Lumberjack - Definition of our team project

Marino Oliveros Blanco NIU: 1668563
Luis Domene García NIU: 1673659
Alejandra Reinares Guerreros NIU: 1665499
Álvaro Sáenz-Torre de Torre NIU: 1672425
Joan Bayona Corbalán NIU: 1667446

Scope:
Potential Features

- Real-Time logs score computation.
- Extract CSV of suspicious logs with the reasons in order to be checked by a data analyst.
- A single log analyzer where you can introduce a specific log that you want to check, so that it provides score and reasons.
- The model will be retrained with new data every now and then. The specific amount of time between retrainings will be selected by the company. Another option will be to retrain the model after a certain amount of logs.
- Our product is NOT responsible for determining which logs are malicious. It only determines which logs are suspicious (abnormal activity) in order for them to be checked by a data analyst

Quality:
Our product will be presented as a web application, working in real time, this web app will be built using Python Django; Django is used by many successful companies to develop their web-apps like Instagram, Spotify or even CyberChef, on a more cybersecurityesque approach.

Lumberjack will be a top-notch cybersecurity measure, correctly discriminating against malicious logs. The app will have the capabilities to be linked to any web register and perform its functions there. Lumberjack is fueled by a machine learning algorithm trained to analyze logs with above human capabilities. We ensure that the logs are kept private and only available to the client of its particular registry.

Resources:
As a team of 5 soon-to-be AI professionals we will use open-source frameworks to produce Lumberjack, Django in itself is open source as well as any AI model that we built will be made open source to ensure trust with our clients and not violate anyone’s privacy. The development process will be updated and explained step by step in a ‘Git-like’ service.

Risks:

- Lumberjack could suffer from an enormous quantity of logs.
- Being an AI model based web-app, we require data to train the model, data that could be insufficient.
- As a cybersecurity application, Lumberjack must be secure itself and protect the privacy of each one of its clients.

Other Constraints:
Our team believes in being open-source, so all of the software we create/use will be open-source.