cisco Live!

Let’s go

#CiscoLive

The bridge to possible

Automating Detection & Response Outcomes using Cisco XDR

.. and how CX Automation can help!

Aman Sardana, Scott Dozier
Engineering Architects, Cisco CX Services & Product Portfolio
@amsardana, @ScottDozier_

BRKATO-1557

Cisco Webex App

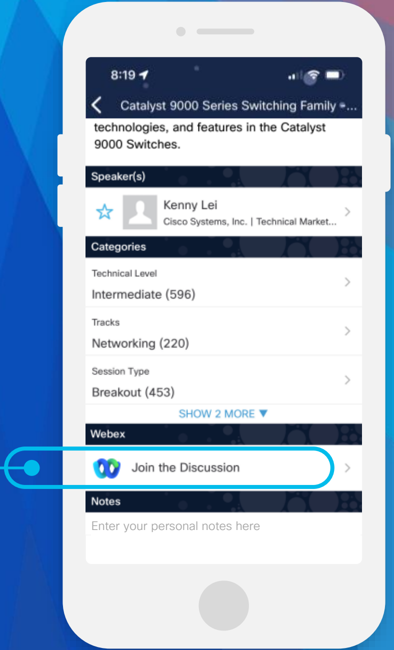
Questions?

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 June 9, 2023.



8:19

Catalyst 9000 Series Switching Family ...

technologies, and features in the Catalyst 9000 Switches.

Speaker(s)

Kenny Lei
Cisco Systems, Inc. | Technical Market...

Categories

Technical Level
Intermediate (596)

Tracks
Networking (220)

Session Type
Breakout (453)

SHOW 2 MORE ▼

Webex

Join the Discussion

Notes

Enter your personal notes here

https://ciscolive.ciscoevents.com/ciscolivebot/#BRKATO-1557

Safe Harbor Statement

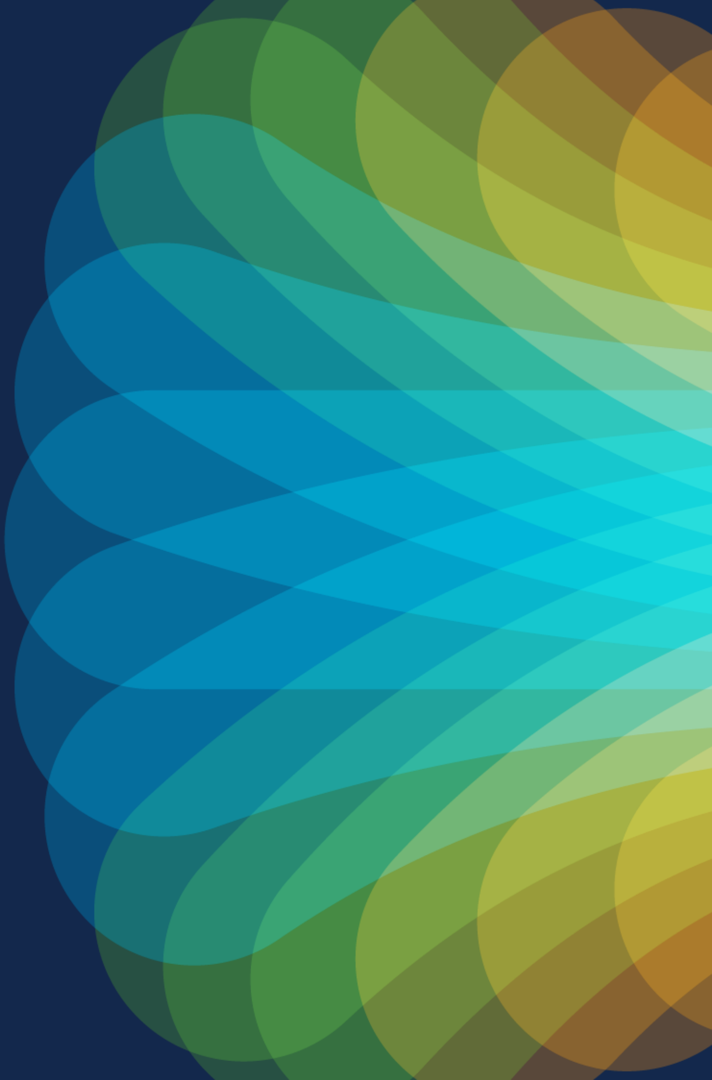
This presentation contains projections and other forward-looking statements regarding future events or the future financial performance of Cisco, including future operating results.

These projections and statements are only predictions. Actual events or results may differ materially from those in the projections or other forward-looking statements.

Agenda

- Introduction to Cisco XDR
- Automating with XDR Automate
  Do it yourself.
- Command & Control Use Case + Demo!
  We'll show you how to.
- Cisco Secure Managed Detection & Response
  We'll do it for you.
- Conclusion

Introduction to Cisco XDR



In a hybrid, multi-vendor, multi-vector universe

Everyone is an insider

+30%

of all incidents involved stolen credentials or malicious insiders

Attacks start from anywhere

45%

of breaches occurred in the cloud, and 19% due to a compromise at a business partner

Alert fatigue is real

37%

of IT and SecOps pros say swelling alert volume, and complexity increases job difficulty

Expanding attack surface

22%

increase in the the average cost of a data breach where hybrid work was a factor

Source: IBM Security and Ponemon Institute 2022 Cost of a Data Breach Study

What is Cisco Extended Detection & Response?

