The bridge to possible

Security Automation

Developing with Cisco XDR

Matt Vander Horst
Technical Leader

DEVNET-1083

Cisco Webex App

Questions?

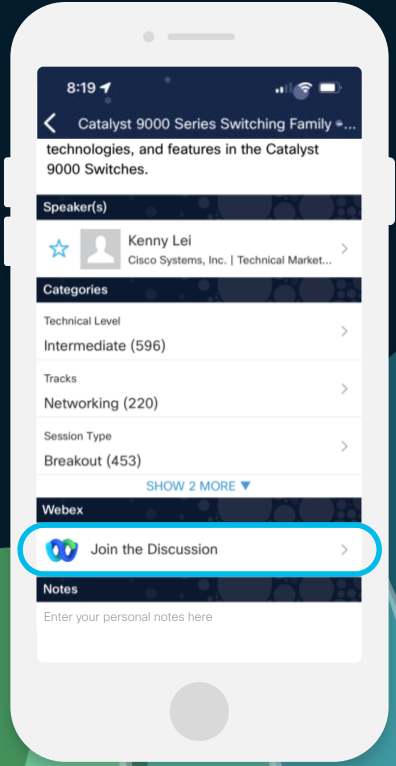
Use Cisco Webex App to chat
with the speaker after the session

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 7, 2024.

https://ciscolive.ciscoevents.com/ciscolivebot/#DEVNET-1083



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

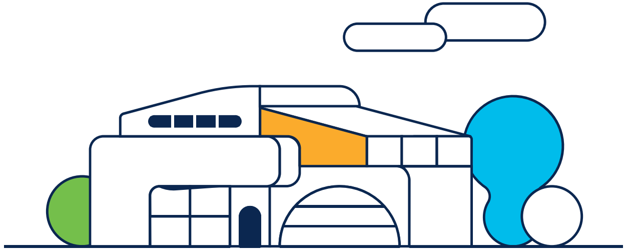
Enter your personal notes here

Matt Vander Horst

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

Agenda

- XDR Overview
- Integrations
- APIs
- Automation
- Resources



cisco Live!

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

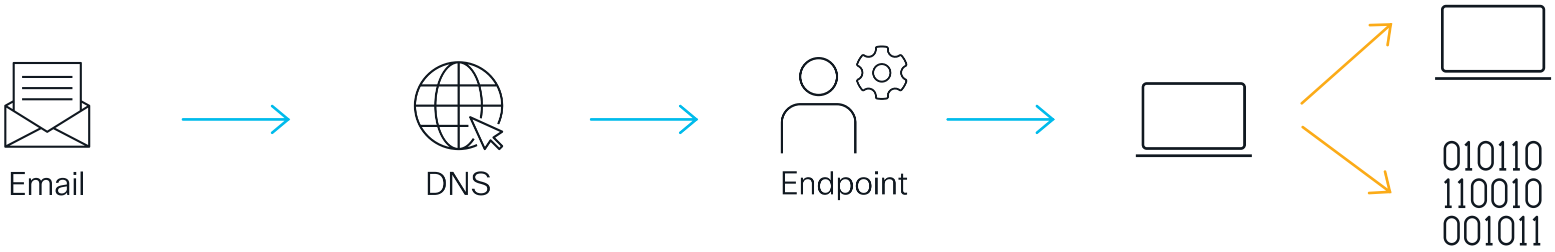
Elevate productivity

- 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



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

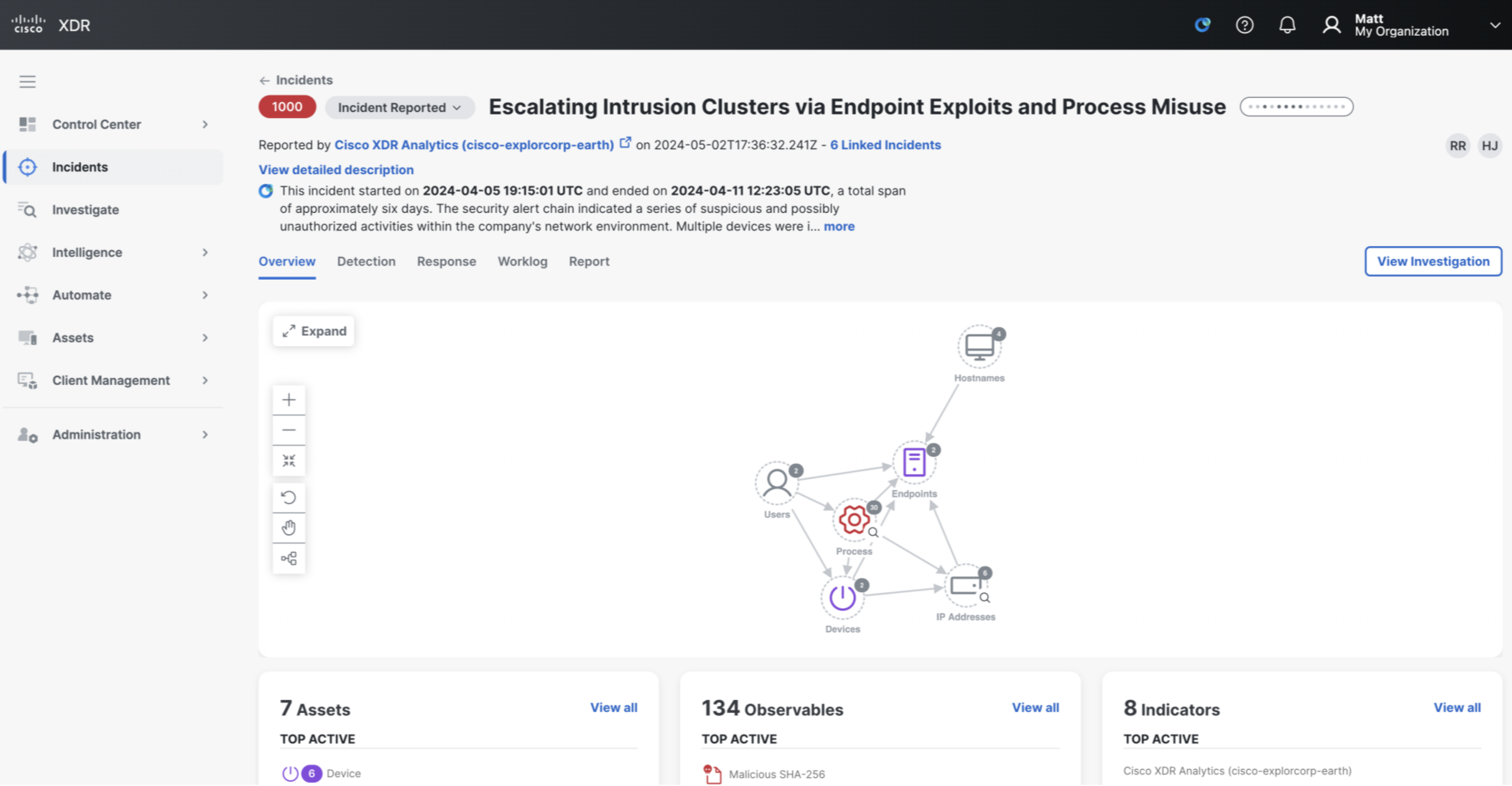
T1189: Drive-by Compromise

T1570: Lateral Tool Transfer

T1087: Account Discovery: Domain Account

T1048: System Network Connections Discovery

Vendor A	Vendor C	Vendor E	Vendor G	Vendor D



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

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

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)

Developing with XDR

Integrations

APIs

Automation

Integrations

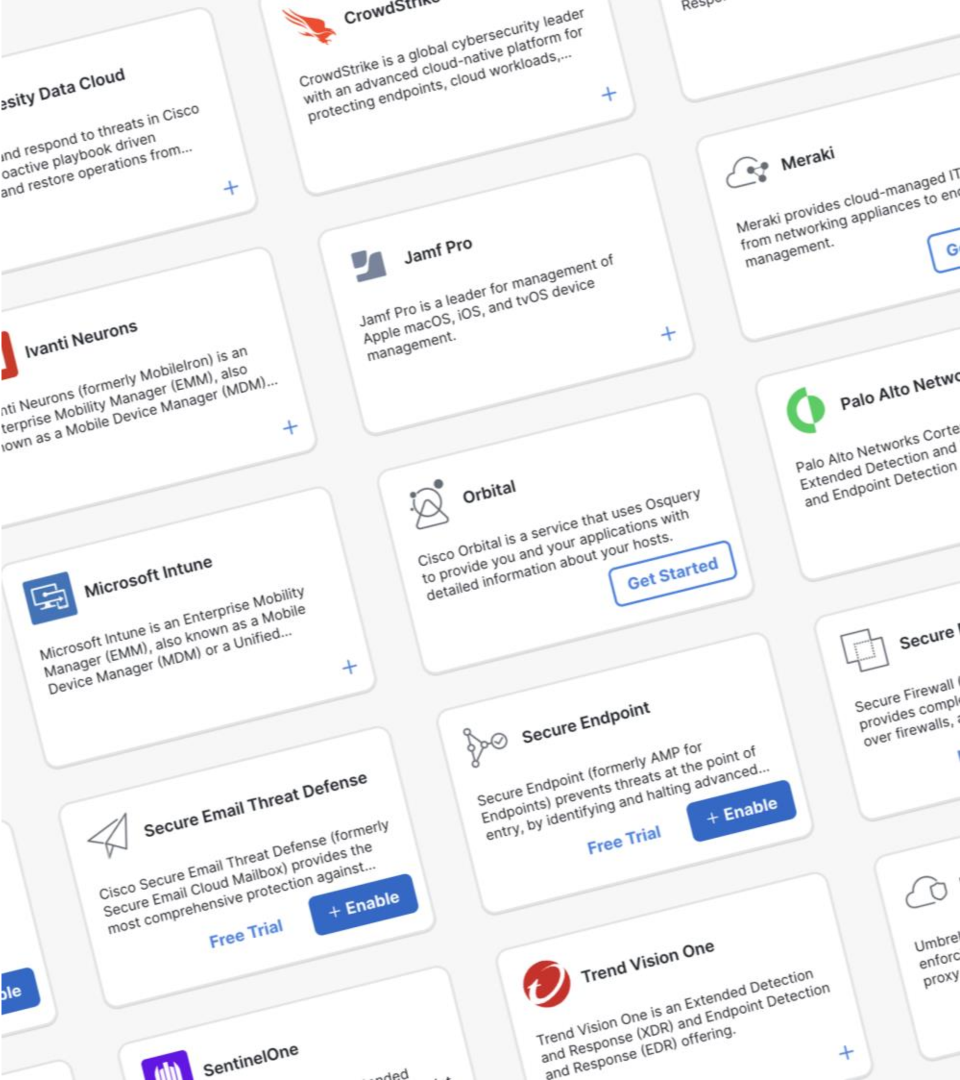
- Allow XDR to communicate with other products
  - Both Cisco and third party
- Use the Cisco Threat Intelligence Model (CTIM) to represent data
- Available by:
  - Configuring in XDR
  - Browsing Cisco's GitHub[1]
  - Writing your own[2]

[1] Some of the integration code in GitHub is outdated.

