elastic | The Search Analytics Company

Advantage AI

Transforming Secops With AI to Stop Today’ threats

whoami

- Principal Security Architect
- Elastic Global Security Specialists Group
- Passionate about Security Operations and Intelligence

Marvin Ngoma

[“CISSP”, “GSOM”, “Msc”]

Outline

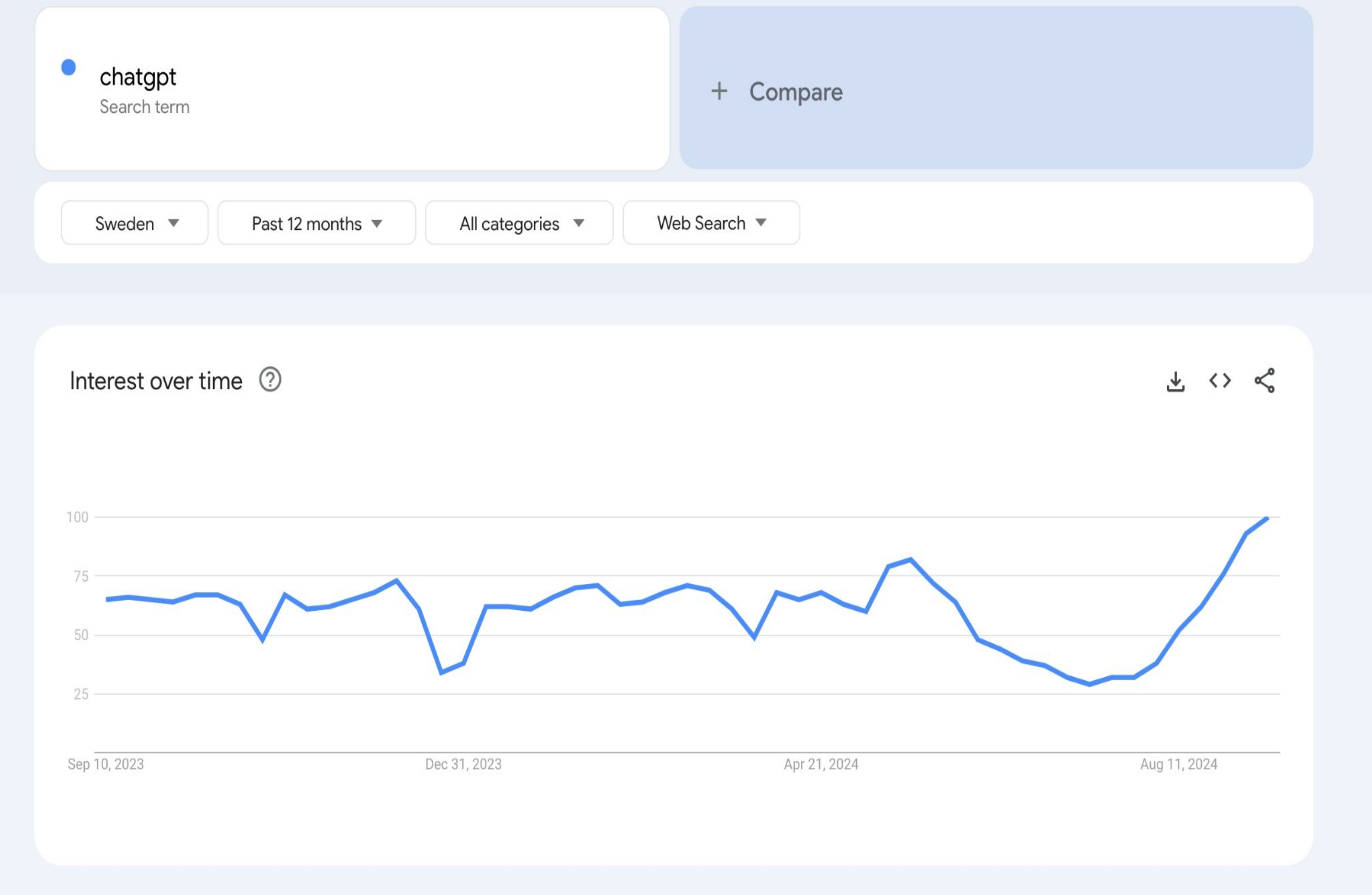
- Current trends with AI
- SOC challenges
- Where AI fits in: Workflows
- Considerations and best practices for AI adoption

elastic

One year on, where are we?

