AI & Data Resiliency: Secure Practices and Observability Insights

Splunk Observability
Strategy & Product Overview

cisco Connect

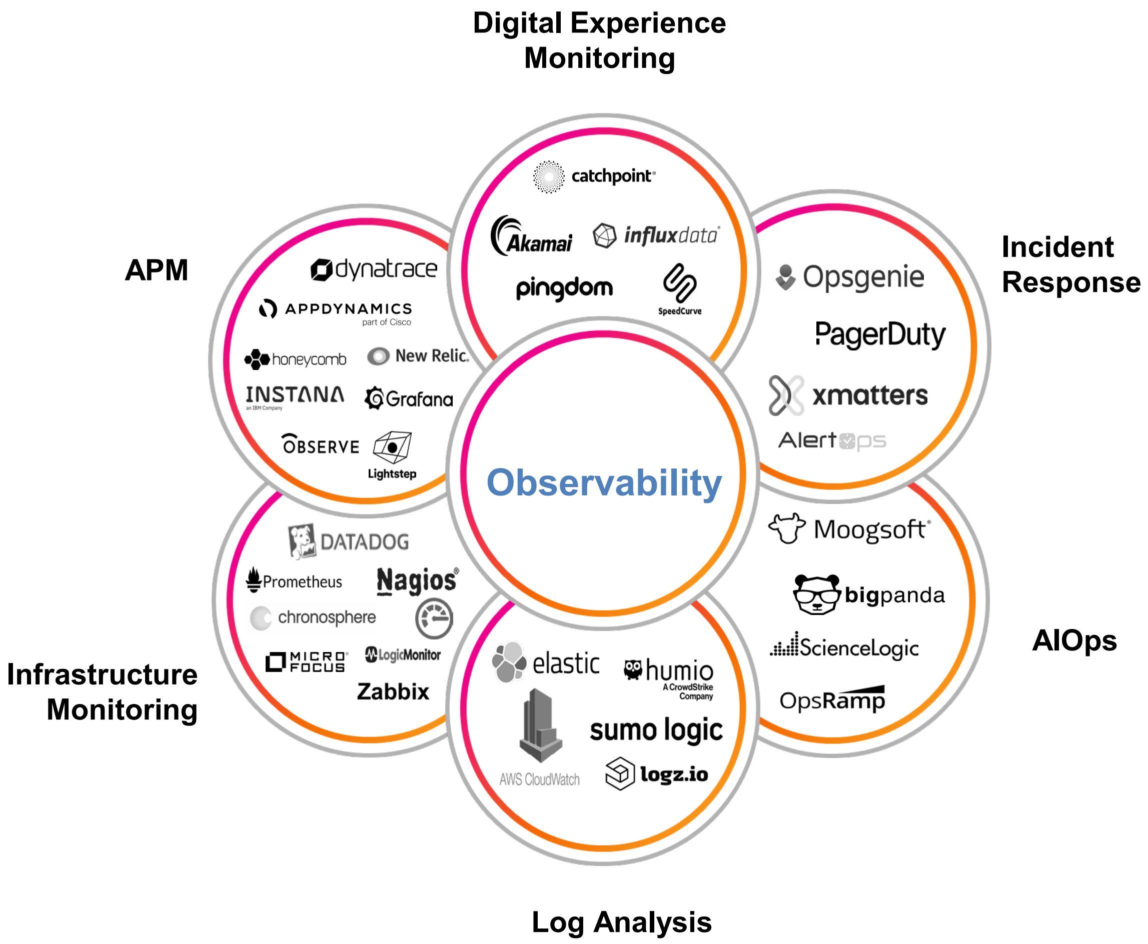
Trevor Fink
Observability Solutions Architect
trfink@cisco.com

Observability for AI

Resistance Is Futile!

