

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



Cisco XDR Automation

Getting started with workflows and atomics

Matt Vander Horst
Leader, Technical Content
DEVWKS-1190

CISCO *Live!*

#CiscoLiveAPJC



Cisco Webex App

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.



<https://ciscolive.ciscoevents.com/ciscolivebot/#DEVWKS-1190>



Matt Vander Horst

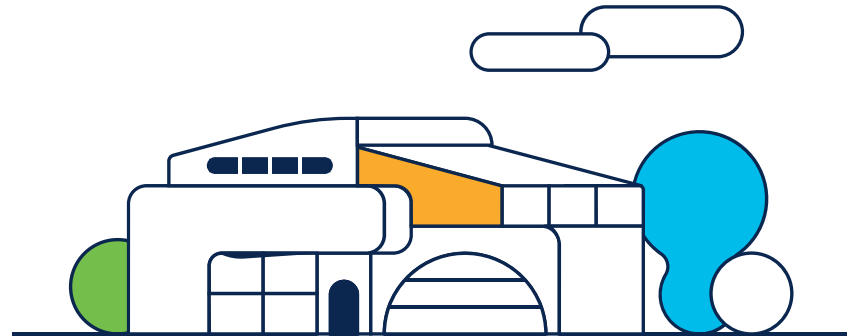
- 8 years at a Fortune 100 insurance company
 - Network engineering
 - Cisco ISE
 - Software/DevOps
- 4.5 years at Cisco
 - SecureX → XDR
 - Integrations and automation
- VP of Spoiling

