elastic | The Search Analytics Company

DIVING THROUGH RCAs: A QUEST FOR RELIABILITY

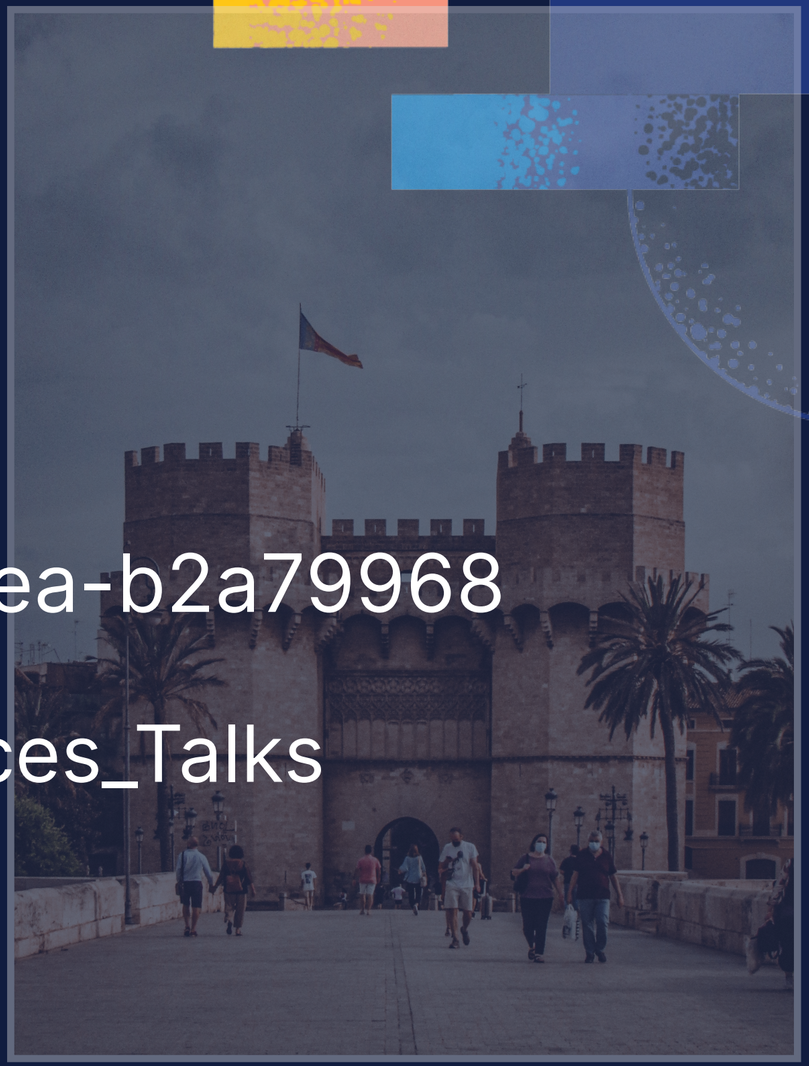
DIANA TODEA - SRE

DEVOPSDAYS GENEVA MAY 2024

DIANA TODEA - OBSERVABILITY SRE

https://www.linkedin.com/in/diana-todea-b2a79968

https://github.com/didiViking/Conferences_Talks



