Breaking silos between DevOps and SecOps

Moises Cosio
Principal Product Manager

IT/Ops and Security shared challenges

129

Apps Deployed

Within organizations to run everyday operations

45%

IT Spending

In cloud Infrastructure Hybrid is the new normal

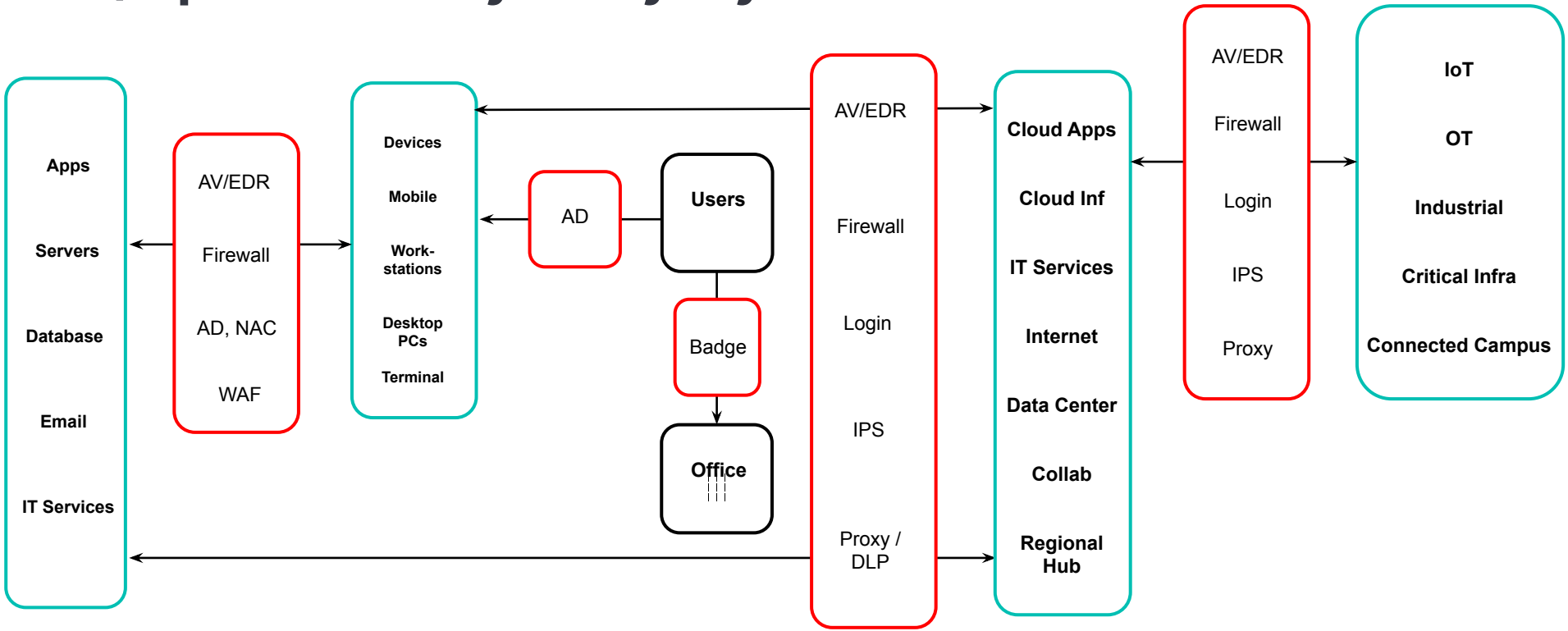
24×7

Global Operations

Pushing continuous delivery and higher agility

elastic

IT/Ops & Security everyday Interactions

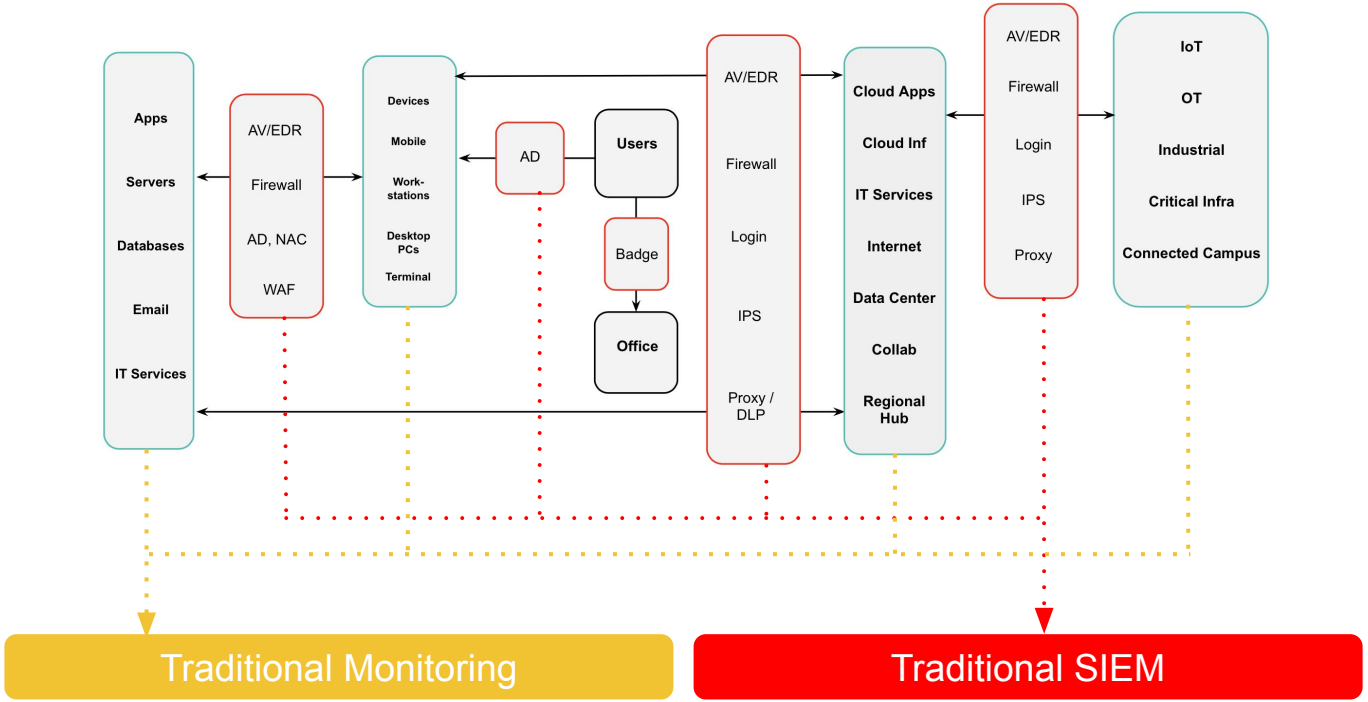


Red = Security (Enforcing)
Green = IT (Enabling)

