



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

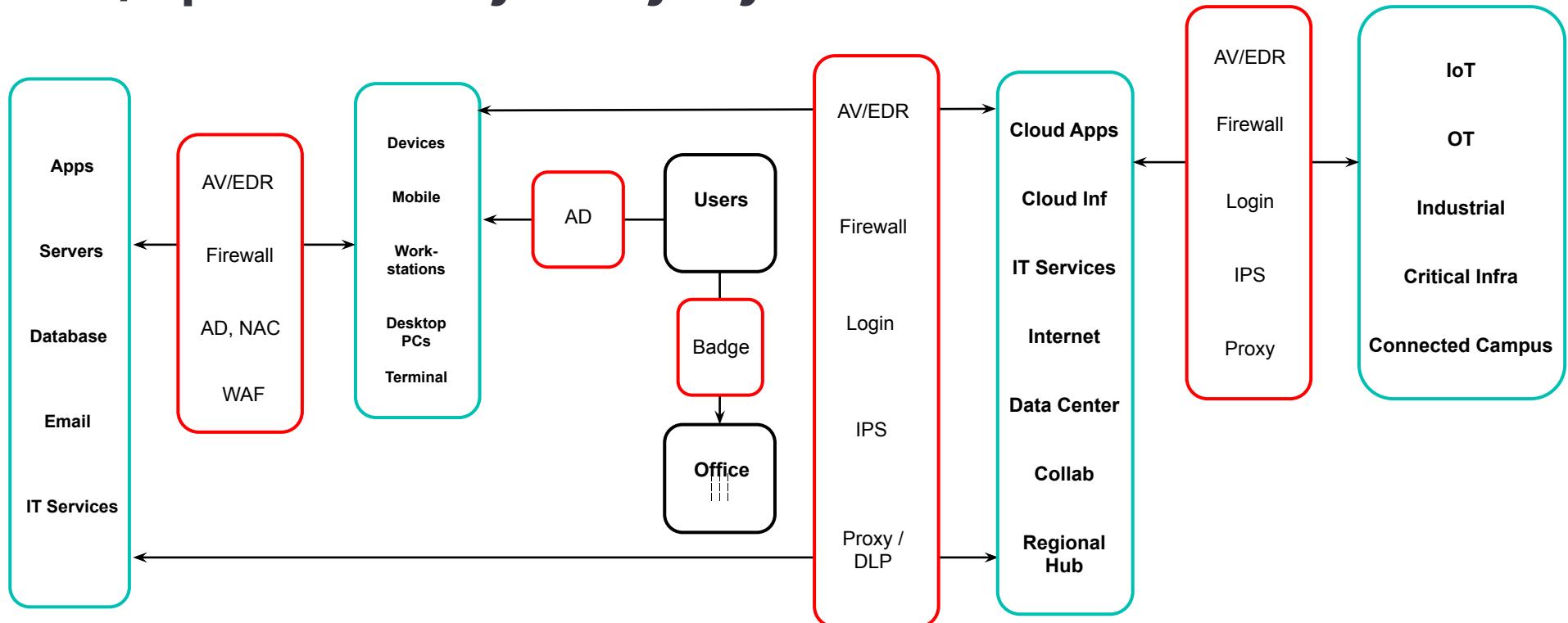
In cloud Infrastructure
Hybrid is the new
normal