A means to detect more, act faster, elevate productivity, build resilience

Detect the most sophisticated threats

- Multi-vector detection: network, cloud, endpoint, email, and more
- Enriched incidents with asset insights, threat intel
- Optimized for multi-vendor environments

Act on what truly matters, faster

- Prioritize threats by greatest material risk
- Unified context to streamline investigations
- Evidence-backed recommendations

Elevate productivity

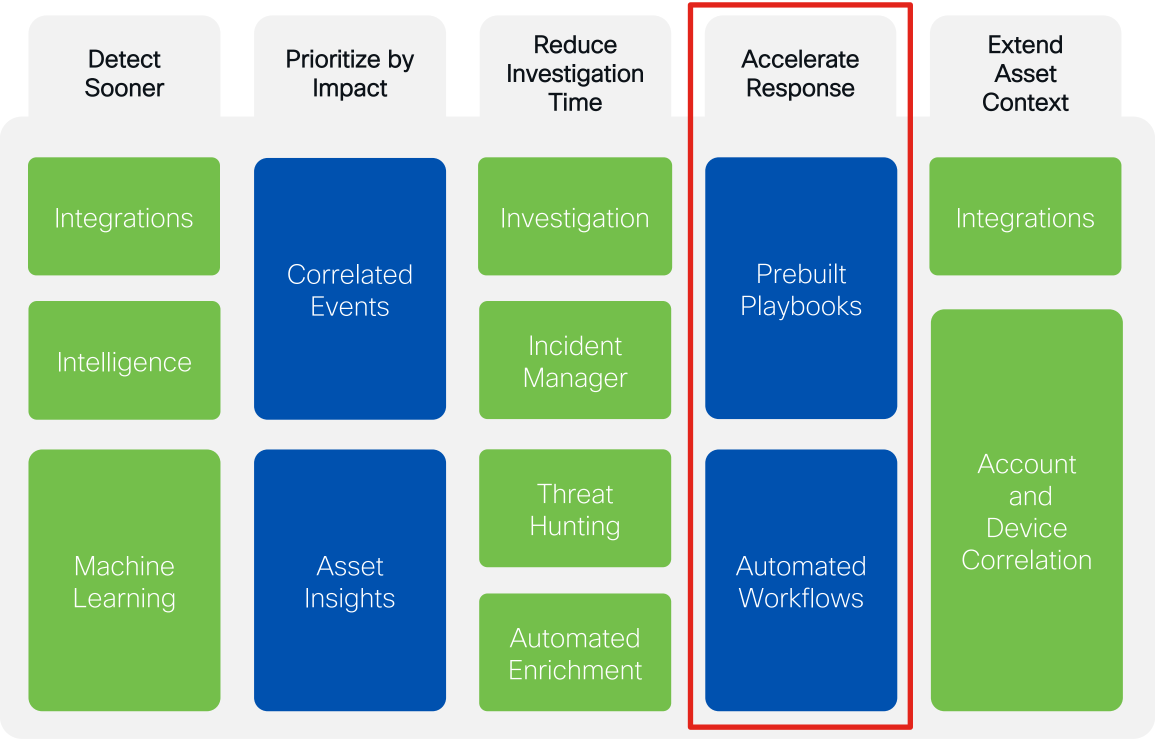
- Focus on what matters and filter out the noise
- Boost limited resources for maximum value
- Automate tasks and focus on, strategic tasks

Build resilience

- Close security gaps
- Anticipate what's next through actionable intel
- Get stronger, everyday with continuous, quantifiable improvement

Learn more about Cisco XDR at Cisco Live: BRKSEC-2113 (June 7), BRKSEC-3116 (June 8)

XDR Outcomes & Components



Detect Sooner
- Integrations
- Intelligence
- Machine Learning

Prioritize by Impact
- Correlated Events
- Asset Insights

Reduce Investigation Time
- Investigation
- Incident Manager
- Threat Hunting
- Automated Enrichment

Accelerate Response
- Prebuilt Playbooks
- Automated Workflows

Extend Asset Context
- Integrations
- Account and Device Correlation

Powerful, flexible automation

Response

Analyst triggers a workflow from within the incident manager or a pivot menu

Automation rules

An incident matches a pre-defined rule and a workflow is triggered

And more...

Workflows triggered by users, APIs, webhooks, schedules, and more

Automating with XDR Automate

Author security response workflows at lightning speed.

What is XDR Automate?

Simplify & streamline common IT tasks

Create no-to-low-code workflows for commons tasks across all IT domains

Create security workflows

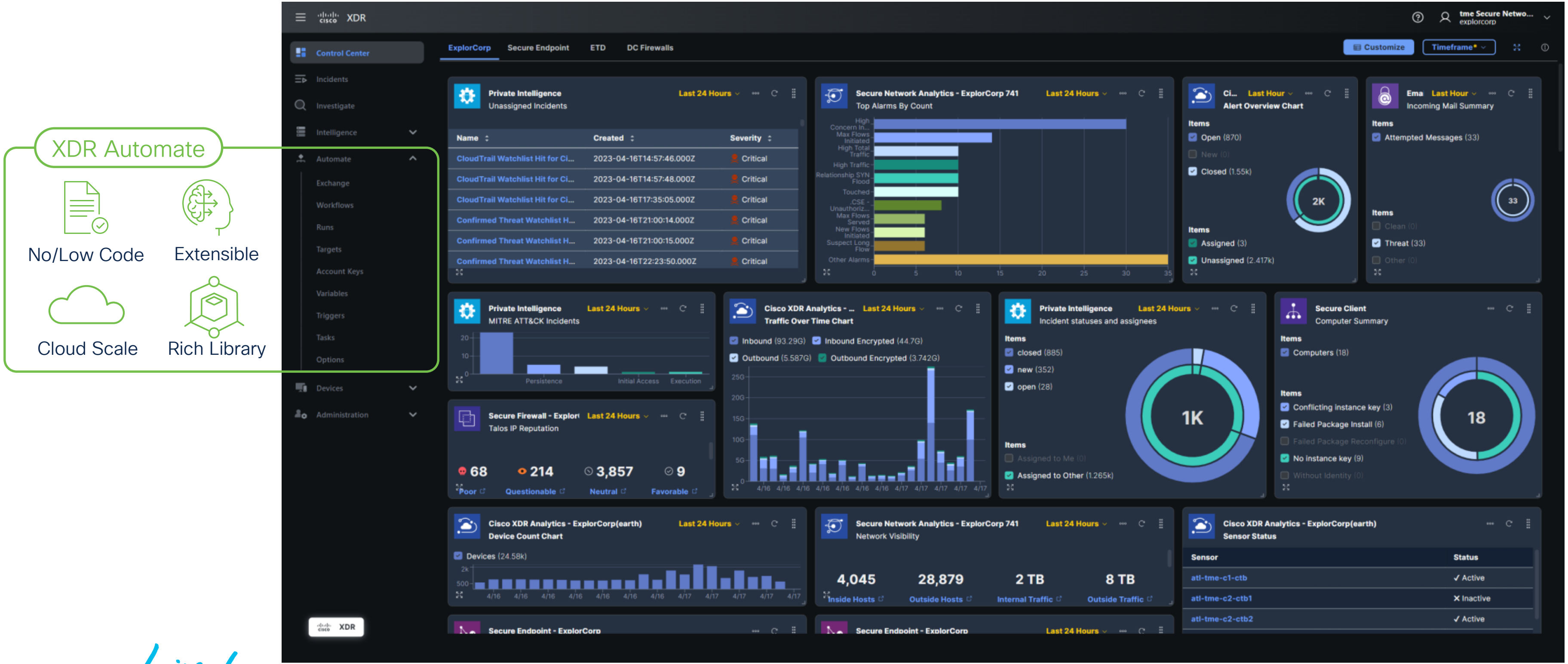
Investigate security events and automate responses using pre-built atomics