[2] Not all XDR capabilities are supported in custom integrations.

We have over 90 integrations built in

http://cs.co/9001pQZLV



esity Data Cloud

nd respond to threats in Cisco
oactive playbook driven
and restore operations from...

CrowdStrike

CrowdStrike is a global cybersecurity leader with an advanced cloud-native platform for protecting endpoints, cloud workloads,...

Respo

Ivanti Neurons

nti Neurons (formerly MobileIron) is an
terprise Mobility Manager (EMM), also
own as a Mobile Device Manager (MDM)...

Jamf Pro

Jamf Pro is a leader for management of Apple macOS, iOS, and tvOS device management.

Meraki

Meraki provides cloud-managed IT
from networking appliances to en
management.

Microsoft Intune

Microsoft Intune is an Enterprise Mobility Manager (EMM), also known as a Mobile Device Manager (MDM) or a Unified...

Orbital

Cisco Orbital is a service that uses Osquery to provide you and your applications with detailed information about your hosts.

Palo Alto Netw

Palo Alto Networks Corte
Extended Detection and
and Endpoint Detection

Secure Endpoint

Secure Endpoint (formerly AMP for Endpoints) prevents threats at the point of entry, by identifying and halting advanced...

Secure

Secure Firewall
provides compl
over firewalls,

Secure Email Threat Defense

Cisco Secure Email Threat Defense (formerly Secure Email Cloud Mailbox) provides the most comprehensive protection against...

Trend Vision One

Trend Vision One is an Extended Detection and Response (XDR) and Endpoint Detection and Response (EDR) offering.

SentinelOne

nded

Umbrel
enforc
proxy

cisco Live!

Integration capabilities

Dashboard

Deliberate

Devices

Observe Observables

Observe Targets

Refer

Respond

Users

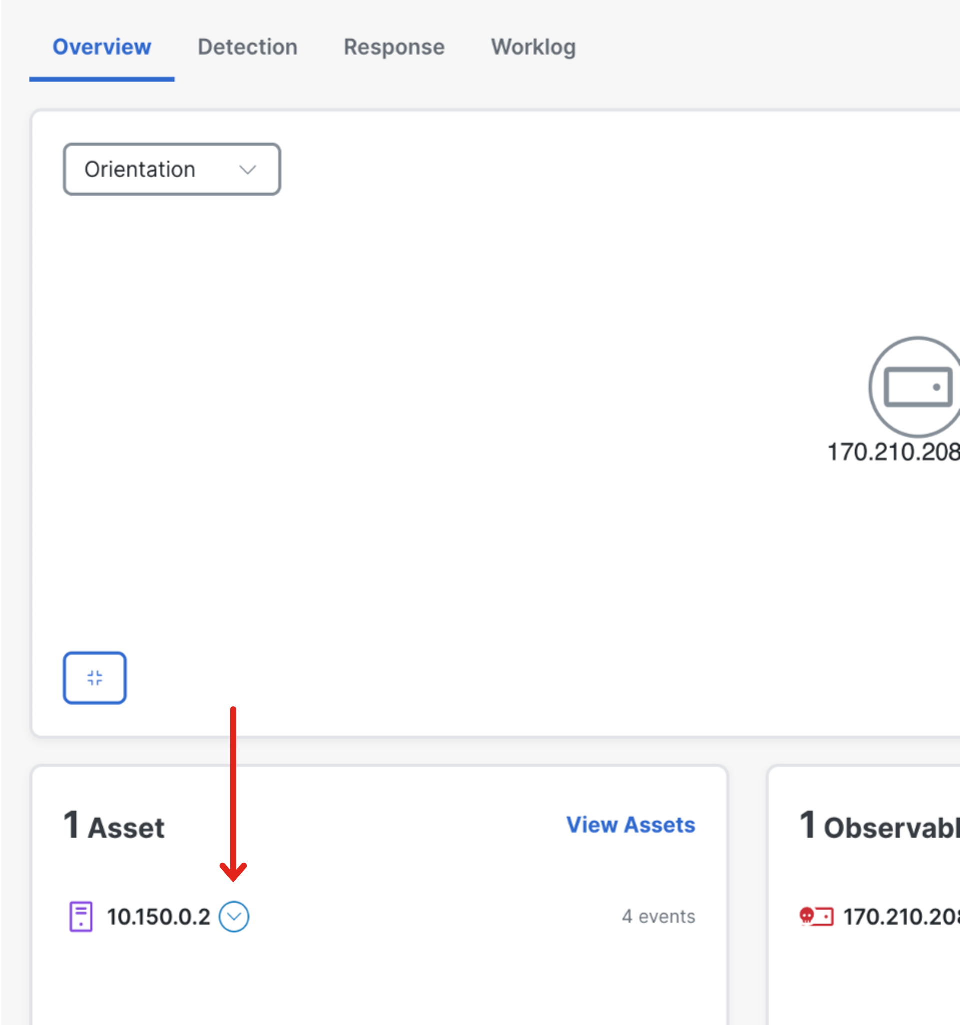
Integration capabilities

- 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

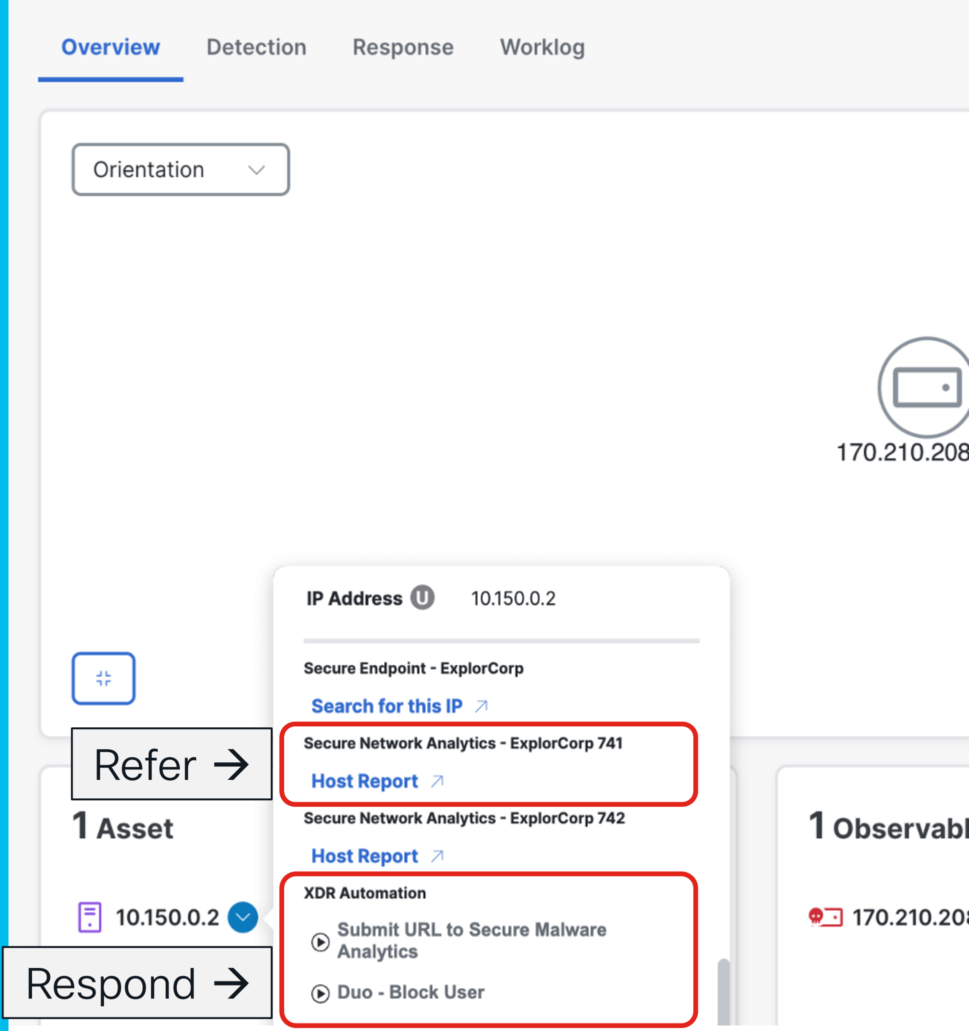
Integration capabilities

- 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?



What's a pivot menu?



