

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

MAHENDRA KUTARE, FOUNDER & CEO, DEEPTAIL

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

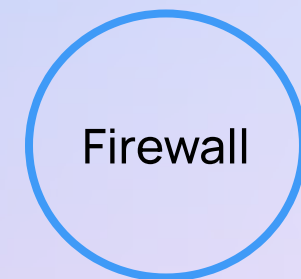
The Reality

Security Engineers/Analysts

Are doing more work to investigate the firehose of findings

Increase in
Attack Vectors =>

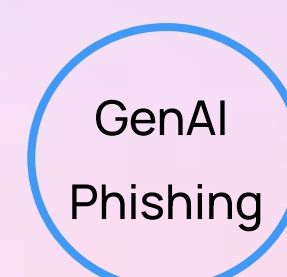
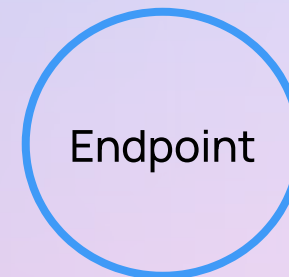
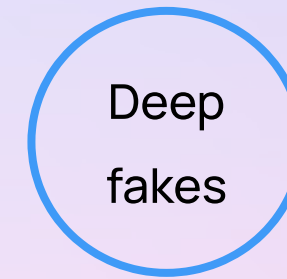
Traditional



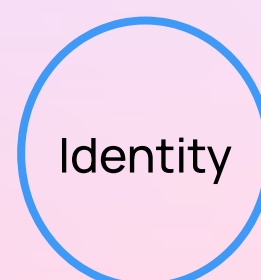
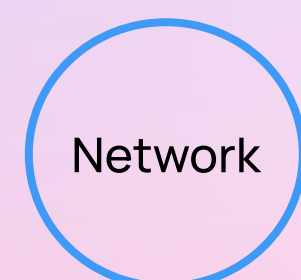
Modern



New



Increase in
Tools =>

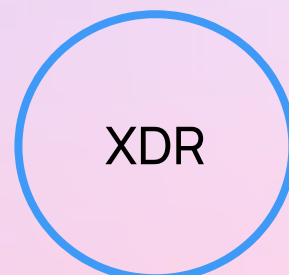


Security Engineers/Analysts

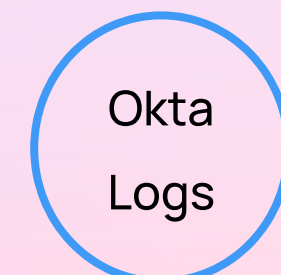
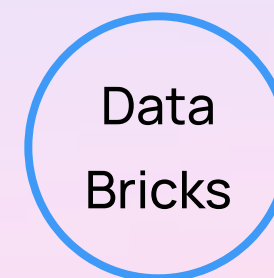
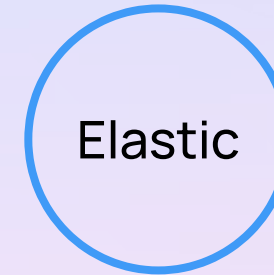
Are doing more work (queries) with the increase in data sources

Increase in
Tools =>
Increase in
Data sources =>

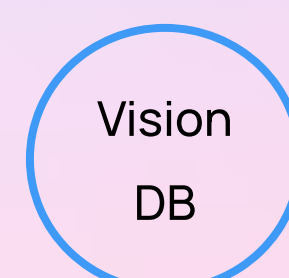
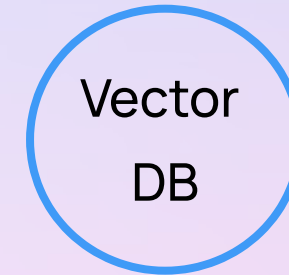
Traditional



