Édition_2024 / 14_11_2024

SÉCURITÉ & QUALITÉ DU CODE

DEVCON#23

L'approche RAG pour la cyber-sécurité

David Pilato
@dadoonet

aws

elastic

Hewlett Packard Enterprise

JFrog

PROGRAMMEZ!
LE MAGAZINE DES DÉVELOPPEURS

BenQ

ESGI
école supérieure de génie informatique

DEVCON#23 : MERCI AUX PARTENAIRES DE LA DEVCON et du HORS-SERIE SECURITE

aws

Hewlett Packard Enterprise

elastic

JFrog

MERCI À

ESGI
école supérieure de
génie informatique

PARTENAIRE SPÉCIAL HARDWARE

BenQ

PROGRAMMEZ!
LE MAGAZINE DES DÉVELOPPEURS

Elasticsearch

You Know, for Search

elastic

elastic

> These are not the droids you are looking for.

elastic

```
GET /_analyze
{
  "char_filter": [ "html_strip" ],
  "tokenizer": "standard",
  "filter": [ "lowercase", "stop", "snowball" ],
  "text": "These are <em>not</em> the droids
           you are looking for."
}
```

These are <em>not</em> the **droids** **you** are **looking** for.

```
{ "tokens": [{
      "token": "droid",
      "start_offset": 27, "end_offset": 33,
      "type": "<ALPHANUM>", "position": 4
    },{
      "token": "you",
      "start_offset": 34, "end_offset": 37,
      "type": "<ALPHANUM>", "position": 5
    }, {
      "token": "look",
      "start_offset": 42, "end_offset": 49,
      "type": "<ALPHANUM>", "position": 7
    }]}
```

Elasticsearch

You Know, for Search

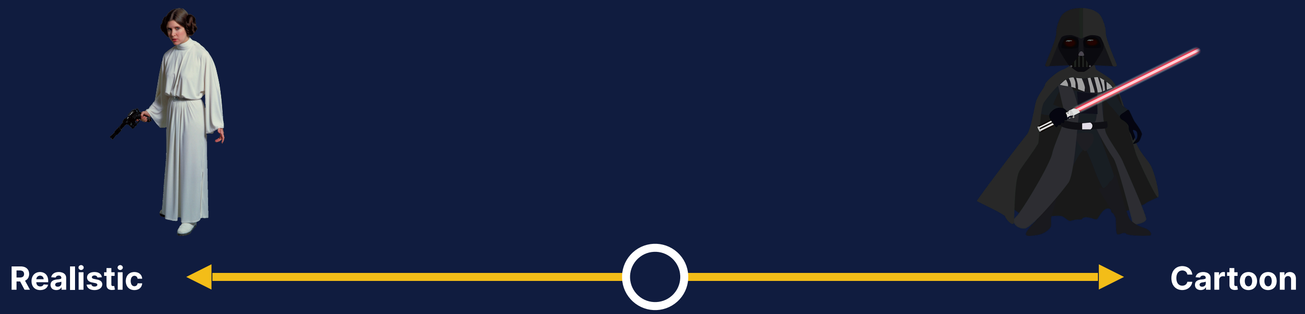
Elasticsearch

You Know, for **Vector** Search

elastic

Embeddings represent your data

Example: 1-dimensional vector



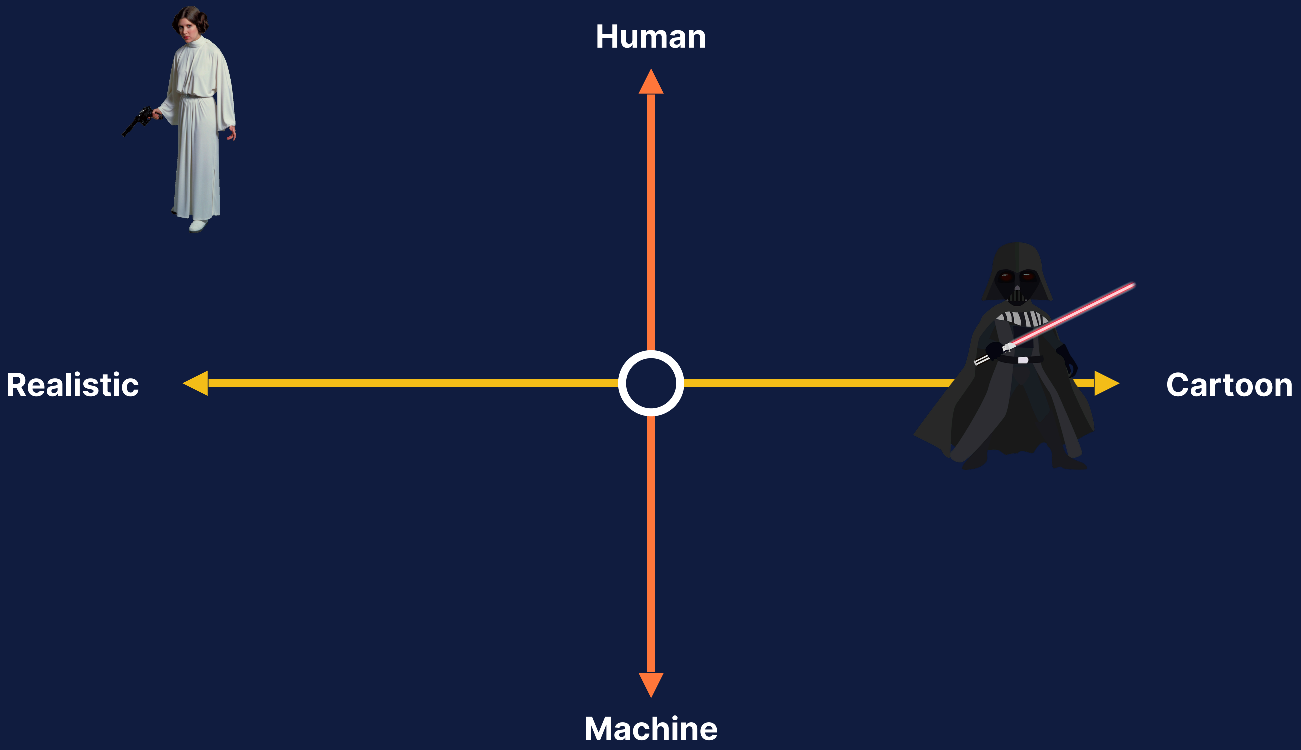
Realistic

Cartoon

Character	Vector
	[-1]
	[1]

Multiple dimensions

represent different data aspects



Human

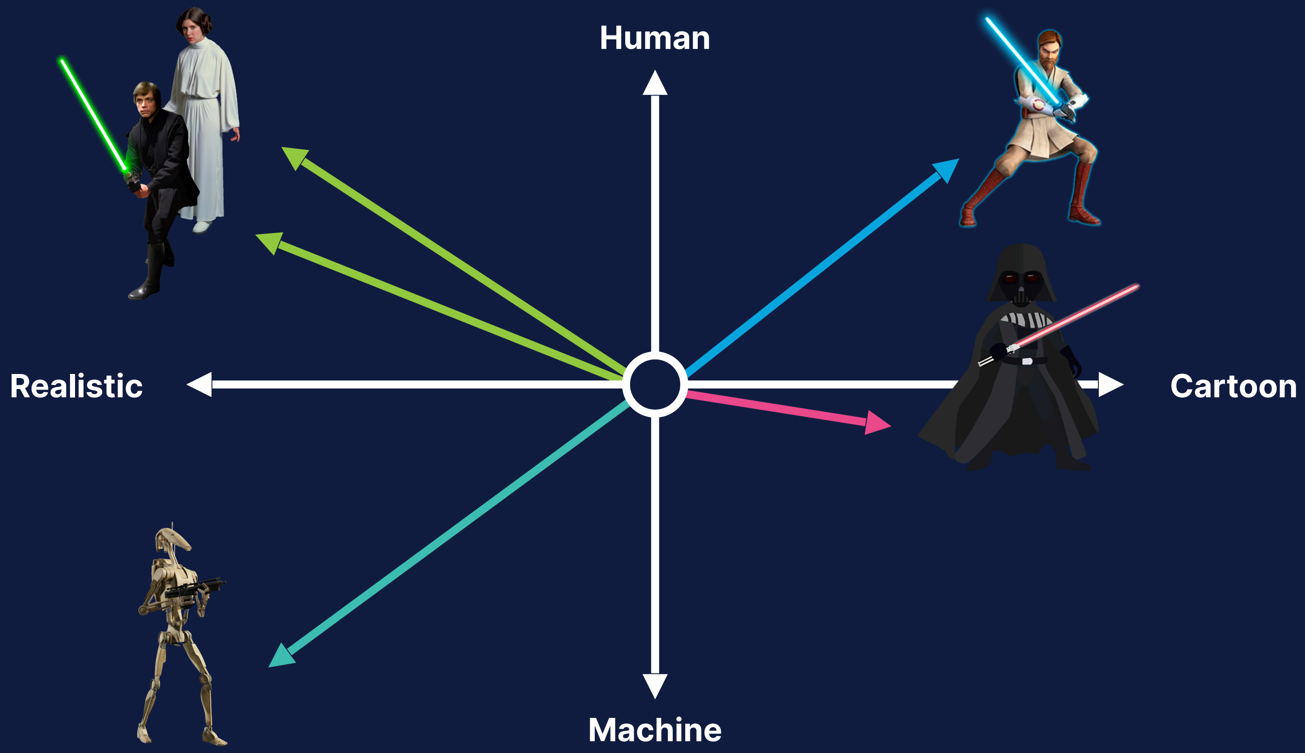
Realistic

Cartoon

Machine

Character	Vector
	[-1, 1]
	[1, 0]