Interest in AI tools such as ChatGPT

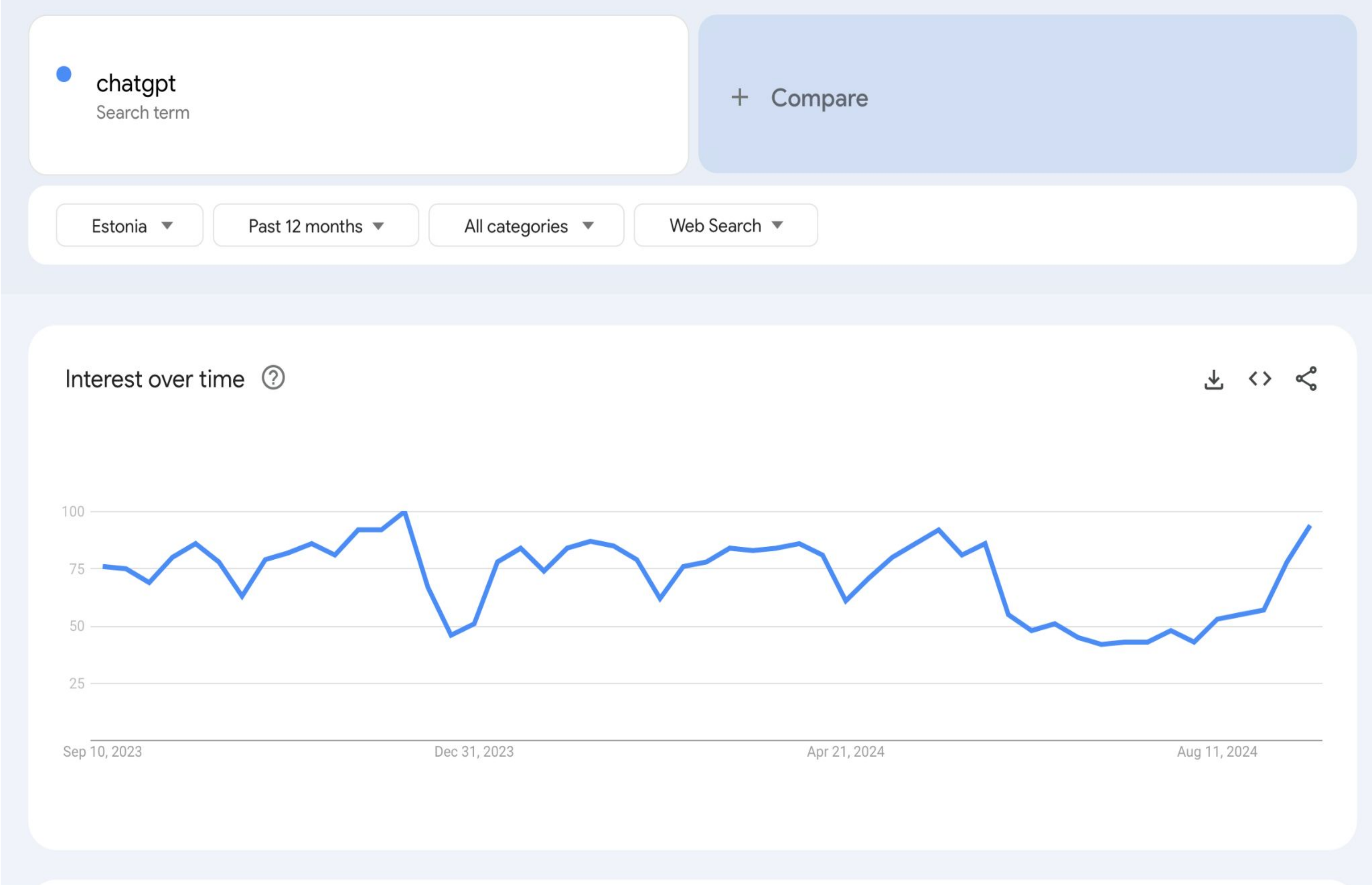
(Sweden)



chatgpt
Search term

Interest in AI tools such as ChatGPT

(Estonia)



