

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



Security Automation

Developing with Cisco XDR

Matt Vander Horst
Leader, Technical Content
DEVNET-1083

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/#DEVNET-1083>



Matt Vander Horst

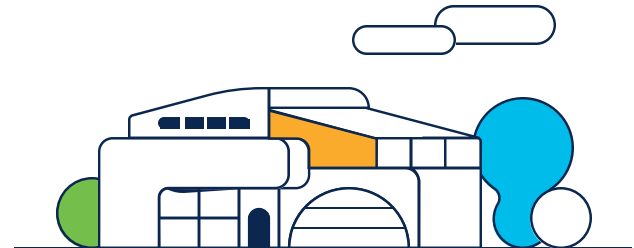
- 8 years at a Fortune 100 insurance company
 - Network engineering
 - Cisco ISE
 - Software/DevOps
- 4.5 years at Cisco
 - SecureX → XDR
 - Integrations and automation
- VP of Spoiling

cisco *Live!*



Agenda

- XDR Overview
- Integrations
- APIs
- Automation
- Resources



The XDR promise



Collection of telemetry
from multiple security tools



Application of analytics to the
collected and homogenized
data to arrive at a detection
of maliciousness



Response and remediation
of that maliciousness



The Cisco approach to XDR

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

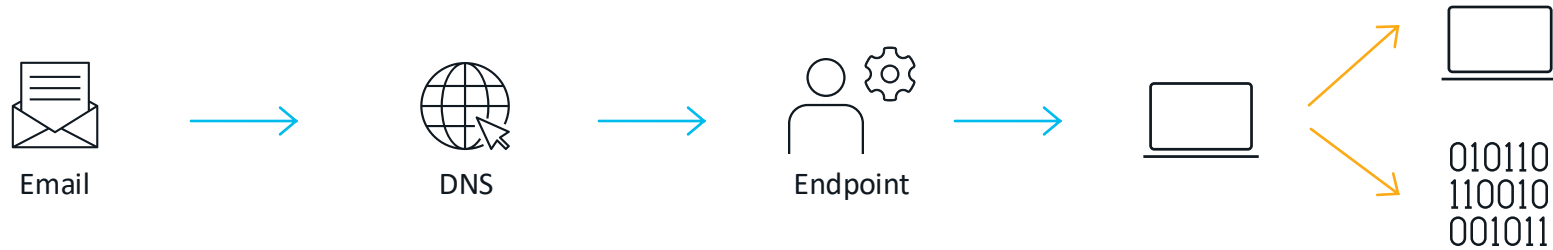
Build resilience



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

Stop advanced threats like ransomware

Most attacks use a sequence like this...



A well-tailored and personalized email causes a user to click...

Which goes to a questionable web site...

Which leads to a strange process being created locally on the user's device...

That process will connect to another machine or directly to their data

T1055: Process Injection

T1566: Spear phishing

T1189: Drive-by Compromise

T1570: Lateral Tool Transfer

T1087: Account Discovery: Domain Account

T1048: System Network Connections Discovery

Vendor A

Vendor C

Vendor E

Vendor G

Vendor D



← Incidents

1000

Incident Reported ▾

Escalating Intrusion Clusters via Endpoint Exploits and Process Misuse

Reported by [Cisco XDR Analytics \(cisco-explorcorp-earth\)](#) on 2024-05-02T17:36:32.241Z - [6 Linked Incidents](#)

RR HJ

[View detailed description](#)

This incident started on **2024-04-05 19:15:01 UTC** and ended on **2024-04-11 12:23:05 UTC**, a total span of approximately six days. The security alert chain indicated a series of suspicious and possibly unauthorized activities within the company's network environment. Multiple devices were i... [more](#)

Overview

Detection

Response

Worklog

Report

[View Investigation](#)

 Expand



7 Assets

[View all](#)

TOP ACTIVE



6 Device

134 Observables

[View all](#)

