



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

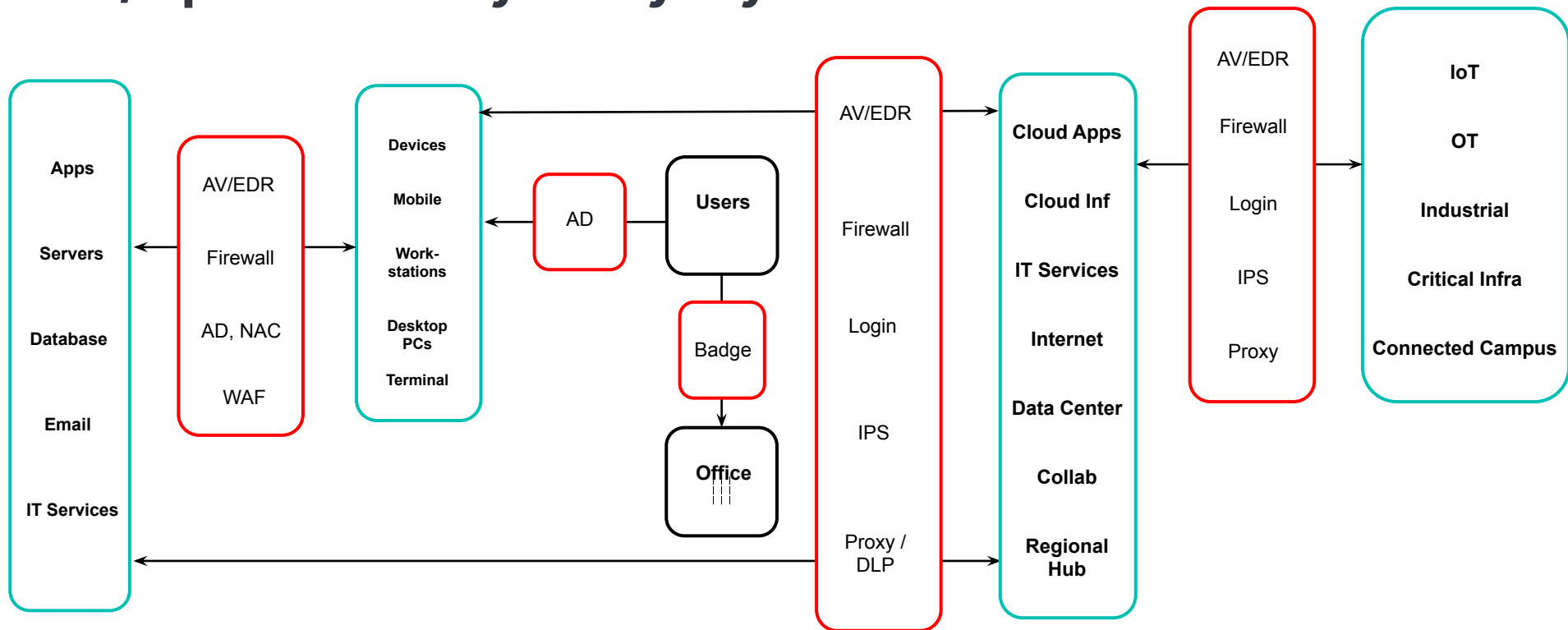
In cloud Infrastructure
Hybrid is the new
normal

