



Reduce Alert Noise and Resolve the Issues that Matter Most with Splunk IT Service Intelligence (ITSI)

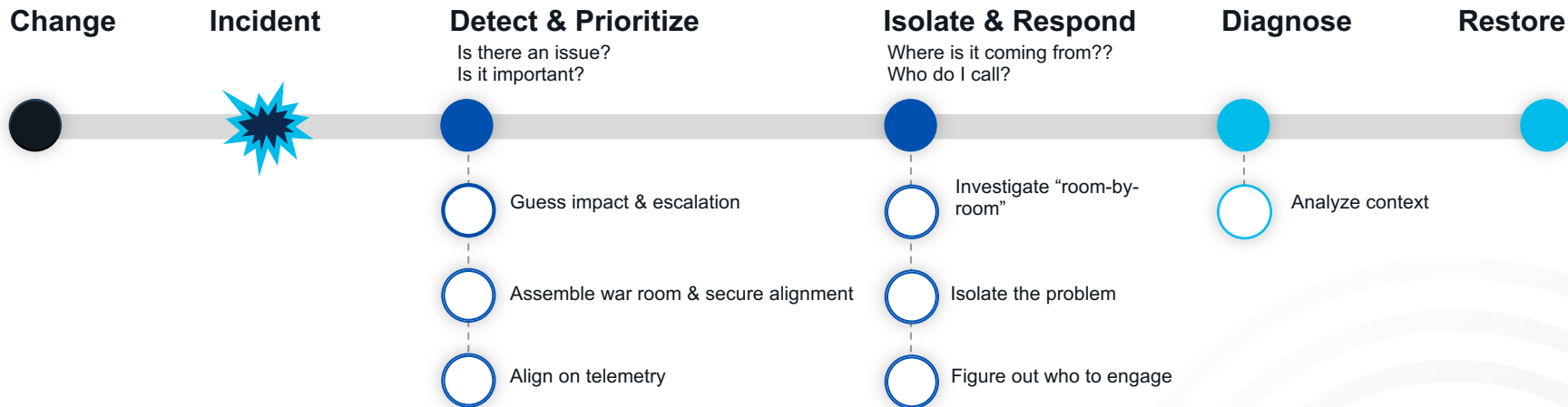
Tapan Shah - Director of Product
Isha Gandhi - Sr. Product Manager
BRKOBS-1939



Today's Plan

- Ingredients for effective Incident Management
- Introduction to Event Analytics in IT Service Intelligence (ITSI)
- Demo of ITSI
- Q&A

It Takes Too Long to Detect | Investigate | Respond



Top trends impacting IT Operations teams today

2.7X

more alerts to process
daily than 5 years ago

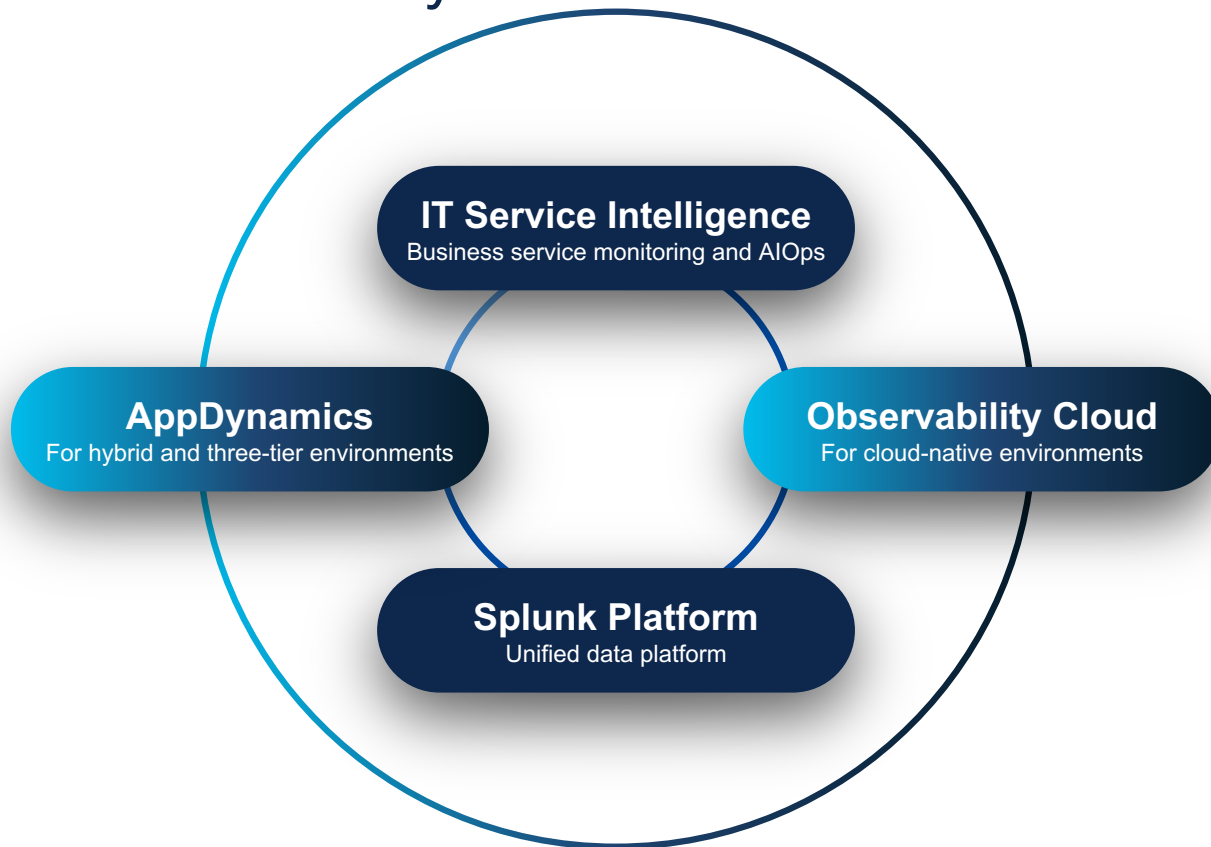
84%

of IT organizations say event
correlation is their top need

\$365K

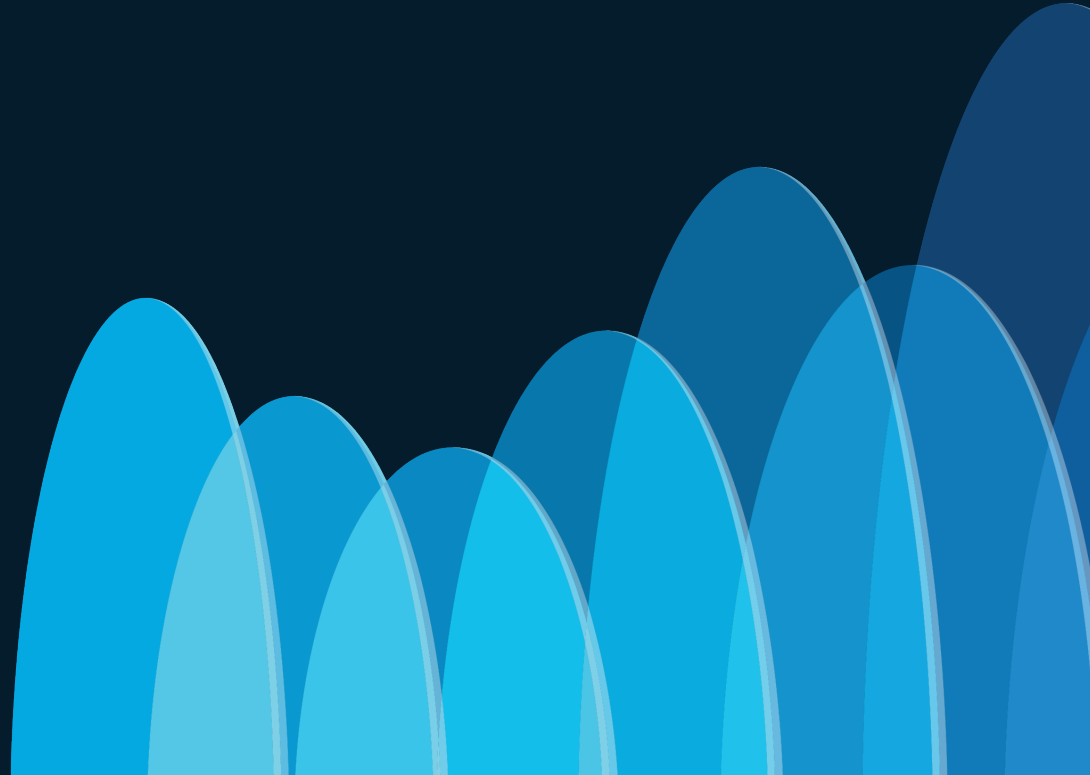
in lost revenue and
productivity annually

