

CISCO *Live!*

Let's go

#CiscoLive



The bridge to possible

# Cisco XDR with Firewall

Adi Sankar, Technical Marketing Engineer  
BRKSEC-2090

CISCO *Live!*

#CiscoLive



# Cisco Webex App

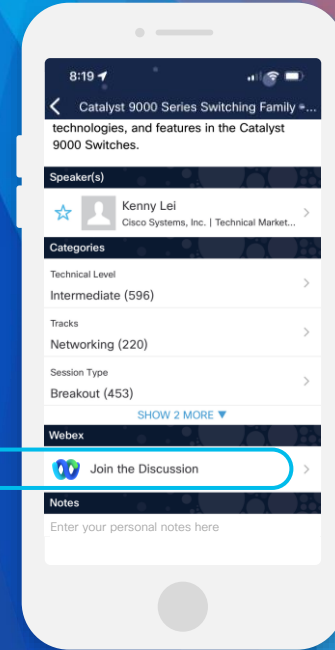
## Questions?

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 9, 2023.



<https://cislive.ciscoevents.com/cislivebot/#BRKSEC-2090>

# Session Abstract

Cisco XDR is the broadest most integrated platform in the world. In this session attendees will see the power of Firewall and XDR integration. This includes Firewall event data sent to XDR analytics and how this raw telemetry is used to create detections. Firewall enrichment to XDR investigations and using XDR automate with Firewall API's. Attendees should have a basic understanding of Cisco Secure Firewall. Attendees do not require knowledge of XDR since all components will be covered in detail.

# About Me...

2016 – CCNA (Routing and Switching)

2017 – CCNP (Switching)

2018 – 2020 – TAC Engineer, Firewall Team

2020 – 2023 – Technical Marketing Engineer, XDR

## Areas of Expertise

Security (ASA, FTD, FMC)

dCloud Demo (XDR)

API

Python

## Time Pass

Engineers Day at the Museum

Habitat For Humanity

FIRST Robotics

F1 Race

Soccer



Nov 2013



Dec 2013



April 2023



July 2012



3D-Printing Cisco US2020 – 2013



Aug 2011



Aug 2012



Oct 2014



Dec 2014

Team (3459) PyroTech

**CISCO** *Live!*

# Agenda

CISCO *Live!*

- The power of XDR
- How Cisco Secure Firewall boosts XDR
- What is Security Services Exchange and how does it work with Secure Firewall?
- Demo time!
- Next steps / Resources

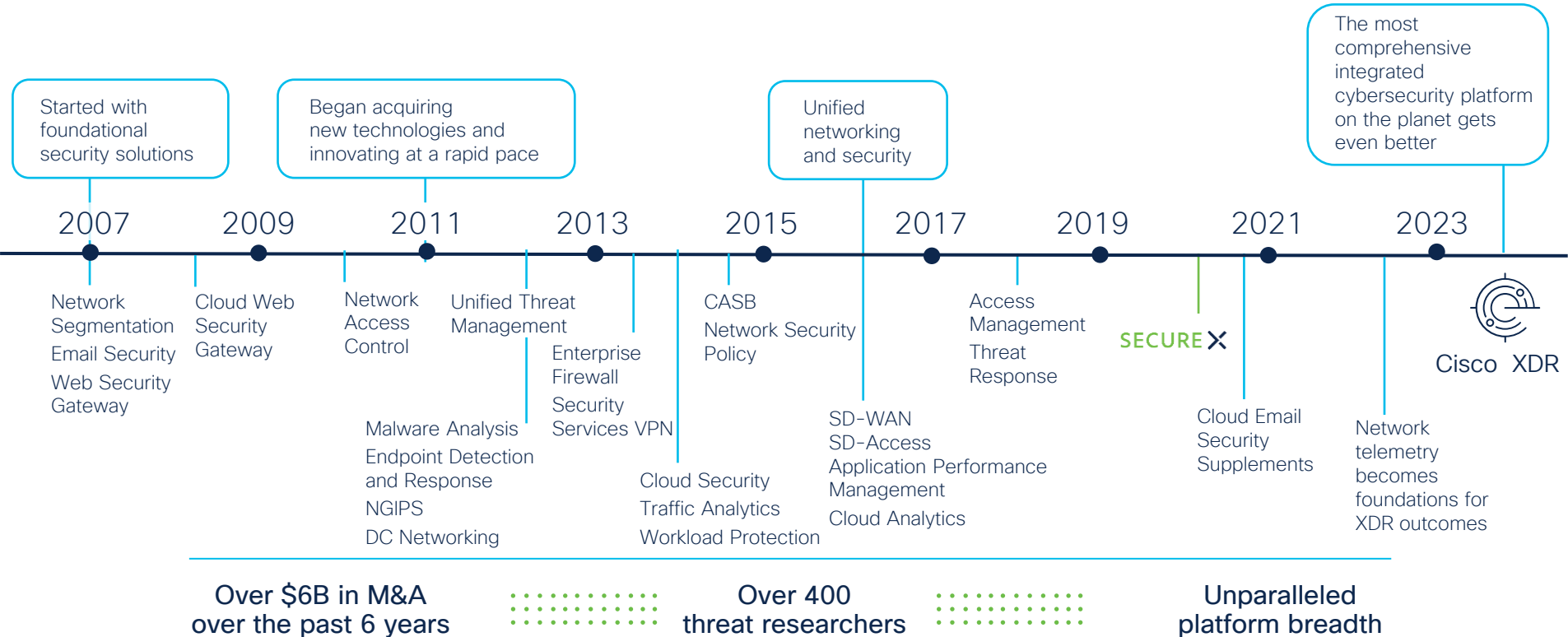


## OBJECTIVES



- What is XDR and how it can enhance your Security Operations?
- How can you integrate your Firewall with XDR?
- How does the Firewall and XDR integration work behind the scenes?
- 5 valuable use cases you can enable today!!

# Building a platform takes time and engineering talent



# An XDR is as good as its outcomes

Where are we **most exposed** to risk? How good are we at detecting attacks **early**?

1 Detect Sooner

Prioritize by Impact

2

Are we **prioritizing the attacks** that represent the largest **material impacts** to our business?

How quickly are we able to understand the **full scope** and **entry vectors** of attacks?

3 Reduce Investigation Time

Accelerate Response

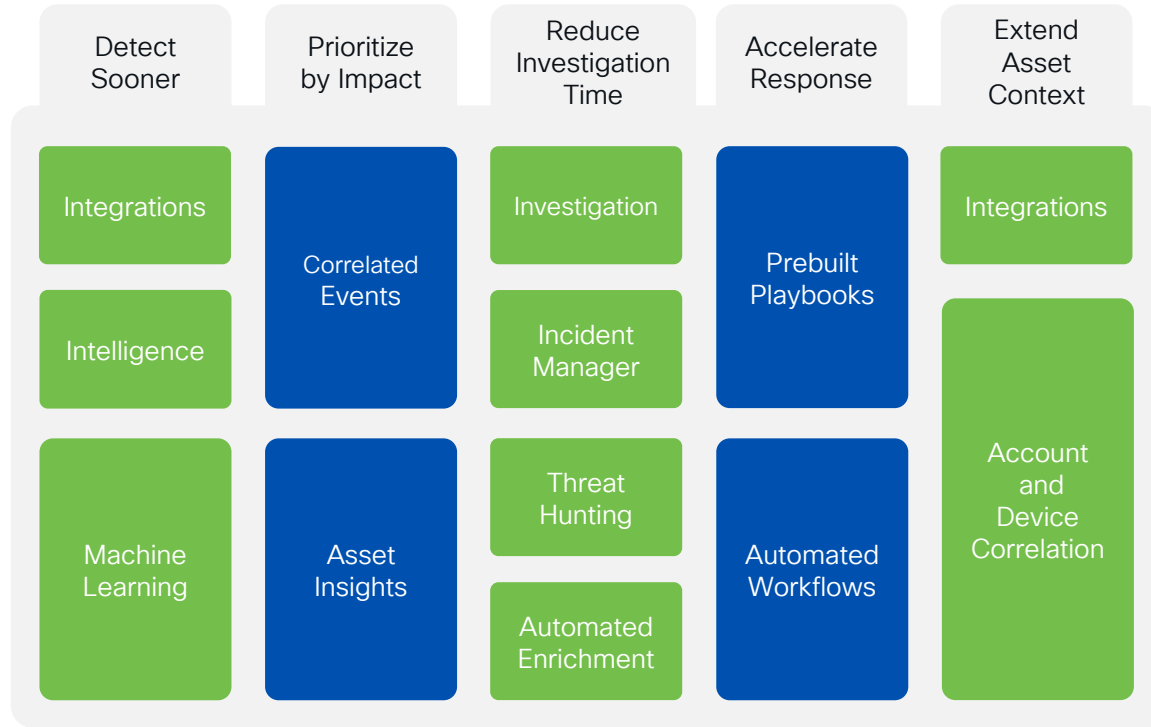
4

How fast can we **confidently respond**? How much can SecOps **automate**? Are we **improving** our time to respond?

Do we have **full visibility** into all our assets? Can we **reliably identify** a device and who uses it?

5 Extend Asset Context

# XDR outcomes and components



**Analytics**  
Detections based on raw telemetry

**Incidents**  
Security alerts, correlated, prioritized and enriched

**Integrations**  
built-in, pre-built or custom

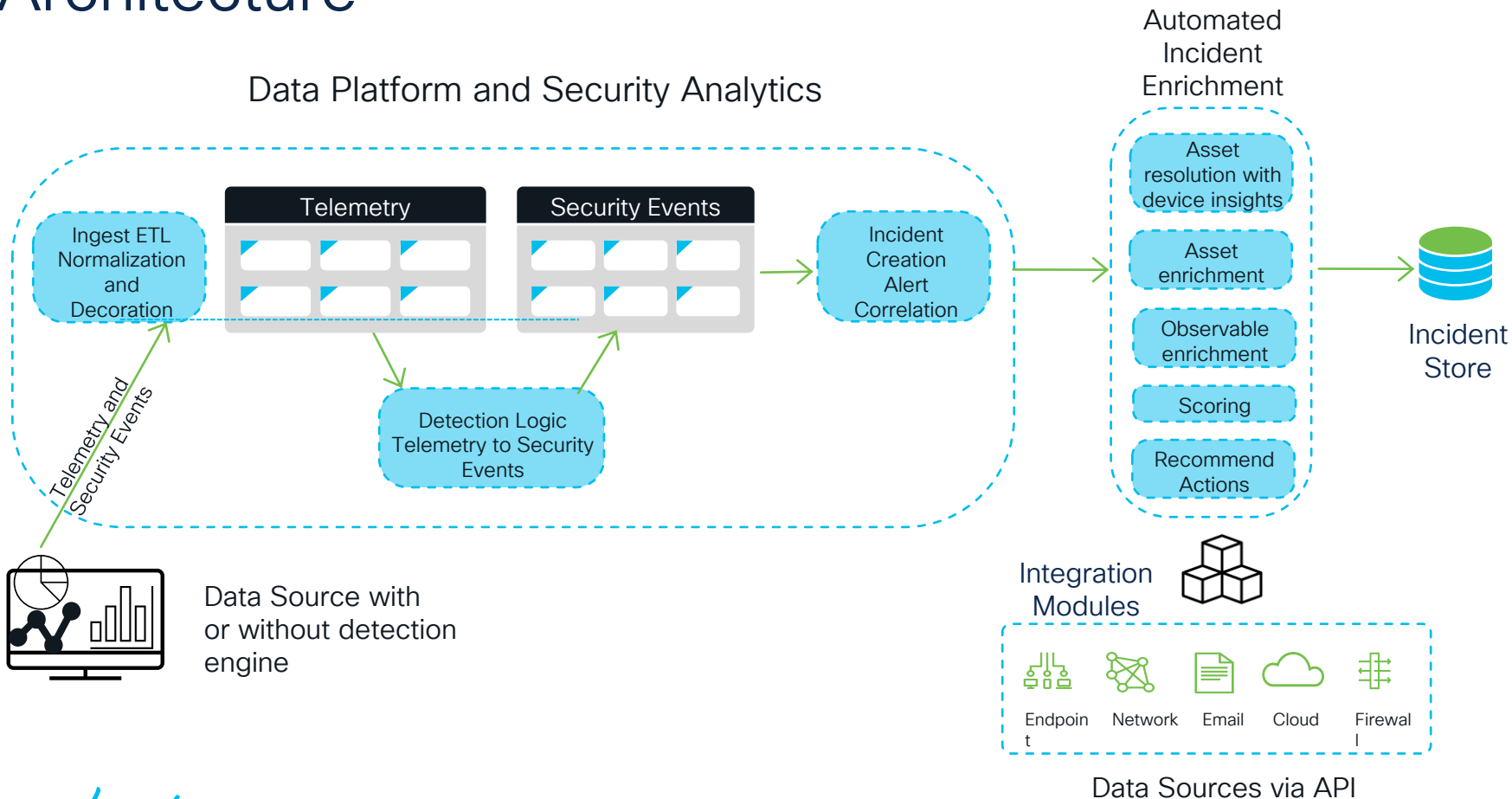
**Investigate**  
is at the core of the platform

**Automate**  
drag-drop GUI for no/low code

**Devices**  
device inventory with the contextual awareness

# Architecture

## Data Platform and Security Analytics



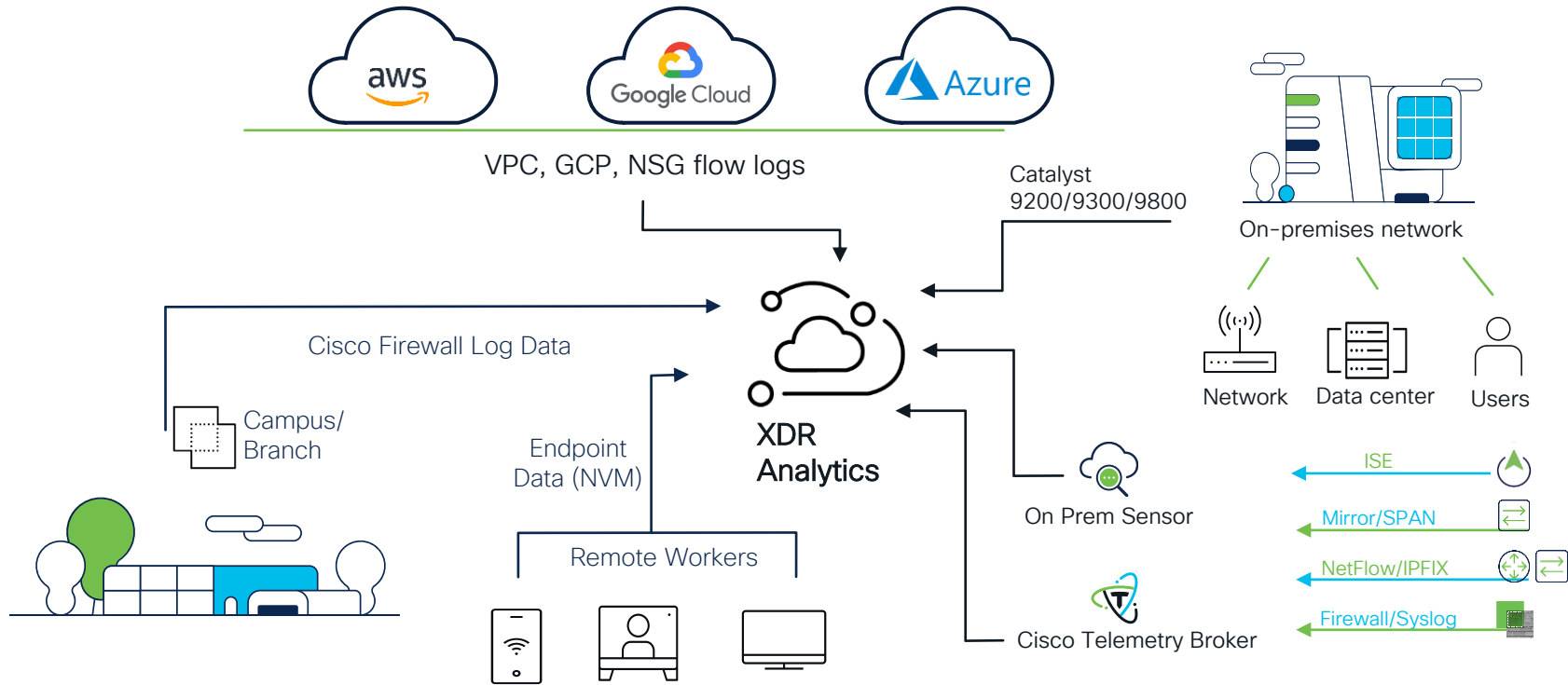
# Overview Demo

# XDR Analytics



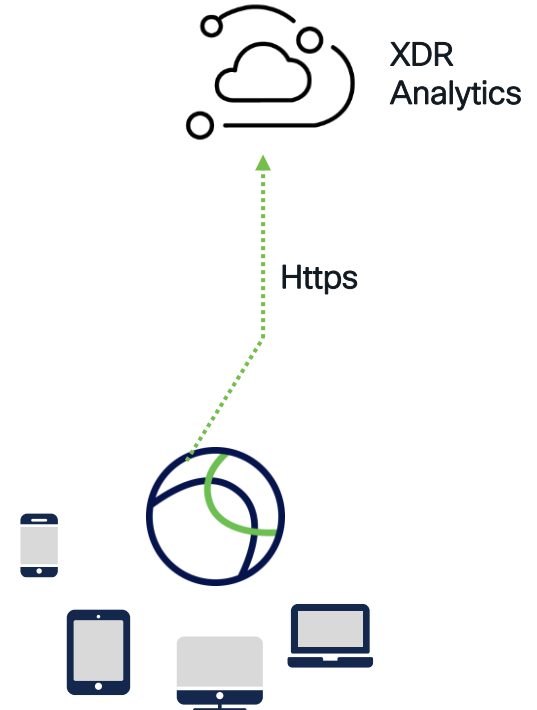
# Raw Telemetry sources for XDR Analytics

## Flexible ingest for dynamic environments

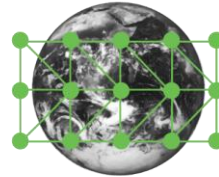
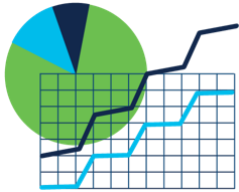


# NVM Data to XDR analytics

Start Time*
End Time*
Source IP*
Source Port*
Destination IP*
Destination Port*
Bytes Sent*
Bytes Received*
Packet Count* (derived)
Protocol*
Interface Info UID
Interface Index
Interface Type
Interface Name
Interface Details List
Interface Mac Addr.
UDID
User
User Account Type
Agent Version
Virtual Station Name
OS Name
OS Version
OS Edition
System Manufacturer
System Type
Process Account*
Process Account Type
Process ID
Process Name*
Process Hash*
Process Path
Process Args
Parent Process ID
Parent Process Account
Process Account
Parent Process Name*
Parent Process Hash*
Parent Process Path
Parent Process Args
Host Name
DNS Suffix
Module Name List
Module Hash List
Parent Process Name
Parent Process Hash



# XDR Analytics detections from raw telemetry



## Behavioral analytics

- Anomaly detection through statistical learning
- Cloud specific behavior analysis
- Role-based analytics
- Data movement analytics

## Cloud Alerts

- Alerts tailored to AWS, GCP and Azure
- Leverage native cloud security controls
- Detect security relevant configuration changes
- Assess your cloud security posture

## Global Threat Alerts

- Machine learning based threat detection
- Intel gathered from across the Cisco ecosystem
- Detect threats within encrypted traffic without decrypting

## Talos threat intel

- Malware classification
- Knowledge and correlation of global campaigns to local threats
- Threatening IP, URL and Domain Communication Detections

# Comprehensive Hybrid Cloud protection through detections



## Public Cloud Alerts

- Abnormal User
- AWS EC2 Startup Script Modified
- AWS Lambda Invocation Spike
- AWS Snapshot Exfiltration
- Azure Exposed Services
- Azure Transfer Data To Cloud Account
- Geographically Unusual AWS/Azure API Usage
- Unusually Large EC2 Instance
- +40 more detections...



## Private Network/On-prem

- Amplification Attack
- Exceptional Domain Controller
- Geographically Unusual Remote Access
- LDAP Connection Spike
- Meterpreter C&C Success
- Potential Data/Database Exfiltration
- Protocol Forgery
- Repeated Umbrella Sinkhole Communications
- Unusual DNS Connection
- Vulnerable Transport Security Protocol
- +60 more detections...



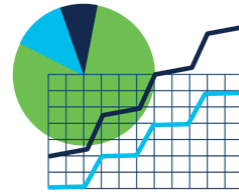
## Firewall logging

- Potentially Harmful Hidden File Ext
- Repeated Watchlist Communications
- Suspicious User Agent
- Talos Intelligence Watchlist Hits
- Unusual External Server
- Unusual File Extension from New External Server
- +72 on-prem detections

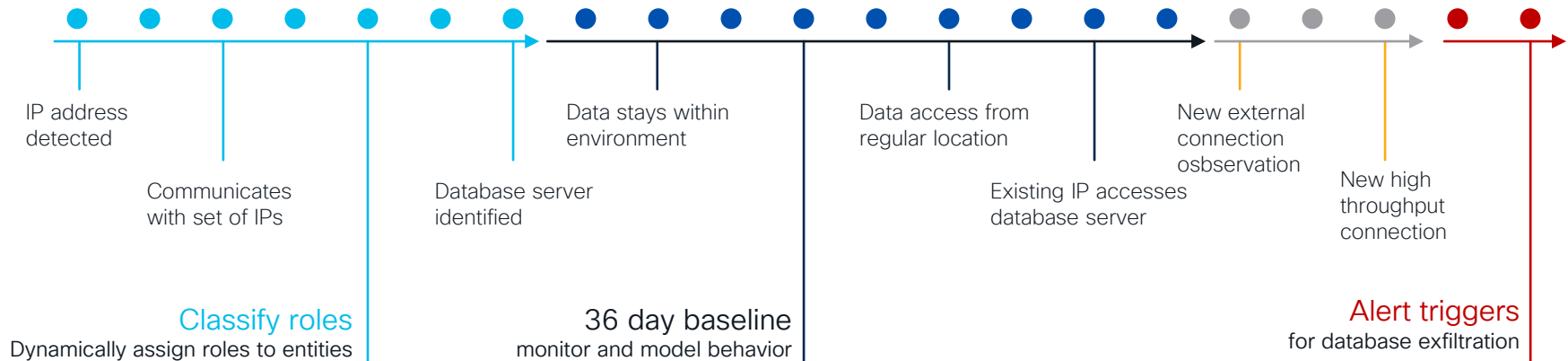
The **efficacy of all XDR Analytics alerts stands at approximately 96%**, with a monthly customer response rate on over 5000 alerts!

# Detect abnormal activity using entity modeling

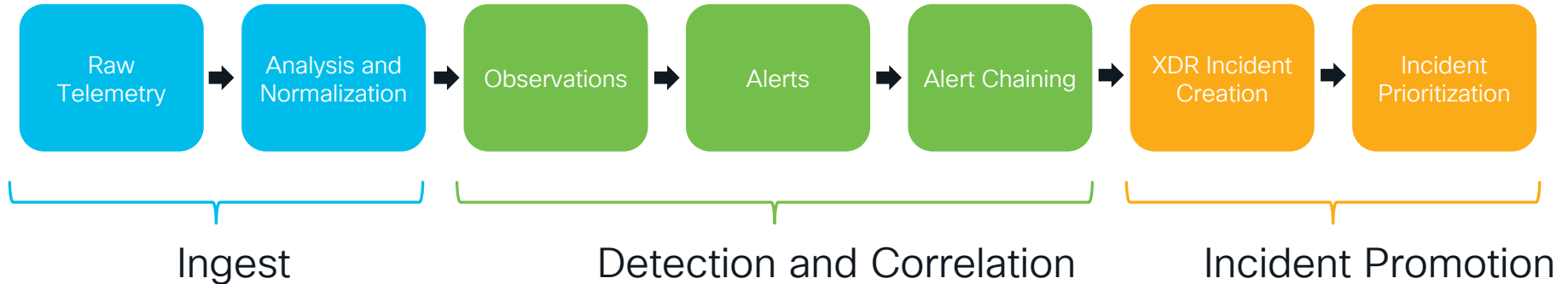
30+ detections  
active on day zero



130+ available  
alerts

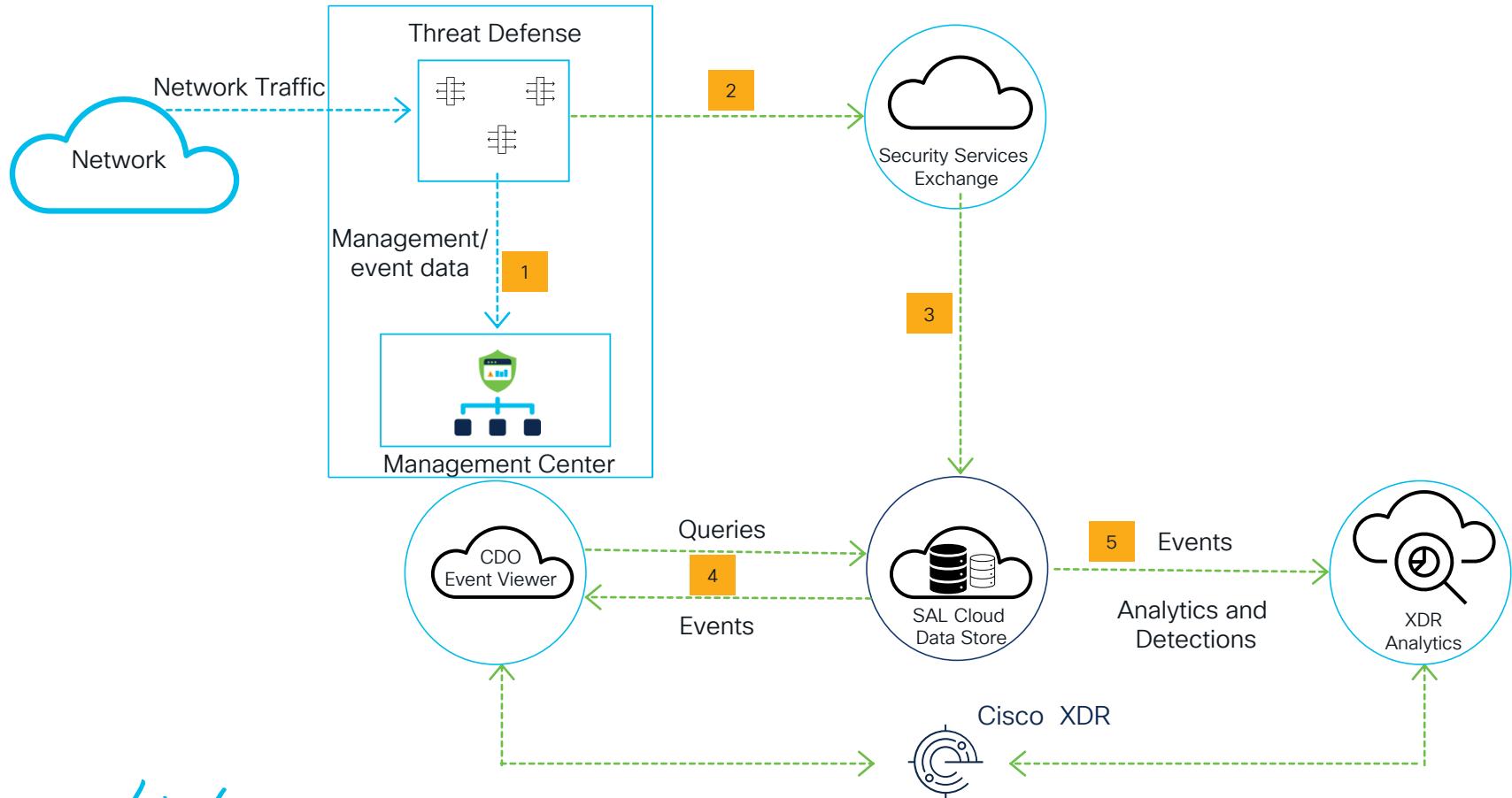


# XDR Analytics detection and incident creation path



XDR Analytics covers end-to-end from raw telemetry to correlated, prioritized incidents which are enriched with context

# Eventing High Level Flow



# Flow Processing Fully Explained

As it happens

Every 10 minutes

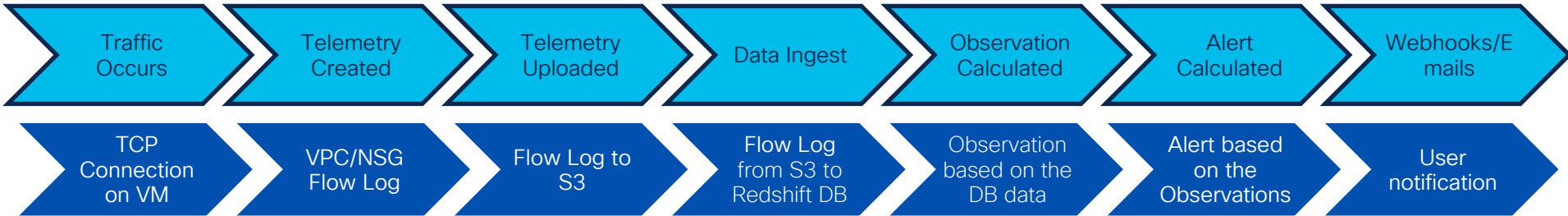
Typically, takes ~15 minutes

Every 10 mins add .gz file to queue + processing time

Tasks are scheduled either every 10 mins, 1 hour or 1 day + long processing time

Tasks are scheduled either every 10 mins, 1 hour or 1 day + short processing time

