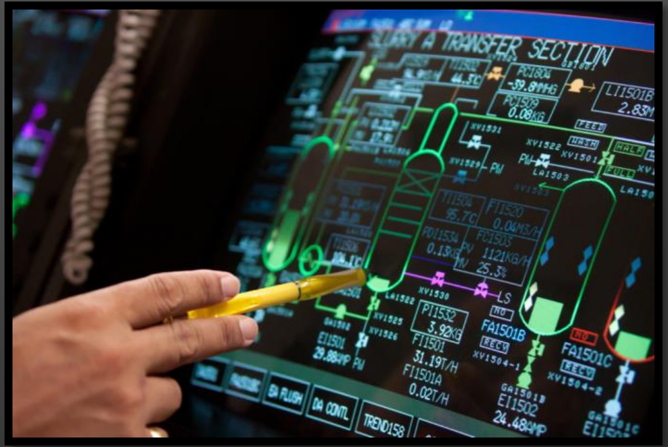
1. Integrate selected SIEM with the PowerCyber infrastructure.
   - Compare SIEMS, Set up machines
2. Within SIEM, implement intrusion detection mechanisms.
   - Master node, forward nodes, network communication
3. Develop ML/DL capabilities to enhance our project's defenses.
   - Supervised, Semi-Supervised, unsupervised, reinforcement
   - Pytorch, TensorFlow, Keras
4. Assume red team role to pentest the defense infrastructure using MITRE Caldera.
   - Create attacks and defenses

Project Management – Tracking Procedures



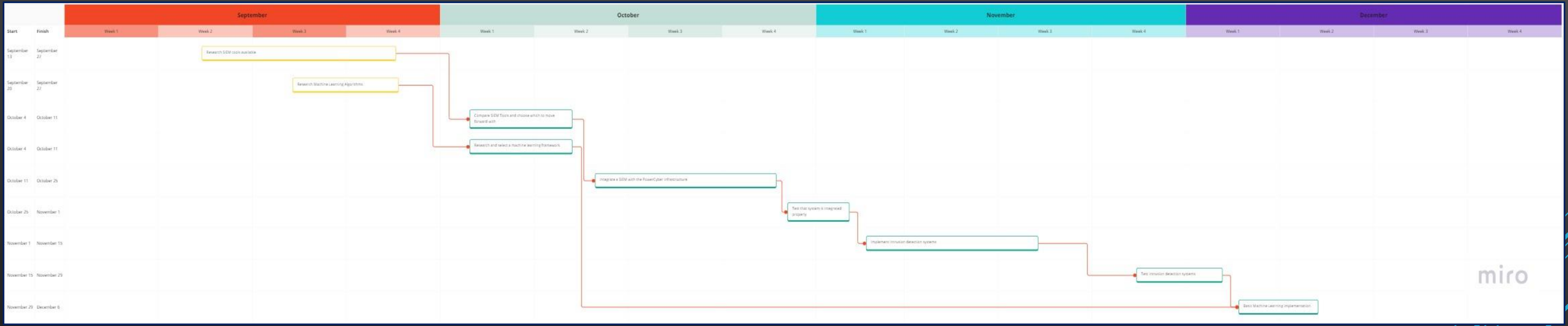
- Project management style: Agile
  - We set milestones and establish primary tasks from which to branch.
  - This way we can keep our adviser up to date on our progress and move forward only when we feel confident with our work on the milestone.
- To track progress and stay organized we use GitLab, Trello, OneDrive.
- Discord is used for communication and holding group meetings.
- The visual workspace platform Miro is used to facilitate collaboration on assignments.

Proposed Milestones, Metrics and Evaluation Criteria



- Maintain SIEM uptime based on critical infrastructure threshold of 99.99%
- IDS precision: logging and monitoring system captures meaningful data from all the nodes.
- Launch targeted attacks from Kali VM node, triage on SIEM.
- Detect 100% of attacks launched against PowerCyber systems.
- Compare and contrast commercial and open source SIEM solutions.
- Using machine learning, detect any attacks that are not previously defined. Act automatically based on training data.
- Properly establish docker environment.

Timeline and Schedule



Research SIEM Tools	Research Machine Learning Algorithms	Compare SIEM Tools	Research Machine Learning Framework	Integrate SIEM	Test System is integrated properly	Implement IDS	Test IDS	Implement Machine Learning
Sept 13	Sept 20	October 4	October 4	October 11	October 25	November 1	November 15	November 29
Sept 27	Sept 27	October 11	October 11	October 25	November 1	November 15	November 29	December 6

Risks Management And Mitigation Strategies

Risk	Mitigation
Compatibility issues with PyTorch.	If PyTorch has issues parsing data logs, we need to make sure that software is up to date and communication between software used to train ML model is not misconfigured.
Issues with the PowerCyber infrastructure. Unexpected downtime, updates and maintenance.	Push to GitLab. Take snapshots of the VMs used to host security onion nodes. Could offload logs periodically in the case of a power system issue such as the one that occurred in August 2023.
Issues feeding data into Security Onion.	Test our architecture in a sandbox.
PowerCyber infrastructure is attacked.	Use Mitre Caldera to simulate and test adversary actions? Building the sandbox node to test attacks
Potential Issues with Mitre Caldera adversary emulation platform.	Caldera docker attacks could be pushed to GitHub and not exist locally.
SaaS Platform Availability	Given that the software solutions we use are all in the cloud it is possible that their servers go down temporarily. In that case, creating backups and snapshots to start up quickly once they're back up is crucial.
Security onion system bugs – how do we mitigate this?	Vulnerabilities within our SIEM platform may compromise the reliability of our project. Staying up to date and following any news related to the software we use is key.
No supply chain risks	Our project has no physical parts to order or wait on. All software based.

Personnel Effort Requirements

Task	Estimated Time
Research SIEM Tools available - SecurityOnion, Gravwell, Splunk	5 - 10 hours
Research various Machine Learning algorithms - Reinforcement learning, decision-making, etc.	5 - 10 hours
Compare SIEM tools and choose which to move forward with	2 - 5 hours
Research and select a machine learning framework - Pytorch, Keras, TensorFlow	5 – 10 hours
Integrate SIEM with the PowerCyber infrastructure - Create boxes, nodes, master node, and various other systems needed	15 - 20 hours
Test that system is integrated properly	5 – 10 hours
Implement Intrusion Detection System and other various cyber security defenses	15 - 20 hours
Test IDS - Make sure proper things are being detected	5 – 10 hours
Basic machine learning implementation for SIEM and IDS systems	10 – 15 hours