Modern



Upcoming



Increase in Mean
Time to Investigate =>

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

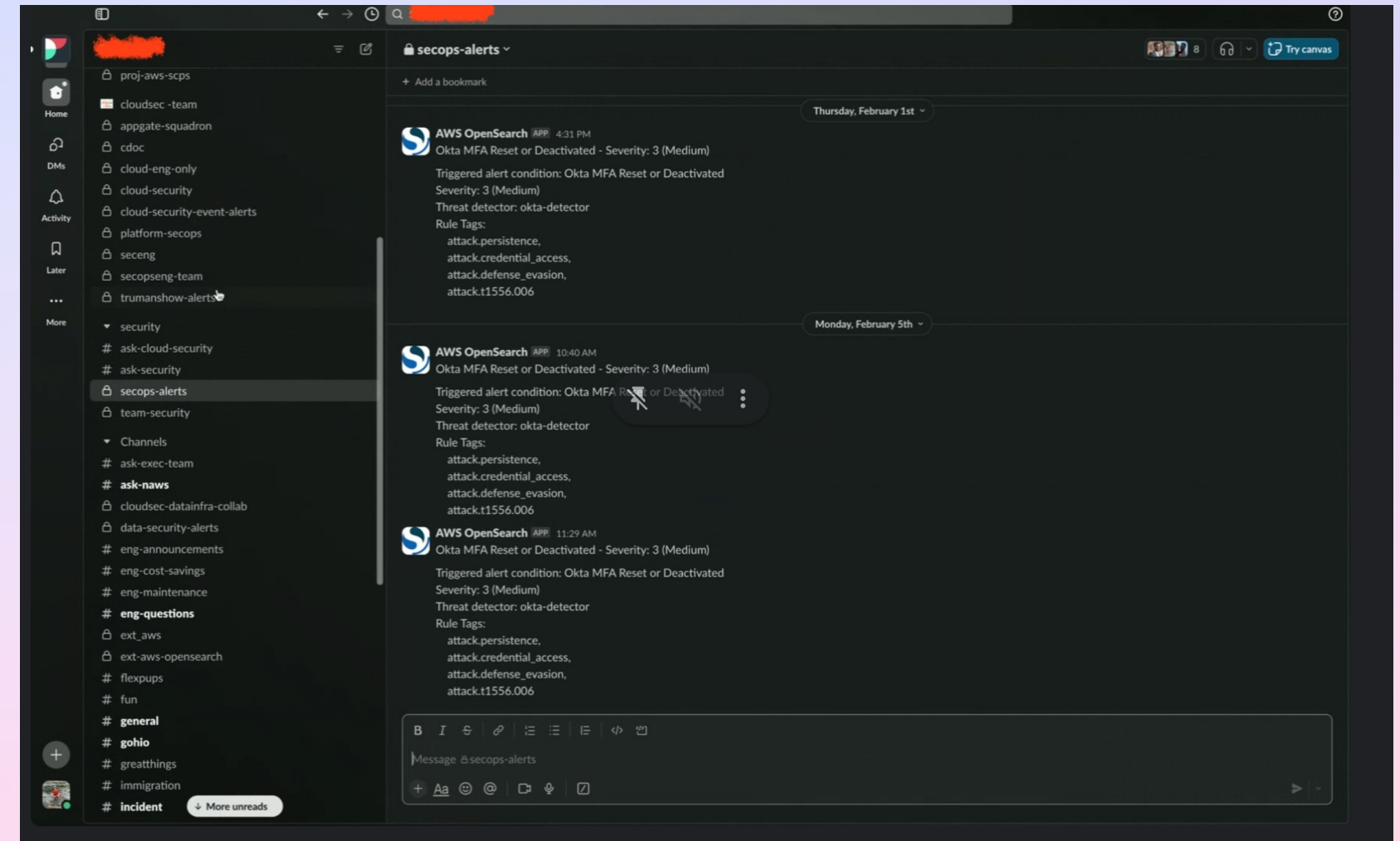
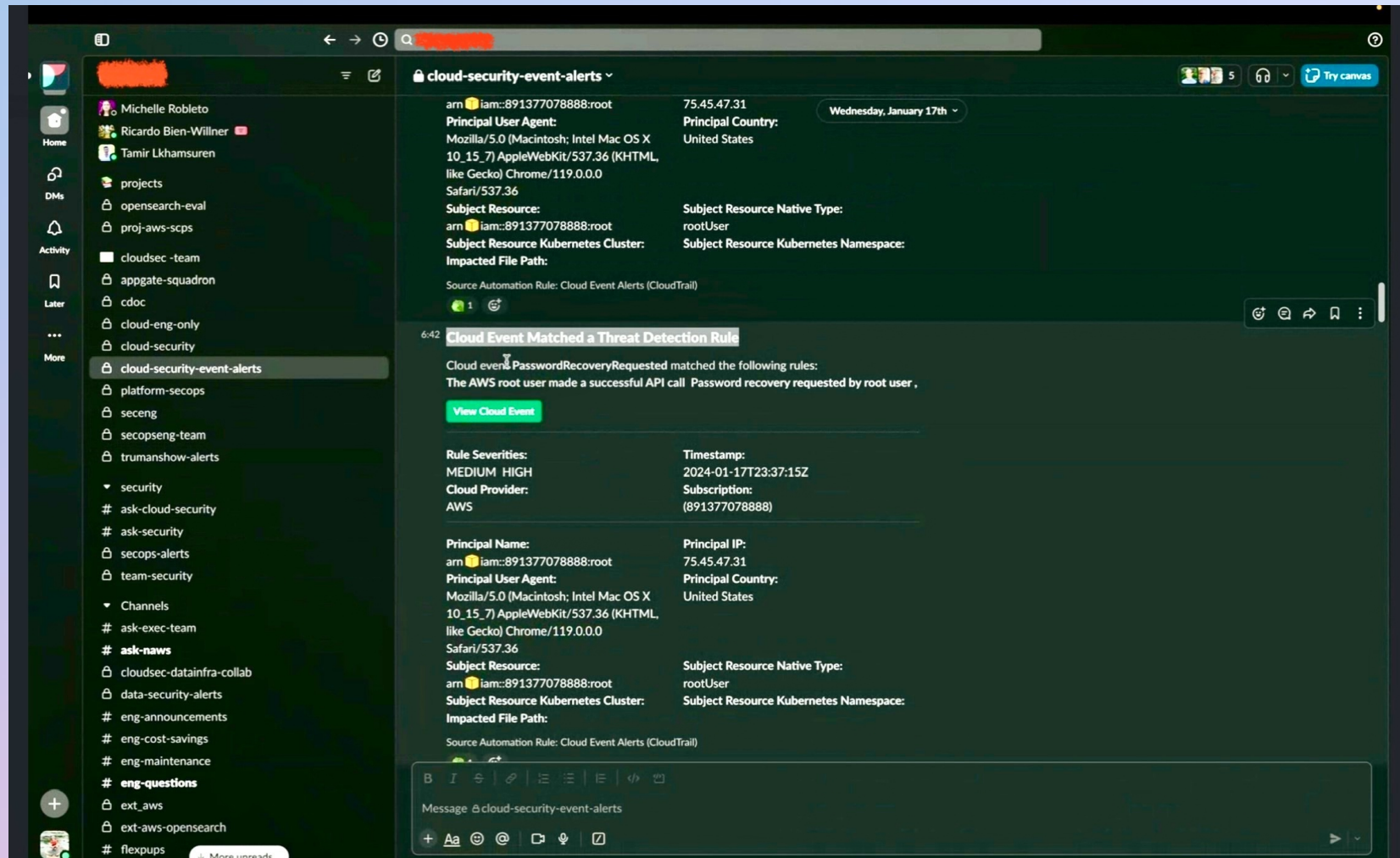
JIRA

