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

Jhon Masschelein
Principal Solutions Architect

/me

Jhon Masschelein
Jhon@Elastic.co

Elastic	Principal Solutions Architect (3,5y)
Microsoft Azure	Solution Architect Data&A.I. (3y)
Hortonworks	Solution Engineer (2y)
SurfSara	HPC DevOps Engineer (5y)
Silicon Graphics	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)²

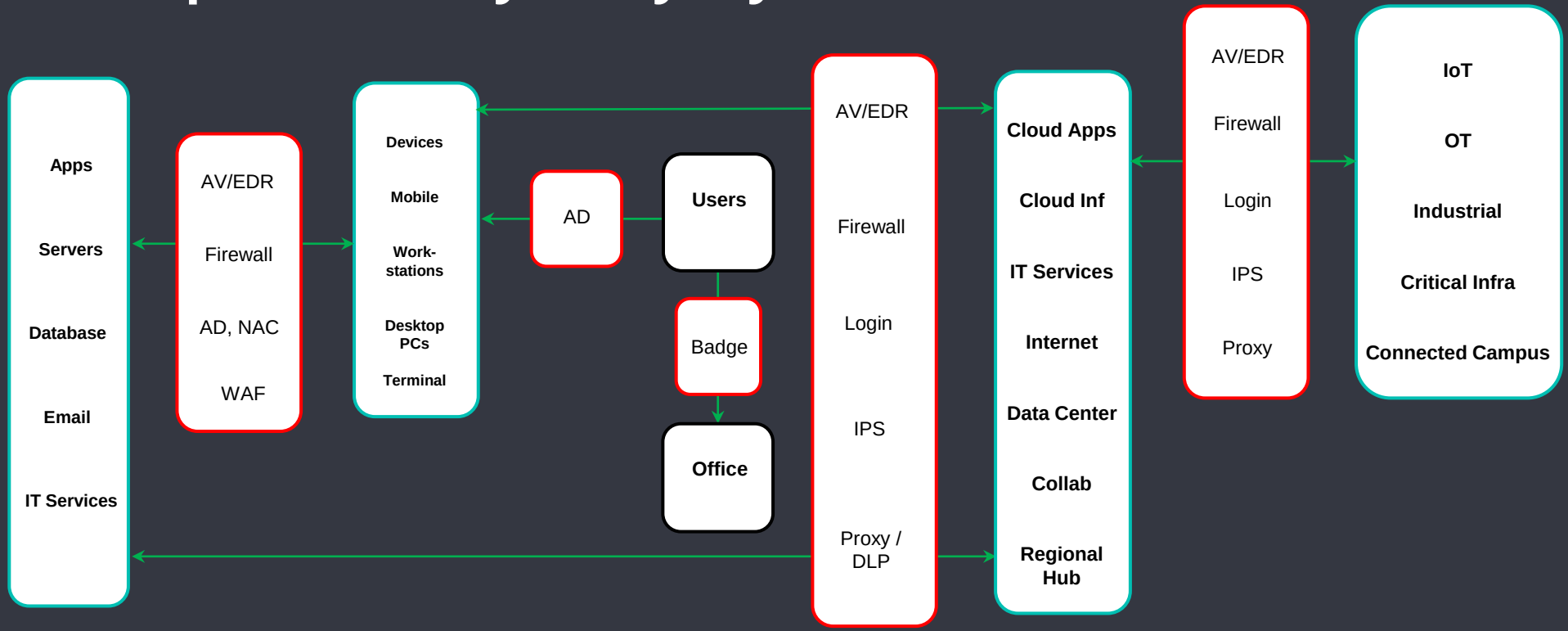
Cyber attacks and fraudulent activities are increasing

15%
Annual cybercrime growth through 2025

$205B+
Online fraud losses in the next five years

64%
Organizations affected by cyber shortage

IT/Ops & Security everyday Interactions

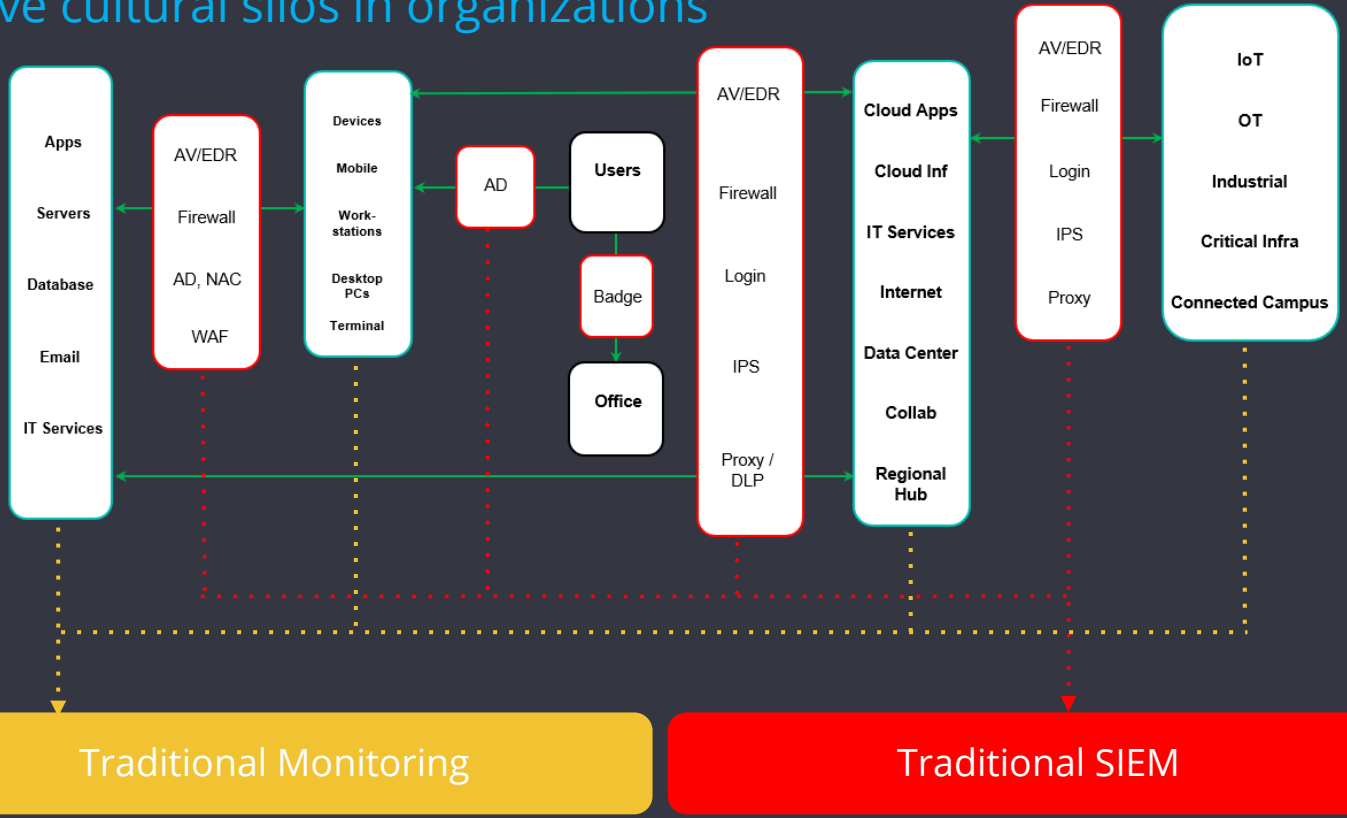


Red = Security (Enforcing)
Green = IT (Enabling)

