How a "Less is More" Approach Stems the Sprawl of Security Data and Makes it More Actionable

MAHENDRA KUTARE, FOUNDER & CEO, DEEPTRAIL

About Me

1. Data/ML/Computer Vision Infra - Motive, Inc ($3B val)
2. Data/ML/Computer Vision Infra - NIO, Inc (NYSE: NIO)
3. Distributed Systems/Data/ML Infra - Mesosphere, Inc (Acq. by Nutanix)
4. Security Data/ML Infra - E8Security, Inc (Acq. by VMware)
5. Observability Monitoring Infra - Boundary, Inc (Acq. by BMC)
6. Distributed Systems (Monalytics) Research - Georgia Tech Atlanta

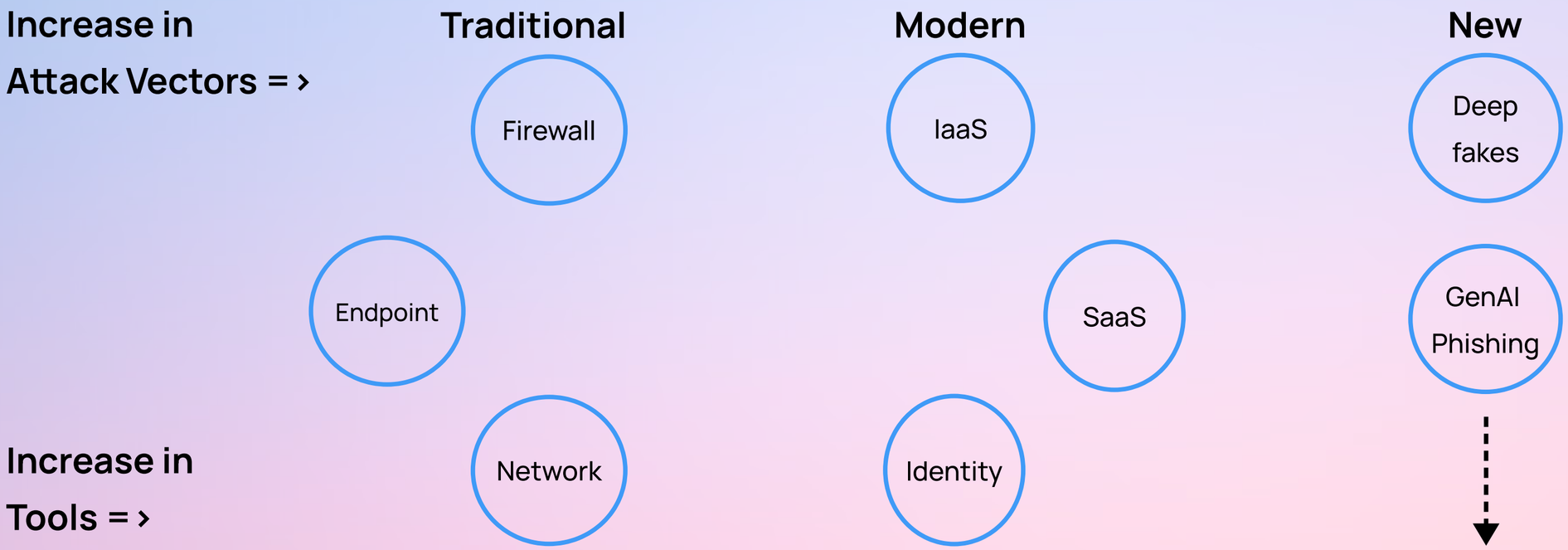
Agenda

- The Reality
- The Shift
- Challenges in building AI-first security product
- DeepTrail - Our Approach

