WHO are we empathizing with?

Security Analysts: These are the professionals responsible for monitoring and responding to security threats. They need the system to effectively identify and respond to potential intrusions

Making a secure detection system

What do they need to DO?

1. **Detect Threats**: Security analysts need to efficiently identify potential security threats or intrusions in the network and systems.
2. **Investigate Alerts**: They must thoroughly investigate and analyze security alerts to determine if they are genuine threats or false alarms.
3. **Collaborate**: Security analysts often work in teams, so they need to collaborate with colleagues to share insights and coordinate responses to threats.
4. **Stay Informed**: To be effective, they need access to up-to-date threat intelligence and information about emerging security risks.

What do they THINK and FEEL?

PAINS

- Difficulty in distinguishing between legitimate and malicious activities.
- The fear of a security breach that could compromise sensitive data.
- Overwhelmed by the sheer volume of alerts generated by traditional IDS systems.

GAINS

- improved accuracy in threat detection.
- More time for proactive security measures.
- Increased peace of mind when it comes to network security.

What other thoughts and feelings might influence their behavior?

What do they HEAR?

- Industry news and reports about the latest cyber threats.
- Information from colleagues about recent incidents or alerts.
- Vendor or product recommendations from the cybersecurity community.
- Company management discussing the importance of network security.

What do they SEE?

What do they see in the marketplace?
What do they see in their immediate environment?
What do they see others saying and doing?
What are they watching and reading?

What do they SAY?

I need a system that can effectively detect and respond to security threats.

What do they DO?

Regularly monitor security logs, investigate alerts, and collaborate with colleagues