

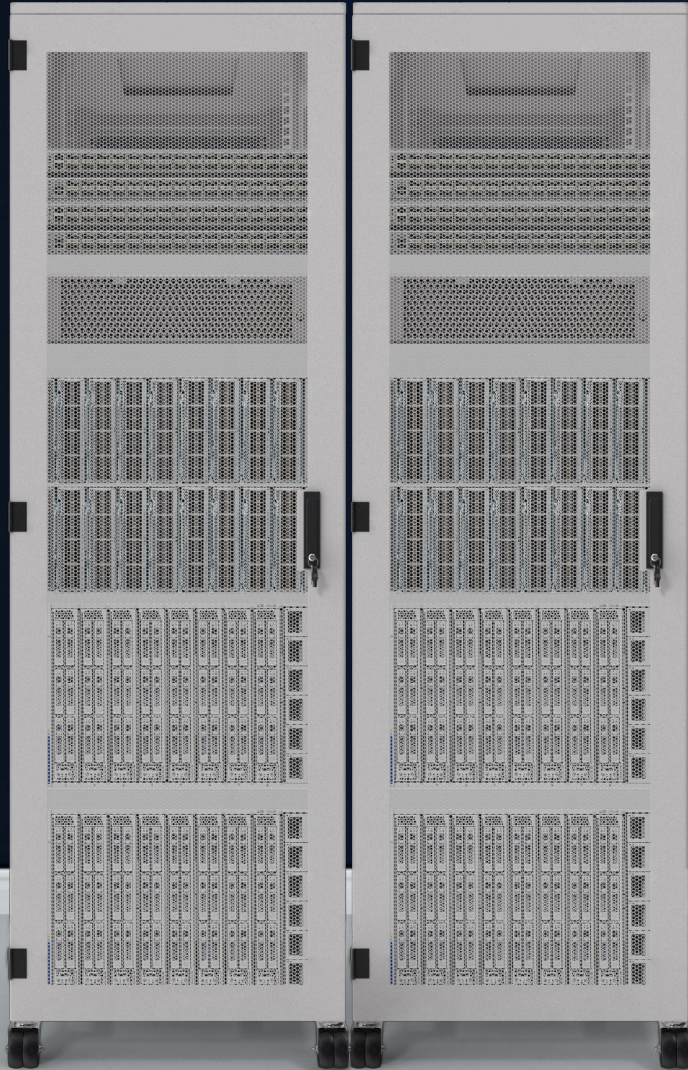
AI-Driven Assurance: Network Operations Reimagined