TOP ACTIVE



Malicious SHA-256

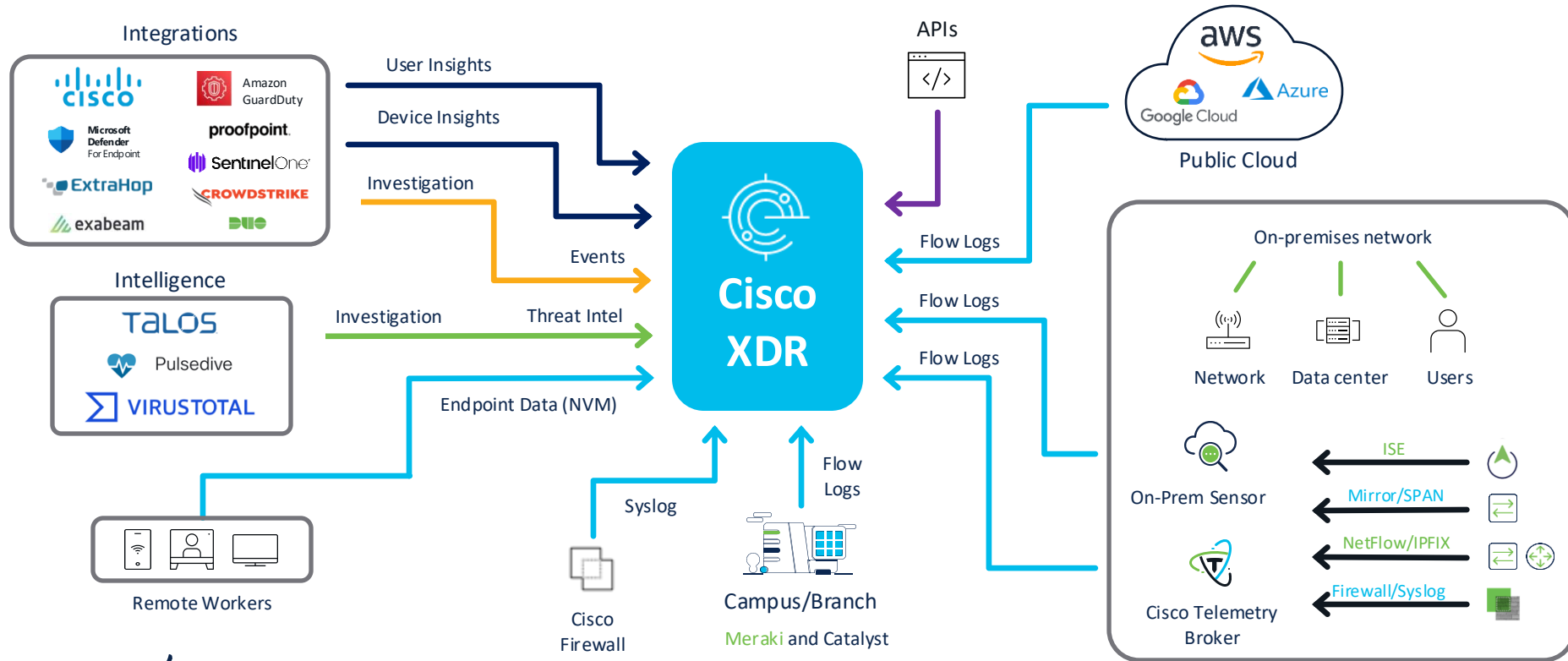
8 Indicators

[View all](#)

TOP ACTIVE

Cisco XDR Analytics (cisco-explorcorp-earth)