IP Address U 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

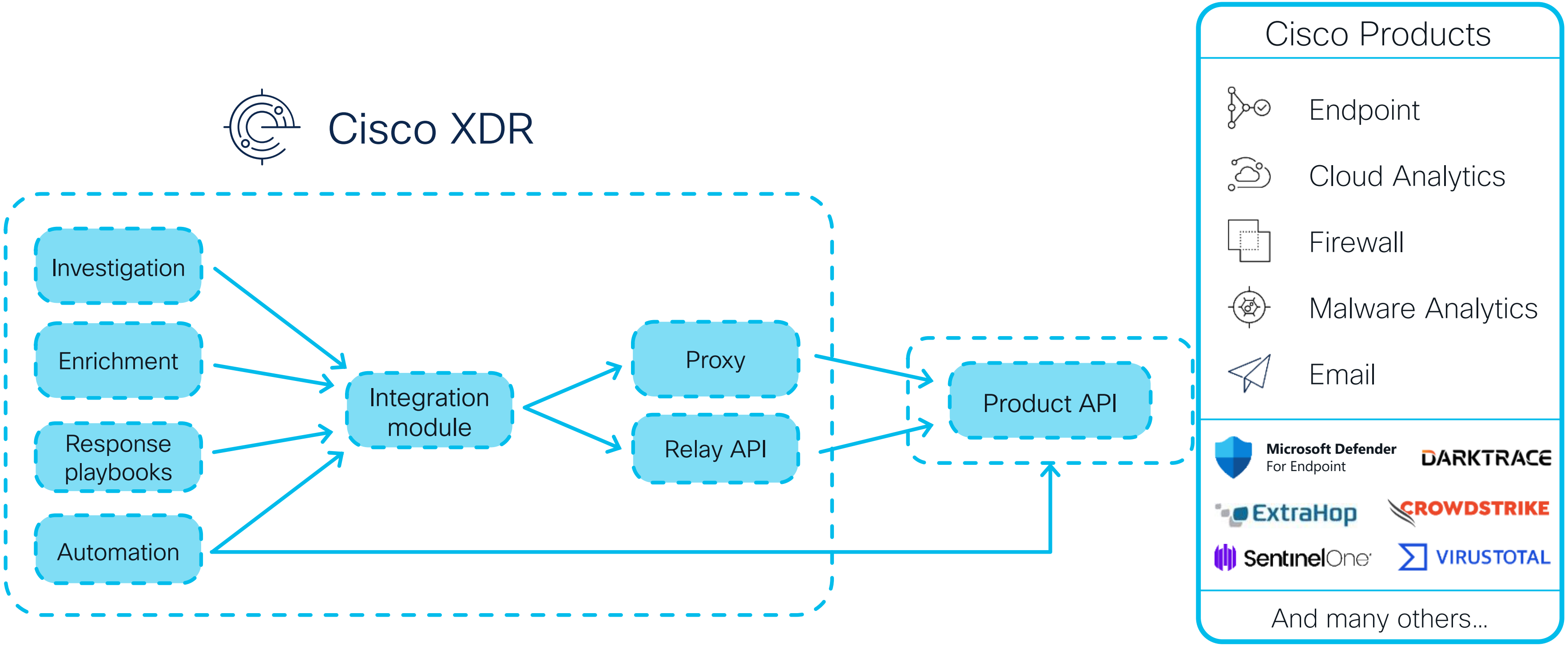
- Submit URL to Secure Malware Analytics
- Duo - Block User

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 between disparate events

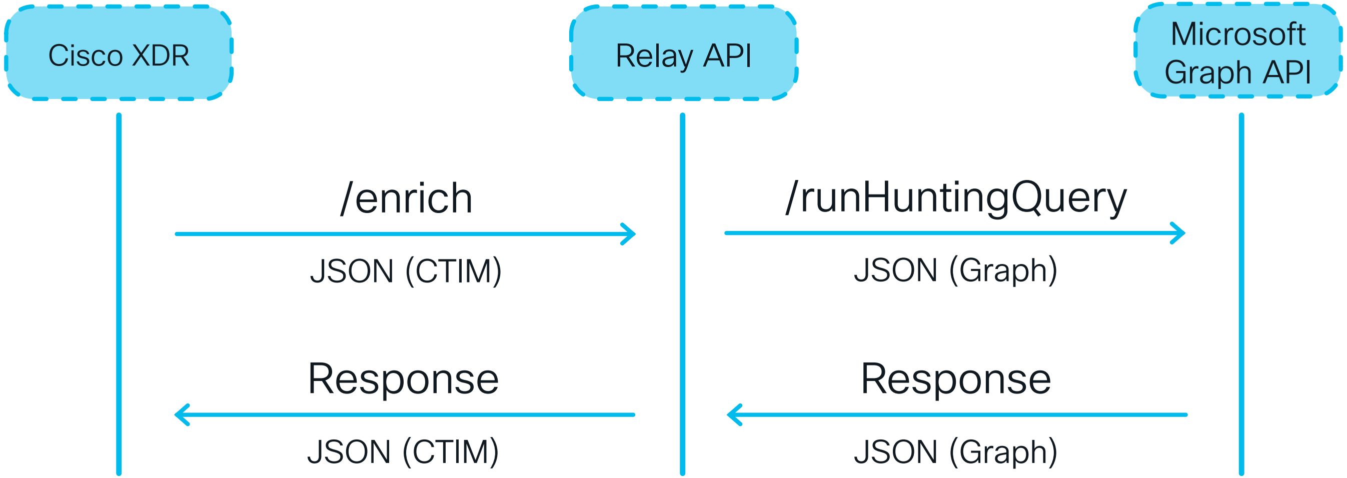
(These are the capabilities you can’t add to a custom integration)

Integration architecture



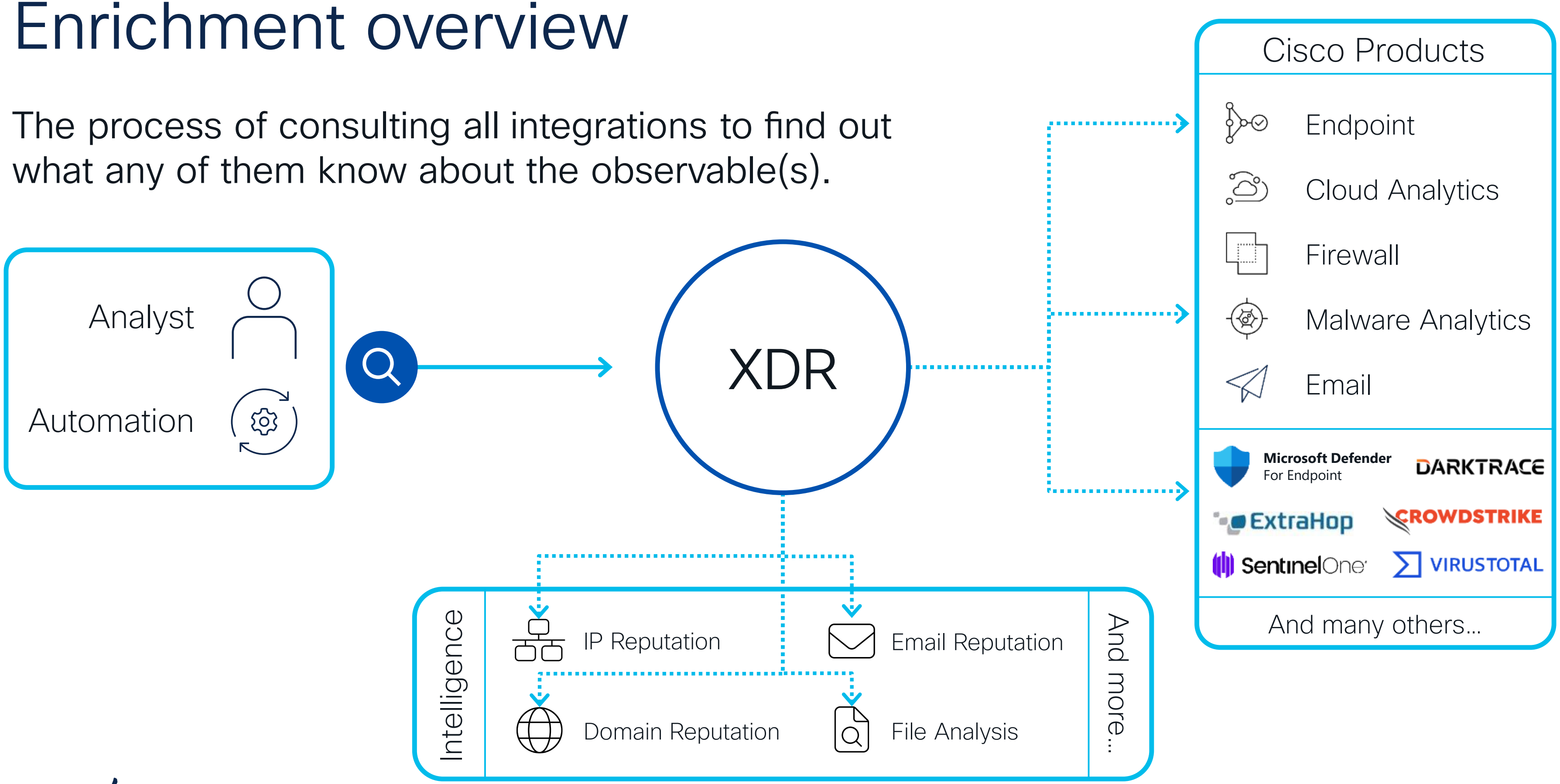
Relay APIs

- 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).