ITLGEN-2006

Jon Woolwine
Director, Technical Systems Engineering,
Cisco

Jacob Foxe
Site Reliability Engineer,
Cisco

cisco Live !
IT Leadership Program



opportunity The ~~imperative~~ to reimagine network operations

SAN JOSE

14:30:48

BANGALORE

02:30:48

LONDON

21:30:48

Legacy Network Operations Landscape 18 Months Ago



Outsourced 1st
Tier Network
Operations

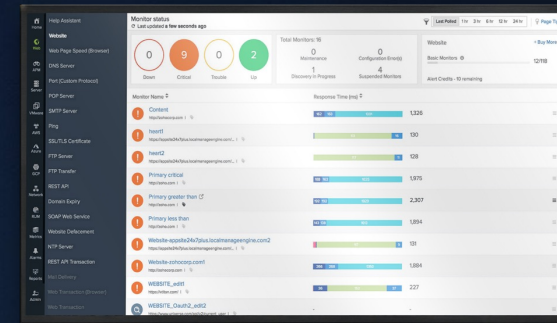


Robust Network
Source of Truth



Deep Visibility
Multiple
Assurance Tools

70,000
network devices



Legacy Network Operations

Network Assurance Challenges



Noise
Overload



Assurance Tool
Proliferation



Manual
Correlation

LONDON

21:30:48

Noise Overload

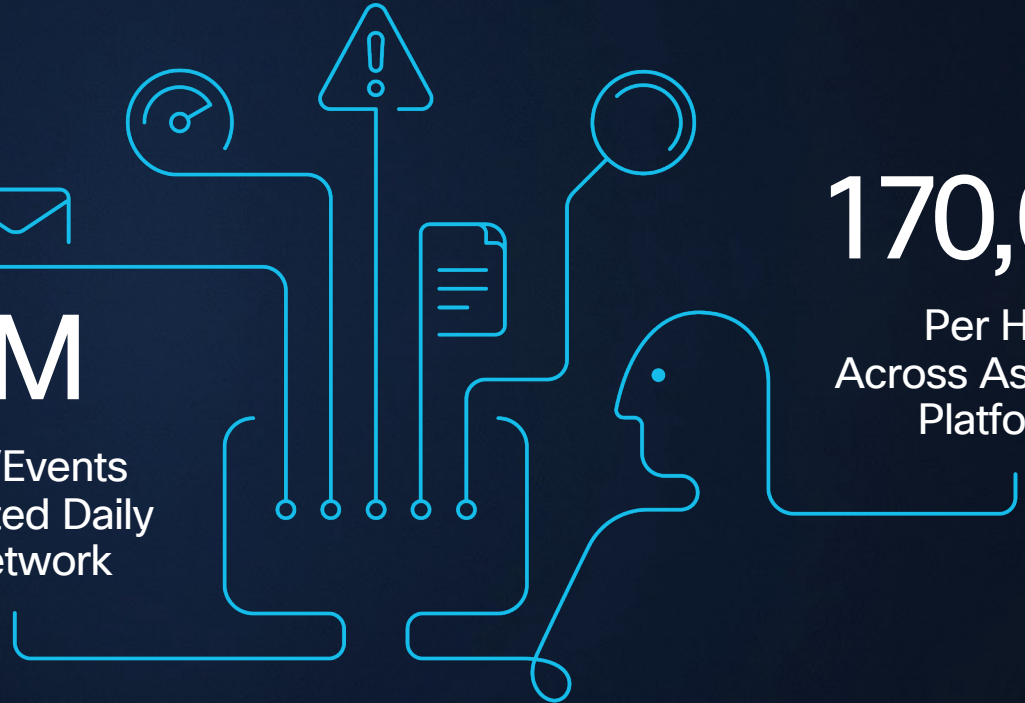


4M

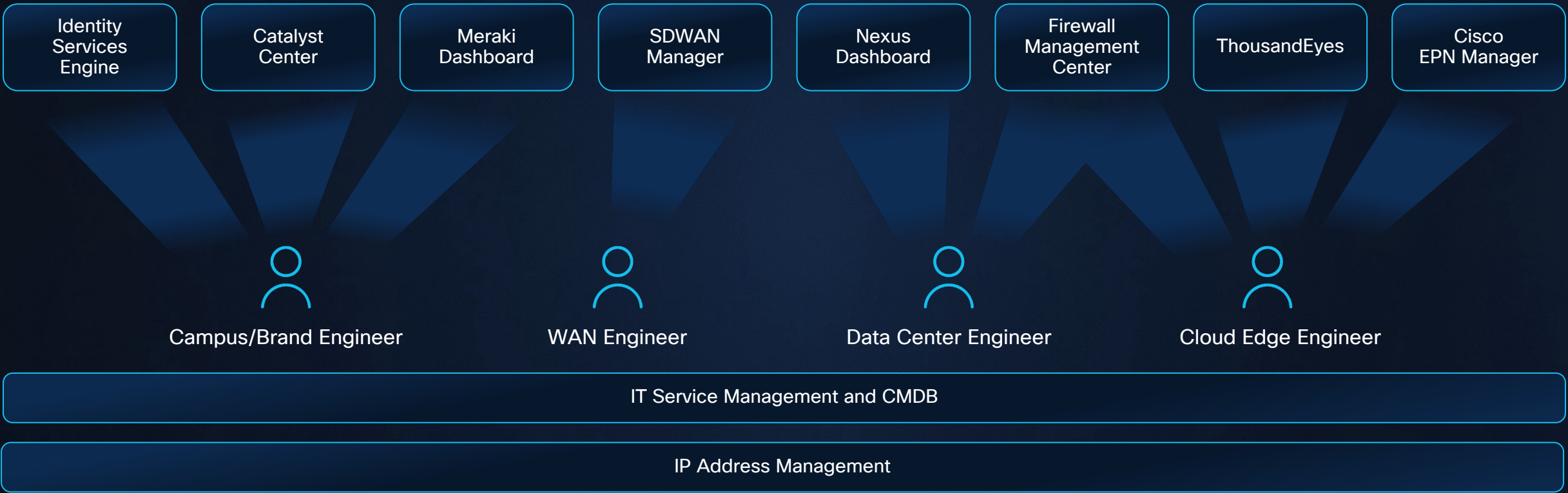
Alerts/Events
Generated Daily
on Network