elastic

Technology data silos

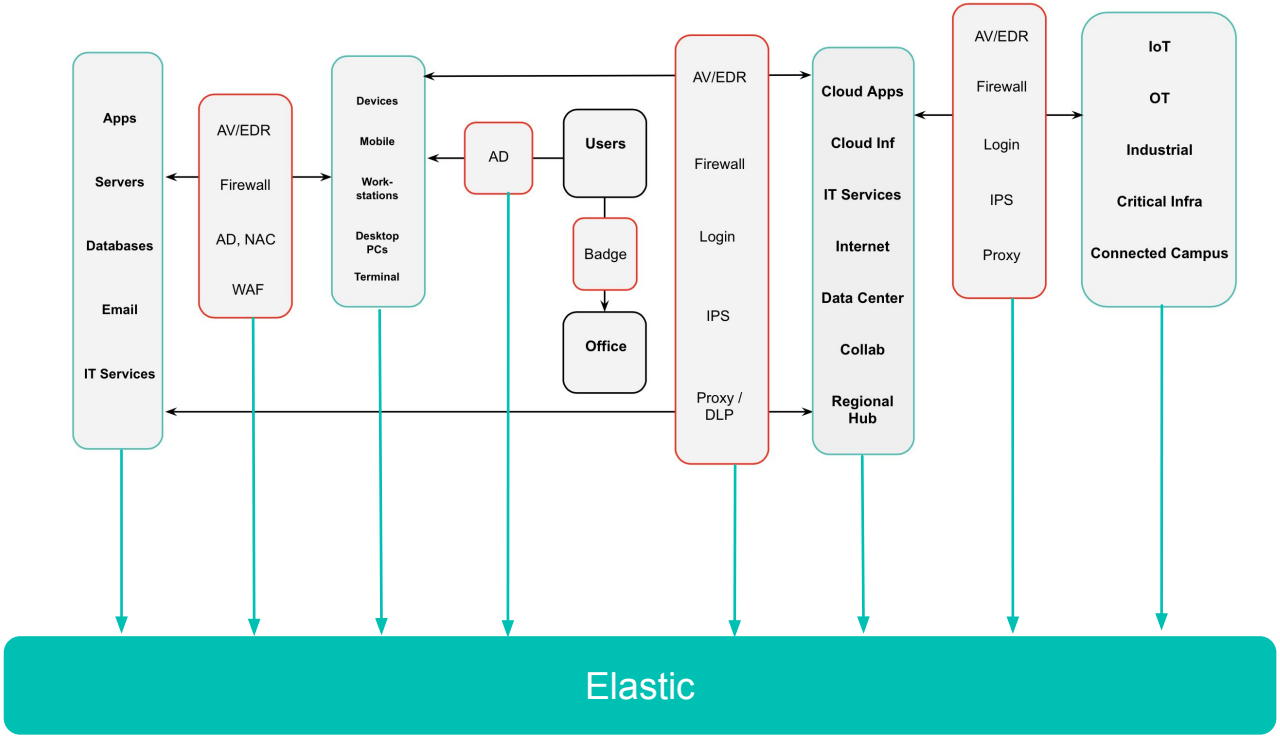
That drive cultural silos in organizations



elastic

Single, unified, powerful platform

To Drive MTTR to ZERO



Benefits

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

Demo

Observability + Security in Elastic Stack

+

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

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

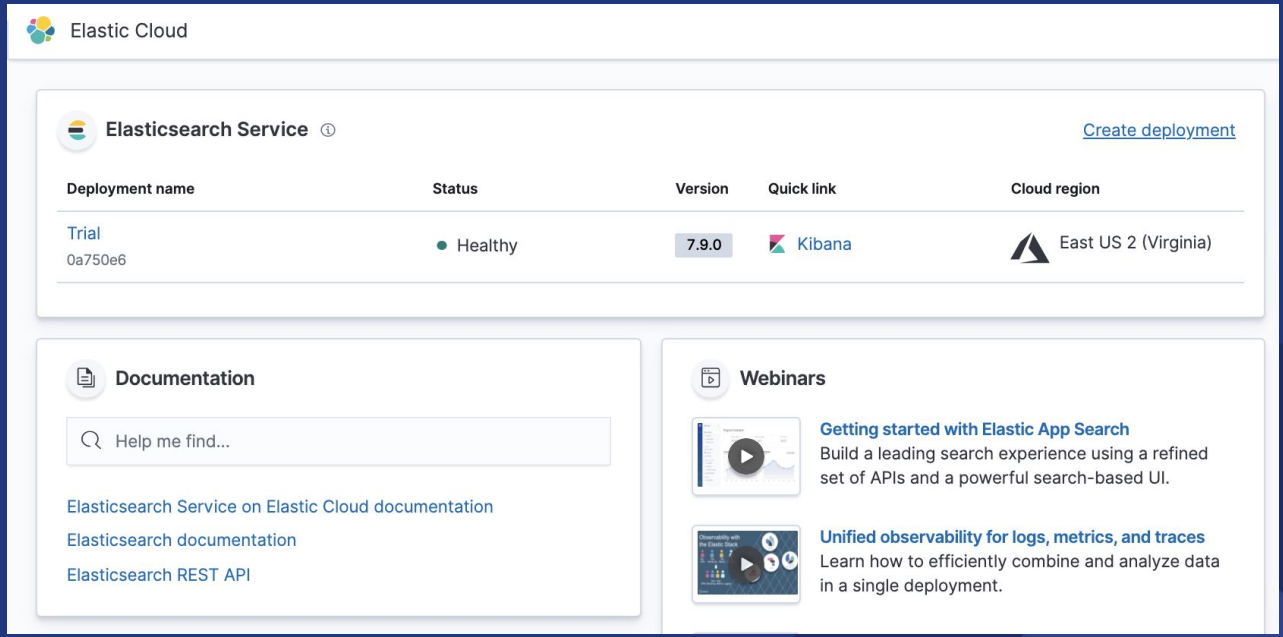
Federate across these deployments with cross-cluster search