cisco *Live!*



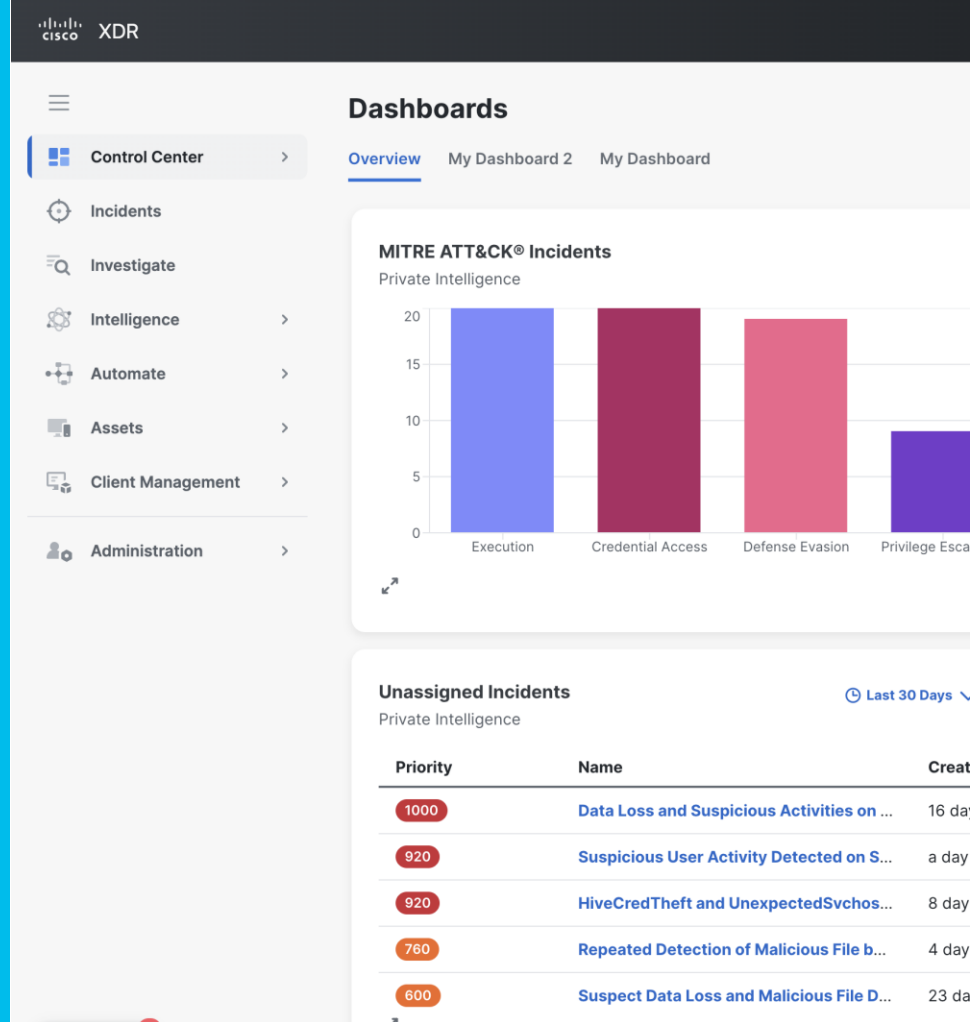
Agenda

- Introduction
- Workshop
- Resources



What is Cisco XDR?

- Extended detection and response
- Integrates with both Cisco and third-party products
- Various features including: control center, incidents, investigate, automate, assets, and more

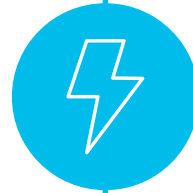


Automation outcomes



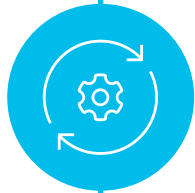
Investigate

Reduce time to investigate by automating data collection and incident generation



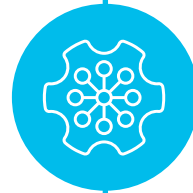
Respond

Automated or one-click responses that can combine multiple products in one action



Simplify

Eliminate repetitive tasks that waste valuable analyst time



Integrate

Bring products and services together in new ways to address emerging threats

Cisco Meraki - MX - L3 Outbound Firewall Block

Last Modified: November 22, 2023 at 11:38:50 AM

Validated

Commit

View Runs

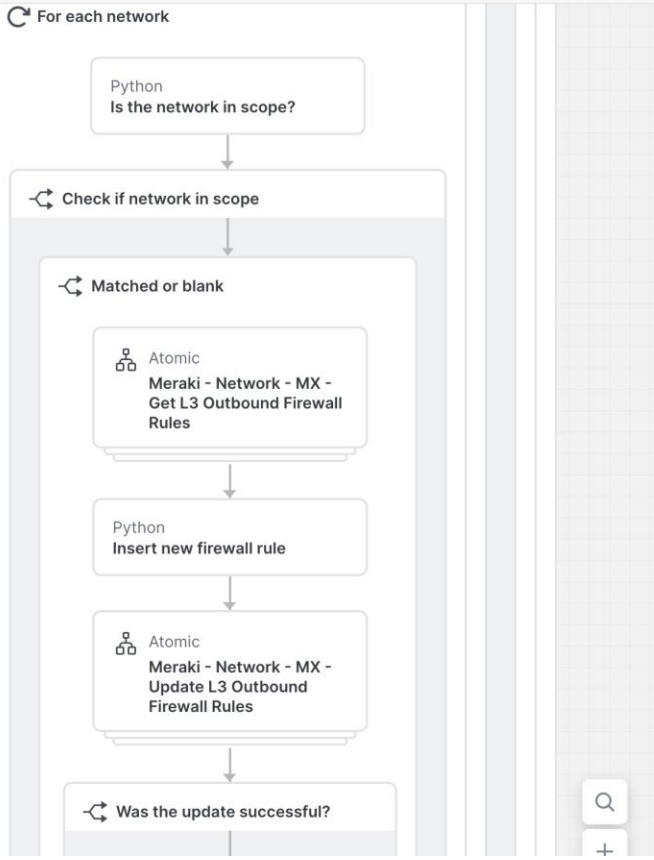
Run

Settings

Search activities

Activities Logic Workflows

- Core
- AWS Service
- Ansible Tower
- Cisco API Console
- Cisco Defense Orchestrator
- Cisco Duo Security
- Cisco ISE
- Cisco Meraki
- Cisco Orbital
- Cisco PSIRT OpenVuln
- Cisco Secure Cloud Analytics
- Cisco Secure Email
- Cisco Secure Endpoint



