Can you smell what the SNOC is cooking?

CPAE 2025

Al Parsons aliparso@cisco.com
Senior Partner Solutions Engineer

June 2025

© 2025 SPLUNK LLC

Forward-looking statements

This presentation may contain forward-looking statements that are subject to the safe harbors created under the Securities Act of 1933, as amended, and the Securities Exchange Act of 1934, as amended. All statements other than statements of historical facts are statements that could be deemed forward-looking statements. These statements are based on current expectations, estimates, forecasts, and projections about the industries in which we operate and the beliefs and assumptions of our management based on the information currently available to us. Words such as “expects,” “anticipates,” “targets,” “goals,” “projects,” “intends,” “plans,” “believes,” “momentum,” “seeks,” “estimates,” “continues,” “endeavors,” “strives,” “may,” variations of such words, and similar expressions are intended to identify such forward-looking statements. In addition, any statements that refer to (1) our goals, commitments, and programs; (2) our business plans, initiatives, and objectives; and (3) our assumptions and expectations, including our expectations regarding our financial performance, products, technology, strategy, customers, markets, acquisitions and investments are forward-looking statements. These forward-looking statements are not guarantees of future performance and involve significant risks, uncertainties and other factors that may cause our actual results, performance or achievements to be materially different from results, performance or achievements expressed or implied by the forward-looking statements contained in this presentation. Readers are cautioned that these forward-looking statements are only predictions and are subject to risks, uncertainties, and assumptions that are difficult to predict, including those identified in the “Risk Factors” section of Cisco’s most recent report on Form 10-Q filed on February 20, 2024 and its most recent report on Form 10-K filed on September 7, 2023, as well as the “Risk Factors” section of Splunk’s most recent report on Form 10-Q filed with the SEC on November 28, 2023. The forward-looking statements made in this presentation are made as of the time and date of this presentation. If reviewed after the initial presentation, even if made available by Cisco or Splunk, on Cisco or Splunk’s website or otherwise, it may not contain current or accurate information. Cisco and Splunk undertake no obligation to revise or update any forward-looking statements for any reason, except as required by law.

In addition, any information about new products, features, functionality or our roadmap outlines our general product direction and is subject to change at any time without notice. It is for informational purposes only and shall not be incorporated into any contract or other commitment or be relied upon in making a purchasing decision. We undertake no commitment, promise or obligation either to develop the features or functionalities described, in beta or in preview (used interchangeably), or to include any such feature or functionality in a future release. The development, release, and timing of any features or functionality described for our products remains at our sole discretion.

Splunk, Splunk> and Turn Data Into Doing are trademarks and registered trademarks of Splunk LLC in the United States and other countries. All other brand names, product names or trademarks belong to their respective owners.

© 2025 Splunk LLC. All rights reserved.

splunk> a CISCO company

Al Parsons

Senior Partner Solutions Engineer

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

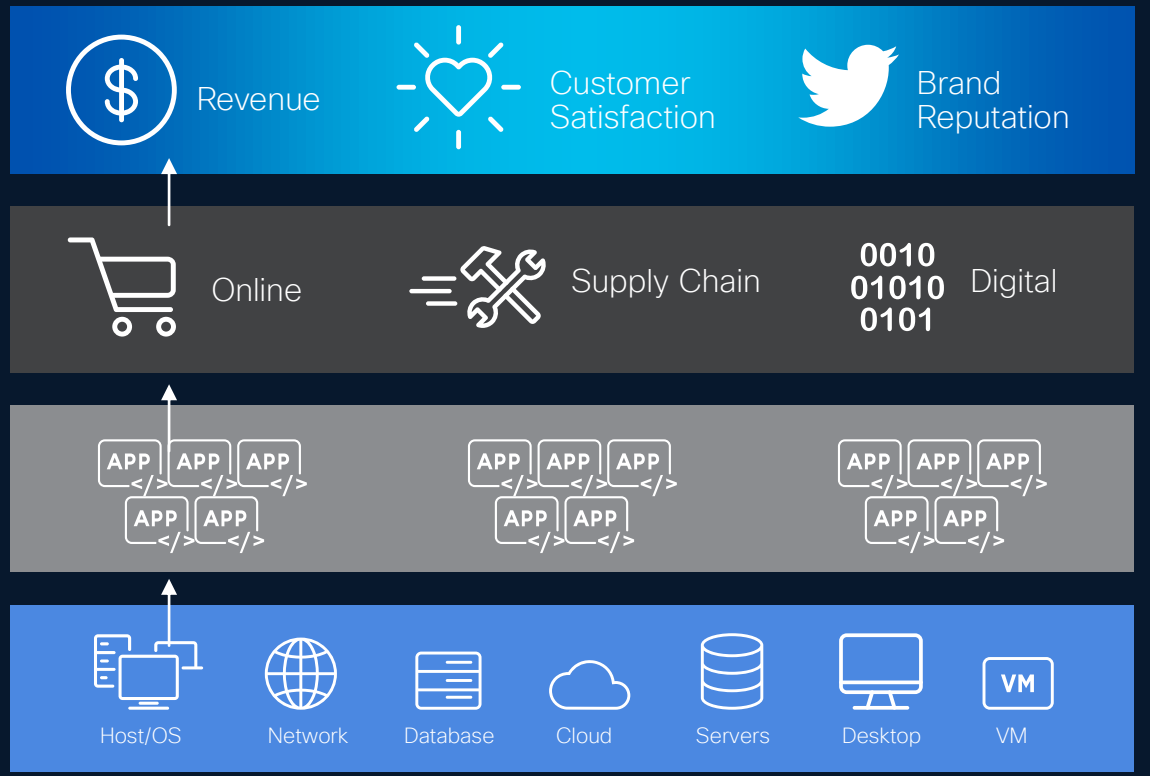
The Partner Architect's Role in Digital Resilience