Centralize technologies

Orchestrate actions across technologies and vendors to create a cohesive system

What is XDR Automate?

Included with XDR Essentials, Advantage & Premier



XDR Automate

No/Low Code

Extensible

Cloud Scale

Rich Library

Private Intelligence Last 24 Hours
Unassigned Incidents

Name	Created	Severity
CloudTrail Watchlist Hit for Ci...	2023-04-16T14:57:46.000Z	Critical
CloudTrail Watchlist Hit for Ci...	2023-04-16T14:57:48.000Z	Critical
CloudTrail Watchlist Hit for Ci...	2023-04-16T17:35:05.000Z	Critical
Confirmed Threat Watchlist H...	2023-04-16T21:00:14.000Z	Critical
Confirmed Threat Watchlist H...	2023-04-16T21:00:15.000Z	Critical
Confirmed Threat Watchlist H...	2023-04-16T22:23:50.000Z	Critical

Secure Network Analytics - ExplorCorp 741 Last 24 Hours
Top Alarms By Count

Ci... Last Hour
Alert Overview Chart

Items
☑ Open (870)
□ New (0)
☑ Closed (1.55k)

2K

Items
☑ Assigned (3)
☑ Unassigned (2.417k)

Ema Last Hour
Incoming Mail Summary

Items
☑ Attempted Messages (33)

33

Items
□ Clean (0)
☑ Threat (33)
□ Other (0)

Private Intelligence Last 24 Hours
MITRE ATT&CK Incidents

Cisco XDR Analytics - ... Last 24 Hours
Traffic Over Time Chart

☑ Inbound (93.29G) ☑ Inbound Encrypted (44.7G)
☑ Outbound (5.587G) ☑ Outbound Encrypted (3.742G)

Private Intelligence Last 24 Hours
Incident statuses and assignees

Items
☑ closed (885)
☑ new (352)
☑ open (28)

1K

Items
□ Assigned to Me (0)
☑ Assigned to Other (1.265k)

Secure Client
Computer Summary

Items
☑ Computers (18)

18

Items
☑ Conflicting instance key (3)
☑ Failed Package Install (6)
□ Failed Package Reconfigure (0)
☑ No instance key (9)
□ Without Identity (0)

Secure Firewall - Explor! Last 24 Hours
Talos IP Reputation

68	214	3,857	9
Poor	Questionable	Neutral	Favorable

Cisco XDR Analytics - ExplorCorp(earth) Last 24 Hours
Device Count Chart

☑ Devices (24.58k)

Secure Network Analytics - ExplorCorp 741 Last 24 Hours
Network Visibility

4,045	28,879	2 TB	8 TB
Inside Hosts	Outside Hosts	Internal Traffic	Outside Traffic

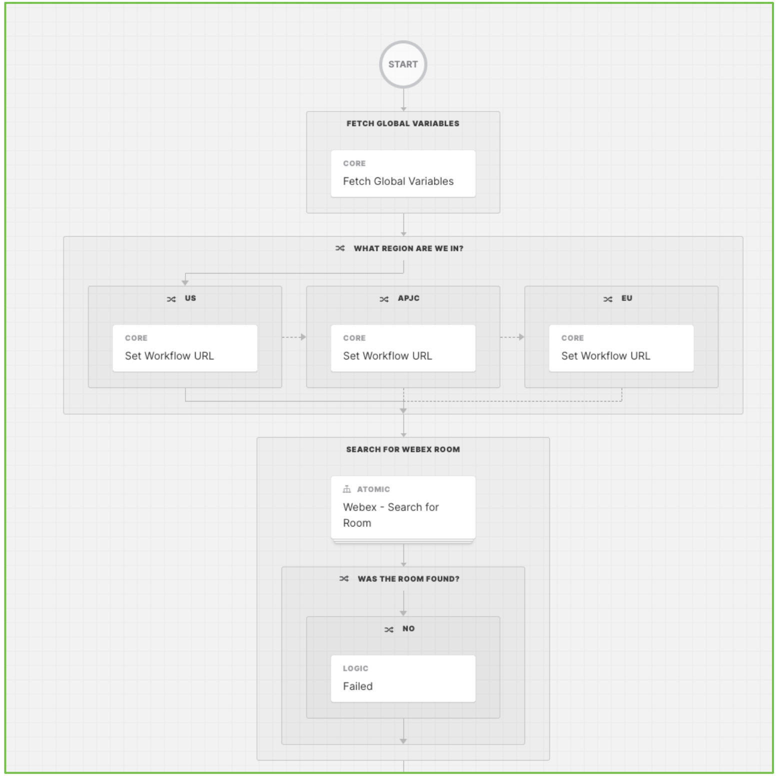
Cisco XDR Analytics - ExplorCorp(earth)
Sensor Status

Sensor	Status
atl-tme-c1-ctb	✓ Active
atl-tme-c2-ctb1	✕ Inactive
atl-tme-c2-ctb2	✓ Active