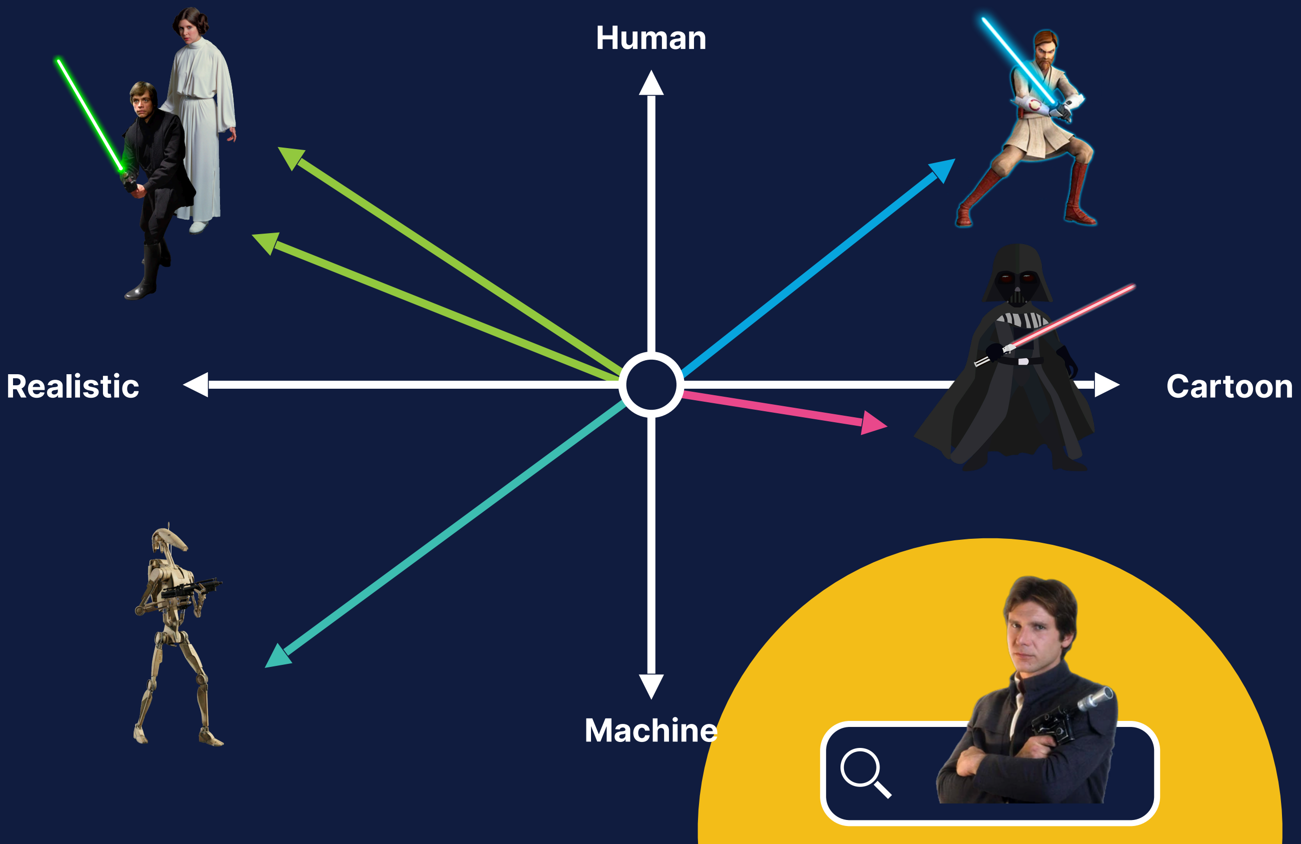
Similar data
is grouped together



Character	Vector
	[-1.0, 1.0]
	[1.0, 0.0]
	[-1.0, 0.8]
	[1.0, 1.0]
	[-1.0, -1.0]

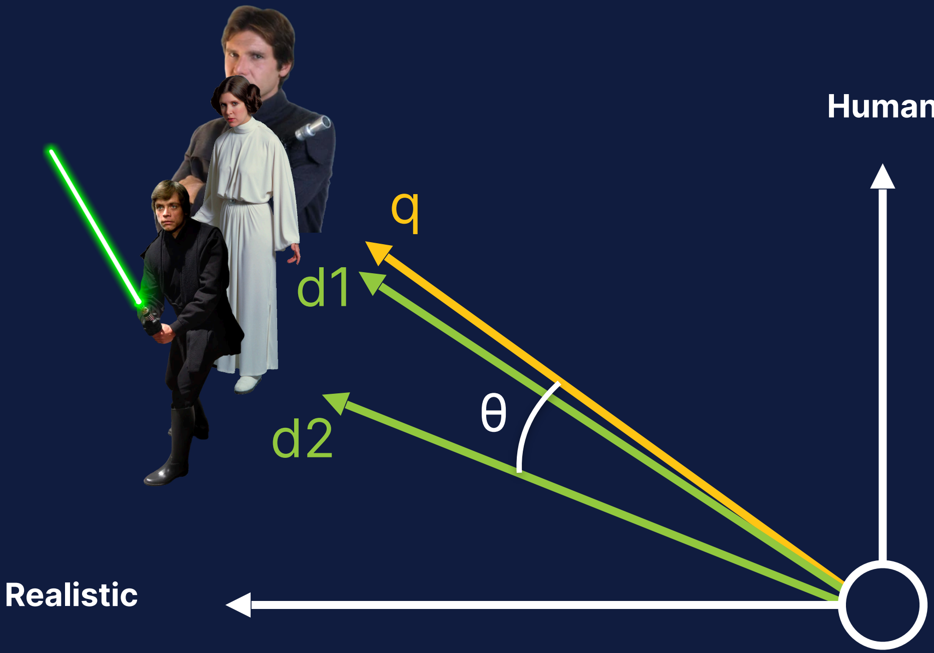
Vector search ranks objects

by similarity (~relevance) to the query



Rank	Result
Query	
1	
2	
3	
4	
5	

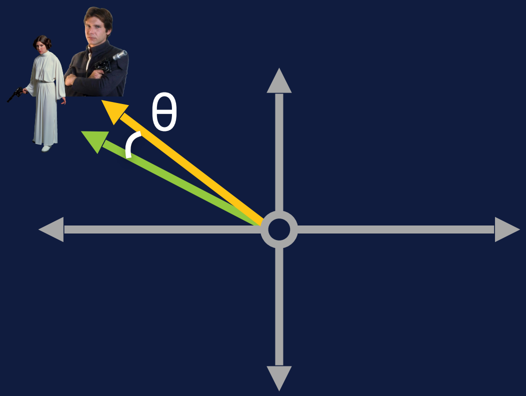
Similarity



$$cos(\theta) = \frac{\vec{q} \times \vec{d}}{|\vec{q}| \times |\vec{d}|}$$

$$\_score = \frac{1 + cos(\theta)}{2}$$

Similarity: cosine (cosine)