New alert event triggered + processing time



SSH on TCP/22

Traffic information collected and aggregated

Flow Log file (.gz) is uploaded to S3 bucket

Downloads Flow Log file from S3, processes it, and uploads results to internal Redshift DB

Timing depends on the individual Observation

Timing depends on the individual Alert

Notifications are only for Alerts

# Alerts with MITRE ATT&CK Tactics and Techniques

## Single menu for all alert configuration

Alert Type	History	Priority	Enabled	Publish to SecureX	Telemetry	MITRE ATT&CK Tactics	MITRE ATT&CK Techniques
<b>AWS Config Rule Violation</b> An AWS Config rule was violated. This alert uses the AWS Config Compliance observation and indicates that the resource is not compliant with configured AWS Config rules.	0 Days	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Persistence	Account Manipulation
<b>AWS Console Login Failures</b> The user root and failed to log in to the AWS Console several times. This alert uses the AWS CloudTrail Event observation and may indicate an unauthorized user is attempting to gain access.	0 Days	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Credential Access	Brute Force
<b>AWS Detector Modified</b> An AWS GuardDuty detector was deleted or disabled. This alert uses the AWS CloudTrail Event observation and may indicate an attempt to avoid detection of malicious activity.	0 Days	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Defense Evasion	Impact Determination
<b>AWS Domain Takeover</b> An AWS domain was transferred to another account. This alert uses the AWS CloudTrail Event observation and may indicate an attempt to hijack your domain to another account. It can be a sign of malicious activity or a violation of security policies.	0 Days	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Initial Access	Compromise Information
<b>AWS EC2 Startup Script Modified</b> An AWS EC2 instance was stopped and user data was modified. User data allows passing a script which runs after the instance starts. This alert uses the AWS CloudTrail Event observation and may indicate an attempt by a malicious actor to establish persistence or escalate malicious code.	1 Days	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Persistence	Sort of Logic Injections
<b>AWS ECS Credential Access</b> An ECS Task Definition was registered with a container command which will obtain credentials from the AWS IAM Role service. This alert uses the AWS CloudTrail Event observation and may indicate an attacker is attempting to obtain service credentials.	0 Days	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Persistence	Impact Normal Image
<b>AWS IAM Anywhere Trust Anchor Created</b> A new IAM Roles Anywhere trust anchor has been created. This can be legitimate activity, but could also indicate an adversary attempting to establish persistent access to the account from outside AWS.	0 Days	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Persistence	Account Manipulation
<b>AWS IAM User Takeover</b> An AWS access key was created for another user. This alert uses the AWS CloudTrail Event observation and may indicate an attacker is attempting to establish persistence in the event their method of initial access is revoked. It can be a sign of malicious activity or a violation of security policies.	0 Days	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Persistence	Account Manipulation
<b>AWS Inspector Finding</b> AWS Inspector reported a high or critical-severity finding for the device. This alert uses the Amazon Inspector Finding observation and indicates that the resource is not complying with best practices.	0 Days	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Persistence	Account Manipulation
<b>AWS Lambda Invocation Spike</b> AWS Lambda function was invoked a record number of times. This alert uses the AWS Lambda Metric: Duetter observation and may indicate operational problems or a denial of service attack.	14 Days	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Impact	Resource Hijacking
<b>AWS Lambda Persistence</b> A new AWS Lambda function has been created and associated with a new CloudWatch event. This might indicate an attempt for persistence by adding a backdoor to newly created resources.	0 Days	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Persistence	Event Triggered Execution

Source of the telemetry  
Telemetry source of the alert

Alert on what's important to you  
with the option to enable or disable specific alerts

Hover for a brief description or click to pivot to MITRE for more information

98%+ of XDR Analytics alerts are mapped to the MITRE ATT&CK framework

## Understand how alerts map to MITRE Tactics and Techniques

[XDR Analytics mapping to the MITRE ATT&CK Enterprise Matrix](#)

# Alert Chains

- Related alerts are correlated by common indicators
- Mapped to the MITRE ATT&CK Framework
- Chains are summarized with “at a Glance”
- Alert activity is plotted over time in an alert timeline
- Visualizations with alert connection graph

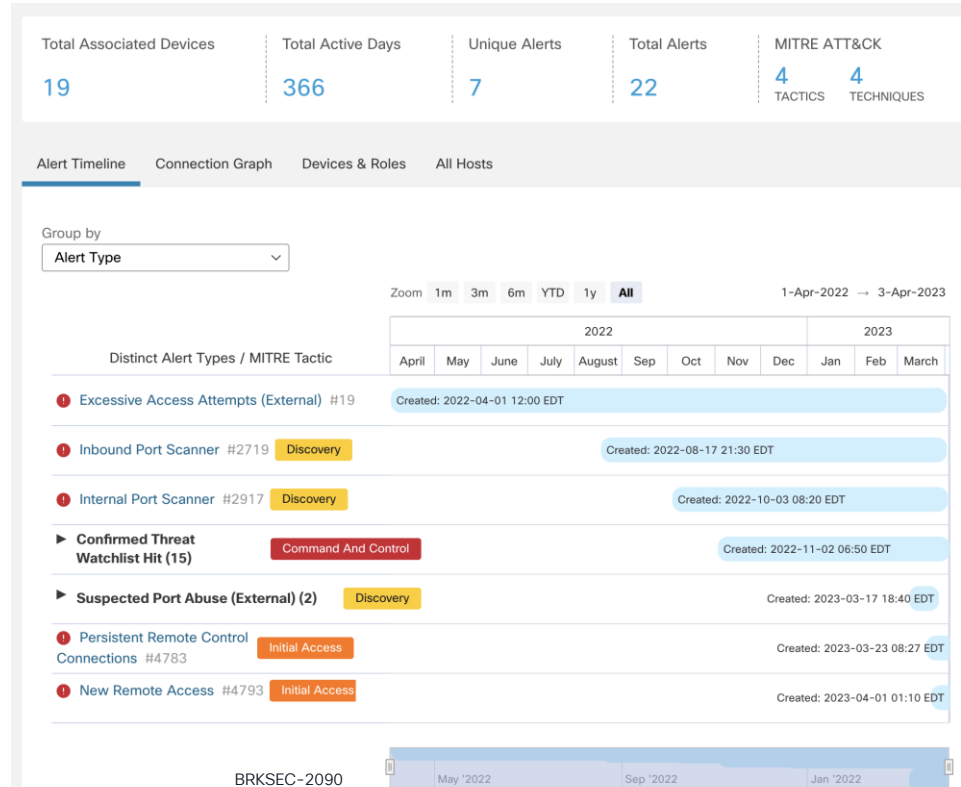
## Alert Chain at a Glance

Created 2022-04-01 12:00:00 EDT  
Last Active 2023-04-03 10:00:00 EDT  
Alert Chain ID 569  
Status ! Open

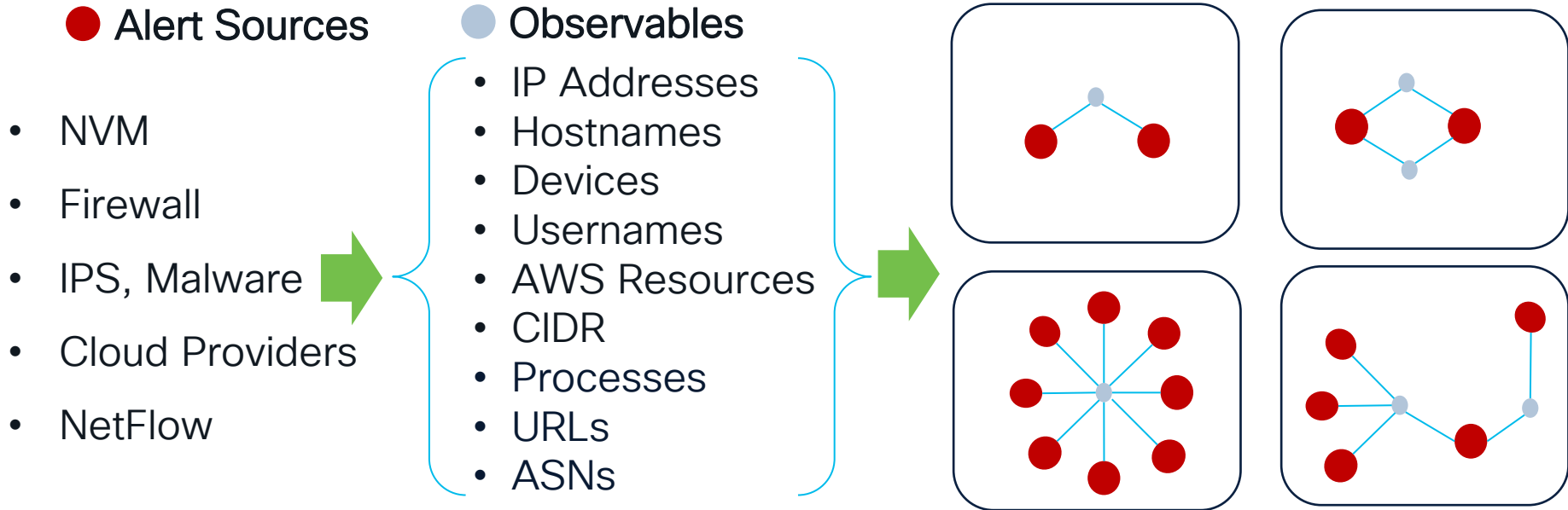
**Chaining Patterns**  
Credential Access → Discovery (2) → Command And Control (5) →  
Discovery (2) → Initial Access → Command And Control (10) →  
Initial Access

Post an Incident [Post to SecureX Incident Manager](#) ⓘ

**Common Indicators** ▲ i-06c189f3c85251a7d

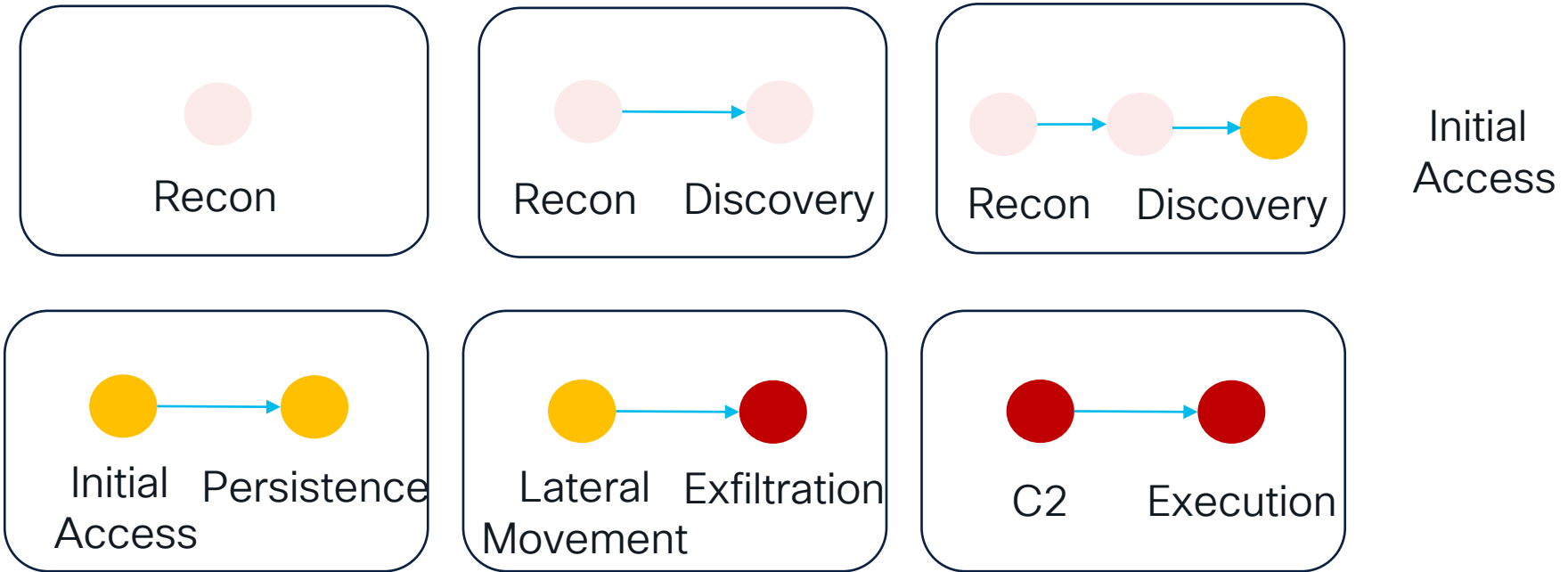


# Chaining attacks based on common observables



Leverage Common Observables to relate alerts coming from multiple sources and with different threat vectors in one attack chain.

# Capturing Attacker Intentions using MITRE ATT&CK



# Incidents

# Incidents

Prioritized Incidents based on severity

- Reduces clutter by prioritizing highest risk incidents
- Automatically enriched (investigated)
- Enrichment status displayed on incidents in list
- Created from Critical/High Endpoint events
- More to come

The screenshot shows the Cisco XDR Incidents dashboard. At the top, there are three summary boxes: "497 Incidents", "9 New Incidents", and "309 Open Incidents". Below these is a search bar and a filter for "Status: Incident Reported". The main area is a table of incidents with columns for Priority, Name, and Source. The incidents are sorted by priority, with the highest priority (1000) at the top.

Priority	Name	Source
1000	EC2AMAZ-AHQFEJR in group Audit @ 20230417 08:16:38	Secure Endpoint
1000	Geographically Unusual Remote Access for Cisco - Lawrenceville Lab (Earth)	Cisco Secure Cloud Analy...
1000	Heartbeat Connection Count for Cisco - Lawrenceville Lab (Earth)	Cisco Secure Cloud Analy...
1000	c4-3650-1-g1-8-win10 in group Earth Clients @ 20230406 13:51:59	Secure Endpoint
1000	c5-9300-1-g1-8-win10 in group Pluto Clients @ 20230406 13:52:57	Secure Endpoint
924	Attack Chain: "Multiple Threat Indicators Triggered" for Cisco - Lawrenceville Lab (Earth)	Cisco Secure Cloud Analy...
873	c1-4506-2-g3-13-win10 in group Mars Clients @ 20230406 13:52:31	Secure Endpoint
783	c3-9300-1-g1-0-7-win10 in group Audit @ 20230411 08:48:54	Secure Endpoint
765	Persistent Remote Control Connections for Cisco - Lawrenceville Lab (Earth)	Cisco Secure Cloud Analy...
523	c1-4506-1-g3-14-win10 in group Mars Clients @ 20230411 20:27:12	Secure Endpoint
392	c1-9300-1-g1-13-ublnx in group Mars Clients @ 20230411 18:26:19	Secure Endpoint

# Automatically Create Incidents With Secure Endpoint

Secure Endpoint



Security events automatically create incidents in Incident Manager based on severity

Manually promote events as incidents from Secure Endpoint Inbox

Cisco XDR Incidents

31 Require Attention 0 In Progress 0 Resolved

Begin Work Mark Resolved Move to Group... Promote to Incident Manager

Sort Date

**Demo\_Command\_Line\_Arguments\_Meterpreter in group Triage** 100 1 event

Hostname	Demo_Command_Line_Arguments_Meterpreter	Group	Triage
Operating System	Windows 10 (Build 19044.1486)	Policy	Triage
Connector Version	8.1.7.21417	Internal IP	102.36.243.208
Install Date	2023-04-27 03:30:24 UTC	External IP	5.63.112.225
Connector GUID	29867707-10e4-4aaa-aec8-7d9270460497	Last Seen	2023-05-27 03:30:24 UTC
Processor ID	9ae374082d15bf6	Cisco Secure Client ID	N/A
		Kenna Risk Score	100

Related Compromise Events

**High** W32.PossibleName... 935c1861...65d44ad2 2023-05-27 02:32:58 UTC

Vulnerabilities

No known software vulnerabilities observed.

Events Device Trajectory Diagnostics View Changes

Start Isolation Scan... Diagnose... Move to Group... Begin Work Mark Resolved Promote to Incident Manager

Priority **1000** Status **New**

## Demo\_Command\_Line\_Arguments\_Meterpreter in group...

Reported by [Secure Endpoint](#) 6 days ago

Assigned Unassigned

MITRE (.....)

### Priority score breakdown

**1000** | 100 Detection Risk | 10 Asset Value at Risk

### Short description

### Long description

Incident Title  
Demo\_Command\_Line\_Arguments\_Meterpreter

Promoted at  
2023-05-22 21:25:15 UTC

Promotion method  
Manual

Indicators  
**W32.PossibleNamedPipeImpersonation.ioc:** A named pipe was created in a manner similar to that used for local privilege escalation through named pipe impersonation. Tools such as meterpreter often use this technique to escalate to NT Authority\System.

MITRE Tactics  
TA0004: Privilege Escalation

Host name  
Demo\_Command\_Line\_Arguments\_Meterpreter

[View Incident Detail](#)

# Automatically Create Incidents With XDR Analytics

XDR  
Analytics



Create incidents automatically in  
Incident Manger as part of alert  
settings

Manually promote alerts as part of XDR  
Analytics alert workflow

Cisco XDR  
Incidents

Alert Type	History	Priority	Enabled	Publish to SecureX	Telemetry
<input type="text" value="url"/>					
<b>Potentially Harmful Hidden File Extension</b> Device has encountered a file with a potentially harmful hidden extension. The alert uses the Multiple File Extensions observation, requires URL data provided by firewalls via the Cisco Security Analytics and Logging (SAL) integration, and may indicate the device has downloaded malware.	0 Days	Normal Default Priority: Normal	<input checked="" type="checkbox"/> Default: Enabled	<input checked="" type="checkbox"/>	ETA   Firewall
<b>Suspected Malicious URL</b> The device communicated with a suspected malicious URL. The alert uses the Suspected Malicious URL observation and requires URL data provided by firewalls via the Cisco Security Analytics and Logging (SAL) integration or Enhanced Netflow.	0 Days	High Default Priority: Normal	<input checked="" type="checkbox"/> Default: Enabled	<input checked="" type="checkbox"/>	ETA   Firewall North-South
<b>Unusual File Extension from New External Server</b> A new file extension, unseen in the recent past, was exchanged between the entity and a new external server. This might indicate a malware attempting to communicate with its command and control center. This alert uses the New File Extension and the New External Server observations. The former requires URL data provided by firewalls via the Cisco Security Analytics and Logging (SAL) integration.	1 Days	Normal Default Priority: Normal	<input checked="" type="checkbox"/> Default: Disabled	<input checked="" type="checkbox"/>	Firewall   Firewall North-South

Configure severity and publication settings in  
Secure Cloud Analytics

Priority **765** Status Incident Report... ✕

### Suspected Malicious URL on ip 192-168-249-115

Reported by [Cisco Secure Cloud Analytics \(cisco-dcloud-rtp\)](#) 1 day ago  
Assigned Unassigned  
MITRE \*\*\*\*\*

---

**Priority score breakdown** ⌵

**765** 76 10  
Detection Risk Asset Value at Risk

---

**Short description** ⌵

Suspected Malicious URL for Cisco Demo (RTP)

---

**Long description** ⌵

Alert  
Suspected Malicious URL - #11941

Tenant  
Cisco Demo (RTP) (cisco-dcloud-rtp)

Source  
ip-192-168-249-115.us-east-2.compute.internal

Description  
The device communicated with a suspected malicious URL. The alert uses the Suspected Malicious URL observation and requires URL data provided by firewalls via the Cisco Security Analytics and Logging (SAL) integration or Enhanced Netflow.

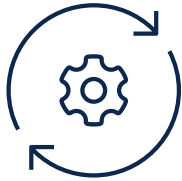
Next Steps  
Reference the supporting observations to determine what URL the entity accessed. Determine if the

[View Incident Detail](#)

# Automatically Create Incidents

## With Cisco XDR Automate

Cisco  
XDR  
Automate



Workflow polls API on  
scheduled interval.

If detections is found  
incident is automatically  
created

Cisco XDR  
Incidents

PROPERTIES: THREAT RESPONSE - CREATE INCIDENT

Threat Response - Create Incident

Workflow

Threat Response - Create Incident

\* INPUT

\* Incident Confidence

\* TLP Value

Incident Description   
## Please check sightings tab and below for more information.  
\*\*Message:\*\* [Message]  
\*\*Meraki Rule ID:\*\* [Rule ID]  
\*\*Action taken:\*\* [Action]

\* Incident Status

\* Incident Title

Access Token

Priority **1000** Status **New**

### SG-CertName-Observable Incident with Suspicious...

Reported by **Cisco XDR Automate** 18 days ago  
Assigned Unassigned  
MITRE

**Priority score breakdown**

<b>1000</b>	<b>100</b> Detection Risk	<b>10</b> Asset Value at Risk
-------------	------------------------------	----------------------------------

**Short description**

Hareesh INT Correlated Incident with Suspicious Activity (NVM + CrowdStrike) - [Test incident created by SXO]

**Long description**

**Description:** A process running has a hash matching one in a list of known malicious process hashes.  
**Recommended Next Steps:** Isolate the endpoint and investigate if a malicious executable was run.

[View Incident Detail](#)

# Prioritize by impact

- Single view for incidents from multiple sources
- Enhanced incident view focused on the most critical incidents
- Incidents prioritized by business impact and asset value

**1000**

**100**

Detection  
Risk

**10**

Asset  
Value at Risk

The screenshot displays the 'Incidents' dashboard with the following components:

- Summary Cards:** 62 Incidents, 33 New Incidents, 8 Open Incidents.
- Search and Filters:** Search bar with 62 matching results and a Filters dropdown.
- Incident List Table:**

<input type="checkbox"/>	Priority	Name	Source
<input type="checkbox"/>	1000	Malicious Process and Suspicious SMB/RDP Activity - Doc Test Do ...	Cisco Secure Clou...
<input type="checkbox"/>	1000	Unusual External Server for This is localhost	Cisco Stealthwatc...
<input type="checkbox"/>	1000	AWS Inspector Finding for This is localhost	Cisco Stealthwatc...
<input type="checkbox"/>	1000	Command and Control DNS Activities	Umbrella
<input type="checkbox"/>	928	Formula Test.Mar27.Critical.TTP(58).AssetValue[8]	FormulaTest
<input type="checkbox"/>	928	F1.03-06d.Critical.TTP(58).AssetValue[10]	FormulaTest
<input type="checkbox"/>	835	Attack Graph Test - 109 Observables	FormulaTest
<input type="checkbox"/>	800	F1.03-06a.Critical.TTP(50).AssetValue[NULL]	FormulaTest
<input type="checkbox"/>	765	New Internal Device for This is localhost	Cisco Stealthwatc...
<input type="checkbox"/>	765	Azure Permissive Security Group for TD&R RSA	Cisco Secure Clou...
<input type="checkbox"/>	742	F1.03-08.Critical.TTP(58).AssetValue[8]	FormulaTest

# Identify the most impactful incidents based on risk

$$1000 \quad | \quad \begin{matrix} 100 \\ \text{Detection} \\ \text{Risk} \end{matrix} \quad \begin{matrix} 10 \\ \text{Asset} \\ \text{Value at Risk} \end{matrix}$$

$$\begin{matrix} \text{Priority Score} \\ 0-1000 \end{matrix} = \begin{matrix} \text{Detection Risk} \\ 0-100 \end{matrix} \times \begin{matrix} \text{Asset Value} \\ 0-10 \end{matrix}$$

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

# Walk through incidents step-by-step

## Progressive reveal of details

Looking into an incident is a progressive experience where the relevant data is revealed as needed without overwhelming the SOC analyst

Priority	Name
1000	Malicious Process and Suspicious SMB/RDP Activity Detect
1000	Unusual External Server for This is localhost

## Rich incident details

Incidents are enriched with data gathered from multiple sources including assets, indicators, observables and others. Associated MITRE attack Tactics and techniques detailed with risk scoring

Priority **1000** Status **New**

### Malicious Process and Suspicious SMB/RDP...

Reported by **Cisco Secure Cloud Analytics (rsa)**  
15 hours ago

Assigned **BM** **JF**

MITRE **\*\*\*\*\***

---

#### Priority score breakdown

**1000**

- 100 Detection Risk
- 10 Asset Value at Risk

---

#### Short description

This feature is currently under active development

---

#### Long description

Alert Chain  
fb56eea65af173cd7286d510722e4f8f7e5c8613

Description

[View Incident Detail](#)

**MITRE | ATT&CK** View all Tactics

#### Tactics

TA0002: Execution **100**

The adversary is trying to run malicious code. Execution consists of techniques that result in adversary-controlled code running on a local or remote system. Techniques that run malicious code are often paired with techniques from all other tactics to achieve broader goals, like exploring a network or stealing data. For example, an adversary might use a remote access tool to run a PowerShell script that does Remote System Discovery.

TA0008: Lateral Movement **66**

Orientation

NT AUTHORITY\NETW...  
C:\Windows\System...  
virtualmachinesw...  
System  
dc-2.org1.net  
dc-2.org1.net  
10.0.1.6

---

#### 4 Assets

[View Assets](#)

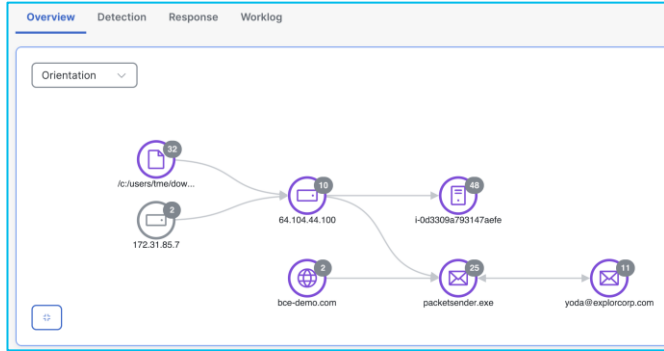
- virtualmachines/win-vic-2 (6 events)
- virtualmachines/win-dc-0 (5 events)
- virtualmachines/win-vic-6 (4 events)
- virtualmachines/kali (1 event)

---

#### 31 Observables

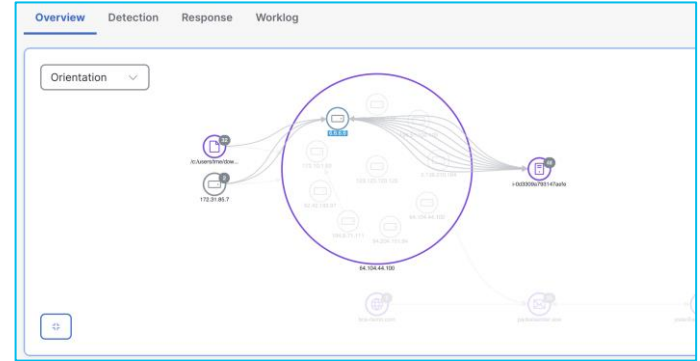
- NT AUTHORITY\SYSTEM
- C:\Windows\System32\svchost.exe
- svchost.exe
- SYSTEM

# Walk through incidents step-by-step - Overview



## Simplified Graphical view

A simple yet powerful graph tool to identify observables and their relations. Expand the view for additional details.



16 Assets	View Assets	31 Observables	View Observables	11 Indicators	View Indicators
MIKE-WIN10	85 events	6.6.6.6	303 events	Cisco Secure Cloud Analytics (cisco-explor... <b>Remote Access</b>	6 events
i-0e682308df7f7bf0a	41 events	1bf529e3f6bff6d974443...	118 events	Cisco Secure Cloud Analytics (cisco-explor... <b>User Watchlist Hit</b>	3 events
i-0d3309a793147aefe	26 events	94.204.151.84	16 events	Cisco Secure Cloud Analytics (cisco-explor... <b>Watchlist Interaction</b>	3 events
EC2AMAZ-AHQFEJR	18 events	64.104.44.100	6 events	Cisco Secure Cloud Analytics (cisco-explor... <b>Geographically Unusual Remote Acc...</b>	3 events
EC2AMAZ-MTKLEVO	13 events	3.136.210.164	5 events		

The incident overview displays details such as; involved assets, the list of observables with their respective dispositions and the indicators that are related to them.

# Walk through incidents step-by-step – Detection

The interface displays a list of detection events with the following columns: First Seen, Severity, Source, Indicators, and Observables. The events are filtered by severity (High and Critical) and source (Secure Endpoint, NGFW Event Service, and Cisco Secure Cloud Analytics).

