CAPSTONE DESIGN EXPO

Computer Science

CS 316

Near Real Time Anomaly Detection

Team members: Gavin Cutchin, Gabriella Rivera, Jared Dunn | **Faculty adviser:** Dr. Changqing Luo | **Sponsor:** Capital One | **Mentor:** Geeta Shyamala

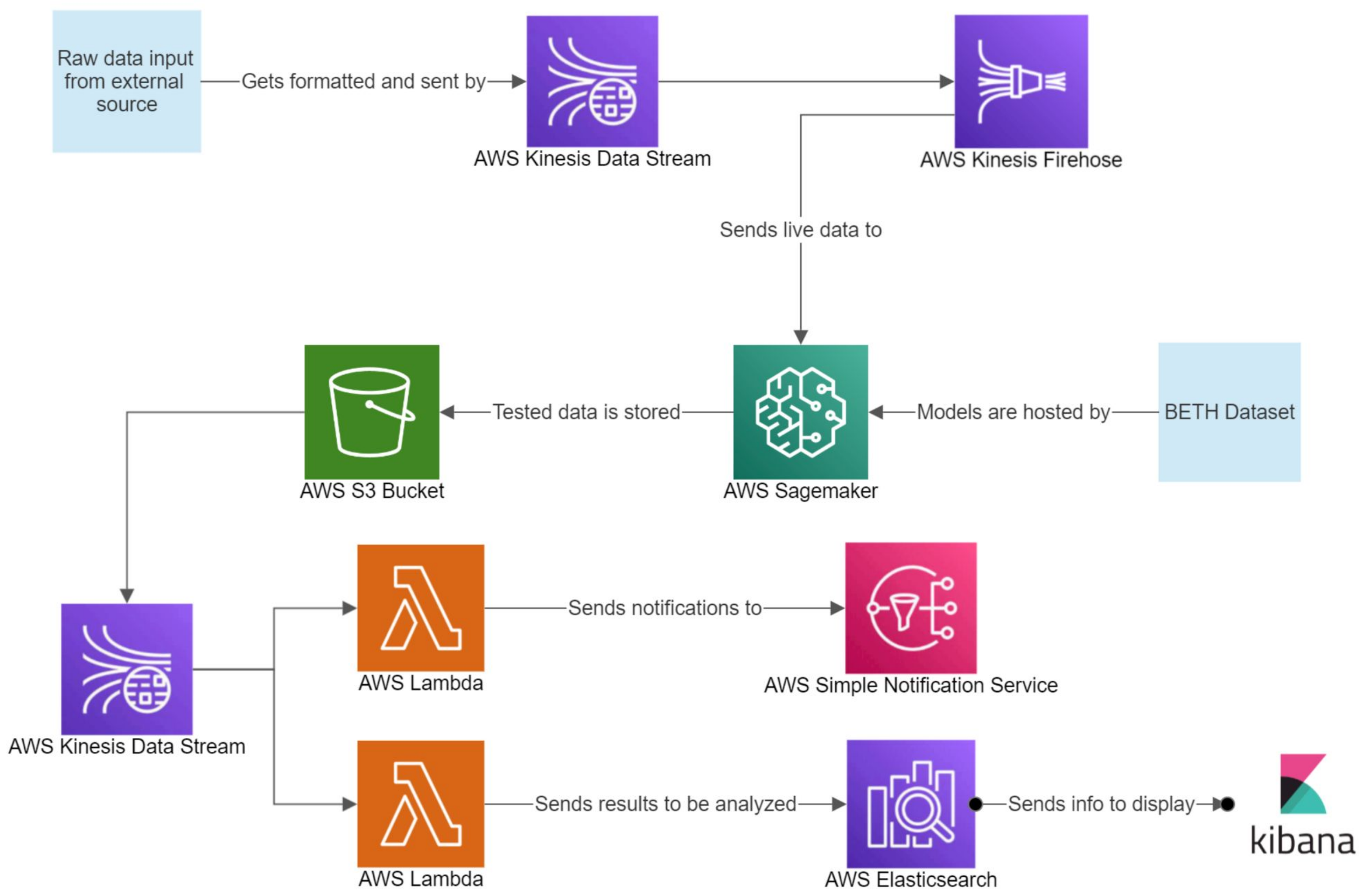
Problem Statement

- Anyone with sensitive information requires a way to protect their information and assess threats the moment they occur.
- The goal of this project is to develop an application that reads event logs and alerts the user of anomalies when they happen.
- Anomaly detection of entity behavior from event logs is possible by using data that has been synthetically produced to benchmark machine learning and create the basis for the anomaly decision process.
- Using this benchmark, any new event logs will be compared against the machine learning model and produce the expected result.

