Moving at the Speed of Security:

Adapting as Quickly as the Threat Landscape Evolves

September 14, 2023

Outline

- Digitization and cybersecurity trends
- The Nordic-Baltic region: 1 year on
- The Rise of AI: opportunities for security

elastic

whoami

- Sr Security Architect
- Part of the Elastic Global Security Specialists Group
- Builder of Security Intelligence & Operations Capability
- Lover of everything security (...and yes, I have other hobbies too!)

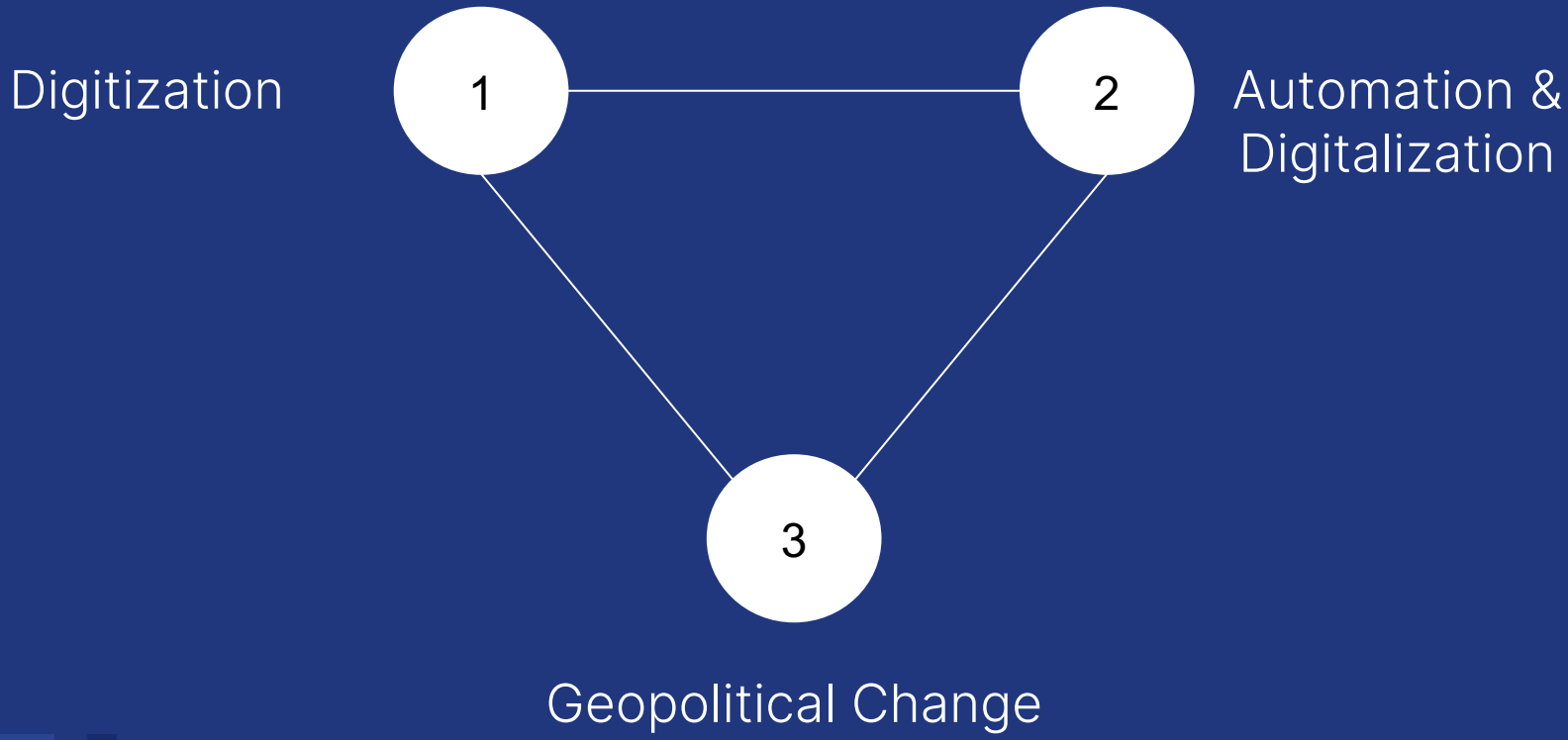
Marvin Ngoma

["CISSP", "GSOM", "Msc"]