First Seen	Severity	Source	Indicators	Observables
2023-04-18T17:27:20.000Z	High	Secure Endpoint		1bf529e3f6bff6d97444319f48c4059...
2023-04-17T15:18:17.000Z	High	Secure Endpoint	W32.PowershellDownloadedExecutable.i	de96a6e69944335375dc1ac238336...
2023-04-17T13:10:44.000Z	High	NGFW Event Service	Security Intelligence event - IP_Reputac	172.10.1.63 123.123.123.123
2023-04-17T13:10:36.000Z	High	NGFW Event Service	Security Intelligence event - IP_Reputac	172.10.1.63 6.6.6.6
2023-04-17T12:10:00.000Z	Critical	Cisco Secure Cloud Analytics (ci...	Watchlist Interaction	6.6.6.6
2023-04-17T12:10:00.000Z	Critical	Cisco Secure Cloud Analytics (ci...	Watchlist Interaction	6.6.6.6
2023-04-17T12:10:00.000Z	Critical	Cisco Secure Cloud Analytics (ci...	User Watchlist Hit	

**Filters:**

- Severity: All, Critical, High, Medium, Low, None, Unknown, Info
- Source: All, Source (dropdown)
- Severity: All, Severity (dropdown)

**Source Selection:**

- Secure Email Threat Defense
- Cisco Secure Cloud Analytics (cisco-explorcorp-earth)
- AMP Event
- Secure Endpoint
- Cisco Secure Network Analytics
- CESA/NVM
- NGFW Event Service

**Drill down into Detection Details**

Identify the events that caused an incidents along their sources, severity and the associated observables with their relations. Apply filtering capabilities to narrow down the search faster and easier.

**Relations:** 172.10.1.63 Connected to 6.6.6.6

**Indicators:** 1  
NGFW Event Service  
Security Intelligence event - IP\_ReputationSL\_Category - ExplorCorp\_Malicious\_IPs  
ExplorCorp\_Malicious\_IPs

**Assets:** 1  
172.10.1.63

**Observables:** 2  
172.10.1.63  
6.6.6.6

# Walk through incidents step-by-step – Response

The image displays a sequence of four overlapping screenshots from a security management interface, illustrating the 'Response' phase of an incident response workflow. Each screenshot shows a navigation menu on the left with tabs for Overview, Detection, Response, and Worklog. The 'Response' tab is active in all views.

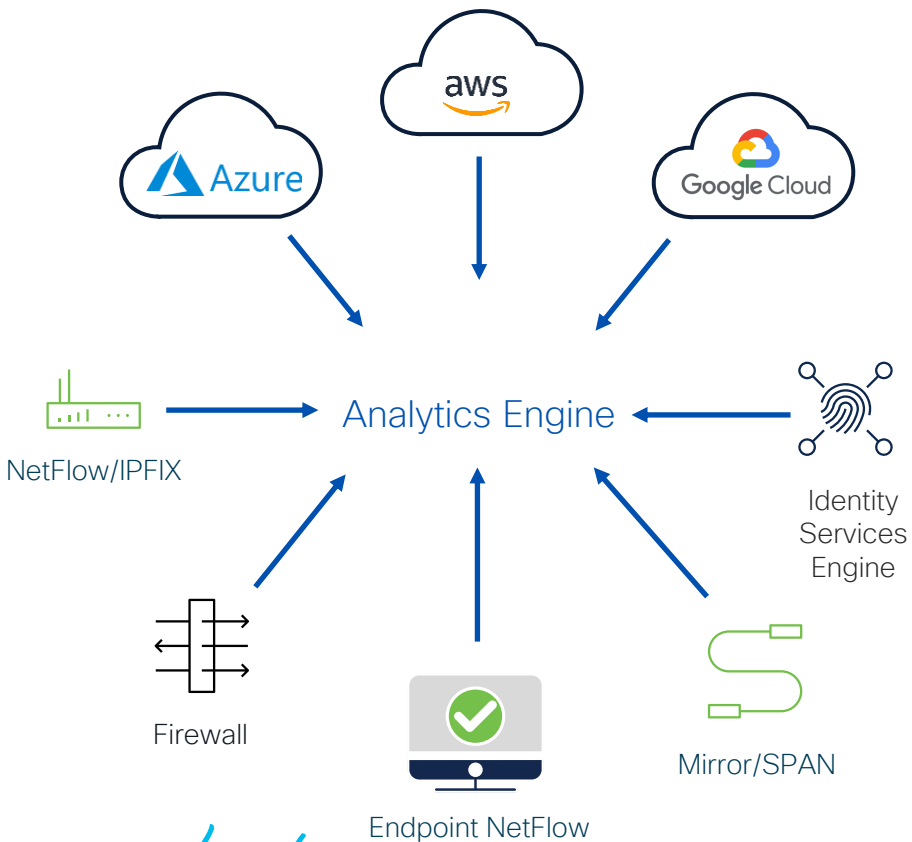
- First Screenshot:** Shows the 'Review Incident' task under the 'Identification' phase. The description is: "Add a note to record the evidence (indicators and reasoning) that supports the decision for assigning a status of Rej...".
- Second Screenshot:** Shows the 'Identify Affected Hosts' task under the 'Containment' phase. The description is: "Add note with summary of findings on the investigations of hosts found with malicious indicators".
- Third Screenshot:** Shows two tasks under the 'Eradication' phase: 'Mitigate or Remediate Vulnerabilities' (description: "Add a note on what are the affecting vulnerabilities linked to the incident and how mitigations or remediation is going...") and 'Remove Malicious Content' (description: "Add a note on the action achieved to ensure the removal of the malware.").
- Fourth Screenshot:** Shows three tasks under the 'Recovery' phase: 'Validate Eradicated Hosts' (description: "Confirm and acknowledge eradication steps are working as expected and number of infected host(s) is dropping."), 'Validate Restored Hosts' (description: "Validate that each re-imaged system was completed by verifying new image creation date"), and 'Implement Recovery Monitoring' (description: "Add a note on how you are going to monitor newly recovered systems for additional monitoring for any anomalies or ...").

## Prebuilt Guided Response

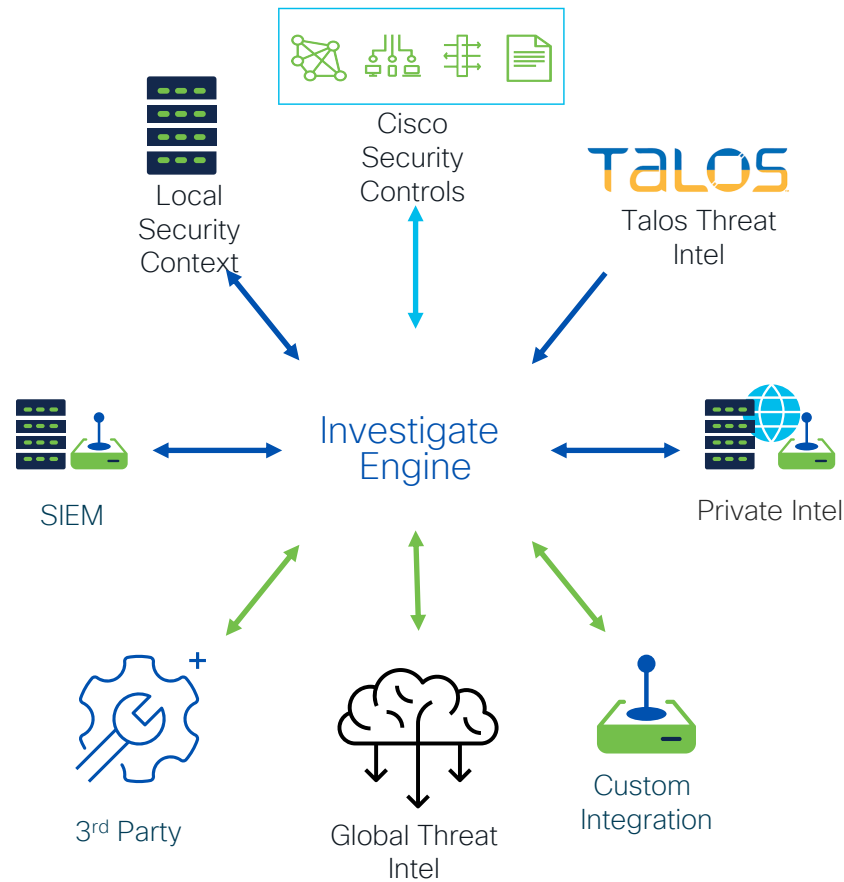
Go through a step-by-step guided response action for an incident using the provided flow of actions to achieve a faster and well documented response.

# Integrations (Data Ingestion and API Enrichment)

# Data Ingestion



# API Enrichment



# Integrations for partner technologies

The screenshot displays the Cisco XDR interface with a grid of integration cards. Each card includes a logo, the product name, and a brief description of the integration's capabilities. The cards are arranged in a 4x5 grid. A green arrow points from the top right of the grid towards a graphic of interlocking gears on the right side of the slide.

Integration	Description
APIVod	Threat Analysis APIs for Threat Detection & Prevention
AbusePDB IP Checker	Check IP addresses against AbusePDB's abusive IP database.
Akamai	Security Center provides answers to essential questions in the most intuitive and simple way
AlienVault Open Threat Exchange	The AlienVault Open Threat Exchange (OTX) is the world's most authoritative open threat information sharing and analysis network.
Amazon GuardDuty	Amazon GuardDuty - Intelligent threat protection for accounts and workloads.
Bastille Networks	RF monitoring for wireless intrusion detection and policy enforcement.
Censys	Censys is a platform that helps information security practitioners discover, monitor, and analyze devices that are accessible from the Internet.
CrowdStrike	CrowdStrike is a global cybersecurity leader with an advanced cloud-native platform for protecting endpoints, cloud workloads, identities and data.
CrowdStrike	CrowdStrike is a global cybersecurity leader with an advanced cloud-native platform for protecting endpoints, cloud workloads, identities and data.
CrowdStrike CSTA	CrowdStrike is a global cybersecurity leader with an advanced cloud-native platform for protecting endpoints, cloud workloads, identities and data.
CyberCime Tracker	Featuring FIFTY message echos covering ALL computer systems: Art, Wizard, Hacking, Phishing, Technology, BBS Support, Demos, Coding, Sound...
Devo	Devo is cloud-native logging and security analytics.
Exabeam	Exabeam Fusion combines XDR and SIEM into a single, cloud-delivered platform that enables you to leverage integrated threat detection, investigation...
Farsight Security DNSDB®	Farsight Security DNSDB® is the world's largest DNS intelligence database that provides a unique, fact-based, multifaceted view of the configuration of the...
Generic Serverless Relay	Generic Serverless Relay module that can be used when developing new integrations
Google Chronicle	Chronicle is a cloud service, built as a specialized layer on top of core Google infrastructure, designed so that enterprises can privately retain, analyze and...
Google Safe Browsing	Safe Browsing is a Google service that lets client applications check URLs against Google's constantly updated lists of unsafe web resources. Examples of...
Graylog	Graylog is a leading centralized log management solution built to open standards for capturing, storing, and enabling real-time analysis of terabytes of...
Have I Been Pwned	Have I Been Pwned allows you to search across multiple data breaches to see if your email address has been compromised.
IBM X-Force Exchange	IBM X-Force Exchange is a threat intelligence sharing platform enabling research on security threats, aggregation of intelligence, and collaboration with...
IstPhishing	The IstPhishing Threat Detection Rest API allows to check in real time and in a fully automated process whether an URL is a phishing or a spam website.
Ivanti Neurons	Ivanti Neurons (Formerly MobileIron) is an Enterprise Mobility Manager (EMM), also known as a Mobile Device Manager (MDM) or a Unified Endpoint...
Janit Pro	Janit Pro is a leader for management of Apple macOS, iOS, and tvOS device management.
LogRhythm	LogRhythm empowering users to successfully reduce risk by rapidly detecting, responding to and neutralizing damaging cyberthreats.
MISP	MISP - Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing.



# XDR Integrations API enrichment

\*Community/open source

Relay server translates from 3<sup>rd</sup> party data model and APIs to Cisco Threat Intelligence Model and XDR APIs

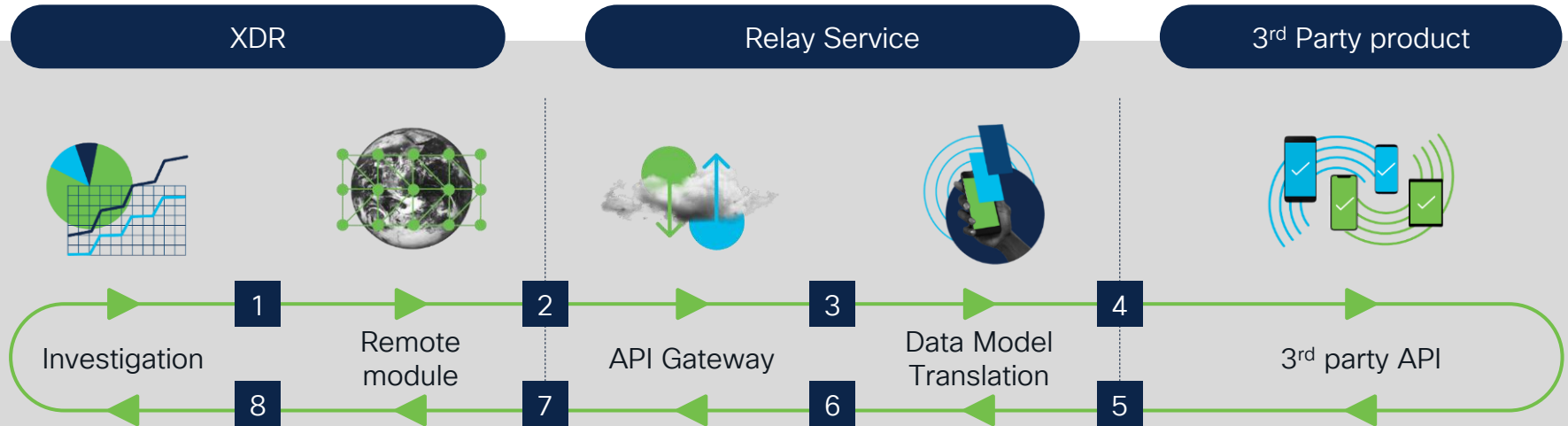
- Many available by default (examples below)
- [Write your own!](#)
- Templates and examples available on Github

Abuse IPDB*	Pulsedive*
APIVoid*	SecurityTrails
CyberCrime Tracker*	See One Feed App*
Cyberprotect Threatscore*	SpyCloud
Farsight Security	urlscan.io*
Google Chronicle	Gigamon
Google Safe Browsing	ThreatINSIGHT
Google VirusTotal*	Qualys IOC
Have I Been Pwned*	Radware WAF and DDoS
Microsoft Graph Security	Signal Sciences
	AlienVault OTX*

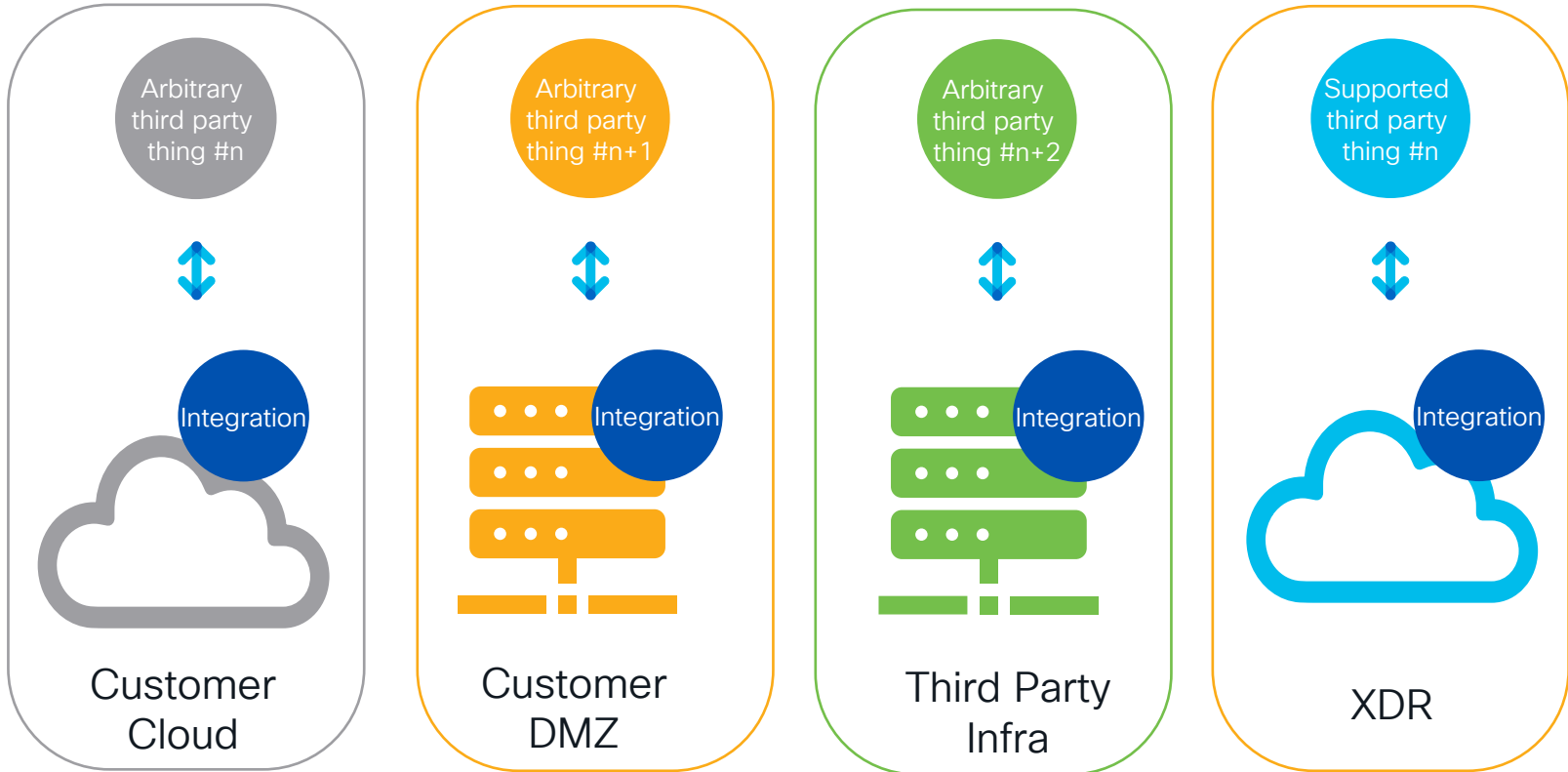
# Relay API

Template and documentation - <http://cs.co/api-template>

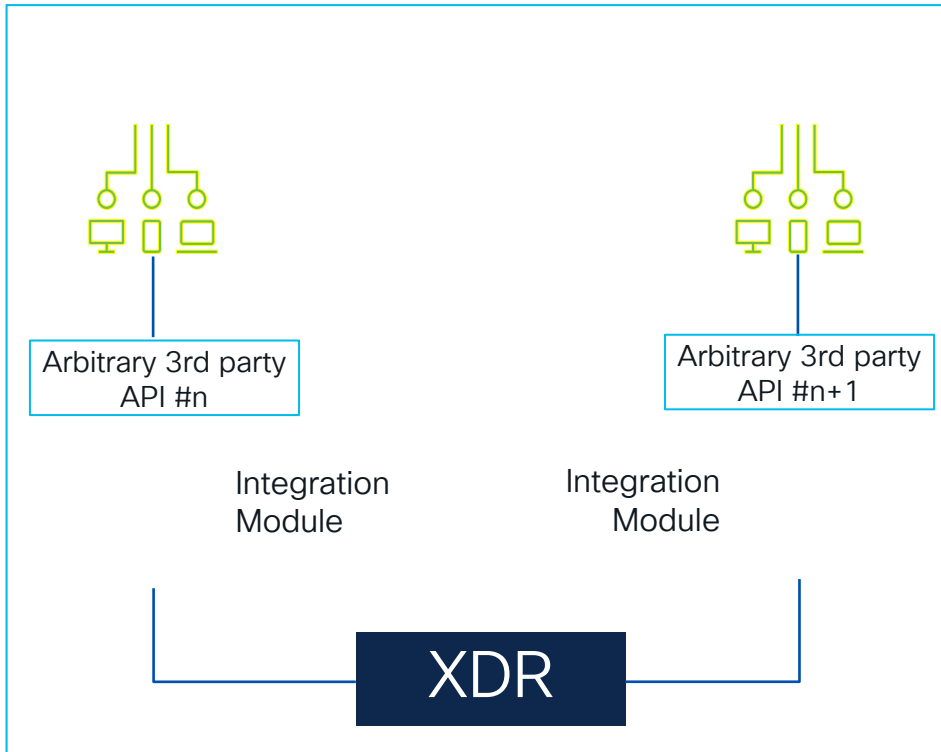
Bundle builder - <http://cs.co/bundle-builder>



# Where do the relay servers live?



# Integration Supported APIs



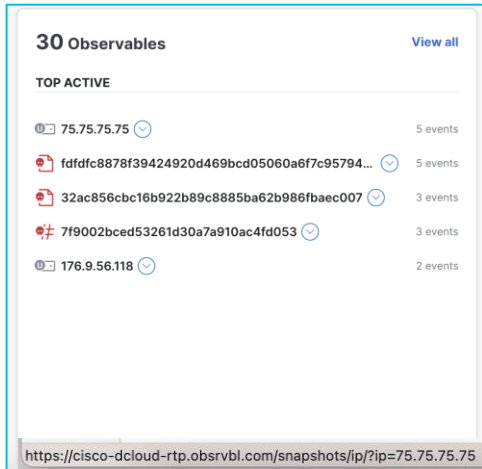
```
"supported-apis": [  
  "health",  
  "refer/observables",  
  "observe/observables",  
  "deliberate/observables",  
  "observe/targets",  
  "respond/trigger",  
  "respond/observables",  
  "tiles",  
  "tiles/tile",  
  "tiles/tile-data"  
]
```

# Integration Supported APIs

## refer/observables

Dynamically creates URL to offer deep link pivot in drop down menu

```
@enrich_api.route('/refer/observables',  
methods=['POST'])  
def refer_observables():  
    token = get_jwt()  
    observable = get_observables()  
    json_refer = do_something_cool(url)  
    return jsonify_data(json_refer)
```

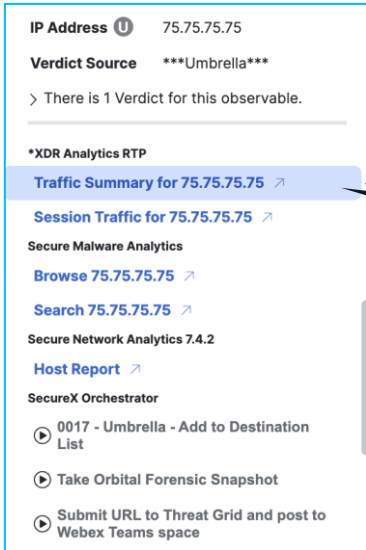


30 Observables [View all](#)

TOP ACTIVE

- 75.75.75.75 5 events
- fdfdcf8878f39424920d469bcd05060a6f7c95794... 5 events
- 32ac856cbc16b922b89c8885ba62b986fbaec007 3 events
- 7f9002bcd53261d30a7a910ac4fd053 3 events
- 176.9.56.118 2 events

<https://cisco-dcloud-rtp.obsrvbl.com/snapshots/ip/?ip=75.75.75.75>



IP Address ⓘ 75.75.75.75

Verdict Source \*\*\*Umbrella\*\*\*

> There is 1 Verdict for this observable.

\*XDR Analytics RTP

- [Traffic Summary for 75.75.75.75](#)
- [Session Traffic for 75.75.75.75](#)
- [Browse 75.75.75.75](#)
- [Search 75.75.75.75](#)

Secure Malware Analytics

Secure Network Analytics 7.4.2

Host Report

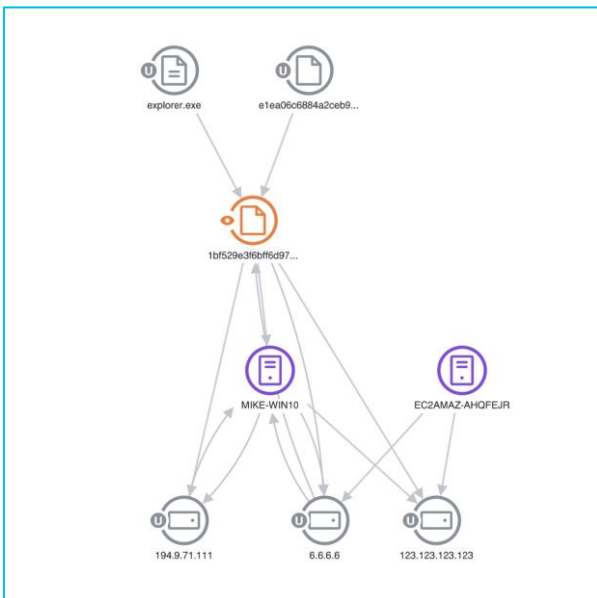
SecureX Orchestrator

- 0017 - Umbrella - Add to Destination List
- Take Orbital Forensic Snapshot
- Submit URL to Threat Grid and post to Webex Teams space

View the traffic summary for 75.75.75.75

Dynamic URL

# Integration Supported APIs



### Meraki Event: File Scanned

First Seen: 2023-04-12T10:44:29.837Z

**High**

**Reported by**

Module: Meraki Security Events Module  
Source: Meraki MX Module

**Short description**

**Long description**

File Type	File Size (Bytes)	URI
MS_EXE	193688	http://www.favorite-icons

**Relations** 4

- 192.168.201.91 Connected to
- 6.6.6.6
- 1bf529e3f6bff6d974443... Downloaded by
- 192.168.201.91
- 6.6.6.6 Downloaded from
- 1bf529e3f6bff6d97444319f48c4059ed...
- MidYearBonus.exe Filename of
- 1bf529e3f6bff6d97444319f48c4059ed...

**Indicators** 0

## observe/observables

Queries end technology for information regarding about a particular observable. The response is a Cisco Threat Intelligence Model (CTIM) entity such as a sighting

```
@enrich_api.route('/observe/observables', methods=['POST'])
def observe_observables():
    # Get JWT credentials and observables
    g.sightings = []
    # Iterate through observables and query sightings for each observable
    for observable in observables:
        response = query_sightings(observable['value'], credentials)
        # Convert each event in the response to CTIM
        for event in response:
            this_sighting = mapping.sighting(observable, event)
            g.sightings.append(this_sighting[0])
    # Return the JSON response
    return jsonify_result()
```

# Integration Supported APIs

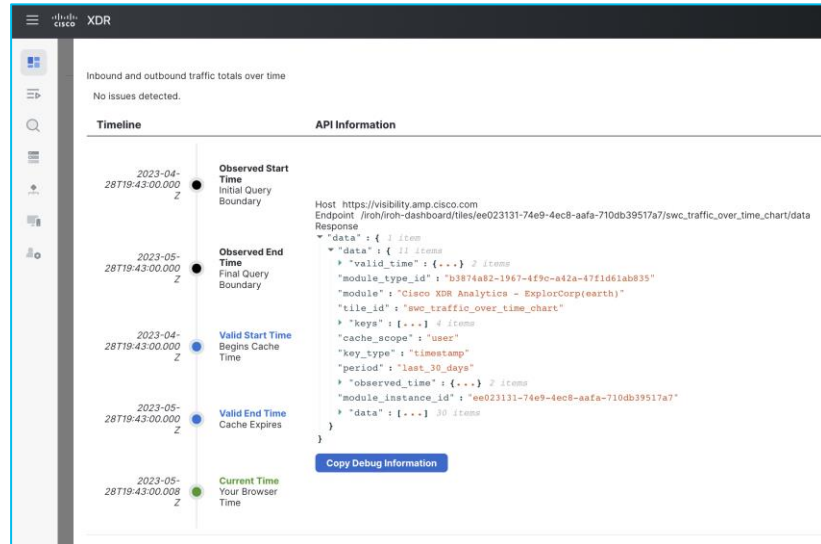
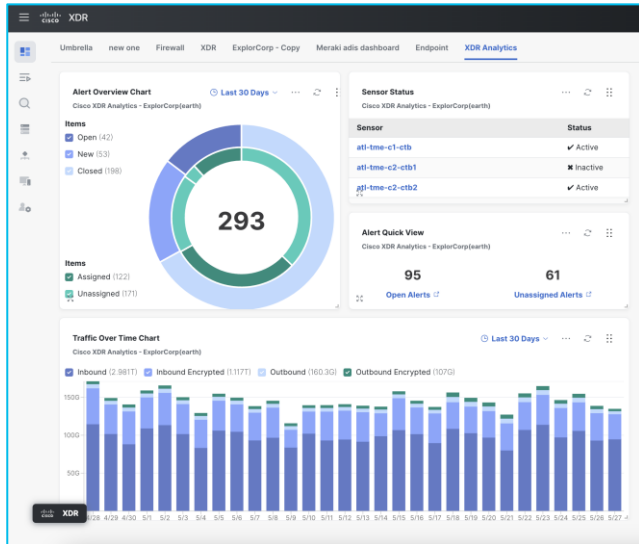
## tiles/tile-data

Queries end technology for high-level metrics and stats to be surfaced in a control center tile. The response is sent back with the data formatted to match what the tile template is expecting

```
@dashboard_api.route('/tiles', methods=['POST'])
def tiles():
    _ = get_jwt()
    return jsonify_data([])

@dashboard_api.route('/tiles/tile', methods=['POST'])
def tile():
    _ = get_jwt()
    _ = get_json(DashboardTileSchema())
    return jsonify_data({})

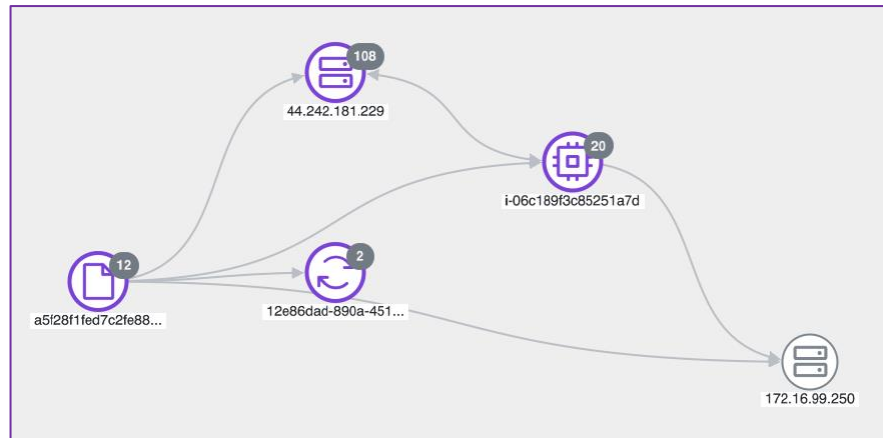
@dashboard_api.route('/tiles/tile-data', methods=['POST'])
def tile_data():
    _ = get_jwt()
    _ = get_json(DashboardTileDataSchema())
    return jsonify_data({})
```



# Investigate

# Reduce investigation time

- Interactive, visual representations of incidents
- Event correlation and incident chaining to group related intelligence
- Automated enrichment for the most critical incidents, ensuring intelligence is gathered immediately



Distinct Alert Types / MITRE Tactic		2023
		May
Internal Port Scanner #11916	Discovery	Created: 2023-05-11 11:19 EDT
Potential Data Exfiltration #11917	Exfiltration	Created: 2023-05-16 08:31 EDT
Outbound SMB Connection Spike #11920	Reconnaissance	Created: 2023-05-17 16:50 EDT
DNS Abuse #11918	Exfiltration	Created: 2023-05-17 17:02 EDT
New Unusual DNS Resolver #11919	Command And Control	Created: 2023-05-18 12:48 EDT
Outbound Traffic Spike #11921	Exfiltration	Created: 2023-05-19 17:37 EDT
Country Set Deviation #11922	Initial Access	Created: 2023-05-22 09:55 EDT
Malicious Process Detected #11924	Execution	Created: 2023-05-22 17:55 EDT
Suspicious Process Path #11925	Defense Evasion	Created: 2023-05-22 18:01 EDT
LDAP Connection from Suspicious Process #11926	Credential Access	Created: 2023-05-22 18:32 EDT
Suspected Malicious URL #11923	Initial Access	Created: 2023-05-23 12:34 EDT
Suspected Cryptocurrency Activity #11927	Impact	Created: 2023-05-24 23:25 EDT

# Investigate with intelligence, context and response

## Global Intelligence



Endpoint security  
Malware intelligence  
Internet intelligence



VirusTotal and  
other third parties

Are these observables  
suspicious or malicious?

