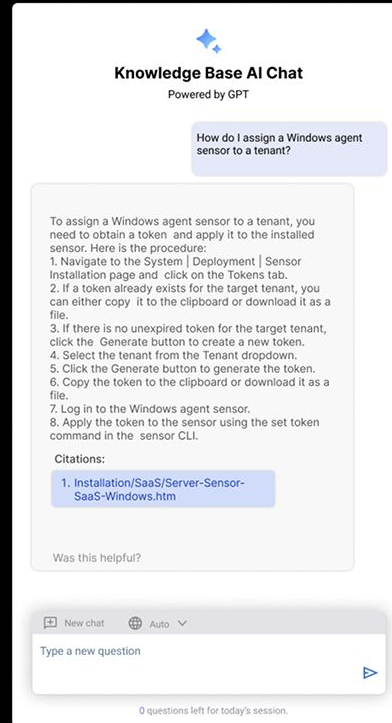
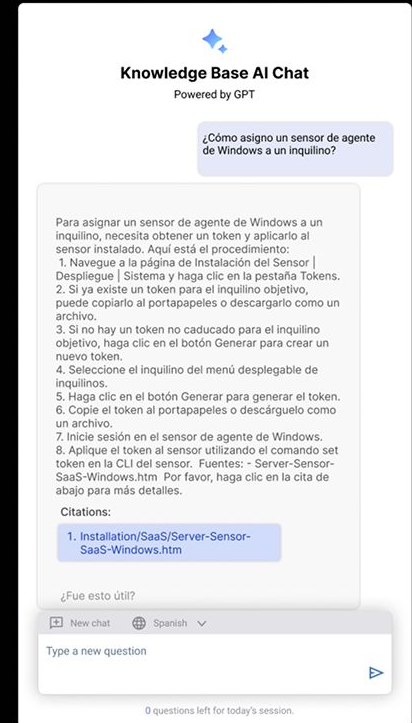


## Case Study 1: AI Investigator – The Foundation 2023

- Proactive AI Vision: My 'Zero to One' Initiative
- Foundational Step: KB Chat's Immediate Value
- Enabling Complex AI: Proving Concept & Tech



Auto-detected Language



Manual Selected Language

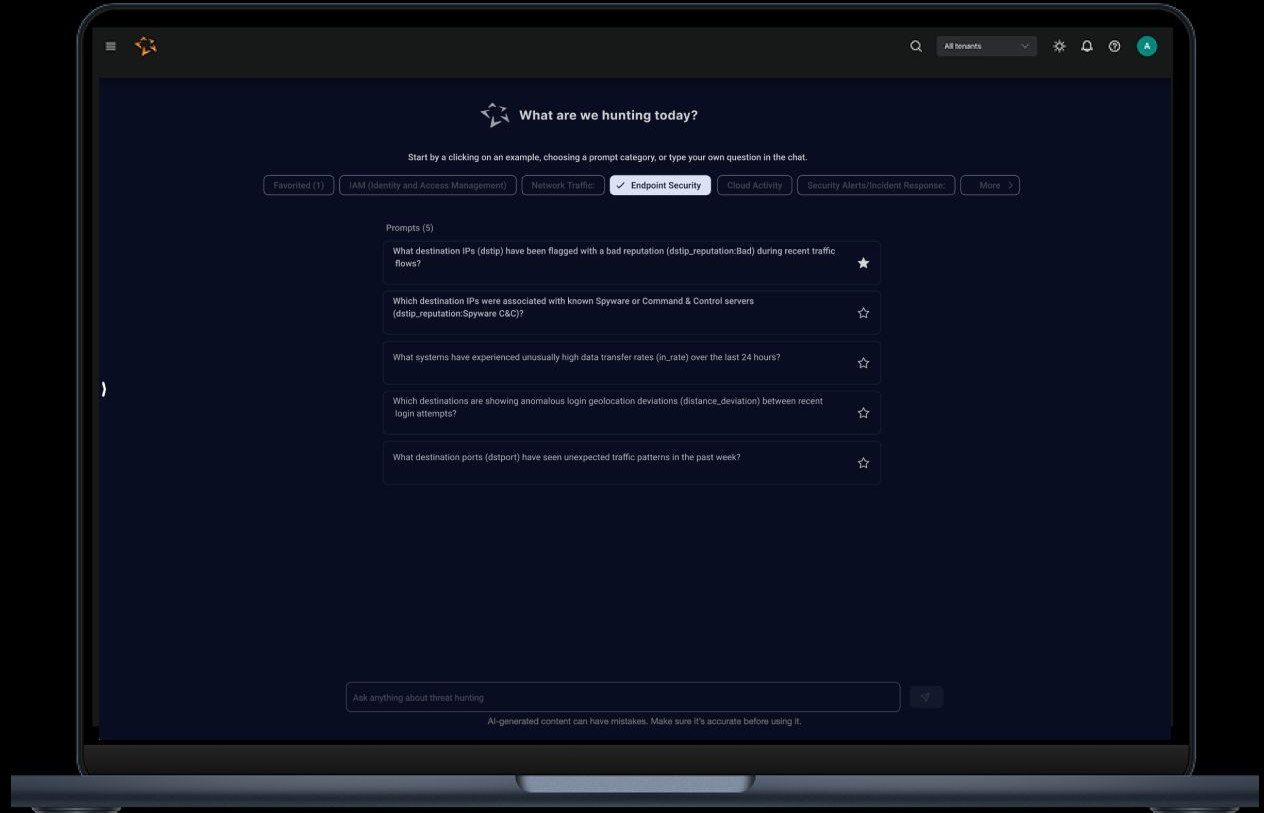
## The Core Problem: Overwhelmed Analysts, Hindered Investigations