Application Landscape Has Changed

Data is Scattered
Across a Myriad of Vendors



Digital Experience Monitoring

APM

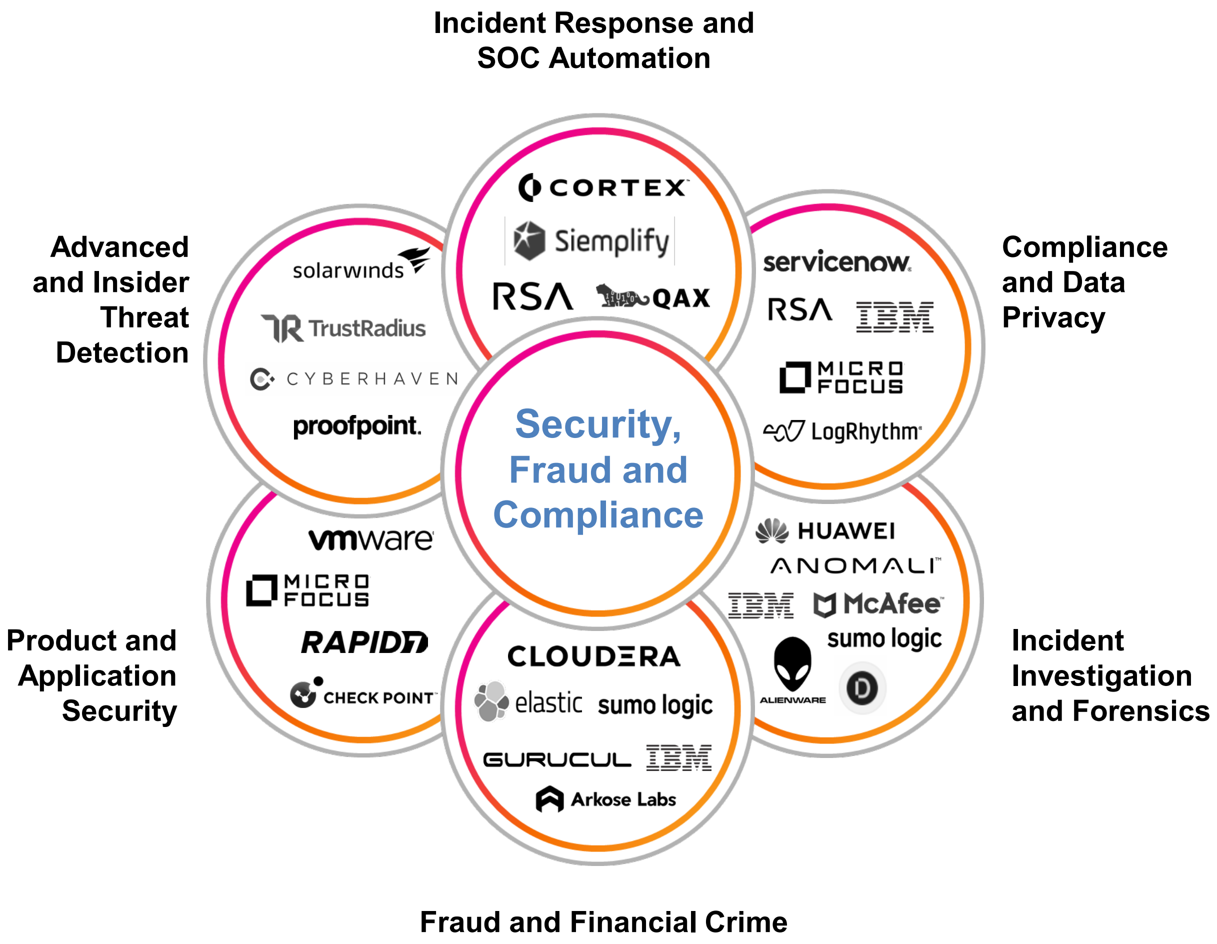
Incident Response

Observability

Infrastructure Monitoring

AIOps

Log Analysis



Incident Response and SOC Automation

Advanced and Insider Threat Detection

Compliance and Data Privacy

Security, Fraud and Compliance

Product and Application Security

Incident Investigation and Forensics

Fraud and Financial Crime

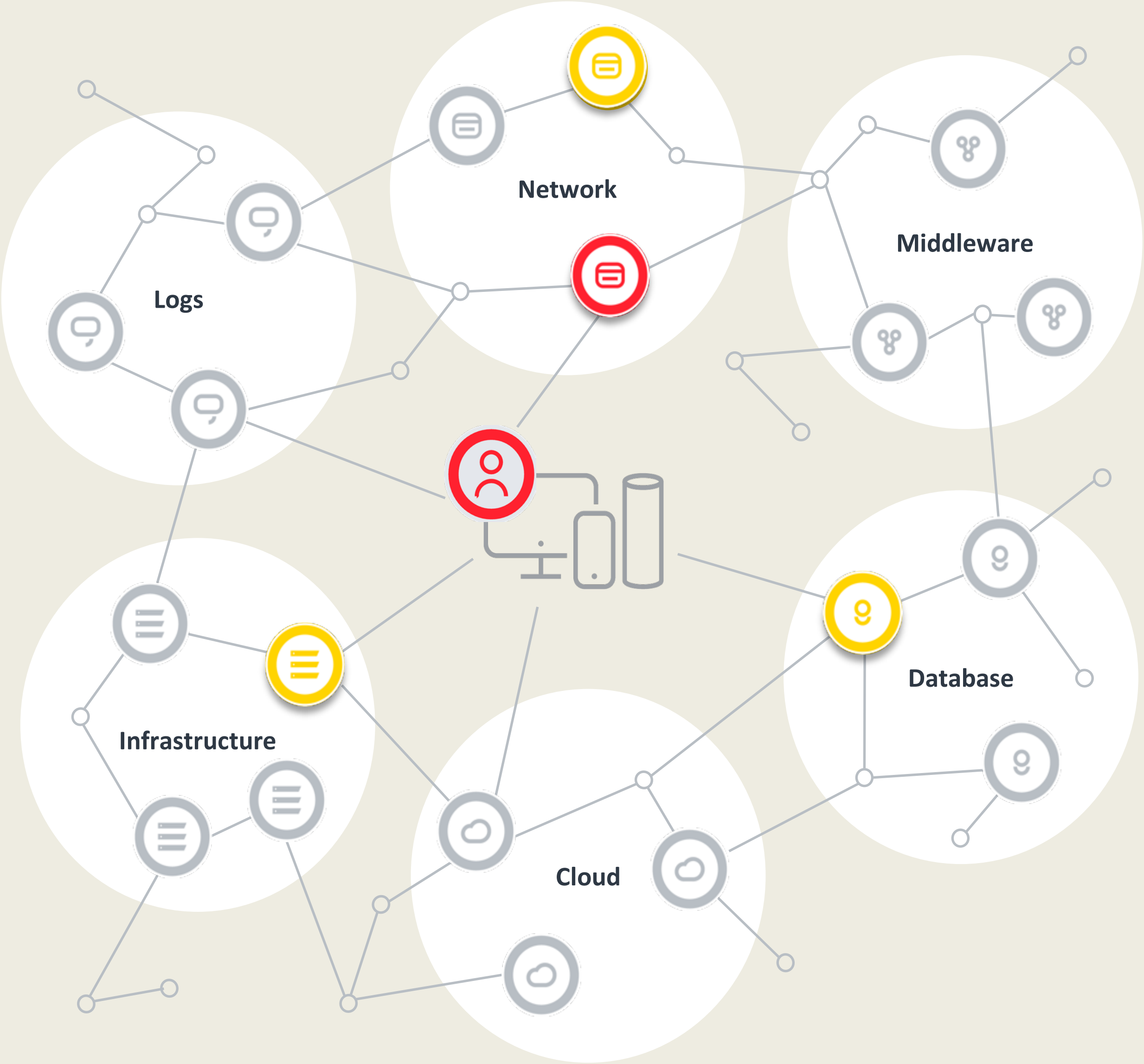
It’s hard to be resilient.

Complex environments expand attack surface and failure points.

Growing data volumes sit in silos and are increasingly hard to manage.

Regulations require real-time risk assessments.

The AI era is accelerating all these challenges and creating entirely new ones.



