



# A Higher Level of Security with an Integrated, Scalable Platform.

---

Jhon Masschelein  
Principal Solutions Architect



/me

Jhon Masschelein

Jhon@Elastic.co

Elastic

Microsoft Azure

Hortonworks

SurfSara

Silicon Graphics

Principal Solutions Architect (3,5y)

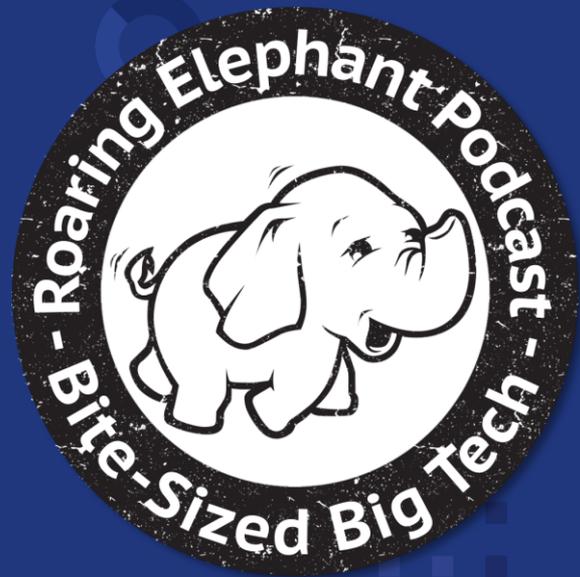
Solution Architect Data&A.I. (3y)

Solution Engineer (2y)

HPC DevOps Engineer (5y)

Customer Support Engineer (13y)

Co-Host Roaring Elephant Podcast (7y)



elastic

# Forces of change impacting the public sector

The digital experience is evolving

52%

Employees prefer remote work

60%

Citizens comfortable with digital services

50%

Data sharing programs formalizing

Migration to cloud and AI/ML adoption is accelerating

\$41.9B

Government cloud spend by 2025

\$204B

AI solution global spend by 2025

Sources: [McKinsey](#), [PUBLIC \(UK\)](#), [Gartner](#), [Report Linker](#), [Business Wire](#), [Cybercrime Magazine](#), [Juniper Research](#), [\(ISC\)<sup>2</sup>](#)