- Data Overload: Alert Fatigue & Cognitive Strain
- Complex Tools: Slow Investigations & Missed Threats
- Business Risk: Prioritizing AI for Critical Needs



## AI Investigator - My Role & Team

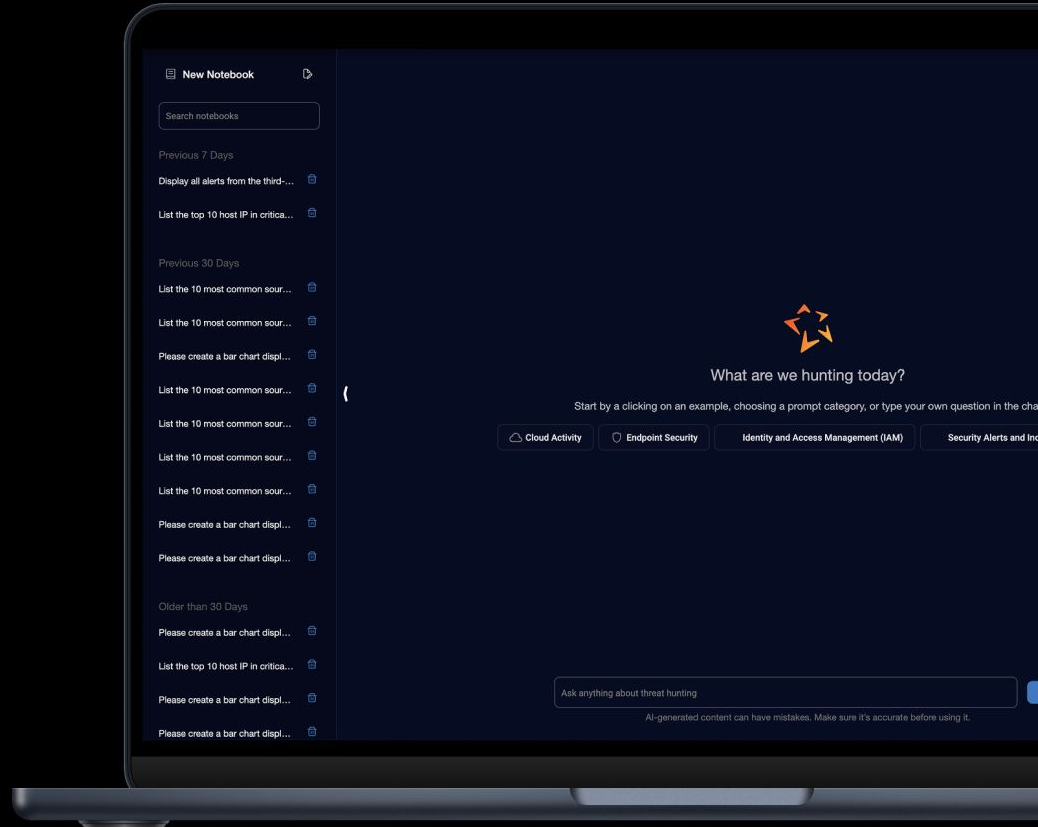
- Lead 0→1 designer
- Partnered with 1 UI developer + 1 PM + ML lead
- Time-boxed to 3 months MVP



# The Solution: Conversational Investigation

## Conversational Interface:

- AI-powered conversational investigations with natural language.
- Notebook functionality for persistent interaction history.
- Predefined question categories for guided exploration.



## Observation to Innovation: Mastering Conversational Context

Suggested followups:

...Last 30 days

...Last 90 days

...Last 6 months

...11/11/2024 16:52:51- 11/18/2024 16:52:51

this thurs to next friday

AI-generated content can have mistakes. Make sure to verify the content.