The Reality

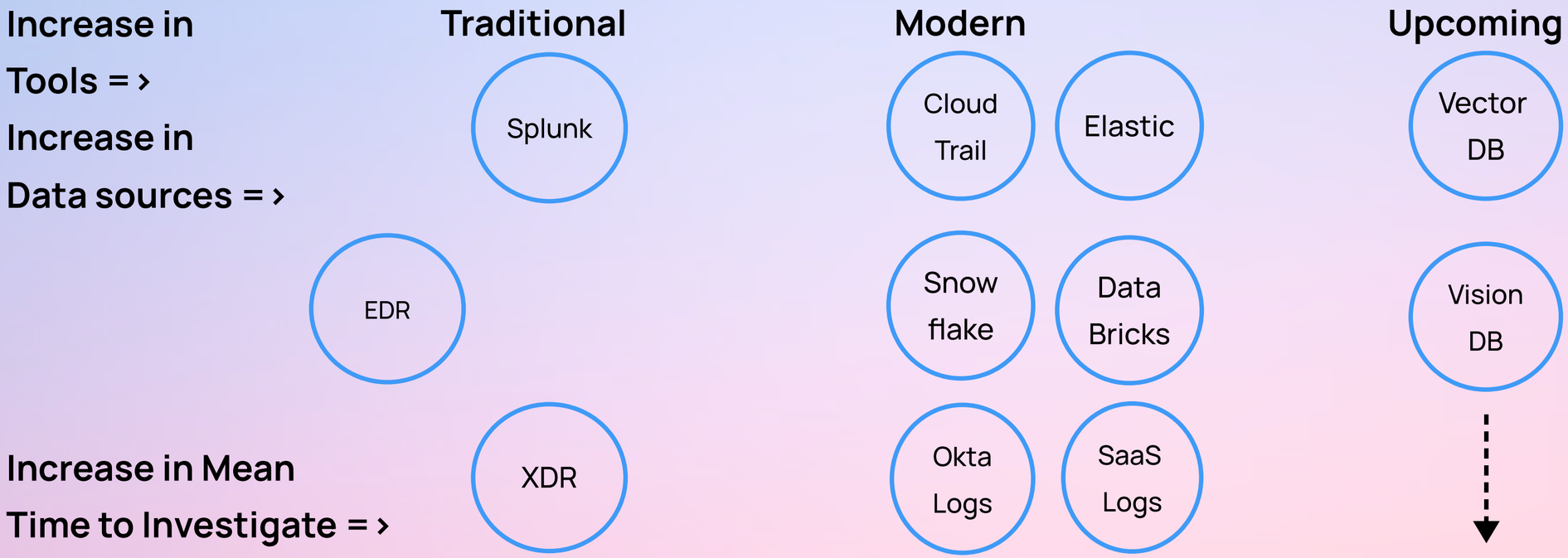
Security Engineers/Analysts

Are doing more work to investigate the firehose of findings



Security Engineers/Analysts

Are doing more work (queries) with the increase in data sources



Security Engineer/Analyst

Doing more tasks with increase and complexity of investigations

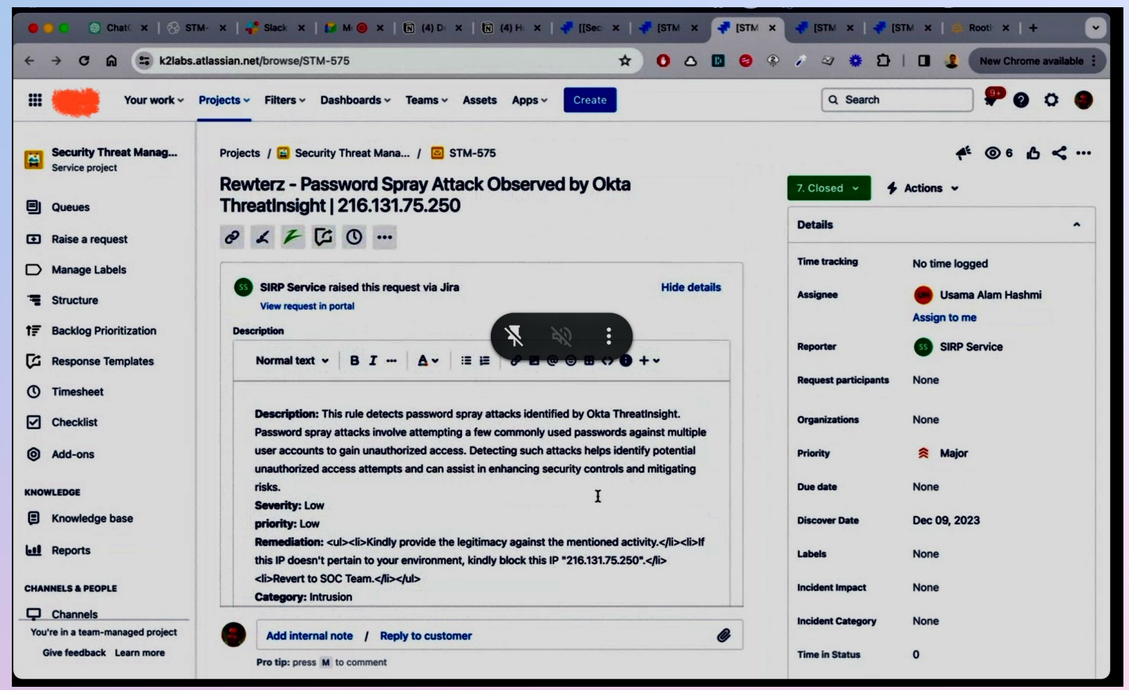
Doing more communication and coordination across teams