Telemetry sources for Cisco XDR



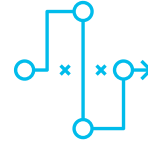
Developing with XDR



Integrations



APIs



Automation

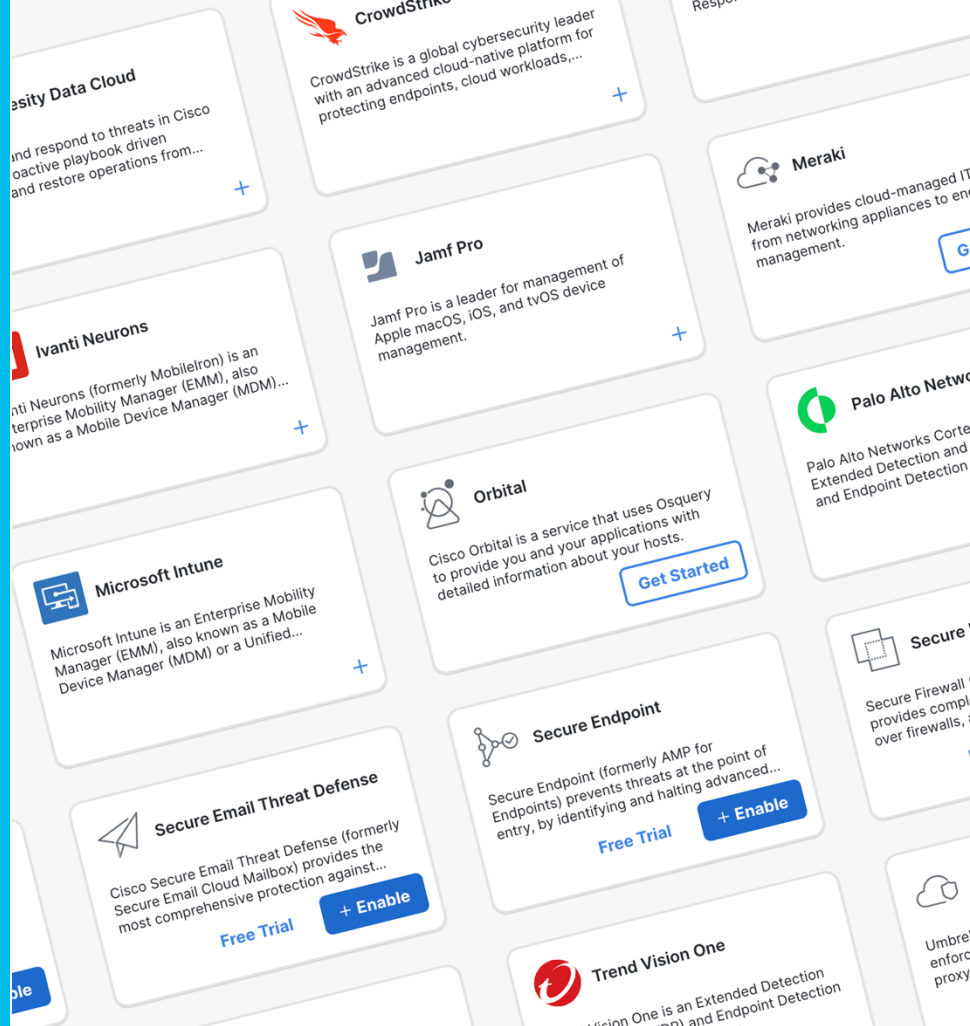
Integrations

- Allow XDR to communicate with other products
 - Both Cisco and third party
- Use the Cisco Threat Intelligence Model (CTIM) to represent data
- Available by:
 - Configuring in XDR
 - Browsing Cisco's GitHub¹
 - Writing your own²

¹ Some of the integration code in GitHub is outdated.

² Not all XDR capabilities are supported in custom integrations.

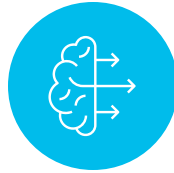
CISCO *Live!*



Integration capabilities



Dashboard



Deliberate



Devices



Observe
Observables



Observe Targets



Refer



Respond



Users

Integration capabilities

- Dashboard
 - Tiles with data that can be displayed on your XDR dashboards
- Deliberate
 - Provides verdicts with a disposition (clean, suspicious, malicious, unknown)
- Observe → Observables
 - Provides a summary of sightings for an observable

Integration capabilities

- Observe → Targets
 - Provides a summary of data for targets related to an observable
- Refer
 - Provides links to other resources or tools in the pivot menu
- Respond
 - Allows users to take actions in the integrated product from the pivot menu

What's a pivot menu?

Orientation



1 Asset

[View Assets](#)

 10.150.0.2



4 events

1 Observable

 170.210.208

What's a pivot menu?

Overview

Detection

Response

Worklog

Orientation

1 Asset

10.150.0.2

Refer →

Respond →

IP Address ⓘ 10.150.0.2

Secure Endpoint - ExplorCorp

Search for this IP ↗

Secure Network Analytics - ExplorCorp 741

Host Report ↗

Secure Network Analytics - ExplorCorp 742

Host Report ↗

XDR Automation

Submit URL to Secure Malware Analytics

Duo - Block User

1 Observabl

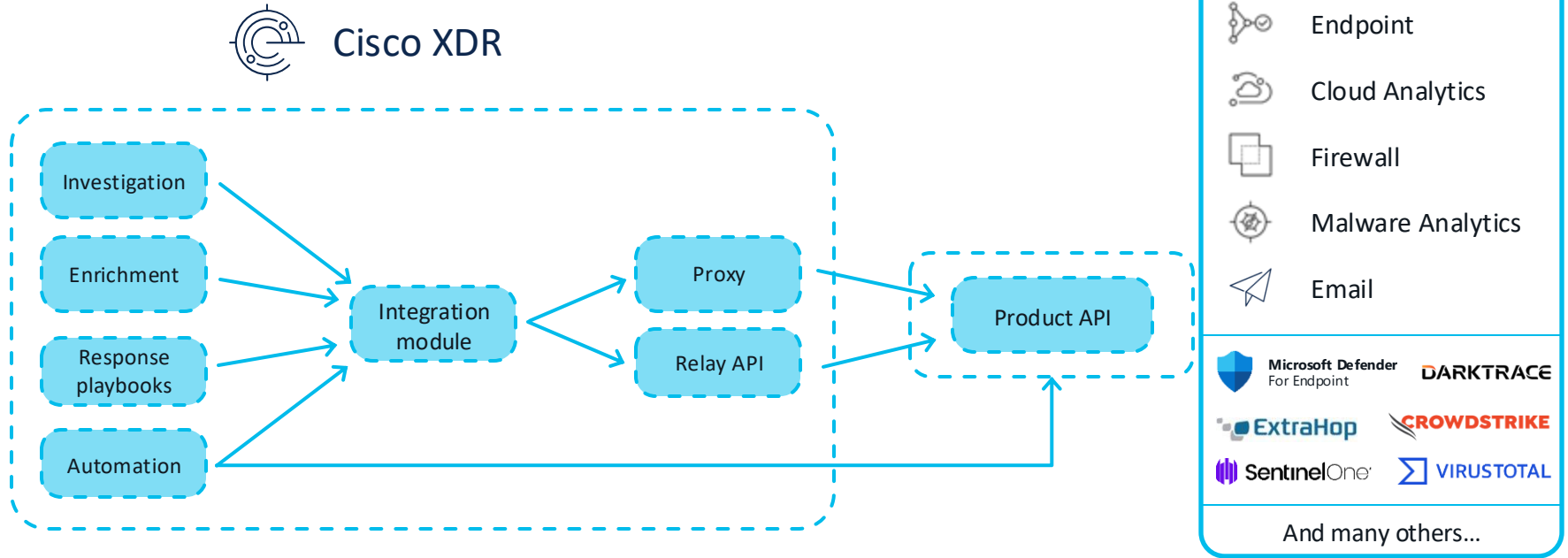
170.210.208

Integration capabilities

- Devices
 - Information about assets and their management and/or security posture
- Users
 - Information about users from an identity manager
- Telemetry
 - Raw data used to generate detections and correlations

