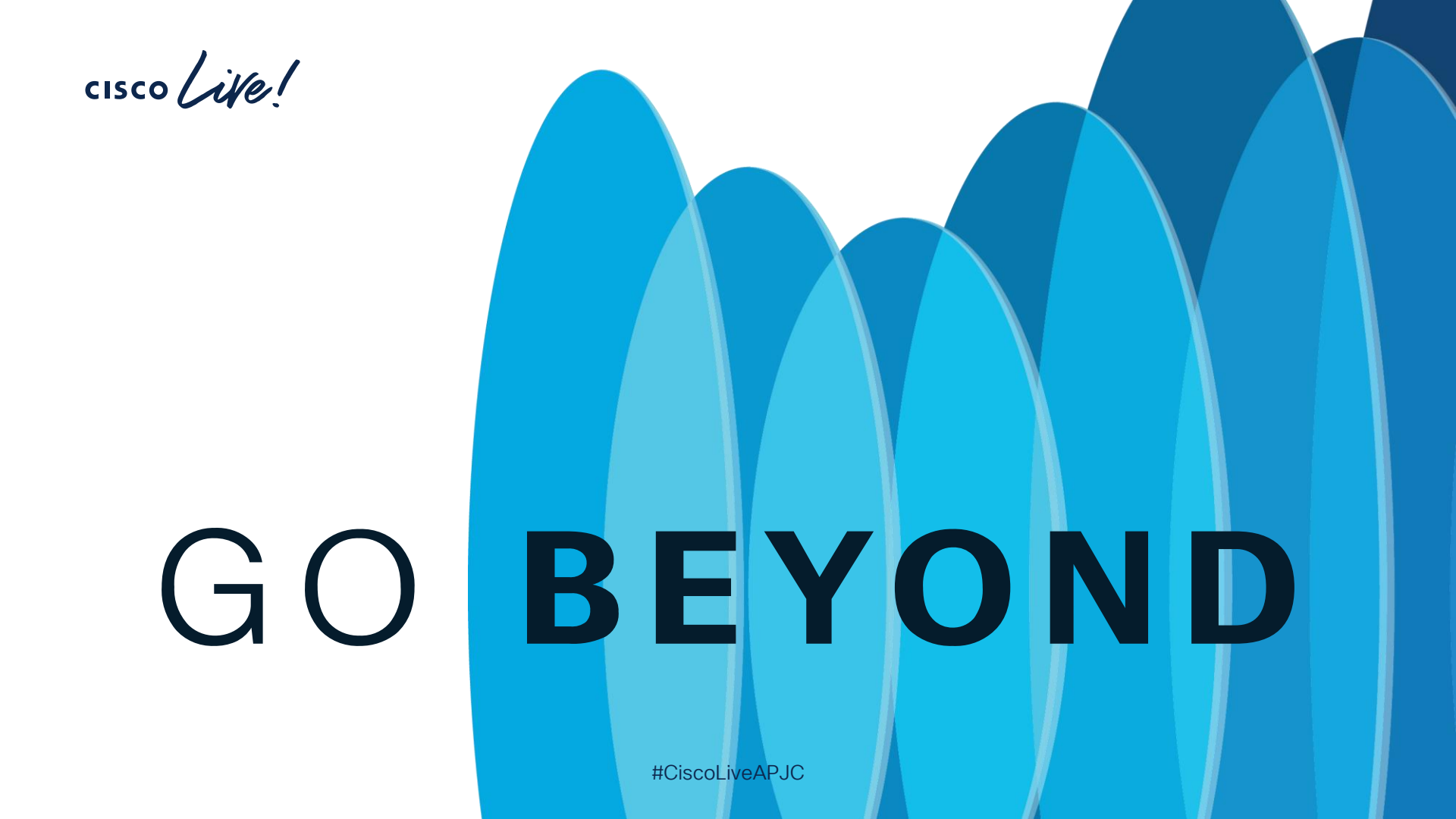

cisco Live!
GO BEYOND
#CiscoLiveAPJC

Simplify the Analyst Experience by Harnessing AI and Machine Learning

Using AI for SecOps Efficiency

Jay Kripalani, Senior Security Solution Architect - Splunk
@jkripala

BRKSEC-2586

Cisco Webex App

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2586

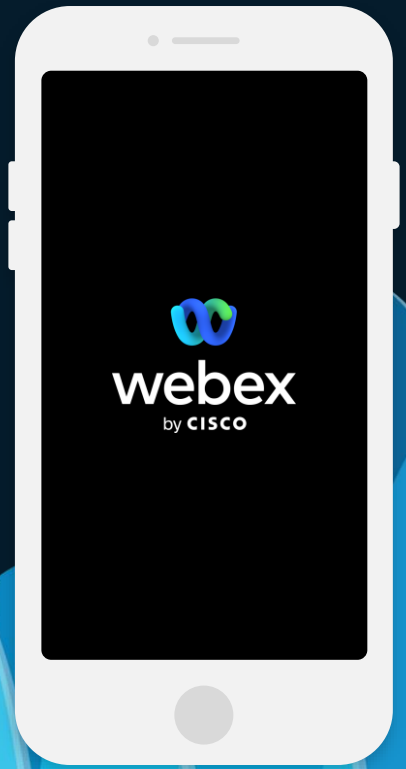
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

