



The bridge to possible

Incident Response with Cisco XDR

How to level up your SOC using both Guided
and Automated Response

Christopher van der Made
Leader, Engineering Product Management - Cisco XDR

BRKSEC-2502

CISCO *Live!*

#CiscoLive

Cisco Webex App

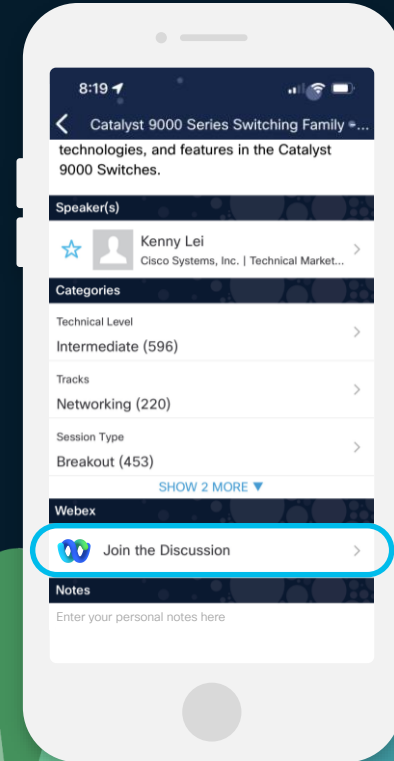
Questions?

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.





Continue your education

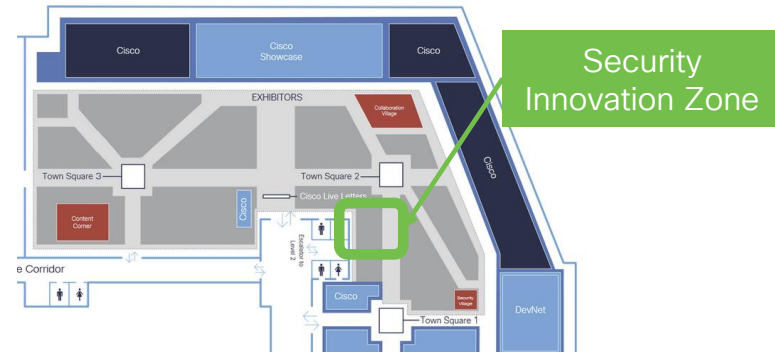
CISCO Live!

- Hear Tom Gillis at the Security Deep Dive Keynote KDDSEC-1000!

*Securing User to Application and
Everything in Between*

Wednesday, June 5 | 1 – 2pm

- Visit us at the Security Innovation Zone (#4435) for demos and workshops



Setting expectations...



Not an intro
to Cisco XDR



Reference
slides



Hidden slides
in PDF



Subject to
changes



Please ask
questions!



Webex Q&A



Workflows
available

whoami

- Christopher van der Made
- Half Dutch, Half American, living in Rotterdam (NL)
- Studied at University of Amsterdam (NL):
 - Major: Neuroscience, Minor: Computer Science
 - Masters: Information Science
- “Born and raised” in Cisco:
 - Joined Cisco’s graduate program in 2015 as Associate Systems Engineer
 - Consulting Systems Engineer for Security in Northern Europe team from 2016–2020
 - Developer Advocate for Security in Developer Relations team (Cisco DevNet) from 2020–2022
 - Engineering Product Manager for Cisco XDR (and SecureX), with focus on Automation from 2022 and onwards...
 - Hobbies: coding, brewing&drinking, cooking&eating, board sports.



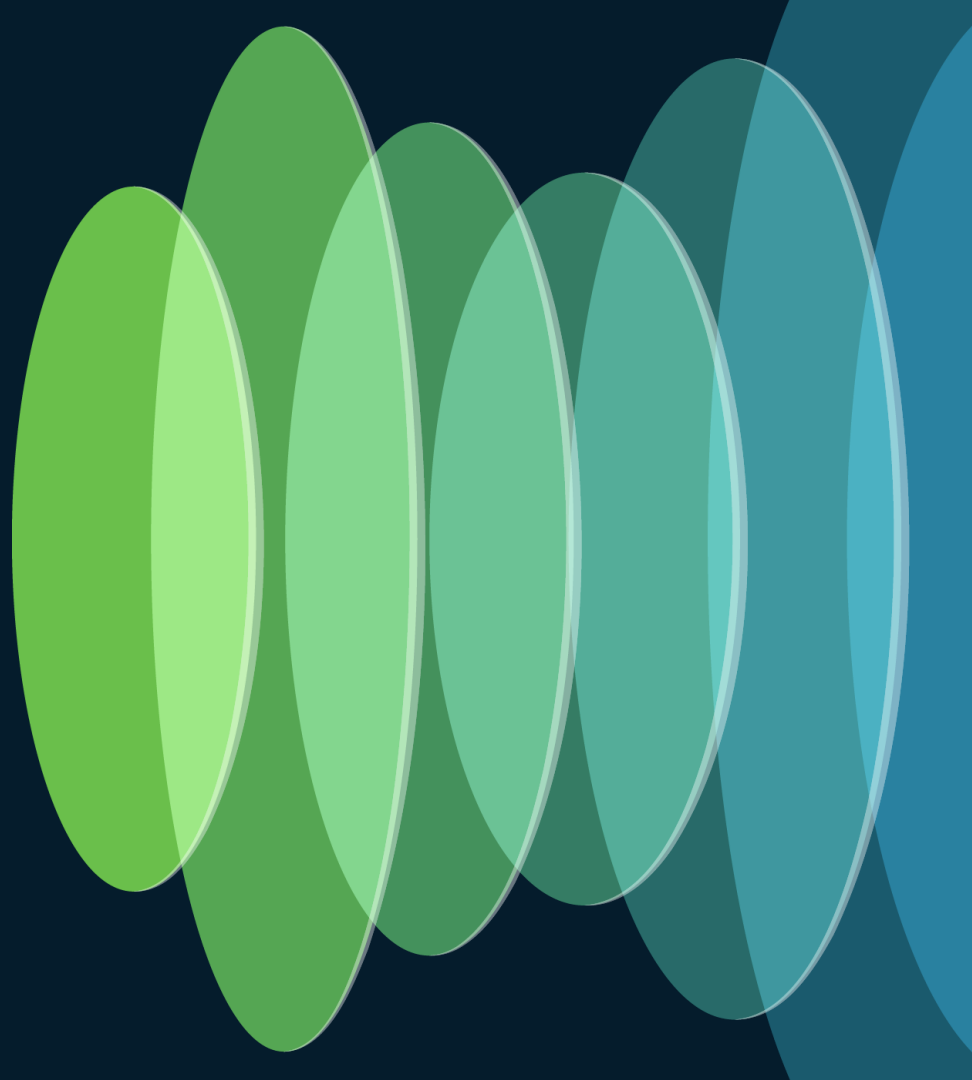
Agenda

- What is Incident Response?
- How to perform Incident Response with Cisco XDR?
 - Introduction to Cisco XDR (Automation)
 - Pivot Menu
 - Playbook Tasks
 - Automation Rules
- Let's put it to practice!
- Future?

Agenda

- What is Incident Response?
- How to perform Incident Response with Cisco XDR?
 - Introduction to Cisco XDR (Automation)
 - Pivot Menu
 - Playbook Tasks
 - Automation Rules
- Let's put it to practice!
- Future?

What is Incident Response?





Detection

Find indicators of activity based on intelligence and generate a detection. Correlate detection(s) into an alerts.



Response

*Validate detection(s) and intelligence, **confirm incident**, then contain and eradicate the threat on affected systems.*



Recovery

Restore the affected systems back to “business as usual”. Create report.



Detection

Find indicators of activity based on intelligence and generate a detection. Correlate detection(s) into an alerts.



Response

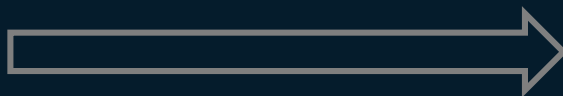
*Validate detection(s) and intelligence, **confirm incident**, then contain and eradicate the threat on affected systems.*



Recovery

Restore the affected systems back to “business as usual”. Create Incident report.

MITRE



PICERL

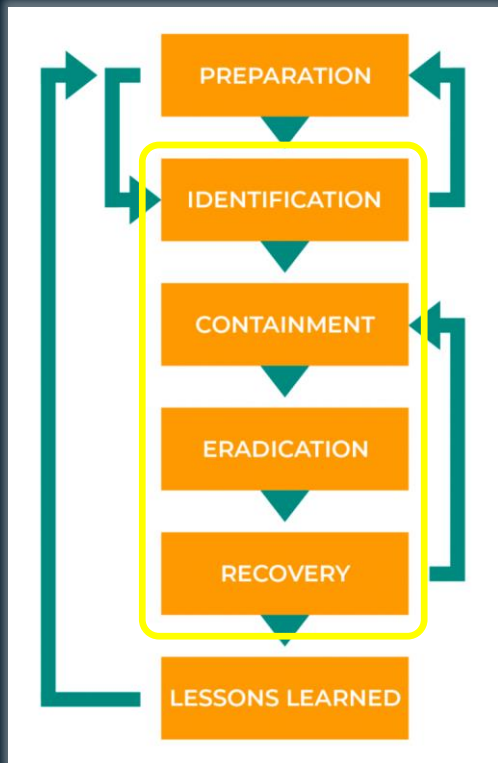
Preparation, Identification, Containment, Eradication, Recovery, Lessons Learned

**ATT&CK,
DeTT&CT**

D3FEND

RE&CT

CISCO *Live!*



REACT Enterprise Matrix

Preparation	Identification	Containment	Eradiation	Recovery	Lessons Learned
102 Items	63 Items	26 Items	8 Items	14 Items	2 Items
Practice	List victims of security alert	Patch vulnerability	Report incident to external companies	Reinstall host from golden image	Develop incident report
Take trainings	List host vulnerabilities	Block external IP address	Remove rogue network device	Restore data from backup	Conduct lessons learned exercise
Raise personnel awareness	Put compromised accounts on monitoring	Block internal IP address	Delete email message	Unblock blocked IP	
Make personnel report suspicious activity	List hosts communicated with internal domain	Block external domain	Remove file	Unblock blocked domain	
Set up relevant data collection	List hosts communicated with internal IP	Block internal domain	Remove registry key	Unblock blocked URL	
Set up a centralized long-term log storage	List hosts communicated with internal URL	Block external URL	Remove service	Unblock blocked port	
Develop communication map	Analyze domain name	Block internal URL	Revoke authentication credentials	Unblock blocked user	
Make sure there are backups	Analyze IP	Block port external communication	Remove user account	Unblock domain on email	
Get network architecture map	Analyze url	Block port internal communication		Unblock sender on email	
Get access control matrix	List hosts communicated by port	Block user external communication		Restore quarantined email message	
Develop assets knowledge base	List hosts connected to VPN	Block user internal communication		Restore quarantined file	
Check analysis toolset	List hosts connected to intranet	Block data transferring by content pattern		Unblock blocked process	
Access vulnerability management system logs	List data transferred	Block domain on email		Enable disabled service	
Connect with trusted communities	Collect transferred data	Block sender on email		Unblock locked user account	
Access external network flow logs	Identify transferred data	Quarantine email message			
Access internal network flow logs	List hosts communicated with external domain	Quarantine file by format			
Access internal HTTP logs	List hosts communicated with external IP	Quarantine file by hash			
Access external HTTP logs	List hosts communicated with external URL	Quarantine file by path			
Access internal DNS logs	Find data transferred by content pattern	Quarantine file by content pattern			
Access external DNS logs	Analyze user-agent	Block process by executable path			
Access VPN logs	List Firewall rules	Block process by executable metadata			
Access DHCP logs	List users opened email message	Block process by executable hash			
Access internal packet capture data	Collect email message	Block process by executable format			
Access external packet capture data	List email message receivers	Block process by executable content pattern			
Get ability to block external IP address	Make sure email message is phishing	Disable system service			
Get ability to block internal IP address	Extract observable from email message	Lock user account			
Get ability to block external domain	Analyze email address				
Get ability to block internal domain	List files created				
Get ability to block external URL	List files modified				
Get ability to block internal URL	List files deleted				
Get ability to block port external communication	List files downloaded				

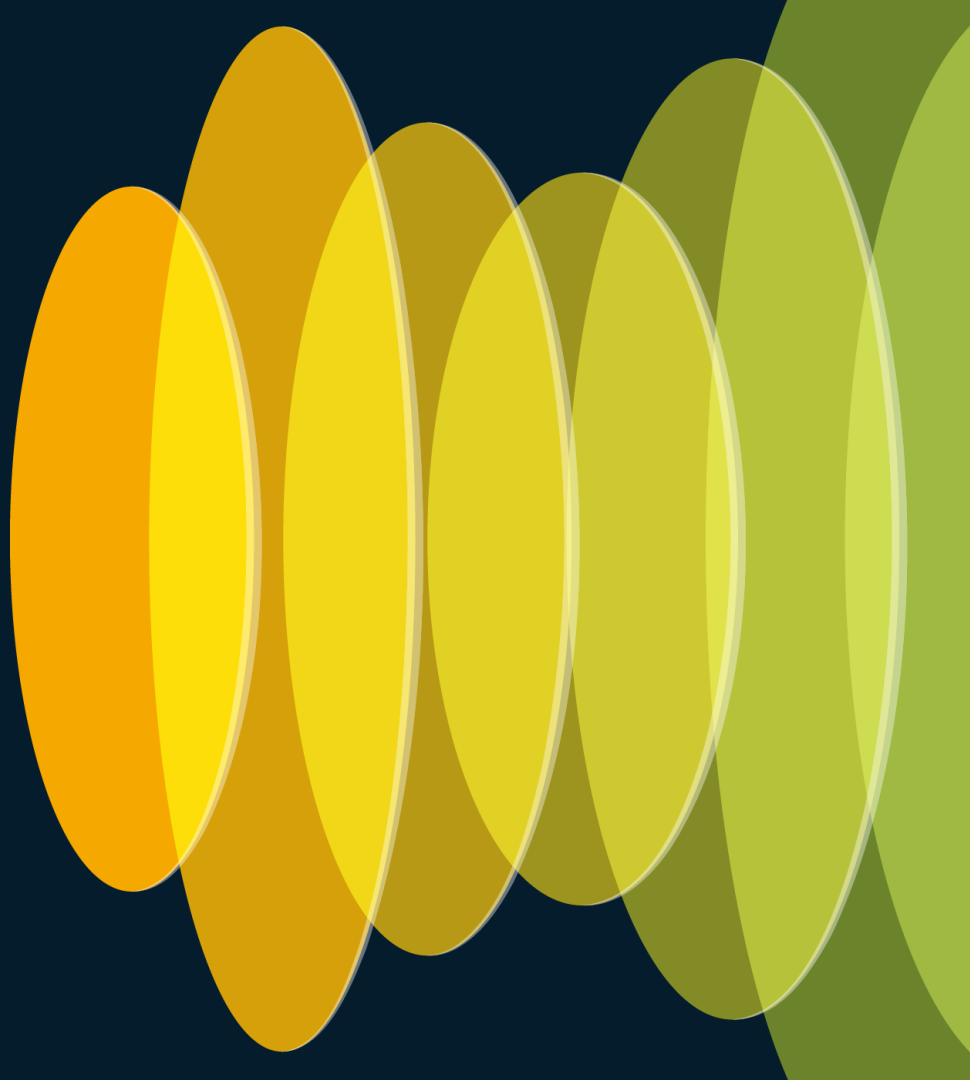
Legend:

- #FFD300 General category
- #FFC300 Network category
- #FFC300 Email category
- #FFC300 File category
- #FFC300 Process category
- #FFC300 Configuration category
- #FFC300 Identity category

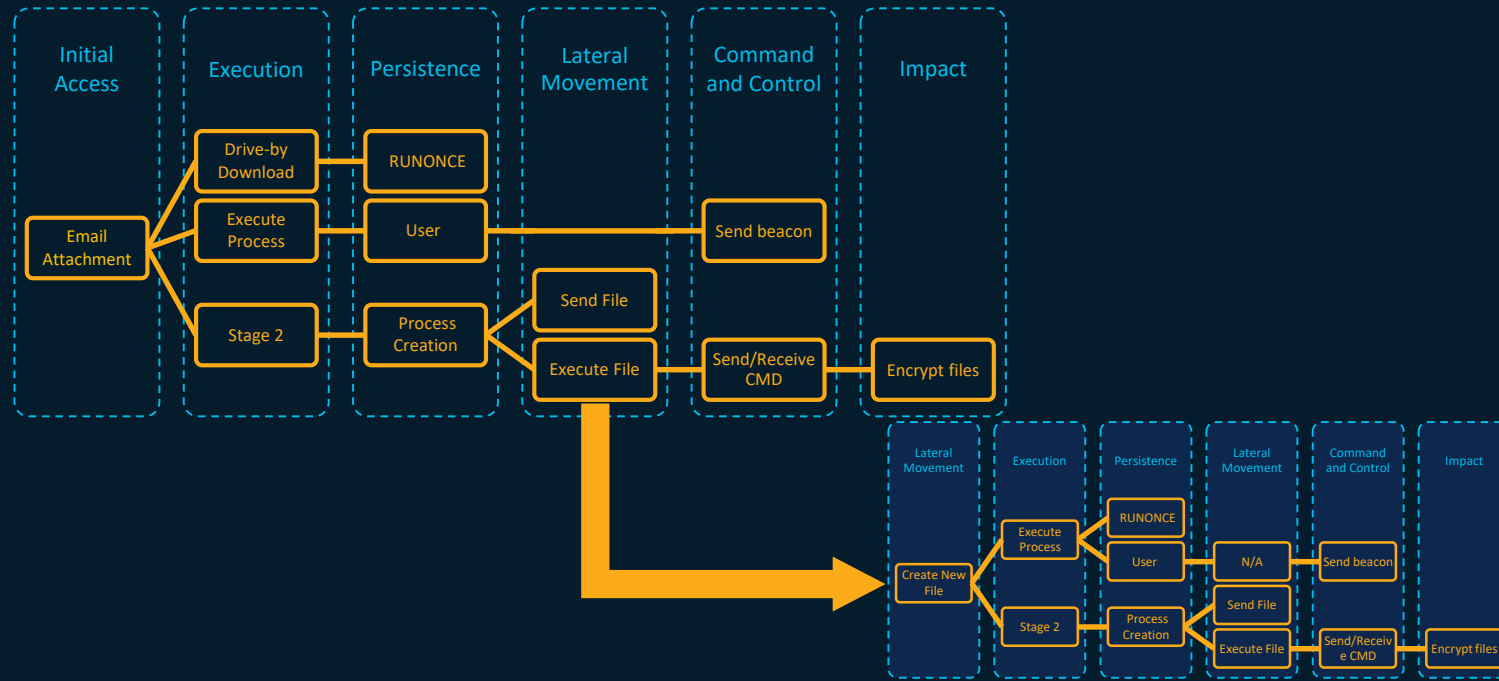
<https://www.sans.org/media/score/504-incident-response-cycle.pdf>

<https://atc-project.github.io/react-navigator/>

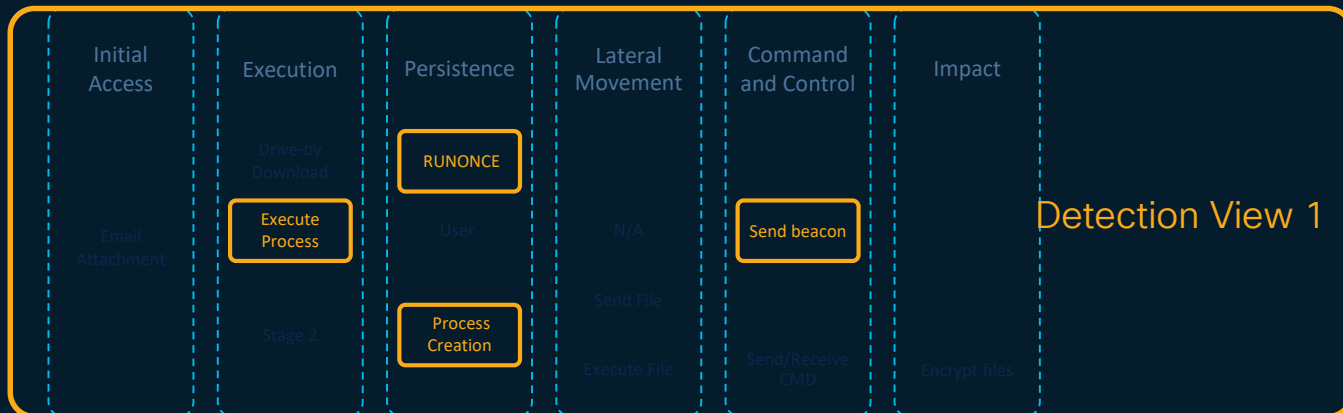
An example Incident Response use case



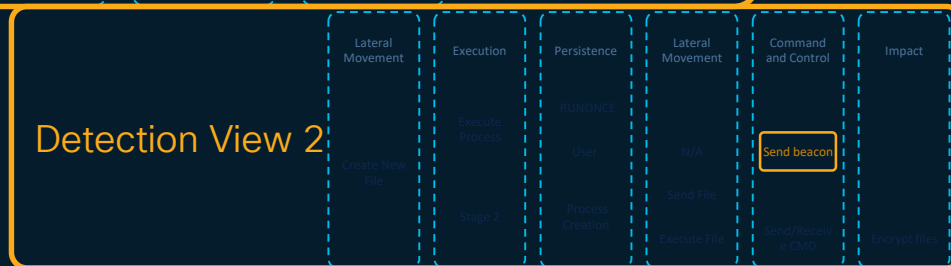
Example Use Case: Ransomware Attack



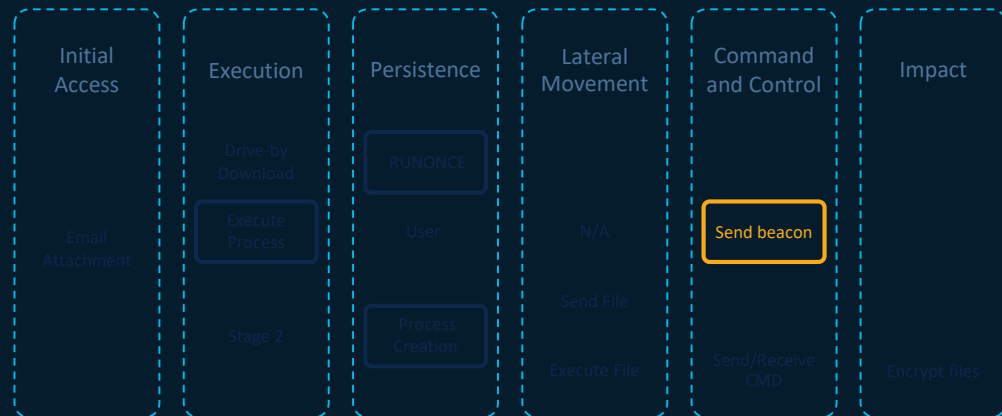
From Detection to Identification



Where is the **urgency** of response needed?

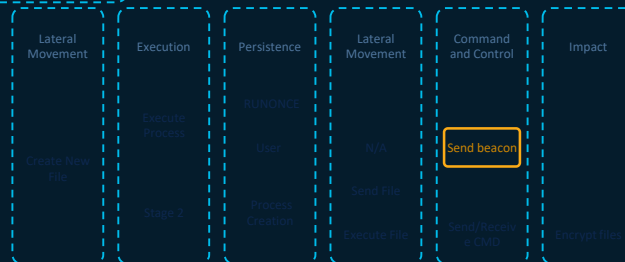


Initial Detection



How do we Triage only this alert for initial Response, Escalation or False-positive?

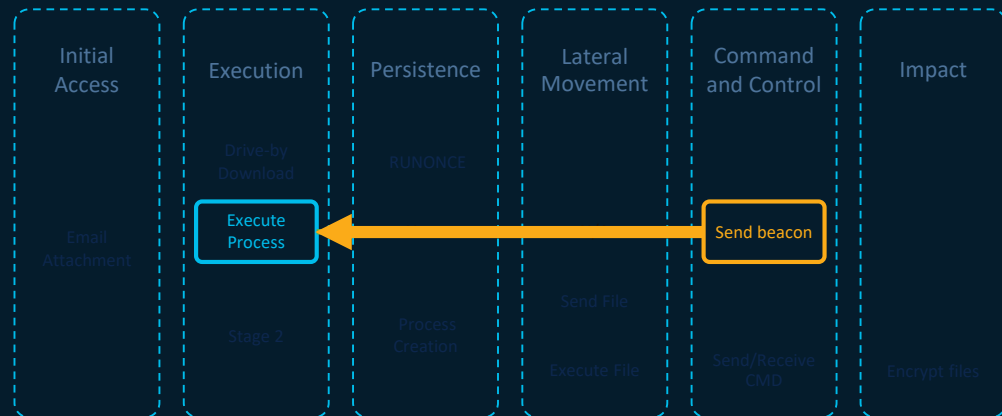
What process called the network beacon and are the beacons related?



From Detection to Identification

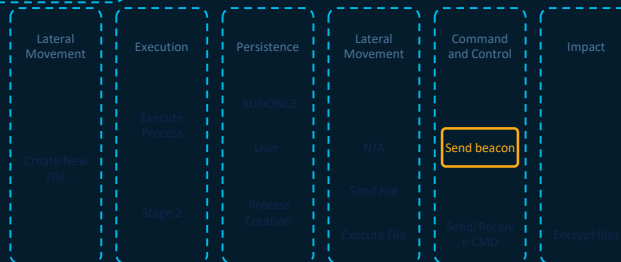
Initial
Detection(s)

Identification
(backward)



By using **backward chaining** we can focus on confirming this alert

What is the process tree of that executable?

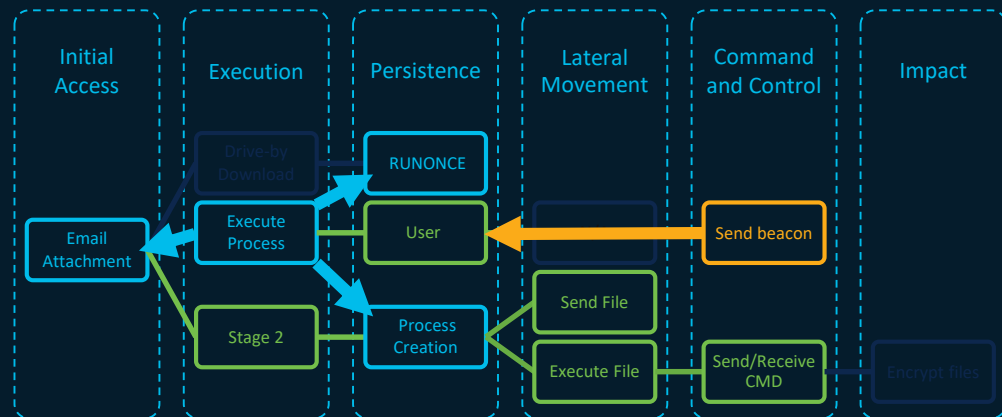


Detection to Identification

Initial
Detection(s)

Identification
(backward)

Identification
(forward)

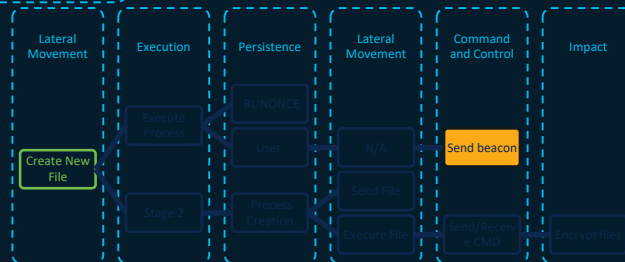


By using **forward chaining** we not only confirm but also understand the impact

Next step(s) for containment and root cause analysis.

What is the process tree of that executable?

Was there lateral movement?

