GRID-SIEM: CYBERSECURITY FOR POWERGRID

JANUARY 24, 2024

SENIOR DESIGN

GROUP 29

DESIGN REVIEW - ACCOMPLISHMENTS

- Gravwell
  - Still very base level, not much has been done
  - Planning on implementing 1 sensor with backfill mode to pick up slack while we are down/updating
- Security Onion
  - Manager Search node on a zone and sensors in all zones, it collects data and sends it back to the manager
    - Currently only manger and 1 sensor works at the moment
  - Different tools installed like CyberChef, Kibana, Elastic Fleet

DESIGN REVIEW – ACCOMPLISHMENTS

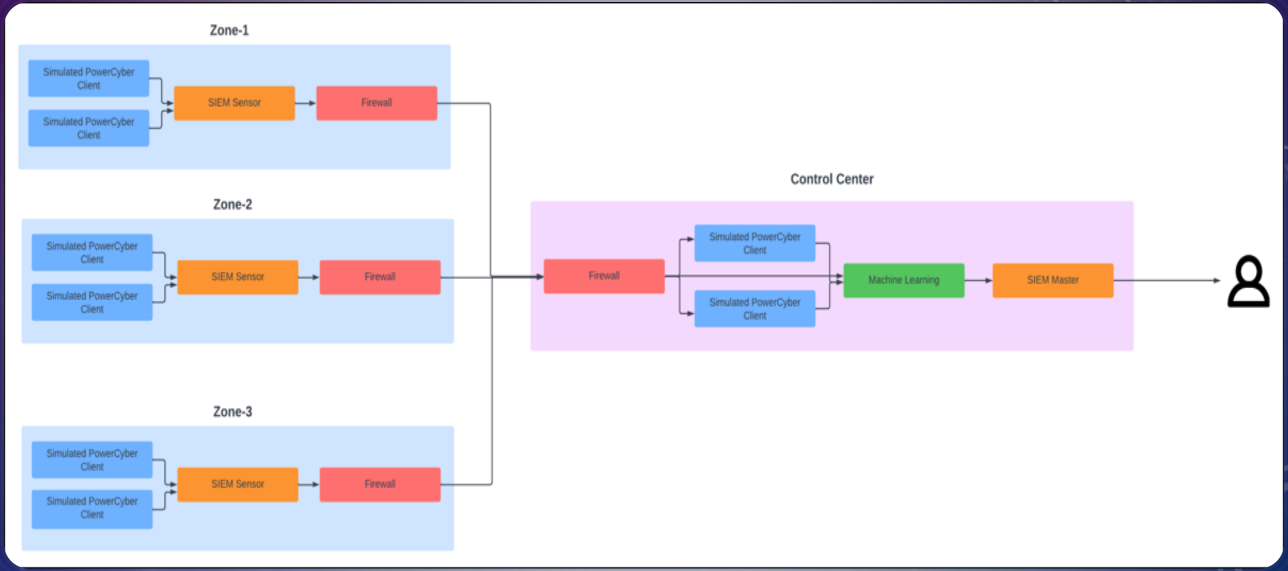
- ML
  - Train the labeled and unlabeled ML on raw PCAP logs from master SO node and a malware dump from Contagio
  - Clean trained data
  - Determine performance metrics and prediction accuracy
  - Script outline and detailed plan in place now ready for full implementation and debugging
- Mitre Caldera
  - Have the capabilities to run multiple basic attacks
    - Turn on/off power or generators
  - Many different plugins implemented for various protocols
    - DNP3, modbus, bacnet

DESIGN REVIEW

- Things Learned from Last Semester
    - Skills such as navigating and setup of a SIEM tool, familiarity with MITRE Caldera and attack payloads, general introduction to machine learning, and introduction to the Power Cyber testbed environment
    - Explaining and presenting require a more high-level approach, more context, and a greater distinction between previous semesters' work and where our project fits in
    - Gravwell is different than what we had initially thought
- Next Steps
    - Researching Gravwell and implementations online to review whether there is a place in our project for it
    - Performing an attack and verifying that the SIEM tool catches it
    - Furthering the machine learning portion of the project through training and refining
    - Reviewing attacks and getting more familiar with crafting payloads
    - Adding a SIEM Manager Search node for each zone and adjusting SIEM Manager rules and exploring Salt for remote code execution

