WHO are we empathizing with?

IT Security Analysts
Cyber Attack Victims
Security AdministratorsRegulators and Compliance Auditors
C-Suite Executives
Machine Learning Engineers
End Users
Ethical Hackers and Penetration Testers

GOAL

What do they need to DO?

Automate routine tasks to focus on complex threats, continually update skills
Stay informed about security best practices and promptly report suspicious activities.
Regularly assess security ROI and explore emerging technologies
Follow security guidelines even if they involve extra steps.
Coordinate with organizations to implement security recommendations.

PAINS

What are their fears, frustrations, and anxieties?

The challenge of keeping up with evolving threats and the potential for alert fatigue.

Fear and anxiety caused by potential cyberattacks and data breaches.

Balancing security budgets, managing complex security solutions, and potential resistance to change.

The complexity of AI models, resource-intensive training, and the need for large datasets.

The challenge of keeping up with changing regulations and ensuring organizations adhere to them.

Balancing cybersecurity investments with other budgetary demands and understanding technical complexities.

The responsibility of continuously probing systems for vulnerabilities and potential resistance from security teams.

GAINS

What are their wants, needs, hopes, and dreams?

Opportunities to identify and address vulnerabilities, contribute to stronger security, and a sense of accomplishment.

Increased confidence in data security, easy access to services, and trust in the organization's commitment to safeguarding data.

Strengthened brand reputation, customer trust, and protection against financial losses due to cyber incidents.

Assurance that organizations are meeting compliance standards, reducing data breaches and legal penalties.

Satisfaction from developing cutting-edge security algorithms and contributing to improved cybersecurity.

Improved cost-effectiveness in managing security, reduced risks, and better resource allocation.

Improved cost-effectiveness in managing security, reduced risks, and better resource allocation.

What other thoughts and feelings might influence their behavior?

Balance job security concerns with staying at the forefront of cybersecurity, feeling pressure to manage alerts.

Expect data security, experience frustration with security hurdles, and trust organizations prioritizing security.

Juggle budget constraints, the risk of breaches, and the effectiveness of security solutions.

Embrace the excitement of AI, while addressing data quality and bias issues.

Find excitement in discovering vulnerabilities, frustration when organizations are slow to respond, and a sense of duty to improve security.

Feel a sense of duty to uphold regulations and frustration when organizations resist compliance.

Experience mistrust, vulnerability, and relief in response to data breaches and security measures.

Balance job security concerns with staying at the forefront of cybersecurity, feeling pressure to manage alerts.

Evaluate business impact, make strategic decisions, and fear reputational damage from breaches.

What do they Think?

Concerned about staying ahead of cyber threats.

Worried about data breaches and their consequences.

Considering the cost and effectiveness of security solutions.

Identifying vulnerabilities to strengthen security.

Considering the business impact of cyber threats.

Expecting their data and information to be secure.

Focusing on regulatory compliance and data protection.

Focused on enhancing the detection algorithms.

What do they SEE?

Vulnerability assessment reports
Authentication prompts and security warnings.
Budget proposals for security improvements.
Reports and security policies.
Unauthorized access attempts and suspicious activities.
The need for efficient intrusion detection systems.
A flood of alerts and logs that need quick analysis.
Data sets and model training iterations.

What do they SAY?

We need better tools to detect threats accurately
I want my data to be secure.
We need a cost-effective and robust solution.
AI can revolutionize intrusion detection.
Compliance is crucial for data security.
We need to protect our brand and customer.
I want my data to be safe and easy to access.
We help organizations stay one step ahead of attackers.

What do they Feel?

The thrill of discovering and mitigating weaknesses.
Concerned about the safety of their personal information.
The responsibility for making the right cybersecurity investments.
The need for organizations to adhere to cybersecurity standards.
Excitement about the potential of AI in cybersecurity.
The pressure to balance security and budget constraints.
Frustration, fear, and vulnerability.
Anxious about the volume and sophistication of attacks.