Your job is to embed Security, Assurance & Observability across all of this

© 2025 Cisco and/or its affiliates. All rights reserved.
Cisco Confidential

Digital resilience is hard

Team struggle to correlate cause and effect



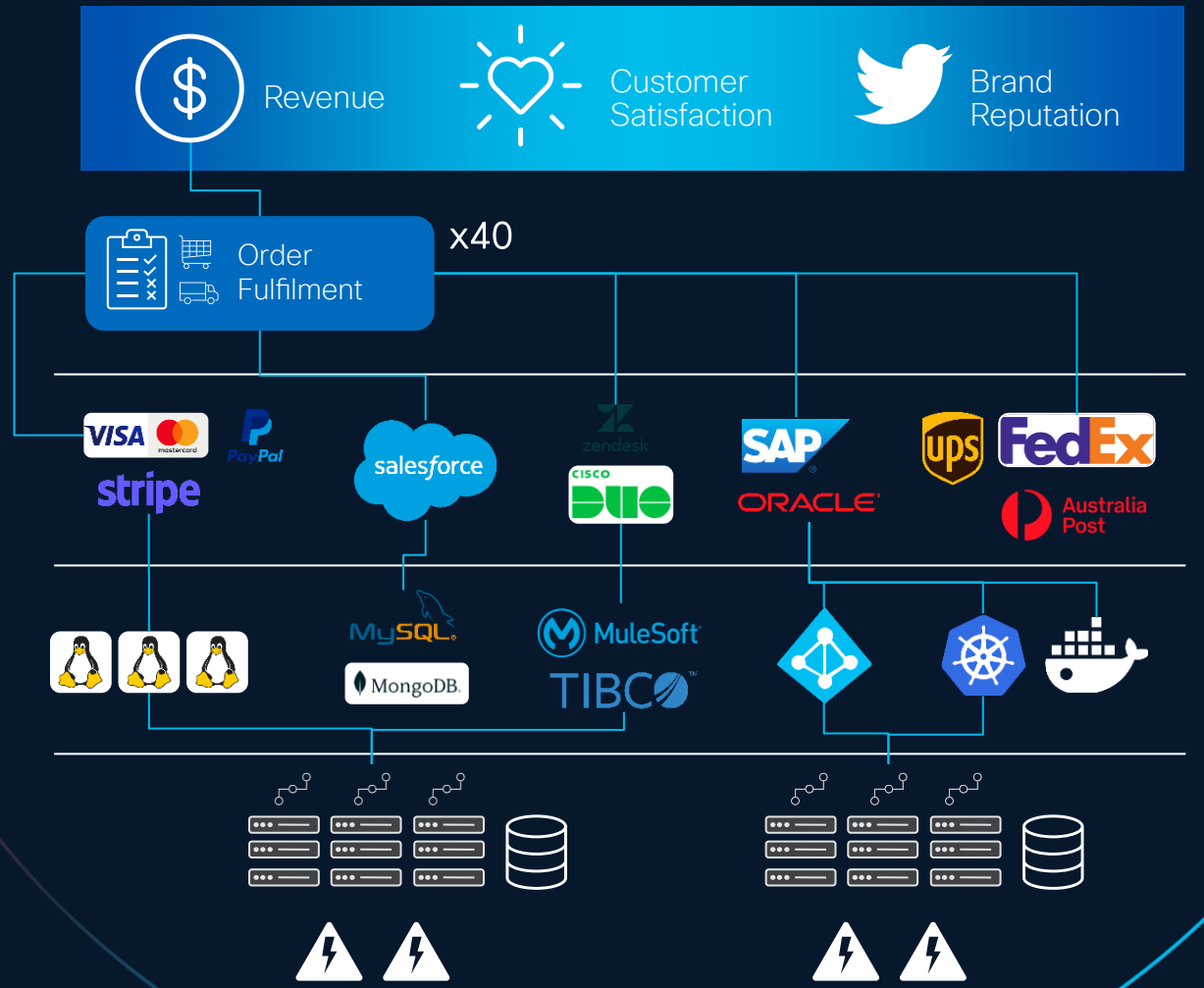
Traditional solutions focus on infrastructure-level monitoring & performance reporting

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Digital resilience is hard

Team struggle to correlate cause and effect



KPIs

Service layer

eCommerce, Customer Support, Marketing, HR, R&D, Compliance, Supply Chain, Manufacturing

