WHO are we empathizing with?

We are empathizing with security analysts who are responsible for hunting for threats in network data

GOAL

What do they need to DO?

Security analysts monitor security alerts, manually search for threats in network data, and respond to security incidents.
* Network engineers design, implement, and maintain networks. They also monitor network performance and troubleshoot network problems.
IT managers oversee the IT department and its staff. They also develop and implement IT policies and procedures.

What do they HEAR?

Security analysts and network engineers hear about the latest security threats from a variety of sources, including news articles, security blogs, and industry conferences.

IT managers hear about the latest security threats from the same sources, but they also hear from their security teams about the specific threats that are targeting their organization.

What do they THINK and FEEL?

PAINS

Manually searching through network logs is time-consuming and tedious.
Keeping up with the volume and complexity of network data is difficult.
Identifying and correlating threats across different sources of data is challenging.
Prioritizing threats and focusing on the most important ones is difficult.
Staying ahead of the latest threats and vulnerabilities is difficult.
Lack of resources and support can make it difficult to do effective threat hunting.

GAINS

Automate the process of threat hunting, freeing up analysts to focus on more strategic tasks.
Provide visibility into the entire network, making it easier to identify and correlate threats.
Provide insights into the latest threats and vulnerabilities, helping analysts to stay ahead of the curve.
Help analysts to prioritize their work and to focus on the most important threats.
Reduce the time and effort required to detect and respond to threats.
Improve the overall security posture of the organization.

What do they SEE?

Multiple systems are infected with the same malware family.
Suspicious network activity between different systems.
Attempts to exfiltrate data from multiple systems.

What do they SAY?

In the future, security analysts and network engineers will be able to use AI-powered threat hunting tools to detect and respond to threats more quickly and effectively. This will free them up to focus on more strategic tasks.

What do they DO?

* Security analysts monitor security alerts, manually search for threats in network data, and respond to security incidents.
* Network engineers design, implement, and maintain networks. They also monitor network performance and troubleshoot network problems.