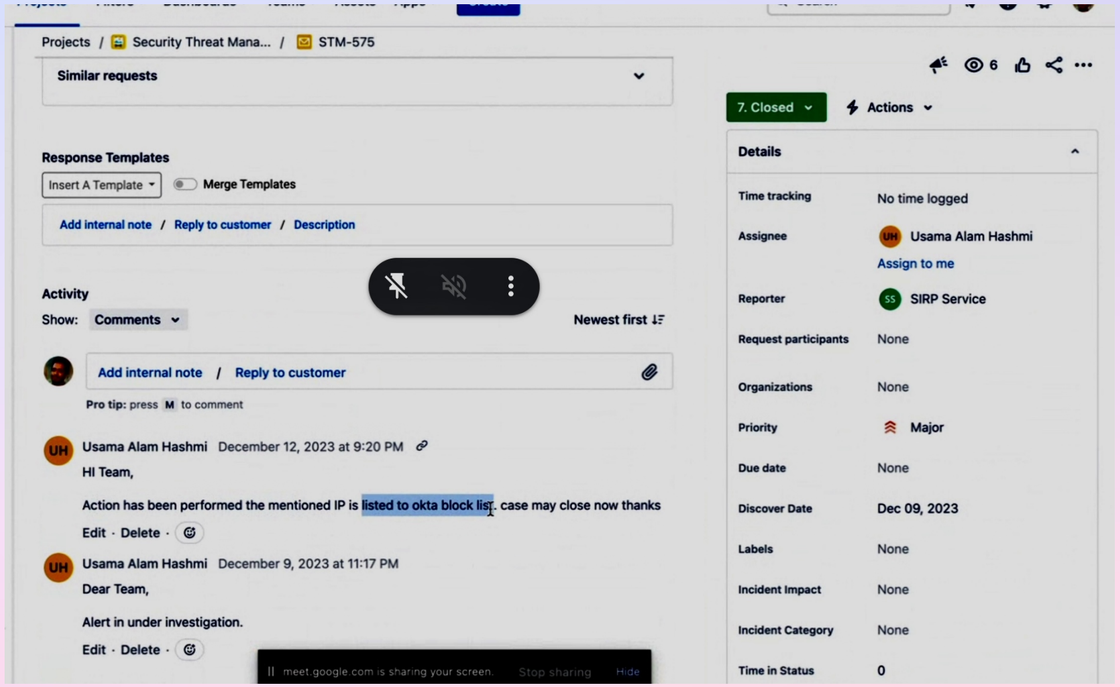
Are able to work on only 49% of the issues assigned


I'm fried. I'm tapped out.