elastic

Technology data silos

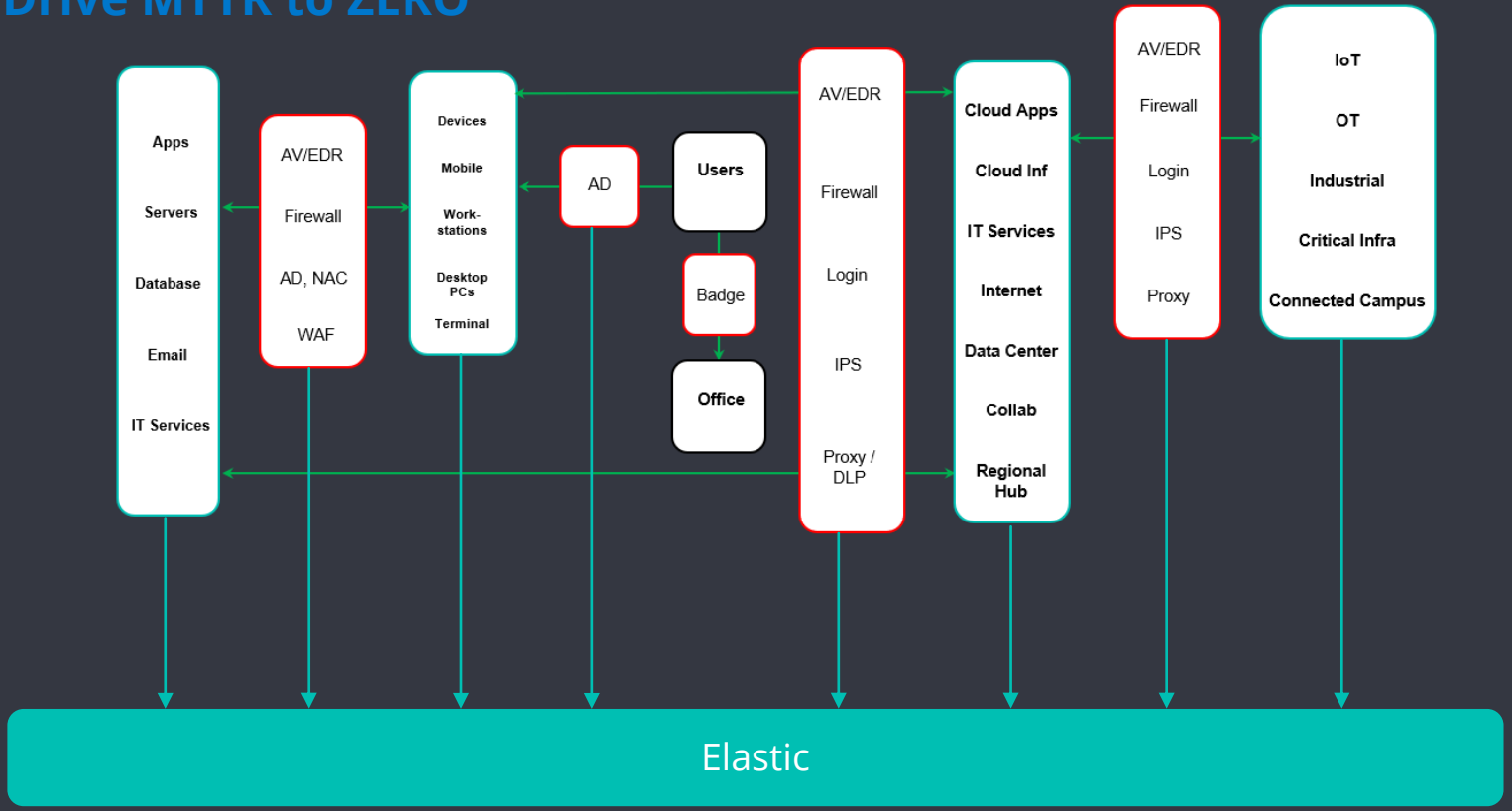
That drive cultural silos in organizations



elastic

Single, unified, powerful platform

To Drive MTTR to ZERO

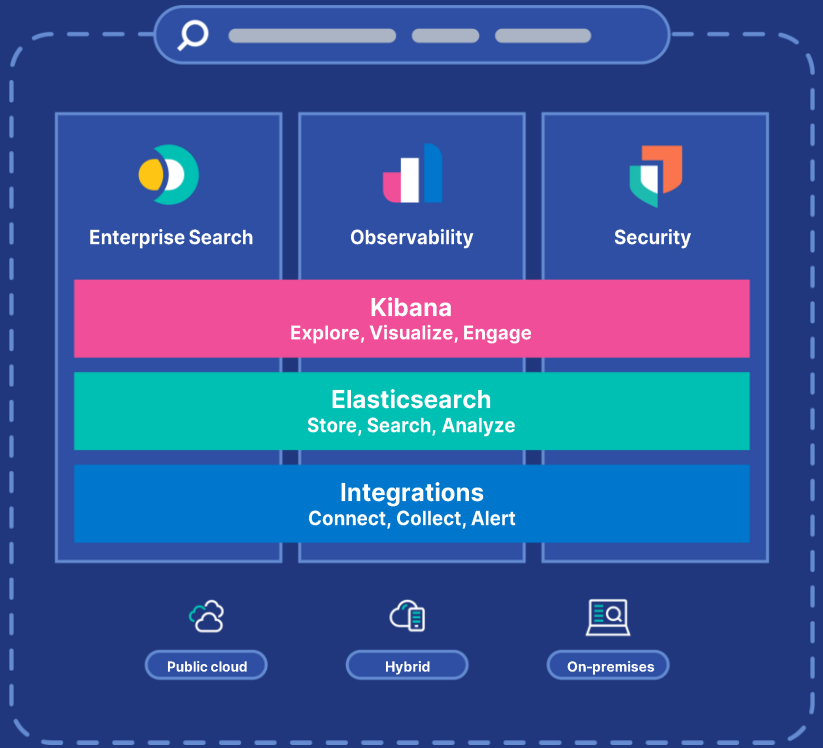


elastic

Benefits

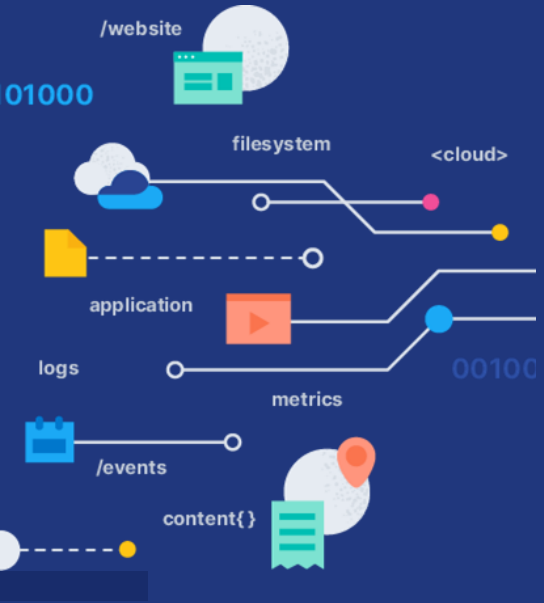
- Avoid data duplication
- Improve shared communication
- Reduce operating frictions
- Reduce costs while keeping services **up** and our organizations **secured**