Analyst

Automation

XDR

Cisco Products

- Endpoint
- Cloud Analytics
- Firewall
- Malware Analytics
- Email

Microsoft Defender For Endpoint

DARKTRACE

ExtraHop

CROWDSTRIKE

SentinelOne

VIRUSTOTAL

And many others…

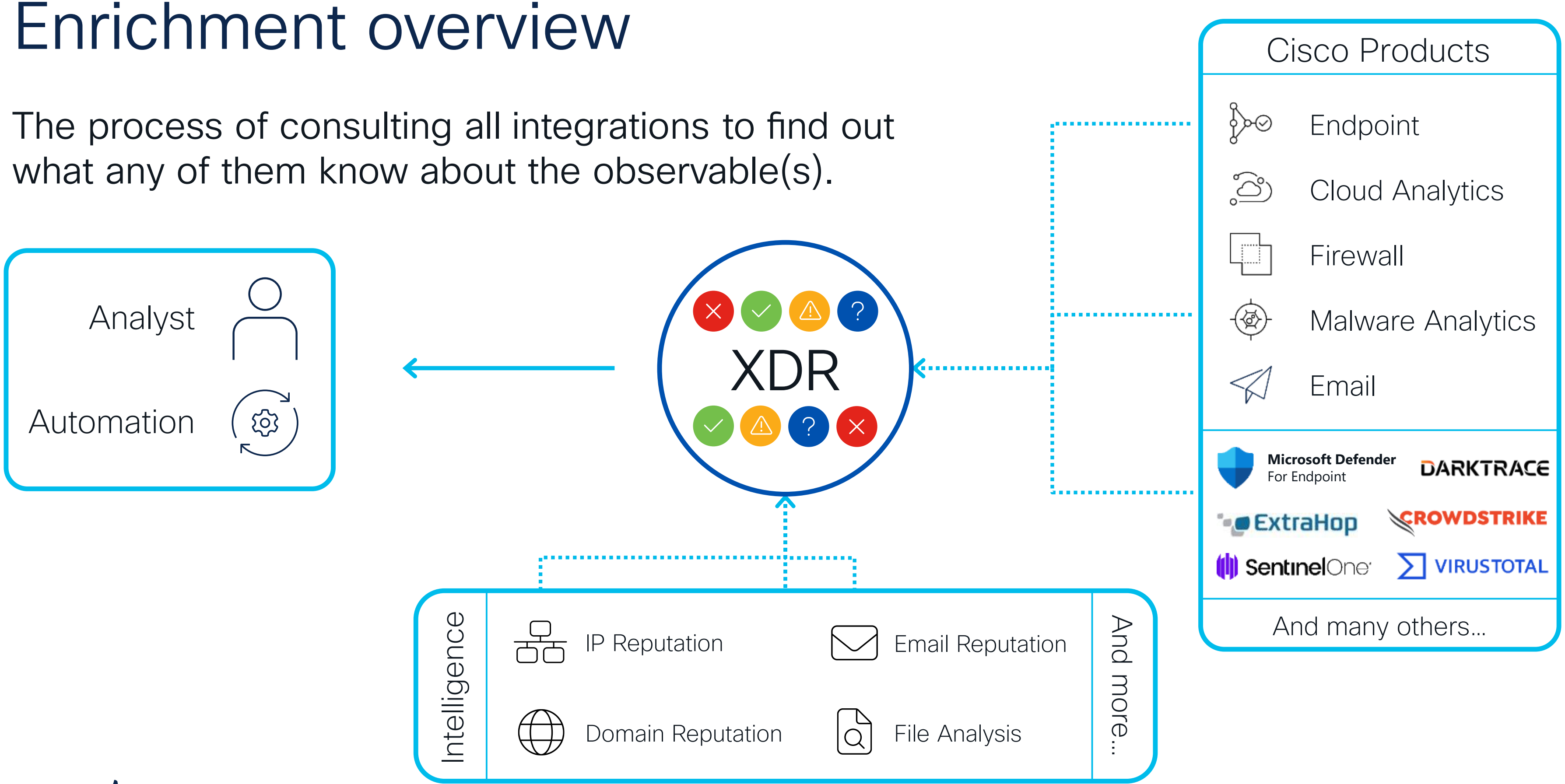
Intelligence

- IP Reputation
- Email Reputation
- Domain Reputation
- File Analysis

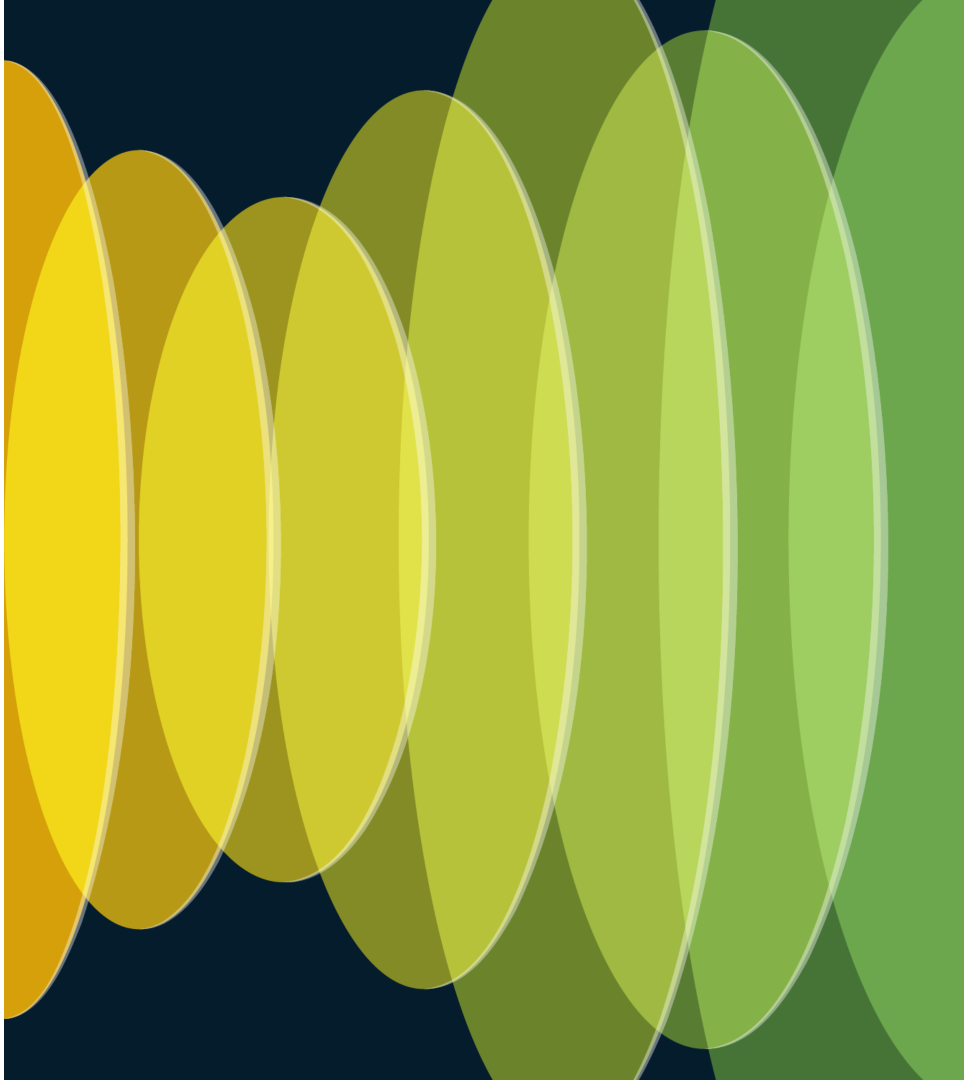
And more…

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

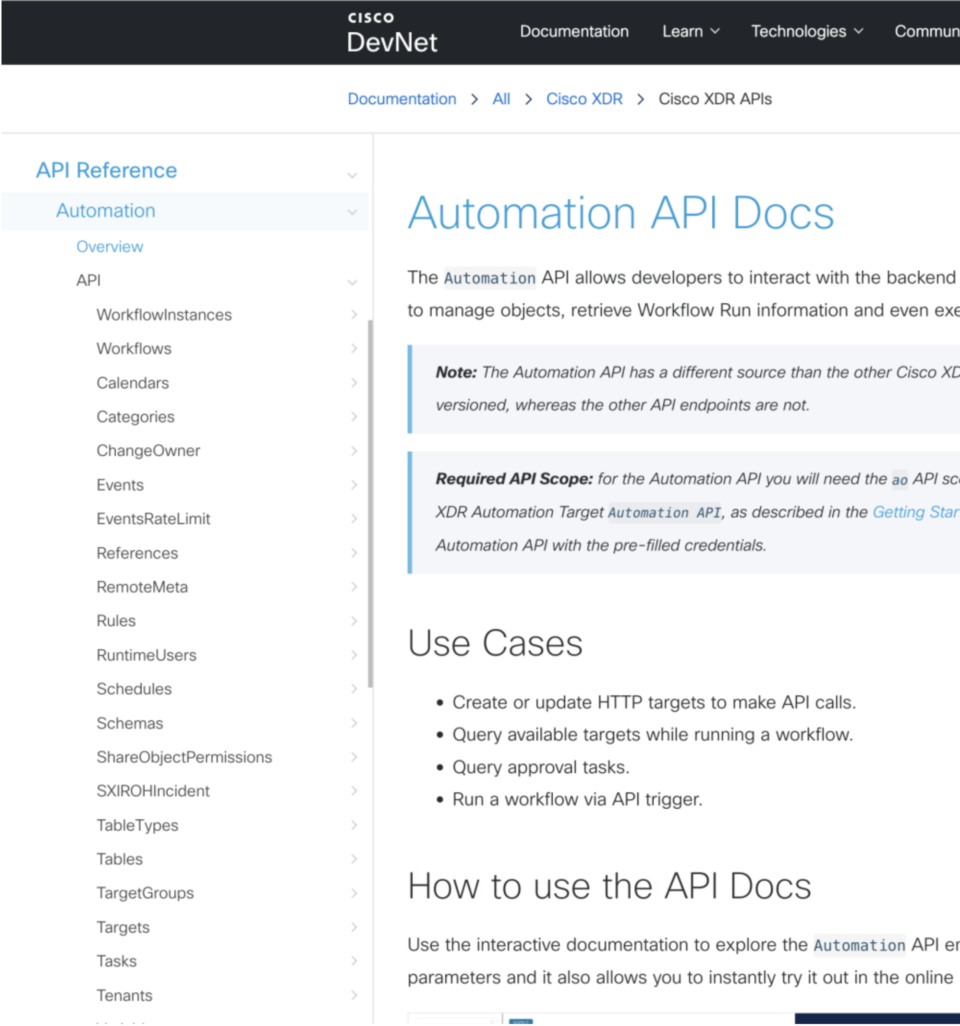
Proxy

Public Intelligence

Response

APIs: Automate

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



Automation API Docs

The `Automation` API allows developers to interact with the backend
to manage objects, retrieve Workflow Run information and even exe