Splunk Observability



IT Service Intelligence

CISCO *Live!*



Splunk® IT Service Intelligence

Reduce alert noise for faster issue resolution

Isolate incidents when they happen, quickly investigate & triage root causes

Visibility into business KPIs and tech stack health

Ensure performance by connecting infra and app metrics across data sources to business KPIs

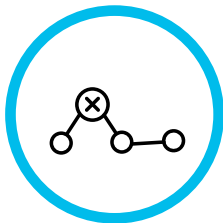
Better customer experience with fewer outages

Prevent end user impacting incidents by predicting degradation using AI and machine learning



Splunk® IT Service Intelligence

Anomaly
Detection



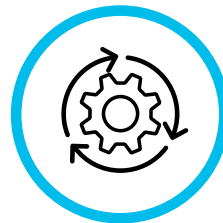
Alert Noise
Reduction



Probable Root
Cause



Automation &
Remediation



Proactive
Outage
Prevention



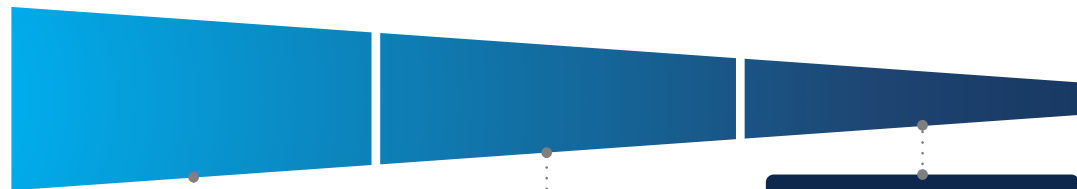
Align to what the business cares about

Accelerate MTTR with alert noise reduction

100k
Events / Minute

10s
Episodes

10
Escalations



Event Grouping

Automated Actions

Episode Management

User defined
groups

AI/ML

Create tickets

Bi-directional
updates

Execute
playbook

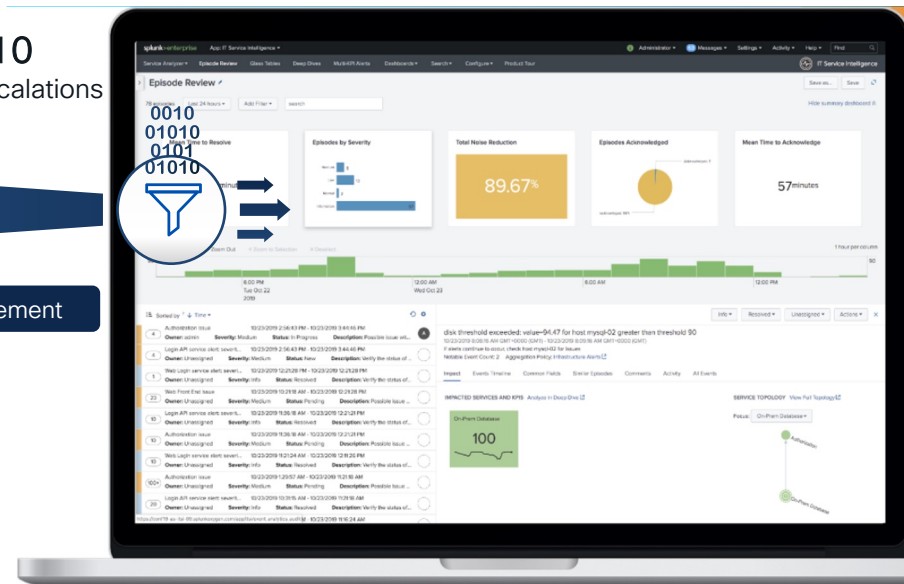
Run script

Manage
episodes

Investigate

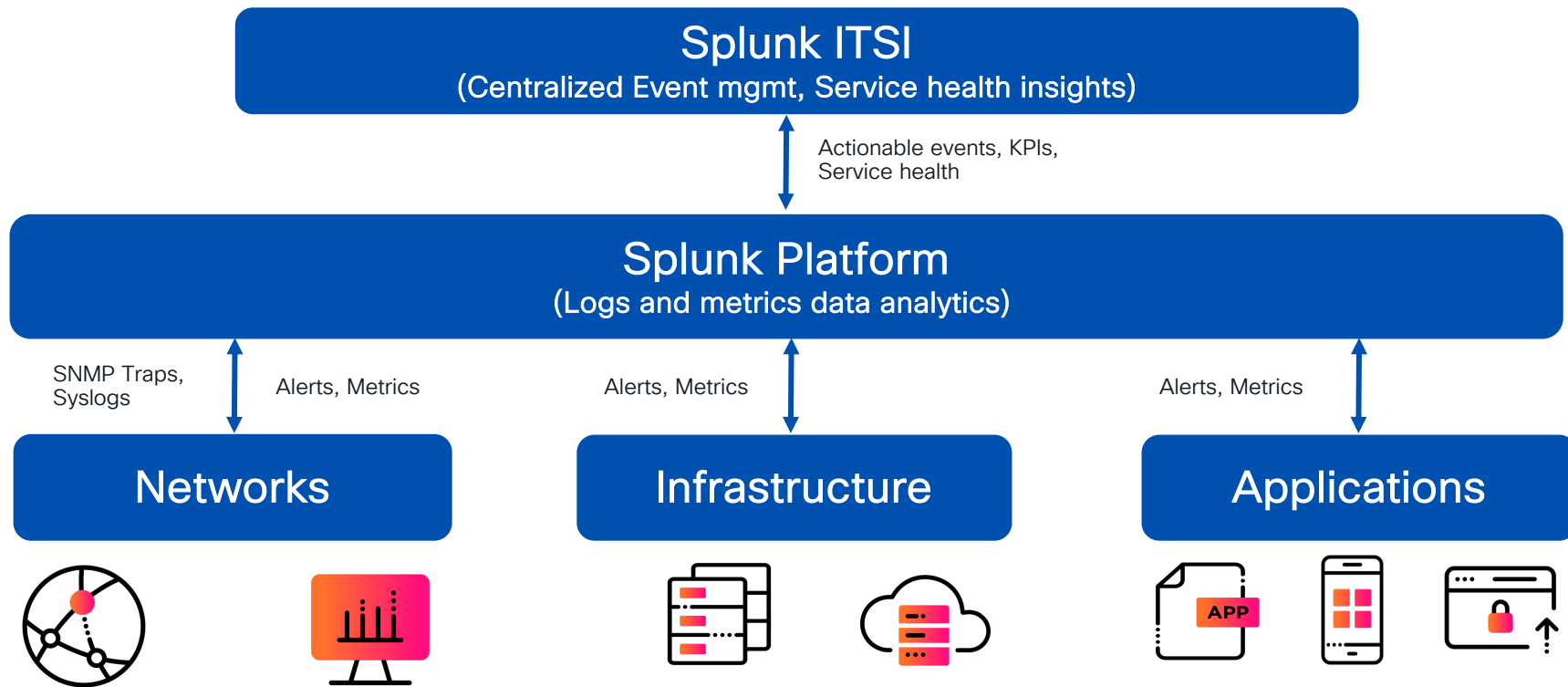
Resolve

Escalate



