

TELEKOM AI HACKATHON FOR DIVERSITY

DETECT TO PROTECT

Team Green

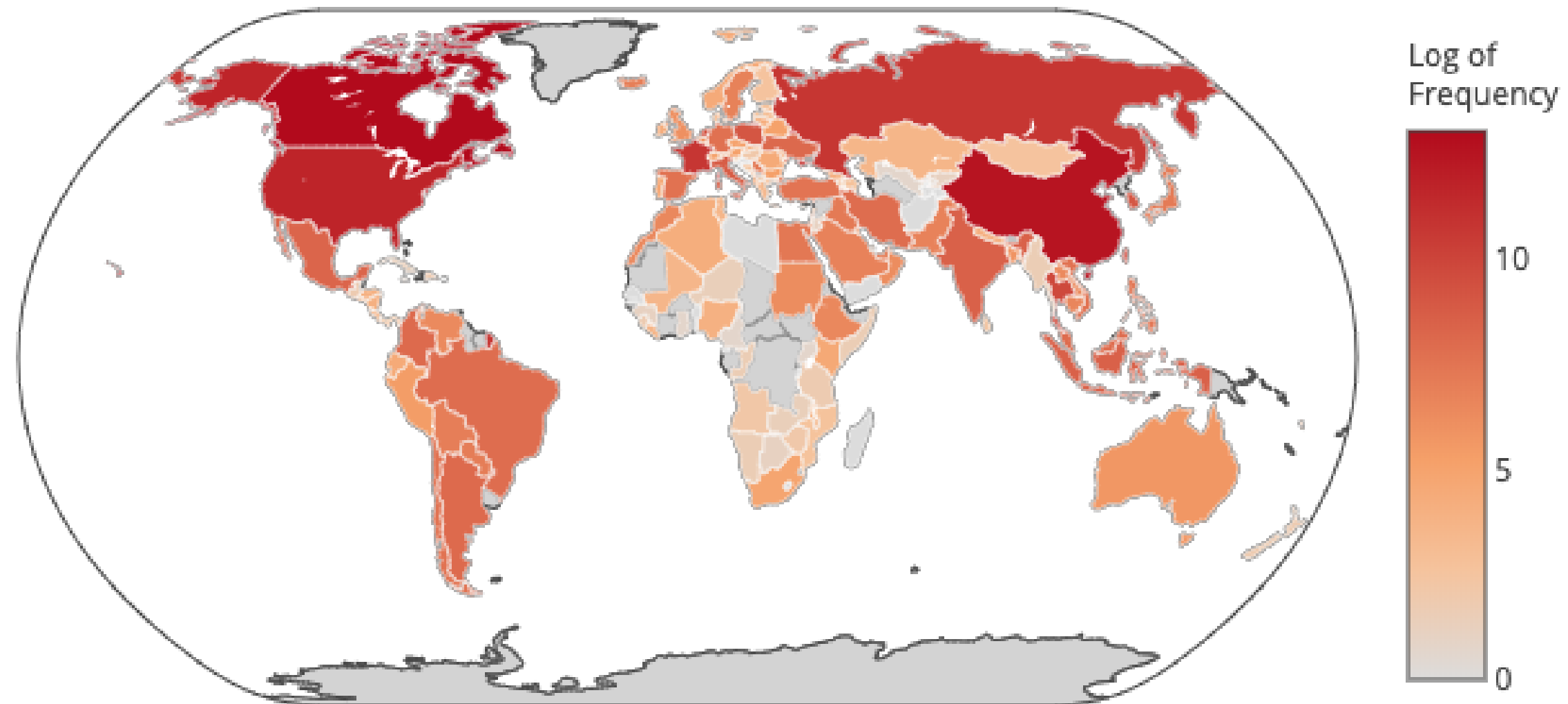
Challenge