> ***Note:*** *The Automation API has a different source than the other Cisco XD versioned, whereas the other API endpoints are not.*

> ***Required API Scope:*** *for the Automation API you will need the* `ao` *API sc XDR Automation Target* `Automation API`*, as described in the Getting Star Automation API with the pre-filled credentials.*

Use Cases

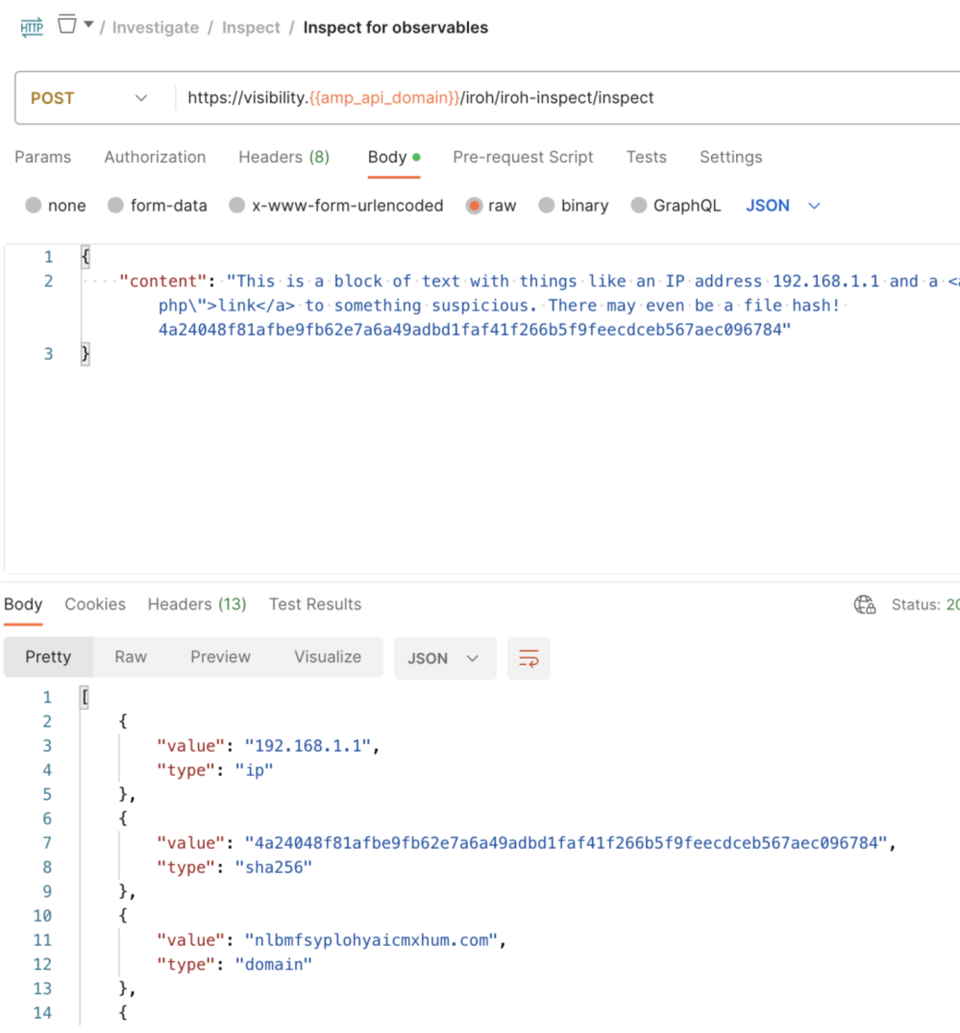
- Create or update HTTP targets to make API calls.
- Query available targets while running a workflow.
- Query approval tasks.
- Run a workflow via API trigger.

How to use the API Docs

Use the interactive documentation to explore the `Automation` API er
parameters and it also allows you to instantly try it out in the online

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…



/ Investigate / Inspect / Inspect for observables

POST https://visibility.{{amp_api_domain}}/iroh/iroh-inspect/inspect

Body: ● raw JSON

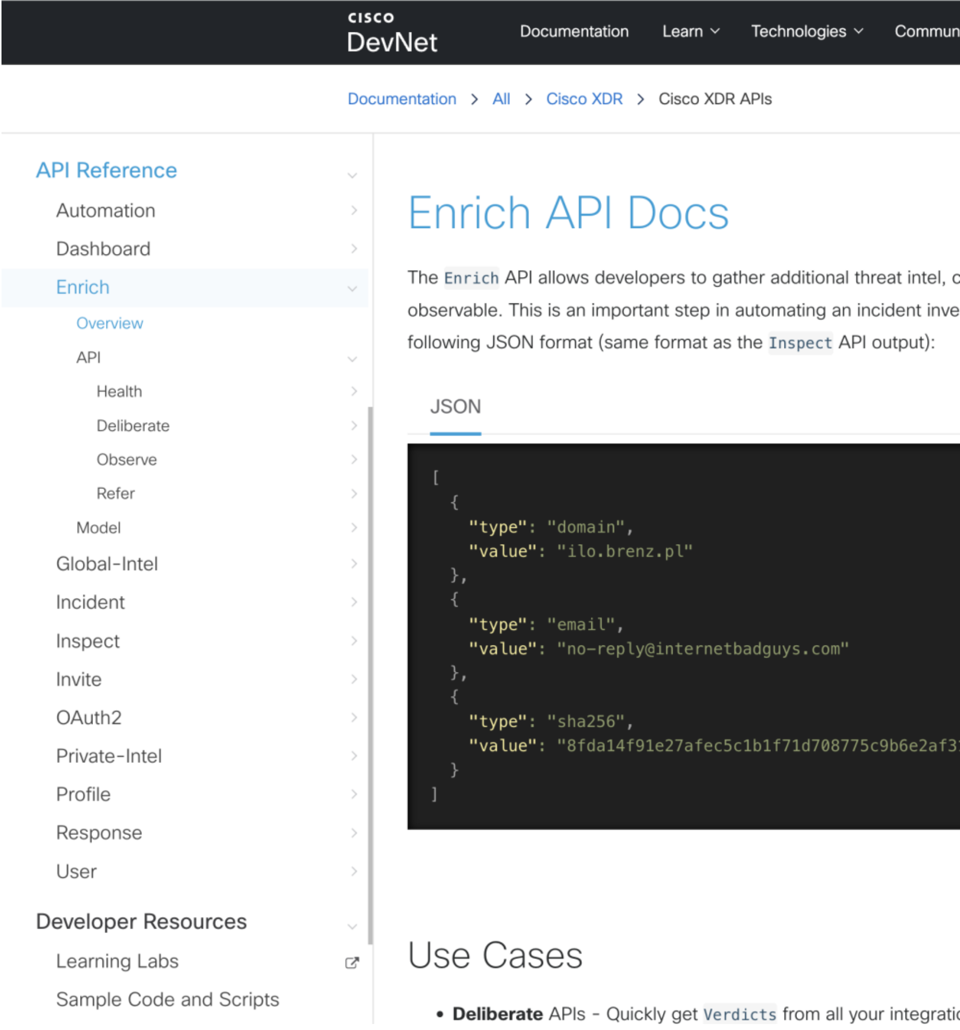
```
{
    "content": "This is a block of text with things like an IP address 192.168.1.1 and a <a
        php\">link</a> to something suspicious. There may even be a file hash!
        4a24048f81afbe9fb62e7a6a49adbd1faf41f266b5f9feecdceb567aec096784"
}
```

Body: Pretty JSON

```
[
    {
        "value": "192.168.1.1",
        "type": "ip"
    },
    {
        "value": "4a24048f81afbe9fb62e7a6a49adbd1faf41f266b5f9feecdceb567aec096784",
        "type": "sha256"
    },
    {
        "value": "nlbmfsyplohyaicmxhum.com",
        "type": "domain"
    },
    {
```

APIs: Enrich

- Uses the Cisco Threat Intelligence Model (CTIM)
- APIs:
    - Observe
    - Deliberate
    - Refer



Enrich API Docs

The `Enrich` API allows developers to gather additional threat intel, c
observable. This is an important step in automating an incident inve
following JSON format (same format as the `Inspect` API output):

```
[
  {
    "type": "domain",
    "value": "ilo.brenz.pl"
  },
  {
    "type": "email",
    "value": "no-reply@internetbadguys.com"
  },
  {
    "type": "sha256",
    "value": "8fda14f91e27afec5c1b1f71d708775c9b6e2af3
  }
]
```