Cyber attacks and fraudulent activities are increasing

15%

Annual cybercrime growth through 2025

\$205B<sup>+</sup>

Online fraud losses in the next five years

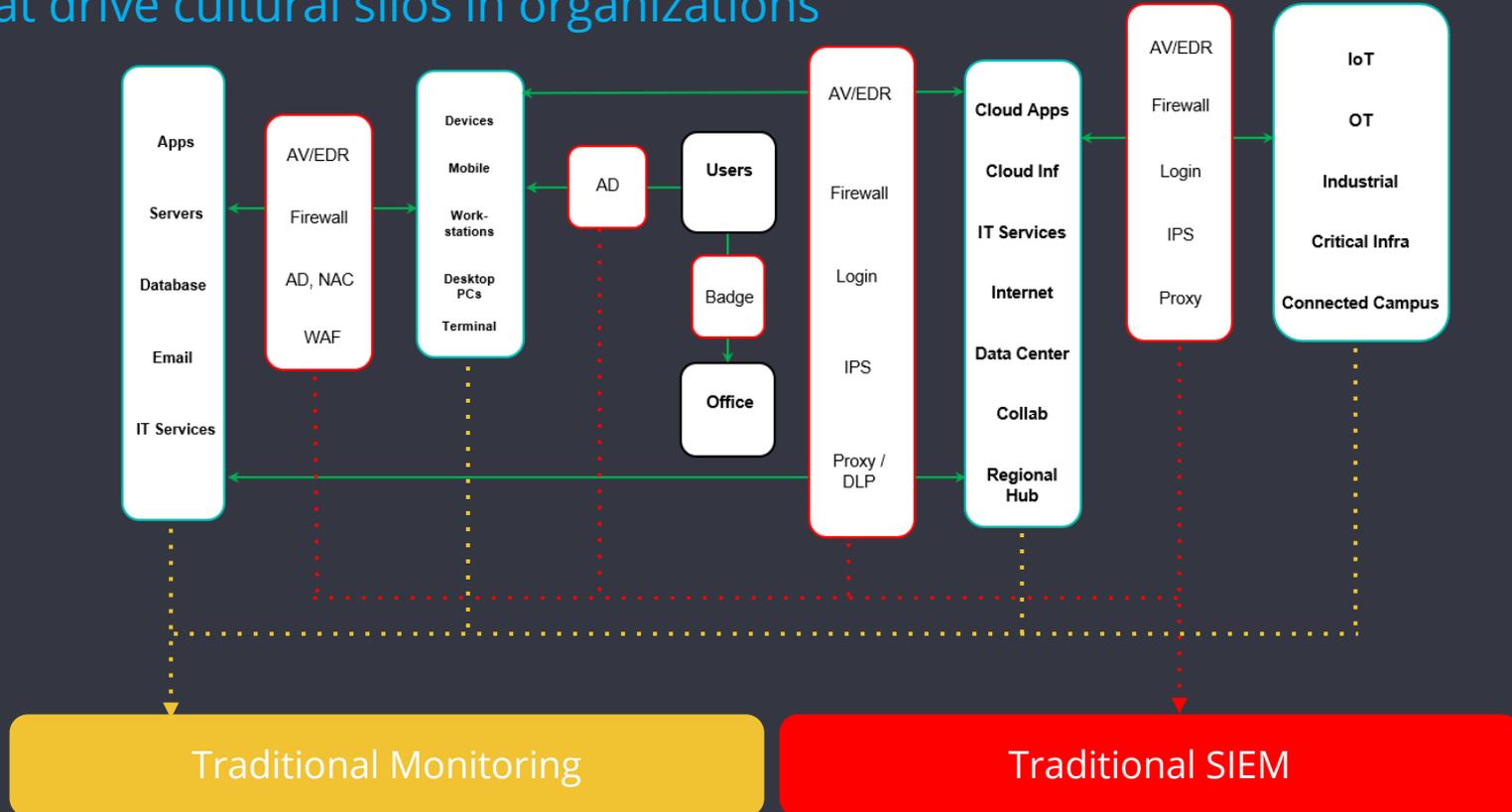
64%

Organizations affected by cyber shortage



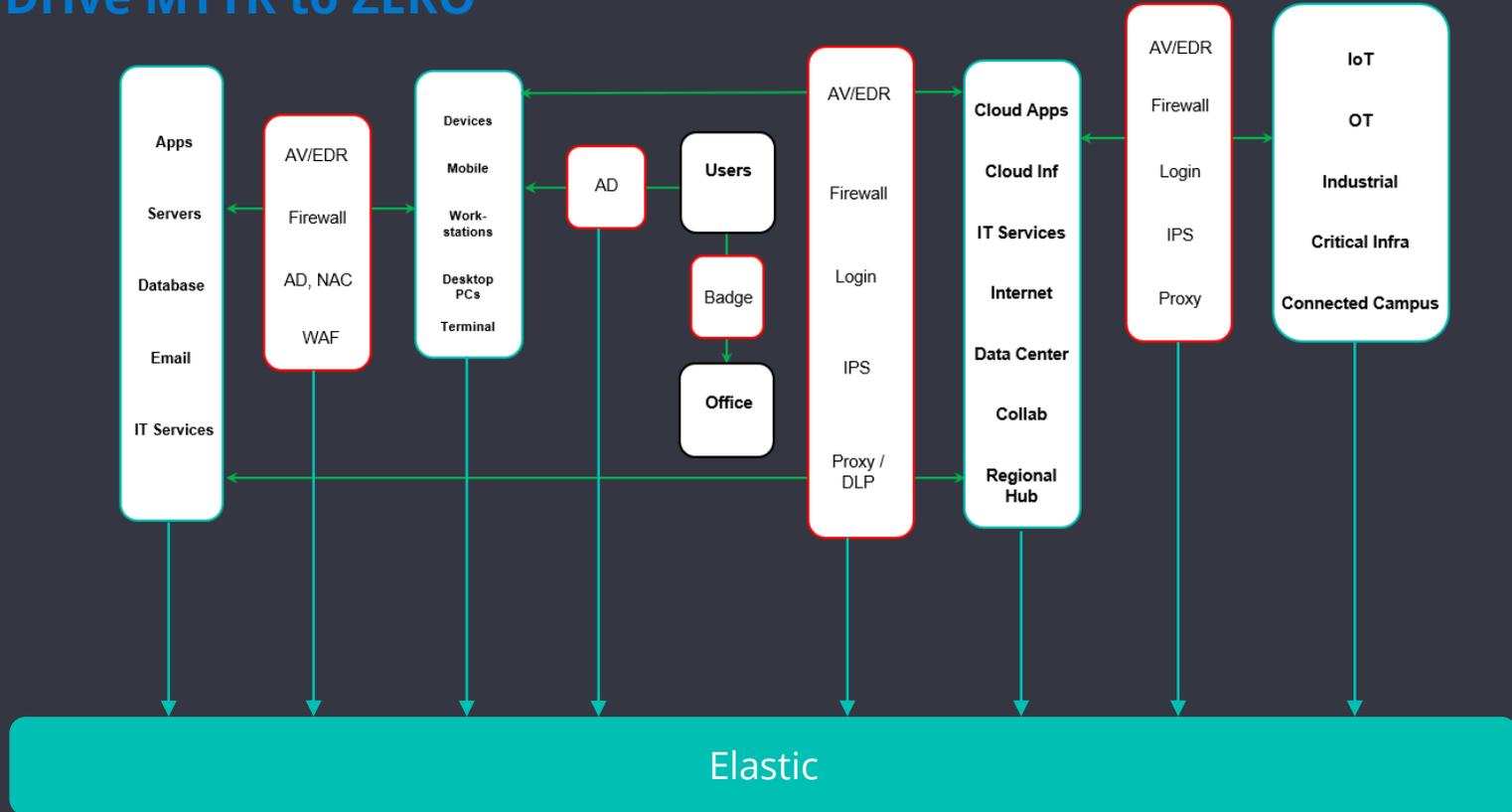
# Technology data silos

That drive cultural silos in organizations



# Single, unified, powerful platform

To Drive MTTR to ZERO



# Benefits

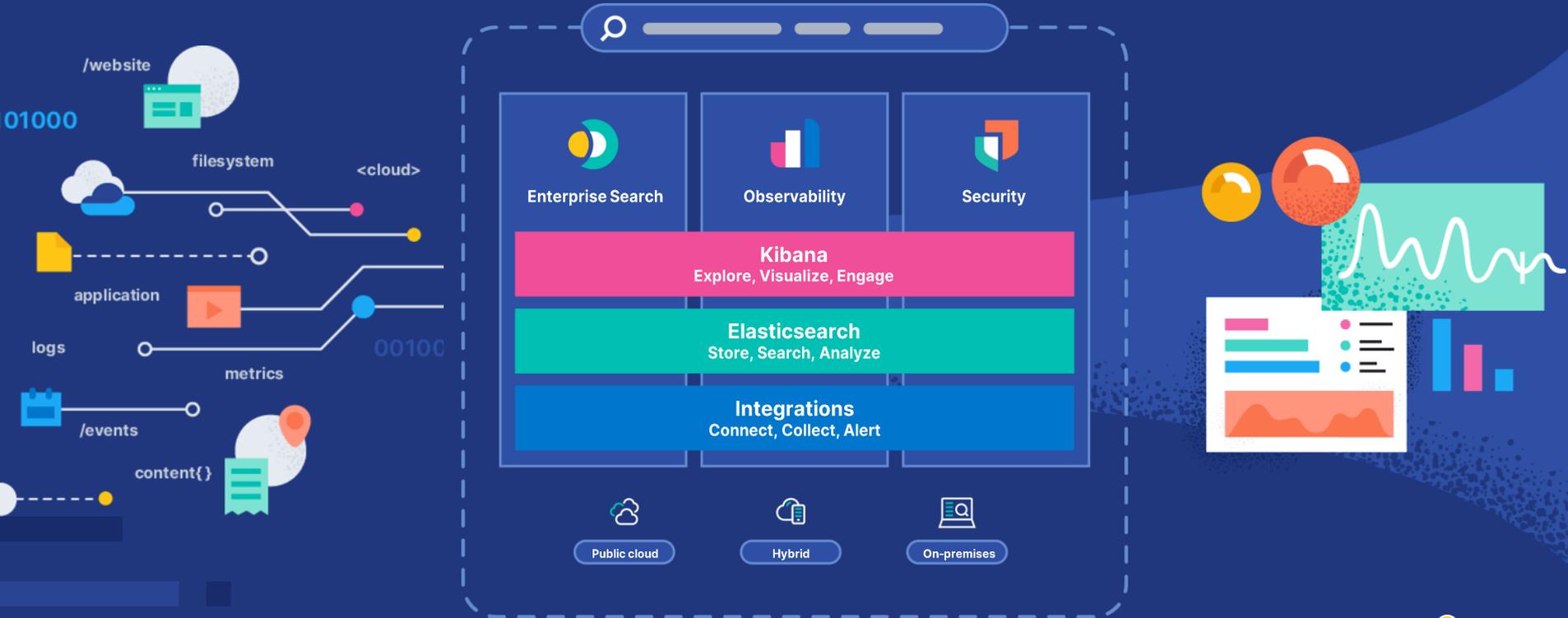
- Avoid data duplication
- Improve shared communication
- Reduce operating frictions
- Reduce costs while keeping services **up** and our organizations **secured**



