

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC

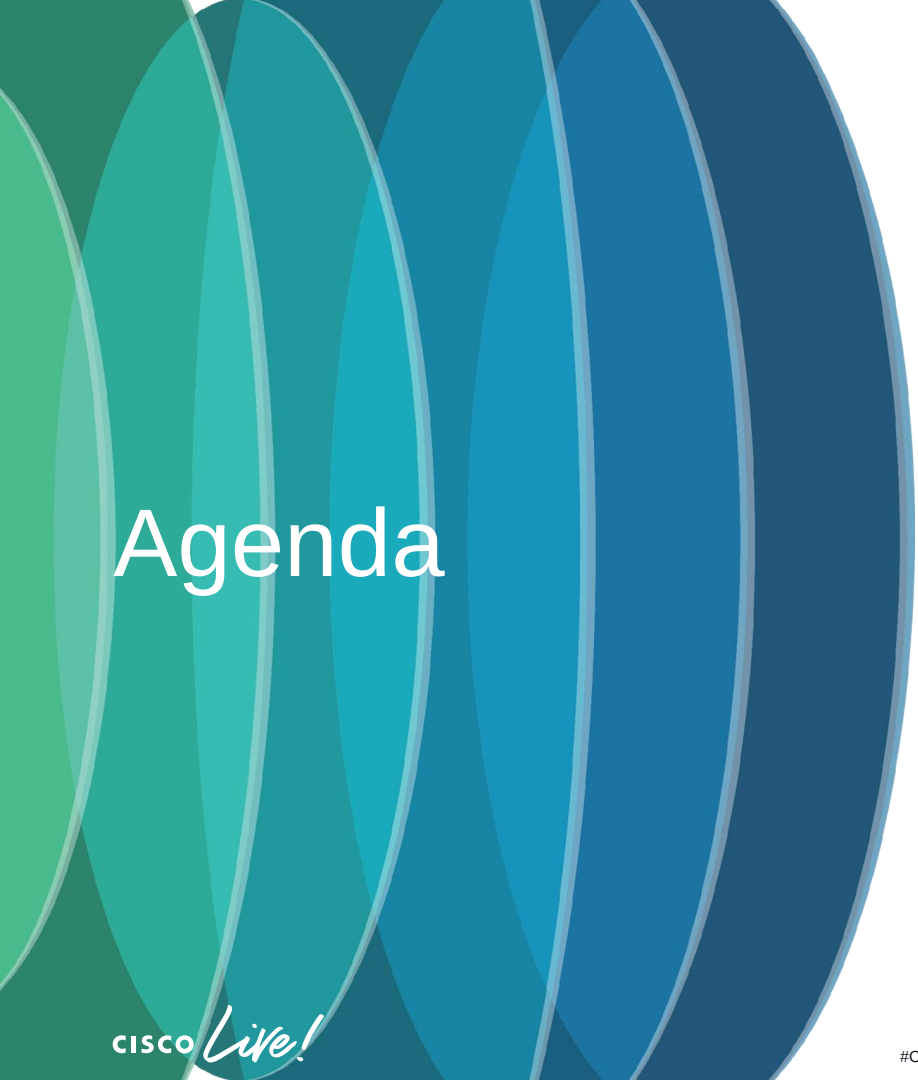


AI in Observability

Mukund Babbar
Staff Solutions Architect
Session ID - BRKAPP-2548



#CiscoLiveAPJC



Agenda

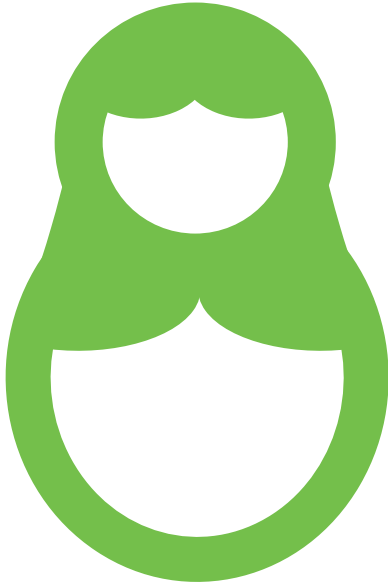
- AI concepts
- Why AI in Observability
- How Splunk can help?
- Embedded and Custom AI/ML
- AI assistant

What is AI?

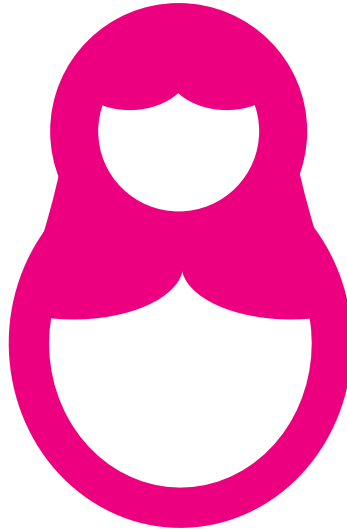


What is AI?