Understand cyberattack patterns from honeypot data

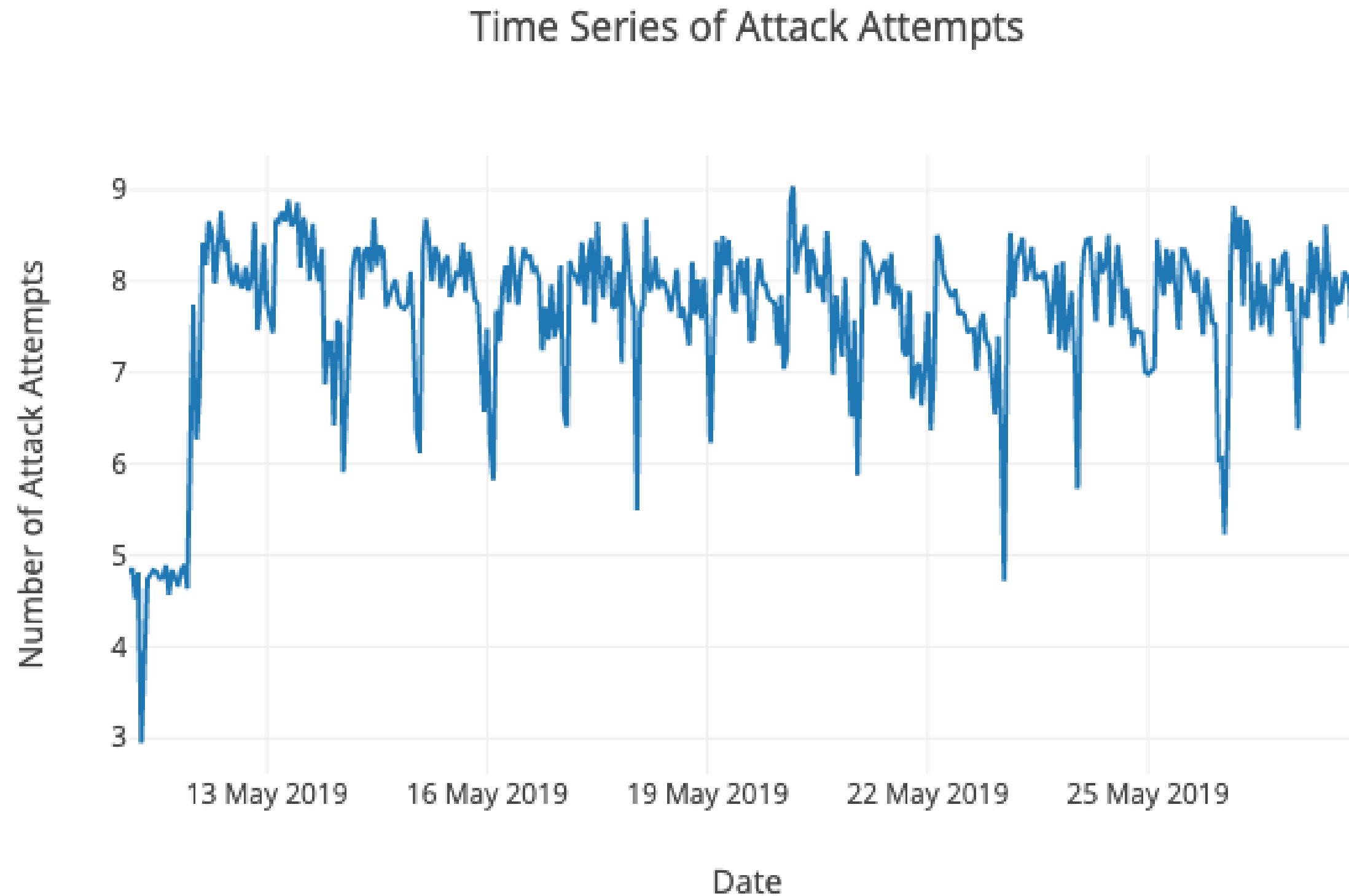
Generate business recommendations from insights

