sdmay22-38

Members:

- Alex Nicolellis
- Jung Ho Suh
- Muhamed Stilic
- Pallavi Santhosh

1.1 Problem Statement

Our team is using cybersecurity tools to design a surveillance program for power distribution companies to detect and prevent electronic security breaches.

1.2 Requirements & Constraints

Functional Requirements:

1. The surveillance program **shall** analyze alerts across time.
2. The surveillance program **shall** display alerts to allow for easy human access and understanding.
3. The surveillance program **shall** show visualization of intrusion detection results using SecurityOnion and SIEM.
4. The surveillance program **shall** conduct *vulnerability scanning of specific IP addresses.*
5. The surveillance program **shall** verify incoming alerts and discard false positives.
6. The surveillance program **shall** be able to zoom in to the details of the alert.
7. The surveillance program **shall** be able to show corresponding sensors to each anomaly.
8. The surveillance program **shall** be able to send information to the alert correlation master through the cloud system.
9. The surveillance program **shall** be able to log information about the events that happen.
10. The surveillance program **shall** be able to allow users to add/edit rules of each sensor.
11. The surveillance program **shall** be able to detect temporal and spatial correlated anomalies.
12. The surveillance system **shall** be able to use machine learning to detect anomalies.
13. The surveillance system **shall** be able to visualize the graphs from the logs.
14. The surveillance system **shall** be able to sort all of the results for the user.
15. The surveillance system **shall** be able to be modified into different power plant cloud systems.

Non-Functional Requirements:

1. Would need internet speeds up to 1Tb/s.
2. User Interface should be easy for the power plant users to operate the system.
3. Should have backup systems in case one is shutdown.
4. The system should be able to have strong processing requirements to run so there are no interuptions.
5. The system must have images for each report to let users know how the attacks are happening.
6. The system should have a log tab for easy access to the related logs.

7. The alerts should be sent at a speed of 1-5ms for quick recovery.
8. The layout of the program should be easy for the user to navigate through and make edits to rules.
9. The design of the logs should make the anomalies easy for the user to understand.
10. The alert should be colorized to indicate what anomalies are critical or not.
11. The system should be reliable and have no bugs when dealing with issues.
12. There should be an application or website where a user can add or edit rules and view reports.
13. The login system should only allow people who have authority to access the surveillance program.
14. The system should be able to process a large amount of information without crashing.
15. The security system should encrypt all information related to security.
16. The cloud system should operate 24/7 to mitigate threats.

Constraints:

1. Interact with a pre-existing system of sensors.
2. Interface with the provided cloud computing system.
3. Use industrial standard protocols such as **DNP3**, and **Modbus**.
4. Use **SecurityOnion** tools

1.3 Engineering Standards

Standard	Application	Justification
IEEE 1711.2-2019	**Grid**	Protects communication of intelligent devices in the power industry.
IEEE 2030.5	**Grid**	Defines the proper manner to convey secure application messages.
IEEE 692-2013	**SecurityOnion**	Addresses cybersecurity and control related equipment requirements for threat assessment.
IEEE 2413-2019	**Grid**	Defines proper architecture for internet of things technologies

ISO IEC 27039-2015	**IDPS**	Provides guidelines for selection, deployment, and operations of intrusion detection system detection and prevention systems. (**IDPS**)
ISO/IEC 27017:2015	**AWS**	Provides guidance on the information security aspects of cloud computing, recommending the implementation of cloud-specific information security controls that supplement the guidance of the **ISO/IEC 27002** and **ISO/IEC 27001** standards.
IEEE 802	**Wireshark**	Describes recommended practices for communication over various types of networks, such as wireless networks.
IEEE P2994	**OpenVAS**	Defines a mechanism for evaluating IoT application security.

1.4 Intended Uses and Users

As of now, the detection system in place is lacking a master program to analyze security breach alerts. Once implemented, the anomaly detection system will possess a deeper understanding of the anomalies it senses. A major benefit of our program will be that it takes away the need for a host to double check whether or not a detected anomaly is a false positive because it will be able to do that as part of its design.

Power distribution and utility companies (ex. City of Ames Iowa Electric Services) will benefit from the implementation of this project because they are the ones who will have to deal with intrusions on the grid. More areas include (but are not limited to) DER field devices, plant controllers, and grid edge hardware.