Workflow Properties

Cisco Meraki - MX - L3 Outbound Firewall Block

Version

Git Repository

Select

Git Version

No Versions Available

General

Display Name*

46 / 64

Cisco Meraki - MX - L3 Outbound Firewall Block

Owner

user@cisco.com

Description

536 / 1024

This workflow appears in the pivot menu and allows a user to block an IP address on a Cisco Meraki MX L3 outbound firewall (using the input observable as the rule's destination). Supported observables: ip, ipv6

Target: Meraki

☐ Clean up after successful execution

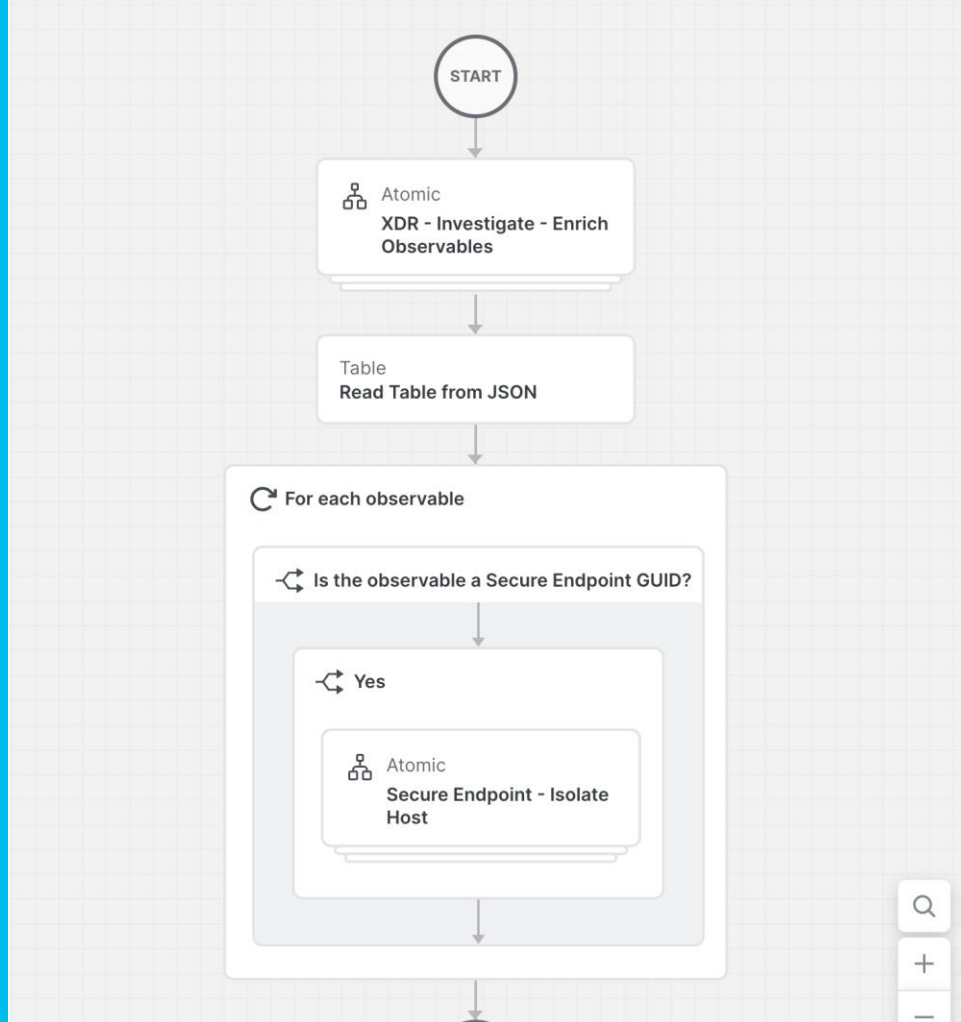
If checked, the workflow run and any underlying task(s) will be deleted when the run succeeds. Failed runs will not be deleted.