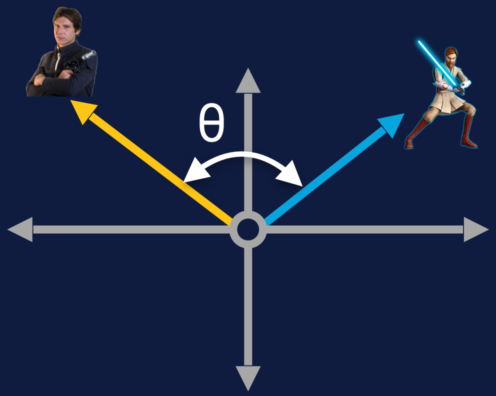


Similar vectors

θ close to 0

cos(θ) close to **1**

$$\_score = \frac{1+1}{2} = 1$$

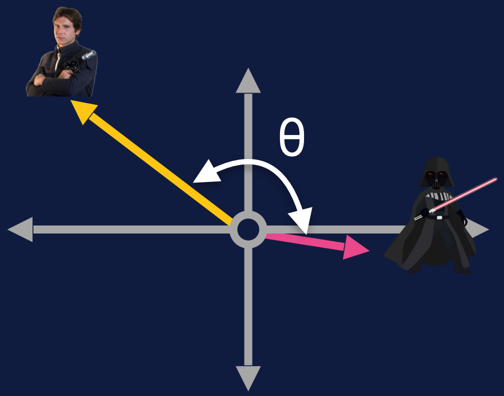


Orthogonal vectors

θ close to 90°

cos(θ) close to **0**

$$\_score = \frac{1+0}{2} = 0.5$$



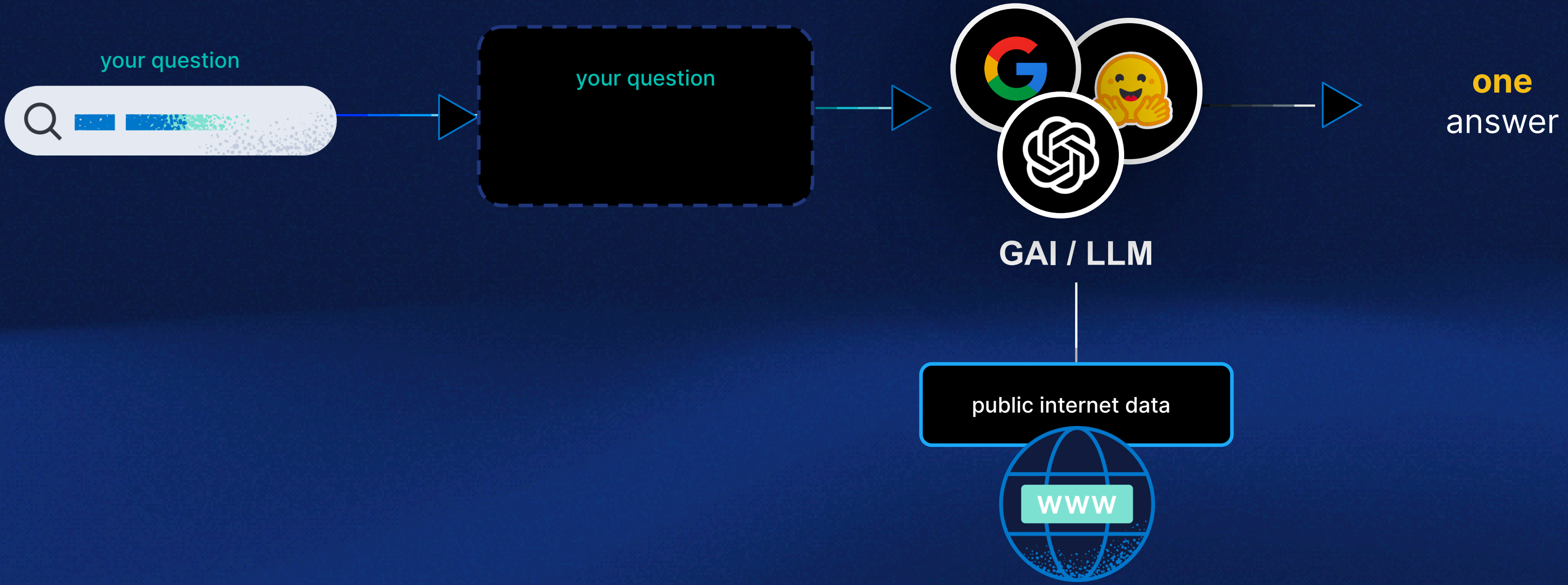
Opposite vectors

θ close to 180°

cos(θ) close to **-1**

$$\_score = \frac{1-1}{2} = 0$$

LLM: opportunities and limits



your question

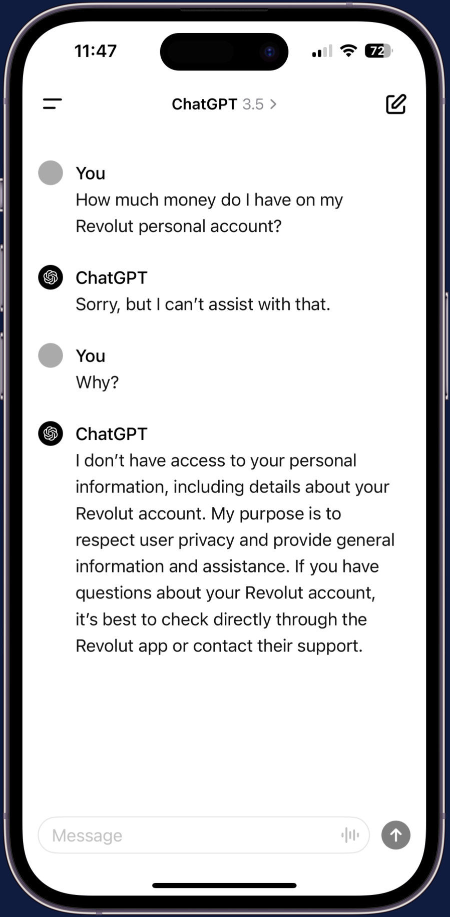
your question

GAI / LLM

public internet data

one answer

elastic



You

How much money do I have on my Revolut personal account?

ChatGPT

Sorry, but I can’t assist with that.

You

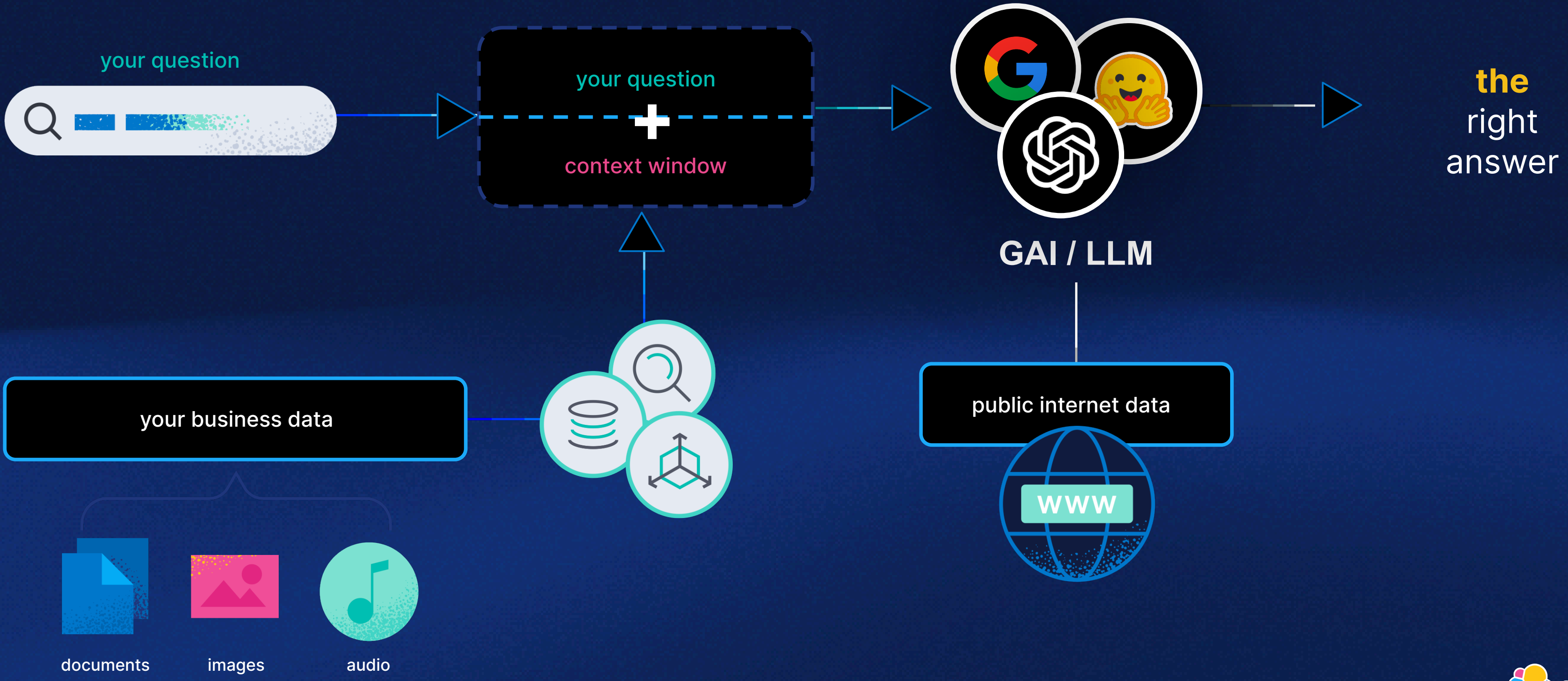
Why?