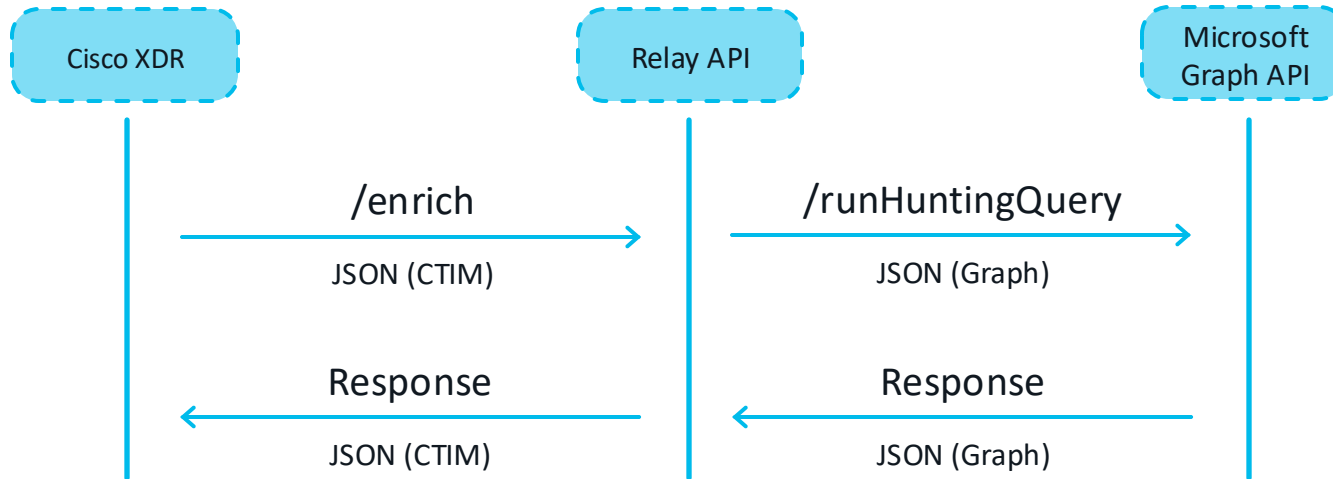
(These are the capabilities you can't add to a custom integration)