**Observables:** 1 ) File hash, 2) IP address, 3) Domain, 4) URL, 5) Email addresses, etc..

## Local security context



Endpoint security



Email security



Analytics

Have we seen these observables? Where?  
Which endpoints connected to the domain/URL?



Cloud security



Network firewall



Secure Web  
Appliance

## Response actions

Block destinations

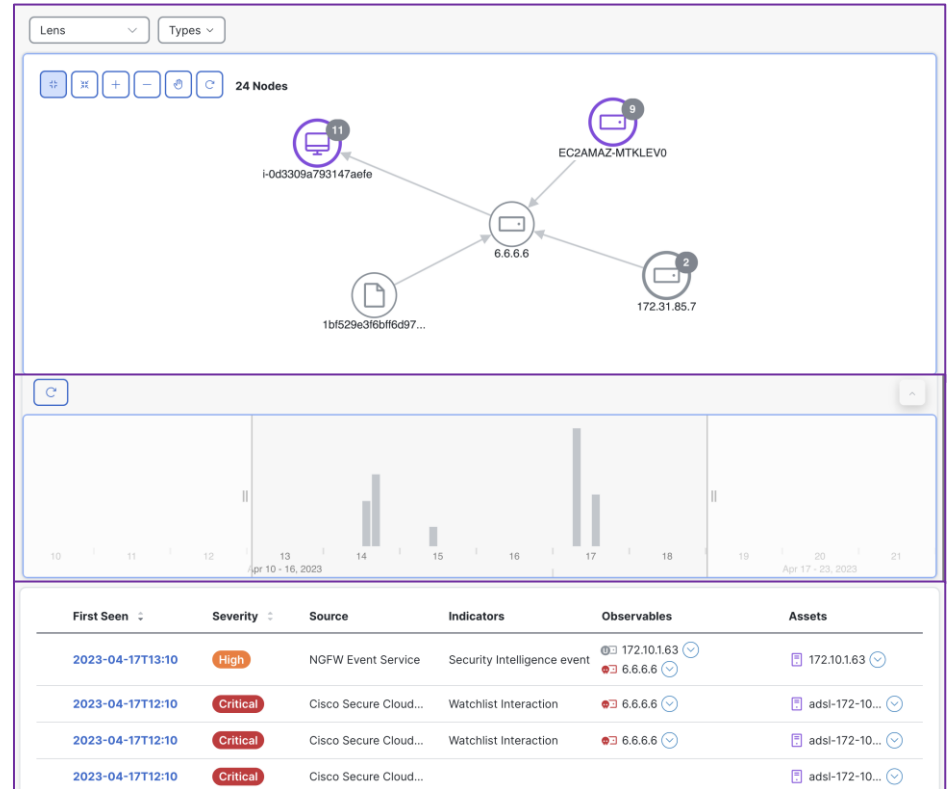
Block files

Isolate hosts

What can I do about  
it right now?

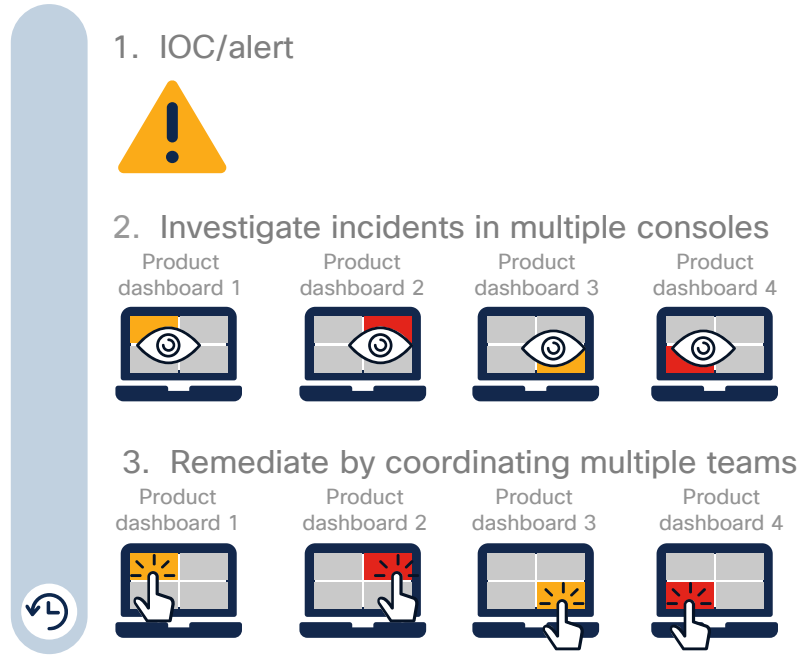
# Accelerate investigation With Cisco XDR

- Aggregate and query global intel and local context in one view
- Visualize the impact of threats across your environment
- Understand the chronological order of sightings via the timeline
- Take immediate response actions such as isolating a host or blocking an attacker

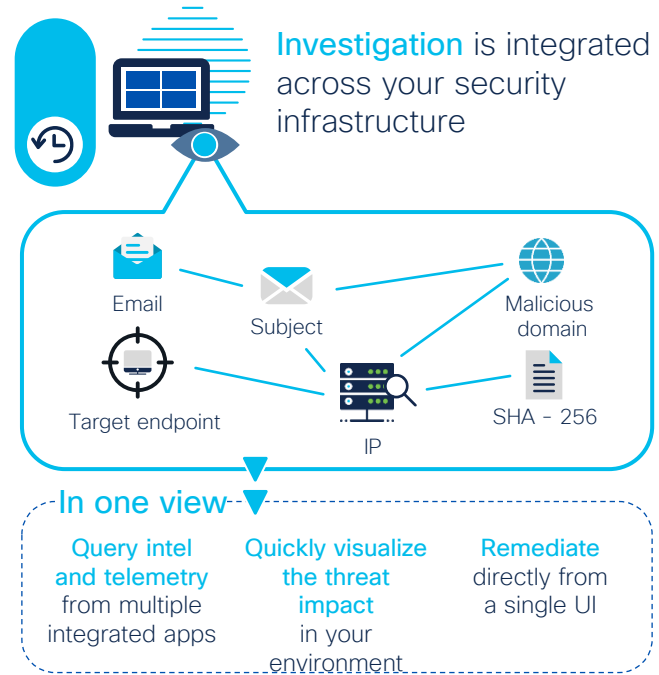


# How true simplicity is experienced

Without XDR: ~32 minutes

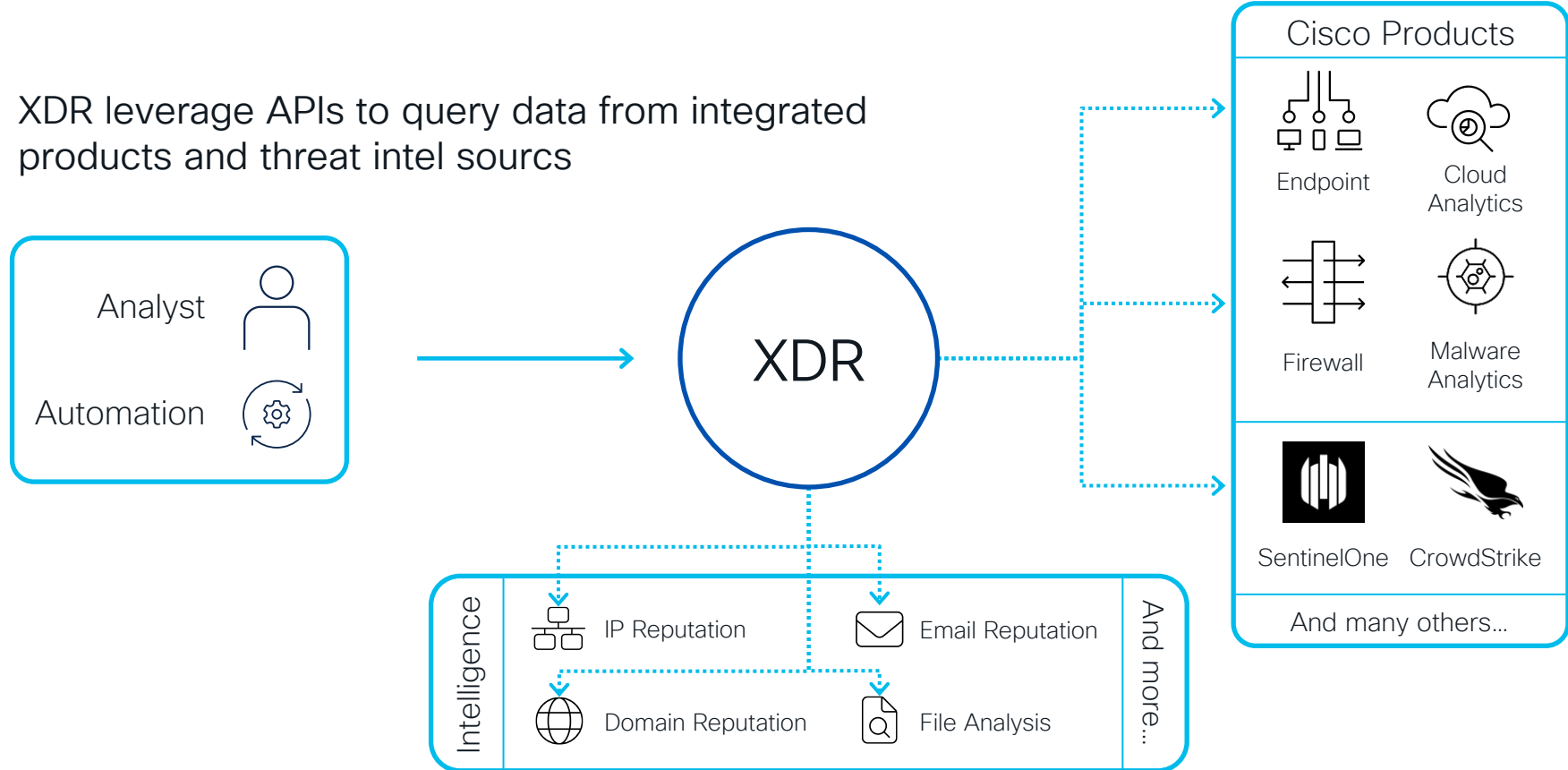


With XDR: five minutes



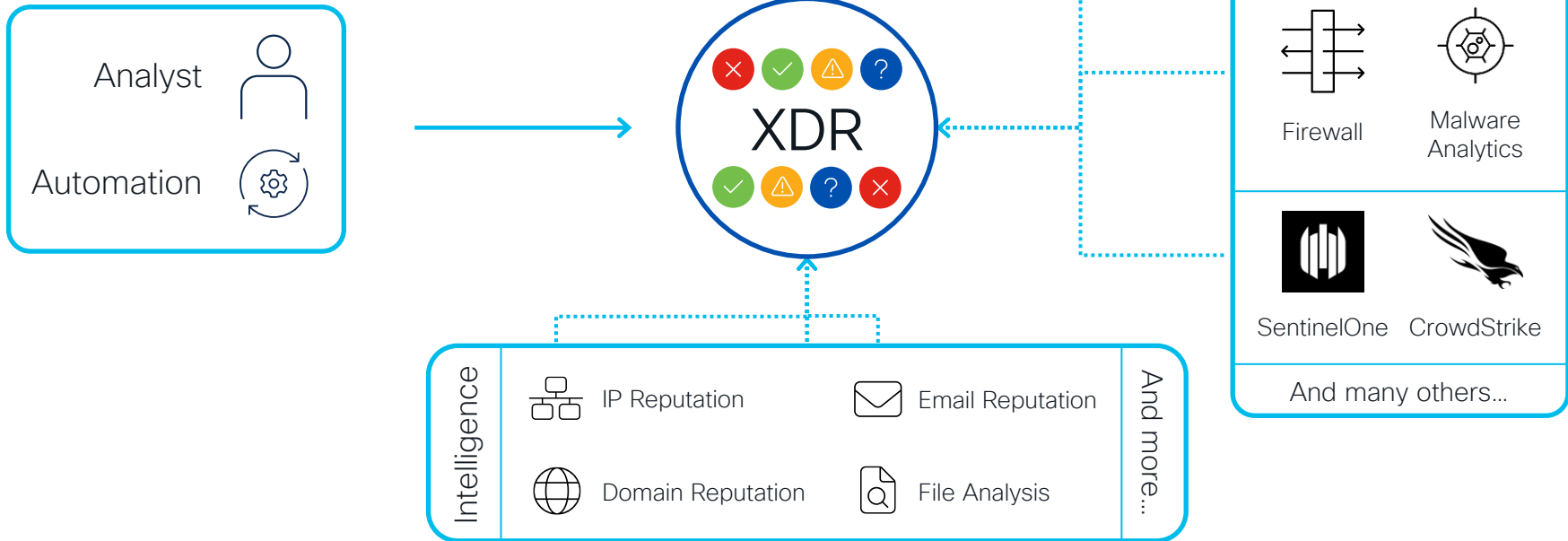
# Investigation query integration and threat intel

XDR leverage APIs to query data from integrated products and threat intel sources



# Correlate and merge information

Correlate dispositions from multiple sources and merge it in a single view



# XDR Investigate API's

The screenshot shows the 'INSPECT' API configuration page. At the top, it displays the method 'POST' and the path '/iroh/iroh-inspect/inspect'. A description reads 'return extracted observables from some raw text'. Below this, the 'required scopes' are listed as 'inspect:read'. A 'Parameters' section contains a 'Try it out' button. The main configuration area is a table with columns 'Name' and 'Description'. A parameter named 'StrContent' is marked as 'required' and has a description 'object (body)'. An 'Example Value' field shows a JSON object: { "content": "string" }. Below the example, a dropdown menu for 'Parameter content type' is set to 'application/json'.

Cisco XDR uses the inspect API to extract observables (IP's, Domains, sha256, etc.) from raw text. This eliminates the need to reformat defanged observables before submission. This API returns an array of observables with their type and value.

```
{  
  "content":  
    "some_string_containing_6.6.6.6_observables"  
}
```

# XDR Investigate API's

**Deliberate** This set of routes allow to quickly get answers from your integrations You might use them at the start of any investigation to quickly get answers from your modules if something is bad. ^

**POST** /iroh/iroh-enrich/deliberate/observables Get Observable verdicts

**Health** This set of routes allow to check the health of your integrations setup Verify if your modules are setup correctly and if your credentials are correct. ^

**POST** /iroh/iroh-enrich/health Health check all the modules

**POST** /iroh/iroh-enrich/health/{module\_instance\_id} Health check one module

**Observe** This set of routes allow to get in depth investigation data about a threat You might use them at the start of any investigation to get the full picture and get to know if something has been seen in your environment.

**POST** /iroh/iroh-enrich/observe/observables Enrich Observables

**POST** /iroh/iroh-enrich/observe/targets Enrich Targets

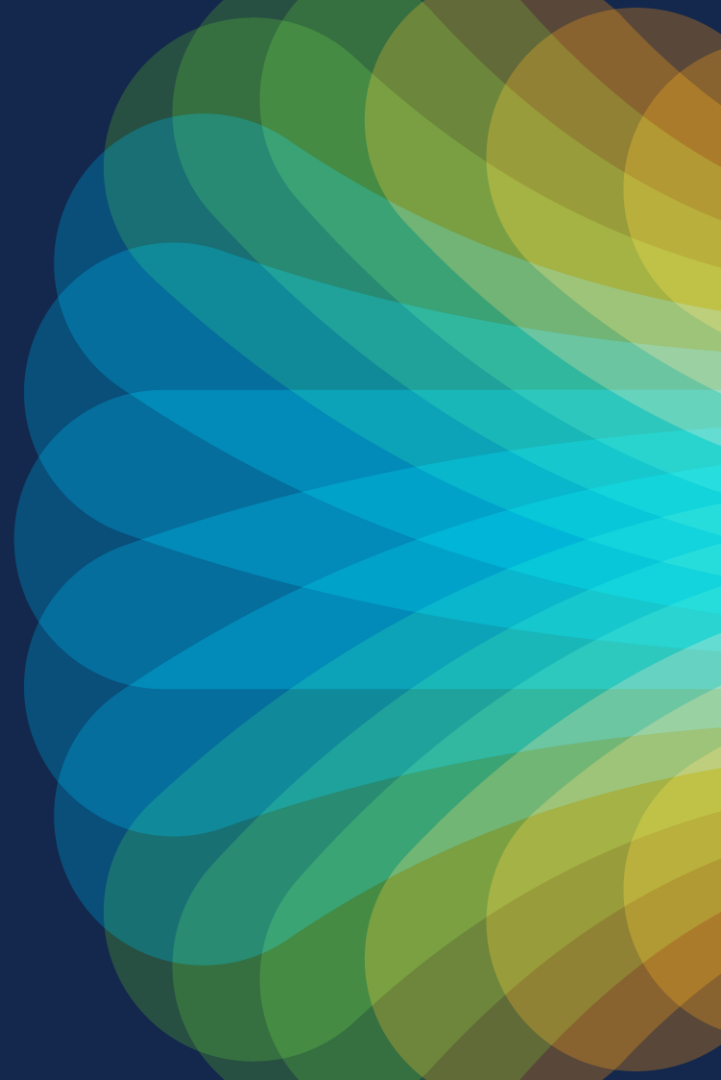
**Refer** This set of routes allow to get relevant Reference links and quickly pivot pursuing your investigation on a specific product interface. ^

**POST** /iroh/iroh-enrich/refer/observables

```
[
  {
    "type": "domain",
    "value": "ilo.brenz.pl"
  },
  {
    "type": "email",
    "value": "no-reply@internetbadguys.com"
  },
  {
    "type": "sha256",
    "value": "8fda14f91e..."
  }
]
```

Cisco XDR uses the enrich API to query all enabled modules supporting the enrichment protocol with the supplied Observables in order to get any related Threat Context

# Automate/Response



# Introducing XDR Automate

Process **automation**  
**made simple** with a  
no/low-code drag-  
drop interface



## Investigate

Reduce research and response times with workflows and playbooks that execute at machine speed



## Automate

Eliminate repetitive tasks and reduce MTTR to increase productivity and focus on mission-critical projects



## Integrate

Unique turnkey approach to quickly integrate with other systems and solutions to expand your toolbox

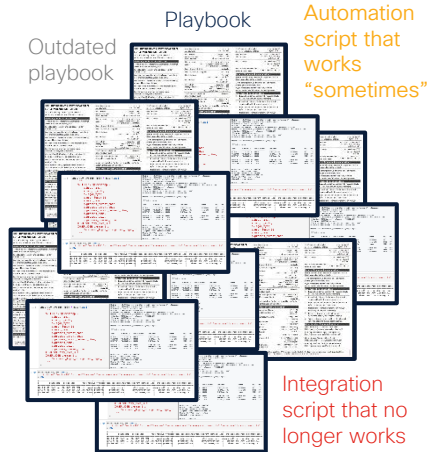


## Scale

Automation that scales infinitely and never takes a day off, delivering the same SLA around the clock

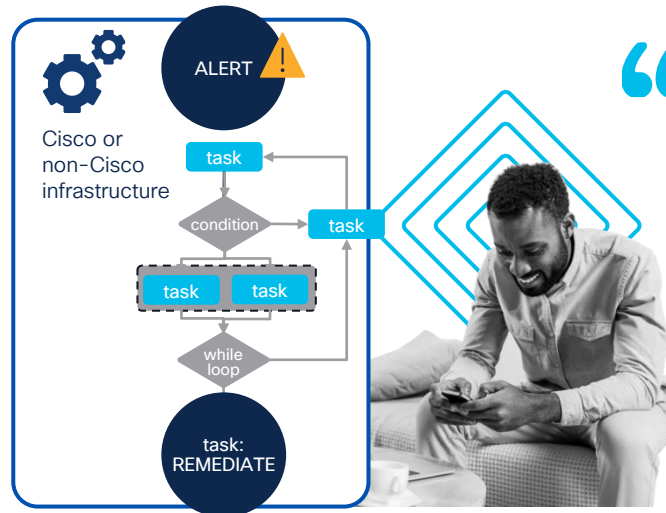
# Maximizing operational efficiency

Before: Repetitive, human-powered tasks



Solution: Orchestrating security across the full lifecycle

Pre-built or customizable workflows



After: I combined 9 tasks across 3 security tools, 2 infrastructure systems, and 3 teams in one keystroke!

“

I make automated playbook changes in minutes with a drag-drop interface

We have never communicated faster: Our approvals are automated

My top 5 most frustrating tasks have all be automated

# XDR Automate



A screenshot of the DNA Center Webex Teams Demo Run interface, showing a successful execution of a workflow. The title is "DNA Center Webex Teams Demo Run" with a status of "SUCCESS" and "Version 1.0.0". The workflow consists of several activities:

- CORE ACTIVITIES:** Includes a search bar and a warning icon.
- WEB SERVICE:** "DNAC - Get Network Device".
- TABLE ACTIVITIES:** "Read Network Device Call Into Table".
- WEB SERVICE:** "Webex Teams - Room Created".
- TABLE ACTIVITIES:** "Read Rooms Response".
- LOOP OVER ROOMS RESPONSE:** A loop structure with a "2 of 100" indicator. Inside the loop, there is a decision "IS ROOM FOUND?". If "YES", it executes three CORE ACTIVITIES: "Update Room Found Var", "Set Room Id", and "Room Found Variable Set".

# Core concepts

## Workflows

Simple or complex chain of actions that accomplish a specific outcome.

## Atomic actions

Small, reusable workflows like functions in traditional programming.

## Runs

Previous executions of workflows and atomics. Can be used to see what a workflow did and troubleshoot issues.

## Targets

Resources that workflows can communicate with, such as HTTP APIs, email servers, or infrastructure

## Account Keys

Credentials used when communicating with targets. Come in a various types to match the various target types.

## Variables (Global)

Used to store data between workflow executions or to share data between different workflows. Come in various types for different types of data.

# Core concepts

## Triggers

Different ways workflows can be triggered to execute including schedules, automation rules, webhooks, and more.

## Tasks

Built-in mechanism for workflows to ask for input. Typically used for approvals, but the response actions are customizable.

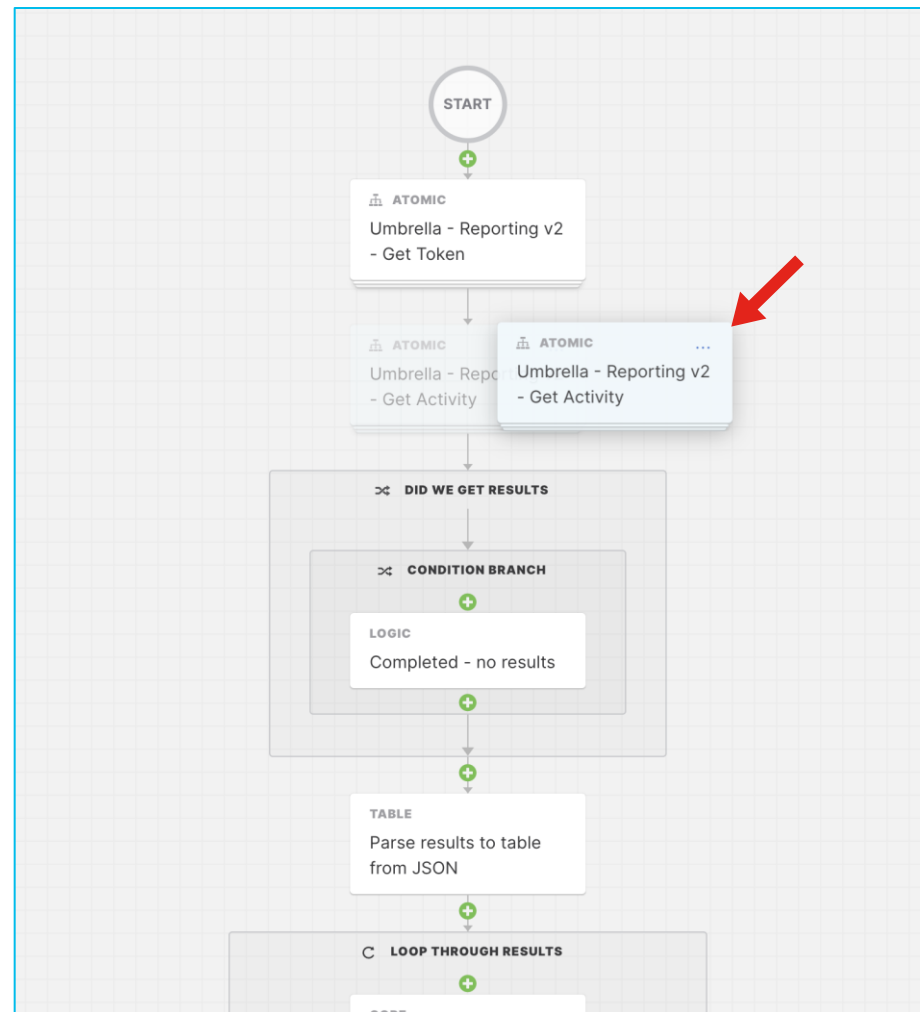
## Remotes

Can be deployed on-premises behind a firewall to enable integration with on-premises resources.

# What is a workflow?

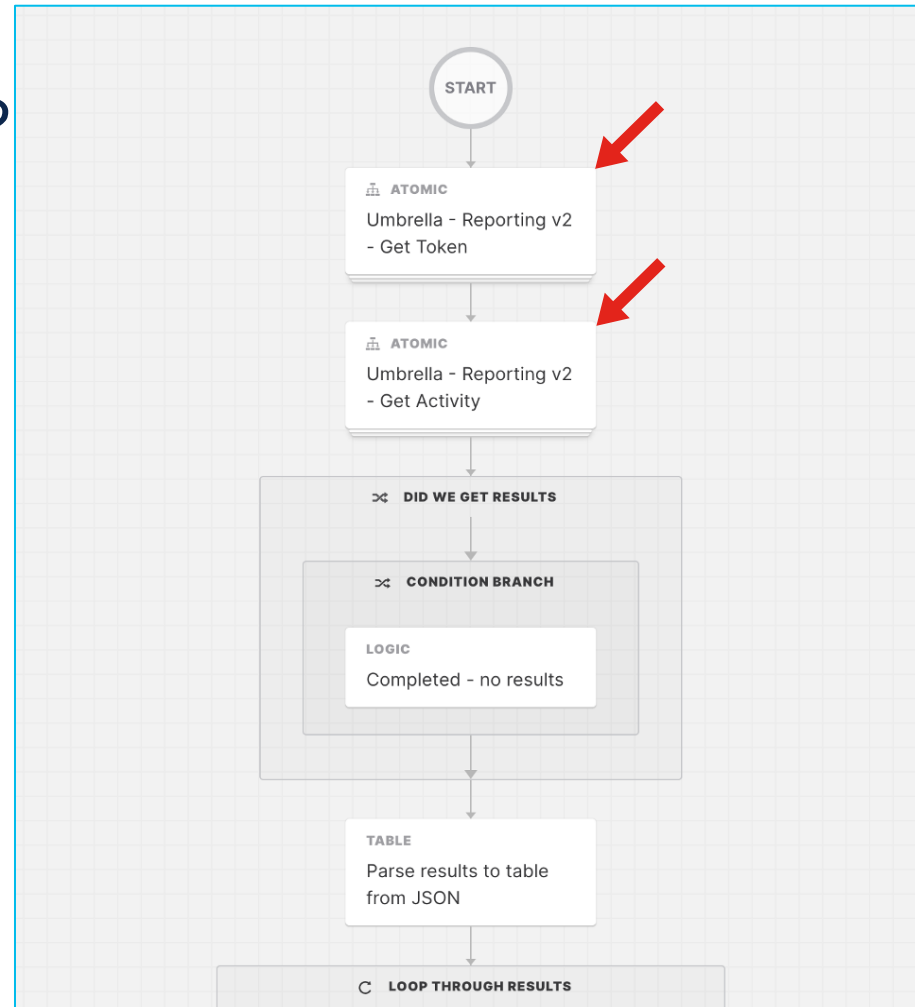
Simple or complex series of actions that accomplish a specific outcome.