Secure Endpoint - ExplorCorp

Secure Endpoint - ExplorCorp Last 24 Hours

XDR Automate: Basic Concepts



- Workflow - Sequence of activities
- Activities - Actions such as HTTP requests, JSON parsing, or Python script execution
- Targets - Endpoints to execute an action against
- Variables - References to stored information that is passed between activities
- Account Keys – Otherwise known as credentials and attached to targets
- Triggers - Cause a workflow to execute based on an ‘automation rule’
- Tasks – Allow human interaction (approvals)

XDR Automate: Variables

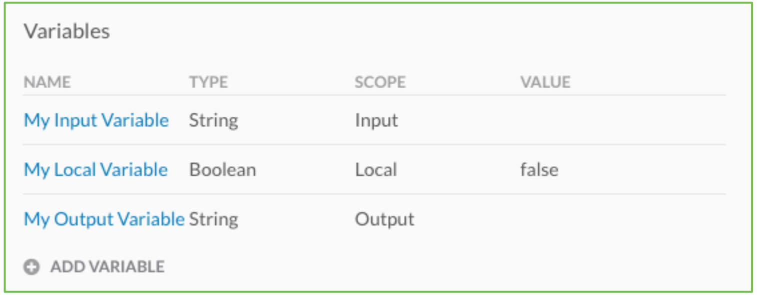
Types

- Boolean
- Date Time
- Decimal
- Integer
- Secure String
- String
- Table
- Custom Types

Scopes

- Global
- Environment
- Workflow
  - Local
  - Input
  - Output
  - Static

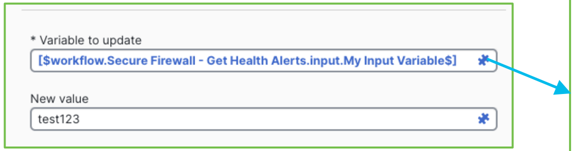
Creation



Variables

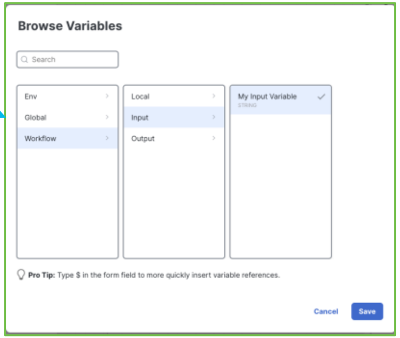
NAME	TYPE	SCOPE	VALUE
My Input Variable	String	Input	
My Local Variable	Boolean	Local	false
My Output Variable	String	Output	

Usage



* Variable to update: [$workflow.Secure Firewall - Get Health Alerts.input.My Input Variable$]

New value: test123



Browse Variables

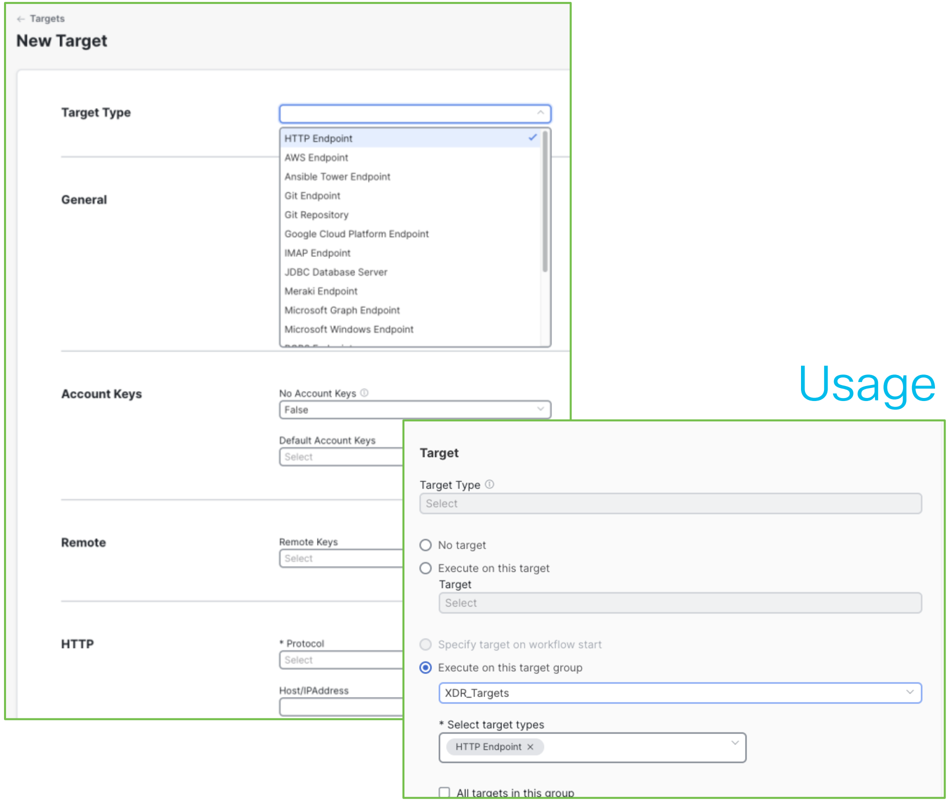
Pro Tip: Type $ in the form field to more quickly insert variable references.

XDR Automate: Targets

- Targets are the endpoints that are assigned to an activity in the workflow so the activity can "target" the communication.
- Targets come in many types including HTTP, AWS, Meraki, Unix/Linux, etc.
- Targets can have an account key associated, but not required.
- Target groups can be configured to provide a collection of targets to a workflow.

Creation

Usage



← 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
- Microsoft Windows Endpoint

General

Account Keys

No Account Keys: False

Default Account Keys: Select

Remote

Remote Keys: Select

HTTP

* Protocol: Select

Host/IPAddress:

Target

Target Type: Select

○ No target

○ Execute on this target

Target: Select

○ Specify target on workflow start

● Execute on this target group

XDR_Targets

* Select target types: HTTP Endpoint ×

□ All targets in this group

XDR Automate: Activities

Activities are the “Action Blocks” that handle all the steps in a workflow. Activities handle things such as HTTP Requests, JSON parsing, or conditional checks.