1. Find this session in the Cisco Live 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

Webex spaces will be moderated by the speaker until November 15, 2024.



cisco Live!

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

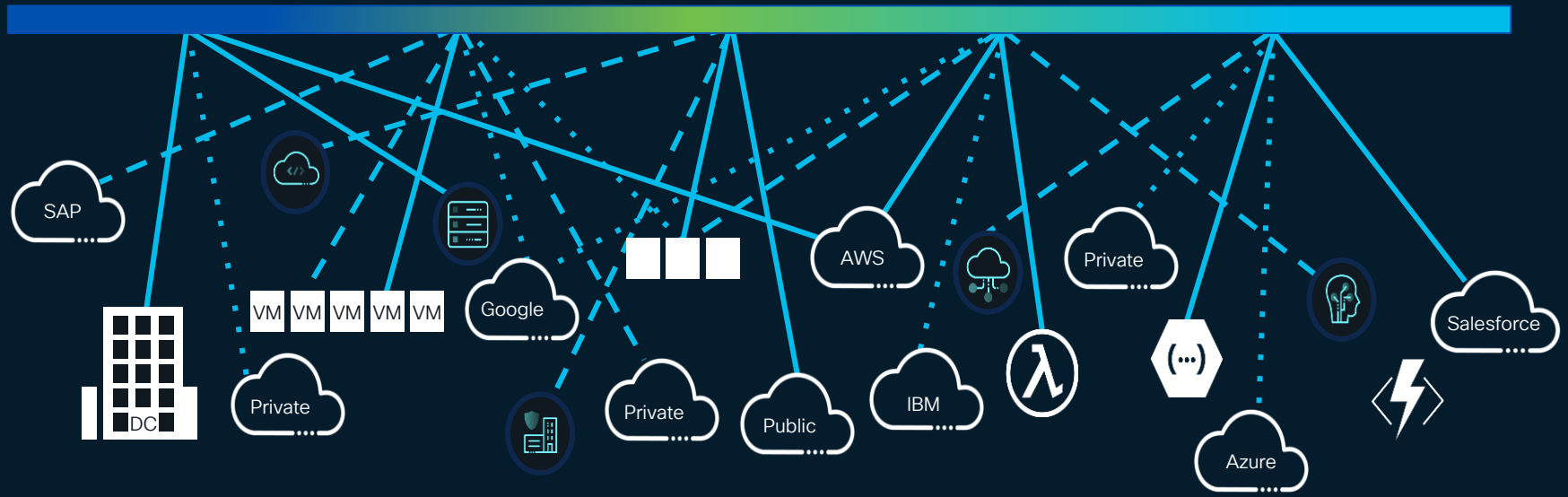
Forward-looking statements

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 May 21, 2024 and its most recent report on Form 10-K filed on September 7, 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.

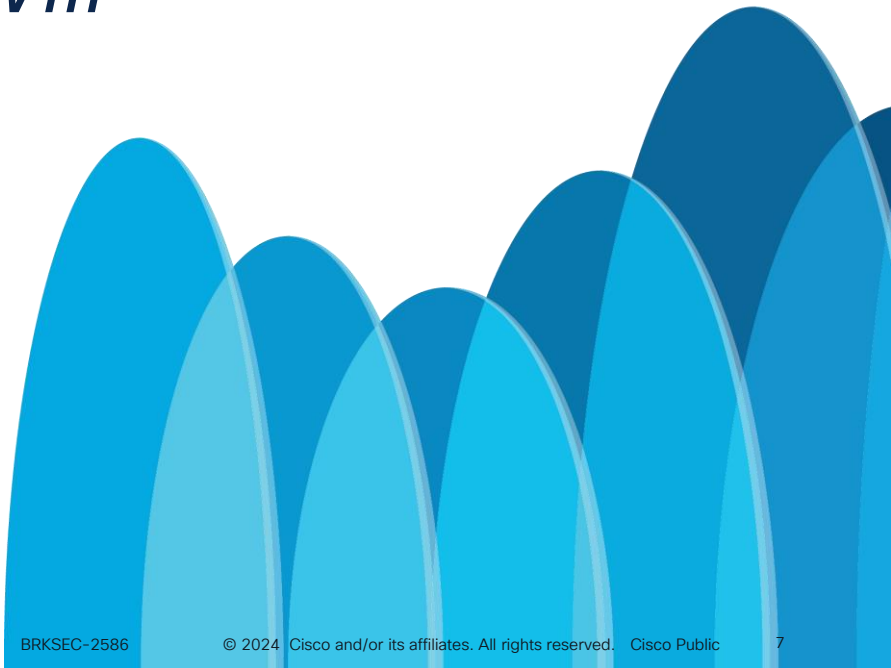
Splunk and Splunk> are trademarks and registered trademarks of Splunk Inc. in the United States and other countries. All other brand names, product names, or trademarks belong to their respective owners. © 2024 Splunk Inc. All rights reserved.