☐ Is atomic workflow ⓘ

An atomic workflow will be listed under the Activity Group header you select or create in the list to the

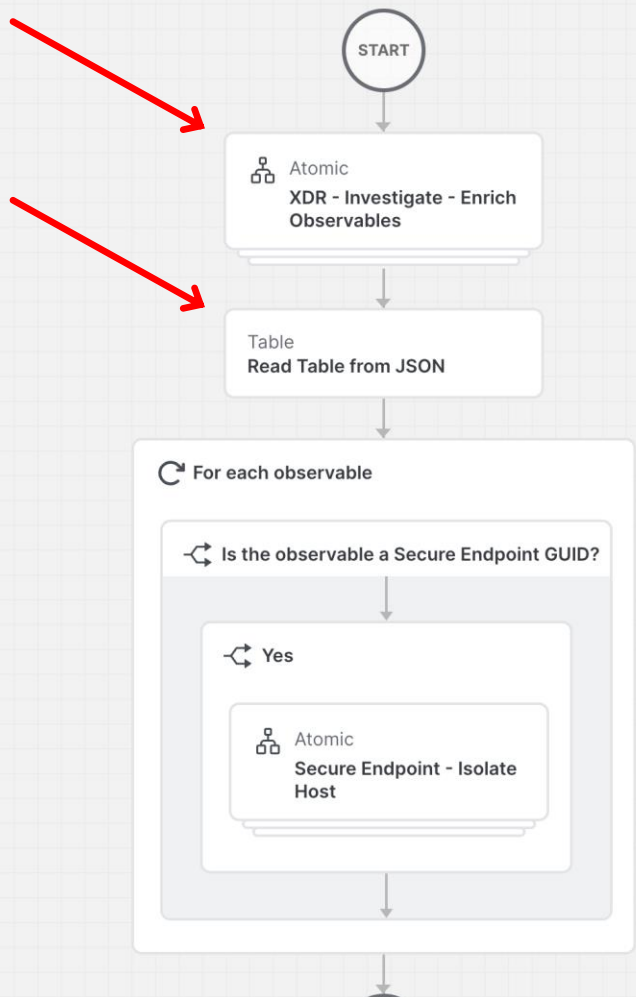
Workflows

- A simple or complex series of activities that accomplish a task or series of tasks
- Built using the drag and drop workflow editor
 - Activities toolbox (left)
 - Canvas (middle)
 - Properties editor (right)



Activities

- A single step in a workflow
- Generally, come in two forms:
 - Adapters
 - Atomic actions
- Adapters: Pre-compiled and part of the platform (cannot be managed by the customer)
- Atomic actions: next slide....



Targets

- The “things” you want your workflows to be able to communicate with
- Can leverage Account Keys for authentication
- Come in many different types:
 - HTTP Endpoint
 - SMTP Endpoint
 - And so on...

CISCO *Live!*

← Targets

New Target

Target Type

- HTTP Endpoint ✓
- AWS Endpoint
- Ansible Tower Endpoint
- Git Endpoint
- Git Repository
- Google Cloud Platform Endpoint
- IMAP Endpoint
- JDBC Database Server
- Meraki Endpoint
- Microsoft Graph Endpoint

General

Systems and resources you want your workflows to be able to communicate with.

Account Keys

Use an account key if the target requires authentication.