Manager of Managers (MoM) for single pane of glass

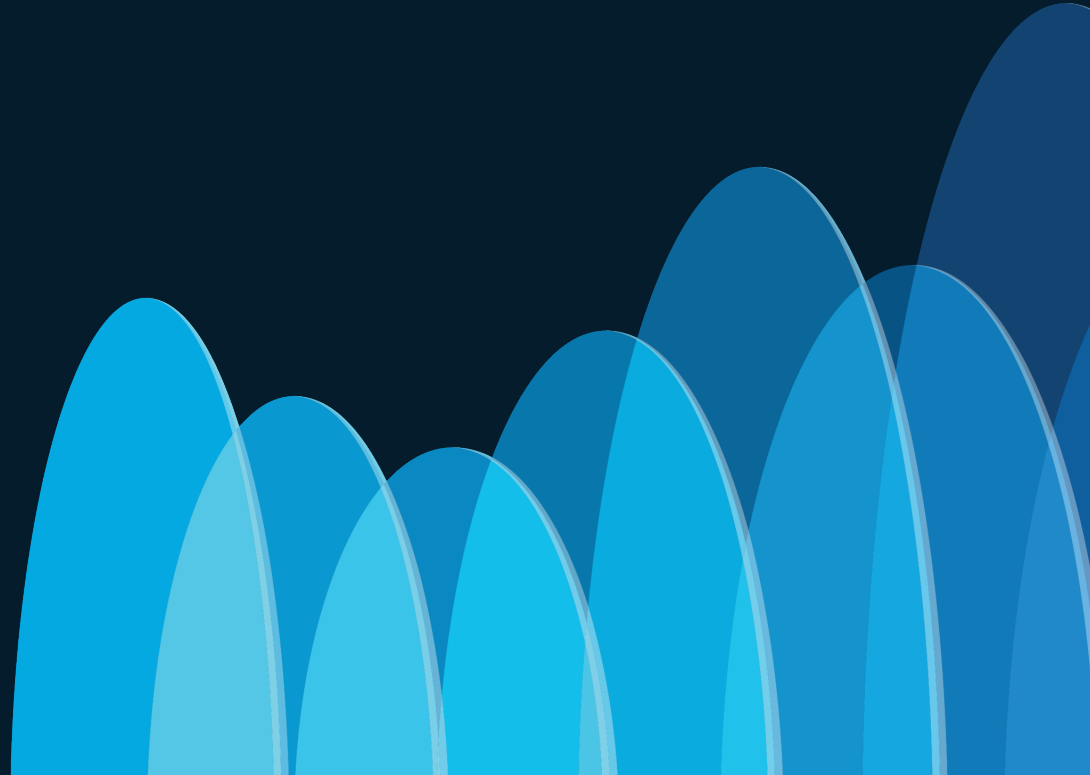
Cross-domain data correlation for network, infrastructure, app, user experience



Top use cases for network event correlations

- 1. Deduplication / suppression of alerts** (incl. SNMP traps)
 - Same alert coming from the same network device
 - Same alert coming from multiple network devices
 - Multiple alerts from the same device
 - Trap or alert storm detection and suppression of noisy sources / traps
- 2. Automated down/up alert correlations**
- 3. Detecting flapping interfaces via up/down alert patterns**
- 4. Parent-child alert correlations**
 - Sub-interface alerts under physical interface alerts
 - Network device to NIC alert correlations
- 5. Topology based alert correlations**

Closed Loop Incident Management



Ingredients for Closed Loop Incident Management

Step 1

Ingest & Normalize



Services, KPIs, entities
Logs, metrics, events

splunk>

Ingredients for Closed Loop Incident Management

Step 1

Ingest & Normalize



Services, KPIs, entities
Logs, metrics, events

splunk>

Step 2

Enrich & Contextualize



Detect anomalies



Deduplicate & suppress

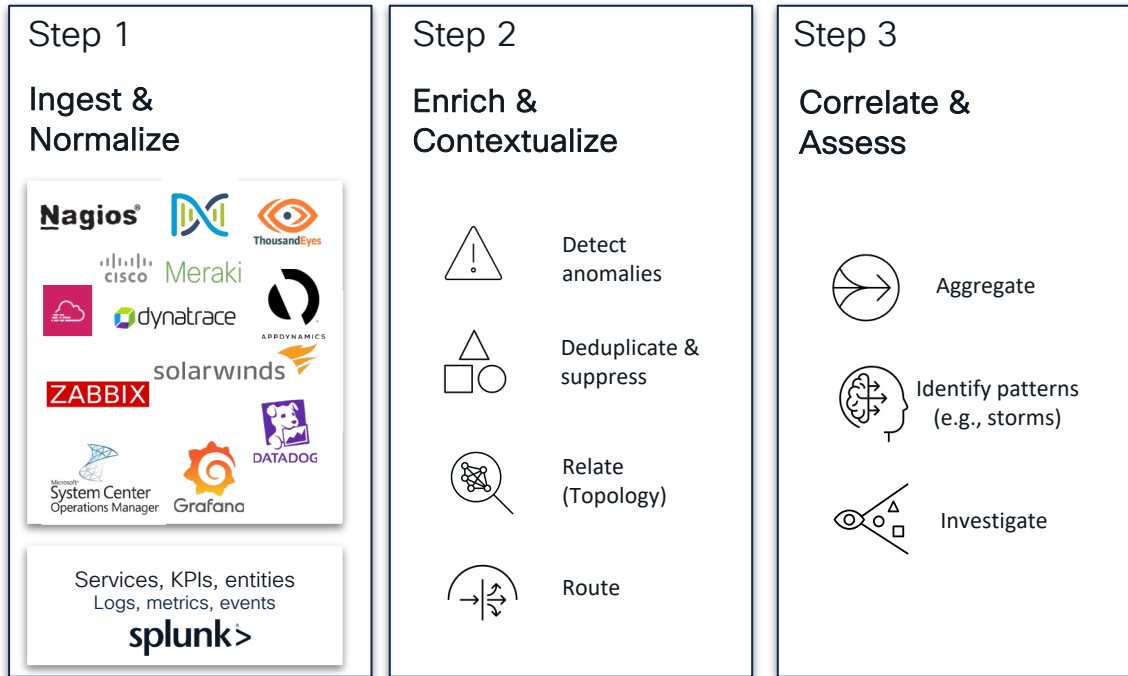


Relate (Topology)



