



Elastic Security, an overview

Customer Zero: Elastic's InfoSec organisation

Thorben Jändling



Search. Observe. Protect.

Thorben Jändling

Principal Solutions Architect

in the

Global Security Specialist Group

@ Elastic.co



eMail

thorbenj@elastic.co



slack







@thorbenj on **elasticstack.slack.com**
(Public community slack)



Career as a Security Engineer for various national CSIRTs
<https://www.linkedin.com/in/thorbenj/>



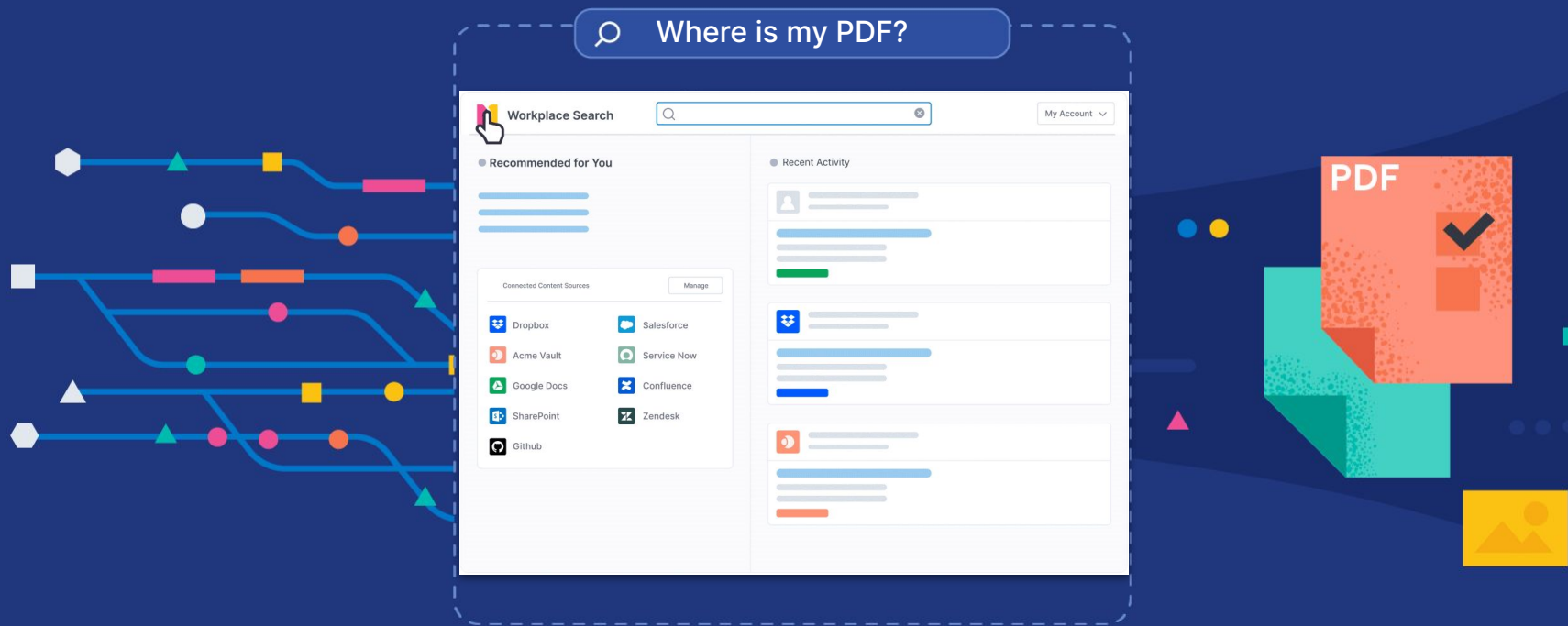
Agenda

-  A brief introduction to what Elastic does
-  An overview of the success customer zero is having
-  Elastic Security demo tour
-  How all this percolates into our offerings
-  Wrap up & where to find more information
-  Thank you

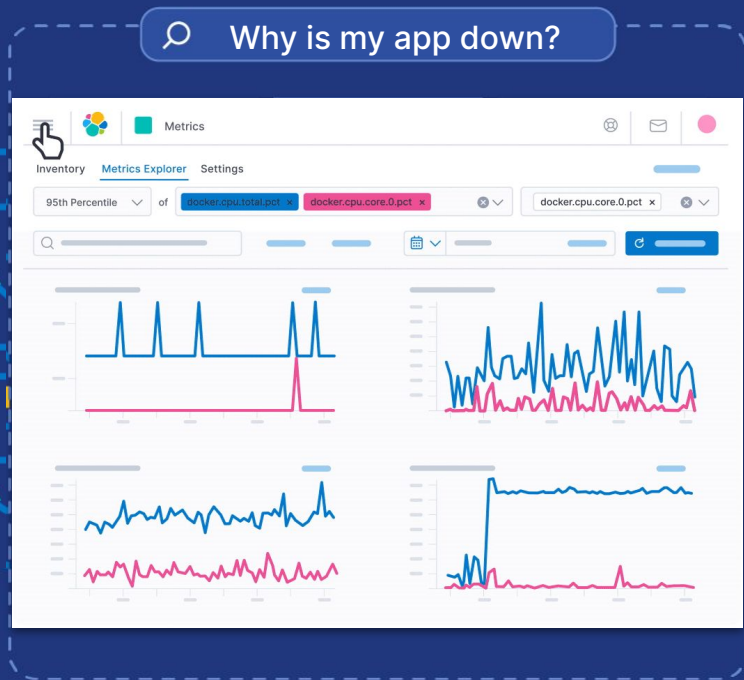
SEARCH. SOLVE. SUCCEED.

