GE Cybersecurity Software Development Hackathon

Project Overview

Scenario:

GE employees receive thousands of phishing attempts each day from external players attempting to gain access to GE systems and steal GE Intellectual Property. GE has many security measures in place in order to stop these emails from getting through. These security measures look for several “indicators” in all parts of the email that it uses to determine what should and shouldn’t be allowed through. However, sometimes the systems are unable to decide, at which point, the GE Cybersecurity Analysts take over and decide on each themselves.

Recently, there has been a large increase in the amount of emails the analysts have been getting, and they have been unable to keep up with the growing list. You have been tasked with solving this problem for the analysts using software, however you can. The only requirements you have been given are the software solution must be able to get the data from the endpoint that has been created for you and facilitate the process of determining what is a true positive and what is a false positive.

Notes from the Analysts to keep in mind:

1.) The analysts began creating a solution with the same intention, but were unable to finish. You are free to use this solution, or start from scratch if you’d like.

2.) Since this solution is for cybersecurity purposes, its own cybersecurity is important. The more secure and less vulnerable it is, the better.

3.) This solution will be used by an entire team of cyber security analysts to do their job everyday, so its important that it is easy to use and good at what it does.

4.) The analysts’ current process for this doing this task is slow and unreliable. It is important that this new solution does not have same issues.

5.) The analysts have noticed patterns in the emails that come to them like similar senders, contents, or subjects, some are targeted at similar recipients, some have clearly unsafe attachments, etc. A solution that can find and reflect these patterns would be helpful.

6.) The endpoint that the data is coming from can be problematic, often losing or repeating or changing the data. The analysts think it would be very helpful to ensure that they are getting all of it correctly and be able to view any of it when they need to.

7.) There are no wrong answers to this problem and all progress is good progress.

The analysts know that developing a software solution is not an easy or quick task, especially under your given constraints, and hope that you will work with your team on what you think is most interesting or important or helpful. Some of the best solutions come from trying something new complemented by doing something you know well. There are many other teams also trying to build the best solution possible, so ingenuity and teamwork are key. The winnings solution(s) will be chosen based on effort, execution, creativity, and, especially, how you communicate the work that you did.