ChatGPT

I don’t have access to your personal information, including details about your Revolut account. My purpose is to respect user privacy and provide general information and assistance. If you have questions about your Revolut account, it’s best to check directly through the Revolut app or contact their support.

elastic

Retrieval Augmented Generation



your question

your question

context window

GAI / LLM

the right answer

your business data

public internet data

documents

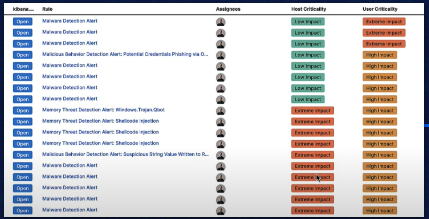
images

audio

elastic

Attack Discovery

100s of alerts



kibana....	Rule	Assignees	Host Criticality	User Criticality
Open	Malware Detection Alert		Low Impact	Extreme Impact
Open	Malware Detection Alert		Low Impact	Extreme Impact
Open	Malware Detection Alert		Low Impact	Extreme Impact
Open	Malicious Behavior Detection Alert: Potential Credentials Phishing via O...		Low Impact	High Impact
Open	Malware Detection Alert		Low Impact	High Impact
Open	Malware Detection Alert		Low Impact	High Impact
Open	Malware Detection Alert		Low Impact	High Impact
Open	Malware Detection Alert		Low Impact	High Impact
Open	Memory Threat Detection Alert: Windows.Trojan.Qbot		Extreme Impact	High Impact
Open	Memory Threat Detection Alert: Shellcode Injection		Extreme Impact	High Impact
Open	Memory Threat Detection Alert: Shellcode Injection		Extreme Impact	High Impact
Open	Memory Threat Detection Alert: Shellcode Injection		Extreme Impact	High Impact
Open	Malicious Behavior Detection Alert: Suspicious String Value Written to R...		Extreme Impact	High Impact
Open	Malware Detection Alert		Extreme Impact	High Impact
Open	Malware Detection Alert		Extreme Impact	High Impact
Open	Malware Detection Alert		Extreme Impact	High Impact
Open	Malware Detection Alert		Extreme Impact	High Impact
Open	Malware Detection Alert		Extreme Impact	High Impact

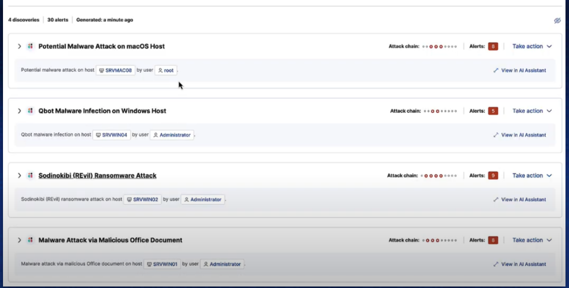
Configurable Anonymization

Summary Prompt

+

Alert Context

Handful of Discoveries mapped across MITRE ATT&CK



4 discoveries | 30 alerts | Generated: a minute ago

Potential Malware Attack on macOS Host — Attack chain: — Alerts: 8 — Take action

Potential malware attack on host SRVMAC08 by user root.

View in AI Assistant

Qbot Malware Infection on Windows Host — Attack chain: — Alerts: 5 — Take action

Qbot malware infection on host SRVWIN04 by user Administrator.

View in AI Assistant

Sodinokibi (REvil) Ransomware Attack — Attack chain: — Alerts: 9 — Take action

Sodinokibi (REvil) ransomware attack on host SRVWIN02 by user Administrator.

View in AI Assistant

Malware Attack via Malicious Office Document — Attack chain: — Alerts: 8 — Take action

Malware attack via malicious Office document on host SRVWIN01 by user Administrator.