# The Elastic Search Platform



# The Elastic Search Platform



# Driving DevSecOps

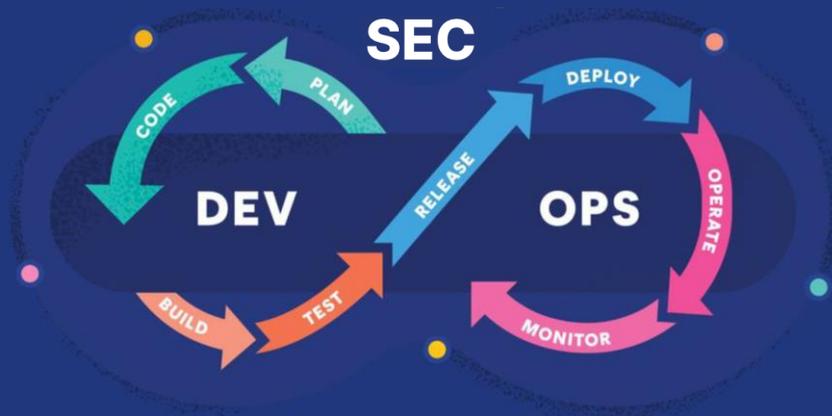
Automatically deploy agent into pipelines to gather all log, metrics, APM and synthetics data

Seamless visibility in production across all tiers of application stacks

Model new threats and monitor throughout the lifecycle

Secure endpoints with pre and post execution prevention

Proactive alerts for issues across the application stack



Correlate operational issues for rapid RCA

Monitor pre-prod testing to find operational and security issues early in the cycle

Leverage >600 pre-built detections covering MITRE ATTACK and beyond

Visualise the entire CI/CD pipeline to identify process bottlenecks

Quickly isolate hosts, identify infected systems and stop attacks from spreading

Create cases to monitor issues, collaborate with colleagues and resolve threats

Quickly investigate and take recommended actions

# Driving DevSecOps

Automatically deploy agent into pipelines to gather all log, metrics, APM and synthetics data

Seamless visibility in production across all tiers of application stacks

Model new threats and monitor throughout the lifecycle

Secure endpoints with pre and post execution prevention

Proactive alerts for issues across the application stack

Correlate operational issues for rapid RCA

Monitor pre-prod testing to find operational and security issues early in the cycle

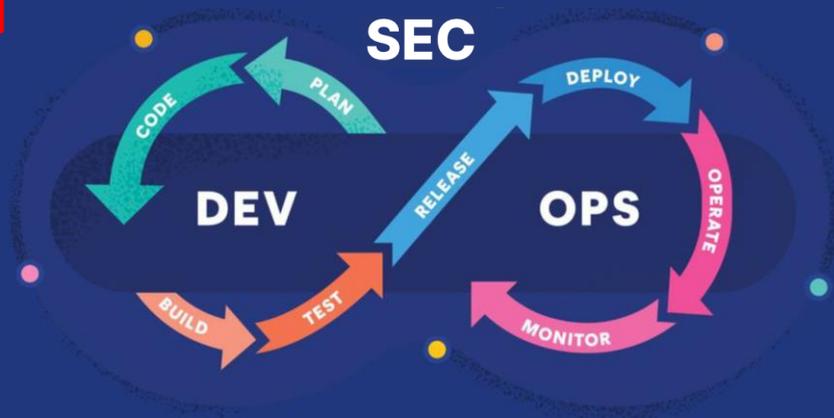
Leverage >600 pre-built detections covering MITRE ATTACK and beyond

Visualise the entire CI/CD pipeline to identify process bottlenecks

Quickly isolate hosts, identify infected systems and stop attacks from spreading

Create cases to monitor issues, collaborate with colleagues and resolve threats

Quickly investigate and take recommended actions



# Limitless XDR

XDR modernizes security operations, enabling analytics across all data, automating key processes, and bringing native endpoint security to every host.

SIEM

Endpoint  
Security

Cloud  
Security

# Security without Limits

Endpoint

Cloud

SIEM/Security Analytics

*Pre-execution*

*Post-execution*

*Response*

Security insights

Monitoring and reporting

Analyst collaboration

*Continuous cloud-native security*

*Workload runtime security*

Malware prevention

Behavior-based prevention

Host isolation

Threat hunting

Advanced threat detection

Incident response

Build-time

Deployment-time

Runtime

Ransomware prevention

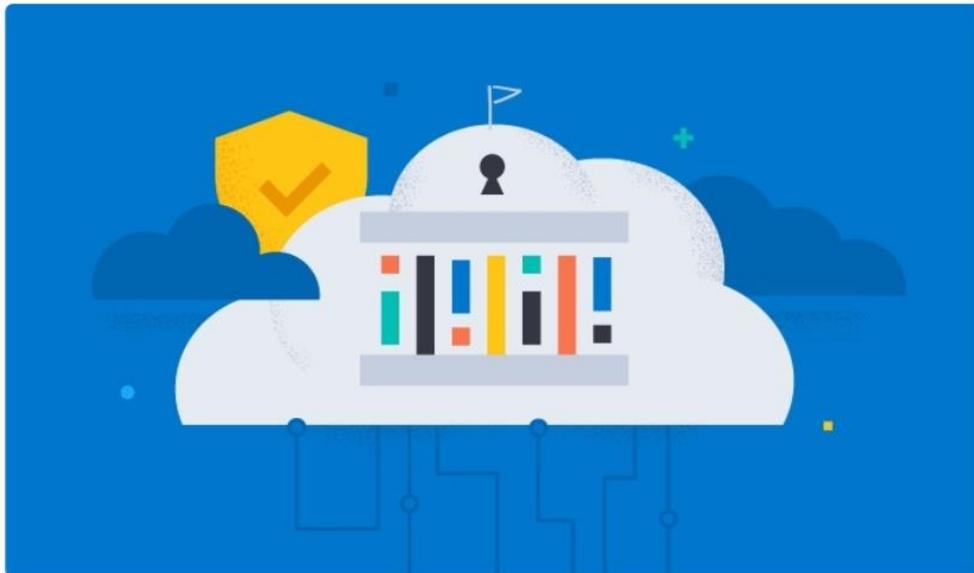
Advanced ransomware protection

Asset management with osquery

Memory protection

*Coming soon*

**Elastic announces Elastic Security for Cloud,  
delivering new posture management and  
workload protection capabilities** 8-June-2022



<https://www.elastic.co/blog/secure-your-cloud-with-elastic-security>

# The Elastic Value



## Open & Integrated

Flexible [data ingest](#) and community support with no vendor lock-in



## Native Protections

Boost mean time to protection with built-in prevention, detection and response



## Analyst Workflows

Simplify deployment and management with a single stack & integrated workflows



## Contextual Insights

Investigate and hunt with a limitless data store powered by market leading search



## Security + Observability

Secure the endpoint and cloud applications, or address customer experience, from a single interface



## Start Small, Scale Up

Start simple or go big on cloud-scale solution with [simple and flexible](#) pricing