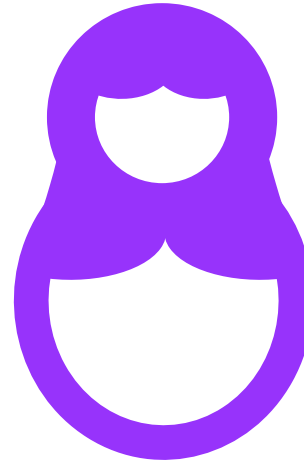
Artificial
Intelligence



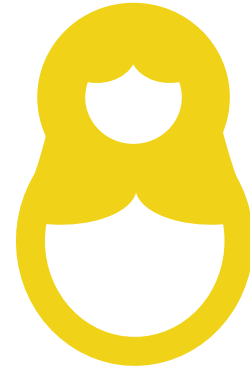
Machine
Learning



Deep
Learning



GenAI

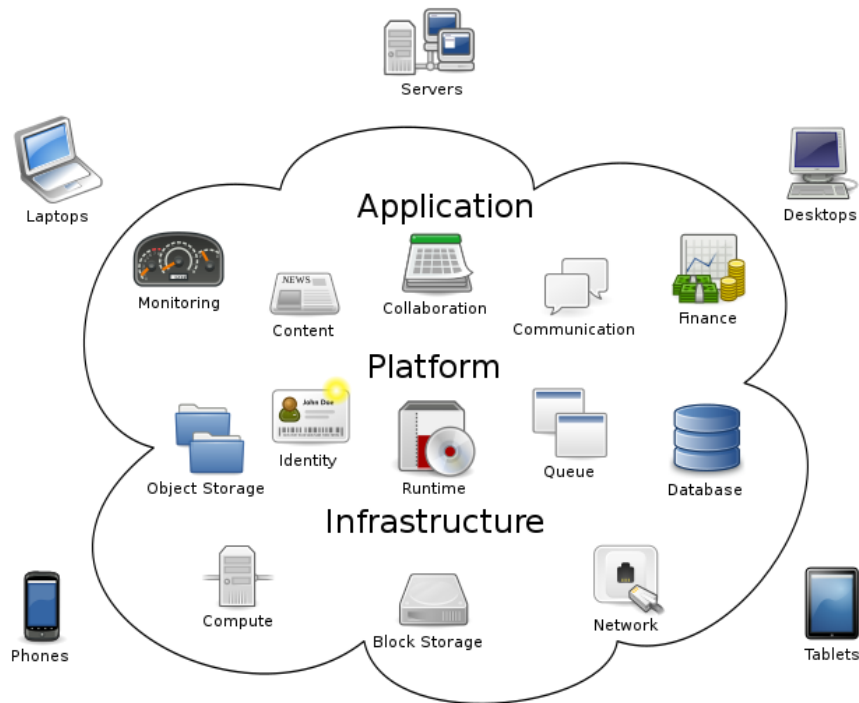


Why AI in Observability?



Have you ever...

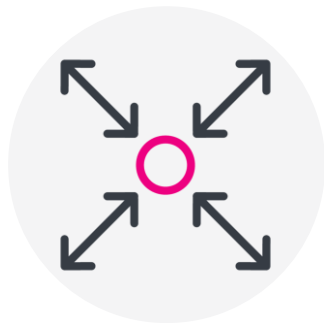
...felt
overwhelmed
by the
complexity
of your tech
stack?



...been asked to
learn new tools
and processes
when you don't
have the time?