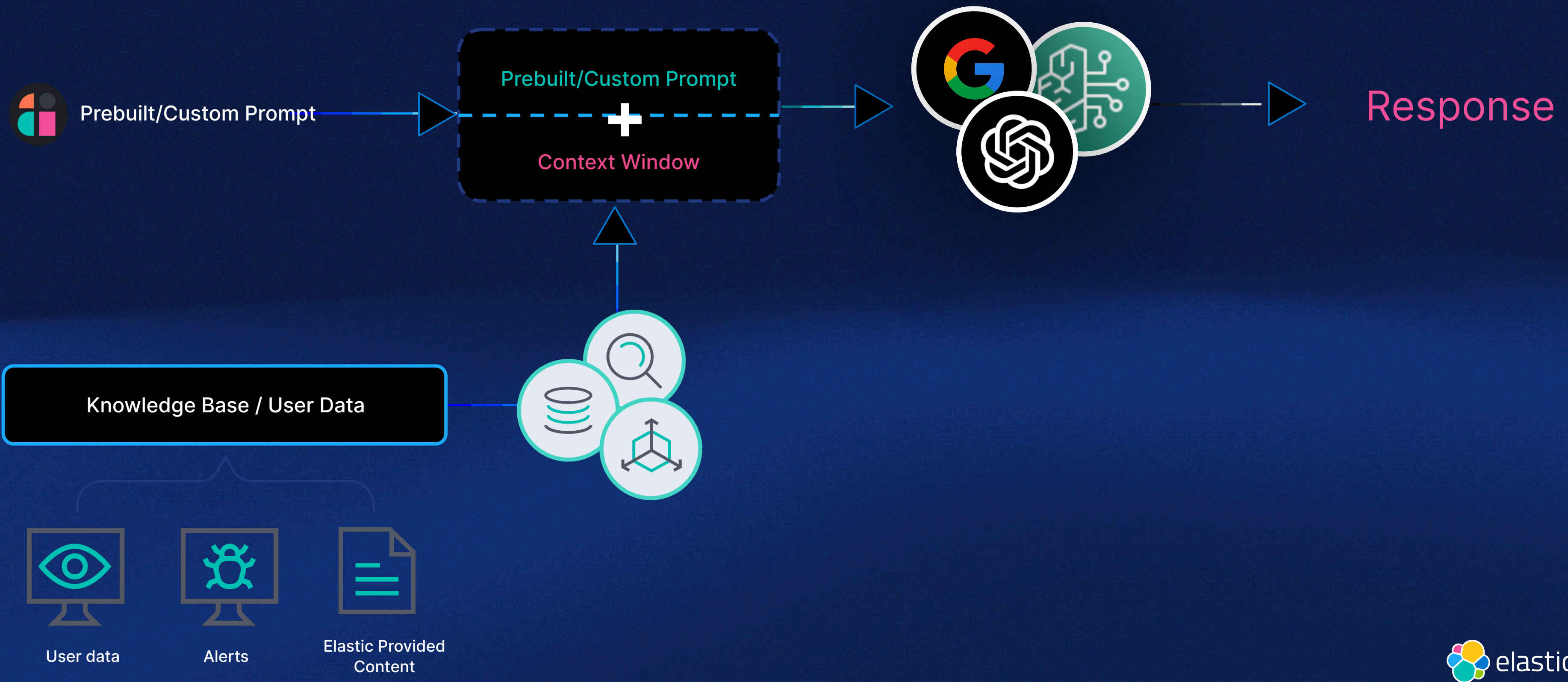
View in AI Assistant

Alert Context

Elastic Detections

Other Detections

Elastic AI Assistant



Prebuilt/Custom Prompt

Prebuilt/Custom Prompt

Context Window

Response

Knowledge Base / User Data

User data

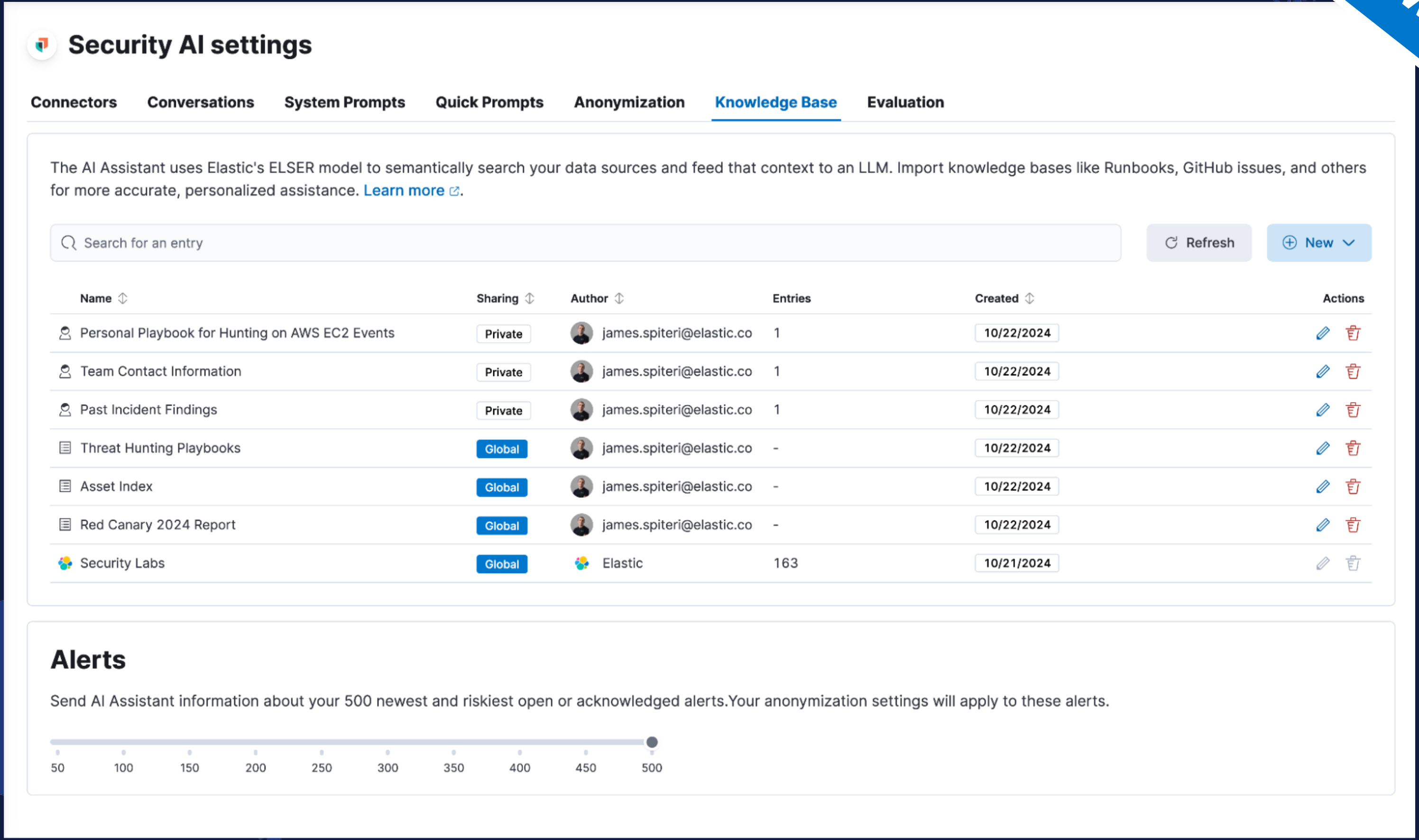
Alerts

Elastic Provided Content

Demo

Attack Discovery

elastic



Security AI settings

The AI Assistant uses Elastic's ELSER model to semantically search your data sources and feed that context to an LLM. Import knowledge bases like Runbooks, GitHub issues, and others for more accurate, personalized assistance. Learn more.

Name	Sharing	Author	Entries	Created	Actions
Personal Playbook for Hunting on AWS EC2 Events	Private	james.spiteri@elastic.co	1	10/22/2024	
Team Contact Information	Private	james.spiteri@elastic.co	1	10/22/2024	
Past Incident Findings	Private	james.spiteri@elastic.co	1	10/22/2024	
Threat Hunting Playbooks	Global	james.spiteri@elastic.co	-	10/22/2024	
Asset Index	Global	james.spiteri@elastic.co	-	10/22/2024	
Red Canary 2024 Report	Global	james.spiteri@elastic.co	-	10/22/2024	
Security Labs	Global	Elastic	163	10/21/2024	

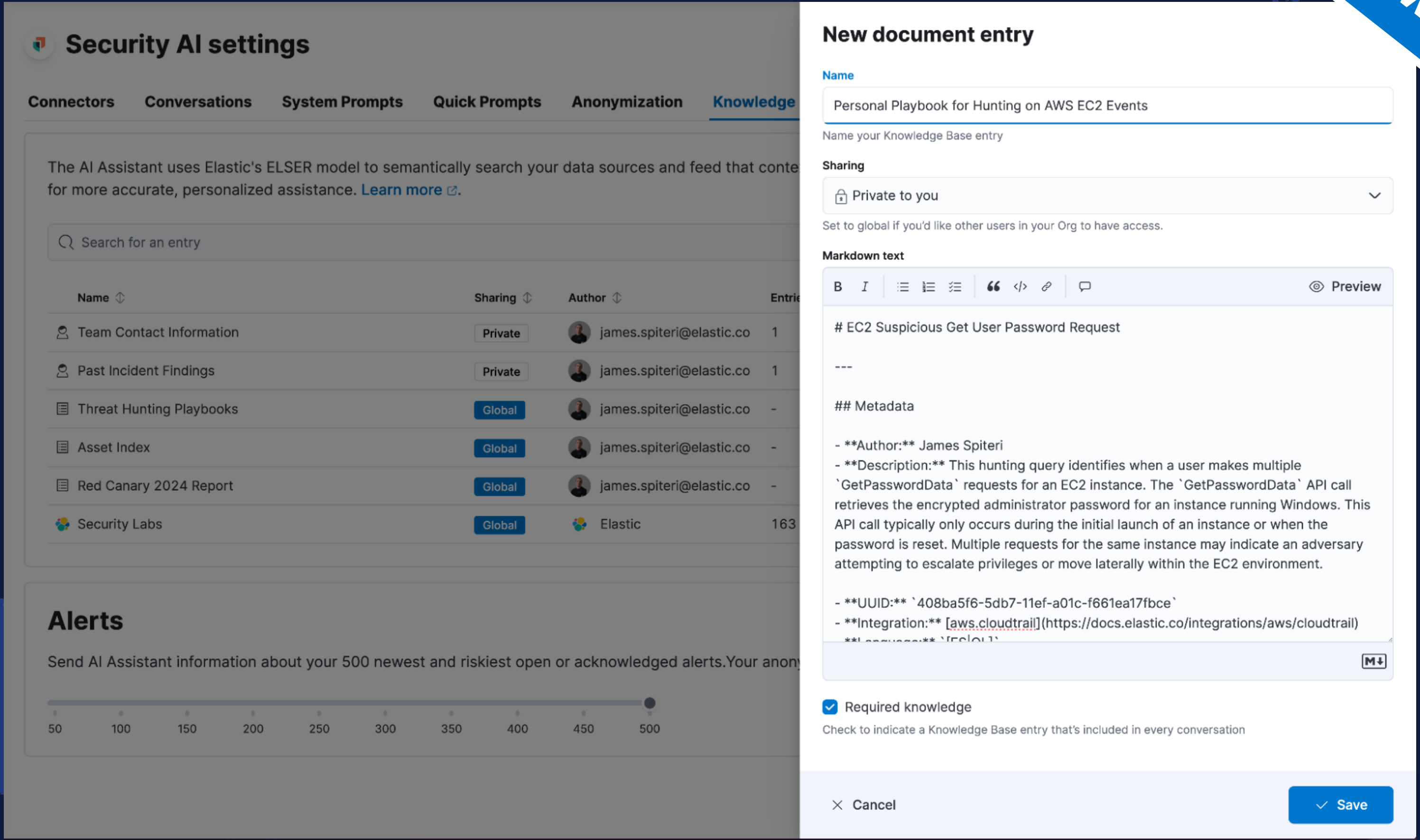
Alerts

Send AI Assistant information about your 500 newest and riskiest open or acknowledged alerts.Your anonymization settings will apply to these alerts.

new in 8.16

elastic

new in 8.16



Security AI settings

The AI Assistant uses Elastic's ELSER model to semantically search your data sources and feed that conte
for more accurate, personalized assistance. Learn more

Search for an entry

Name	Sharing	Author	Entrie
Team Contact Information	Private	james.spiteri@elastic.co	1
Past Incident Findings	Private	james.spiteri@elastic.co	1
Threat Hunting Playbooks	Global	james.spiteri@elastic.co	-
Asset Index	Global	james.spiteri@elastic.co	-
Red Canary 2024 Report	Global	james.spiteri@elastic.co	-
Security Labs	Global	Elastic	163

Alerts

Send AI Assistant information about your 500 newest and riskiest open or acknowledged alerts.Your anon

New document entry

Name: Personal Playbook for Hunting on AWS EC2 Events

Name your Knowledge Base entry

Sharing: Private to you

Set to global if you'd like other users in your Org to have access.