Current Ticketing Tools

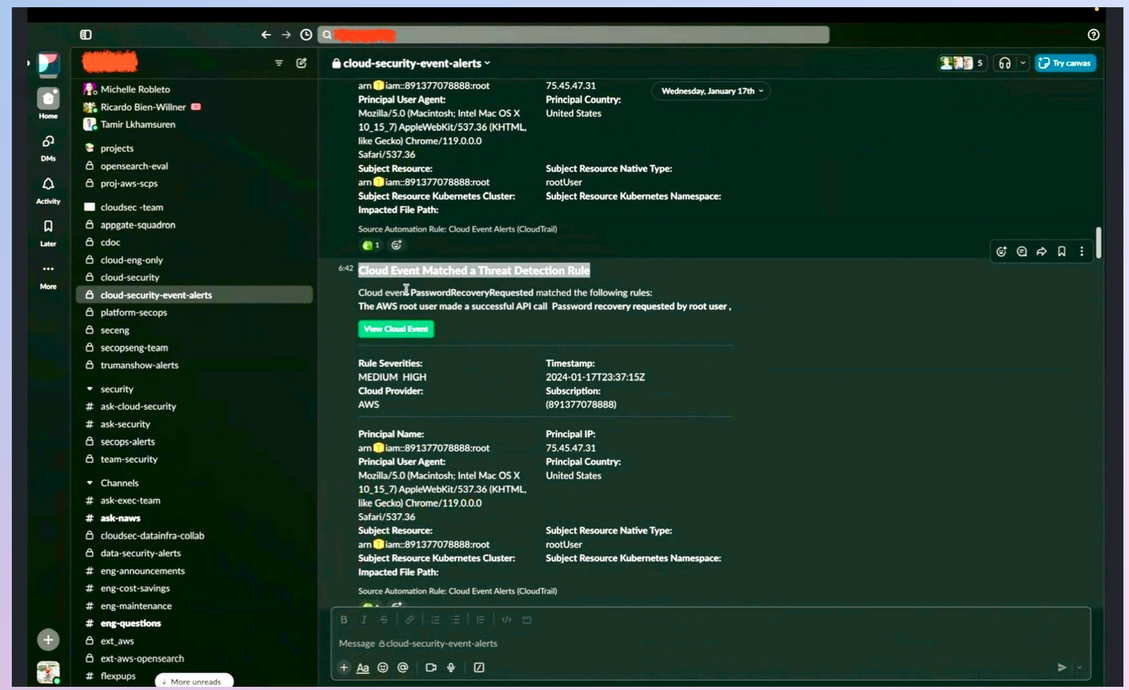
JIRA

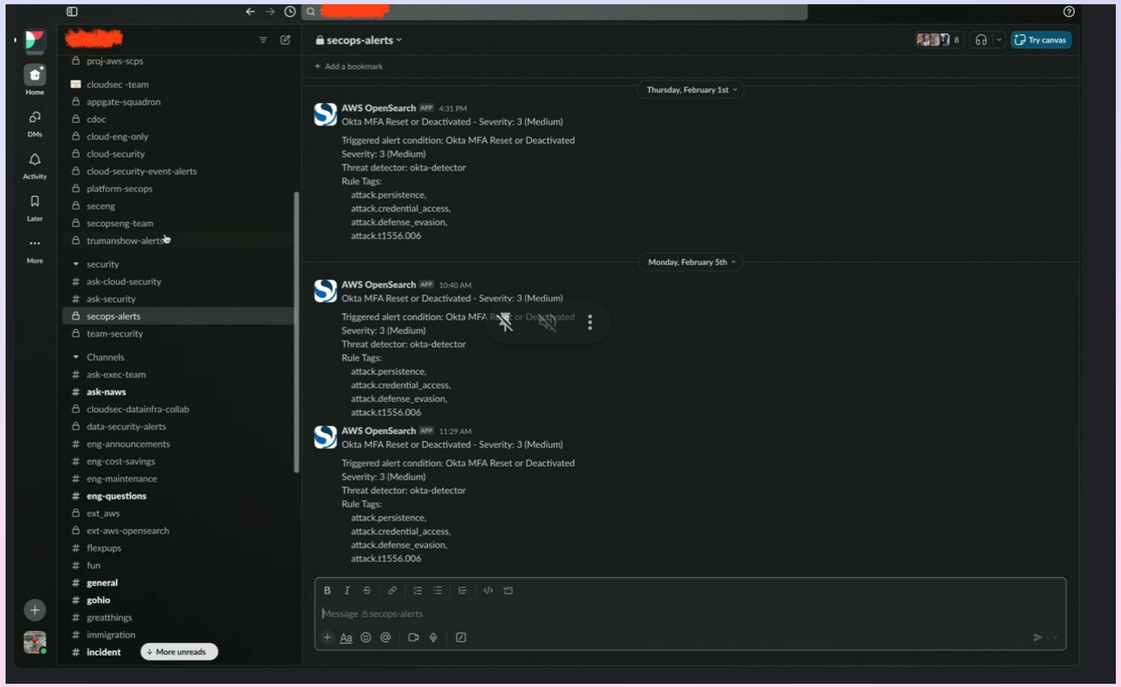




Current Communication Tools

Slack/Teams






I CAN'T.
IT'S-IT'S TOO MUCH.