- User Behavior Observed: Ignoring UI Date Pickers
- User Intent: Maintaining Records, Prompting New Ranges
- My Design Response: Proposing Conversational Context & Natural Language

# Design Principles: Building Trust and Transparency



What are we hunting today?

Favorited (5) Defender for Endpoint Exchange Github Enterprise Microsoft 365 Debug Microsoft Entra ID NextDLP Reveal >

Microsoft 365 Debug (10)

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.



Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.



Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.



Microsoft 365 Debug

Which users have experienced multiple failed login attempts (login\_result:fail) across multiple systems (msg\_origin:source)?



Microsoft 365 Debug

What users successfully logged in but were flagged for brute force attacks (login\_result:sucess\_brute\_forced)?



Microsoft 365 Debug

Which users had their multi-factor authentication (MFA) fail (login\_result:mfa\_fail) during recent login attempts?



Microsoft 365 Debug

What users have logged in successfully using MFA (login\_result:mfa\_success)?



Microsoft 365 Debug

What destination IPs (dstip) have been flagged with a bad reputation (dstip\_reputation:Bad) during recent traffic flows?



Microsoft 365



- **Transparency:** Explain AI reasoning.
- **Explainability:** Provide clear insight explanations.
- **Control:** Allow analysts to refine AI results.
- **Context:** Integrate AI insights into workflow.

## Impact: Amplifying Human Expertise

- Reduced investigation time
- Increased analyst confidence
- Improved threat detection

**30%**

Reduction in average investigation time for high-priority incidents.

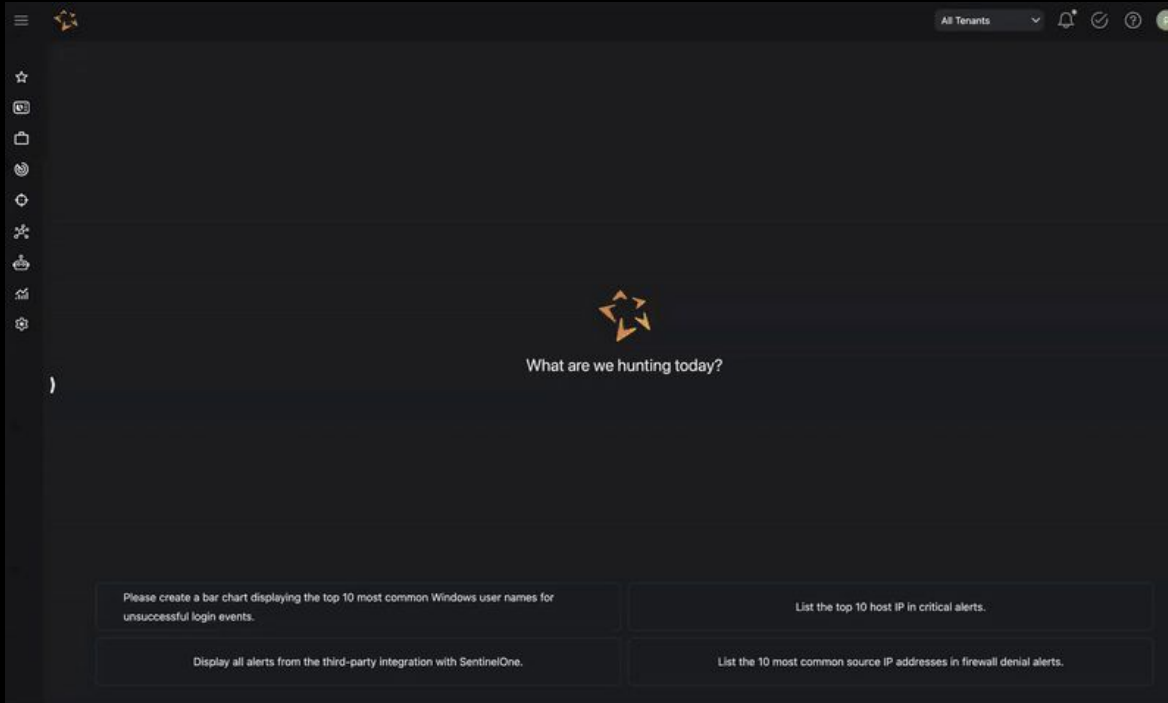
**15%**

Increase in the number of previously undetected threats identified.

**40%**

Increase in analysts reporting they feel "confident" or "very confident" in their conclusions.

## SIMPLIFYING THE COMPLEX. POWERING THE FUTURE.



- User-Centered AI Innovation
- Tackling Complex Enterprise Challenges
- Driving Tangible Business Impact