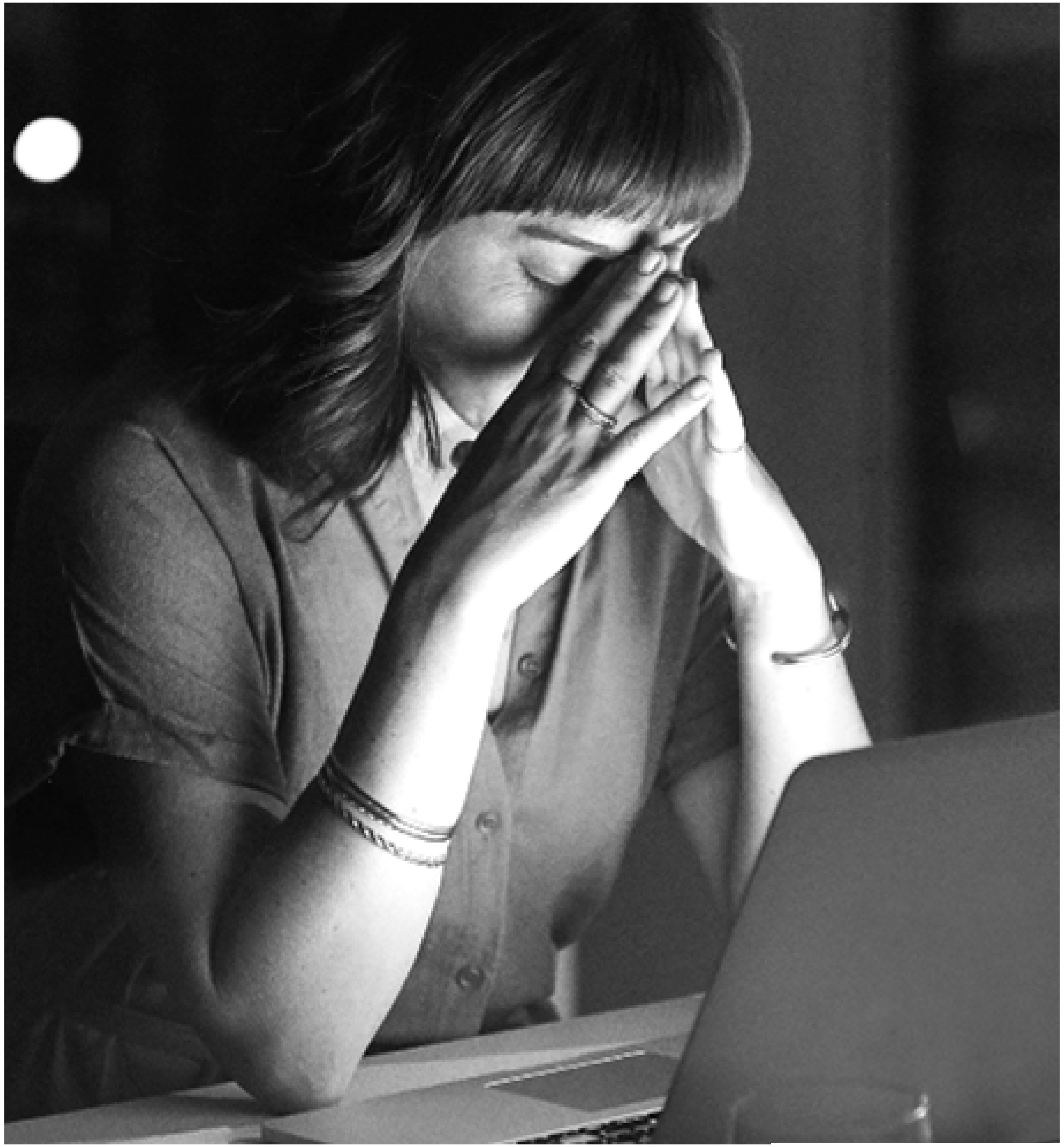
Digital resilience is a high stakes challenge.

$9.4M

average cost of data breach in US

$365k

cost of downtime per hour



Build digital resilience with Splunk.

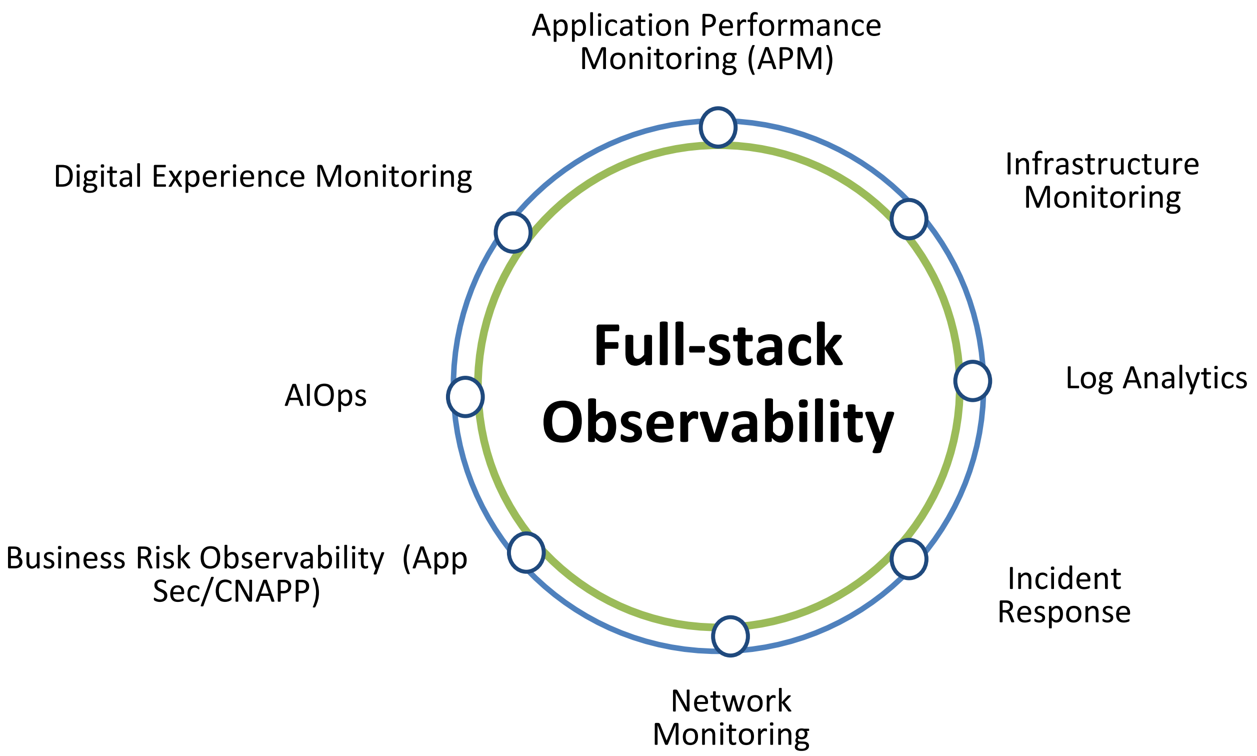
Splunk brings SecOps, ITOps and engineering together to…

