elastic | The Search Analytics Company

Mastering Risk with Qualys: The Elastic Journey

Qualys Security Conference London

Wed 27, 2024

https://ela.st/qsc24london

We build search solutions on a single stack

- Search
- Observability
- Security

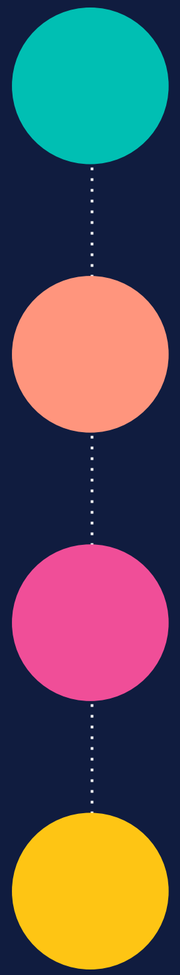
elastic

Clément Fouque

Vulnerability Management lead Elastic

elastic

Plan



Environment

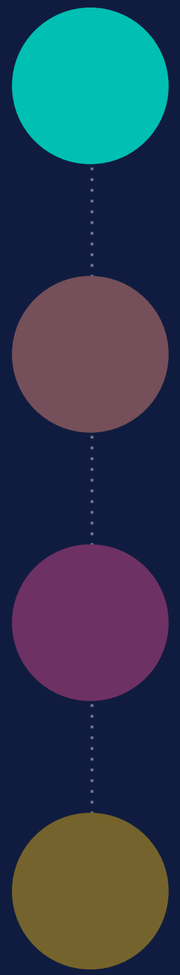
Asset Inventory

Vulnerability Management

Evolutions

elastic

Plan



Environment

Asset Inventory

Vulnerability management

Evolutions

elastic

Elastic InfoSec challenges

Globally distributed workforce

~3,200
Elasticians

44
Countries

Cloud native implementation

okta

slack G Suite GitHub

salesforce aws Office 365

Microsoft Azure workday.

elastic

InfoSec by the numbers (daily)