170,000

Per Hour
Across Assurance
Platforms

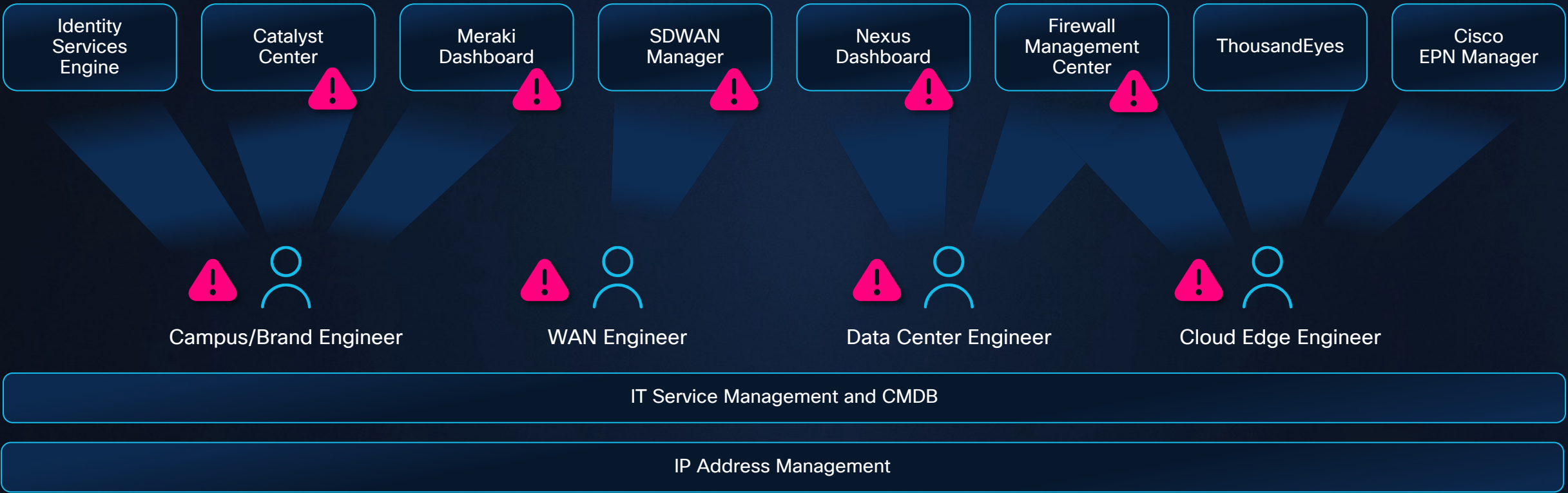


Assurance Tool Proliferation: Siloed Data, Tools, & Teams



 12,000 incidents per month

Real World Manual Correlation



Legacy Network Operations Business View



Failure-centric
Operations



Minor
Improvements
in MTTR



Minimal
Efficiency
Gains



Reimagining Network Operations

Constraints

*Budget
& Resources*

*No Impact on
Operational Metrics*



Strategy

SAN JOSE

14:30:48

BANGALORE

02:30:48

LONDON



Bring Network
Operations
In-house



Network
Observability &
Automation

*the
opportunity*



AI-powered
Network
Operations

Approach

1

2

3

4

5

Agentic AI: Moving from Theory to the Practical Use Case

58% Companies are open to using GenAI but require clear use cases with proven business value.

Gartner, Agentic NetOps Will Revolutionize Network Operations, 6 August 2025.
GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally and is used herein with permission. All rights reserved.

SAN JOSE

14:30:48

BANGALORE

02:30:48

LONDON

Approach

1

2

3

4

5

Approach

Steps We Took

1

Insource
Network
Operations

2

Capitalize
on Existing
Assurance
Tools

3

Unify
Observability
with Splunk

4

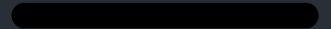
Enrich Events
with Context

5

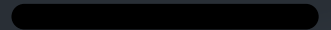
Automate
with
AI-assisted
Workflows

Impact

Noise



Tool Proliferation



Manual Correlation



1 Insource Network Operations



People & Process

Organizational Change Management

SRE Hiring & Upskilling

Portfolio Realignment

Tier 1 Network Support



Tooling

Rapid Transition

Basic Up/Down Monitoring & Alerting

Reuse of Existing Tool

CMDB
(network source of truth)