Prevent major issues

Remediate faster

Adapt quickly

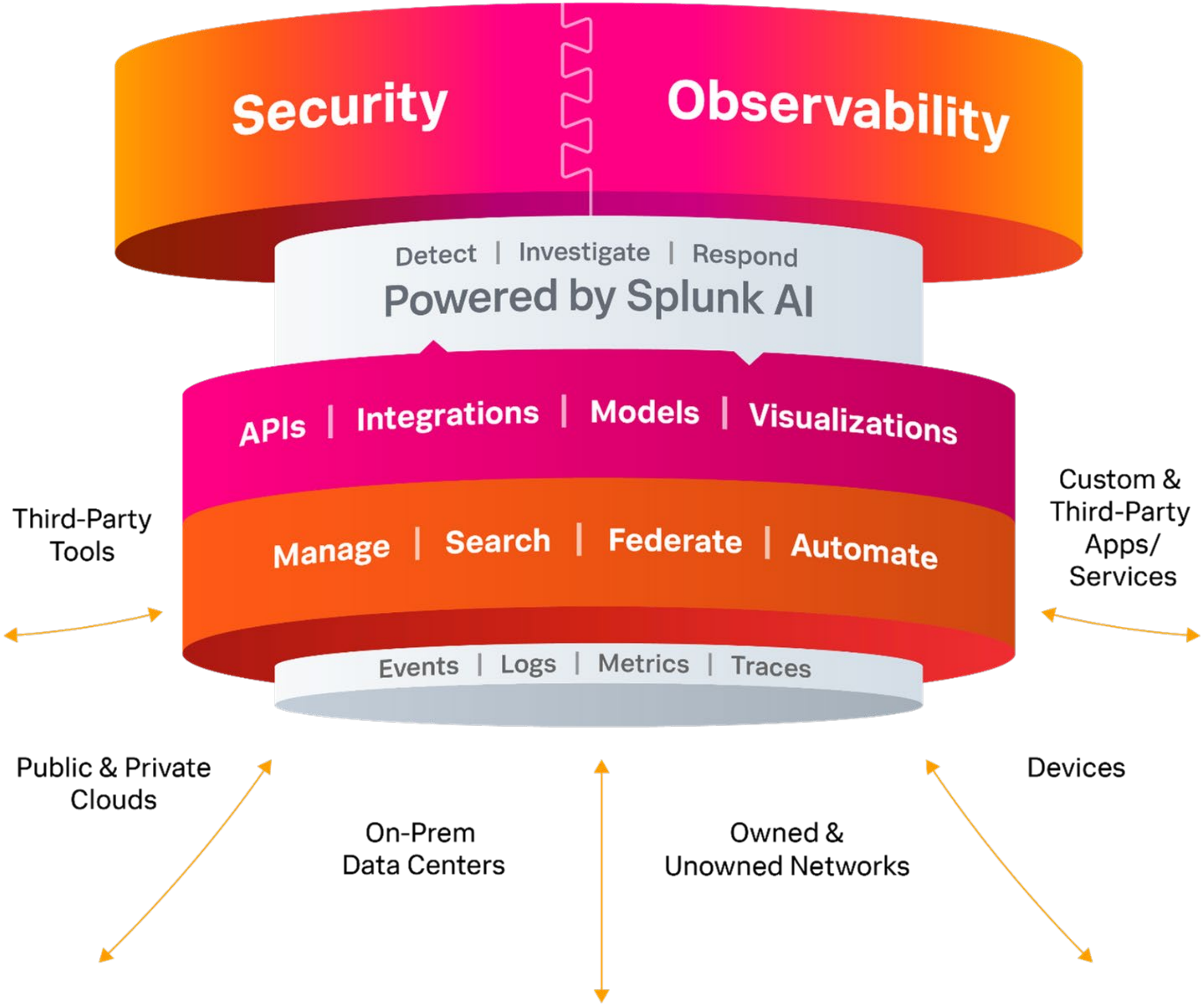
Observability for your entire enterprise


Application Performance Monitoring (APM)
Infrastructure Monitoring
Log Analytics
Incident Response
Network Monitoring
Business Risk Observability (App Sec/CNAPP)
AIOps
Digital Experience Monitoring
Full-stack Observability

Real-Time Insight | AI Powered | Federated | OpenTelemetry Native | Extensible | Correlated MELT | Business Context

On-Prem | Hybrid Cloud | Multi-Cloud | Cloud-Native

The Unified Security and Observability Platform


Security
Observability
Detect | Investigate | Respond
Powered by Splunk AI
APIs | Integrations | Models | Visualizations
Manage | Search | Federate | Automate
Events | Logs | Metrics | Traces
Third-Party Tools
Custom & Third-Party Apps/ Services
Public & Private Clouds
On-Prem Data Centers
Owned & Unowned Networks
Devices