# The Elastic Value



## Open & Integrated

Flexible [data ingest](#) and community support with no vendor lock-in



## Native Protections

Boost mean time to protection with built-in prevention, detection and response



## Analyst Workflows

Simplify deployment and management with a single stack & integrated workflows



## Contextual Insights

Investigate and hunt with a limitless data store powered by market leading search



## Security + Observability

Secure the endpoint and cloud applications, or address customer experience, from a single interface



## Start Small, Scale Up

Start simple or go big on cloud-scale solution with [simple and flexible](#) pricing

Baseline Informatie-beveiliging Overheid



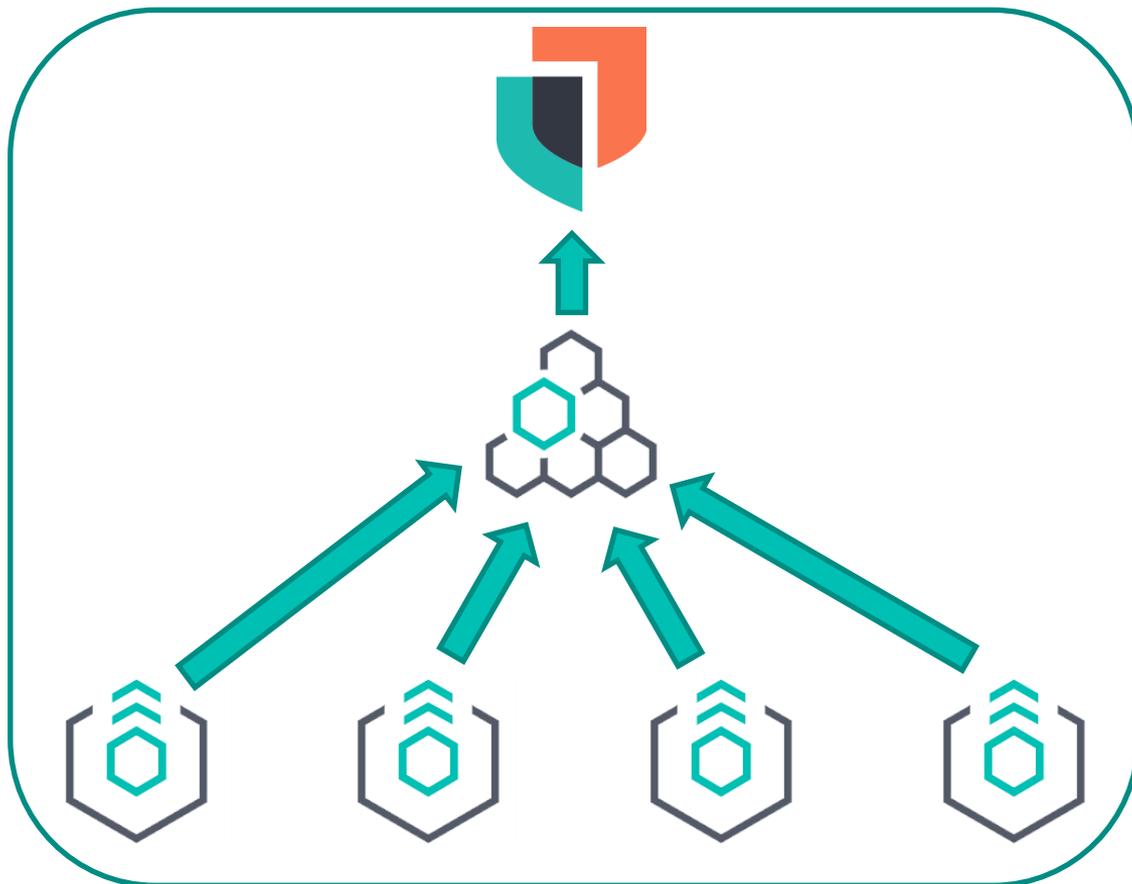
# Scalability

# Single Department

 Elastic Deployment

 Elastic Fleet

 Elastic Agent



Network A

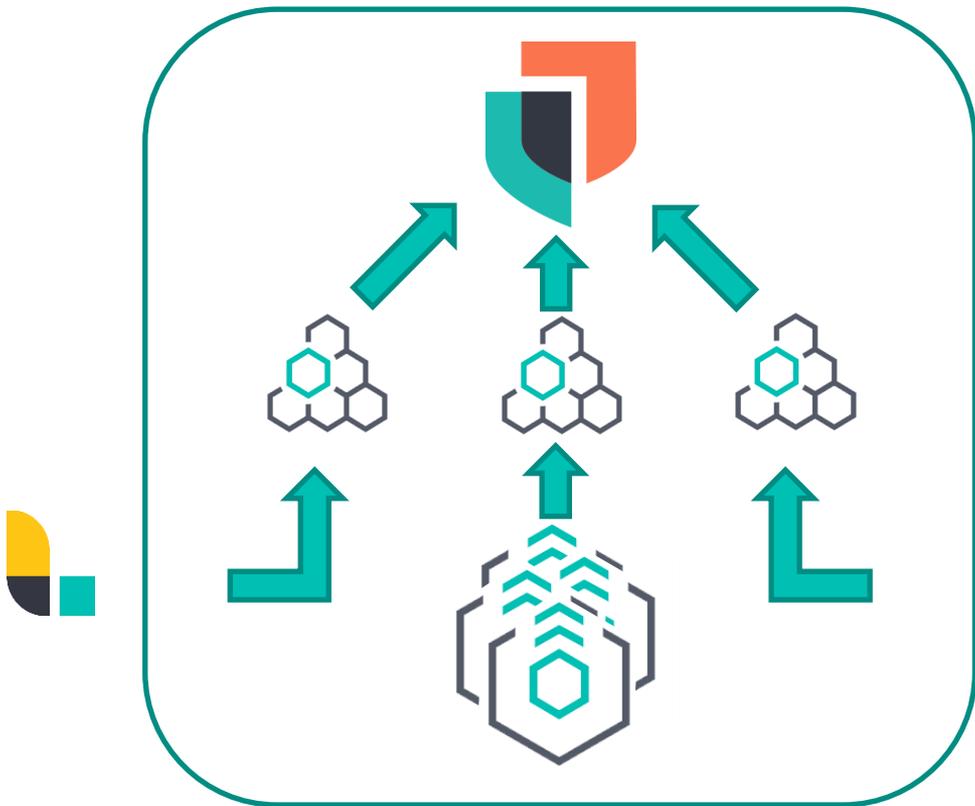
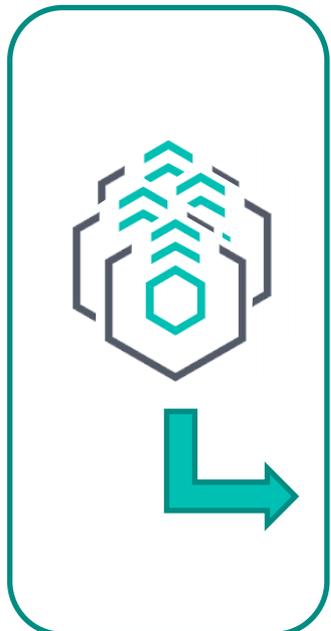
 Elastic Deployment