24x7

Global Operations

Pushing continuous
delivery and higher
agility

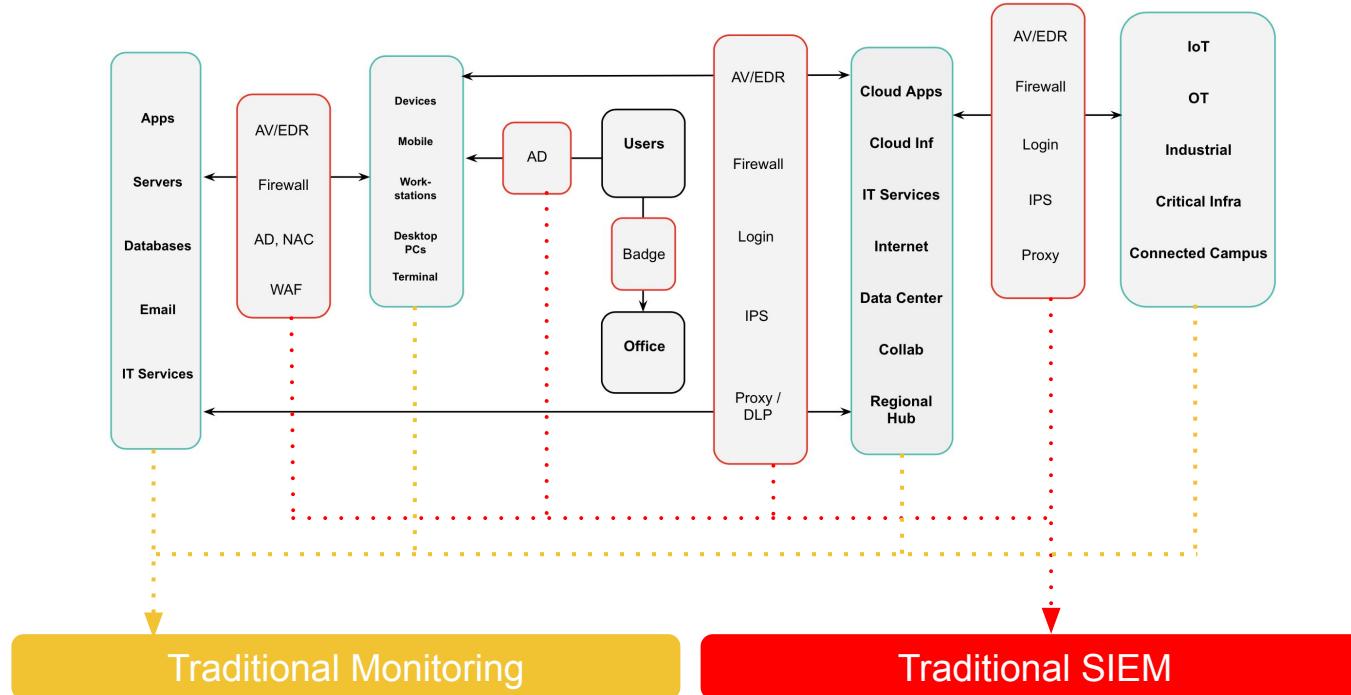
IT/Ops & Security everyday Interactions



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

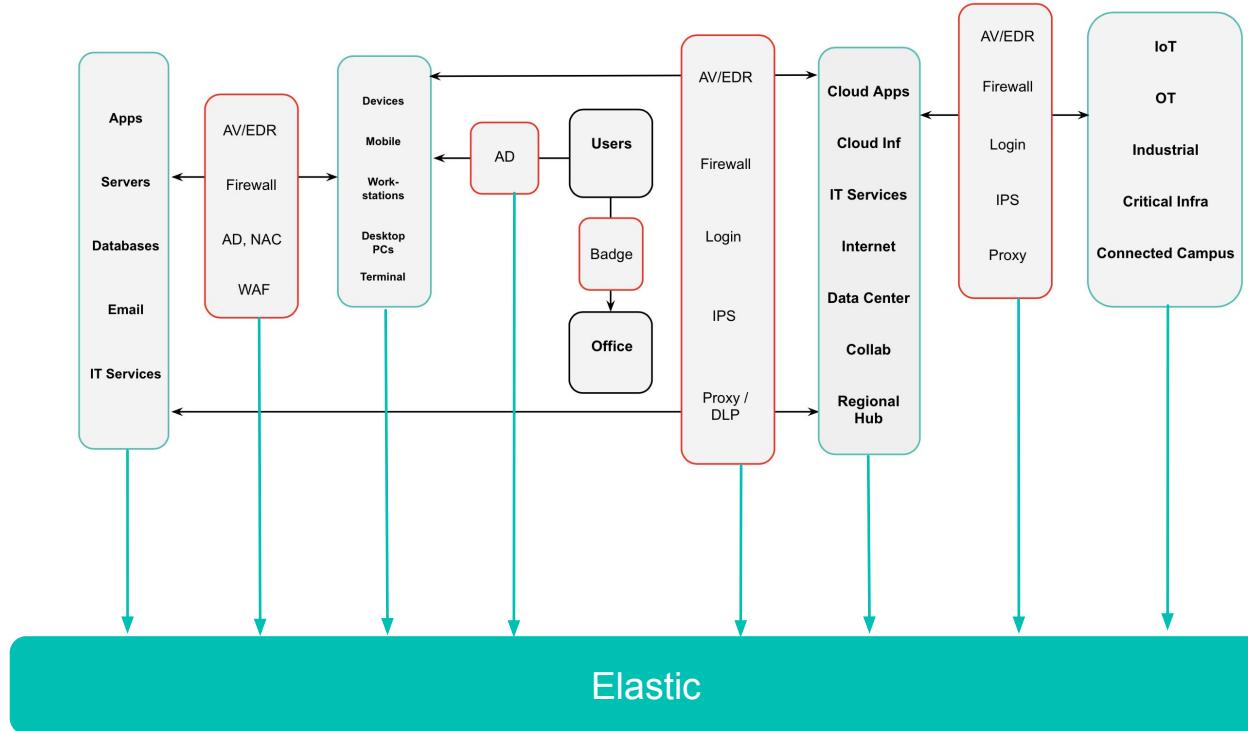
Technology data silos

That drive cultural silos in organizations



Single, unified, powerful platform

To Drive MTTR to ZERO



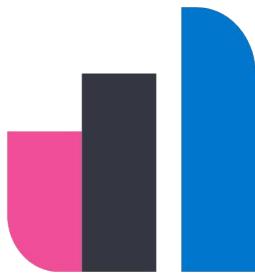
Benefits

- 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



Microsoft Azure

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



Microsoft Azure

Federate across these deployments with cross-cluster search

See it for yourself

Try in Elastic Cloud

cloud.elastic.co

The screenshot shows the Elastic Cloud interface. At the top, there is a navigation bar with the Elastic Cloud logo and a search bar. Below the navigation bar, there is a table for the Elasticsearch Service. The table has columns for Deployment name, Status, Version, Quick link, and Cloud region. There is one row for a deployment named "Trial" with the ID "0a750e6". The status is "Healthy", the version is "7.9.0", the quick link is "Kibana", and the cloud region is "East US 2 (Virginia)". There is a "Create deployment" button in the top right corner of the table. Below the table, there are two cards. The first card is for "Documentation" and contains a search bar with the placeholder "Help me find...", a link to "Elasticsearch Service on Elastic Cloud documentation", and links to "Elasticsearch documentation" and "Elasticsearch REST API". The second card is for "Webinars" and contains a video thumbnail for "Getting started with Elastic App Search" with the description "Build a leading search experience using a refined set of APIs and a powerful search-based UI.", and a video thumbnail for "Unified observability for logs, metrics, and traces" with the description "Learn how to efficiently combine and analyze data in a single deployment".

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

[Create deployment](#)

Documentation

[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

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

Custom logs Collect your custom logs.