Splunk AI

Splunk is not new to

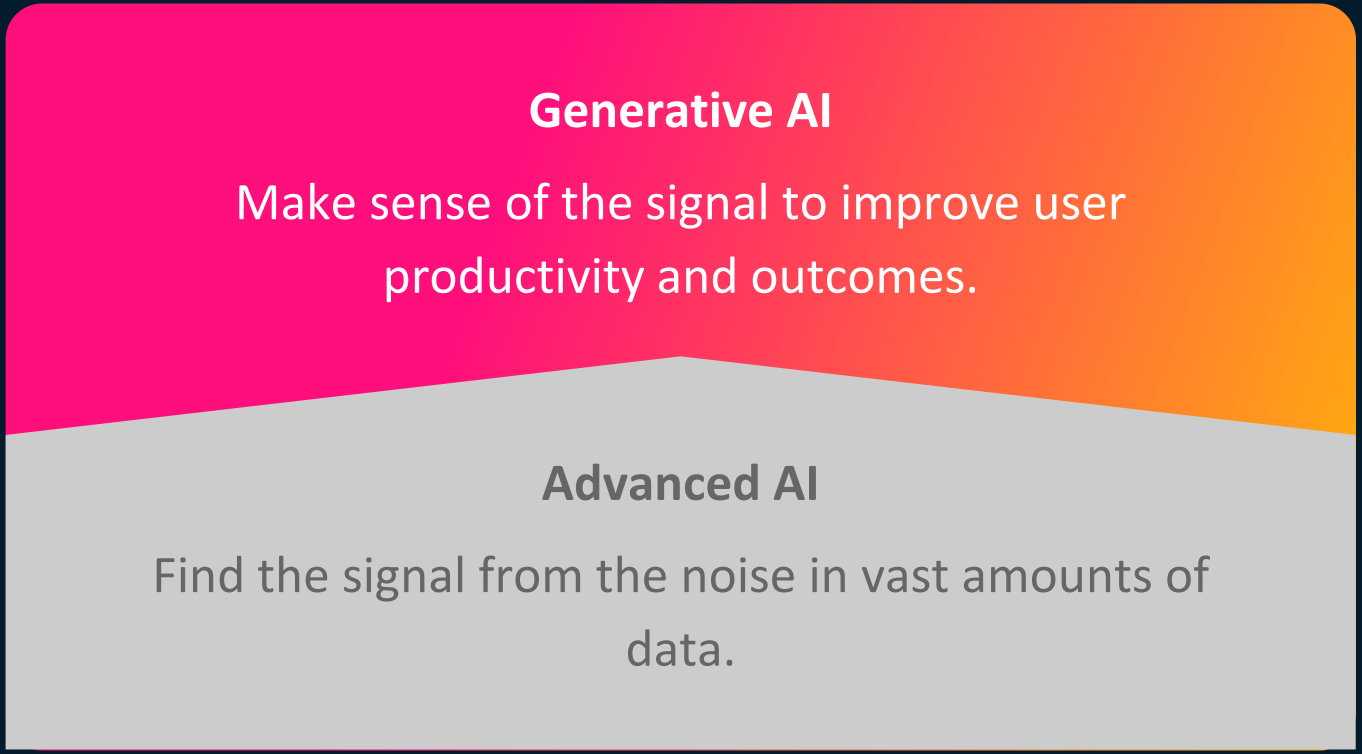
AI

cisco Connect

Supercharge digital resilience with AI

Where are we investing?

Accelerate detection, investigation and response.



Generative AI

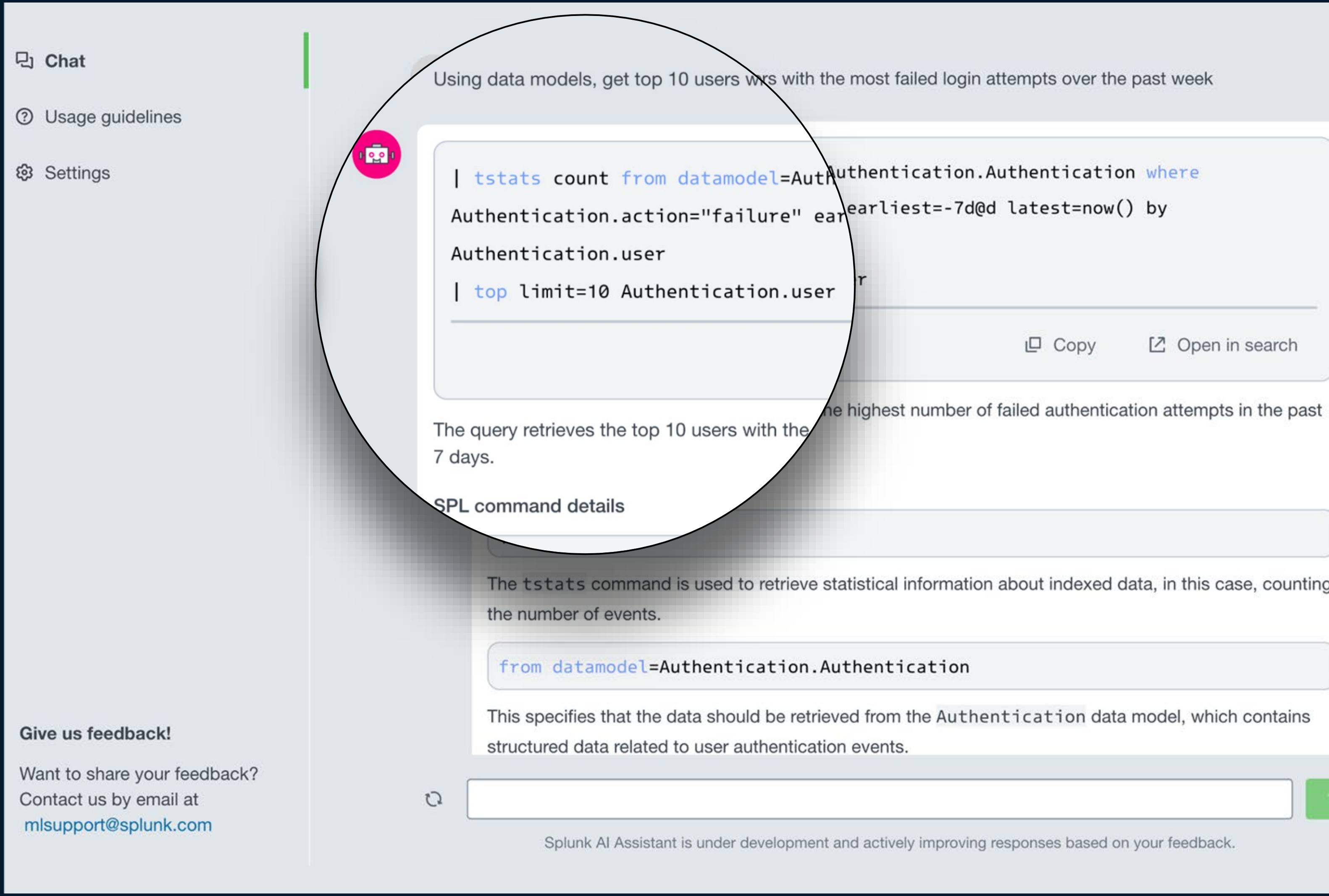
Make sense of the signal to improve user productivity and outcomes.

Advanced AI

Find the signal from the noise in vast amounts of data.

Splunk AI Assistant for SPL

- Upskill new and advanced Splunk users quickly.
- Explain or write SPL with bi-directionally translation.
- Access the full knowledge base for answers in product.



Using data models, get top 10 users with the most failed login attempts over the past week

```
| tstats count from datamodel=Authentication.Authentication where
Authentication.action="failure" earliest=-7d@d latest=now() by
Authentication.user
| top limit=10 Authentication.user
```

The query retrieves the top 10 users with the highest number of failed authentication attempts in the past 7 days.