There's been a breach.

Status Quo Problems

User Problems

Fatigue - Tedious, laborious, unsatisfying, and repetitive work

Low Retention - Less opportunities to grow and do impactful work.

Lack of Tools - Not enough tools to do investigations

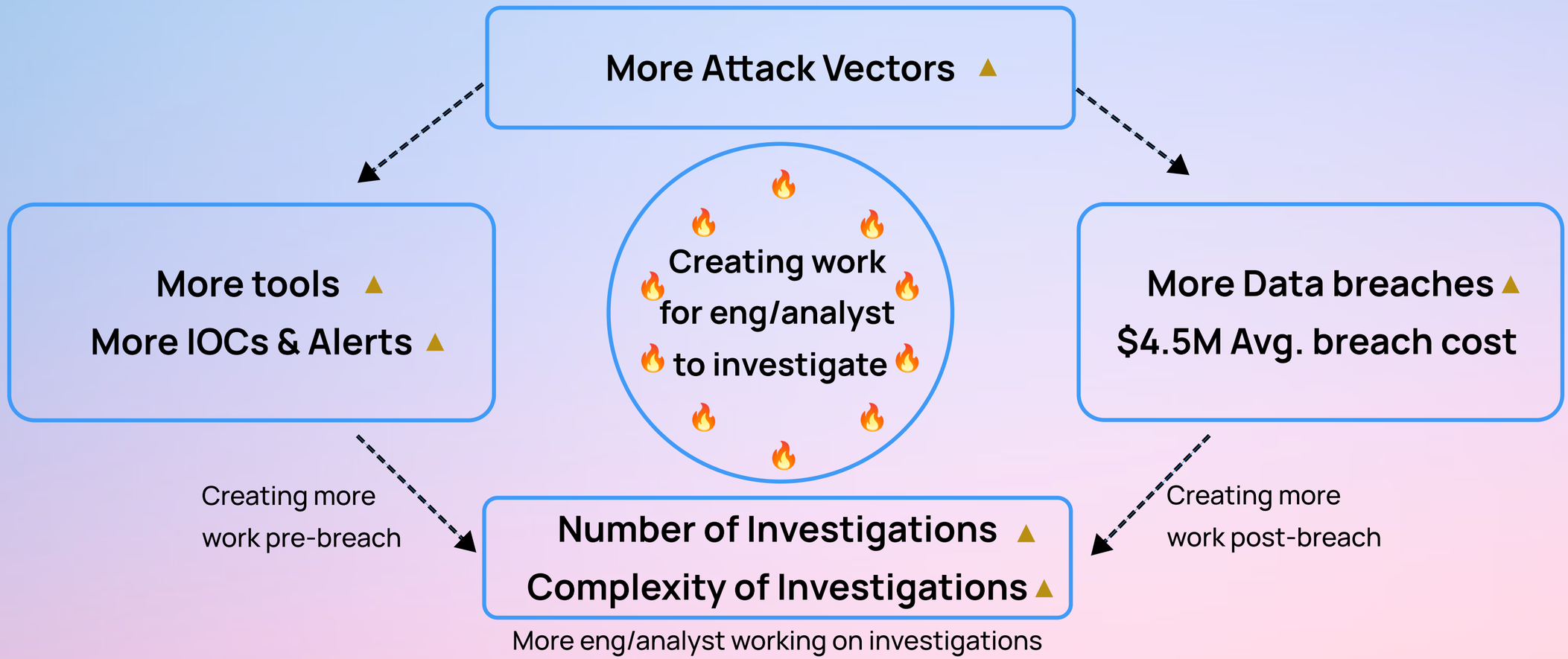
Organization Problems

Risk - Higher risk of data breaches

Cost - Higher operating cost of security team

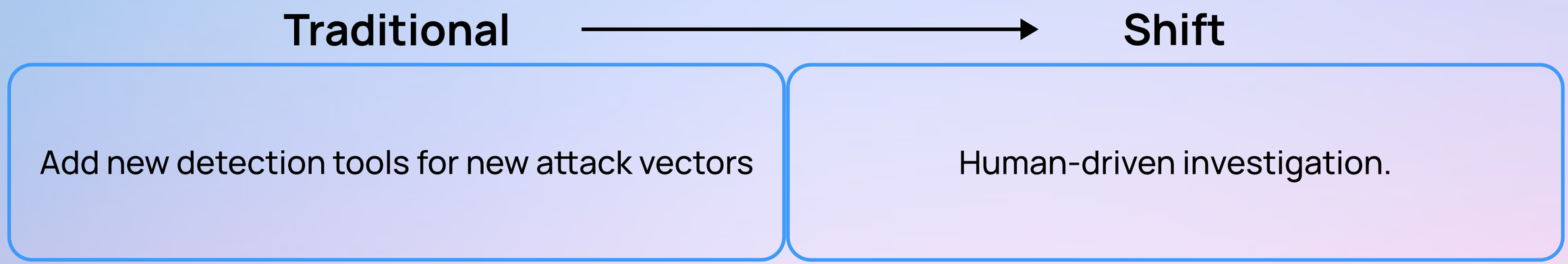
Talent - Retention and training analysts and engineers

Vicious Cycle of Security



Fundamental shift in the security space

Security



Security is no longer a tools problem, it is an investigation problem.

Customer Insights

Phase-1 Key Insights

It is a well-known huge problem!

Lack of tools for pre-breach investigations.

Lack of appetite to replace vendor stack.

Phase-2 Key Insights

Lack of trust with the AI-system.

Lack of simple intuitive UX experience.

Huge time spent communicating with other teams.

Phase-3 Key Insights

In spite of adding tools, users are still overwhelmed.

Falling short of truly helping with the work.

Dont't add additional work for the user.


HELP ME!

Challenges in building AI first product for security investigations

Building a delightful user experience for an autonomous enterprise product

Building the user trust with AI first system

Unbundling the security investigation from compliance

95% of investigation need less than 30 days of data

Security compliance require upto 1 year of data

Running investigations on centralized vs distributed data

Fortune 500 and large enterprises run traditional data architectures with Splunk for security as general purpose central storage and query system

Modern cloud native and SaaS companies use cheaper storage and query across distributed data sources