24x7

Global Operations

Pushing continuous
delivery and higher
agility

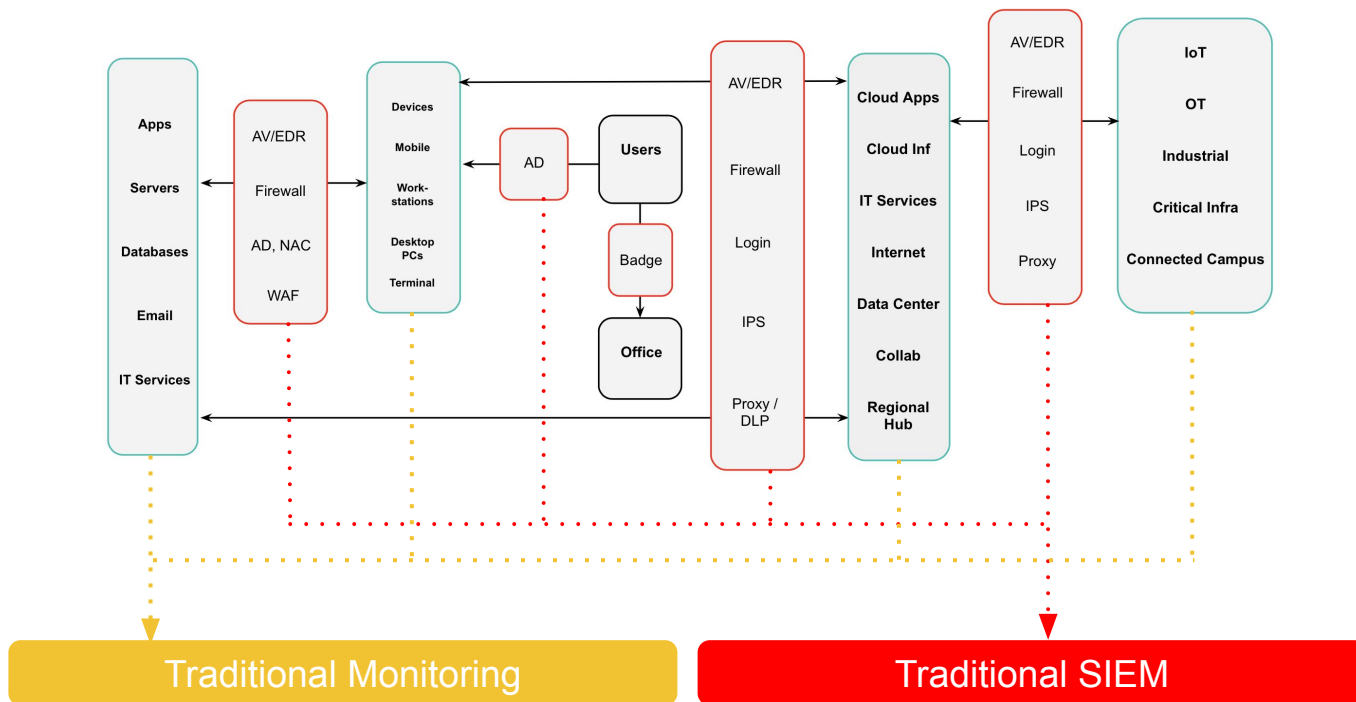
IT/Ops & Security everyday Interactions



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

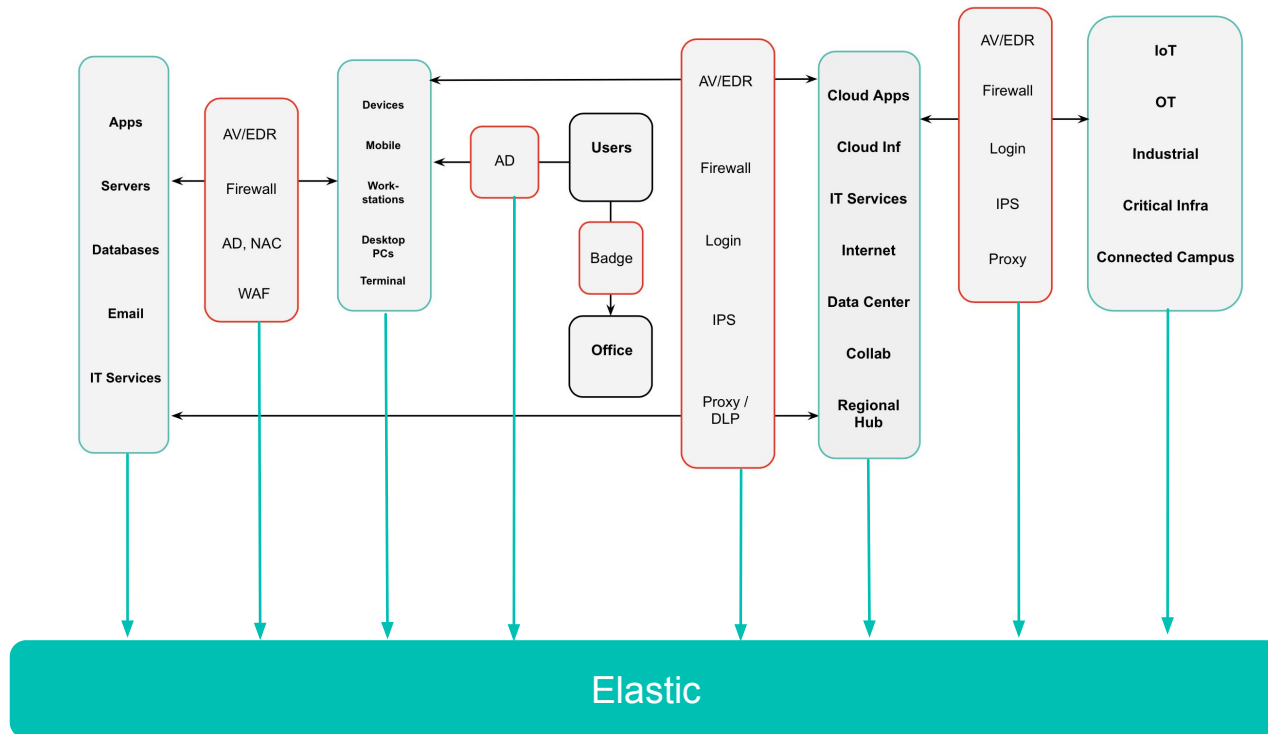
Technology data silos

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**



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

Centrally manage multiple deployments on your infra



Elastic Cloud on Kubernetes



Elastic Cloud

Deploy instantly on AWS, Azure or Google Cloud



Deploy your way, anywhere

Select a deployment model for your unique needs



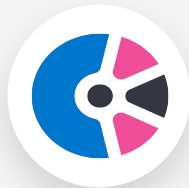
Self-Managed

Install a single package



Elastic Cloud Enterprise

Centrally manage multiple deployments on your infra



Elastic Cloud on Kubernetes



Elastic Cloud

Deploy instantly on AWS, Azure or Google Cloud