150TB

Security data

Enables us to monitor for abnormal and security relevant activity

600GB

Endpoint data

Amount of security data ingested daily from Elastic end user endpoints

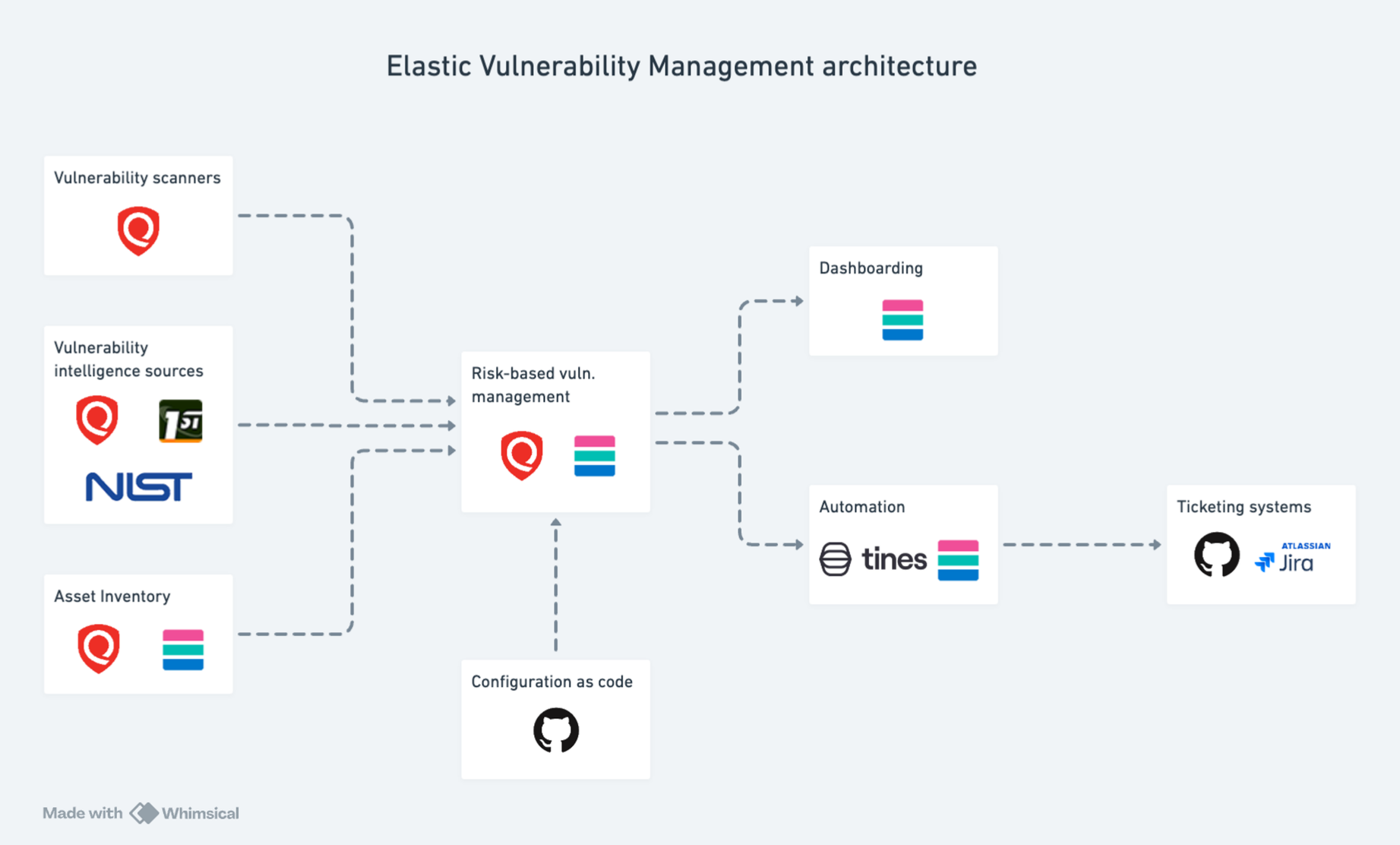
>450K

Endpoints

Globally dispersed cloud instances, virtual desktop environments, containers and user workstations

elastic

Architecture



https://www.elastic.co/blog/how-infosec-uses-elastic-stack-vulnerability-management
https://docs.elastic.co/integrations/qualys_vmdr

1.2 FTE

Architecture

Automatisation

Culture

- 40K Qualys agent
- 2K Policy Compliance
- 120+ connectors (15 TotalCloud)
- 5 container scanning
- 5 web applications scanning

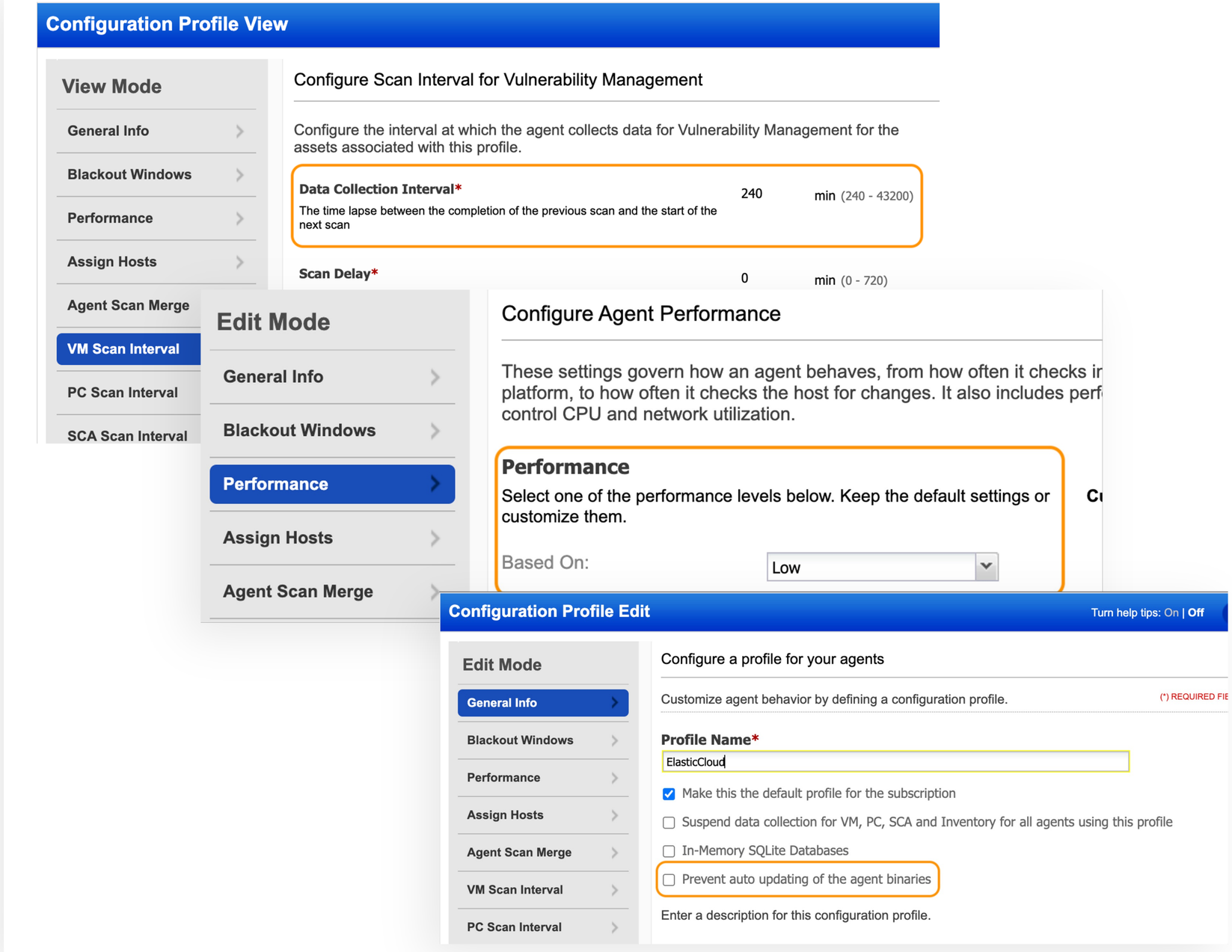
Cloud agents

Centralized management

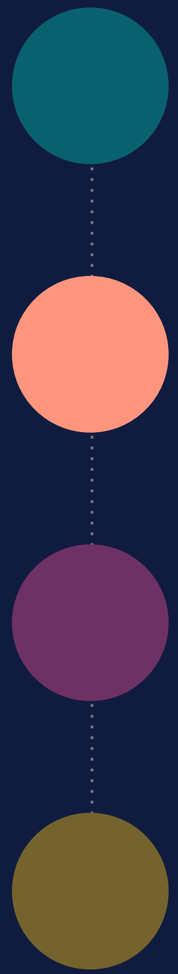
Scan every 4 hours

No performance impact

Automatic update (agent and QIDs)