Integration architecture



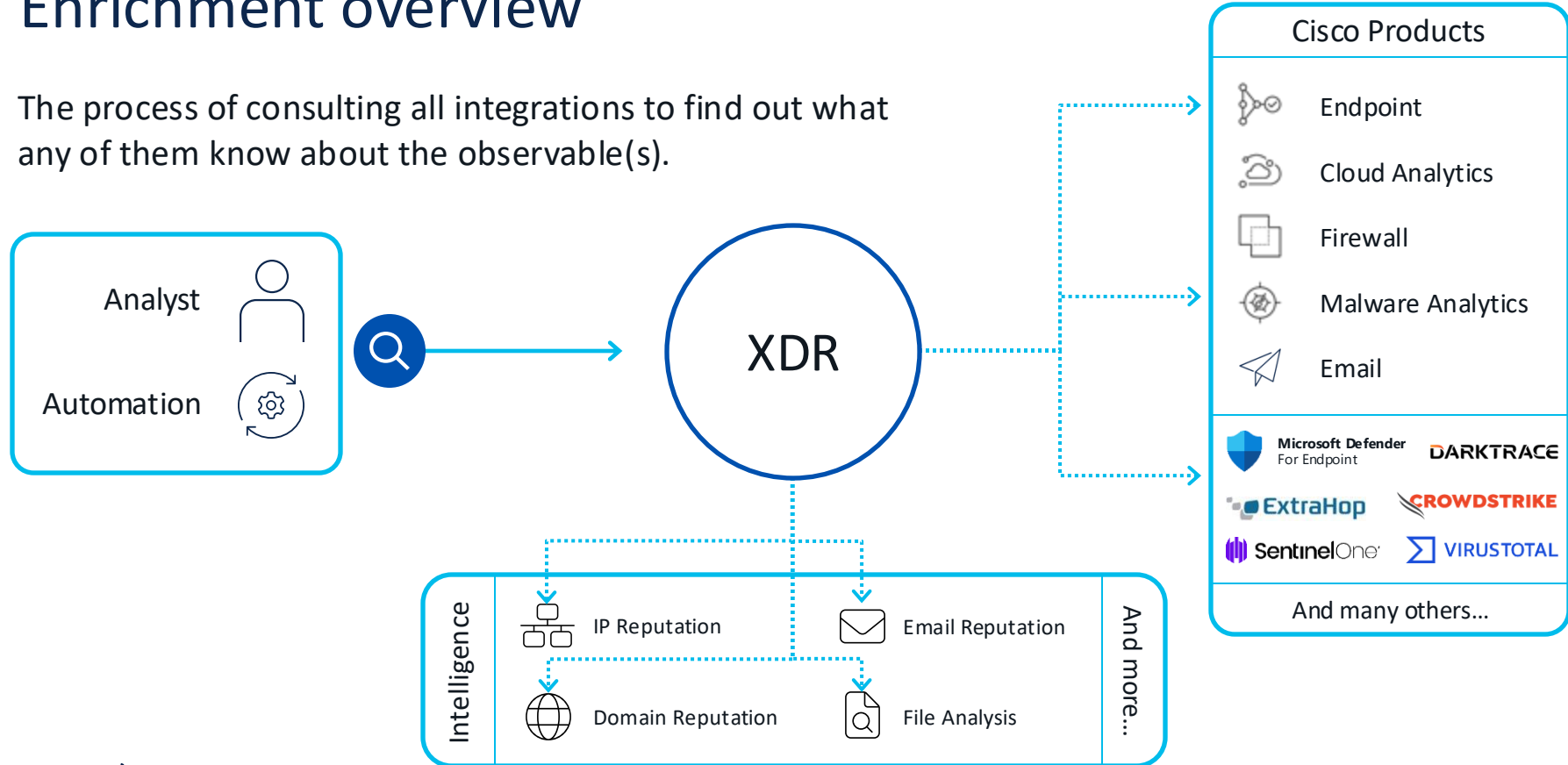
Relay APIs

- Translate data between Cisco XDR and other products
- HTTP-based API (very few requirements)



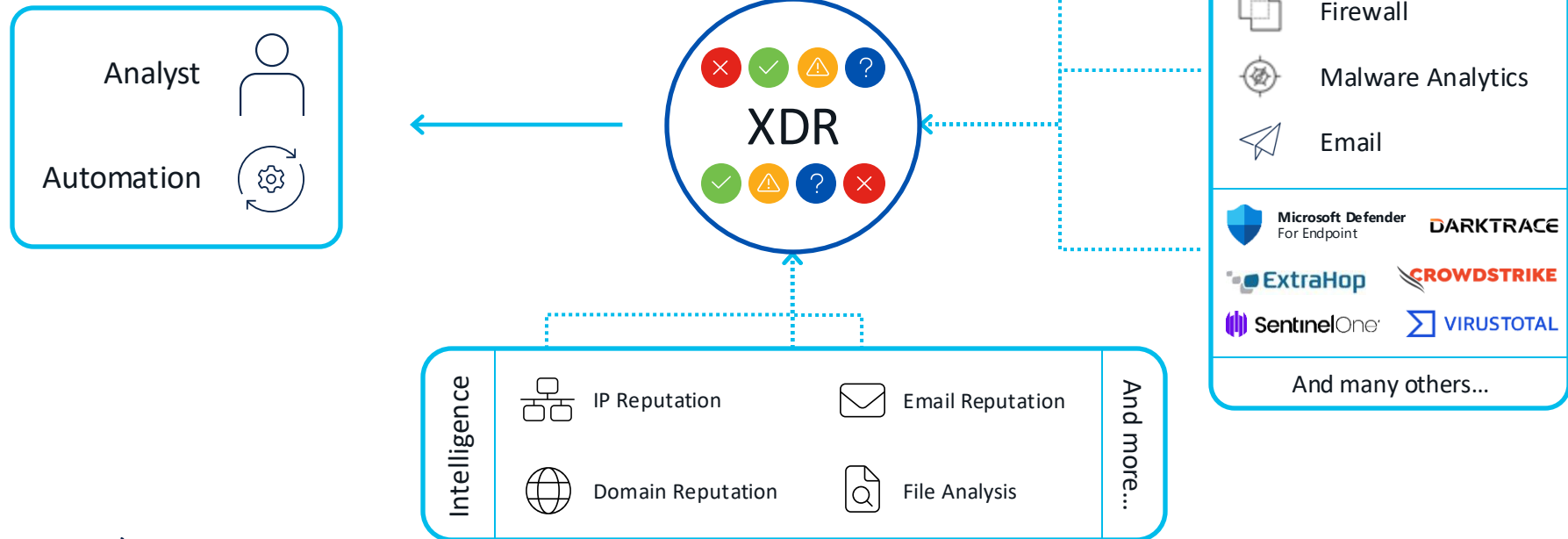
Enrichment overview

The process of consulting all integrations to find out what any of them know about the observable(s).



Enrichment overview

The process of consulting all integrations to find out what any of them know about the observable(s).



Integrations demo



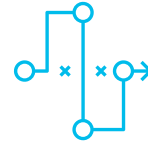
Developing with XDR



Integrations



APIs



Automation

XDR APIs

- Cisco XDR has multiple different APIs
- Provide unique functionality
 - For example: inspecting content for observables
- Provide a conduit to integrations and their data
- Require an API key generated in XDR
 - With the appropriate scopes for the APIs you want to use

XDR APIs



Automation



Devices



Enrich



Inspect



Private Intelligence



Proxy



Public Intelligence



Response

APIs: Automate

- Triggering a workflow
- Getting information about workflows and workflow runs
- Creating and managing:
 - Targets
 - Account Keys
 - And more...