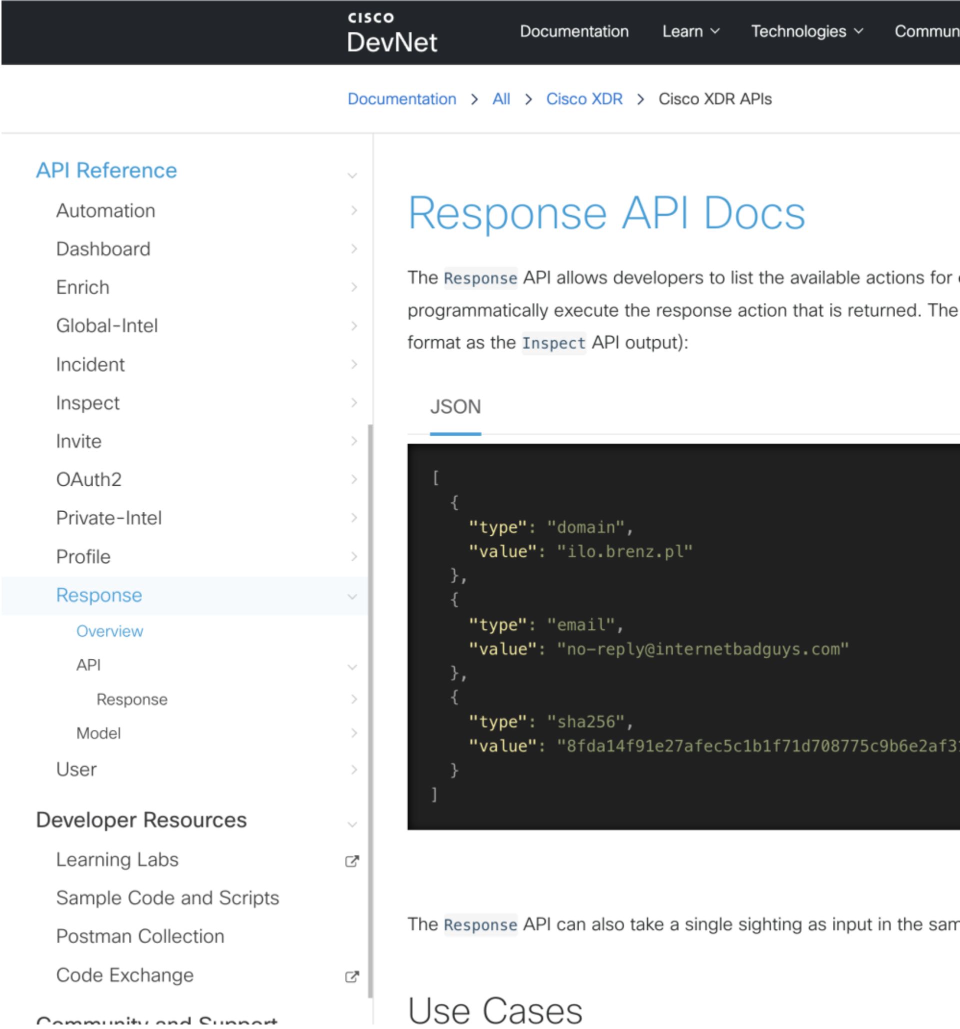
Use Cases

- **Deliberate** APIs - Quickly get `Verdicts` from all your integratio

cisco Live!

APIs: Respond

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



Response API Docs

The `Response` API allows developers to list the available actions for
programmatically execute the response action that is returned. The
format as the `Inspect` API output):

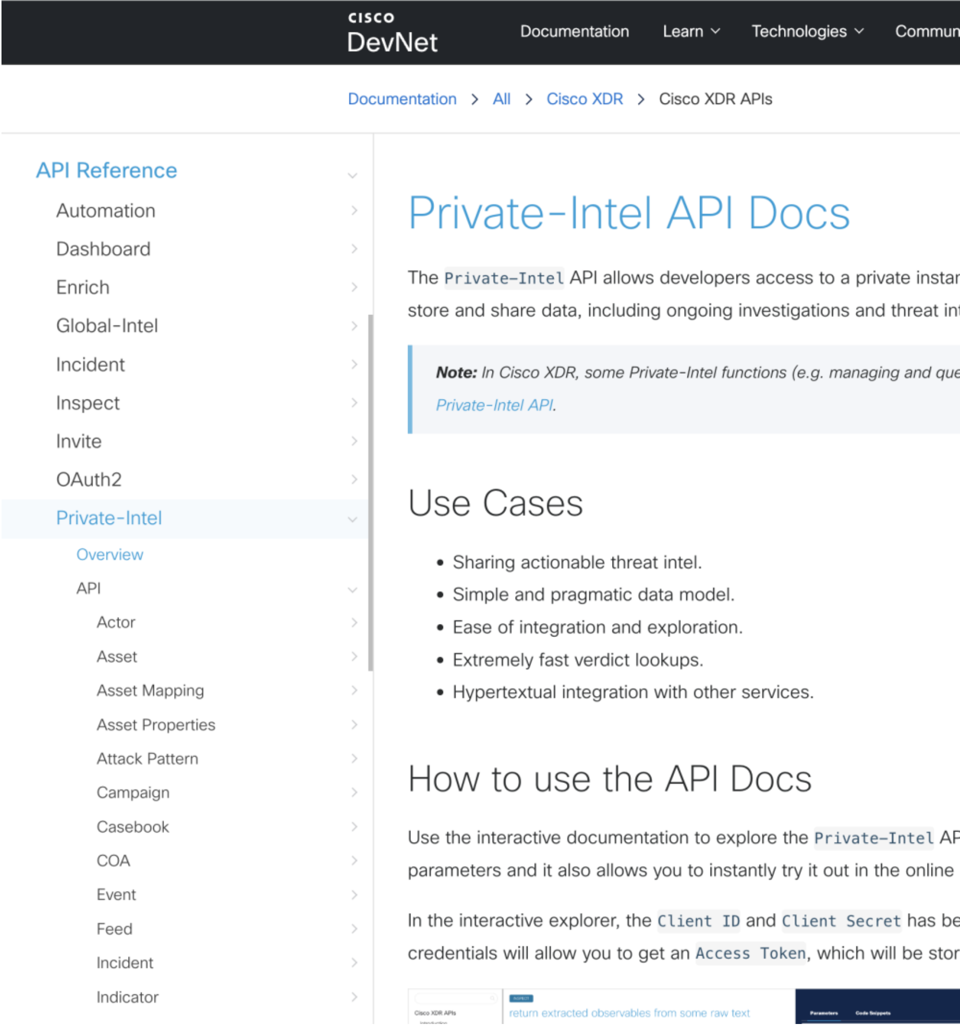
```
[
  {
    "type": "domain",
    "value": "ilo.brenz.pl"
  },
  {
    "type": "email",
    "value": "no-reply@internetbadguys.com"
  },
  {
    "type": "sha256",
    "value": "8fda14f91e27afec5c1b1f71d708775c9b6e2af3
  }
]
```

The `Response` API can also take a single sighting as input in the sam

Use Cases

APIs: Private Intelligence

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



Private-Intel API Docs

The `Private-Intel` API allows developers access to a private instar
store and share data, including ongoing investigations and threat in

> ***Note:** In Cisco XDR, some Private-Intel functions (e.g. managing and que*
> *Private-Intel API.*

Use Cases

- Sharing actionable threat intel.
- Simple and pragmatic data model.
- Ease of integration and exploration.
- Extremely fast verdict lookups.
- Hypertextual integration with other services.

How to use the API Docs

Use the interactive documentation to explore the `Private-Intel` AP
parameters and it also allows you to instantly try it out in the online

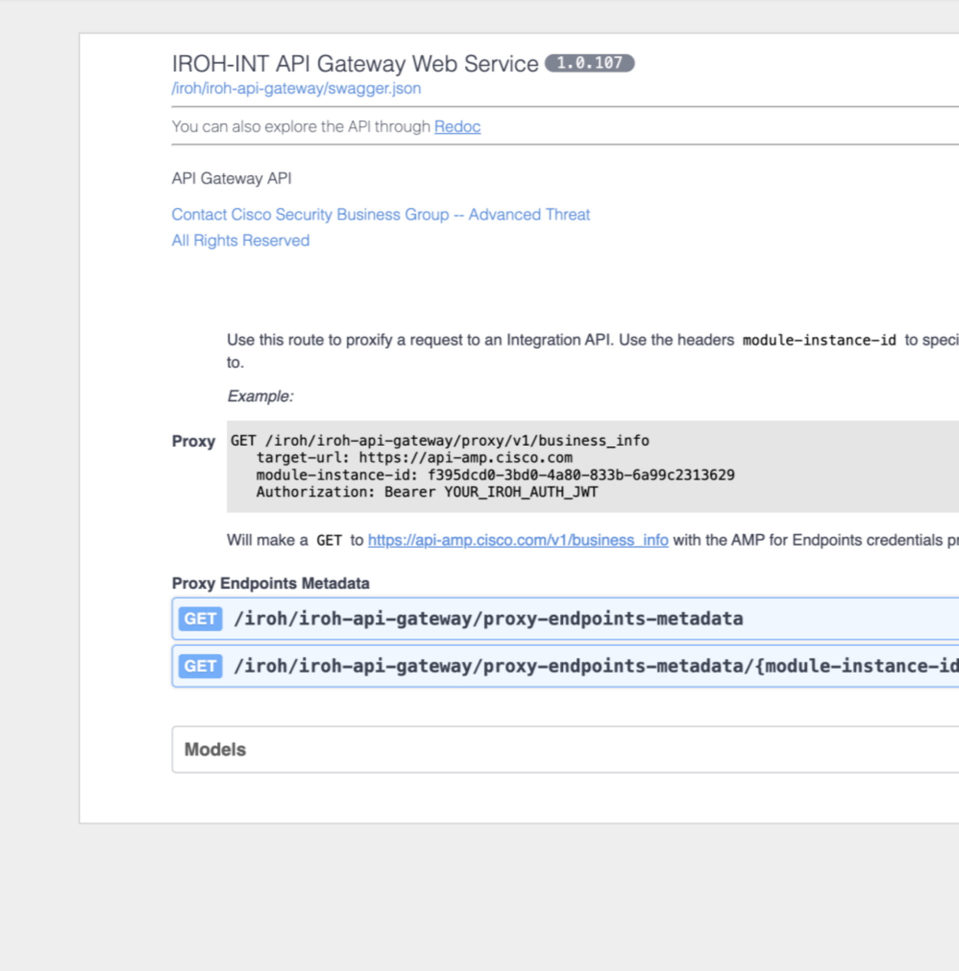
In the interactive explorer, the `Client ID` and `Client Secret` has be
credentials will allow you to get an `Access Token`, which will be stor

cisco Live!