Social Value

- In an age of rapidly advancing technology, we must be vigilant of entity behavior that may pose a threat to data and network security.
- This project aims to detect these behaviors and ultimately prevent malicious actions.
- This proactive approach can have a positive impact on the world by helping to prevent financial disruption as well as maintaining reliability in the technology that we use in our daily lives.
- In such a perilous world, maintaining trust and reliability between a company and its users is proving to be a vital necessity.

Flow Diagram



Raw data input from external source

Gets formatted and sent by

AWS Kinesis Data Stream

AWS Kinesis Firehose

Sends live data to

AWS S3 Bucket

Tested data is stored

AWS Sagemaker

Models are hosted by

BETH Dataset

AWS Kinesis Data Stream

AWS Lambda

Sends notifications to

AWS Simple Notification Service

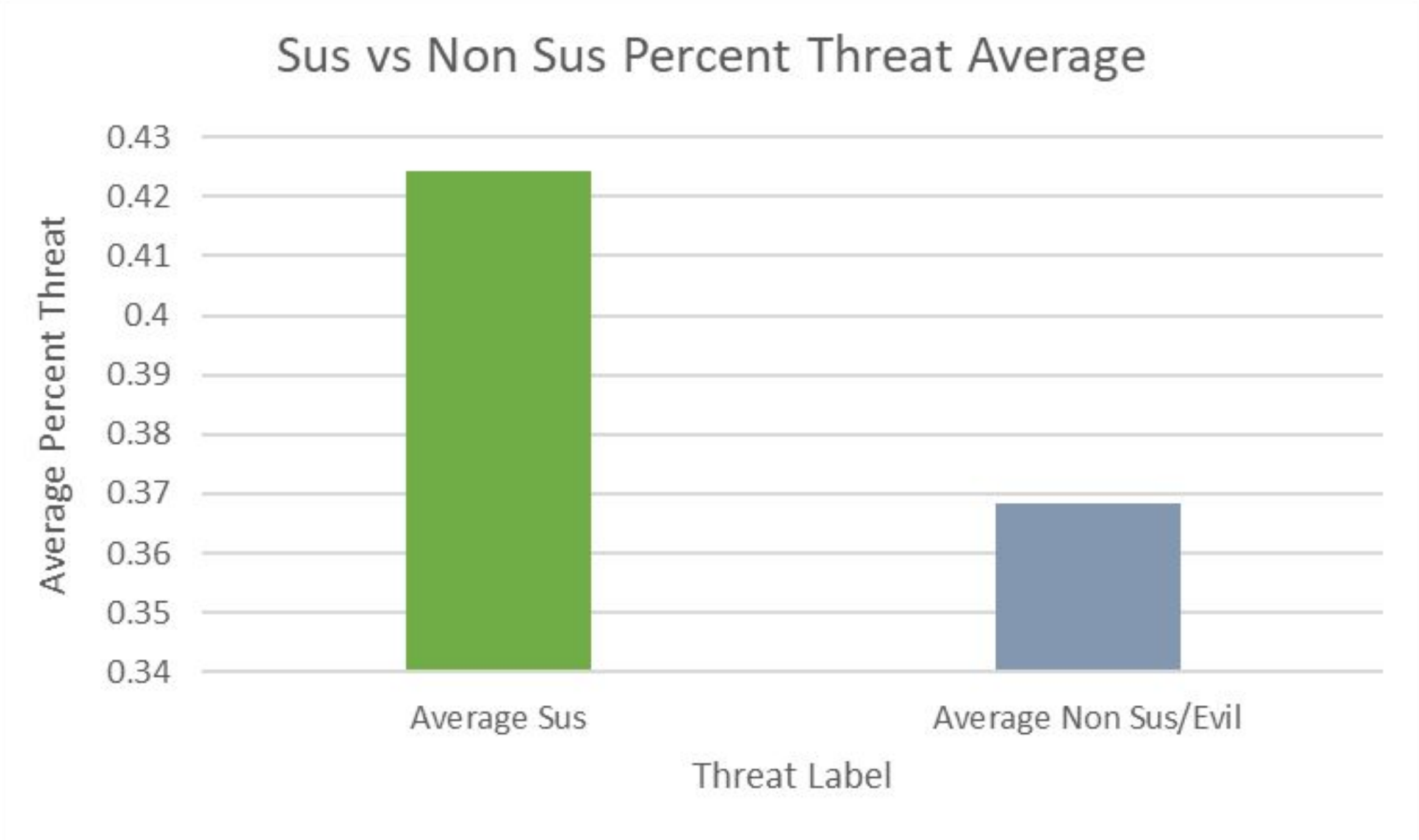
AWS Lambda

