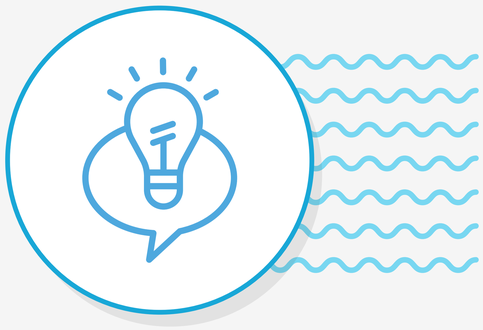

Brainstorm & idea prioritization

Brainstorming and idea prioritization for the concept of network anomaly detection using artificial intelligence to detect unusual patterns within network traffic Brainstorm and idea Prioritization for the concept of Network Anomaly Detection

10 minutes

1 hour to collaborate

2-4 people

1

Problem statement

Problem statemen on how to implement the Network anomaly detection

5 minutes

PROBLEM

How might we create an advanced tool powered by artificial intelligence to detect unusual patterns within network traffic?

Key rules of brainstorming

To run an smooth and productive session

- Stay in topic.
- Encourage wild ideas.
- Defer judgment.
- Listen to others.
- Go for volume.
- If possible, be visual.

2

Brainstorm

Ideas from each team member

10 minutes

ROHIT

Determine whether an unsupervised approach or supervised learning is more appropriate

Determine the primary objectives of network anomaly detection

KARTHIK

Collection of wide range of data sources

Processing the data

LEVIN

Develop models that understand normal user behavior and detect deviations, which could be indicative of insider threats

Develop a feedback mechanism to continuously train and improve the AI model

VASAN

Building a data set and labeling them accordingly

Integrating AI Tools

3

Group ideas

Group ideas for Network Anomaly Detection

20 minutes

Data and data sources

Data Integration: Explore ways to collect and integrate diverse data sources, including logs, network traffic, system metrics, and security event data.

Data Preprocessing: Develop strategies for data cleaning, normalization, and feature engineering to make the data suitable for AI models.

Artificial intelligence Techniques

Machine Learning Models: Consider various machine learning models like deep learning, random forests, and clustering algorithms for anomaly detection.

Reinforcement Learning: Explore the application of reinforcement learning for adaptive and self-improving network security.

Reporting

Anomaly Visualization: Design effective visualization tools to help operators and analysts understand network anomalies.

Reporting Dashboard: Create comprehensive reporting dashboards that provide insights into network health and security.

4

Prioritize

Ideas that are important and feasible.

20 minutes