Digital Transformation Made Detection, Investigation and Response Harder



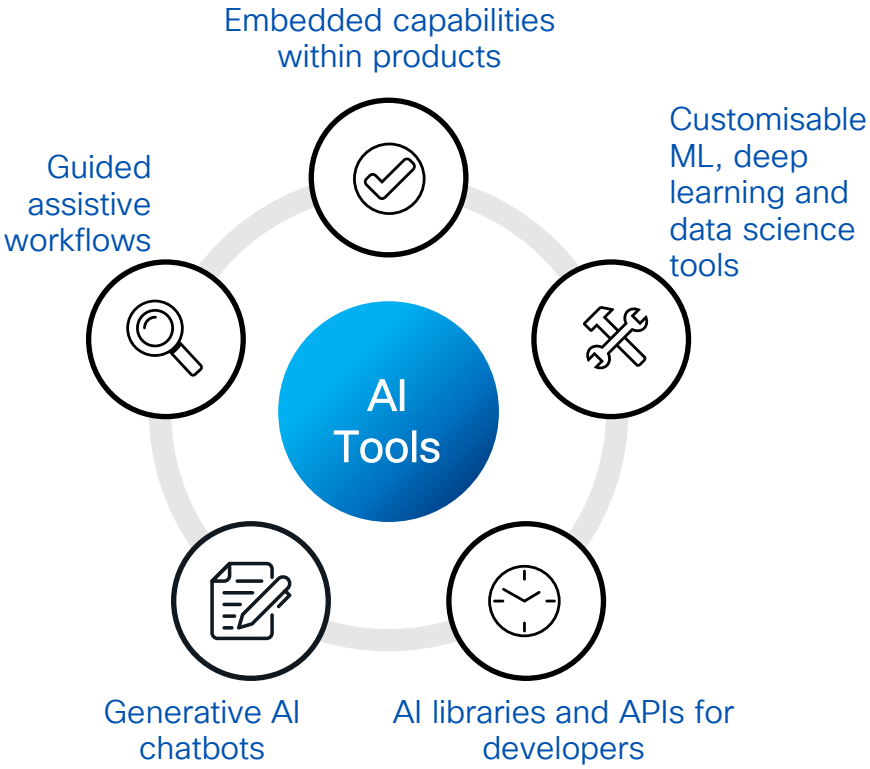
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

The Next ~~10~~ Years Will Be Defined By AI Adoption



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Splunk's Secret AI-Super Power is Data!



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Our AI Product Philosophy

Domain Specific	Human in the Loop	Open and Extensible
Focused on Security and Observability	Human-assisted AI for detection, investigation, and response	Easily integrated with third party frameworks

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

How can Splunk help you in your AI journey?

Building AI Models

Help build AI models on the highest data quality

Securing and monitoring AI

Monitor and secure AI data, infrastructure and and governance

Leveraging AI in Splunk

Improve security and observability outcomes with AI

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Where are we investing?