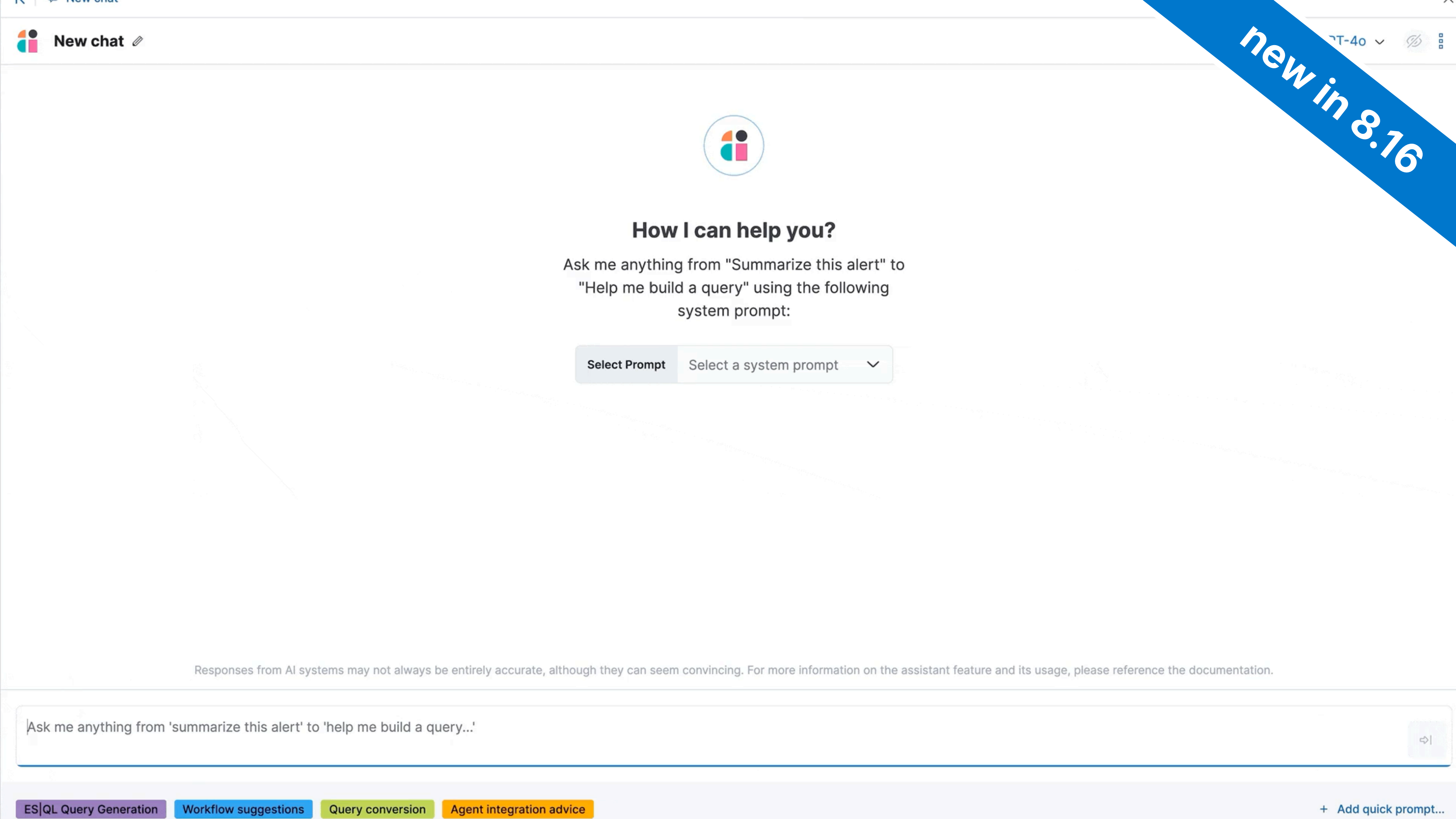
Markdown text

```
# EC2 Suspicious Get User Password Request

---

## Metadata

- **Author:** James Spiteri
- **Description:** This hunting query identifies when a user makes multiple `GetPasswordData` requests for an EC2 instance. The `GetPasswordData` API call retrieves the encrypted administrator password for an instance running Windows. This API call typically only occurs during the initial launch of an instance or when the password is reset. Multiple requests for the same instance may indicate an adversary attempting to escalate privileges or move laterally within the EC2 environment.

- **UUID:** `408ba5f6-5db7-11ef-a01c-f661ea17fbce`
- **Integration:** [aws.cloudtrail](https://docs.elastic.co/integrations/aws/cloudtrail)
- **Language:** `[ES|QL]`
```

☑ Required knowledge

Check to indicate a Knowledge Base entry that's included in every conversation

elastic



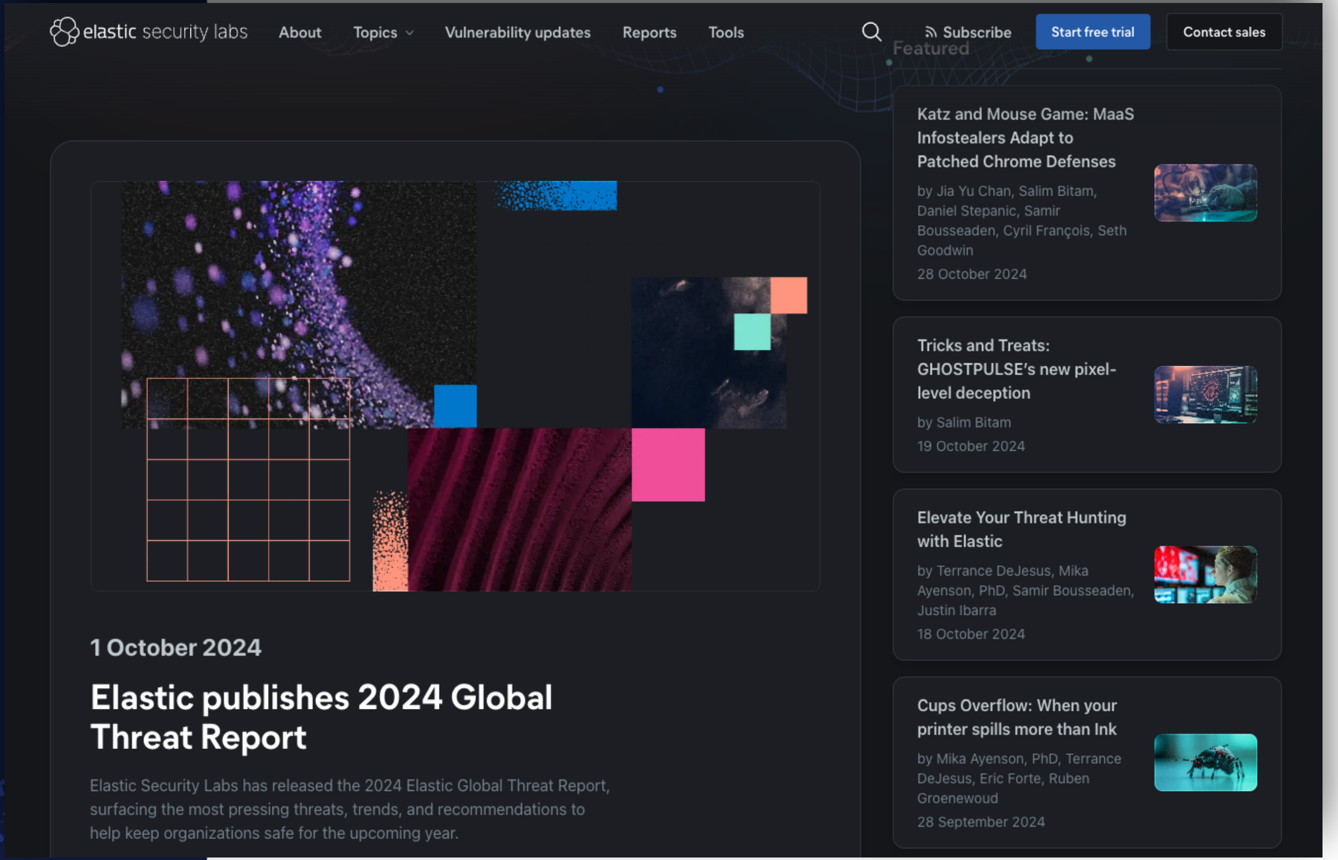
How I can help you?