Telekom Honeypot Attack Origin

Honeypot Attacks Origin by Country



Overall patterns of attacks

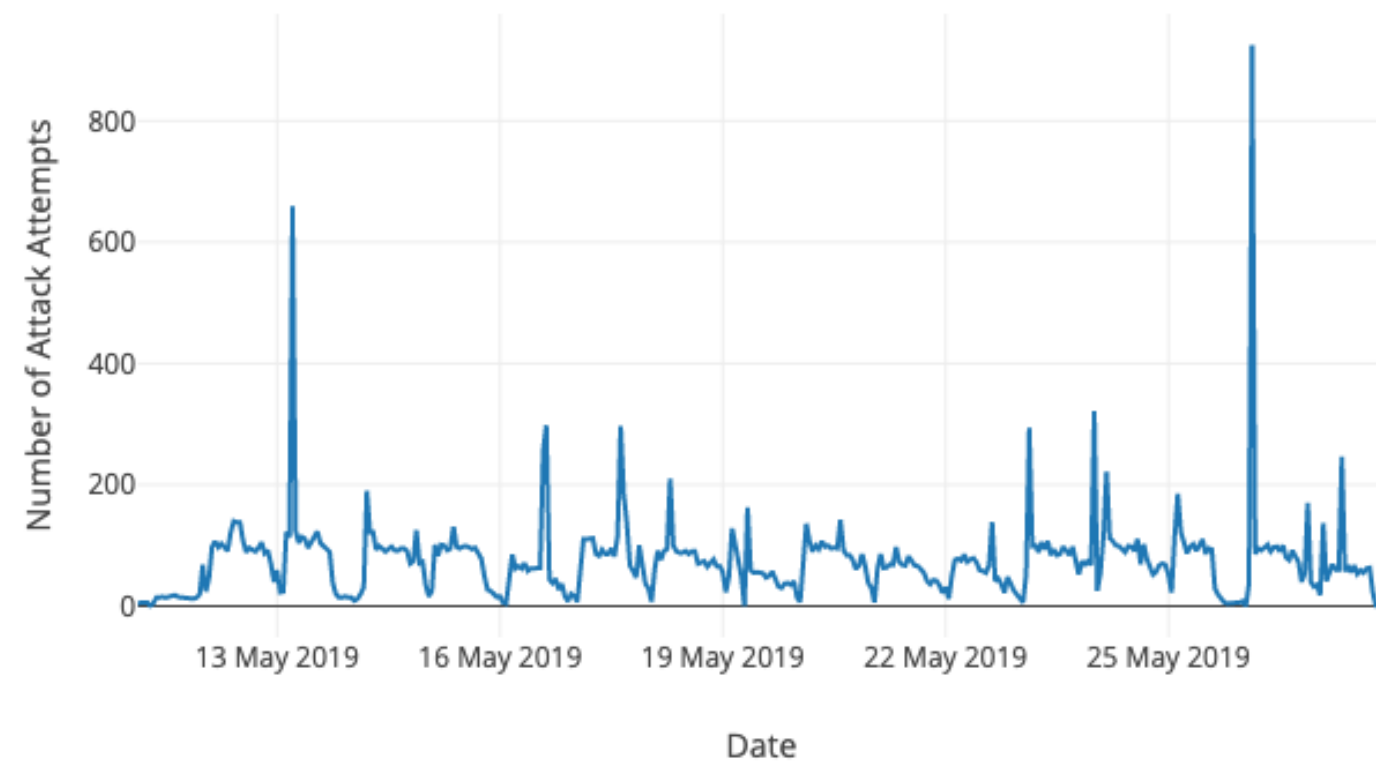


ATTACK PATTERNS