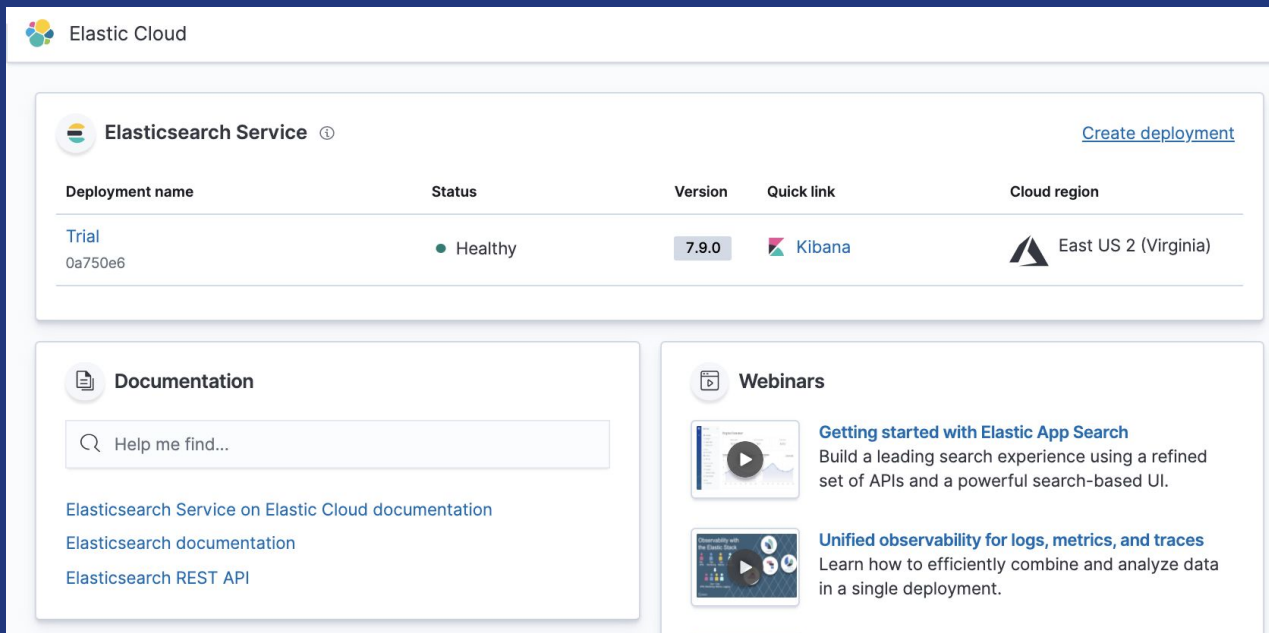


Federate across these deployments with cross-cluster search

See it for yourself


Try in Elastic Cloud



cloud.elastic.co




The screenshot displays the Elastic Cloud console interface. At the top, the 'Elasticsearch Service' is shown with a 'Create deployment' link. Below this is a table listing the deployment details. The table has five columns: Deployment name, Status, Version, Quick link, and Cloud region. A single deployment is listed with the name 'Trial' (ID: 0a750e6), a 'Healthy' status, version '7.9.0', a 'Kibana' quick link, and is located in the 'East US 2 (Virginia)' region. Below the table, there are two sections: 'Documentation' and 'Webinars'. The 'Documentation' section includes a search bar and links to 'Elasticsearch Service on Elastic Cloud documentation', 'Elasticsearch documentation', and 'Elasticsearch REST API'. The 'Webinars' section features two video thumbnails with titles: 'Getting started with Elastic App Search' and 'Unified observability for logs, metrics, and traces'.

Elastic Cloud

 **Elasticsearch Service** ⓘ [Create deployment](#)

Deployment name	Status	Version	Quick link	Cloud region
Trial 0a750e6	● Healthy	7.9.0	 Kibana	 East US 2 (Virginia)


 **Documentation**


🔍 Help me find...


[Elasticsearch Service on Elastic Cloud documentation](#)

[Elasticsearch documentation](#)

[Elasticsearch REST API](#)

 **Webinars**

 **Getting started with Elastic App Search**
Build a leading search experience using a refined set of APIs and a powerful search-based UI.

 **Unified observability for logs, metrics, and traces**
Learn how to efficiently combine and analyze data in a single deployment.