API Reference

Automation

Overview

API

WorkflowInstances

Workflows

Calendars

Categories

ChangeOwner

Events

EventsRateLimit

References

RemoteMeta

Rules

RuntimeUsers

Schedules

Schemas

ShareObjectPermissions

SKIROHIncident

TableTypes

Tables

TargetGroups

Targets

Tasks

Tenants

DEVNET

Documentation

Learn

Technologies

Communities

Documentation > All > Cisco XDR > Cisco XDR APIs

Automation API Docs

The Automation API allows developers to interact with the backend to manage objects, retrieve Workflow Run information and even execute workflows.

Note: The Automation API has a different source than the other Cisco XDR APIs. It is not versioned, whereas the other API endpoints are not.

Required API Scope: for the Automation API you will need the `ao` API scope. The Automation API uses the `ao` API scope, as described in the [Getting Started](#) document. The Automation API with the pre-filled credentials.

Use Cases

- Create or update HTTP targets to make API calls.
- Query available targets while running a workflow.
- Query approval tasks.
- Run a workflow via API trigger.

How to use the API Docs

Use the interactive documentation to explore the Automation API endpoints, their parameters and it also allows you to instantly try it out in the online playground.

DEVNET-1083

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

29

APIs: Inspect

- Takes an arbitrary block of text and extracts observables from it
- Simple and easy way to extract things to investigate from content like emails, blog posts, threat intel websites, and more...

The screenshot displays the Cisco DevNet API Inspector interface. At the top, the breadcrumb navigation shows 'Investigate / Inspect / Inspect for observables'. The main area shows a POST request to the endpoint `https://visibility.{{amp_api_domain}}/iroh/iroh-inspect/inspect`. The 'Body' tab is selected, showing the request body as a JSON object with a 'content' field. The content is a string describing a block of text with an IP address and a file hash. Below the request body, the 'Body' tab is also selected, showing the extracted observables in a structured JSON format. The observables are:

```
{
  "value": "192.168.1.1",
  "type": "ip"
},
{
  "value": "4a24048f81afbe9fb62e7a6a49adb1faf41f266b5f9feecdceb567aec096784",
  "type": "sha256"
},
{
  "value": "nlbmfsyphoiaicmxhum.com",
  "type": "domain"
}
```

The bottom of the interface shows the status 'Status: 200' and the page number '30'.

CISCO *Live!*

- ## Documentation

- Exposes response actions made available by integrated products
- Also includes some automation workflows
- Actions are specific to one or more observable types

- Uses the Cisco Threat Intelligence Model (CTIM)
- APIs for:
 - Feeds
 - Incidents
 - Indicators
 - Judgements
 - Sightings
 - Verdicts

APIs: Proxy

- Forwards HTTP requests to integrated products
 - If they support the proxy...
- Abstracts connection information such as the host and credentials
 - Automatically added at runtime
- Used by multiple XDR features and can be used via the API

IROH-INT API Gateway Web Service **1.0.107**

</iroh/iroh-api-gateway/swagger.json>

You can also explore the API through [Redoc](#)

API Gateway API

[Contact Cisco Security Business Group -- Advanced Threat](#)

All Rights Reserved

Use this route to proxyify a request to an Integration API. Use the headers `module-instance-id` to specify the target API to.

Example:

```
Proxy GET /iroh/iroh-api-gateway/proxy/v1/business_info
      target-url: https://api-amp.cisco.com
      module-instance-id: f395dcd0-3bd0-4a80-833b-6a99c2313629
      Authorization: Bearer YOUR_IROH_AUTH_JWT
```

Will make a GET to https://api-amp.cisco.com/v1/business_info with the AMP for Endpoints credentials provided.