The Elastic Search Platform



elastic

The Elastic Search Platform



Enterprise Search

Observability

Security

Kibana
Explore, Visualize, Engage

Elasticsearch
Store, Search, Analyze

Integrations
Connect, Collect, Alert

Public cloud

Hybrid

On-premises

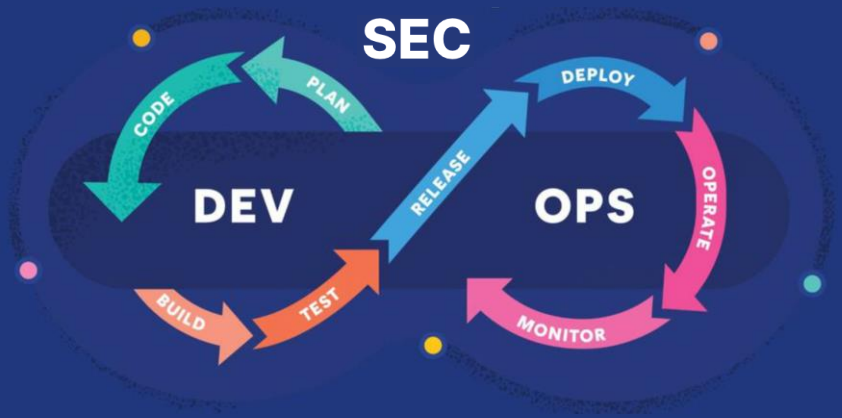
elastic

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

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

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

Quickly investigate and take recommended actions

Visualise the entire CICD 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

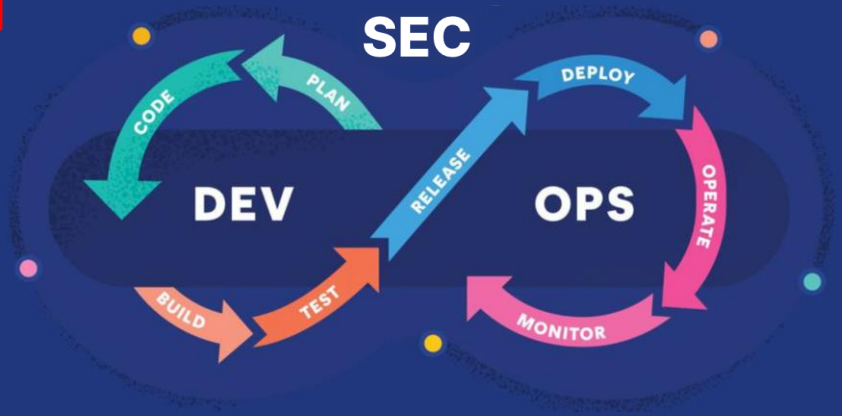
elastic

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

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

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

Quickly investigate and take recommended actions