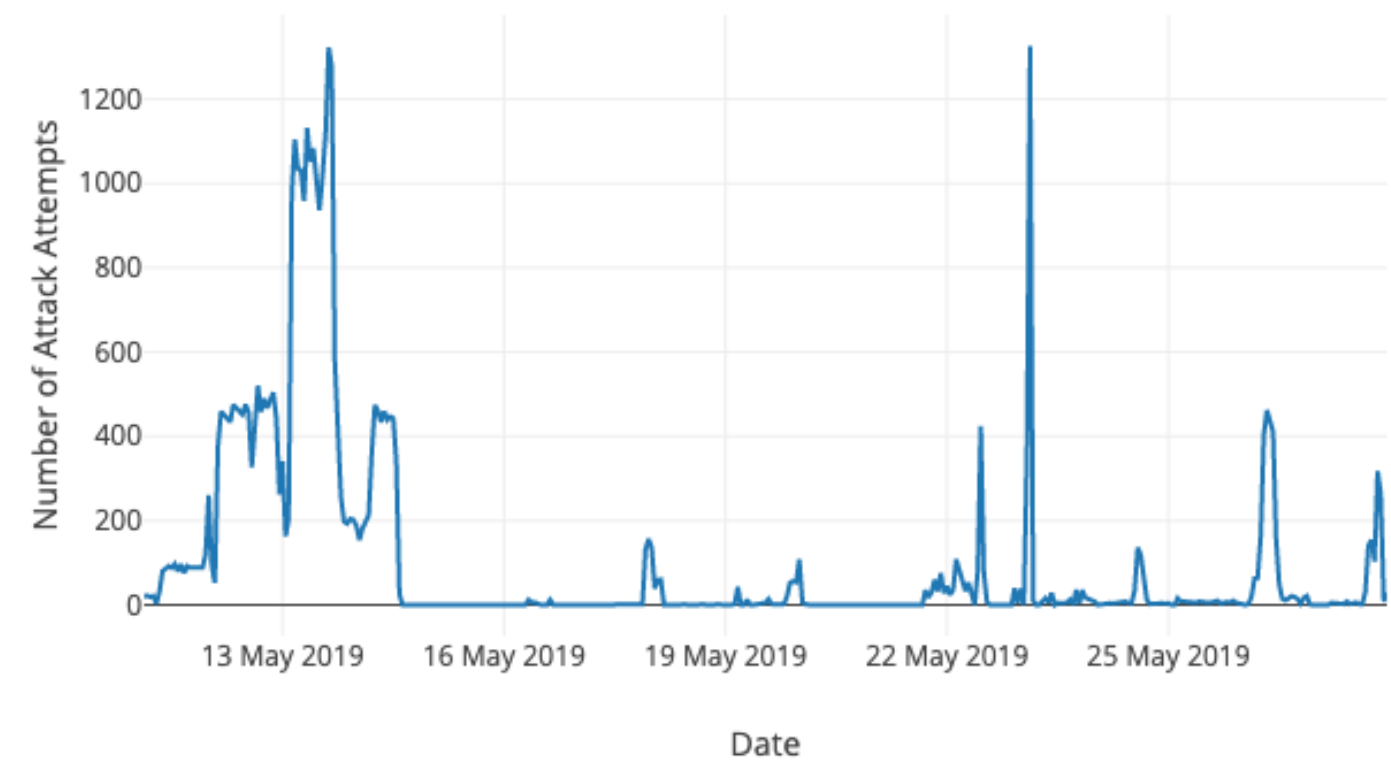
Regular

Irregular

Time Series of Attack Attempts (37.751,-97.822)



Time Series of Attack Attempts (54.9978,73.4001)