It's harder than ever to troubleshoot fast



Increasingly
complex
environments



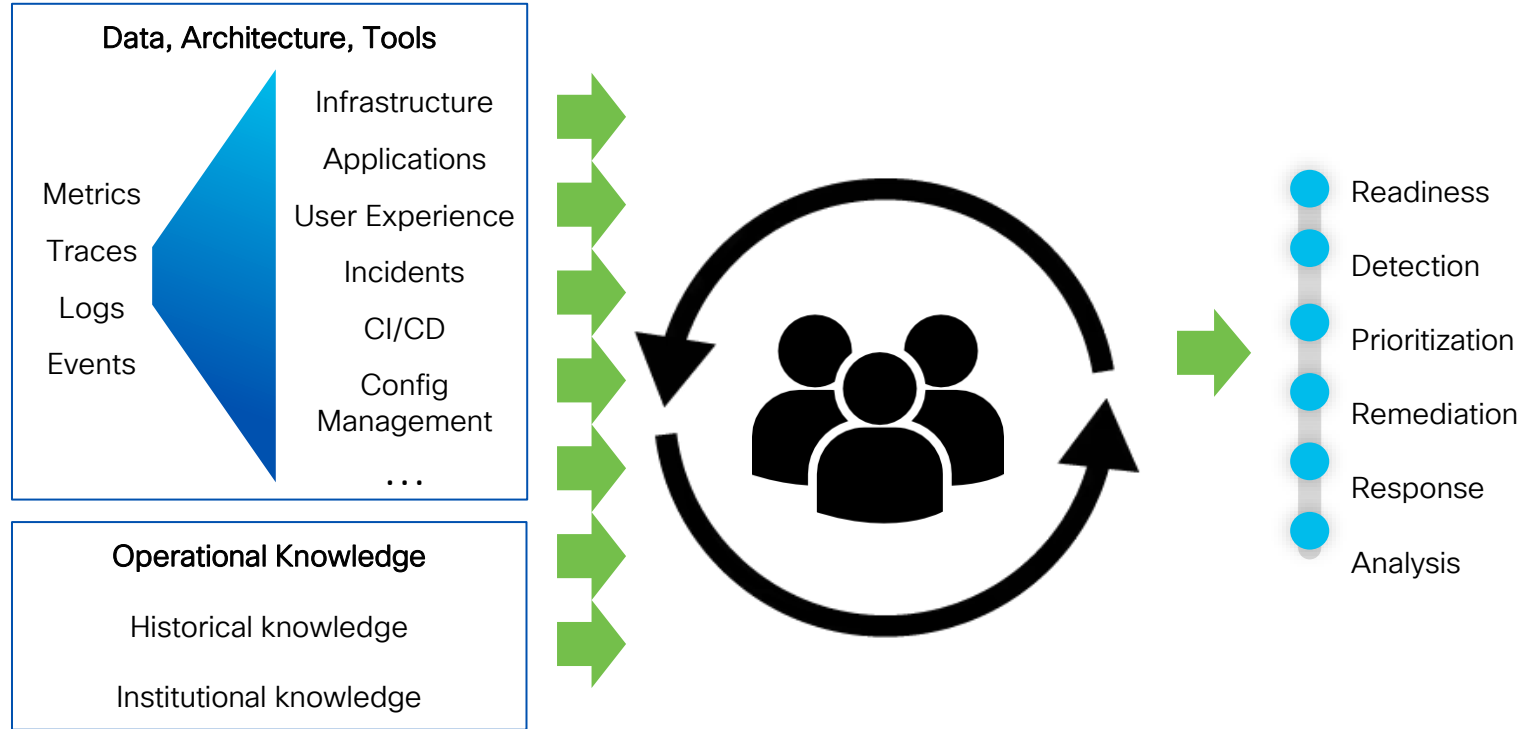
Explosion of
monitoring solutions



No time for
learning new tools
or processes

Complex Data, Architecture and Tools

Too much toil, guesswork and expensive manual effort

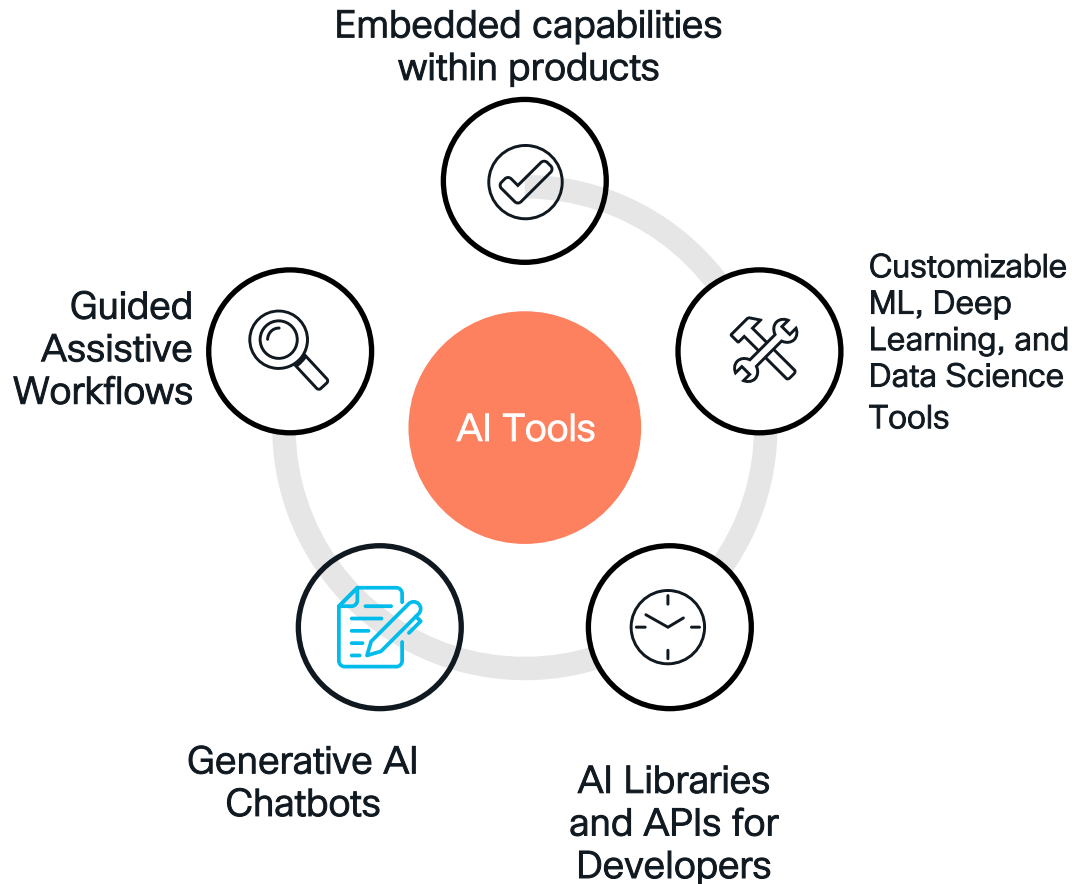


...spent hours
looking for
the root cause
and debugging
outages?

<https://pixabay.com/vectors/employee-desk-stress-exhausted-6038877/>

Where is **AI leveraged**
in Splunk products?

Splunk
has been
innovating
with AI
for a while
now.