Route

Ingredients for Closed Loop Incident Management

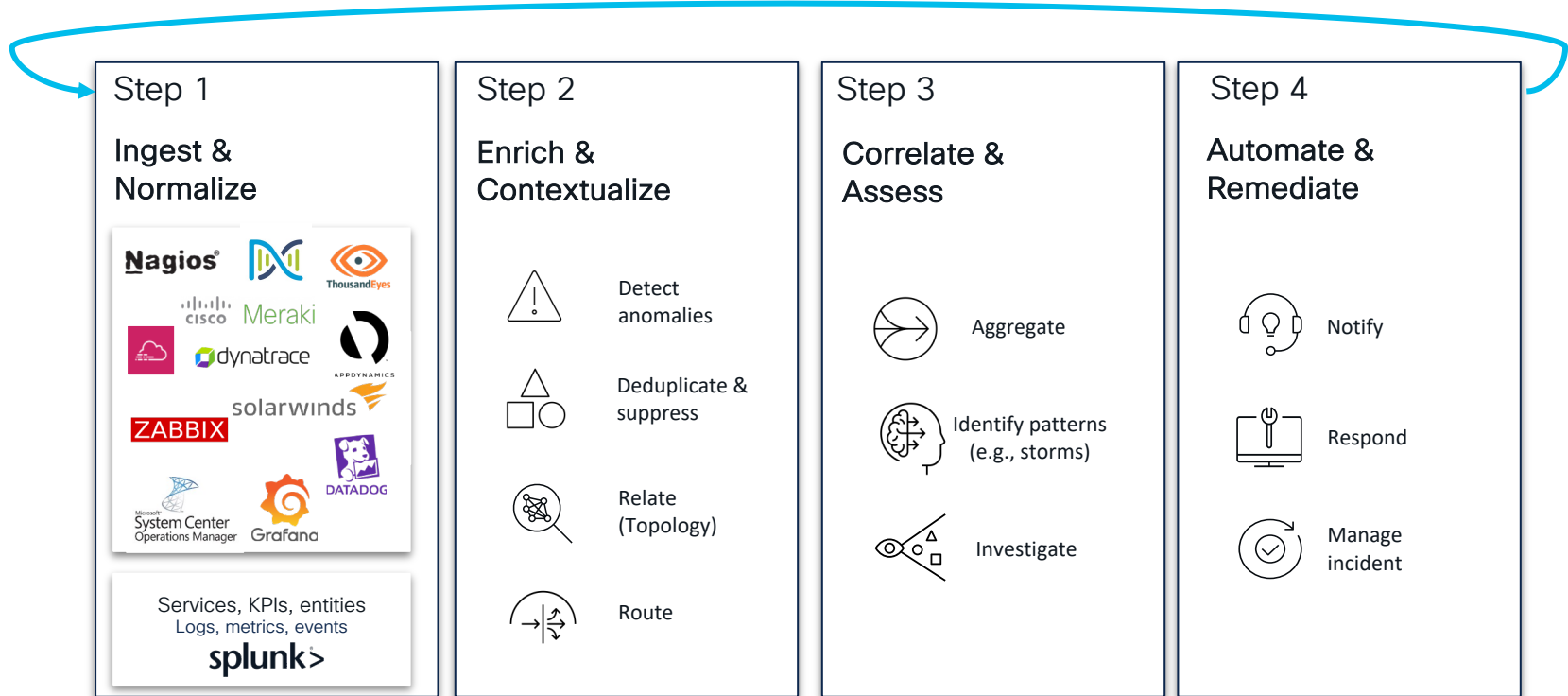


Ingredients for Closed Loop Incident Management



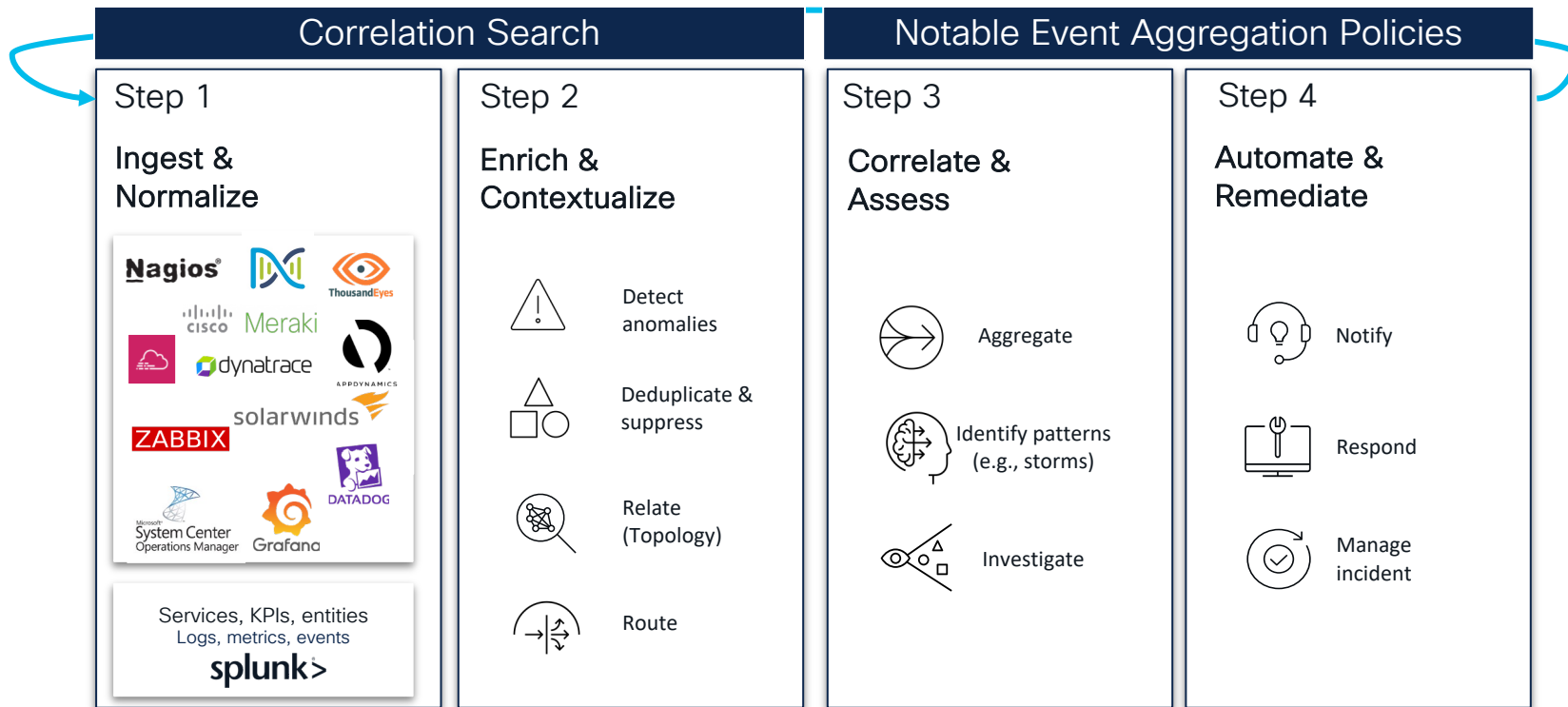
Ingredients for Closed Loop Incident Management