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 API / Th



IROH-INT API Gateway Web Service

/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 proxify a request to an Integration API. Use the headers `module-instance-id` to speci
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
```

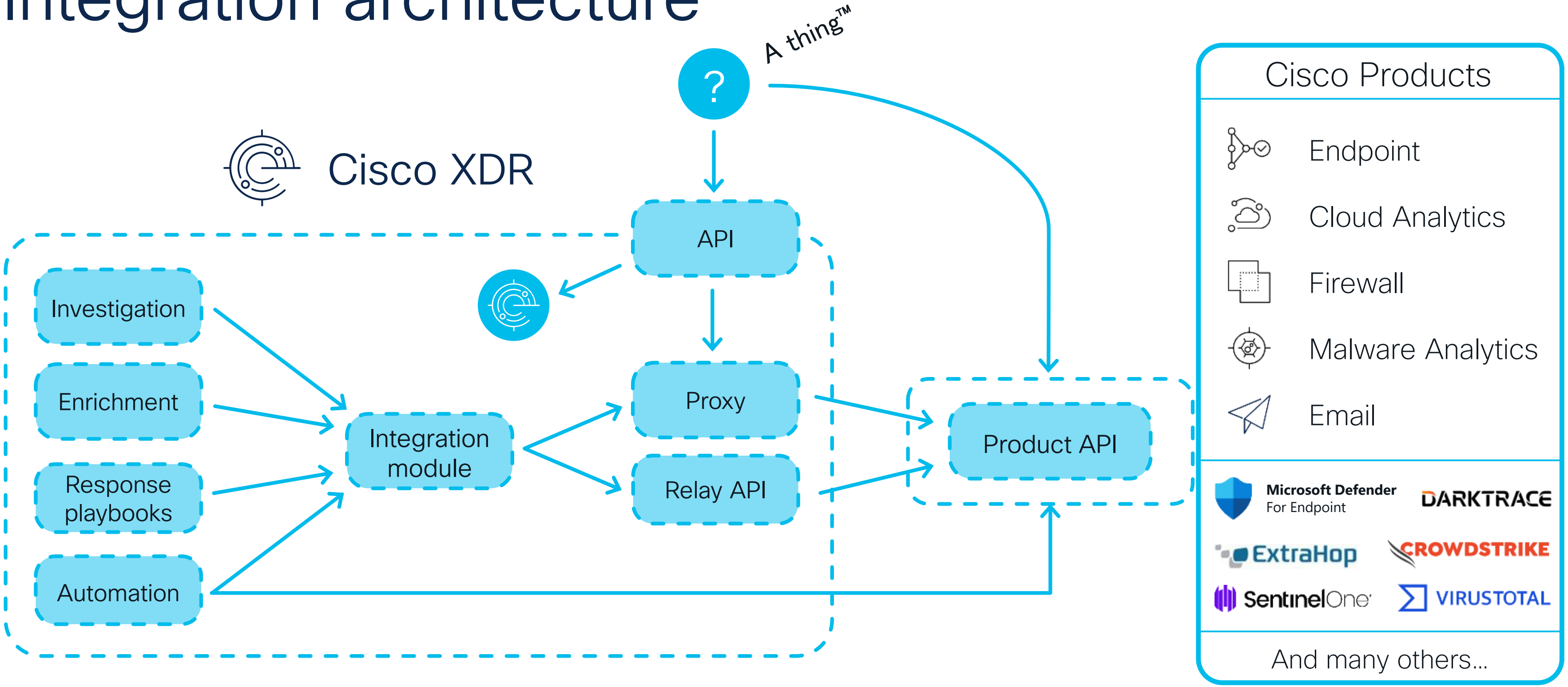
Will make a `GET` to https://api-amp.cisco.com/v1/business_info with the AMP for Endpoints credentials p

Proxy Endpoints Metadata

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

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

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

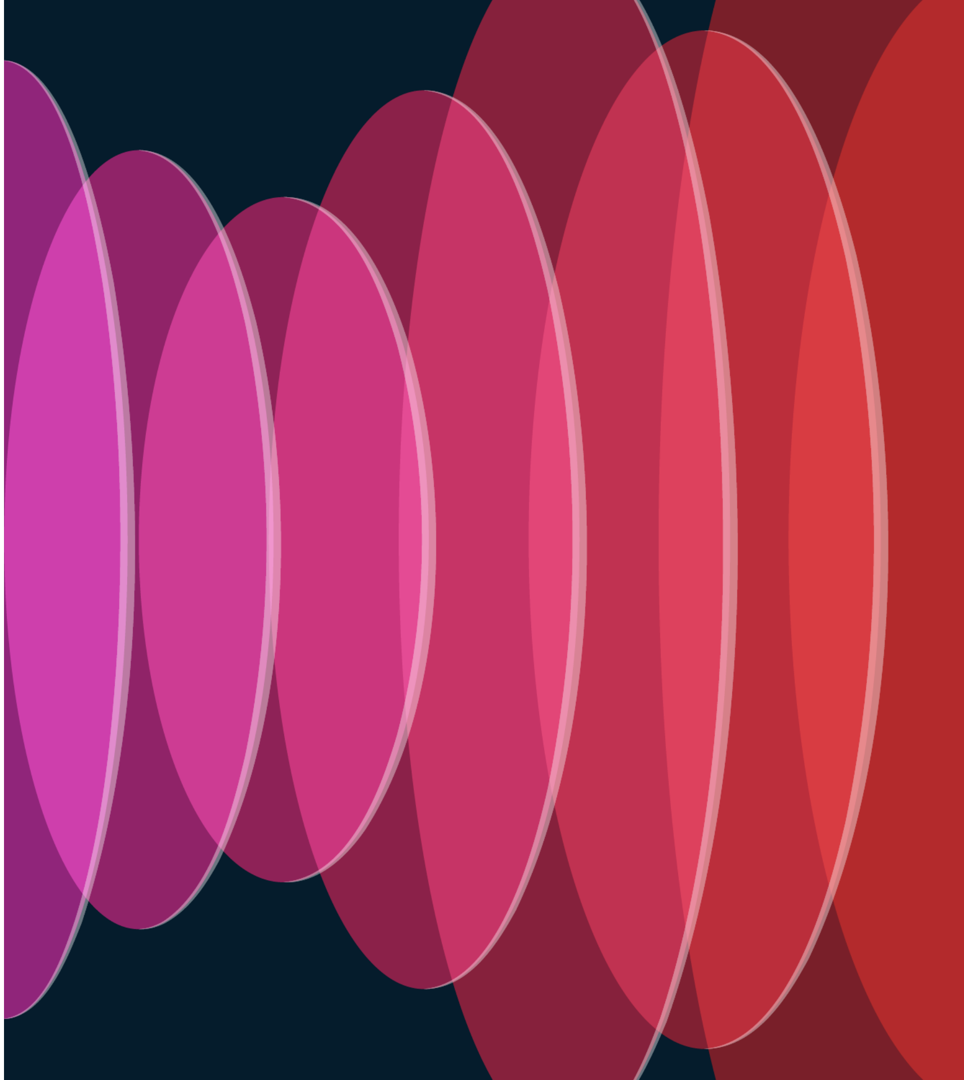
Respond

- 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

Respond

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

Investigate and Respond

Fetch IOCs

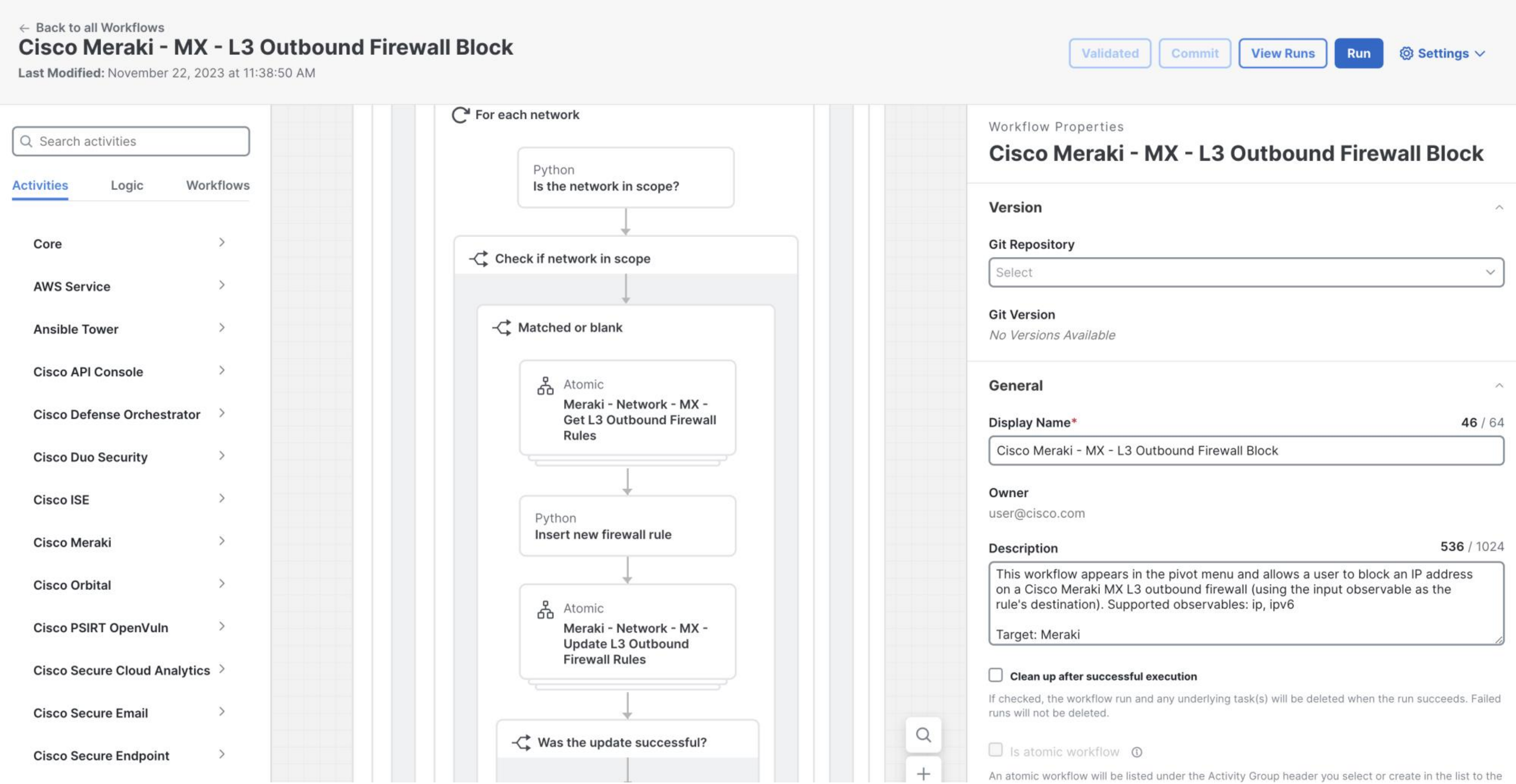
IOCs can be gathered from any number of sources including threat research websites, blogs/RSS feeds, and so on

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

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

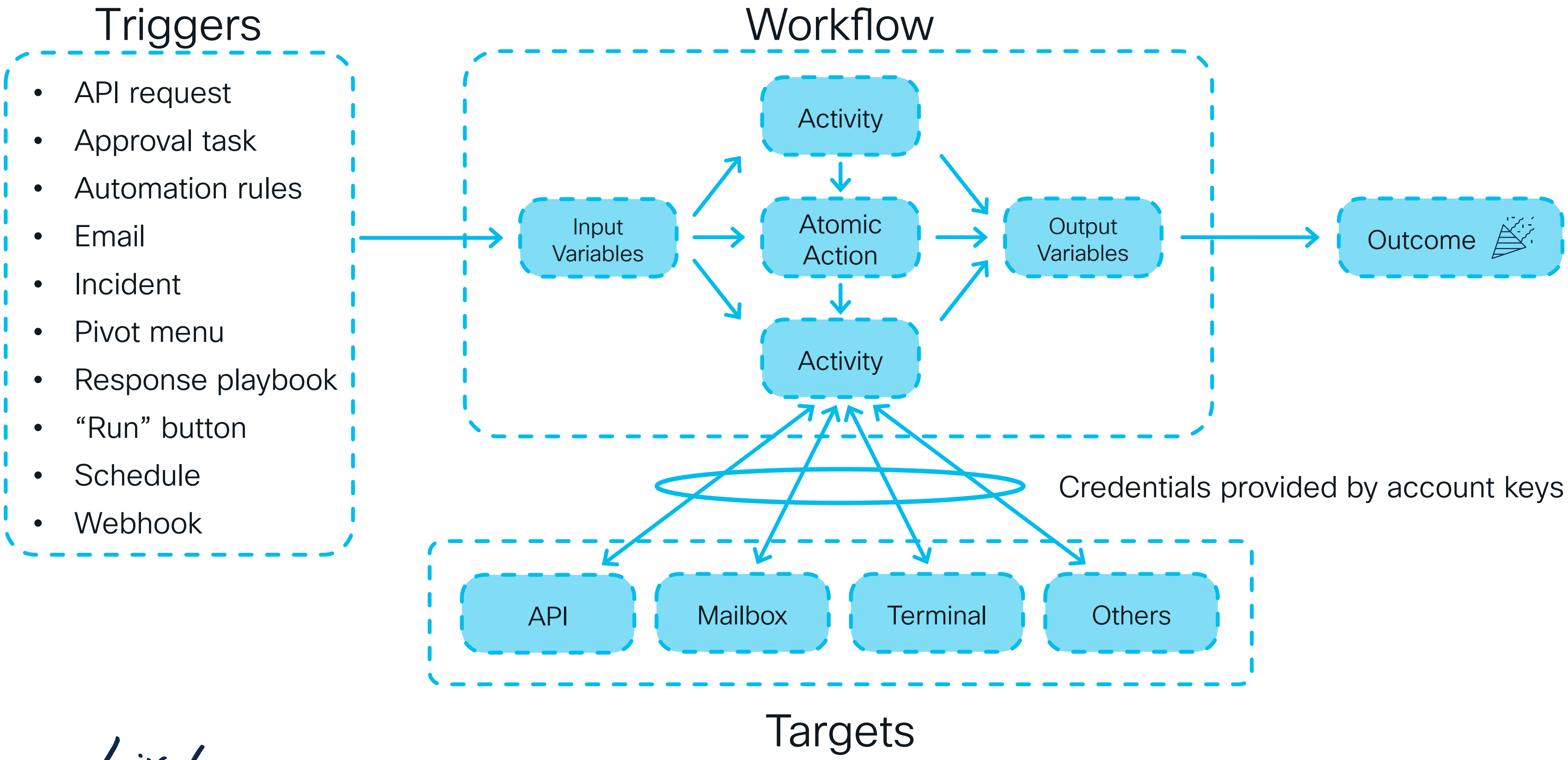
☐ **Clean up after successful execution**

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

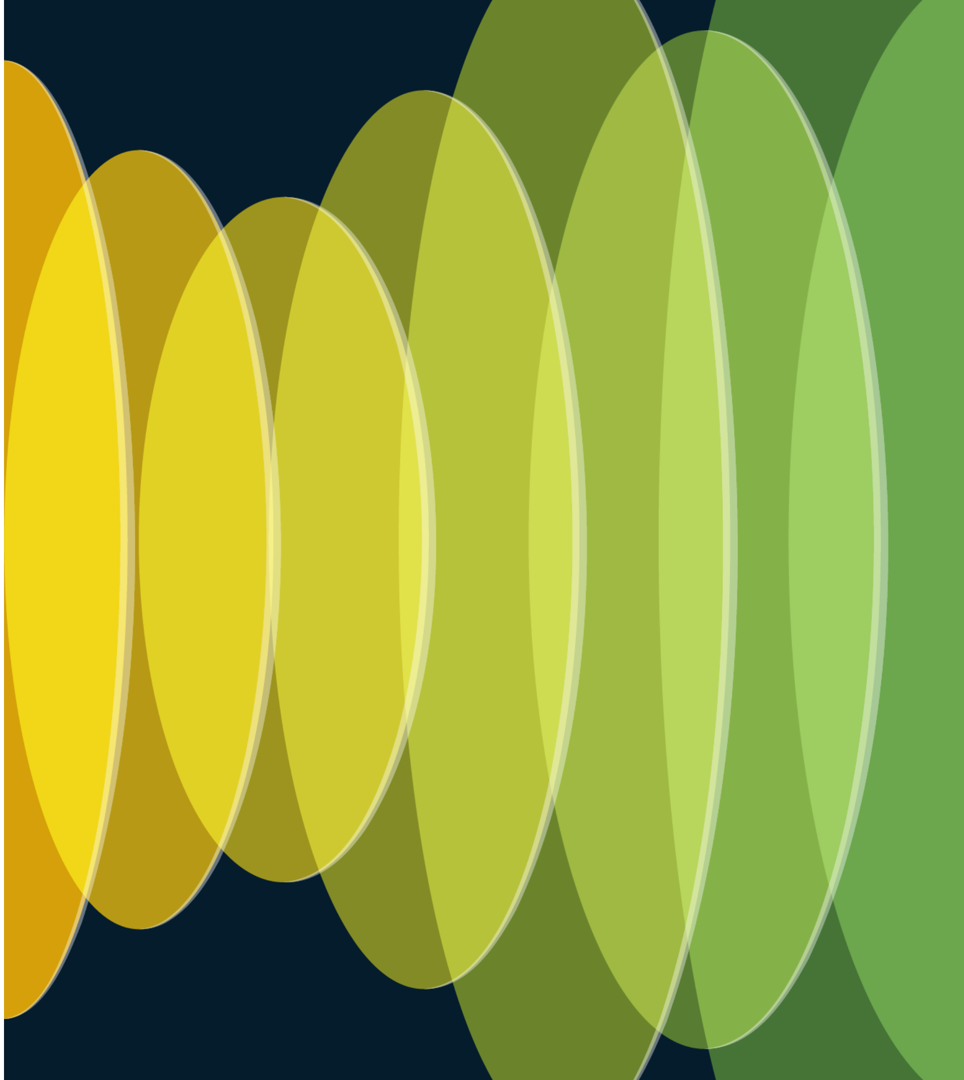
☐ Is atomic workflow ⓘ

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

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

Technical Leader

Accelerate your SOC with Cisco XDR