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

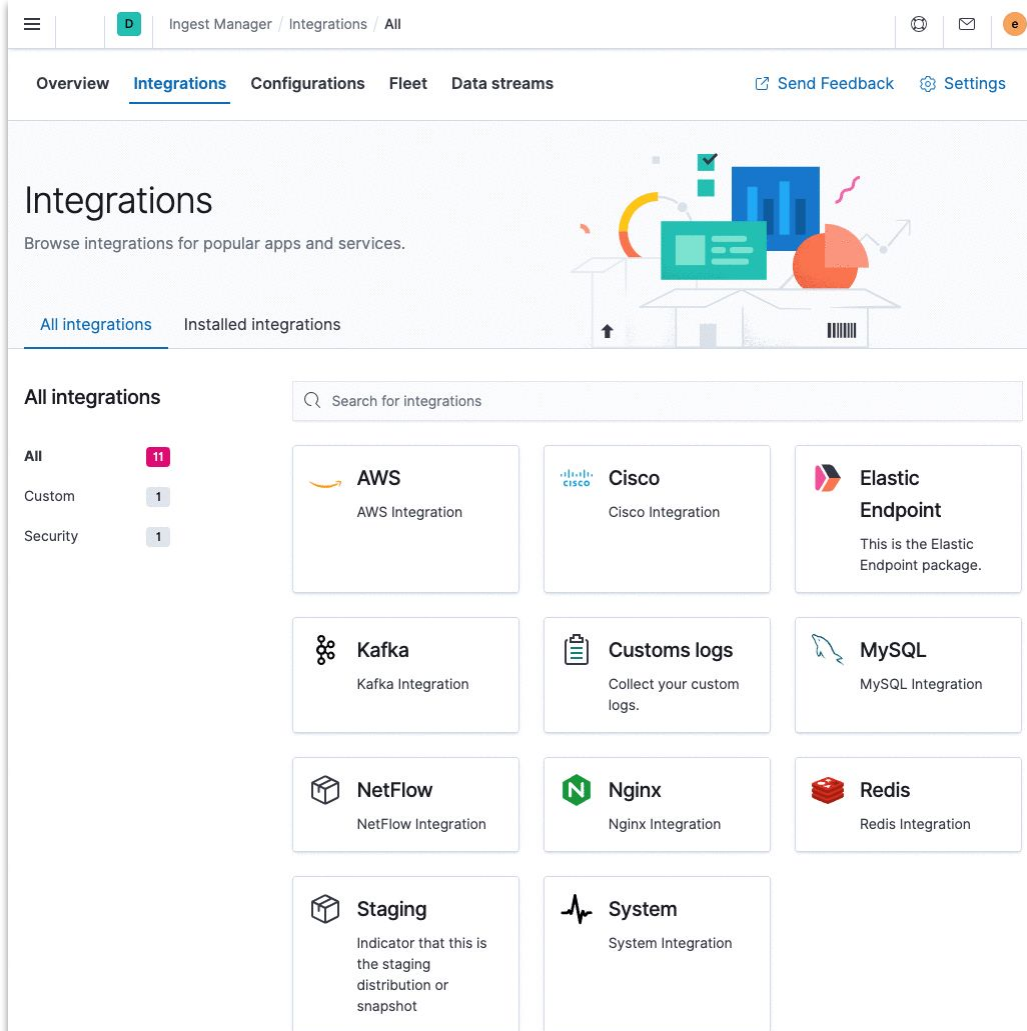
Go from data to dashboard in minutes

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



The screenshot shows the 'Integrations' page in the Ingest Manager. The top navigation bar includes 'Overview', 'Integrations' (active), 'Configurations', 'Fleet', and 'Data streams'. On the right, there are links for 'Send Feedback' and 'Settings'. The main heading is 'Integrations' with the subtitle 'Browse integrations for popular apps and services.' Below this, there are tabs for 'All integrations' (active) and 'Installed integrations'. A search bar is labeled 'Search for integrations'. On the left, a filter sidebar shows 'All' (11), 'Custom' (1), and 'Security' (1). The main area displays a grid of integration cards: AWS, Cisco, Elastic Endpoint, Kafka, Customs logs, MySQL, NetFlow, Nginx, Redis, Staging, and System. Each card includes an icon, the integration name, and a brief description.

Integrations

Browse integrations for popular apps and services.

