A Cyber ChatBot

There needs to be disruption in how cybersecurity experts do their work. It is estimated that there will soon be a shortfall of a million cybersecurity analysts needed to protect computer systems worldwide. For this project, we want to investigate the construction of a Cyber Chatbot. A powerful chatbot that can perform menial or repetitive tasks or work along side human analysts could significantly increase the effectiveness of security analysts and help with the increasing demand for humans.

A Cyber Chatbot should be able to answer relatively simple questions about a file asked in natural language. For example, a question like "*Do you think that this file is malware?*" should get an answer like "*I found 13 models that have made a prediction on this file, with 7 out of these 13 models predicting this file to be a Trojan. The other 6 models predict it to be either a Worm (4 models, 85%) or an Adware (2 models, 80%). The average likelihood of it being a Trojan is 71%*" perhaps followed by a summary table presenting the result for each matching model. Such an answer requires the chatbot to understand which models can answer the user question then summarizes the models results in a few sentences. Given that it is a natural language chatbot, question like "*Is it Malware?*", "*Could it be Malware?*" and similar (including grammar/spelling mistake) should yield the same results.

Project Ideas:

1. Download the Demisto Chatbot (https://dbot.demisto.com) and identify three to five important features. Try reimplement using Lex.
2. Access CavazosLab research data and identify parts of the data that could be used to answer English-like queries.

The deliverable for this project should follow the format of the AWS Serverless Chatbot Competition (https://aws.amazon.com/blogs/aws/enter-the-aws-serverless-chatbot-competition/). The team could use with Lex from Amazon as a starting point. Another chatbot framework could be used, but this should be discussed with the instructor. The code should be implemented on AWS using Python.