Ideation Phase

Empathize & Discover

DATE	15-10-2023
TEAM ID	4.1
PROJECT NAME	NETWORK ANOMALY DETECTION

MENTOR : P MANOJ

Team Members :

C DEVAKI NANDAN REDDY

S NIHAL AHMED

EMPATHY MAPPING :

WHO are we empathizing with?
WHO are we empathizing with?

Concern for the organization's data and infrastructure.

Frustration with the complexity of identifying network anomalies.

GOAL

The pressure to respond quickly to security incidents.

What do they need to DO?
What do they need to DO?

A desire to stay ahead of cyber threats and protect the network.

Graphs and visualizations of network traffic.

What do they HEAR?
What They Hear

Feedback from colleagues about potential incidents.

Security experts discussing emerging threats.

User complaints about network performance issues.

Updates and recommendations from security software vendors.

What do they THINK and FEEL?

PAINS
Balancing network performance with security measures.

GAINS
Improved network security through proactive anomaly detection.

Null data or incomplete datasets.

The fear of missing a critical anomaly.

Enhanced knowledge and experience in the field.

Satisfaction from successfully thwarting potential threats.

Dealing with a high volume of alerts, many of which are false positives.

Duplicate data.

Different scales of measurement.

improve business, IT and application performance

freeing up time to plan and execute more performance-driving strategies.

Inconsistent data formats.

The constant stress of maintaining network security.

Job security and recognition for protecting the organization.

they can indicate potential risks, control failures, or business opportunities

What other thoughts and feelings might influence their behavior?

Alerts and notifications from security tools.

Documentation of past network security incidents.

Reports on security breaches in the industry.

What do they SEE?
What They See

"I need to ensure our network is secure and free from any malicious activities."

What do they SAY?
Network Security Analyst

"I constantly monitor network traffic for unusual patterns or activities."

"It's challenging to distinguish between normal and anomalous network behavior."

"I worry about false positives that can lead to unnecessary alarms."

What do they DO?
What do they do today?
What behavior have we observed?
What can we imagine them doing?

Analyze network traffic logs and data in real-time.

Set up and manage intrusion detection systems (IDS) and intrusion prevention systems (IPS).

Collaborate with colleagues to investigate and mitigate security incidents.

Stay updated on the latest threats and vulnerabilities in the network security field.

If anomaly detection is applied, this kind of repetitive work can be eliminated