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

Responses from AI systems may not always be entirely accurate, although they can seem convincing. For more information on the assistant feature and its usage, please reference the documentation.

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

Elastic Security Labs



1 October 2024

Elastic publishes 2024 Global Threat Report

Elastic Security Labs has released the 2024 Elastic Global Threat Report, surfacing the most pressing threats, trends, and recommendations to help keep organizations safe for the upcoming year.

Katz and Mouse Game: MaaS Infostealers Adapt to Patched Chrome Defenses

by Jia Yu Chan, Salim Bitam, Daniel Stepanic, Samir Bousseaden, Cyril François, Seth Goodwin

28 October 2024

Tricks and Treats: GHOSTPULSE's new pixel-level deception

by Salim Bitam

19 October 2024

Elevate Your Threat Hunting with Elastic

by Terrance DeJesus, Mika Ayenson, PhD, Samir Bousseaden, Justin Ibarra

18 October 2024

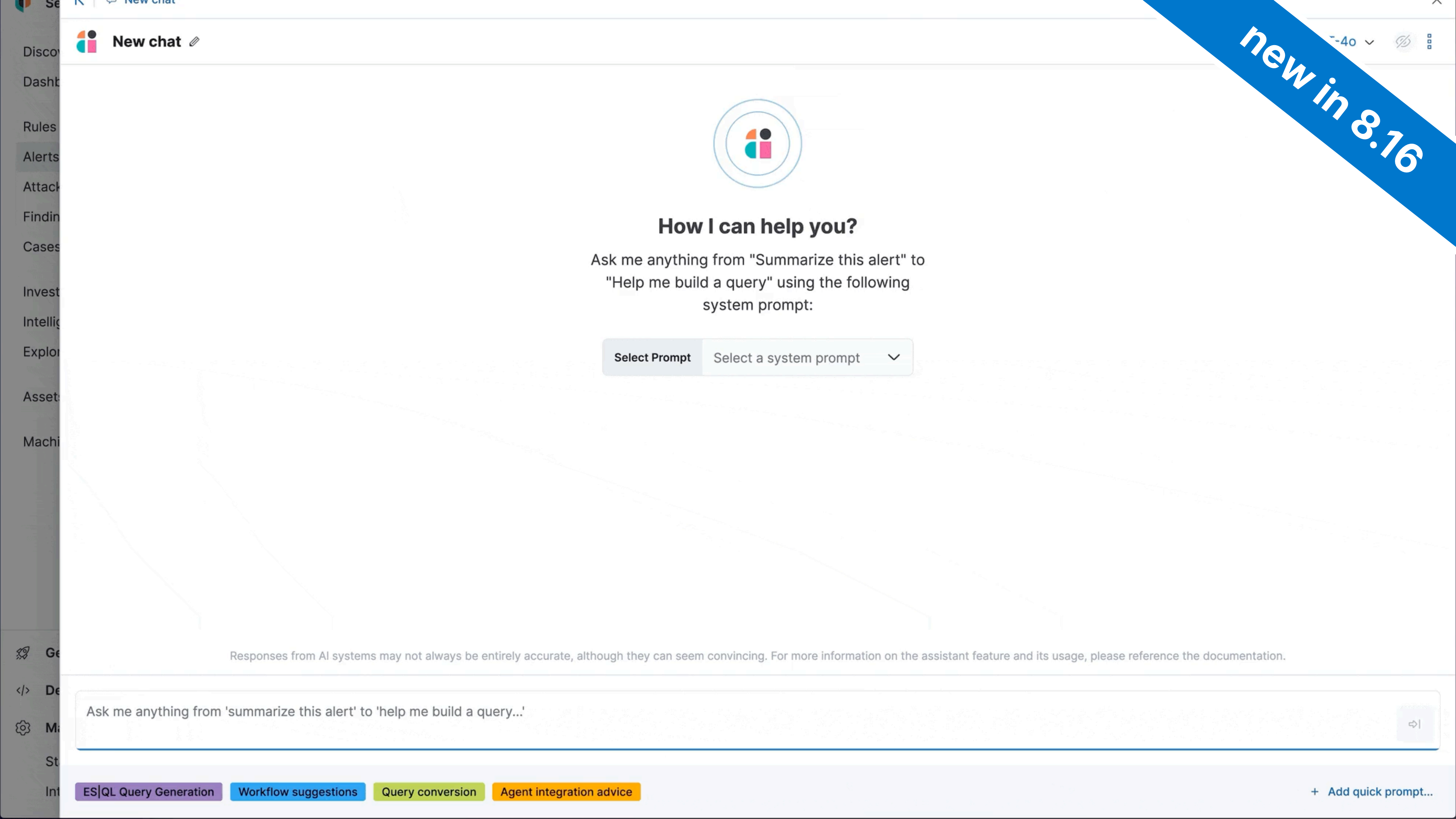
Cups Overflow: When your printer spills more than Ink

by Mika Ayenson, PhD, Terrance DeJesus, Eric Forte, Ruben Groenewoud

28 September 2024

https://www.elastic.co/security-labs

elastic



new in 8.16

New chat

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

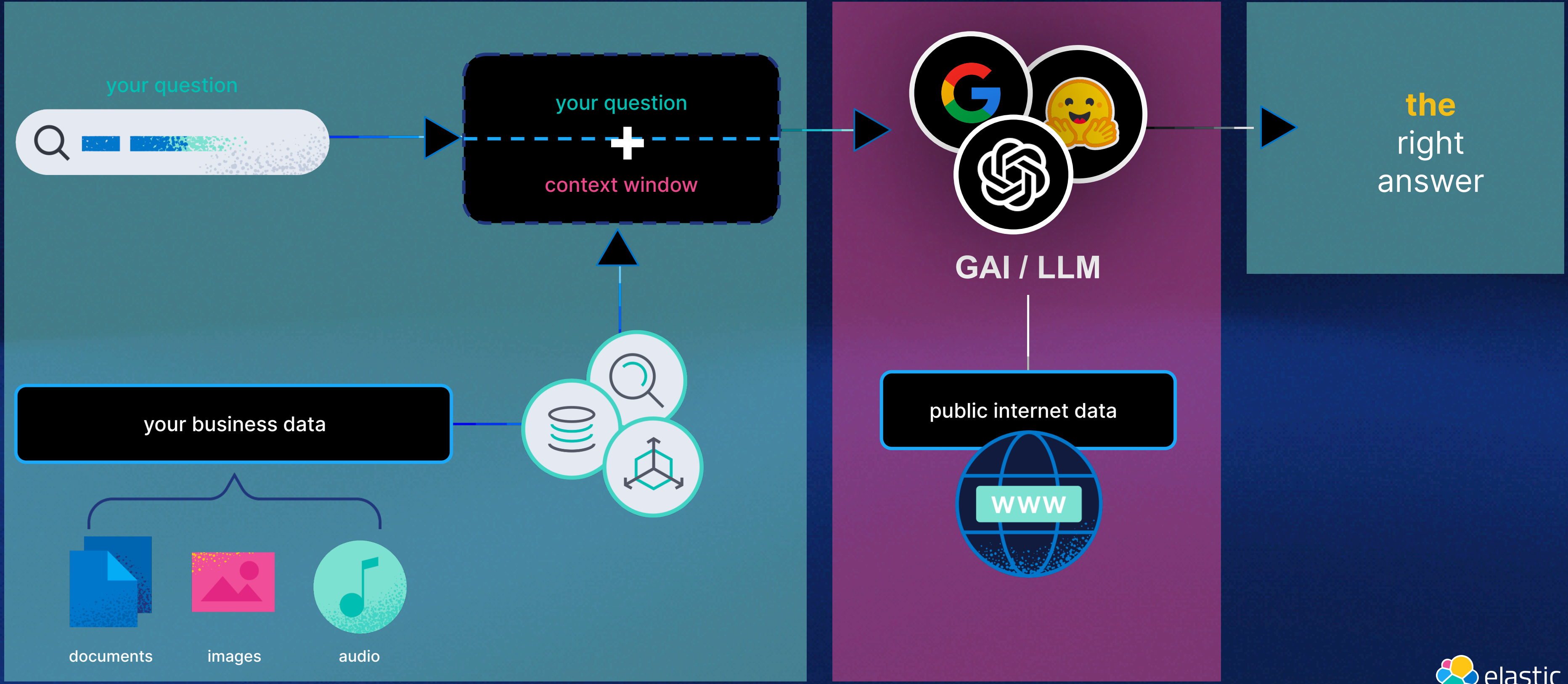
Responses from AI systems may not always be entirely accurate, although they can seem convincing. For more information on the assistant feature and its usage, please reference the documentation.