MySQL MySQL Integration

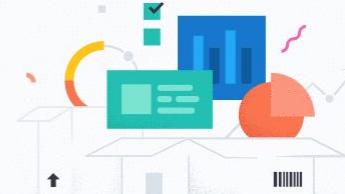
NetFlow NetFlow Integration

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
```

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



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.

Search...

Show reserved roles

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

Unified Issue Detection

Free and Open Detection Engine

Speed and Scale

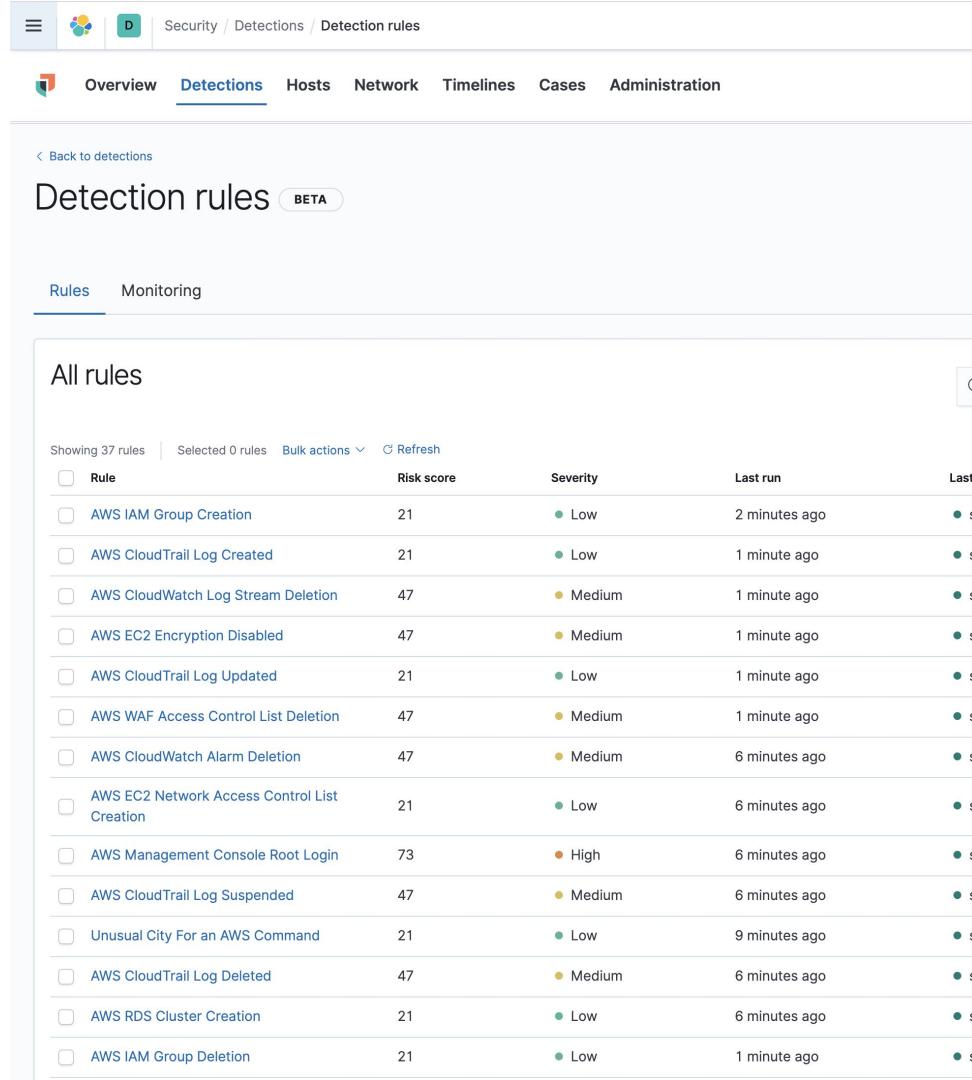
Powered by the Elastic stack

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 'Detection rules' page in a web application. At the top, there are navigation links: Overview, Detections (which is underlined), Hosts, Network, Timelines, Cases, and Administration. Below that, a 'BETA' label is visible. A 'Back to detections' link is present. The main section is titled 'All rules' and displays a table of 37 entries. The table columns are: Rule, Risk score, Severity, Last run, and a partially visible 'Last' column. Each row represents a different AWS event or configuration change, such as 'AWS IAM Group Creation', 'AWS CloudTrail Log Created', and 'AWS EC2 Encryption Disabled'. The 'Severity' column uses color-coded circles (green for Low, yellow for Medium, orange for High) to indicate the risk level of each rule.

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

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



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

Community-driven

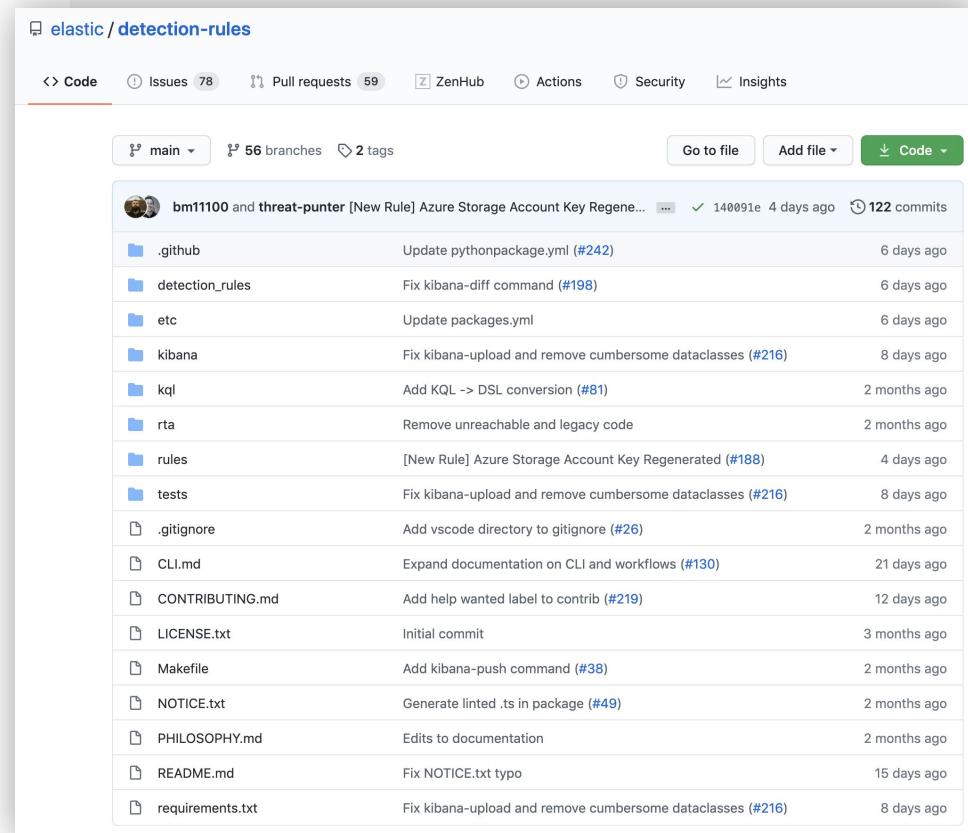
Building shared knowledge across Security and Operations communities

Always growing

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

Always available

Detections are free and under Elastic License



The screenshot shows the GitHub repository `elastic / detection-rules`. The repository has 78 issues, 59 pull requests, and 122 commits. The main branch is the latest, with 56 branches and 2 tags. The commits are listed in reverse chronological order, showing contributions from various maintainers like `bm11100` and `threat-punter`. The commits cover various aspects of rule development, including updates to `pythonpackage.yml`, `kibana-diff`, `packages.yml`, and `KQL` to `DSL` conversion. Other commits include fixes for `kibana-upload`, `cumbersome dataclasses`, and `CLI` documentation. The repository is actively maintained, with commits from the past 15 days.