Accelerate detection, investigation and response

Sense Making

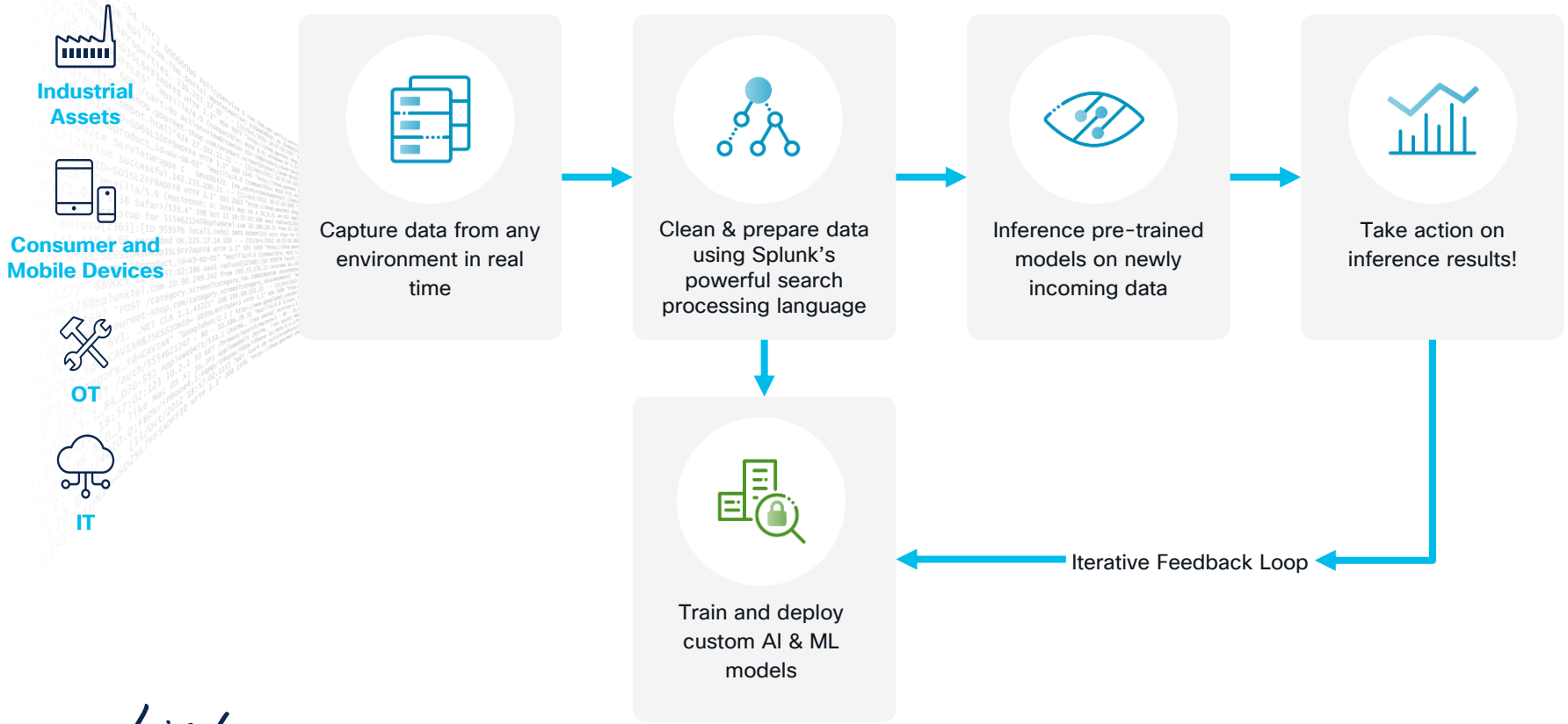
Make sense of the signal to improve user productivity and outcomes.

Finding Signals

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

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Splunk's Customizable AI & ML Pipeline

