Requirements & Engineering Standards Lightning Talk

GROUP 29

GRID-SIEM

TEAM: ELLA COOK, WESTIN CHAMBERLAIN, TRENT BICKFORD AND DANIEL OCAMPO

Problem Statement

- Overview of Project.
- What are the two main parts of the project?
- What is the project trying to solve? Why is it needed?
- What is this presentation covering?

Requirements and Constraints

- What are some significant requirements to consider for our project?
  - SIEM Nodes collect information from PowerCyber
  - Uptime near 99.99% / High availability
  - Easy to understand dashboard
- How do constraints limit what can be accomplished?
  - Focus on constraints rather than features
- What could be done as a group to reduce the impact of constraints?
  - Split up work

Engineering Standards

- ISO/IEC 27001 – This standard will be used to manage cyber risk and cyber resilience throughout the design of the project.
- NIST Cybersecurity Framework 2.0 - This standard is a combination of industry and government guidance to best follow modern cyber security practices.
- MITRE ATT&CK Framework – The MITRE ATT&CK Framework will be used along with MITRE Caldera to identify and model threats and attacks against the power grid.
- MITRE D3FEND Framework – The MITRE D3FEND Framework will be used alongside the ATT&CK Framework to implement all possible countermeasures to known cyber-attacks.
- IEEE C37.2040 Cybersecurity Requirements for Substation Automation, Protection, and Control Systems – The automation of the power grid and security measures will follow this standard.
- IEEE P1402 Physical Security of Electrical Power Substations – The physical security of the PowerCyber environment will align with the IEEE P1402 standard to mitigate risk.
- NVD CVSS v3.0 – used to score the severity of the attacks we create
- IEEE P2863 Recommended Practice for Organizational Governance of Artificial Intelligence – Specifies implementation and compliance with artificial intelligence.

Intended Users and Uses

- **Who benefits from the results of your project?**
  - The developers of the PowerCyber infrastructure at Iowa State University.
  - The IT community invested in securing industrial control systems.
  - Students at Iowa State within the ECPE department could learn from our project
- **Who cares that it exists?**
  - Dr. Ravikumar is invested in the outcome of the project.
  - Students at Iowa State could later use it as a tool to learn about attacking and defending critical infrastructure.
  - SecurityOnion enthusiasts and the open-source software community would take interest in our use and implementation of the free SIEM-solution.
- **How will they use it?**
  - The final product will be used to ensure the PowerGrid can operate with minimal overall risk of a cyber-attack and resulting down time.
  - Students can use our project to test their ability to attack and defend an OT system.
  - Since the final product should ideally be a safe and secure power grid, students could test their red and blue team skills by attempting to break into and then patch the Grid-SIEM. This could serve as a supplementary component to the ISU CDC.