AMAZON ORIGINAL
Them
ABOUT
GODDAMN
TIME

Introducting DeepTrail

Don’t create work - Do the work!

DeepTrail's generative AI agents and proprietary LLMs power security investigations by autonomously planning and executing investigations for security teams.

DeepTrail AI-First Approach

Do the work - not just assist or create work!

Guided and explainable approach to UX/UI

LLMs learn like plans security engineer/analyst do!

Agents learn tools behavious and execute plans!

Before DeepTrail

Password Spray Attack

Current Investigation Stages	Tools	Actions
1 Payload Analysis & Plan	JSON Summarizer	Summarize and create an action plan
2 Initial Metadata Check	JSON Query	Check geo location of an IP
3 Historical Behavior Check	Elastic/Splunk/Snowflake	Check past similar alerts from the same IP/User and their investigations and their resolution - Elastic/Splunk
4 IP/User Activity Check	Okta/CloudTrail/Wiz	Check the last 7 days and current activities by IP/User - Okta and Cloud Trail
5 Unique Device/User Check	Stych	Check if the device and browser fingerprint of the event matches with the user's previous sessions

Password Spray Attack

Current Investigation Stages	Tools	Actions
6 IP Reputation Check	AbuseIPDB	Call external API for malicious IP check - AbuseIP DB
7 Internal Communication	Slack/Teams	Check with the employee if the IP belong to them or not and find the manager of the employee
8 Attack Surface Check	(E/X)DR/Splunk/Snowflake	Check if similar alerts are fired for the other users. Is the attack surface increasing?
9 Organization Impact Check	(E/X)DR/Splunk/Snowflake	Monitor other attacked employees and their activities and their logins to other applications and suspicious activities
10 User Persona Check	Okta/AD	Check if user is CEO or engineer for different actions