elastic

See it for yourself

Try in Elastic Cloud

cloud.elastic.co



elastic

Supporting slides

Observability + Security in Elastic Stack

Unified User Interface	Eliminate swivel chair analysis
Unified Issue Detection	Free and open detection engine, ML, and Alerting
Unified RBAC	Secure data based on “need to know” policies
Unified Schema	Speed up analysis with cross-source correlation
Unified Data Collection	Deploy a single agent for observability and security
Deploy Anywhere	Achieve “data gravity” in hybrid environments
Observability **Security**	One powerful datastore — Elasticsearch.
One pricing model	Simplify and control spend

Unified Data Collection

Single Agent

100s of integrations

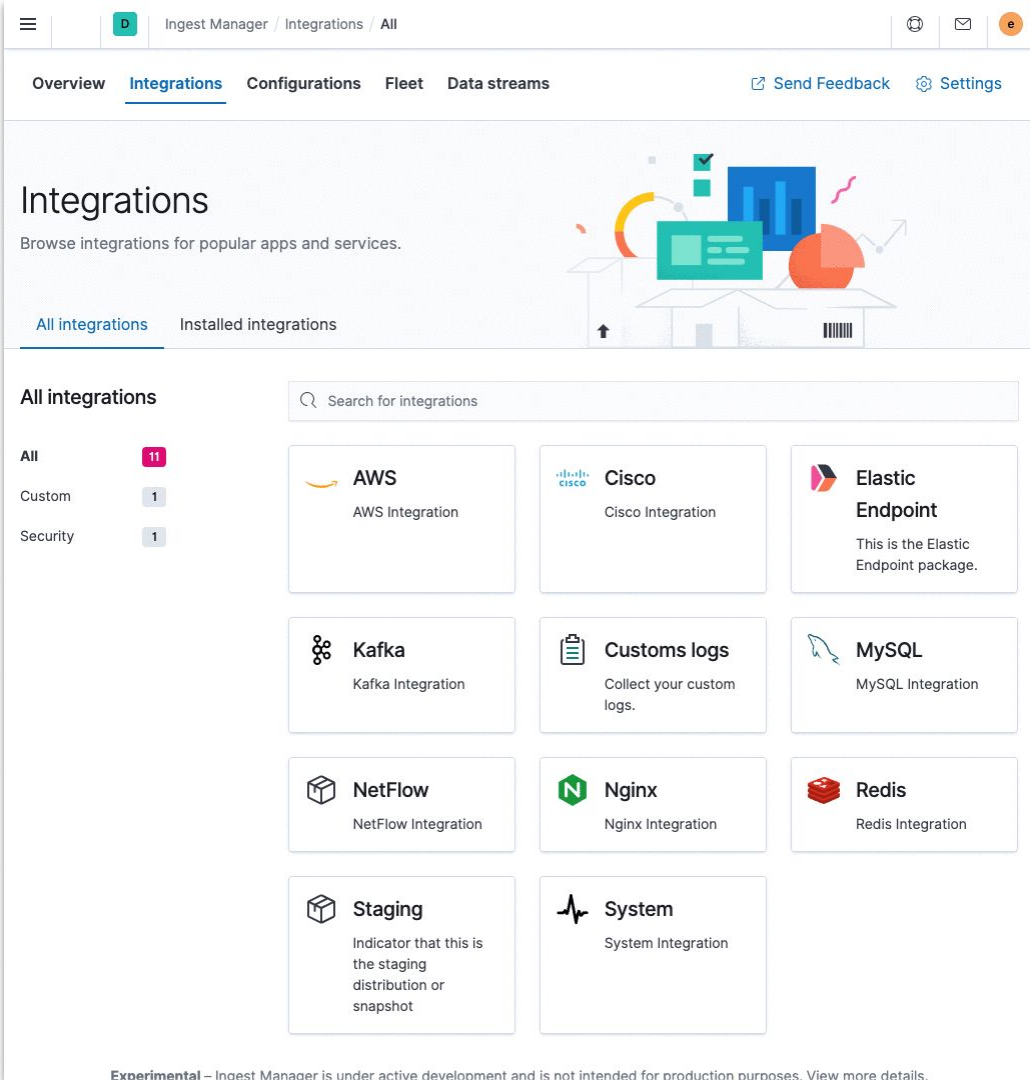
Go from data to dashboard in minutes

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

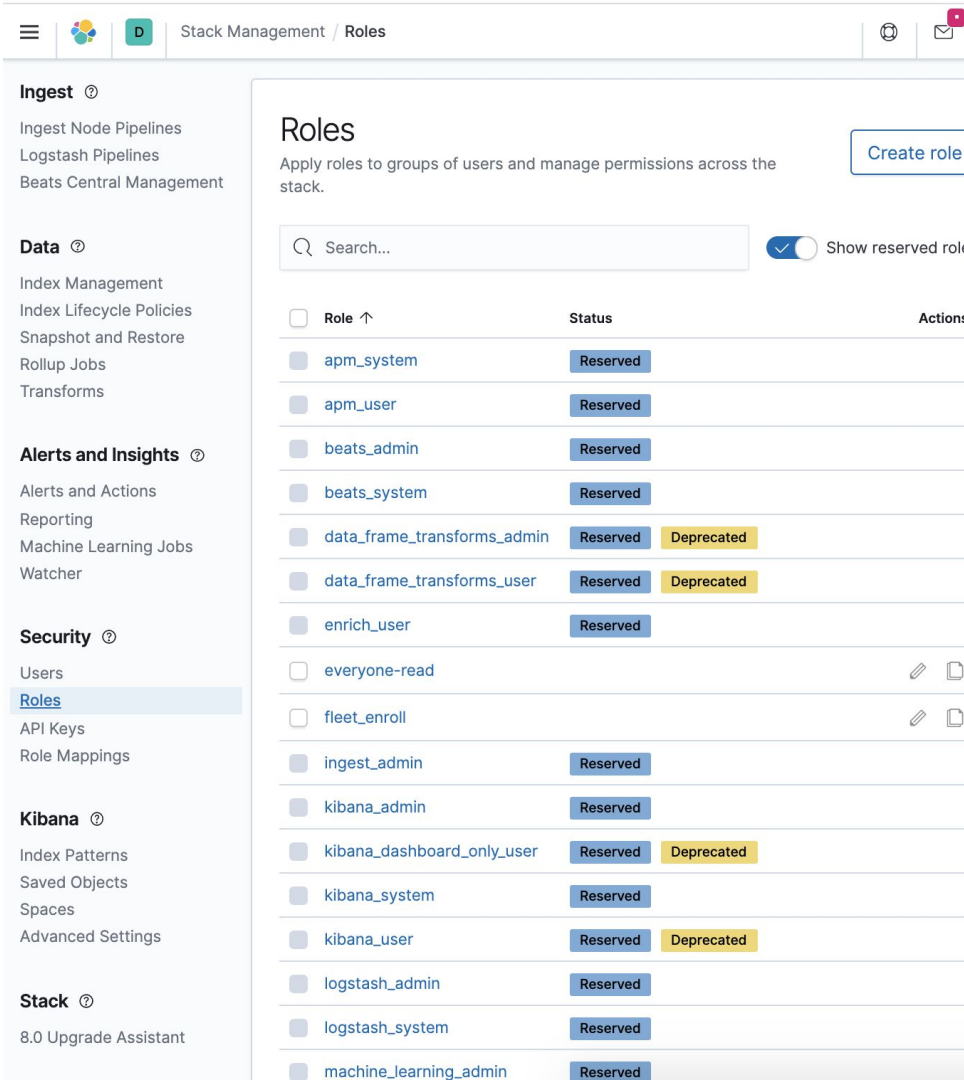
Advanced data-level security