chatgpt
Search term

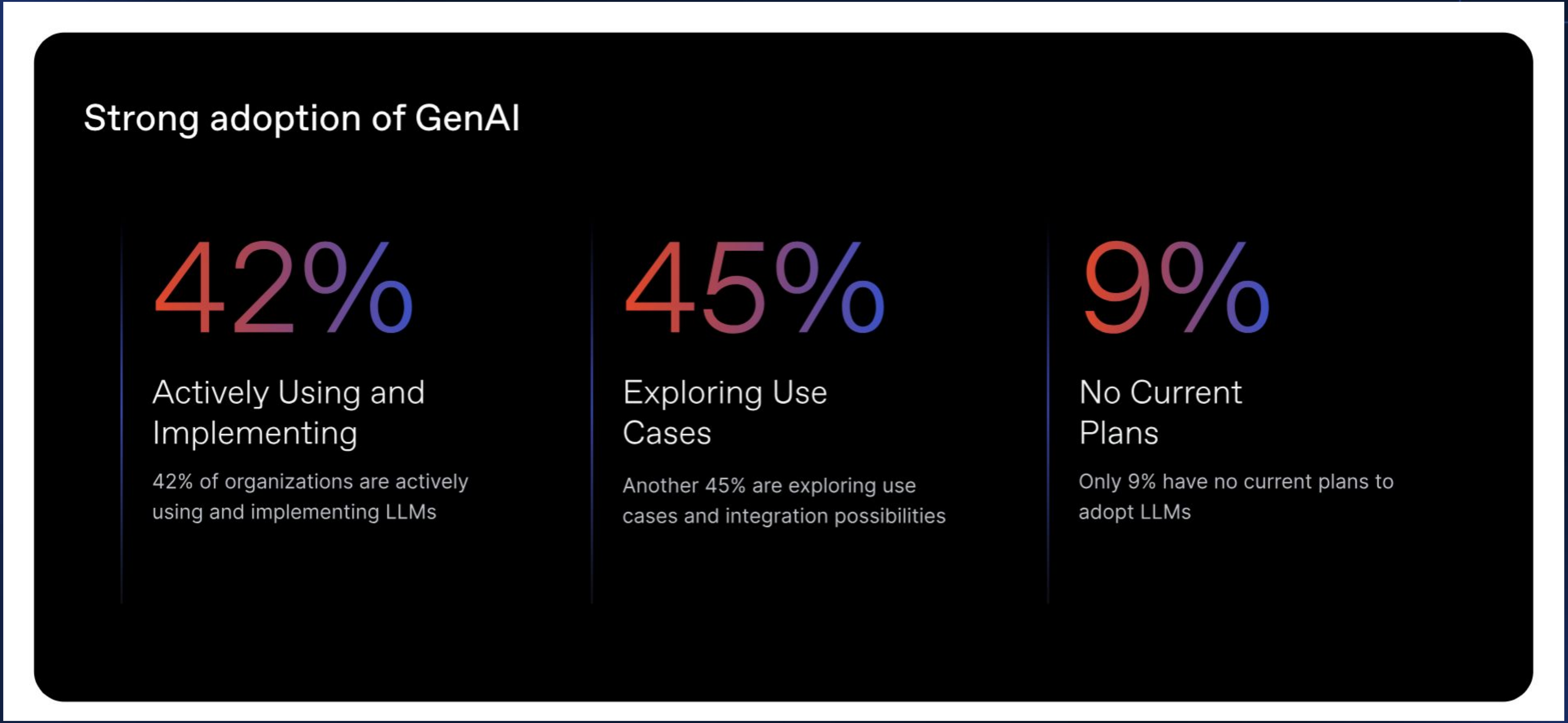
+ Compare

Estonia ▾ Past 12 months ▾ All categories ▾ Web Search ▾

Interest over time

elastic

AI adoption in organizations isn’t slowing down either!



Strong adoption of GenAI

42%

Actively Using and Implementing

42% of organizations are actively using and implementing LLMs

45%

Exploring Use Cases

Another 45% are exploring use cases and integration possibilities

9%

No Current Plans

Only 9% have no current plans to adopt LLMs

https://www.lakera.ai/event/lakera-global-genai-security-readiness-report-deep-dive

"AI won’t replace humans — but humans with AI will replace humans without AI"

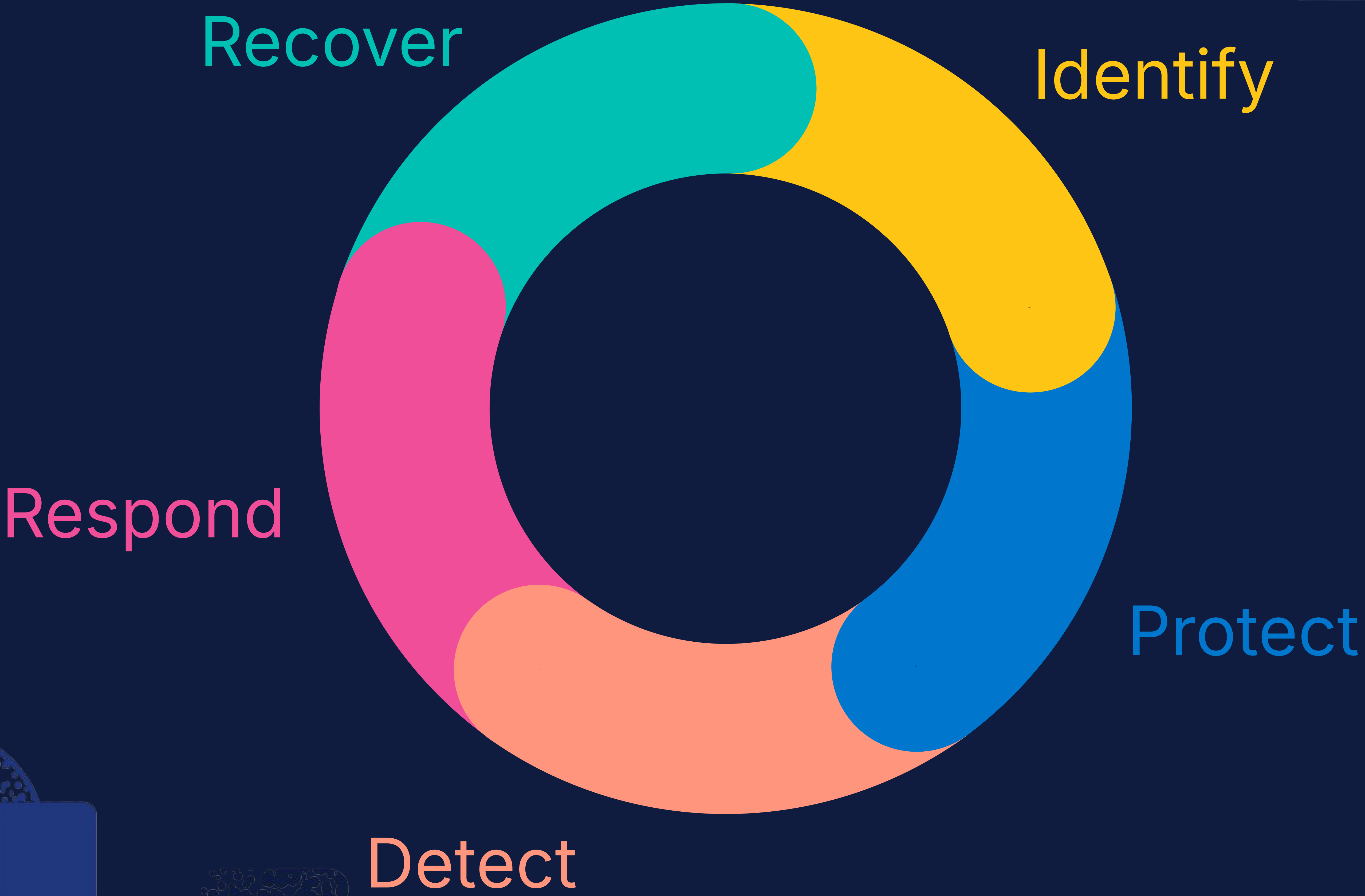
- Prof. Karim Lakhani, Harvard Business School