In this always on world

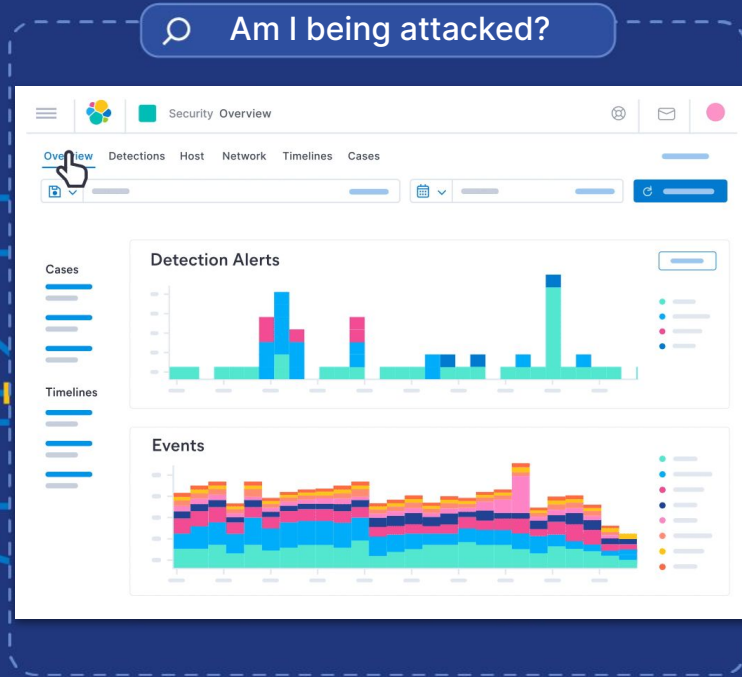
The best platform for Enterprise Search



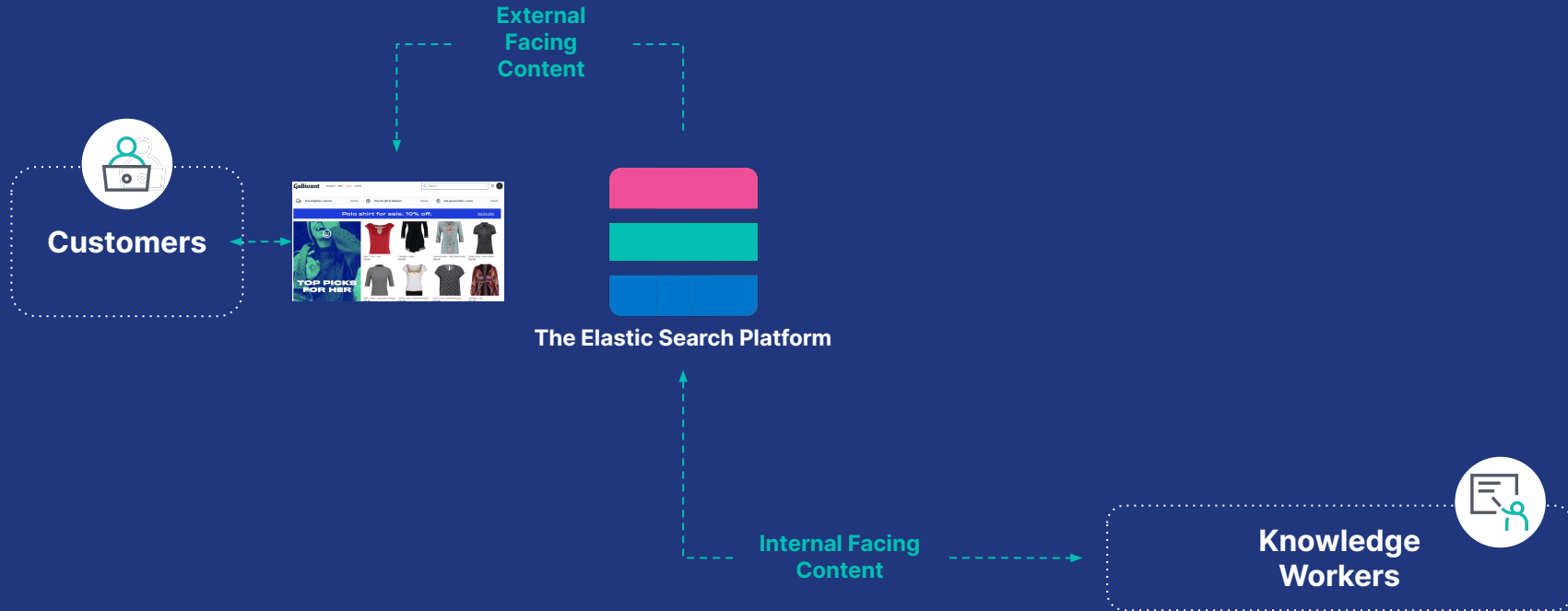
The best platform for Observability



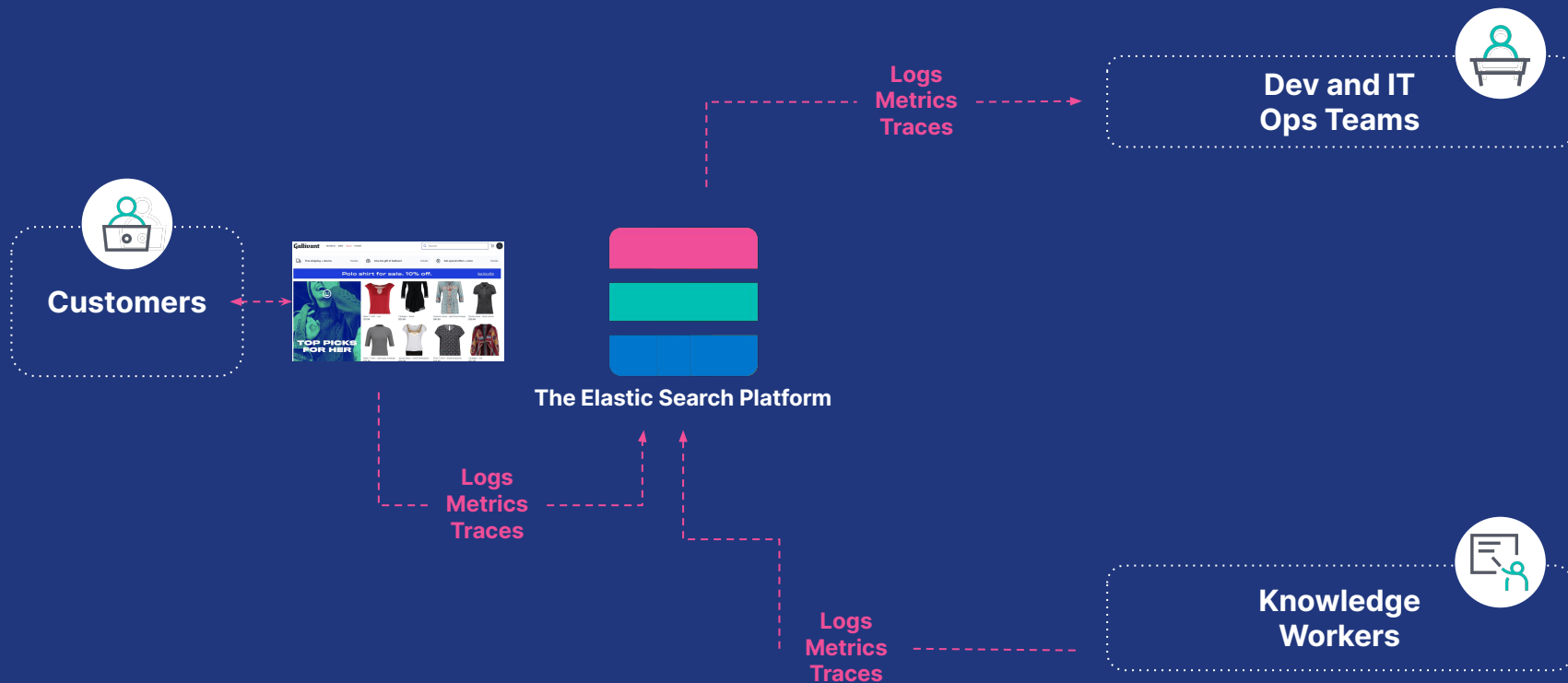
The best platform for Security



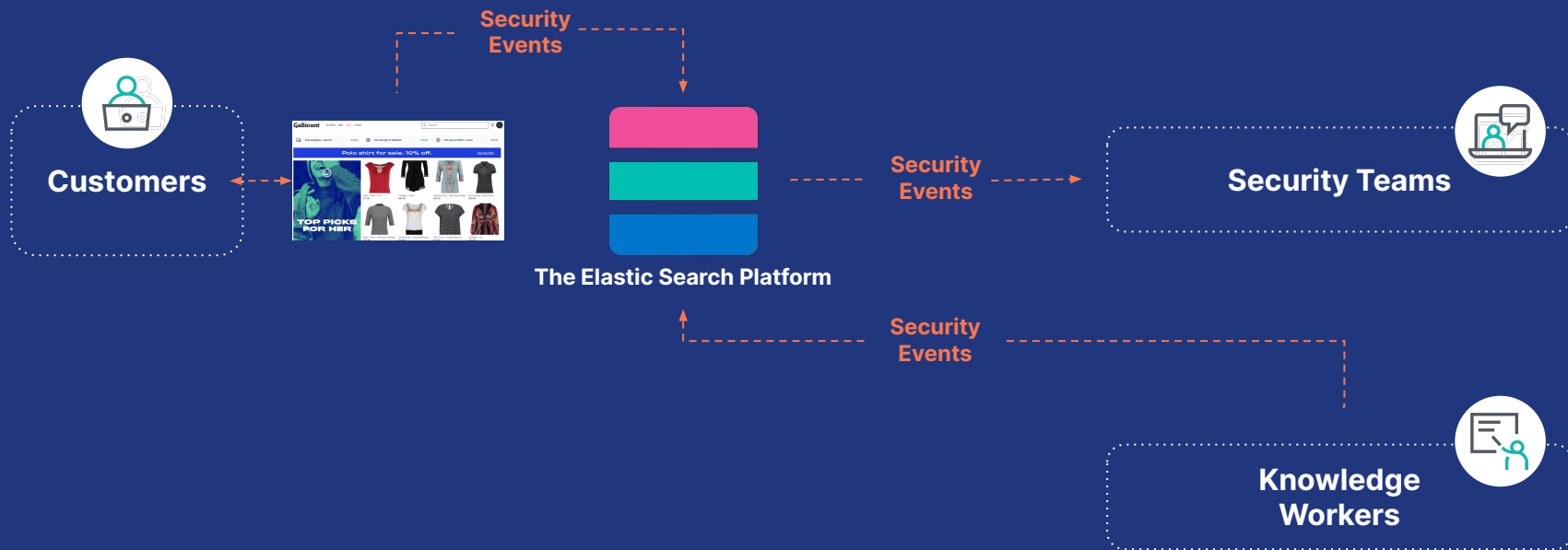
A platform for Enterprise Search



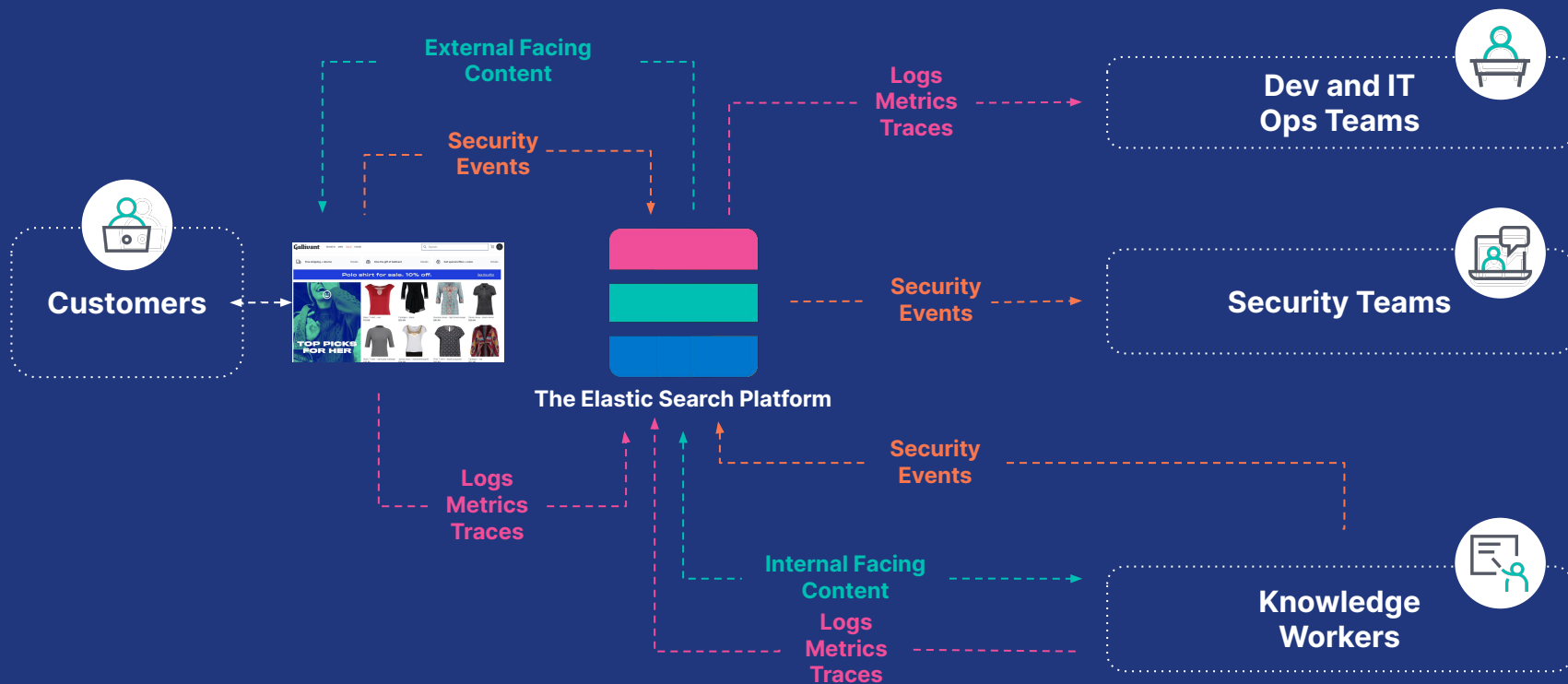
A platform for Observability



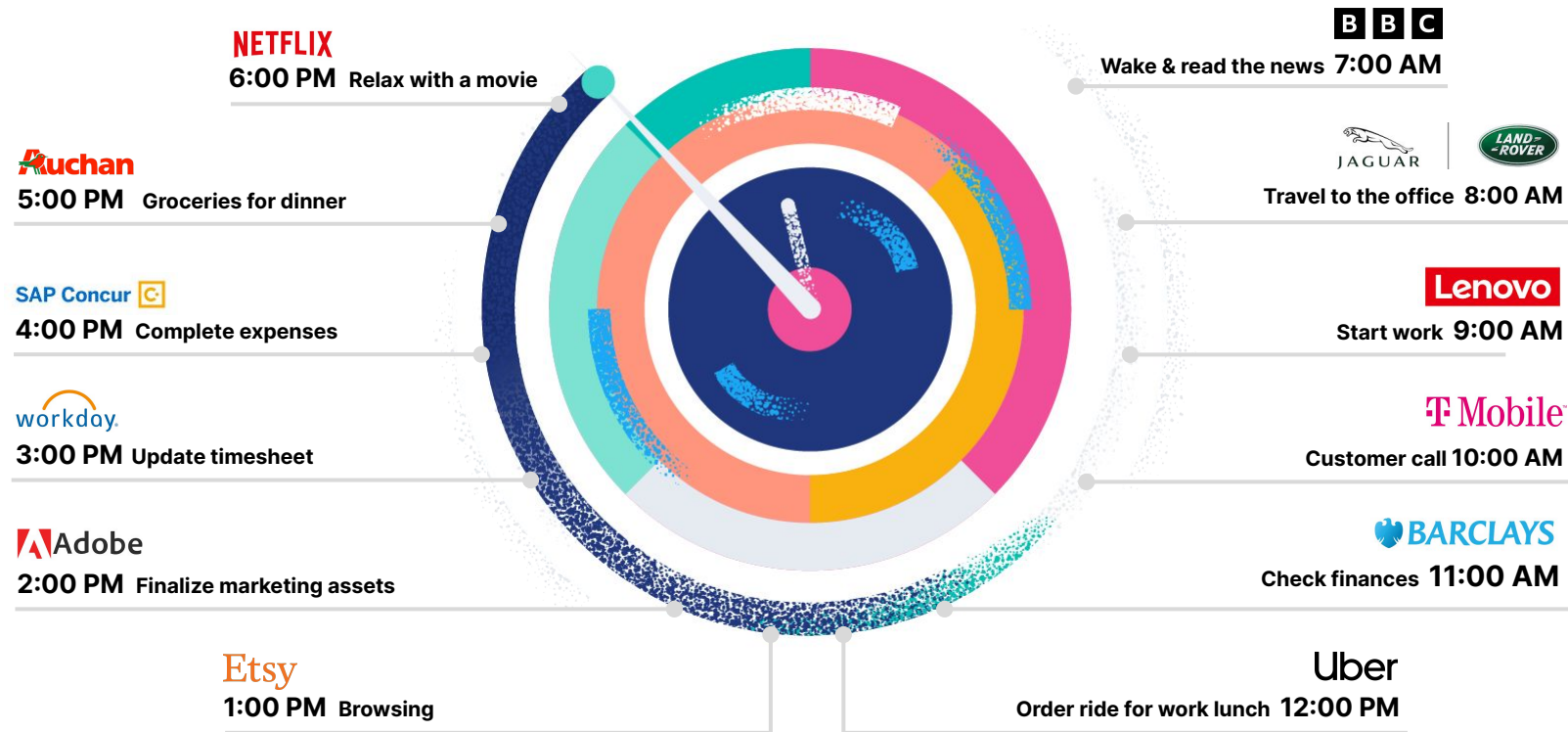
A platform for **Security**



A platform for all your needs



Follow the Sun with Elastic in EMEA

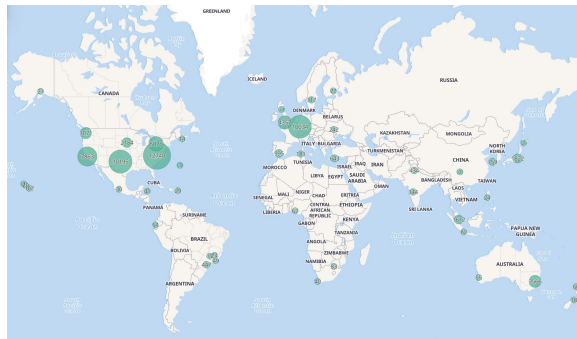


Our InfoSec team

Elastic InfoSec Challenges:

1) Company itself

Globally Distributed Workforce



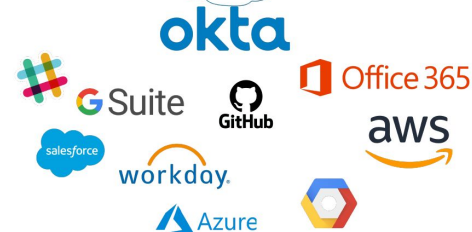
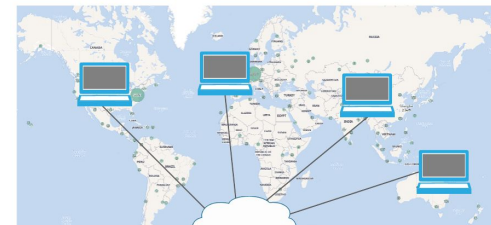
~3,000

ELASTICIANS

42

COUNTRIES

Cloud Native Implementation