Business layer

Order management – Warehouse management – Transport – Payments

Application services

Physical & virtual OS – Database – Middleware – App servers

Infrastructure

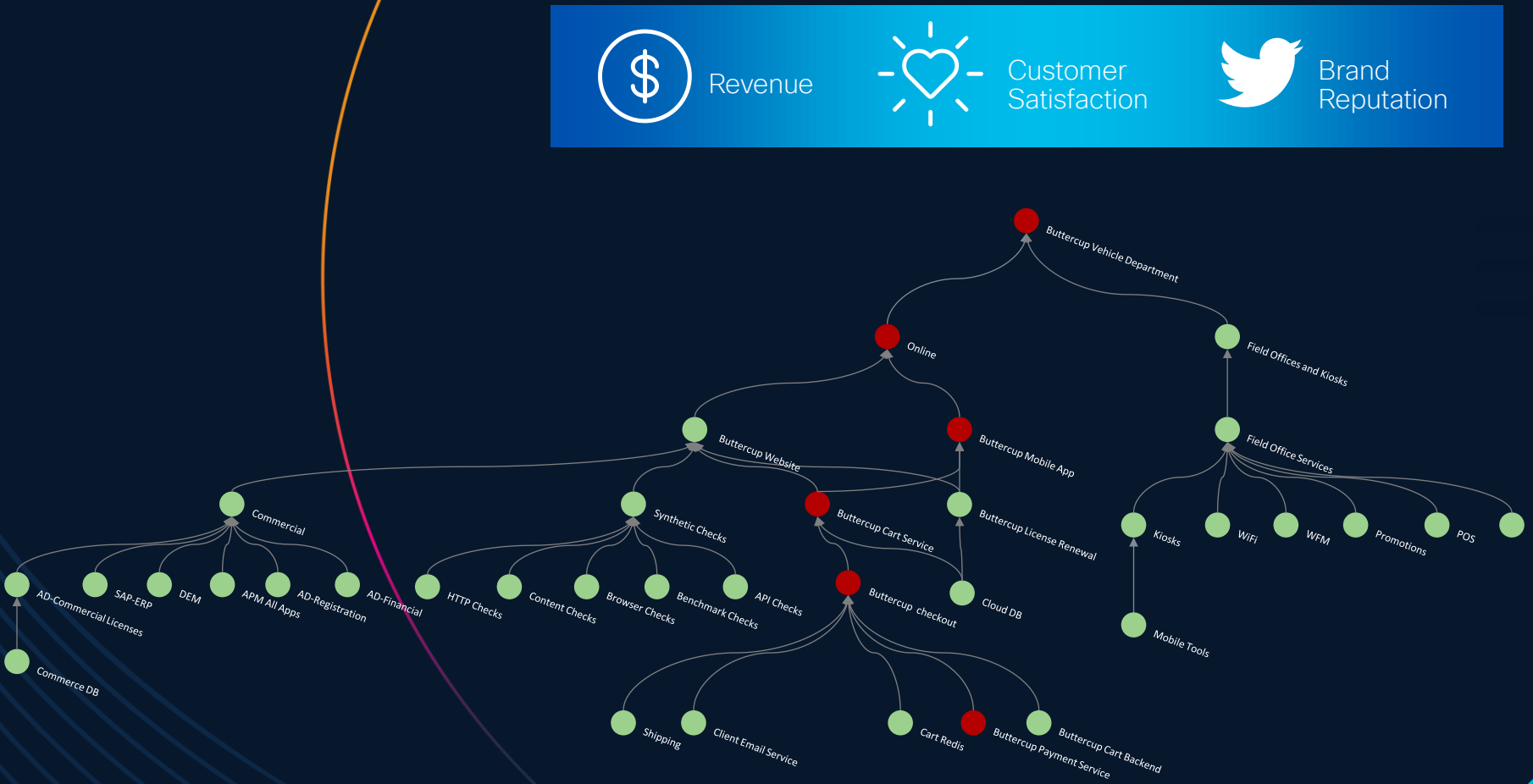
Power – Servers – Networking – Storage

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Splunk + Cisco make it easy

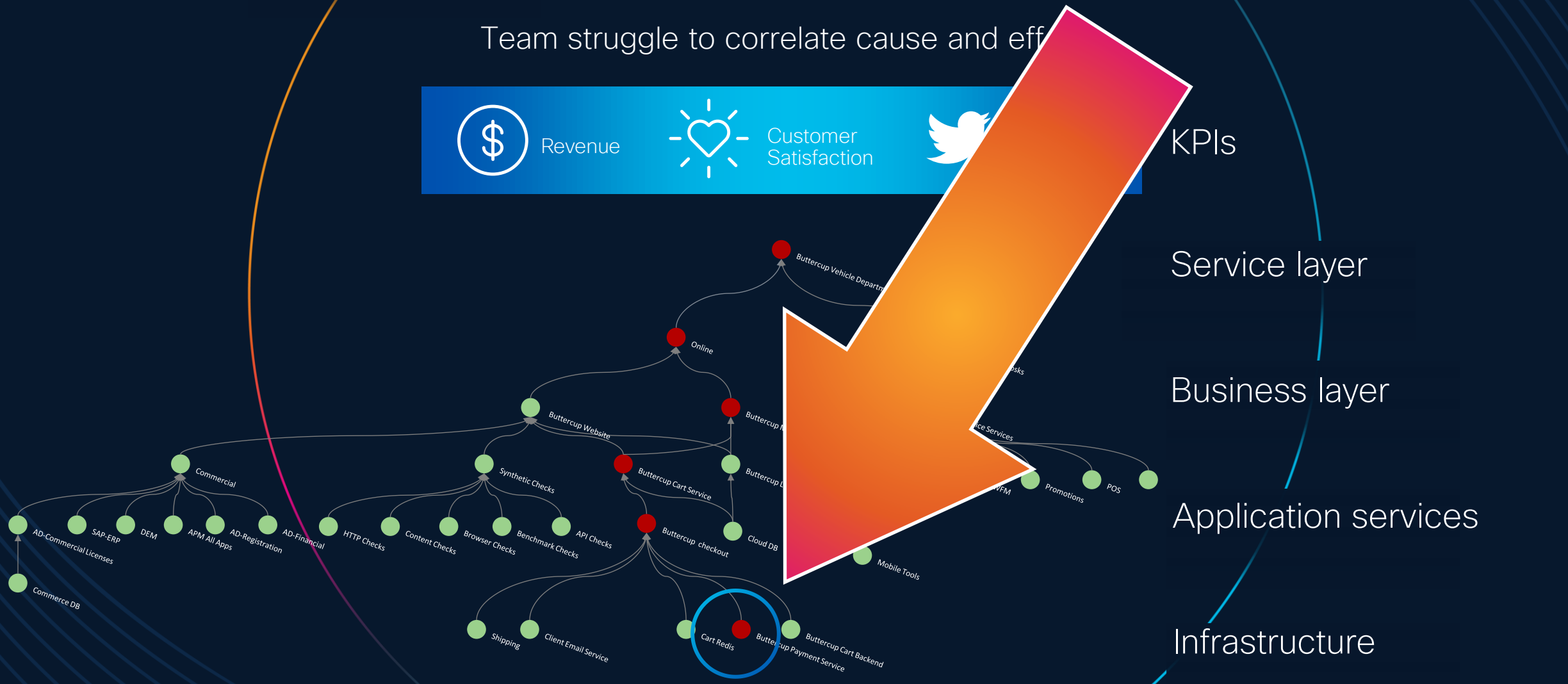
Team struggle to correlate cause and effect



© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Splunk + Cisco make it easy



© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

What is Splunk?

Splunk is a high-volume, real-time search engine that can take in any data from any source in any format

See

End-to-end, real time visibility

All your data in the one place with no sampling/blindspots

Act

Investigate across massive data sets and take **action** fast

Search, dashboard, alert & report

Extend

Extend the **platform** to use data to solve problems across the business

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

POLL

Level-set: What are we talking about

SOC

Threat detections and incident response

Watches for cyber threats 24/7

Detects and responds to security incidents.

Analyses suspicious activity.

Manages security tools and alerts.

Protects data and ensures compliance.

Wants a secure and resilient technology environment

© 2025 Cisco and/or its affiliates. All rights reserved.

Level-set: What are we talking about

SOC

Threat detections and incident response

Watches for cyber threats 24/7

Detects and responds to security incidents.

Analyses suspicious activity.

Manages security tools and alerts.

Protects data and ensures compliance.

NOC

Network monitoring and incident resolution

Monitors IT networks 24/7

Fixes network outages & slowdowns.

Handles network device health and alerts.

Network maintenance and updates

Both want a secure and resilient technology environment

© 2025 Cisco and/or its affiliates. All rights reserved.

Level-set: What are we talking about

SOC

Threat detections and incident response

Watches for cyber threats 24/7

Detects and responds to security incidents.

Analyses suspicious activity.

Manages security tools and alerts.

Protects data and ensures compliance.

+

NOC

Network monitoring and incident resolution

Monitors IT networks 24/7

Fixes network outages & slowdowns.

Handles network device health and alerts.

Network maintenance and updates

=

SNOC

Unified network and security incident response

Responds to any IT or security incident.

Uses shared dashboards, data and workflows

Improves uptime and threat response

Want a secure and resilient technology environment

Do it in the one place

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

“

How are your clients currently separating their NOC and SOC teams?

What challenges do they face as a result?

”

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Why are we trending towards the SNOC?

A SNOC breaks down the walls between network and security operations, giving you a single team, single view, and single workflow for faster, smarter, and more cost-effective protection and performance.

Unified View:
One team, one dashboard for both security and network issues

Faster Response:
No delays or handoffs—incidents get resolved quicker.

Lower Costs:
Fewer tools, less duplication, more efficient use of staff.

Better Collaboration:
No silos or finger-pointing; everyone works together.

Smarter Decisions:
See the full picture for accurate root cause analysis.

Improved Resilience:
Ready for complex attacks and outages—stronger uptime.