Let’s bring it to Security

What challenges is today’s SOC facing?

Security operations **challenges**

- Growing attack surface
- Low-fidelity detections
- Overtaxed SecOps teams



Identify

Protect

Detect

Respond

Recover

Alert overload: Challenges faced by SOC teams

$3.3B Annual cost for managing manual alert triage

4,482 Average daily alerts that SOC teams receive

3 hrs/day Time spent manually triaging the alerts

67% Alerts beyond analyst capacity

83% Reported alerts are false positives,
not worth investigating

Source: [90% of SOC analysts believe current threat detection tools are effective]

elastic

The **AI era** is here

Attacks are becoming more advanced and pervasive

- Global cybercrime ecosystem facilitates sophisticated attacks
- AI boosts social engineering, exploit development, vuln scanning & more

The SOC must counter threats to minimize damage

- Financial loss
- Operational disruption
- Exposure of sensitive data
- Reputational damage

elastic

SIEM is evolving

SIEM 1.0

The birth of SIEM

- Log centralization
- Compliance and IR focus
- Visibility for the security team

Legacy

SIEM 2.0

Detections, Machine Learning, Automation, and Orchestration

- Finding threats missed by others
- ML augments rules-based detection
- UEBA added as a core use case
- Facilitating response and remediation workflows
- TDIR emerges (Threat Detection, Investigation, and Response)

Recent

SIEM 3.0

Generative AI Revolution

- Accelerating existing teams with AI-driven workflows
- Addressing the skill gap challenge
- Democratizing security