BRKSEC-1023

Today @ 1:00 PM

Getting started with Cisco XDR Automation workflows and atomics

DEVWKS-1190

Tomorrow @ 11:00 AM

Tomorrow @ 12:00 PM

Christopher Van Der Made

Engineering Product Manager

Incident Response With Cisco XDR: How To Level Up Your SOC Using Both Guided and Automated Response

BRKSEC-2502

Tomorrow @ 10:30 AM

Other XDR sessions

Christopher Van Der Made

Engineering Product Manager

Making the R count double in Cisco XDR: How to Automate your Security Operations (SecOps) within 10 Clicks

DEVNET-2214

Tomorrow @ 4:00 PM

Matthew Robertson

Distinguished TME

Extended Detection with Cisco XDR: Data, Analytics and Attack Chains

BRKSEC-2178

Thursday @ 11:00 AM

Aaron Woland

Distinguished TME

Cisco XDR – Making Sense of the Solution and How it's a Security Productivity Tool

BRKSEC-2113

Thursday @ 1:00 PM

Complete Your Session Evaluations

Complete a minimum of 4 session surveys and the Overall Event Survey to be entered in a drawing to **win 1 of 5 full conference passes** to Cisco Live 2025.

Earn 100 points per survey completed and compete on the Cisco Live Challenge leaderboard.

Level up and earn **exclusive prizes!**

Complete your surveys in the **Cisco Live mobile app.**

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

#CiscoLive

Continue your learning journey after the event with Cisco DevNet!

→ Personalized learning modules

→ Live interactive tooling

→ Other resources

Scan to get started