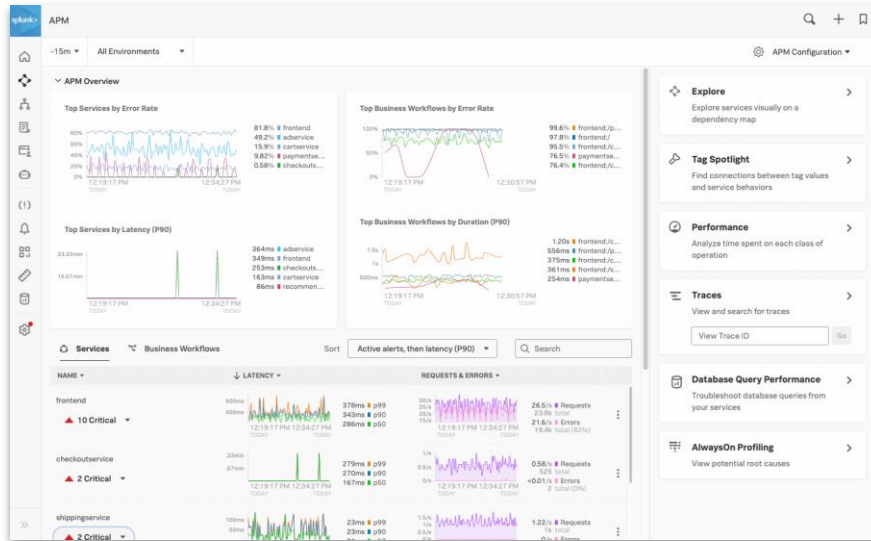


AI Embedded within Products



Splunk Application and Infrastructure Monitoring

More accurate and efficient alerting for your infrastructure and services



Use machine learning to **improve accuracy** and **reduce manual effort** across infrastructure and service alerting

- Establish performance baselines across every service
- Automate alerting by receiving recommendations for the biggest spikes in latency, errors, and resource utilization
- Easily customize alert thresholds and subscribe to notifications for specific services or teams

Splunk IT Service Intelligence (ITSI)

Splunk's AIOps Solution

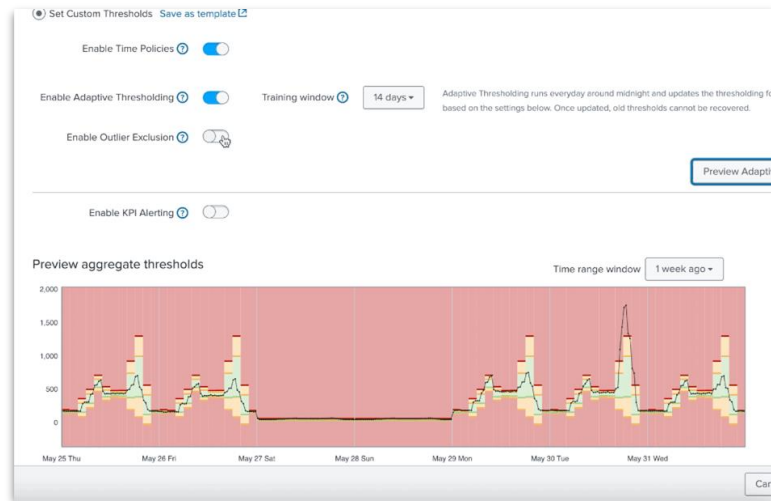
Splunk ITSI applies machine learning to **proactively prevent outages** by correlating and reducing alerts, monitoring service health, and streamlining incident management.

- Alert correlation to reduce alert noise
- Adaptive (dynamic) thresholds incorporate seasonality
- Outlier Exclusion in Adaptive Thresholds
- Find and suggest similar historical incidents
- Predict service health to prevent outages

.conf24 ★

New updates!

- ML-Assisted Thresholding (*Preview*)



Powerful Machine Learning Across The Platform

Make IT Effective, Proactive and Predictive

Anomaly Detection



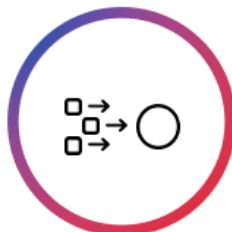
Alerts triggered automatically by anomalous activity
Incident responders can see across all silos to find a quicker MTTR

Dynamic Thresholding



Thresholds adapt in real time
Trend and alert on anomalous behaviour
Prevent service degradation

Event Clustering



Detect and highlight the events that matter
Prioritize events that need action taken

Intelligent Alerting



Advanced problem detection increases alert fidelity
Automatically identify and alert on risky service behaviour

Prediction



Predict outages and anomalies before they occur
Act on predictions so services are not affected

Splunk On-Call

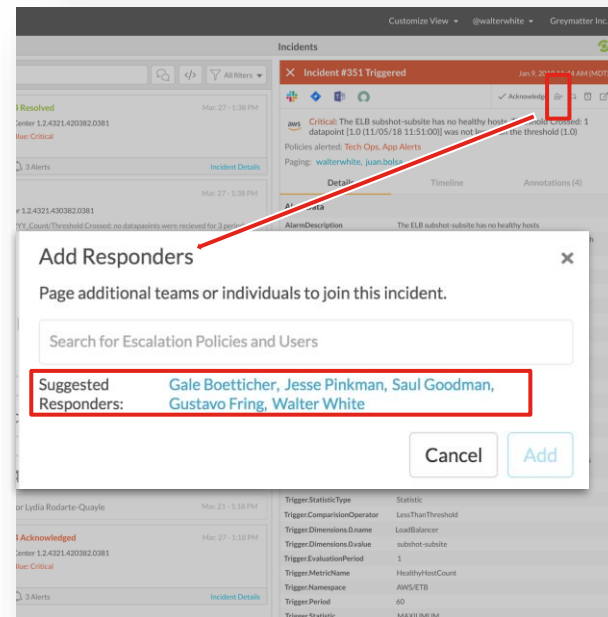
Incident Correlation

Splunk On-Call **leverages ML** to correlate like incidents and decipher which person or people have worked on similar incidents in the past.

The **Suggested Responders** are listed when a user clicks **Add Responder**—making it possible to loop in knowledgeable colleague/s to the firefight in moments.