Lessons Learned

Value of Foundational Data: CMDB

Siloed Domains and Tools

Power of Unifying Events

Impact

Noise



Tool Proliferation



Manual Correlation



A Snapshot of Our Monitoring

TOTAL EVENTS TRIGGERED		TOTAL EVENTS CLEARED		TOTAL ACTIVE EVENTS		EVENTS BY TRIGGER TYPE		EVENTS BY SEVERITY		EVENTS BY DEVICE																											
163		131		32		<table><thead><tr><th>EVENT TRIGGER</th><th>EVENT COUNT</th></tr></thead><tbody><tr><td>Unavailable by ICMP pi...</td><td>150</td></tr><tr><td>No SNMP data collecti...</td><td>8</td></tr><tr><td>Composite Unavailable</td><td>3</td></tr><tr><td>Unavailable by SSH</td><td>2</td></tr></tbody></table>		EVENT TRIGGER	EVENT COUNT	Unavailable by ICMP pi...	150	No SNMP data collecti...	8	Composite Unavailable	3	Unavailable by SSH	2	<table><thead><tr><th>SEVERITY</th><th>EVENT COUN</th></tr></thead><tbody><tr><td>CRITICAL</td><td>15</td></tr><tr><td>MAJOR</td><td>1</td></tr></tbody></table>		SEVERITY	EVENT COUN	CRITICAL	15	MAJOR	1	<table><thead><tr><th>DEVICE NAME</th><th>EVENT COUN</th></tr></thead><tbody><tr><td>[id]-[id]-[id].cisco.com</td><td>72</td></tr><tr><td>[id]-[id]-[id].cisco.com</td><td>7</td></tr><tr><td>[id]-[id]-[id].cisco.com</td><td>7</td></tr><tr><td>[id]-[id]-[id].cisco.com</td><td>6</td></tr></tbody></table>		DEVICE NAME	EVENT COUN	[id]-[id]-[id].cisco.com	72	[id]-[id]-[id].cisco.com	7	[id]-[id]-[id].cisco.com	7	[id]-[id]-[id].cisco.com	6
EVENT TRIGGER	EVENT COUNT																																				
Unavailable by ICMP pi...	150																																				
No SNMP data collecti...	8																																				
Composite Unavailable	3																																				
Unavailable by SSH	2																																				
SEVERITY	EVENT COUN																																				
CRITICAL	15																																				
MAJOR	1																																				
DEVICE NAME	EVENT COUN																																				
[id]-[id]-[id].cisco.com	72																																				
[id]-[id]-[id].cisco.com	7																																				
[id]-[id]-[id].cisco.com	7																																				
[id]-[id]-[id].cisco.com	6																																				
EVENTS BY CRITICALITY				EVENTS BY LOCATION																																	
CRITICALITY		EVENT COUNT		LOCATION		EVENT COUNT																															
4		1		SCC01A		1																															
5		1		PAR03		1																															
3		1		BIR01		1																															
				SHN24		1																															

EVENTS

EVENT TIME (Browser Time Zone)	EVENTID	HOST ID	DEVICE	ENDPOINT SYS_ID	SEVERITY	EVENT CRITICALITY	EVENT MESSAGE
2025-10-17 04:10:22	1886503...	57946	[id-1234-abcd].cisco.com	67927698dbe6e600727ff...	CRITICAL	4	C4 - [id-1234-abc].cisco.com - Unavailable by ICMP Ping
2025-10-17 07:08:11	1887004...	61136	[id-1234-abcd].cisco.com	fc49faa31befdd10f9b955f...	CRITICAL	4	C4 - [id-1234-abc].cisco.com - Unavailable by ICMP Ping
2025-10-17 07:08:05	1887004...	61130	[id-1234-abcd].cisco.com	ab6a694b1b10a9dc00115...	CRITICAL	4	C4 - [id-1234-abc].cisco.com - Unavailable by ICMP Ping
2025-10-17 07:08:01	1887003...	61126	[id-1234-abcd].cisco.com	5271bed397aaa950df9f7f...	CRITICAL	4	C4 - [id-1234-abc].cisco.com - Unavailable by ICMP Ping
2025-10-17 07:08:00	1887003...	61125	[id-1234-abcd].cisco.com	3741b693976ea950b985...	CRITICAL	4	C4 - [id-1234-abc].cisco.com - Unavailable by ICMP Ping

2

Capitalize on Existing Assurance Tools

Operationalize Advanced Features



Advantages

Beyond Basic Monitoring
& Alerting

Machine Learning
Capabilities

Deep Visibility



Behavior Changes

Resist Jumping into CLI

Starting Point for
Tier 1 Troubleshooting

Limited Access to CLI



Lessons Learned

Assurance Tools Amplify
the Signal

Offloaded Manual Correlation

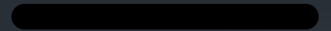
Changing Engineer Behavior

Impact

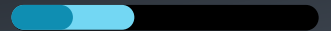
Noise



Tool Proliferation



Manual Correlation





Something is affecting
Wi-Fi users in Site MND01



Resolution: ISE Server Outage



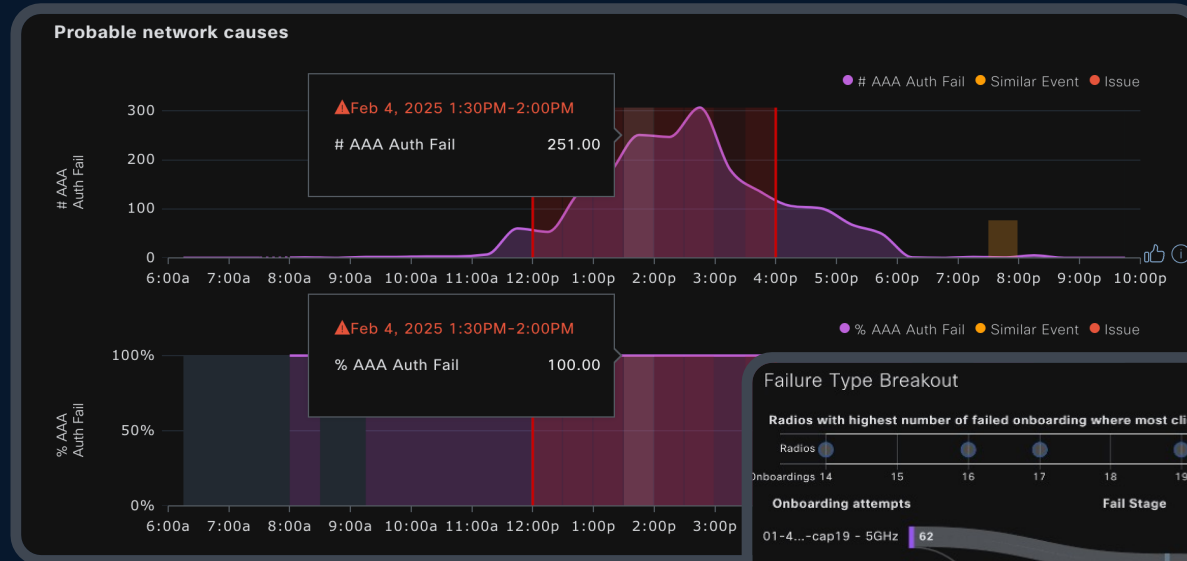
(P2) Excessive Time to Connect:
High Deviation from Baseline