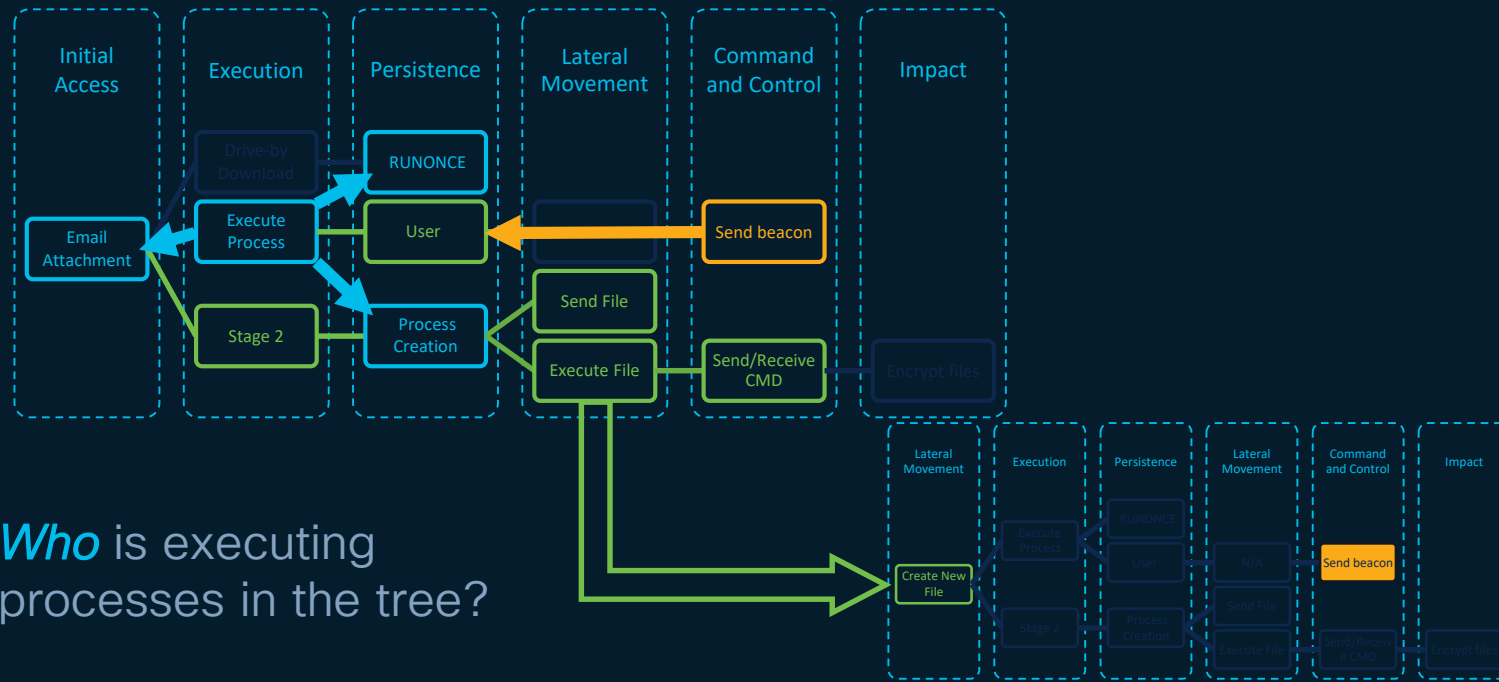


Detection to Identification

Initial
Detection(s)

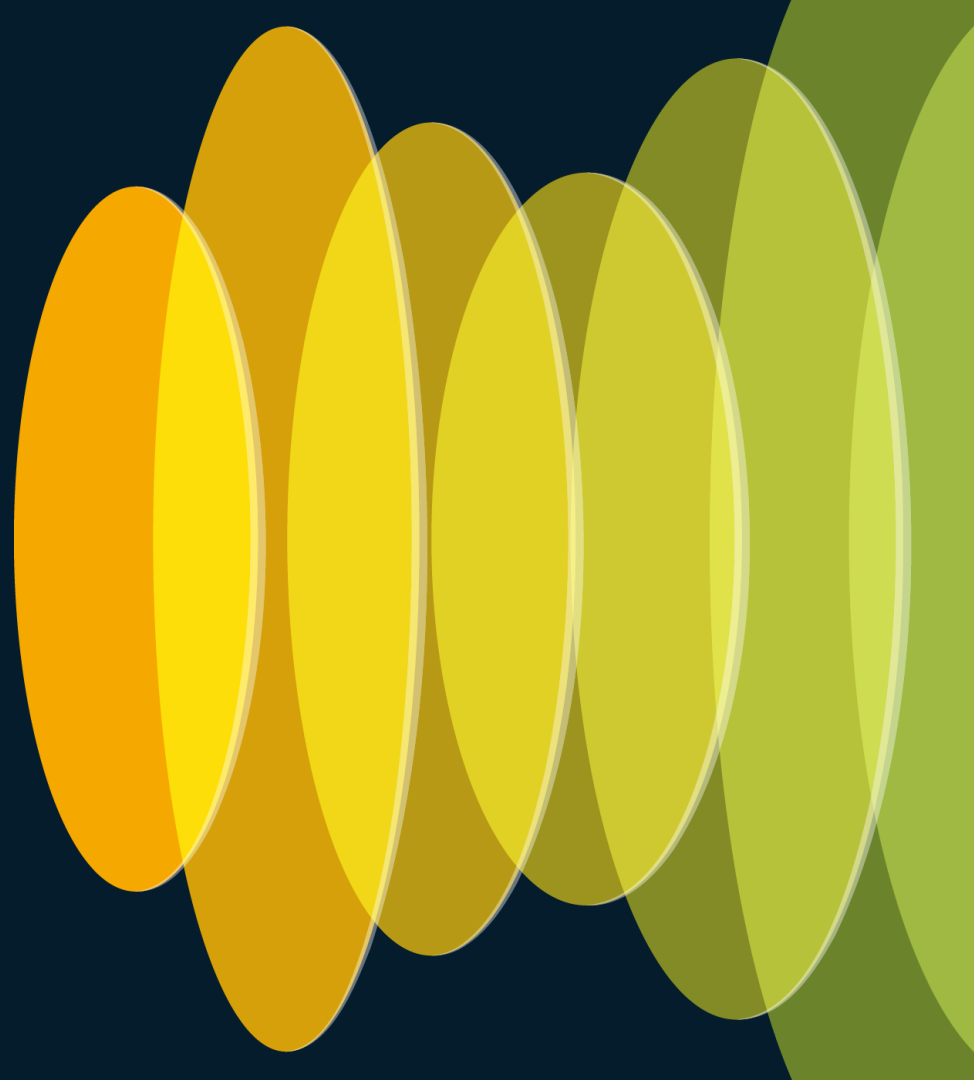
Identification
(backward)

Identification
(forward)

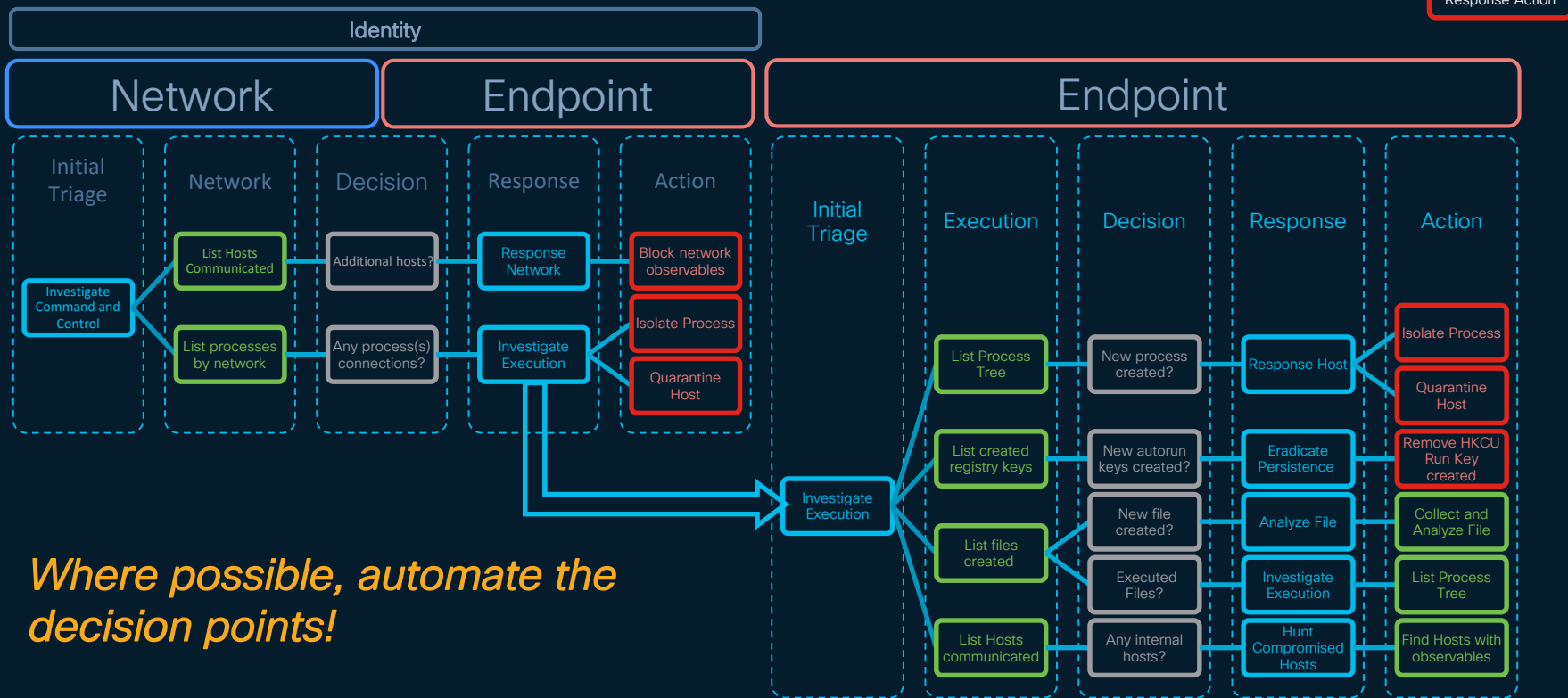


Who is executing
processes in the tree?

Let's turn this into
a “Playbook”!



The full Playbook



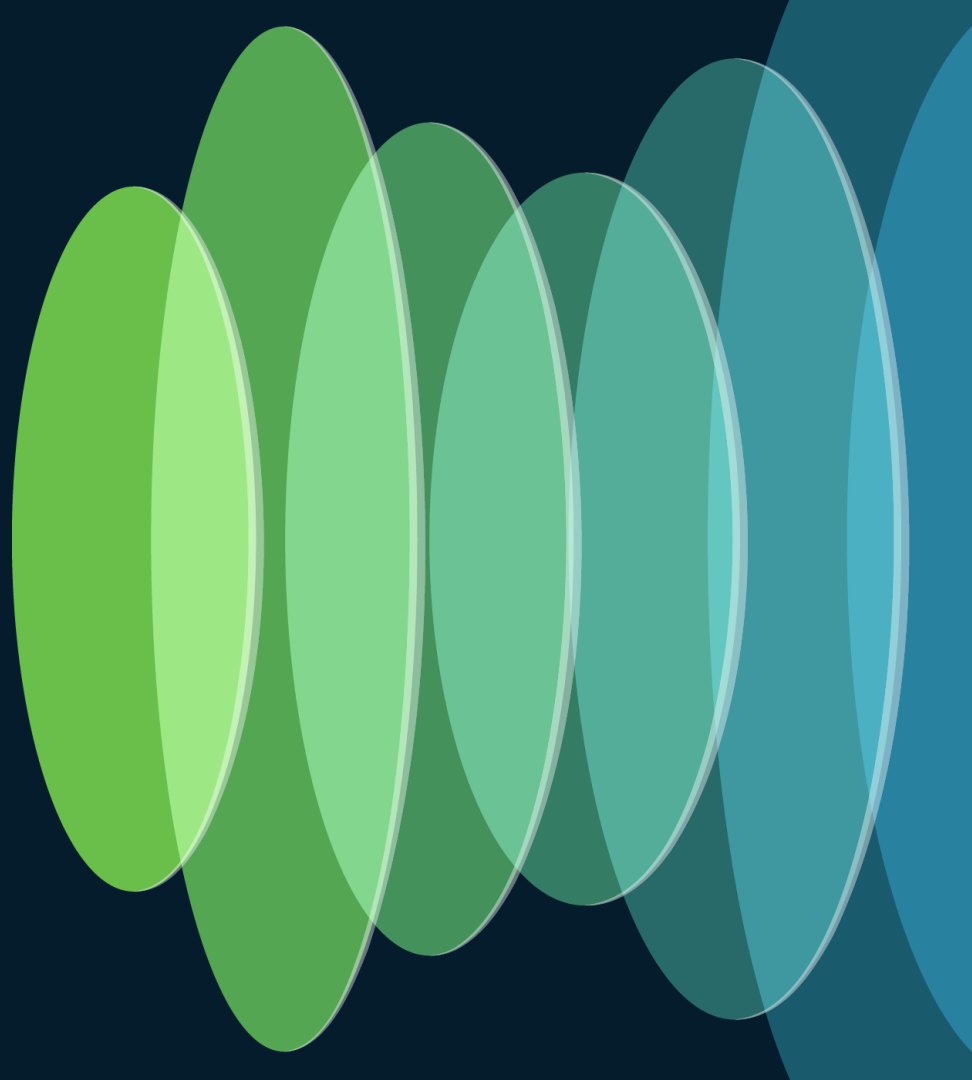
Agenda

- ~~What is Incident Response?~~
- How to perform Incident Response with Cisco XDR?
 - Introduction to Cisco XDR (Automation)
 - Pivot Menu
 - Playbook Tasks
 - Automation Rules
- Let's put it to practice!
- Future?

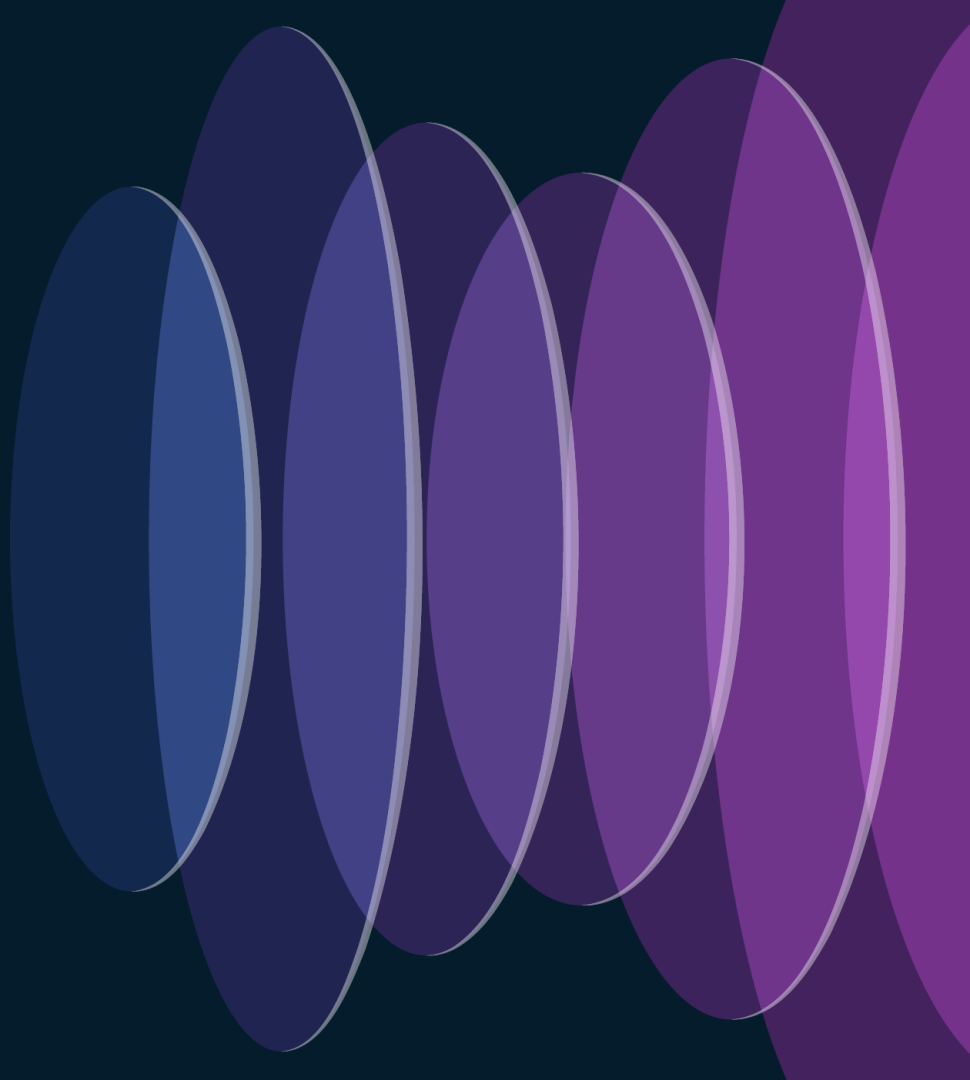
Agenda

- ~~What is Incident Response?~~
- How to perform Incident Response with Cisco XDR?
 - Introduction to Cisco XDR (Automation)
 - Pivot Menu
 - Playbook Tasks
 - Automation Rules
 - Let's put it to practice!
 - Future?

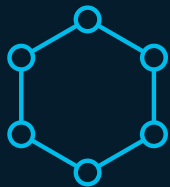
How to perform Incident Response with Cisco XDR?



IR with Cisco XDR: Introduction



What is eXtended Detection and Response?



Collection of detections and raw telemetry from multiple sensor technologies across your environment



Application of advanced analytics to the collected and normalized evidence to produce correlated and prioritized detections of malicious activity



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

Identify the most impactful incidents using Risk

736

92

Detection
Risk

8

Asset
Value at Risk

$$\text{Priority Score} = \text{Detection Risk} \times \text{Asset Value}$$

1-1000 1-100 1-10

The Incident total priority score used to prioritize incidents

Detection Risk composed of multiple values:

- MITRE TTP Financial Risk
- Number of MITRE TTPs
- Source Severity

User Defined Asset Value represent the value of the asset involved in the incident

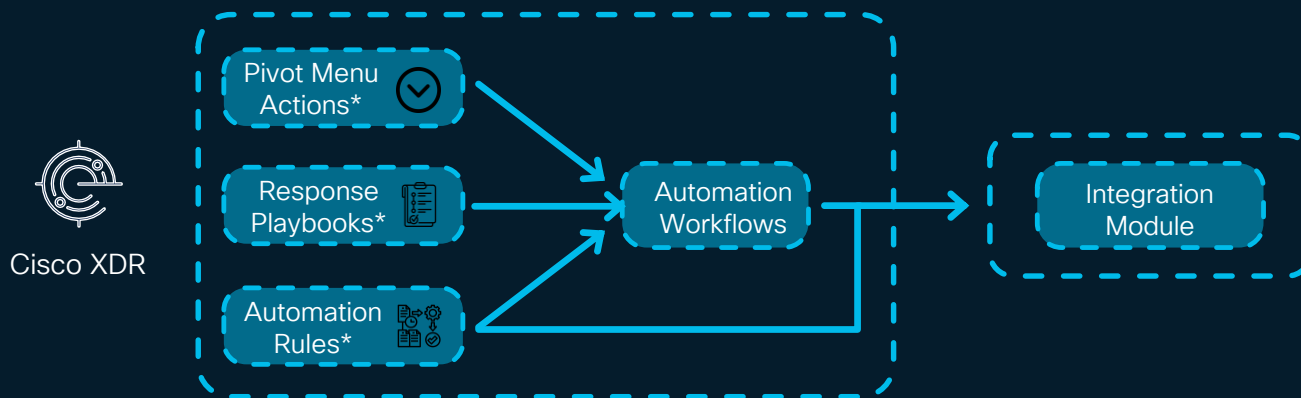
Incident Response Architecture

Wide variety of actions

Retrieve additional context from device, isolate hosts, block IPs on firewalls, quarantine messages in a mailbox, and much more...

Dynamic Response

Response actions can be automated, guided or manual (i.e. unguided).



Cisco Products



Endpoint



Cloud Analytics



Firewall



Malware Analytics



SentinelOne

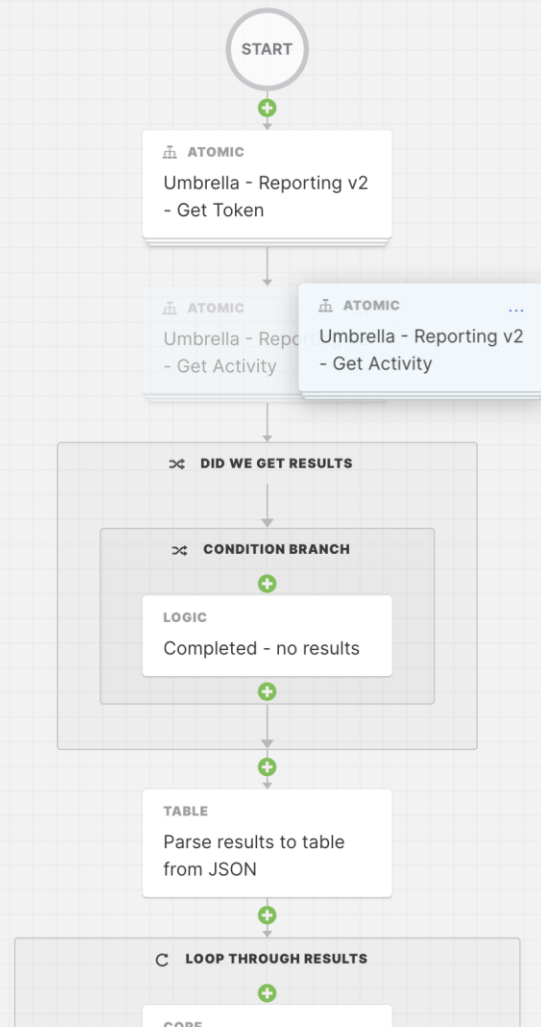


CrowdStrike

And many others...

XDR Automation


- A “no-to-low-code” drag and drop editor that allows you to build simple or complex workflows.
 - No code required, but Python can be used.
 - Powers the Response playbook feature in the incident manager using out of the box workflows.
 - Pre-written workflows are available for import from Cisco or a broader community.
 - Wide variety of use cases that are not limited to security or XDR-related outcomes.




Automation Workflow Runs

Automation Triggers

Pivot Menu Actions 

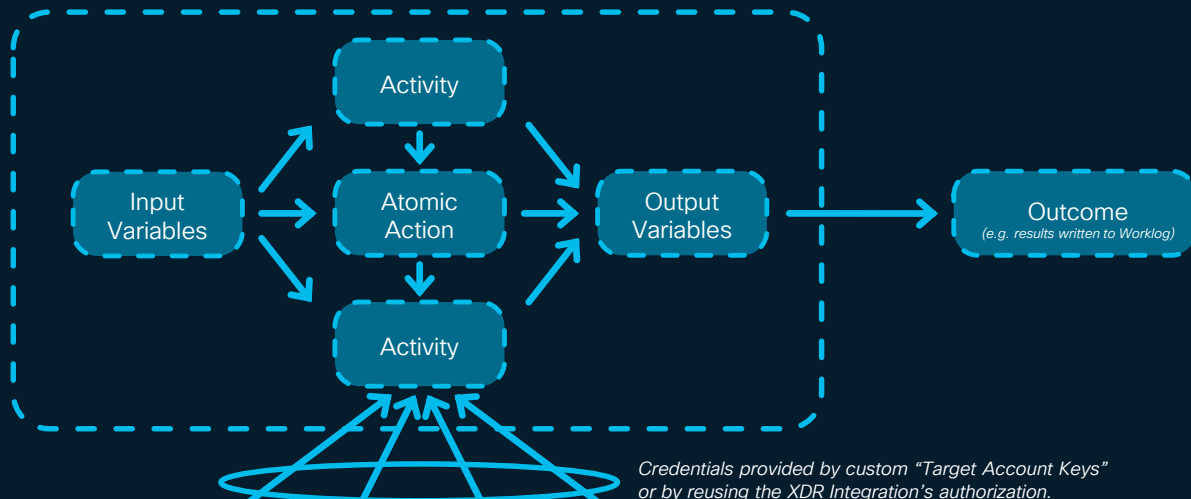
Response Playbooks 

Automation Rules 

Other Trigger types:

- API request
- Task Approval
- Incoming Email
- Manual "Run" button
- Schedule/Calendar
- Incoming Webhook

Automation Workflow



Credentials provided by custom "Target Account Keys" or by reusing the [XDR Integration](#)'s authorization.



Automation Targets



Pivot Menu Actions

- Trigger: manually in XDR UI or via Ribbon
- Input: single Observable only, single type (e.g. IP, Domain, etc.)
- Audit: currently no audit trail (only the Workflow Run)*
- Method: IROH Response API or Workflow with Pivot Menu template



Response Playbooks

- Trigger: manually in XDR Incident Details > Response tab
- Input: Incident or selection of Observables
- Audit: XDR Incident Details > Worklog tab and Workflow Runs
- Method: Workflow with Incident Response template



Automation Rules

- Trigger: automatically, on Incident creation or status change
- Input: Incident, but possible to act on Observables via Workflow logic
- Audit: XDR Incident Details > Worklog tab and Workflow Runs
- Method: 1 or more Workflows with Incident Response template

What are “Playbooks” in Cisco XDR?



Playbook

A bundle of Phases and Tasks. Phases contain 1 or more Tasks. Tasks will include instructions and optionally an Automation Workflow.

Cisco Managed Playbook available using System Workflows. Also possible to create custom and assign to incidents using Assignment Rules.



Workflows

Contains one or more Atomic Actions, designed for a specific use case. Can be triggered automatically via Rules, or manually via Tasks.

System Workflows available that can that work based on Integrations, out-of-the-box.



Atomic Actions

Lower-level Workflows, which can be used as building blocks. Often self-contained workflows that are like a function in traditional programming.

Many System Atomics available, for Cisco and third-party.

XDR Integrations











- Sometimes referred to as “Integration Modules” or “Modules”
- Cisco XDR has 85+ built-in Integrations:
 - On-prem and SaaS possible
 - Mix of security products, intelligence sources, device managers, and more
 - Easy to enable and configure
 - API based
 - Custom Integrations possible!

Integrations

Q Search

Filters

My Integrations

Integration Name	Name	Status
Orbital	Orbital	 Connected
XDR Analytics	Secure Cloud Analytics	 Connected
Email Security	Secure Email and Web Manager	 Connected
Secure Endpoint	Secure Endpoint	 Connected
Secure Firewall	Secure Firewall	 Connected
Secure Network Analytics	Secure Network Analytics	 Connected
Umbrella	Umbrella	 Connected
AlienVault Open Threat Exchange	AlienVault Open Threat Exchange	 Connected
CrowdStrike	CrowdStrike	 Connected
CyberCrime Tracker	CyberCrime Tracker	 Error

Automation Targets

- Come in many different types, depending on the resource you're communicating with.
- Most common types:
 - HTTP Endpoint (used by most APIs)
 - SMTP Endpoint
 - SSH (Terminal) Endpoint
- Can be associated with an Account Key for authentication.
- Some target types support XDR Automation remote and/or the use of a proxy.

[← 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

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 ⓘ

False

Default Account Keys

Select

Remote

Remote Keys

Select

Integration Targets

- Many XDR Integrations support automated creation of targets in XDR Automation (all new/updated):
 - When a supported integration is configured in XDR, a corresponding Target will be created in Automation.
 - Target will be read-only and have its type listed as the Target Type.
 - Integration Targets are a sub-type of the HTTP Endpoint target type.
 - Integration Targets make workflow sharing and installation much simpler since they require no configuration.

[← Targets](#)

Edit CrowdStrike

Target Type

ⓘ This target has been provided by a CrowdStrike Integration Module and does not require an Account Key selection.

General

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

Display Name

Description

Account Keys

Use an account key if the target requires authentication.

No Account Keys ⓘ

Default Account Keys

Remote

Remote Keys

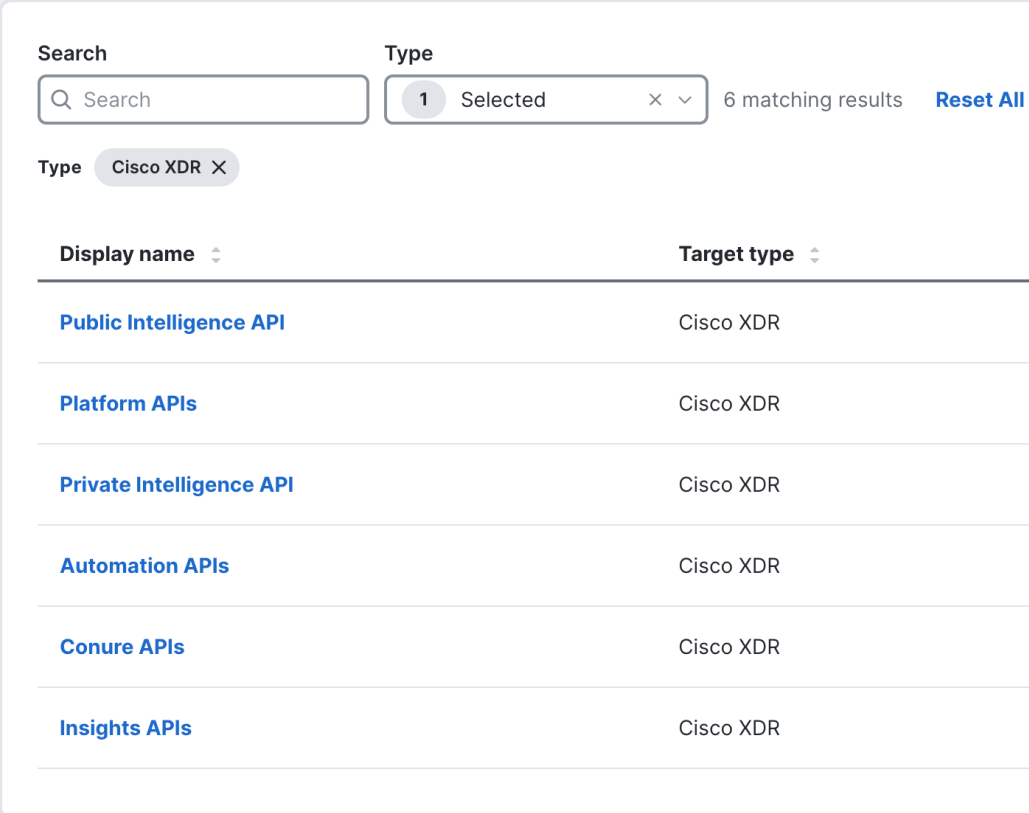
XDR API targets

- Built-in Targets for various XDR APIs to streamline operations or custom integrations within the XDR product:
 - **Public Intelligence API:** Database of intelligence from multiple sources available to any XDR customer.
 - **Private Intelligence API:** Database of intelligence that's private to your organization.
 - **Platform APIs:** APIs for investigation, response, incident management, and more.
 - **Automation APIs:** APIs for managing objects like targets and account keys, starting workflows, and more.

Targets

Targets are systems and resources you want your workflows to be able to communicate with. Target Groups are a dynamic collection of targets to use in a workflow.

[Targets](#) Target Groups



The screenshot shows the 'Targets' management interface. At the top, there is a 'Search' bar and a 'Type' dropdown menu. The 'Type' dropdown is set to 'Cisco XDR' and shows '1 Selected'. To the right of the dropdown, it says '6 matching results' and there is a 'Reset All' link. Below the search bar, there is a table with two columns: 'Display name' and 'Target type'. The table lists six targets, all of which are 'Cisco XDR' type.