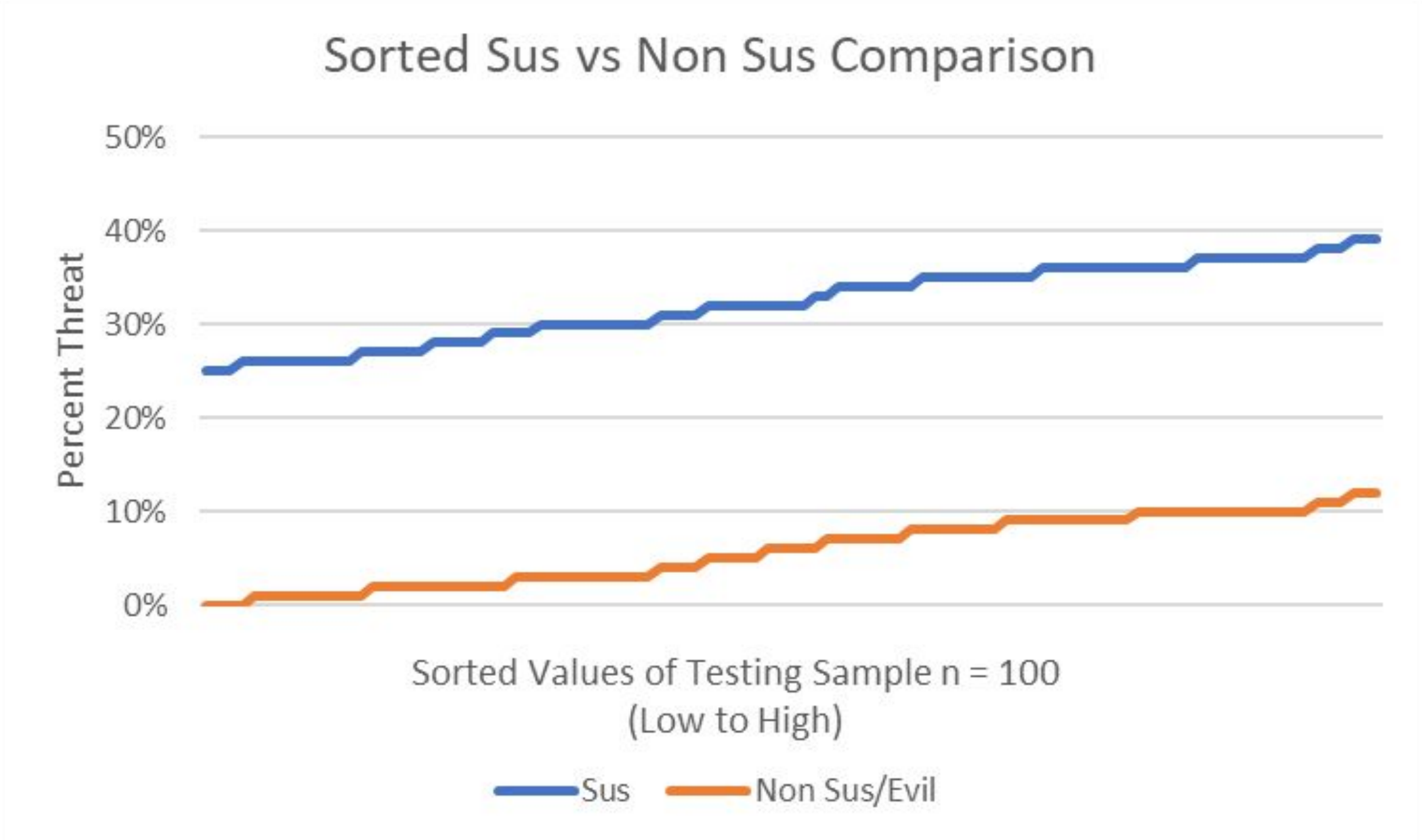
Sends results to be analyzed

AWS Elasticsearch

Sends info to display

kibana


Sus vs Non Sus Percent Threat Average


Sorted Sus vs Non Sus Comparison

Features

- The model can takes in data, processes the data, and could use it as baseline or labels them as Evil or Friendly
- A notification can be sent with the results being seen for the network traffic
- The model will record results of the data and automatically save the information to a S3 bucket csv file

What's Next

- To see how impactful the model can be we can evaluate its performance over time and see the advantages it delivers
- We can integrate a notification system along with the model where stakeholders can take action when an anomaly is detected
- Have an automated response or action take place when an anomaly is detected that doesn't need an action from a user

aws jupyter NumPy PyTorch scikit learn TensorFlow

VCU College of Engineering