 Elastic Fleet

 Elastic Agent

 Elastic Logstash

# Single Organization – Multiple Departments



 Elastic Deployment

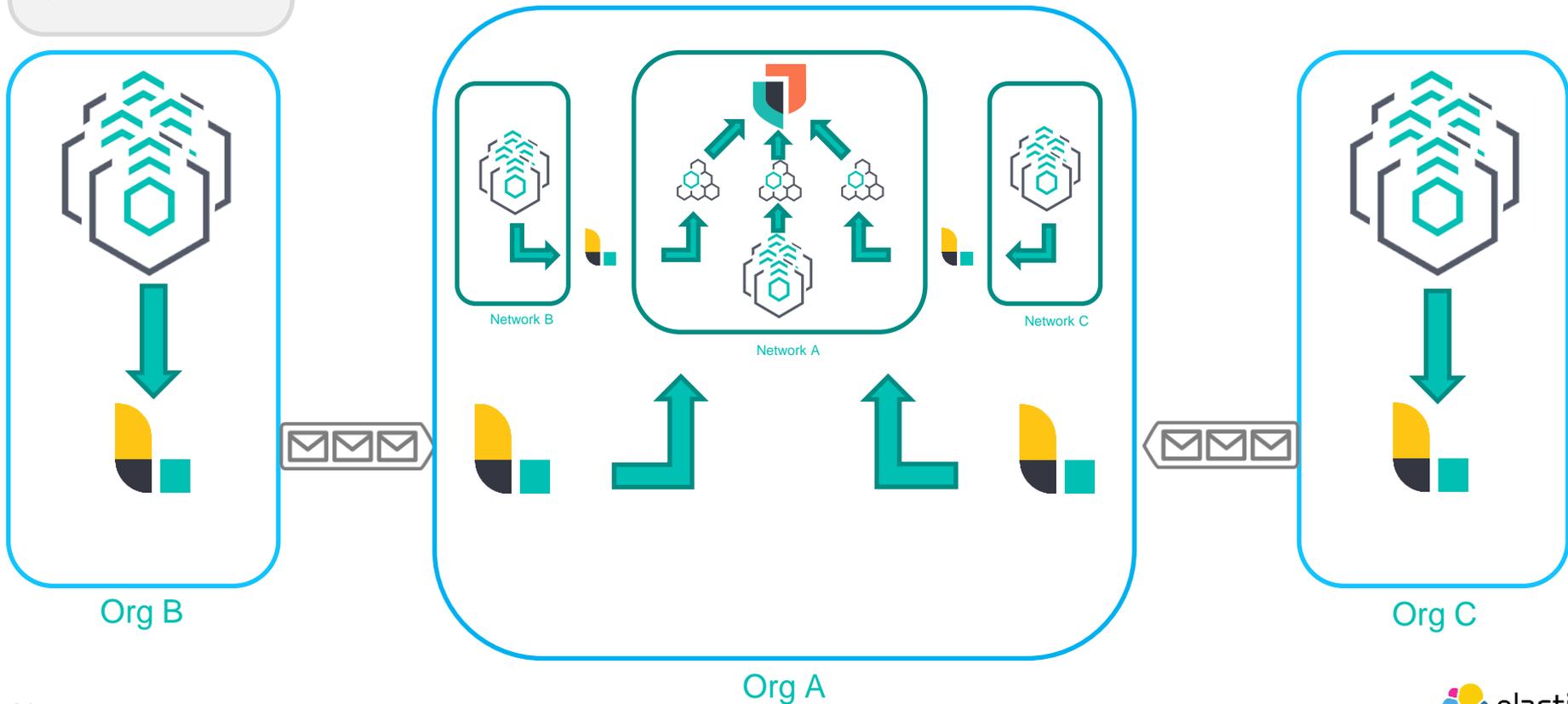
 Elastic Fleet

 Elastic Agent

# Multiple Organizations, External Monitoring

 Elastic Logstash

 Message Bus



# Decentralized Deployment

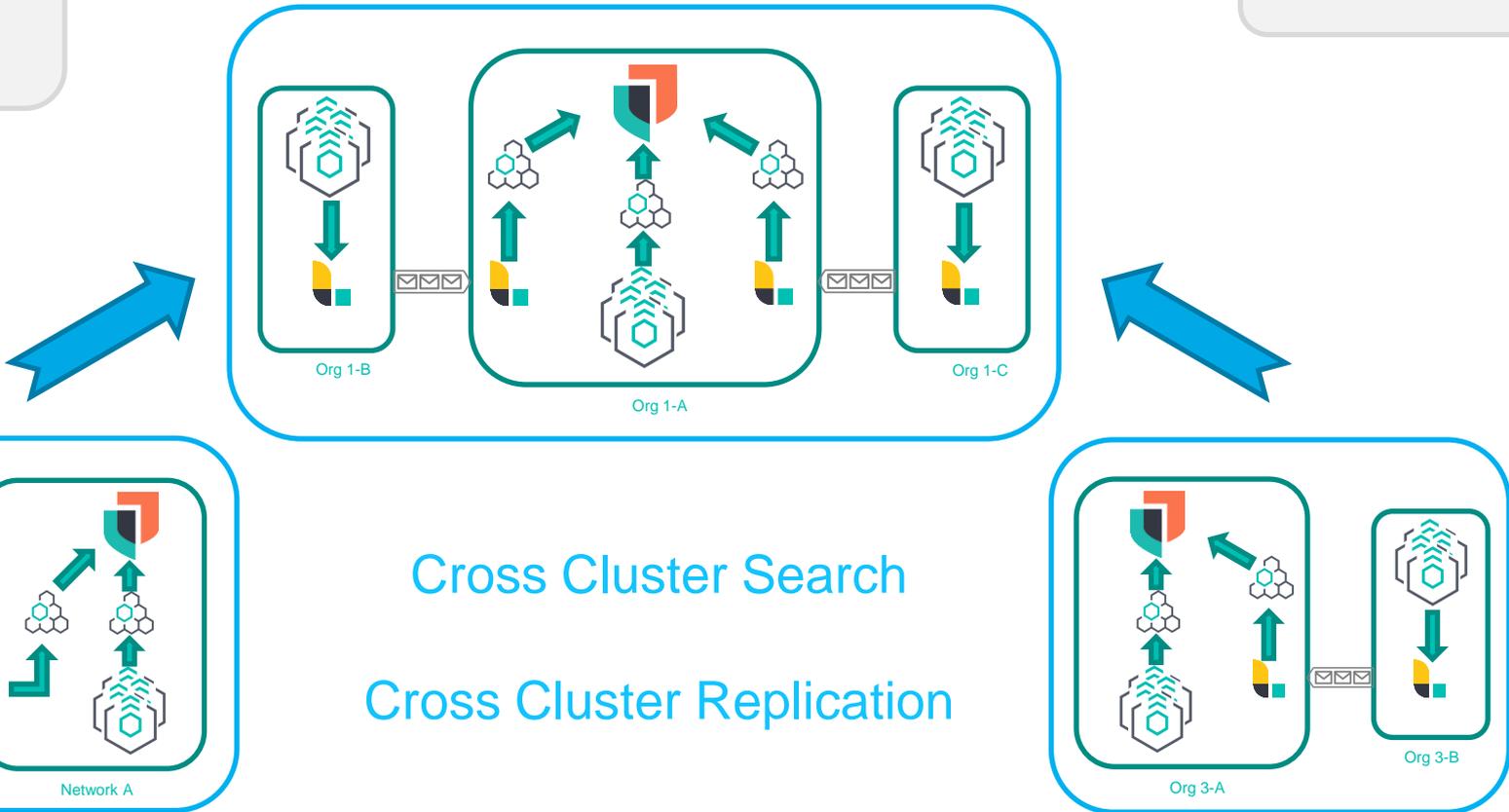
 Elastic Deployment

 Elastic Fleet

 Elastic Agent

 Elastic Logstash

 Message Bus



Cross Cluster Search  
Cross Cluster Replication

# Examples



# SecureNed: alleen samen houden we Nederland digitaal veilig

© NCSC

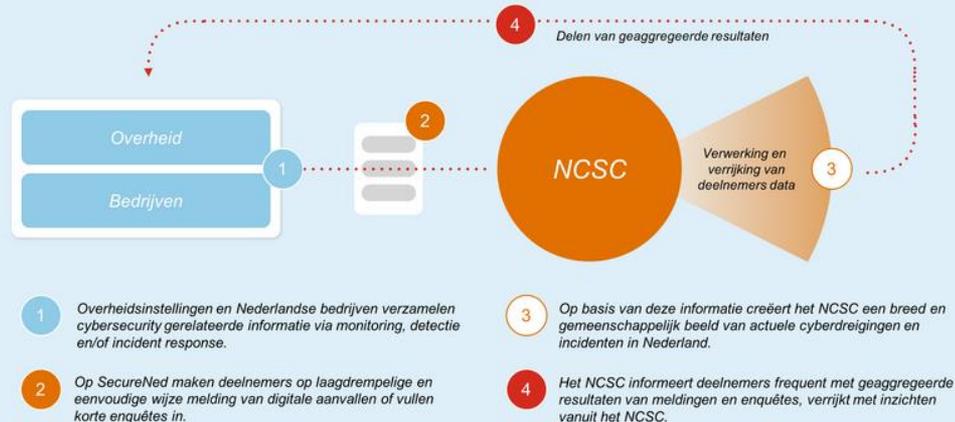
Nederlandse instellingen, bedrijven en burgers krijgen steeds vaker te maken met cybercriminaliteit en digitale dreigingen. Omdat we Nederland alleen digitaal veilig kunnen houden werkt het NCSC samen met overheden en bedrijven via SecureNed. Een uniek samenwerkingsverband