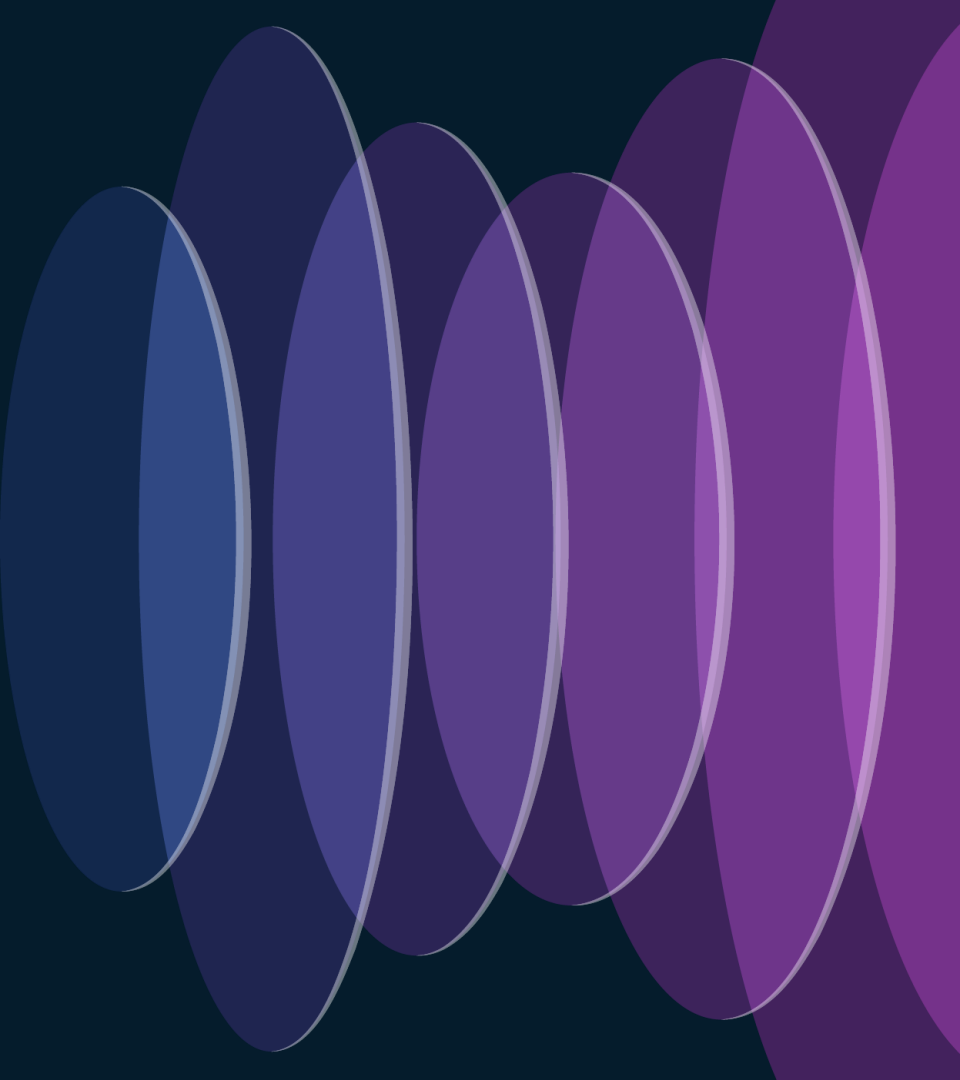
Display name	Target type
Public Intelligence API	Cisco XDR
Platform APIs	Cisco XDR
Private Intelligence API	Cisco XDR
Automation APIs	Cisco XDR
Conure APIs	Cisco XDR
Insights APIs	Cisco XDR

Agenda

- ~~What is Incident Response?~~
- How to perform Incident Response with Cisco XDR?
 - ~~Introduction to Cisco XDR (Automation)~~
 - Pivot Menu
 - Playbook Tasks
 - Automation Rules
- Let's put it to practice!
- Future?

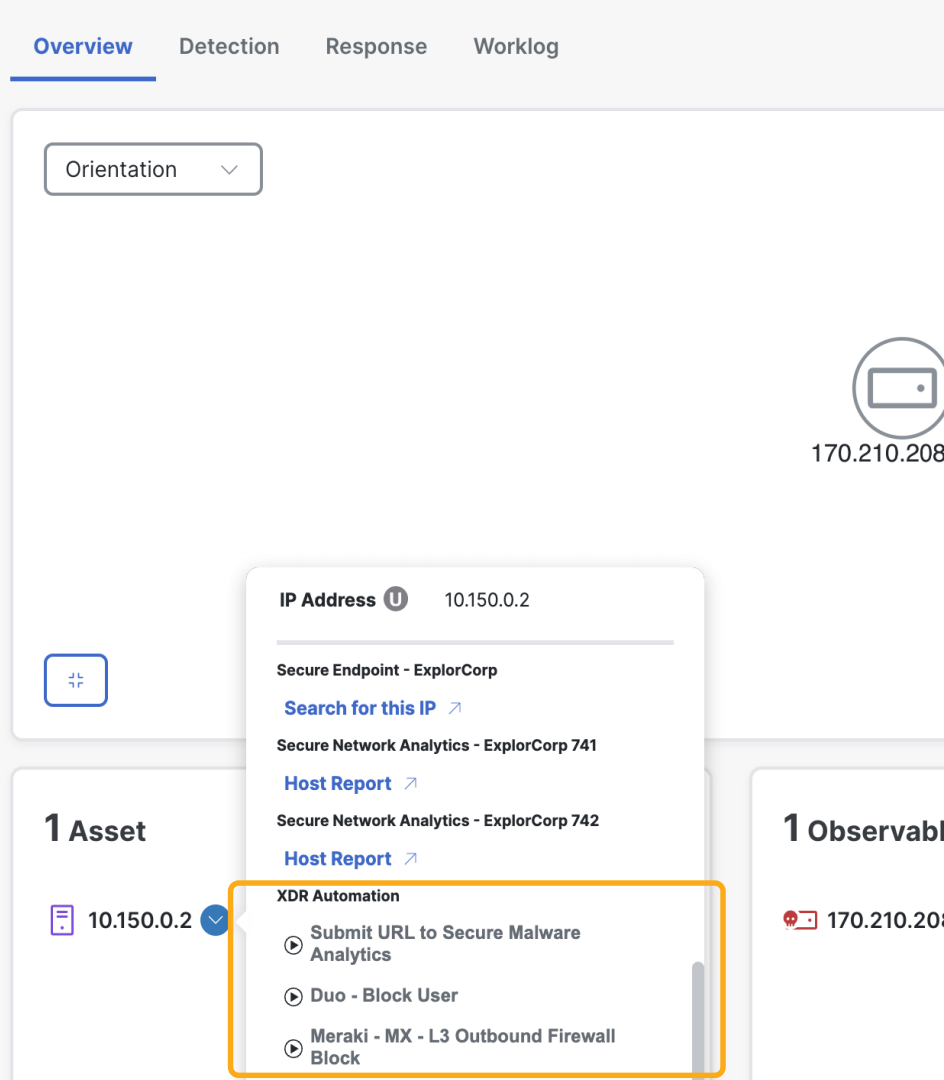


IR with Cisco XDR: Pivot Menu



Pivot Menu Actions

- Triggered for a single "Observable" from various parts of XDR, including within Investigations, Incidents and even from the "Ribbon".
- The available actions are dependent on the Observable Type (e.g. domain, IP, SHA256, etc.)
- Allow you to take actions such as:
 - Creating a "Judgement"
 - Linking out to other products to view additional information
 - Taking a response action via an Integration (IROH Response API)
 - Executing Automation Workflows with the "Pivot Menu" template



Automation Workflows with “Pivot Menu” template

What is the intent of this workflow?

Blank Custom Workflow

Incident Response Workflow

Pivot Menu 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.

Import Workflow + Create Workflow

Card View List View

Last modified	Actions
24/04/2024, 23:35:18	...
24/04/2024, 23:30:12	...
24/04/2024, 23:30:01	...
24/04/2024, 22:58:21	...
24/04/2024, 22:58:21	...
24/04/2024, 22:58:09	...

Cancel Continue

Workflow is unlocked Share Validate View Runs Run Settings

Workflow Properties

Cisco Live Demo

Variables

Name	Type	Scope	Value	Required
observable_type	String	Input		True
observable_value	String	Input		True

+ Add Variable

Response Options

Workflow Intent

Pivot Menu

Observable Type(s)

SHA256

New Pivot Menu Workflow

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.

Workflow display name* 15 / 64

Cisco Live Demo

Observable Type(s)*

All

Domain

Email

Hostname

IP

IPv6

MD5

SHA1

SHA256

URL

User

Continue

4 Observables

TOP ACTIVE

Unknown Domain

moreinternetbadguys.com

Clean IP Address

8.8.8.8

Malicious SHA-256

795db7bdad1befdd3ad942be79715f6b0c5083d...

Malicious Domain

SHA-256 795db7bdad1b...590c9628790f

Verdict Source AMP File Reputation

1 Verdict

Investigate observable

Create Judgment

Copy value

Add to new case

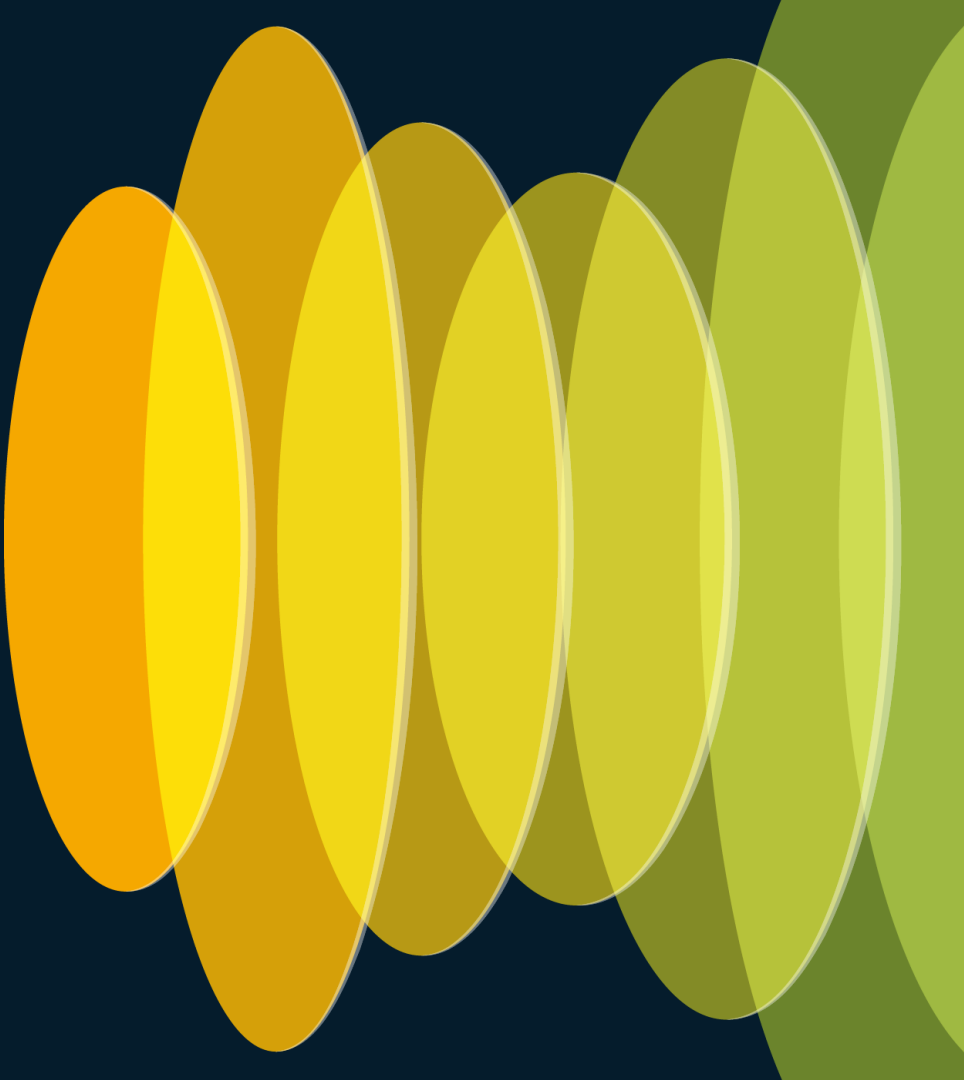
Add to active case

Automation

Cisco Live Demo



Demo: Create a new Pivot Menu Workflow



Cisco XDR - Administration

xdr.us.security.cisco.com/administration/integrations

All Bookmarks

XDR

Christopher Van ...
Cisco - chrivand

Integrations

Q Search

Capabilities

Authorship Type

My Integrations

Integration Name	Name	Status	Authorship Type
Orbital CHRIVAND	Orbital	Connected	Cisco Managed
Orbital [second]	Orbital	Connected	Cisco Managed
Secure Endpoint - MSSP Tenant B	Secure Endpoint	Connected	Cisco Managed
Duo Beta	Secure Access by Duo (Deprecated)	Connected	Cisco Managed
Shodan Test	Shodan	Connected	Cisco Managed
Slack	Slack	Connected	
VirusTotal	VirusTotal	Connected	Cisco Managed
Webex (Bots by Christopher)	Webex	Connected	Cisco Managed

Cisco XDR - Automate

xdr.us.security.cisco.com/automate/workflows

XDR

Christopher Van ...
Cisco - chrivand

Workflows

Workflows allow you to investigate security events, automate responses, and eliminate repetitive tasks by using activities, logic, and even other workflows to communicate with other systems and resources. From here you can access, create, and import workflows.

All Workflows 152 Atomics 546 Recents Favorites 1

Workflows

Search

Status

Q Search

Select

Display name

PROD: Scheduled XDR Ideas to Webex

PROD: Scheduled SNA Ideas to Webex

Scheduled IROH Healthcheck to Webex

NEW - CHRIVAND - CLEMEA24 - Create Incident

XDR - Automation Rule - Update Incident Properties

XDR - Restore Systems

XDR - Contain Incident: Assets

XDR - Confirm Incident

XDR - Identify Vulnerabilities

Incident Response

Incident Response

Incident Response

Incident Response

Incident Response

Incident Response

Incident Response

Incident Response

Validated

Validated

Validated

Validated

Validated

Validated

Validated

Validated

System

System

System

System

System

System

System

System

Last modified

23/05/2024, 08:00:06

23/05/2024, 08:00:01

21/05/2024, 13:19:55

21/05/2024, 11:27:53

16/05/2024, 22:36:42

15/05/2024, 21:32:21

15/05/2024, 21:32:20

15/05/2024, 21:32:18

15/05/2024, 21:32:17

Actions

...

...

...

...

...

...

...

...

Import Workflow

Create Workflow

Card View

List View

What is the intent of this workflow?

Blank Custom Workflow

Incident Response Workflow

Pivot Menu 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

#CiscoLive

BRKSEC-2502

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

42

Cisco XDR - Automate

xdr.us.security.cisco.com/automate/workflows

All Bookmarks

XDR

?

🔔

👤 Christopher Van ...
Cisco - chrivand

Workflows

Workflows allow you to investigate security events, automate responses, and eliminate repetitive tasks by using activities, logic, and even other workflows to communicate with other systems and resources. From here you can access, create, and import workflows.

All Workflows 153 ▾ Atomics 546 Recents Favorites 1

Workflows

Search

Status

Category

Search

Select

Select

Display name

Cisco Live Vegas Demo: Send User Webex Message

Send a warning message to a user when involved in an incident...

PROD: Scheduled XDR Ideas to Webex

PROD: Scheduled SNA Ideas to Webex

Scheduled IROH Healthcheck to Webex

NEW - CHRIVAND - CLEMEA24 - Create Incident

XDR - Automation Rule - Update Incident Properties

XDR - Restore Systems

XDR - Contain Incident: Assets

XDR - Confirm Incident

Owner

Last modified

Actions

chrivand@cisco.com

23/05/2024, 11:35:24

...

chrivand@cisco.com

23/05/2024, 08:00:06

...

chrivand@cisco.com

23/05/2024, 08:00:01

...

chrivand@cisco.com

21/05/2024, 13:19:55

...

chrivand@cisco.com

21/05/2024, 11:27:53

...

DevNet

Validated

Incident Automation Rule

Validated

Incident Response

Validated

Incident Response

Validated

Incident Response

Validated

New Pivot Menu Workflow

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.

Workflow display name*

46 / 64

Cisco Live Vegas Demo: Send User Webex Message

Observable Type(s)*

Email X

Cancel

Continue

#CiscoLive

BRKSEC-2502

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

43

Cisco XDR - Automate

xdr.us.security.cisco.com/automate/workflows/edit/02EJYH2JC2TCB1cwqiyluRuyfYER7TfYxrY

All Bookmarks

← Back to all Workflows

Cisco Live Vegas Demo: Send User Webex Message

Last Modified: 23 May 2024 at 11:28:55

Workflow is unlocked

Share

Validate

View Runs

Run

Settings

Search activities

ActivitiesLogicWorkflows

Core

Ansible Tower

Atomic

AWS Service

Check Point Quantum Smart-1

Cisco API Console

Cisco Defense Orchestrator

Cisco Duo: Admin API

Cisco Duo: Auth API

Cisco ISE

Cisco Meraki

Cisco Orbital

Cisco PSIRT openVuln

Cisco Secure Cloud

Drag activity here

+

-

Warning 1

Workflow Properties

Cisco Live Vegas Demo: Send User Webex Message

General

Variables

Response Options

Automation Rules

Ver

Exc

Tar

Platform APIs

Private Intelligence API

Public Intelligence API

Secure Endpoint - Cisco - chrivand - v1

Secure Endpoint - MSSP Tenant B - v1

Slack

Webex (Bots by Christopher)

Other Targets

AMP_Target

+ Add New

Select

Specify target on workflow start

Execute on this target group

#CiscoLive

BRKSEC-2502

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

44

Cisco XDR - Automate

xdr.us.security.cisco.com/automate/workflows/edit/02EJYH2JC2TCB1cwqiyluRuYfYER7TfYxry

All Bookmarks

← Back to all Workflows

Cisco Live Vegas Demo: Send User Webex Message

Last Modified: 23 May 2024 at 11:30:57

Workflow is unlocked

Share

Validate

View Runs

Run

Settings

webex

ActivitiesLogicWorkflows

Cisco Webex

Webex - Add Member to Room

Webex - Create Room

Webex - Post Message to Room

Webex - Search for People

Webex - Search for Room

Webex - Search for Team

Webex - Send Message to Person

Cisco Webex Teams

Cisco SecureX - Webex Teams - Post Message to Room [POC]

Workflows

CISA - Software Advisories to Webex

START

Atomic Webex - Send Message to Person

END

Properties: Webex - Send Message To Person

Webex - Send Message To Person

General

Display Name*30 / 64

Webex - Send Message to Person

Description0 / 1024

☐ Continue Workflow Execution On Failure

☐ Skip activity execution

Workflow*

Webex - Send Message to Person

Input*

Recipient ID ⓘ

Access Token ⓘ

Plain Text Message ⓘ

Markdown Message ⓘ

Cisco XDR - Automate

xdr.us.security.cisco.com/automate/workflows/edit/02EJYH2JC2TCB1cwqiyluRuyfYER7TfYxrY

🔍 ☆ 🌐 ⌂ 🔴 ⋮

📁 All Bookmarks

← Back to all Workflows

Cisco Live Vegas Demo: Send User Webex Message

Last Modified: 23 May 2024 at 11:30:57

Workflow is unlocked

Share

Validate

View Runs

Run

Settings

🔍 webex

ActivitiesLogicWorkflows

Cisco Webex

Webex - Add Member to Room

Webex - Create Room

Webex - Post Message to Room

Webex - Search for People

Webex - Search for Room

Webex - Search for Team

Webex - Send Message to Person

Cisco Webex Teams

Cisco SecureX - Webex Teams - Post Message to Room [POC]

Workflows

CISA - Software Advisories to Webex

Browse Variables

🔍 Search

Env

Global

Workflow

Input

Output

Target

observable_type

observable_value

CancelSave

Properties: Webex - Send Message To Person

Webex - Send Message To Person

Recipient ID

Access Token

Plain Text Message

Markdown Message

Recipient Email

Files

Attachments

Target

Target*

Target Type*

HTTP Endpoint

Cisco XDR - Automate

xdr.us.security.cisco.com/automate/workflows/edit/02EJYH2JC2TCB1cwqiyluRuyfYER7TfYxY

🏠 ☆ 🔒 ⌵ ⚙️

All Bookmarks

← Back to all Workflows

Cisco Live Vegas Demo: Send User Webex Message

Last Modified: 23 May 2024 at 11:30:57

Workflow is unlocked

Share

Validate

View Runs

Run

Settings

webex

ActivitiesLogicWorkflows

Cisco Webex

Webex - Add Member to Room

Webex - Create Room

Webex - Post Message to Room

Webex - Search for People

Webex - Search for Room

Webex - Search for Team

Webex - Send Message to Person

Cisco Webex Teams

Cisco SecureX - Webex Teams - Post Message to Room [POC]

Workflows

CISA - Software Advisories to Webex

START

Atomic Webex - Send Message to Person

END

Properties: Webex - Send Message To Person

Webex - Send Message To Person

Recipient ID

Access Token

Plain Text Message

Markdown Message

Recipient Email

Files

Attachments

Target

Cisco XDR - Automate

xdr.us.security.cisco.com/automate/workflows/edit/02EJYH2JC2TCB1cwqiyyuRuyfYER7TfYxry

🔖 ☆ 🔒 ⌵ 🔴

All Bookmarks

← Back to all Workflows

Cisco Live Vegas Demo: Send User Webex Message

Last Modified: 23 May 2024 at 11:35:24

Workflow is unlocked

Share

Validate

View Runs

Run

Settings

Search activities

ActivitiesLogicWorkflows

Core>

Ansible Tower>

Atomic>

AWS Service>

Check Point Quantum Smart-1>

Cisco API Console>

Cisco Defense Orchestrator>

Cisco Duo: Admin API>

Cisco Duo: Auth API>

Cisco ISE>

Cisco Meraki>

Cisco Orbital>

Cisco PSIRT openVuln>

Cisco Secure Cloud>

START

AtomicWebex - Send Message to Person

END

Workflow Properties

Cisco Live Vegas Demo: Send User Webex Message

General

Display Name*46 / 64

Cisco Live Vegas Demo: Send User Webex Message

Owner

chrivand@cisco.com

Description102 / 1024

Send a warning message to a user when involved in an incident to turn off devices, using Cisco Webex.

☐ 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 left.

Category

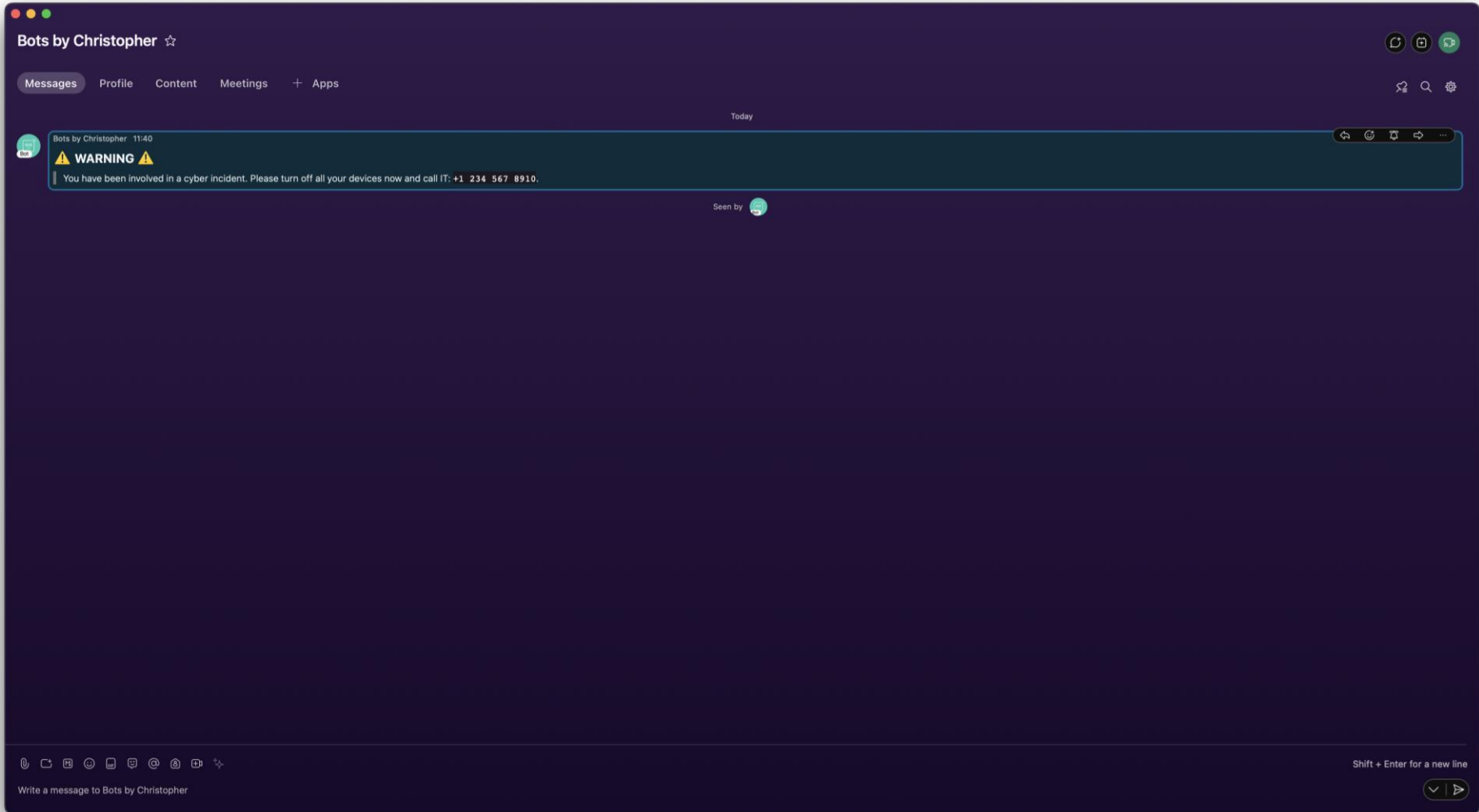
Select

Variables

Response Options

Automation Rules

← Incidents



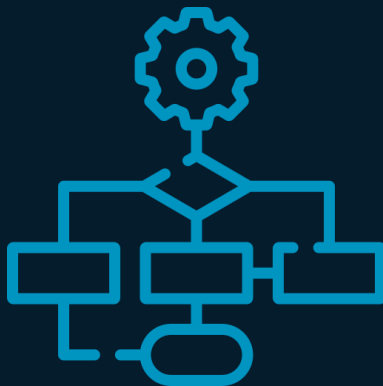


Demo breakdown...



Trigger

Action from
Pivot Menu



Operation

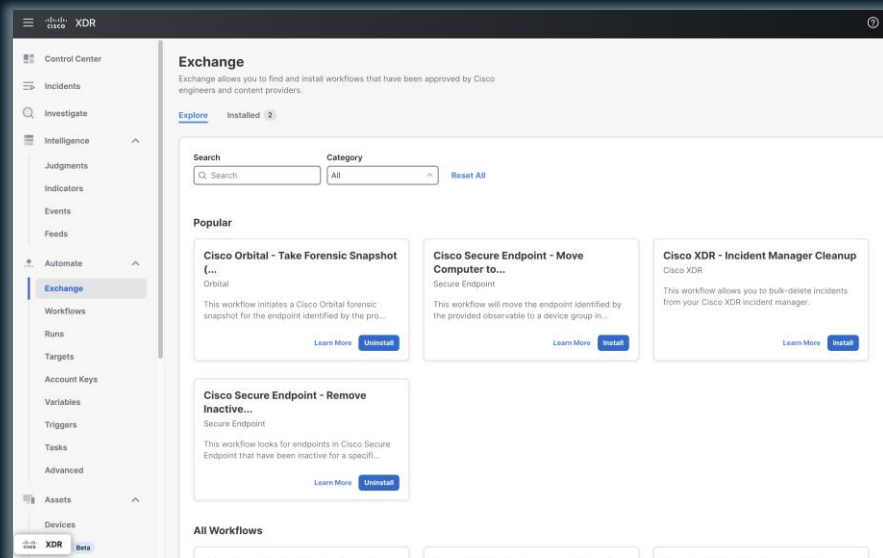
Send Webex
Message To
User



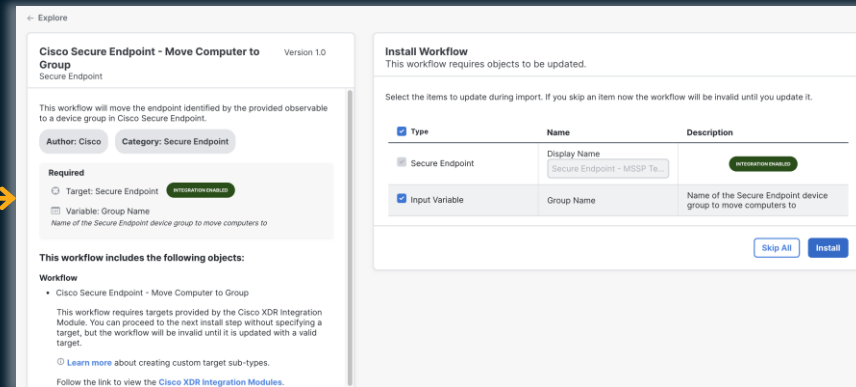
Outcome

Notify
Affected User*

Don't want to create your own?