Core

- Set Variable
- Split String
- JSONPath Query
- Calculate Date
- Find String
- Match Regex
- (more)

Logic

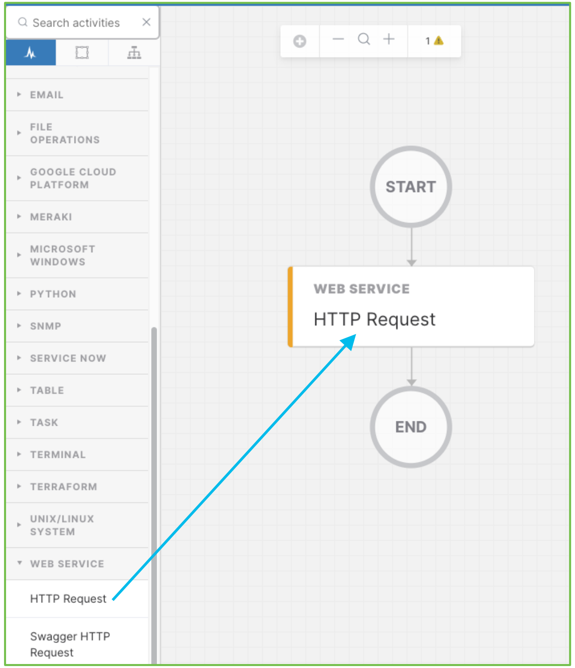
- Condition Block
- For Each
- While Loop
- Break
- Completed
- Group
- Parallel Block
- Continue

Other Categories

- AWS Service
- Cisco ISE
- Ansible Tower
- Database
- Email
- File Operations
- Table
- Unix/Linux

+ more!

Usage

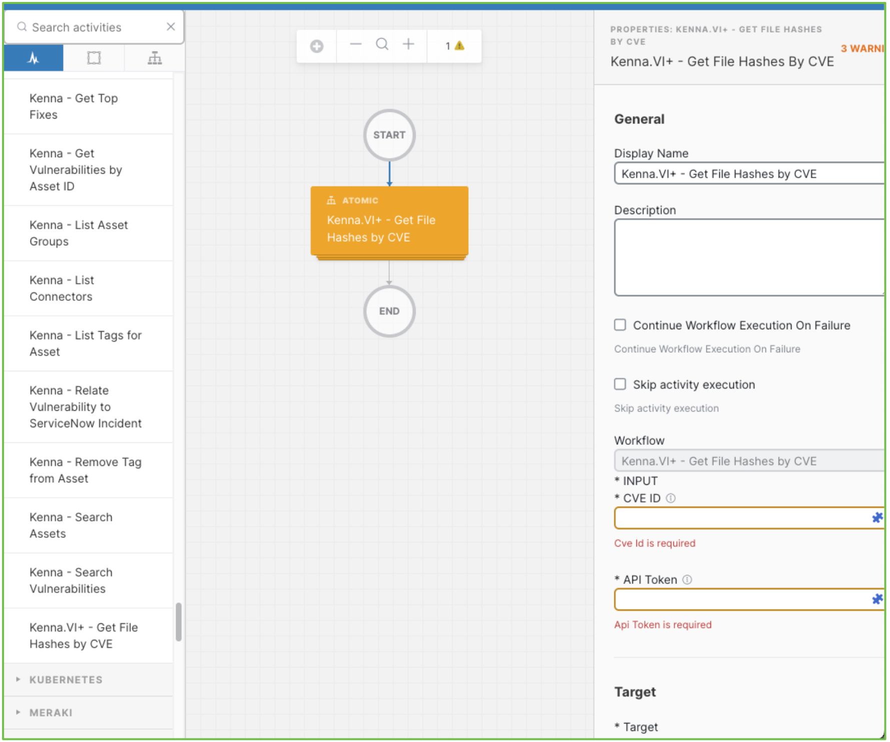


XDR Automate: Atomics

Atomic actions are self-contained workflows similar to a function in traditional programming.

- XDR Automate contains many pre-built atomics, allowing you to interact with many different products such as ThreatQ, Umbrella, ServiceNow, Kenna, Meraki and more.
- Atomics can be added to workflows in the same manner as activities.
- You can turn your own workflows into atomics!

Usage



Kenna - Get Top Fixes
Kenna - Get Vulnerabilities by Asset ID
Kenna - List Asset Groups
Kenna - List Connectors
Kenna - List Tags for Asset
Kenna - Relate Vulnerability to ServiceNow Incident
Kenna - Remove Tag from Asset
Kenna - Search Assets
Kenna - Search Vulnerabilities
Kenna.VI+ - Get File Hashes by CVE

