

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



Building Incident Response Actions for Meraki using Cisco XDR Orchestration Workflows

Achieve Automated Response Actions for Different
Use Cases

Awais Khan – Solutions Engineer
DEVNET-2057

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/#DEVNET-2057>

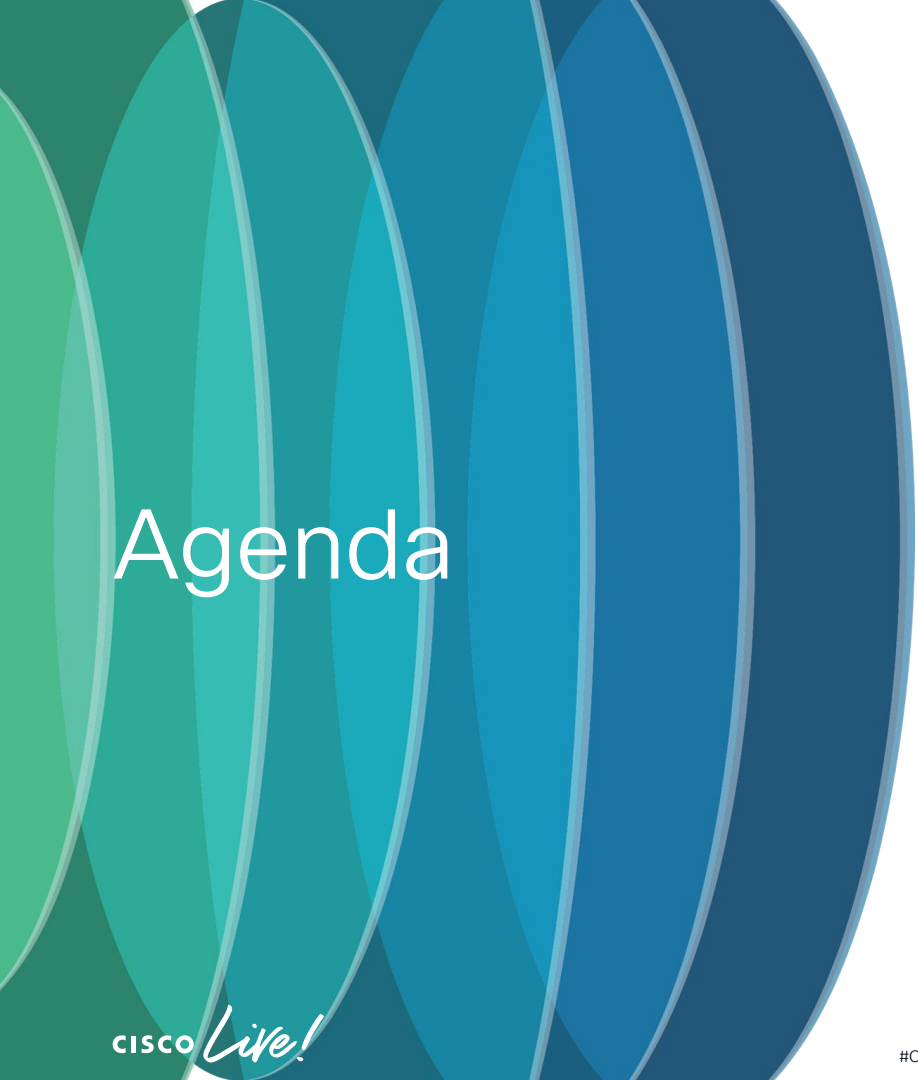


About me



- Sydneysider
- Proud father of two girls
- Foodie
- Love cricket
- Enjoy cooking for stress relief





Agenda

- Introduction
- Response options
- Building my first workflow
- Let's automate the response
- Conclusion

What is XDR?



Collection of raw telemetry & detections from multiple security tools & sensors



Application of advanced analytics to the collected and normalised evidence to produce correlated and prioritised detections of malicious activity

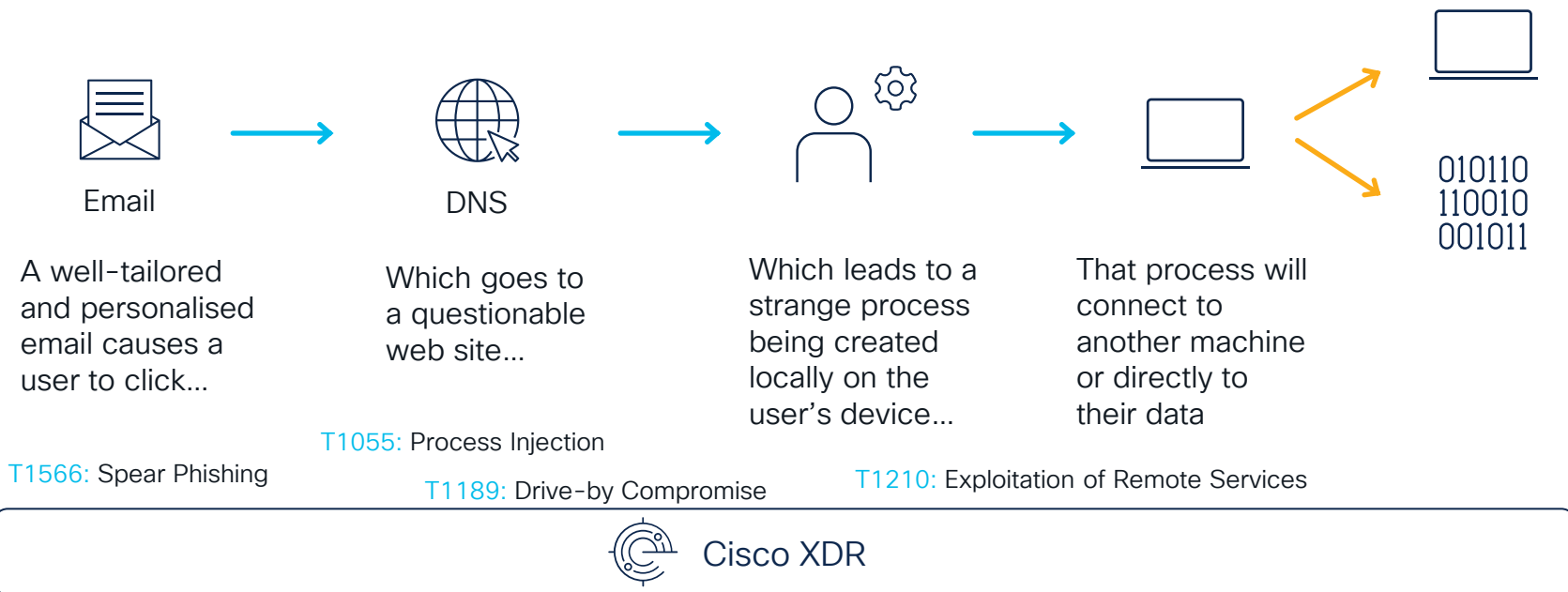


Guided or automated responses across multiple control planes to quickly and effectively contain, mitigate, and eradicate the threat.