Visualise the entire CICD 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

elastic

Limitless XDR

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

SIEM

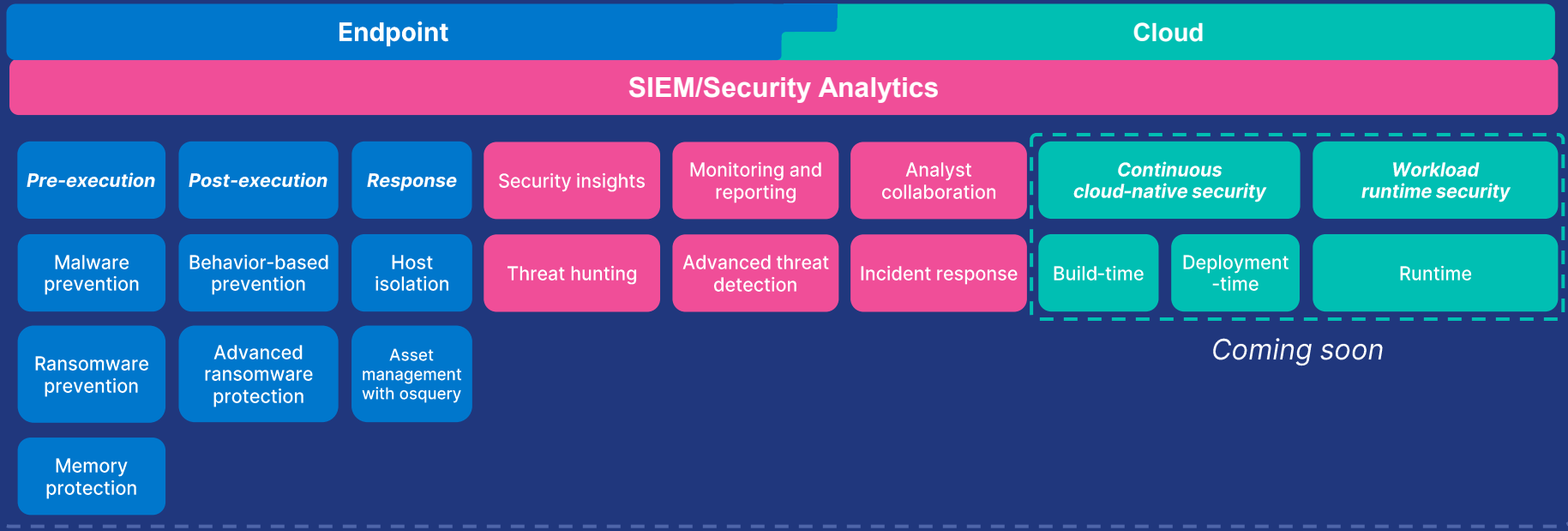
Endpoint Security

Cloud Security

elastic

Elastic Security

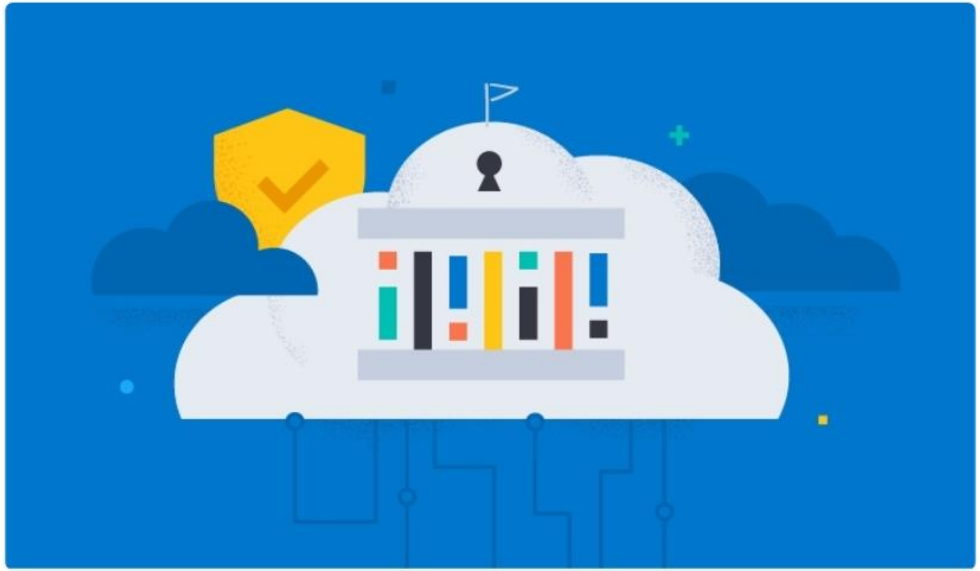
Security without Limits



Elastic Security

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

elastic

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

elastic

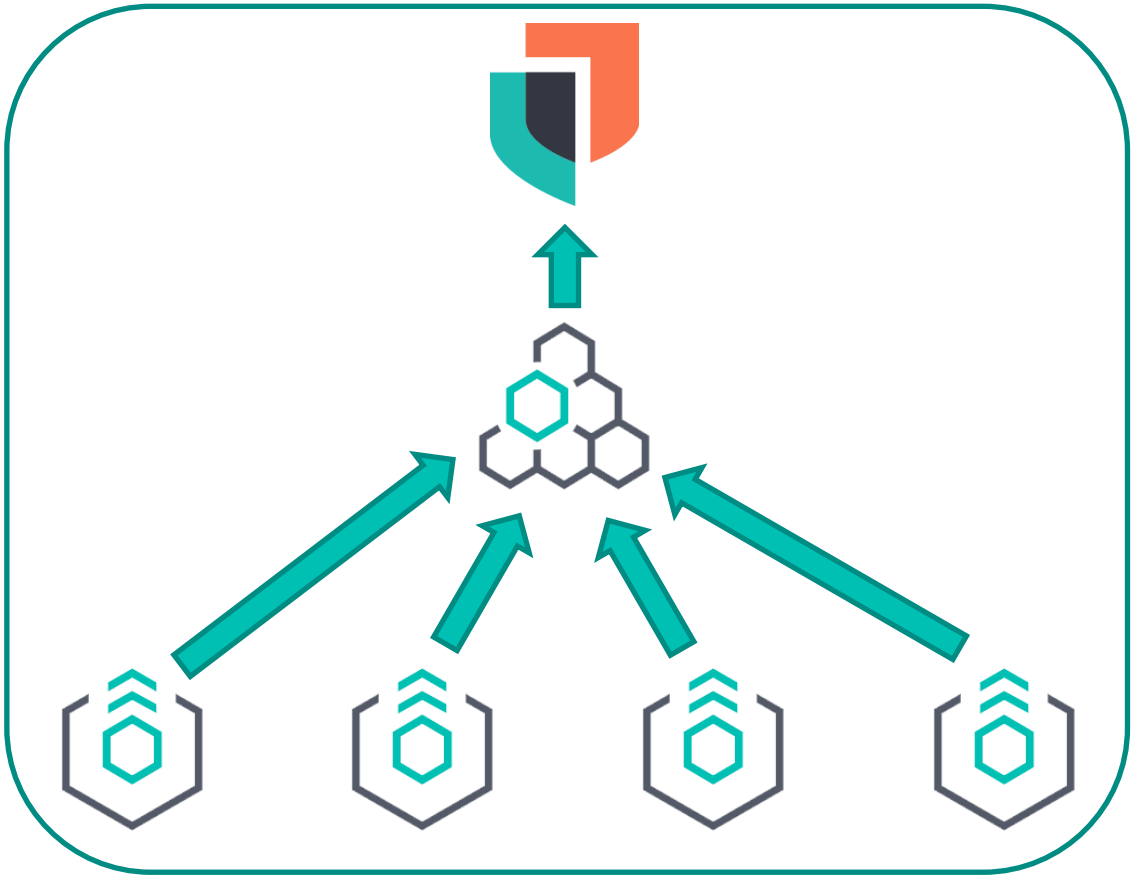
Scalability

Elastic Deployment

Elastic Fleet

Elastic Agent

Single Department



Network A

elastic

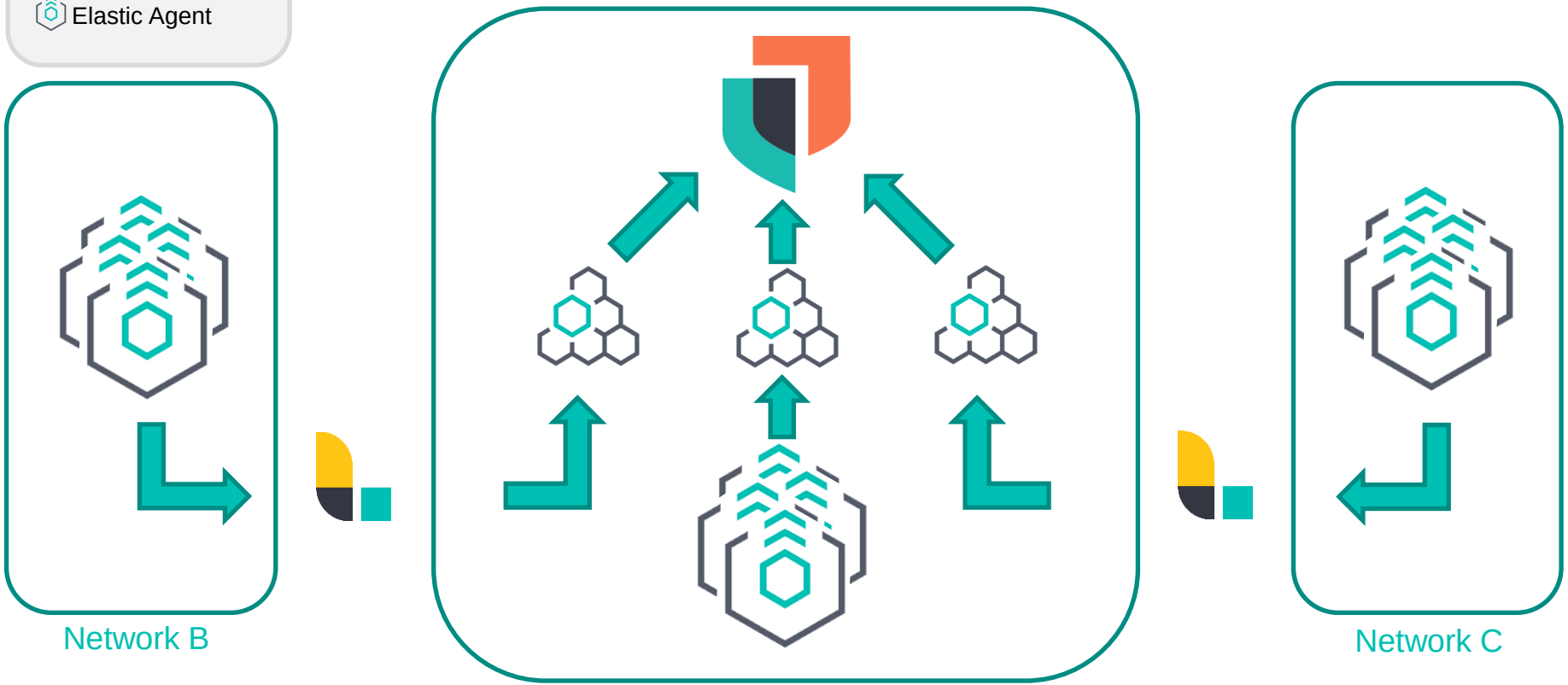
Elastic Deployment

Elastic Fleet

Elastic Agent

Elastic Logstash

Single Organization – Multiple Departments



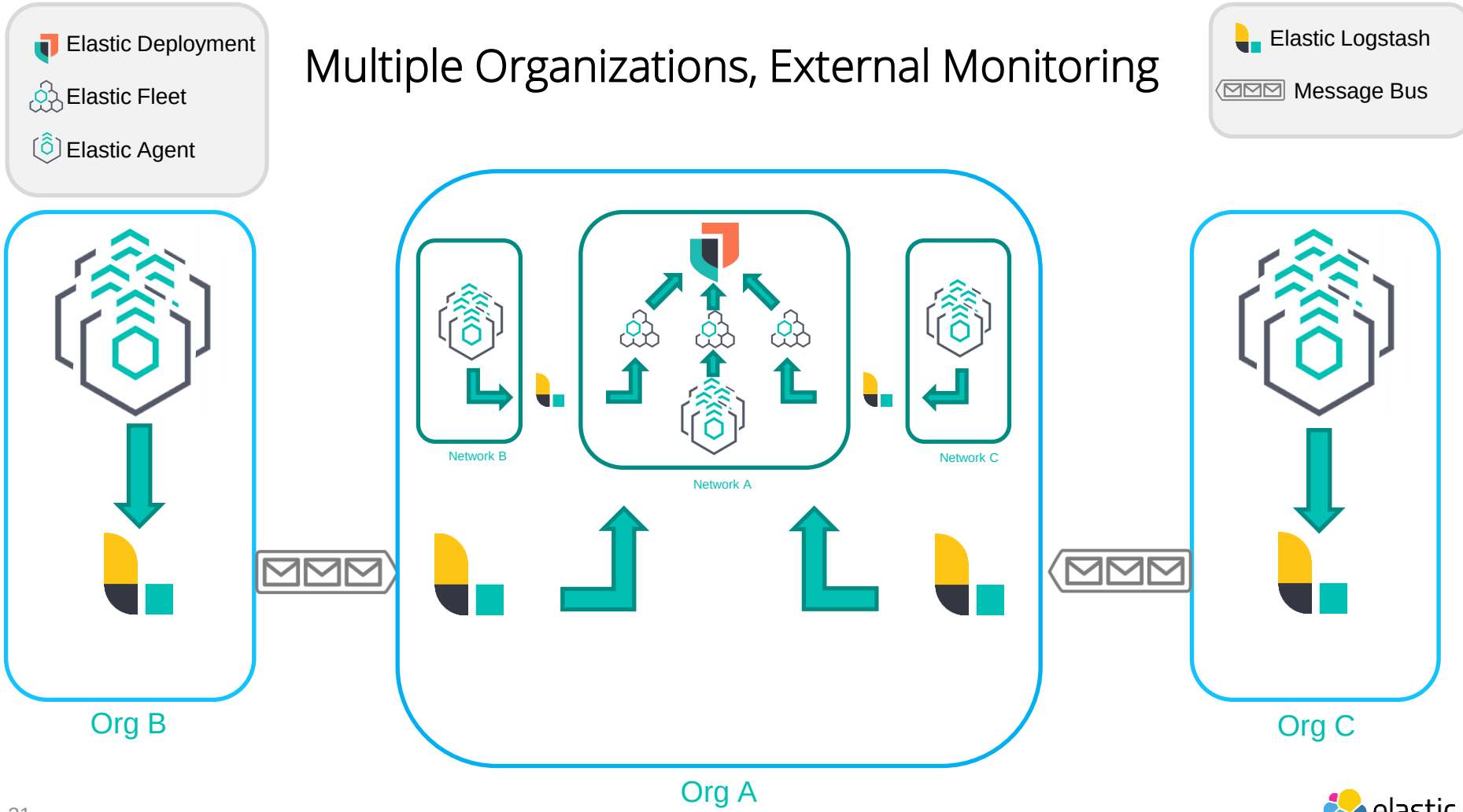
Network B

Network A

Network C