HNA CatC AI Assurance 04/02/2025, 15:56

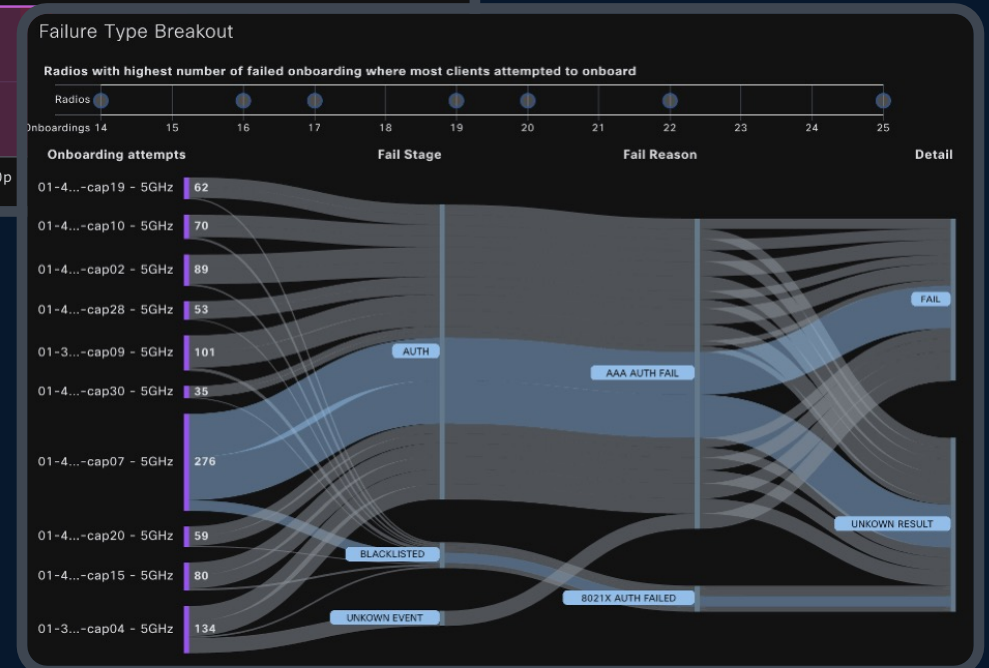
Cisco DNA Center Notification

Source DNA: dna.[id].cisco.com
Center IP:
Severity: 2
Category: WARN
Timestamp: 2025-02-04 12:00:00
Issue Name: Excessive time to connect - At least 78% increase in time on [network] in Global/[location-id]/[id].
Issue Description: The network is experiencing excessive onboarding time compared to usual. Clients are taking longer than the usual time to connect to SSID [network].
Issue Status: active

[Cisco DNA Center Issue Details](#)



Deviation observed
from what Catalyst
Center deems as
“normal” flagging
AAA failures.



