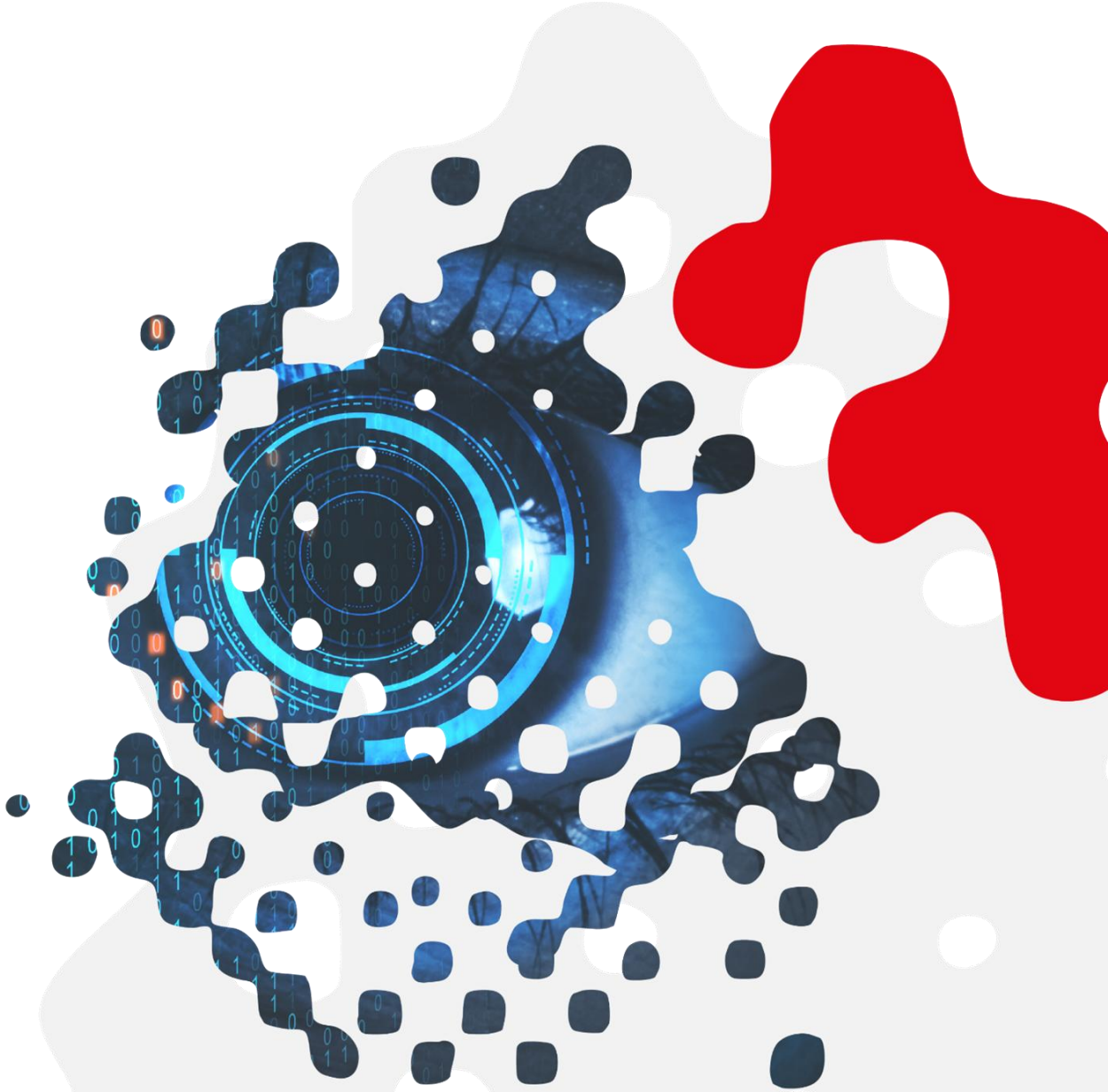
NetEye Conference DACH 2026

“Mehr als SIEM: **Security Intelligence und IT Observability mit Elastic und NetEye”**

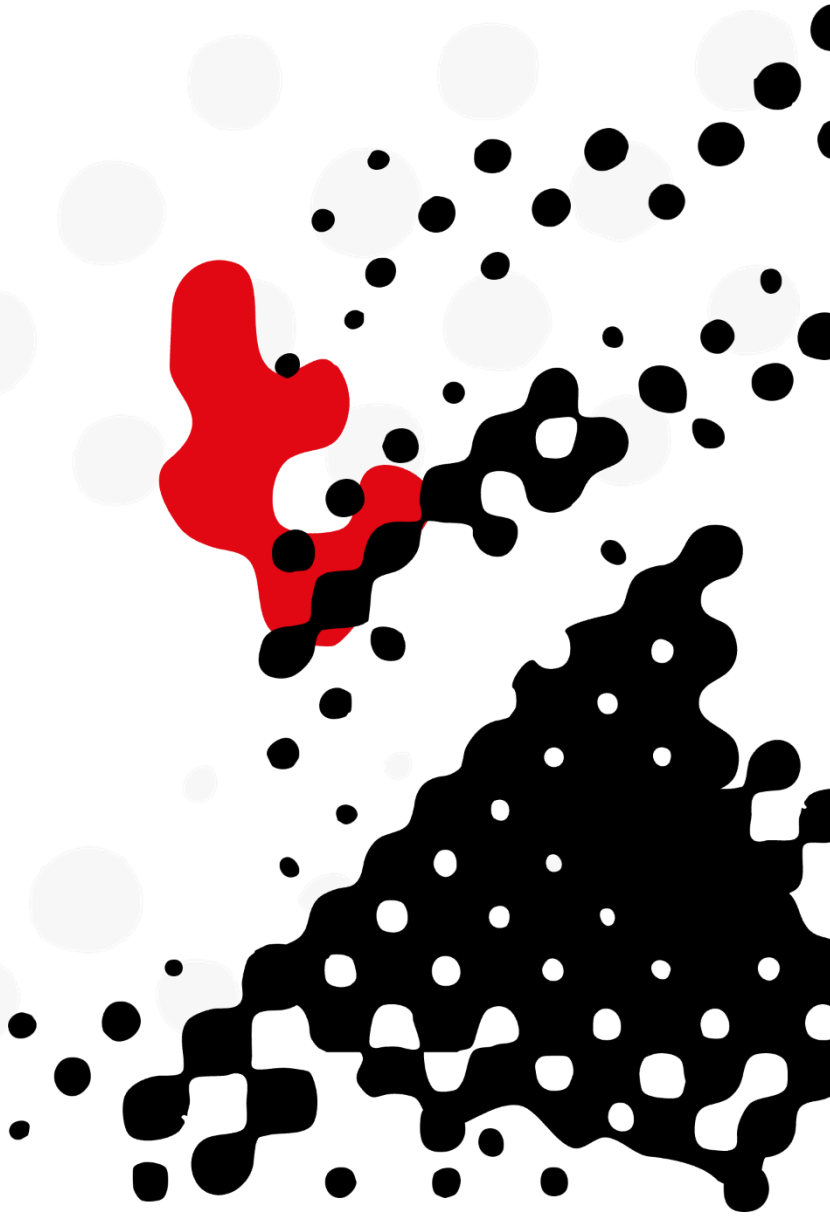


Markus Breuer
Security Specialist, DACH @ Elastic

NetEye Conference DACH 2026 | WÜRTH IT | GRAVITATE

Agenda

- **The evolving threat landscape:** how AI is accelerating attacks
- **Beyond SIEM:** the path to an AI-native security operations platform
- **Live demo & case study:** observability and security in manufacturing



The world has changed.

Nation-state capabilities are now commoditized. AI has collapsed the cost of attack. Breakout times are measured in seconds, not hours.



elastic











Month 2026	Ø Cyberattacks p. Enterprise/Week (GER)	Growth vs. previous CY
January	1.314	+16 %
February …	1.345	+11 %
July	1.723	+40 %
August	1.834	+53 %





Zego (Produktionsstopp / Insolvenzantrag, Anfang 2026): Nach einem schweren Cyberangriff kam es zu einem fast sechswöchigen Produktionsstopp, der letztlich in einen Insolvenzantrag mündete. Security-Insider

NetEye Conference DACH 2026

WÜRTH | IT

GRAVITATE

elastic

Who is Elastic?

ELASTIC AT A GLANCE

Founded
in 2012

4,200+
employees

42
countries with employees

1500+
Partners globally

Head Quarter
Amsterdam, Netherlands

25,200+
subscription customers

54%
of Fortune 500 companies trust Elastic

450+
Turnkey integrations

DOWNLOADS

5.2 Billion

CERTIFICATIONS

Compliance Standards

PCI DSS
FedRAMP
CSA Star
ISO/IEC 27001
ISO/IEC 27017
ISO/IEC 27018
ISAE 3000
SOC 2
SOC 3
TISAX
HIPAA
Cyber Essentials Plus
IRAP
CyberGRX
https://www.elastic.co/de/trust

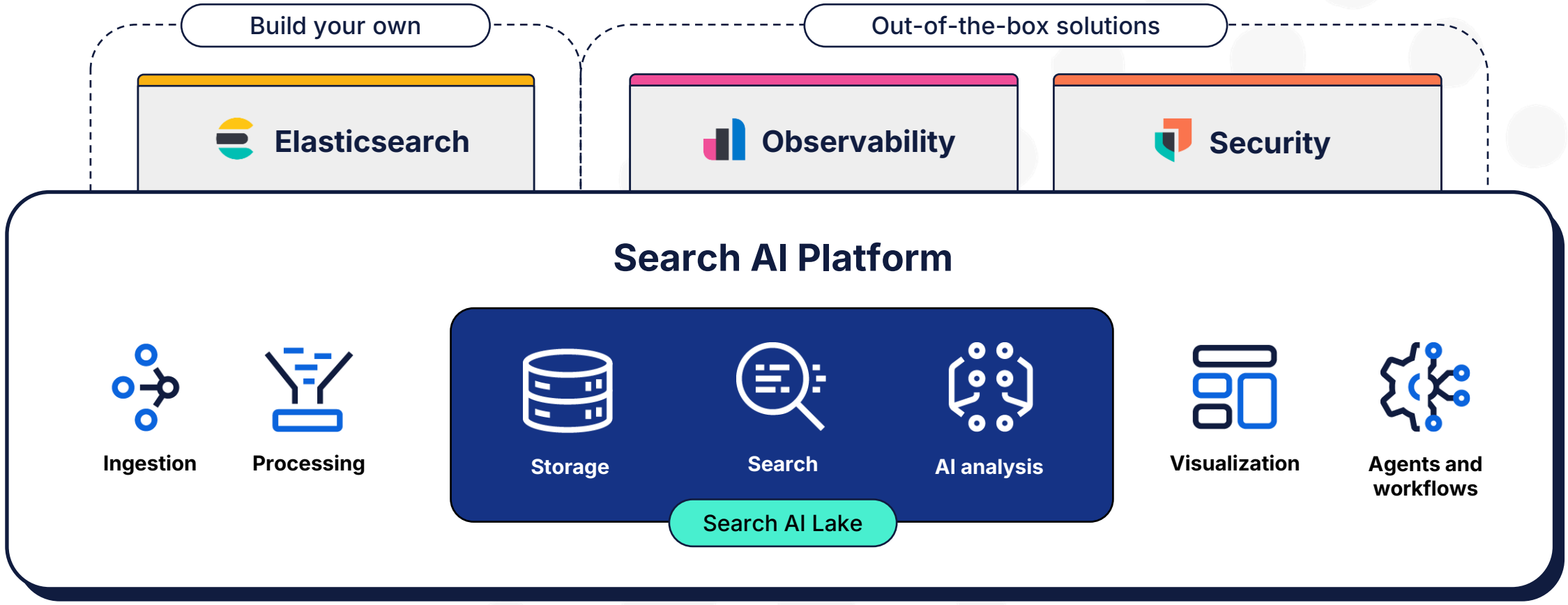
https://www.elastic.co/about

FINANCIALS

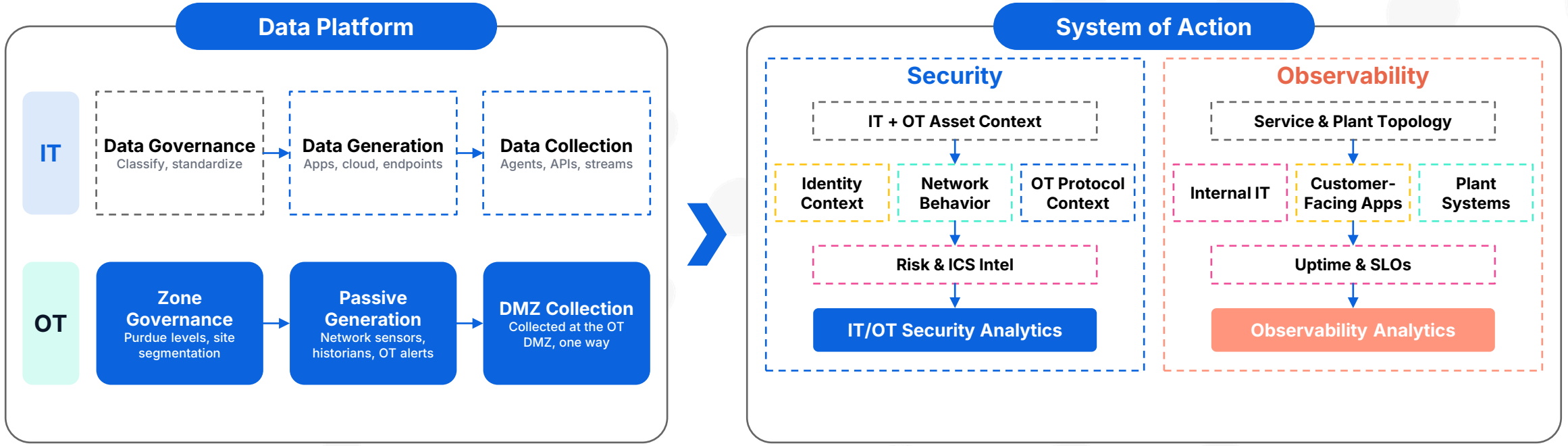
FY2025 Highlights

$1.483B	$688M	1,510+	~112%
Total Revenue	Elastic Cloud Revenue	$100K ACV customers	Net Expansion Rate

One **platform**, two out-of-the-box **solutions**, the freedom to **build anything**



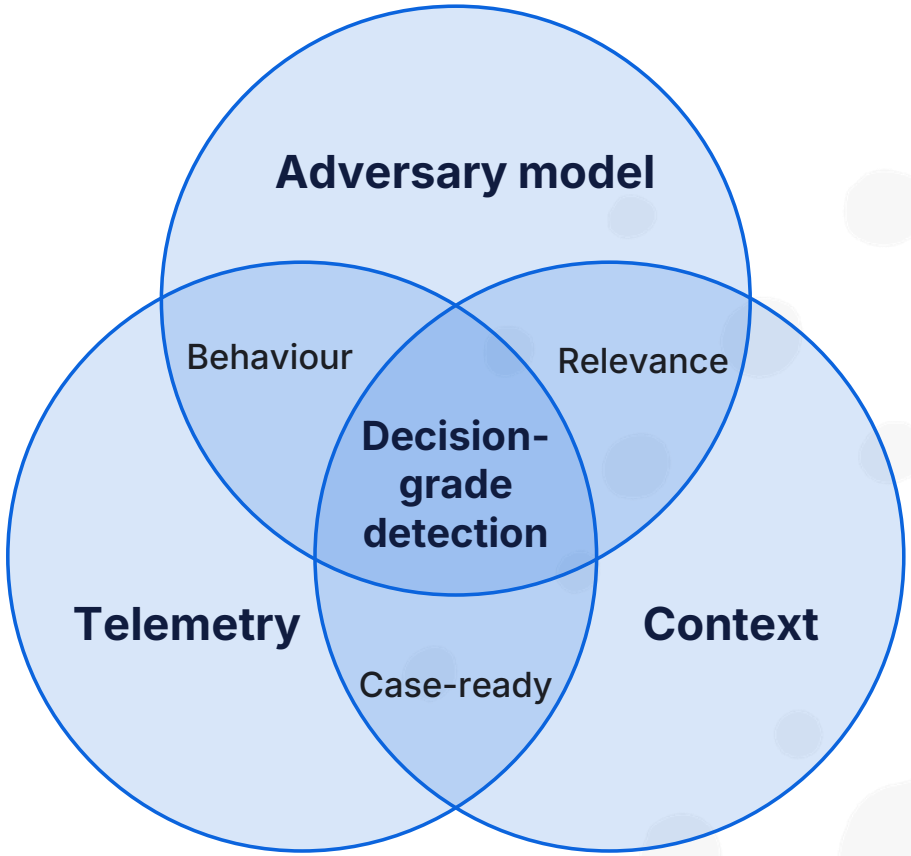
The “platformization” of IT and OT is bringing observability and security analytics together



Data Governance	Data Pipeline	Data Storage	Analytics	Response
Classify. Standardize	Enrich. Route. Transform	Hot. Warm. Cold. Frozen	Search. Investigate. Report	Detect. Respond. Automate

The path to increased analyst productivity and reduced risk

Adopting AI in the SOC means giving analysts decision-grade detection against sophisticated attacks



Telemetry

- Endpoint agents
- Network data
- Existing SIEM sources
- OT monitoring data

Adversary model

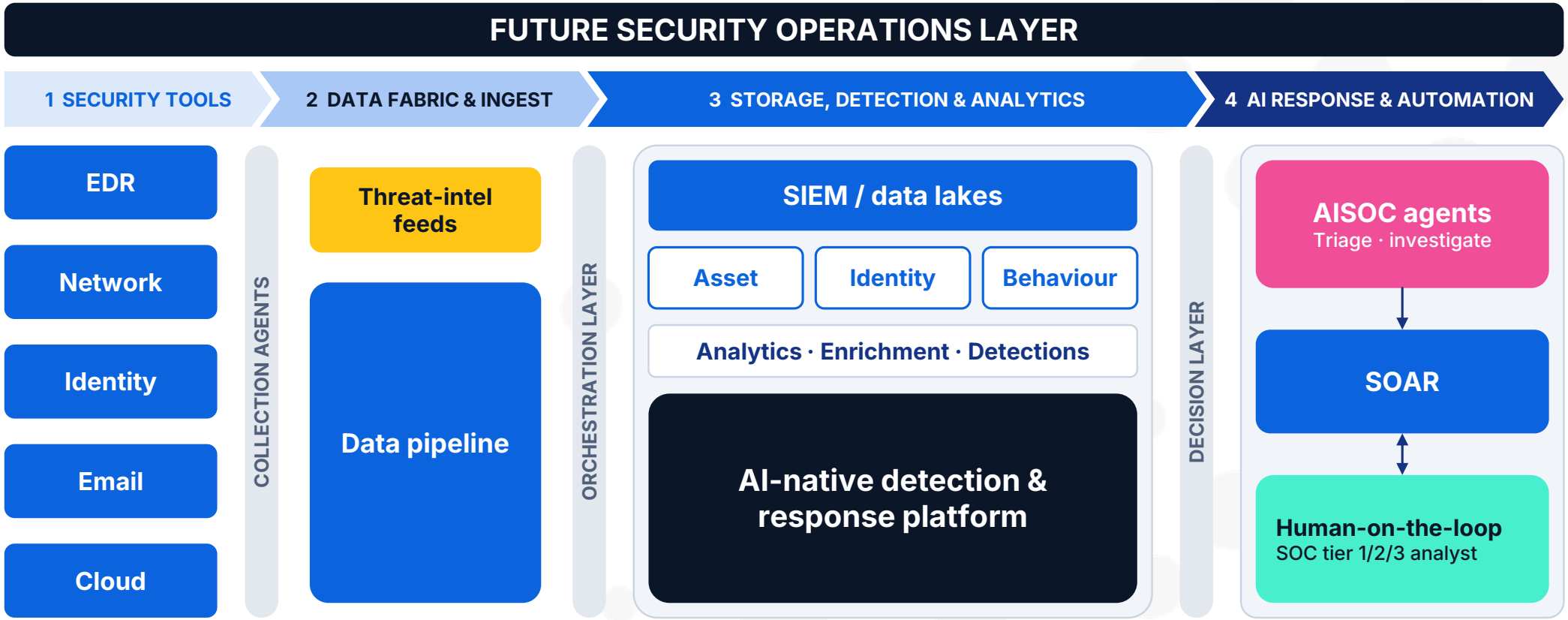
- ATT&CK-mapped rules
- Behavioural detections
- Detection-as-code
- OT attack techniques

Context

- AI-assisted triage
- Asset criticality
- Threat intel feeds
- Case history

Evolution of security analytics

A hypothetical, AI-native security operations architecture



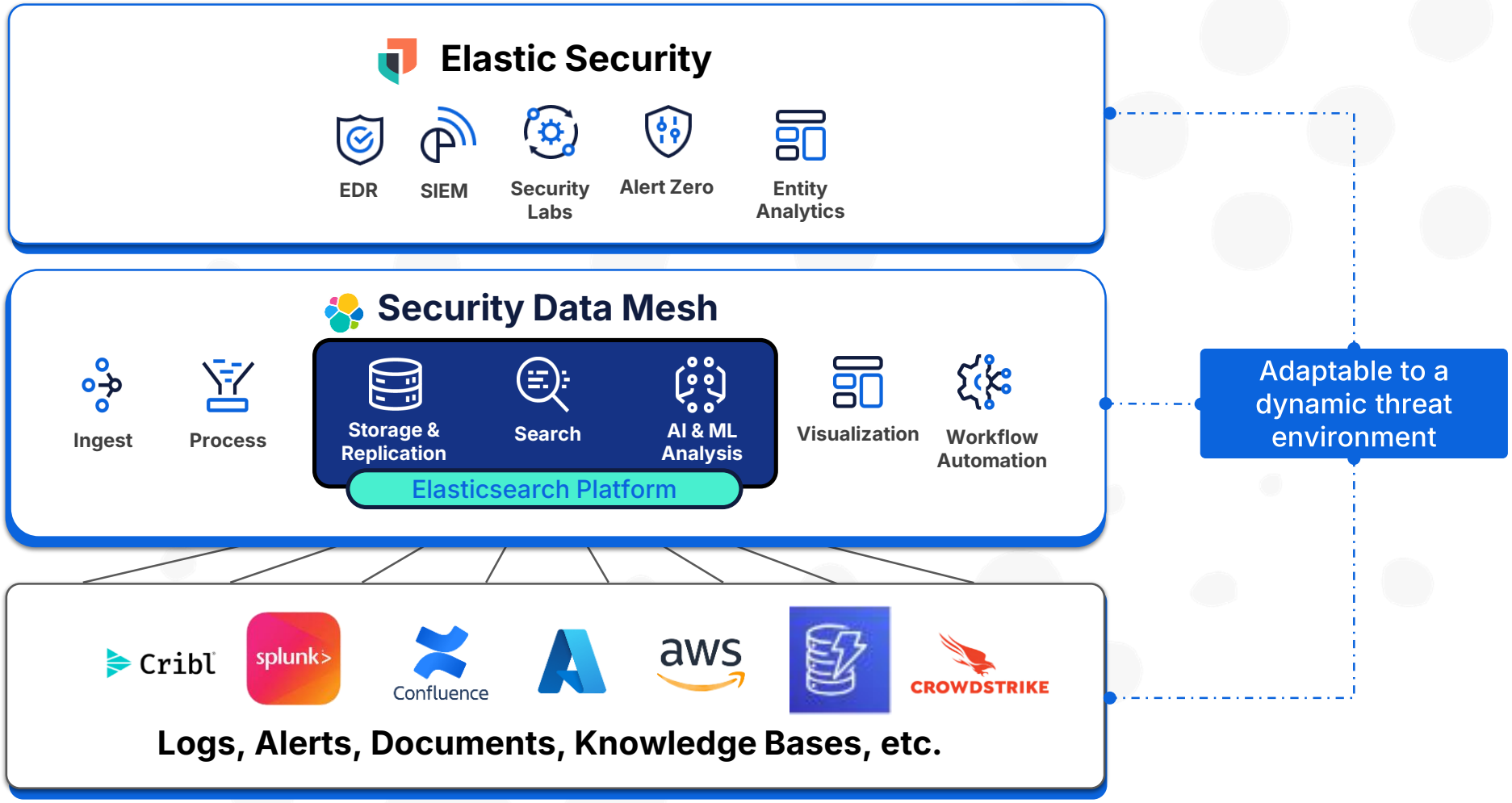
Elastic's own TDIR team is 10 people, protecting ~4,000 employees across 35 countries against ~250 TB of security data a day.

Elastic will improve SOC analyst experiences & reduce security risk

Integrates...
The AI SOC

Starts with...
The platform

Built on...
Your Structured & Unstructured Data



DEMO

Live demo: how Elastic uses AI to distill millions of events a day into a handful of context-rich SOC cases - from ingestion through automated triage to response, working alongside NetEye.



SIEMENS

Manufacturing | Germany

~170

SOC cases distilled from 6 billion events a day

~5,000 hrs

of analyst time reclaimed every year

> **We have effectively given our team 5,000 hours back every year, time we now invest in staying ahead of adversaries rather than catching up with logs.**
>
> Ricardo Oliveira, Head Engineering Protection and Automation Solutions, Siemens

The challenge

- ~2.5–3 people a year lost to running data-centre infrastructure
- New detection rules queued in a 3–4 week backlog
- Factory team found problems only after users did

With Elastic

- 6 billion events a day correlated into ~170 SOC cases across 300,000+ endpoints
- Detection rules ship in under a week
- Machine learning flags behavioural deviations and cuts false positives
- Amberg factory team now spots issues before users do

Thank you.

From SIEM to an AI-native security and observability platform, with Elastic and NetEye.

Markus Breuer | Security Specialist, Elastic DACH |
elastic.co/security

NetEye