All integrations Installed 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

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
```

Advanced data-level security

- Powerful RBAC, ABAC
- Document level security
- Field level security
- Encryption at rest/transit
- Audit logging
- SSO (SAML, OIDC)
- CIS hardening
- Vulnerability Scanning

HIPAA
CSA Star Level 2
SOC 2 Type I, II, SOC 3
ISO 27001/27107/27018
FedRAMP
GDPR compliant ops

Stack Management / Roles

Ingest

Ingest Node Pipelines
Logstash Pipelines
Beats Central Management

Data

Index Management
Index Lifecycle Policies
Snapshot and Restore
Rollup Jobs
Transforms

Alerts and Insights

Alerts and Actions
Reporting
Machine Learning Jobs
Watcher

Security

- Users
- [Roles](#)
- API Keys
- Role Mappings

Kibana

Index Patterns
Saved Objects
Spaces
Advanced Settings

Stack

8.0 Upgrade Assistant

Roles

Apply roles to groups of users and manage permissions across the stack.

Create role

Show reserved roles

<input type="checkbox"/> Role ↑	Status	Actions
<input type="checkbox"/> apm_system	Reserved	
<input type="checkbox"/> apm_user	Reserved	
<input type="checkbox"/> beats_admin	Reserved	
<input type="checkbox"/> beats_system	Reserved	
<input type="checkbox"/> data_frame_transforms_admin	Reserved	Deprecated
<input type="checkbox"/> data_frame_transforms_user	Reserved	Deprecated
<input type="checkbox"/> enrich_user	Reserved	
<input type="checkbox"/> everyone-read		
<input type="checkbox"/> fleet_enroll		
<input type="checkbox"/> ingest_admin	Reserved	
<input type="checkbox"/> kibana_admin	Reserved	
<input type="checkbox"/> kibana_dashboard_only_user	Reserved	Deprecated
<input type="checkbox"/> kibana_system	Reserved	
<input type="checkbox"/> kibana_user	Reserved	Deprecated
<input type="checkbox"/> logstash_admin	Reserved	
<input type="checkbox"/> logstash_system	Reserved	
<input type="checkbox"/> machine_learning_admin	Reserved	

Unified Issue Detection

Free and Open Detection Engine

Speed and Scale

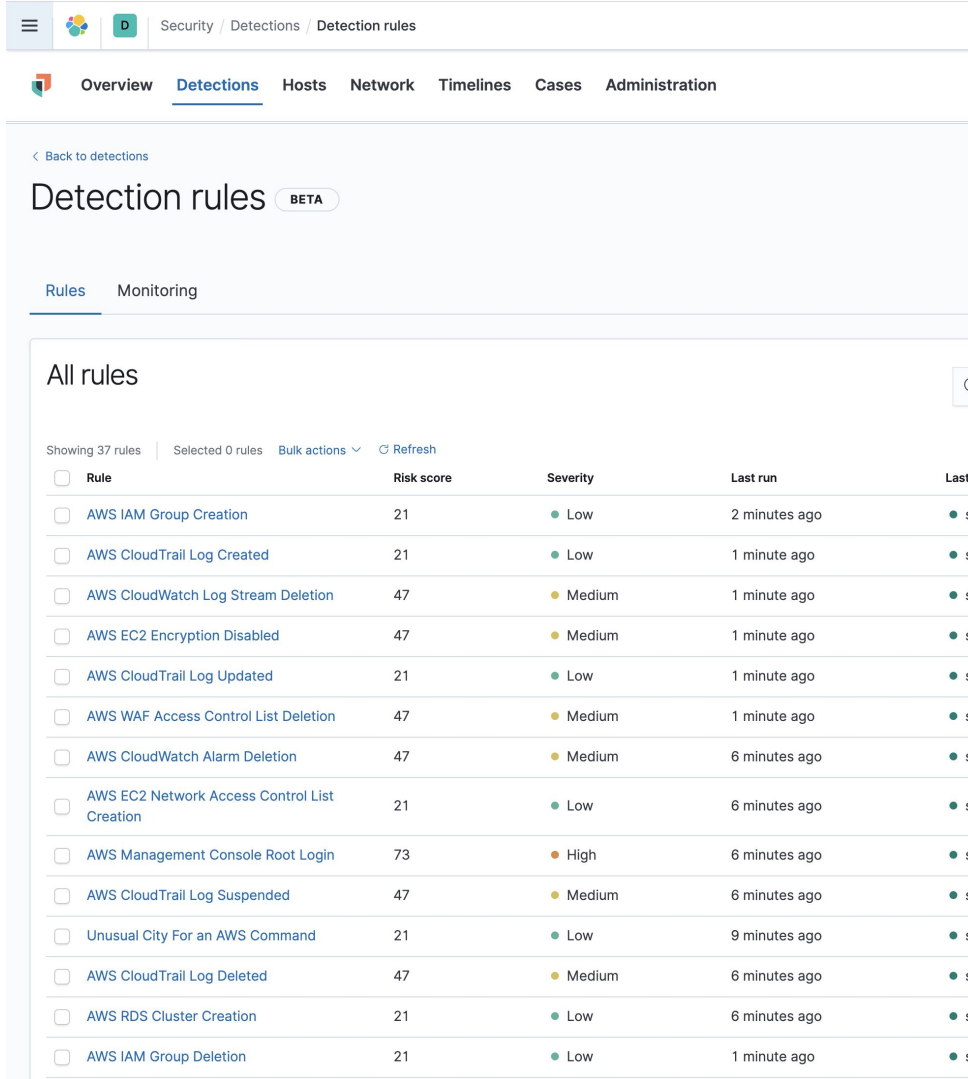
Powered by the Elastic stack