The screenshot shows the Cisco XDR Control Center interface. The left sidebar contains navigation options: Control Center, Incidents, Investigate, Intelligence, Judgments, Indicators, Events, Feeds, Automate, Exchange (highlighted), Workflows, Runs, Targets, Account Keys, Variables, Triggers, Tasks, Advanced, Assets, and Devices. The main content area is titled 'Exchange' and includes a search bar, a category dropdown set to 'All', and a 'Reset All' button. Below this, there are three 'Popular' workflow cards: 'Cisco Orbital - Take Forensic Snapshot', 'Cisco Secure Endpoint - Move Computer to...', and 'Cisco XDR - Incident Manager Cleanup'. Each card has a 'Learn More' link and an 'Install' button. At the bottom, there is a section for 'All Workflows'.



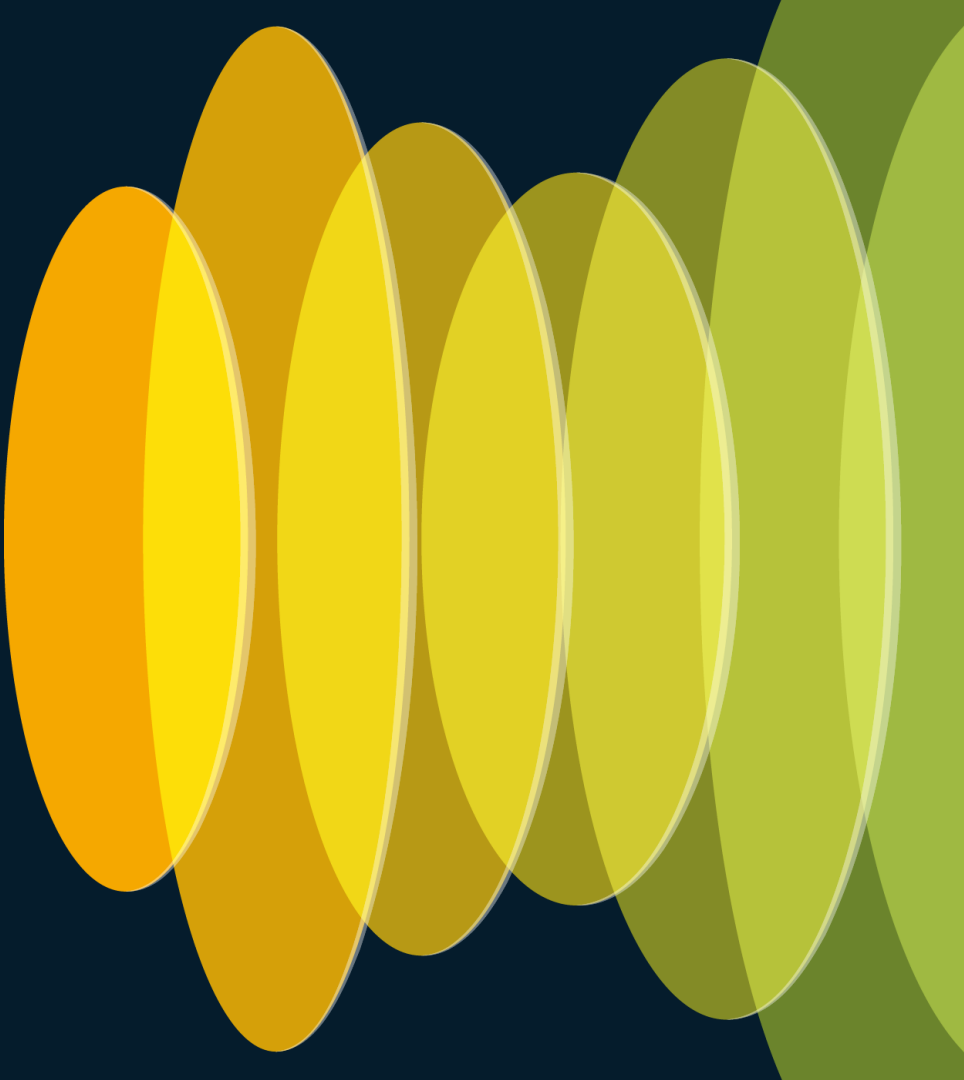
The screenshot shows the details for the 'Cisco Secure Endpoint - Move Computer to Group' workflow. The workflow is authored by Cisco and is categorized under 'Secure Endpoint'. It is described as a workflow that moves the endpoint identified by the provided observable to a device group in Cisco Secure Endpoint. The 'Required' section lists two items: 'Target: Secure Endpoint' (with a status of 'Integration Enabled') and 'Variable: Group Name' (described as 'Name of the Secure Endpoint device group to move computers to'). The 'This workflow includes the following objects:' section lists the 'Cisco Secure Endpoint - Move Computer to Group' workflow, which requires targets provided by the Cisco XDR Integration Module. A link to 'Learn more about creating custom target sub-types' is provided. The 'Install Workflow' section on the right indicates that the workflow requires objects to be updated and provides a table for selecting items to update during import.

Type	Name	Description
<input type="checkbox"/> Secure Endpoint	Display Name Secure Endpoint - MSSP Te...	INTRODUCTION ENABLED
<input checked="" type="checkbox"/> Input Variable	Group Name	Name of the Secure Endpoint device group to move computers to

Buttons: Skip All, Install



Demo: Use a pre-built Pivot Menu Workflow



Cisco XDR - Administration

xdr.us.security.cisco.com/administration/integrations/b50f5091-a208-464e-84cc-964063e0463f/edit

All Bookmarks

Cisco XDR

Christopher Van ...
Cisco - chrivand

Integrations

✓ This integration module has no issues. You can explore Automation workflows in [Exchange](#).

Orbital

Cisco Managed

Orbital is an advanced capability in Cisco Secure Endpoint that is designed to make security investigation and threat hunting simple by providing an implementation of powerful Osquery technology on each of your Secure Endpoint-enabled endpoints. Orbital allows you to create custom queries to look across your network for anything of interest, but also comes with over a hundred pre-canned queries, allowing you to quickly run complex queries on any or all endpoints. This capability enables you to gain deeper visibility on what happened to any endpoint at any given time by taking a snapshot of its current state. Whether you are doing an investigation as part of incident response, threat hunting, IT operations, or vulnerability and compliance, we get you the answers you need about your endpoints fast. Orbital can enrich information presented in the relations graph by pivoting into Orbital to query and gather additional intelligence about your host, IP, IP4, IP6, MAC, and OS, etc. The Orbital app is available on the ribbon and it allows you to run a live query. You can view metrics and your recent queries in the right panel.

This integration also creates a target automatically in Automation for out-of-box workflows.

Intro to Orbital, a New Endpoint Security Evolution

Query Catalog / etc_hosts_monitoring

Hosts File Monitoring

Created by Cisco 02/12/19. Updated 08/15/19.

This query is applicable to Windows, Linux and MacOS. The hosts file is the local host database which is checked before a name resolution request is sent to a DNS server. A host entry consists of a hostname, and it's corresponding IP address. It is often used by the malware authors to redirect traffic from the intended destination to sites hosting malicious or unwanted content. It may also be used to block legitimate content such as AV signature updates. On the other hand, it can be used legitimately, and this query may need to be customized to exclude legitimate entries.

ID etc_hosts_monitoring

OS Windows, Linux, Darwin

Categories Posture Assessment

ATT&CK™ Techniques Fallback Channels, Web Service

ATT&CK™ Tactics Command and Control

Catalog queries are designed to run independently.

SQLSELECT address, hostnames FROM etc_hosts WHERE

EDIT INTEGRATION

Connected

Integration Name*

Orbital CHRIVAND

✓ Integration with Device Insights

Delete

Save

Cisco XDR

https://xdr.us.security.cisco.com/automate/exchange?category=Orbital

#CiscoLive

BRKSEC-2502

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

54

Cisco XDR - AdministrationCisco XDR - Automate

xdr.us.security.cisco.com/automate/exchange/explore

All Bookmarks

XDR

?

🔔

👤 Christopher Van ...
Cisco - chrivand

☰

🏠

🕒

🔍

⚙️

🔗

📁

👤

Exchange

Exchange allows you to find and install workflows that are Cisco Managed, Cisco Verified or have been developed by the Community. Find more information about the content types in [our documentation](#).

[Explore](#) [Installed 3](#) [3 Updates available](#) [Submissions](#)

Search

Category

1 Selected

✕

Authorship Type

Select

▼

[Reset All](#)

Cisco Orbital - Take Forensic Snapshot (Linux)

Cisco Managed

This workflow initiates a Cisco Orbital forensic snapshot for the endpoint identified by the provided observable. This version 0...

[Learn More](#) [Install](#)

Cisco Orbital - Take Forensic Snapshot (macOS)

Cisco Managed

This workflow initiates a Cisco Orbital forensic snapshot for the endpoint identified by the provided observable. This version 0...

[Learn More](#) [Install](#)

Cisco Orbital - Take Forensic Snapshot (Windows)

Cisco Managed

This workflow initiates a Cisco Orbital forensic snapshot for the endpoint identified by the provided observable. This version 0...

[Learn More](#) [Install](#)

Cisco Orbital - Execute Query for Incident Assets

Cisco Managed

This workflow works with an incident automation rule or playbook task to execute an Orbital query on an XDR incident's assets.

[More](#) [Update](#)

Cisco Orbital - Execute Script for Incident Assets

Cisco Managed

This workflow works with an incident automation rule or playbook task to execute an Orbital script on an XDR incident's assets.

[Learn More](#) [Install](#)

Cisco Orbital - Execute Script for Selected Assets

Cisco Managed

This workflow works with an incident response playbook to execute an Orbital script on user-selected assets from an XDR incident...

[Learn More](#) [Install](#)

Cisco Orbital - Execute Query for Selected Assets

Cisco Managed

This workflow works with an incident response playbook to execute an Orbital query on user-selected assets from an XDR incident...

[Learn More](#) [Install](#)

XDR

Workflows

Workflows allow you to investigate security events, automate responses, and eliminate repetitive tasks by using activities, logic, and even other workflows to communicate with other systems and resources. From here you can access, create, and import workflows.

All Workflows 153 Atomics 546 Recents Favorites 1

Workflows

[↓ Import Workflow](#)

[+ Create Workflow](#)

Search

Status

Category

Reset All

Card View

List View

Display name	Categories	Status	Owner	Last modified	Actions
Cisco Orbital - Take Forensic Snapshot (Windows) 🔗 This workflow initiates a Cisco Orbital forensic snapshot for...	Exchange	✔ Validated	chrivand@cisco.com	23/05/2024, 11:54:21	...
Cisco Live Vegas Demo: Send User Webex Message 🔗 Send a warning message to a user when involved in an incident...		✔ Validated	chrivand@cisco.com	23/05/2024, 11:40:03	...
Cisco XDR - Execute Orbital Query for Incident Assets 🔗 This workflow works with an incident automation rule to execu...	Exchange, Automation Rule	✔ Validated	chrivand@cisco.com	23/05/2024, 11:39:03	...
Cisco XDR - Send Webex Message for New Incidents 🔗 This workflow works with an incident automation rule to send...	Exchange, Incident Automation Rule	Updated	chrivand@cisco.com	23/05/2024, 11:39:03	...
NEW - CHRIVAND - CLEMEA24 - Create Incident 🔗 This is a sample workflow how to create a Incident using the...	DevNet	✔ Validated	chrivand@cisco.com	23/05/2024, 11:38:53	...
PROD: Scheduled XDR Ideas to Webex 🔗	Aha.io Automation	Updated	chrivand@cisco.com	23/05/2024, 08:00:06	...
PROD: Scheduled SNA Ideas to Webex 🔗	Aha.io Automation	✔ Duplicate completed	chrivand@cisco.com	23/05/2024, 08:00:01	...
Scheduled IROH Healthcheck to Webex 🔗 This workflows runs a (scheduled) "Cisco XDR Integration Modu...	Cisco XDR	✔ Export completed	chrivand@cisco.com	21/05/2024, 13:19:55	...
XDR - Automation Rule - Update Incident Properties 🔗	🌟 Incident Automation Rule	✔ Validated	System	16/05/2024, 22:36:42	...

Cisco XDR - AutomateCisco XDR - Incidents

xdr.us.security.cisco.com/incidents/incident-64322795-2aa5-49bd-8d0b-106680ae434a/overview?drawer=graphNode&drawerGraphNodeId=6f8773ee

Cisco XDR

Christopher Van ...explorcorp

Incidents

1000Open

CHRIVAND CLUS - Malware Executed on MY-DEVICE-42 - Incident by Cisco XDR Automation

Reported by Cisco XDR Automation on 2024-05-23T11:10:29.640Z

View detailed description

Created by an Automation workflow.

OverviewDetectionResponseWorklogReport

Expand

This workflow initiates a Cisco Orbital forensic snapshot for the endpoint identified by the provided observable. This version of the workflow takes a forensic snapshot designed for devices running Microsoft Windows. Supported observables: IP address, MAC address, hostname, Secure Endpoint Computer ID, Orbital node ID Target: Orbital - v0 Steps: [] Make sure the observable is supported and set the corresponding local variable [] Execute a forensic snapshot

10 Assets

TOP ACTIVE

Endpoint Workstation
dapqa-crwd-227 events

Endpoint Workstation
dapqa-crwd-325 events

View all

26 Observables

TOP ACTIVE

Malicious URL
http://www.examplebotnetdomain.com101 events

Malicious Domain
internetbadguys.com8 events

View all

3 Indicators

TOP ACTIVE

network-opendns-malicious

network-dns-category-phis

TALOS
SID:1:34305:2 Adobe Flash

View events

Endpoint

c1-3850-2-g1-24-centos-12-102

Hostnamec1-3850-2-g1-24-centos-12-102

Talos Intelligence

Search for this hostname

Trend Vision One

Open in Vision One Search

XDR Automation

*CHRIVAND - Cisco Live Vegas: Send User Webex Message

*Cisco Orbital - Take Forensic Snapshot (Windows)

*Run Orbital Query Using Hostname

Submit URL to Secure Malware Analytics

Move Computer to Triage Group

ServiceNow - Request Firewall NullRoute

Meraki - MX - L3 Outbound Firewall Block

MAC Address
52:54:00:38:9f:ab

MAC Address
00:50:56:be:b9:89

Indicators

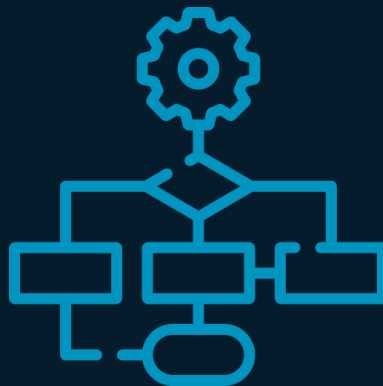
0

Demo breakdown...



Trigger

Action from
Pivot Menu



Operation

Take Snapshot
with Orbital



Outcome

Get forensic
context during
Investigation

When to use this Incident Response type?

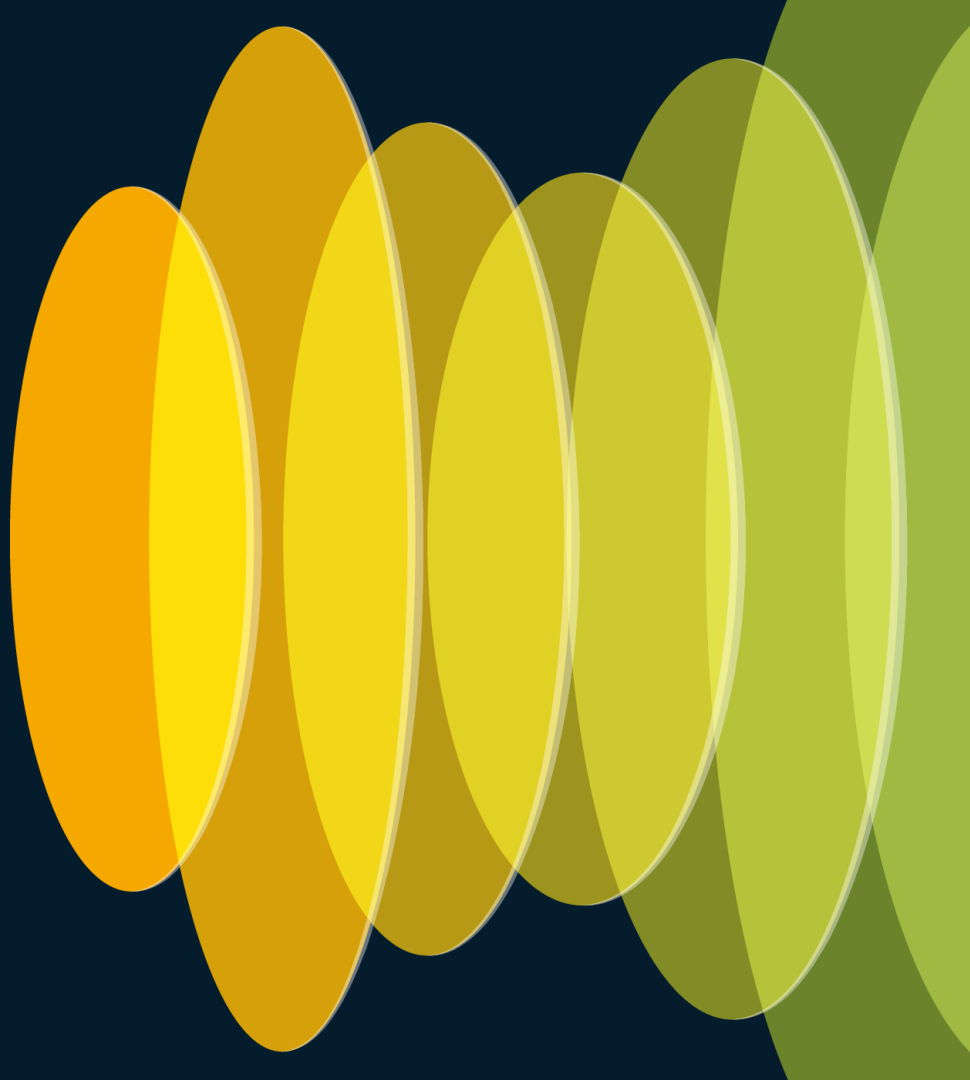
- Quick response actions ideal for senior Security Analyst and Incident Responders.
- Possible to taken actions throughout the XDR UI and Ribbon, not just in the Incident Response tab.
- Currently no Audit Log yet for these actions (other than Workflow Run), which makes them sub-optimal for Containment, Eradication and Recovery.
- Recommendation to use during Investigations and Identification phase.
- Relatively slower compared to Automation Rules.

Agenda

- ~~What is Incident Response?~~
- How to perform Incident Response with Cisco XDR?
 - ~~Introduction to Cisco XDR (Automation)~~
 - ~~Pivot Menu~~
 - Playbook Tasks
 - Automation Rules
- Let's put it to practice!
- Future?



IR with Cisco XDR: Response Playbook Tasks



Use Case > Playbook > Phase > Tasks > Workflow > Atomic

Playbook (e.g. Ransomware Defense)

Phase (e.g. Identification)

Task

Instructions

Workflow(s)

Atomic

Decision(s)



Playbook

Cisco Managed Incident Playbook ⓘ

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

Identification

Containment

Eradication

Recovery

Phase

Review Incident

Add Note

Add a note to record the evidence for assigning a status of Rejected, Open, or Incident Reported.

Analyze Indicators

Add Note

Create judgment(s), as necessary, and add a note confirming any Malicious or Suspicious reputations.

Identify Affected Hosts

Add Note

Add a note with summary of findings on the investigations of hosts found with malicious indicators.

Task

Confirm Incident

Execute

Update the incident status to "Incident Reported" and, if the incident has assignees start a chat room for triage and collaboration

This automation workflow updates the incident status to "Incident Response" and, if the incident has assignees and a compatible messaging integration is enabled, the workflow creates a chat room for incident triage and collaboration.

This workflow should only be used after confirming that the incident involves malicious, improper usage, or unauthorized activity that violates company policy.

Incident Response Workflow

Click **Execute** to run the workflow. The results of this workflow will be visible in the incident Worklog.

Document and Notify

Execute

Create an incident ticket with the appropriate parameters and contextual incident information.

Default Playbook and System Workflows

Workflows

Workflows allow you to investigate security events, automate responses, and eliminate repetitive tasks by using activities, logic, and even other workflows to communicate with other systems and resources. From here you can access, create, and import workflows.

All Workflows 7

Atoms 407

Recents

Favorites 2

Workflows

Import Workflow

Create Workflow

Search

Ready State

Category

Q Search

Select

1 Selected

7 matching results

Reset All

Card View

List View

Category Incident Response

Add to Saved Filters

Display name

Categories

Status

Owner

Last modified

Actions

XDR - Contain Incident: Assets

This workflow consumes one or more hostnames and attempts to iso...

Incident Response

Validated

system

05/01/2024, 14:46:42

...

XDR - Document and Notify

This workflow parses an XDR incident and creates a matching/link...

Incident Response

Validated

system

05/01/2024, 14:46:42

...

XDR - Restore Systems

This workflow consumes one or more hostnames and attempts to un...

Incident Response

Validated

system

21/12/2023, 17:26:23

...

XDR - Identify Vulnerabilities

This workflow consumes one or more hostnames and attempts to fet...

Incident Response

Updated

system

08/12/2023, 17:51:15

...

XDR - Contain Incident: File Hashes

This workflow consumes one or more file hashes and attempts to b...

Incident Response

Validated

system

06/12/2023, 20:47:24

...

XDR - Contain Incident: Domains

This workflow consumes one or more domains and attempts to block...

Incident Response

Validated

system

06/12/2023, 20:47:10

...

XDR - Contain Incident: URLs

This workflow consumes one or more URLs and attempts to block th...

Incident Response

Validated

system

06/12/2023, 20:47:10

...



Look familiar?

Document and Notify

Create an incident ticket with the appropriate parameters and contextual incident information.

Execute

Contain Incident: Assets

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

Contain Incident: Domains

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

Contain Incident: URLs

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

Contain Incident: File Hashes

Contain file hash indicators of compromise to stop the spread of malicious activity.

Identify Vulnerabilities

Scan host(s) for vulnerabilities, add a note about the recommended patches, and add a service request for patching.

Select

Validate Eradicated Hosts and Unquarantine Assets

Confirm and acknowledge eradication steps are working as expected and number of infected host(s) is dropping.

Select

Category Incident Response X Add to Saved Filters v

Display name

Categories

XDR - Contain Incident: Assets

This workflow consumes one or more hostnames and attempts to iso...

Incident Resp

XDR - Document and Notify

This workflow parses an XDR incident and creates a matching/link...

Incident Resp

XDR - Restore Systems

This workflow consumes one or more hostnames and attempts to un...

Incident Resp

XDR - Identify Vulnerabilities

This workflow consumes one or more hostnames and attempts to fet...

Incident Resp

XDR - Contain Incident: File Hashes

This workflow consumes one or more file hashes and attempts to b...

Incident Resp

XDR - Contain Incident: Domains

This workflow consumes one or more domains and attempts to block...

Incident Resp

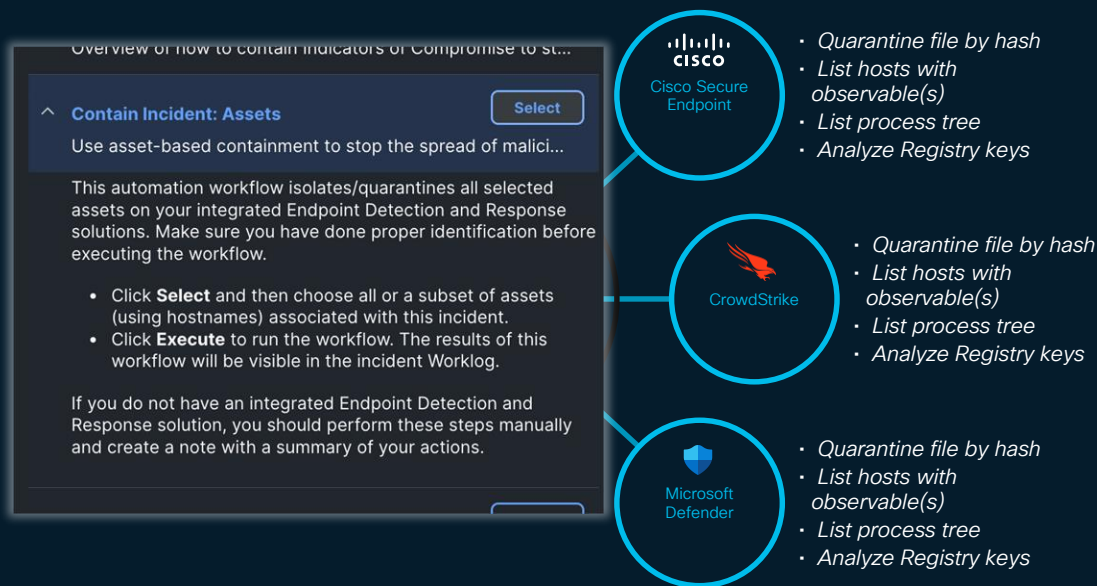
XDR - Contain Incident: URLs

This workflow consumes one or more URLs and attempts to block th...

Incident Resp



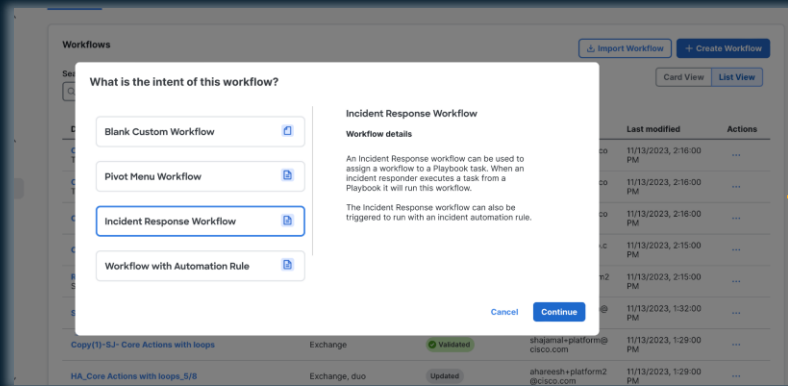
System Workflows are Integration “agnostic”



Incident Response Template

Unified Workflow Template that can be used both for Playbook Tasks and Automation Rules, making them interchangeable and reusable.

Used for Playbook Tasks that work on entire Incident object (e.g. Create ServiceNow Ticket).



New Incident Response Workflow

Incident Response workflows can be used for Playbook Tasks and/or be used with Incident Automation Rules. By selecting this type, you will be able to select the Workflow from the Playbook Editor when editing a Task.

Workflow display name* 33 / 64

Notifying upon confirmed incident

Action(s)*

Notify x

Observable Type(s)*

None (general incident workflow) x

Incident Automation Rule (optional)

Type to search incident rule

Cancel Continue

Document and Notify

Execute

Create an incident ticket with the appropriate parameters and contextual incident information.

This automation workflow creates a ticket in your integrated IT Services Management tool and adds the ticket to this incident.

Click **Execute** to run the workflow. The results of this workflow will be visible in the incident Worklog.

If this task needs to be done manually, gather any missing information below and add it to a ticket:

- Incident title and URL.
- Summary of findings from Review Incident task note.
- Name of targets affected with the device meta data.

New Incident Response Workflow

Incident Response workflows can be used for Playbook Tasks and/or be used with Incident Automation Rules. By selecting this type, you will be able to select the Workflow from the Playbook Editor when editing a Task.

Workflow display name* 33 / 64

Block Domains to Contain Incident

Action(s)*

Contain x

Observable Type(s)*

Domain x

Incident Automation Rule (optional)

Type to search incident rule

Cancel Continue

TEST1 - Malware Executed on MY-DEVICE-42 - Incident by Cisco XDR Auto

Automation on 2024-01-15T10:00:21.000Z

Workflow: View Long Description

Response Working

Contain Incident: IP's

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

Contain Incident: Domains

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

This automation workflow blocks the selected domain names on your integrated network policy enforcement solutions. Make sure you have done proper identification before executing the workflow.

- Click **Select** and then choose all or a subset of domains associated with this incident.
- Click **Execute** to run the workflow. The results of this workflow will be visible in the incident Worklog.

If you do not have an integrated network policy enforcement solution, you should perform these steps manually and create a note with a summary of your actions.

2 Observables

Search

Domain

example@redteam.com 1 event

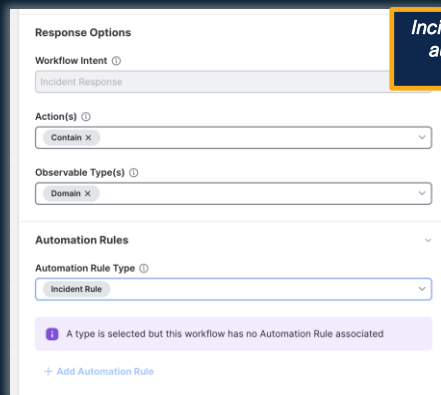
internal@redteam.com 1 event

Actions

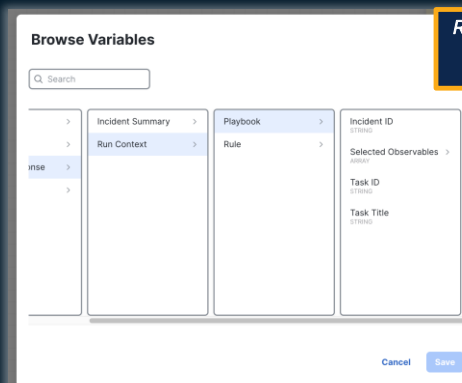
No action

Used for Playbook Tasks that work on specific Incident Observables (e.g. Block IP Addresses on Firewall).