UNSPLASH Juan Puyo

elastic

ALERTS

INCIDENT

INCIDENT CHANNEL

CUSTOMERS

MANAGERS

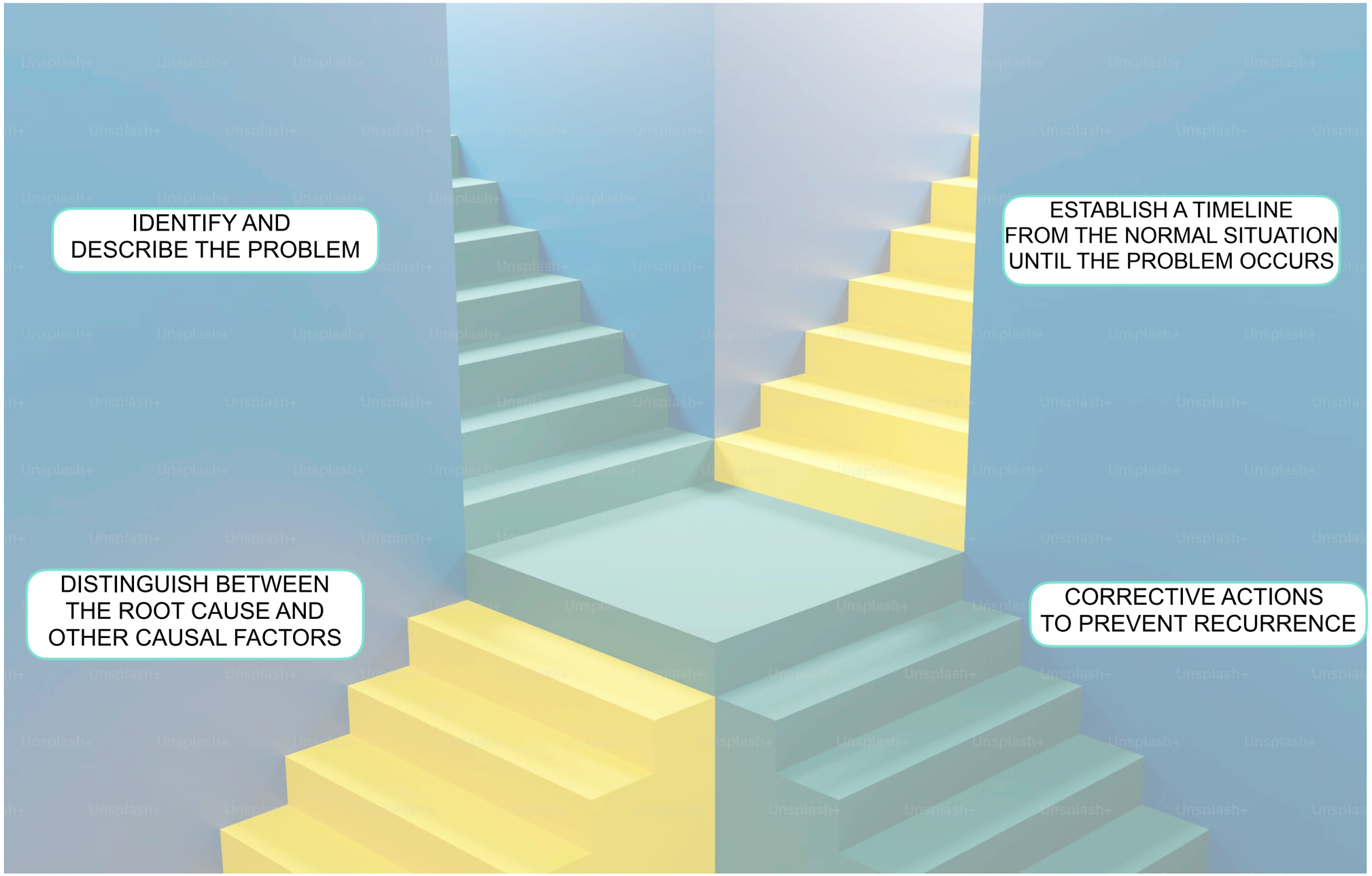
elastic

WHAT IS ROOT CAUSE ANALYSIS?

Root cause analysis (RCA) is the process of discovering the root causes of problems in order to identify appropriate solutions.