Benefits:

- Reduce isolation
- Leverage tribal knowledge to reduce MTTR
- Improve morale/ reduce burn out

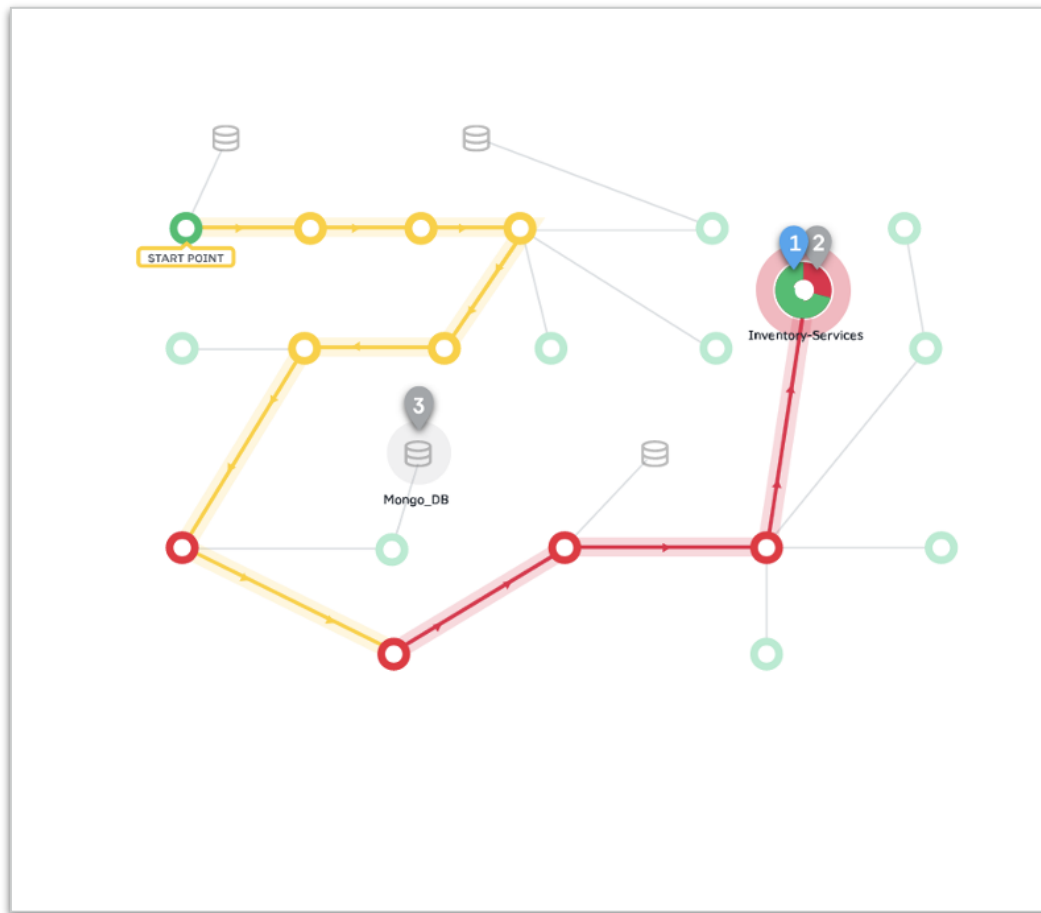


Automated RCA

When an anomaly gets detected for a particular Business Transaction (BT), next step is to understand why or the probable root cause.

Anomaly Detection uses AI capabilities to enable Automated Root Cause Analysis to monitor the health of all the entities involved in that BT and shows the suspected causes.

It further allows user to drill down into deviating metrics and snapshots, as desired.



Custom AI & ML



Splunk's Customizable AI & ML Pipeline



Industrial Assets



Consumer and
Mobile Devices



OT



IT



Capture data from any
environment in real
time



Clean & prepare data
using Splunk's
powerful search
processing language



Inference pre-trained
models on newly
incoming data



Take action on
inference results!



Train and deploy
custom AI & ML
models

Iterative Feedback Loop

Splunk Enterprise

| anomaly detection command

New Search

Save As ▼Create Table ViewClose

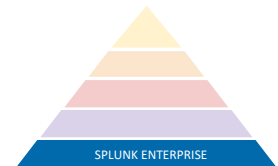
| inputlookup logins.csv | anomalydetectionLast 7 days ▼

✓ 3 results (4/13/22 1:00:00.000 PM to 4/20/22 1:49:41.000 PM)No Event Sampling ▼ Job ▼Smart Mode ▼