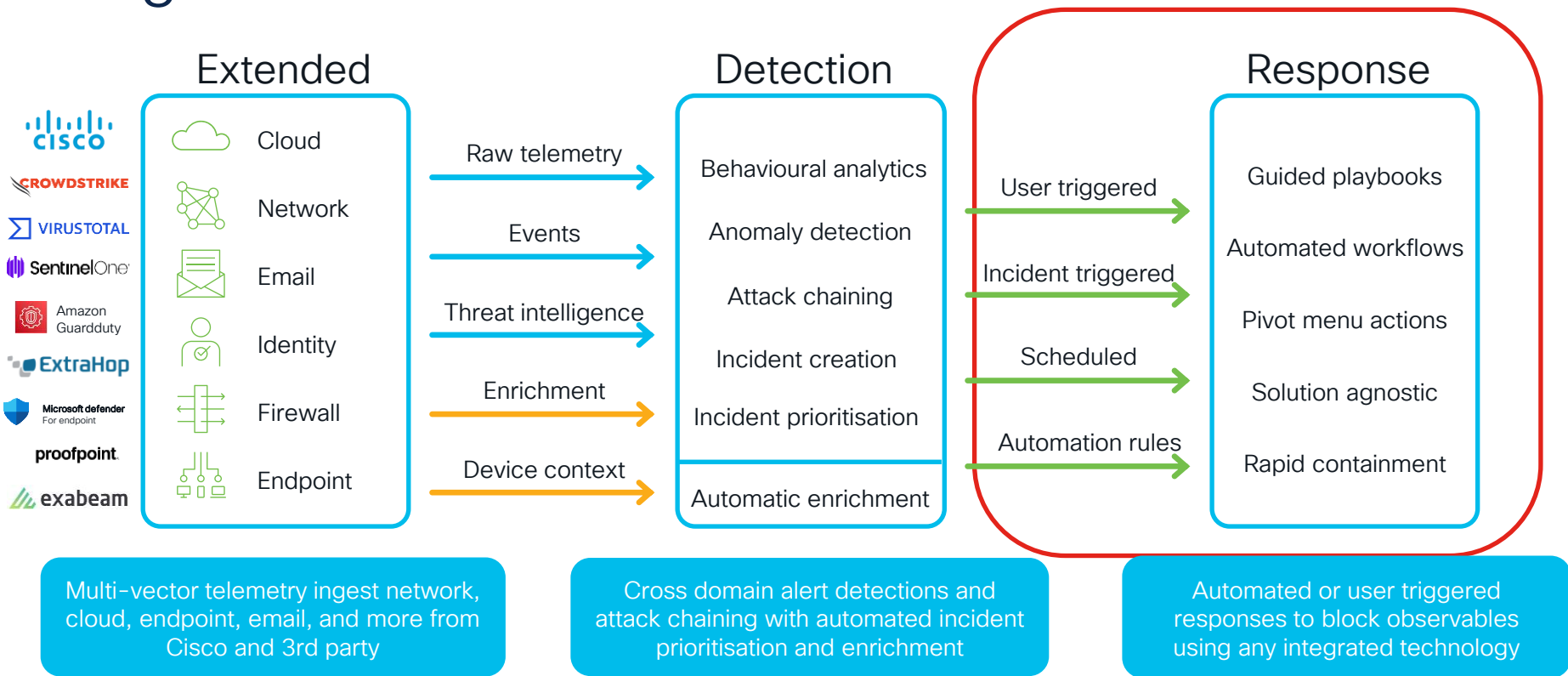


Stop advanced threats like ransomware

Most attacks use a sequence like this...



High level architecture



- Control Center
- Incidents
- Investigate
- Intelligence
- Automate
- Assets
- Client Management
- Administration

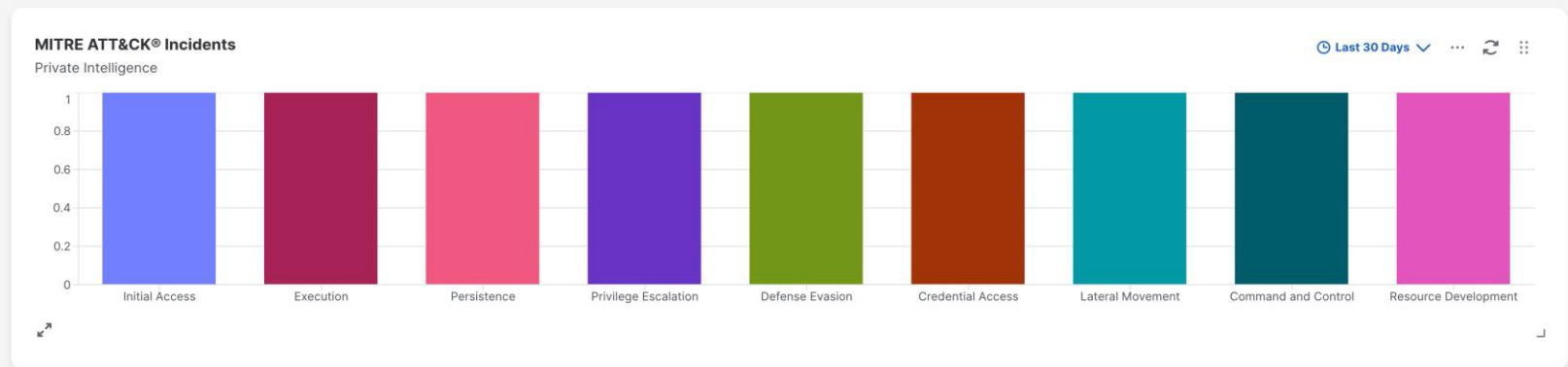
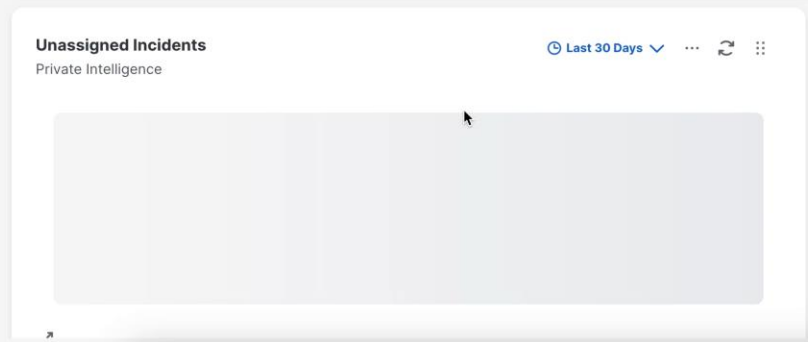
Dashboards

- Overview
- Secure Endpoint
- Secure Cloud Analytics NDR
- Private Intelligence
- Test

Full screen

Customize Dashboards

Last 30 Days (4 of 4)



Team Mean Time Summary

Private Intelligence

Last 30 Days

Mean Time to Engage

0 mins

down 0 mins from last month

Incidents Engaged

0

Mean time to Resolution

1 days 22 hrs 33 mins

up 1 days 22 hrs 33 mins from last month

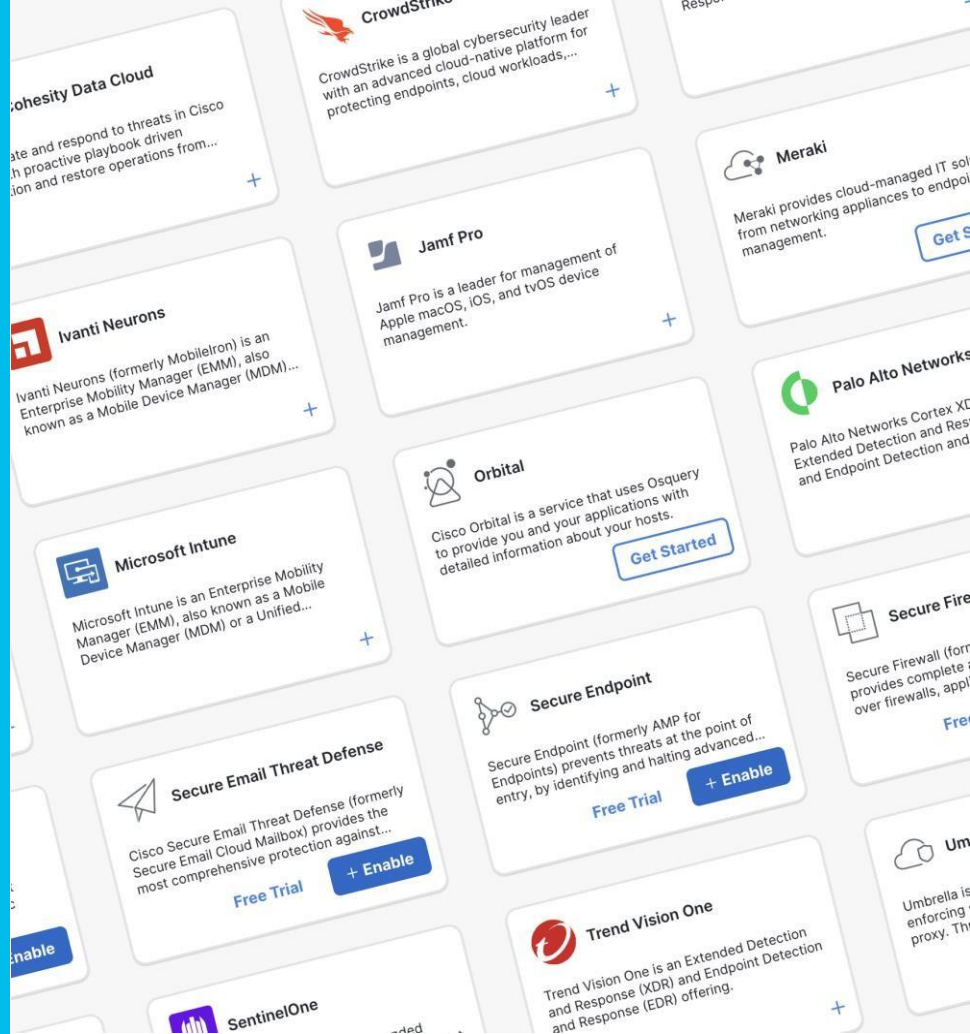
Incidents Resolved

1

We have over 90 built-in integrations



CISCO *Live!*



Integration Capabilities



Capabilities:

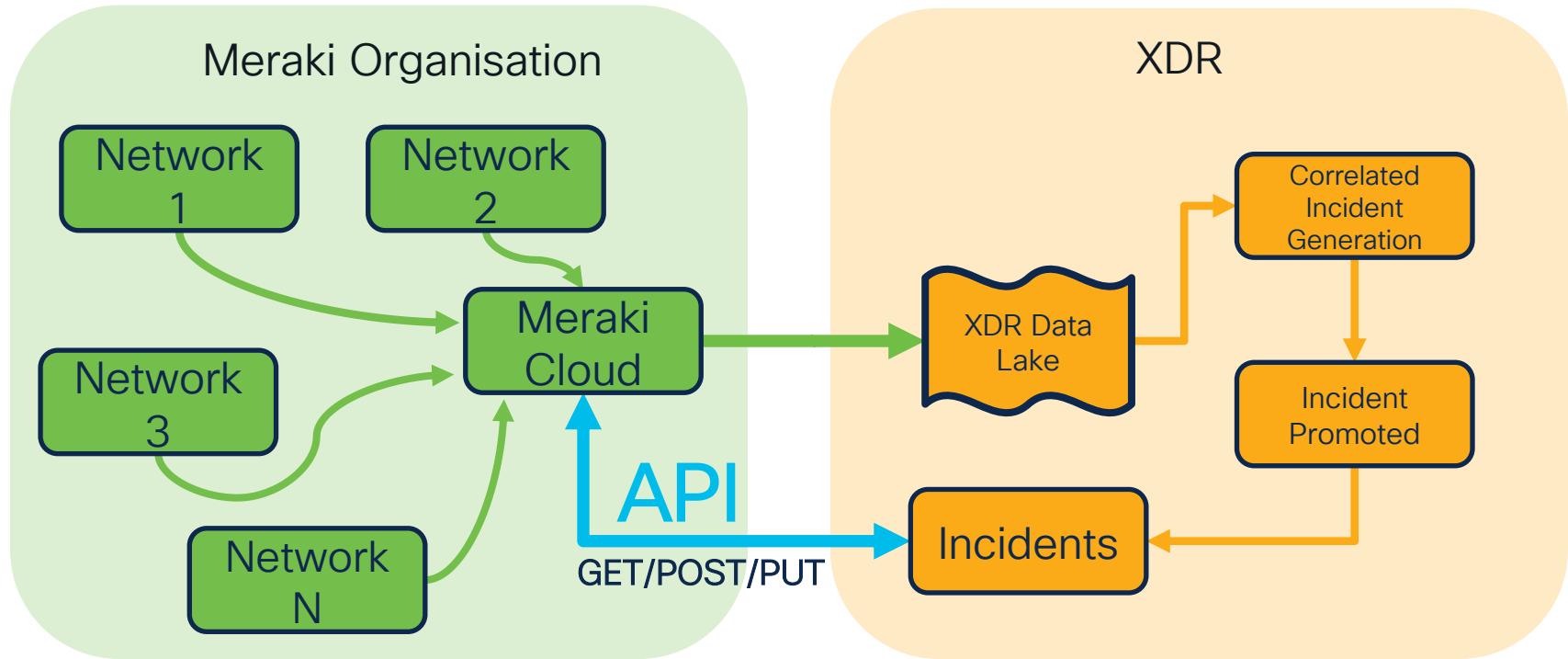
- Detection analytics and correlation
- Threat hunting and investigation
- Asset insights and context
- Automation and response

Available:

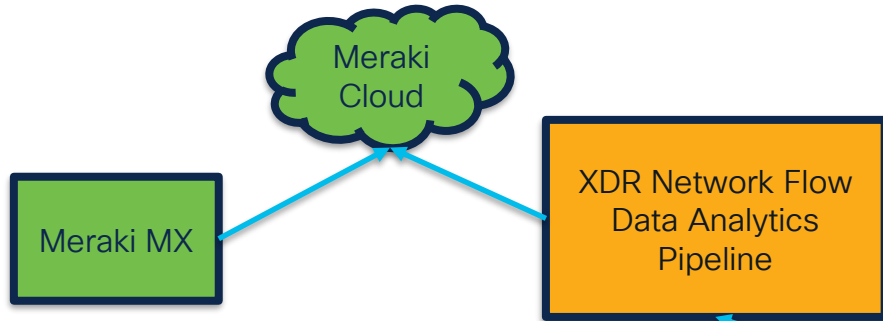
- Enabling in XDR
- Browsing Cisco's Github
- Write your own

MX & XDR Integration

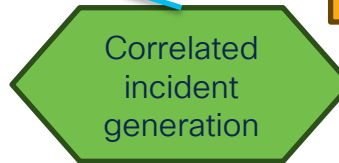
High-level Overview: API



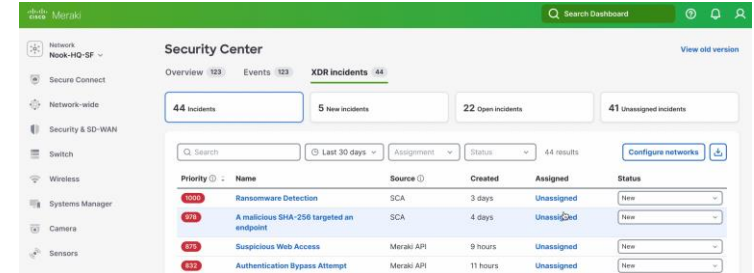
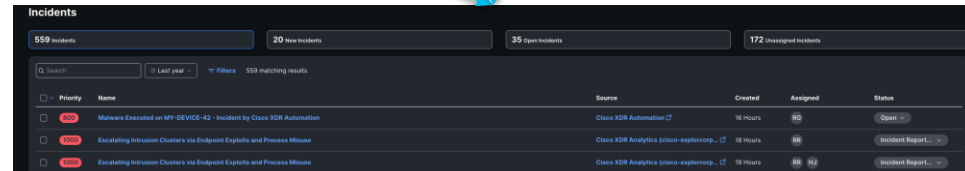
Meraki MX and XDR integration!