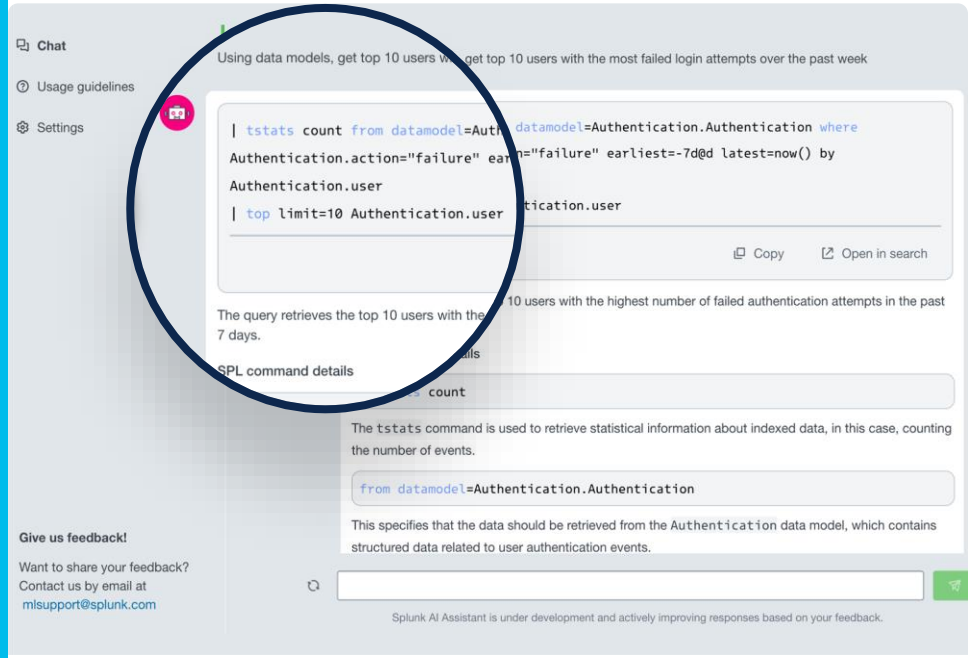


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

New AI Assistant for SPL

Preview in Q1 & GA in Q2

- Upskill new and advanced Splunk users quickly.
- Translate bi-directionally between NL and SPL.