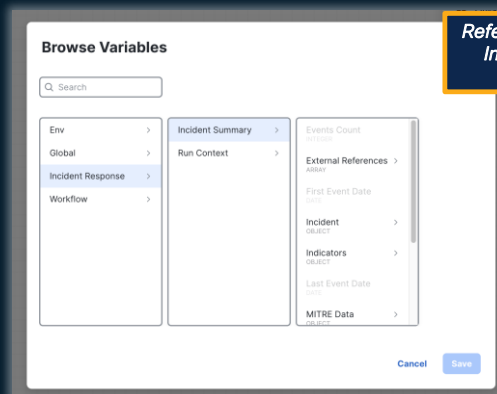
Working with the IR Template



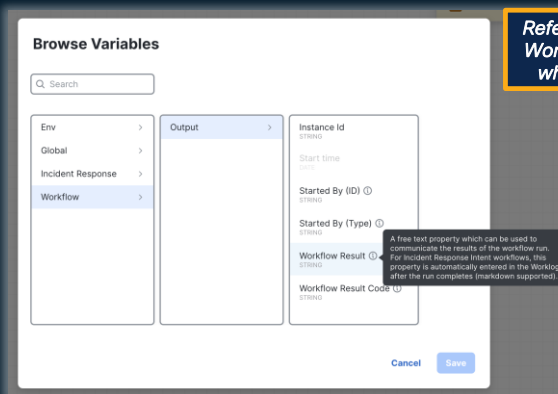
Incident Rule Type will be set automatically, as variable references are unified



Reference to specific fields of Automation Rule (e.g. Rule name or conditions)

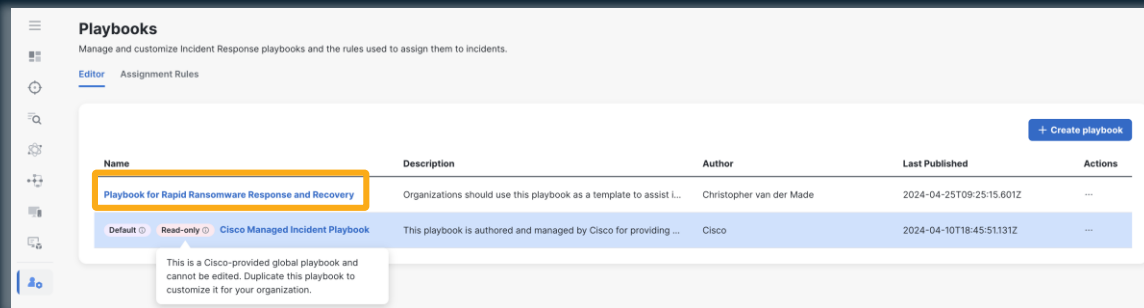


Reference to specific fields of Incident (e.g. Assignees, Priority Score, etc.)



Reference to specific fields of Workflow Run (e.g. when and who/how was it triggered)

The Playbook “Editor”



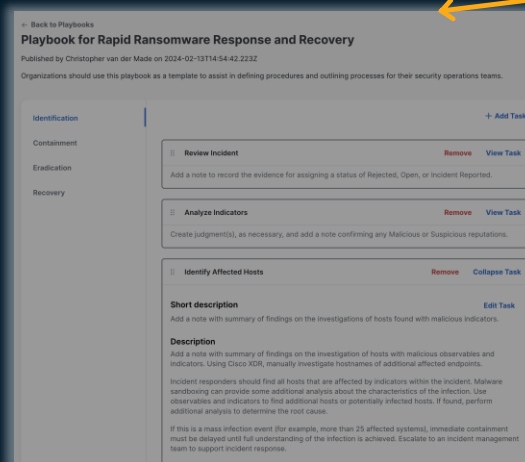
Playbooks
Manage and customize Incident Response playbooks and the rules used to assign them to incidents.

Editor | Assignment Rules

[+ Create playbook](#)

Name	Description	Author	Last Published	Actions		
Playbook for Rapid Ransomware Response and Recovery	Organizations should use this playbook as a template to assist L...	Christopher van der Made	2024-04-25T09:25:15.601Z	...		
Default	Read-only	Cisco Managed Incident Playbook	This playbook is authored and managed by Cisco for providing ...	Cisco	2024-04-10T18:45:51.131Z	...

This is a Cisco-provided global playbook and cannot be edited. Duplicate this playbook to customize it for your organization.



Playbook for Rapid Ransomware Response and Recovery
Published by Christopher van der Made on 2024-02-13T14:54:42.223Z
Organizations should use this playbook as a template to assist in defining procedures and outlining processes for their security operations teams.

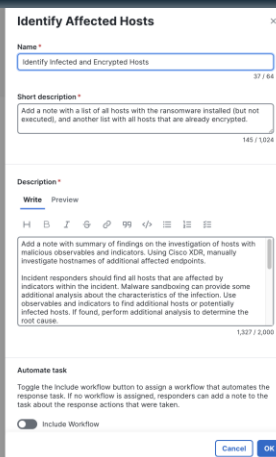
Identification | [+ Add Task](#)

Review Incident [Remove](#) [View Task](#)
Add a note to record the evidence for assigning a status of Rejected, Open, or Incident Reported.

Analyze Indicators [Remove](#) [View Task](#)
Create judgment(s), as necessary, and add a note confirming any Malicious or Suspicious reputations.

Identify Affected Hosts [Remove](#) [Collapse Task](#) [Edit Task](#)
Add a note with summary of findings on the investigations of hosts found with malicious indicators.

Description
Add a note with summary of findings on the investigation of hosts with malicious observables and indicators. Using Cisco XDR, manually investigate hostnames of additional affected endpoints.
Incident responders should find all hosts that are affected by indicators within the incident. Malware sandboxing can provide some additional analysis about the characteristics of the infection. Use observables and indicators to find additional hosts or potentially infected hosts. If found, perform additional analysis to determine the root cause.
If this is a mass infection event (for example, more than 25 affected systems), immediate containment must be delayed until full understanding of the infection is achieved. Escalate to an incident management team to support incident response.



Identify Affected Hosts

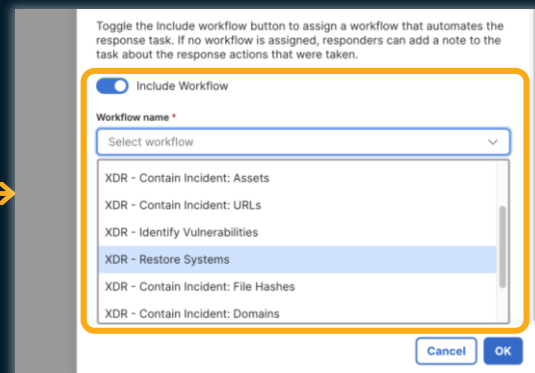
Name *
Identify Infected and Encrypted Hosts 37 / 64

Short description *
Add a note with a list of all hosts with the ransomware installed (but not executed), and another list with all hosts that are already encrypted. 145 / 1024

Description *
Write **Preview**
Add a note with summary of findings on the investigation of hosts with malicious observables and indicators. Using Cisco XDR, manually investigate hostnames of additional affected endpoints.
Incident responders should find all hosts that are affected by indicators within the incident. Malware sandboxing can provide some additional analysis about the characteristics of the infection. Use observables and indicators to find additional hosts or potentially infected hosts. If found, perform additional analysis to determine the root cause. 1,337 / 2,000

Automate task
Toggle the Include workflow button to assign a workflow that automates the response task. If no workflow is assigned, responders can add a note to the task about the response actions that were taken.
☐ Include Workflow

[Cancel](#) [OK](#)



Toggle the Include workflow button to assign a workflow that automates the response task. If no workflow is assigned, responders can add a note to the task about the response actions that were taken.

☒ Include Workflow

Workflow name *
Select workflow

- XDR - Contain Incident: Assets
- XDR - Contain Incident: URLs
- XDR - Identify Vulnerabilities
- XDR - Restore Systems**
- XDR - Contain Incident: File Hashes
- XDR - Contain Incident: Domains

[Cancel](#) [OK](#)

The Playbook “Assignment Rules”

New Playbook Assignment Rule ✕

⚠️ You have unsaved changes ⓘ

Title*
Ransomware TTPs

Description*
Assign my Cisco XDR Playbook to a Ransomware Incident

Conditions

☒ ALL of these conditions must be met
☐ ANY of these conditions can be met

Property	Comparison	Value	
Global - Incident > Scores	Greater than or eq...	750	...
Title - MITRE Data > Data > All ite...	Equal	Impact	...
All Items - Incident > Techniques	Equal	T1486	...

[+ Add Condition](#)

Playbook
Cisco XDR Playbook

Cancel OK

Incidents

Blocked Command and Control DNS Activities

Created via Umbrella 2m ago · [Linked Incidents](#)

A device is involved in excessive malicious Command and Control communication, which is already flagged and blocked by Umbrella. The Command and Control traffic may be blocked. [View More](#)

Overview Detection **Response** Worklog

Cisco XDR Playbook ⓘ Decision text of the playbook will be shown here.
Published: August 6, 2023 at 10:09:00 PM

Identify Affected Hosts [Add Note](#)
Add note with summary of findings on the investigations of hosts found with malicious indicators. [more](#)

Containment [Exclude](#)
Contain Incident: Overview
Overview of how to contain Indicators of Compromise to stop the spread of malicious activity. [more](#)

Eradication [Select](#)
Contain Incident: Assets
Use asset-based containment to stop the spread of malicious activity. [more](#)

Recovery [Select](#)
Contain Incident: IPs
Contain IP indicators of compromise to stop the spread of malicious activity. [more](#)

[Select](#)
Contain Incident: Domains
Contain domain indicators of compromise to stop the spread of malicious activity. [more](#)

[Select](#)
Contain Incident: URLs
Contain URL indicators of compromise to stop the spread of malicious activity. [more](#)

[Select](#)
Contain Incident: File Hashes
Contain file hash indicators of compromise to stop the spread of malicious activity. [more](#)

[Add Note](#)
Implement Additional Monitoring
Implement additional monitoring that reviews not only host/network containment or eradication success. [more](#)

[Add Note](#)
Identify Vulnerabilities

[Back](#) [Go to Eradication](#)

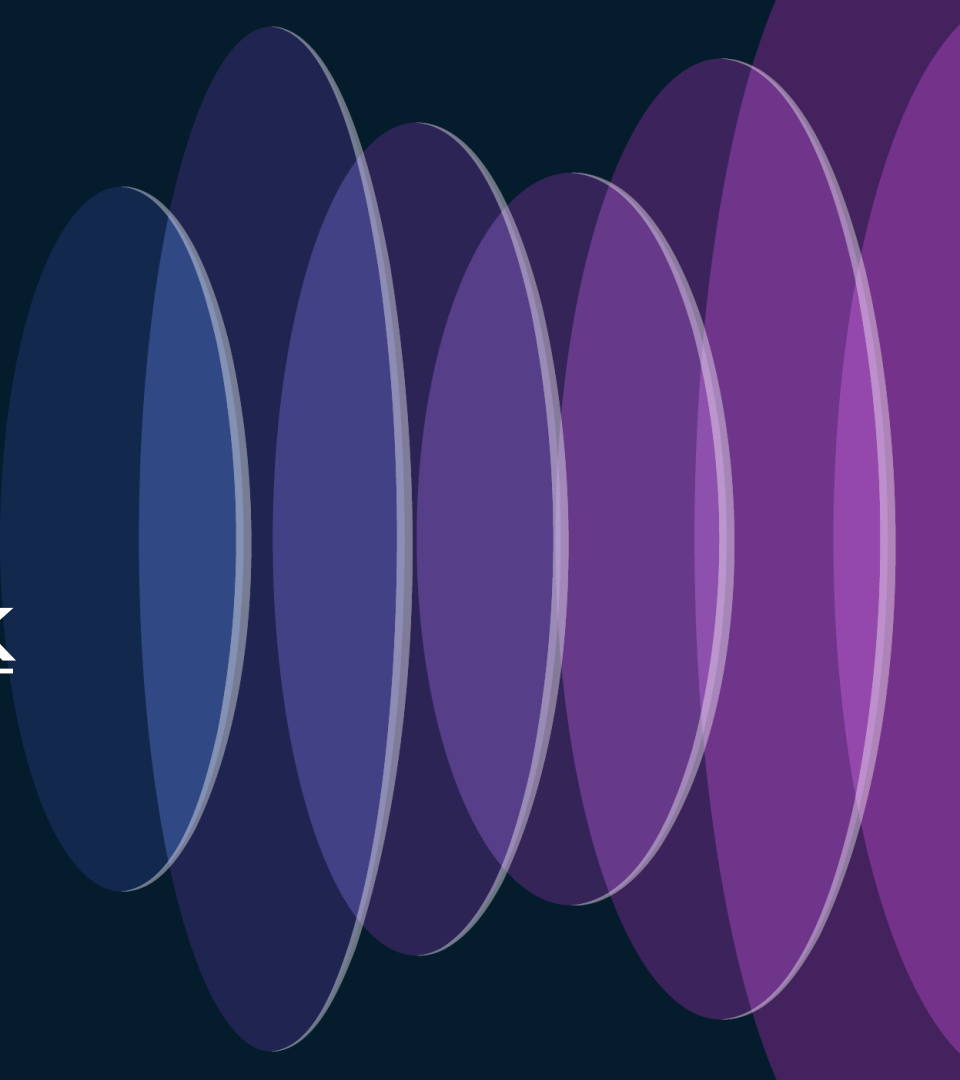
Response Action Log [View Notes](#) [Export](#)

- 2022-02-12 21:10:45 AM
Marked Contain Incident: Assets as complete
- 2022-02-12 21:10:15 AM
Executed workflow for Contain Incident: Assets

[View](#)



Demo: Using the Response Playbook



Cisco XDR - AutomateCisco XDR - IncidentsResults | Orbital

xdr.us.security.cisco.com/incidents/incident-64322795-2aa5-49bd-8d0b-106680ae434a/response

All Bookmarks

Cisco XDR

4

Cisco XDR

4

Christopher Van ...
explorcorp

Incidents

1000Open

CHRIVAND CLUS - Malware Executed on MY-DEVICE-42 - Incident by Cisco XDR Automation

Reported by Cisco XDR Automation on 2024-05-23T11:10:29.640Z

View detailed description

Created by an Automation workflow.

OverviewDetectionResponseWorklogReport

View Investigation

Cisco Managed Incident Playbook

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

Identification

Containment

Eradication

Recovery

Review Incident

Add Note

Add a note to record the evidence for assigning a status of Rejected, Open, or Incident Reported.

Analyze Indicators

Add Note

Create judgment(s), as necessary, and add a note confirming any Malicious or Suspicious reputations.

Identify Affected Hosts

Add Note

Add a note with summary of findings on the investigations of hosts found with malicious indicators.

Confirm Incident

Execute

Update the incident status to "Incident Reported" and, if the incident has assignees start a chat room for triage and collaboration

This automation workflow updates the incident status to "Incident Response" and, if the incident has assignees and a compatible messaging integration is enabled, the workflow creates a chat room for incident triage and collaboration.

This workflow should only be used after confirming that the incident involves malicious, improper usage, or unauthorized activity that violates company policy.

Click **Execute** to run the workflow. The results of this workflow will be visible in the incident Worklog.

Document and Notify

Execute

Create an incident ticket with the appropriate parameters and contextual incident information.

Actions taken

No actions taken

#CiscoLive

BRKSEC-2502

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

74

Cisco XDR - AutomateCisco XDR - IncidentsResults | Orbital

xdr.us.security.cisco.com/incidents/incident-64322795-2aa5-49bd-8d0b-106680ae434a/worklog/notes

All Bookmarks

XDR

XDR4

Christopher Van ...explorcorp

Incidents

1000Incident Reported

CHRIVAND CLUS - Malware Executed on MY-DEVICE-42 - Incident by Cisco XDR Automation

Reported by Cisco XDR Automation on 2024-05-23T11:10:29.640Z

View detailed description

Created by an Automation workflow.

OverviewDetectionResponseWorklogReport

View Investigation

NotesAudit Log

Sort by: NewestAdd Note

Created by: Automation Workflow

2024-05-23T11:28:14.695Z

[RESPONSE TASK] Confirm Incident

XDR - Confirm Incident started by chrivand@cisco.com completed successfully:

Incident status updated to Incident Reported.

Webex room Cisco XDR Incident: CHRIVAND CLUS - Malware Executed on MY-DEVICE-42 - Incident. created successfully.

Added "chrivand@cisco.com" to Webex room.

Created by: Automation Workflow

2024-05-23T11:27:55.962Z

[RESPONSE TASK] Confirm Incident

Workflow: XDR - Confirm Incident started by chrivand@cisco.com

Created by: Automation Workflow

2024-05-23T11:11:26.918Z

[AUTOMATION RULE]

Cohesity - Take Protection Group Snapshot for Affected VMs started by Score greater than 800 completed successfully:

Cisco XDR Incident: CHRIVAND CLUS - Malware Executed on MY-DEVICE-42 - Inciden... ☆

Messages

People (2)

Content

Meetings

+

Apps

Meet

🔍

🔍

⚙️

This starts the 'Cisco XDR Incident: CHRIVAND CLUS - Malware Executed on MY-DEVICE-42 - Inciden...' space, created by Bots by Christopher. 13:28

Bots by Christopher

13:28

Cisco XDR

New Incident

Title: CHRIVAND CLUS - Malware Executed on M...

Source: Cisco XDR Automation

Score: 1000

This is a new Incident, created by an Automation workflow.

> This is an example ransomware Incident, where 2 devic...

View Incident

This Webex room was created by Cisco XDR automation for the incident CHRIVAND CLUS - Malware Executed on MY-DEVICE-42 - Incident by Cisco XDR Automation after it was confirmed by chrivand@cisco.com for collaboration on next steps to resolve the incident. Please remember to add notes to the incident worklog to document actions taken.

Bots by Christopher added you to this space. Welcome. 13:28

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

🔍

Shift + Enter for a new line

Write a message to Cisco XDR Incident: CHRIVAND CLUS - Malware Executed on MY-DEVICE-42 - Inciden...

✓

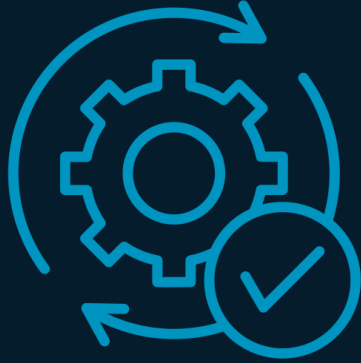
➤

#CiscoLive

BRKSEC-2502

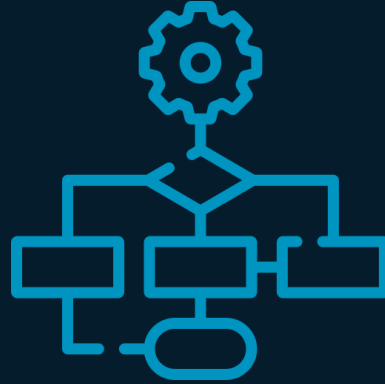
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

76



Trigger

Task from
Playbook



Operation

Confirm
Incident with
Webex

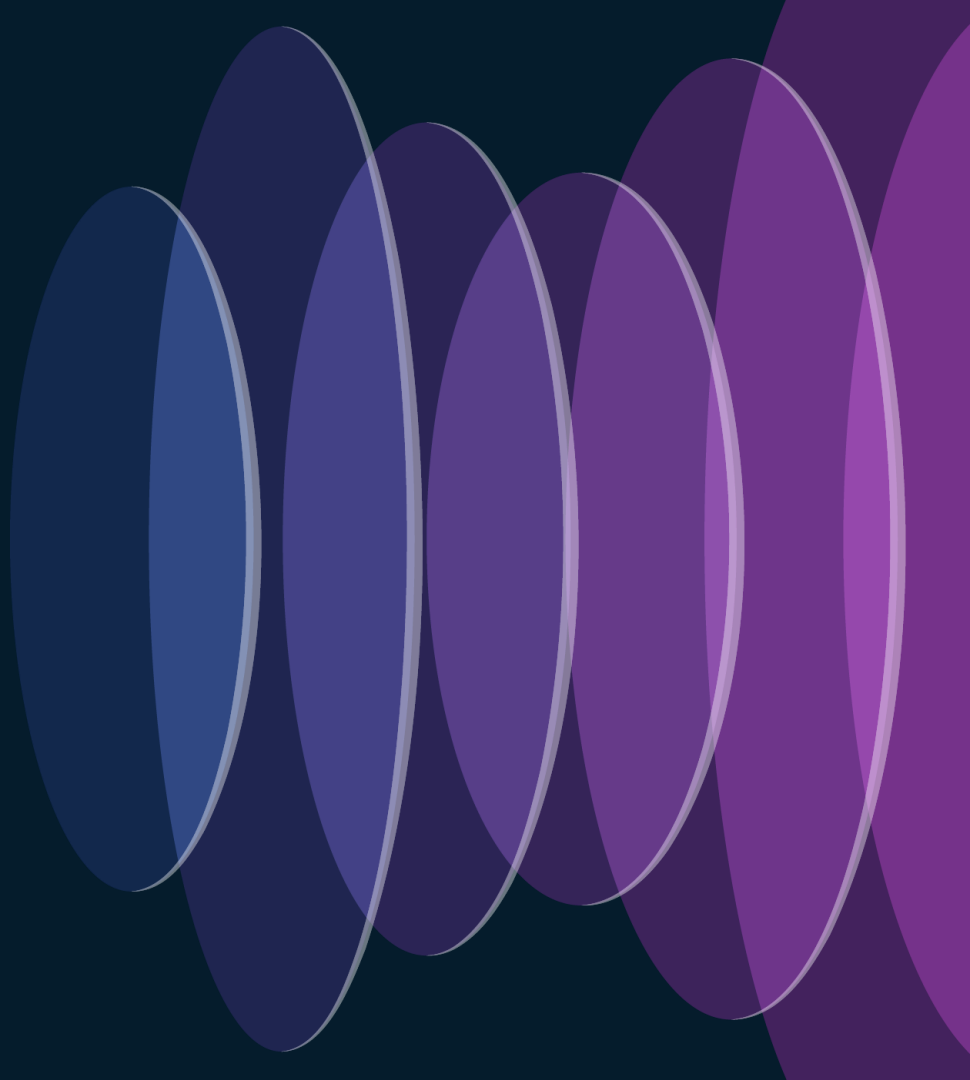


Outcome

Incident
Confirmed and
War Room
Created



Demo: Build your own Playbook



Cisco XDR - AutomateCisco XDR - AdministrationCisco XDR - AutomateResults | Orbital

xdr.us.security.cisco.com/administration/playbooks

XDR

XDR

XDR

Christopher Van ...explorcorp

Playbooks

Manage and customize Incident Response playbooks and the rules used to assign them to incidents.

EditorAssignment Rules

+ Create playbook

Name	Description	Author	Last Published	Actions
Christopher's Demo Playbook with Webex	This should be used for demo purposes only.	Christopher van der Made	2024-05-23T11:50:58.120Z	...
My Custom Playbook	—	Hanna Jabbour	2024-05-09T11:12:42.101Z	...
RSA Incident Playbook	—	Matt Vander Horst	2024-04-25T14:23:21.834Z	...
Default ⓘ Read-only ⓘ Cisco Managed Incident Playbook	This playbook is authored and managed by Cisco for providing a defa...	Cisco	2024-04-10T18:45:51.131Z	...
Cisco Auto... <div>This is a Cisco-provided global playbook and cannot be edited. Duplicate this playbook to customize it for your organization.</div>	This playbook is authored and managed by Cisco for providing a defa...	Rob Gresham	2024-04-01T16:21:31.383Z	...
AJ's test pla...	Playbook to test	AJ Shipley	2024-03-28T19:30:45.630Z	...





Cisco XDR - AutomateCisco XDR - AdministrationCisco XDR - AutomateResults | Orbital

xdr.us.security.cisco.com/administration/playbooks/ac125490-ead7-4990-b0a4-1cf7712d668a?phaseld=be9fc1a0-3ebd-4934-9c3d-bb9ea4d0c663

All Bookmarks

XDR

XDR

    Christopher Van ...
explorcorp

Back to Playbooks

Christopher's Demo Playbook with Webex

Published by Christopher van der Made on 2024-05-23T11:50:00.956Z
This is used for demo purposes only.

Set as default playbookEdit Playbook

Identification

Containment

Eradication

Recovery

Placeholder Task TitleView Task

Placeholder task description.

Workflows

Workflows allow you to investigate security events, automate responses, and eliminate repetitive tasks by using activities, logic, and even other workflows to communicate with other systems and resources. From here you can access, create, and import workflows.

All Workflows 68 Atomics 475 Recents Favorites 1

Workflows

Search Status

Q Search Select

Display name

CHRVIVAND - Cisco Live Vegas: Playbook Task Work
Creates a Webex space and adds the user who executed the task.

CHRVIVAND - Cisco Live Vegas: Send User Webex Message
Send a warning message to a user (using the Pivot Menu Workflow).

CHRVIVAND - Cisco Live Vegas: Create Incident with Automation Rule
This is a sample workflow how to create an Incident with Automation Rule.

Cohesity - Take Protection Group Snapshot for Affected VMs
This workflow is triggered by an automation rule when a VM is affected.

Cohesity - Identify Restore Point for Affected Virtual Machine
This workflow is triggered by an automation rule as soon as a VM is affected.

Cisco Orbital - Take Forensic Snapshot (Windows) for Malware Analysis
This workflow initiates a Cisco Orbital forensic snapshot for malware analysis.

Talos - Blog Post to XDR Casebook
This workflow takes a Talos blog post, conducts an investigation, and creates a casebook entry.

Talos - Get New Blog Posts
This workflow consumes the Talos Intelligence Blog RSS feed and updates the casebook.

Duplicate Incident based on Attack Chain ID

What is the intent of this workflow?

Blank Custom Workflow

Incident Response Workflow

Pivot Menu Workflow

Workflow with Automation Rule

Incident Response Workflow

Workflow details

Incident Response workflows can be used for Playbook Tasks and/or be used with Incident Automation Rules. By selecting this type, you will be able to select the Workflow from the Playbook Editor when editing a Task.

Cancel Continue

Last modified	Actions
23/05/2024, 13:45:44	...
23/05/2024, 13:42:03	...
23/05/2024, 13:41:54	...
23/05/2024, 13:11:20	...
23/05/2024, 13:11:20	...
23/05/2024, 12:31:42	...
22/05/2024, 23:30:26	...
22/05/2024, 23:30:02	...

Cisco XDR - AutomateCisco XDR - AdministrationCisco XDR - AutomateResults | Orbital

xdr.us.security.cisco.com/automate/workflows

XDR

Christopher Van ...explorcorp

Workflows

Workflows allow you to investigate security events, automate responses, and eliminate repetitive tasks by using activities, logic, and even other workflows to communicate with other systems and resources. From here you can access, create, and import workflows.

All Workflows 68Atomics 475RecentsFavorites 1

SearchStatusCategory

SearchSelectSelect

Display name

CHIRIVAND - Cisco Live Vegas: Playbook Task Workflow wit...

Creates a Webex space and adds the user who executed the Play...

CHIRIVAND - Cisco Live Vegas: Send User Webex Message

Send a warning message to a user (using the Pivot Menu on an...

CHIRIVAND - Cisco Live Vegas: Create Incident w. resolve...

This is a sample workflow how to create a Incident using the...

Cohesity - Take Protection Group Snapshot for Affected...

This workflow is triggered by an automation rule when an inci...

Cohesity - Identify Restore Point for Affected Virtual...

This workflow is triggered by an automation rule as soon as a...

Cisco Orbital - Take Forensic Snapshot (Windows)

This workflow initiates a Cisco Orbital forensic snapshot for...

Talos - Blog Post to XDR Casebook

This workflow takes a Talos blog post, conducts an investigat...

Talos - Get New Blog Posts

This workflow consumes the Talos Intelligence Blog RSS feed a...

Duplicate Incident based on Attack Chain ID

Import WorkflowCreate Workflow

Card ViewList View

Owner	Last modified	Actions
chrivand@cisco.com	23/05/2024, 13:45:44	...
chrivand@cisco.com	23/05/2024, 13:42:03	...
chrivand@cisco.com	23/05/2024, 13:41:54	...
adisanka+explor@cisco.com	23/05/2024, 13:11:20	...
adisanka+explor@cisco.com	23/05/2024, 13:11:20	...
robgresh+explor@cisco.com	23/05/2024, 12:31:42	...
mavander@cisco.com	22/05/2024, 23:30:26	...
mavander@cisco.com	22/05/2024, 23:30:02	...
chrisand@cisco.com	23/05/2024, 13:41:54	...

New Incident Response Workflow

Incident Response workflows can be used for Playbook Tasks and/or be used with Incident Automation Rules. By selecting this type, you will be able to select the Workflow from the Playbook Editor when editing a Task.

Workflow display name* 62 / 64

CHIRIVAND - Cisco Live Vegas: Playbook Task Workflow w

Action(s)*

Notify X

Observable Type(s)*

None (general incident workflow) X

Incident Automation Rule (optional)

Type to search incident rule

CancelContinue

#CiscoLive

BRKSEC-2502

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

82

← Back to all Workflows

CHRIVAND - Cisco Live Vegas: Playbook Task Workflow with Webex

Last Modified: 23 May 2024 at 13:45:34

Workflow is locked

Share

Validated

View Runs

Run

Settings

START

Atomic
Webex - Create Room

Atomic
Webex - Add Member to Room

Atomic
Webex - Post Message to Room

Core
Set Workflow Result Output

END

Q

+

-

Workflow Properties

CHRIVAND - Cisco Live Vegas: Playbook Task Workflow With Webex

General

Display Name*62 / 64

CHRIVAND - Cisco Live Vegas: Playbook Task Workflow with Webex

Owner

chrivand@cisco.com

Description77 / 1024

Creates a Webex space and adds the user who executed the Playbook Task to it.

☐ 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 left.