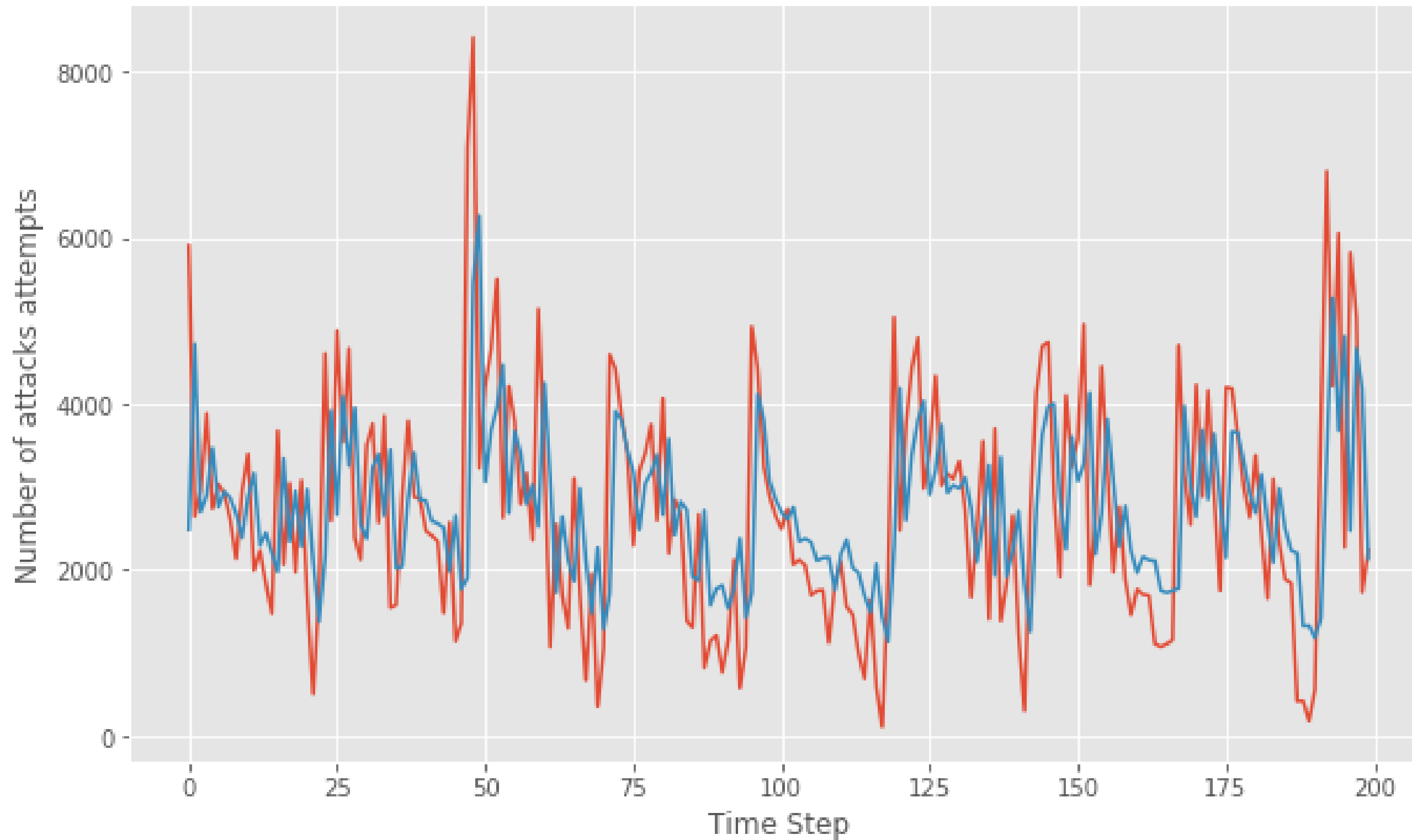
Solution Stack

Recurrent Neural Network

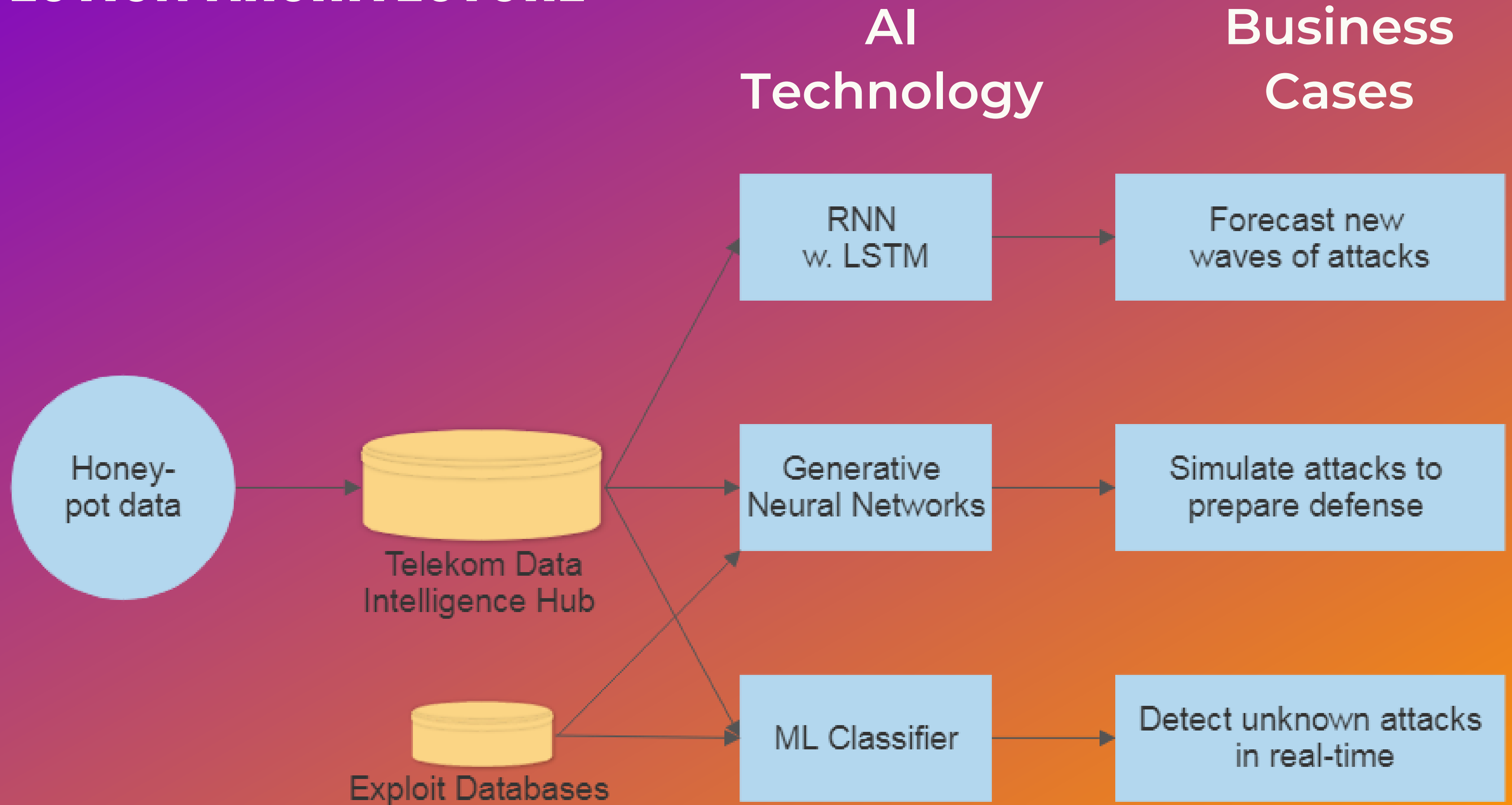
Generative Neural Network

Forecast potential waves of attacks

Forecast cyberattacks on Telekom with Recurrent Neural Networks (Actual vs. Prediction)