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

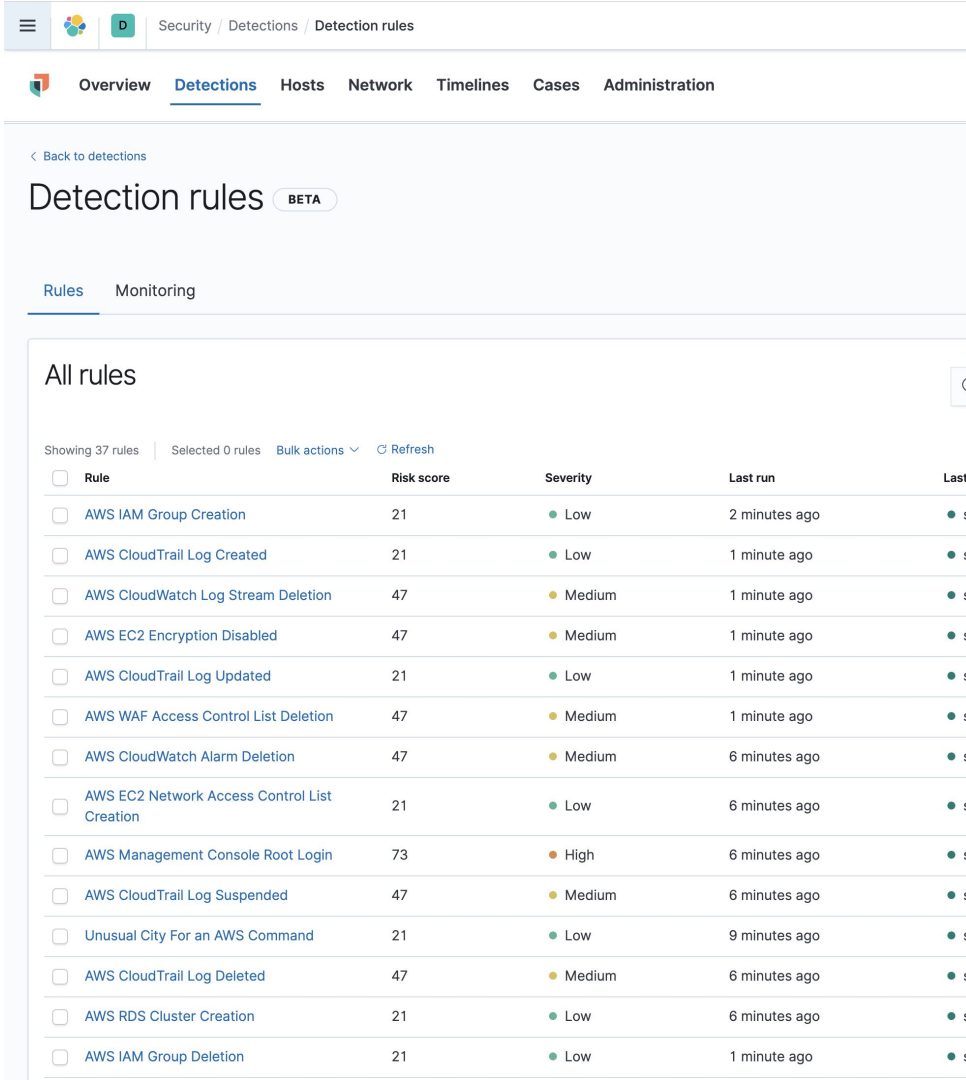
Powered by the Elastic stack

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

SecOps prebuilt rules

Cloud and SaaS

Covering main vendors and remote workforce use cases

SecOps main use cases

Leveraging infrastructure and access events for: *Access Management, Configuration validations and Network and log activity auditing*

APM events