Future

elastic

AI-driven security analytics

Powered by the Elastic Search AI Platform

Accelerate onboarding of custom data sources

Triage a flood of alerts down to the attacks that matter

Augment expertise to boost SOC productivity

Unlock generative AI for your SOC

Open LLM ecosystem

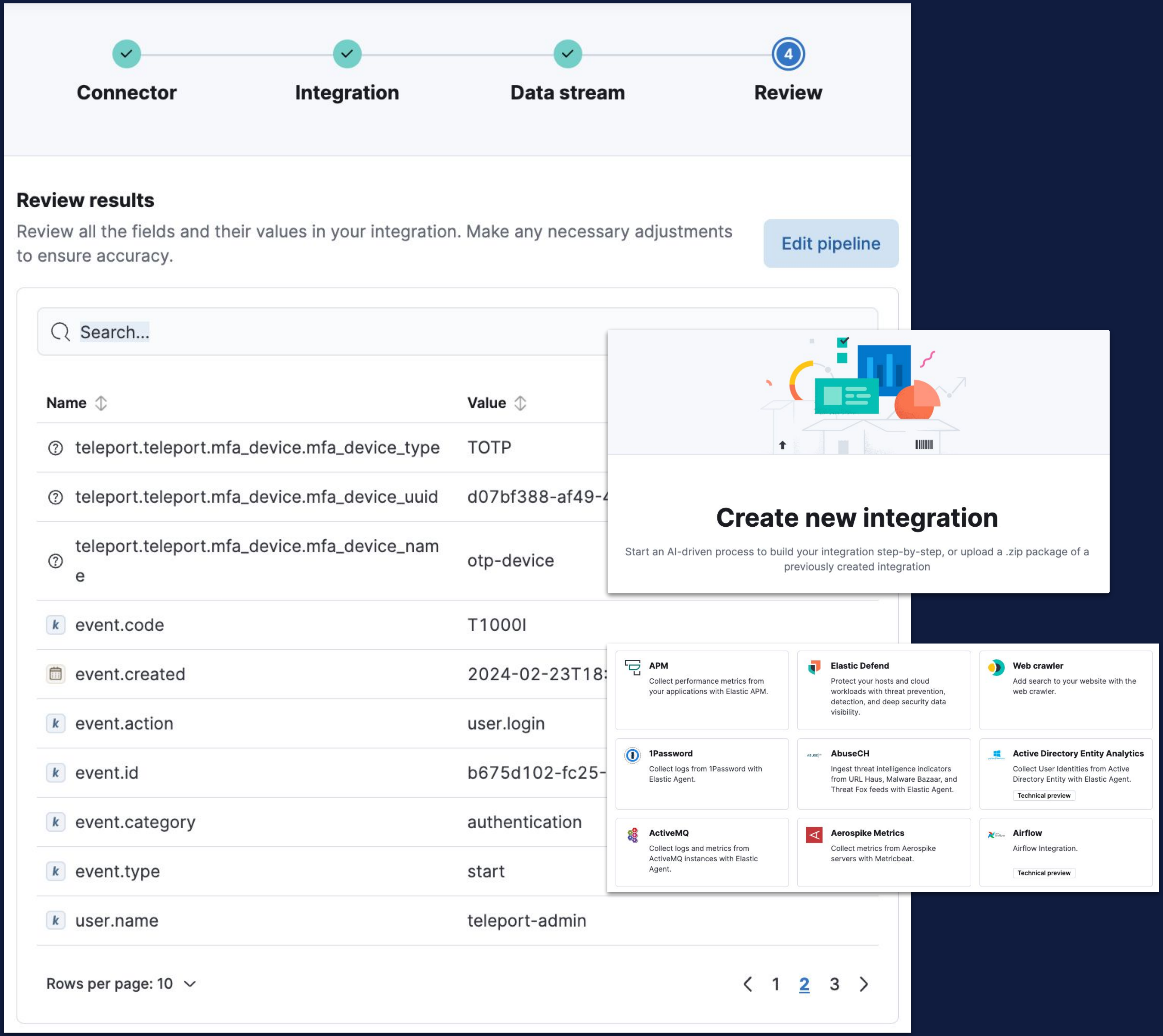
- Retrieval augmented generation
- Real-time visibility
- Security and privacy

NEW

ACCELERATE DATA ONBOARDING

Automatic Import

- Create custom data integrations in minutes, not days
- Extend visibility beyond Elastic’s 400+ prebuilt data integrations
- Reduce the cost, complexity, and stress of SIEM migration



Review results

Review all the fields and their values in your integration. Make any necessary adjustments to ensure accuracy.

Name	Value
teleport.teleport.mfa_device.mfa_device_type	TOTP
teleport.teleport.mfa_device.mfa_device_uuid	d07bf388-af49-4
teleport.teleport.mfa_device.mfa_device_name	otp-device
event.code	T1000I
event.created	2024-02-23T18:
event.action	user.login
event.id	b675d102-fc25-
event.category	authentication
event.type	start
user.name	teleport-admin

Create new integration

Start an AI-driven process to build your integration step-by-step, or upload a .zip package of a previously created integration

APM
Collect performance metrics from your applications with Elastic APM.

Elastic Defend
Protect your hosts and cloud workloads with threat prevention, detection, and deep security data visibility.

Web crawler
Add search to your website with the web crawler.

1Password
Collect logs from 1Password with Elastic Agent.

AbuseCH
Ingest threat intelligence indicators from URL Haus, Malware Bazaar, and Threat Fox feeds with Elastic Agent.

Active Directory Entity Analytics
Collect User Identities from Active Directory Entity with Elastic Agent.
Technical preview

ActiveMQ
Collect logs and metrics from ActiveMQ instances with Elastic Agent.