Plan



Environment

Asset Inventory

Vulnerability management

Evolutions

elastic

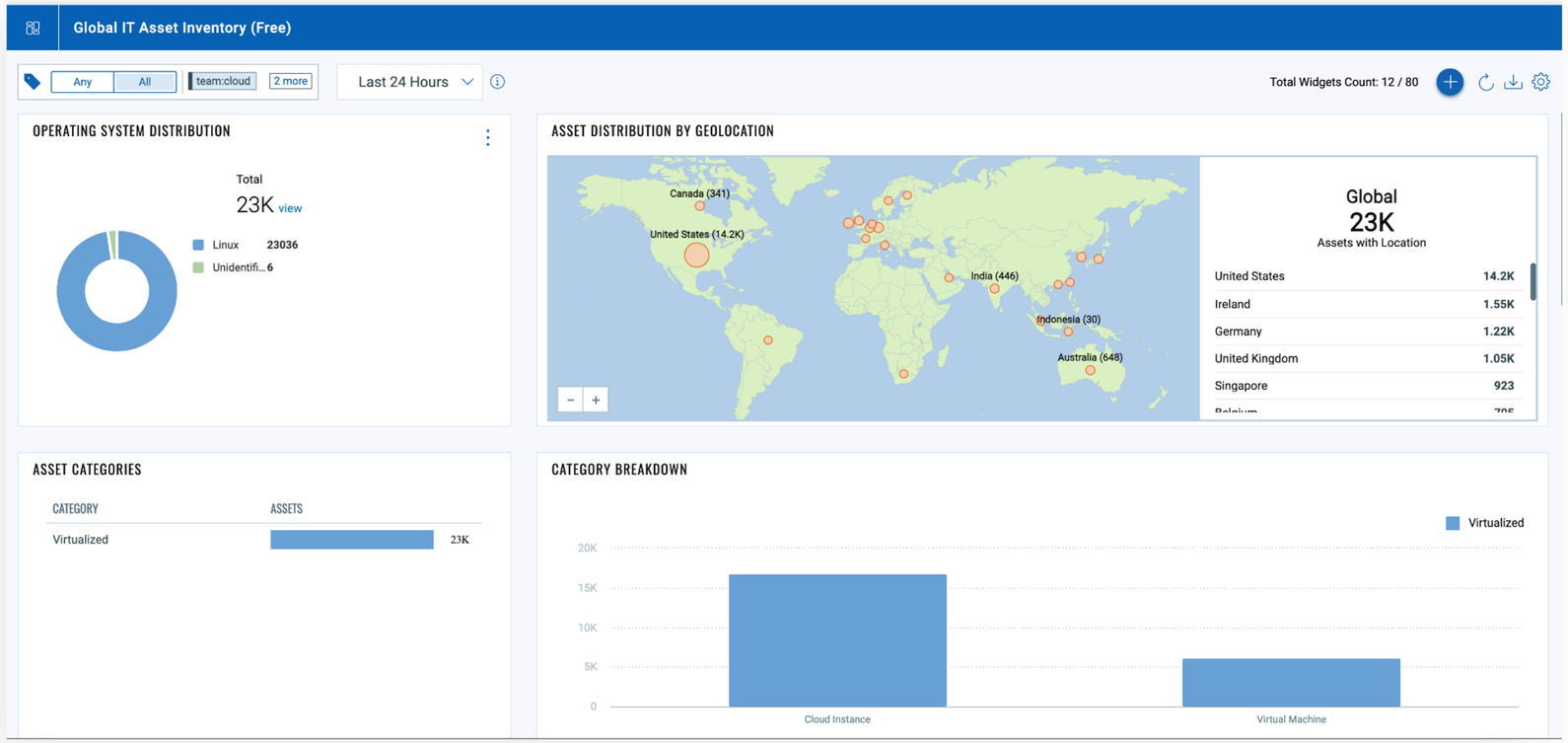
Why and how have an asset inventory?