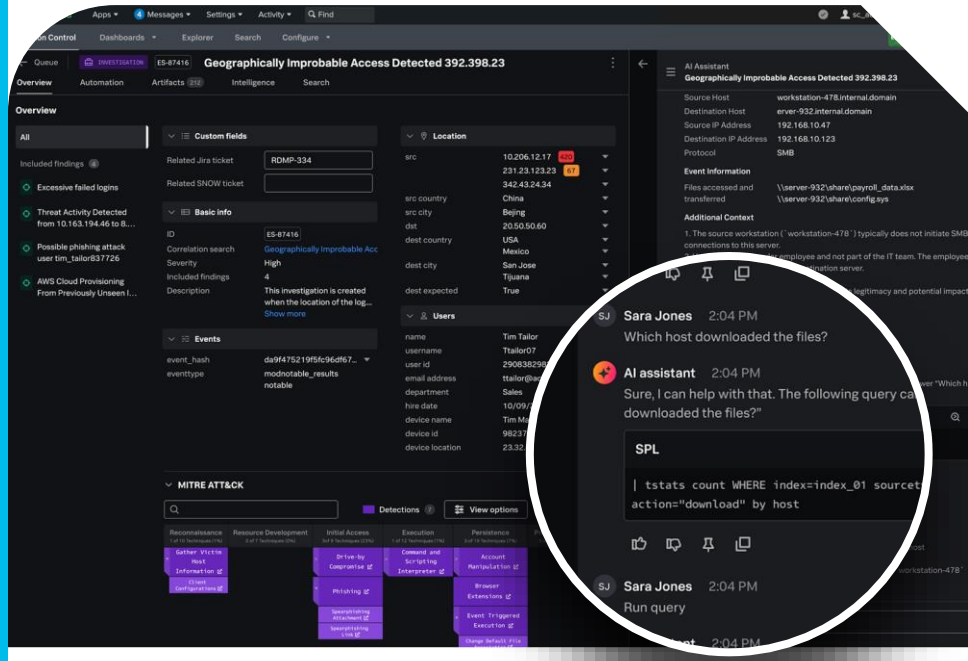


© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

New AI Assistant in Enterprise Security

Coming Soon

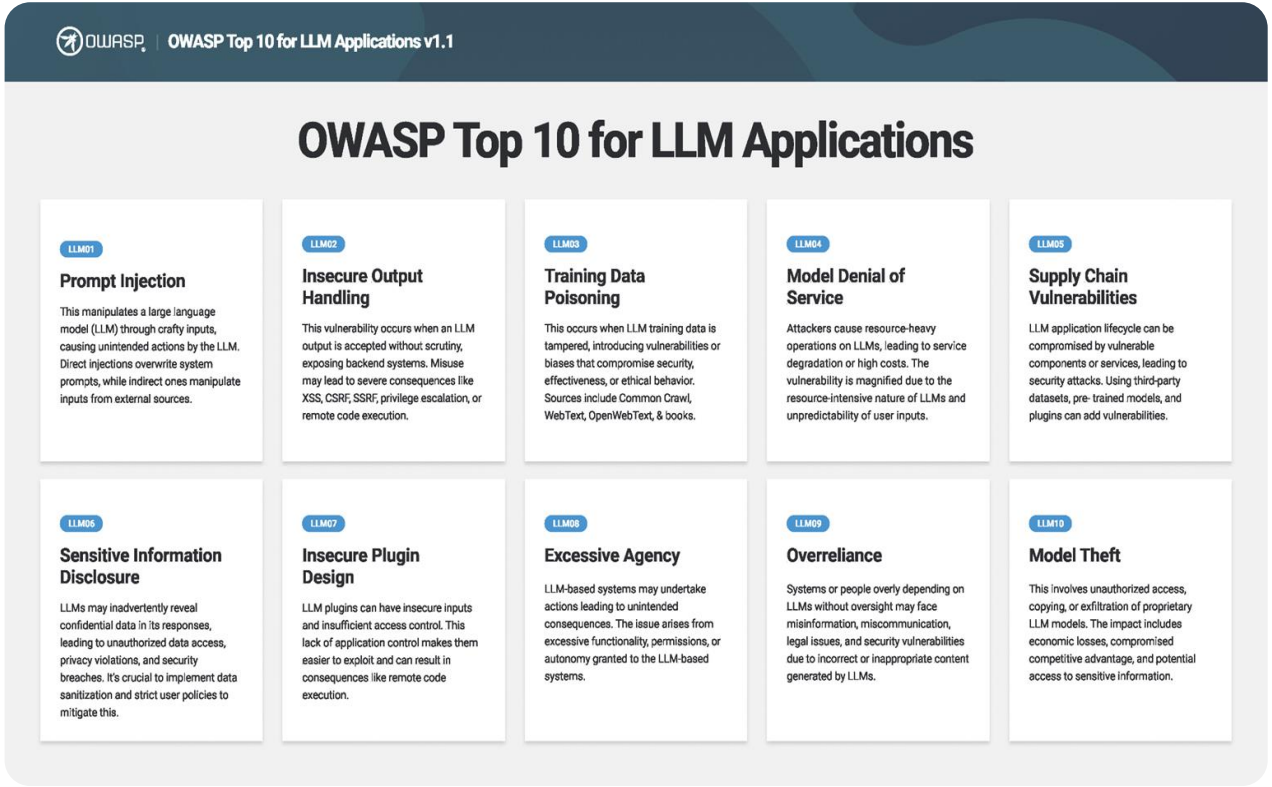
- Investigate faster.
- Answer analyst questions to speed up daily workflows.
- Save time while addressing threats more rapidly.
- Access natively within Splunk ES.



© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

SURGe by Splunk

SEC1928 – SURGe Minicon: LLM Lifeguard: Protecting LLMs Using Splunk and the OWASP Top 10 for LLM Applications



cisco Live!

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Cisco + Splunk
Power and protect the AI revolution

Infrastructure for AI

Networking and compute solutions for training AI models at scale

Data for AI

Massive breadth and depth of data across domains is the foundation for AI models

Observability for AI

Observability supports trustworthy, performant, and reliable AI deployment

AI for Security

AI solutions improve efficiency, efficacy, and economics of defending against security threats

Security for AI

Cisco's Identity Intelligence and User Protection and Splunk's analytics help protect enterprises in their use of AI from within

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

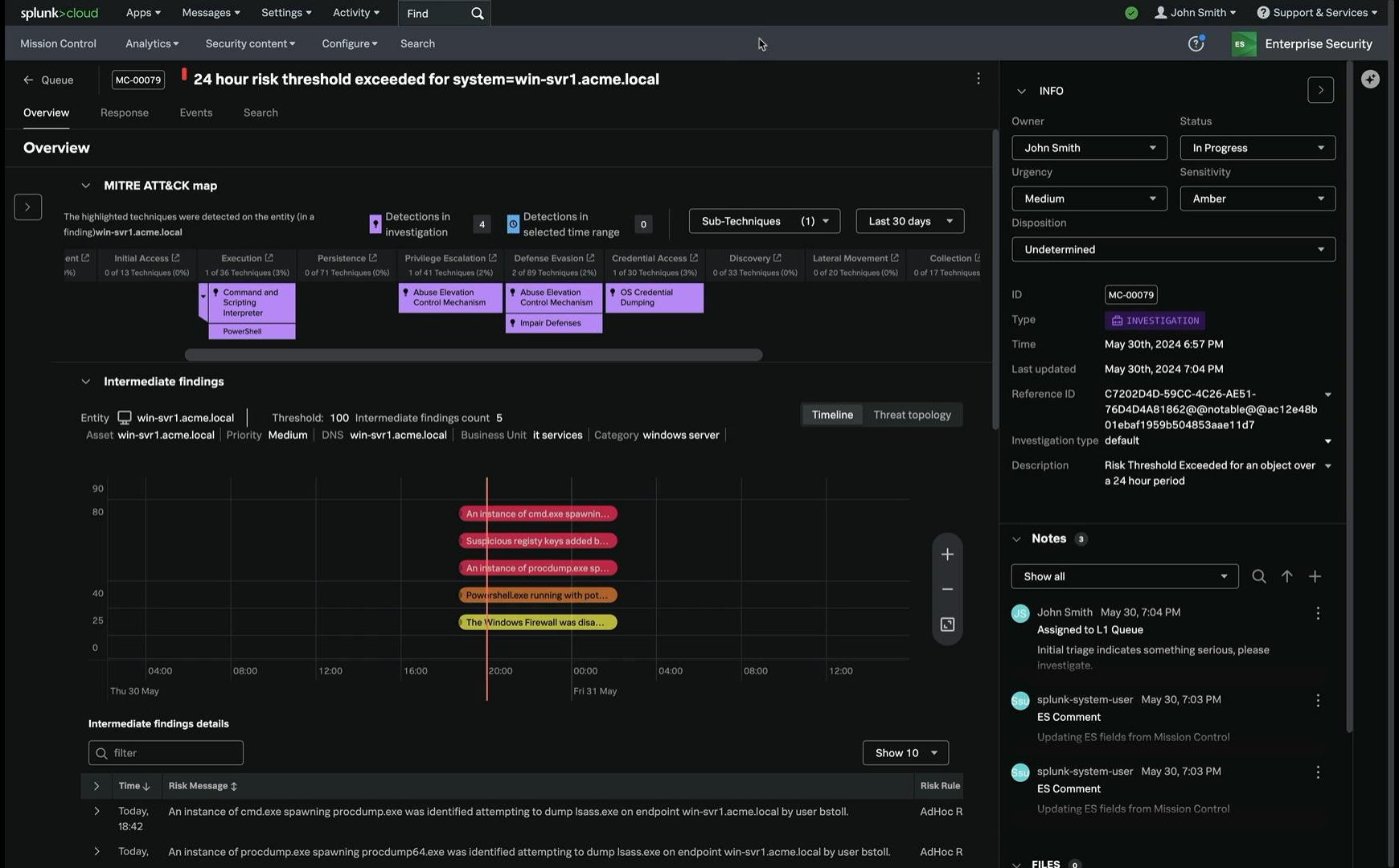
What's next for security assistive AI @ Splunk