- Performing automated investigations
- Responding to an incident
- Automating routine tasks to save SOC time
- And more... workflows aren't limited to security use cases



# What is an atomic action?

- Atomics are small, re-usable activities like a function in traditional programming.
- Think of a workflow as a script and an atomic as a function within the script.
- Built using the same workflow editor but appear in the activity toolbox when building a workflow.
- Good for repetitive tasks like sending a Webex message or isolating an endpoint in an EDR.



# Powerful, flexible automation



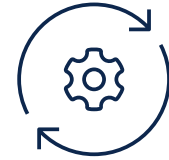
## Response

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



## Automation rules

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



## And more...

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

# Accelerate response

- Ability to respond throughout the interface
- Simplified response workflows available from within incidents
- Broad set of workflows to achieve a variety of outcomes
- Four stages to resolution:



Identify



Contain



Eradicate



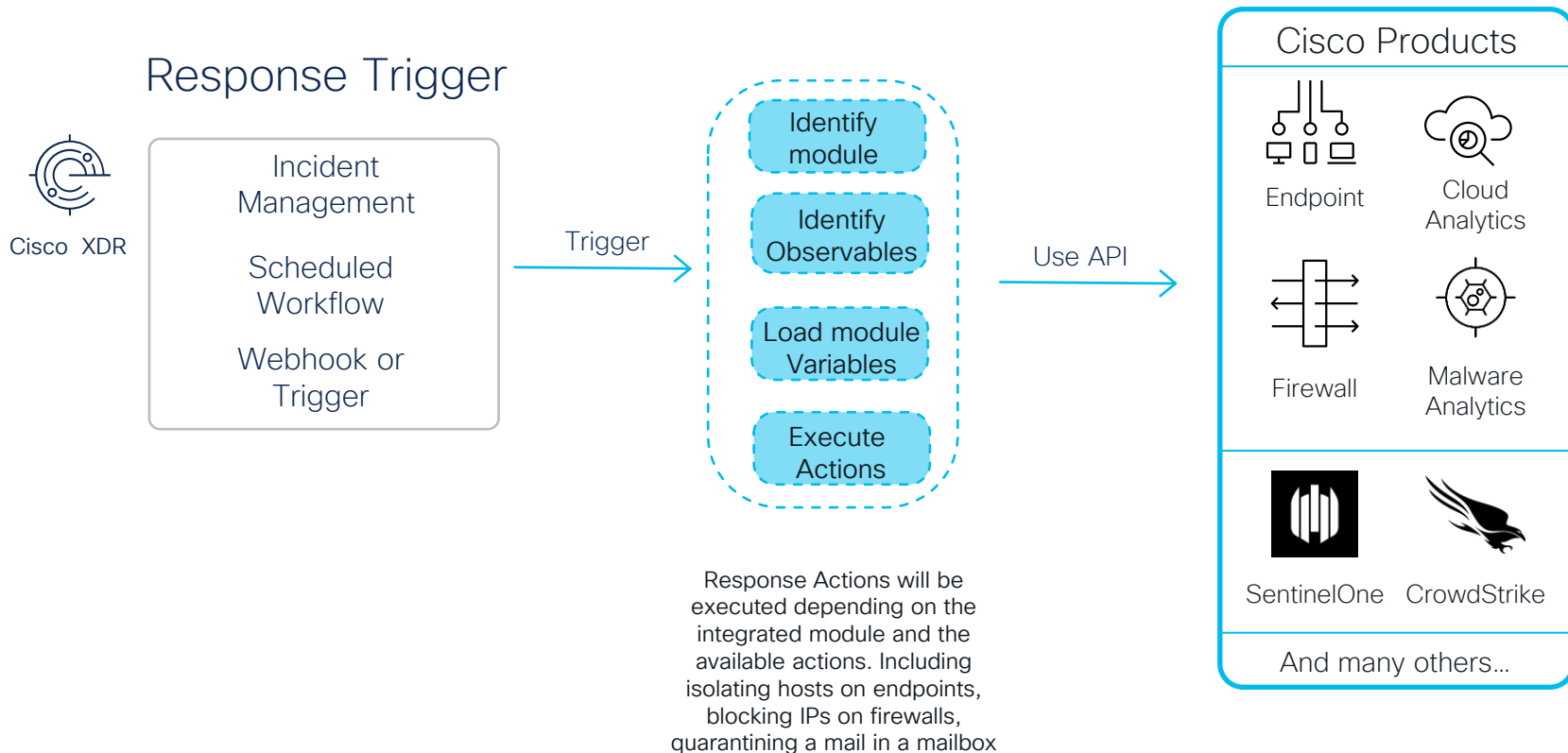
Recover

The screenshot displays a security response interface with a sidebar on the left and a main content area on the right. The sidebar lists four stages: Identification, Containment, Eradication, and Recovery. The main content area shows a workflow for incident resolution, with the following steps:

- Identify Affected Hosts** (Add Note): Add note with summary of findings on the investigations of hosts found with malicious indicators.
- Contain Incident: Overview** (Add Note): Overview of how to contain Indicators of Compromise to stop the spread of malicious activity.
- Contain Incident: Assets** (Select): Use asset-based containment to stop the spread of malicious activity. This automation workflow will network isolate/quarantine all selected assets on your integrated Endpoint Detection & Response solutions. After clicking Execute, you will be able to choose all or a subset of assets associated with this incident. Please make sure you have done proper identification before executing the workflow.
- Contain Incident: IPs** (Add Note): Contain IP indicators of compromise to stop the spread of malicious activity.
- Contain Incident: Domains** (Select): Contain domain indicators of compromise to stop the spread of malicious activity.
- Contain Incident: URLs** (Select): Contain URL indicators of compromise to stop the spread of malicious activity.

At the bottom right, there are two buttons: "Back" and "Go to Eradication →".

# Response



# Pivot menu

Accessed by clicking the icon next to an observable:

- During investigations
- In the incident manager
- While using the XDR ribbon

Provides various actions including:

- Creating a judgement
- Adding an observable to a case
- Deep link pivot to other products for additional information
- Taking a response action via an integrated product
- Executing a response workflow in XDR Automation

The screenshot displays a security dashboard interface. On the left, a list of observables is shown under the heading "31 Observables". The first observable is "6.6.6.6" with a skull icon and a dropdown arrow. A pivot menu is open for this observable, showing the following information:

- IP Address** (skull icon): 6.6.6.6
- Verdict Source**: Talos Intelligence
- There are 2 Verdicts for this observable.
- [Search for this IP](#)
- [Browse IP](#)
- Talos Intelligence**
  - [Search for this IP](#)
- Umbrella - ExplorCorp**
  - [IP view for 6.6.6.6](#)
- XDR Automation**
  - [Move Computer to Triage Group](#)
  - [Submit URL to Secure Malware Analytics](#)
  - [Meraki - MX - L3 Outbound Firewall Block](#)
  - [Umbrella - Add to Destination List](#)
  - [ServiceNow - Request Firewall NullRoute](#)

The background shows a list of other observables: "1bf529e3f6...", "94.204.151.8...", "64.104.44.1...", and "3.136.210.16...".

# Automation rules

## Triggers

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

### Automation Rules

Events

Webhooks

Calendars

Schedules

Search

Q Search



Type

Select



Reset All

Display name

On/off

Description

Incident notifications to Webex



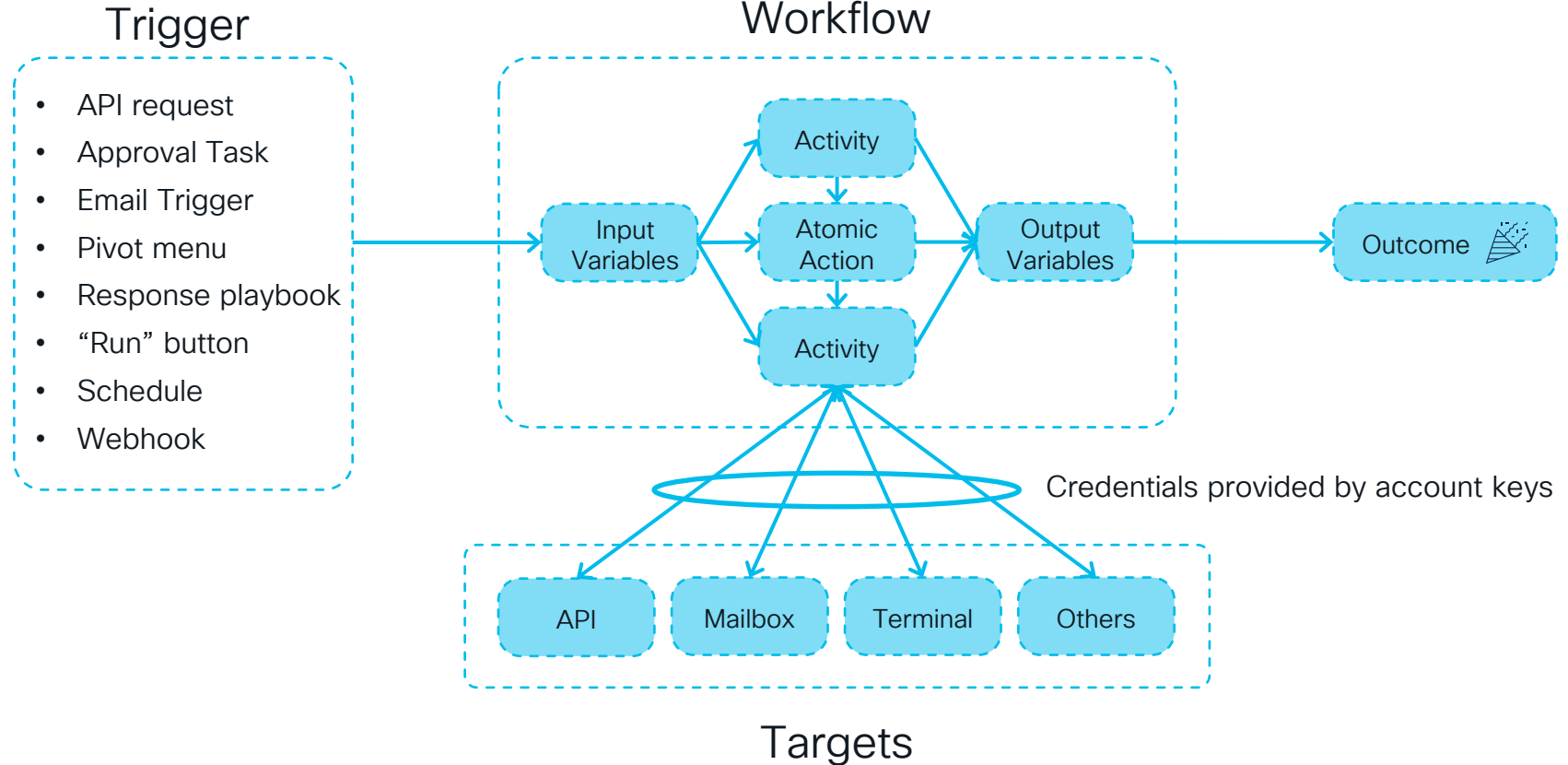
Check for Talos blog posts



Current automation rule types:

- 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 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 address

# Flow diagram

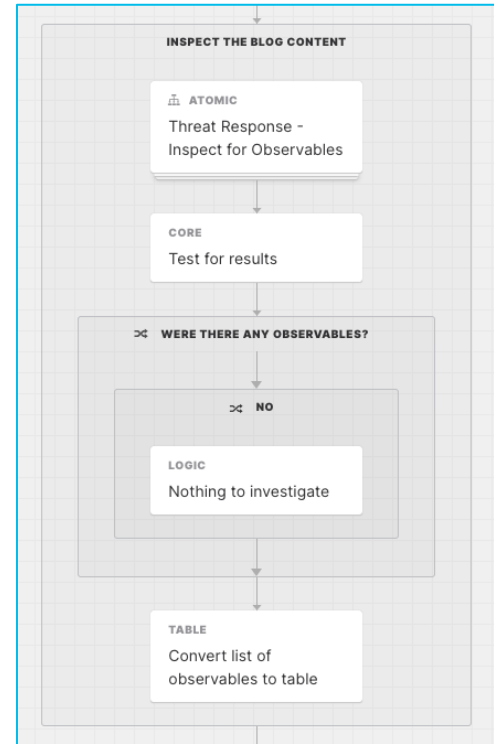


# Automation, with the click of a button

Leverage your existing integrations to automate investigation and response

- Collect and parse intelligence
- Conduct investigations based on various triggers
- Respond at machine speed
- 75+ pre-built workflows available to import

Build custom workflows or import pre-built use cases from Cisco



# Exchange

Workflow ecosystem designed for discovering and importing content

- Streamlined workflow installation process from within the orchestration console.
- Offers a searchable workflow index to find content easier
- Configuration wizard helps user configure the required targets/account keys upon installation

Benefits: Users can start automating with Orchestration in under 15 minutes – Getting value of XDR Orchestration is streamlined

The screenshot shows the Cisco Exchange workflow ecosystem interface. At the top, there's a header "Exchange" with a sub-header "Exchange allows you to find and install workflows that have been approved by Cisco engineers and content providers." Below this, there are search and category filters. The "Search" field contains "Search" and the "Category" dropdown is set to "All".

The "Popular" section features two workflow cards:

- Talos - Blog Post To SecureX Casebook**: Xchange. Description: "Takes a Talos blog post, conducts an investigation into it using Cisco Threat Response, and then puts the results in a SecureX casebook. I...". Buttons: "Learn More", "Installed".
- Threat Response Phishing Investigation**: Xchange. Description: "This workflow monitors a mailbox for incoming phishing reports. When an email is received, the workflow investigates its attachments and a...". Buttons: "Learn More", "Install".

The "All Workflows" section features two workflow cards:

- Azure AD - Get Blocked Sign-Ins (Locked...)**: Xchange. Description: "This workflow checks for sign-ins that were blocked because the account was locked out in Microsoft Azure (error code 50053). If any resul...". Buttons: "Learn More", "Install".
- Azure AD - Get New Users**: Xchange. Description: "This workflow checks for users that were created within the past X hours in Microsoft Azure (the timeframe is configurable). If any result...". Buttons: "Learn More", "Install".

At the bottom, there's a partial view of a workflow card:

- Duo - Investigate User**: Xchange.

# Workflows and atomics

- Shows all the organization's installed workflows and atomic actions
- Card view (default) or list view
- Tabs for workflows, atomics, recent workflows, and favorited workflows.
- Workflows can be favorited by clicking the star icon on their tile or list row
- Workflows can be searched

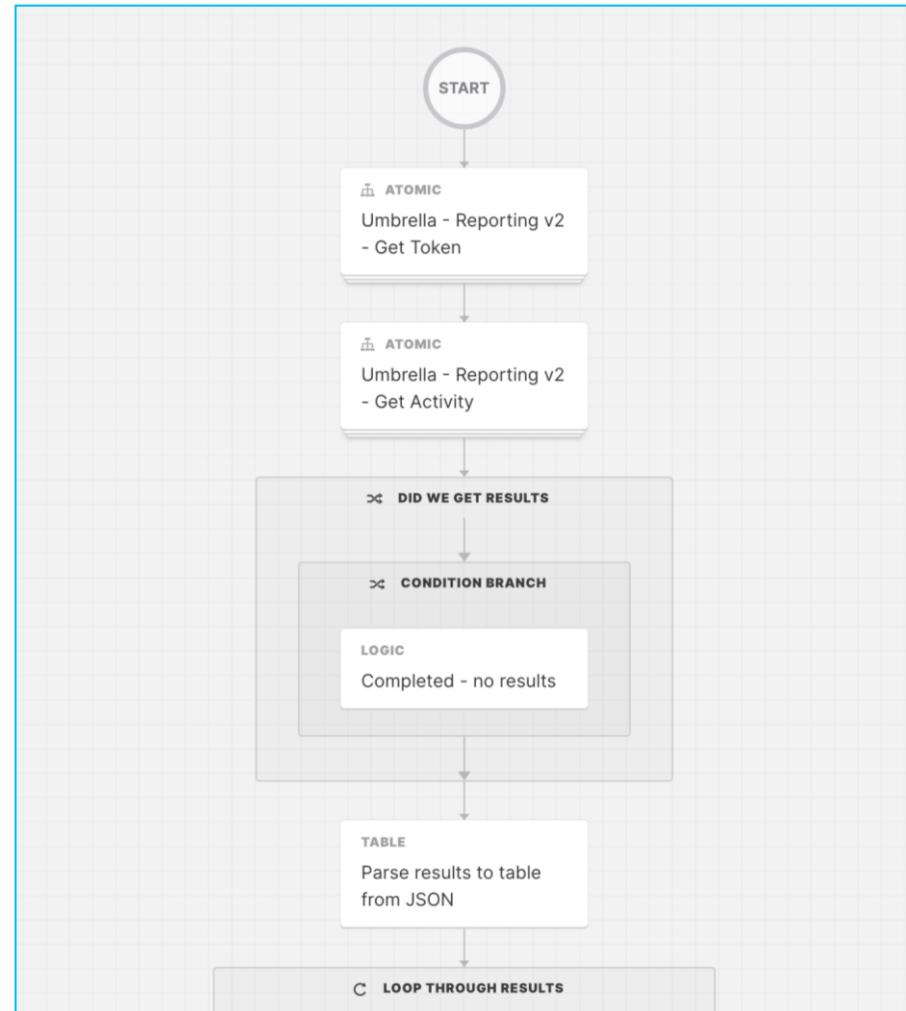
The screenshot displays the 'All Workflows' section of the Cisco XDR console. At the top, there are navigation tabs for 'All Workflows' (28), 'Atomics' (206), 'Recents', and 'Favorites' (0). Below the tabs, there are filters for 'Search', 'Ready State', and 'Category', along with a 'Reset All' button. The main area shows a grid of workflow cards. Each card includes a title, a brief description, a status indicator (e.g., 'Validated', 'Updated'), and a star icon for favoriting. The cards shown are: 'Umbrella - Search DNS Activity b...' (Validated), 'Secure Firewall - Incident Monit...' (Updated), 'Submit URL to Secure Malware Ana...' (Updated), and 'Talos - Get New Blog P...' (Validated).

The screenshot displays the 'All Workflows' section of the Cisco XDR console in list view. It features the same navigation tabs and filters as the card view. The workflow list is as follows:

Display name	Categories	Status	Owner
Umbrella - Search DNS Activity b... This workflow searches and returns Cisco...		Validated	user@cisco.com
Secure Firewall - Incident Monit... This workflow fetches Cisco Secure Firewall...		Updated	user@cisco.com
Check for Umbrella Security Even... This workflow searches and returns Cisco...		Validated	user@cisco.com
Submit URL to Secure Malware Ana... This workflow submits a URL to Cisco Secure...	response	Updated	user@cisco.com
Talos - Get New Blog Posts This workflow consumes the Talos Intelligence...		Validated	user@cisco.com
XDR - Contain Incident: Assets		Export completed	user@cisco.com

# Workflow editor

- “No-to-low code” drag and drop editor where you can build simple or complex workflows and atomic actions.
- Toolbox of pre-written activities for various functions and products.
- No coding skills required, but Python scripts are supported.
- Supports logic like traditional scripting such as conditionals and loops.
- Three primary sections: toolbox, canvas, and property editor.



# Devices



# Devices



## **Extensive visibility into your devices**

Combined inventory from both security and device management products



## **Provides asset context to investigations**

Differentiate between a generic target and an asset that belongs to you



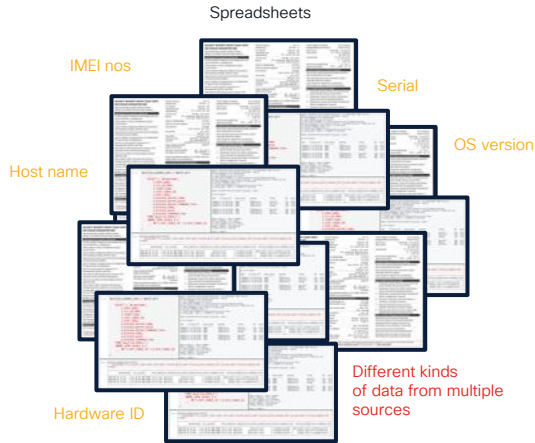
## **Configuration and management of Cisco Secure Client**

Cloud-based management of Secure Client profiles and deployments

# Gain contextual insights into your devices

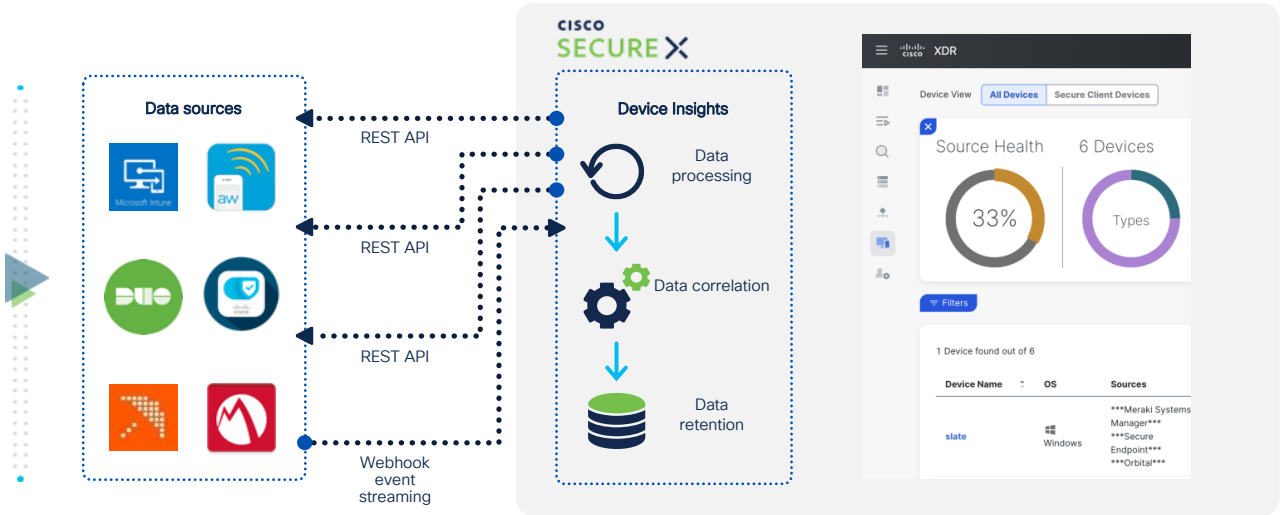
## Before:

Multiple spreadsheets, no combined view of the denominator



## Solution:

Comprehensive device inventory all in one place!



## After:

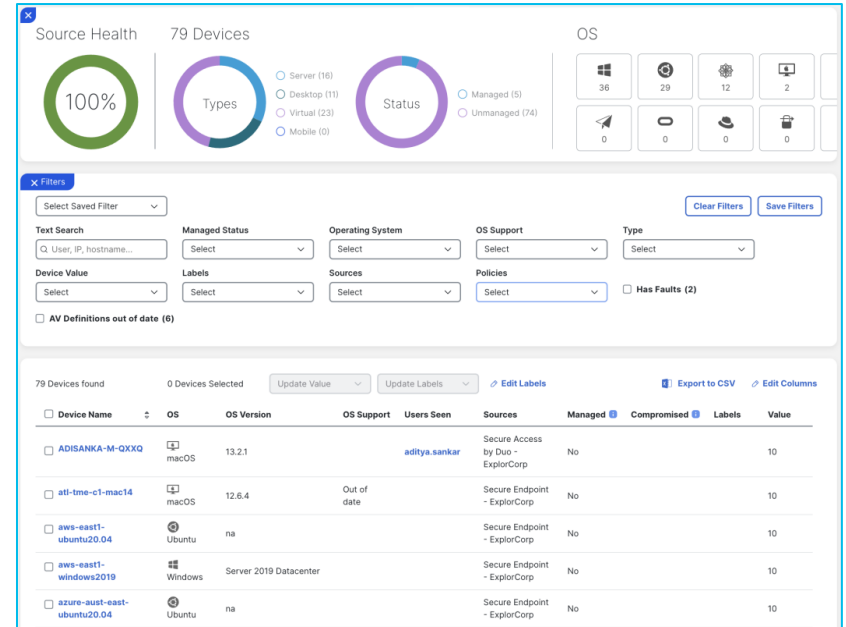
Gain unified visibility and contextual awareness to help you act on potential threats faster!

# What is Device Insights?

Device Insights is a feature in XDR that unifies multiple device managers, endpoint detection and response tools, AV and other endpoint security products and then brings the details those tools and solutions provide into a unified view within XDR.

With Device Insights, you'll be able to answer these all-important questions:

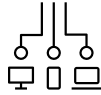
- What **types of devices** are connected to our network?
- What **users** have been accessing those devices?
- Where are those devices **located**?
- What **vulnerabilities** are associated with those devices?
- Which **security agents** are installed?
- Is our security software **up to date**?
- What **context** do we have from **technologies beyond the endpoint**?