DESIGN CHANGES

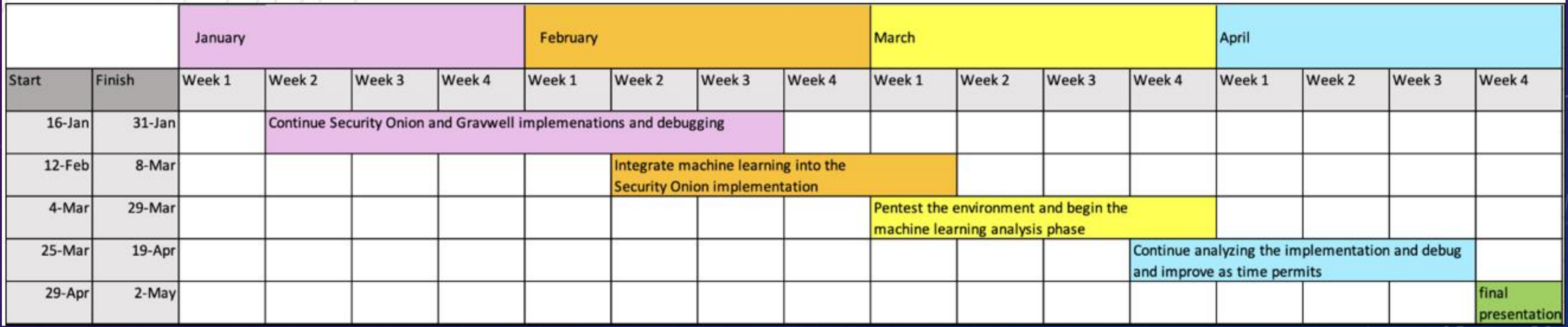
- Changes to Design
  - Reviewing where Gravwell can be implemented
  - Machine Learning component will initially be trained on PCAP files from Security Onion
  - Design Plan remains the same from last semester


Zone-1
Simulated PowerCyber Client
Simulated PowerCyber Client
SIEM Sensor
Firewall
Zone-2
Simulated PowerCyber Client
Simulated PowerCyber Client
SIEM Sensor
Firewall
Zone-3
Simulated PowerCyber Client
Simulated PowerCyber Client
SIEM Sensor
Firewall
Control Center
Firewall
Simulated PowerCyber Client
Simulated PowerCyber Client
Machine Learning
SIEM Master

OBJECTIVES AND REQUIREMENTS FOR 492

- Provide a complete and functional design
- Deliver a final report
- Deliver a project poster and final presentation
- Take a more iterative and cyclic approach to the project in terms of implementation
- Receive continuous feedback and adjust where necessary
    - weekly basis
- Engage in peer feedback activities in lecture

SCHEDULE & MILESTONES



		January				February				March				April			
Start	Finish	Week 1	Week 2	Week 3	Week 4	Week 1	Week 2	Week 3	Week 4	Week 1	Week 2	Week 3	Week 4	Week 1	Week 2	Week 3	Week 4
16-Jan	31-Jan		Continue Security Onion and Gravwell implemenations and debugging														
12-Feb	8-Mar						Integrate machine learning into the Security Onion implementation										
4-Mar	29-Mar									Pentest the environment and begin the machine learning analysis phase							
25-Mar	19-Apr												Continue analyzing the implementation and debug and improve as time permits				
29-Apr	2-May																final presentation

TEAM PROCESS IN REVIEW

- Communication: Still happens over discord and serves as the most effective method.
- Roles and Responsibilities: All group members still have their same roles as last semester, the plan for this semester is to all work on the same portion of the project before moving on.
- Goal Alignment: Project goals have remained consistent with the objectives set during the fall semester, any adjustment in the technology or procedure will not significantly impact the final deliverables.
- Task Management/Team Collaboration: To stay on track throughout the semester we have split up the project into four main portions our team will tackle each one in a set number of weeks. We will accomplish this by meeting regularly and checking-in, either in person or virtually twice every week.
- Feedback Mechanism/Adaptability: We expect each other to complete our dedicated portion of the project and ask for help if we encounter any issues. While meeting with our adviser Dr. Ravikumar throughout the semester to discuss project progress.
- Timeline and Milestones: Timeline is reasonable for what needs to be accomplished before the end of the semester.

QUESTIONS

- ?