SOLUTION ARCHITECTURE



ETHICAL ASPECTS

- ANONYMITY
- PRIVACY-PRESERVING

SCALABILITY

- SIMPLICITY OF DEPLOYMENT
- EASE ON NETWORK LOAD

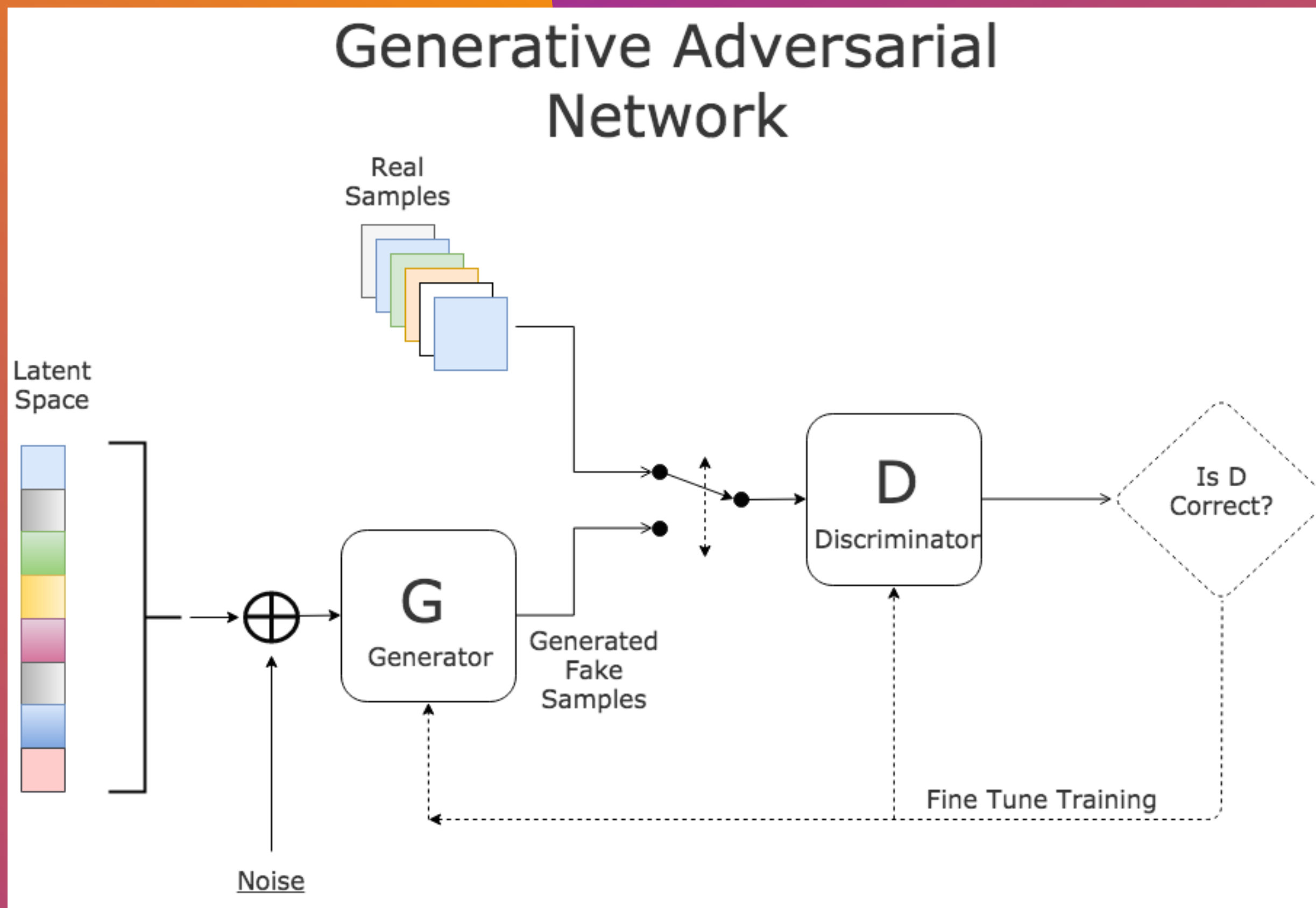


TELEKOM AI HACKATHON FOR DIVERSITY

THANK YOU!