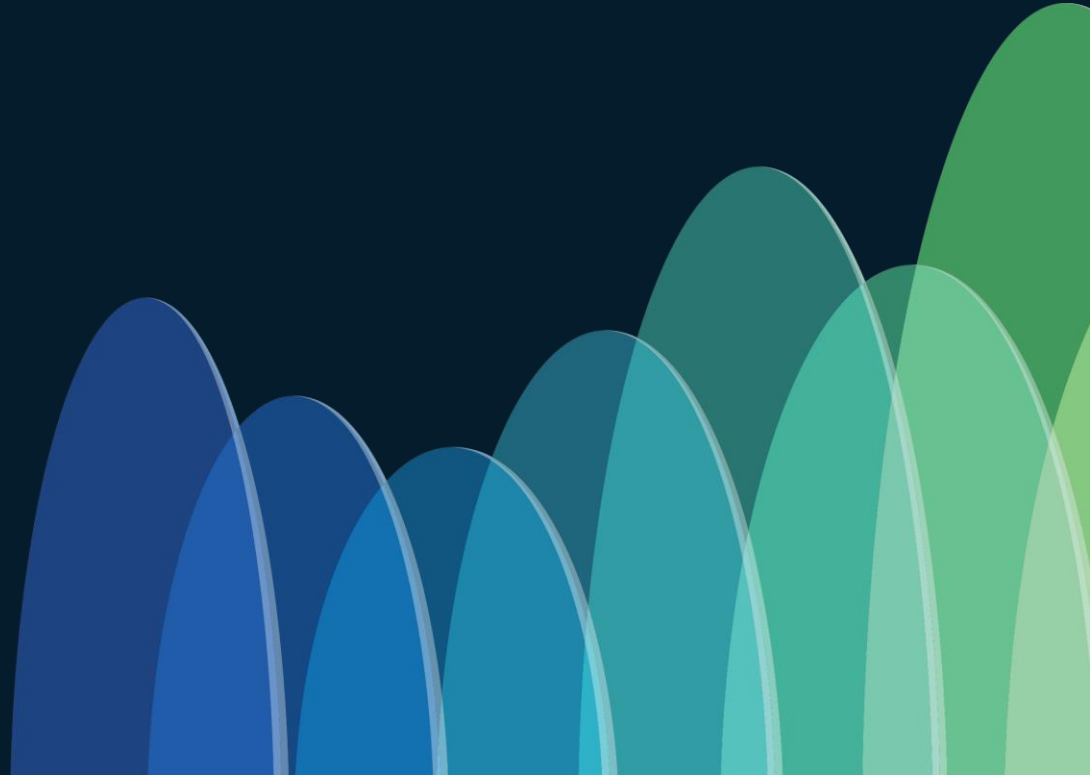
- Meraki MX exports flow logs direct to Meraki cloud
- XDR reads flow logs for configured orgs/networks
- XDR analytics does its thing



- Incidents appear in XDR Incident Manager
- XDR Incident Manager can be operated on from the Meraki Dashboard



Response



Response options

- Guided one-click response
- Pivot menu
- Automated response

Guided response

Single-click response actions:

- Contain assets
- Contain hashes, URL, domain
- Create ServiceNow tickets
- Run vuln scans

Cisco Managed Incident Playbook ⓘ

Published April 10, 2024 at 6:45:51 PM

Identification

Containment

Eradication

Recovery

▼

Contain Incident: Overview

Execute ⓘ

Overview of how to contain Indicators of Compromise to stop the spread of malicious ac...

▼

Contain Incident: Assets

Execute ⓘ

Use asset-based containment to stop the spread of malicious activity.

▼

Contain Incident: IPs

Execute ⓘ

Contain IP indicators of compromise to stop the spread of malicious activity.

▼

Contain Incident: Domains

Execute ⓘ

Contain domain indicators of compromise to stop the spread of malicious activity.

▼

Contain Incident: URLs

Execute ⓘ

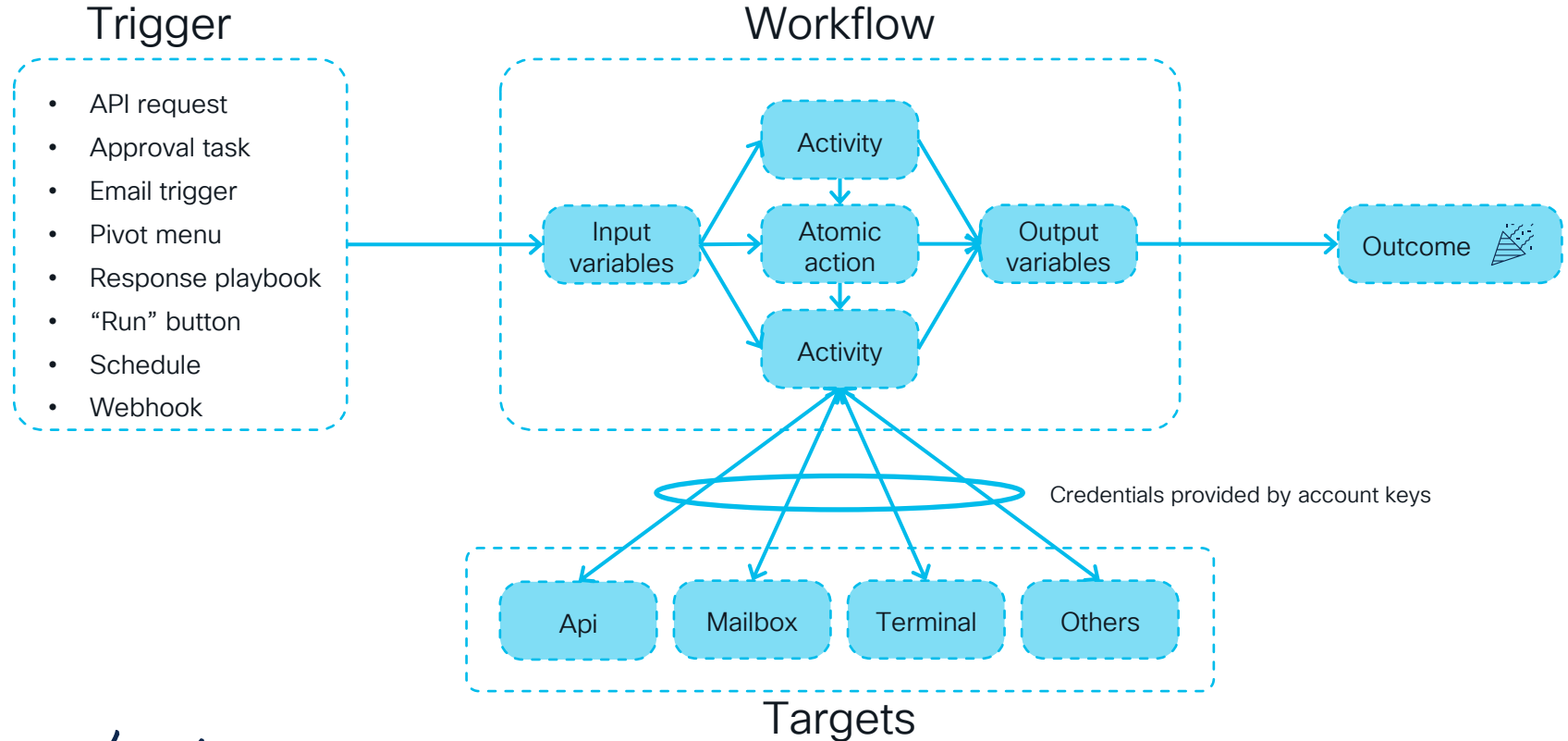
Contain URL indicators of compromise to stop the spread of malicious activity.