- Continue to augment the analyst experience
  - Incident Prioritization
  - Incident Response
  - Automation Guidance
  - Guided → Assisted
  - Prompts → Functions
- Empower the security engineer
  - Detection engineering support
  - Automation engineering support

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

Demo – AI Assistant in Splunk Enterprise Security

cisco Live!


splunk>cloud
Apps
Messages
Settings
Activity
Find
John Smith
Support & Services
Mission Control
Analytics
Security content
Configure
Search
Enterprise Security
Queue
MC-00079
24 hour risk threshold exceeded for system=win-svr1.acme.local
Overview
Response
Events
Search
Overview
MITRE ATT&CK map
The highlighted techniques were detected on the entity (in a finding)win-svr1.acme.local
Detections in investigation 4
Detections in selected time range 0
Sub-Techniques (1)
Last 30 days
Initial Access 0 of 13 Techniques (0%)
Execution 1 of 36 Techniques (3%)
Persistence 0 of 71 Techniques (0%)
Privilege Escalation 1 of 41 Techniques (2%)
Defense Evasion 2 of 89 Techniques (2%)
Credential Access 1 of 30 Techniques (3%)
Discovery 0 of 33 Techniques (0%)
Lateral Movement 0 of 20 Techniques (0%)
Collection 0 of 17 Techniques
Command and Scripting Interpreter
PowerShell
Abuse Elevation Control Mechanism
Abuse Elevation Control Mechanism
Impair Defenses
OS Credential Dumping
Intermediate findings
Entity win-svr1.acme.local
Threshold: 100 Intermediate findings count 5
Asset win-svr1.acme.local
Priority Medium
DNS win-svr1.acme.local
Business Unit it services
Category windows server
Timeline
Threat topology
An instance of cmd.exe spawnin...
Suspicious registy keys added b...
An instance of procdump.exe sp...
Powershell.exe running with pot...
The Windows Firewall was disa...
Thu 30 May
Fri 31 May
Intermediate findings details
filter
Show 10
Time
Risk Message
Risk Rule
Today, 18:42
An instance of cmd.exe spawning procdump.exe was identified attempting to dump lsass.exe on endpoint win-svr1.acme.local by user bstoll.
AdHoc R
Today,
An instance of procdump.exe spawning procdump64.exe was identified attempting to dump lsass.exe on endpoint win-svr1.acme.local by user bstoll.
AdHoc R
INFO
Owner
John Smith
Status
In Progress
Urgency
Medium
Sensitivity
Amber
Disposition
Undetermined
ID
MC-00079
Type
INVESTIGATION
Time
May 30th, 2024 6:57 PM
Last updated
May 30th, 2024 7:04 PM
Reference ID
C7202D4D-59CC-4C26-AE51-76D4D4A81862@@notable@@ac12e48b01ebaf1959b504853aae11d7
Investigation type
default
Description
Risk Threshold Exceeded for an object over a 24 hour period
Notes
Show all
John Smith May 30, 7:04 PM
Assigned to L1 Queue
Initial triage indicates something serious, please investigate.
splunk-system-user May 30, 7:03 PM
ES Comment
Updating ES fields from Mission Control
splunk-system-user May 30, 7:03 PM
ES Comment
Updating ES fields from Mission Control
FILES

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**.