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

ES|QL Query Generation | Workflow suggestions | Query conversion | Agent integration advice

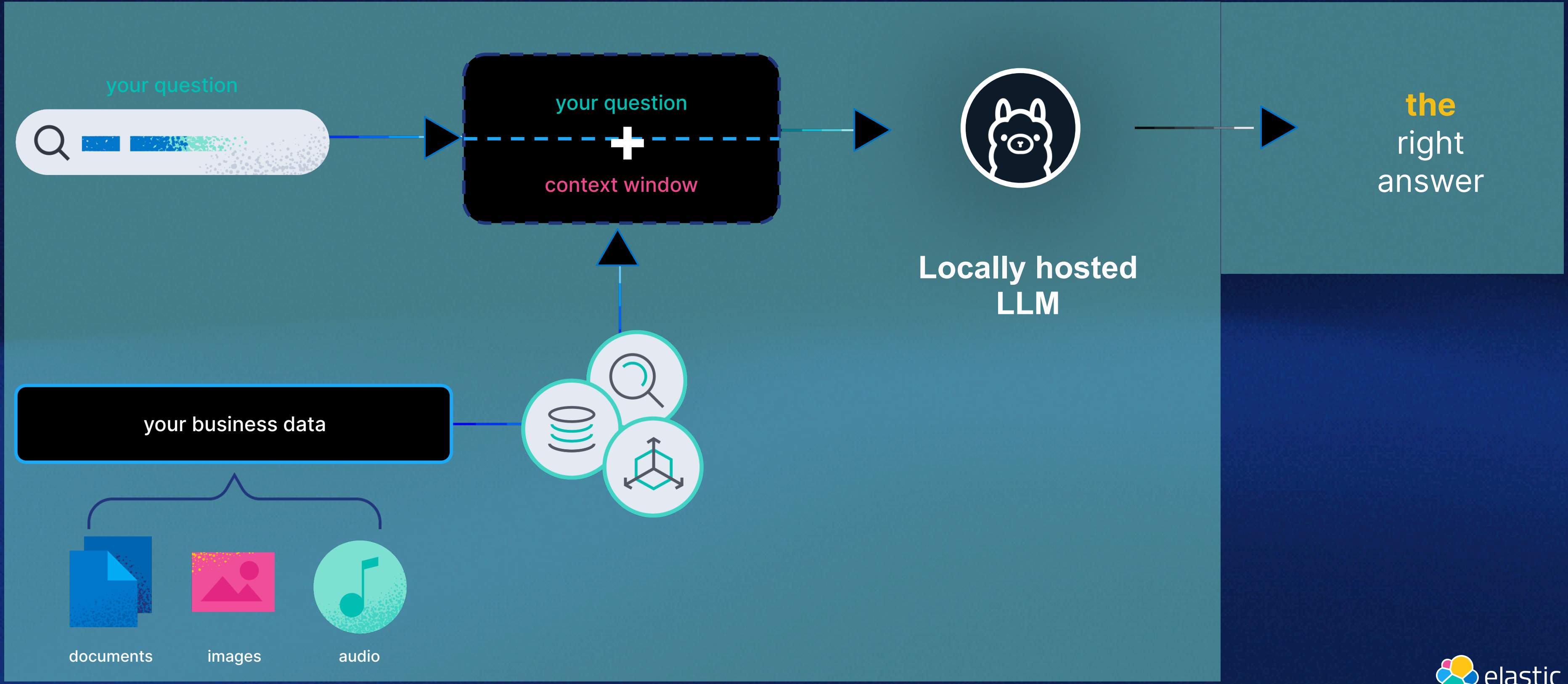
+ Add quick prompt...

Retrieval Augmented Generation



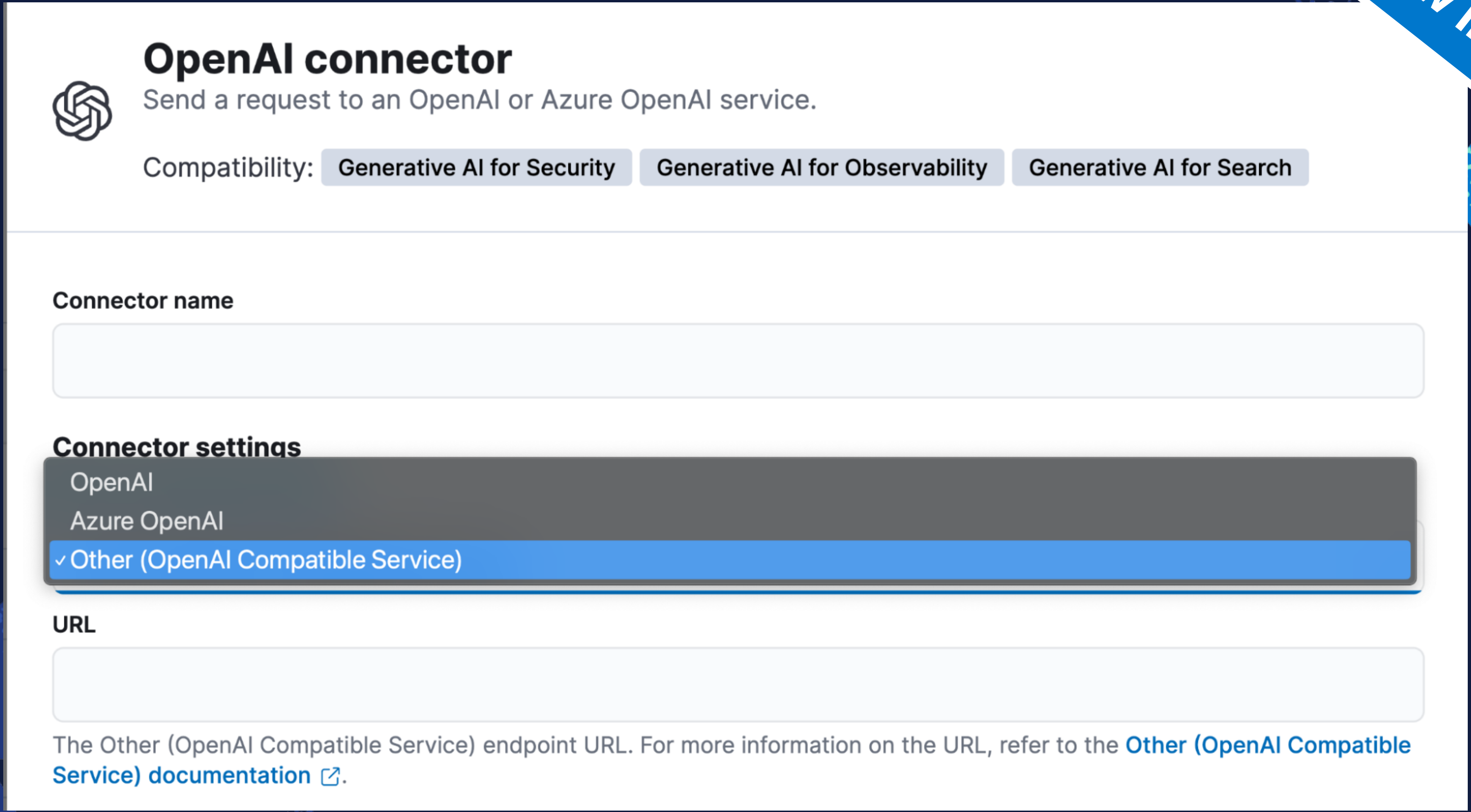
elastic

Retrieval Augmented Generation



elastic

new in 8.16



OpenAI connector

Send a request to an OpenAI or Azure OpenAI service.

Compatibility: Generative AI for Security | Generative AI for Observability | Generative AI for Search

Connector name

Connector settings

OpenAI

Azure OpenAI

✓ Other (OpenAI Compatible Service)

URL

The Other (OpenAI Compatible Service) endpoint URL. For more information on the URL, refer to the Other (OpenAI Compatible Service) documentation.

Édition_2024 / 14_11_2024

aws

elastic

Hewlett Packard
Enterprise

JFrog

BenQ

ESGI
école supérieure de
génie informatique

SÉCURITÉ & QUALITÉ DU CODE

DEVCON#23

L'approche RAG pour la cyber-sécurité

David Pilato
@dadoonet