gericht op het onderling uitwisselen van informatie over cyberdreigingen en incidenten. Op basis van de gedeelde informatie kunnen deelnemers maatregelen nemen om schade te voorkomen of te beperken. SecureNed maakt deze informatiedeling eenvoudig, effectief, maar ook veilig. Wat vandaag een incident is bij de één, is een goede waarschuwing voor de ander.

[SecureNed | Nationaal Cyber Security Centrum \(ncsc.nl\)](https://www.ncsc.nl)



Nationaal Cyber Security Centrum  
Ministerie van Justitie en Veiligheid

## Hoe werkt SecureNed?



Beeld: ©NCSC



Ministerie van Defensie



# Our approach to vulnerabilities

a company wide responsibility

Defensie Cyber Security Centrum



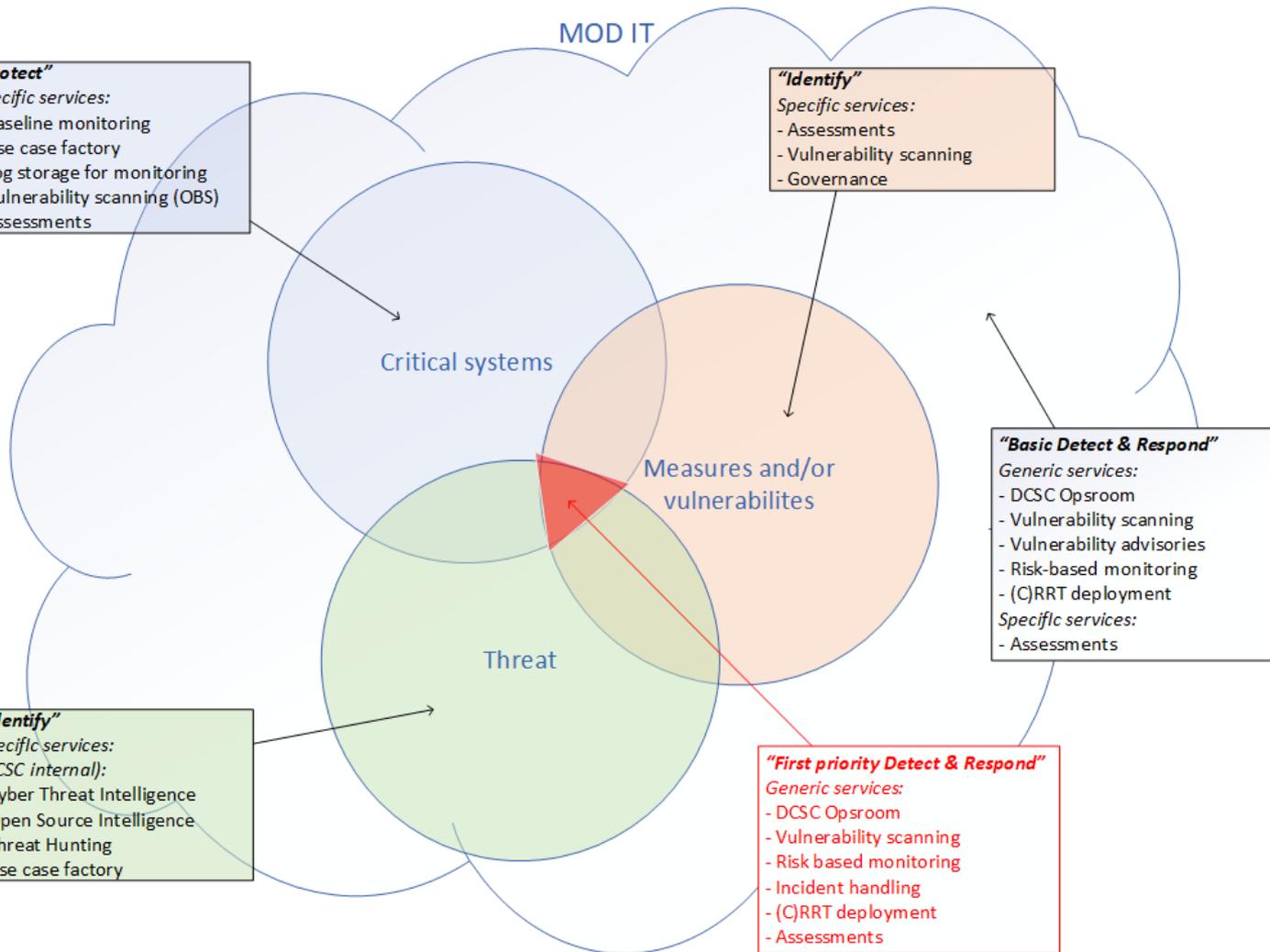
**"Protect"**  
Specific services:  
- Baseline monitoring  
- Use case factory  
- Log storage for monitoring  
- Vulnerability scanning (OBS)  
- Assessments