SPL command details

The `tstats` command is used to retrieve statistical information about indexed data, in this case, counting the number of events.

```
from datamodel=Authentication.Authentication
```

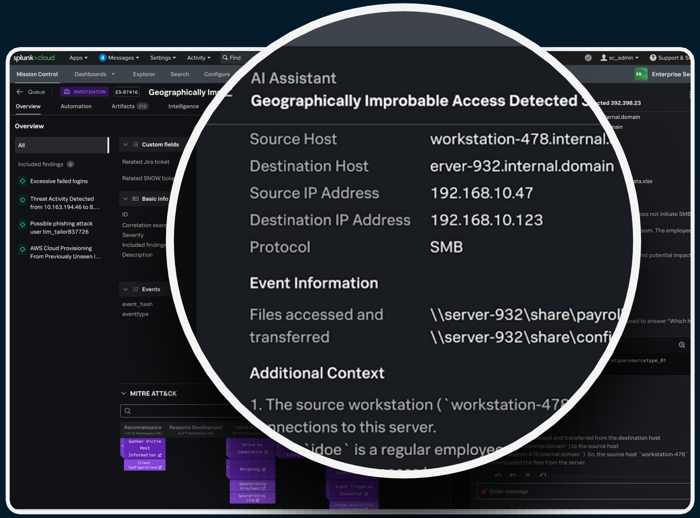
This specifies that the data should be retrieved from the `Authentication` data model, which contains structured data related to user authentication events.

Give us feedback!

Want to share your feedback? Contact us by email at mlsupport@splunk.com

Splunk AI Assistant is under development and actively improving responses based on your feedback.

AI Assistant in Security



AI Assistant

Geographically Improbable Access Detected

Source Host	workstation-478.internal
Destination Host	erver-932.internal.domain
Source IP Address	192.168.10.47
Destination IP Address	192.168.10.123
Protocol	SMB

Event Information

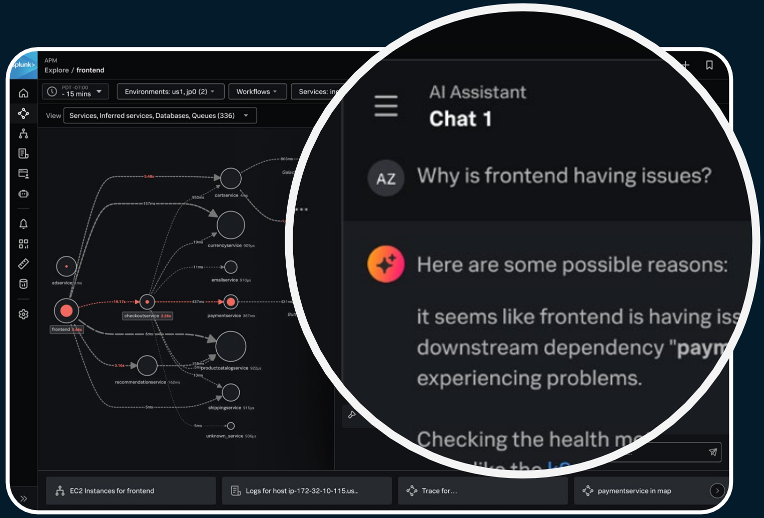
Files accessed and transferred	\\server-932\share\payrol \\server-932\share\confi

Additional Context

1. The source workstation (`workstation-47 nnections to this server.

`jdoe` is a regular employee

AI Assistant in Observability Cloud



AI Assistant

Chat 1

AZ Why is frontend having issues?

Here are some possible reasons:

it seems like frontend is having iss downstream dependency "paym experiencing problems.

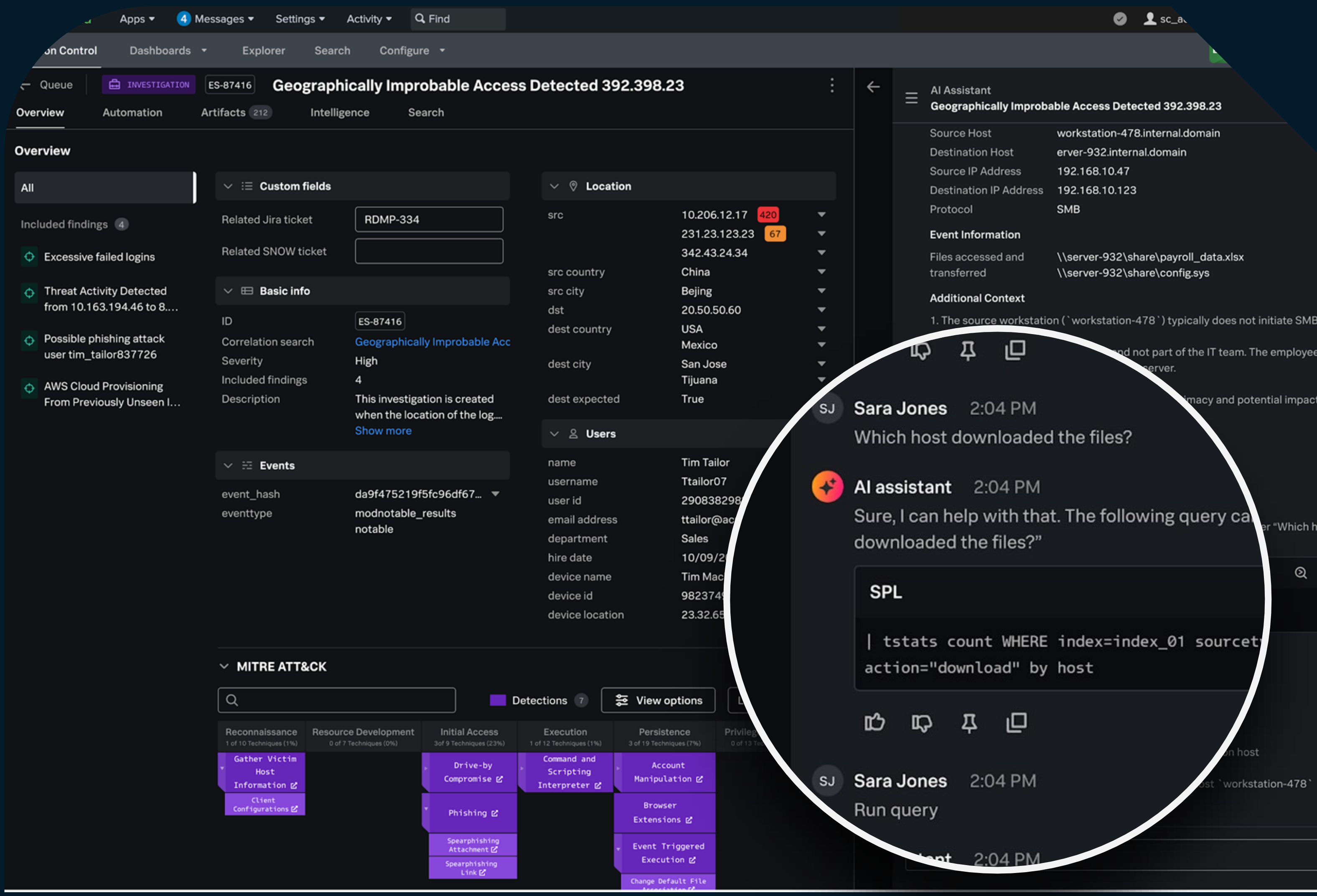
Checking the health m

EC2 Instances for frontend
Logs for host ip-172-32-10-115.us...
Trace for...
paymentservice in map