Free*

Easy to implement

Automatic purge

Risk management



Qualys tags

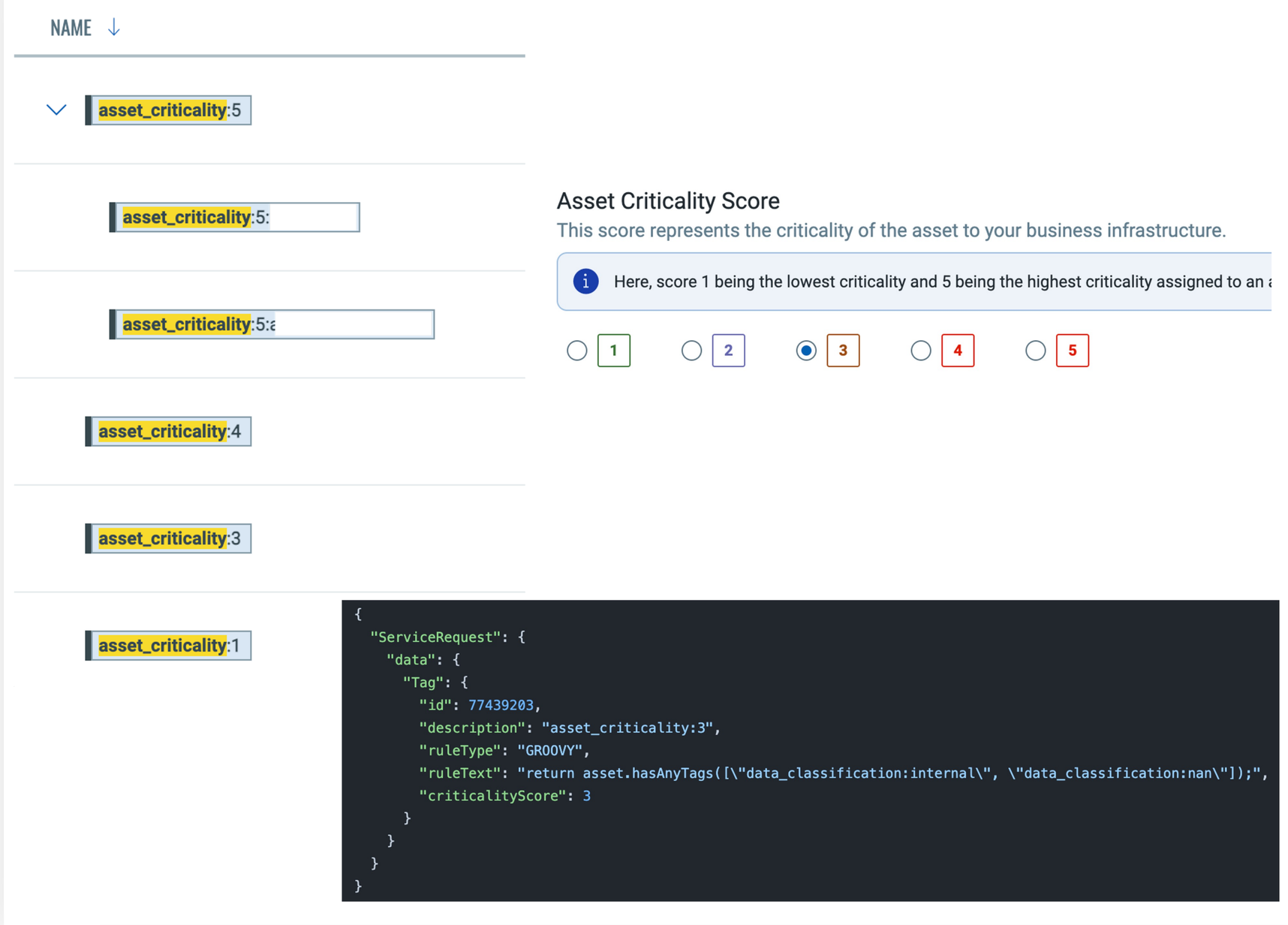
Enrichment

Parent/child relation

Access based on tags

Define criticality

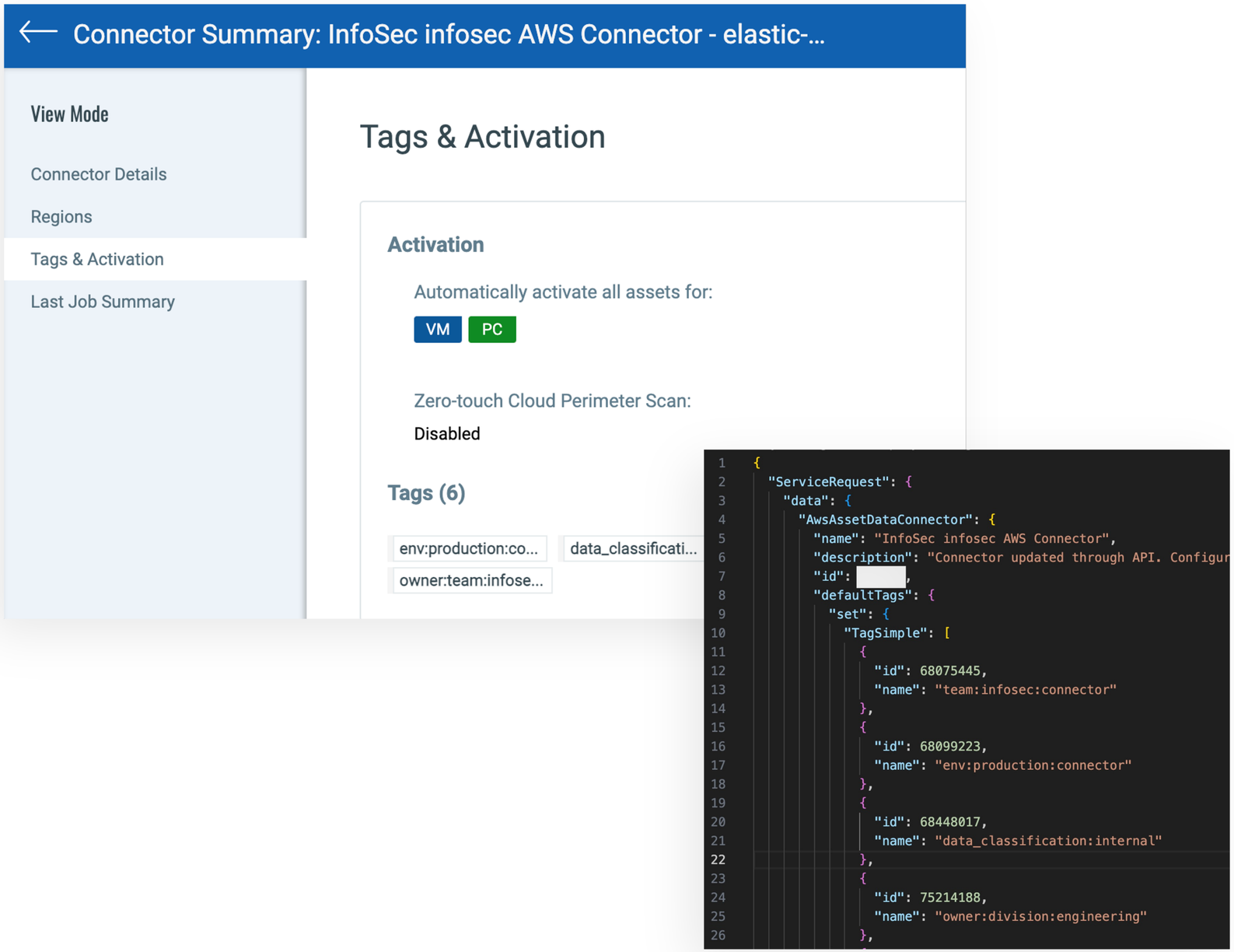
API



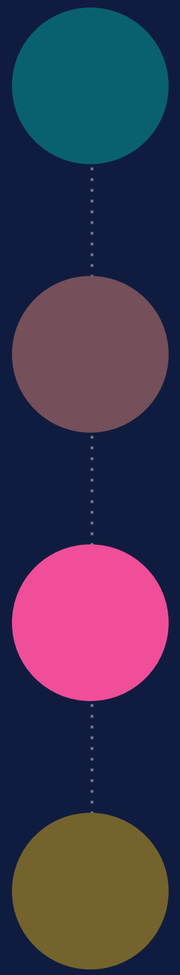
Qualys cloud connectors

2 modes: inventory and compliance

API



Plan



Environment

Asset Inventory

Vulnerability management

Evolutions

elastic

Priorisation

Qualys Detection Score

Asset Risk Score

NAME	CRITICALITY	TruRisk™ Score	OPERATING SYSTEM	HARDWARE
i 57 1 C 53	4	650	Canonical Ubuntu Bionic B... 18.04 LTS 18.04.6 LTS	Amazon Web Servic... Amazon EC2 M5 m5... Cloud Instance
i 52 1 1 7	4	650	Canonical Ubuntu Bionic B... 18.04 LTS 18.04.6 LTS	Amazon Web Servic... Amazon EC2 M5 m5... Cloud Instance
i 5-98 1 C 75	3	504	Canonical Ubuntu Jammy ... 22.04 LTS 22.04.2 LTS	Xen Project HVM domU Virtual Machine

Exception Management

Search list

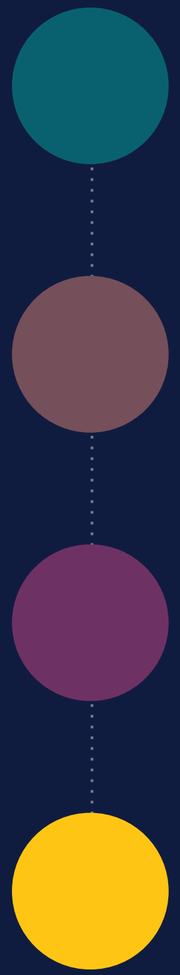
Remediation policies

Tickets

API

376157	Apache Log4j Remote Code Execution (RCE) Vulnerability (Log4Shell) Fixed Ignored	100
376178	Apache Log4j Remote Code Execution (RCE) Vulnerability (CVE-2021-45046) (Log4Shell) Fixed Ignored	100
376194	Apache Log4j Denial of Service (D Fixed Ignored	95
376209	Apache Log4j Remote Code Execu Fixed Ignored	95