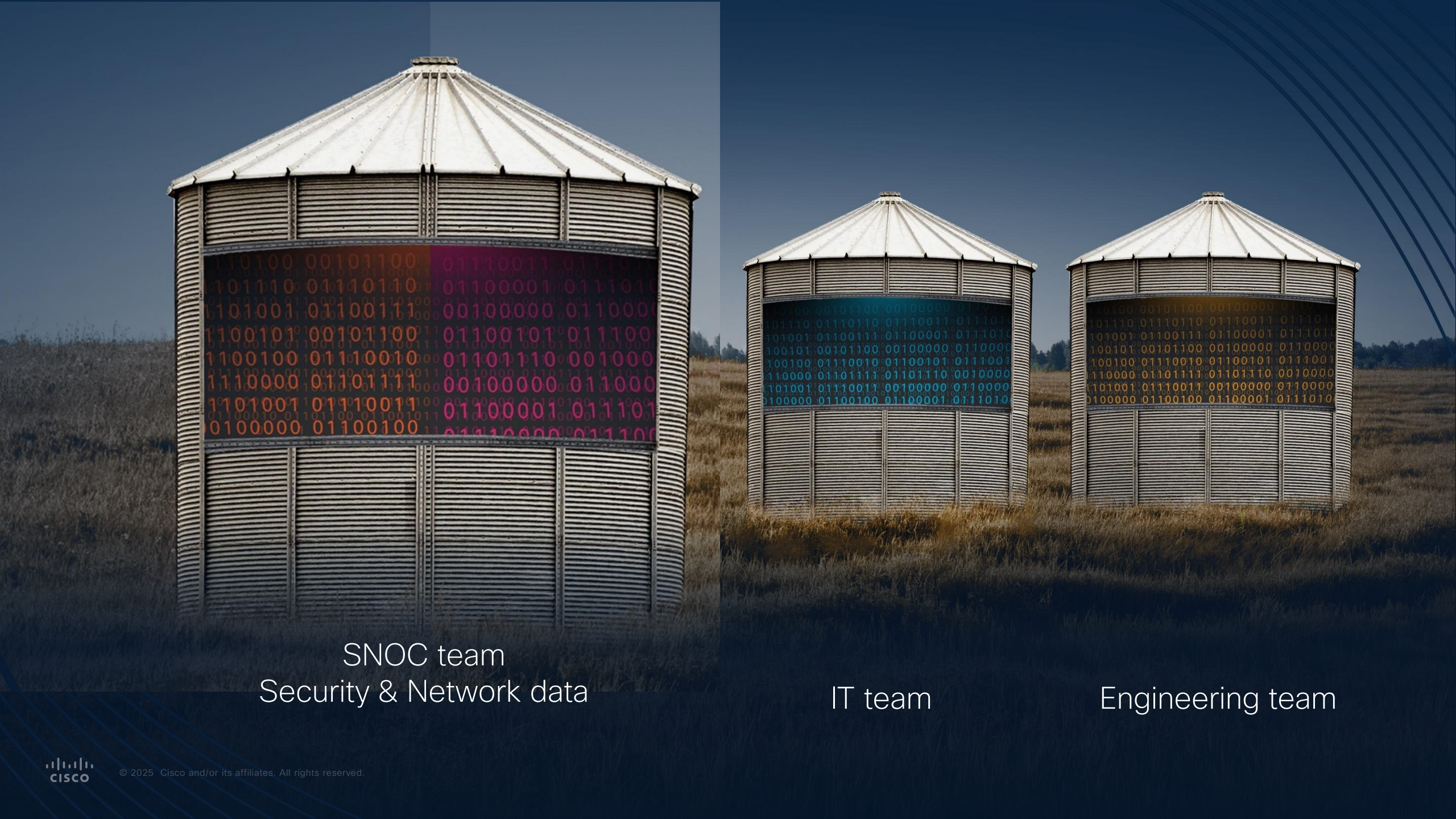
© 2025 Cisco and/or its affiliates. All rights reserved.

Supercharge your managed service offering or help clients do the same

Benefit	Details & Supporting Data
Faster Incident Response	Integrated teams enable faster mean time to detect (MTTD) and mean time to respond (MTTR), reducing downtime and limiting damage
Reduced Outage Costs	Median outage costs are 37% lower with unified observability and incident handling
Comprehensive Threat Detection	Real-time correlation of network anomalies and security threats creates a more complete and accurate view
Cost Optimisation	Eliminates duplicate tools and overlapping personnel, leading to significant cost savings
Resource Efficiency	Cross-trained staff and unified workflows allow teams to handle more incidents
Minimised Downtime	Integrated response processes speed up troubleshooting, minimizing business disruption
Higher Revenue for Providers	MSPs/MSSPs offering integrated services see higher average revenue per client
Improved Security Outcomes	Earlier detection and containment of threats, reducing risk of breaches and data loss

© 2025 Cisco and/or its affiliates. All rights reserved.
Cisco Confidential

© 2025 Cisco and/or its affiliates. All rights reserved.



© 2025 Cisco and/or its affiliates. All rights reserved.

“

How hard is it to hard to break out from the Networking silo?

What are the biggest barriers?

”

© 2025 Cisco and/or its affiliates. All rights reserved.

If it’s all so great, why haven’t people done this before?

People

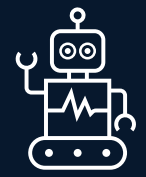
Talent gaps
Most engineers are specialise in either network or security, not both.

Multiple third-party vendors: If network and security operations are already outsourced to different providers, merging into a SNOC is difficult or impossible without major contractual and operational changes.

Process

Change is hard
Integrating workflows is difficult - SNOC requires unified ticketing, alert management, playbooks, and leadership alignment.

If these aren’t well-defined, it can cause confusion, duplicated work, or missed alerts. If everything is everyone’s job, critical issues may be missed.



Technology

Having the right underlying platform

AI wasn’t there
To be successful you need the right Machine Learning (ML) and Artificial Intelligence (AI) platforms to sort out what’s important, at scale, to surface what’s critical for SNOC specialists. Otherwise too many false positives and too little time

© 2025 Cisco and/or its affiliates. All rights reserved.
Cisco Confidential

What’s changed?

© 2025 Cisco and/or its affiliates. All rights reserved.

What’s changed?

AI

© 2025 Cisco and/or its affiliates. All rights reserved.

Where have you seen AI genuinely help in the NOC / SOC / SNOC?

(if at all?)

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Why AI made a SNOC (more) possible

If it’s all so great, why haven’t people done this before?

People

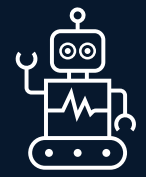
Talent gaps
Most engineers are specialise in either network or security, not both.

Multiple third-party vendors: If network and security operations are already outsourced to different providers, merging into a SNOC is difficult or impossible without major contractual and operational changes.

Process

Change is hard
Integrating workflows is difficult - SNOC requires unified ticketing, alert management, playbooks, and leadership alignment.

If these aren’t well-defined, it can cause confusion, duplicated work, or missed alerts.
If everything is everyone’s job, critical issues may be missed.



Technology

Having the right underlying platform

AI wasn’t there
To be successful you need the right Machine Learning (ML) and Artificial Intelligence (AI) platforms to sort out what’s important, at scale, to surface what’s critical for SNOC specialists.
Otherwise too many false positives and too little time

© 2025 Cisco and/or its affiliates. All rights reserved.
Cisco Confidential

Technology | Build the SNOC with Cisco + Splunk

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Delivering the essential elements of a Unified TDIR Platform

The foundation for the SNOC of the future

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Technology | Splunk's approach to AI

Generative AI

Make everyone an expert

Reduce need for environment and tool expertise by simplifying analysis and investigations.

Machine and Deep Learning

Detect and predict

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

Correlate and diagnose

Aggregate and analyze all data to investigate and identify root causes.

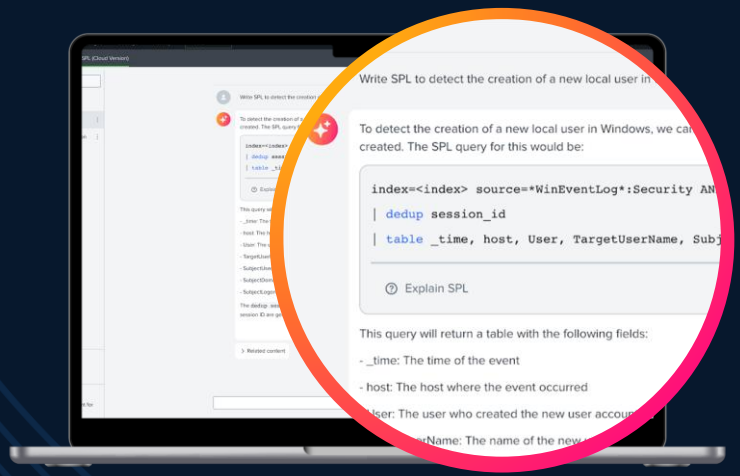
© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

People | Bridge the knowledge gap with AI Assistants everywhere

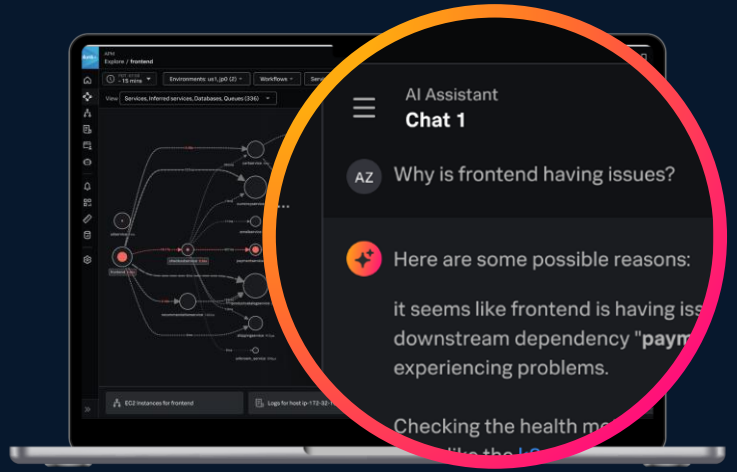
Increase productivity and deliver faster detection and response

AI Assistant for SPL



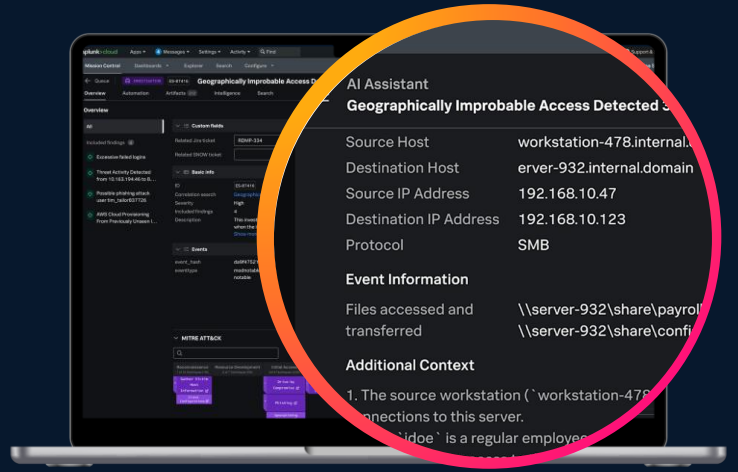
Generally Available

AI Assistant in Observability Cloud



Generally Available

AI Assistant in Enterprise Security



Preview

© 2025 Cisco and/or its affiliates. All rights reserved.

People | Bridge the knowledge gap with AI Assistants everywhere

Make everyone a SNOC expert

Faster Insights and Content

"Which K8s nodes have memory utilization more than 90%?"

Assisted Troubleshooting

"What is wrong with my payment service?"

Chat with Your Data

"List critical incidents impacting checkout service"

© 2025 Cisco and/or its affiliates. All rights reserved.