Pivot menu

- Built-in response actions
- Build your own

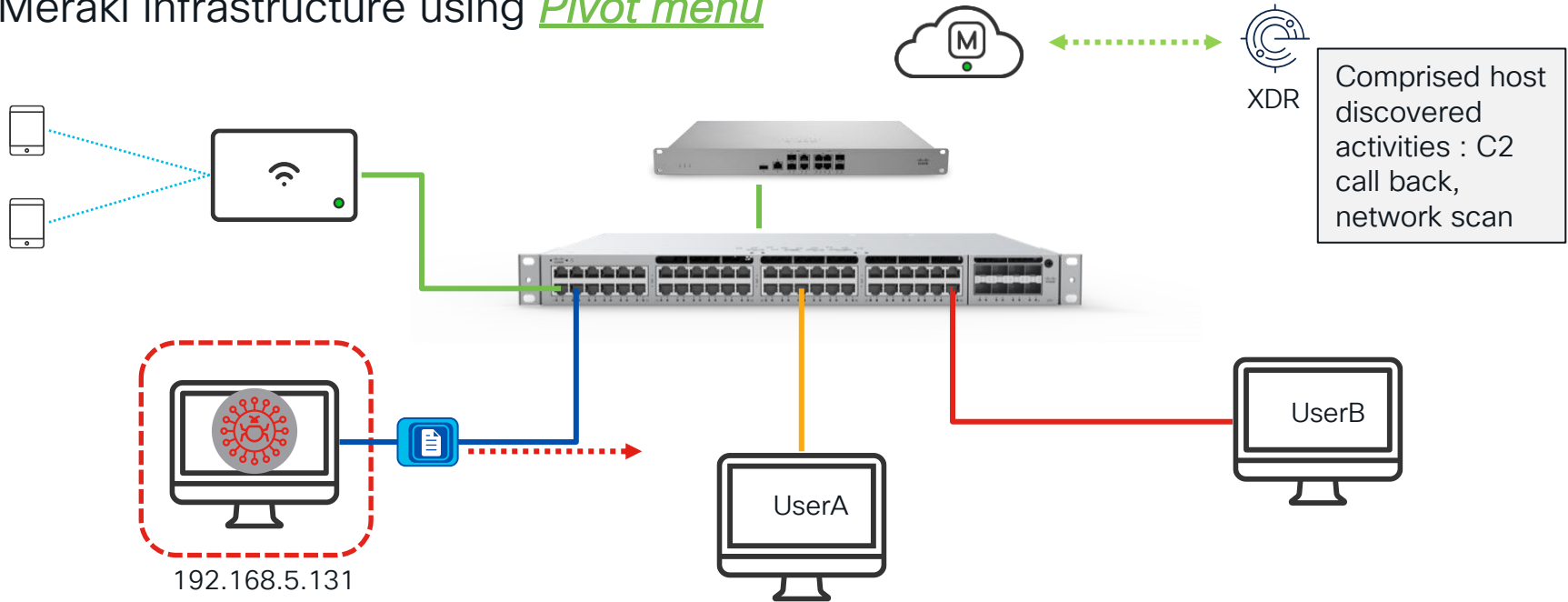
The screenshot displays the Cisco SecureX interface. At the top, a vertical toolbar contains icons for adding (+), removing (-), zooming (X), undo (↶), redo (↷), and a pivot menu icon (a square with a circle inside). Below this, a diagram shows a flow from an endpoint icon labeled 'ona-a152e3.awakha...' to a network icon labeled '192.168.130.113'. The main content area is divided into two panels: '2 Assets' and '2 Observables'. The '2 Assets' panel lists 'Endpoint' with 'ona-a152e3.awakhan-lab.com' (2 events) and 'Network' with '192.168.130.113' (1 event). The '2 Observables' panel lists 'Unknown IP Address' with '192.168.10.205' (2 events) and 'Unknown SWC De' with '2449' (1 event). A context menu is open over the '192.168.10.205' observable, showing options: 'IP Address 192.168.10.205', 'Create Judgment', 'Copy value', 'Copy defanged value', '+ Add to new case', and '+ Add to active case'. Below these are 'Automation' actions: '*Meraki Host Isolation', 'Fortinet - FortiGate - Block URL, IP, or Domain', 'ISE - Quarantine Endpoint', 'Secure Firewall - Block Observable (Direct)', '2019 - Meraki - MX - L3 Outbound Firewall Block', 'Host Isolation with Tier 2 Approval', and 'Umbrella - Add to Blacklist'. A white box with the text 'Respond →' and an arrow points to the 'Respond' button in the context menu.

Flow diagram



Building my first orchestration workflow

- Usecase: Isolate un-managed/BYOD/IOT compromised endpoint on the Meraki infrastructure using Pivot menu



Building my first orchestration workflow – cont.



- Using Meraki dashboard APIs to isolate a user in a single network
- Pre-requisites:
 - API key
 - Network-ID
 - Group policy in Meraki dashboard with restricted access
 - Policy-ID

Building my first orchestration workflow – cont.

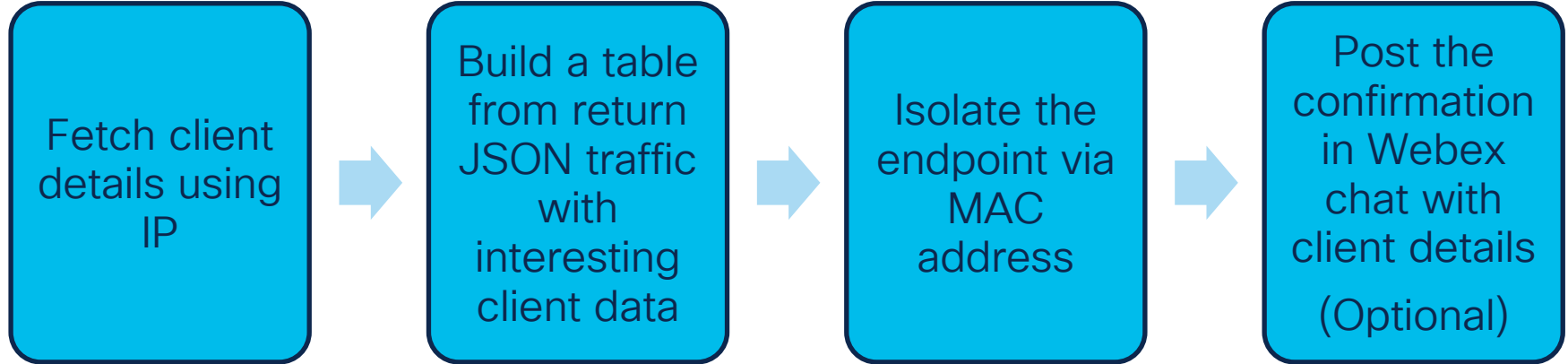
The screenshot displays the Cisco DevNet Developer Hub interface. At the top, the navigation bar includes the Cisco DevNet logo, a 'SIGN UP FREE' button, a 'LOG IN' button, and a search bar. Below the navigation bar, the breadcrumb trail reads 'Meraki > API > Dashboard API'. The left sidebar contains a tree view of API endpoints under the 'Meraki' section, with 'clients' expanded to show 'Update Network Client Policy' (PUT).

The main content area is titled 'Update Network Client Policy' and includes the following details:

- Operation ID:** `updateNetworkClientPolicy`
- Description:** Update the policy assigned to a client on the network. Clients can be identified by a client key or either the MAC or IP depending on whether the network uses Track-by-IP.
- Endpoint:** `PUT /networks/{networkId}/clients/{clientId}/policy`
- Request Parameters:** `networkId` (required, string) and `clientId` (required, string).
- Path:** `Network ID`

On the right side, a 'Configuration' panel is visible, showing the 'Parameters' tab. It includes input fields for 'Client ID' and 'Network ID', and a 'Request Body (JSON)' section with a description for 'devicePolicy'.

Building my first orchestration workflow – cont.



Building my first orchestration workflow – cont.

