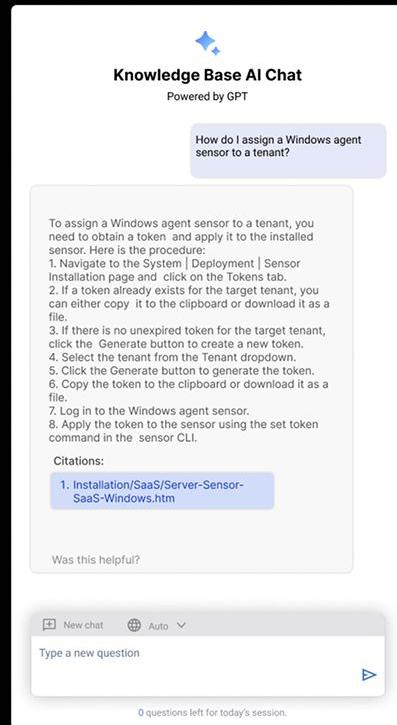
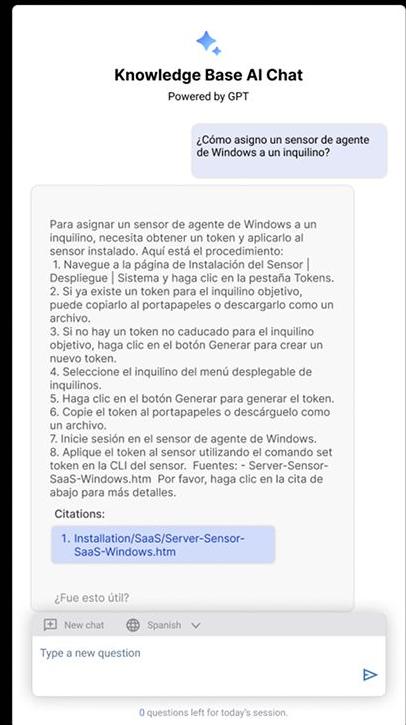


# Case Study 1: AI Investigator - The Foundation 2023

- 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

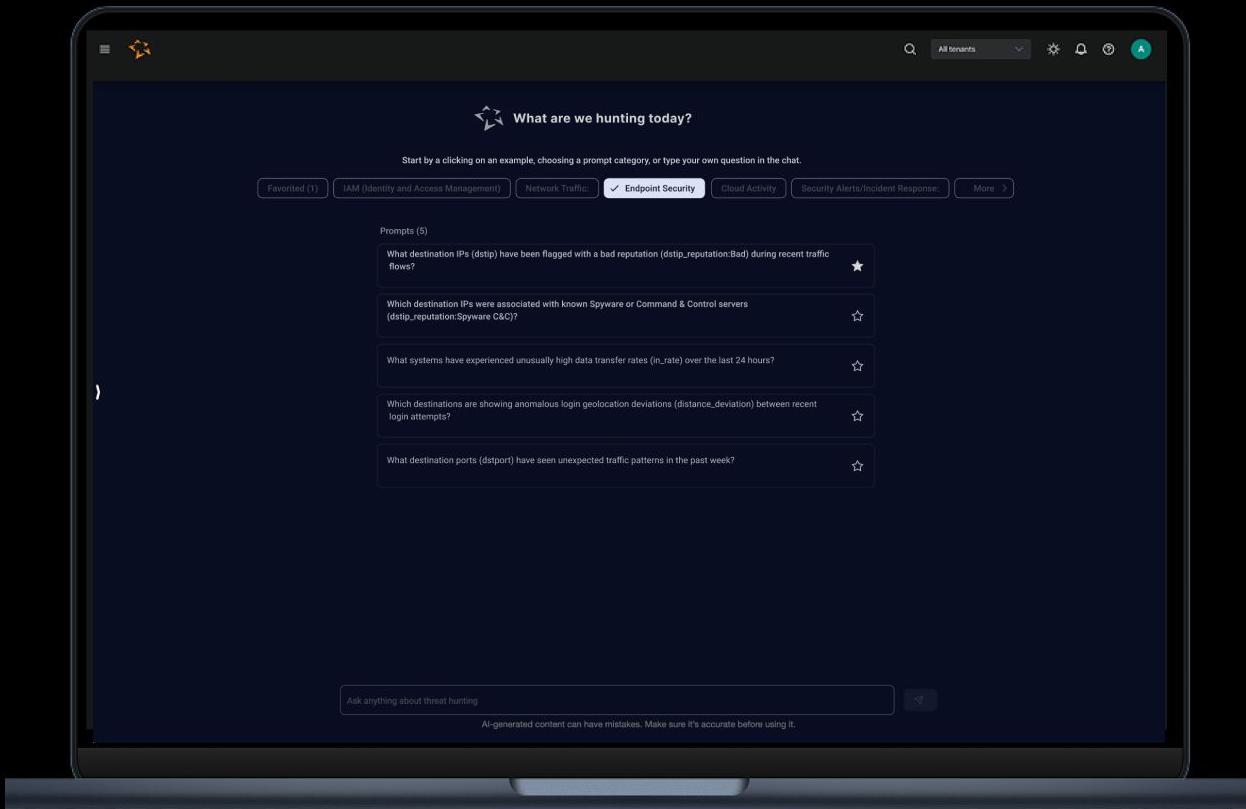
## The Core Problem: Overwhelmed Analysts, Hindered Investigations