Step 5 Continuous Improvement

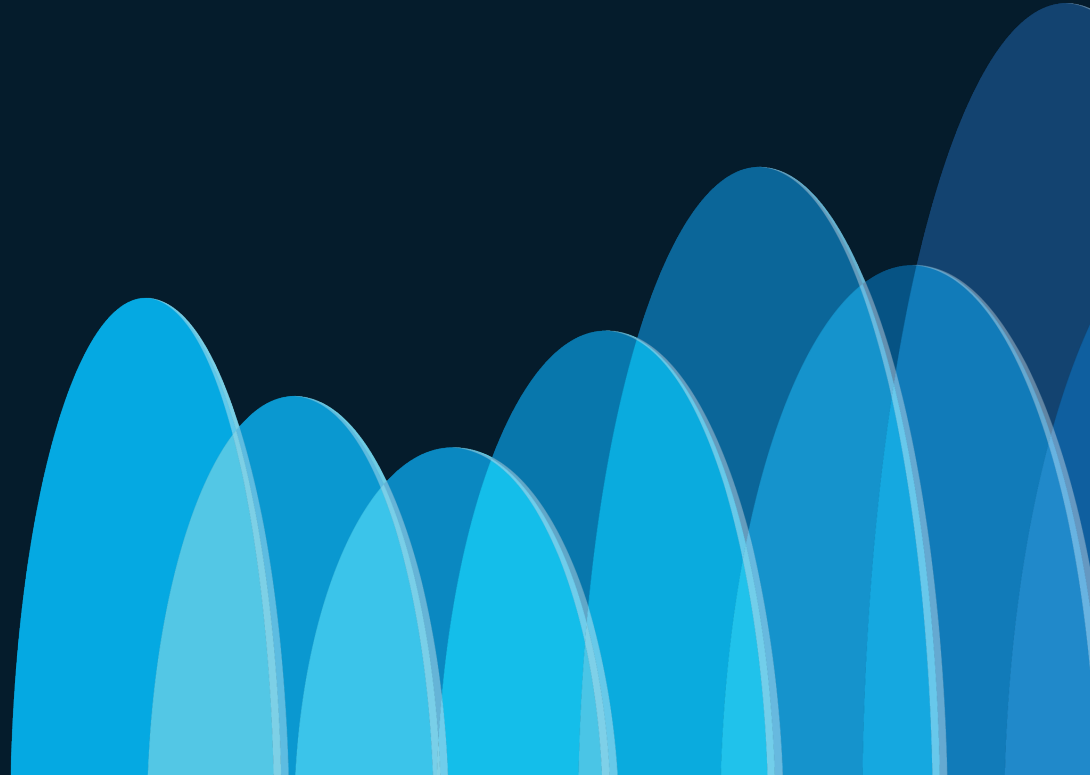


Ingredients for Closed Loop Incident Management

Step 5 Continuous Improvement

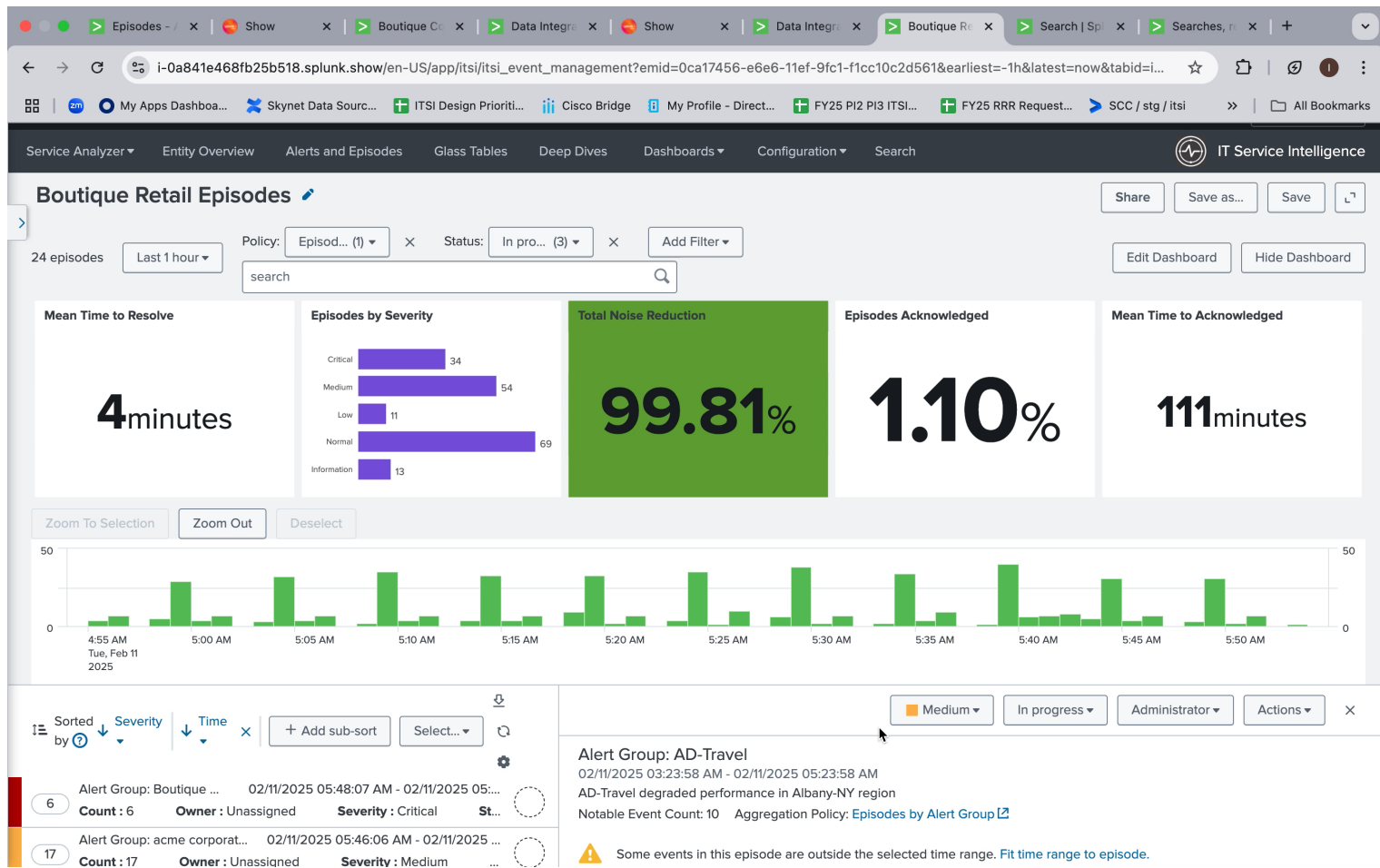


Let's see it in
action



Video

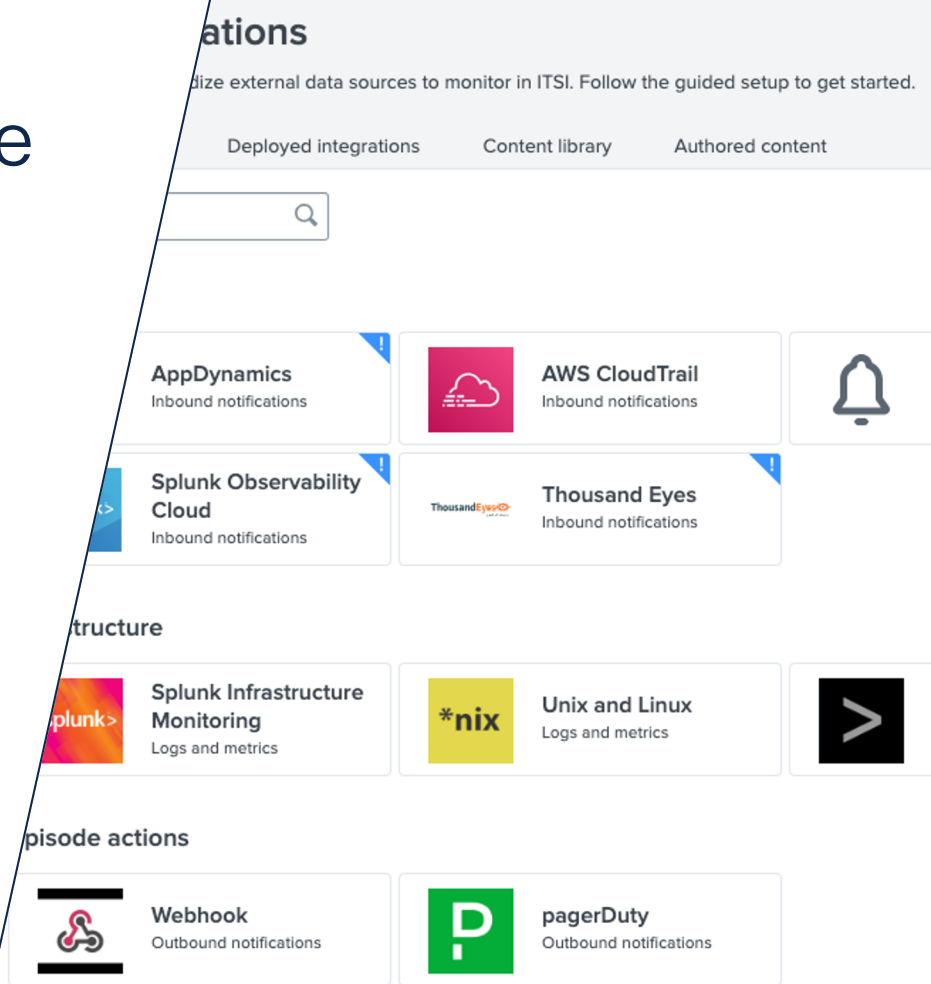




Step 1: Ingest & Normalize

Cross-domain alert ingestion and creation

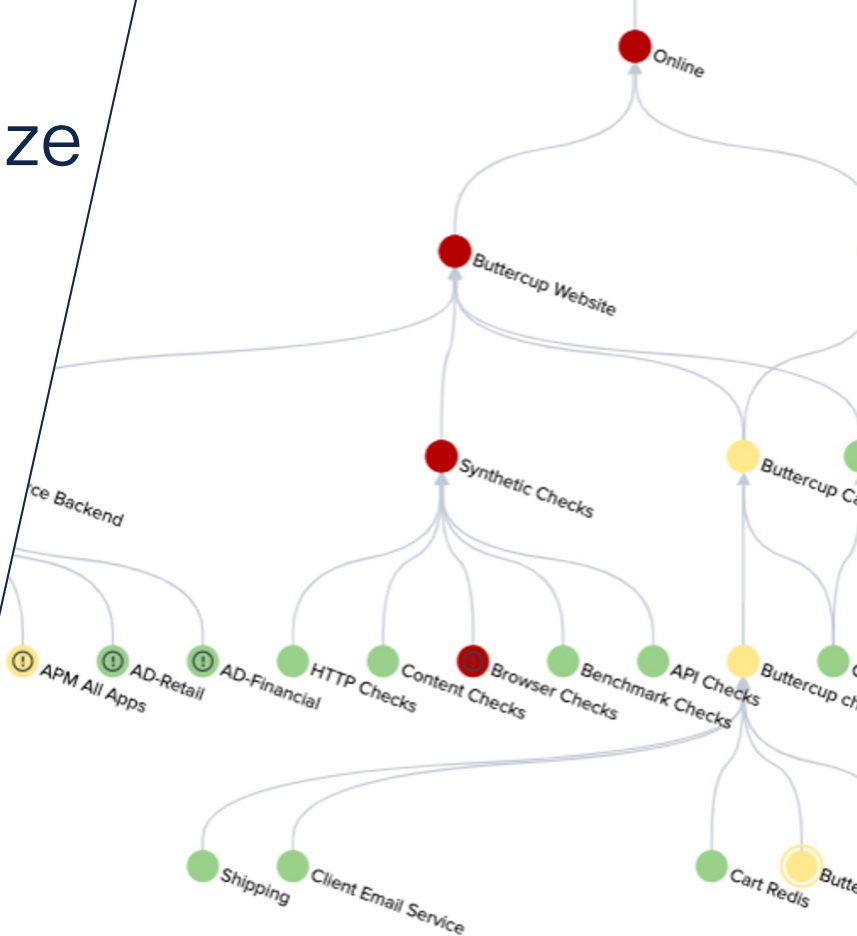
- Use the ITSI Content Pack for Monitoring and Alerting
- Standardize your data using the Common Information Model
- Include key metadata for correlation and routing in alert payload (e.g. drill-down links, dependencies, affected entities, assignment group)



Step 2: Enrich & Contextualize

Augment and prepare alerts for correlation

- Import key entities and services from your CMDB or asset management tools
- Derive dynamic service, KPI and maintenance window enrichment through service topology
- Proactively anomalies on your KPIs and entities with
 - Automated ML-based thresholding
 - Service health predictive analytics



Step 3: Correlate & Assess

Cluster alerts into episodes to accelerate MTI

- Out-of-the-box aggregation policies (NEAPs) to create episodes