elastic

Multiple Organizations, External Monitoring

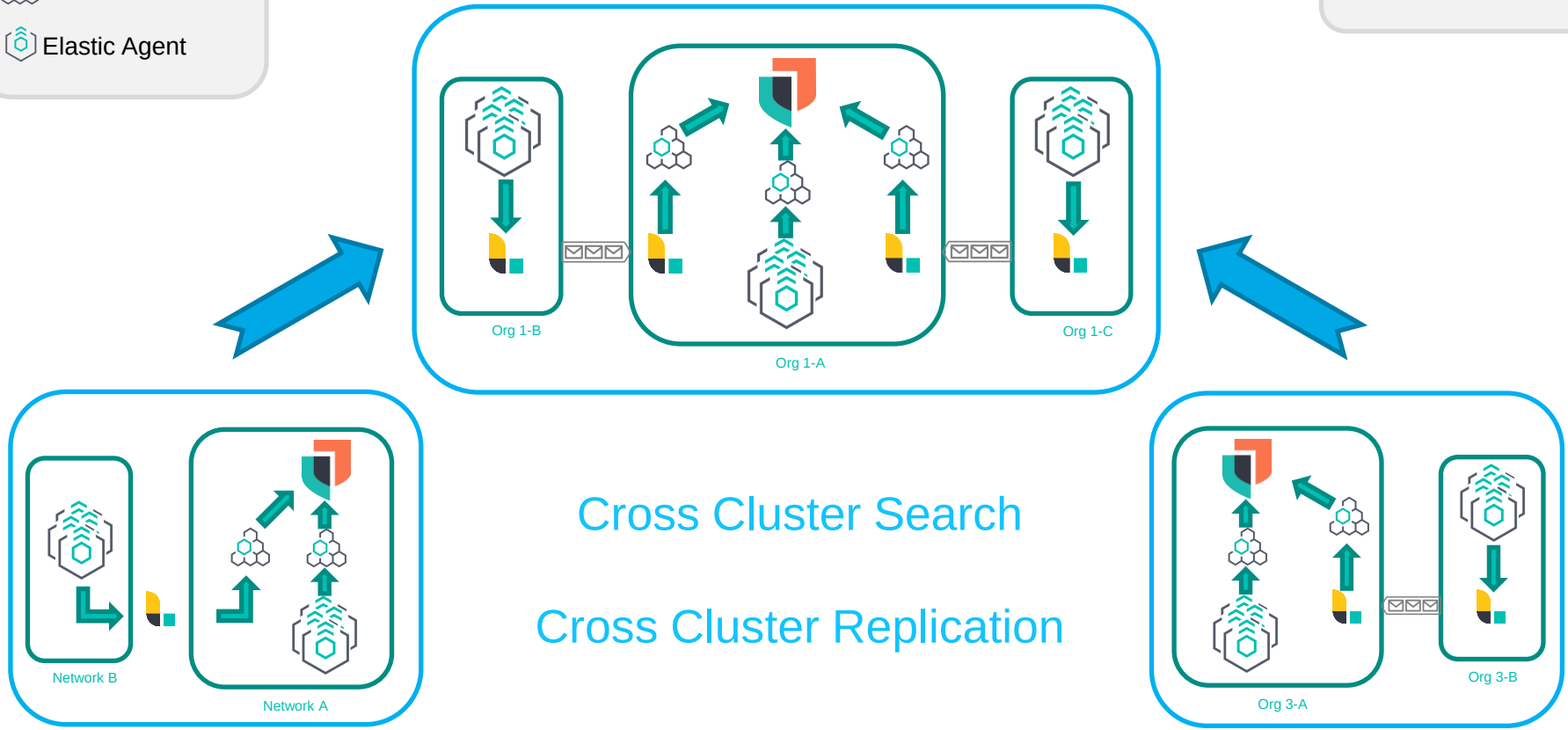


elastic

Decentralized Deployment

Elastic Deployment
Elastic Fleet
Elastic Agent

Elastic Logstash
Message Bus



Cross Cluster Search

Cross Cluster Replication

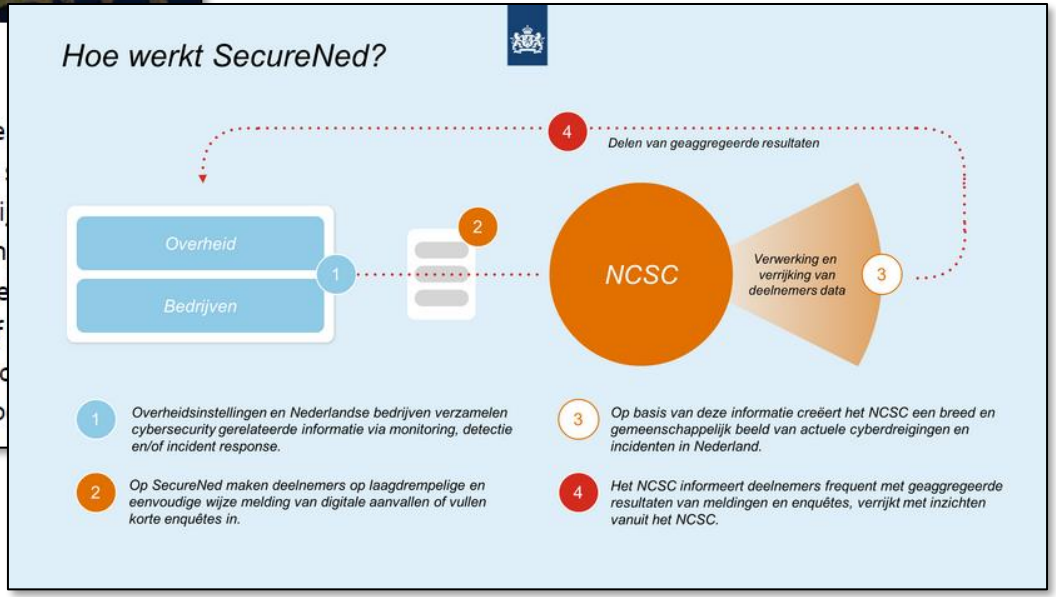
elastic

Examples

Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Nederlandse instellingen, bedrijven en burgers krijgen steeds vaker te
cybercriminaliteit en digitale dreigingen. Omdat we Nederland alleen
veilig kunnen houden werkt het NCSC samen met overheden en bedri
SecureNed. Een uniek samenwerkingsverband gericht op het onderlin
informatie over cyberdreigingen en incidenten. Op basis van de gedee
kunnen deelnemers maatregelen nemen om schade te voorkomen of
SecureNed maakt deze informatiedeling eenvoudig, effectief, maar oc