InfoSec by the numbers (Daily)

150TB

Security Data

¹⁴ Enables us to monitor for abnormal and security relevant activity

600GB

Endpoint Data

Amount of security data ingested daily from Elastic end user endpoints

>450K

Endpoints

Globally dispersed cloud instances, virtual desktop environments, and user workstations



Elastic InfoSec Challenges:

2) Elastic's customers



60

Cloud
regions



25'000+

Machines



60'000+

Clusters



~600'000

Containers



~20'000

Customer
subscriptions

InfoSec Fundamental Use Cases



**Governance/
Compliance**



**Risk
Management**



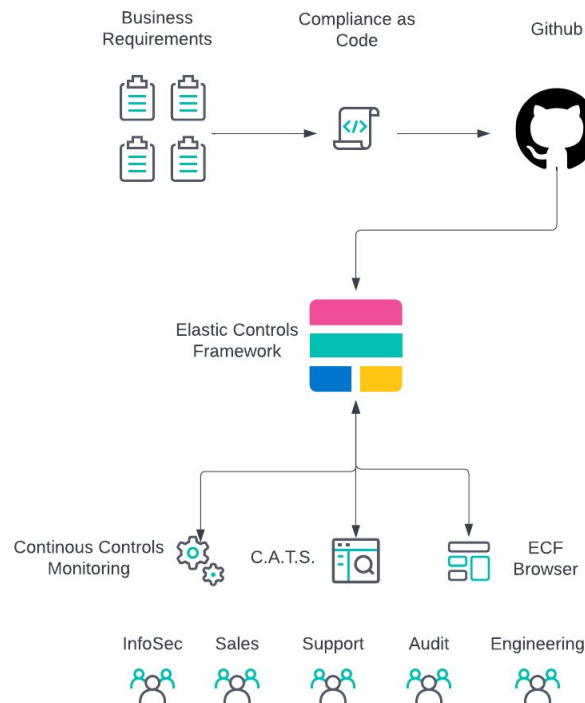
**Vulnerability
Management**



**Threat
Management**

Elastic Controls Framework

- Consolidates all compliance frameworks into a single source
- Enables multiple integrations points across the enterprise