☰

Control Center >

Incidents >

Investigate >

Intelligence >

Automate >

Assets >

Client Management >

Administration >

Automate

Exchange

Workflows

Runs

Targets

Account Keys

Variables

Triggers

Tasks

Advanced

HTTP

Protocol*

HTTPS

Host/IPAddress*

api.meraki.com

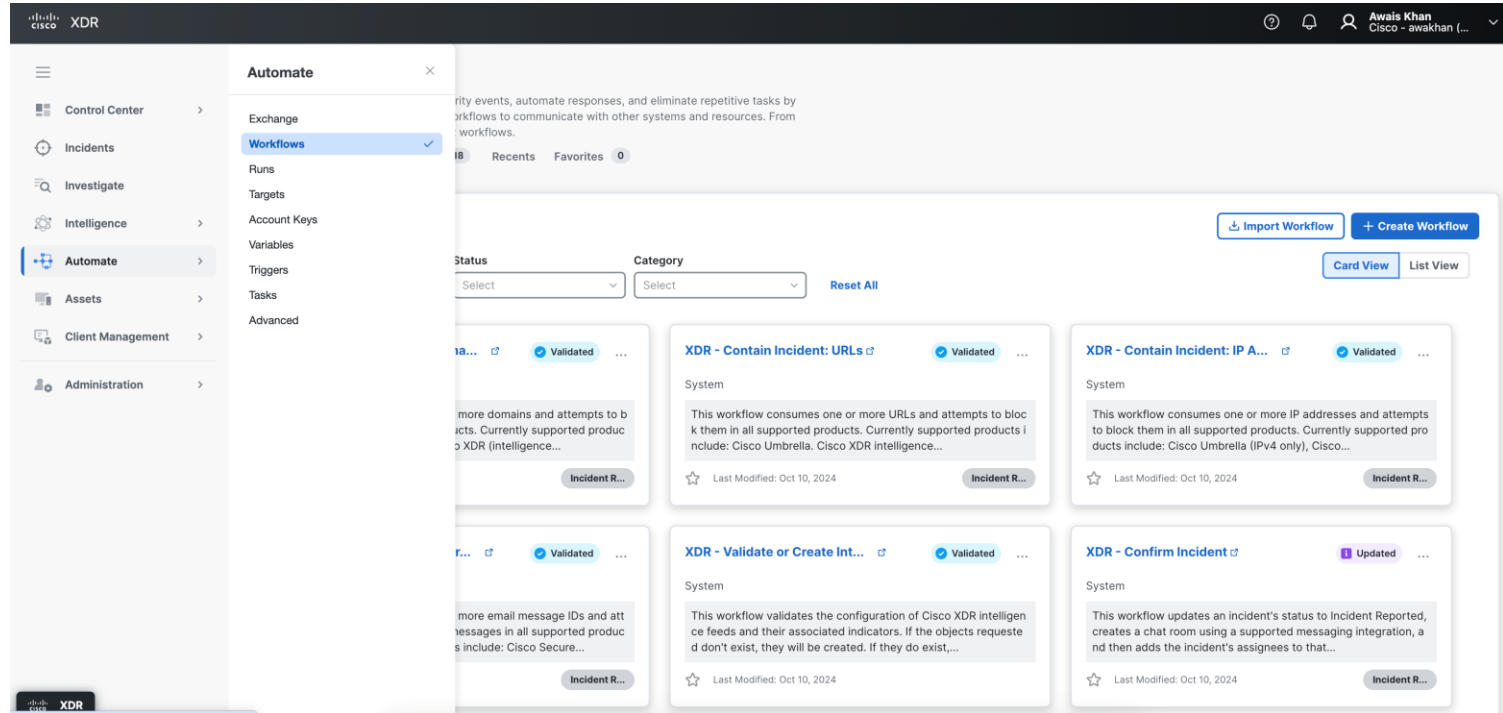
Port

Path

/api/v1

☐ Disable server certificate validation

Building my first orchestration workflow – cont.



Building my first orchestration workflow – cont.

What is the intent of this workflow?

Blank Custom Workflow

Incident Response Workflow

Pivot Menu Workflow

Playbook Task Workflow

Workflow with Automation Rule

Pivot Menu Workflow

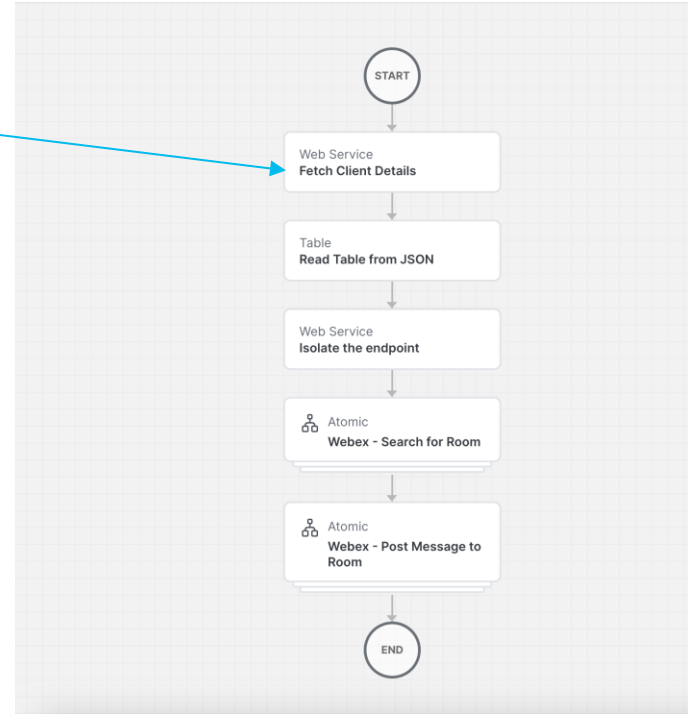
Workflow details

Pivot menu workflows allow you to take response actions from an observable throughout Cisco XDR. Pivot menus appear during investigation, in incidents, and in the XDR Ribbon.

[Cancel](#)[Continue](#)

Building my first orchestration workflow – cont.

1) GET API Call
/networks/[NETWORKID]/clients?i
p=[observable_value]

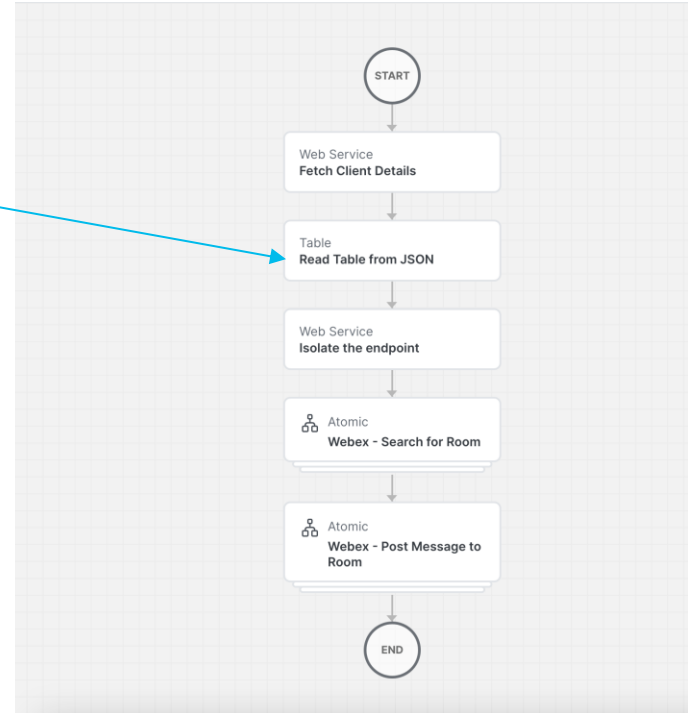


Building my first orchestration workflow – cont.

2) Save the JSON response in a table with values of Interest

Response:

Id, mac, description, ipv4, ipv6, user, firstSeen, lastSeen, manufacturer, os, devicetype, serial-number, recent device connection, SSID,



Building my first orchestration workflow – cont.

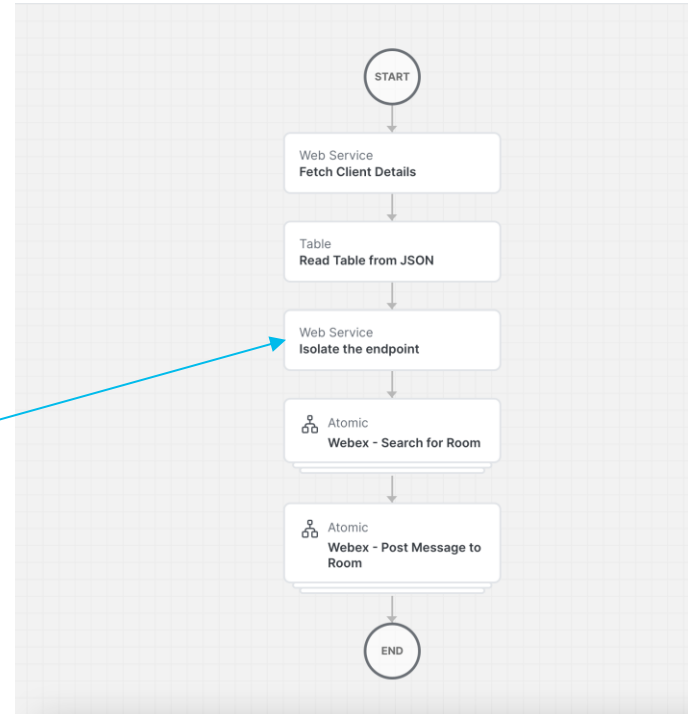
3) PUT API Call

URL:

/networks/[Network_ID]/clients/[MAC]/policy

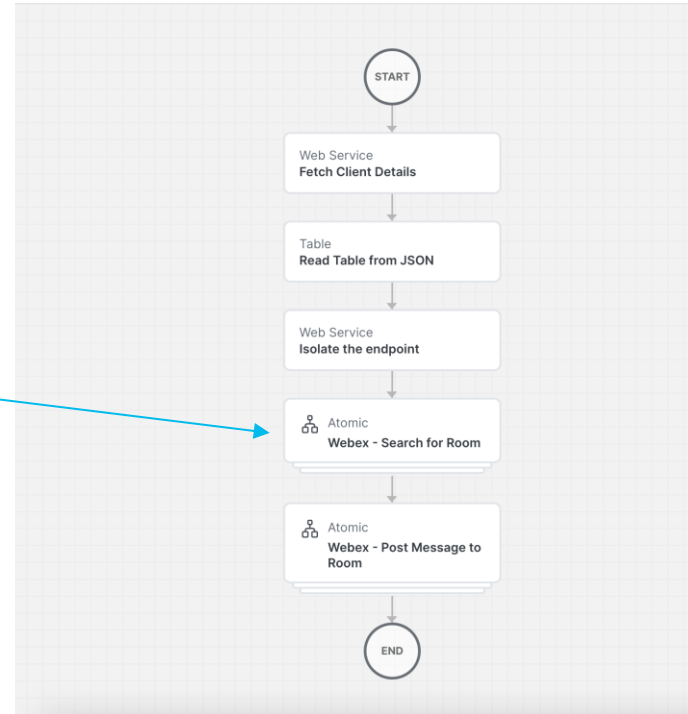
Request Body:

```
{  
  "devicePolicy": "Group policy",  
  "groupPolicyId": "[Policy-ID]"  
}
```



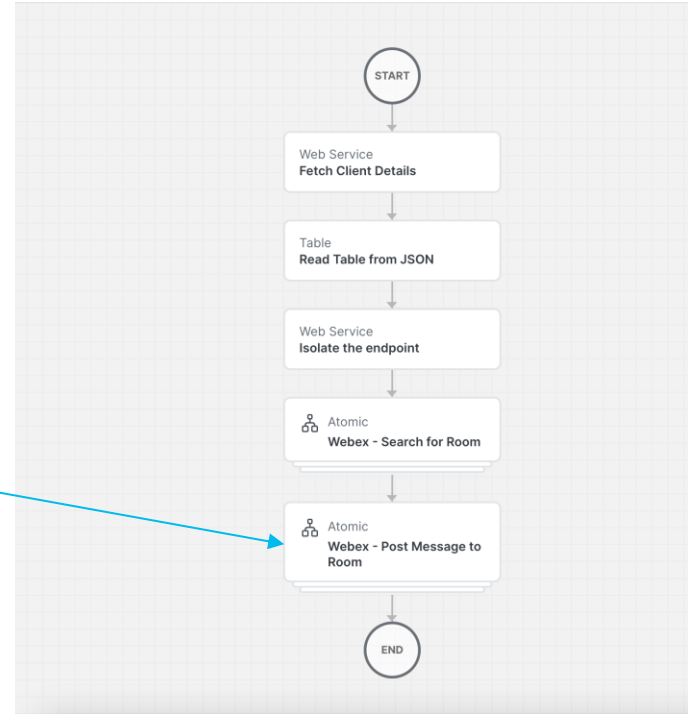
Building my first orchestration workflow – cont.

4) Get the Room ID of the Webex Room – using pre-defined Atomic Object for Webex



Building my first orchestration workflow – cont.

5) Post message to the Webex Room about the activity



New Investigation

Paste log entry, IP address, domain, etc

0 / 2,000

Saved Investigations

Q Search

0 matching results

There are no saved investigations to display

🔗 📄 📝 😊 📱 🗣️ @ 🏠 📺 ✨

Shift + Enter for a new line

• • • awakhan — awakhan@ona-a152e3: ~ — ping 192.168.130.113 — 86x29

```

64 bytes from 192.168.138.113: icmp_seq=34 ttl=64 time=273.357 ms
64 bytes from 192.168.138.113: icmp_seq=35 ttl=64 time=263.143 ms
64 bytes from 192.168.138.113: icmp_seq=36 ttl=64 time=161.793 ms
64 bytes from 192.168.138.113: icmp_seq=37 ttl=64 time=31.771 ms
64 bytes from 192.168.138.113: icmp_seq=38 ttl=64 time=49.262 ms
64 bytes from 192.168.138.113: icmp_seq=39 ttl=64 time=10.000 ms
64 bytes from 192.168.138.113: icmp_seq=40 ttl=64 time=137.946 ms
64 bytes from 192.168.138.113: icmp_seq=41 ttl=64 time=59.655 ms
64 bytes from 192.168.138.113: icmp_seq=42 ttl=64 time=45.558 ms
64 bytes from 192.168.138.113: icmp_seq=43 ttl=64 time=46.174 ms
64 bytes from 192.168.138.113: icmp_seq=44 ttl=64 time=65.619 ms
64 bytes from 192.168.138.113: icmp_seq=45 ttl=64 time=134.038 ms
64 bytes from 192.168.138.113: icmp_seq=46 ttl=64 time=10.000 ms
64 bytes from 192.168.138.113: icmp_seq=47 ttl=64 time=10.157 ms
64 bytes from 192.168.138.113: icmp_seq=48 ttl=64 time=150.374 ms
64 bytes from 192.168.138.113: icmp_seq=49 ttl=64 time=122.137 ms
64 bytes from 192.168.138.113: icmp_seq=50 ttl=64 time=82.766 ms
64 bytes from 192.168.138.113: icmp_seq=51 ttl=64 time=7.533 ms
64 bytes from 192.168.138.113: icmp_seq=52 ttl=64 time=8.777 ms
64 bytes from 192.168.138.113: icmp_seq=53 ttl=64 time=8.095 ms
64 bytes from 192.168.138.113: icmp_seq=54 ttl=64 time=8.777 ms
64 bytes from 192.168.138.113: icmp_seq=55 ttl=64 time=16.273 ms
64 bytes from 192.168.138.113: icmp_seq=56 ttl=64 time=29.416 ms
64 bytes from 192.168.138.113: icmp_seq=57 ttl=64 time=7.867 ms
64 bytes from 192.168.138.113: icmp_seq=58 ttl=64 time=7.893 ms
64 bytes from 192.168.138.113: icmp_seq=59 ttl=64 time=7.893 ms
64 bytes from 192.168.138.113: icmp_seq=60 ttl=64 time=150.411 ms
64 bytes from 192.168.138.113: icmp_seq=61 ttl=64 time=285.761 ms