Commit	Author	Message	Age
<code>bm11100 and threat-punter [New Rule] Azure Storage Account Key Regene...</code>	<code>bm11100 and threat-punter</code>	<code>[New Rule] Azure Storage Account Key Regene...</code>	4 days ago
<code>.github</code>		<code>Update pythonpackage.yml (#242)</code>	6 days ago
<code>detection_rules</code>		<code>Fix kibana-diff command (#198)</code>	6 days ago
<code>etc</code>		<code>Update packages.yml</code>	6 days ago
<code>kibana</code>		<code>Fix kibana-upload and remove cumbersome dataclasses (#216)</code>	8 days ago
<code>kql</code>		<code>Add KQL -> DSL conversion (#81)</code>	2 months ago
<code>rta</code>		<code>Remove unreachable and legacy code</code>	2 months ago
<code>rules</code>		<code>[New Rule] Azure Storage Account Key Regenerated (#188)</code>	4 days ago
<code>tests</code>		<code>Fix kibana-upload and remove cumbersome dataclasses (#216)</code>	8 days ago
<code>.gitignore</code>		<code>Add vscode directory to gitignore (#26)</code>	2 months ago
<code>CLI.md</code>		<code>Expand documentation on CLI and workflows (#130)</code>	21 days ago
<code>CONTRIBUTING.md</code>		<code>Add help wanted label to contrib (#219)</code>	12 days ago
<code>LICENSE.txt</code>		<code>Initial commit</code>	3 months ago
<code>Makefile</code>		<code>Add kibana-push command (#38)</code>	2 months ago
<code>NOTICE.txt</code>		<code>Generate linted .ts in package (#49)</code>	2 months ago
<code>PHILOSOPHY.md</code>		<code>Edits to documentation</code>	2 months ago
<code>README.md</code>		<code>Fix NOTICE.txt typo</code>	15 days ago
<code>requirements.txt</code>		<code>Fix kibana-upload and remove cumbersome dataclasses (#216)</code>	8 days ago

Unified User Interface

SecOps > Cloud > AWS