Name _____

Please enter yo

Background

Describe the re

Asset(s) at risk

Which equipment

Threat Communi

Who is the thre

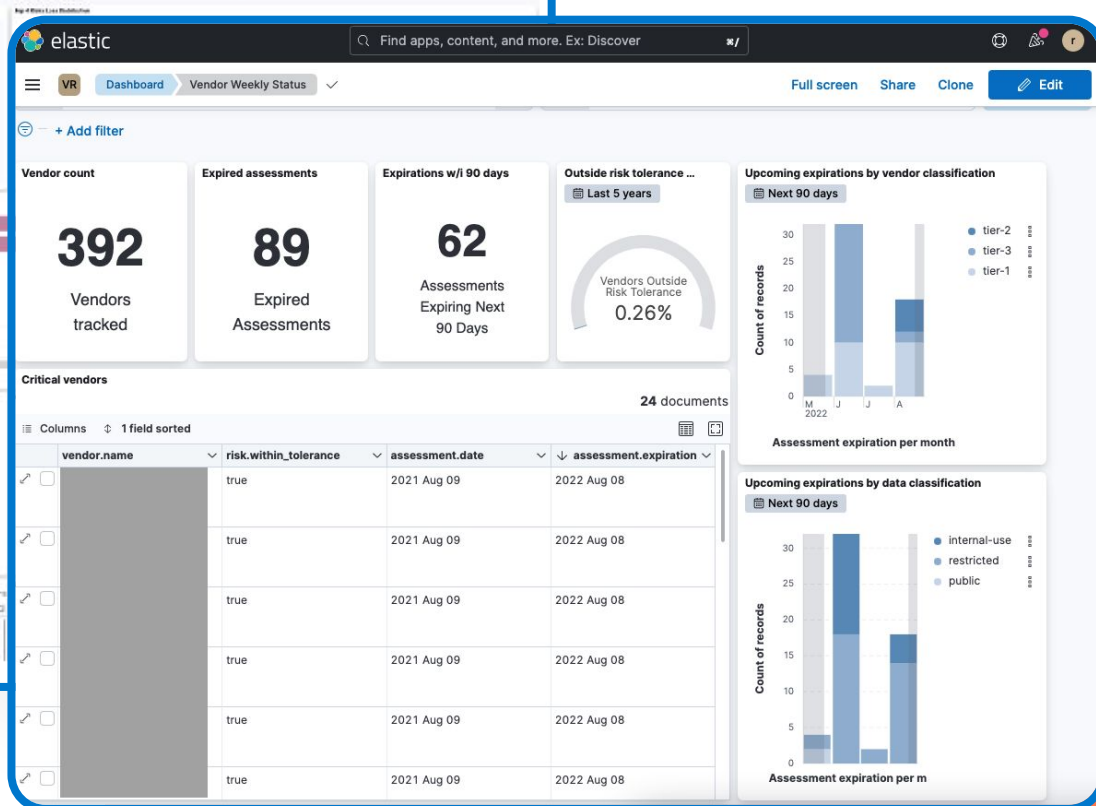
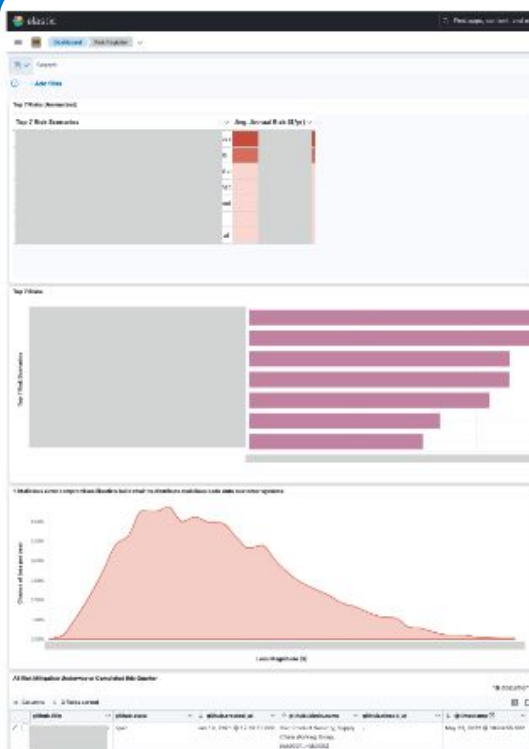
Contacts

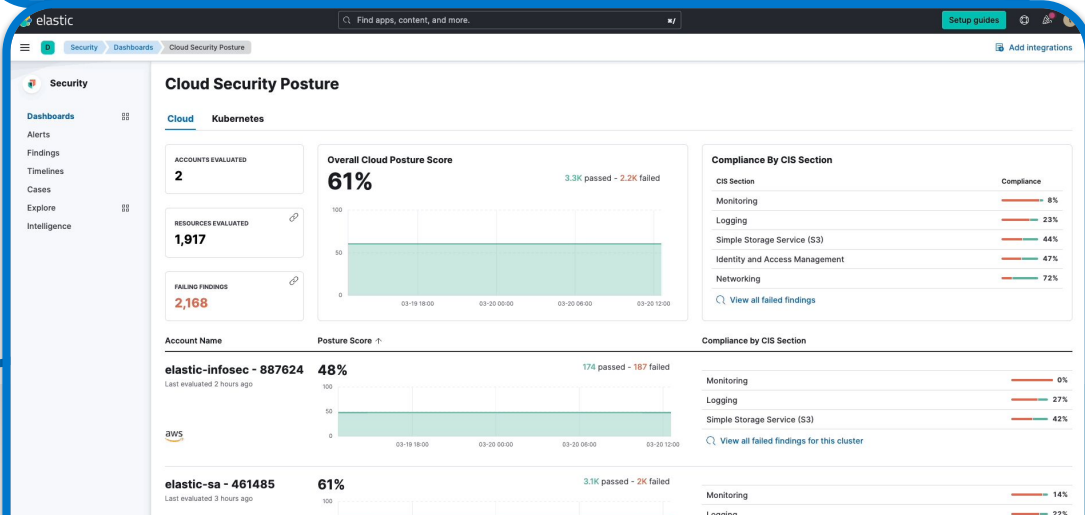
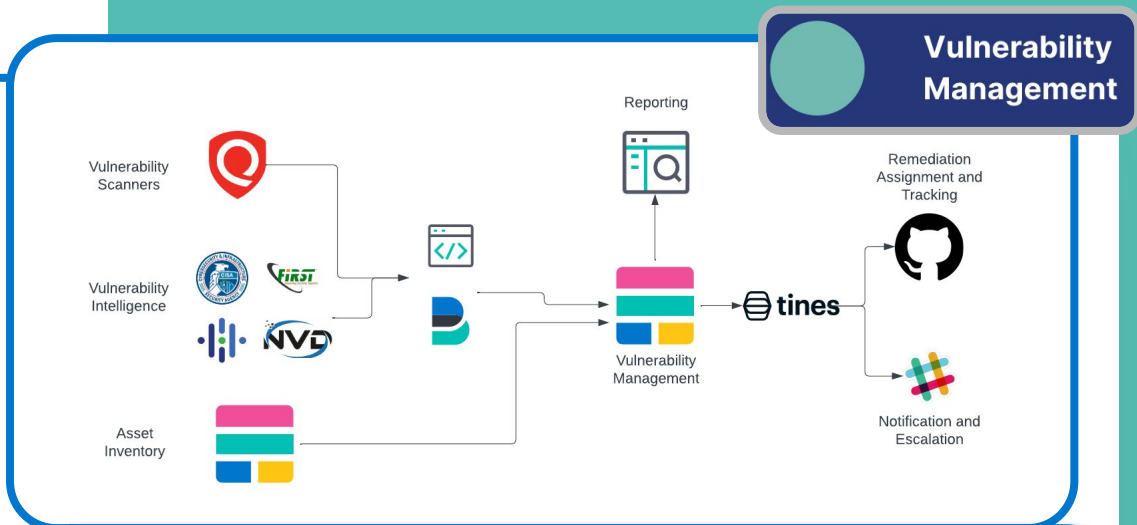
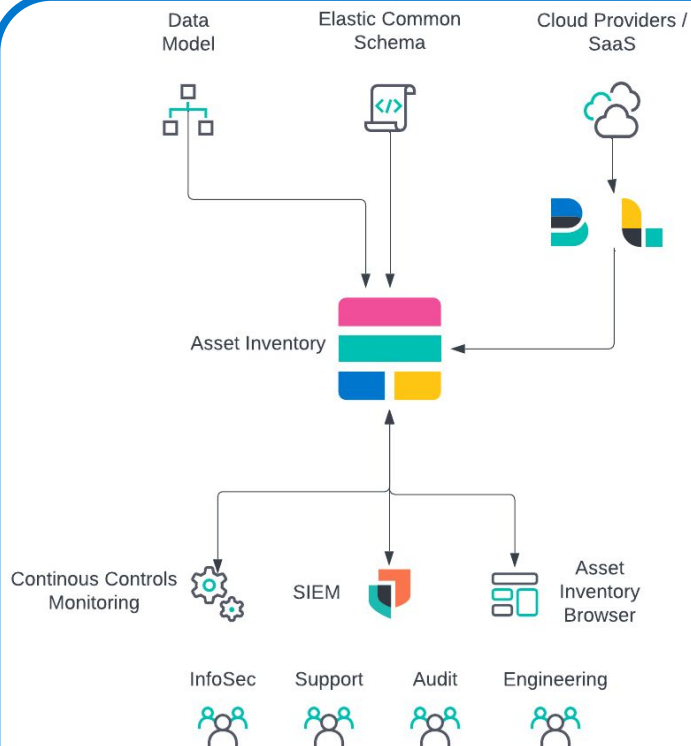
Provide any rel

Subject / Purpos

'Determine the

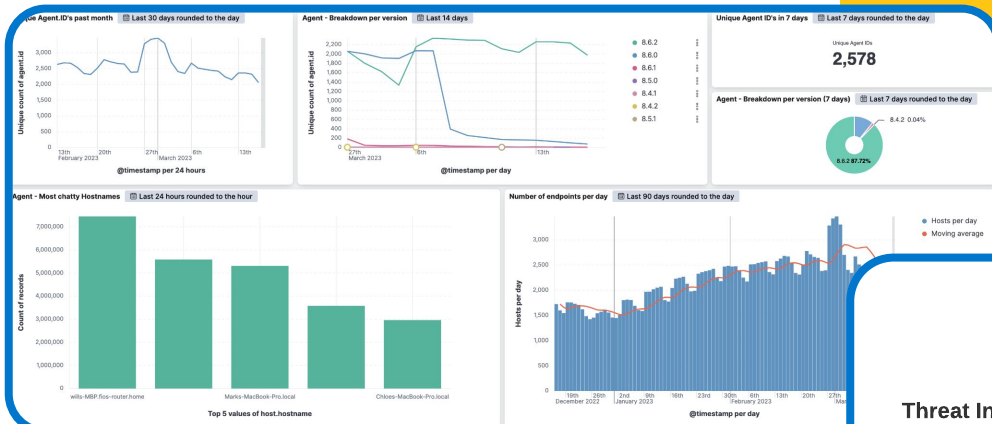
Submit







Threat Management



Additional Information

Thank you for confirming this event.