 - **Deduplicate** Source, Alarm
 - **Correlate** Services, Alert Group
- Prioritize incidents by easily identifying unique and risky episodes
- Use Alert and Episode Storm Detection to identify issues and common root cause across episodes



Step 4: Automate & Remediate

Accelerate MTTR with automated actions

- Automate ticket creation and updates with Action Rules
 - Bi-directional integration with ServiceNow, Jira ITSM, BMC Remedy/Helix
 - Outbound webhook integrations (E.g. PagerDuty, Splunk On-call)
- Auto-remediate by
 - Integrating with your automation tools (E.g. Ansible, Puppet, SOAR)
 - Executing custom scripts
 - Integrating homegrown tools using alert actions

Action Rules

Define action rules to take automated actions on an episode when

> If a specific event occurs, then add a comment for the episode

> If the episode is broken, then change status to Closed for the

> If a specific event occurs, and the number of events in this episode

> If a specific event occurs, then change status to Closed for the

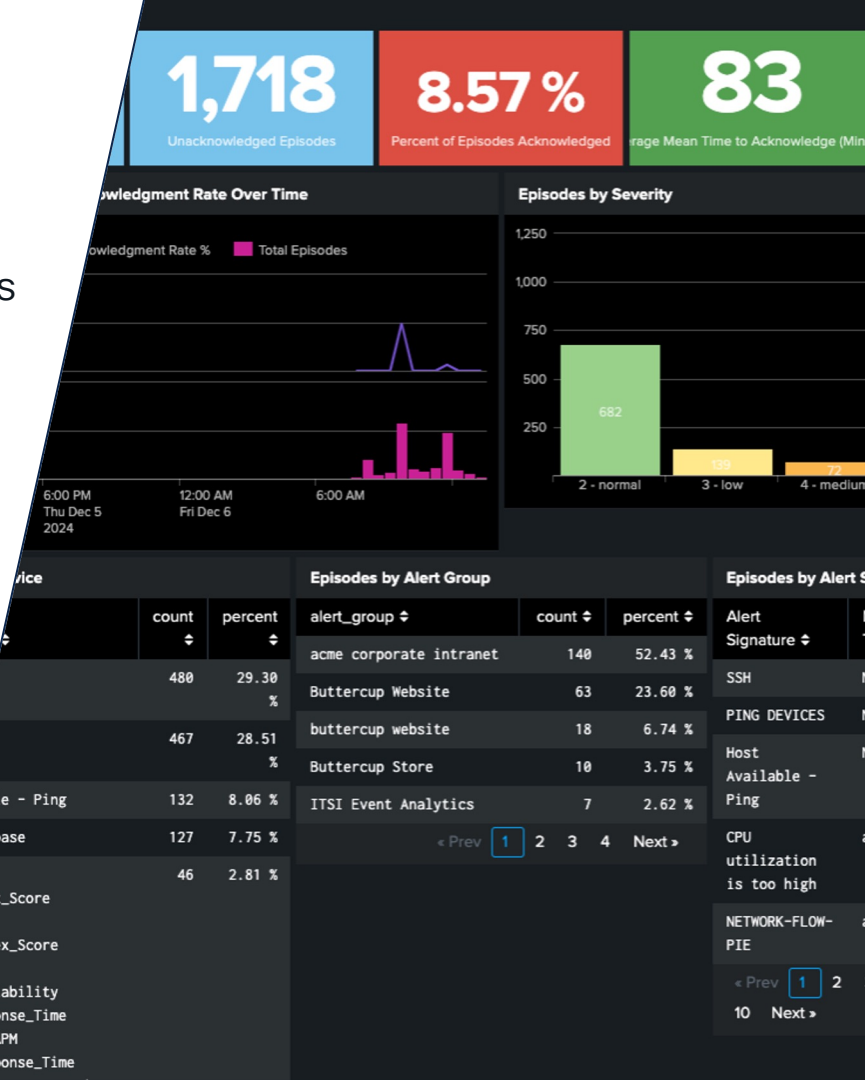
> If a specific event occurs, then add a comment for the episode