# Supported sources



Duo Access  
Duo Beyond



Secure Endpoint



Umbrella (DNS)  
Windows / macOS



Meraki SM



Secure Client



Orbital

---

## Third Party



CrowdStrike



SentinelOne



Microsoft Intune



Jamf Pro



Ivanti Neurons  
(formerly MobileIron)



VMware  
Workspace ONE  
(formerly Airwatch)

# Data import process



## Normalize

Merge source-specific attributes into a common data schema



## Deduplicate

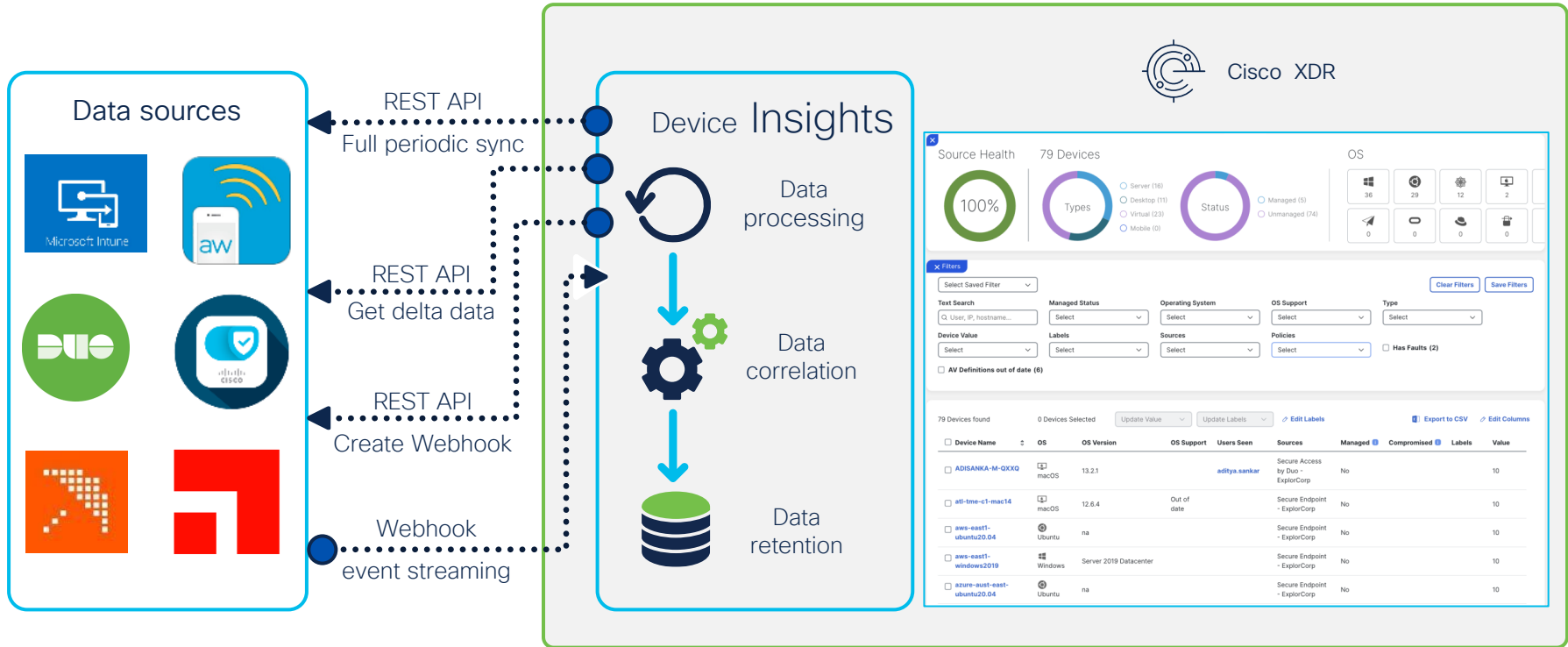
Remove duplicate or insignificant details from each record



## Correlate

Combine different records for the same device into one unified record

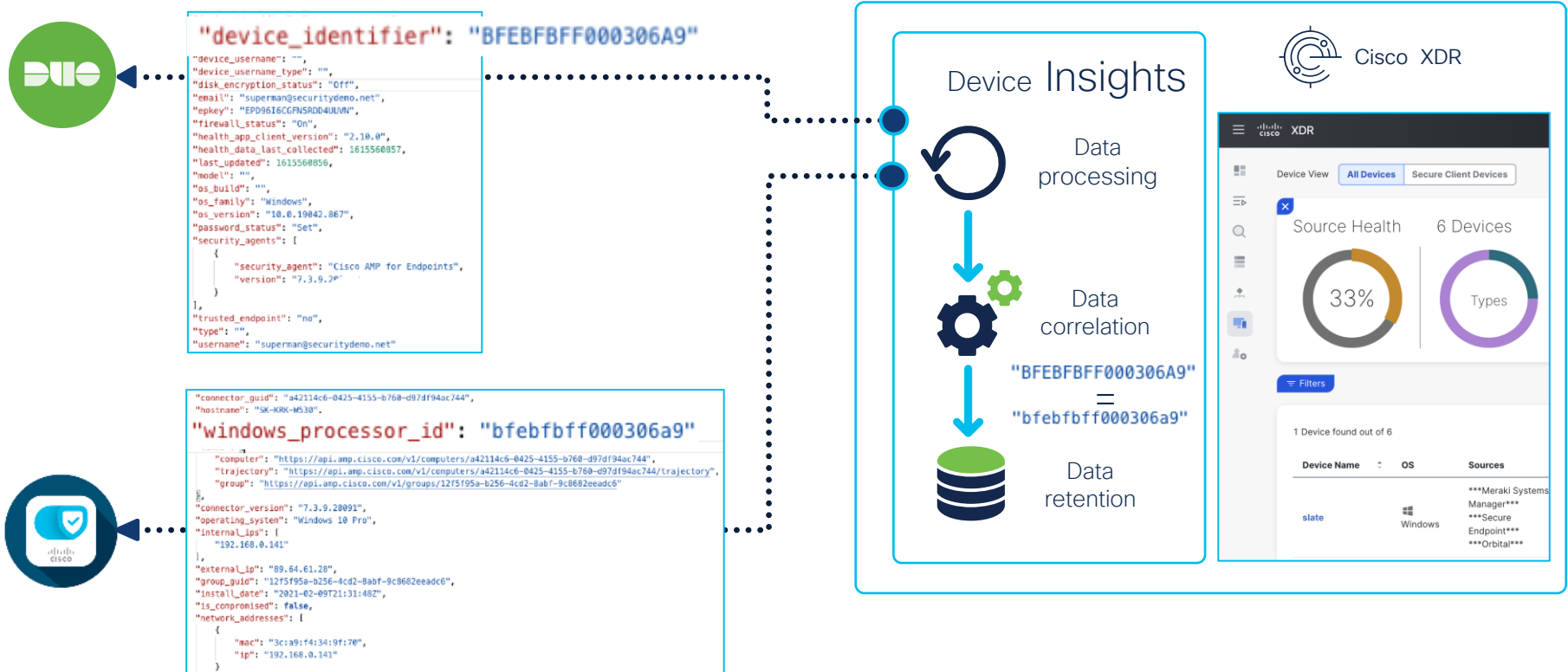
# XDR Device Insights high level architecture



# Communication methods - examples



# Data merging example (simplified)



# Data merging priorities

Not all attributes used for merging are equally reliable. To overcome this, Device Insights is designed in a way that allows using the most reliable keys first.

When there is a possibility to match on multiple attributes, Device Insights sets the priority based on the list shown below to ensure we have obtained the best possible match

- Hardware ID
- Serial
- MAC
- IMEI
- Hostname

The screenshot displays four device detail cards in a grid layout. Each card shows the device name, logo, and a list of attributes such as 'Last Seen', 'Policy', 'Group', 'Install Date', 'Connector', 'Version', 'Users', 'Local Users', 'Computer SID', 'Node OS', 'Version', 'Release', 'Architecture', 'Client Type', 'Client Version', 'Reported OS', and 'Version'. The Secure Client card also includes 'Cloud Management' and 'Modules' information. A 'Device Events' link is visible at the bottom right of the Secure Client card.

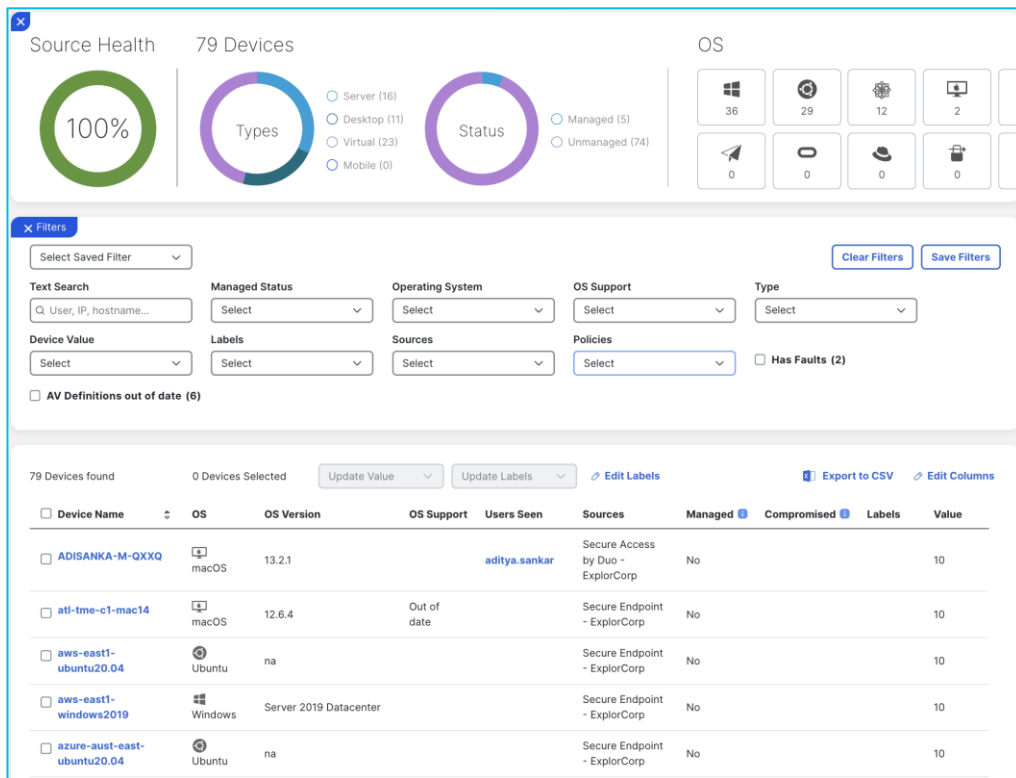
Device Name	Attributes
Secure Endpoint - ExplorCorp	Last Seen: 2023-05-27T21:44:37.000Z Policy: Protect Group: Mars Clients Install Date: 2022-11-15T10:02:08.000Z Connector: 8.1.7.21417 Version:
Meraki Systems Manager - ExplorCorp	Last Seen: 2023-05-26T21:48:18.000Z Tags: recently-added App Users: MIKE-WIN10tme Auto Tags: geo_compliant, pc, windows_agent_enrollment, windows_profile_enrollment
Orbital - ExplorCorp	Last Seen: 2023-05-29T12:37:38.440Z Users: tme Local Users: Administrator, DefaultAccount, Guest, tme, WDAGUtilityAccount Computer SID: S-1-5-21-3025806627-2025052165-512010680 Node OS: windows Version: v1.27.2 Release: 10.0.19044 Architecture: amd64
Umbrella - ExplorCorp	Last Seen: 2023-05-27T05:37:25.000Z Policy: Default Policy Client Type: AnyConnect Client Version: 5.0.2075 Reported OS: Windows Reported OS Version: 10
Secure Client	Last Seen: 2023-05-29T05:44:26.497Z Deployment: Secure Client Deployment ExplorCorp CSC Version: 5.0.02075 Secure Endpoint: 8.1.7.21417 Version: Cloud Management: 1.0.1.400 Version: Modules: Cloud Management v.1.0.1.400, Cisco Secure Endpoint v.8.1.7.21417, AnyConnect VPN v.5.0.02075, Umbrella v.5.0.02075, DART v.5.0.02075, Network Visibility Module v.5.0.02075 CSC UDID: cc2b22ab-57db-4051-932a-e5c4aa6f8b6b AC UDID: 68cca45cda768ff468753ec52f80bc18428fb048 Device Events

# Next-level asset resolution and inventory

- Inventory from traditional device managers combined with rich context from security products
- Customizable reporting on your devices and their security posture
- Additional context for XDR-driven investigations to Identify a “target” versus an “asset”
- Management of Cisco Secure Client profiles and deployments

The screenshot displays a dashboard with three main sections, each representing a different security product. Each section includes a logo, a name, and a list of attributes such as 'Last Seen', 'Policy', 'Group', 'Install Date', 'Connector', 'Version', 'Users', 'Local Users', 'Computer SID', 'Node OS', 'Version', 'Release', 'Architecture', 'Client Type', 'Client Version', 'Reported OS', and 'Version'. The products shown are Secure Endpoint - ExplorCorp, Orbital - ExplorCorp, and Umbrella - ExplorCorp. To the right of these sections, there is a larger panel for 'Meraki Systems Manager - ExplorCorp' and 'Secure Client', which includes additional details like 'Tags', 'App Users', 'Auto Tags', 'Deployment', 'CSC Version', 'Secure Endpoint', 'Cloud Management', 'Modules', 'AnyConnect VPN', 'Umbrella', 'DART', 'Network Visibility Module', 'CSC UDID', and 'AC UDID'. A 'Device Events' link is visible at the bottom right of the Secure Client section.

# Inventory



- Shows a list of devices from all integrated sources
- Allows for searching and filtering of devices based on various criteria including:
  - Management status
  - Device type
  - Operating system
  - Simple attributes (name, MAC address, IP address, etc.)
  - Sources (inclusive/exclusive)
- Columns can be customized, and device lists can be exported to a CSV
- “Secure Client Devices” tab shows information about Cisco Secure Client for devices if CSC is enabled

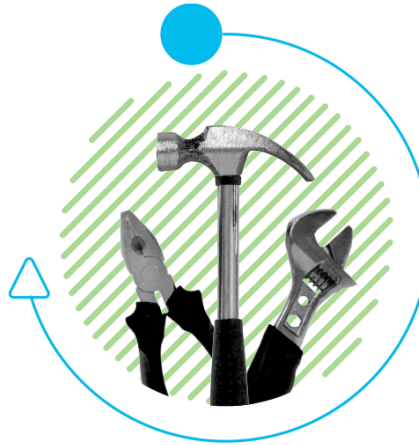
# Cisco Secure Client: Security agent consolidation

Built upon AnyConnect, the Secure Client is our next-generation software which introduces Cisco Secure Endpoint as a fully integrated module and offers optional Cloud Management via SecureX with Device Insights.

AnyConnect VPN module + VPN Management Tunnel is an **always-on intelligent VPN**

Secure Endpoint module protects your endpoint from threats and **reduces your number of clients**

Network Visibility Module delivers a continuous feed of high-value **endpoint telemetry**



ISE Posture performs **endpoint posture assessment**

Umbrella Roaming Security module adds **DNS-layer security**

XDR enables you to create **cloud-managed deployments** of Secure Client.

# Deployments

- Combination of packages and profiles to be deployed to a group of endpoints
- Package options:
  - Cloud Management
  - Cisco Secure Endpoint
  - AnyConnect Modules: VPN, Umbrella Roaming Client, DART, ISE Posture, Secure Firewall Posture, Network Access Manager, Network Visibility Module
- Different deployments can be assigned to different devices
- A Secure Client installer is generated for each deployment
  - Full installer: heavy installer that contains all necessary modules
  - Network installer: lightweight installer that downloads modules as needed

The screenshot shows the configuration page for an NVM to Direct XDR Deployment. At the top, there are buttons for 'Save', 'Full Installer', and 'Network Installer'. The page is divided into two main sections, each representing a different deployment version.

**Top Section (Beta 1.0.1.400):**

- Version: Beta (1.0.1.400)
- Cloud Management: NVM to Direct XDR CM
- Secure Endpoint: Choose an Instance
- Button: Choose a Group

**Bottom Section (Beta 5.0.2810.0):**

- Version: Beta (5.0.2810.0)
- AnyConnect VPN: Create Profile
- Start Before Logon: Off
- Umbrella: Choose a Profile
- Diagnostics and Reporting Tool: On
- ISE Posture: Create Profile
- Secure Firewall Posture: Off
- Network Access Manager: Create Profile
- Network Visibility Module: NVM to Cloud Direct

# Profiles

- Configurations for the various modules that can be deployed via Secure Client
- Cloud-based profile editors replace the legacy, Windows-only XML profile editors for:
  - Cloud Management
  - Customer Experience Feedback
  - ISE Posture
  - Local Policy
  - Network Visibility Module
  - VPN
  - VPN Management Tunnel

The screenshot shows the 'Cloud Management Profiles' configuration interface for 'NVM to Direct XDR CM'. At the top, there are action buttons: 'Edit Name', 'Delete', 'Reset Changes', 'Cancel', 'Make A Copy', 'Save', and 'Download'. The configuration is organized into four sections:

- Identity Service Settings:** Includes a toggle for 'Enable Debug Logging' which is currently turned off.
- Package Manager Service Settings:** Includes a 'Logging Level\*' dropdown menu set to 'Error', a 'Check-in Interval\*' dropdown menu set to '8 Hours', and a toggle for 'Notify User When Reboot Is Required' which is turned on.
- Cloud Management Service Settings:** Includes a 'Logging Level\*' dropdown menu set to 'Error'.
- Product Update Window:** Includes a toggle for 'Enable Product Update Window' which is turned off. A note below states: 'If not enabled, product updates can happen at any time. If enabled, product updates will only occur within the specified update window.'

# Incident Response Demo

# Agenda

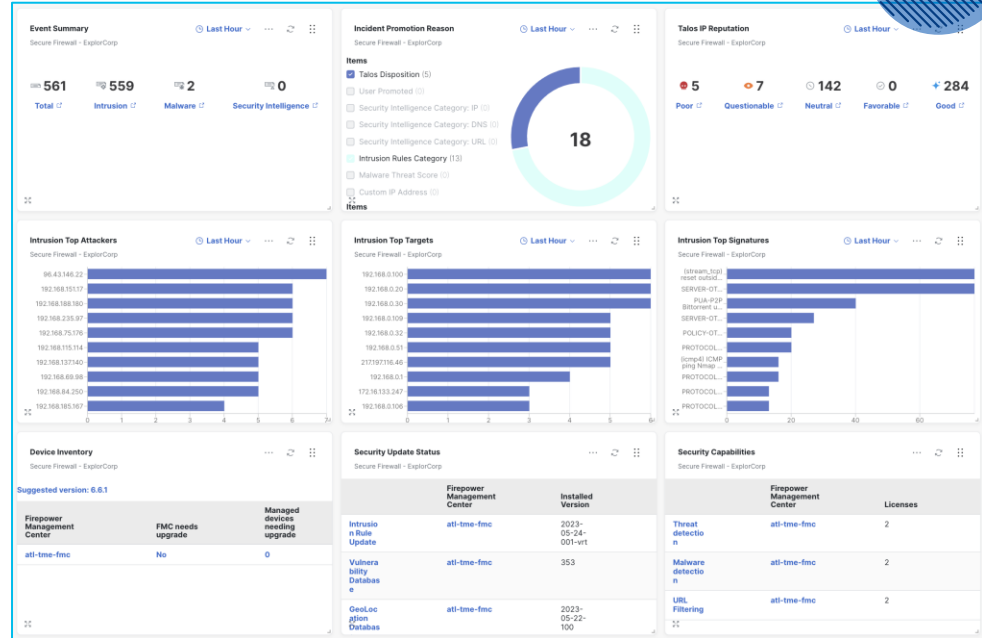
CISCO *Live!*

- The power of XDR
- How Cisco Secure Firewall boosts XDR
- What is Security Services Exchange and how does it work with Secure Firewall?
- Demo time!
- Next steps / Resources

# Secure Firewall

## Dashboard tiles

- Raw event summary
- Incident promotion reason
- Talos IP reputation
- Intrusion top attackers
- Intrusion top targets
- Intrusion top signatures
- Security Capabilities (FMC)
- Security Update Status (FMC)
- Device Inventory(FMC)



# Secure Firewall

## Enrichment

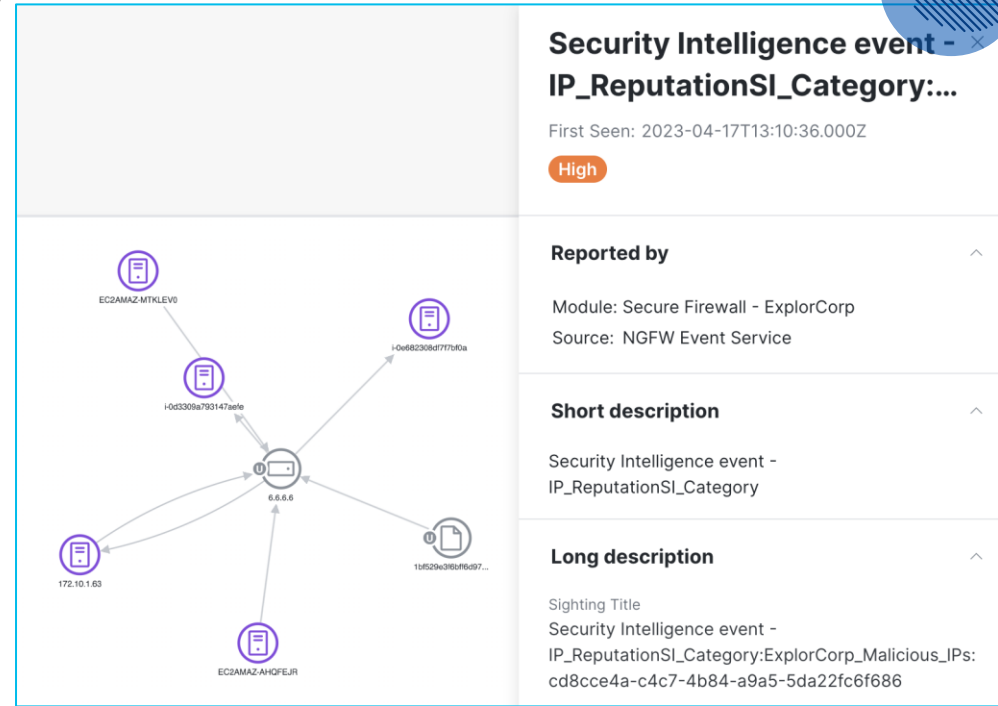
- Local IP sightings

## Reference

- Pivot point to sighting event

## Promote events

- Promote alerts from Analytics to incidents in XDR



**Security Intelligence event - IP\_ReputationSI\_Category:...**

First Seen: 2023-04-17T13:10:36.000Z

**High**

**Reported by**

Module: Secure Firewall - ExplorCorp  
Source: NGFW Event Service

**Short description**

Security Intelligence event - IP\_ReputationSI\_Category

**Long description**

Sighting Title  
Security Intelligence event - IP\_ReputationSI\_Category:ExplorCorp\_Malicious\_IPs: cd8cce4a-c4c7-4b84-a9a5-5da22fc6f686

The network diagram shows a central node labeled '0.0.0.0' with five arrows pointing to surrounding nodes. The nodes are: 'EC2AMAZ-MTKLEVO' (top), '1-0e682368d77f7b0a' (top-right), '1-0e3309a793147ae0' (middle), '172.10.1.63' (bottom-left), and 'EC2AMAZ-AHQPELR' (bottom). Each node is represented by a purple icon of a document with a magnifying glass.

# Secure Firewall

## Triage events

- See triaged network security events in the prioritized incidents list.

## Incident management

- Assign to others, change status, link incidents or add notes

## Maintain context

- View incidents in the XDR ribbon or the browser extension

**765** Incident Reported - **Suspected Malicious URL on ip 192-168-249-115** View Investigation Unassigned

Reported by Cisco Secure Cloud Analytics (cisco-dcloud-rtp) on 2023-05-26T13:41:55.000Z - 7 Linked Incidents

Suspected Malicious URL for Cisco Demo (RTP) [View Long Description](#)

Overview Detection Response Worklog

**Priority score breakdown**

<b>765</b>	<b>76</b>	<b>10</b>
Detection Risk	Asset Value at Risk	

**Short description**

Suspected Malicious URL for Cisco Demo (RTP)

**Long description**

Alert  
Suspected Malicious URL - #11941

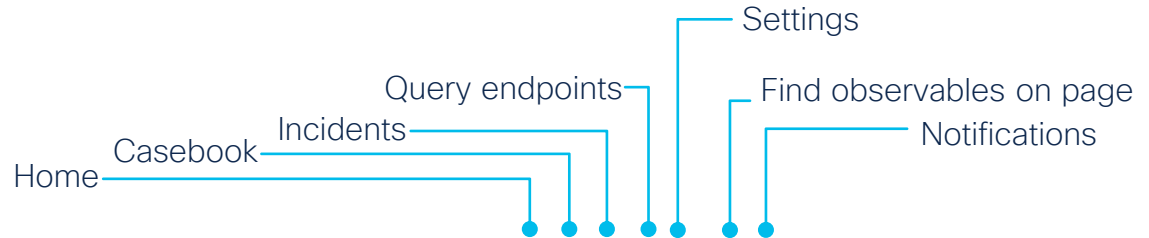
Tenant  
Cisco Demo (RTP) (cisco-dcloud-rtp)

Source  
ip-192-168-249-115.us-east-2.compute.internal

Description  
The device communicated with a suspected malicious URL. The alert uses the Suspected Malicious URL observation and requires URL data provided by firewalls via the Cisco Security Analytics and Logging (SAL) integration or Enhanced Netflow.

[View Incident Detail](#)

# Never lose context with XDR Ribbon



The screenshot displays the Cisco XDR CASEBOOK interface. The top navigation bar includes a search bar and a ribbon with icons for Home, Casebook, Incidents, Query endpoints, Settings, Find observables on page, and Notifications. The main content area is divided into several sections:

- Left Sidebar:** A list of cases under "Owned By Me" and "Owned By Others". The selected case is "Load RAT Grows Up-LU" with 29 Observables.
- Overview Panel:** Shows details for the selected case, including creation date (May 25, 2023, 10:50:53 AM), owner (user210 dcloud\_sxv2), and a summary section.
- Linked Incidents:** A section indicating "No linked incidents...".
- Observables Panel:** A search bar and a list of observables: 10 Domains (1 + 18 - 1 0 9 U), 10 SHA-256 (0 + 10 - 0 0 0 U), and 9 URLs (0 + 0 1 0 8 U).
- Notes Panel:** A section for notes, containing a note about the "Talos Loda Rat Grows Up investigation" with a link to the blog.

# XDR ribbon

- XDR ribbon allows you to carry the most relevant security context and threat intelligence with you across all products
- Transport framework for functionality: Take the capabilities of XDR and your integrated products with you when you go to any other product console. Have all your best tools handy
- Ties products together and provides unified experience and broad response capabilities across all the products
- Cross-launch capability: Pivot into any other products from the ribbon
- Ribbon apps: Brokered by XDR, provided by XDR and other products





# PSIRT Impact Monitoring

**Problem:** A network administrator is continuously monitoring for new PSIRT announcements and checking to see if their devices are vulnerable

**Solution:** This orchestration workflow will check for new PSIRTs then compare your devices version and notify you if any vulnerable devices were found.

SXO-WF QA 3:05 PM

## PSIRT advisory alert

One or more devices managed by Secure Firewall Manager require software updates due to a High PSIRT/CVE advisory. A [ServiceNow Incident](#) has been created. [Click here](#) to view the PSIRT advisory.

1 | FTDv (FTD) at 172.16.0.10 is running software version 7.1.0 and needs to be upgraded.

## PSIRT advisory alert

One or more devices managed by Secure Firewall Manager require software updates due to a High PSIRT/CVE advisory. A [ServiceNow Incident](#) has been created. [Click here](#) to view the PSIRT advisory.

1 | FTDv (FTD) at 172.16.0.10 is running software version 7.1.0 and needs to be upgraded.

## PSIRT advisory alert

One or more devices managed by Secure Firewall Manager require software updates due to a High PSIRT/CVE advisory. A [ServiceNow Incident](#) has been created. [Click here](#) to view the PSIRT advisory.

1 | FTDv (FTD) at 172.16.0.10 is running software version 7.1.0 and needs to be upgraded.

## PSIRT advisory alert

One or more devices managed by Secure Firewall Manager require software updates due to a High PSIRT/CVE advisory. A [ServiceNow Incident](#) has been created. [Click here](#) to view the PSIRT advisory.

1 | FTDv (FTD) at 172.16.0.10 is running software version 7.1.0 and needs to be upgraded.

## PSIRT advisory alert

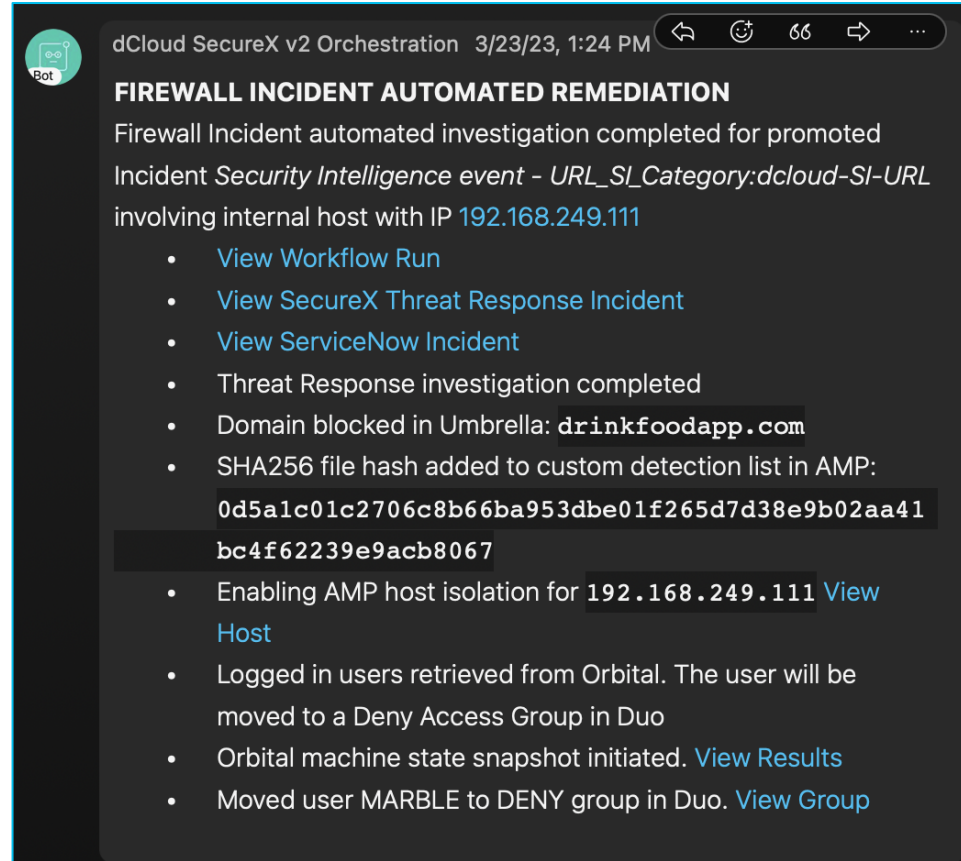
One or more devices managed by Secure Firewall Manager require software updates due to a Medium PSIRT/CVE advisory. A [ServiceNow Incident](#) has been created. [Click here](#) to view the PSIRT advisory.

1 | FTDv (FTD) at 172.16.0.10 is running software version 7.1.0 and needs to be upgraded.  
2 | FTD-test (ASA) at 127.0.0.1 is running software version 9.14.4 and needs to be upgraded.  
3

# Impact Red Remediation

**Problem:** A high priority intrusion event is detected by the Firewall. Adam, the analyst, needs to remediate quickly across multiple technologies.