To assist the Information Security team with detection tuning, please provide any additional details you believe may be relevant to this alert being triggered.

Details

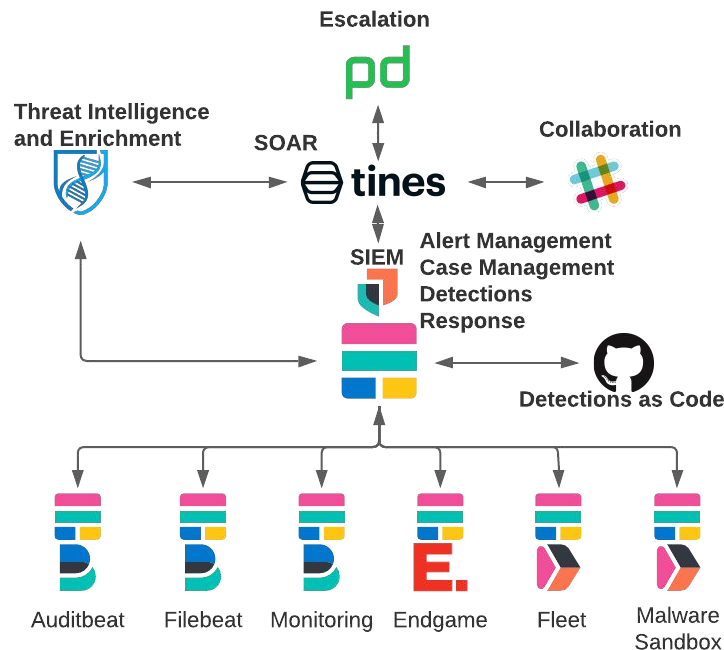
I added my new phone to Okta for MFA

Follow-Up

- ☐ I would like Information Security to contact me regarding this event.
- ☒ No need to contact me, this should clear it up.

Close

Submit



ON-DEMAND WEBINAR

Creating a Security Center of Excellence With Elastic



sitecore[®]
Own the experience[®]

Hosted by:



Adam Button
Director of Cyber Security
Sitecore

Overview

Hear how Sitecore uses Elastic SIEM for their new 'Security Operations Center as a Service' offering (SOCaaS), which has allowed the company to automate more than 91% of their workflows, increasing productivity in security and compliance, which has reduced time-to-fix issues with minimal human capital.



[https://
ela.st/23-sitecore](https://ela.st/23-sitecore)



SITECORE[®]

Sitecore Optimizes Experiences for their Customers with Elastic

"Elastic ECE significantly reduces the burden on our Platform team, saving time and reducing costs"

Tim Van Gehuchten, Vice President of Platform Engineering

PROFILE

About: Founded in 2001, this award winning digital experience innovator powers the online presence of many global household brand website.

Industry: Software and Technology

Location: Benelux, USA, Global

GOALS

- To reduce complexities for customers dealing with content
- Empower their customers to respond to fast changing business conditions
- Make findability a simple task

SOLUTIONS

- Identify bottlenecks with **Elastic Observability APM** to improve their customer service
- Protect marketing content with **Elastic Security**
- Built an internal PaaS offering based on Microsoft Azure and **Elastic ECE**

RESULTS

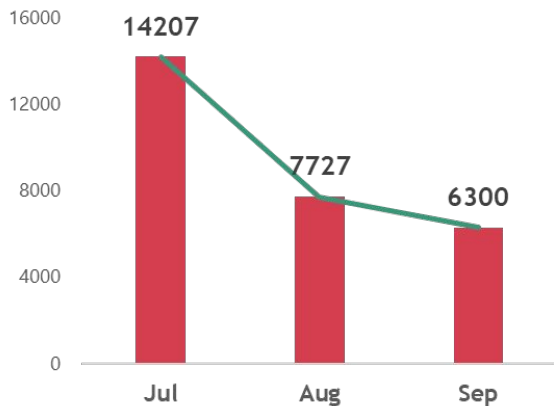
- Clients can accelerate their campaign execution.
- Providing a 360-degree view of all content to their customers some with 10 million content items
- Reduced infrastructure maintenance burden on the Sitecore platform

SOC Operations - Facts

OUR SOC OFFICE



INCIDENT TREND (2022)



ERROR RATE

9%

AVG. TIME TO RESOLVE

12min

AUTOMATION RATE

96%

[https://
ela.st/23-sitecore](https://ela.st/23-sitecore)

Booking.com

CUSTOMER SUCCESS STORY

**How Booking.com is
tackling unparalleled
growth, complexity, and
scale with Elastic**



<https://ela.st/23-booking>

(<https://www.elastic.co/videos/how-booking-com-is-tackling-unparalleled-growth-complexity-and-scale-with-elastic>)

Life as a CISO

Dealing with vendors

**Your cool features are not
business outcomes**

**Assuring me your product
can solve all my problems**



**Telling me what problems I
have**

**Pushing for a large
purchase / deployment**

Scaling with confidence

Improving time to value for security teams

87.5%
Improvement

24 Months

3

Products

3 tools, 3
licences

22

SOC Analysts

Level 1 & 2 / 24x7

5TB

Daily Ingest

30 data sources

50K

Events per second

Daily bursts to 100K

3 Months

1

Products

1 tool, 1 licence

4

SOC Analysts

Distributed / 24x7

32TB

Daily Ingest

23 data sources

350K

Events per second

Minimal bursting

Elastic Security tour

Demo

Bring your data

Detect, Investigate & Respond

cloud



network



host



user



email



threat intel



Native protection

Block threats with **Elastic Agent**

laptops & desktops



servers & VM's



containers & kubernetes



cloud providers



Elastic Security

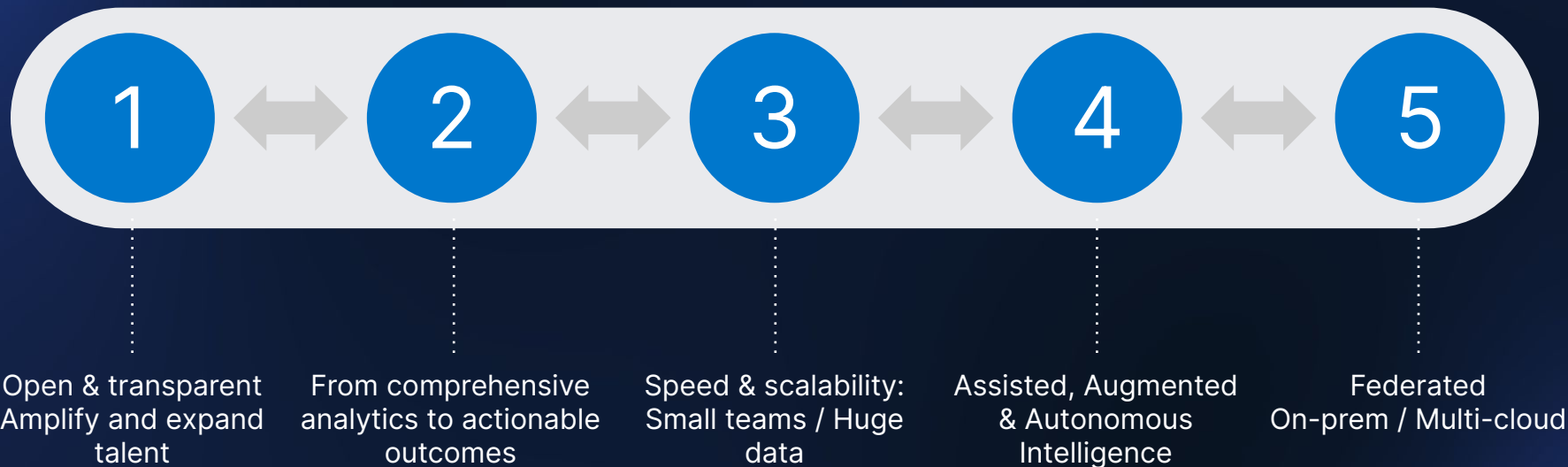
SIEM & Security
Analytics

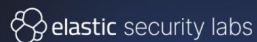
Endpoint Security

Cloud Security

Powered by Elastic Security Labs - Threat Research

Security Operations for the Modern Enterprise





2023 Elastic Global Threat Report - Spring

Elastic publishes 2023 Global Threat Report Spring Edition

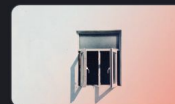
This week, we're publishing a new version of this report that's online and interactive, which includes additional data covering the remainder of 2022, written using Elastic technologies.