EventsPatterns**Statistics (3)**Visualization

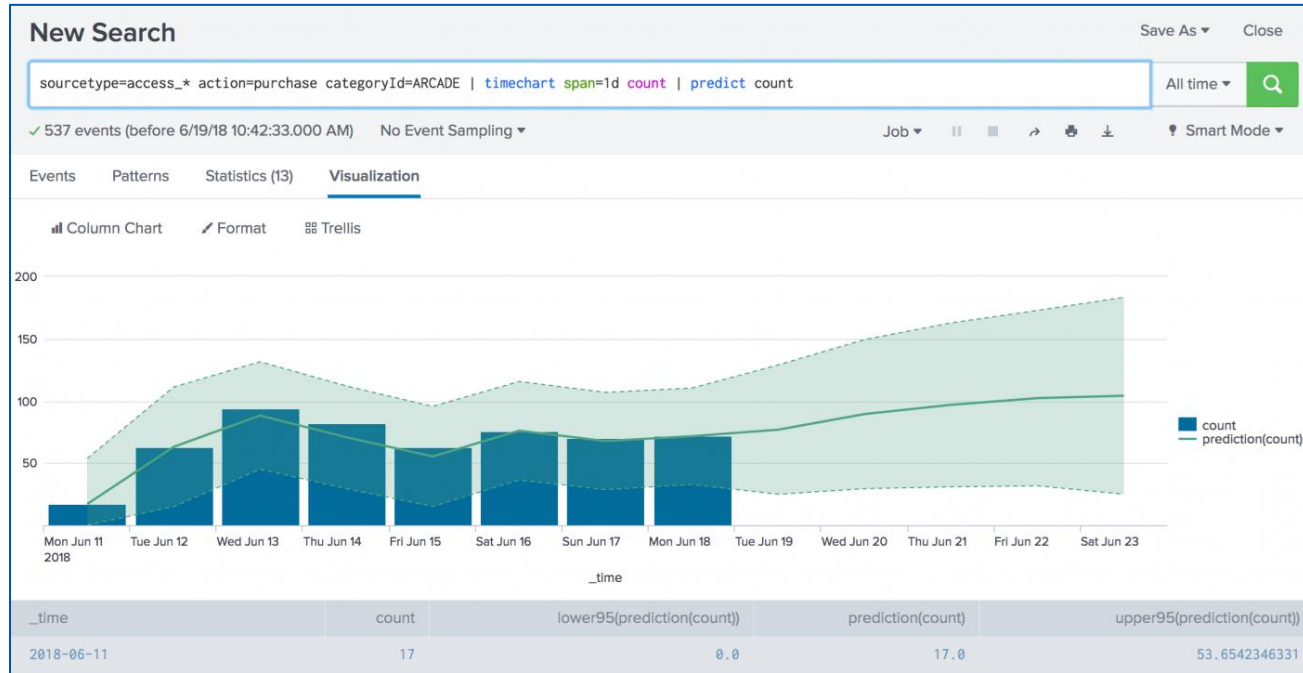
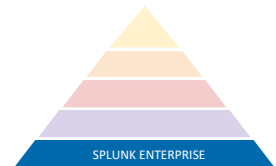
20 Per Page ▼ FormatPreview ▼

_time ↕	log_event_prob ↕ 	logins ↕ 	max_freq ↕ 	probable_cause ↕ 	probable_cause_freq ↕ 
2015-11-30 16:00	-5.4327	508	0.29343	logins	0.00437
2015-11-30 17:00	-5.4327	540	0.29343	logins	0.00437
2015-11-30 18:00	-5.4327	527	0.29343	logins	0.00437



Splunk Enterprise

| predict command



Splunk App for Anomaly Detection 1.1

Find anomalies in time-series datasets in just a few clicks!



Beginner friendly

No need for complex SPL queries, parameter tuning, or knowledge of statistics



Quick and simple

The app detects anomalies with a couple of clicks - no trial and error required



Helps ensure accuracy

Health check diagnostics determine if the user's dataset is fit for anomaly detection with the app's algorithm



End-to-end operationalization workflow

Create anomaly detection jobs to run at regular intervals and generate alerts

Step 2: Add the Dataset
Use an SPL query to input your dataset. An example SPL query is provided that you can use to explore the app. Note that as the number of

1 | `inputlookup numenta_art_daily_flateidfile.csv`

Step 3: Select Field for Anomaly Detection
Select a field from your dataset for anomaly detection. Only numeric fields are listed in the drop-down menu.

Field For Detection

✓ Search successful.

Preview Data **Anomaly Data**

Step 4: Save & Operationalize Job
Save this anomaly detection job. From the Job Dashboard, schedule when the job is run. Once scheduled, you can create job-related alerts.

Click **Open in Search** to open a new Splunk search; the query updates a model every time it runs; to

Splunk Data Science and Deep Learning 5.1

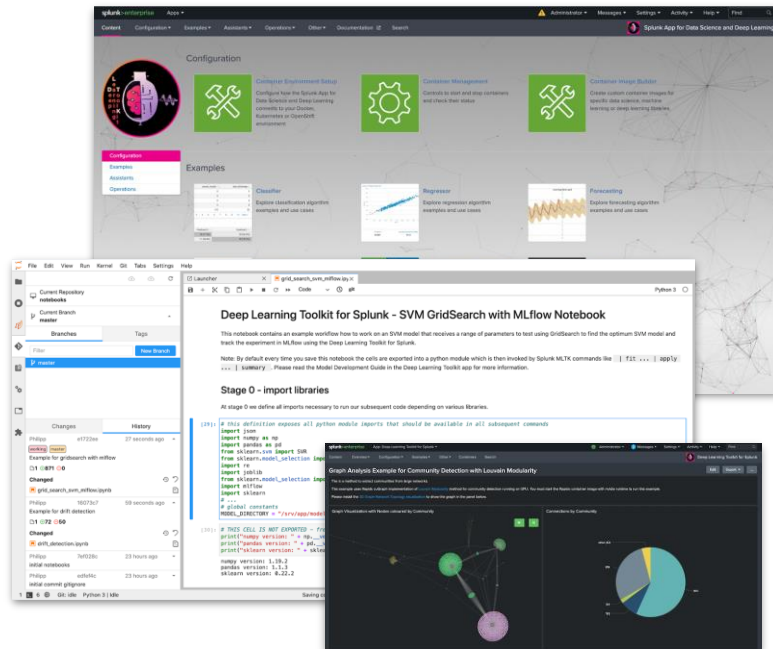
Extension for MLTK to operationalize advanced custom AI / ML use cases

Built for Data Scientists

- **35+ Code Examples:** Guided model building, testing, and deployment of data science and deep learning frameworks
- **Container Management:** Models can be productionized for scalability & optimization of resources, e.g. CPU & GPU
- **State of the art AI frameworks and tools:** Jupyter Lab, MLflow, PyTorch, TensorFlow, SpaCy, DASK, Rapids, Spark, ...
- **Flexible deployments and open source:** deploy on-prem, hybrid or in the cloud. Github repository for customization.