Marvin Ngoma
https://www.linkedin.com/in/tyolani

elastic

Where are we today?



elastic

Global security trends driving rapid change

Security challenges are compounding ~~quickly~~ quicker than anticipated

Trend #1:

Accelerated digital transformation and cloud migration

175ZB

predicted worldwide data growth by 2025*

288

# of apps the average enterprise must manage**

Trend #2:

Adversaries extremely motivated to accomplish missions

$10.5T

expected global cost of cybercrime by 2025*

70%

malware attacks involving zero-day, evasive malware****

* IDC, Data Age 2025 report
** Blissfully, 2020 Annual SaaS Trends report
*** Cybersecurity Ventures, Cyberwarfare in the C-Suite report
**** Infosecurity Magazine, Evasive Malware Threats on the Rise article

elastic

Let us bring it closer to home…

….what are we seeing in the Nordic-Baltic region?

First…. A quick recap of 2022…

- Effects Of Covid
  - Accelerated digitization
  - Redefined processes
  - New cyber security challenges
- Geopolitical Climate
  - A surge in digital warfare
  - Alliance influences attack patterns

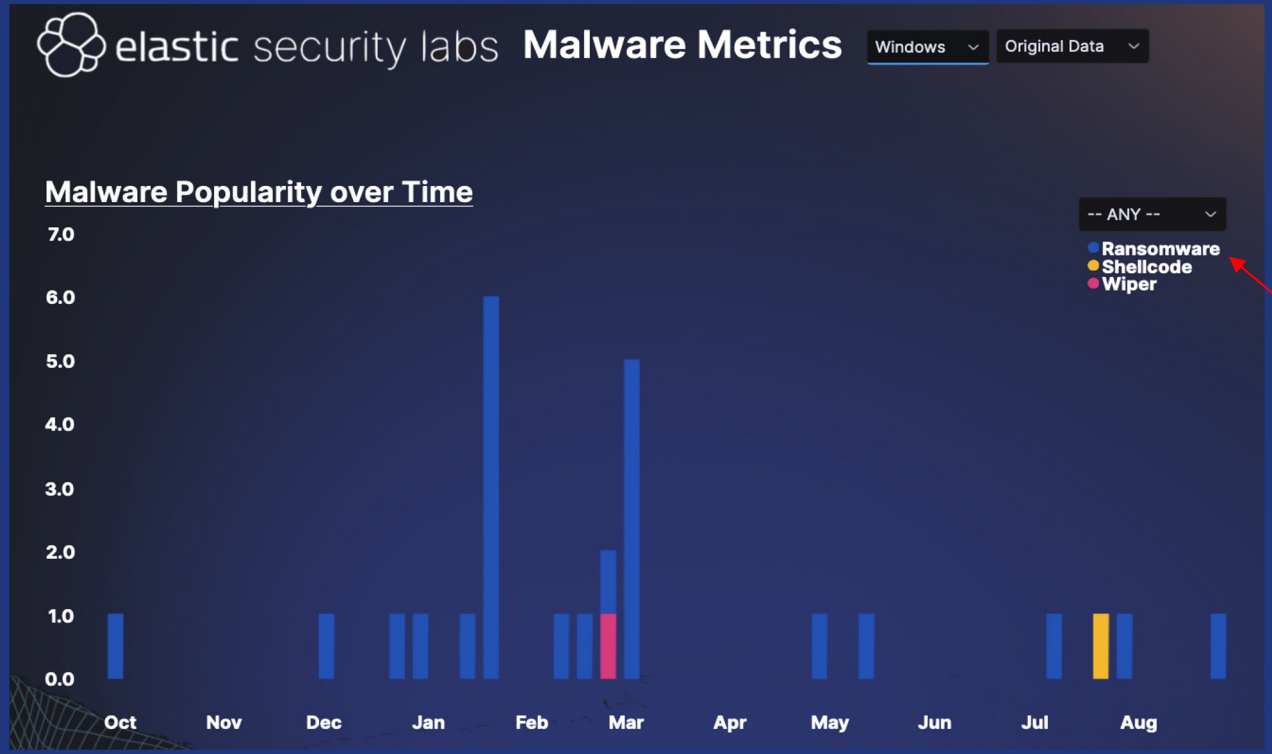
So far in 2023...