3 Unify Observability with Splunk

All MELT Data into One Observability Platform



Converged Platform

MELT from All Network Devices and Assurance Platforms

Automated Configuration Changes

Grouping Events into Situations



Behavior Changes

Splunk as Starting Point for Tier 1 Triaging

Splunk Dashboards and Queries Facilitate Triaging

Assurance Tools for Drill-Down



Lessons Learned

Breakdown of Data AND Team Silos

Missing Context Through ITSM and CMDB

Remained Human-Driven, Operationally Reactive

Impact

Noise



Tool Proliferation



Manual Correlation





Site PAR03 is Down



Resolution: Case Raised with ISP



Event Timeline: Alerts in Multiple Data Sources Received in 30 Minutes

_time ^	alert_source ^	ci_name ^	subcategory ^
2025-10-17 14:06:04.838	vManage	[id]-[id]-sdwag-gw1	sla_violation_packet_drop
2025-10-17 14:06:04.838	vManage	[id]-[id]-sdwag-gw1	sla_violation_packet_drop
2025-10-17 14:06:04.846	vManage	[id]-[id]-sdwan-gw2	bfd_tloc_state_change
2025-10-17 14:06:04.846	vManage	[id]-[id]-sdwan-gw2	bfd_tloc_state_change
2025-10-17 14:06:04.846	vManage	[id]-[id]-sdwan-gw1	bfd_tloc_state_change
2025-10-17 14:06:04.846	vManage	[id]-[id]-sdwan-gw1	bfd_tloc_state_change
2025-10-17 14:06:04.846	vManage	[id]-[id]-sdwan-gw1	bfd_tloc_state_change
2025-10-17 14:06:04.846	vManage	[id]-[id]-sdwan-gw1	bfd_tloc_state_change
2025-10-17 14:06:19.973	vManage	[id]-[id]-sdwan-gw2	bfd_node_state_change
2025-10-17 14:06:19.973	vManage	[id]-[id]-sdwan-gw2	bfd_node_state_change
2025-10-17 14:06:19.973	vManage	[id]-[id]-sdwan-gw1	bfd_node_state_change
2025-10-17 14:06:19.973	vManage	[id]-[id]-sdwan-gw1	bfd_node_state_change
2025-10-17 14:06:34.776	vManage	[id]-[id]-sdwan-gw1	bfd_node_state_change
2025-10-17 14:06:34.776	vManage	[id]-[id]-sdwan-gw1	bfd_node_state_change
2025-10-17 14:08:04.746	Zabbix	[id]-[id]-lab-gw1	Unavailable by ICMP ping
2025-10-17 14:08:04.746	Zabbix	[id]-[id]-sdwan-gw2	Unavailable by ICMP ping

index=neoeven

vMa
2 M

✓ 85 events

Events (85)

Timeline for



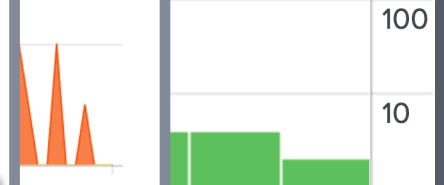
- DNAC - N
- DNAC - N
- DNAC - N
- Zabbix -
- Zabbix -
- Zabbix -
- vManage
- vManage

ate time range ▾



Fast Mode ▾

minute per column



splunk>

4

Enrich Events with Context



Automated Processes

Integration of External Data Sources for Enrichment

Events Linked to Configuration Items

Planned Maintenance Context



Behavior Changes

No Changes to Tier 1 Triaging in Splunk

More Context Visible within Events in Splunk

Avoids Swivel Chairing Over to ITSM and CMDB



Lessons Learned

Automated Data Enrichment Reduces Manual Effort

Instant Context Empowers Engineers to Act Quickly

SRE Skills Needed

Impact

Noise



Tool Proliferation



Manual Correlation





Office CAE02 is Down



Planned Power Maintenance Confirmed



Everything is Alerting in Multiple Platforms – Received 221 Events in 30 Minutes

_time ▾	alert_source ▴ ▾ ✎	ci_name ▴ ▾ ✎	subcategory ▴ ▾ ✎	chg_number ▴ ▾ ✎	chg_outage ▴ ▾ ✎
2025-10-19 05:26:17.327	Meraki	[id]-[id]-cap00	stopped_reporting	['CHG1994380']	[<ChangeOutage.YES: 'Yes'>]
2025-10-19 05:26:02.522	DNAC	[id]-[id]-gw1	NETWORK-NETWORKS-2-272	['CHG1994380']	[<ChangeOutage.YES: 'Yes'>]
2025-10-19 05:26:02.522	network_Splunk	[id]-[id]-gw1	INTERFACE STATE CHANGE	['CHG1994380']	[<ChangeOutage.YES: 'Yes'>]
2025-10-19 05:25:47.209	Outage CR	Yes			geOutage.YES: 'Yes'>]
2025-10-19 05:25:17.234	* Summary	CAE02 – WPR Statutory Integration Test. Full-power down. Start time: 19OCT2025 at 08:00AM			
2025-10-19 05:25:17.233	Meraki	[id]-[id]-cap00	unreachable	['CHG1994380']	[<ChangeOutage.YES: 'Yes'>]
2025-10-19 05:25:17.233	Meraki	[id]-[id]-cap00	unreachable	['CHG1994380']	[<ChangeOutage.YES: 'Yes'>]