**"Identify"**  
Specific services:  
- Assessments  
- Vulnerability scanning  
- Governance

**"Identify"**  
Specific services:  
(DCSC internal):  
- Cyber Threat Intelligence  
- Open Source Intelligence  
- Threat Hunting  
- Use case factory

**"First priority Detect & Respond"**  
Generic services:  
- DCSC Opsroom  
- Vulnerability scanning  
- Risk based monitoring  
- Incident handling  
- (C)RRT deployment  
- Assessments

**"Basic Detect & Respond"**  
Generic services:  
- DCSC Opsroom  
- Vulnerability scanning  
- Vulnerability advisories  
- Risk-based monitoring  
- (C)RRT deployment  
Specific services:  
- Assessments



# Upcoming relevant events

[December 18, 2022] [Webinar] Cybersecurity trends in 2023: Modernizing security operations

<https://www.elastic.co/virtual-events/2023-cybersecurity-trends>

[January 24, 2023] Preparing for the NIS2 directive with Elastic Security

<https://events.elastic.co/prep-for-nis2-with-elastic-security>

[January 24, 2023] [Webinar] Search & Stream with Elastic Enterprise Search

<https://events.elastic.co/2023-01-24-streamsearch>

[January 26, 2023] [Webinar] Getting the most out of Elastic Observability with logs, metrics, and APM

<https://events.elastic.co/getting-the-most-elastic-observ>

[January 31, 2023] [Webinar] Elastic Security: Capture the Flag Workshop

<https://events.elastic.co/2022-01-31-ctf-emea>

[February 9th, 2023] [Webinar] Getting the most out of Elastic Security with threat hunting and Cloud posture

<https://events.elastic.co/getting-the-most-elastic-security-threat-hunting-cloud-posture>

[March 7-9, 2023] [Online, Free] ElasticON Global

<https://www.elasticon.com/event/e473ab1b-88b4-4326-aa8d-e6054a566e48/summary>

Try out the latest and greatest Elastic capabilities for free with

a 14- day cloud trial : <https://ela.st/23eceu>



# Questions?

# cloud.elastic.co



Cloud



Elasticsearch Service

[Create deployment](#)

Deployment name	Status	Version	Cloud region	Quick link
THX 1138	Healthy	8.1.0	Azure - Netherlands (westeurope)	



Documentation

Help me find...

[Elasticsearch Service on Elastic Cloud documentation](#)

[Elasticsearch documentation](#)

[Elasticsearch REST API](#)



Support

Having some trouble? Reach out to us.

[Contact support](#)



Community

[Join an ElasticON event](#)

Hear success stories, lessons learned, tips,...

FEBRUARY 11, 2022



[Join Elastic at Kangaroot Open22 Belgium](#)

MARCH 29, 02:00 AM

[Elastic Security 101](#)

MARCH 29, 02:00 AM

[Events portal](#)

Engage with our community! [Visit our forum](#), [join us on Slack](#), or [contribute to the Elastic Stack on GitHub](#).

# Extra Slides

# Deploy your way, anywhere

Select a deployment model for your unique needs



**Self-Managed**

Install a single package



**Elastic Cloud  
Enterprise**

Centrally manage multiple  
deployments on your infra



**Elastic Cloud on  
Kubernetes**



**Elastic Cloud**

Deploy instantly on AWS,  
Azure or Google Cloud



**Federate across these deployments with cross-cluster search**

# Unified Data Collection

## Single Agent

### 100s of integrations

Go from data to dashboard in minutes

### Central ingest management

Monitor and manage all your agents, at scale, from a single place

### Across observability and security

Collect events across data sources to enable both use cases

Ingest Manager / Integrations / All

Overview **Integrations** Configurations Fleet Data streams [Send Feedback](#) [Settings](#)

## Integrations

Browse integrations for popular apps and services.

All integrations Installed integrations

### All integrations

Search for integrations

- All 11
- Custom 1
- Security 1

**AWS**  
AWS Integration

**Cisco**  
Cisco Integration

**Elastic Endpoint**  
This is the Elastic Endpoint package.

**Kafka**  
Kafka Integration

**Customs logs**  
Collect your custom logs.

**MySQL**  
MySQL Integration

**NetFlow**  
NetFlow Integration

**Nginx**  
Nginx Integration

**Redis**  
Redis Integration

**Staging**  
Indicator that this is the staging distribution or snapshot

**System**  
System Integration

**Experimental** – Ingest Manager is under active development and is not intended for production purposes. View more details.

# Unified Schema

## Elastic Common Schema (ECS)

- Defines a **common** set of fields and objects to ingest data into Elasticsearch
- Enables **cross-source analysis** of diverse data
- Designed to be **extensible**
- ECS is **adopted** throughout the Elastic Stack
- Contributions & feedback welcome at <https://github.com/elastic/ecs>

## Searching *without* ECS

```
src:10.42.42.42
OR client_ip:10.42.42.42
OR apache2.access.remote_ip:
  10.42.42.42
OR context.user.ip:10.42.42.42
OR src_ip:10.42.42.42
```

## Searching *with* ECS

```
source.ip:10.42.42.42
```

# Unified RBAC

## Advanced data-level security

### Security Controls

Powerful RBAC, ABAC

Document level security

Field level security

Encryption at rest/transit

Audit logging

SSO (SAML, OIDC)