SOURCE: TABLEAU

elastic


IDENTIFY AND
DESCRIBE THE PROBLEM
ESTABLISH A TIMELINE
FROM THE NORMAL SITUATION
UNTIL THE PROBLEM OCCURS
DISTINGUISH BETWEEN
THE ROOT CAUSE AND
OTHER CAUSAL FACTORS
CORRECTIVE ACTIONS
TO PREVENT RECURRENCE

elastic

POSTMORTEM CULTURE

mistake

blame

failure

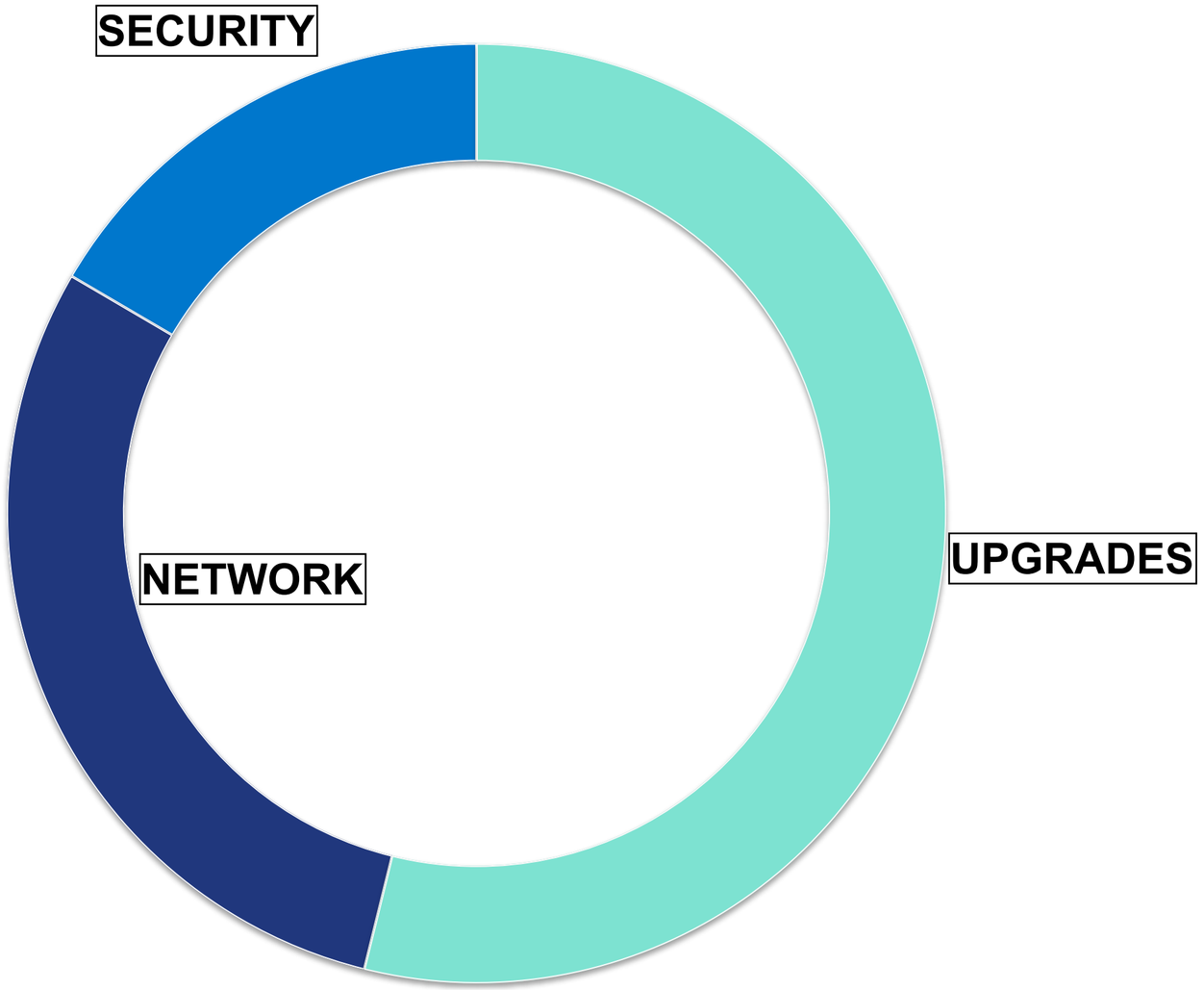
collaboration

open communication

postmortem reviews

elastic

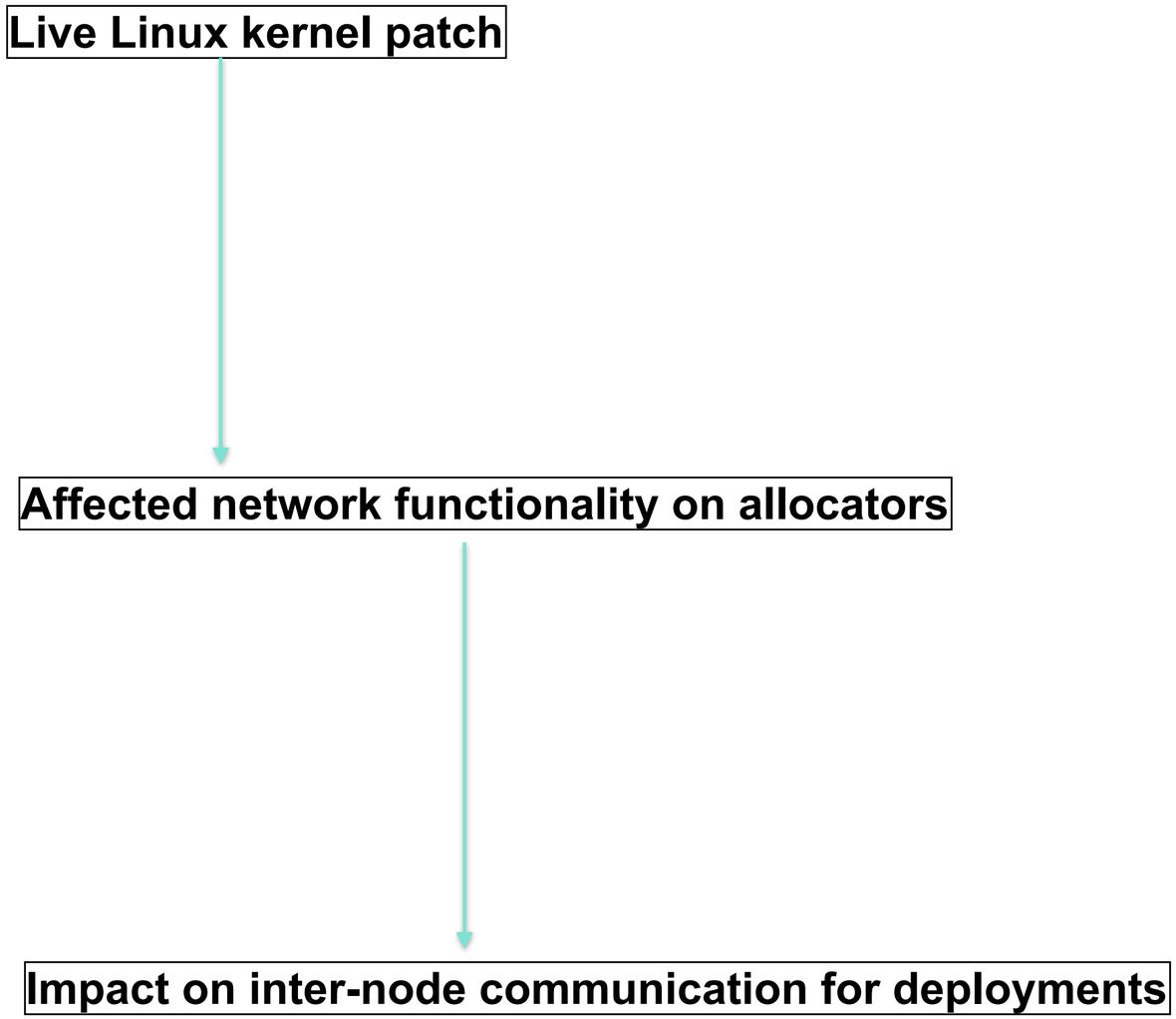
TOP SEVERITY 1 AND 2 INCIDENTS' ROOT CAUSES