**Solution:** An XDR orchestration workflow investigates the event and waits for approval. Once approval is granted, automated remediation at the DNS, application, and endpoint level are taken.



dCloud SecureX v2 Orchestration 3/23/23, 1:24 PM

**FIREWALL INCIDENT AUTOMATED REMEDIATION**

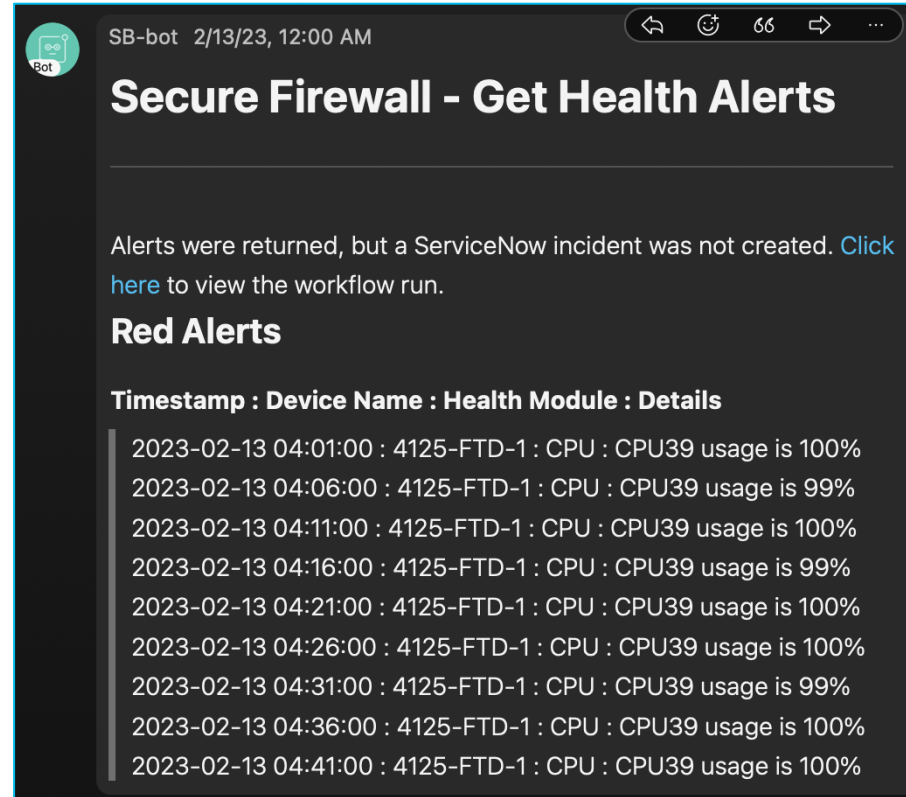
Firewall Incident automated investigation completed for promoted Incident *Security Intelligence event - URL\_SI\_Category:dcloud-SI-URL* involving internal host with IP **192.168.249.111**

- [View Workflow Run](#)
- [View SecureX Threat Response Incident](#)
- [View ServiceNow Incident](#)
- Threat Response investigation completed
- Domain blocked in Umbrella: **drinkfoodapp.com**
- SHA256 file hash added to custom detection list in AMP:  
**0d5a1c01c2706c8b66ba953dbe01f265d7d38e9b02aa41bc4f62239e9acb8067**
- Enabling AMP host isolation for **192.168.249.111** [View Host](#)
- Logged in users retrieved from Orbital. The user will be moved to a Deny Access Group in Duo
- Orbital machine state snapshot initiated. [View Results](#)
- Moved user MARBLE to DENY group in Duo. [View Group](#)

# Firewall Health Monitoring

**Problem:** A network administrator is trying to maintain a healthy network but sometimes a device gets into an unhealthy state. It can take time to react these issue the network administrator is not aware.

**Solution:** This orchestration workflow will check for health alerts from your devices and proactively notify via Webex teams, Slack, or email.



SB-bot 2/13/23, 12:00 AM

## Secure Firewall - Get Health Alerts

Alerts were returned, but a ServiceNow incident was not created. [Click here](#) to view the workflow run.

### Red Alerts

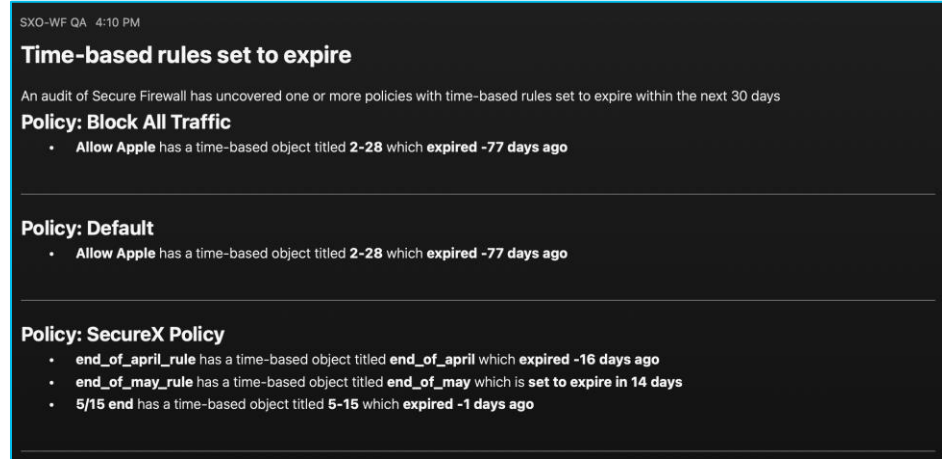
**Timestamp : Device Name : Health Module : Details**

2023-02-13 04:01:00	4125-FTD-1	CPU	CPU39 usage is 100%
2023-02-13 04:06:00	4125-FTD-1	CPU	CPU39 usage is 99%
2023-02-13 04:11:00	4125-FTD-1	CPU	CPU39 usage is 100%
2023-02-13 04:16:00	4125-FTD-1	CPU	CPU39 usage is 99%
2023-02-13 04:21:00	4125-FTD-1	CPU	CPU39 usage is 100%
2023-02-13 04:26:00	4125-FTD-1	CPU	CPU39 usage is 100%
2023-02-13 04:31:00	4125-FTD-1	CPU	CPU39 usage is 99%
2023-02-13 04:36:00	4125-FTD-1	CPU	CPU39 usage is 100%
2023-02-13 04:41:00	4125-FTD-1	CPU	CPU39 usage is 100%

# Expiring Time Based Objects

**Problem:** As a network administrator it is always challenging to manage your policies. Some rules in the policy may not be active due to an expired time range and finding expired rules can be time consuming.

**Solution:** This orchestration workflow will check rules that have already expired or will expire soon and proactively notify you of which rules to review.



# Block Observables on Firewall

**Problem:** Adam the analyst, is reviewing an endpoint alert. He notices an unknown IP address related to a compromise on the endpoint. Adam wants to act by blocking this IP address on the firewall, but he doesn't have access to Firepower Management Center.

**Solution:** Using the pivot menu Adam can block the IP address at the click of a button from anywhere.

The screenshot displays a security dashboard interface. On the left, a list of 'TOP ACTIVE' observables is shown, including the IP address 6.6.6.6. A pivot menu is open over the 6.6.6.6 entry, showing a 'Secure Firewall - Block Observable' option. The menu also lists other actions like 'Move Computer to Triage Group' and 'Submit URL to Secure Malware Analytics'. A tooltip above the menu provides details for the IP address 6.6.6.6, including its source (Talos Intelligence) and a note that there are 2 verdicts for this observable.

**31 Observables**

**TOP ACTIVE**

- 6.6.6.6
- 1bf529e3f6...
- 94.204.151.8
- 64.104.44.10
- 3.136.210.16

**IP Address** 6.6.6.6

**Verdict Source** Talos Intelligence

> There are 2 Verdicts for this observable.

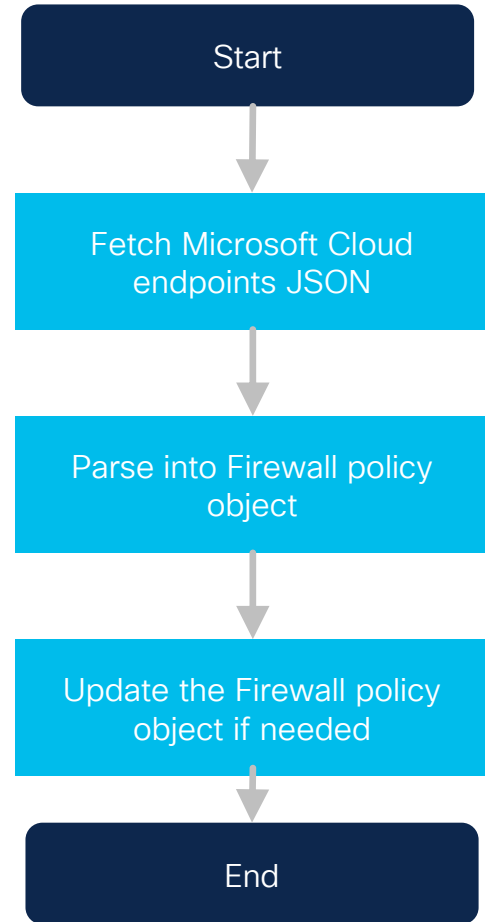
**Secure Firewall - Block Observable**

- Move Computer to Triage Group
- Submit URL to Secure Malware Analytics
- Meraki - MX - L3 Outbound Firewall Block
- Umbrella - Add to Destination List
- ServiceNow - Request Firewall NullRoute

## O365 to FMC network object

**Problem:** Many network administrators need to keep track of Office 365 ip ranges. These ranges are constantly changing and updating Firewall policy objects can be very time consuming.

**Solution:** An XDR orchestration workflow fetches the ranges from Microsoft and updates the policy object. The workflow can be scheduled to run once a day ensuring the policy is always up to date.



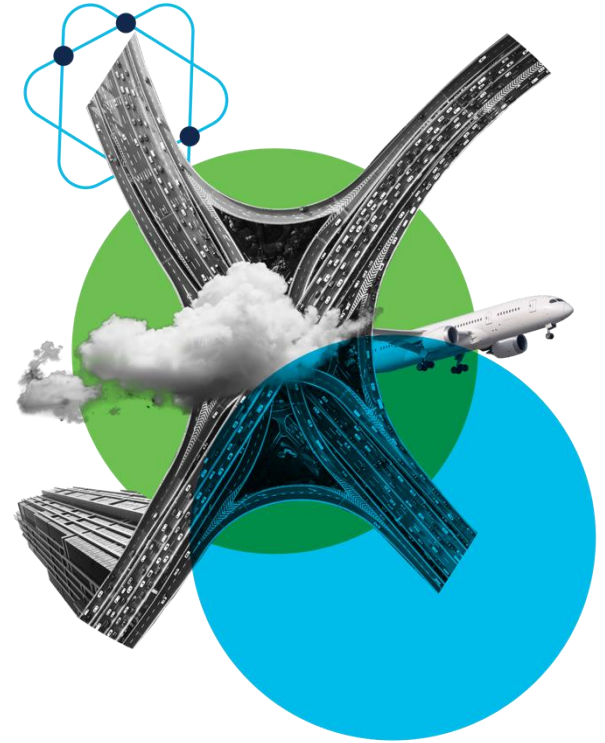
# Agenda

CISCO *Live!*

- The power of Cisco XDR
- How Cisco Secure Firewall boosts XDR
- What is Security Services Exchange and how does it work with Secure Firewall?
- Demo time!
- Next steps / Resources

# Security Services Exchange

“A secure distributed infrastructure to enable data acquisition, data processing and data publishing for data from products/devices on-premises to the Cisco Cloud.”



# Connecting Devices & Enabling Customer Cloud Services

## Integrated Cloud services

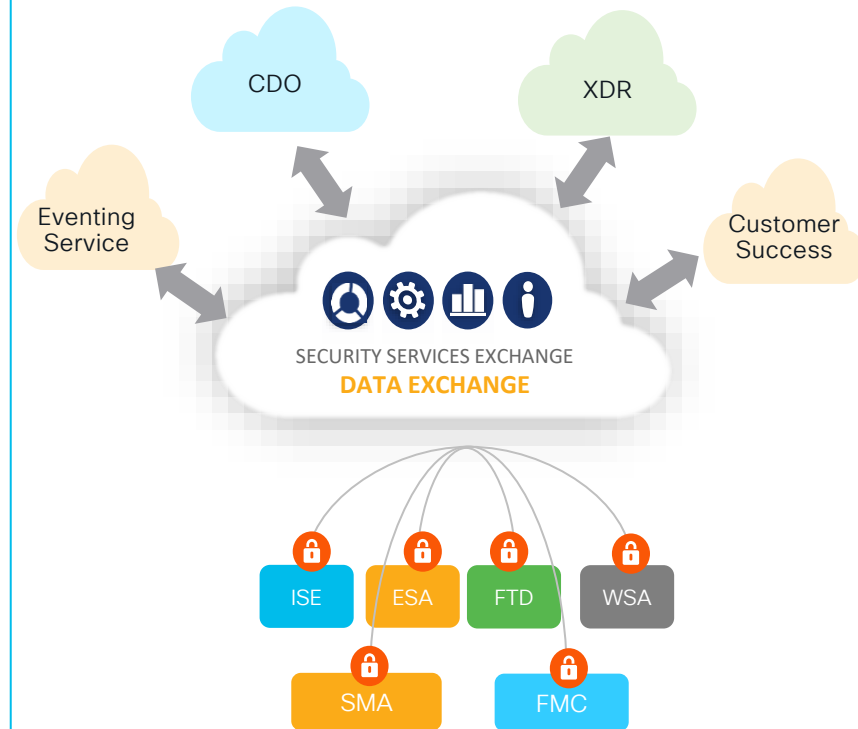
- Cisco Defense Orchestrator (CDO)
- XDR
- Cisco TAC
- Customer Success

## Core Infrastructure Services

- Identity and Tenancy
- Secure device registration
- Application registration and discovery
- Data publishing

## Device Connector / Agent

- Secure Bi-Directional Channel
- REST, CLI, WebSocket
- File Upload / Download
- Services Management
- Products: FMC, FTD\*, ESA, WSA, SMA, ISE, SNA
- \* = Events are SENT to SSX and stored for 7 days



# SSX Core Functions

## Identity and tenancy

- Brokered identity
- Common tenant context
- Application onboarding and provisioning
- Issuance of tokens and claims

## Secure Device Registration

- Leverage Cisco's Smart Accounts
- Present token to SSX registration service
- Device added to SSX tenant device database

## Bi-directional device control channel

- Per-tenant, per-device secure control channel
- Send commands and receive responses from devices
- Unicast (today) or multicast
- Receive files and other bulk items from devices

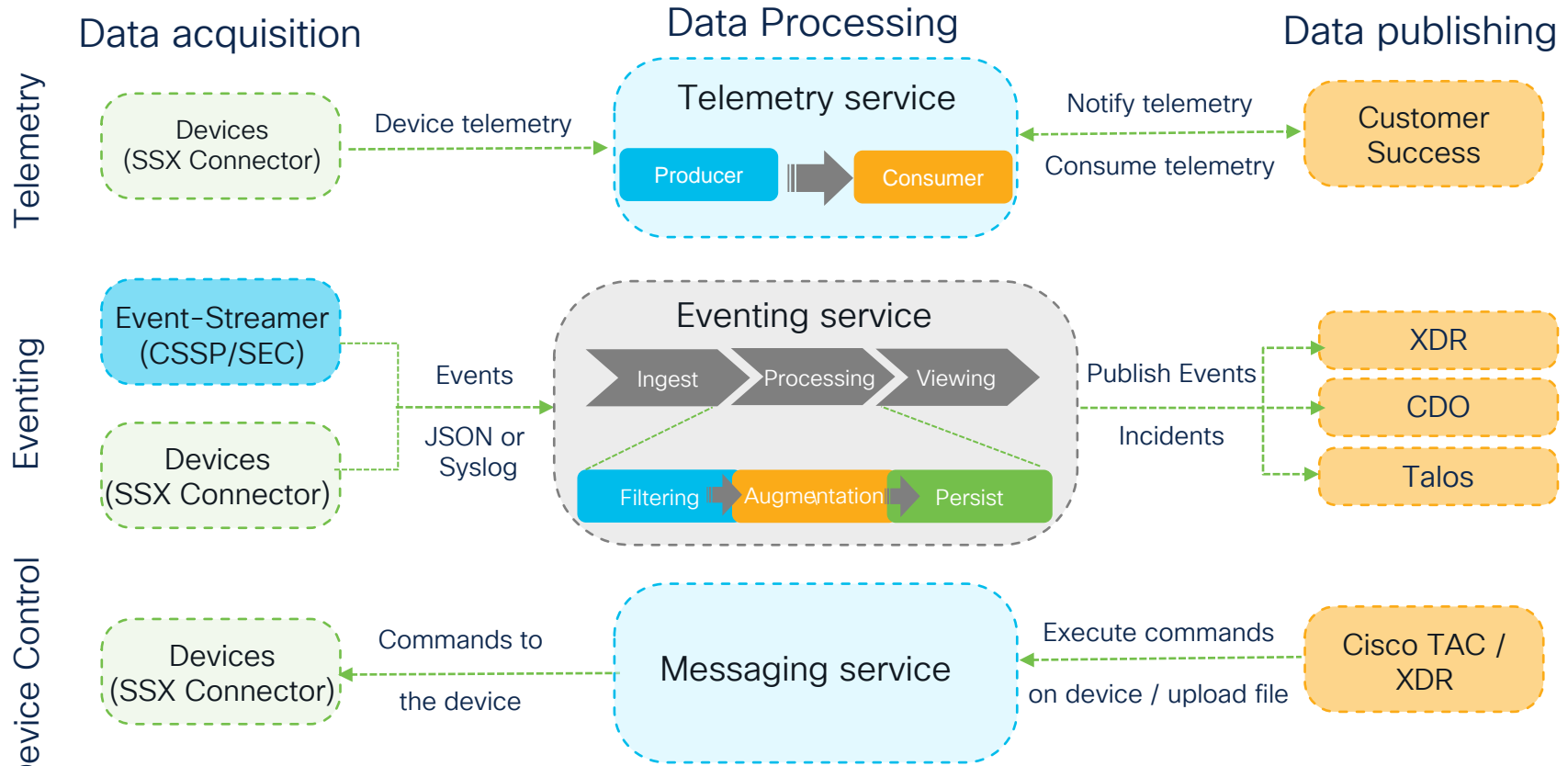
## Application Registration and Discovery

- Applications provide end-points for data consumption (and other)
- Devices receive list of end-points for one or more SSX services

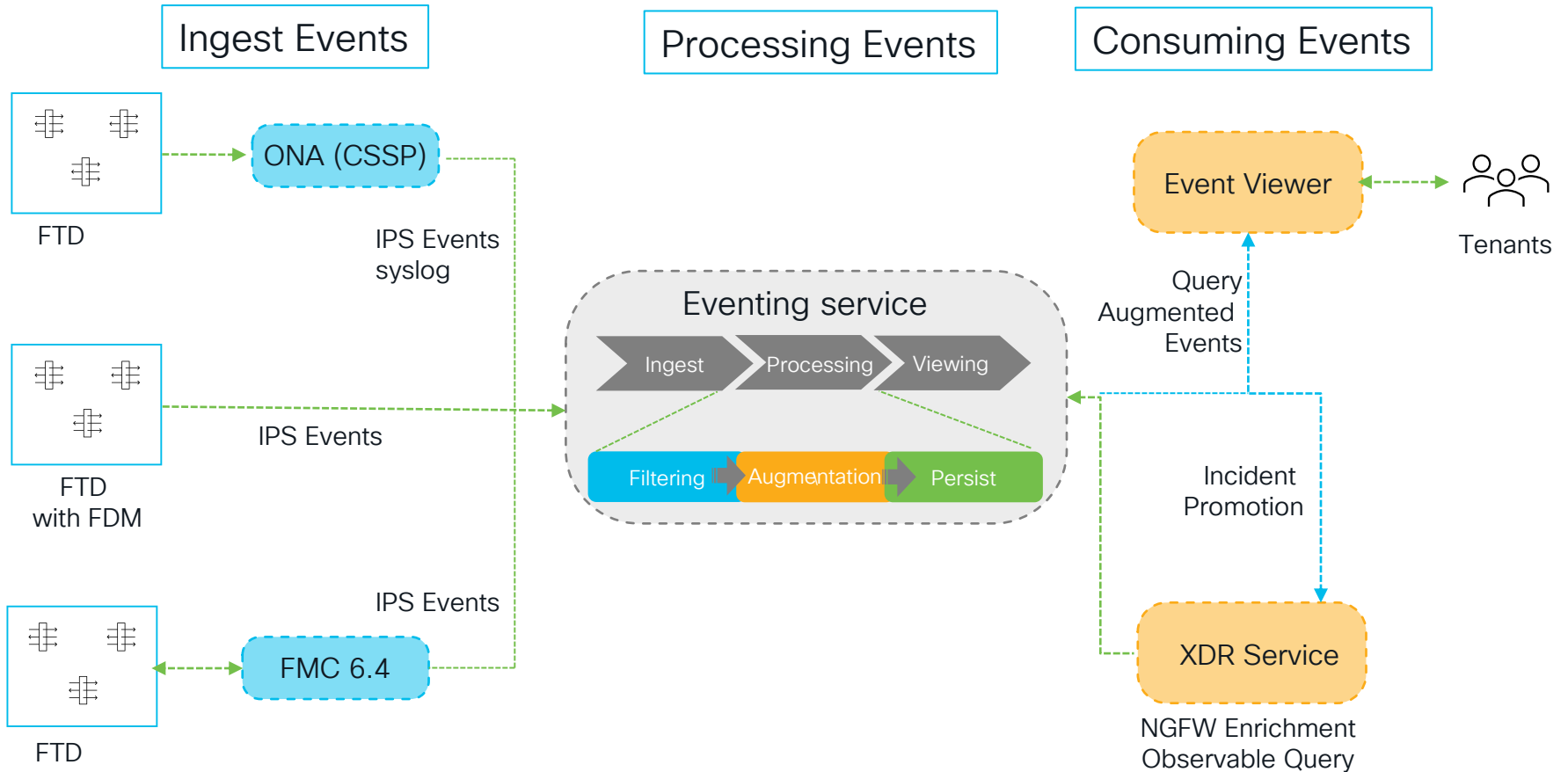
## Data Publishing

- During registration, services provides data consumption end-point(s)
- Based on subscription, device connector is provided with appropriate end-point to deliver data
- SSX created JWT is presented to consuming service