No Account Keys ⓘ

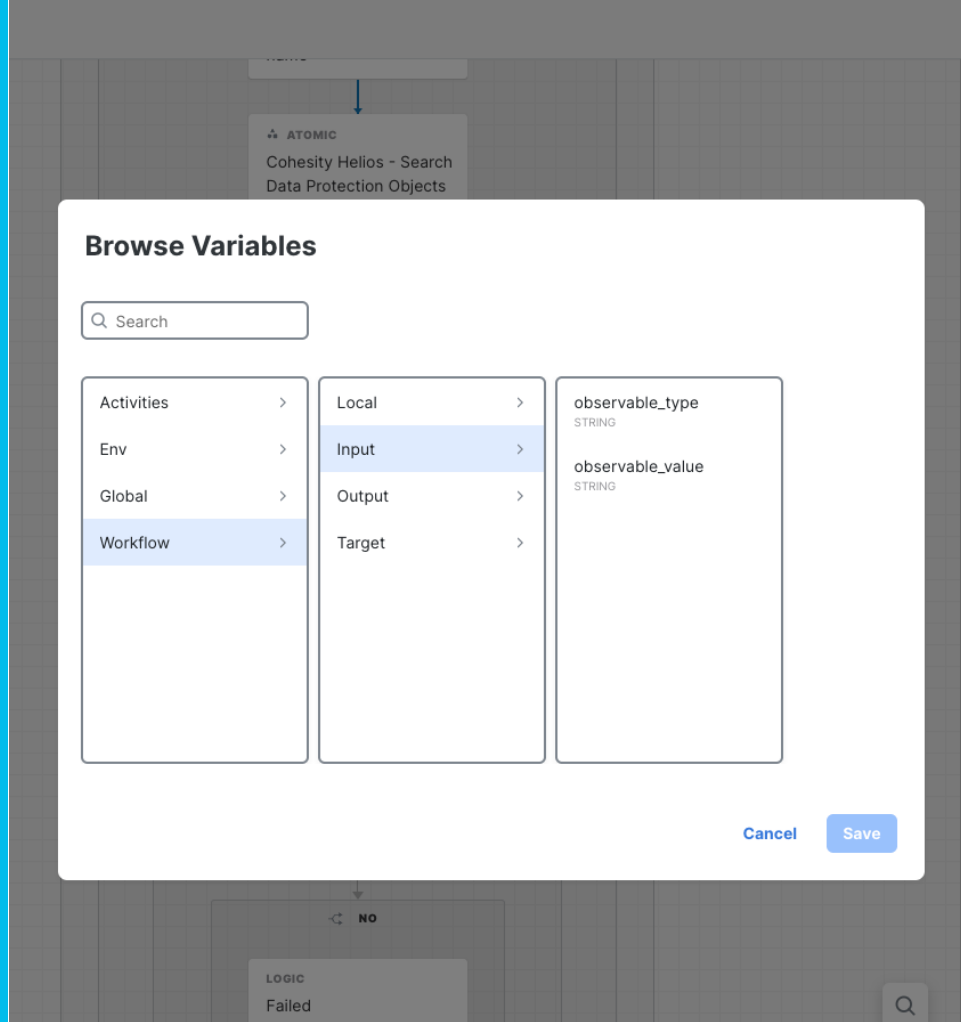
Default Account Keys

Remote

Remote Keys

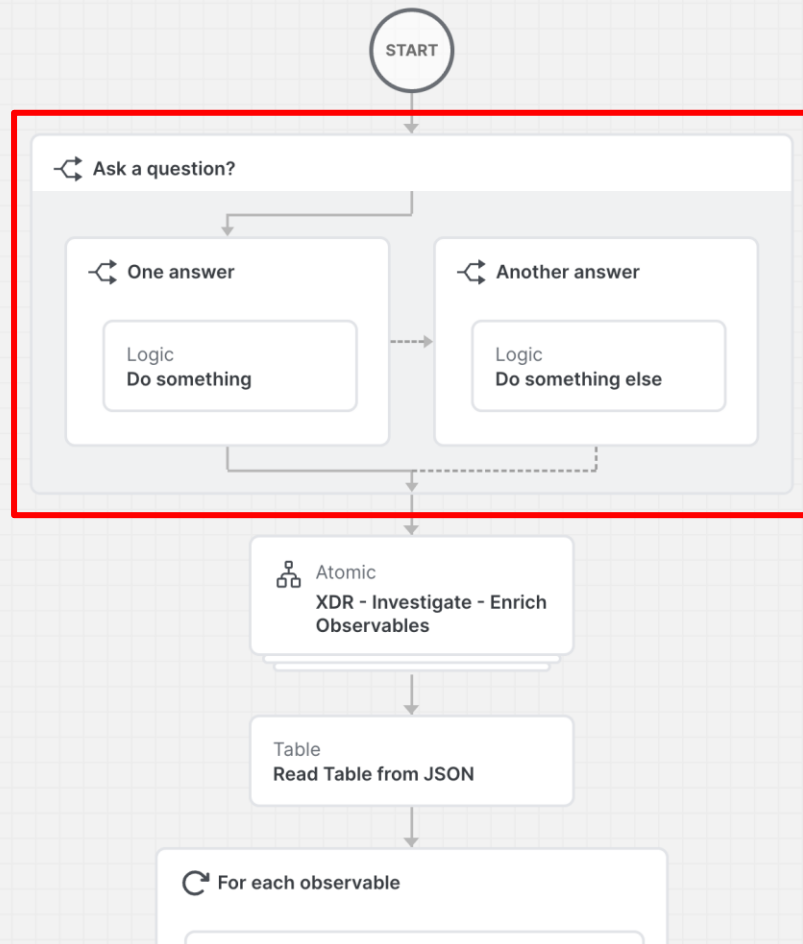
Variables

- Can be defined within workflows or at a global level
- Used to store and pass information within or between workflows
- Come in different types for different types of data
 - Strings, Integers, Booleans, etc.