By Devon Kerr
24 April 2023

Featured

Elastic Security Labs discovers the LOBSHOT malware

By Daniel Stepanic
25 April 2023



Elastic Global Threat Report Multipart Series Overview

By Devon Kerr
17 April 2023



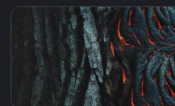
Attack chain leads to XWORM and AGENTTESLA

By Salim Bitam
07 April 2023



Elastic users protected from SUDDENICON's supply chain attack

By Daniel Stepanic, Remco Sprooten
30 March 2023



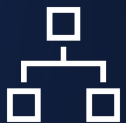
Elastic Security Labs

Elastic Security

Prevent → Investigate → Respond



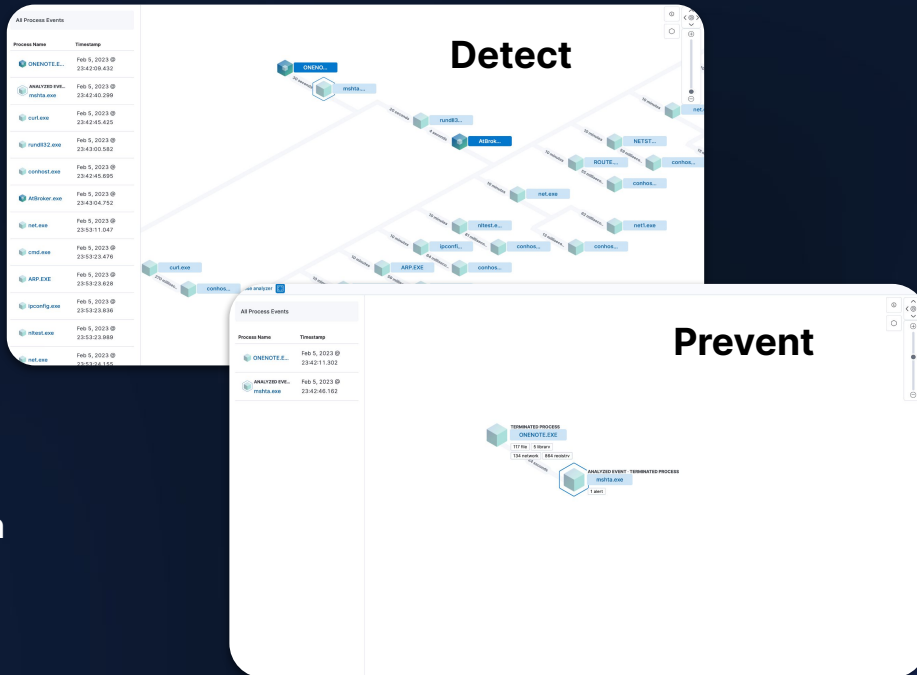
Stop attacks
before they start



Automated
investigation to
accelerate your team



Remediate the threat in
the same workflow



Elastic Security

Prevent

Investigate

Respond



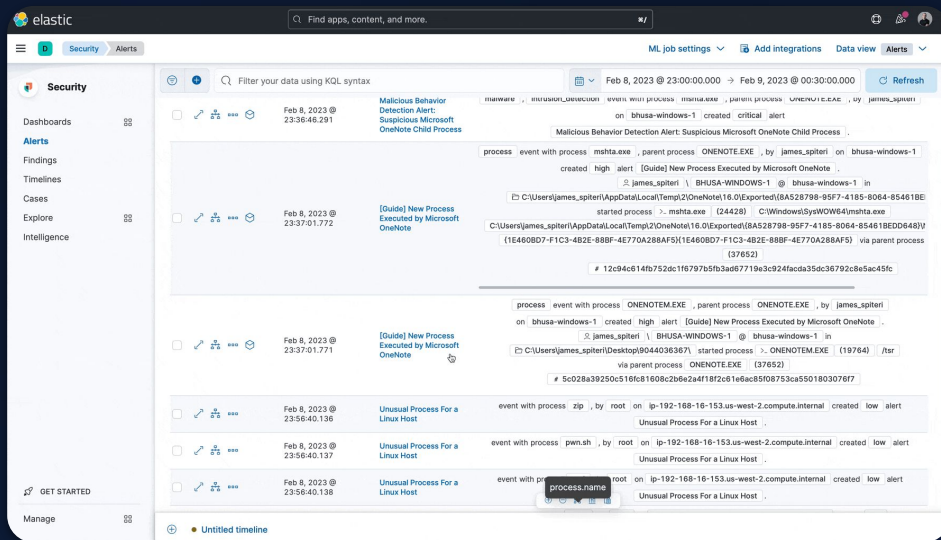
Stop attacks
before they start



Automated
investigation to
accelerate your team



Remediate the threat in
the same workflow



Elastic Security

Prevent

Investigate

Respond



Stop attacks
before they start



Automated
investigation to
accelerate your team



Remediate the threat in
the same workflow

The screenshot shows the Elastic Security console interface. On the left is a sidebar with navigation options: Dashboards, Alerts, Findings, Timelines, Cases, Explore, and Intelligence. The main area displays a list of alerts under the 'Alerts' tab. A specific alert is expanded on the right, titled 'Malicious Behavior Detection Alert: Suspicious Microsoft OneNote Child Process'. This alert occurred on Feb 8, 2023, at 23:36:46.291. The expanded view includes tabs for Overview, Threat Intel, Table, JSON, and Osquery Results. The Overview tab shows a rule description: 'OneNote application. This may indicate an attempt to execute malicious embedded objects from a .one file.' It also includes an 'Insights' section with related cases and alerts, and an 'Enriched data' section showing host risk classification (Current: Critical, Original: Moderate). A 'Take action' button is visible at the bottom right of the alert details.

Scaling with confidence

Improving time to value for security teams

24 Months

3

Products

3 tools, 3
licences

22

SOC Analysts

Level 1 & 2 / 24x7

5TB

Daily Ingest

30 data sources

50K

Events per second

Daily bursts to 100K

3 Months

1

Products

1 tool, 1 licence

4

SOC Analysts

Distributed / 24x7

32TB

Daily Ingest

23 data sources

350K

Events per second

Minimal bursting

Unified Data Platform

1 2 3 4 5

Elastic Controls Framework

- Consolidates all compliance frameworks into a single source of truth
- Enables multiple integration points across the enterprise

Governance/
Compliance

Risk
Management

Vulnerability
Management

Threat
Management

SOCRATES

Create Default Risk Assessment Request

Name Email Department

Please enter your request details

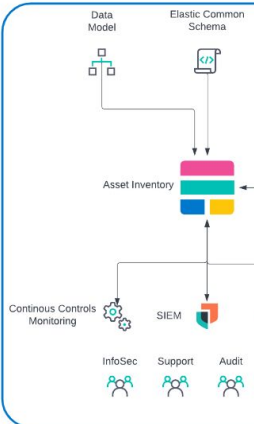
Background
Describe the request

Assets at risk
Which equipment is at risk?

Threat Community
Who is the threat?

Contacts
Provide any relevant contacts

Subject / Purpose
Determine the purpose of the request



Additional Information

Thank you for confirming this event.

To assist the Information Security team with detection tuning, please provide any additional details you believe may be relevant to this alert being triggered.

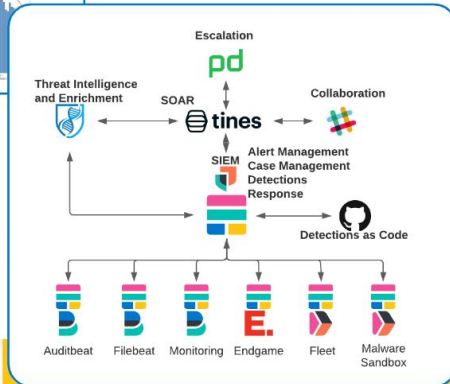
Details

I added my new phone to Qikita for MFA

Follow-Up

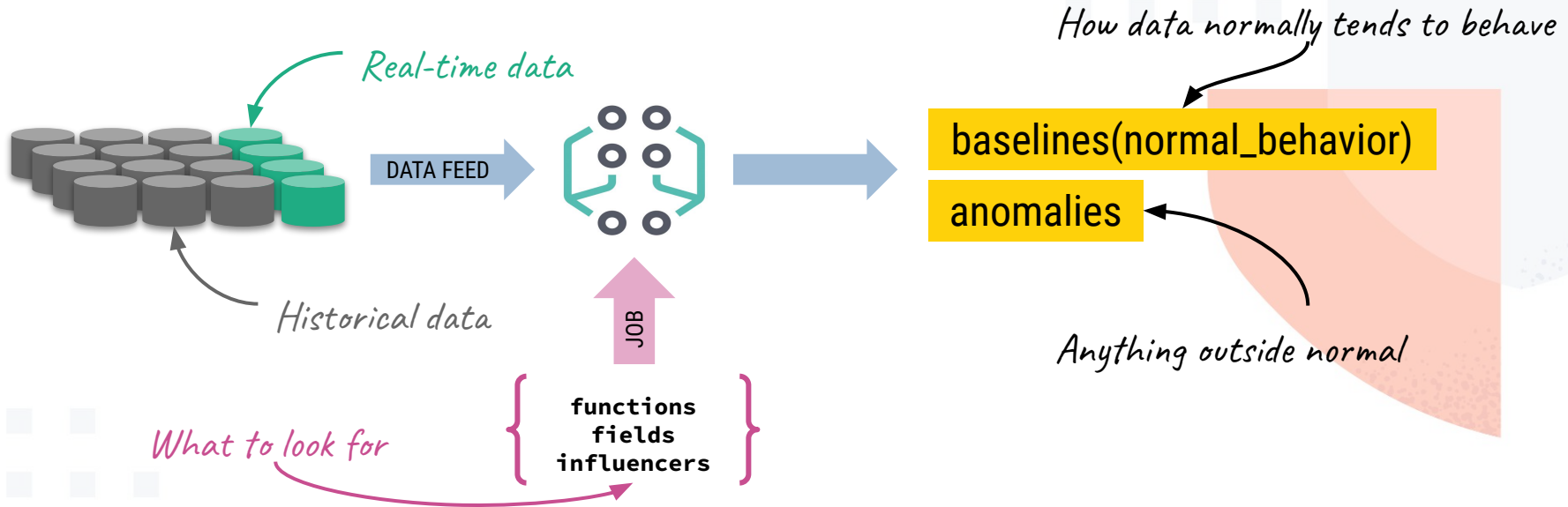
☐ I would like Information Security to contact me regarding this event.