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



# AI Investigator - My Role & Team

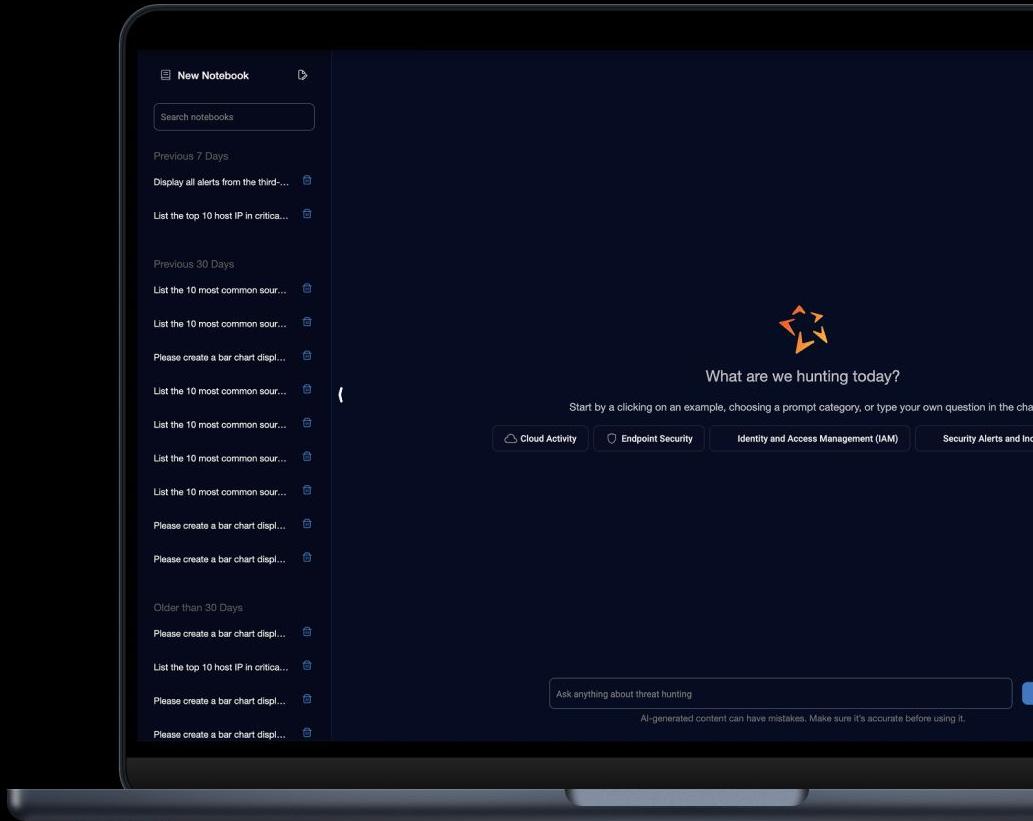
- Lead 0→1 designer
- Partnered with 1 UI developer + 1 PM + ML lead
- Time-boxed to 3 months MVP



# 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:

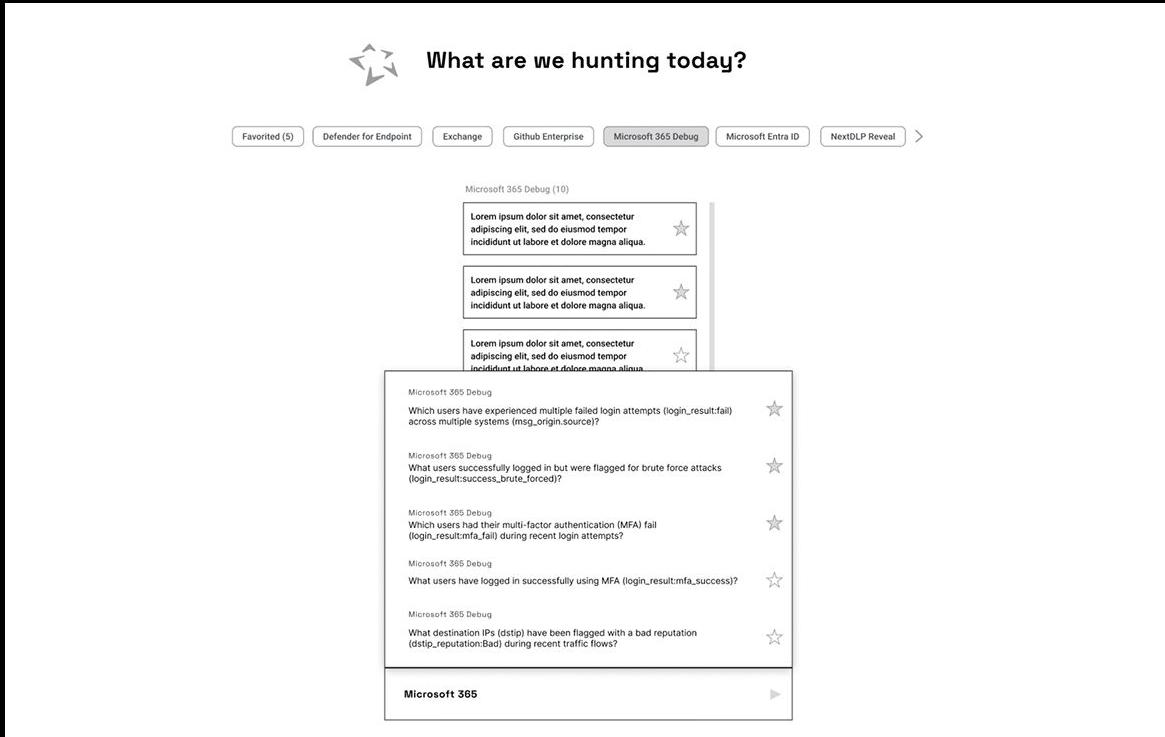
...Last 30 days    ...Last 90 days    ...Last 6 months    ...11/11/2024 16:52:51- 11/18/2024 16:52:51

this thurs to next friday

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

- 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



The wireframe shows a user interface for a hunting tool. At the top, there is a navigation bar with a search icon and the text "What are we hunting today?". Below the navigation bar are several buttons: "Favorited (5)", "Defender for Endpoint", "Exchange", "Github Enterprise", "Microsoft 365 Debug", "Microsoft Entra ID", and "NextDLP Reveal". A right-pointing arrow is also present.