```

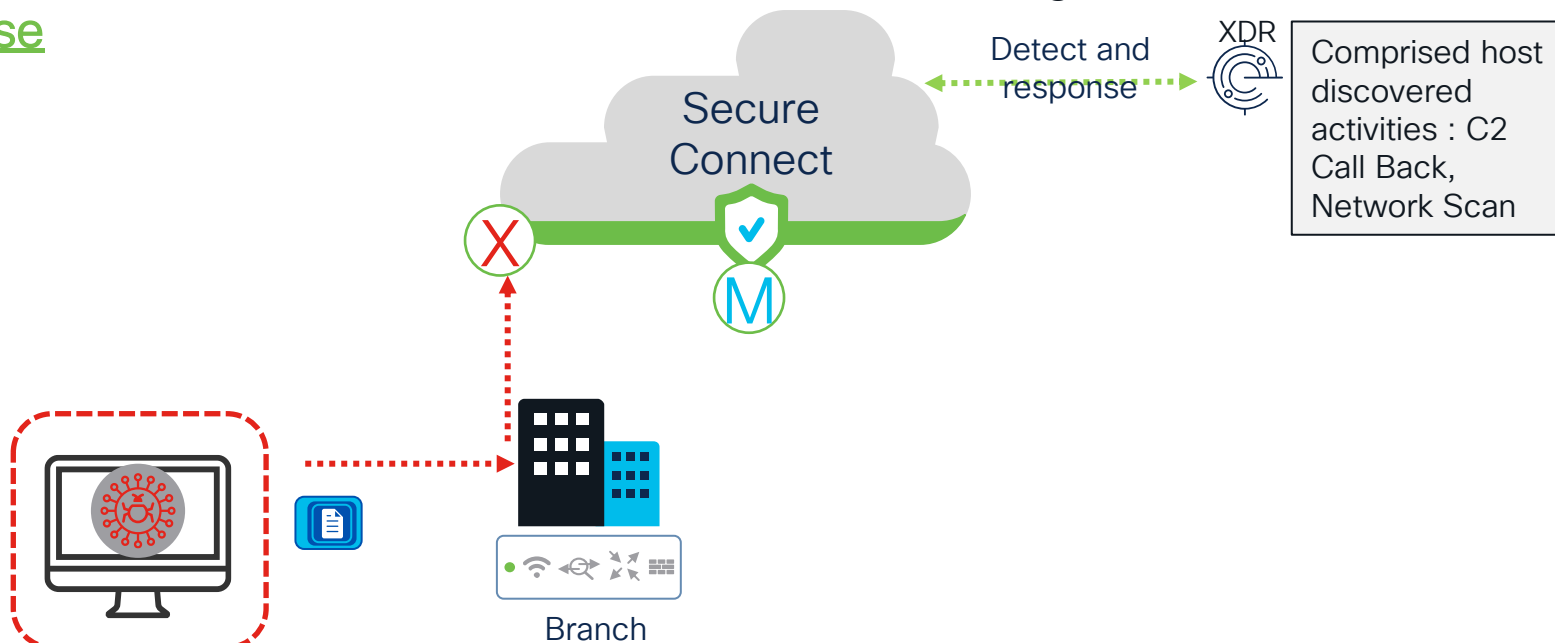

Automation

- How I can automate the response actions?

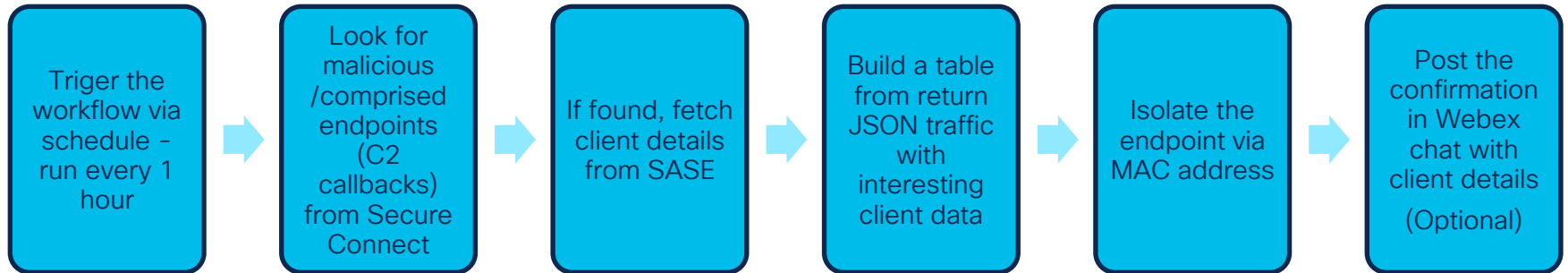
- Email trigger
- Webhook
- Schedule
- API request

Let's automate – customized threat detection and response using SASE and XDR

- Use case: Isolate un-managed/BYOD/IOT compromised endpoint on the Meraki infrastructure once discovered in SASE using automated response



Let's automate



Cisco XDR - Automate

Meraki Dashboard

Security Activity

n189.meraki.com/o/fNjzKd9c/manage/organization/secure_connect/policy_overview?from=secure_connect+polices_overview

Meraki

Search Dashboard

Global Overview

Organization
Awais Home

Network
Awais Home

Secure Connect

Network-wide

Assurance New

Security & SD-WAN

Switching

Wireless

Insight

Organization

Find in Menu

Low impactMedium impactHigh impact

DNS PoliciesFirewall PoliciesWeb PoliciesDLP PoliciesBrowser Access Policies

You may need multiple types of policies to achieve one goal. Broader (but lower impact) concerns can be filtered with broad policies, and specific (but high impact) concerns should be controlled by specific and targeted policies. See [Umbrella Policies Best Practices documentation](#) for details.

Policies for Meraki-managed networks and remote access are managed by [Meraki Group Policies](#)

DNS Policies

Enabled Policies
2 default policy

Disabled Policies
0

Configure DNS Policies

Firewall Policies

Enabled Policies
5 default policy

Disabled Policies
1

Configure Firewall Policies

Web Policies

Enabled Policies
2

Disabled Policies
0

Configure Web Policies

DLP Policies

Enabled Policies
1

Disabled Policies
0

Configure DLP Policies

Browser Access Policies

Enabled Policies
2 default policy

Disabled Policies
0

Configure Browser Access Policies

XDR Orchestration Awais Lab

Meet

Messages

People (2)

Content

Meetings

Apps

Shift + Enter for a new line

Write a message to XDR Orchestration Awais Lab

awakhan — awakhan@ona-a152e3: — ping 192.168.130.113 — 86x29

64 bytes from 192.168.130.113: icmp_seq=2445 ttl=64 time=90.084 ms
64 bytes from 192.168.130.113: icmp_seq=2446 ttl=64 time=278.701 ms
64 bytes from 192.168.130.113: icmp_seq=2447 ttl=64 time=633.122 ms
64 bytes from 192.168.130.113: icmp_seq=2448 ttl=64 time=49.164 ms
64 bytes from 192.168.130.113: icmp_seq=2449 ttl=64 time=641.081 ms
64 bytes from 192.168.130.113: icmp_seq=2450 ttl=64 time=160.849 ms
64 bytes from 192.168.130.113: icmp_seq=2451 ttl=64 time=512.566 ms
64 bytes from 192.168.130.113: icmp_seq=2452 ttl=64 time=378.273 ms
64 bytes from 192.168.130.113: icmp_seq=2453 ttl=64 time=320.672 ms
64 bytes from 192.168.130.113: icmp_seq=2454 ttl=64 time=577.151 ms
64 bytes from 192.168.130.113: icmp_seq=2455 ttl=64 time=196.851 ms
64 bytes from 192.168.130.113: icmp_seq=2456 ttl=64 time=470.940 ms
64 bytes from 192.168.130.113: icmp_seq=2457 ttl=64 time=185.438 ms
64 bytes from 192.168.130.113: icmp_seq=2458 ttl=64 time=435.838 ms
64 bytes from 192.168.130.113: icmp_seq=2459 ttl=64 time=639.004 ms
64 bytes from 192.168.130.113: icmp_seq=2460 ttl=64 time=181.690 ms
64 bytes from 192.168.130.113: icmp_seq=2461 ttl=64 time=476.890 ms
64 bytes from 192.168.130.113: icmp_seq=2462 ttl=64 time=44.023 ms
64 bytes from 192.168.130.113: icmp_seq=2463 ttl=64 time=65.524 ms
64 bytes from 192.168.130.113: icmp_seq=2464 ttl=64 time=642.327 ms
64 bytes from 192.168.130.113: icmp_seq=2465 ttl=64 time=175.321 ms
64 bytes from 192.168.130.113: icmp_seq=2466 ttl=64 time=480.883 ms
64 bytes from 192.168.130.113: icmp_seq=2467 ttl=64 time=183.204 ms
64 bytes from 192.168.130.113: icmp_seq=2468 ttl=64 time=416.898 ms
64 bytes from 192.168.130.113: icmp_seq=2469 ttl=64 time=584.258 ms
64 bytes from 192.168.130.113: icmp_seq=2470 ttl=64 time=270.308 ms
64 bytes from 192.168.130.113: icmp_seq=2471 ttl=64 time=477.914 ms
64 bytes from 192.168.130.113: icmp_seq=2472 ttl=64 time=188.682 ms

Keynote Deep Dives

Wednesday
10:30am – 11:30am



Experiences Amplified:
How AI Can Fuel Better Employee and Customer Experiences

Level 1
Room 106



Smart, Secure, Seamless:
Transforming Experiences with Next-Generation Networking

Level 2
Room 204



Harness a Bold New Era:
Transform Data Centre and Service Provider Connectivity

Level 2
Room 203



Securing User to Application and Everything in Between

Level 2
Melbourne Room 2



Unlocking Digital Resilience through Unified Observability

The HUB
Centre Stage

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