Plan



Environment

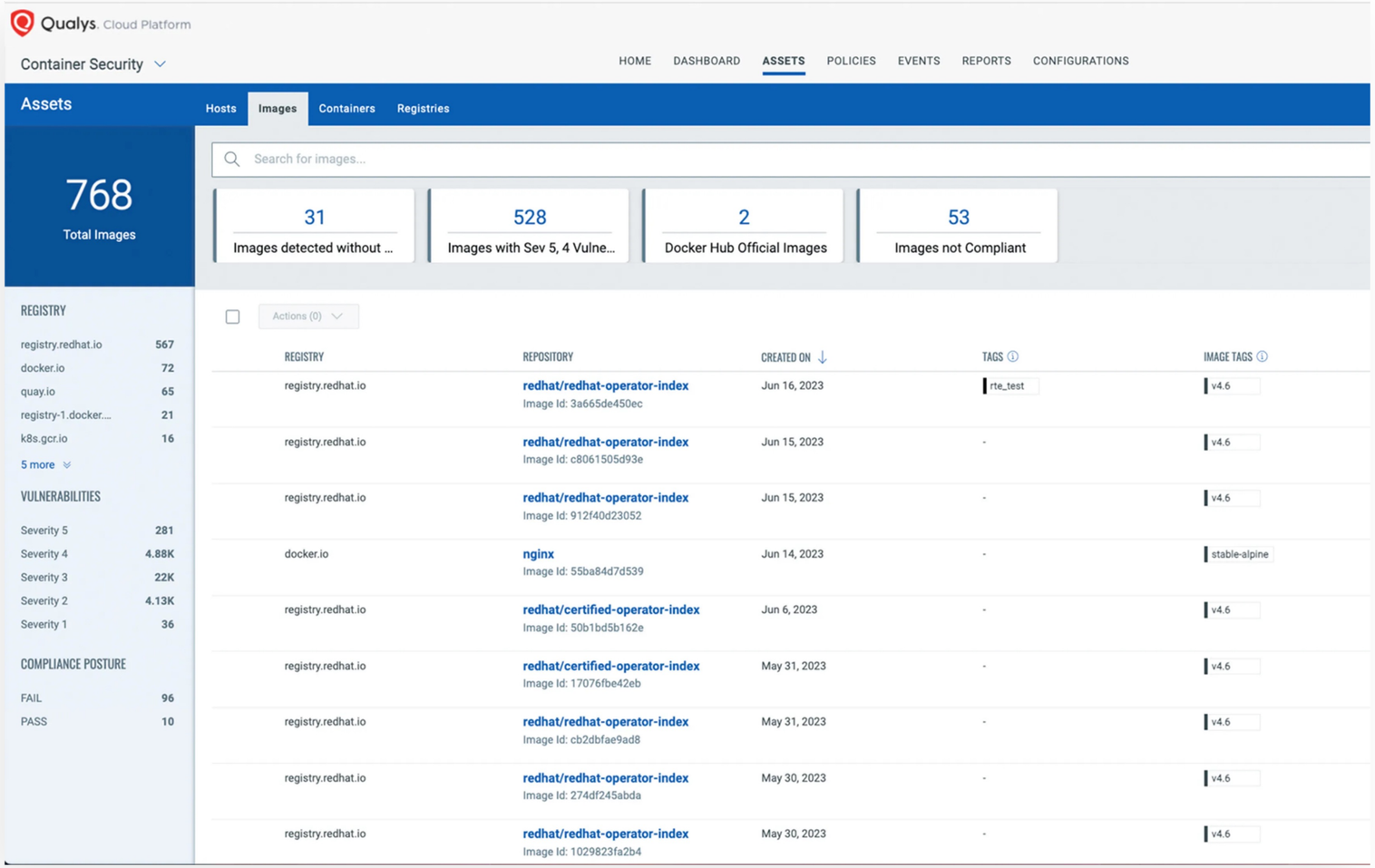
Asset Inventory

Vulnerability management

Evolutions

elastic

Container scanning
Patch Management



Master your risk with Qualys

1

Asset Inventory

Tags

Connectors

2

TrueRisk

Qualys Detection Score

Asset Risk Score

3

Reporting

API

elastic