Better detection | Faster investigation | Accelerated actions

AI Assistant in Security

- Investigate faster.
- Answer analyst questions to speed up daily workflows.
- Save time while addressing threats more rapidly.
- Access natively within Splunk ES.



ES-87416 Geographically Improbable Access Detected 392.398.23

Overview

Included findings 4

- Excessive failed logins
- Threat Activity Detected from 10.163.194.46 to 8.…
- Possible phishing attack user tim_tailor837726
- AWS Cloud Provisioning From Previously Unseen I…

Custom fields

Related Jira ticket: RDMP-334
Related SNOW ticket:

Basic info

ID: ES-87416
Correlation search: Geographically Improbable Acc
Severity: High
Included findings: 4
Description: This investigation is created when the location of the log…. Show more

Events

event_hash: da9f475219f5fc96df67…
eventtype: modnotable_results notable

Location

src: 10.206.12.17 420
231.23.123.23 67
342.43.24.34
src country: China
src city: Bejing
dst: 20.50.50.60
dest country: USA
Mexico
dest city: San Jose
Tijuana
dest expected: True

Users

name: Tim Tailor
username: Ttailor07
user id: 290838298
email address: ttailor@ac
department: Sales
hire date: 10/09/2
device name: Tim Mac
device id: 982374
device location: 23.32.65

MITRE ATT&CK

AI Assistant
Geographically Improbable Access Detected 392.398.23

Source Host: workstation-478.internal.domain
Destination Host: erver-932.internal.domain
Source IP Address: 192.168.10.47
Destination IP Address: 192.168.10.123
Protocol: SMB

Event Information

Files accessed and transferred: \\server-932\share\payroll_data.xlsx
\\server-932\share\config.sys

Additional Context

1. The source workstation (`workstation-478`) typically does not initiate SMB
nd not part of the IT team. The employee
erver.
imacy and potential impact

SJ Sara Jones 2:04 PM
Which host downloaded the files?

AI assistant 2:04 PM
Sure, I can help with that. The following query ca
downloaded the files?"

SPL

```
| tstats count WHERE index=index_01 sourcet
action="download" by host
```

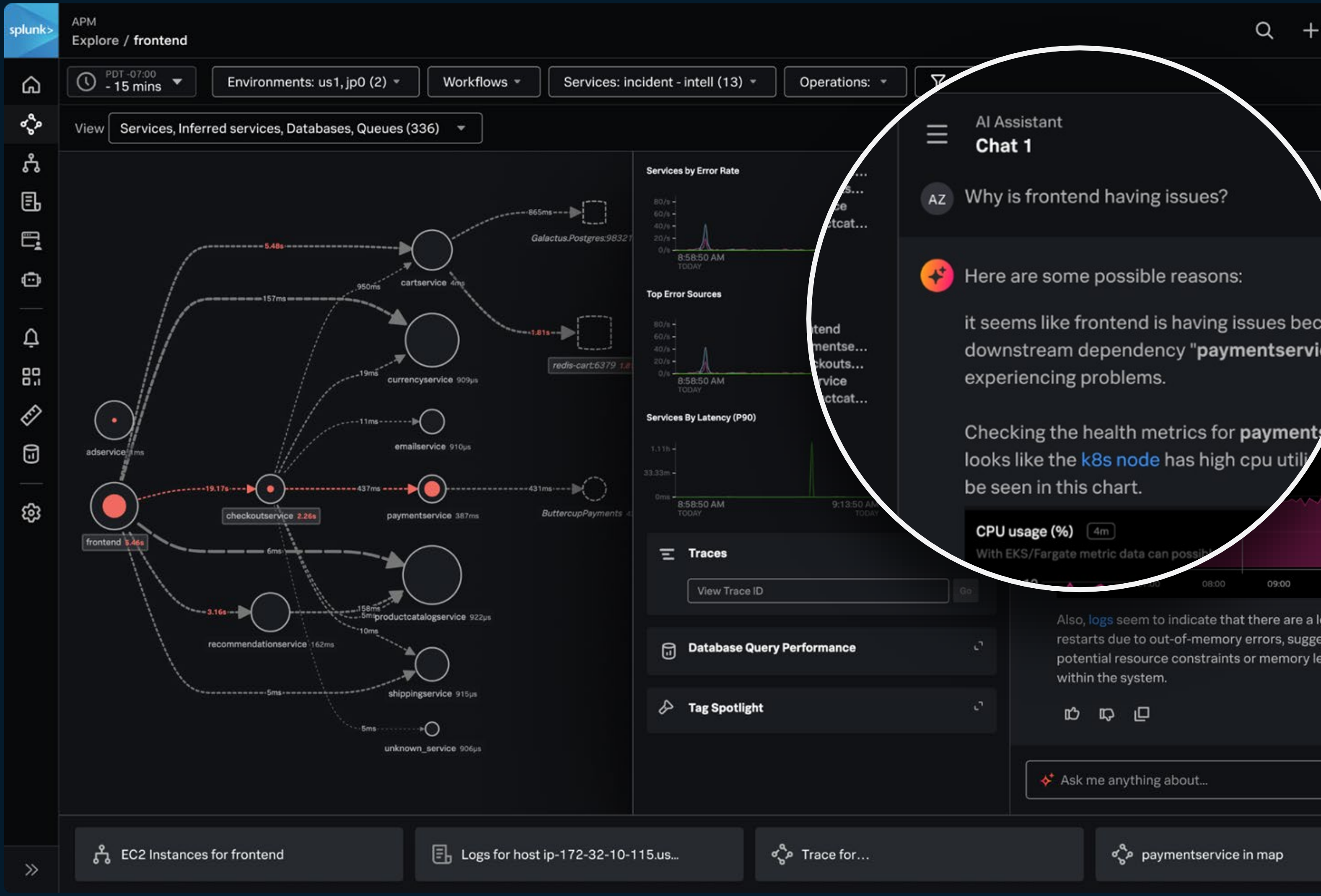
SJ Sara Jones 2:04 PM
Run query

2:04 PM

cisco Connect

AI Assistant in Observability

- Get insights and content faster.
- Troubleshoot with assistance.
- Receive onboarding and support.