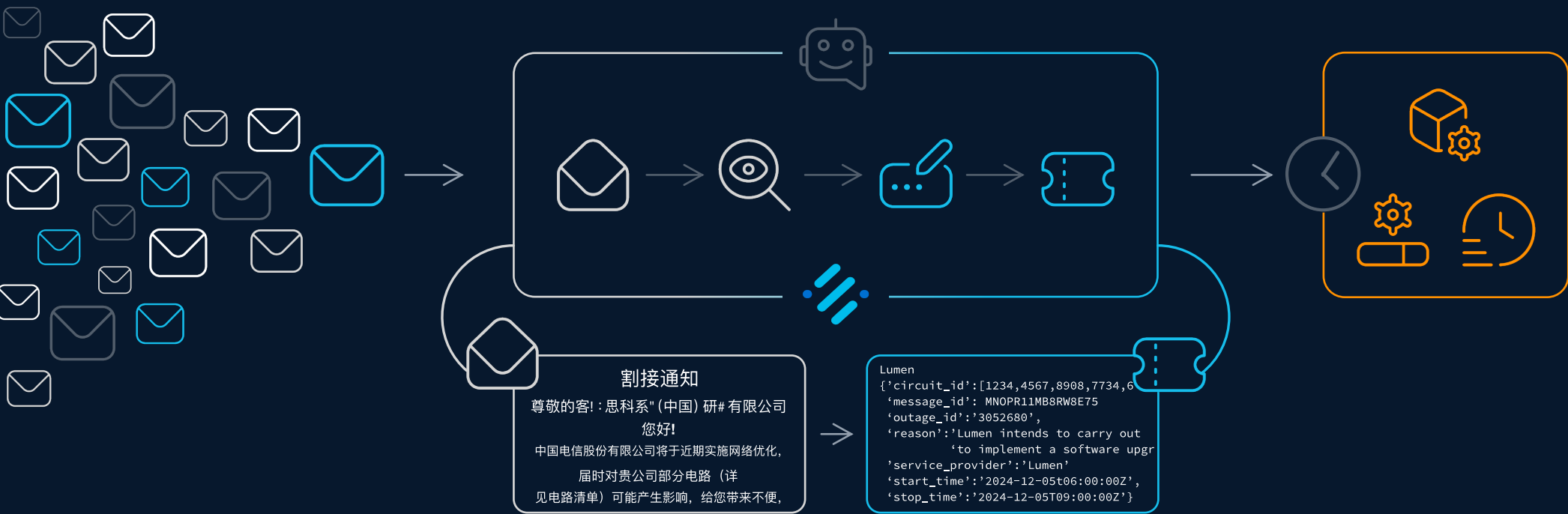
Enrichment: Service Provider Maintenance

Process: AI-Driven

Incoming Provider
Maintenance Notifications

Agent Reads, Prompts for
JSON, Posts CR to ESP

CR Submission
& Lifecycle



Automate with AI-Assisted Workflows



Automated Processes

Instant Incident Creation
in ServiceNow

Automated Webex
Messaging for Critical Events

Automated ISP Engagement

AI-assisted Triaging and
Closure of Incidents



Solution Highlights

Data Foundation:
CMDB, ITSM, Run Books

In-house Action Engine

Cisco Sanctioned GenAI
Assistant



Lessons Learned

Shift from Reactive
to Proactive

Start with Low Risk

Opportunity to Shift
to Splunk in Future

Impact

Noise



Tool Proliferation



Manual Correlation





Network Device Connectivity



Resolved: 16 mins

Detected
22:14



Alert Ingested

*Summary

Connectivity Issue - [id]-wan-wg1-[id]

*Description

Rule matched: WAN - Interface Connectivity
- Auto Triage - network-devops-wan

Severity: medium

Summary: 3 events (1 active) from sources:
DNAC, network_Splunk.



Incident Created

Opened
22:14



Run Commands and
Check Knowledge

```
show_commands: ["show ip eigrp  
vrf 1 neighbor",  
"show eigrp address-family ipv6  
vrf 1 neighbors"]
```

```
controllers: ["dnac-rcdn9-prd"]
```

```
tools: ["run_commands",  
"search_knowledge_base"]
```



LLM Analysis

user_prompt: "For this issue to be cleared, the EIGRP neighbor must be restored. If the incident description contains adjacency up, then this is not an EIGRP issue and the incident should be resolved immediately."



Incident Resolved

Resolved
22:30

Priority ▲ Issue Type ▲

P2 Network Device Interface Connectivity
- EIGRP Adjacency Failure

AA auto-triage.gen generic account (aut... Additional comments • 2025-10-27 22:30:35