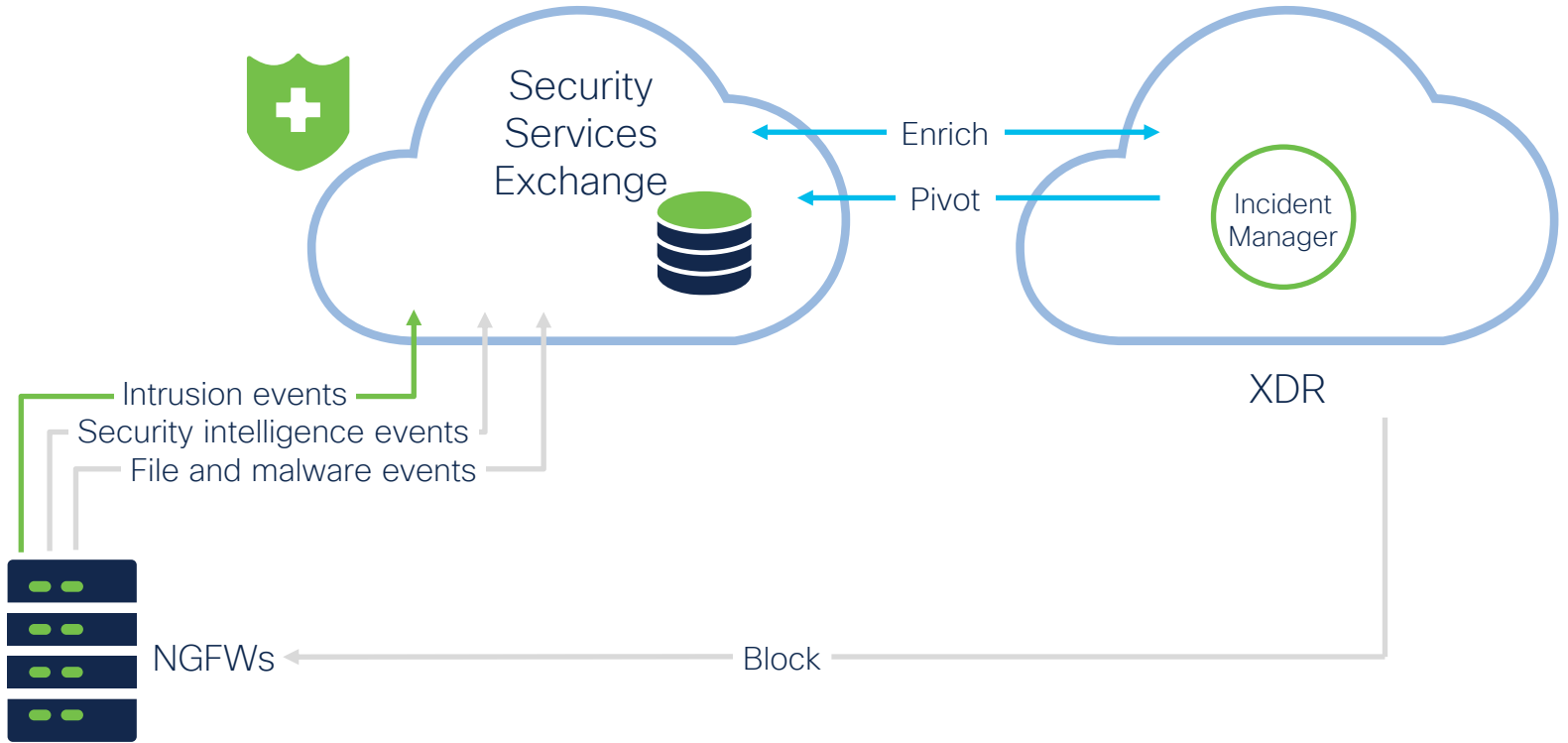
# Supported Data pipelines



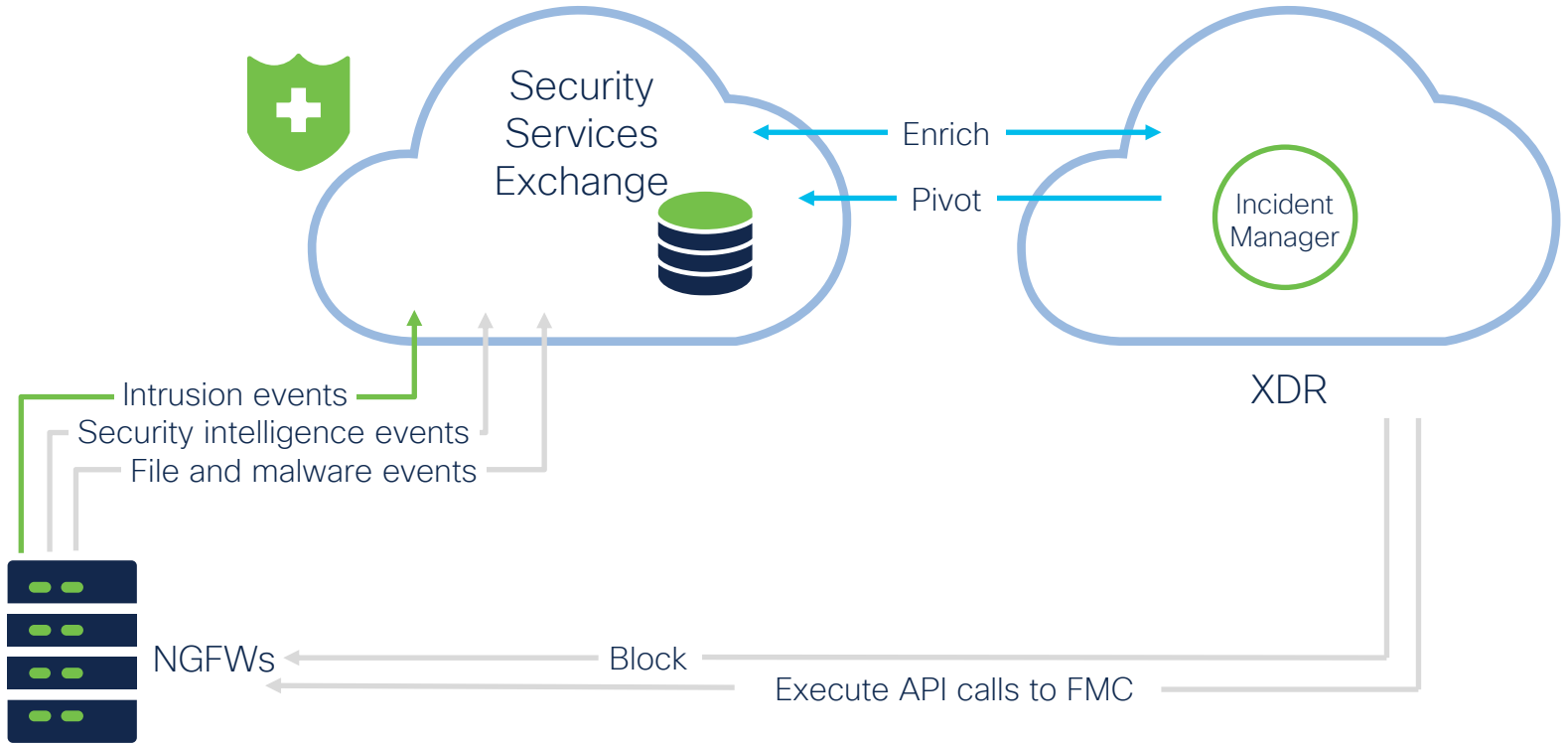
# Eventing Service



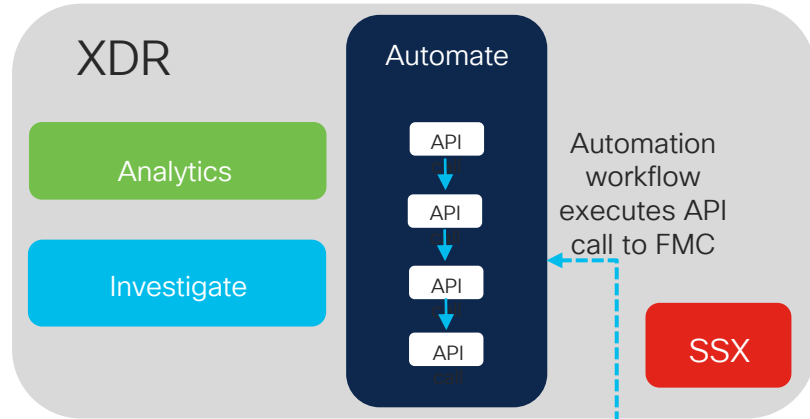
# Secure Firewall



# Secure Firewall



# Cloud to on-prem API Proxy

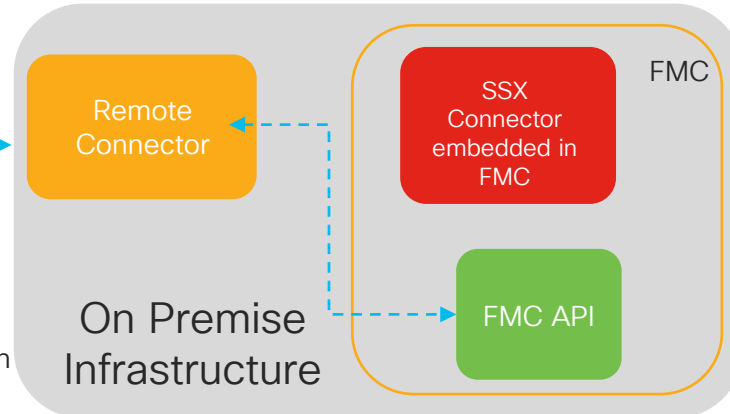


## Requirements

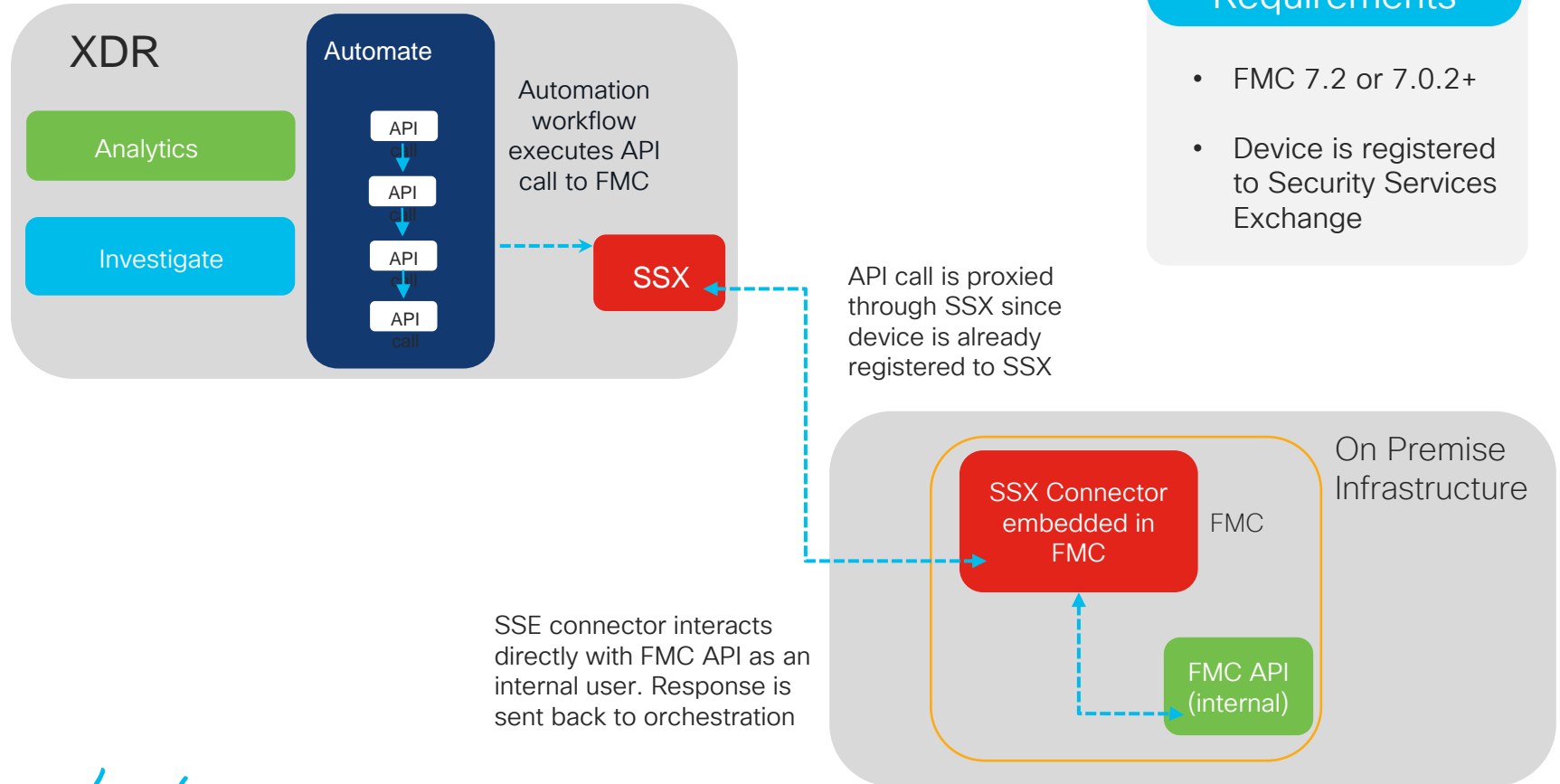
- Any FMC version
- Remote appliance deployed in vCenter
- Outbound access on TCP 8883

API call is sent to orchestration remote based on target configuration

Authenticate to API as an external user and execute API call. Response is sent back through orchestration remote



# Cloud to on-prem API Proxy



## XDR + FMC + Orchestration Remote VM

- Not version specific
- Requires deployment of VM on VMware
- Versatile to interact with other on-premise API's
- Outbound TCP 8333 may require edge Firewall changes
- A few additional configuration steps

## XDR + FMC + API proxy

- Requires 7.2+ or 7.0.2+
- Requires device registered to SSX
- Easier for customers / built in experience
- Importing workflows is plug-n-play

# Sec Services Exchange Proxy API Swagger Int.

visibility.amp.cisco.com/iroh/iroh-sse/index.html#/SSE/post\_iroh\_iroh\_sse\_device\_id\_api\_proxy

- GET /iroh/iroh-sse/device List SSE Devices
- GET /iroh/iroh-sse/device/{device-id} Read an SSE Device
- DELETE /iroh/iroh-sse/device/{device-id} Delete an SSE Device
- PATCH /iroh/iroh-sse/device/{device-id} Patch an SSE Device
- POST /iroh/iroh-sse/device/{device-id}/api-proxy** Send command payloads to a SSE device through the API Proxy

required\_scopes: sse/api-proxy:read

Parameters Cancel

Name	Description
<b>device-id</b> * required string (path)	186d4b11-6b8f-4e71-a997-758ae10f8af0

**APIProxyRequestPayload** \* required  
array[object]  
(body)

Edit Value | Model

```
[{"headers": {"Content-Type": "application/json"}, "operation": "POST", "scheme": "http", "command": "/api/fmc_config/v1/domain/a276abec-e0f2-11e3-8169-6d9ed49b625f/object/hosts", "commandId": "1234", "timeout": 110,}
```

Cancel

# Security Services Exchange Proxy API request fields

“operation” defines the method (ex: POST, PUT, GET, DELETE)

“command” is the FMC API path to execute one

“body” is the request payload which is identical to the payload used directly on the FMC API

“scheme”, “timeout”, “headers” and “commandId” can be left as static values matching the default

```
[{
  "headers": {
    "Content-Type": "application/json"
  },
  "operation": "POST",
  "scheme": "http",
  "command": "/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/object/hosts",
  "commandId": "1234",
  "timeout": 110,
  "body": {
    "type": "Host",
    "value": "11.22.33.44",
    "overridable": false,
    "description": "Host created from XDR",
    "name": "XDR Object"
  }
}]
```

# Sample Response

```
{
  "data": [
    {
      "headers": {...},
      "operation": "POST",
      "scheme": "http",
      "command": "/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/object/hosts",
      "commandId": "1234",
      "body": {
        "description": "Host created from XDR Automate",
        "id": "005056BE-CE57-0ed3-0000-115964118593",
        "links": {
          "parent": "https://localhost/api/local/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/object/networkaddresses",
          "self": "https://localhost/api/local/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-6d9ed49b625f/object/hosts/005056BE-CE57-0ed3-0000-115964118593"
        },
        "metadata": {...},
        "code": "201",
        "timeout": 110
      }
    }
  ]
}
```

# Configure the integration

- 1 Enable XDR
- 2 Enable XDR Automate
- 3 Select a user role for XDR workflows
- 4 Save the configuration

The screenshot shows the 'SecureX Setup' page in the Firewall Management Center. The page is divided into four numbered sections:

- 1 Cloud Region:** This setting determines where events are sent to, if configured to send to the cloud, as well as data generated by the Cisco Success Network and Cisco Support Diagnostics tools. The 'Current Region' is set to 'us-east-1 (US Region)'. A green callout '1' points to a green checkmark indicating 'SecureX is enabled for US Region.' with a 'Disable SecureX' button below it.
- 2 SecureX Enablement:** After completing this configuration, the SecureX ribbon will show up at the bottom of each page. A green callout '2' points to the 'SecureX is enabled for US Region.' message.
- 3 Event Configuration:** This section includes checkboxes for 'Send events to the cloud' (checked), 'Intrusion events' (checked), 'File and malware events' (checked), and 'Connection Events' (checked). There are radio buttons for 'Security' and 'All' (selected). A callout '3' points to the 'All' radio button.
- 4 Orchestration:** This section includes a checkbox for 'Enable SecureX Orchestration' (checked). Below it, there is a dropdown menu for 'Assigned Role' set to 'Administrator'. A callout '4' points to the 'Administrator' dropdown.

At the bottom of the page, there is a navigation bar with a close button (X), a home button (house icon), a search button (magnifying glass), and a plus sign (+).

# Configure the integration

ADD INTEGRATION

**Secure Email Threat Defense**  
Formerly Secure Email Cloud Mailbox

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

**+ Enable**

**Secure Email and Web Manager**  
Formerly SMA Email

Cisco Secure Email and Web Manager (formerly SMA Email) centralizes management and reporting functions across multiple Cisco email and web...

**Secure Firewall**  
Formerly Firepower

Secure Firewall (formerly Firepower) provides complete and unified management for firewall application control, intrusion prevention, URL filtering...

**1**

**Secure Malware Analytics**  
Formerly Threat Grid

Cisco Secure Malware Analytics (formerly Cisco Threat Grid) combines advanced sandboxing with threat intelligence into a powerful solution to protect...

Module Name

atl-tme-fmc

**Manage Devices** **Check for New Devices**

	Version	Status	Description	IP Address
atl-tme-fmc	7.2.0	Registered	10.90.12.219 atl-tme-fmc	10.90.12.219
atl-tme-fmc-log.cisco.com	7.2.3	Registered	10.90.12.236 atl-tme-fmc-log.cisco.com	10.90.12.236
atl-tme-fp4100-1 (FMC managed)	7.2.0	Registered	10.90.12.210 atl-tme-fp4100-1 (FMC managed)	10.90.12.210
atl-tme-fp4100-2 (FMC managed)	7.2.0	Registered	10.90.12.220 atl-tme-fp4100-2 (FMC managed)	10.90.12.220
atl-tme-ftd-log (FMC managed)	7.2.3	Registered	10.90.12.237 atl-tme-ftd-log (FMC managed)	10.90.12.237

5 per page 1-5 of 5 << < 1 / 1 > >>

Dashboard

Dashboard of the tiles associated with this integration module, which can be shared by members of your organization.

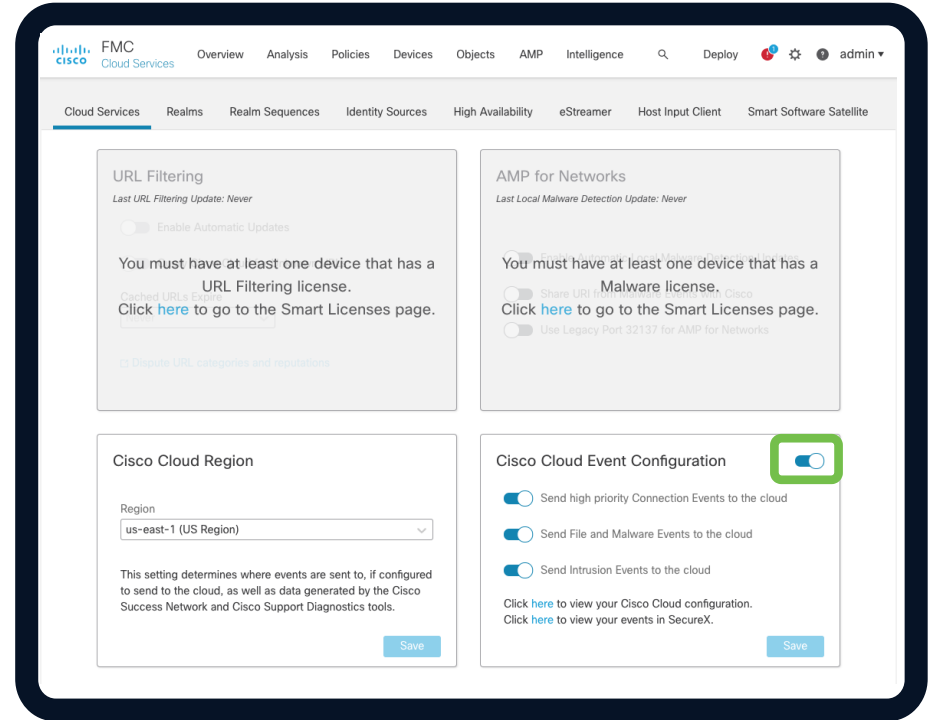
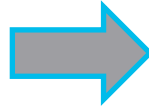
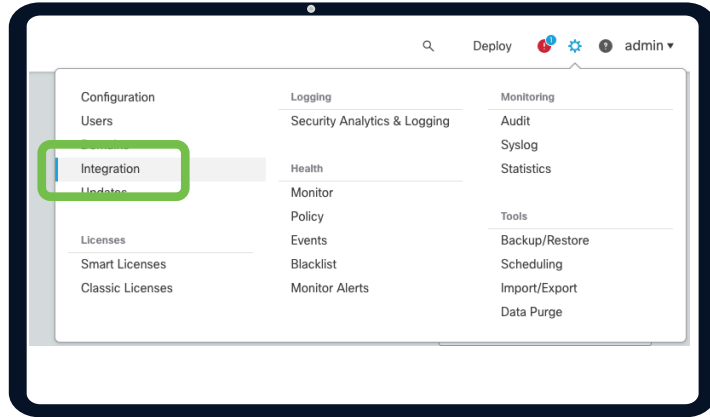
**2**

**Save**

**1** Add Firewall module

**2** Save the module

# Enable Cloud Event Configuration



# Sign up for XDR

## Launch

Choose your region:

North America

Sign in with your account:

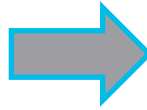
[SecureX via SecureX Sign-On](#)  
For new and existing SecureX users.

[SecureX via Cisco Security Account](#)  
For existing Threat Response & AMP users.

[SecureX via Cisco Threat Grid](#)  
For Threat Grid users.

Umbrella, CDO, SWC, SWE, Tetration, ESA, WSA, or Duo users log in with SecureX Sign-On

[Create an Account](#) [Legacy Site](#) | [Login Help](#) ?



## Account Activation

To start using SecureX, please configure your first product to activate your account.

If you are an AMP for Endpoints or Threat Grid customer, please ask that account administrator to invite you to their organization to get started.

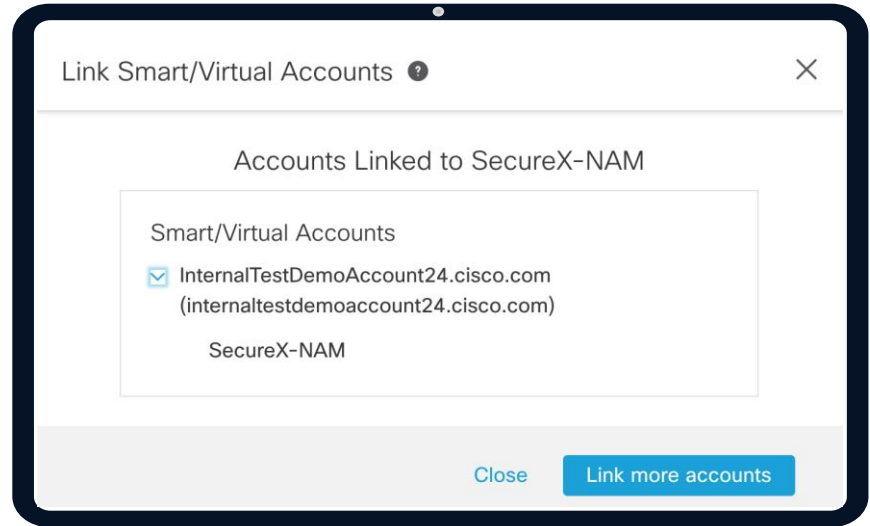
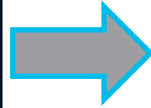
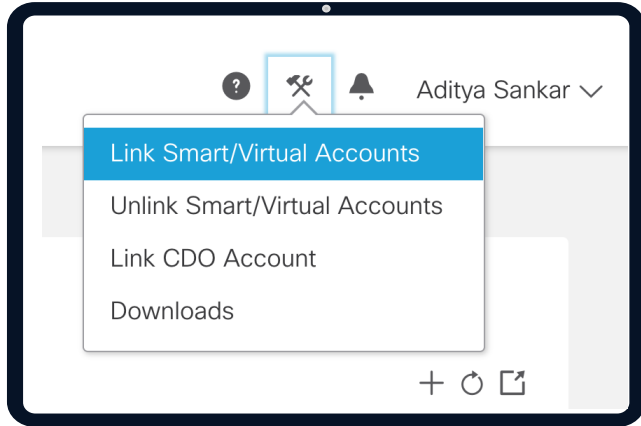
Configure integration modules such as Umbrella or AMP for Endpoints

[Configure](#)

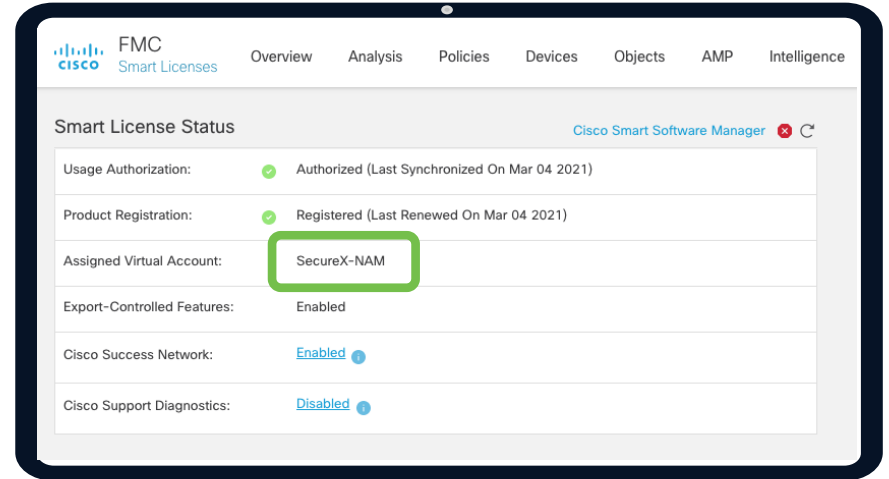
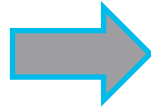
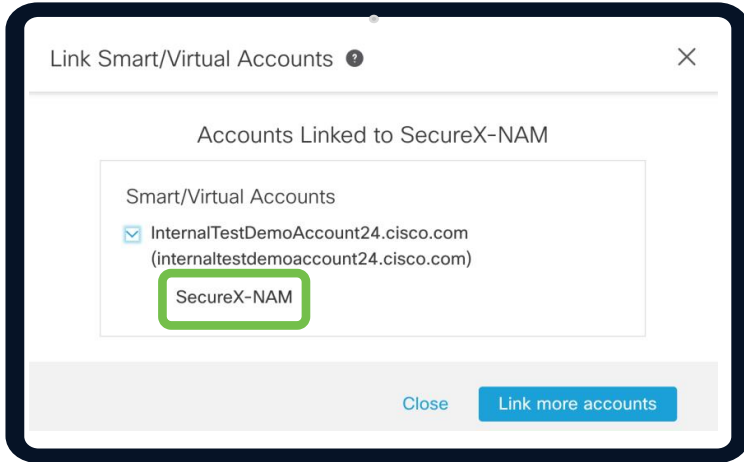
Connect a Device such as SMA Email/Web, Firepower, Email Security Appliance, WSA or Stealthwatch Enterprise

[Connect](#)

# Link Smart License Account to SSX



# Devices are onboarded to XDR



Full configuration video at  
[cs.co/XDR\\_videos](https://cs.co/XDR_videos)

# Firewall and XDR Demo

# Agenda

CISCO *Live!*

- The power of Cisco XDR
- How Cisco Secure Firewall boosts XDR
- What is Security Services Exchange and how does it work with Secure Firewall?
- Demo time!
- Next steps / Resources



## OBJECTIVES



- What is XDR and how it can enhance your Security Operations?
- How can you integrate your Firewall with XDR?
- How does the Firewall and XDR integration work behind the scenes?
- 5 valuable use cases you can enable today for **FREE!!**

# Agenda

CISCO *Live!*

- The power of Cisco XDR
- How Cisco Secure Firewall boosts XDR
- What is Security Services Exchange and how does it work with Secure Firewall?
- Demo time!
- Next steps / Resources

# XDR Resources

<http://cisco.com/go/securex>

<http://learnsecurex.cisco.com>

[http://cs.co/SecureX\\_videos](http://cs.co/SecureX_videos)

<http://security.cisco.com>



# Learning Map

## Security

### Threat Detection & Response

Learn how SecureX Threat Response is an investigation and remediation application that dramatically simplifies security by cutting the time and manual effort required for threat hunting and incident response.



Las Vegas, NV | June 4-8, 2023

If you are unable to attend a live session, you can watch it in the On-Demand Library after the event.

# Capture the Flag with XDR

Stop by Capture the Flag to get some hands-on experience working with XDR as a security analyst on a mission!

**Mission:** - 3.8 - SOC Life Simplified with XDR  
**Section:** - 3 - Blue Team powered by Cisco Secure

**Other Associated CTF Portals:** [ctf.us23-portal](#) Shared by fagioli (Bruno Fagioli),

**Mission Description:**  
Blue Team:  
XDR allows SOC teams to quickly and efficiently move away from endless investigation and instead spend their time remediating the most critical incidents across their Cisco and third party security stack. Sam (SOC Analyst) starts their day reviewing their queue to determine if any critical incidents have occurred to determine what actions to take and if needed handed off to the IR team (Remi).

<b>Overall Difficulty:</b> Easy	<b>Recommended For:</b> SecOps
<b>Time to Complete:</b> 01H:00M	<b>Mission Author:</b> Danny Rodriguez

**Key Takeaways from this Mission:**  
Cisco XDR addresses one of the biggest challenges of keeping up with ever-evolving threats and a growing attack surface: it **integrates with a selection of third-party products including competitive 3<sup>rd</sup> party ED, NDR, firewall, and email solutions.**

Day	Hours
Monday	8:30 AM to 6 PM
Tuesday	8:30 AM to 5 PM
Wednesday	8:30 AM to 5 PM
Thursday	8:30 AM to 1 PM



Want to learn more about XDR and see a live demo?

Visit us in the Cisco Showcase @ World of Solutions!

Day	Hours
Monday	10 AM to 6 PM
Tuesday	10 AM to 5 PM
Wednesday	10 AM to 5 PM
Thursday	10 AM to 1 PM



# DEVNET

Want to learn more about  
developing with XDR?

*Visit us in the DevNet Zone!*

Demo Booth

Tuesday from 9:30 AM to 5 PM

Theater Session

DEVNET-1083  
Tuesday at 1 PM

# Fill out your session surveys!



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



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



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

# Complete your Online Session Evaluation



# Continue your education

CISCO *Live!*

- 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](http://www.CiscoLive.com/on-demand)

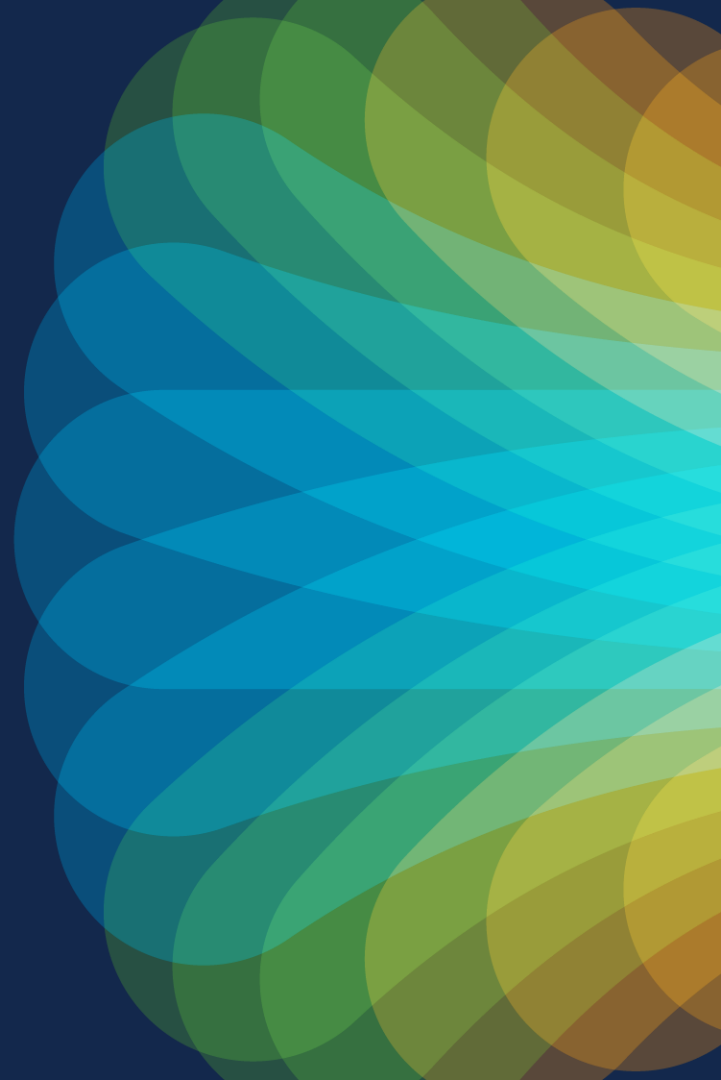


The bridge to possible

# Thank you

CISCO *Live!*

#CiscoLive

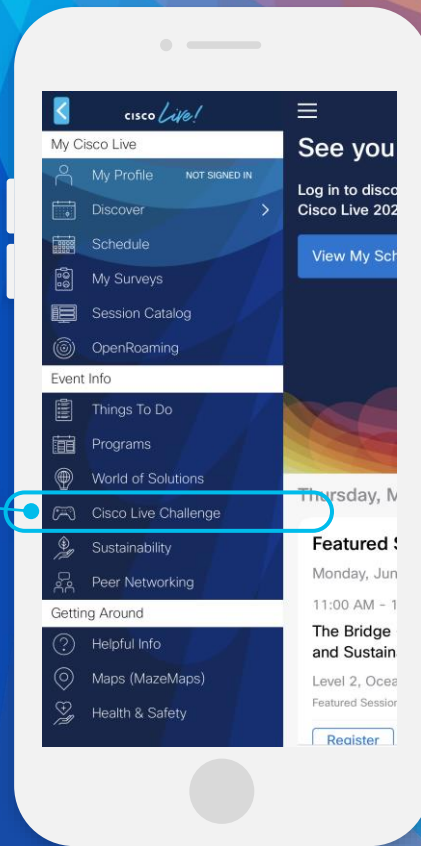
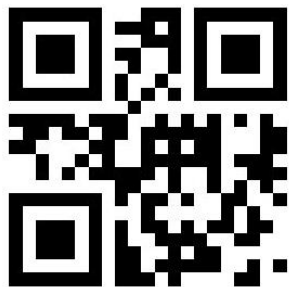


# Cisco Live Challenge

Gamify your Cisco Live experience!  
Get points for attending this session!

## How:

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



The Cisco Live! logo features the word "CISCO" in a bold, black, sans-serif font, followed by "Live!" in a black, cursive script font. The background of the entire image is a vibrant, multi-colored abstract pattern of overlapping, wavy bands in shades of red, orange, yellow, green, and blue, radiating from a bright white center on the right side.

CISCO *Live!*

Let's go

#CiscoLive