PROPERTIES: KENNA.VI+ - GET FILE HASHES BY CVE

Kenna.VI+ - Get File Hashes By CVE

General

Display Name: Kenna.VI+ - Get File Hashes by CVE

Description

☐ Continue Workflow Execution On Failure
Continue Workflow Execution On Failure

☐ Skip activity execution
Skip activity execution

Workflow: Kenna.VI+ - Get File Hashes by CVE

* INPUT

* CVE ID
Cve Id is required

* API Token
Api Token is required

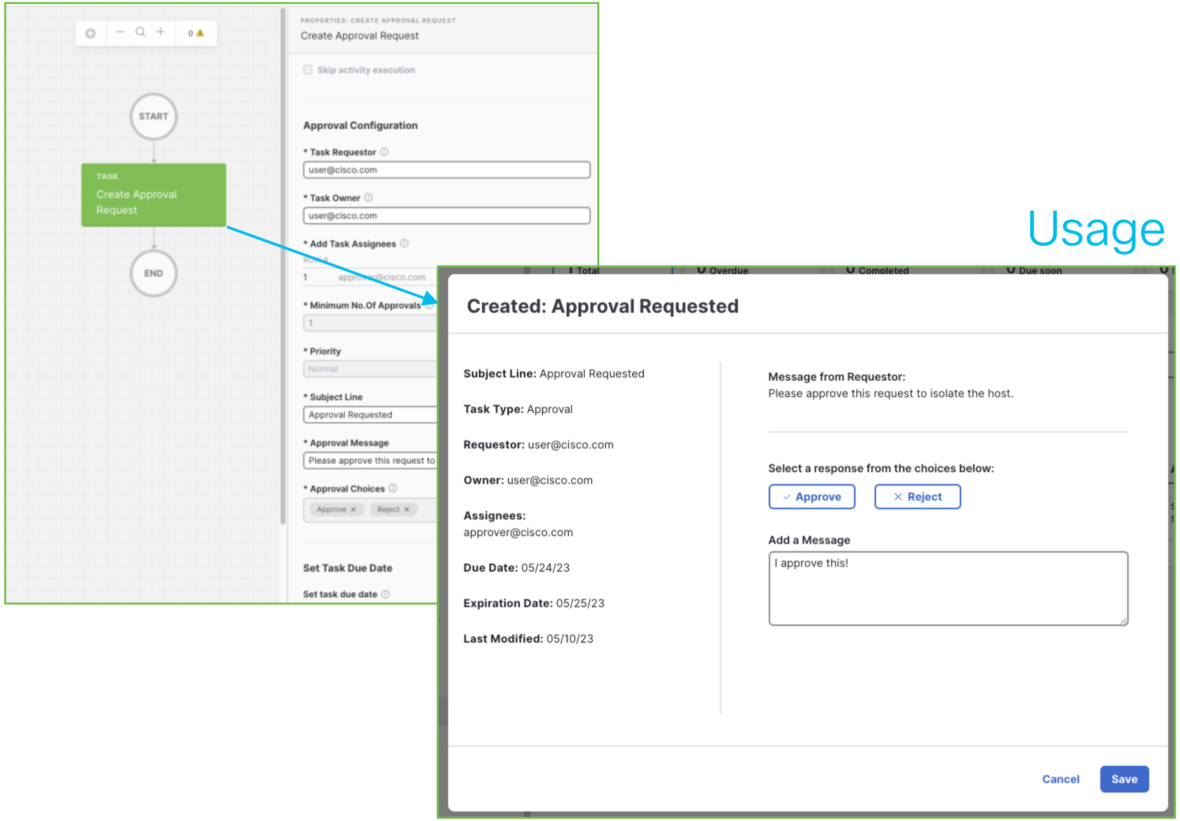
Target

* Target

XDR Automate: Tasks

Tasks allow your workflow to pause and wait for an event (email/incident/webhook) or approval from a human.

Usage



PROPERTIES: CREATE APPROVAL REQUEST

Create Approval Request

□ Skip activity execution

Approval Configuration

* Task Requestor: user@cisco.com

* Task Owner: user@cisco.com

* Add Task Assignees: 1 approver@cisco.com

* Minimum No.Of Approvals: 1

* Priority: Normal

* Subject Line: Approval Requested

* Approval Message: Please approve this request to

* Approval Choices: Approve × Reject ×

Set Task Due Date

Set task due date

Created: Approval Requested

Subject Line: Approval Requested

Task Type: Approval

Requestor: user@cisco.com

Owner: user@cisco.com

Assignees:
approver@cisco.com

Due Date: 05/24/23

Expiration Date: 05/25/23

Last Modified: 05/10/23

Message from Requestor:
Please approve this request to isolate the host.

Select a response from the choices below:

✓ Approve ✕ Reject

Add a Message

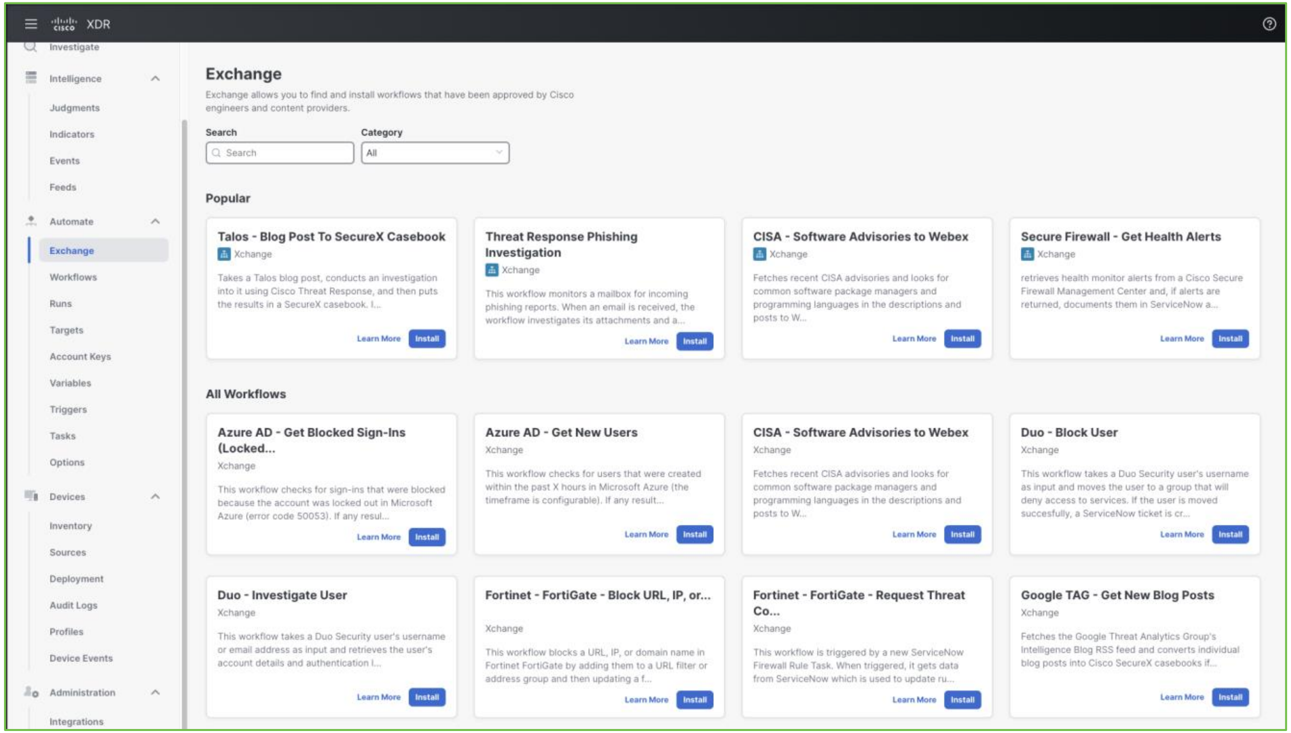
I approve this!