New updates in version 5.1!

- Two AI assistants to leverage LLMs to build and train models for text summarization and text classification use cases
- Customizable for adapting to own domain specific data

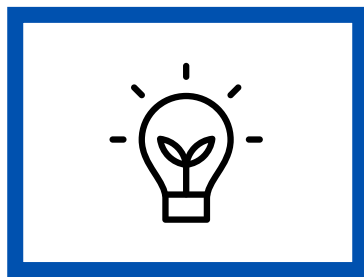


Generative AI



Splunk Observability Approach to AI

Combining predictive analytics, accelerated investigation, and workflow enhancements



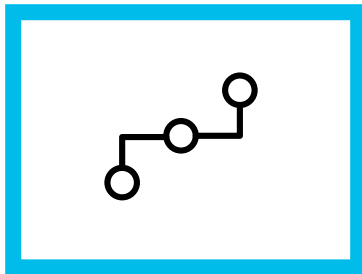
Generative AI Capabilities

Make Everyone an Expert

Reduce need for environment and tool expertise by simplifying content creation and investigation workflows

Detect and Predict

Real-time, streaming analysis to forecast trends and detect anomalies



Foundational ML / AI Capabilities

Correlate and Diagnose

Aggregate / analyse all data to direct investigation and identify root causes

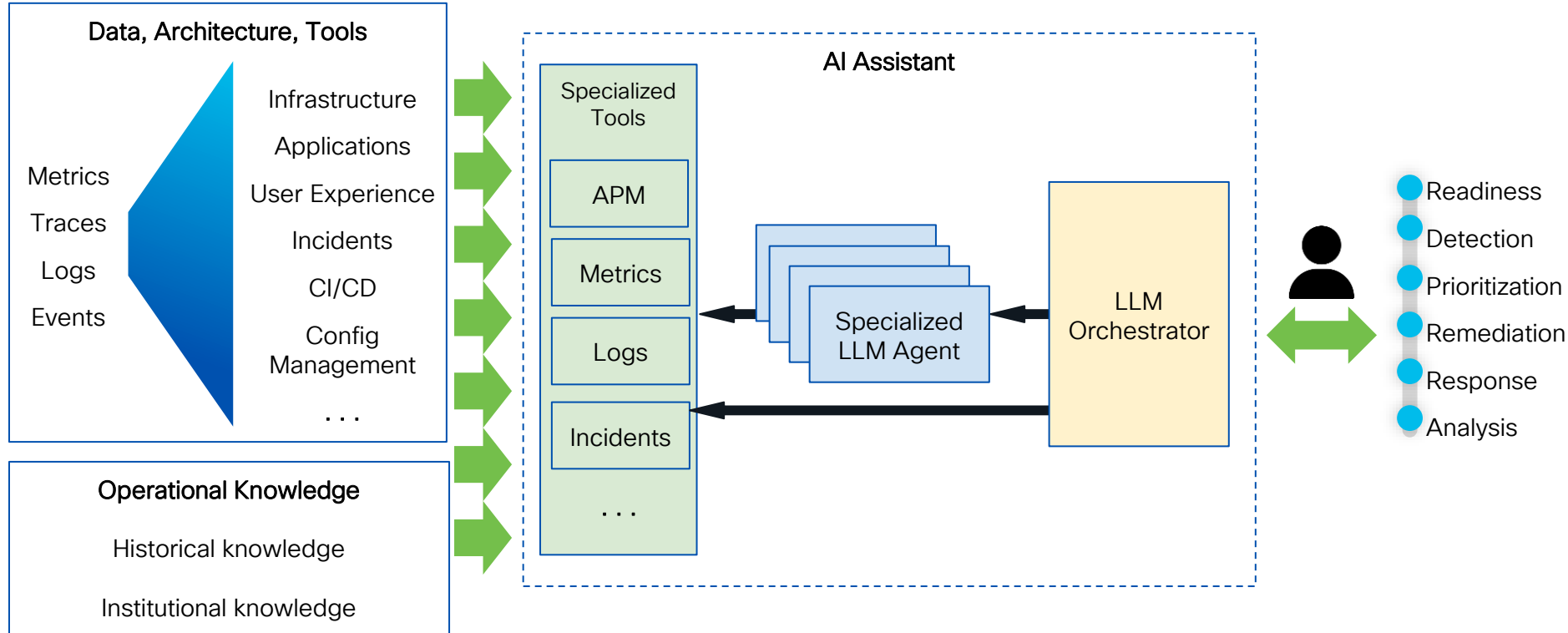
Private Preview AI Assistant in Splunk Observability Cloud

Find and fix issues
faster using natural
language in Splunk®
Observability Cloud

The screenshot displays the Splunk Observability Cloud interface. On the left, a service dependency map is visible, showing a flow from 'frontend' to 'checkoutservice' and 'recommendationservice'. The 'checkoutservice' is highlighted with a red dot and a '1.3% P90 Latency' label. The right side of the image shows a dark-themed chat window for the 'Observability Assistant'. The chat history includes a user query: 'I see 3 critical alerts triggered for paymentservice, can you explain more?' and an assistant response: 'I can certainly help with that!'. The assistant's response text reads: 'The upstream service from paymentservice is called checkoutservice, which had critical alerts triggered 30 minutes before alerts were triggered for paymentservice. Two deployments were made to checkoutservice today. This could be related. You can explore these services visually from the service dependency map in APM, or I can assist you with some metric names to further explore. Which of these next steps would you prefer?'. Below the text are two buttons: 'View service dependency map in apm' and 'Suggesting some metric names'. A hand cursor is pointing at the first button. At the bottom of the chat window is a text input field with a star icon and the placeholder text 'Ask me anything about your environment'. The top right corner of the interface shows '358 days left in trial'.