wat vandaag een incident is bij de één, is een goede waarschuwing vo

SecureNed | Nationaal Cyber Security Centrum (ncsc.nl)



Beeld: ©NCSC

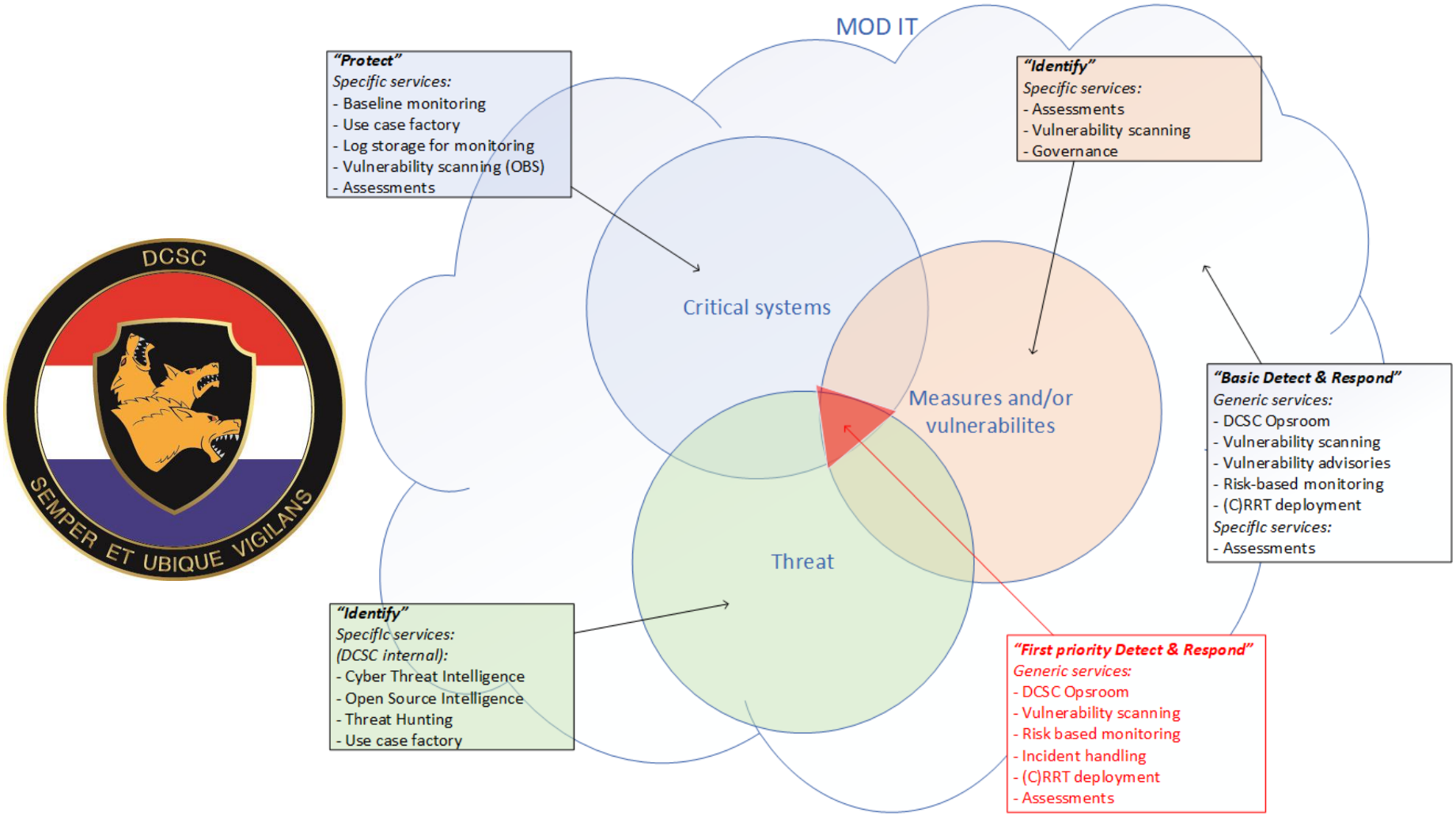
elastic

Ministerie van Defensie

Our approach to vulnerabilities

a company wide responsibility

Defensie Cyber Security Centrum


MOD IT
"Protect"
Specific services:
- Baseline monitoring
- Use case factory
- Log storage for monitoring
- Vulnerability scanning (OBS)
- Assessments
"Identify"
Specific services:
- Assessments
- Vulnerability scanning
- Governance
Critical systems
Measures and/or vulnerabilites
Threat
"Basic Detect & Respond"
Generic services:
- DCSC Opsroom
- Vulnerability scanning
- Vulnerability advisories
- Risk-based monitoring
- (C)RRT deployment
Specifc services:
- Assessments
"Identify"
Specifc 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
DCSC
SEMPER ET UBIQUE VIGILANS