CIS hardening

Vulnerability Scanning

### Platform Compliance

HIPAA

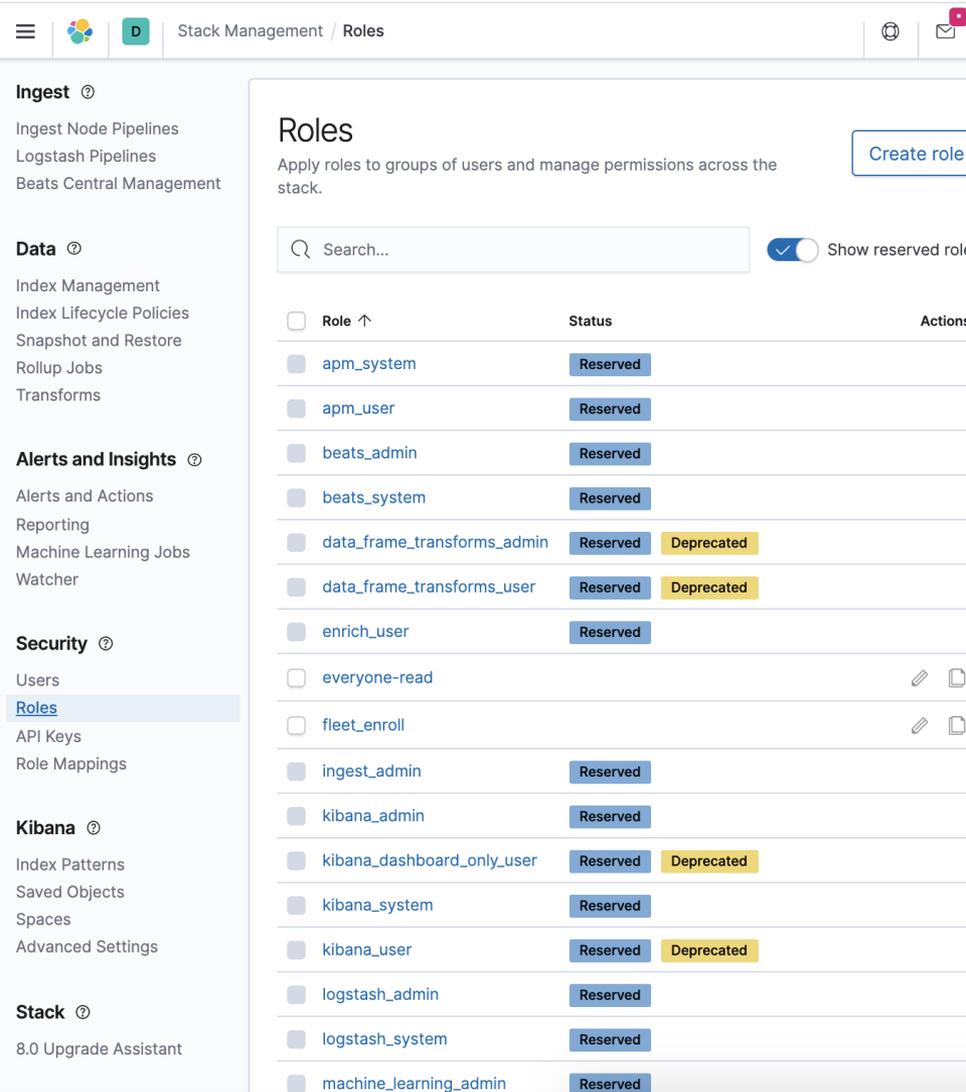
CSA Star Level 2

SOC 2 Type I, II, SOC 3

ISO 27001/27107/27018

FedRAMP

GDPR compliant ops



# Unified Issue Detection

## Free and Open Detection Engine

### Speed and Scale

Powered by the Elastic stack

### Cover all your needs

Build-your-own or leverage free and open prebuilt detections

### Built-in anomaly detection & alerting

Detect known and unknown threats with **detection rules** and **machine learning**

The screenshot shows the AWS Security Center interface for managing detection rules. The breadcrumb trail is "Security / Detections / Detection rules". The navigation menu includes "Overview", "Detections", "Hosts", "Network", "Timelines", "Cases", and "Administration". A "Back to detections" link is visible. The main heading is "Detection rules", with sub-tabs for "Rules" and "Monitoring".

Under the "All rules" section, there are 37 rules displayed. The interface includes a "Showing 37 rules" indicator, a "Selected 0 rules" status, and options for "Bulk actions" and "Refresh".

<input type="checkbox"/>	Rule	Risk score	Severity	Last run	Last
<input type="checkbox"/>	AWS IAM Group Creation	21	Low	2 minutes ago	●
<input type="checkbox"/>	AWS CloudTrail Log Created	21	Low	1 minute ago	●
<input type="checkbox"/>	AWS CloudWatch Log Stream Deletion	47	Medium	1 minute ago	●
<input type="checkbox"/>	AWS EC2 Encryption Disabled	47	Medium	1 minute ago	●
<input type="checkbox"/>	AWS CloudTrail Log Updated	21	Low	1 minute ago	●
<input type="checkbox"/>	AWS WAF Access Control List Deletion	47	Medium	1 minute ago	●
<input type="checkbox"/>	AWS CloudWatch Alarm Deletion	47	Medium	6 minutes ago	●
<input type="checkbox"/>	AWS EC2 Network Access Control List Creation	21	Low	6 minutes ago	●
<input type="checkbox"/>	AWS Management Console Root Login	73	High	6 minutes ago	●
<input type="checkbox"/>	AWS CloudTrail Log Suspended	47	Medium	6 minutes ago	●
<input type="checkbox"/>	Unusual City For an AWS Command	21	Low	9 minutes ago	●
<input type="checkbox"/>	AWS CloudTrail Log Deleted	47	Medium	6 minutes ago	●
<input type="checkbox"/>	AWS RDS Cluster Creation	21	Low	6 minutes ago	●
<input type="checkbox"/>	AWS IAM Group Deletion	21	Low	1 minute ago	●

# Unified Issue Detection

elastic/detection-rules

## Community-driven

Building shared knowledge across Security and Operations communities

## Always growing

Elastic experts and millions of members actively developing new rules in the open

## Always available

Detections are free and under Elastic License

elastic / detection-rules

<> Code Issues 78 Pull requests 59 ZenHub Actions Security Insights

main 56 branches 2 tags Go to file Add file Code

bm11100 and threat-punter [New Rule] Azure Storage Account Key Regene... 140891e 4 days ago 122 commits

.github	Update pythonpackage.yml (#242)	6 days ago
detection_rules	Fix kibana-diff command (#198)	6 days ago
etc	Update packages.yml	6 days ago
kibana	Fix kibana-upload and remove cumbersome dataclasses (#216)	8 days ago
kql	Add KQL -> DSL conversion (#81)	2 months ago
rta	Remove unreachable and legacy code	2 months ago
rules	[New Rule] Azure Storage Account Key Regenerated (#188)	4 days ago
tests	Fix kibana-upload and remove cumbersome dataclasses (#216)	8 days ago
.gitignore	Add vscode directory to gitignore (#26)	2 months ago
CLI.md	Expand documentation on CLI and workflows (#130)	21 days ago
CONTRIBUTING.md	Add help wanted label to contrib (#219)	12 days ago
LICENSE.txt	Initial commit	3 months ago
Makefile	Add kibana-push command (#38)	2 months ago
NOTICE.txt	Generate linted .ts in package (#49)	2 months ago
PHILOSOPHY.md	Edits to documentation	2 months ago
README.md	Fix NOTICE.txt typo	15 days ago
requirements.txt	Fix kibana-upload and remove cumbersome dataclasses (#216)	8 days ago