Category

CHRIVAND

Variables

Name	Type	Scope	Value	Required
------	------	-------	-------	----------

#CiscoLive

BRKSEC-2502

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

83

Cisco XDR - Automate x Cisco XDR - Administration x Cisco XDR - Automate x Results | Orbital x +

← → ↺ xdr.us.security.cisco.com/administration/playbooks/ac125490-ead7-4990-b0a4-1cf7712d668a?phaseId=3a86e8fc-c927-4021-9847-9178e7ab8654

🔍 ☆ ⓘ ⌵ 📁 All Bookmarks

XDR 4

4 Christopher Van ... explorcorp

← Back to Playbooks

Christopher's Demo Playbook with Webex

Published by Christopher van der Made on 2024-04-24T09:28:25.582Z
This is used for demo purposes only.

Cancel Publish Playbook

You have unpublished changes.

Identification

Containment

Eradication

Recovery

Create a Webex Space! Remove Collapse Task

Summary

This will create a new Webex space. Demo purposes only!

Description

Click **Execute** to create a Webex space and to add yourself to it. Demo purposes only!

Automate task

Workflow name

CHRIVAND - Cisco Live Vegas: Playbook Task Workflow with Webex

Workflow description

Creates a Webex space and adds the user who executed the Playbook Task to it.

Action(s)

Notify

Observable type(s)

None

#CiscoLive

BRKSEC-2502

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


85


Cisco XDR - Incidents x Cisco XDR - Administration x Cisco XDR - Automate x Results | Orbital x +





← → ↺ xdr.us.security.cisco.com/administration/playbooks/assignments?drawer=rule&drawerRuleId=02EK1K7O7QZDP1cmspmFXVD1rpOQLLx1JJL

🔍 ☆ ⓘ ⌵ ⌵ ⌵ ⌵ ⌵









All Bookmarks

 XDR

 XDR 4

   4  Christopher Van ... explorcorp ⌵

☰


Playbooks

Manage and customize Incident Response playbooks and the rules used to assign them to incidents.

Editor Assignment Rules

⋮


1

 On

Christopher's Demo Rule

⋮


2

 On

Ransomware Recovery Playbook

⋮

3


 On

Score > 800

If no rules match above then the default playbook [Cisco Managed Incident Playbook](#) will be assigned to the incident

Christopher's Demo Rule

Last modified by Christopher van der Made on 2024-05-23T11:53:50.119Z

 You have unsaved changes ⓘ

Title*

Christopher's Demo Rule

23 / 64



Description*

Assigns my demo Playbook to my own Incidents with CHRIVAND prefix :)

68 / 1,024

Conditions*

☒ ALL of these conditions must be met
☐ ANY of these conditions can be met

Property	Comparison	Value	
Title - Incident	Matches wildcard	*CHRIVAND*	
All items - Incident > Tactics	Includes	Command and Con...	

[+ Add Condition](#)

Playbook*

Christopher's Demo Playbook with Webex

This playbook will be assigned to a new incident when the above conditions are met.

Delete

Cancel

Save




Cisco XDR - Administration xCisco XDR - Incidents xCisco XDR - Automate xResults | Orbital x+

xdr.us.security.cisco.com/incidents/incident-f9255fc5-cd53-4391-85e7-05b6b87b3c14/response


All Bookmarks

XDR

XDR4



4



Christopher Van ...
explorcorp

Incidents

1000Open

CHRIVAND Malware Executed on MY-DEVICE-42 - Incident by Cisco XDR Automation

Reported by Cisco XDR Automation on 2024-05-23T12:02:13.701Z

View detailed description

Created by an Automation workflow.

OverviewDetectionResponseWorklogReport

Christopher's Demo Playbook with Webex

Published May 23, 2024 at 11:50:58 AM

Identification

Containment

Eradication

Recovery

Create a Webex Space!

This will create a new Webex space. Demo purposes only!

Execute

Actions taken

No actions taken

Incident: CHRIVAND Malware Executed on MY-DEVICE-42 - Incident by Cisco XDR Automation ☆

Messages

People (2)

Content

Meetings

+

Apps

Meet

🔍

🔍

⚙️

This starts the 'Incident: CHRIVAND Malware Executed on MY-DEVICE-42 - Incident by Cisco XDR Automation' space, created by Bots by Christopher, 14:11

Bots by Christopher added you to this space. Welcome, 14:11

Bots by Christopher 14:11

New Incident Confirmed: CHRIVAND Malware Executed on MY-DEVICE-42 - Incident by Cisco XDR Automation

Use this space to collaborate and discuss the Incident Response plan. Do not forget to document your actions taken in the Incident Worklog!

Seen by

🔗

📎

🖼️

📄

🗣️

📺

🎤

📌

🔍

Write a message to Incident: CHRIVAND Malware Executed on MY-DEVICE-42 - Incident by Cisco XDR Automation

✓

▶

#CiscoLive

BRKSEC-2502

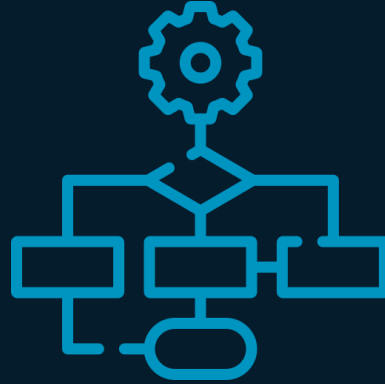
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Public

89



Trigger

Task from
Playbook



Operation

Webex Space
Created



Outcome

Demo

When to use this Incident Response type?

- Guided response ideal for junior Security Analysts and Incident Responders.
- Structure allows for following the proper processes when an Incident has been declared.
- Every response action is automatically entered into the Incident Worklog.
- Relatively slower compared to Automation Rules.

Agenda

- ~~What is Incident Response?~~
- How to perform Incident Response with Cisco XDR?
 - ~~Introduction to Cisco XDR (Automation)~~
 - ~~Pivot Menu~~
 - ~~Playbook Tasks~~
 - Automation Rules
- Let's put it to practice!
- Future?



IR with Cisco XDR: Automation Rules



Automation Rules

- Allow various types of events to cause workflows to run.
 - **Approval Task Rule:** An approval task is acted upon within XDR Automation.
 - **Email Rule:** An email is received in a pre-defined inbox being monitored for new messages.
 - **Incident Rule:** A matching incident is created in the XDR incident manager.
 - **Schedule Rule:** A specific date, time, or interval of time has passed.
 - **Webhook Rule:** An HTTP call was made to a specific webhook URL.

Triggers

To add a trigger to a workflow, configure an automation rule that determines when a workflow is executed, such as on a schedule or when an incident or specific event occurs.

[Reference slide](#)

Automation Rules

Events

Webhooks

Calendars

Schedules

Rule Type

Incident Rules

Other Rules

Search

Search

Priority Incident Rules

Order	Off/on	Display name	Description
1	<input checked="" type="checkbox"/>	Full Scan with Orbital	
2	<input checked="" type="checkbox"/>	My Ransomware Rule	Mitre Tactic Condition
3	<input type="checkbox"/>	My Catch All Rule	[NO CONDITIONS]
4	<input type="checkbox"/>	Demo Rule for Webex Notification	

Standalone Incident Rules

Order	Off/on	Display name	Description
N/A	<input checked="" type="checkbox"/>	Catch all rule for Testing	
N/A	<input type="checkbox"/>	Test Rule Severity	
N/A	<input type="checkbox"/>	Automation Rule for Inspector Poirot	
N/A	<input type="checkbox"/>	Create ServiceNow Ticket for Phishing + C2 Incidents	



Incident rules

- Evaluated when an incident is created in XDR and prioritization and enrichment are complete. Triggers for all Incidents with a priority score and status “New”.*
- Each rule can be configured with its own Conditions and one or more workflows to execute if the criteria are matched.
- Rules can either be in priority order or standalone:
 - Priority rules are evaluated from the top down in order. They can be configured to stop processing of subsequent rules or to continue to the next rule.
 - Standalone rules are evaluated for all incidents.

* soon will trigger on all incident status changes.

Create as priority or standalone rule

Standalone rules will always process if conditions match and not be able to be ordered with priority.

☒ Priority Rule

☐ Standalone Rule

[Reference slide](#)

Stop processing subsequent rules

☒ Stop processing subsequent rules

Enabling this will stop processing any further rules. Disabling means your lower priority rules will also be processed.

Standalone rules will always process if conditions match and not be able to be ordered with priority.

Stop processing subsequent rules

Enabling this will stop processing any further rules. Disabling means your lower priority rules will also be processed.

Conditions

Type of Condition Property

MAIN

+ Add Condition

Browse Variables

Q Search

Incident Rule >

Events Count
INTEGER

First Event Date
DATE

Incident
OBJECT

Indicators
OBJECT

Last Event Date
DATE

MITRE Data
OBJECT

Observables
OBJECT

Source
STRING

Status
STRING

Tactics
ARRAY

Techniques
ARRAY

Timestamp
DATE

Title
STRING

Cancel

Save

Describe your Incident type to trigger on...

Conditions

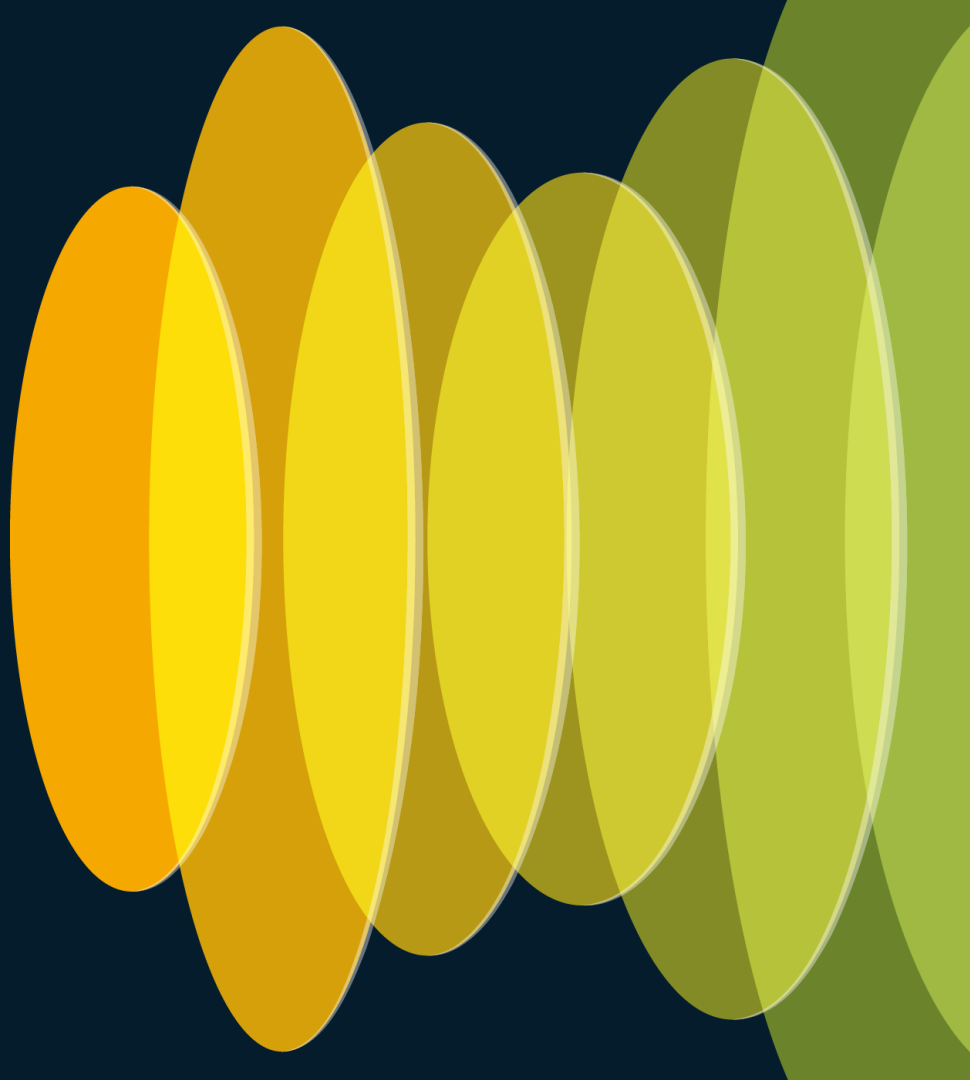
☒ ALL of these conditions must be met
 ☐ ANY of these conditions can be met
 ☐ Advanced

Property	Comparison	Value	
All Items (list) - Incident > Techniques	Includes (case insensitive)	T1486	...
AND			
Description - Incident	Matches wildcard	*ransomware*	...
AND			
Title - Incident	Matches wildcard	*MY-DEVICE-42*	...

[+ Add Condition](#)



Demo: Build an Incident Automation Rule



Triggers

Automation Rules Events Webhooks Calendars Schedules

Rule Type

Incident Rules

Other Rules

Search

🔍 Search

Priority Incident Rules

Standalone Incident Rules

Cisco XDR - Automate

xdr.us.security.cisco.com/automate/triggers/automation-rules/new

Finish update

All Bookmarks

XDR

XDR

Christopher Van ...
explorcorp

Automation Rules

New Ransomware and Encryption Rule

General

Automation Rule matching criteria is based on incident or other metadata, and associated with a set of automation actions by selecting workflows.

Tip: Use exclusive rules to avoid having multiple rules activated for the same trigger. For incident rules you can also use rule priority in combination with the stop processing setting.

Type

Incident Rule

Title*

30 / 64

Ransomware and Encryption Rule

Description

91 / 1024

This rule will trigger when an incident is created with ransomware and encryption symptoms.

Create as priority or standalone rule

Standalone rules will always process if conditions match and not be able to be ordered with priority.

Priority Rule

Standalone Rule

Stop processing subsequent rules

Enabling this will stop processing any further rules. Disabling means your lower priority rules will also be processed.

Stop processing subsequent rules

Cisco XDR - Automate

xdr.us.security.cisco.com/automate/triggers/automation-rules/new

Finish update

All Bookmarks

Cisco XDR

Cisco XDR

Christopher Van ...
explorcorp

Stop processing subsequent rules

Enabling this will stop processing any further rules. Disabling means your lower priority rules will also be processed.

Conditions

ALL of these conditions must be met

ANY of these conditions can be met

Advanced

Property

+ Add Condition

Apply to selected workflows

Select and configure a workflow to associate with this rule, and when the rule is created, its trigger is automatically added to the workflow

+ Add Workflow

Browse Variables

Search

Events Count
INTEGER

External References >
ARRAY

First Event Date
DATE

Incident >
OBJECT

Indicators >
OBJECT

Last Event Date
DATE

Observables >
OBJECT

Short Description
STRING

Source
STRING

Status
STRING

Tactics >
ARRAY

Techniques >
ARRAY

Timestamp
DATE

Title
STRING

First
STRING

All Items (list) <div>✓</div>
STRING

Last
STRING

Cancel

Save

Workflow is required

#CiscoLive

BRKSEC-2502

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

100

Cisco XDR - Automate

xdr.us.security.cisco.com/automate/triggers/automation-rules/new

Finish update

All Bookmarks

XDR

4

XDR

Christopher Van ...

explorcorp

Stop processing subsequent rules

Stop processing subsequent rules

Enabling this will stop processing any further rules. Disabling means your lower priority rules will also be processed.

Conditions

ALL of these conditions must be met

ANY of these conditions can be met

Advanced

Property

All Items (list) - Incident > Techniques

Comparison

Includes

Value

encr

Data Encrypted for Impact (T1486)

Encrypted Channel (T1573)

Weaken Encryption (T1600)

+ Add Condition

Apply to selected workflows

Select and configure a workflow to associate with this rule, and when the rule is created, its trigger is automatically added to the workflow

Workflow: None Selected

On

Select workflow

Type to search workflows

Workflow is required

+ Add Workflow

#CiscoLive

BRKSEC-2502

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

101

Cisco XDR - Automate

xdr.us.security.cisco.com/automate/triggers/automation-rules/new

Finish update

All Bookmarks

Cisco XDR

XDR

Christopher Van ...

explorcorp

Enabling this will stop processing any further rules. Disabling means your lower priority rules will also be processed.

Conditions

☒ ALL of these conditions must be met

☐ ANY of these conditions can be met

☐ Advanced

Property	Comparison	Value
All Items (list) - Incident > Techniques	Includes	Data Encrypted for Impact (T1486)
AND		
Title - Incident	Matches wildcard	*MY-DEVICE-42*
AND		
Status - Incident	Equals	New
AND		
Global - Incident > Scores	Greater than or equals	750

+ Add Condition

Apply to selected workflows

Workflow: None Selected

Select workflow

Cisco XDR - Automate

xdr.us.security.cisco.com/automate/triggers/automation-rules/new

Finish update

All Bookmarks

XDR

XDR

Christopher Van ...
explorcorp

Apply to selected workflows

Select and configure a workflow to associate with this rule, and when the rule is created, its trigger is automatically added to the workflow

Workflow: XDR - Automation Rule - Update Incident Properties

On

Select workflow

XDR - Automation Rule - Update Incident Properties

Assignees (String)

chrivand@cisco.com

Short Description (String)

Title (String)

VEGAS - [\$Rules.IncidentRule.output.Incident.Title\$]

Severity (String)

Status (String)

Open

Description (String)

+ Add Workflow

Turn on this automation rule

Automation rule is on

Incidents

1000

Open

VEGAS - Malware Executed on MY-DEVICE-42 - Incident by Cisco XDR Automation

CM

Reported by Cisco XDR Automation on 2024-05-28T08:32:41.257Z - 2 Linked Incidents

View detailed description

Created by an Automation workflow.

Overview

Detection

Response

Worklog

Report

View Investigation

Notes

Audit Log

Sort by: Newest

Add Note

>

Assignees added by: [Private]

2024-05-28T08:33:37.036Z

>

Status changed by: [Private]

2024-05-28T08:33:37.036Z

▼

Title changed by: [Private]

2024-05-28T08:33:37.036Z

After:

VEGAS - Malware Executed on MY-DEVICE-42 - Incident by Cisco XDR Automation

Before:

Malware Executed on MY-DEVICE-42 - Incident by Cisco XDR Automation

●

Incident Promoted by: [Private]

2024-05-28T08:32:41.409Z

10

per page

1-5 of 5

<<

<

1

/ 1

>

>>

Automation Rules work in real-time*

The image displays the Cisco XDR Automation Rules interface. At the top, a table lists automation rules. The first rule, 'Malware Executed on MY-DEVICE-42 - Incident by Cisco XDR Automati...', has a priority of 1000, is assigned to 'Unassigned', and has a status of 'New'. Below this, a modal window titled 'Workflow: XDR - Automation Rule - Update Incident Properties' shows the configuration for this rule. The workflow is 'On' and 'XDR - Automation Rule - Update Incident Properties'. The configuration includes fields for Assignees (String) with the value 'chrivand@cisco.com', Severity (String), Short Description (String), Description (String), Status (String) with the value 'Open', and Title (String) with the value 'CLEMEA24 - [Rules.Incident.Rule.output.Incident.TitleS]'. At the bottom, another table shows the execution results. The second rule, 'CLEMEA24 - Malware Executed on MY-DEVICE-42 - Incident by Cisco ...', has a priority of 1000, is assigned to 'CM', and has a status of 'Open'. Orange arrows connect the 'Unassigned' status in the top table to the 'Assignees' field in the modal, and the 'New' status to the 'Status' field. Another arrow connects the 'Title' field in the modal to the 'Title' field in the bottom table.

Priority	Name	Source	Created	Assigned	Status
1000	Malware Executed on MY-DEVICE-42 - Incident by Cisco XDR Automati...	Cisco XDR Automat...	1 Second	Unassigned	New

Workflow: XDR - Automation Rule - Update Incident Properties

Select workflow

☒ On

XDR - Automation Rule - Update Incident Properties

Assignees (String)

Severity (String)

Short Description (String)

Description (String)

Status (String)

Title (String)

+ Add Workflow

Priority	Name	Source	Created	Assigned	Status
1000	CLEMEA24 - Malware Executed on MY-DEVICE-42 - Incident by Cisco ...	Cisco XDR Automat...	1 Minute	CM	Open



A brief history of Automation Rules

Validated Commit View Runs Run Settings

Workflow Properties

Incident Triggered Orbital Forensic Snapshot (Windows)

Automation Rules

Automation Rule Type ⓘ

Incident Rule

Full Scan with Orbital ⚡ On

Catch all rule for Testing ⚡ On

+ Add Automation Rule

Triggers (Deprecated) ⓘ

NAME

Full Scan with Orbital

Target

Target Type* ⓘ

HTTP Endpoint

No target

STATUS

Started-polling

Triggers use a reference format that has been deprecated. Your legacy workflow triggers and references to them will continue to work, but it is recommended to move to the new format. For previously referenced Automation Rules, first select the matching Rule type, and subsequently update all variable references from Triggers to Rules. For legacy event definitions, convert to Automation Rules. Learn more about Automation Rules [here](#).

Browse Variables

Search

Env	Incident rule	Output	Events Cour INTEGER
Global		Input	First Event C DATE
Rule			Incident OBJECT
Trigger (Deprecated)			Indicators OBJECT
Workflow			Last Event C DATE

MITRE Data
OBJECT

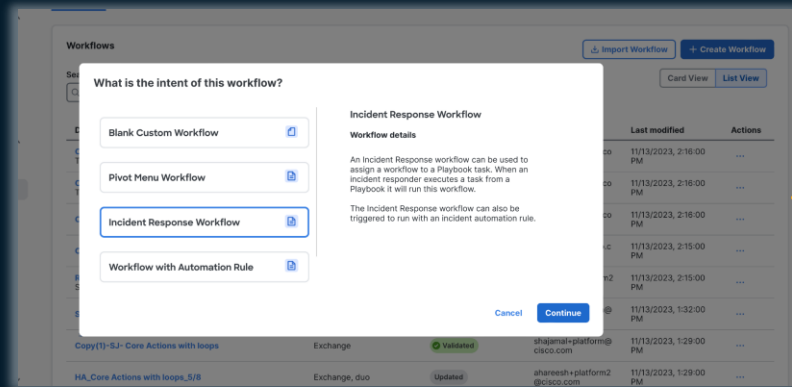
Observable
OBJECT

Cancel Save

Triggers are now implicitly managed by Automation Rules. References to them are generic, so they can be reused and shared independent of the specific Rule!

Incident Response Template

Unified Workflow Template that can be used both for Playbook Tasks and Automation Rules, making them interchangeable and reusable.



New Incident Response Workflow

Incident Response workflows can be used for Playbook Tasks and/or be used with Incident Automation Rules. By selecting this type, you will be able to select the Workflow from the Playbook Editor when editing a Task.

Workflow display name* ① 33 / 64
Notifying upon confirmed incident

Action(s)* ②
Notify X

Observable Type(s)* ③
None (general incident workflow) X

Incident Automation Rule (optional) ④
Type to search incident rule

Cancel Continue

Used for Automation Rules, as they always work on the entire Incident Object (e.g. Create ServiceNow ticket)

Apply to selected workflows

Select and configure a workflow to associate with this rule, and when the rule is created, its trigger is automatically added to the workflow

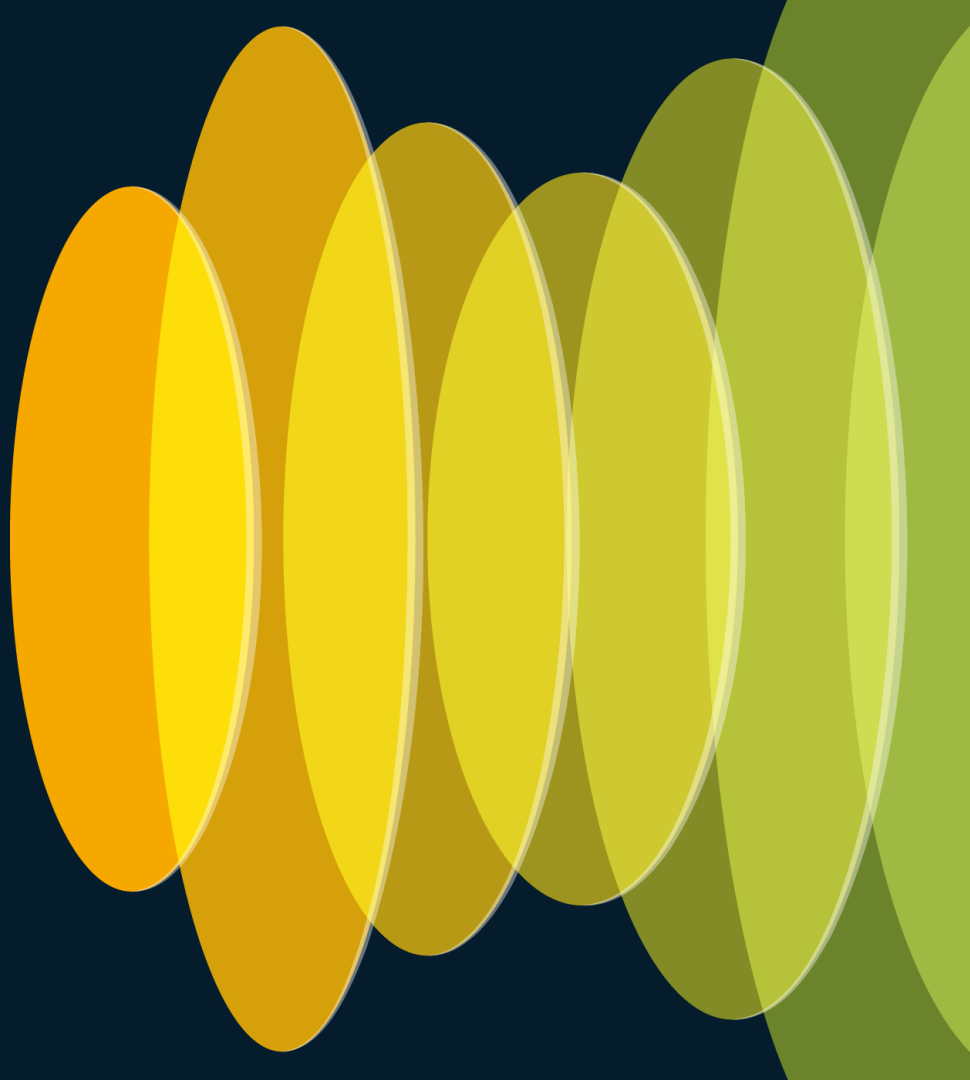
Workflow: XDR - Document and Notify

Select workflow
XDR - Document and Notify

On



Demo: Build an Incident Automation Rule Workflow



Cisco XDR - Automate

xdr.us.security.cisco.com/automate/workflows

Finish update

All Bookmarks

XDR

XDR

Christopher Van ...
explorcorp

Workflows

Workflows allow you to investigate security events, automate responses, and eliminate repetitive tasks by using activities, logic, and even other workflows to communicate with other systems and resources. From here you can access, create, and import workflows.

All Workflows 68Atomics 475RecentsFavorites 1

Workflows

Search

Status

Search

Select

Display name

XDR - Automation Rule - Update Incident Properties
This workflow allows you to update an incident's prop...

XDR - Confirm Incident
This workflow updates an incident's status to Incident

XDR - Contain Incident: URLs
This workflow consumes one or more URLs and atten

Talos - Blog Post to XDR Casebook
This workflow takes a Talos blog post, conducts an in

Talos - Get New Blog Posts
This workflow consumes the Talos Intelligence Blog P

CHRVIVAND - Cisco Live Vegas: Playbook Task Workflow wit...
Creates a Webex space and adds the user who executed the Play...

Create Incident [static json]
This is a sample workflow how to create a Incident using the...

Duplicate Incident based on Attack Chain ID
This is Demo workflow used only when needed for Creating an i...

Cohesity - Identify Restore Point for Affected Virtual...

Import Workflow

Create Workflow

Card View

List View

Last modified

Actions

24/05/2024, 13:01:53

...

24/05/2024, 06:33:15

...

24/05/2024, 06:33:15

...

23/05/2024, 23:30:12

...

23/05/2024, 23:30:00

...

23/05/2024, 19:20:34

...

23/05/2024, 18:10:20

...

23/05/2024, 18:05:20

...

23/05/2024, 14:00:00

...

What is the intent of this workflow?

Blank Custom Workflow

Incident Response Workflow

Pivot Menu Workflow

Workflow with Automation Rule

Incident Response Workflow

Workflow details

Incident Response workflows can be used for Playbook Tasks and/or be used with Incident Automation Rules. By selecting this type, you will be able to select the Workflow from the Playbook Editor when editing a Task.

Cancel

Continue

#CiscoLive

BRKSEC-2502

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

109

Cisco XDR - Automate

xdr.us.security.cisco.com/automate/workflows

Finish update

All Bookmarks

Cisco XDR

Christopher Van ...
explorcorp

Workflows

Workflows allow you to investigate security events, automate responses, and eliminate repetitive tasks by using activities, logic, and even other workflows to communicate with other systems and resources. From here you can access, create, and import workflows.

All Workflows 68 Atomics 475 Recents Favorites 1

Workflows

Search

Status

Category

Search

Select

Select

Display name

XDR - Automation Rule - Update Incident Properties
This workflow allows you to update an incident's properties...

XDR - Confirm Incident
This workflow updates an incident's status to Incident Report...

XDR - Contain Incident: URLs
This workflow consumes one or more URLs and attempts to block...

Talos - Blog Post to XDR Casebook
This workflow takes a Talos blog post, conducts an investigat...

Talos - Get New Blog Posts
This workflow consumes the Talos Intelligence Blog RSS feed a...

CHRVIVAND - Cisco Live Vegas: Playbook Task Workflow wit...
Creates a Webex space and adds the user who executed the Play...

Create Incident [static json]
This is a sample workflow how to create a Incident using the...

Duplicate Incident based on Attack Chain ID
This is Demo workflow used only when needed for Creating an i...

