ABSTRACT:

More than 60% of the world’s population contributed, in some way, to internet traffic in the first quarter of 2021. Distributed computing has been very eventful and is very clear that it is here to stay. Even companies with a long on-premise legacy are rapidly adopting cloud infrastructure to ensure business continuity. Advancements in network security also need to be disruptive to be on par with the ever-growing need. With the proper big data tools, the insights from historical network data can be a game-changer in how enterprises deal with network security. Our project proposal is to make an intelligent security system that can detect ongoing cyber-attacks and classify the kind of attack, to aid in deploying automated countermeasures, in time. We also propose extracting impactful analytical insights from historical and rapid incoming data, as feedback to enterprises to make informed corporate decisions. This equips organizations to be well-prepared and be the front runners in maintaining a state-of-the-art security portfolio.

BIG DATA PROCESSING / INSIGHTS:

- Data loading- Streaming data + ETL
- Anomaly detection
- Cyberattack classification
- Most frequently attacked/vulnerable resources
- Detecting patterns in cyberattacks
- Intelligent Insights – autoscaling on network traffic classified as non-suspicious, recurring analysis of security status, region-based security recommendations

TECHNOLOGIES PROPOSED:

- Spark for model training
- AWS storage – Data / Artefacts like security reports and analysis
- Apache Kafka
- Apache Storm
- Tableau UI for Dashboard

Group Members

1. Gokul Mohanarangan, gma56@sfu.ca, #301436162
2. Pranav Balaji, pba34@sfu.ca , #301427935
3. Shivek Chhabra, shivek_chhabra@sfu.ca, #301432876