Team Green

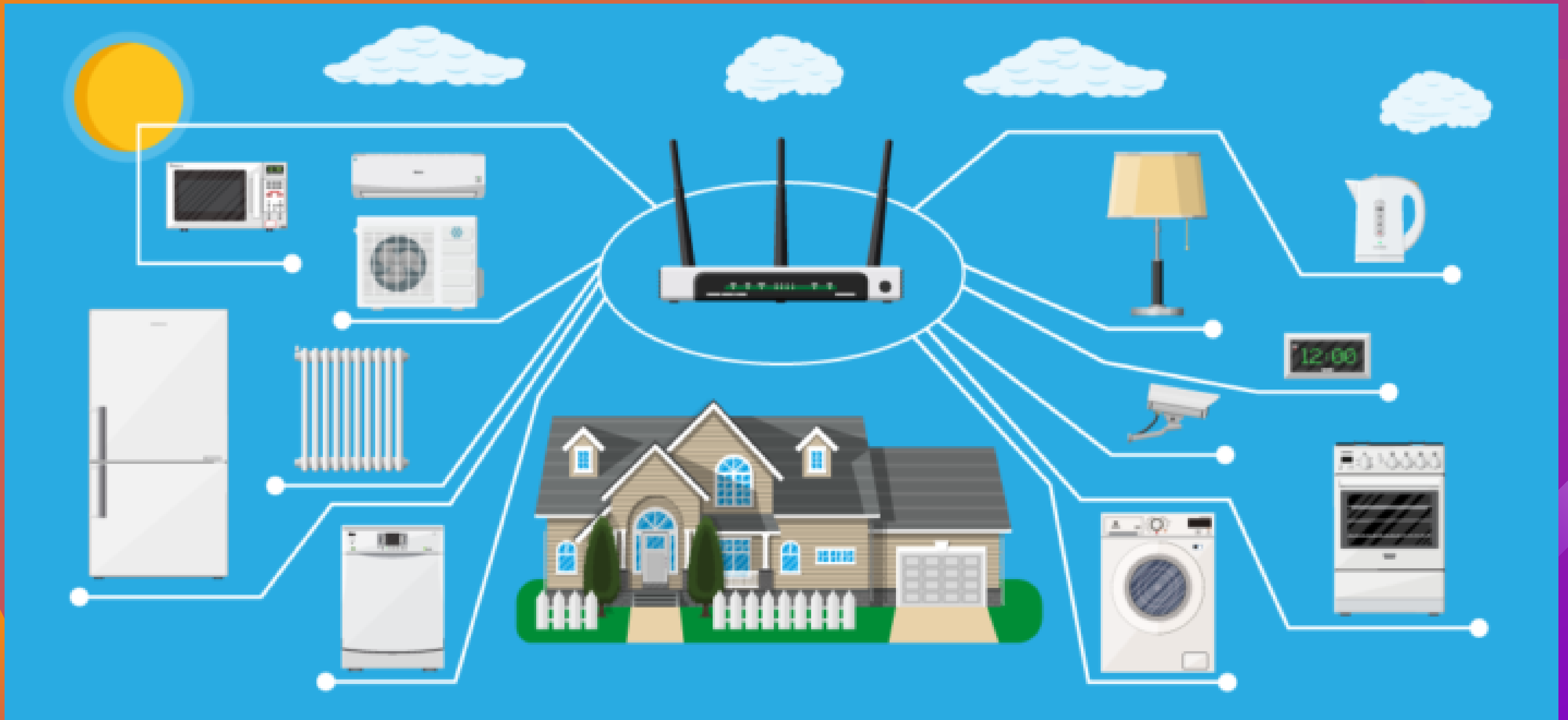
Generate new and unknown attacks



What is Botnet?



Most smart devices (IoT) vulnerable to cyberattacks



SNMP Traffic

Time Series of Attack Attempts (37.751,-97.822)