elastic

5 WHYS METHODOLOGY

1K nodes affected in a region
Incident duration: 5h
Impact duraction: 7h
Impacted allocators: 96
Affected customer deployments: 1042
Affected organizations: 750



elastic

elastic

CUS
TOM
ERS

OBS
ERV
ABIL
ITY

SEC
URI
TY

elastic

FOCUS ON OBSERVABILITY

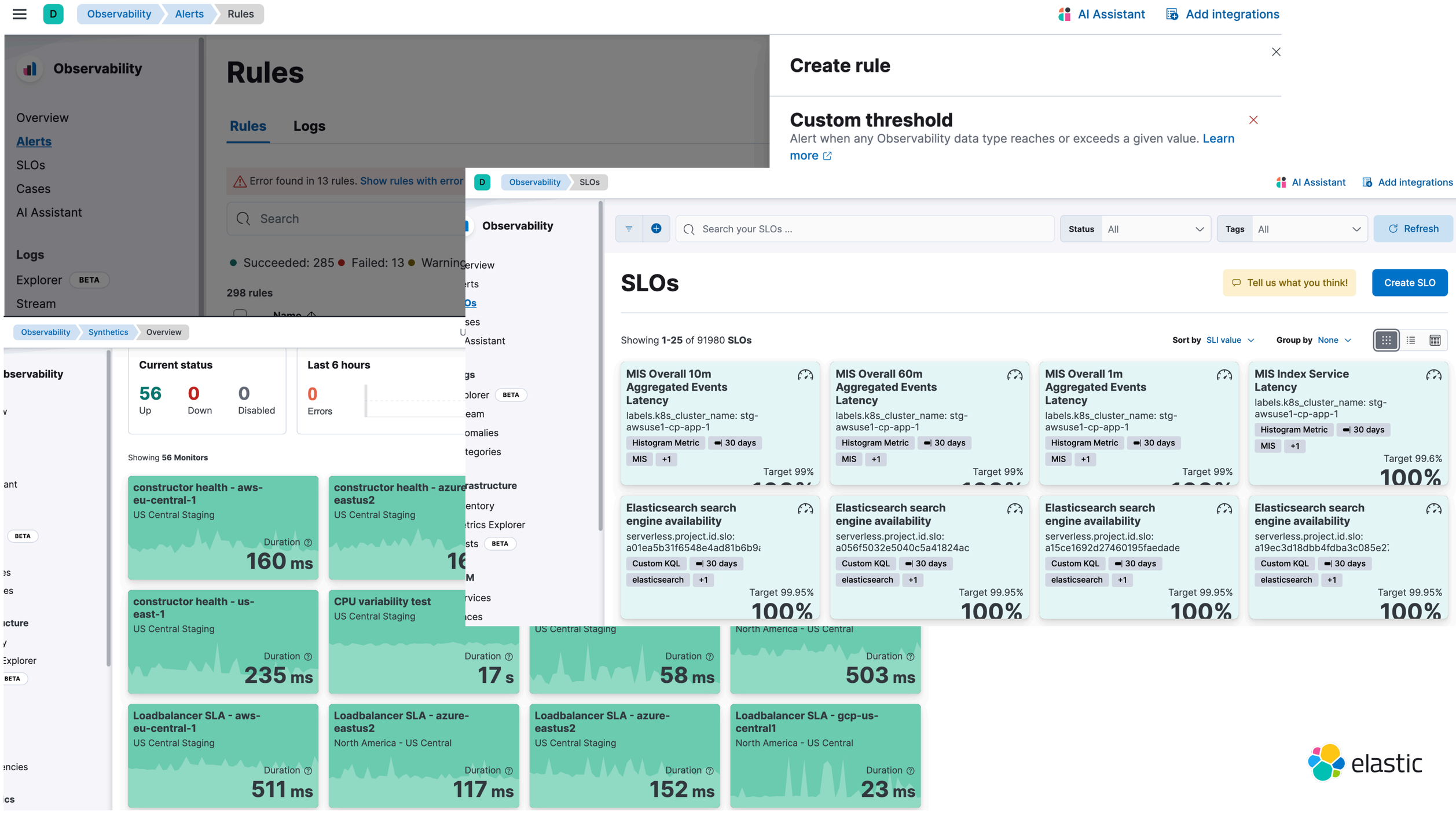
MOVE AWAY FROM 3RD PARTY TOOLS

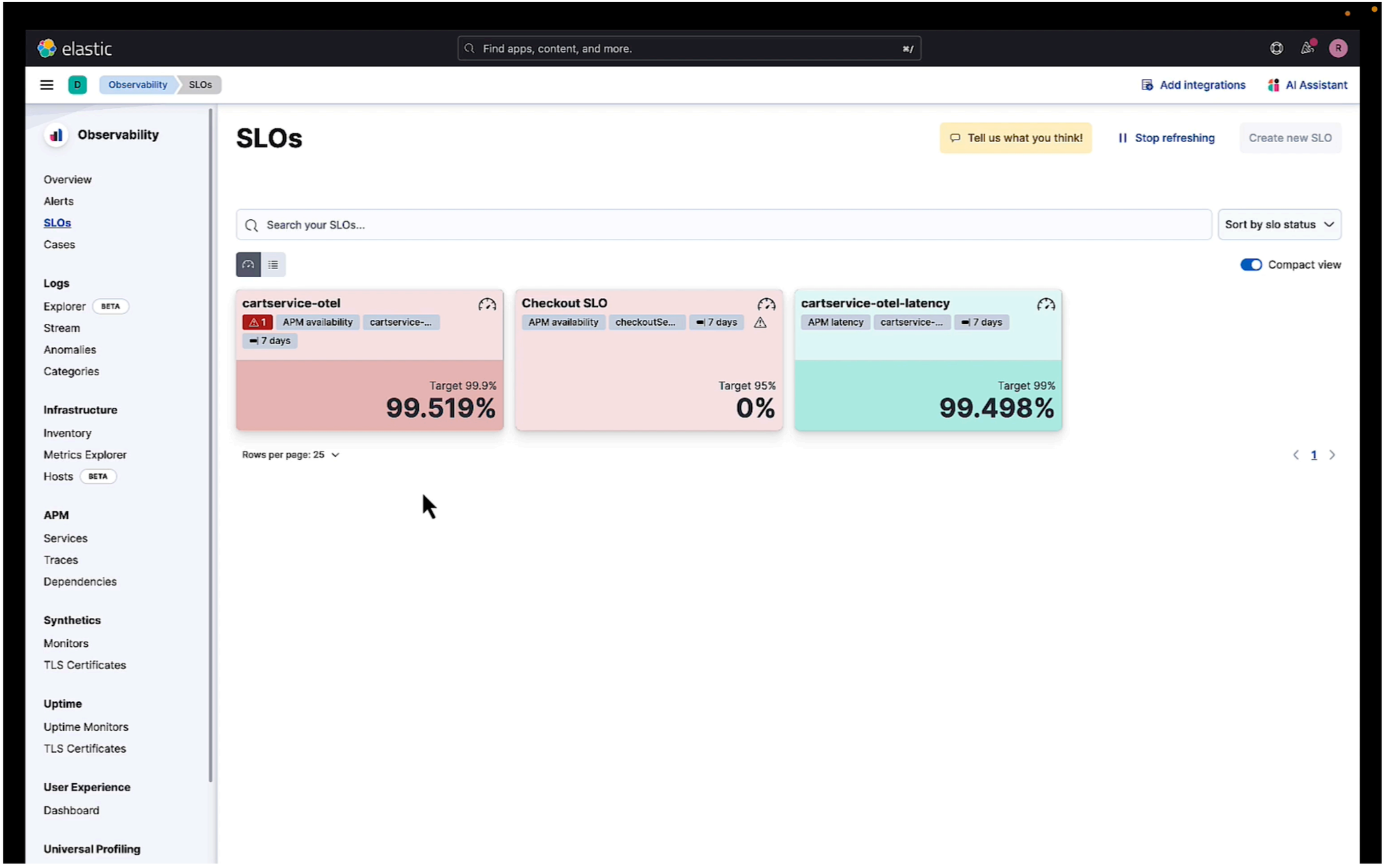
CREATE UPTIME CHECKS (SYNTHETIC MONITORING)

CREATE SLOS AND BURN RATE ALERTS

INTEGRATE WITH ELASTIC OBSERVABILITY AI ASSISTANT

elastic


Observability
Alerts
Rules
AI Assistant
Add integrations
Observability
Overview
Alerts
SLOs
Cases
AI Assistant
Logs
Explorer BETA
Stream
Rules
Rules
Logs
Error found in 13 rules. Show rules with error
Search
Succeeded: 285 Failed: 13 Warning
298 rules
Create rule
Custom threshold
Alert when any Observability data type reaches or exceeds a given value. Learn more
Observability
Synthetics
Overview
Current status
56 Up
0 Down
0 Disabled
Last 6 hours
0 Errors
Showing 56 Monitors
constructor health - aws-eu-central-1
US Central Staging
Duration 160 ms
constructor health - azure-eastus2
US Central Staging
constructor health - us-east-1
US Central Staging
Duration 235 ms
CPU variability test
US Central Staging
Duration 17 s
Loadbalancer SLA - aws-eu-central-1
US Central Staging
Duration 511 ms
Loadbalancer SLA - azure-eastus2
North America - US Central
Duration 117 ms
Loadbalancer SLA - azure-eastus2
US Central Staging
Duration 152 ms
Loadbalancer SLA - gcp-us-central1
North America - US Central
Duration 23 ms
Observability
SLOs
AI Assistant
Add integrations
Search your SLOs ...
Status All
Tags All
Refresh
SLOs
Tell us what you think!
Create SLO
Showing 1-25 of 91980 SLOs
Sort by SLI value
Group by None
MIS Overall 10m Aggregated Events Latency
labels.k8s_cluster_name: stg-awsuse1-cp-app-1
Histogram Metric 30 days MIS +1
Target 99%
MIS Overall 60m Aggregated Events Latency
labels.k8s_cluster_name: stg-awsuse1-cp-app-1
Histogram Metric 30 days MIS +1
Target 99%
MIS Overall 1m Aggregated Events Latency
labels.k8s_cluster_name: stg-awsuse1-cp-app-1
Histogram Metric 30 days MIS +1
Target 99%
MIS Index Service Latency
labels.k8s_cluster_name: stg-awsuse1-cp-app-1
Histogram Metric 30 days MIS +1
Target 99.6%
100%
Elasticsearch search engine availability
serverless.project.id.slo: a01ea5b31f6548e4ad81b6b9
Custom KQL 30 days elasticsearch +1
Target 99.95%
100%
Elasticsearch search engine availability
serverless.project.id.slo: a056f5032e5040c5a41824ac
Custom KQL 30 days elasticsearch +1
Target 99.95%
100%
Elasticsearch search engine availability
serverless.project.id.slo: a15ce1692d27460195faedade
Custom KQL 30 days elasticsearch +1
Target 99.95%
100%
Elasticsearch search engine availability
serverless.project.id.slo: a19ec3d18dbb4fdba3c085e2
Custom KQL 30 days elasticsearch +1
Target 99.95%
100%
elastic