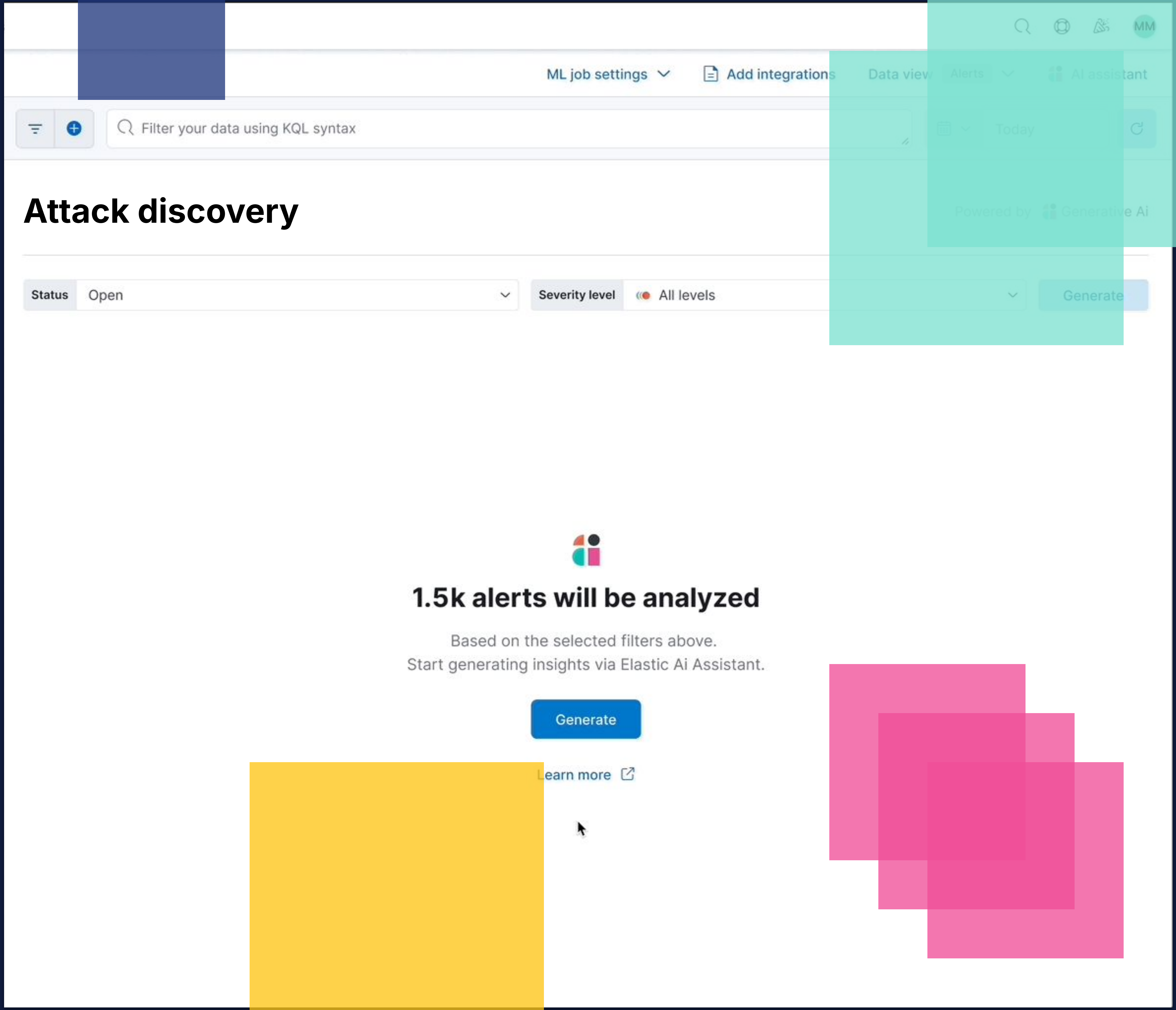
Aerospike Metrics
Collect metrics from Aerospike servers with Metricbeat.

Airflow
Airflow Integration.
Technical preview

AUTOMATE TRIAGE

Attack Discovery

- Prioritize attacks, not alerts
- Assess alerts holistically, rather than as a succession of one-off events
- Get guidance on what to do next, ask follow-up questions, and take immediate action



