1. Hi all, AI has exploded in popularity, and implementing it into an environment requires secure and proper implementation is necessary for a functional model.
2. 1. The corporate team has been developing a chatbot named Vera. In order to use this chatbot in their environment, they have been working to securely implement a ML mechanism that can connect with Lazard’s internal data.
   2. One security measure that is in place is that the model will sit in a private environment, only able to communicate within Lazard’s internal data. Hosting the model on a private network helps protect the model from unauthorized access, data breaches, and other forms of cyber-attacks.
   3. Another security measure that is in place is how you can interact with the model. The only way to connect to the model is through the SPFx user interface.
3. 1. Here is a diagram showing how the chatbot works starting from the user. The user can seamlessly execute tasks in multiple services following orchestrated business processes.
   2. This input is passed through cloudfront and sent to the vera mechanism over HTTPS. From here, Vera gathers the data from its secure area and sends the information back to the user. All the information received and sent out is secured with HTTPS communication.
   3. The communication between user, model, and data are all secured which protect the data while in transit.
4. 1. Other security measures that take protect the model are practices already in place but expanded on.
   2. For example, one recommended practice is to limit the model’s capabilities to only be functional. One way to do this is by implementing a human in the loop control. An example of this could be allowing the model to build a help desk ticket for you, but you have to send it out, the model cannot.
   3. Another recommended practice is to have secure coding and proper input validation and sanitization. This should be used to help filter out malicious inputs and help validate training data and responses from the model.