Leveraging APM data for security detection rules, such as SQL injection attacks

elastic

Unified Issue Detection

elastic/detection-rules

Community-driven

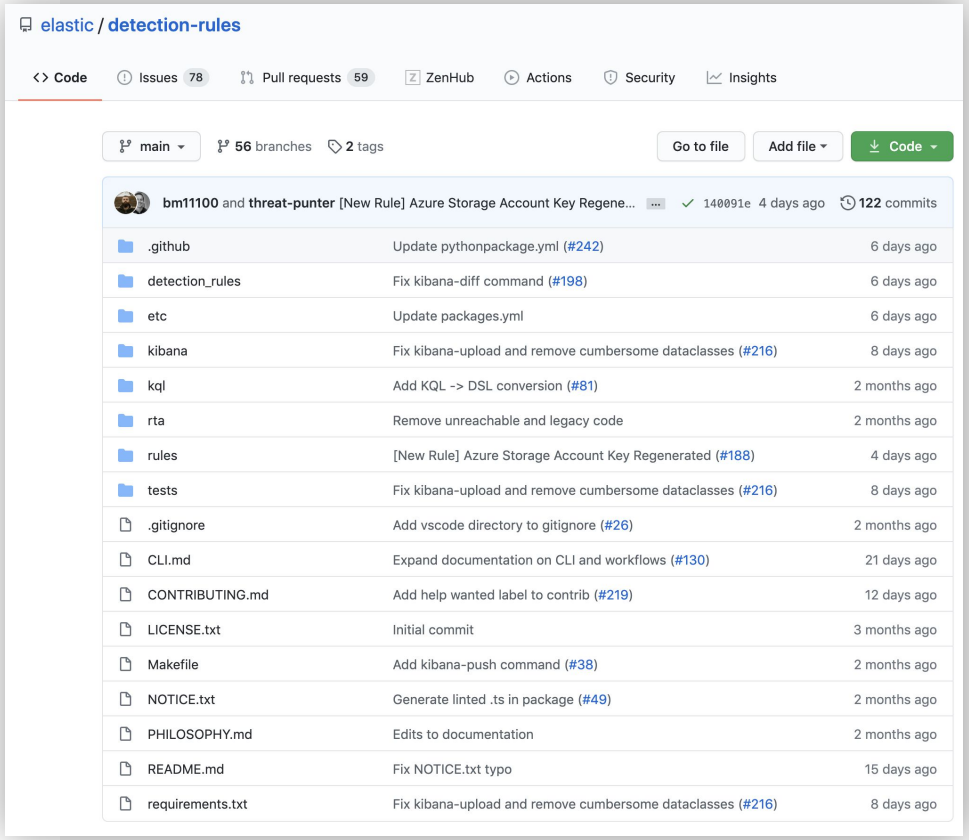
Building shared knowledge across Security and Operations communities

Always growing

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

Always available

Detections are free and under Elastic License



Unified User Interface

SecOps > Cloud > AWS