Why is frontend having issues?

Here are some possible reasons:

it seems like frontend is having issues bec
downstream dependency "**paymentservi**
experiencing problems.

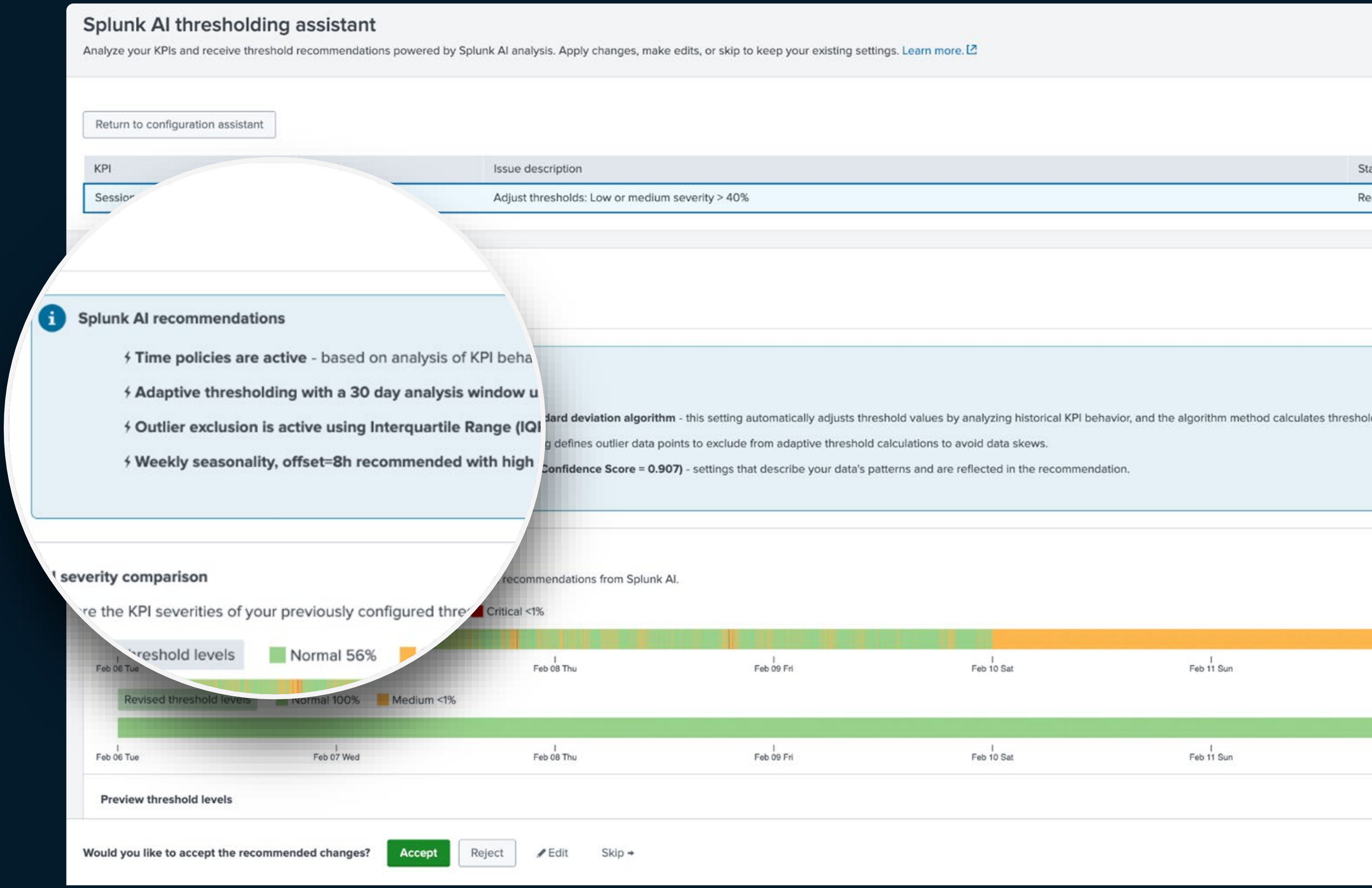
Checking the health metrics for **payment**
looks like the k8s node has high cpu utili
be seen in this chart.

Also, logs seem to indicate that there are a l
restarts due to out-of-memory errors, sugge
potential resource constraints or memory le
within the system.

cisco Connect

Advanced AI for ITSI

- Enhance adaptive thresholding.
- Provide recommendations for each entity.
- Identify behavioral changes over time.
- Achieve faster time-to-value.



Splunk AI thresholding assistant

Analyze your KPIs and receive threshold recommendations powered by Splunk AI analysis. Apply changes, make edits, or skip to keep your existing settings. Learn more.

Return to configuration assistant

KPI	Issue description	Sta
Sessior	Adjust thresholds: Low or medium severity > 40%	Re

Splunk AI recommendations

- **Time policies are active** - based on analysis of KPI beha
- **Adaptive thresholding with a 30 day analysis window u** … **dard deviation algorithm** - this setting automatically adjusts threshold values by analyzing historical KPI behavior, and the algorithm method calculates threshol
- **Outlier exclusion is active using Interquartile Range (IQI** … g defines outlier data points to exclude from adaptive threshold calculations to avoid data skews.
- **Weekly seasonality, offset=8h recommended with high** … **Confidence Score = 0.907)** - settings that describe your data's patterns and are reflected in the recommendation.

severity comparison

re the KPI severities of your previously configured thre … recommendations from Splunk AI.

reshold levels 🟩 Normal 56% … 🟥 Critical <1%

Revised threshold levels 🟩 Normal 100% 🟧 Medium <1%

Preview threshold levels

Would you like to accept the recommended changes? Accept Reject Edit Skip

cisco Connect

Demo

Thank you