- 25% increase in Ransomware *
  - Professionalized & industrialized
  - Attribution now multifaceted
- Significant increase in cyber espionage
- Critical Infrastructure still a huge target
  - The goal is data theft or destruction
  - Attacks are ruthless in nature

*https://www.truesec.com/hub/report/threat-intelligence-report-2023

elastic

Elastic Global Threat Report 2023 spring edition



Ransomware most popular malware observed on Windows systems

https://www.elastic.co/security-labs/elastic-publishes-2023-global-threat-report-spring-edition

Ransomware, Malware, Threat Management

ABB confirms data stolen in Black Basta ransomware attack

Simon Hendery. May 30, 2023

Global industrial automation company ABB has confirmed it had data stolen in an attack attributed to the Black Basta ransomware group.

REUTERS® World Business Markets Sustainability Legal Breakingviews Technology Investigati

Technology

Norway government ministries hit by cyber attack

Reuters

July 24, 2023 10:54 AM GMT+2 · Updated a month ago

OSLO, July 24 (Reuters) - Twelve Norwegian government ministries have been hit by a cyber attack, the Norwegian government said on Monday, the latest attack to hit the public sector of Europe's largest gas supplier and NATO's northernmost member.

"We identified a weakness in the platform of one of our suppliers. That weakness has now been shut," Erik Hope, head of the government agency in charge of providing services to ministries, told a news conference.

Estonian official says parliamentary elections were targeted by cyberattacks

REUTERS® World Business Markets Sustainability Legal Breakingviews Technology Investigat

Europe

Swedish parliament website hit by DDoS attack

Reuters

May 3, 2023 1:30 PM GMT+2 · Updated 4 months ago

STOCKHOLM, May 3 (Reuters) - Sweden's parliament has been hit by a so called distributed denial-of-service (DDoS) attack that has disrupted access to its web page, it said on Wednesday.

The web page was partially down on Tuesday and appeared slow on Wednesday.

"The analysis shows that it is a denial-of-service attack," a parliament spokesperson said. "Right now the web page can be slow and it can be difficult to watch our web casts."

elastic

How is all this impacting security teams?