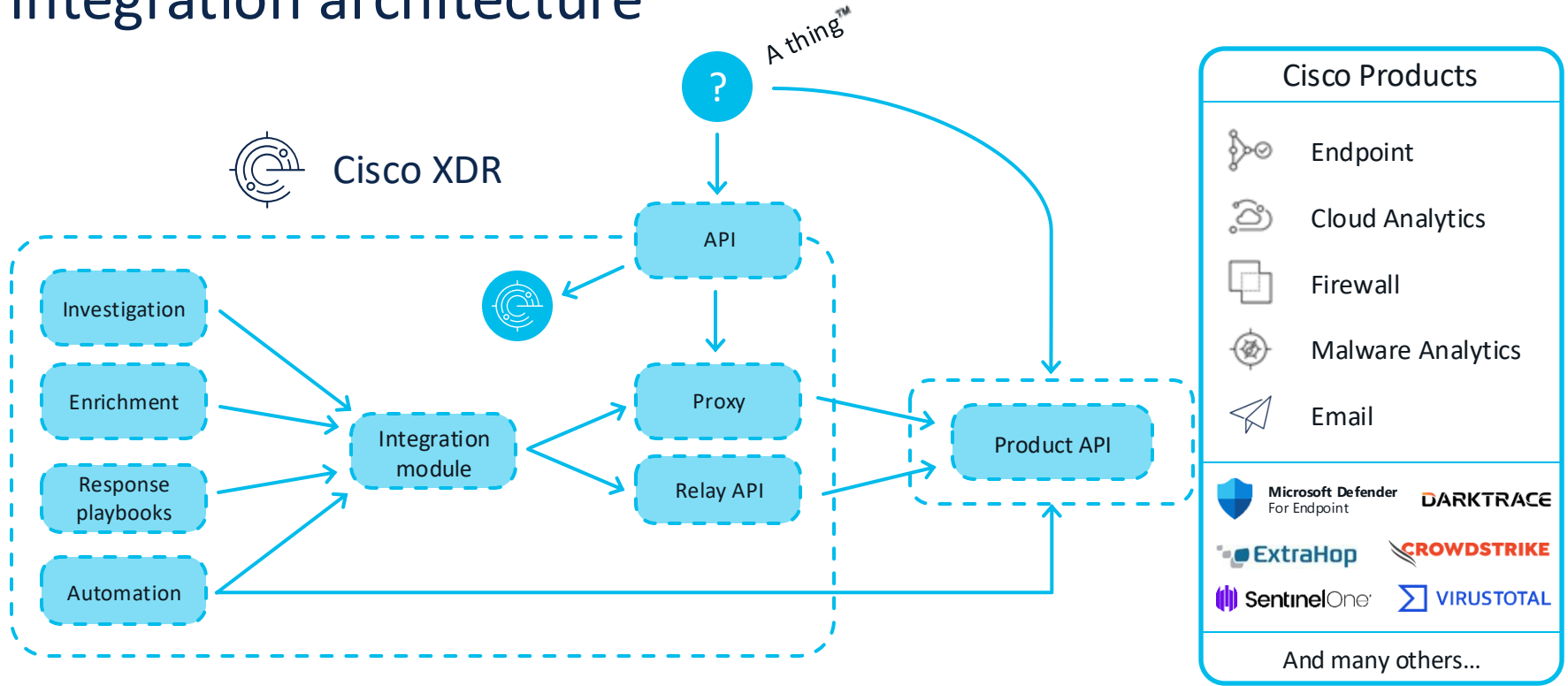
Proxy Endpoints Metadata

GET </iroh/iroh-api-gateway/proxy-endpoints-metadata>

GET </iroh/iroh-api-gateway/proxy-endpoints-metadata/{module-instance-id}>

Models

Integration architecture



What can we do with these APIs?



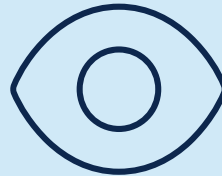
Inspect

- Extract observables from a body of text



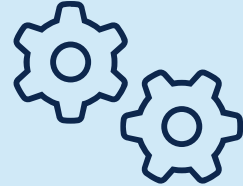
Deliberate

- Get dispositions for observables:
 - Clean
 - Unknown
 - Malicious
 - Suspicious



Observe

- Ask each XDR integration if a given observable was seen in the environment



Respond

- Act against an observable through an XDR module
- Includes workflows and automation rules

What can we do with these APIs?

- Execute an XDR automation workflow from your ITSM platform.
- Execute response actions through integrated products.
- Push intelligence from custom sources into your private intelligence store so it can be used by XDR during investigations.
- Synchronize incidents between XDR and other ticketing platforms.
- Fetch dashboard tile data for inclusion in your “single pane of glass.”
- And more...

API demo



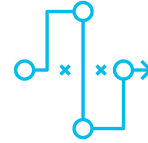
Developing with XDR



Integrations



APIs



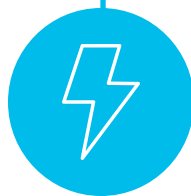
Automation

Automation outcomes



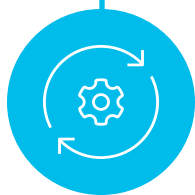
Investigate

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



Fetch IOCs

IOCs can be gathered from any number of sources including threat research websites, blogs/RSS feeds, and so on



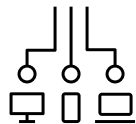
Investigate

Once we have IOCs, we can use XDR via workflows or APIs to investigate using integrated products



Notify

If sightings are found in the environment, we can let analysts know the threat has been seen and remediation is required



Identify

Determine which observables to act against and which action to take



Act

Take the specified action leveraging products integrated with XDR as control points



Fetch IOCs

IOCs can be gathered from any number of sources including threat research websites, blogs/RSS feeds, and so on



Investigate

Once we have IOCs, we can use XDR via workflows or APIs to investigate using integrated products



Respond

Take the specified action leveraging products integrated with XDR as control points

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

For each network

Python
Is the network in scope?

Check if network in scope

Matched or blank

Atomic
Meraki - Network - MX -
Get L3 Outbound Firewall
Rules

Python
Insert new firewall rule

Atomic
Meraki - Network - MX -
Update L3 Outbound
Firewall Rules

Was the update successful?