Filter your data using KQL syntax

Data view: Alerts

Attack discovery

Status: Open

Severity level: All levels

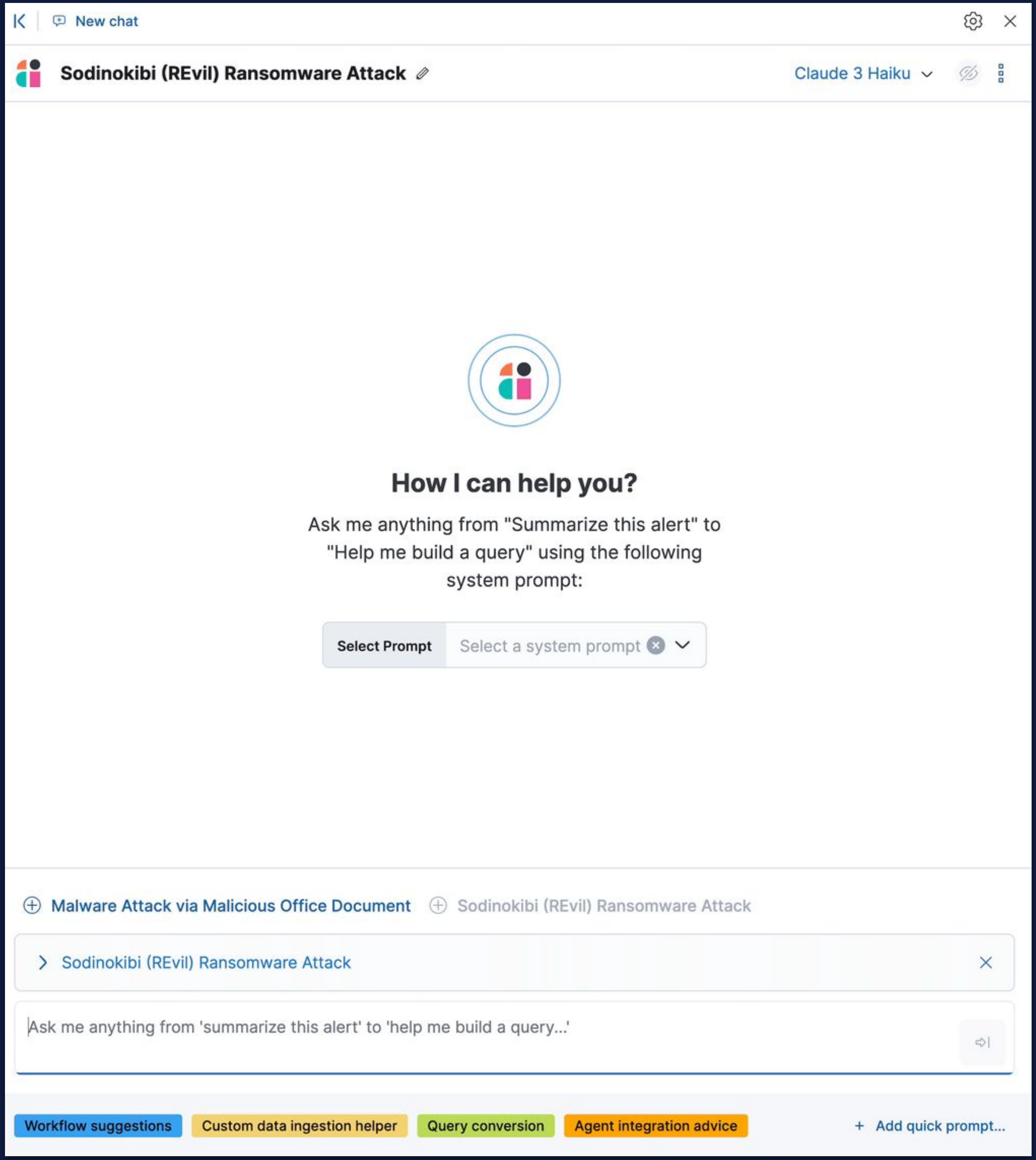
1.5k alerts will be analyzed

Based on the selected filters above.
Start generating insights via Elastic Ai Assistant.

EMPOWER PRACTITIONERS

AI Assistant

- Make every user a power user
- Guide analysts through triage, investigation, and response
- Help admins with routine tasks



Sodinokibi (REvil) Ransomware Attack

How I can help you?

Ask me anything from "Summarize this alert" to "Help me build a query" using the following system prompt:

Select Prompt

Select a system prompt

Malware Attack via Malicious Office Document
Sodinokibi (REvil) Ransomware Attack

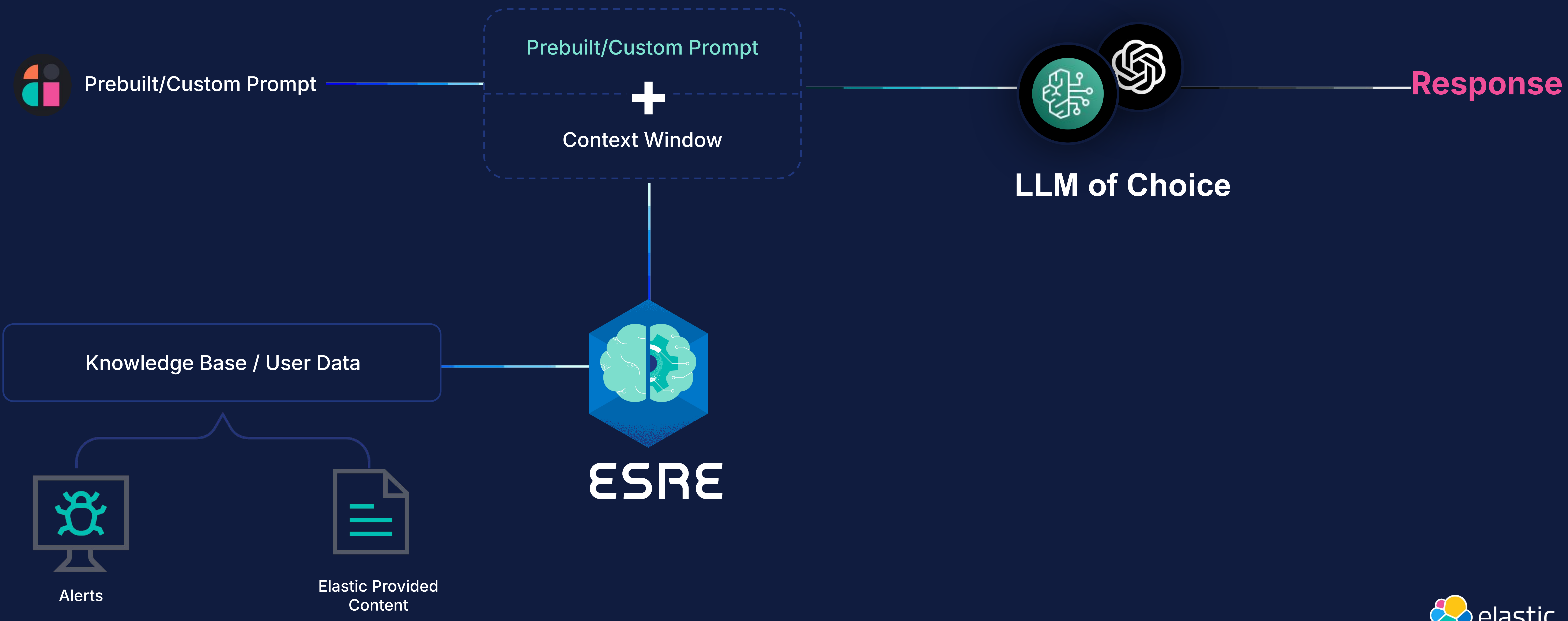
Sodinokibi (REvil) Ransomware Attack

Ask me anything from 'summarize this alert' to 'help me build a query...'

Workflow suggestions
Custom data ingestion helper
Query conversion
Agent integration advice
+ Add quick prompt...

elastic

Elastic AI Assistant - Behind the Scenes



elastic

All this is great, but is AI safe to use?

As with most things, there are always risks

The steps we can take include:

- Ensuring data privacy and confidentiality
- Human validation
- Informed choice of LLM
- Adherence to governance and regulation
- Employee training and awareness

Security can be a bear...

Elastic Security can help.

- Arm every analyst
- Accelerate security workflows
- Improve security posture
- Optimize security budgets
- Centralize security operations

Thank You!

Visit our booth!

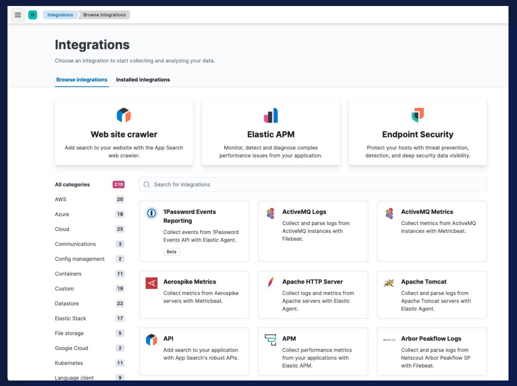
For more information

elastic security labs

Global Threat Report

October 2023

Download the
Elastic security labs
Global Threat Report
elastic.co/security-labs



Integrations

Choose an integration to start collecting and analyzing your data.

Web site crawler
Add search to your website with the App Search web crawler.

Elastic APM
Monitor, detect and diagnose complex performance issues from your application.

Endpoint Security
Protect your hosts with threat prevention, detection, and deep security data visibility.

All categories	210
AWS	20
Azure	18
Cloud	25
Communications	3
Config management	2
Containers	11
Custom	19
Datastore	22
Elastic Stack	17
File storage	5
Google Cloud	2
Kubernetes	11
Language client	9

1Password Events Reporting
Collect events from 1Password Events API with Elastic Agent.
Beta

ActiveMQ Logs
Collect and parse logs from ActiveMQ instances with Filebeat.

ActiveMQ Metrics
Collect metrics from ActiveMQ instances with Metricbeat.

Aerospike Metrics
Collect metrics from Aerospike servers with Metricbeat.

Apache HTTP Server
Collect logs and metrics from Apache servers with Elastic Agent.

Apache Tomcat
Collect and parse logs from Apache Tomcat servers with Elastic Agent.

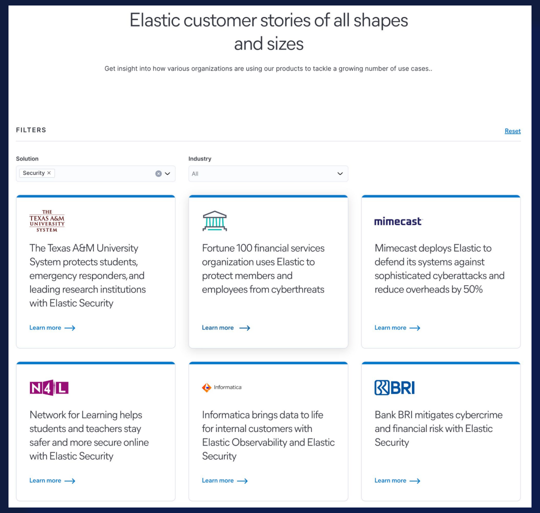
API
Add search to your application with App Search's robust APIs.

APM
Collect performance metrics from your applications with Elastic APM.

Arbor Peakflow Logs
Collect and parse logs from Netscout Arbor Peakflow SP with Filebeat.

Try Elastic Security
for yourself at
cloud.elastic.co

(14 day free trial)



Elastic customer stories of all shapes and sizes

Get insight into how various organizations are using our products to tackle a growing number of use cases..

THE TEXAS A&M UNIVERSITY SYSTEM
The Texas A&M University System protects students, emergency responders, and leading research institutions with Elastic Security
Learn more →

Fortune 100 financial services organization uses Elastic to protect members and employees from cyberthreats
Learn more →

mimecast
Mimecast deploys Elastic to defend its systems against sophisticated cyberattacks and reduce overheads by 50%
Learn more →

N4L
Network for Learning helps students and teachers stay safer and more secure online with Elastic Security
Learn more →

Informatica
Informatica brings data to life for internal customers with Elastic Observability and Elastic Security
Learn more →

BRI
Bank BRI mitigates cybercrime and financial risk with Elastic Security
Learn more →

Check out more
Elastic Security
customer stories

ela.st/security-stories

OH MY MALWARE!

See the power of
prevention with
Elastic Security
ohmymalware.com

elastic