Security teams are struggling to keep up

Reducing risk is hard -- we need answers quickly

Skilled staff shortages

93%

of companies would benefit from an increase in skilled staffing

Days to identify breach

280

days in average for companies to identify a breach

Alert fatigue not improving

49

security technologies in use by the average enterprise***

Inconsistent processes

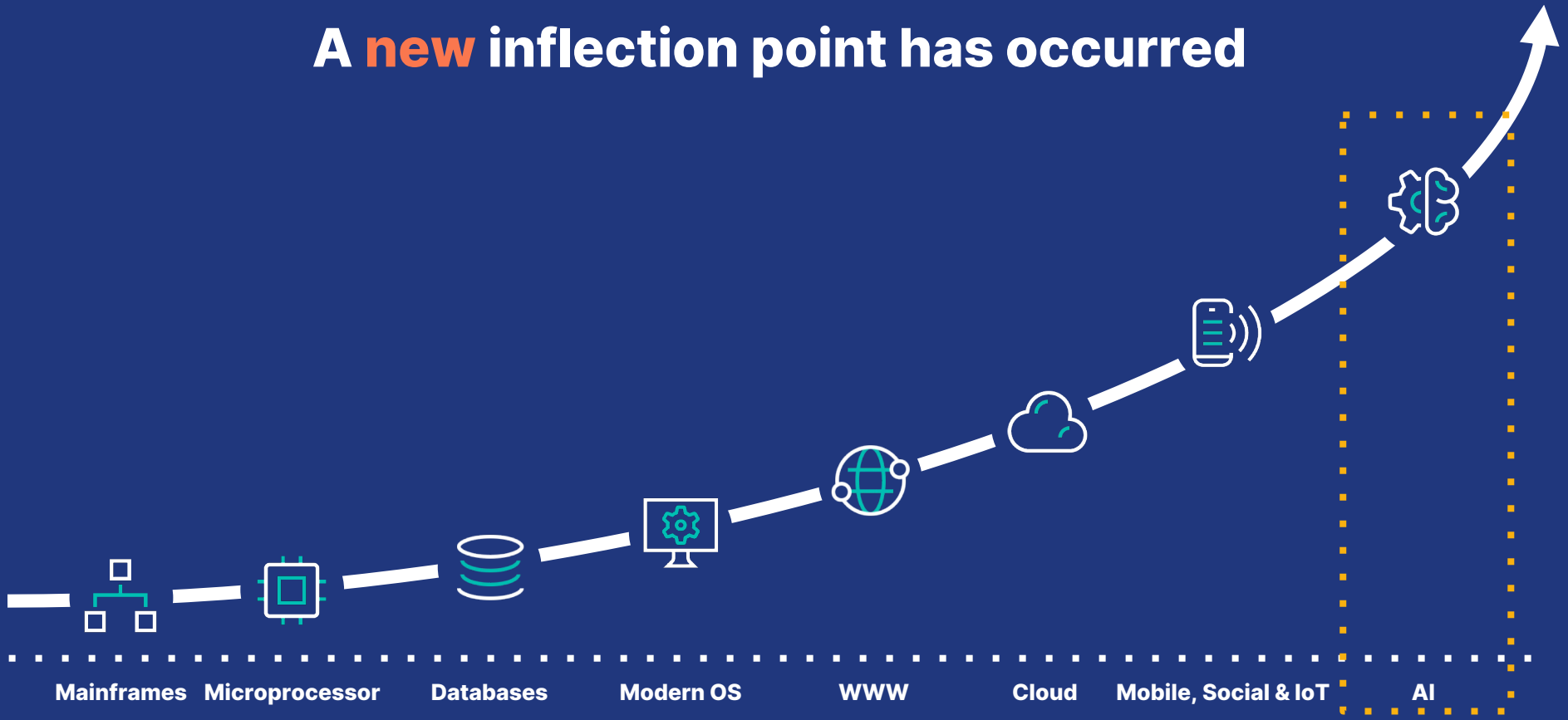
92%

of SOCs agree automation is needed to drive consistency and handle alert volumes

* IDC, Cloud Security Survey: Top Identity and Data Access Risks
** Salesforce.com, IT Integration Challenges for Digital Transformation Report
*** Security Boulevard, Too Many Security Tools Can Be as Bad as Too Few
**** SANS Institute, Common and Best Practices for Security Operations Centers

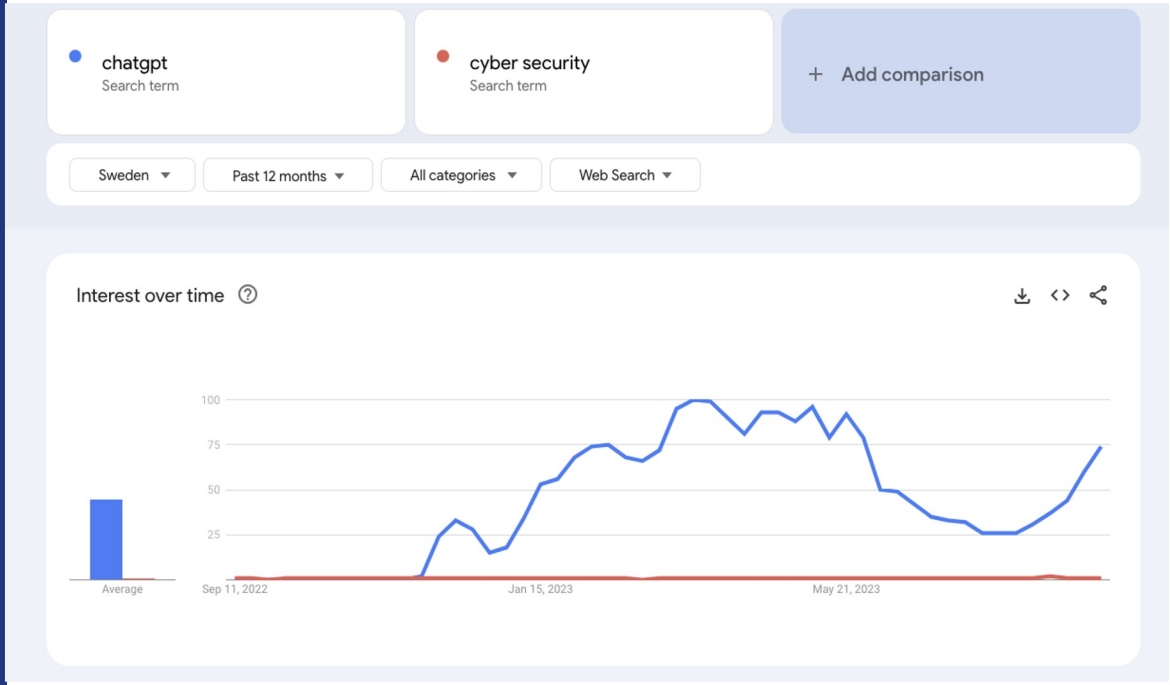
elastic

A new inflection point has occurred



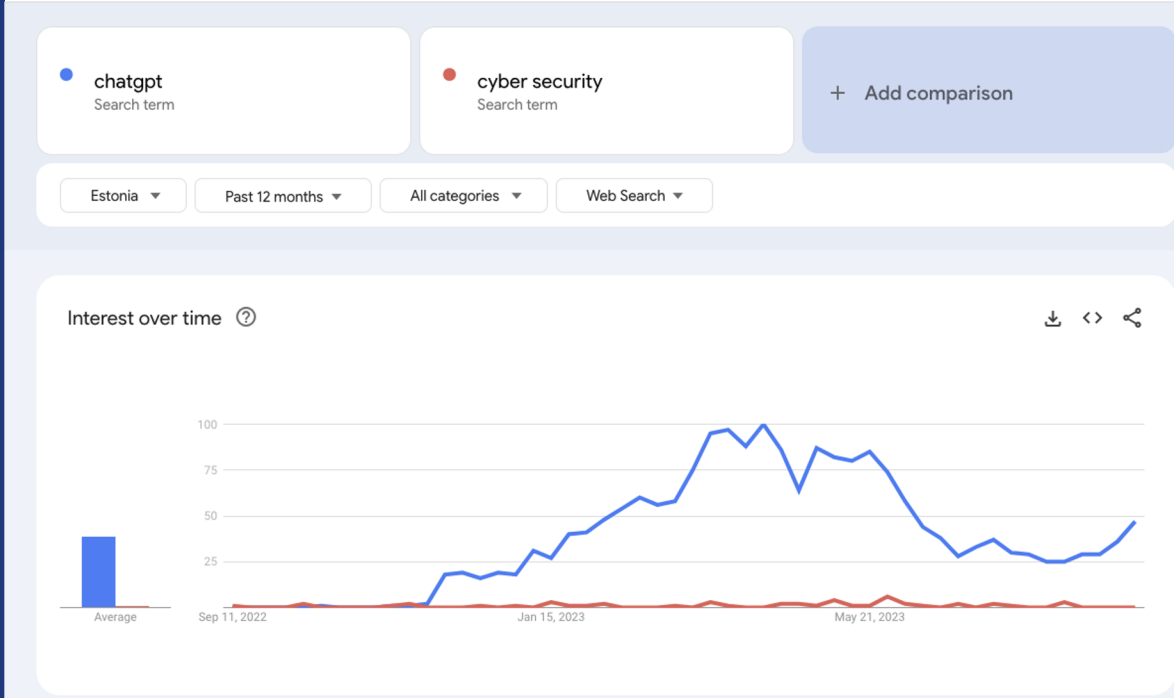
elastic

Interest in AI tools such as ChatGPT (Sweden)



elastic

Interest in AI tools such as ChatGPT (Estonia)



elastic

How can security teams make use of this technology?

What outcomes do we care about?

speed, scale, relevance

Shorter dwell times, minimal damage

Faster remediation of complex threats

Accelerated investigation and response

elastic

Opportunities to augment Security

context, bandwidth, knowledge

Gather context

Quickly decide on the right course of action

Force multiplier

To help analysts do more with their time

Enable new talent

By reducing the barrier to entry and help keep staff on top of novel threats

elastic

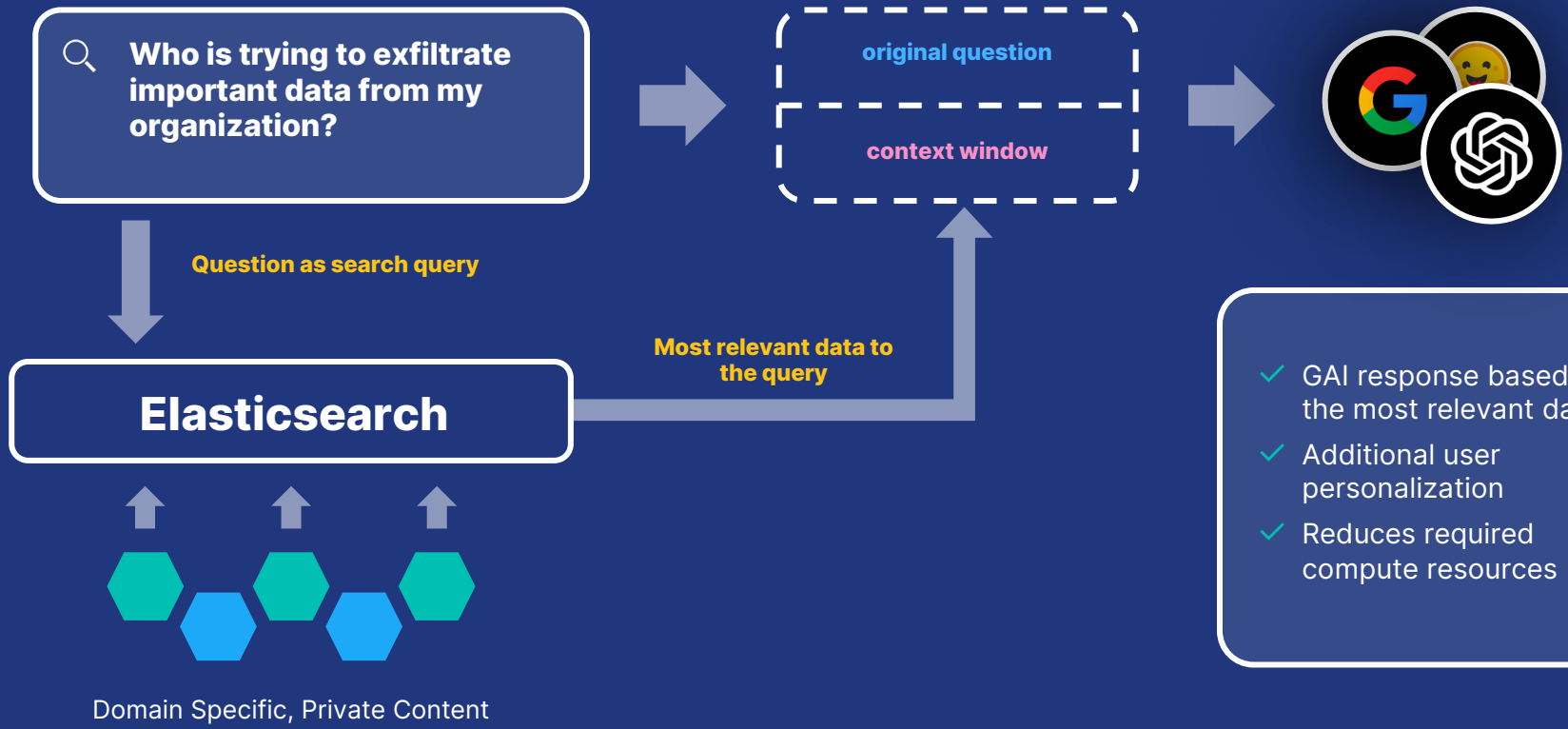
Elastic provides the bridge between private data and GenAI

Sensitive databases
Multi-system / cloud information
Private knowledge bases
Case histories

Visit our booth to see how Elastic does this!

elastic

Elastic + Generative AI increases relevance and scalability at a lower cost



Key takeaways

- Cybercrime still increasing
- New threats are always coming
- Security must be part of business strategy
- Adopt a change mindset for success
- Plan for endemic talent shortages

elastic

“The pace of change has never been this fast.

It will never be this slow again.”

- Justin Trudeau

Visit our booth or even better…..
Join our Happy Hour too!

CybExer Technologies
Toompuiestee 35 · Tallinn

Friday, Sep 15 @ 2 -4 PM EEST

RSVP: https://ela.st/tallinn-happy-hour

elastic

Thank You!!

elastic