+ Add Rule

Step 5: Continuous Improvement

Monitor and advance your Event Analytics workflows increasing auto-remediation

- Leverage Incident and Operations Posture Dashboard to track improvement over time
- Get insights into noisy sources and services with poor health
- Optimize thresholds and monitoring configurations if you're seeing chatty sources with Configuration Assistant



Takeaways

1. Leverage ITSI Event Analytics to reduce alert noise and get actionable insights into episodes
2. Accelerate time to value by normalizing data following the Common Information Model and installing the Content Pack for Monitoring and Alerting
3. Incorporate service dependencies from a CMDB or any other source for topology driven correlation
3. Leverage ITSI's OOTB ML capabilities for proactive detection of anomalies and alert patterns



Webex App

Questions?

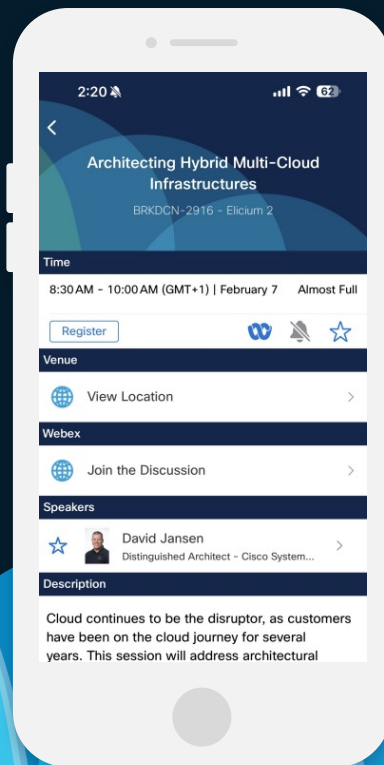
Use the Webex app to chat with the speaker after the session

How

- 1 Find this session in the Cisco Events mobile app
- 2 Click “Join the Discussion”
- 3 Install the Webex app or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

BRKOBS-1939

Webex spaces will be moderated by the speaker until February 28, 2025.



Fill Out Your Session Surveys



Participants who fill out a minimum of 4 session surveys and the overall event survey will get a unique Cisco Live t-shirt.

(from 11:30 on Thursday, while supplies last)



All surveys can be taken in the Cisco Events mobile app or by logging in to the Session Catalog and clicking the 'Participant Dashboard'



Content Catalog

Continue your education



- Visit the Cisco Observability Showcase for related demos
- Book your one-on-one Meet the Engineer meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at ciscolive.com/on-demand. Sessions from this event will be available from March 3.

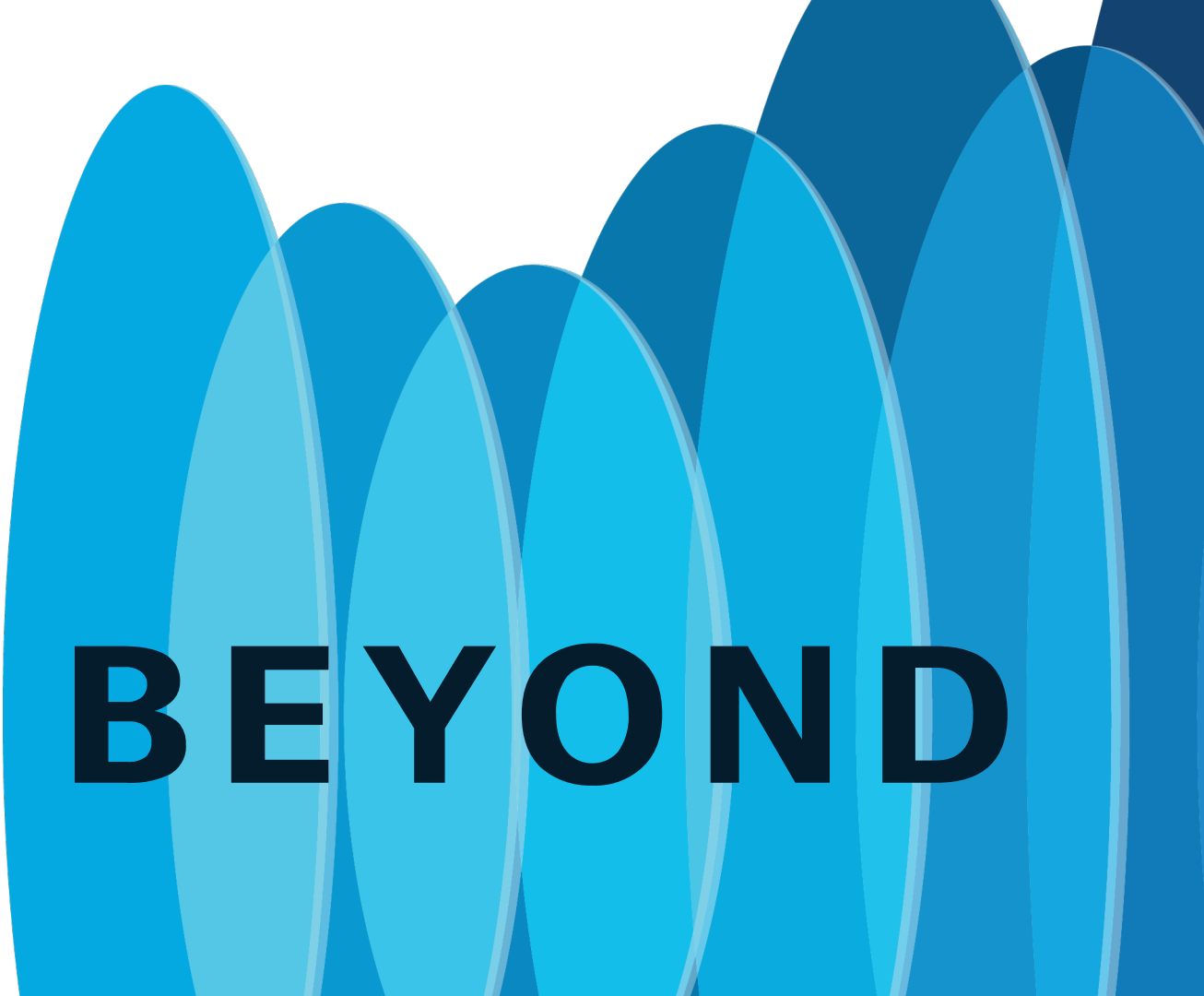
Contact me at: ishgandh@cisco.com,
tapashah@cisco.com