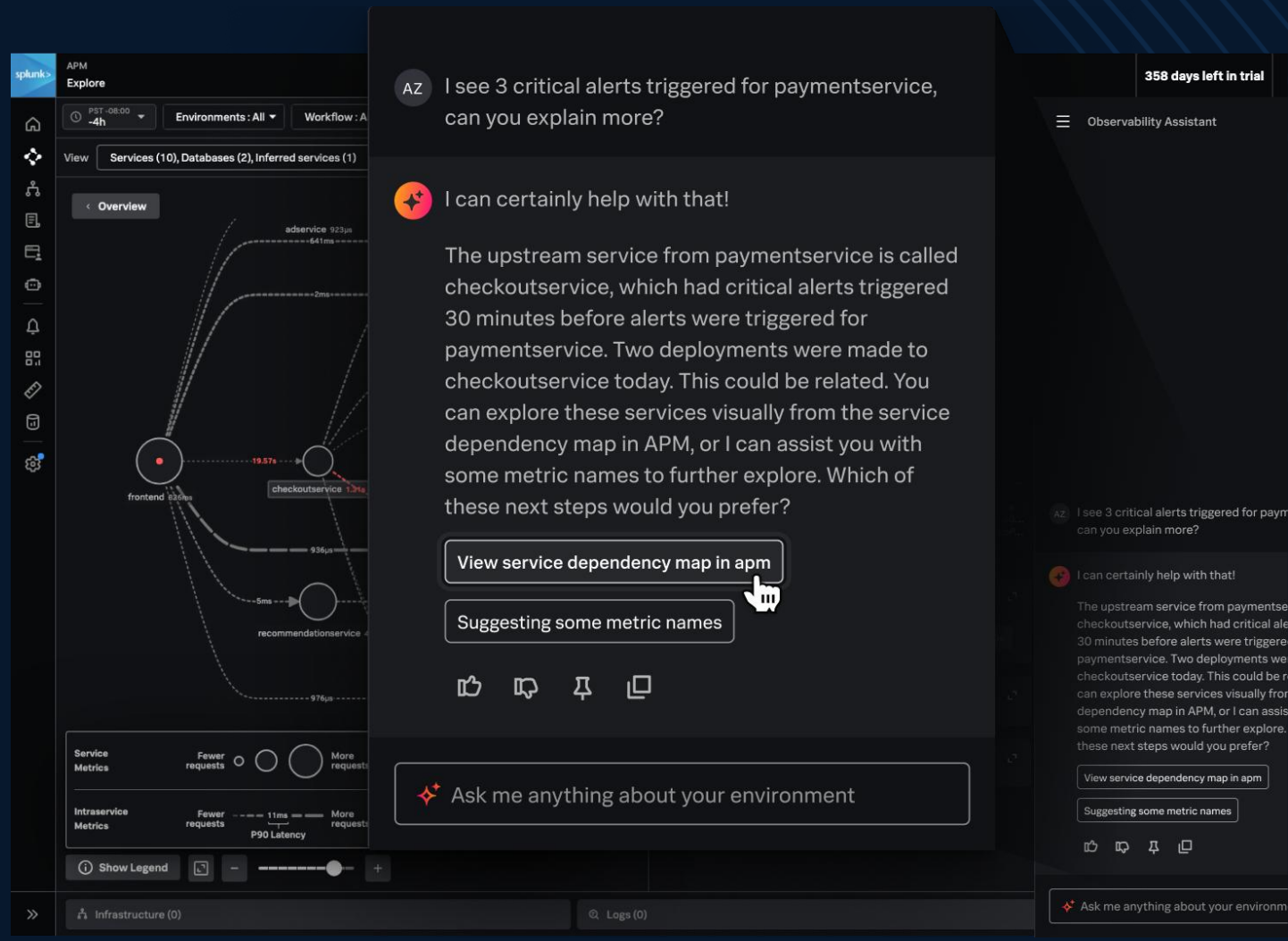
Cisco Confidential

People | Bridge the knowledge gap with AI Assistants everywhere

AI Assistant in Observability Cloud

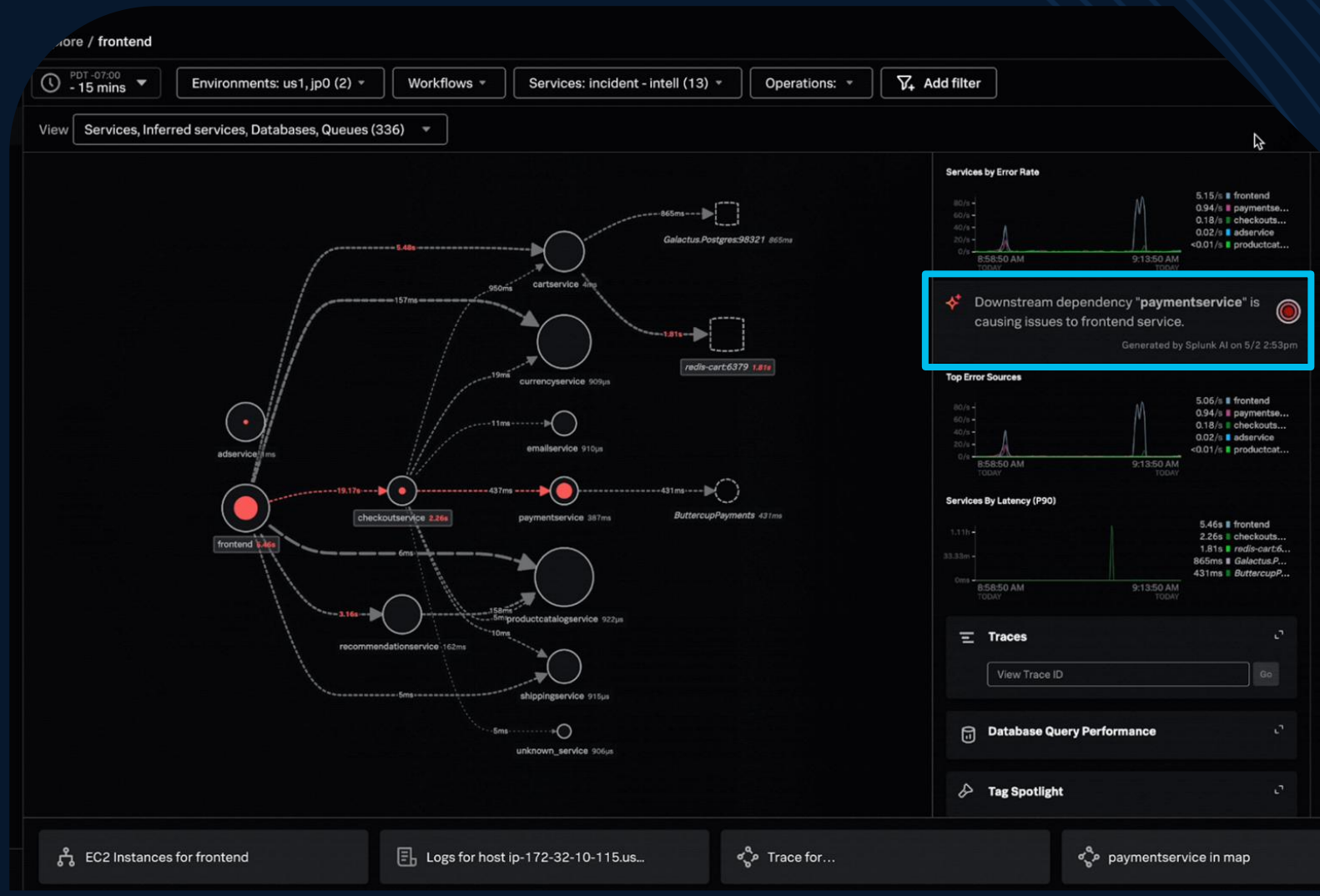
Find and fix issues faster using natural language

- Surface key insights by chatting with your data
- Accelerate investigations and day-to-day monitoring tasks
- Get context and support as you troubleshoot



© 2025 Cisco and/or its affiliates. All rights reserved.

Automated
AI Assisted Troubleshooting (COMING SOON)



© 2025 Cisco and/or its affiliates. All rights reserved.

Process | Agentic AI to automate tasks

*Skill refers to the ability to perform a task or interact with other models, applications or systems.

© 2025 Cisco and/or its affiliates. All rights reserved.
Cisco Confidential

Process | AI Analytics in Splunk Security

Embed AI-powered assistive experiences across the Threat Detection Investigation and Response (TDIR) workflow

Comprehensive security monitoring and visibility

Search and correlate across hybrid, cloud, and on-premises data sources for maximum attack surface coverage. Onboard and normalize data through AI-driven guided workflows.

Faster, accurate threat detection with context

Improve threat detection accuracy with ML-based detections and real-time behavioral analytics.

Accelerated threat investigation and hunting

Streamline repetitive tasks like interpreting and prioritizing high volumes of alerts by providing investigation guidance, automating search queries, summarizing incident findings, and generating investigation reports.

Orchestrated and automated response

Automate TDIR workflows by recommending and executing automated response actions, and summarizing results to help analyst review and determine next steps with confidence.

Continuous improvement

Assist detection engineers to develop, test, deploy, and refine detections effortlessly.

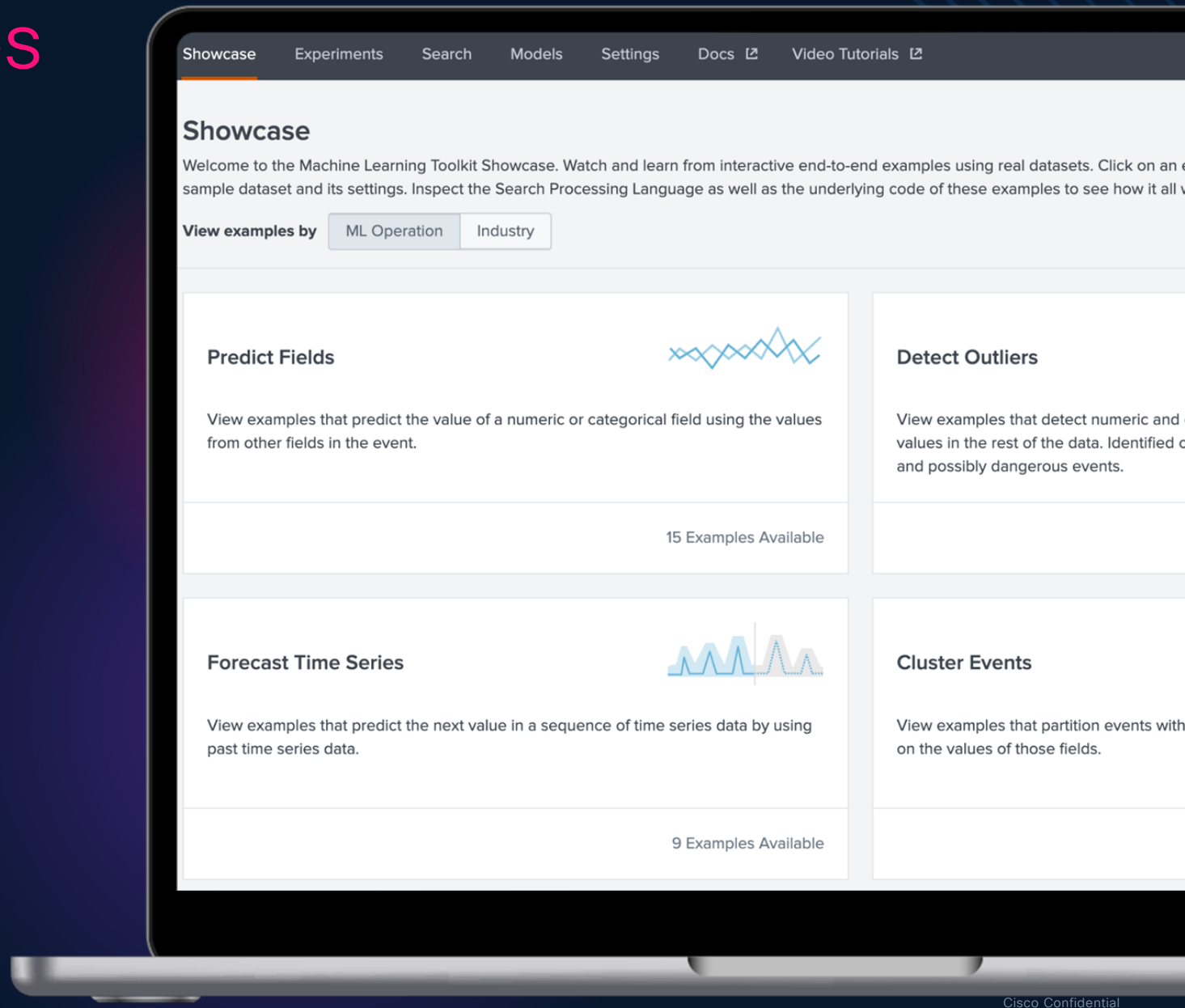
CISCO © 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Customize AI use cases with Machine Learning Toolkit (MLTK)

In Splunk Cloud and Enterprise

- Experiment and model your Splunk data with guided assistant for the whole AI workflow.
- 50+ algorithms to choose from or bring your own model.
- Train and deploy with search commands and operationalize in real-time.

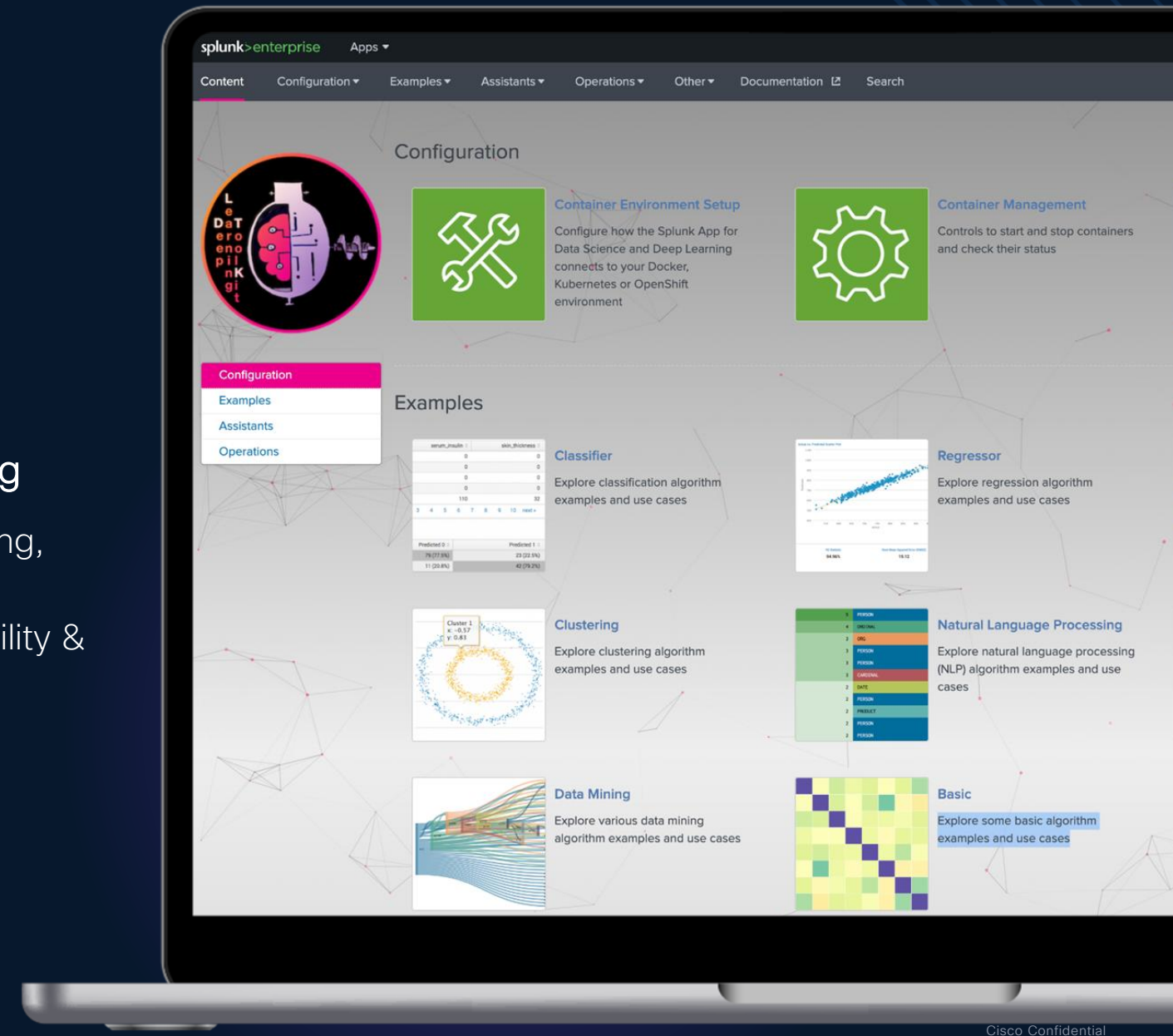


© 2025 Cisco and/or its affiliates. All rights reserved.

Extend MLTK to operationalize advanced custom AI/ML use cases

Splunk App for Data Science and Deep Learning

- **35+ Code Examples:** Guided model building, testing, and deployment
- **Container Management**: productionized for scalability & optimization on CPU & GPU
- State of the art AI frameworks and tools
- Flexible deployments and open source
- Extension to LLMs and VectorDB



© 2025 Cisco and/or its affiliates. All rights reserved.

“

How do you see AI impacting human roles inside a SNOC? Are we shifting skillsets, retasking analysts, or creating new job types?

”

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

“

Where do you think AI adds real value in a SNOC, and where is it overhyped

”

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

What opportunities exist for you to wrap services around a SNOC transformation?

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

What’s the biggest risk in relying on AI-driven detection and response in a SNOC?

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Use cases for AI

Use cases for Ai in the SNOC

Top Use Cases for AI

Incident investigation: Identify patterns, suppress low-fidelity alerts, and automate triage and validation

• Case management: Prioritise, track, and manage security incidents by intelligently enriching and automating cases.

• Workflow generation: Prompt AI to instantly build security automation workflows

• Case summarization: Analyze all relevant data points associated with a security alert to provide easy-to-digest, evidence-backed summaries of complex security cases, improving SOC analysts' efficiency and collaboration.

• Documentation: Automatically generate documentation for complex automated processes, increasing both efficiency and accuracy from shift-handovers to compliance audits.

•Executive reporting: Prompt the system to generate case info in the right tone and level of information for a specific persona, such as for a non-technical executive or board member.

• Team collaboration: Automatically alert Slack or Teams channels when a case is created, escalated, resolved and more.

• Resource optimization: Use AI to assign cases to an available analyst based on workload and shift schedules.

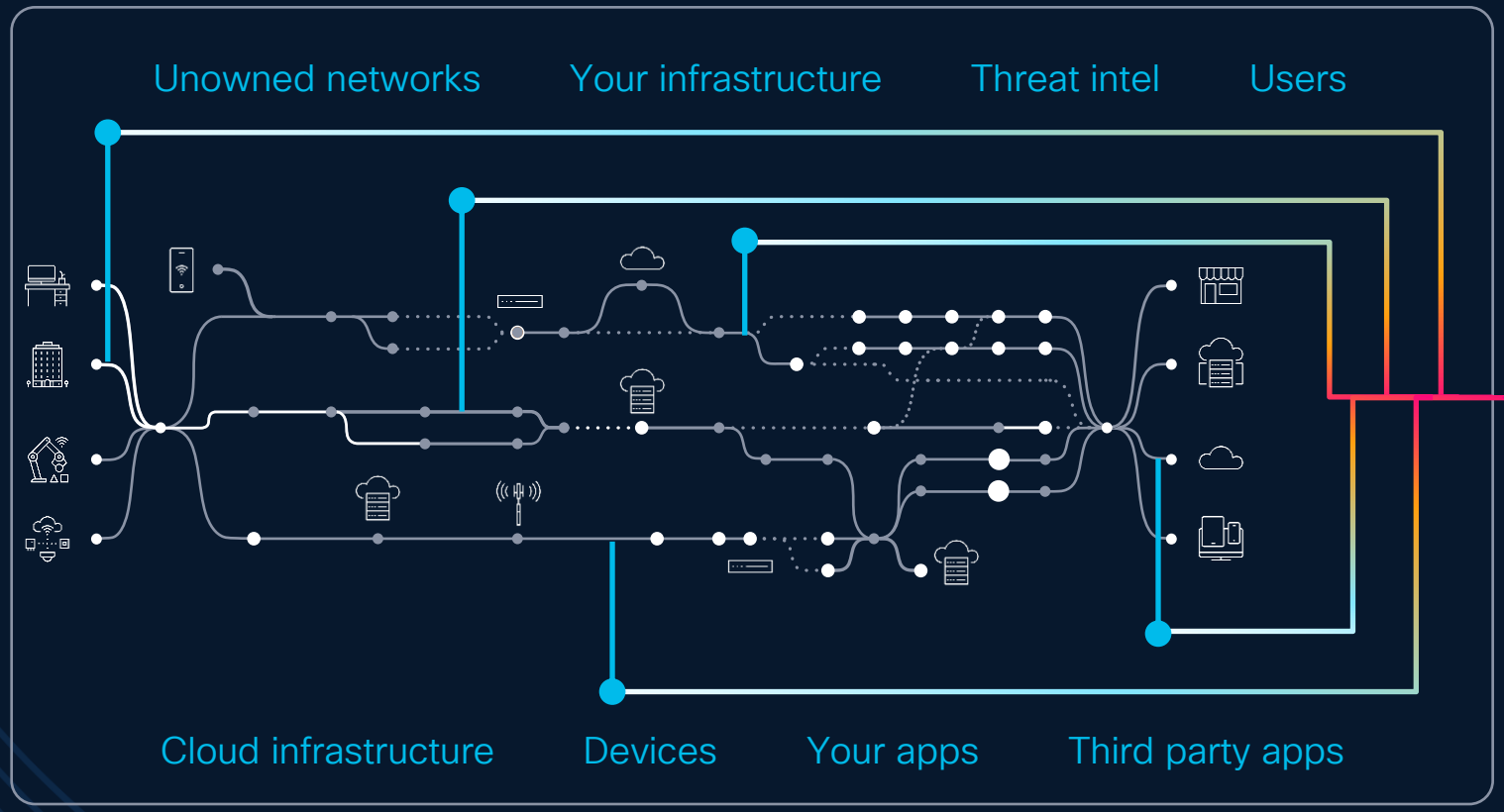
• Data correlation: Combine and correlate data from all of the tools in your security stack, providing a holistic view of your security environment.

• Threat response: Automate tasks like threat detection and containment for faster incident resolution.

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco + ThousandEyes + Splunk

The data platform fueling digital resilience



Data

Assurance

Observability

Data platform

Security Operations

Security
Comprehensive threat detection, investigation & response for orgs of any size & maturity

Assurance
Seamless connectivity across cloud, internet and enterprise networks

Observability
Prevent downtime and optimize experiences with visibility and insights across digital systems

© 2025 Cisco and/or its affiliates. All rights reserved.

Cisco Confidential

Takeaways

Think about usinga SNOC to eliminate silos, with join visibility and faster incident resolution

Real enterprises have seen a 90% reduction in false positives and significantly faster threat detections

Splunk’s AI-powered tools are ready for partner-led solutions to help clients

© 2025 Cisco and/or its affiliates. All rights reserved.