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

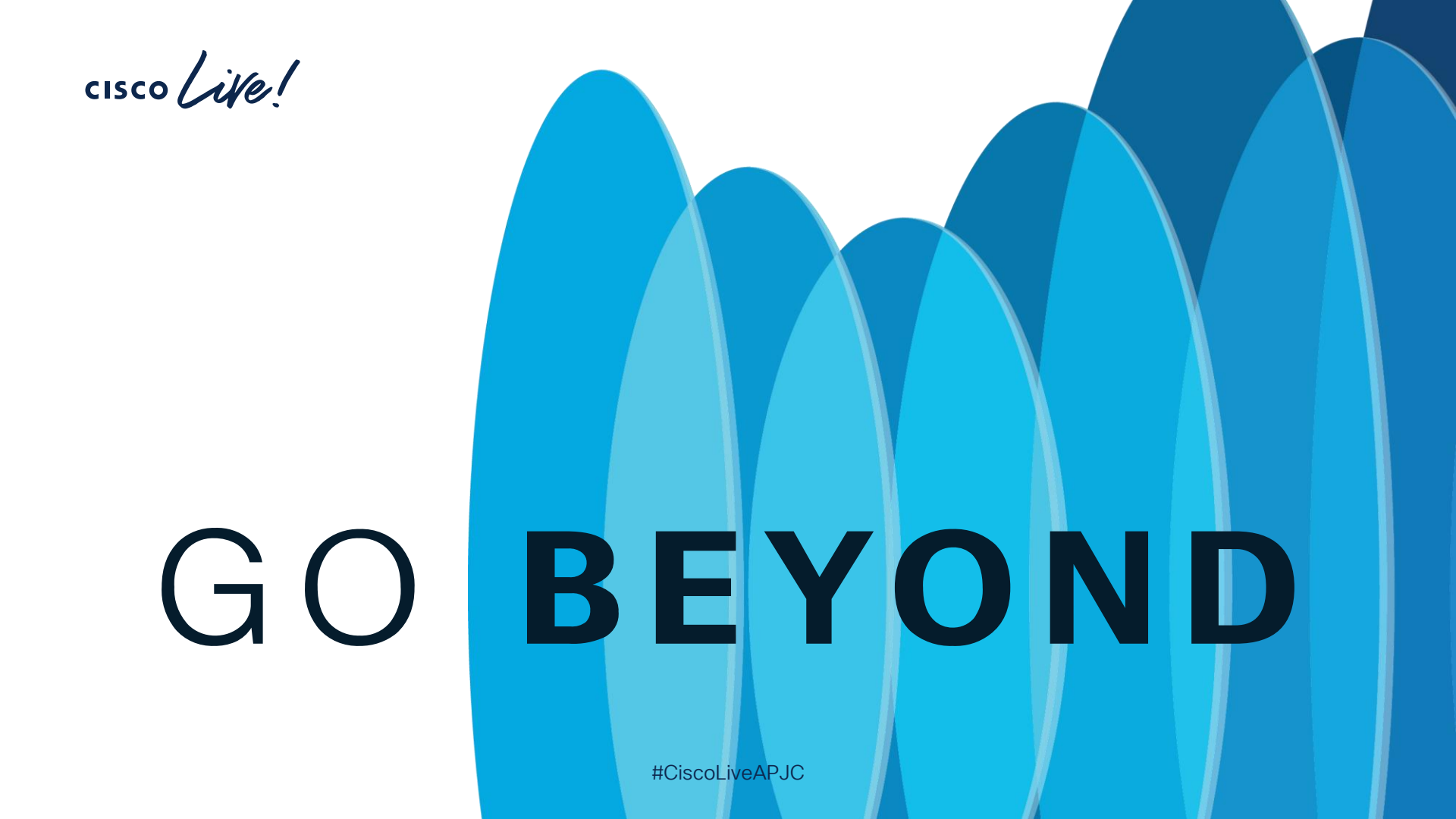
Continue your education

- 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

Contact me at: jkripalani@splunk.com

© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

cisco
Thank you
cisco Live!
#CiscoLiveAPJC


cisco Live!
GO BEYOND
#CiscoLiveAPJC