AI Assistant in Observability

Specialized tools and LLM agents tailored to architectures and data forms



Our goal: Making everyone an observability expert



Accelerate
troubleshooting

Our goal: Making everyone an observability expert



Accelerate
troubleshooting



Get deeper insights



Our goal: Making everyone an observability expert



Accelerate
troubleshooting



Get deeper insights



Increase the
performance of your
tech stack



Our goal: Making everyone an observability expert



Accelerate
troubleshooting

Get deeper insights

Increase the
performance of your
tech stack

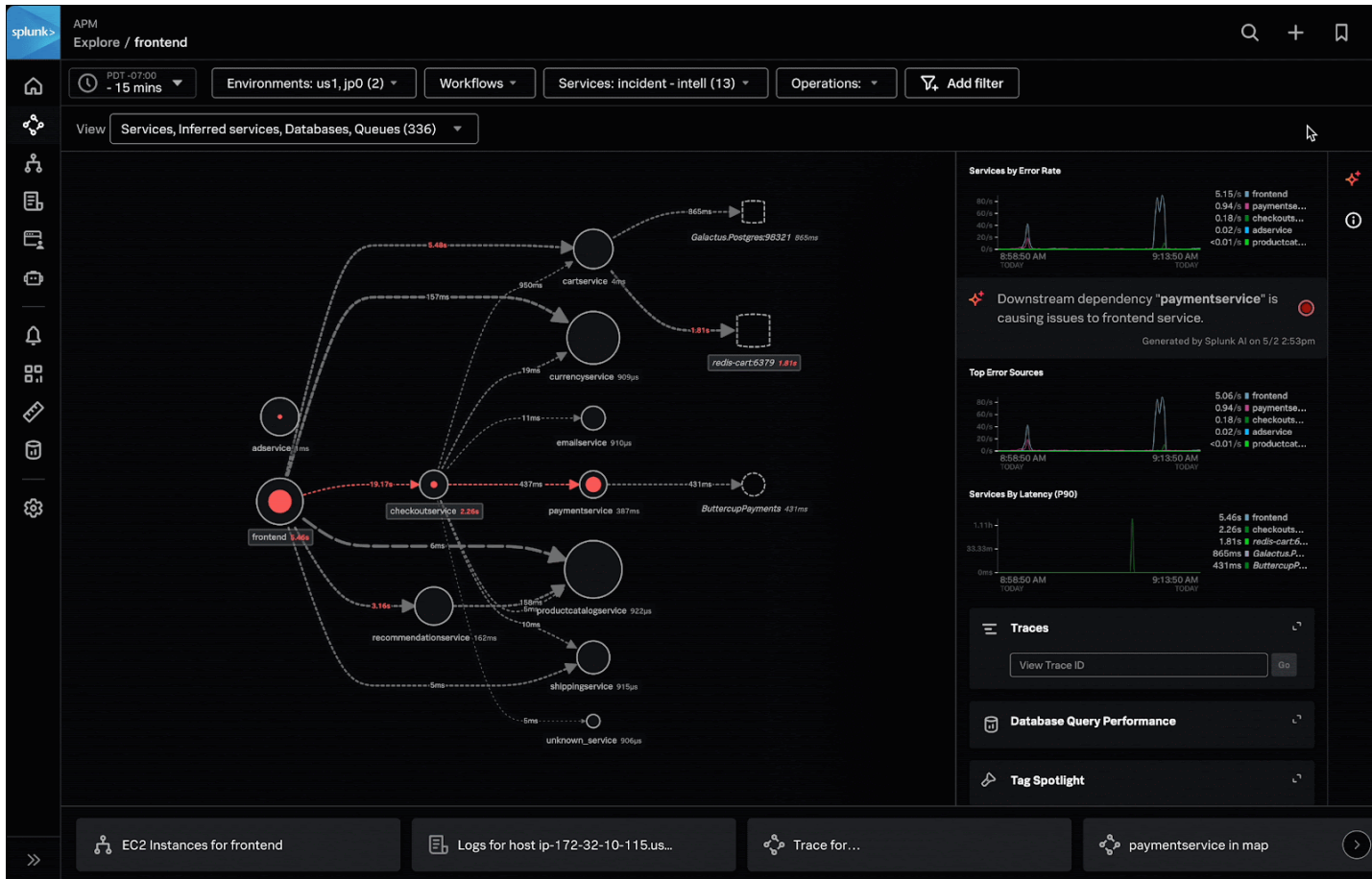
Make the most of
your observability
investment

Demo



Future Direction on Gen AI





Keynote Deep Dives

Wednesday
10:30am – 11:30am



Experiences Amplified:
How AI Can Fuel Better Employee and Customer Experiences

Level 1
Room 106



Smart, Secure, Seamless:
Transforming Experiences with Next-Generation Networking

Level 2
Room 204



Harness a Bold New Era:
Transform Data Centre and Service Provider Connectivity

Level 2
Room 203



Securing User to Application and Everything in Between

Level 2
Melbourne Room 2



Unlocking Digital Resilience through Unified Observability

The HUB
Centre Stage

Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.



Complete your surveys in the **Cisco Live mobile app**.



Continue your education



- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand



Thank you



#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC