Requirements Engineering

Business and Functional Requirements

Functional:

1. Datasets that are designed for the purpose of benchmarking anomaly detection machine learning programs.
2. An understanding of valid anomalies and with that benchmarking/ training a machine learning model to assess dataset anomalies as a threat or not
3. Streaming capabilities for new incoming data so it may be assessed with the data model.
4. Visualization for users to understand the quantity and risk of anomalies that occur.
5. Anomalies must be detected and all network traffic must be logged(suspicious/evil/clean)
6. The system should be able to generate reports or summaries of the anomalies detected.

Non-Functional Requirements:

1. When an anomaly is detected a message is sent to the client in near real time
2. The system should be able to handle increasing amounts of data and users without losing performance or functionality
3. The system should prevent unauthorized access

Business:

1. This project uses Amazon Web Services streaming platforms and would require the setup of streaming logs to the anomaly detection application.

Technical Requirements and our Prioritizing of each is shown in our Trello, a screenshot of it has been submitted.

Available Resources:
Any publicly available datasets can be used to detect anomalous events.
AWS Kinesis/Spark streams, spark streaming, SQL or other similar streaming technologies can be used