Cohesity - Identify Restore Point for Affected Virtual...

Workflow display name*

36 / 64

Auto-Investigate all Incident Assets

Action(s)*

Investigate

Observable Type(s)*

None (general incident workflow)

Incident Automation Rule (optional)

Type to search incident rule

CancelContinue

Import Workflow

Create Workflow

Card ViewList View

Owner	Last modified	Actions
System	24/05/2024, 13:01:53	...
System	24/05/2024, 06:33:15	...
System	24/05/2024, 06:33:15	...
mavander@cisco.com	23/05/2024, 23:30:12	...
mavander@cisco.com	23/05/2024, 23:30:00	...
chrivand@cisco.com	23/05/2024, 19:20:34	...
hanjabbo+explor@cisco.com	23/05/2024, 18:10:20	...
chrivand@cisco.com	23/05/2024, 18:05:20	...
eduardo.cordero@sales.cisco.com	23/05/2024, 14:00:05	...

#CiscoLive

BRKSEC-2502

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

110

Cisco XDR - Automate

xdr.us.security.cisco.com/automate/workflows/edit/02EKW633F604I6zD6FoCsSdjD5MxR7bJmMy

Finish update

All Bookmarks

← Back to all Workflows

CHRIVAND - Cisco Live Vegas: Auto-Investigate Incident Assets

Last Modified: 24 May 2024 at 13:52:57

Workflow is unlocked

Share

Validate

View Runs

Run

Settings

Search activities

ActivitiesLogicWorkflows

Logic

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

START

For Each

- Drag activity here

END

1 Invalid Actions

Warning 1

Properties: For Each

For Each

General

- Display Name8 / 64For Each
- Description0 / 1024
- Source Array*

(x)
- ☐ Continue Workflow Execution On Failure
- ☐ Skip activity execution

Cisco XDR - Automate

xdr.us.security.cisco.com/automate/workflows/edit/02EKW633F604I6zD6FoCsSdjD5MxR7bJmMy

Finish update

All Bookmarks

← Back to all Workflows

CHRVIVAND - Cisco Live Vegas: Auto-Investigate Incident Assets

Last Modified: 24 May 2024 at 13:52:57

Workflow is unlocked

Share

Validate

View Runs

Run

Settings

Search activities

ActivitiesLogicWorkflows

Logic

Break

Completed

Condition Block

Continue

For Each

Group

Parallel Block

Start Point

While Loop

Warning 1

Properties: For Each

For Each

General

Display Name8 / 64

For Each

Description0 / 1024

Source Array*

Continue Workflow Execution On Failure

Skip activity execution

Browse Variables

Search

Incident Summary

Run Context

Incident

Indicators

Last Event Date

Observables

Severity

Source

Targets

Targets Data

Total Count

Cancel

Save

Cisco XDR - Automate

xdr.us.security.cisco.com/automate/workflows/edit/02EKW633F604I6zD6FoCsDjD5MxR7bJmMy

Workflow is unlockedShareValidateView RunsRunSettings

Back to all Workflows

CHRIVAND - Cisco Live Vegas: Auto-Investigate Incident Assets

Last Modified: 28 May 2024 at 09:56:42

Search activities

ActivitiesLogicWorkflows

Core>

Ansible Tower>

AWS Service>

Check Point Quantum Smart-1>

Cisco API Console>

Cisco Defense Orchestrator>

Cisco Duo: Admin API>

Cisco Duo: Auth API>

Cisco ISE>

Cisco Meraki>

Cisco Orbital>

Cisco PSIRT openVuln>

Cisco Secure Cloud Analytics>

Browse Variables

Search

Elapsed time (seconds)
DECIMAL

End time
DATE

Start time
DATE

Succeeded
BOOLEAN

Error
OBJECT

Source Array
ARRAY

Columns

Items

First

Last

Asset ID
STRING

Count
INTEGER

Observable Type
STRING

Type
STRING

Value
STRING

CancelSave

Properties: Orbital - Query - Run Query

Orbital - Query - Run Query

Query Expiration Time (Minutes)* ⓘ
2

Access Token ⓘ

Catalog Query ID ⓘ
logged_in_users

Wait For Query Completion* ⓘ
true

Hostname ⓘ
[Sactivity.For Each.Input.Source Array[@].Value\$]

Secure Endpoint GUID ⓘ

IP Address ⓘ

SQL Query ⓘ

#CiscoLive

BRKSEC-2502

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

113

Cisco XDR - Automate

xdr.us.security.cisco.com/automate/workflows/edit/02EKW633F604I6zD6FoCsSdjD5MxR7bJmMy

All Bookmarks

← Back to all Workflows

CHRIVAND - Cisco Live Vegas: Auto-Investigate Incident Assets

Last Modified: 28 May 2024 at 09:56:17

Workflow is unlocked

Share

Validate

View Runs

Run

Settings

Search activities

ActivitiesLogicWorkflows

Core

Ansible Tower

AWS Service

Check Point Quantum Smart-1

Cisco API Console

Cisco Defense Orchestrator

Cisco Duo: Admin API

Cisco Duo: Auth API

Cisco ISE

Cisco Meraki

Cisco Orbital

Cisco PSIRT openVuln

Cisco Secure Cloud Analytics

START

For Each

Atomic

Orbital - Query - Run Query

END

Warning 1

Workflow Properties

CHRIVAND - Cisco Live Vegas: Auto-Investigate Incident Assets

General

Variables

Response Options

Automation Rules

Ver

Exc

Tar

Orbital - ExplorCorp - v0

Palo Alto Networks Cortex XDR - v1

Platform APIs

Private Intelligence API

Public Intelligence API

+ Add New

Select

Specify target on workflow start

Execute on this target group

Cisco XDR - Automate

xdr.us.security.cisco.com/automate/workflows/edit/02EKW633F604I6zD6FoCsSdjD5MxR7bJmMy

🔍 ☆ ⓘ ⌵ ⚙️ 🔴

All Bookmarks

← Back to all Workflows

CHRVIVAND - Cisco Live Vegas: Auto-Investigate Incident Assets

Last Modified: 28 May 2024 at 09:56:42

Workflow is unlocked

Share

Validate

View Runs

Run

Settings

Search activities

Activities

Logic

Workflows

Core

Ansible Tower

AWS Service

Check Point Quantum Smart-1

Cisco API Console

Cisco Defense Orchestrator

Cisco Duo: Admin API

Cisco Duo: Auth API

Cisco ISE

Cisco Meraki

Cisco Orbital

Cisco PSIRT openVuln

Cisco Secure Cloud Analytics

START

For Each

Atomic

Orbital - Query - Run Query

END

🔍

+

−

Properties: Orbital - Query - Run Query

Orbital - Query - Run Query

Query Expiration Time (Minutes)* ⓘ

2

Access Token ⓘ

Catalog Query ID ⓘ

logged_in_users

Wait For Query Completion* ⓘ

true

Hostname ⓘ

[\$activity.For Each.input.Source Array[@].Value\$]

Secure Endpoint GUID ⓘ

IP Address ⓘ

SQL Query ⓘ

Cisco XDR - Automate

xdr.us.security.cisco.com/automate/workflows/edit/02EKW633F604I6zD6FoCsSdjD5MxR7bJmMy

All Bookmarks

← Back to all Workflows

CHRIVAND - Cisco Live Vegas: Auto-Investigate Incident Assets

Last Modified: 28 May 2024 at 09:56:42

Workflow is unlockedShareValidateView RunsRunSettings

set v

ActivitiesLogicWorkflows

Core

Set Variables

Browse Variables

Search

EnvGlobalWorkflow

Output

Instance Id
STRING

Start time
DATE

Started By (ID)
STRING

Started By (Type)
STRING

Workflow Result
STRING

Workflow Result Code
STRING

A free text property which can be used to communicate the results of the workflow run. For Incident Response Intent workflows, this property is automatically entered in the Worklog after the run completes (markdown supported).

CancelSave

Warning

Properties: Set Variables

Set Variables

13 / 64

0 / 1024

Continue Workflow Execution On Failure

Skip activity execution

Variables

Variables to update*

Variable to update*

New value

+ ADD

Cisco XDR - Automate

xdr.us.security.cisco.com/automate/workflows/edit/02EKW633F604I6zD6FoCsDjD5MxR7bJmMy

All Bookmarks

← Back to all Workflows

CHRIVAND - Cisco Live Vegas: Auto-Investigate Incident Assets

Last Modified: 28 May 2024 at 09:56:42

Workflow is unlocked

Share

Validate

View Runs

Run

Settings

set v

Activities

Logic

Workflows

Core

Set Variables

START

For Each

Atomic

Orbital - Query - Run Query

Core

Set Workflow Output Result

END

Properties: Set Variables

Set Workflow Output Result

General

Display Name26 / 64

Set Workflow Output Result

Description0 / 1024

Continue Workflow Execution On Failure

Skip activity execution

Variables

Variables to update*

Variable to update*

[\$workflow.CHRIVAND - Cisco Live Vegas: Auto-Investigate Incident Assets.output.Workflow Result\$]

New value

[\$workflow.CHRIVAND - Cisco Live Vegas: Auto-Investigate Incident Assets.output.Workflow Result\$]
- Results of 'logged_in_users' Orbital query for [\$activity.For Each.input.Source Array[@.Value\$]: [\$activity.Orbital - Query - Run Query.output.Result\$]]

+ ADD

Cisco XDR - Automate

xdr.us.security.cisco.com/automate/workflows/edit/02EKW633F604I6zD6FoCsSdjD5MxR7bJmMy

🔍 ☆ ⓘ ⌕ ⚙️ ⚠️ ⋮

📁 All Bookmarks

← Back to all Workflows

CHRIVAND - Cisco Live Vegas: Auto-Investigate Incident Assets

Last Modified: 28 May 2024 at 09:56:42

Workflow is unlocked

Share

Validated

View Runs

Run

Settings

set v

ActivitiesLogicWorkflows

Core

Set Variables

START

For Each

Atomic

Orbital - Query - Run Query

Core

Set Workflow Output Result

END

🔍

+

—

Workflow Properties

CHRIVAND - Cisco Live Vegas: Auto-Investigate Incident Assets

General

Variables

Response Options

Automation Rules

Version

Exchange

Target

Credentials

Automation Rule Type ⓘ

Incident Rule

A type is selected but this workflow has no Automation Rule associated

+ Add Automation Rule

Cisco XDR - Automate

xdr.us.security.cisco.com/automate/workflows/edit/02EKW633F604I6zD6FoCsSdjD5MxR7bJmMy

All Bookmarks

Back to all Workflows

CHRIVAND - Cisco Live Vegas: Auto-Investigate Incident Assets

Last Modified: 28 May 2024 at 09:56:42

Workflow is unlocked

Share

Validated

View Runs

Run

Settings

set v

ActivitiesLogicWorkflows

Core

Set Variables

START

END

Workflow Properties

CHRIVAND - Cisco Live Vegas: Auto-Investigate Incident Assets

General

Options

Rules

Rule Type

is selected but this workflow has no Automation Rule associated

Automation Rule

Version

Exchange

Target

Credentials

Select Automation Rule

You can automate this workflow so that it runs on a schedule or whenever an event that you select occurs.

Selected Automation Rule Types

Incident Rule

Automation Rule Name*

Select

Ransomware and Encryption Rule - CHRIVAND

Score greater than 800

Incident notifications to Webex

+ Add New

Cancel

Select

Cisco XDR - Automate

xdr.us.security.cisco.com/automate/workflows/edit/02EKW633F604I6zD6FoCsSdjD5MxR7bJmMy

All Bookmarks

← Back to all Workflows

CHRIVAND - Cisco Live Vegas

Last Modified: 28 May 2024 at 09:59:59

Search activities

ActivitiesLogicWorkflows

Core

Ansible Tower

AWS Service

Check Point Quantum Smart-1

Cisco API Console

Cisco Defense Orchestrator

Cisco Duo: Admin API

Cisco Duo: Auth API

Cisco ISE

Cisco Meraki

Cisco Orbital

Cisco PSIRT openVuln

Cisco Secure Cloud Analytics

View RunsRunSettings

gas: Auto-Investigate

no Automation Rule associated

Edit Ransomware and Encryption Rule - CHRIVAND

chrivand@cisco.com

Short Description (String)

Title (String)

VEGAS - [{Rules.Incident Rule.output.Incident.Title\$}]

Severity (String)

Workflow: CHRIVAND - Cisco Live Vegas: Auto-Investigate Incident Assets

On

Select workflow

CHRIVAND - Cisco Live Vegas: Auto-Investigate Incident...

Turn on this automation rule

Switch between enabling (on) or disabling (off) this rule. This is useful for testing and debugging.

Automation rule is on

Cancel

Submit

#CiscoLive

BRKSEC-2502

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

120

Cisco XDR - Automate

xdr.us.security.cisco.com/automate/workflows/edit/02EKW633F604I6zD6FoCsSdjD5MxR7bJmMy

🏠 ☆ ⓘ ⌕ ⚙️ 🔴 ⋮

All Bookmarks

← Back to all Workflows

CHRIVAND - Cisco Live Vegas: Auto-Investigate Incident Assets

Last Modified: 28 May 2024 at 10:04:10

Workflow is locked

Share

Validated

View Runs

Run

Settings

✓ Incident rule: ransomware and encryption rule - chrivand created successfully

The automation rule you created will start this workflow when the conditions you configured are met. To manage rules for all workflows go to the [Automation Rules page](#).

✕

START

For Each

Atomic

Orbital - Query - Run Query

Core

Set Workflow Output Result

END

🔍

+

-

CHRIVAND - Cisco Live Vegas: Auto-Investigate Incident Assets

General

Variables

Response Options

Automation Rules

Automation Rule Type ⓘ

Incident Rule

Ransomware and Encryption Rule - CHRIVAND

Version

Exchange

Target

Credentials

⚡

On

#CiscoLive

BRKSEC-2502

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

121



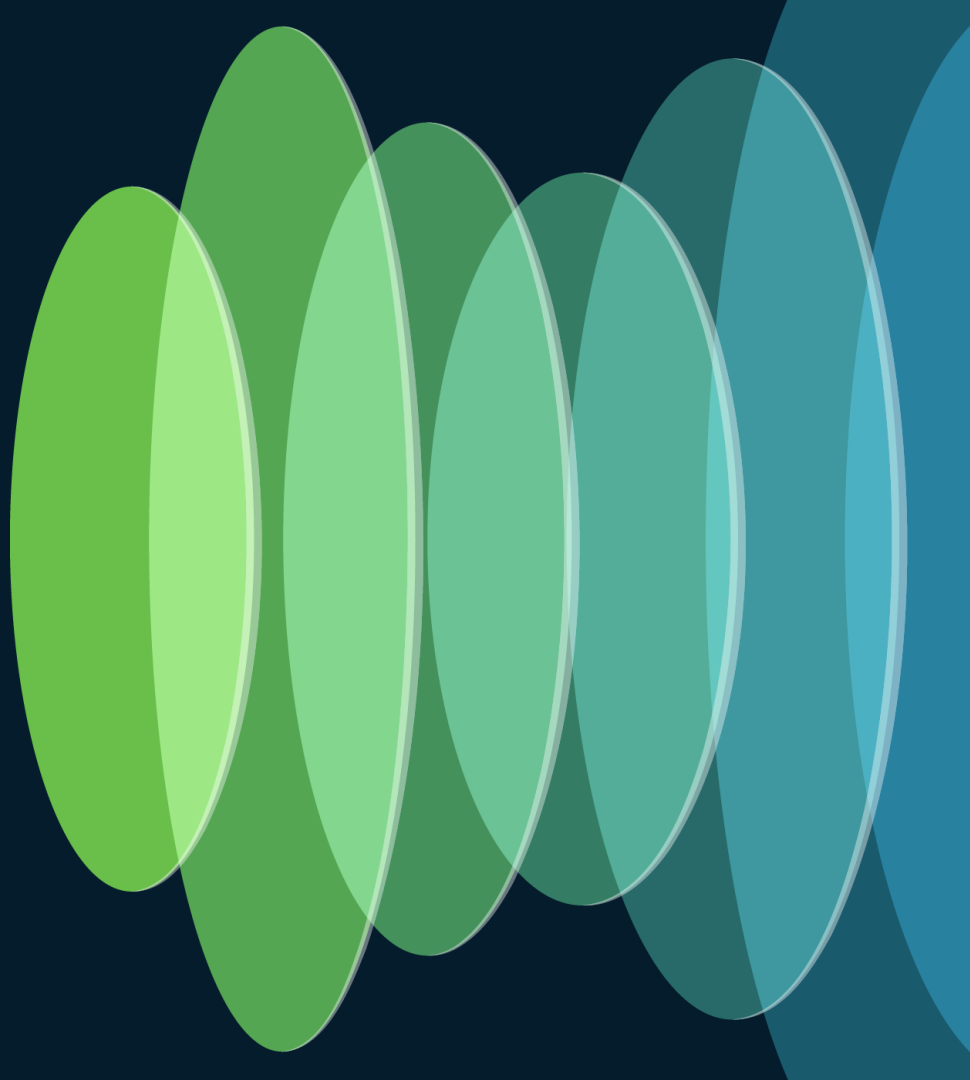
When to use this Incident Response type?

- Ideal for certain actions that need to be taken for all Incidents, or specific types of Incidents, without needing further human involvement.
- Reduces the chance of missing an Incident, as flow is fully automated.
- Every automated action is automatically entered into the Incident Worklog.
- Not recommended for invasive actions like Containment and Eradication, but possible in some cases (use strict Rule Conditions!).

Agenda

- ~~What is Incident Response?~~
- ~~How to perform Incident Response with Cisco XDR?~~
 - ~~Introduction to Cisco XDR (Automation)~~
 - ~~Pivot Menu~~
 - ~~Playbook Tasks~~
 - ~~Automation Rules~~
- Let's put it to practice!
- Future?

Let's put it to
practice!

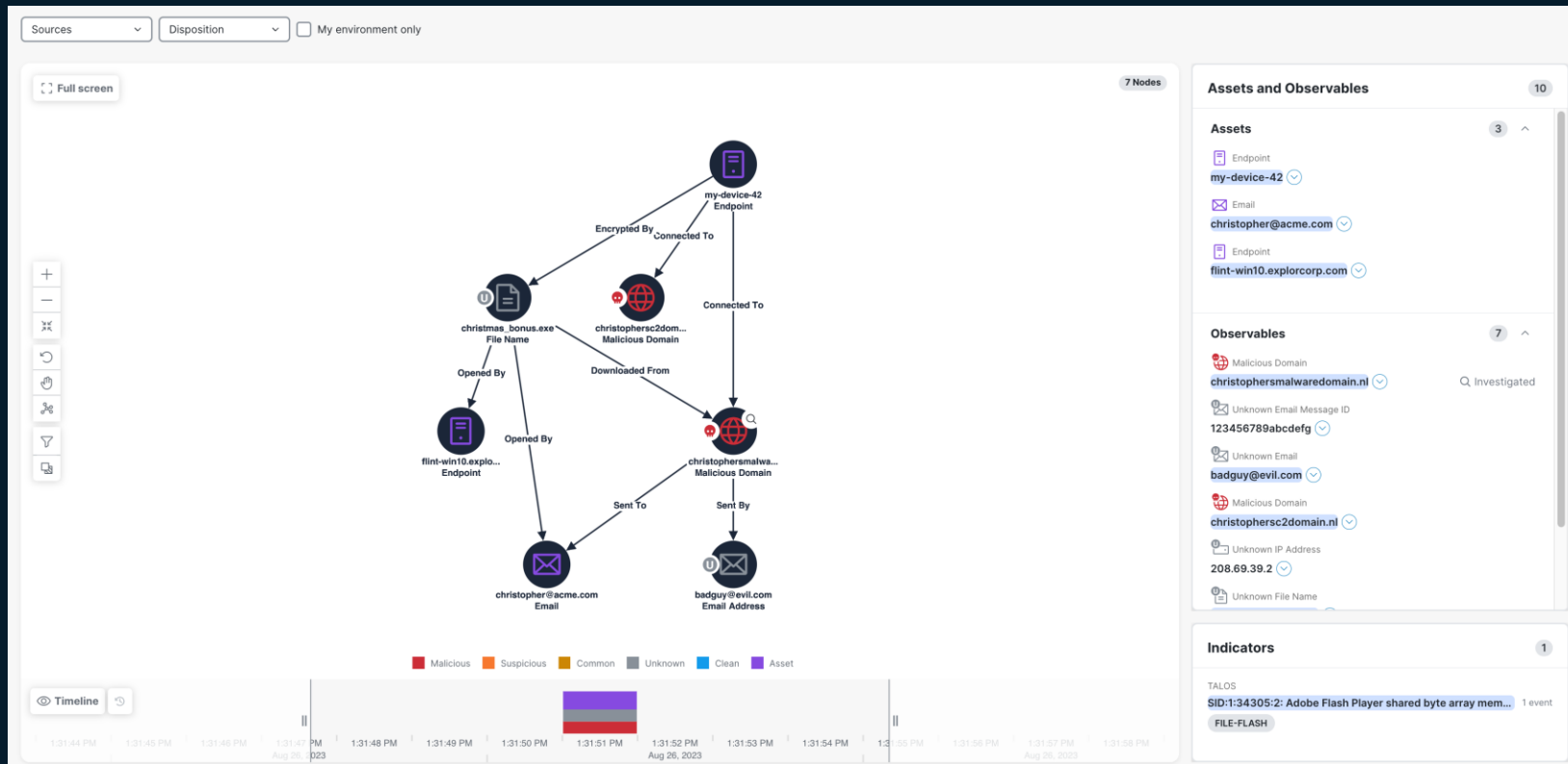


CISCO *Live!*

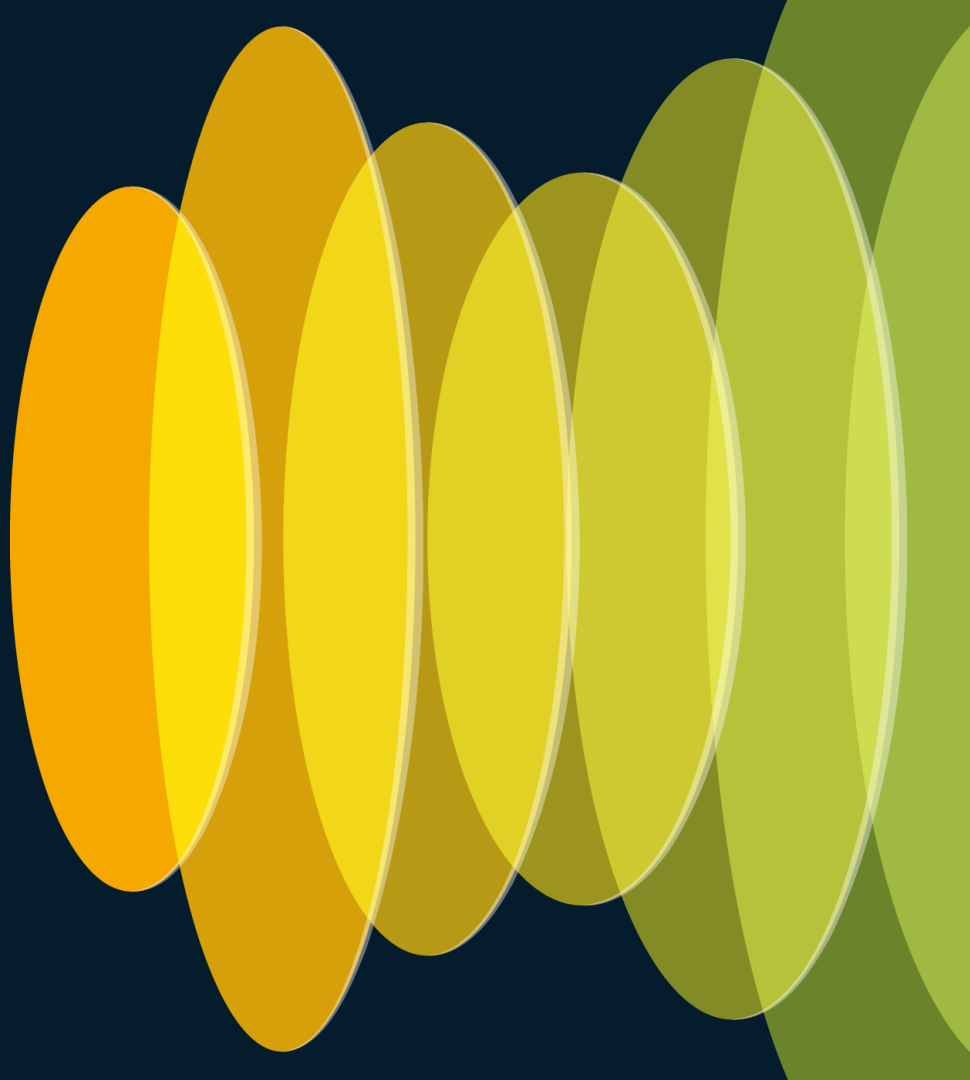
126

**Learn how to create Incidents!*

Investigating the details...



Live Demo: Incident Response for a Ransomware attack



The Incident Response game plan:

Identify



Review the incident, confirm the findings and declare incident in case of a breach.

Contain



Stop the breach from spreading: quarantine impacted hosts, block domains, files, etc.

Eradicate



Mitigate and/or remediate vulnerabilities and remove malicious content from hosts.

Recover

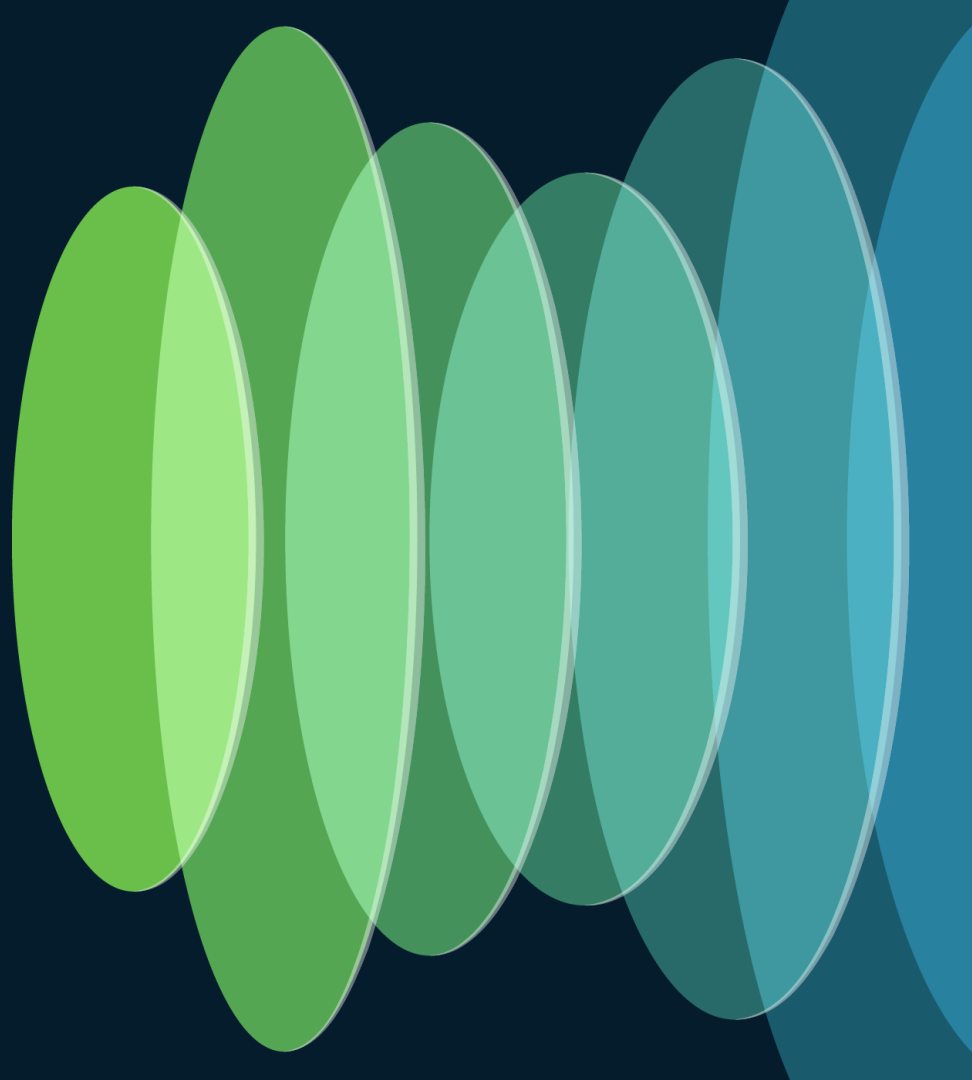


Validate eradication steps and restore impacted services and contained hosts.

Agenda

- ~~What is Incident Response?~~
- ~~How to perform Incident Response with Cisco XDR?~~
 - ~~Introduction to Cisco XDR (Automation)~~
 - ~~Pivot Menu~~
 - ~~Playbook Tasks~~
 - ~~Automation Rules~~
- ~~Let's put it to practice!~~
- Future?

Future?



Playbook Task Status

The screenshot shows the 'Cisco XDR Playbook' interface with tabs for Overview, Detection, Response, and Worklog. The 'Response' tab is active. A sidebar on the left lists sections: Identification, Containment, Eradication, and Recovery. The main content area shows a list of tasks under the 'Containment' section. Each task has a status indicator (Complete, Review required, Running, Errored, Failed, Action required) and an 'Execute' button. A tooltip 'Add note' is visible over the 'Execute' button of the 'Identify Affected Hosts' task. At the bottom, there are 'Back' and 'Go to Eradication' buttons.