OpenTelemetry

elastic

FOCUS ON INFRASTRUCTURE

REMOVE UNUSED ALLOCATORS

UPGRADE TO HIGHER INSTANCE FAMILIES

CHECK THE BILL AND CLEAN UP

elastic

FOCUS ON DOCUMENTATION

elastic

FOCUS ON INCIDENT MANAGEMENT

SPEND **LESS TIME** IN IDENTIFYING INCIDENT SEVERITY

INTEGRATE RUNBOOKS AND DOCUMENTATION

SPEND **MORE TIME** IN FIXING THE ISSUE

AUTOMATE YOUR INCIDENT MANAGEMENT PLATFORM

elastic

FOCUS ON SYSTEM DESIGN

SERVERLESS

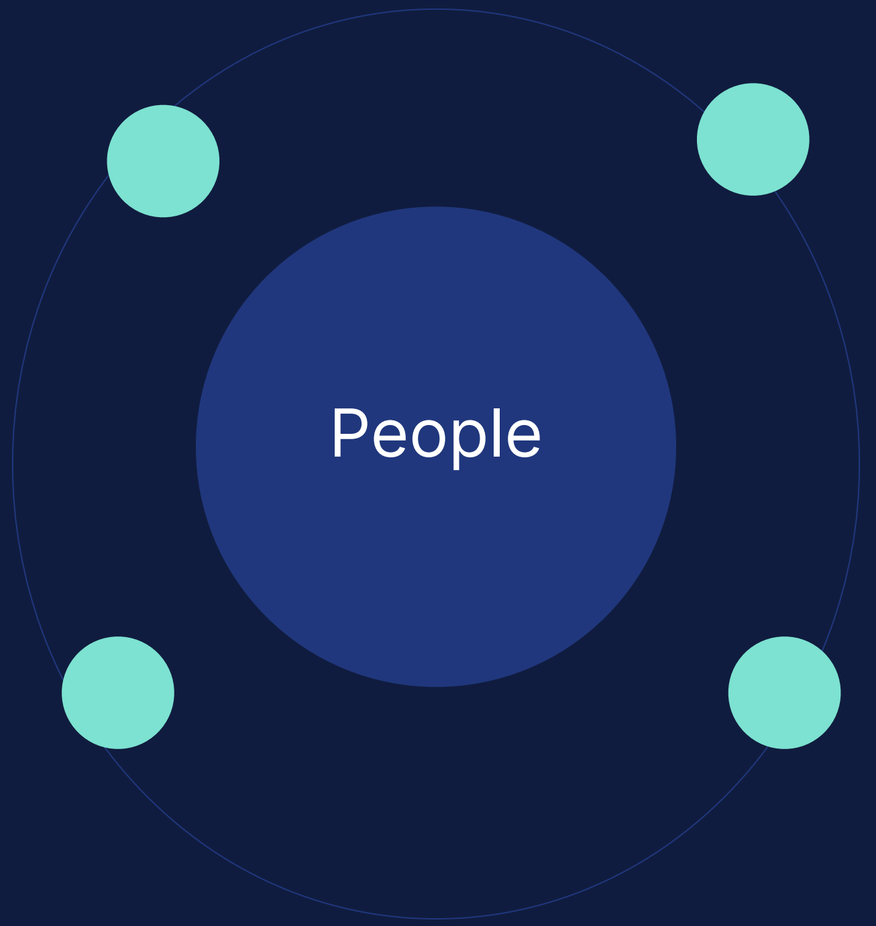
ES|QL

eBPF-BASED PROFILING AGENT DONATION TO OTEL

OBSERVABILITY AI ASSISTANT

EMPOWER

UPSKILL



OBSERVE

DECIDE & REACT

elastic

RESOURCES

- https://sre.google/sre-book/postmortem-culture/
- https://github.com/elastic/elasticsearch/
- https://www.elastic.co/guide/en/elasticsearch/reference/current/esql.html
- https://www.elastic.co/elasticsearch/ai-assistant
- https://www.elastic.co/search-labs
- https://docs.elastic.co/serverless
- https://www.elastic.co/blog/elastic-donation-proposal-to-contribute-profiling-agent-to-opentelemetry
- https://www.elastic.co/observability/opentelemetry

elastic

QUESTIONS?

THANK YOU

YOUR FEEDBACK HERE!

elastic