The screenshot shows the Jira web interface for a ticket titled "Rewterz - Password Spray Attack Observed by Okta ThreatInsight | 216.131.75.250". The ticket is in a "Closed" status. The left sidebar contains navigation options like "Queues", "Raise a request", and "Manage Labels". The main content area includes a description of the attack, its severity (Low), priority (Low), and remediation steps. The right sidebar shows details such as the assignee (Usama Alam Hashmi), reporter (SIRP Service), and priority (Major).

This screenshot shows the activity and response templates for the same ticket. The "Activity" section displays a comment from Usama Alam Hashmi dated December 12, 2023, at 9:20 PM, stating "Action has been performed the mentioned IP is listed to okta block list. case may close now thanks". The "Response Templates" section includes options to "Add internal note" or "Reply to customer". The right sidebar shows details like "Time tracking" (No time logged), "Assignee" (Usama Alam Hashmi), "Reporter" (SIRP Service), and "Priority" (Major).

Current Communication Tools

Slack/Teams



A man in a dark suit, light blue shirt, and patterned tie is shown from the chest up. He has a distressed, almost tearful expression and is looking down and to his left. The background is an office setting with a grey cubicle wall, a calendar, and a desk with a stack of papers.

**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

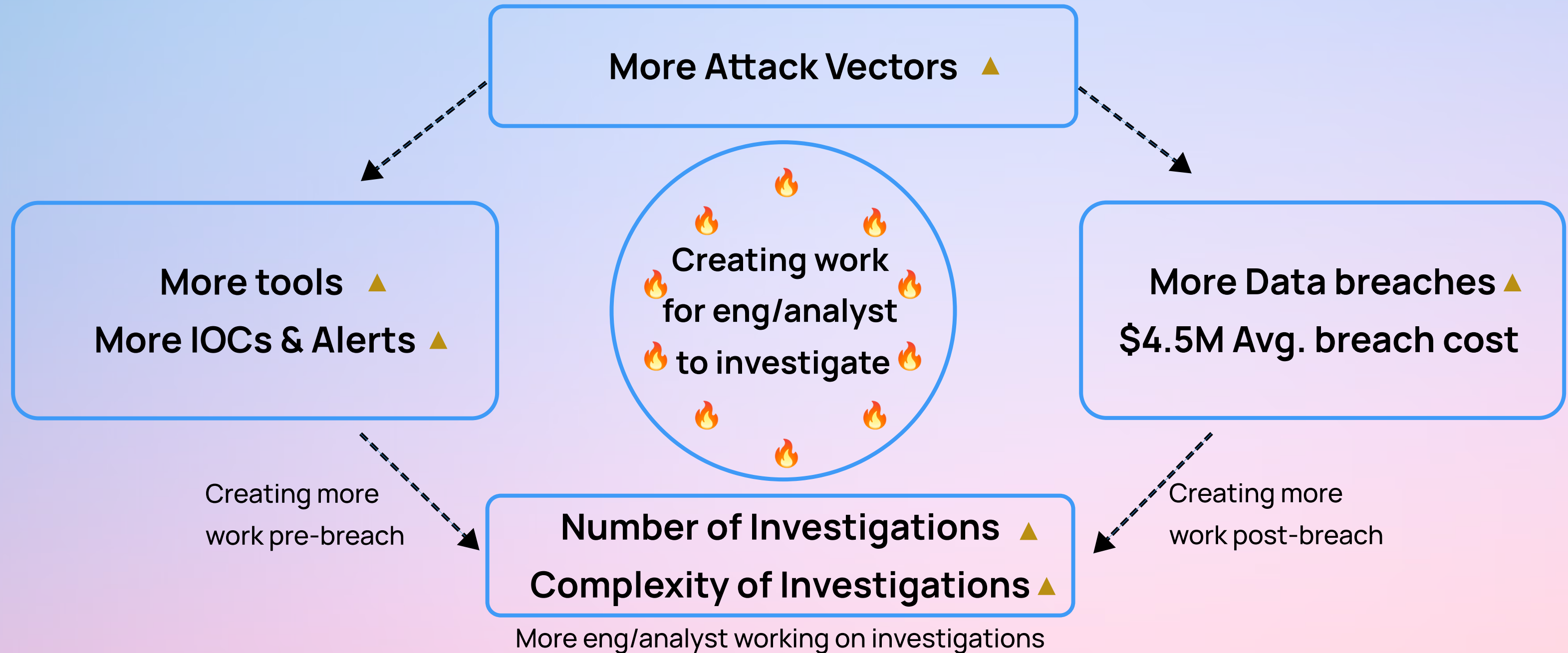
Organization Problems

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

Traditional



Shift

Add new detection tools for new attack vectors

Human-driven investigation.

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.

Don'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

Shan

**ABOUT
GODDAMN
TIME**

Introducing 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 behaviours 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

After DeepTrail - Engineer driving 3 steps

Engineer/Analyst

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

After DeepTrail - Gen AI doing the work

Agents & LLMs

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

A close-up shot of a man with dark hair, wearing a light blue button-down shirt. He has a wide-eyed, open-mouthed expression of surprise or disbelief. The background is dark and out of focus.

**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