The screenshot displays a web-based unified user interface for security operations, specifically for AWS. The top navigation bar includes standard browser controls (New Tab, Back, Forward, Refresh, Search) and a toolbar with 'Upload value lists', 'Import rule...', and a 'Create new rule' button. The main content area is titled 'Detection rules (BETA)' and includes tabs for 'Rules' (selected) and 'Monitoring'. A search bar and filter buttons for 'Tags' (Elastic, Linux, Network, APM, Elastic) and rule count (Elastic rules (203), Custom rules (4)) are located at the top of the list table. The table itself shows 207 rules, each with a checkbox, a link to the rule details, its risk score, severity level (Low, Medium), the time of the last run, the status of the last response (succeeded), and a list of tags. Each row also features an 'Activated' toggle switch and a 'More' options menu (three dots). The table is scrollable, and a 'Refresh' button is visible at the top right of the list area.

<input type="checkbox"/>	Rule	Risk score	Severity	Last run	Last response	Tags	Activated	...
<input type="checkbox"/>	Network Sniffing via Tcpdump	21	Low	1 minute ago	● succeeded	Elastic, Linux	<input checked="" type="checkbox"/>	...
<input type="checkbox"/>	SMTP on Port 26/TCP	21	Low	45 seconds ago	● succeeded	Elastic, Network	<input checked="" type="checkbox"/>	...
<input type="checkbox"/>	Web Application Suspicious Activity: Unauthorized Method	47	Medium	3 minutes ago	● succeeded	APM, Elastic	<input checked="" type="checkbox"/>	...
<input type="checkbox"/>	Web Application Suspicious Activity: No User Agent	47	Medium	3 minutes ago	● succeeded	APM, Elastic	<input checked="" type="checkbox"/>	...
<input type="checkbox"/>	Tor Activity to the Internet	47	Medium	2 minutes ago	● succeeded	Elastic, Network	<input checked="" type="checkbox"/>	...
<input type="checkbox"/>	SQL Traffic to the Internet	47	Medium	2 minutes ago	● succeeded	Elastic, Network	<input checked="" type="checkbox"/>	...
<input type="checkbox"/>	TCP Port 8000 Activity to the Internet	21	Low	2 minutes ago	● succeeded	Elastic, Network	<input checked="" type="checkbox"/>	...