Cancel Save

XDR Automate: Exchange

You don't have to start building workflows from scratch!

Use the Exchange to 1-click install workflows that have been approved by Cisco.



Exchange

Exchange allows you to find and install workflows that have been approved by Cisco engineers and content providers.

Search: Search

Category: All

Popular

Talos - Blog Post To SecureX Casebook
Xchange
Takes a Talos blog post, conducts an investigation into it using Cisco Threat Response, and then puts the results in a SecureX casebook. I...
Learn More | Install

Threat Response Phishing Investigation
Xchange
This workflow monitors a mailbox for incoming phishing reports. When an email is received, the workflow investigates its attachments and a...
Learn More | Install

CISA - Software Advisories to Webex
Xchange
Fetches recent CISA advisories and looks for common software package managers and programming languages in the descriptions and posts to W...
Learn More | Install

Secure Firewall - Get Health Alerts
Xchange
retrieves health monitor alerts from a Cisco Secure Firewall Management Center and, if alerts are returned, documents them in ServiceNow a...
Learn More | Install

All Workflows

Azure AD - Get Blocked Sign-Ins (Locked...
Xchange
This workflow checks for sign-ins that were blocked because the account was locked out in Microsoft Azure (error code 50053). If any resul...
Learn More | Install

Azure AD - Get New Users
Xchange
This workflow checks for users that were created within the past X hours in Microsoft Azure (the timeframe is configurable). If any result...
Learn More | Install

CISA - Software Advisories to Webex
Xchange
Fetches recent CISA advisories and looks for common software package managers and programming languages in the descriptions and posts to W...
Learn More | Install

Duo - Block User
Xchange
This workflow takes a Duo Security user's username as input and moves the user to a group that will deny access to services. If the user is moved succesfully, a ServiceNow ticket is cr...
Learn More | Install

Duo - Investigate User
Xchange
This workflow takes a Duo Security user's username or email address as input and retrieves the user's account details and authentication l...
Learn More | Install

Fortinet - FortiGate - Block URL, IP, or...
Xchange
This workflow blocks a URL, IP, or domain name in Fortinet FortiGate by adding them to a URL filter or address group and then updating a f...
Learn More | Install

Fortinet - FortiGate - Request Threat Co...
Xchange
This workflow is triggered by a new ServiceNow Firewall Rule Task. When triggered, it gets data from ServiceNow which is used to update ru...
Learn More | Install

Google TAG - Get New Blog Posts
Xchange
Fetches the Google Threat Analytics Group's Intelligence Blog RSS feed and converts individual blog posts into Cisco SecureX casebooks if...
Learn More | Install

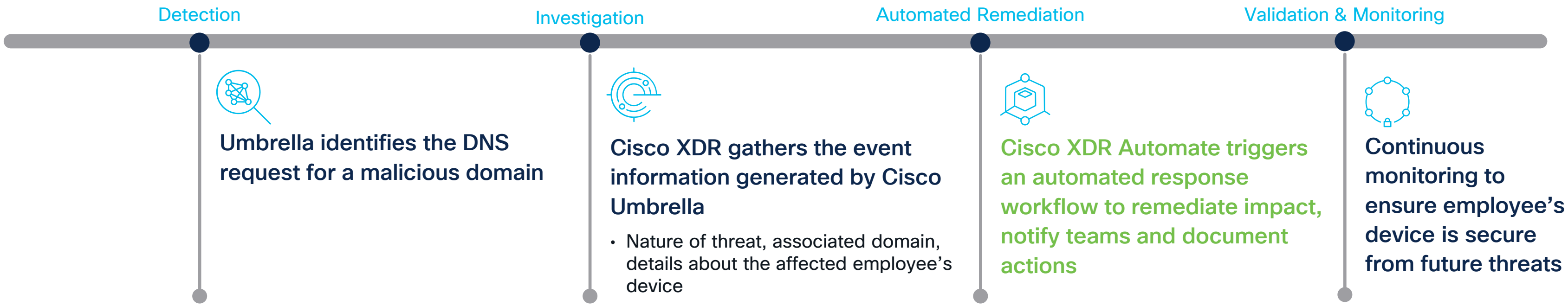
Use Case: Blocking Ransomware Command & Control Callbacks

Using Cisco XDR, Cisco Umbrella & Cisco Secure Endpoint

Scenario

Your organization has several remote employees who are using their personal devices to access sensitive company data.

One of the employee's laptops gets infected with ransomware that attempts to establish command & control communication before initiating data encryption.



Detection

Umbrella identifies the DNS request for a malicious domain

Investigation

Cisco XDR gathers the event information generated by Cisco Umbrella

- Nature of threat, associated domain, details about the affected employee's device

Automated Remediation

Cisco XDR Automate triggers an automated response workflow to remediate impact, notify teams and document actions