After DeepTrail

Password Spray Attack

Engineer/Analyst

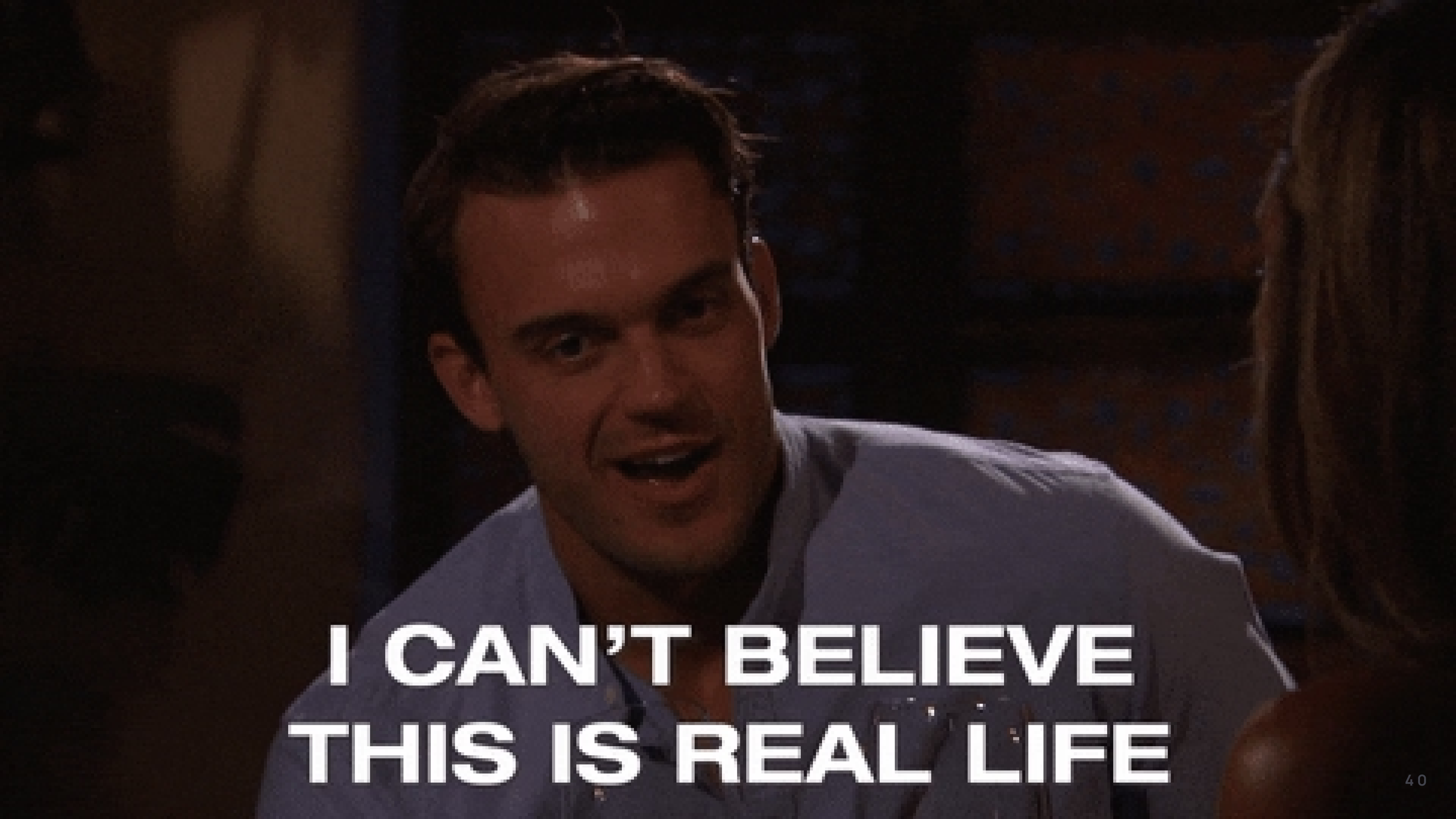
🤖After DeepTrail - Engineer driving 3 steps

1. Review and approve the work done by agents
2. Update and steer the steps executed by agents
3. Provide data to add behaviors and envs to the LLM

Agents & LLMs

🤖After DeepTrail - Gen AI doing the work

1. Autonomously start running each investigation
2. Generates code executable investigation plan
3. Provide output/reason of each step for human trust
4. Executes code plan and produces work output
5. Learn and create investigation plans like humans
6. Answer questions at each stage of investigation


I CAN'T BELIEVE
THIS IS REAL LIFE

DeepTrail Business Outcomes

Reducing cost of security operations

Reducing time to investigate and de-risking breaches

Increasing productivity of security engineers/analysts

DeepTrail

AI-POWERED AUTONOMOUS SECURITY INVESTIGATIONS

Deeptrail

Thank You!

Questions?

+1 (404)-791-1276

mahendra@deeptrail.com

San Francisco