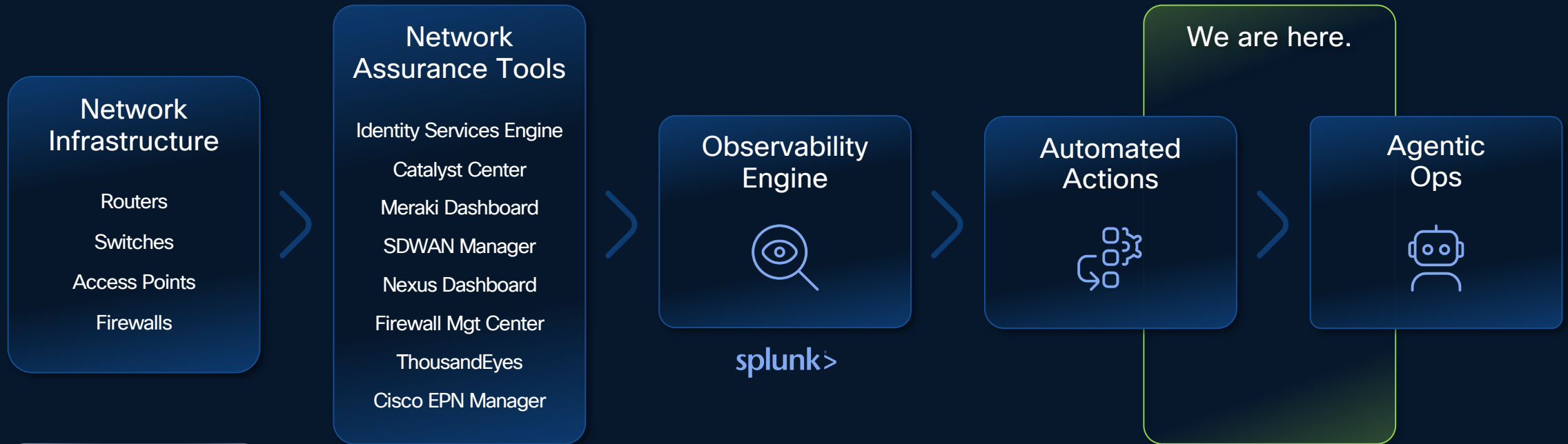
Because the option 'on_issue_cleared' was set to 'resolve', this case has been automatically resolved by the Funnel Auto Triage service.

AA auto-triage.gen generic account (aut... Field changes • 2025-10-27 22:30:35

Incident state Resolved was Work In Progress

70% Reduction in Cases Assigned to Engineers

Evolution of Network Observability Data Pipeline



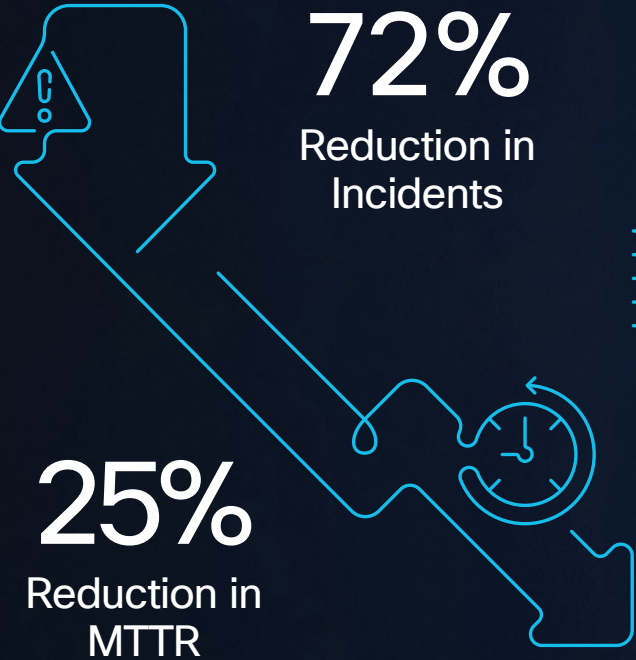
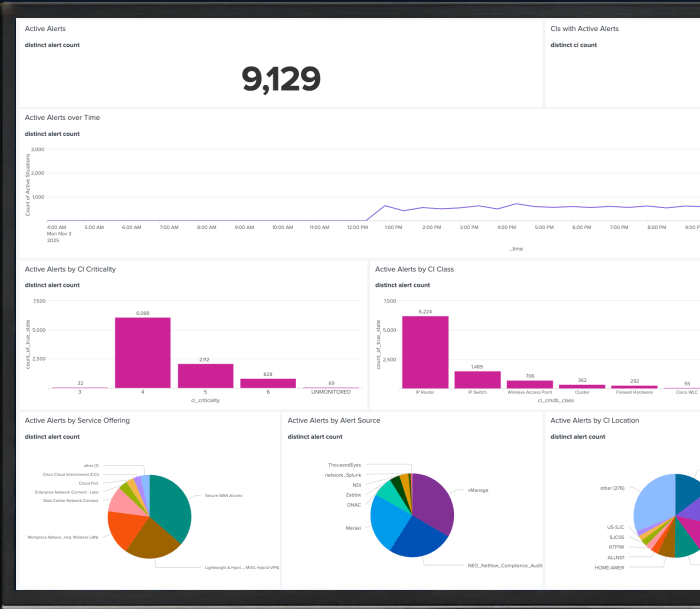
1. IN-HOUSE MONITORING

2. ASSURANCE

3 & 4. MELT INTO SPLUNK, ENRICHMENT

5. ACTIONS

Operational Outcomes



02:30:48

Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to win 1 of 5 full conference passes to Cisco Live 2025.



Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.



Level up and earn exclusive prizes!



Complete your surveys in the Cisco Live mobile app.

Continue your education



Visit the Cisco 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 www.CiscoLive.com/on-demand

Thank you

CISCO Live !