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-obser

[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-threathunting-cloud-posture

[March 7-9, 2023] [Online, Free] ElasticON Global
https://www.elasticon.com/event/e473ab1b-88b4-4326-aa8d-e6054a566e48/summary

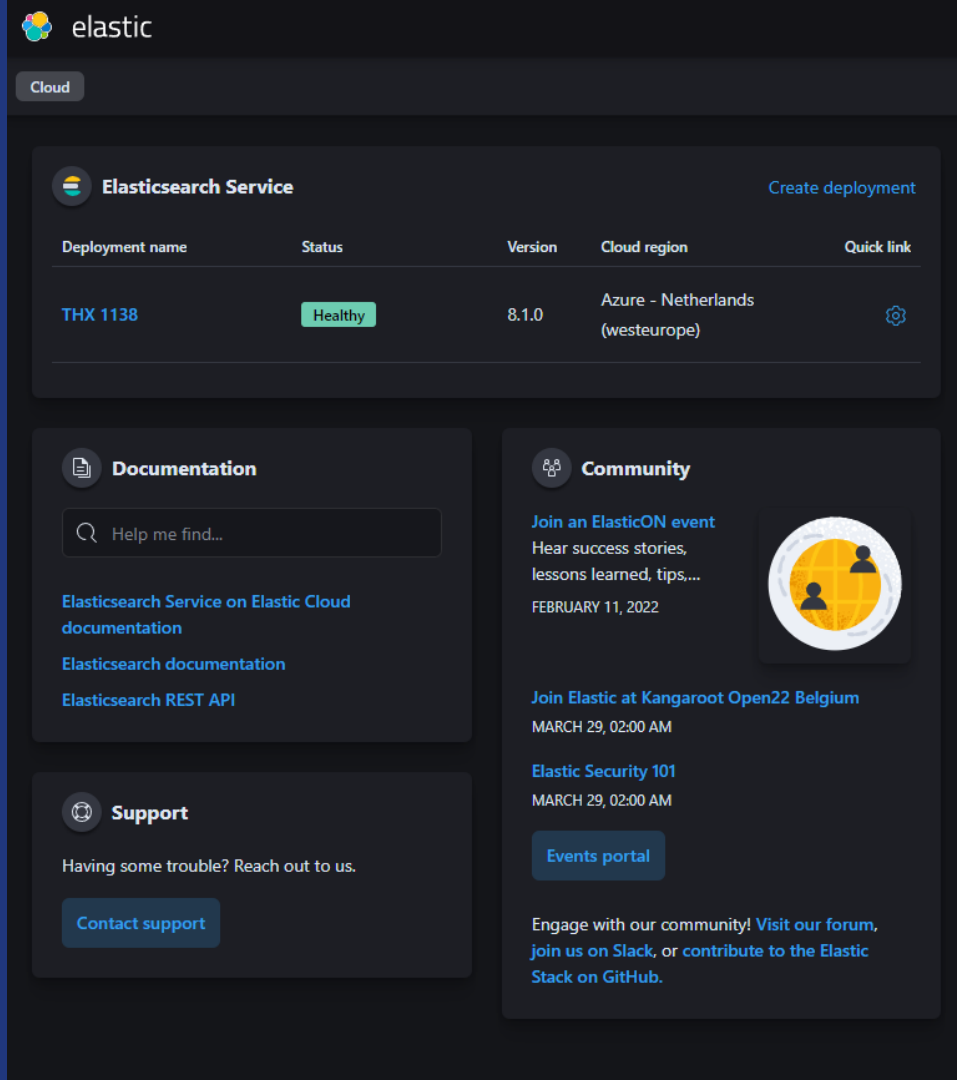
Try out the latest and greatest Elastic capabilities for free wit

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

elastic

Questions?

cloud.elastic.co



Extra Slides

Deploy your way, anywhere

Select a deployment model for your unique needs

Self-Managed

Install a single package

Elastic Cloud Enterprise

Elastic Cloud on Kubernetes

Centrally manage multiple deployments on your infra

Elastic Cloud

Deploy instantly on AWS, Azure or Google Cloud

aws

Microsoft Azure

Federate across these deployments with cross-cluster search

elastic

Unified Data Collection

Single Agent

100s of integrations

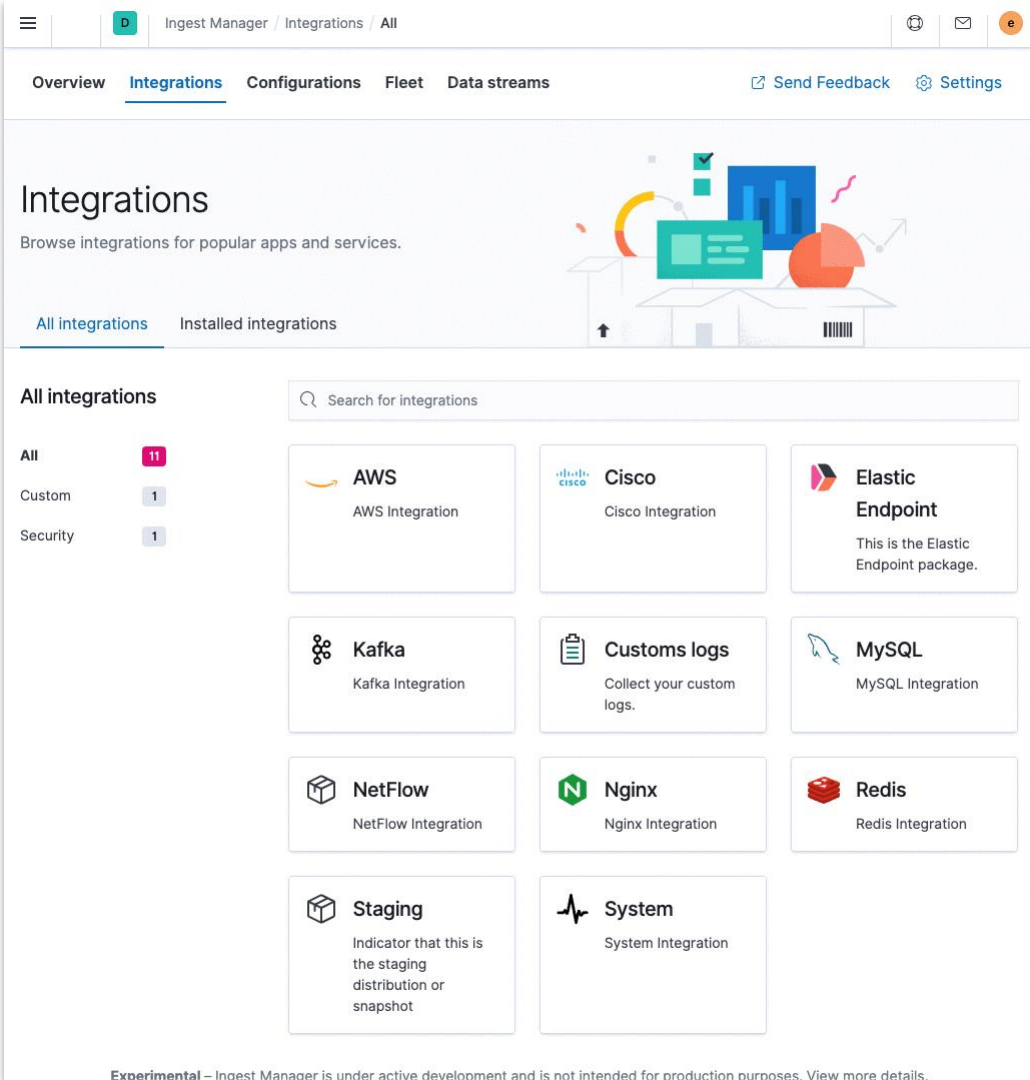
Go from data to dashboard in minutes

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



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
```

elastic

Unified RBAC

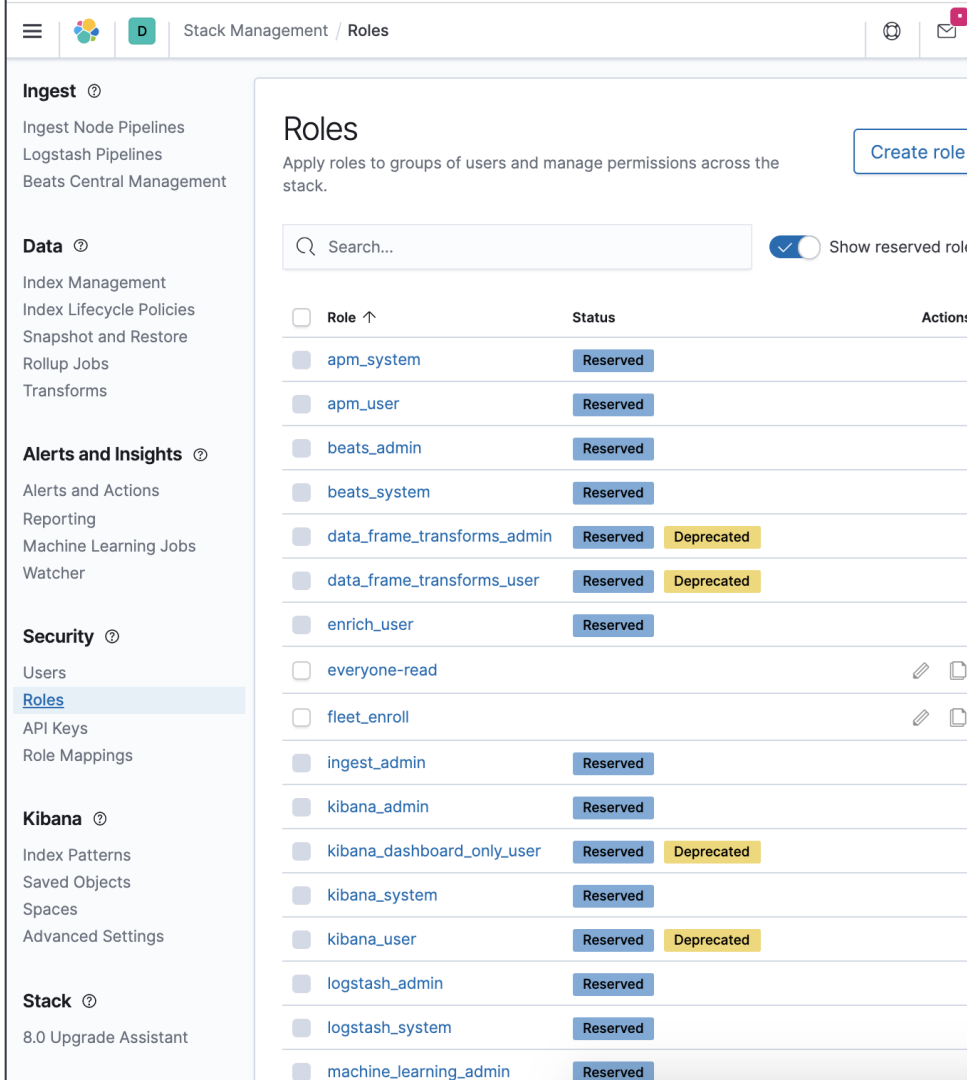
Advanced data-level security

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

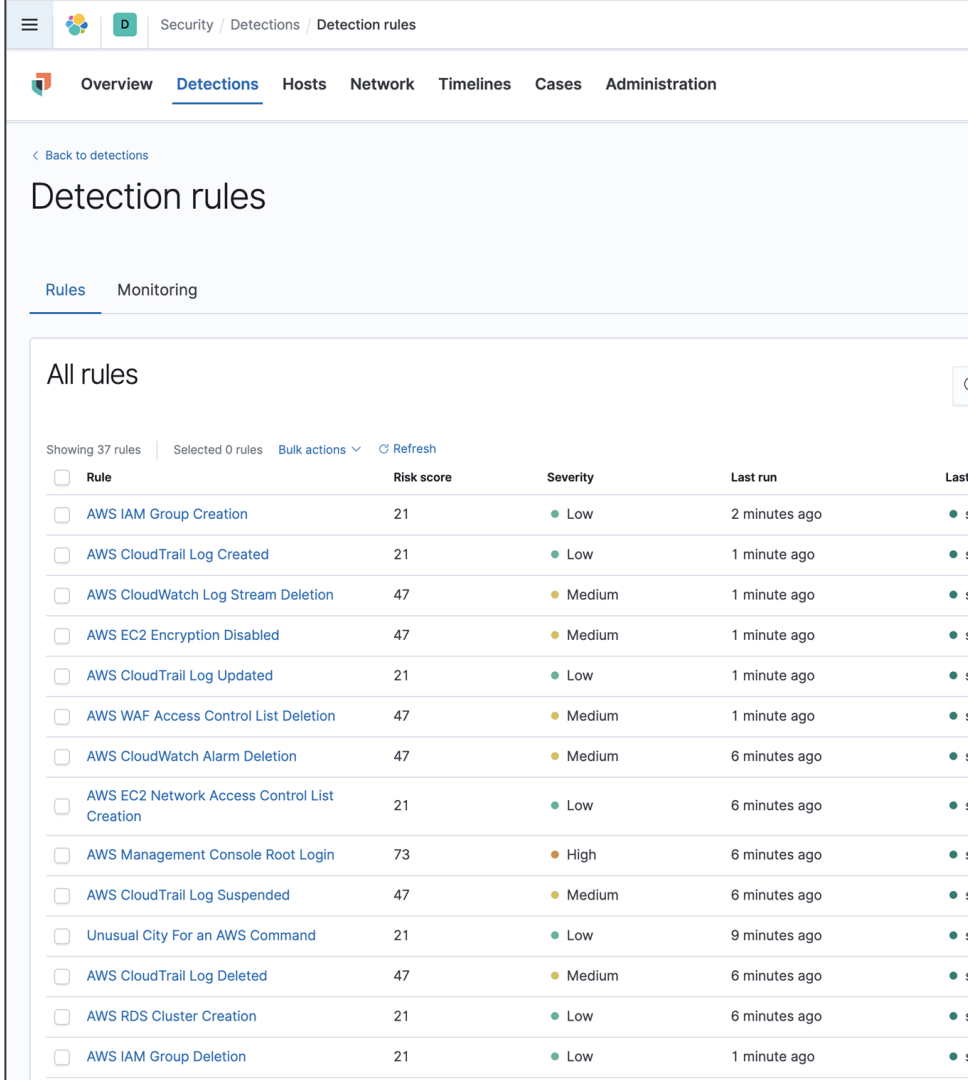
Powered by the Elastic stack

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**



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