Overview Detection **Response** Worklog

Cisco XDR Playbook ⓘ
Published: August 6, 2023 at 10:09:00 PM

Hide not applicable tasks

Identification

Containment

Identify Affected Hosts
Add note with summary of findings on the investigations of hosts found with malicious indicators. [view more](#)

Contain Incident: Overview
Overview of how to contain Indicators of Compromise to stop the spread of malicious activity. [view more](#)

Contain Incident: Assets Complete Execute ⓘ

Use asset-based containment to stop the spread of malicious activity. [view more](#)

Contain Incident: IPs Review required Execute ⓘ

Contain IP indicators of compromise to stop the spread of malicious activity. [view more](#)

Contain Incident: Domains Running Execute ⓘ

Contain domain indicators of compromise to stop the spread of malicious activity. [view more](#)

Contain Incident: URLs Errored Execute ⓘ

Contain URL indicators of compromise to stop the spread of malicious activity. [view more](#)

Contain Incident: File Hashes Failed Execute ⓘ

Contain file hash indicators of compromise to stop the spread of malicious activity. [view more](#)

Contain Incident: Users Action required Execute ⓘ

Contain users by logging out user and email observable types to stop the spread of malicious activity. [view more](#)

Back Go to Eradication →

The screenshot shows a modal dialog titled 'Add Note for Identify Affected Hosts'. It has 'Write' and 'Preview' tabs. Below the tabs is a rich text editor with formatting options (H, B, I, G, link, unlink, code) and a text area. At the bottom right, there is a 'Cancel' button and an 'Add note' button with a dropdown arrow. A tooltip is visible over the 'Add note' button, showing three options: 'Add note', 'Add note and mark as complete', and 'Add note and mark as not applicable'.

Add Note for Identify Affected Hosts

Write Preview

H B I G link unlink code

Add a note...

0 / 2000

Cancel Add note ▼

Add note

Add note and mark as complete

Add note and mark as not applicable

Automation Prompts

The screenshot shows the Cisco XDR Control Center interface. A playbook titled "Blocked Command and Control DNS Activities" is open, showing a list of actions under the "Response" tab. The actions include "Identify Affected Hosts", "Contain Incident: Overview", "Contain Incident: Assets", "Contain Incident: IPs", "Contain Incident: Domains", "Contain Incident: URLs", "Contain Incident: File Hashes", and "Contain Incident: Users". The "Contain Incident: Users" action is highlighted with an orange box, and a red "Action required" prompt is visible next to it. A "View prompt" link is also present. A sidebar on the left shows the navigation menu, and a top bar displays the user's name "Alexander Business Corp.".

This modal window, titled "Contain Incident: Users", displays a list of executed workflows. The first entry is "Executed workflow for Contain Incident: Users requires additional action" with a timestamp of "2022-02-12 21:11:10 UTC" and a "View prompt" link. The second entry is "Alexander Ma executed workflow for Contain Incident: Domains" with a timestamp of "2022-02-12 21:11:10 UTC".

The "Prompt Task" dialog box shows a task type of "Prompt". The due date is "01/31/24" and the expiration date is "01/31/24". The task content is: "We have identified multiple blocklist possibilities. To which would you like to add domain: internetbadguys.com". Below this is a "Select blocklist" dropdown menu. At the bottom right, there are "Cancel" and "Save" buttons.

Automation Rule Enhancements

New Automation Rule

General

Automation rule on ☒

Type

Rule Name

Description

Create as priority or standalone rule ☒ Priority Rule ☐ Standalone Rule

Conditions

☒ ALL of these conditions must be met ☐ ANY of these conditions can be met ☐ Advanced

[+ Add Condition](#)

Apply to selected workflows

☒ ☐ OR

☒ ☐ OR

[+ Add another workflow](#)

Compact and simplified design,
progressive disclosure*

Automation Rules

Automation Rules [Rule History](#) [Webhooks](#) [Schedules](#)

Search Filter 1 Filter 2 Filters 123 results

Event name	Rule name	Type	Matched	Tie
Unusual Endpoint Activity Detected	NK_IncidentRule_PGR_12_Jan	Incident	Yes	3/2
Unusual Endpoint Activity Detected	PT_Incident automation rule 013_1	Webhook	Yes	3/2
Unusual Endpoint Activity Detected	901-WeConditionSchedule	Schedule	Yes	3/2
Unusual Endpoint Activity Detected	CA Rule 2 7/13 Sched	Schedule	No	3/2
Unusual Endpoint Activity Detected	Like Approval Rule 1	Approval task	Yes	3/2
Unusual Endpoint Activity Detected	Rule 17/13	Incident	Yes	3/2
Unusual Endpoint Activity Detected	80 PR2	Incident	No	3/2
Unusual Endpoint Activity Detected	Release charts Incident trigger1	Email	No	3/2
Unusual Endpoint Activity Detected	1395-JF Test	Incident	No	3/2
Unusual Endpoint Activity Detected	Su_Test_Incident	Incident	Yes	3/2

NK_IncidentRule_PGR_12 Jan

Automation Rule Information

Optional description goes here.

Automation Rule Information

Optional description goes here.

Close

History tab for troubleshooting
and audit logging*

Workflow: None Selected

☒ On ☐ Off

[+ Add Workflow](#)

Select workflow

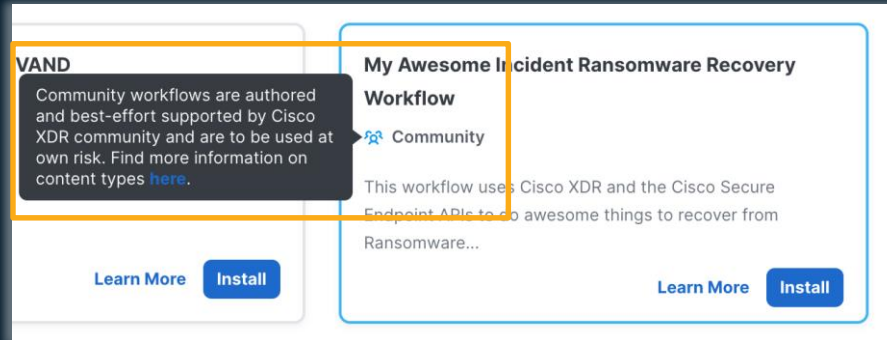
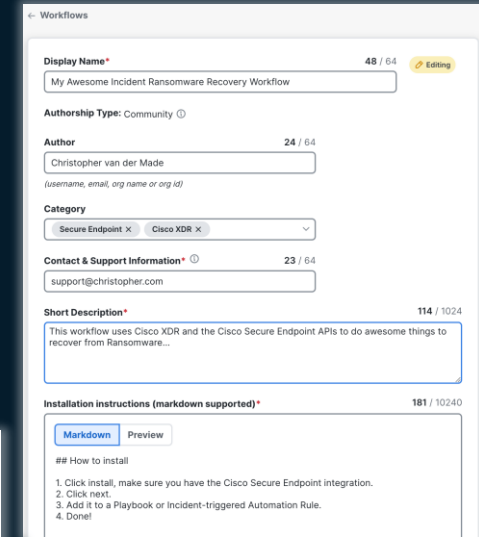
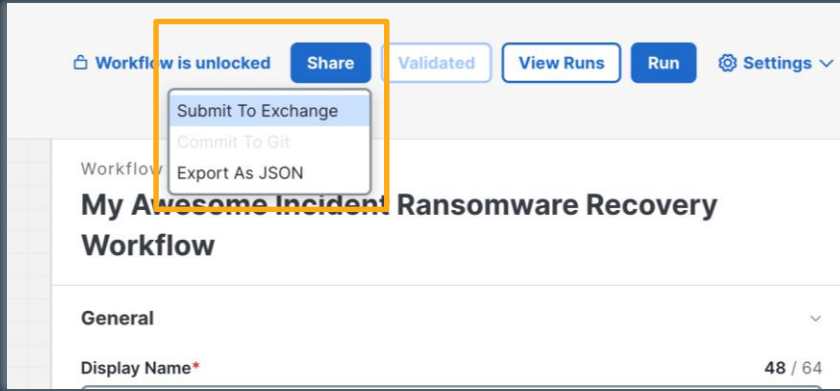
Type to search workflows

- Incident Rule Workflows
- DM Test 2
- DM Test
- XDR - Identify Vulnerabilities (invalid)
- XDR - Restore Systems**
- XDR - Contain Incident: Assets
- XDR - Confirm Incident
- XDR - Contain Incident: URLs
- XDR - Contain Incident: Domains
- XDR - Contain Incident: File Hashes

☒ Automation

Only show relevant Workflows,
Cisco Managed are marked

Automation Exchange for Community



Automation Exchange Ratings

The screenshot displays the Cisco XDR Automation Exchange interface. On the left is a navigation sidebar with options: Control Center, Incidents, Investigate, Intelligence, Automate, Exchange (highlighted), Workflows, Runs, Account Keys, Targets, Variables, Triggers, Tasks, Advanced, Devices, and Administration. The main content area is titled 'Exchange' and includes a description: 'Exchange allows you to find and install workflows that have been approved by Cisco Engineers and content providers.' Below this are tabs for 'Explore', 'Installed' (with a count of 4), '2 Updates available', and 'Submissions'. A search bar and filters for 'Category' (set to 'All') and 'Sort' (set to 'Rating: high to low') are present. The 'Popular' section shows two workflow cards. The first card, 'Fixes to ServiceNow Incidents lorem ipsum dolor sit amet', is by 'Cisco Managed' and has '1921 Installs' and a '4.8 Rating'. A tooltip for this rating shows 'Average Rating: 4.8 out of 5 (2 ratings)' and 'Your Rating: 5.0'. The second card is identical but partially obscured. Buttons for 'Learn More' and 'Uninstall' are visible on the first card.

Exchange

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

[Explore](#) **Installed** 4 2 Updates available [Submissions](#)

Search Category Sort

Popular

Fixes to ServiceNow Incidents lorem ipsum dolor sit amet

Cisco Managed

Searches Secure Malware Analytics for IOCs. Nulla vitae elit libero, a pharetra augue. Maecenas faucibus mollis interdum. Donec id elit non.

1921 Installs

4.8 Rating

Average Rating: 4.8 out of 5 (2 ratings)
Your Rating: 5.0

[Learn More](#) [Uninstall](#)

Featured



Pivot Menu
Actions



Response
Playbooks

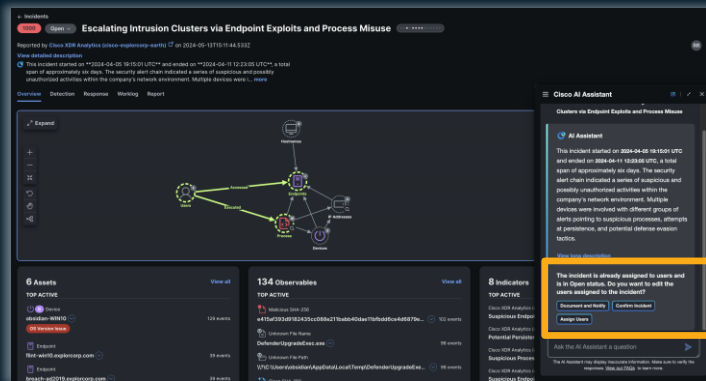
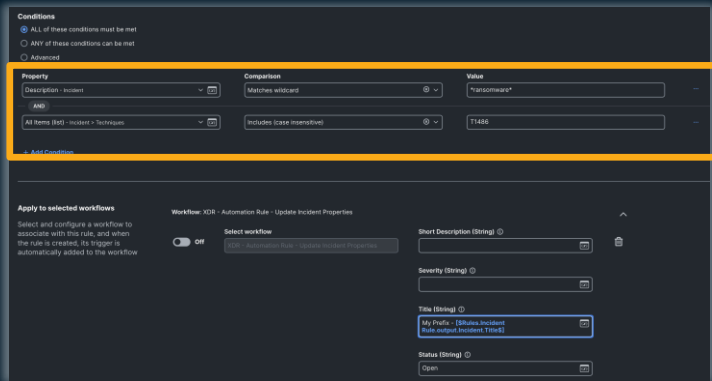
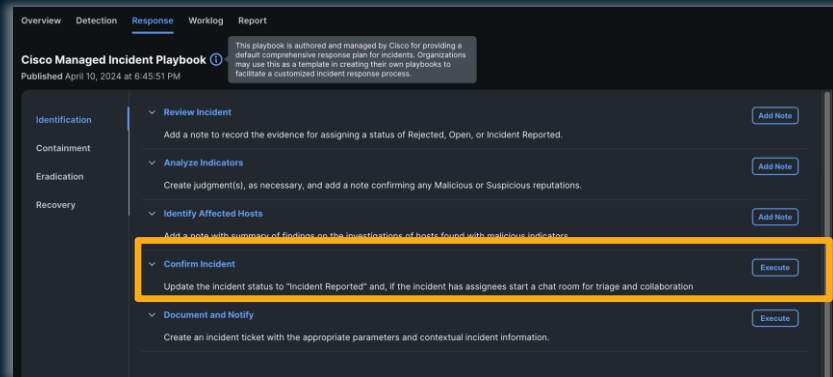
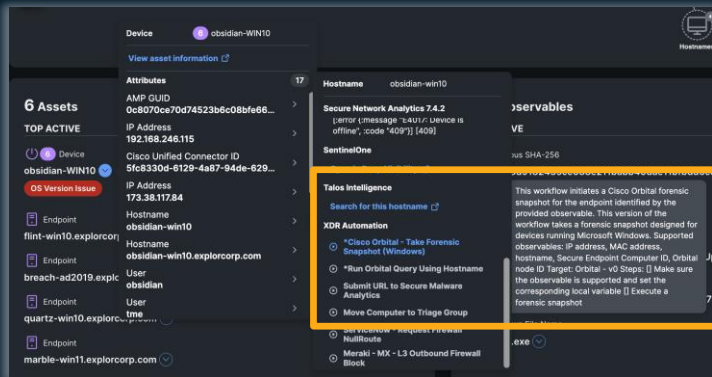


Automation
Rules



AI SOC
Assistant

Executing your Incident Response Workflows



AI Assistant for Security: Interpreting an Incident

Incidents

1000 Incident Reported **Escalating Intrusion Clusters via Endpoint Exploits and Process Misuse**

Reported by Cisco XDR Analytics (cisco-explorcorp-earth) on May 14, 2024 @ 7:35 PM CEST

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 involved... [more](#)

Overview Detection Response Worklog Report

Expand

Assets [View all](#)

TOP ACTIVE

- Device: obsidian-WIN10 129 events
- OS Version Issue
- Endpoint: flint-win10.explorcorp.com 39 events

134 Observables [View all](#)

TOP ACTIVE

- Malicious SHA-256: e415af393d9182435cc088e211babb40dae11bfbd6ce4d687...
- Unknown File Name: DefenderUpgradeExec.exe
- Unknown File Path

Cisco AI Assistant

You

View incident detail for Escalating Intrusion Clusters via Endpoint Exploits and Process Misuse

AI Assistant

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 involved with different groups of alerts pointing to suspicious processes, attempts at persistence, and potential defense evasion tactics.

[View long description](#)

The incident is already assigned to users and is in Incident Reported status. Do you want to edit the users assigned to the incident?

[Contain Incident: URLs](#)

[Validate Eradicated Hosts and Unquarantine Assets](#)

[Contain Incident: File Hashes](#)

Ask the AI Assistant a question

The AI Assistant may display inaccurate information. Make sure to verify the responses. [View our FAQs](#) to learn more.

AI Assistant for Security: Taking the Next Step

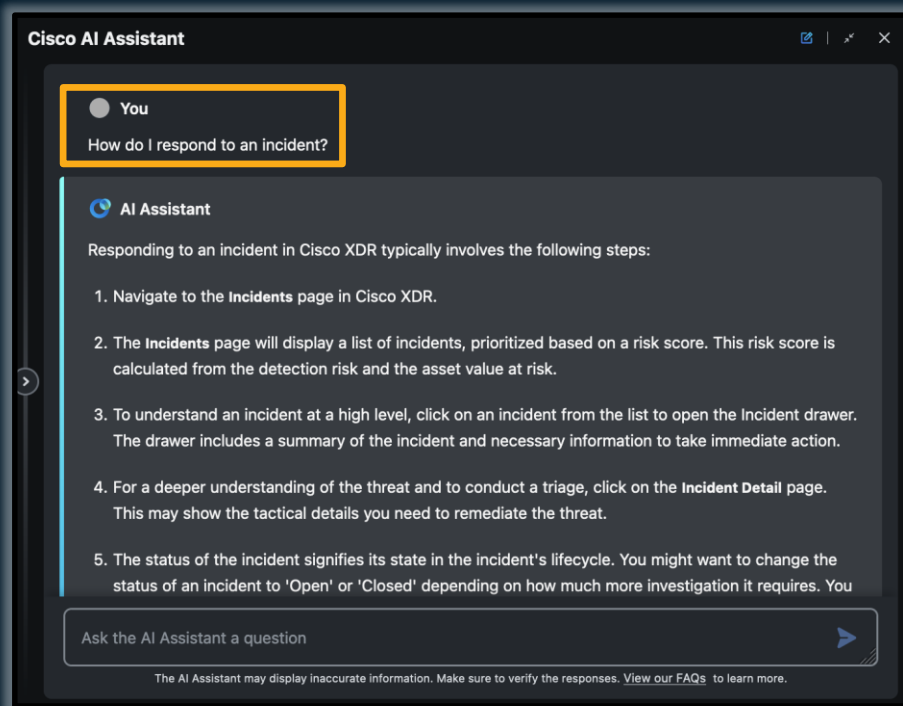
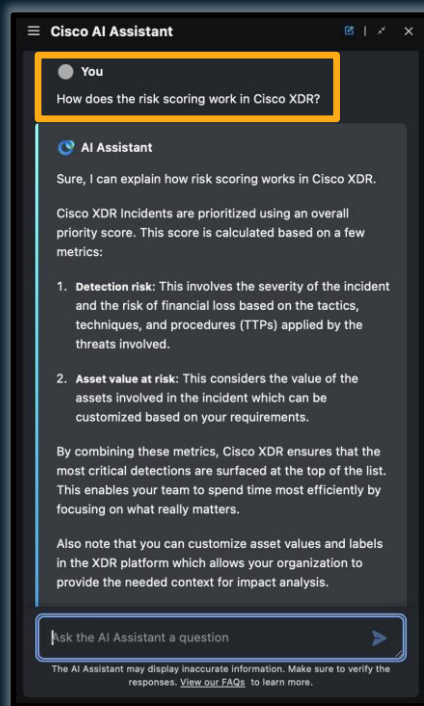
The screenshot displays the Cisco Security Center interface, specifically the 'Incidents' section. The main incident is titled 'Escalating Intrusion Clusters via Endpoint Exploits' and is reported by Cisco XDR Analytics. The incident is currently in the 'Incident Reported' status.

The interface is divided into several panels:

- Incident Details:** Shows the incident title, status, and a detailed description of the intrusion clusters.
- Incident Response Playbook:** A list of steps for handling the incident, including 'Contain Incident: Overview', 'Contain Incident: Assets', 'Contain Incident: IPs', 'Contain Incident: Domains', 'Contain Incident: URLs', 'Contain Incident: File Hashes', and 'Implement Additional Monitoring'.
- Cisco AI Assistant:** A panel that provides guidance and actions for the incident response. It includes a 'View long description' link and a confirmation message: 'The incident is already assigned to users and is in Incident Reported status. Do you want to edit the users assigned to the incident?'. Below this, there are buttons for 'Contain Incident: URLs', 'Contain Incident: File Hashes', and 'Validate Eradicated Hosts and Unquarantine Assets'.
- 2 Items:** A list of items related to the incident, including 'Unknown URL' and 'Unknown URL' with associated event counts.

The 'Contain Incident: URLs' step is highlighted with a yellow box, indicating it is the current focus of the AI Assistant's guidance. The AI Assistant panel also shows a progress bar for the 'Contain Incident: URLs' action, which is currently in progress.

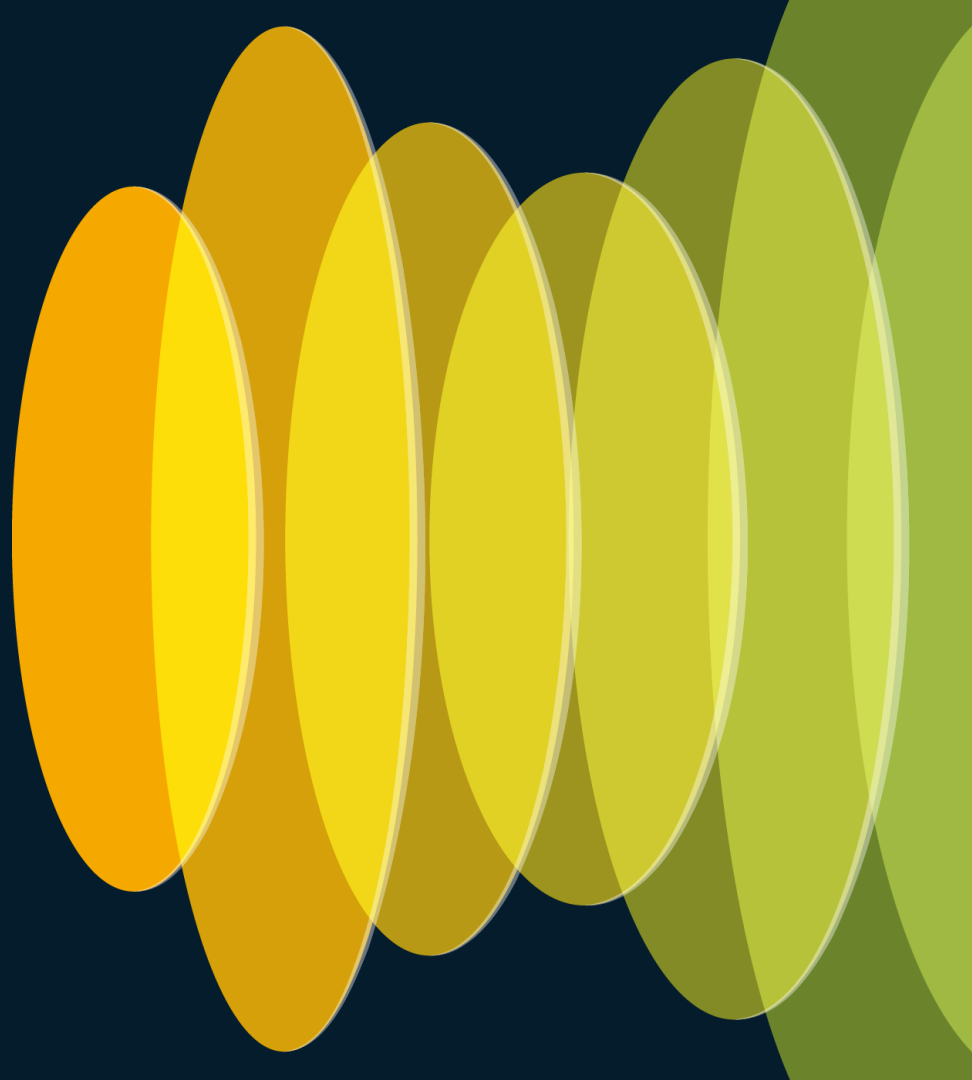
AI Assistant for Security: Asking for Help



Incident Response with the AI Assistant

- The AI Assistant is another medium (on top of the Response UI and Automation Rules) to run through the Playbook.
- The AI Assistant will “recommend” Playbook Tasks that are “relevant” for the specific incident at that point in the Incident Response process:
 - Is the Task valid?
 - Is the Task in a non-final state (i.e. not marked as “Complete” or “Not applicable”)?
 - Does the Incident contain the Observable Type or Asset that the Task Workflow is built for?
- All matching Tasks will be recommended in sequential order of the Playbook.
- In the future more granular Incident Status and Entity State Tracking will be released and used by the AI Assistant to make recommendations.

Closing thoughts...



What have we talked about today?

- Cisco XDR's most common Incident Responses methods:
 - Pivot Menu
 - Playbook Tasks
 - (Incident) Automation Rules
 - AI Assistant (Beta)
- Incident Response is a sequential process
- Some Tasks can be fully automated
- Some Tasks require teamwork between humans and automation
- Cisco XDR can help at any stage!

Cisco Developer Documentation Learn Technologies Community Events

Security > Cisco XDR

Cisco XDR

Cisco Developer Learning Labs Center

Cisco XDR Advanced Labs

- Module Overview
- Create Incident with workflow
- Automation Rules
- Threat Hunting
- Private Threat Intelligence Feeds
- XDR Integration Module with Python

BLOG

Security automation

Investigation response products

Cisco DevNet Documentation Learn Technologies Community Events

Documentation > All > Cisco XDR > Cisco XDR APIs

Cisco XDR APIs

Introduction

- Overview of Cisco XDR APIs
- About the Cisco XDR APIs
- Use Cases

Authentication

Getting Started

API Changelog

Introduction

Cisco XDR collects and correlates data across email, endpoints, servers, cloud workloads, and networks, enabling the detection and response to advanced threats. Threats can then be analyzed, prioritized, hunted, and remediated to prevent data loss and other business impacts. This page contains everything you need to get started with custom integrations and automation with the Cisco XDR platform.

Overview of Cisco XDR APIs

There are many available REST APIs that can be used for integrations. These include the following:

	Description
Automation	Managing Automation objects and running Automation workflows.
Platforms APIs (IROH)	XDR Platform features (see table below).
Incidents and Investigations	Search Incidents and manage Investigations.
Global Intelligence	[Read-Only] Cisco Managed instance of Cisco Threat Intelligence API (CTIA).
Private Intelligence	Private instance of CTIA to manage judgements, indicators and more.
Playbook	Create and manage Incident Response Playbooks.

The Cisco XDR Platform APIs (IROH) are broken down into multiple lower-level API endpoints:

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

Modeling Threat Intelligence in CTIM

- Rate Limits

API Reference

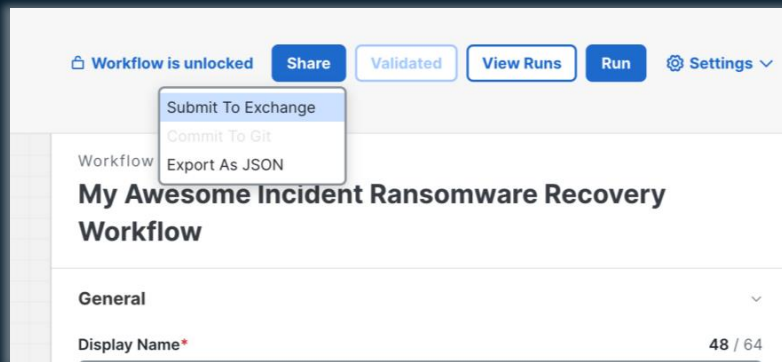
- Automation
- Platform APIs (IROH)
- Incidents and Investigations
- Global Intelligence
- Private Intelligence
- Playbook

Developer Resources

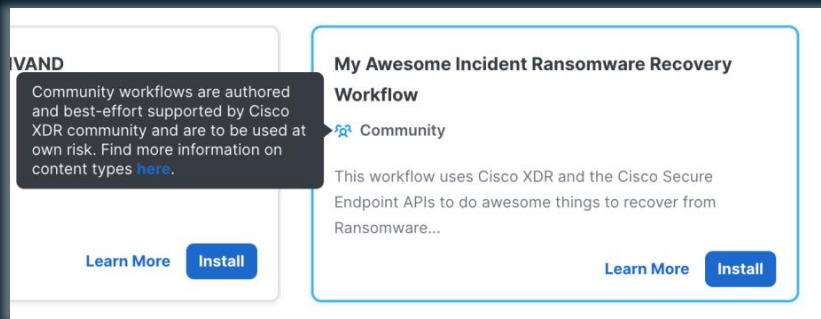
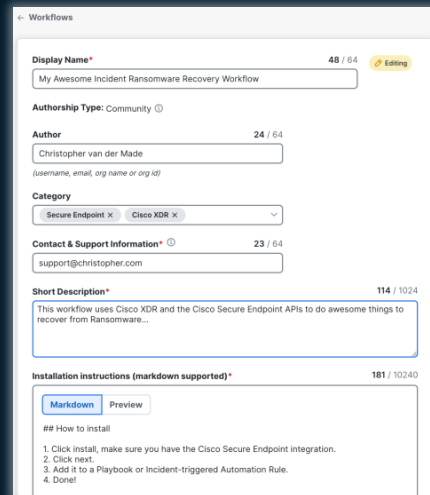
- Learning Labs
- Sample Code and Scripts

Cisco XDR Automation Exchange is now OPEN!

Step 1: build your workflow* and click "Submit to Exchange"



Step 2: fill in all details* and click "Save"



Step 3: it will be reviewed, approved and published to Exchange as "Community"

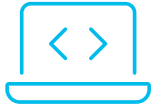
*best practices [HERE](#).

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/>

XDR API resources



Documentation

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



Postman Collection

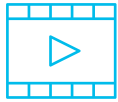
<https://cs.co/xdr-postman-collection>



Postman Environment

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

XDR Automation resources



Videos

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



Documentation

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



DevNet

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

Cisco Security Beta Programs



Influence product design

Design research participants shape the look, feel, & functionality of new product features and offerings



Attention to Feedback

Beta customer bugs and enhancements receive high visibility & priority



Top notch communication

Private conference calls with product team



Training

Customers receive early training & experience with new features



Customer Support

Feature experts will be on-hand & responsive to your issues



Sign-Up Now: <https://cs.co/security-beta>

Agenda

- ~~What is Incident Response?~~
- ~~How to perform Incident Response with Cisco XDR?~~
 - ~~Introduction to Cisco XDR (Automation)~~
 - ~~Pivot Menu~~
 - ~~Playbook Tasks~~
 - ~~Automation Rules~~
- ~~Let's put it to practice!~~
- ~~Future?~~

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

Contact me at: chrivand@cisco.com



The bridge to possible

Thank you

CISCO *Live!*

#CiscoLive