Validation & Monitoring

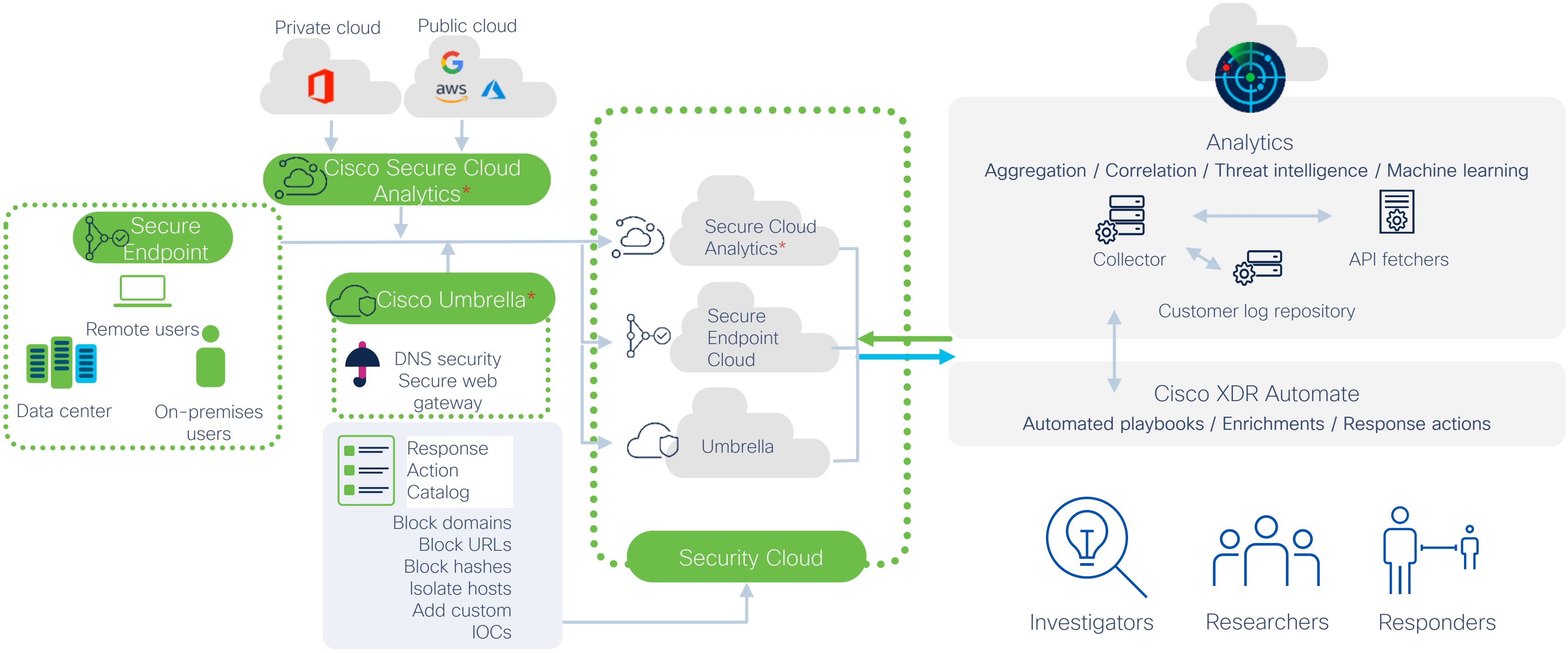
Continuous monitoring to ensure employee's device is secure from future threats

Demo

Cisco Secure Managed Detection & Response (MDR)

We do it for you.

Cisco Secure MDR



Cisco integrated security architecture

Cisco security operations center experts provide monitoring and guidance

*Optional

Conclusion

To summarize..

- To address the threats of tomorrow, we need to change how we look at detection & response today
  - Cisco XDR simplifies security operations, speeds up investigations and accelerates response
  - XDR Automate is a flexible & powerful no-to-low code platform to orchestrate how your organization investigates & responds to threats
- Cisco Managed Detection & Response (MDR) provides the capabilities of Cisco XDR as a managed service with packaged automated response actions
- Cisco CX Automation delivers services as code to help you implement a full DevOps motion across Cisco architectures and solutions

Continue the Conversation with Cisco Customer Experience

VISIT:

1 Visit the **Cisco Customer Experience Booth (#3310)** in the WoS for Lightning Talks, Workshops, and Demos

2 Visit **CX at Cisco Live** website

Credits

Andy Hagar
Security Automation Leader, Cisco CX

Tuan Huynh
Engineering Leader, Cisco CX

Kevin Perkins
Automation Engineer, Cisco CX

Jay Kuhne
Solutions Architect, Cisco CX

Russ Hardison
Sr. Director, Cisco CX

cisco Live!

Questions?

Interact with experts on Webex:
https://ciscolive.ciscoevents.com/ciscolivebot/
#BRKATO-1557

Visit the CX MDR booth at Cisco Live:
SEC-12

View session content on GitHub:
http://cs.co/cl-xdr-automate

Fill out your session surveys!

Attendees who fill out a minimum of four session surveys and the overall event survey will get **Cisco Live-branded socks** (while supplies last)!

Attendees will also earn 100 points in the **Cisco Live Game** for every survey completed.

These points help you get on the leaderboard and increase your chances of winning daily and grand prizes

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

The bridge to possible

Thank you

cisco Live!

Let's go

#CiscoLive

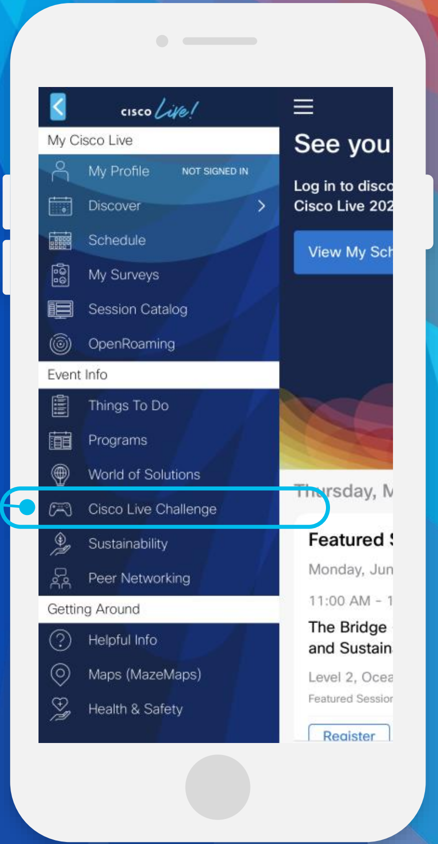
Cisco Live **Challenge**

Gamify your Cisco Live experience!

Get points for attending this session!

How:

1. Open the Cisco Events App.
2. Click on 'Cisco Live Challenge' in the side menu.
3. Click on View Your Badges at the top.
4. Click the + at the bottom of the screen and scan the QR code:



cisco Live!