☒ No need to contact me, this should clear it up.



Elastic Machine Learning

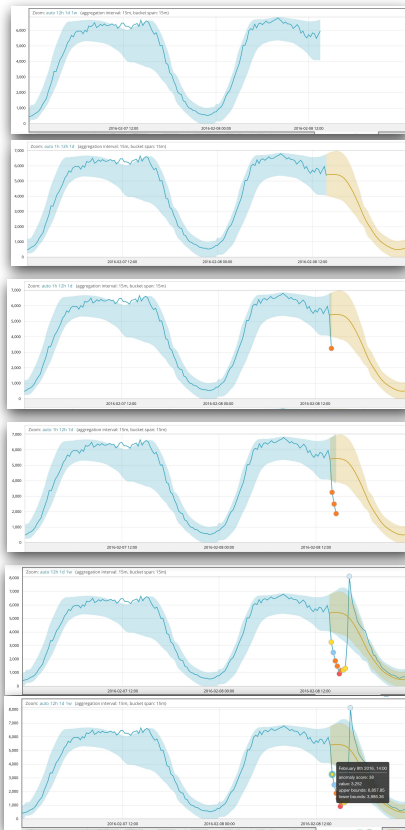
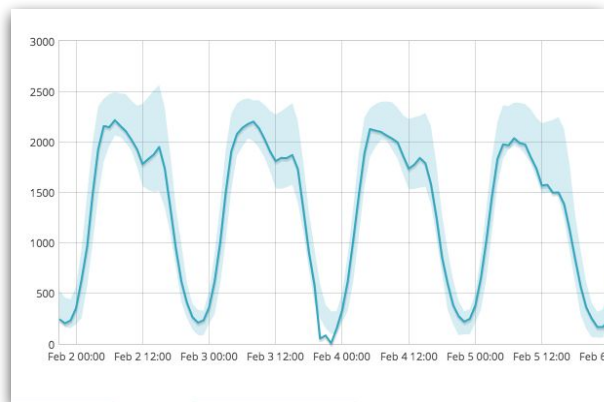
How it works



Predict


1 2 3 4 5


Learn



Operationalise

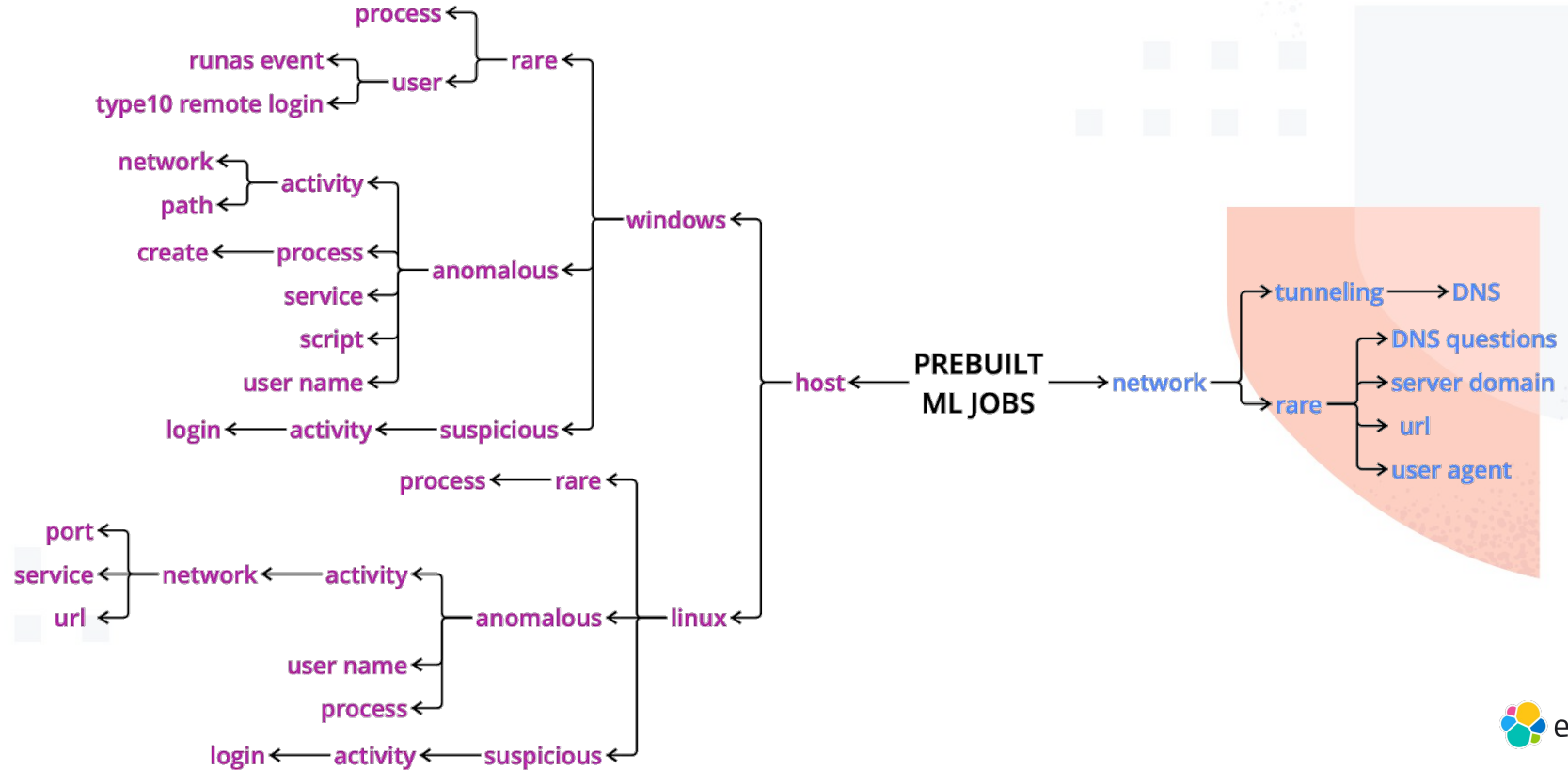
ALERT #2451:
Time: Feb 6th 2016, 15:05
Severity: 94
Description: Critical anomaly in KPI orders per min
Actual: 280
Expected: 1859