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

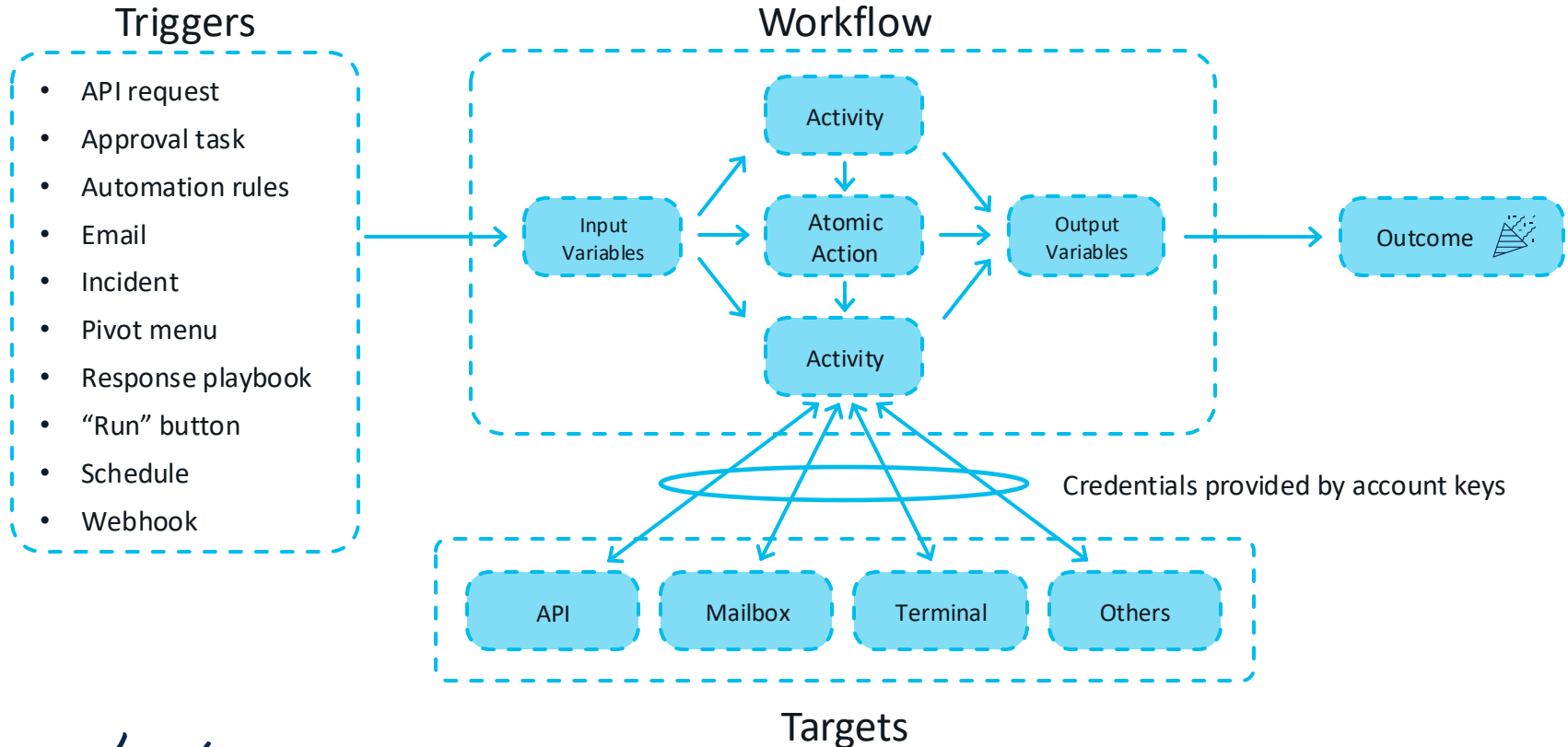
If checked, the workflow run and any underlying task(s) will be deleted when the run succeeds. Failed runs will not be deleted.

☐ Is atomic workflow

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



Flow diagram



Automation demo



Integration resources



Github Repository

<https://github.com/CiscoSecurity/>



Module Maker *(Legacy, but still handy)*

<https://ciscosecurity.github.io/tr-05-module-maker/>



Cisco Threat Intelligence Model (CTIM)

<https://github.com/threatgrid/ctim/>

API resources



Documentation

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



Postman Collection

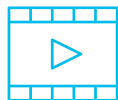
<https://cs.co/xdr-postman-collection>



Postman Environment

<https://cs.co/xdr-postman-environment>

Automation resources



Videos

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



Documentation

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



DevNet

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

Other XDR sessions



Matt Vander Horst
Leader, Technical Content

Getting started with Cisco XDR
Automation workflows and
atomics

DEVWKS-1190

Tomorrow @ 4:00 PM



Aditya Sankar
Technical Leader

XDR Deep Dive

BRKSEC-2596

Tomorrow @ 1:00 PM



Matthew Robertson
Distinguished TME

Extended Detection with Cisco
XDR: Security analytics across
the enterprise

BRKSEC-2178

Tomorrow @ 4:15 PM

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