The main content area displays a list of prompts, each with a title, a description, and a star icon for rating. The prompts are categorized by tool:

- Microsoft 365 Debug (10):**
  - Microsoft 365 Debug: Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. ★
  - Microsoft 365 Debug: Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. ★
  - Microsoft 365 Debug: Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. ★
- Microsoft 365 Debug:**
  - 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:success\_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:**
  - Microsoft 365: What destination IPs (dstip) have been flagged with a bad reputation (dstip\_reputation:Bad) during recent traffic flows? ★

At the bottom of the list, there is a "Microsoft 365" button with a right-pointing arrow.

Wireframe for categorized prompts and auto complete

- **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.

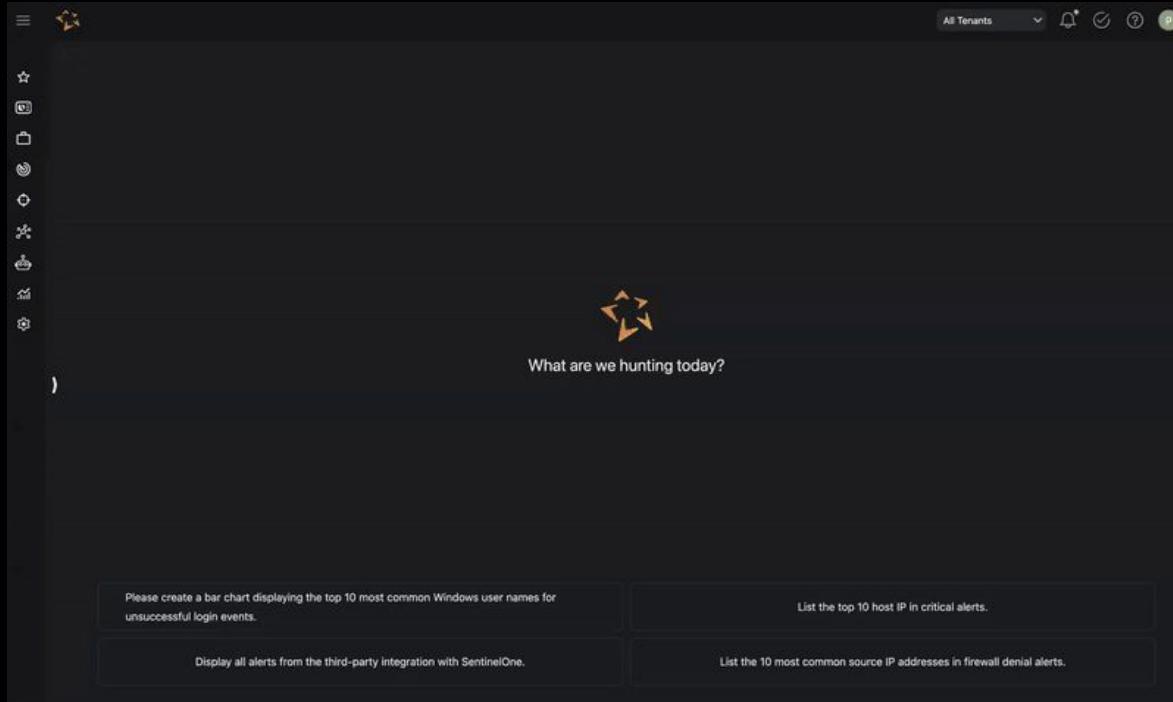
**40%**

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

**15%**

Increase in the number of previously undetected threats identified.

# SIMPLIFYING THE COMPLEX. POWERING THE FUTURE.



All Tenants

What are we hunting today?

Please create a bar chart displaying the top 10 most common Windows user names for unsuccessful login events.

List the top 10 host IP in critical alerts.

Display all alerts from the third-party integration with SentinelOne.

List the 10 most common source IP addresses in firewall denial alerts.

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