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 Elastic Security interface. At the top, there's a navigation bar with a menu icon, a logo, and a 'D' tab. Below it, a breadcrumb trail reads 'Security / Detections / Detection rules'. The main navigation bar includes 'Overview', 'Detections' (which is underlined), 'Hosts', 'Network', 'Timelines', 'Cases', and 'Administration'. Below the navigation bar, there's a '< Back to detections' link and the title 'Detection rules' with a 'BETA' badge. Under the title, there are two tabs: 'Rules' (which is underlined) and 'Monitoring'. The main content area is titled 'All rules' and contains a table of detection rules. The table has columns for 'Rule', 'Risk score', 'Severity', 'Last run', and 'Last status'. There are 37 rules listed, each with a checkbox in the 'Rule' column. The rules include various AWS services and their associated actions, such as 'AWS IAM Group Creation', 'AWS CloudTrail Log Created', 'AWS CloudWatch Log Stream Deletion', 'AWS EC2 Encryption Disabled', 'AWS CloudTrail Log Updated', 'AWS WAF Access Control List Deletion', 'AWS CloudWatch Alarm Deletion', 'AWS EC2 Network Access Control List Creation', 'AWS Management Console Root Login', 'AWS CloudTrail Log Suspended', 'Unusual City For an AWS Command', 'AWS CloudTrail Log Deleted', 'AWS RDS Cluster Creation', and 'AWS IAM Group Deletion'. The 'Risk score' column shows values like 21, 47, and 73. The 'Severity' column shows levels like Low, Medium, and High. The 'Last run' column shows timestamps like '2 minutes ago', '1 minute ago', and '6 minutes ago'. The 'Last status' column shows green and orange dots.

Security / Detections / Detection rules

Overview Detections Hosts Network Timelines Cases Administration

< Back to detections

Detection rules **BETA**

Rules Monitoring

All rules

Showing 37 rules | Selected 0 rules Bulk actions Refresh

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

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

Monitoring and Compliance



... more



Threat Detection and Prevention



Tactics and Techniques

Global actors and threats

MITRE
ATT&CK™

Detect any issues in your environment

Build-your-own

Free and Open Repository

Anomaly detection via
Machine Learning

Advanced Correlation
via detection rules

Unified Issue Detection

[elastic/detection-rules](https://github.com/elastic/detection-rules)

Community-driven

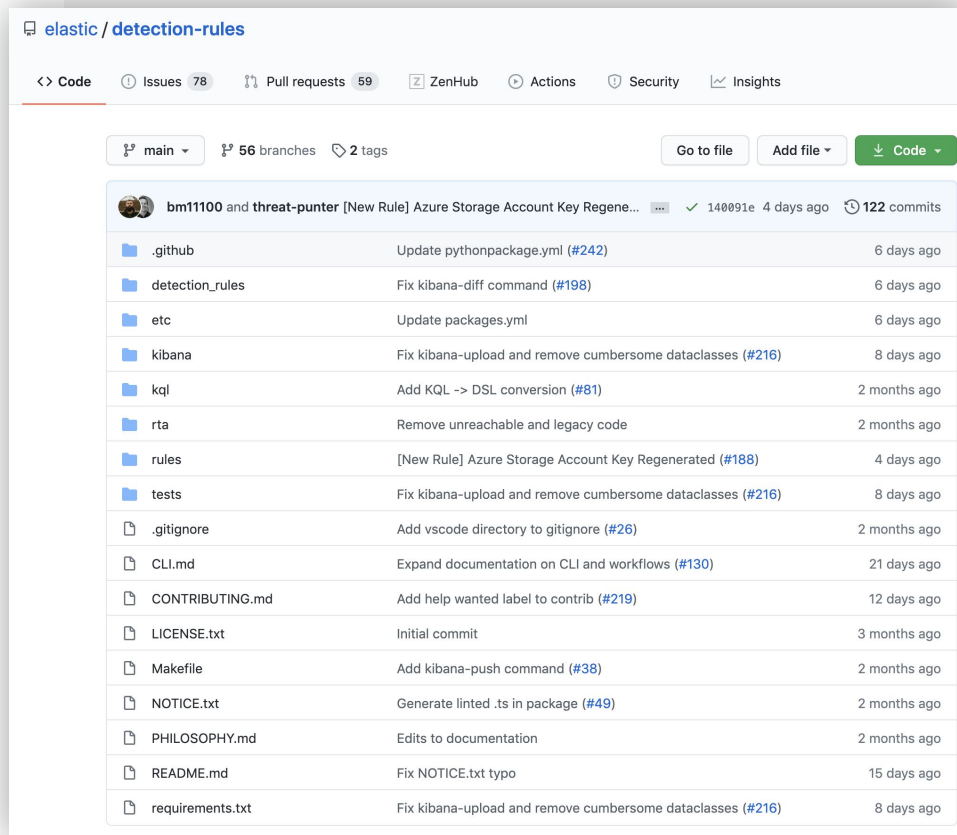
Building shared knowledge across Security and Operations communities

Always growing

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

Always available

Detections are free and under Elastic License



SecOps > Cloud > AWS