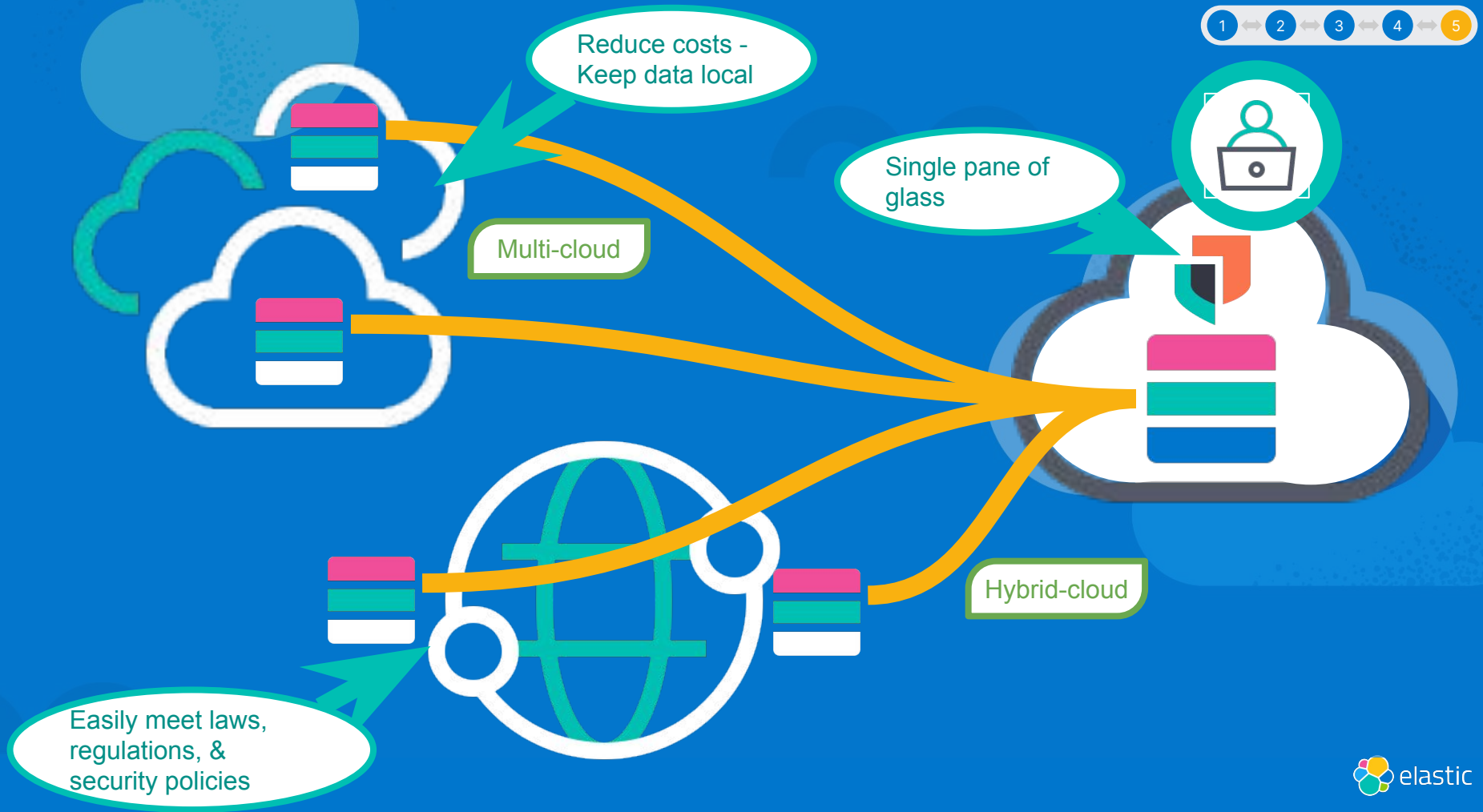
PagerDuty
elastic.pagerduty.com 

> iMessage 

Machine Learning

Overview of Prebuilt Jobs





Bring your data

Detect, Investigate & Respond

cloud



network



host



user



email



threat intel



Native protection

Block threats with Elastic Agent

laptops & desktops



servers & VM's



containers & kubernetes



cloud providers



Elastic Security

SIEM & Security Analytics

Endpoint Security

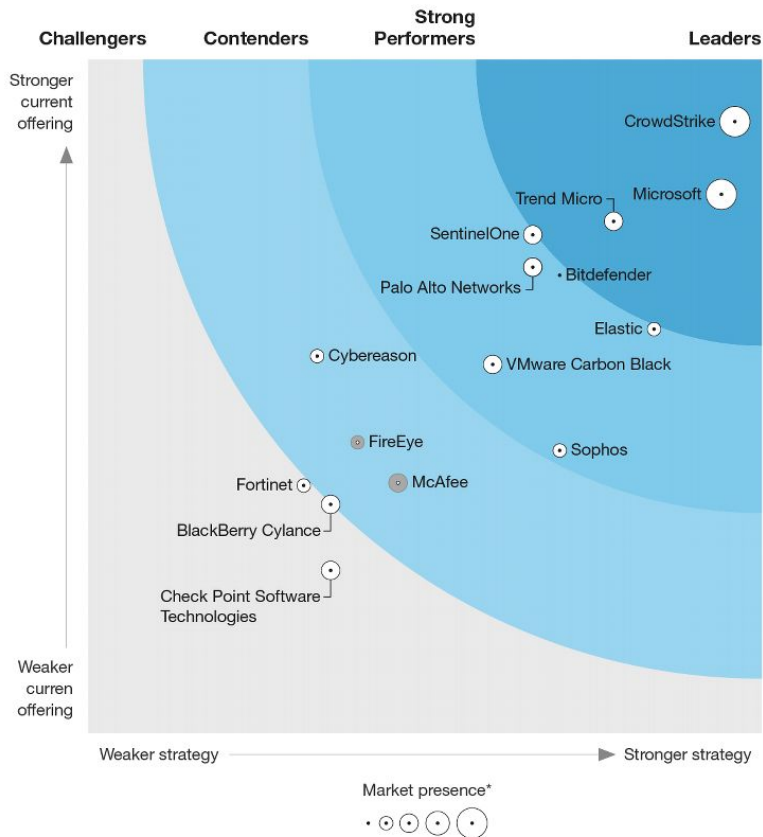
Cloud Security

Powered by Elastic Security Labs - Threat Research

THE FORRESTER WAVE™

Endpoint Detection And Response Providers

Q2 2022



Elastic named a Strong Performer in The Forrester Wave for EDR Providers, Q2 2022

The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester New Wave™ is a graphical representation of Forrester's call on a market. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave™. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.



THE FORRESTER WAVE™

Security Analytics Platforms

Q4 2022



Elastic named a Leader in The Forrester Wave™ Security Analytics Platforms Q4 2022

FORRESTER®

WAVE
LEADER 2022

Security Analytics
Platforms

The Forrester Wave™ is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave™ are trademarks of Forrester Research, Inc. The Forrester New Wave™ is a graphical representation of Forrester's call on a market. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave™. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.





Elastic Security



Security Analytics (& SIEM)



Cloud Security



Endpoint Security



**Elastic
Security
Labs**

Want to find out more?



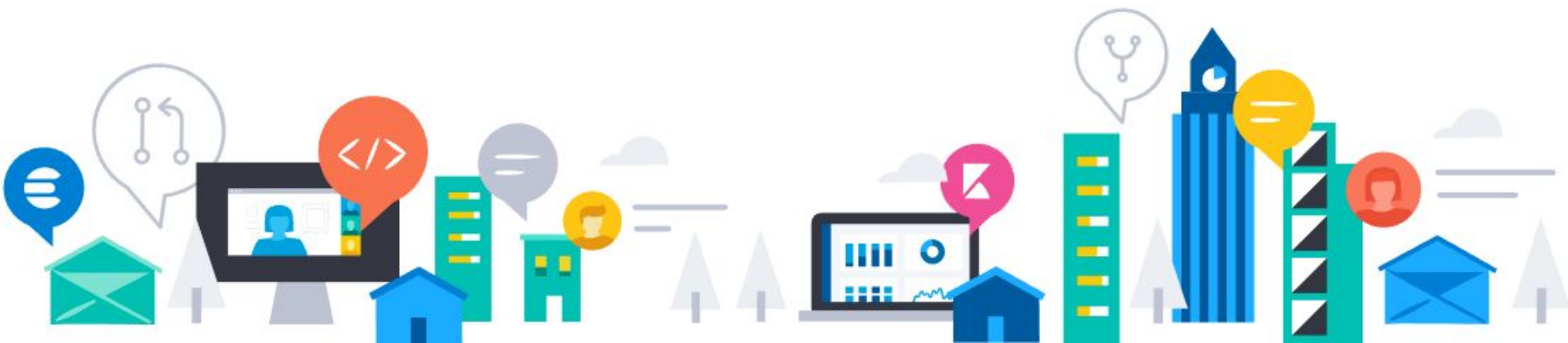
Security Solution:
elastic.co/security/



Security Labs:
elastic.co/security-labs/



Articles & Blogs:
elastic.co/blog/





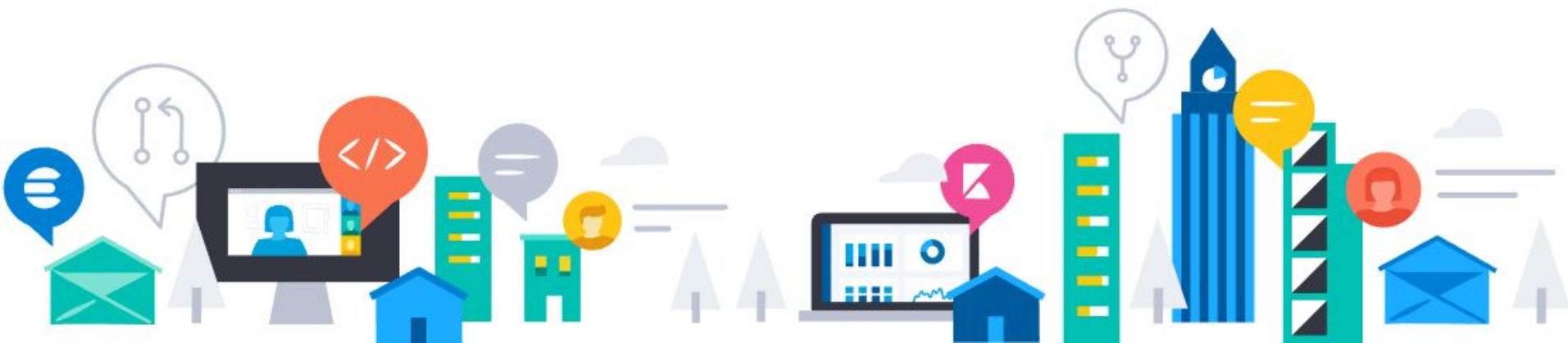
Take a quick spin:
demo.elastic.co



Try free on Cloud:
ela.st/emea-sec-trial



Connect on Slack:
ela.st/slack





Thank You

Search. Observe. Protect.

Safe Harbor Statement

This presentation includes forward-looking statements that are subject to risks and uncertainties. Actual results may differ materially as a result of various risk factors included in the reports on the Forms 10-K, 10-Q, and 8-K, and in other filings we make with the SEC from time to time. Elastic undertakes no obligation to update any of these forward-looking statements.





Appendix: Elastic Security Stack

Prevent, Detect, and Respond



Security

Out-of-the-box solution for security analysts everywhere



Kibana

Visualize your Elasticsearch data and navigate the Elastic Stack



Elasticsearch

A distributed, RESTful search and analytics engine



Beats



Agent



Endpoint



Logstash



Elastic Security Labs

Security content from Elastic and community