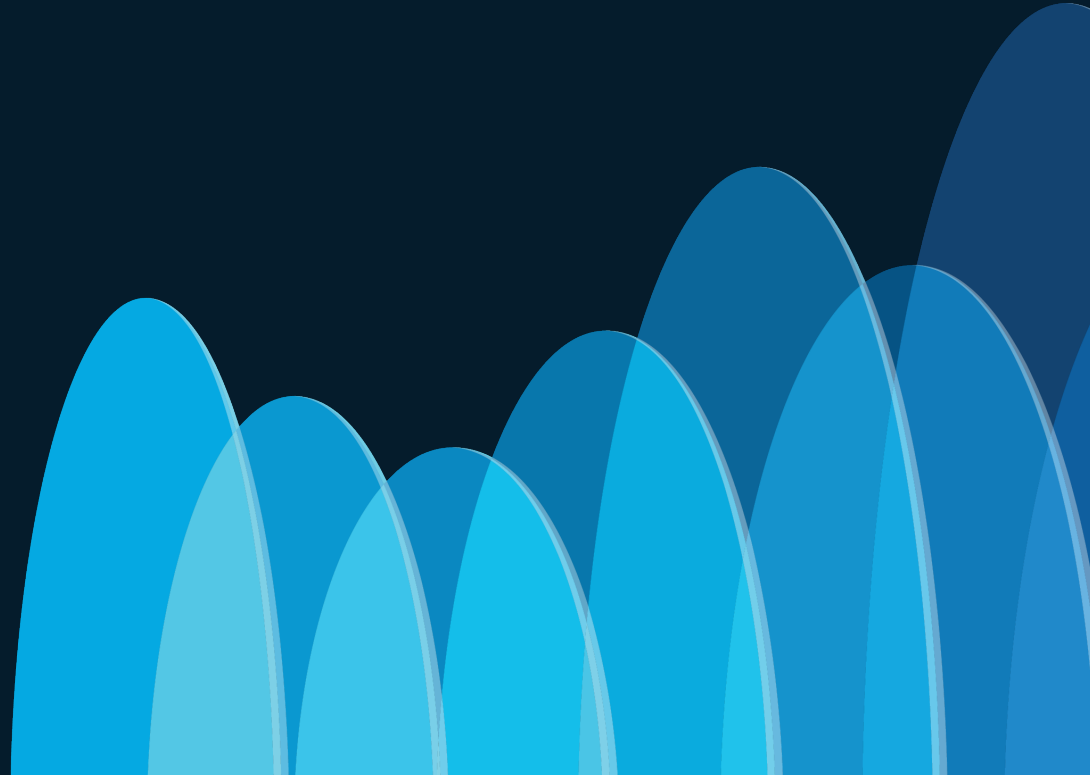
Thank you

CISCO *Live!*

GO BEYOND

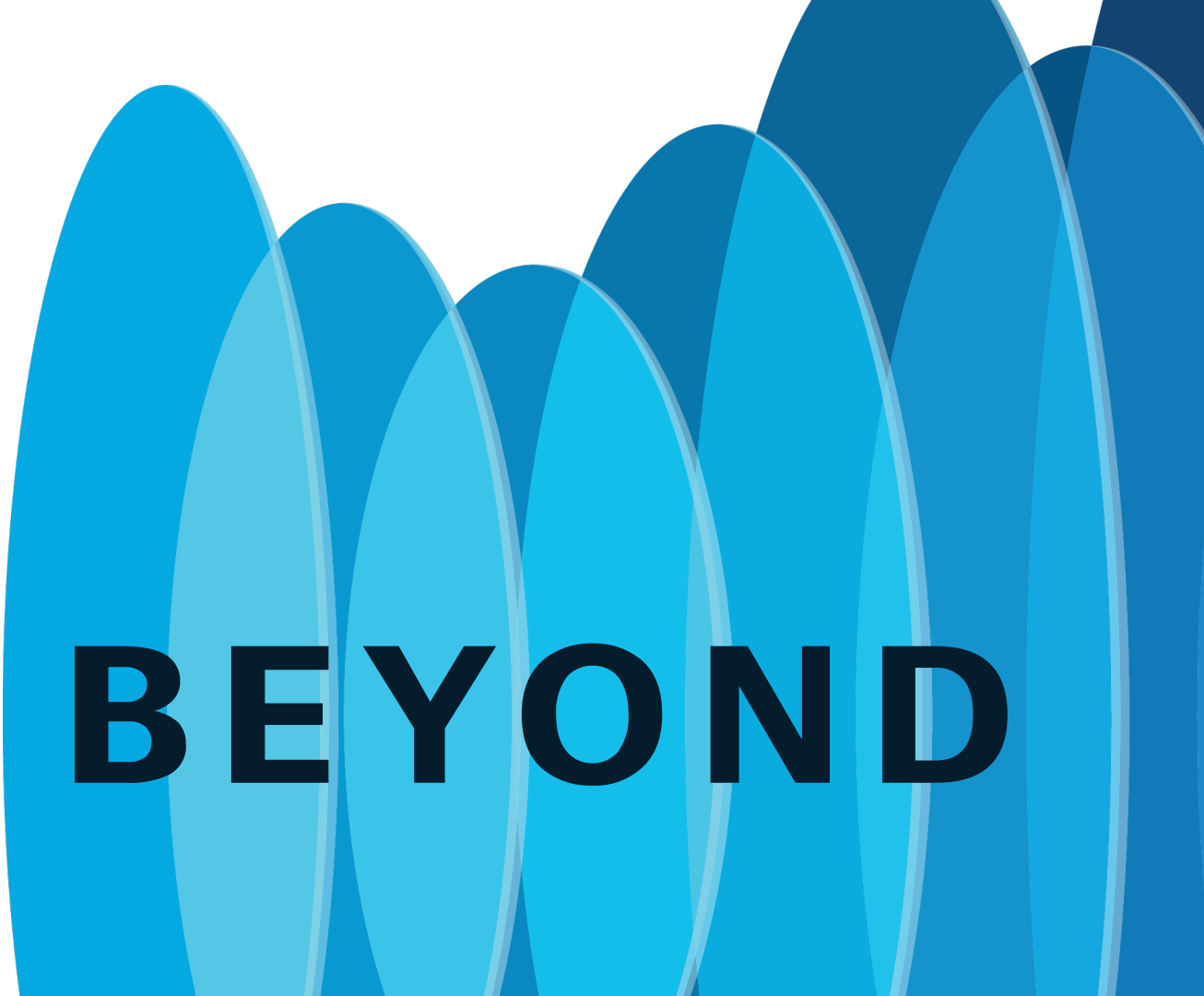
An abstract graphic on the right side of the image consisting of several overlapping, vertically-oriented oval shapes in various shades of blue, ranging from light sky blue to deep navy blue. The ovals are layered to create a sense of depth and movement, extending from the top to the bottom of the frame.

Appendix



CISCO *Live!*

GO BEYOND

The background of the slide features a series of overlapping, teardrop-shaped elements in various shades of blue, ranging from light sky blue to deep navy blue. These shapes are arranged in a way that creates a sense of depth and movement, with some shapes appearing to be in front of others. The overall effect is a modern, abstract design that complements the 'GO BEYOND' theme.