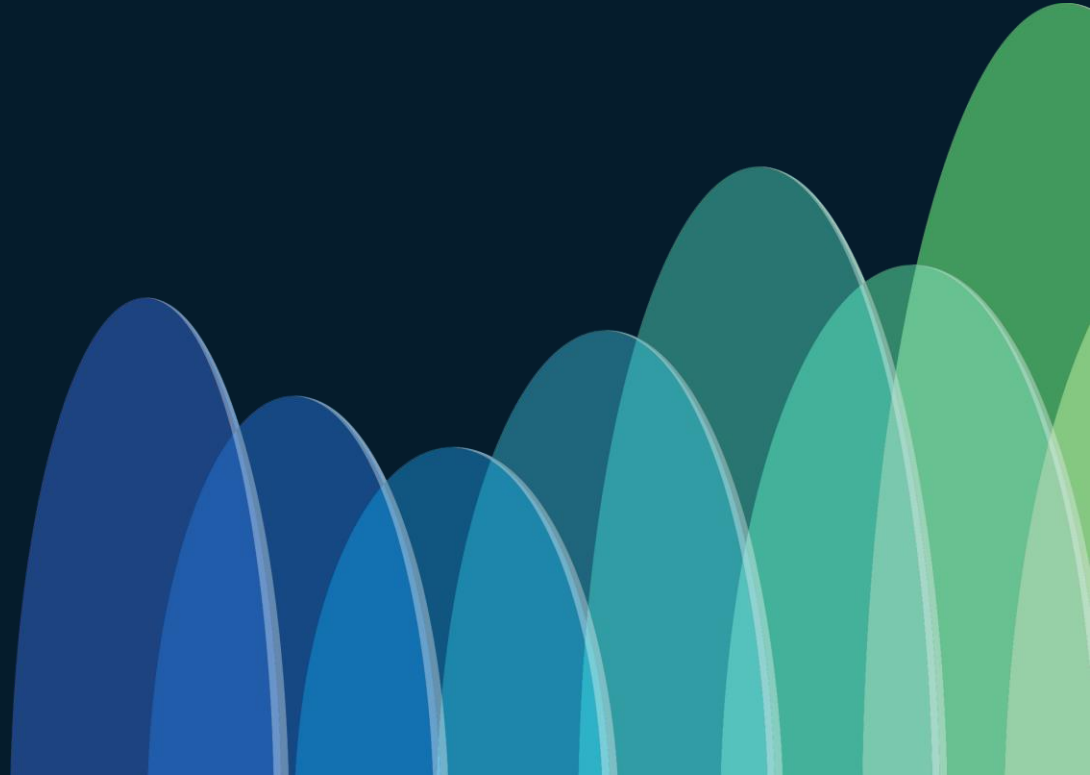


Condition blocks

- Allow workflows to ask a question and take a different path based on the answer
 - Like an “if...else” in traditional scripting
- Can be complex or combine multiple questions with “ands” or “ors”
 - Can have one, two, or more branches



Workshop



Workshop tasks

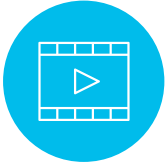
- Create a workflow to find endpoints in Cisco Secure Endpoint by their IP address
- Convert that workflow into an atomic action
- Use our new atomic in a second workflow (to find an endpoint and isolate it)
- Add the second workflow to the XDR pivot menu (time permitting)

Lab environment

<https://cs.co/cl24mel-xdr>

<https://cs.co/xdr-automation-lab>

XDR automation resources



Videos

<https://cs.co/xdr-automation-videos>



Documentation

<https://cs.co/xdr-automation-docs>



DevNet

<https://developer.cisco.com/cisco-xdr>

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

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC