

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC



Cisco XDR with Firewall

Adi Sankar, Technical Marketing Engineer
BRKSEC-2596

Cisco Webex App

Questions?

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

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until November 15, 2024.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-2596>



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

cisco *Live!*



Oct 2014



Dec 2014

Team (3459) PyroTech



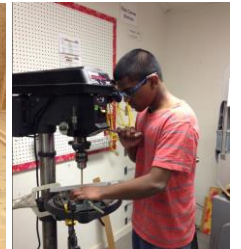
F1 Race Miami – May 2023



3D-Printing Cisco US2020 – 2013



Nov 2013



Dec 2013



July 2012



Aug 2011



Aug 2012

Agenda

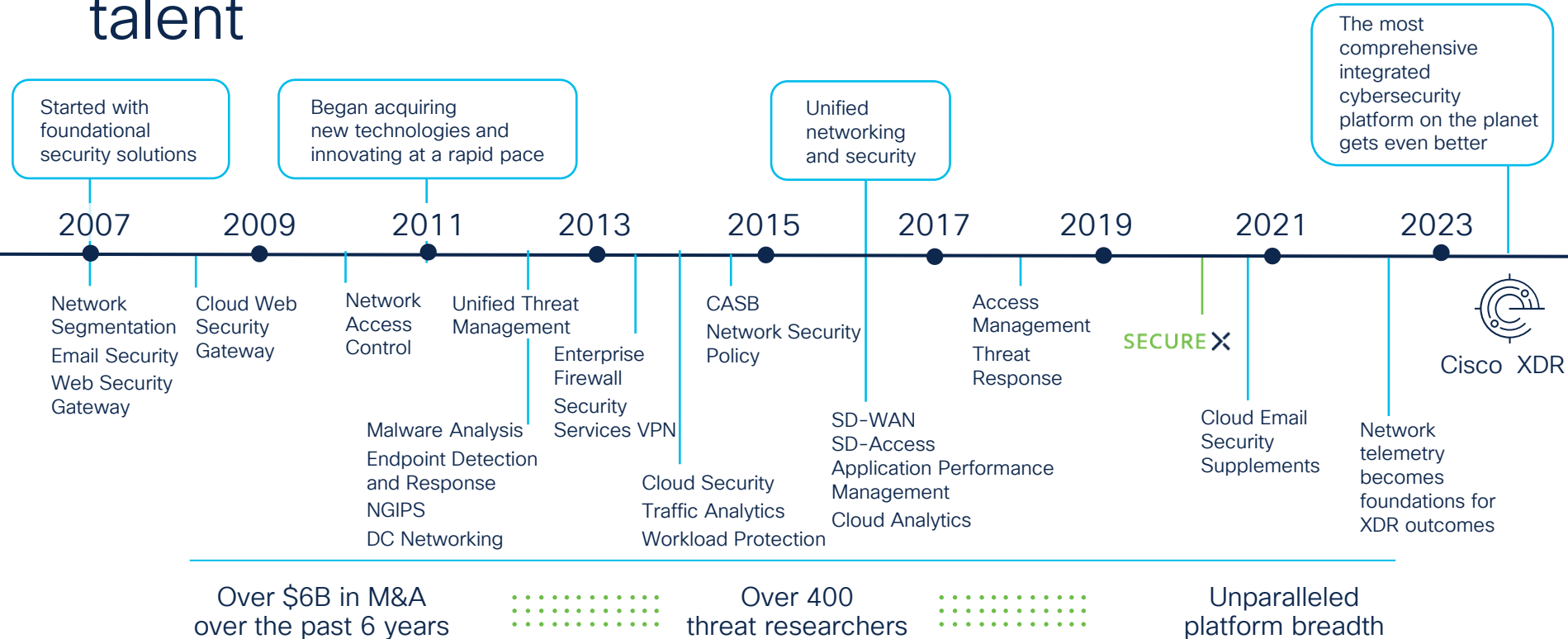
- The power of XDR
- How Cisco Secure Firewall boosts XDR
- What is Security Services Exchange and how does it work with Secure Firewall?
- Demo time!
- Next steps / Resources

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

Prioritise by Impact

2

Are we **prioritising 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

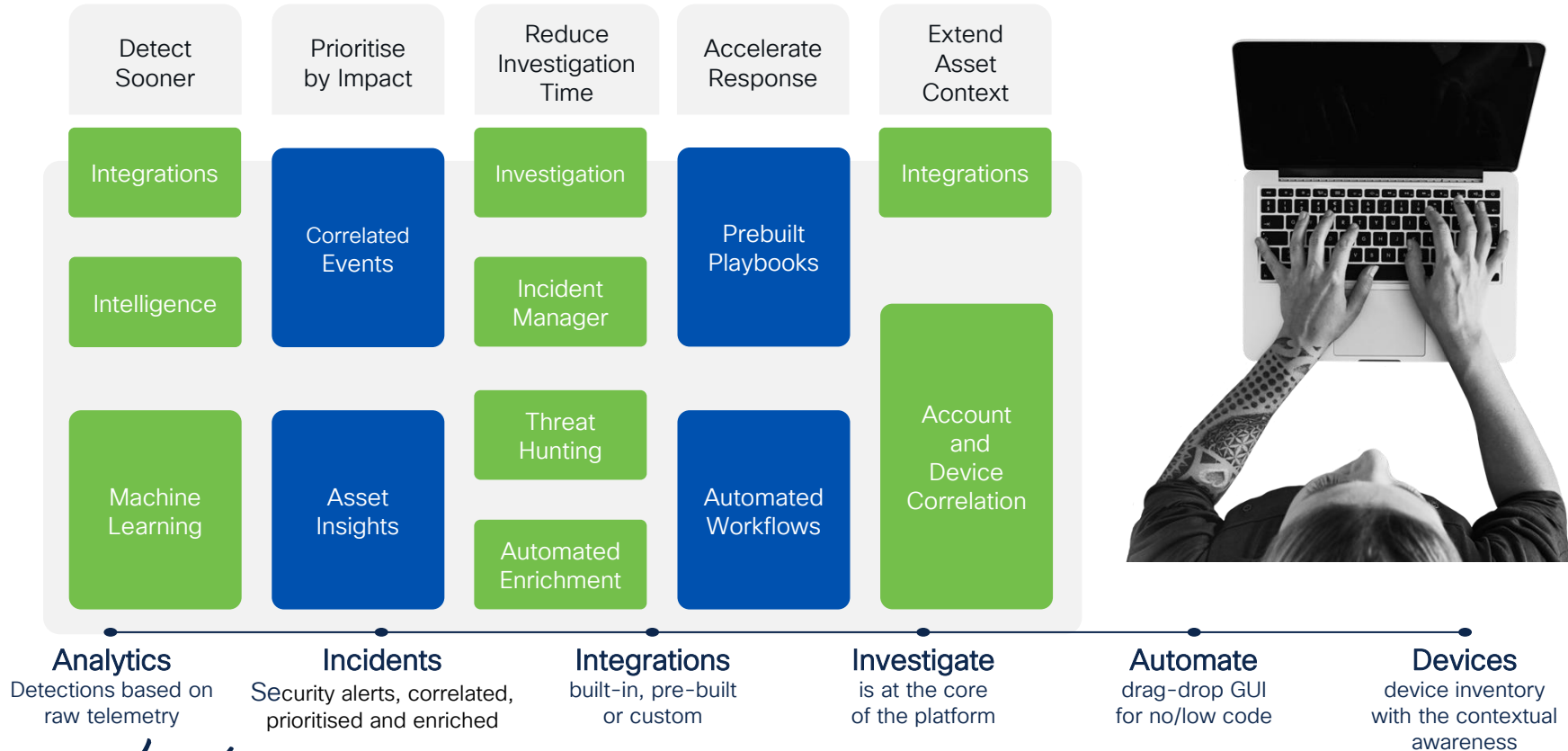
4

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

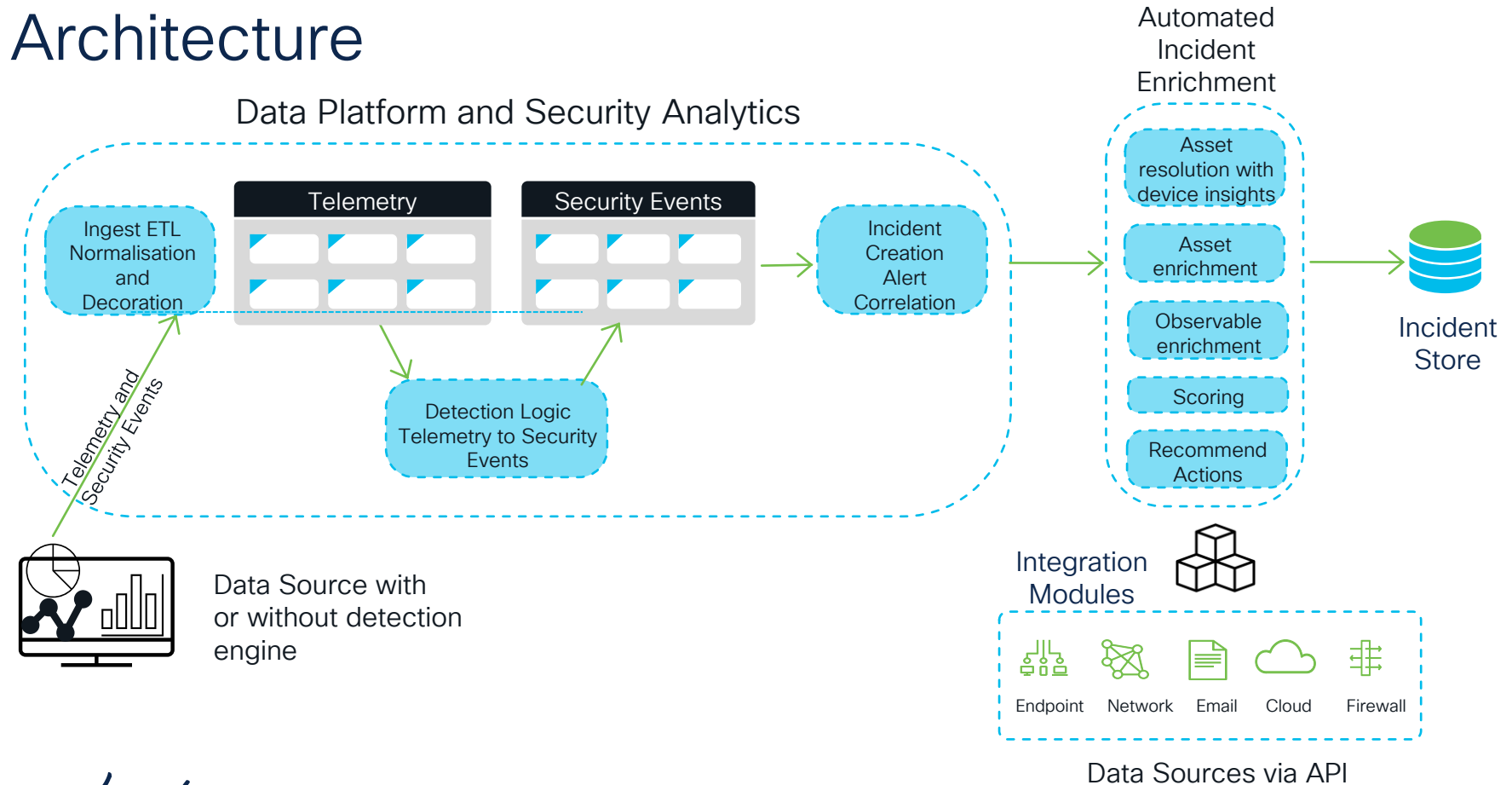
Do we have **full visibility** into all our assets? Can we **reliably identify** a device and who uses it?

5 Extend Asset Context

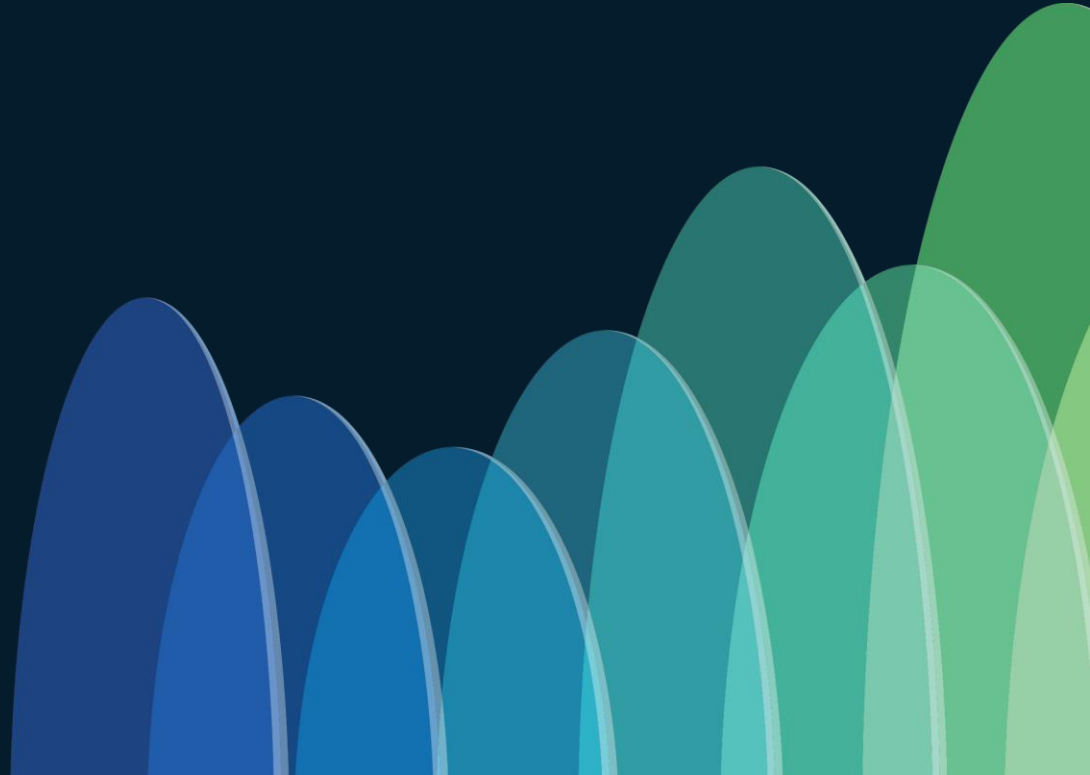
XDR outcomes and components



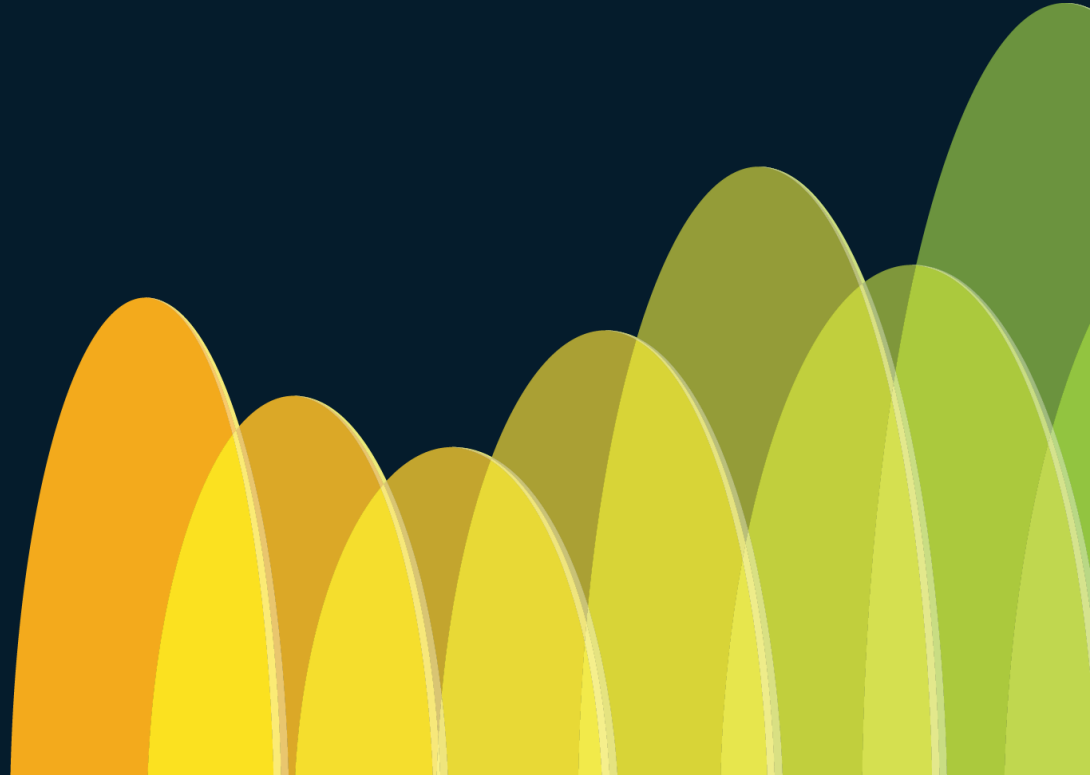
Architecture



Overview Demo

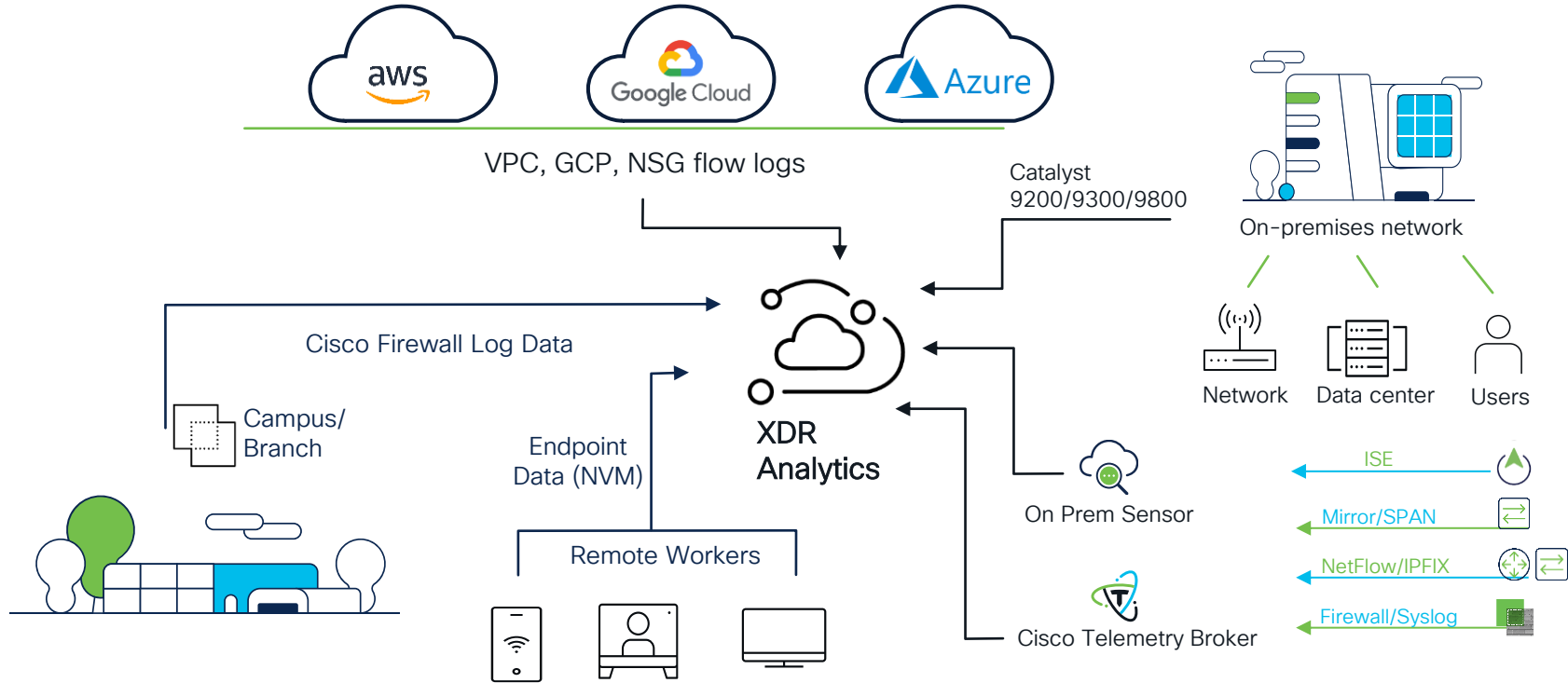


XDR Analytics



Raw Telemetry sources for XDR Analytics

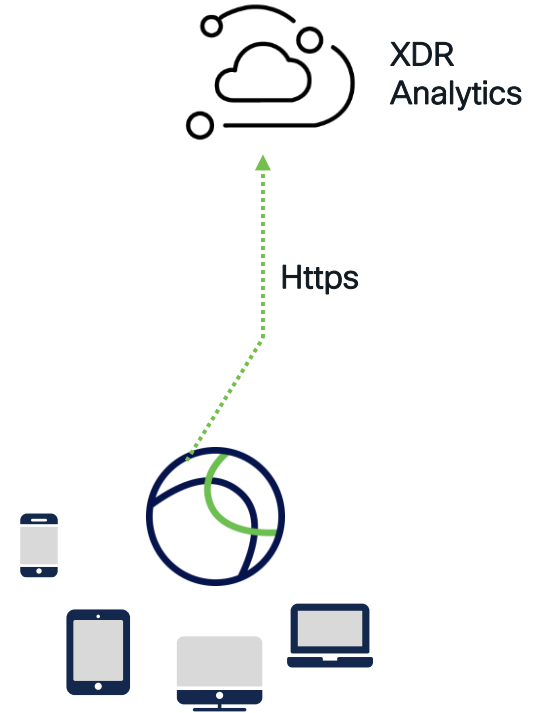
Flexible ingest for dynamic environments



NVM Data to XDR analytics

	Interface Info UID	Process Account*
	Interface Index	Process Account Type
	Interface Type	Process ID
	Interface Name	Process Name*
	Interface Details List	Process Hash*
	Interface Mac Addr.	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

Start Time*	UDID
End Time*	User
Source IP*	User Account Type
Source Port*	Agent Version
Destination IP*	Virtual Station Name
Destination Port*	OS Name
Bytes Sent*	OS Version
Bytes Received*	OS Edition
Packet Count* (derived)	System Manufacturer
Protocol*	System Type



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...

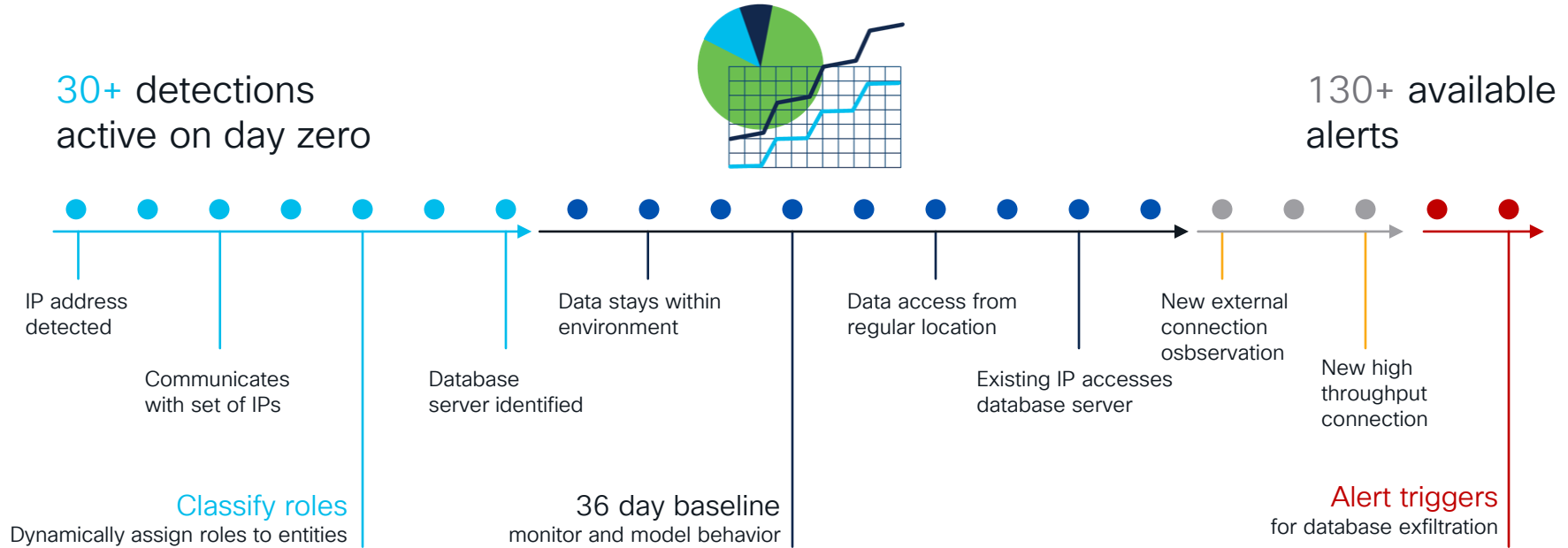


Firewall logging

- 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

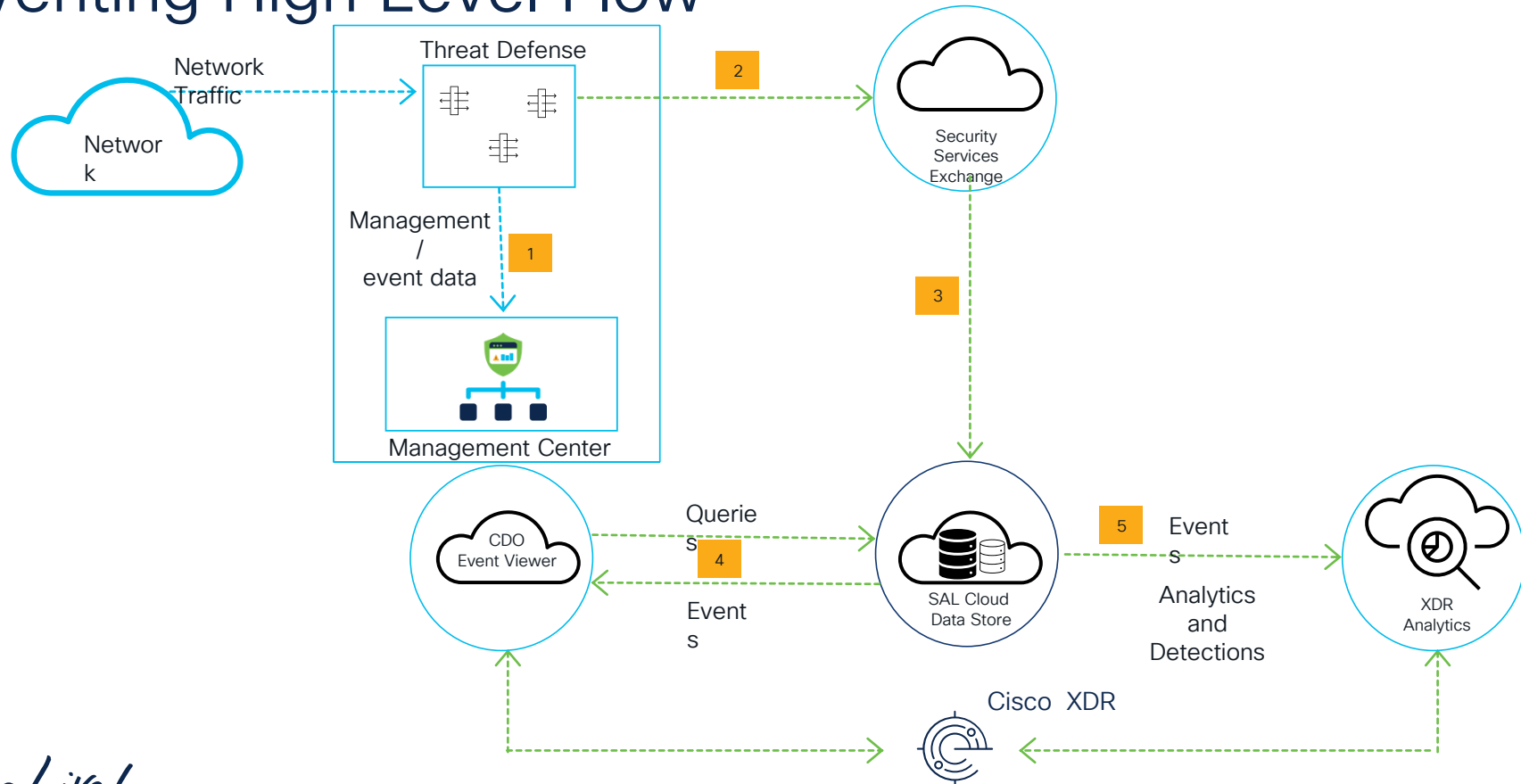


XDR Analytics detection and incident creation path

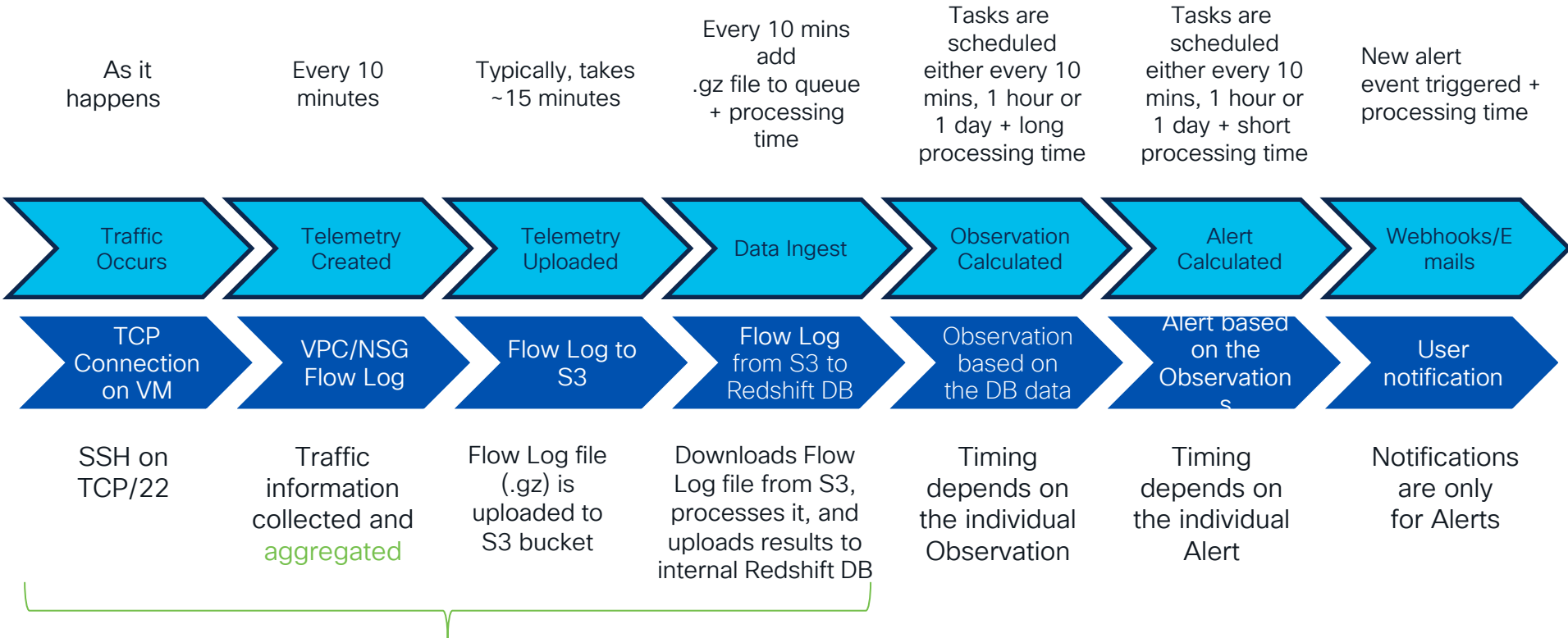


XDR Analytics covers end-to-end from raw telemetry to correlated, prioritised incidents which are enriched with context

Eventing High Level Flow



Flow Processing Fully Explained



Alerts with MITRE ATT&CK Tactics and Techniques

Single menu for all alert configuration

Alert Type	History	Priority	Enabled	Publish to Securonix	Telemetry	MITRE ATT&CK Tactics	MITRE ATT&CK Techniques
AWS Config Rule Violation 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	☐ Default Priority: Normal	☐ Default: Enabled	☐ AWS ARS	Persistence	Account Manipulation
AWS Console Login Failures This user tried 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	☐ Default Priority: Normal	☐ Default: Enabled	☐ AWS CloudTrail logs	Credential Access	Brute Force
AWS Detector Modified 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	☐ Default Priority: Normal	☐ Default: Enabled		Defense Evasion	Impact Information
AWS Domain Takeover 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	☐ Default Priority: Normal	☐ Default: Disabled		Initial Access	Compromise Information
AWS ECS Startup Script Modified An AWS ECS 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 execute malicious code.	1 Days	High	☐ Default Priority: Normal	☐ Default: Disabled		Persistence	Shell or Login Initialization
AWS ECS Credential Access An AWS ECS Task Definition was registered with a container command which will obtain credentials from the AWS Instance Metadata Service. This alert uses the AWS CloudTrail Event observation and may indicate an attacker is attempting to obtain service credentials.	0 Days	High	☐ Default Priority: Normal	☐ Default: Enabled		Persistence	Impact Internal Image
AWS IAM Anywhere Trust Anchor Created 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	☐ Default Priority: Normal	☐ Default: Enabled	☐ AWS CloudTrail logs	Persistence	Account Manipulation
AWS IAM User Takeover 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	☐ Default Priority: Normal	☐ Default: Disabled	☐ AWS CloudTrail logs	Persistence	Account Manipulation
AWS Inspector Finding 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	☐ Default Priority: Normal	☐ Default: Enabled	☐ AWS ARS	Persistence	Account Manipulation
AWS Lambda Invocation Spike An AWS Lambda function was spiked a record number of times. This alert uses the AWS Lambda Metrics: Outlier observation and may indicate operational problems or a denial of service attack.	14 Days	High	☐ Default Priority: Normal	☐ Default: Disabled	☐ AWS ARS	Impact	Resource Hijacking
AWS Lambda Persistence 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	☐ Default Priority: Normal	☐ Default: Enabled	☐ AWS CloudTrail logs	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

Understand how alerts map to MITRE Tactics and Techniques

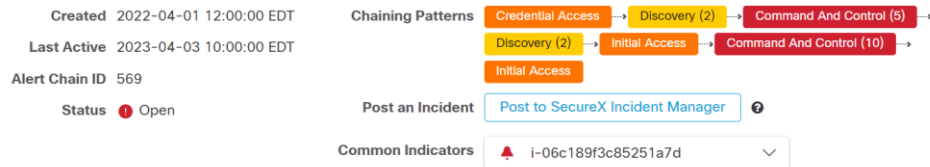
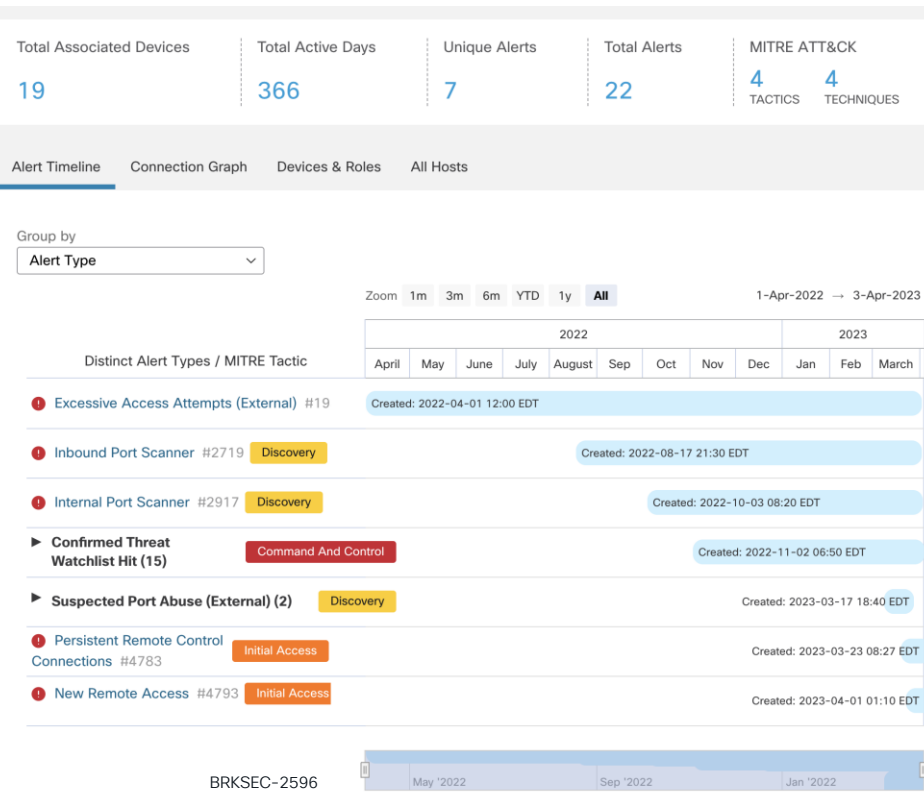
[XDR Analytics mapping to the MITRE ATT&CK Enterprise Matrix](#)

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

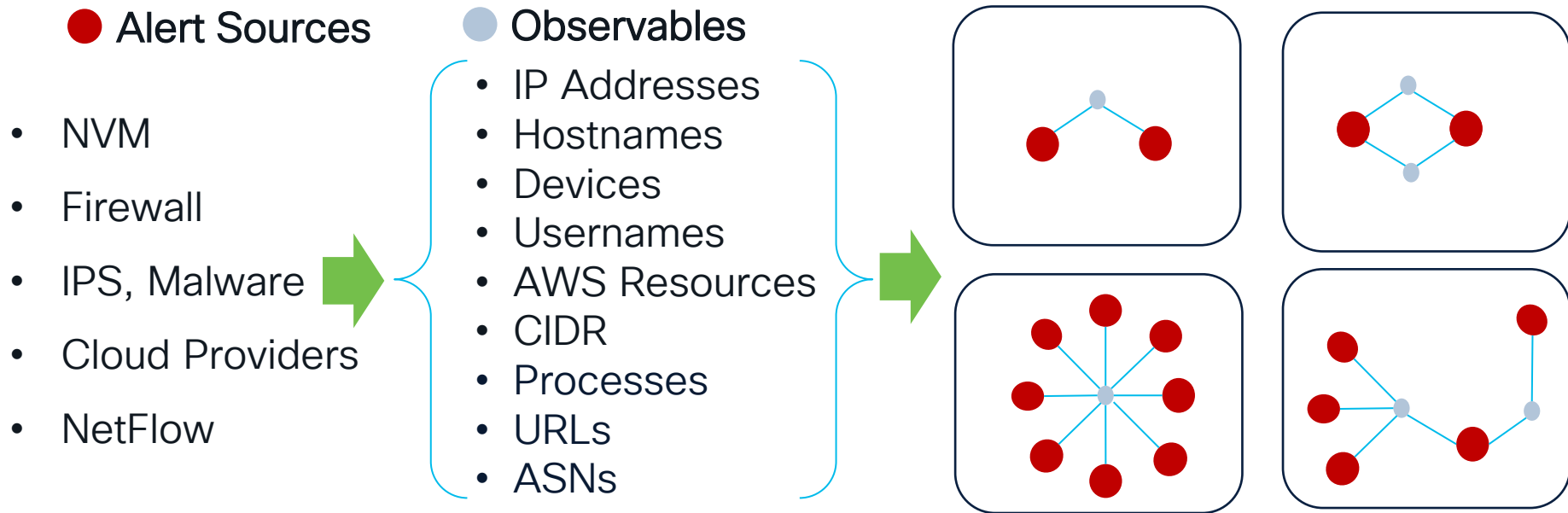
Alert Chains

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

Alert Chain at a Glance



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.

Incidents



Incidents

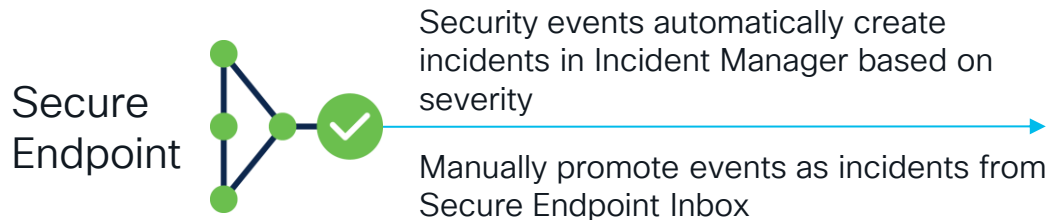
Prioritised Incidents based on severity

- Reduces clutter by prioritising 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, a search bar and filters are visible, showing '11 matching results' for the filter 'Status: Incident Reported'. The main table lists 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



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-ae8b-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.PossibleNamedPipeImpersonation.ioc 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** X

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 Manager 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"/>		<input type="text" value="Normal"/>	<input type="text" value="Enabled"/>	<input type="text" value="Enabled"/>	<input type="text" value="ETA"/>
Potentially Harmful Hidden File Extension 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	<input type="text" value="Normal"/> Default Priority: Normal	<input type="text" value="Enabled"/> Default: Enabled	<input type="text" value="Enabled"/>	<input type="text" value="ETA"/> <input type="text" value="Firewall"/>
Suspected Malicious URL 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	<input type="text" value="High"/> Default Priority: Normal	<input type="text" value="Enabled"/> Default: Enabled	<input type="text" value="Enabled"/>	<input type="text" value="ETA"/> <input type="text" value="Firewall"/> <input type="text" value="North-South"/>
Unusual File Extension from New External Server 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	<input type="text" value="Normal"/> Default Priority: Normal	<input type="text" value="Enabled"/> Default: Disabled	<input type="text" value="Enabled"/>	<input type="text" value="Firewall"/> <input type="text" value="North-South"/>

Configure severity and publication settings in
Secure Cloud Analytics

cisco *Live!*

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
Detection
Risk

10
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



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 ⓘ

High

* TLP Value ⓘ

amber

Incident Description ⓘ

Meraki Security Event: IDS Alert Priority 1 for [\${activity.Remove port from IP address.output.Script Queries.source_ip\$} @ [\${activity.For Each Security Event.input.Source Array[@].ts\$}]

Please check sightings tab and below for more information.

Message: [\${activity.For Each Security Event.input.Source Array[@].message\$}]

Meraki Rule ID: [\${activity.For Each Security Event.input.Source Array[@].ruleid\$}]

Action taken: [\${activity.For Each Security Event.input.Source Array[@].action\$}]

* Incident Status ⓘ

New

* Incident Title ⓘ

Meraki Security Event: IDS Alert Priority 1 for [\${activity.Remove port from IP address.output.Script Queries.source_ip\$} @ [\${activity.For Each Security Event.input.Source Array[@].ts\$}]

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 ⌵

1000

100 Detection Risk

10 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](#)

Prioritise by impact

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

1000

100

Detection
Risk

10

Asset
Value at Risk

Incidents			
62 Incidents		33 New Incidents	8 Open Incidents
<input type="text" value="Search"/> 62 matching results Filters			
☐	Priority	Name	Source
☐	1000	Malicious Process and Suspicious SMB/RDP Activity - Doc Test Do ...	Cisco Secure Clou...
☐	1000	Unusual External Server for This is localhost	Cisco Stealthwatc...
☐	1000	AWS Inspector Finding for This is localhost	Cisco Stealthwatc...
☐	1000	Command and Control DNS Activities	Umbrella
☐	928	Formula Test.Mar27.Critical.TTP(58).AssetValue[8]	FormulaTest
☐	928	F1.03-06d.Critical.TTP(58).AssetValue[10]	FormulaTest
☐	835	Attack Graph Test - 109 Observables	FormulaTest
☐	800	F1.03-06a.Critical.TTP(50).AssetValue[NULL]	FormulaTest
☐	765	New Internal Device for This is localhost	Cisco Stealthwatc...
☐	765	Azure Permissive Security Group for TD&R RSA	Cisco Secure Clou...
☐	742	F1.03-08.Critical.TTP(58).AssetValue[8]	FormulaTest

Identify the most impactful incidents based on risk

1000

100

Detection
Risk

10

Asset
Value at Risk

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

0-1000 0-100 0-10

The Incident total priority score used to prioritise 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

TA0008: Lateral Movement 66

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.

Orientation

```
graph LR
    NT[NT AUTHORITY\SYSTEM] --- C[C:\Windows\System32\svchost.exe]
    NT --- S[System]
    NT --- DO[do-2.org1.net]
    NT --- VM[virtualmachines/w...]
    S --- DO
    S --- VM
    DO --- VM
    DO --- IO[10.0.1.6]
    IO --- VM
    VM --- SV[svchost.exe]
    VM --- SYS[SYSTEM]
```

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

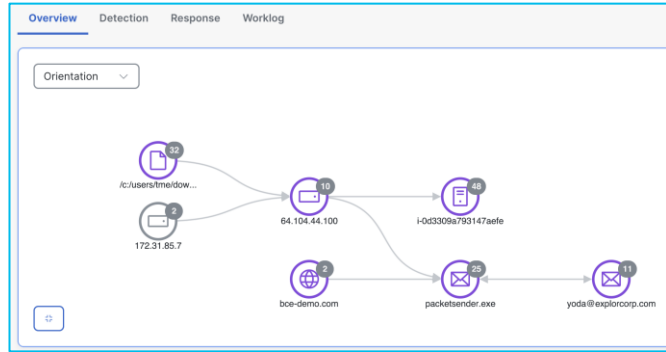
NT AUTHORITY\SYSTEM

C:\Windows\System32\svchost.exe

svchost.exe

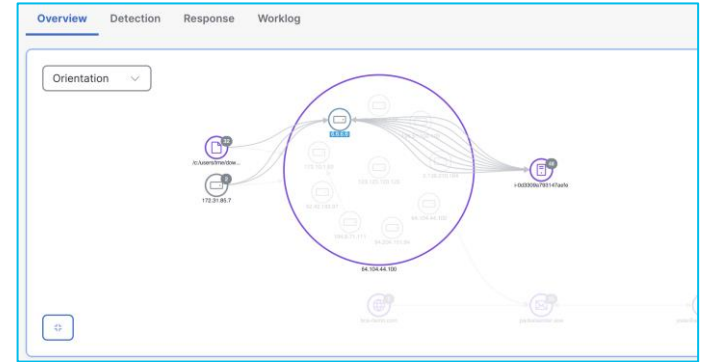
SYSTEM

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...	6 events
i-0e682308df7f7bf0a	41 events	1bf529e3f6bff6d974443...	118 events	Remote Access	
i-0d3309a793147aefe	26 events	94.204.151.84	16 events	Cisco Secure Cloud Analytics (cisco-explor...	3 events
EC2AMAZ-AHQFEJR	18 events	64.104.44.100	6 events	User Watchlist Hit	
EC2AMAZ-MTKLEVO	13 events	3.136.210.164	5 events	Cisco Secure Cloud Analytics (cisco-explor...	3 events
				Watchlist Interaction	
				Cisco Secure Cloud Analytics (cisco-explor...	3 events
				Geographically Unusual Remote Acc...	

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 screenshot displays the Cisco Security Center interface, specifically the Detection tab. The main table lists incidents with columns for First Seen, Severity, Source, Indicators, and Observables. To the left, there are filters for Status (All, Original, Investigated) and Severity (All, Critical, High, Medium, Low, None, Unknown, Info). Below the table, a 'Source' filter dropdown is open, showing a list of sources including Secure Email Threat Defense, Cisco Secure Cloud Analytics, AMP Event, Secure Endpoint, Cisco Secure Network Analytics, CESA/NVM, and NGFW Event Service. To the right, a sidebar shows 'Relations', 'Indicators', 'Assets', and 'Observables' for the selected incident. A blue button at the bottom center reads 'Drill down into Detection Details'.

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	

Relations

- 172.10.1.63 Connected to 6.6.6.6

Indicators

- NGFW Event Service
- Security Intelligence event - IP_ReputationSL_Category - ExplorCorp_Malicious_IPs
- ExplorCorp_Malicious_IPs

Assets

- 172.10.1.63

Observables

- 172.10.1.63
- 6.6.6.6

Source Filter:

- ☐ 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.

Walk through incidents step-by-step – Response

The interface shows a series of steps in the 'Response' tab, each with a description and an 'Add Note' button:

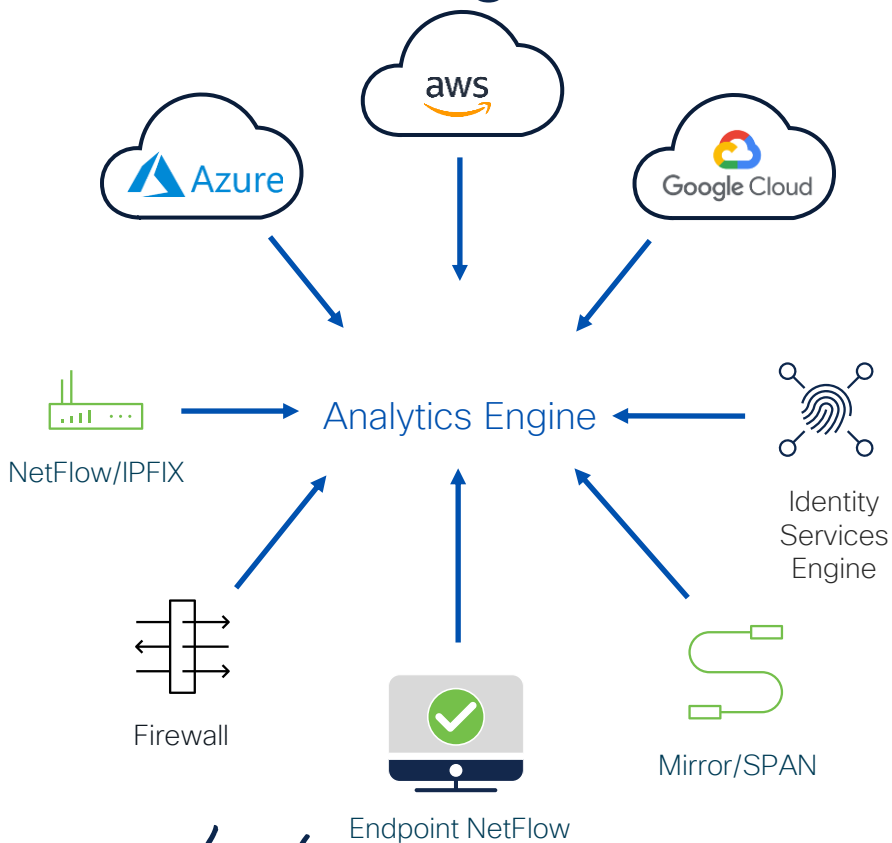
- Review Incident**
Add a note to record the evidence (indicators and reasoning) that supports the decision for assigning a status of Rej...
- Identify Affected Hosts**
Add note with summary of findings on the investigations of hosts found with malicious indicators
- Mitigate or Remediate Vulnerabilities**
Add a note on what are the affecting vulnerabilities linked to the incident and how mitigations or remediation is going...
- Remove Malicious Content**
Add a note on the action achieved to ensure the removal of the malware.
- Validate Eradicated Hosts**
Confirm and acknowledge eradication steps are working as expected and number of infected host(s) is dropping.
- Validate Restored Hosts**
Validate that each re-imaged system was completed by verifying new image creation date
- Implement Recovery Monitoring**
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.

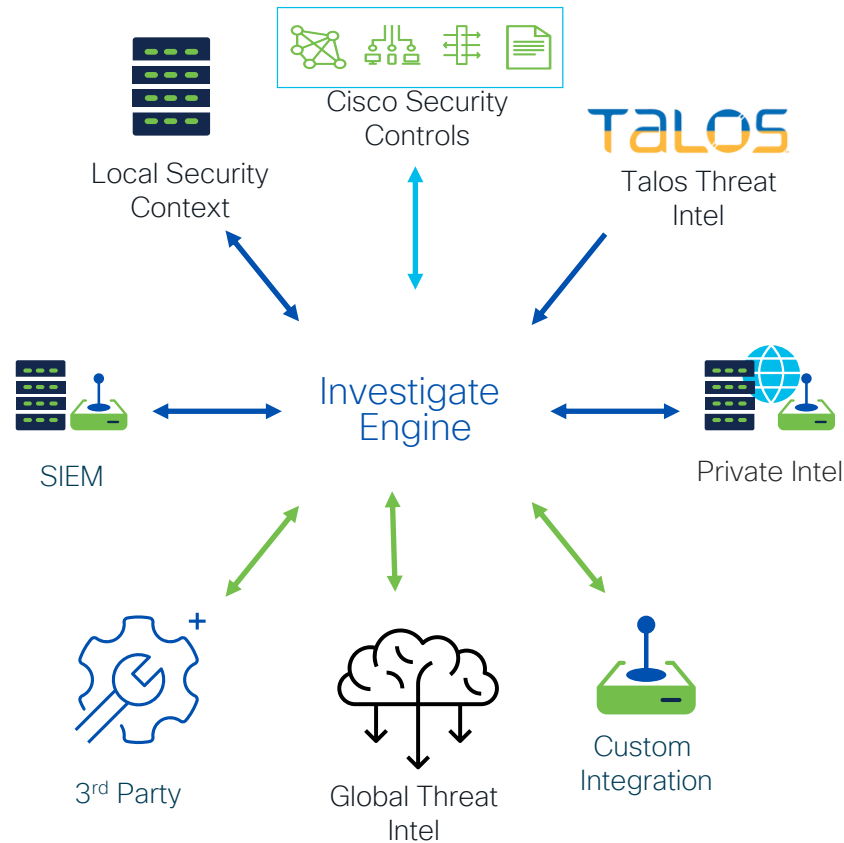
Integrations (Data Ingestion and API Enrichment)

Data Ingestion

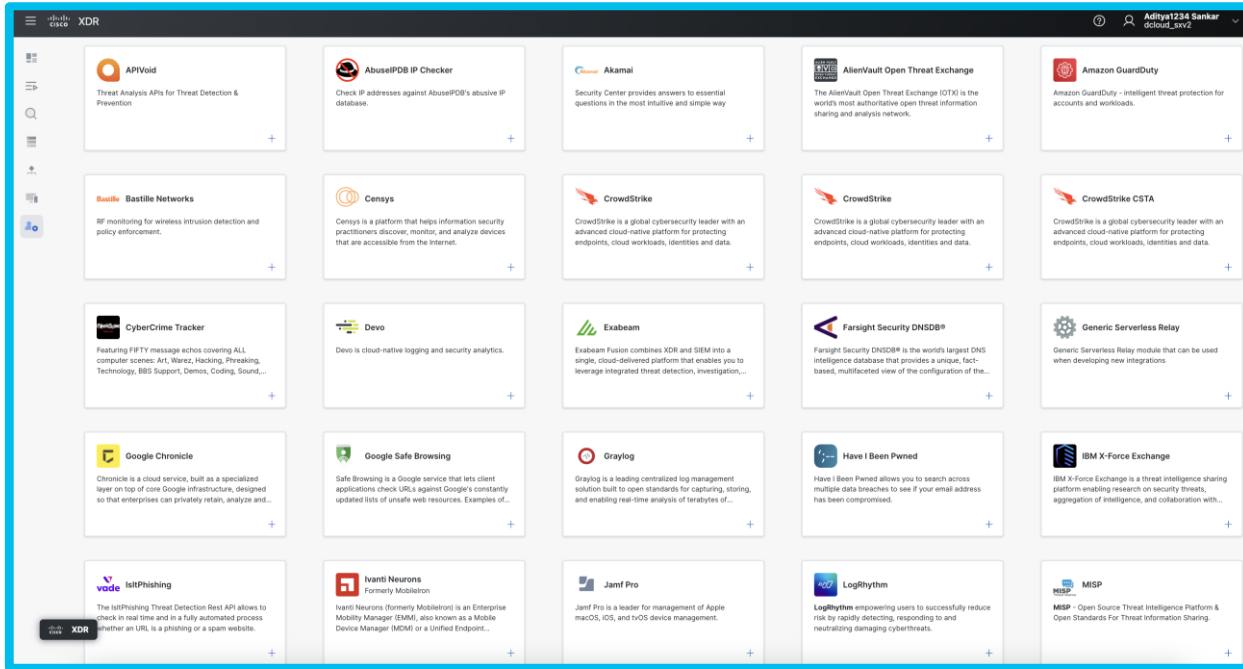


CISCO Live!

API Enrichment



Integrations for partner technologies



XDR Integrations API enrichment

*Community/open source

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

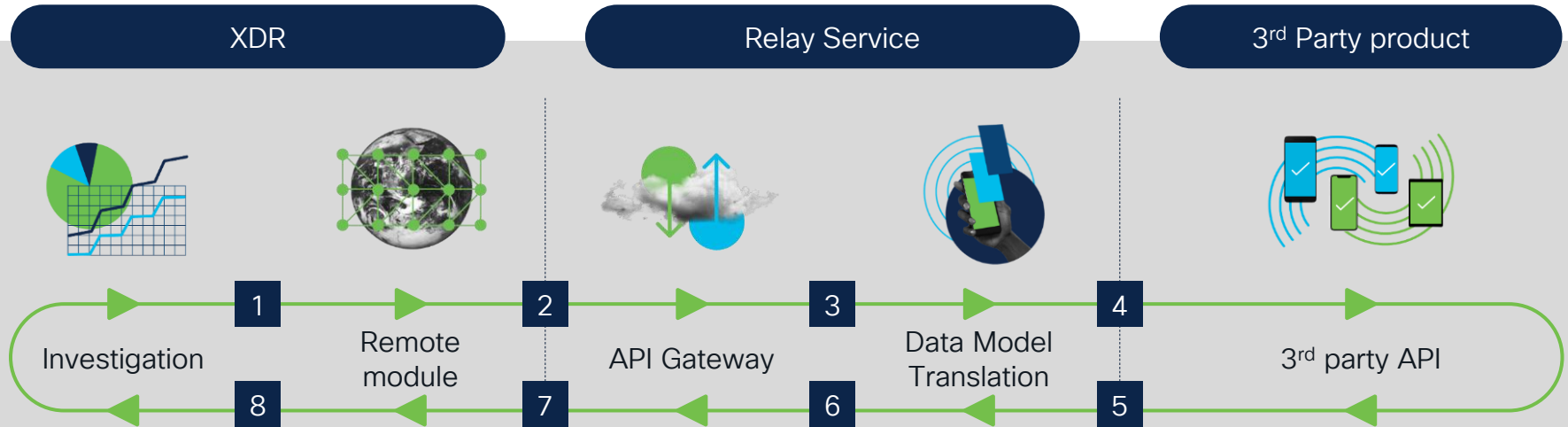
- Many available by default (examples below)
- [Write your own!](#)
- Templates and examples available on Github

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

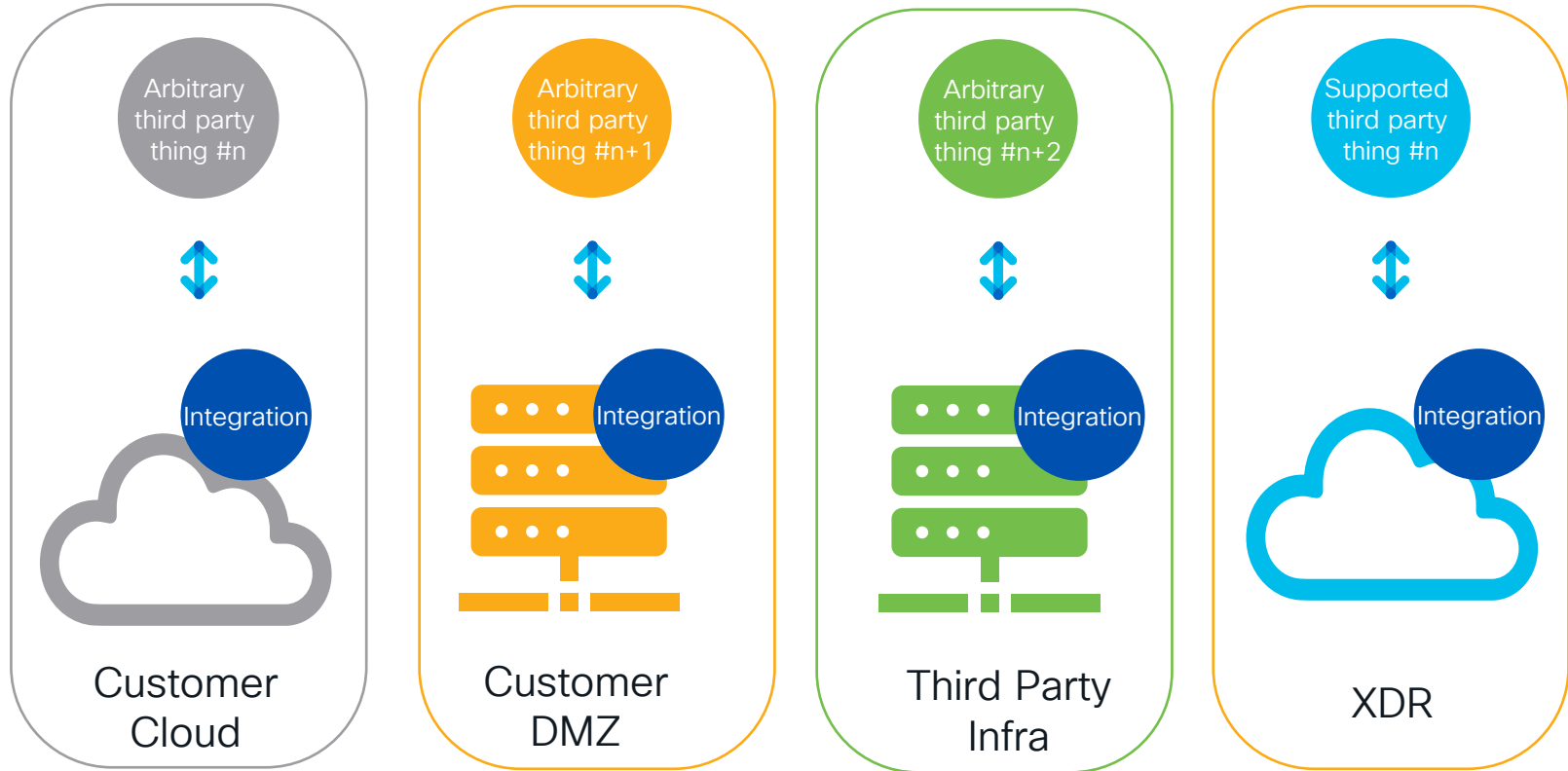
Relay API

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

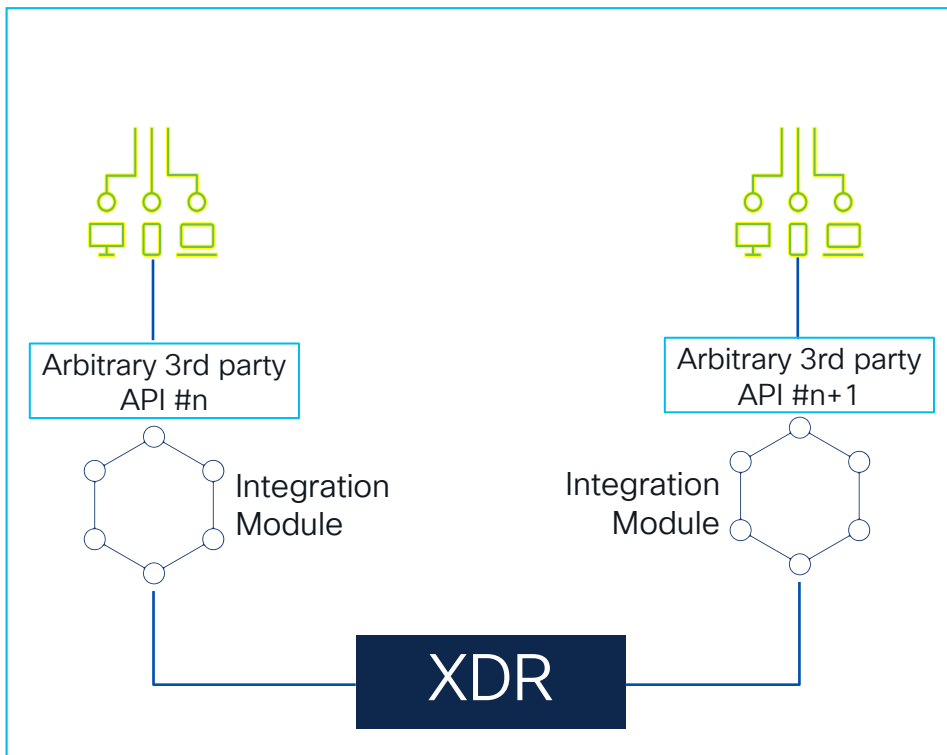
Bundle builder - <http://cs.co/bundle-builder>



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
fd4dfc8878f39424920d469bcd05060a6f7c95794...	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 ↗

Secure Malware Analytics

Browse 75.75.75.75 ↗

Search 75.75.75.75 ↗

Secure Network Analytics 7.4.2

Host Report ↗

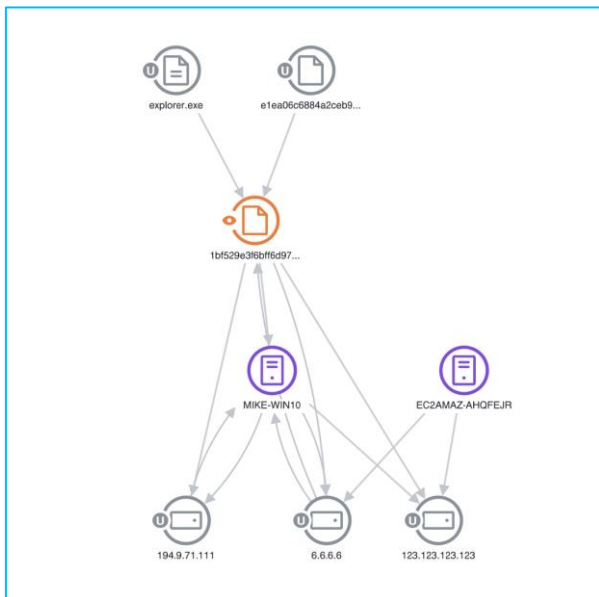
SecureX Orchestrator

- ▶ 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

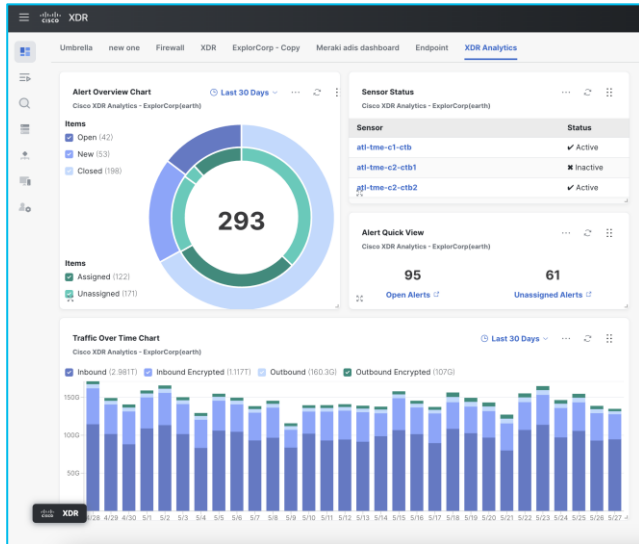
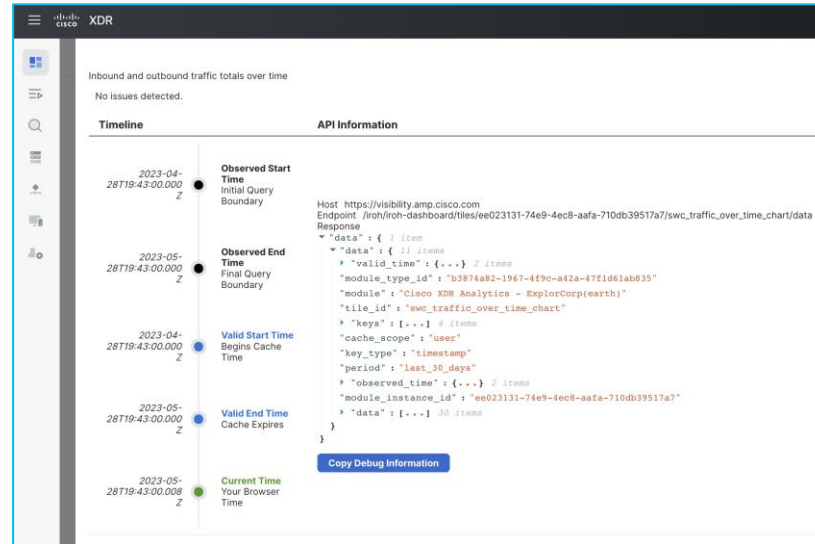
tiles/tile-data

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({})
```

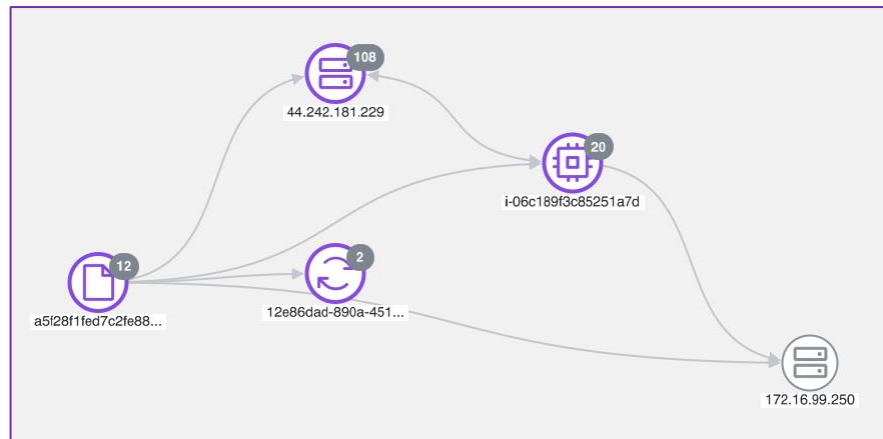


Investigate



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		Zoom	1d	3d	7d	15d	YTD	1y	All	15-May-2023	→	24-May-2023
		2023										
		May										
Internal Port Scanner	#11916	Discovery	Created: 2023-05-15 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?

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

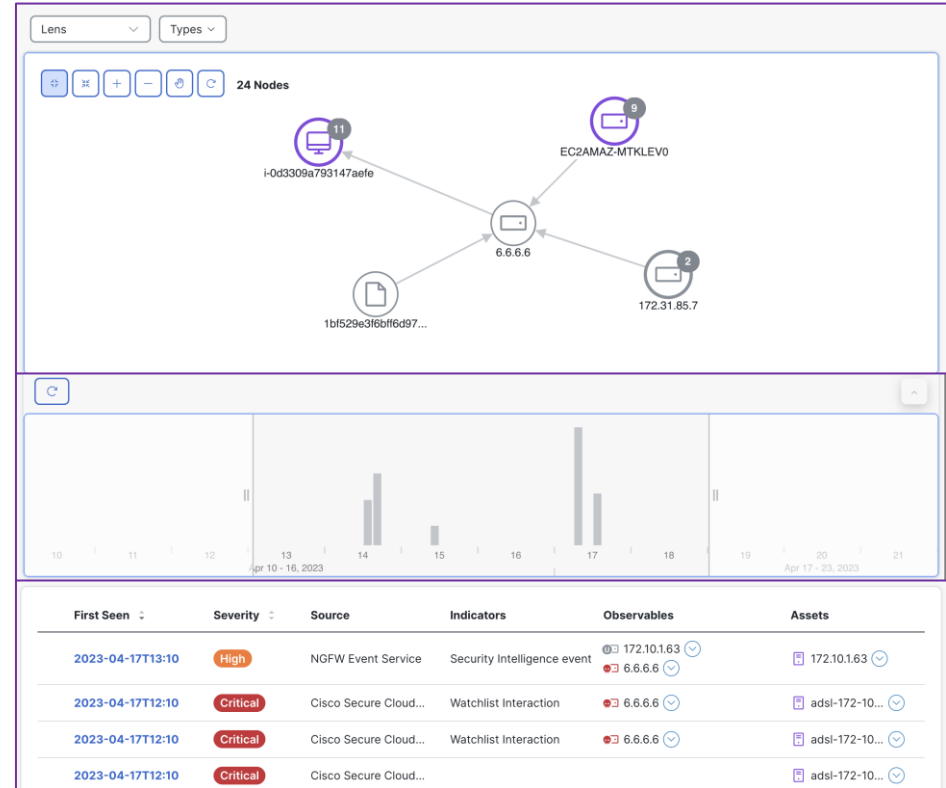
Isolate hosts

What can I do about
it right now?

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

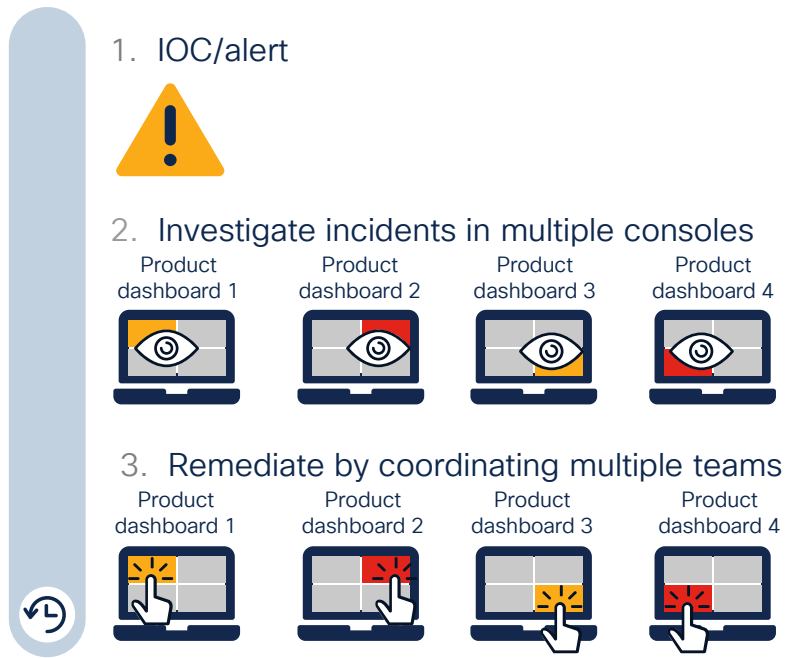
Accelerate investigation With Cisco XDR

- Aggregate and query global intel and local context in one view
- Visualise 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

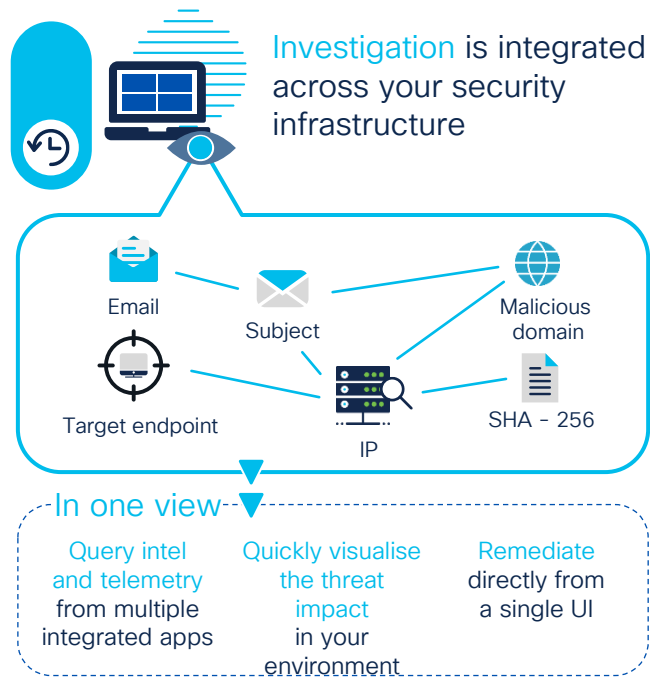


How true simplicity is experienced

Without XDR: ~32 minutes

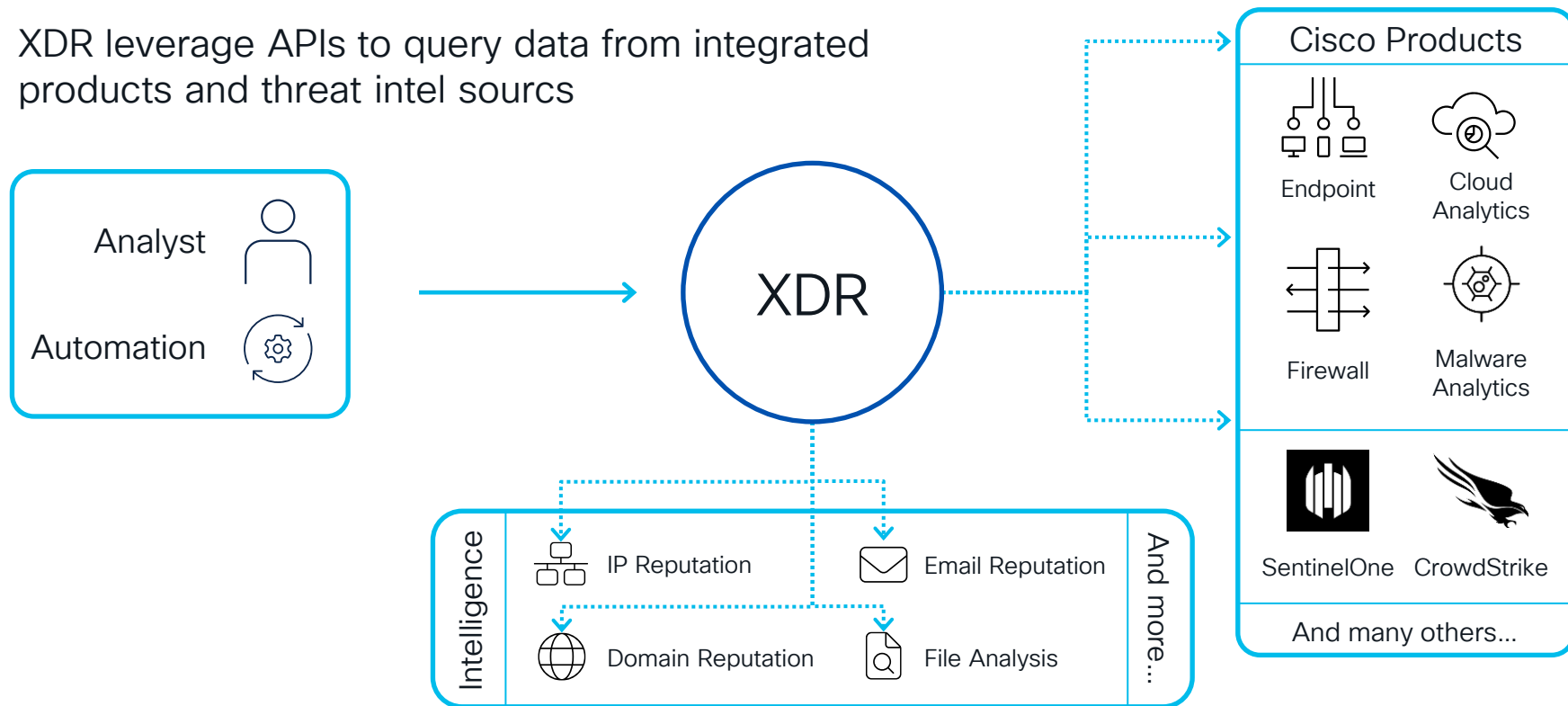


With XDR: five minutes



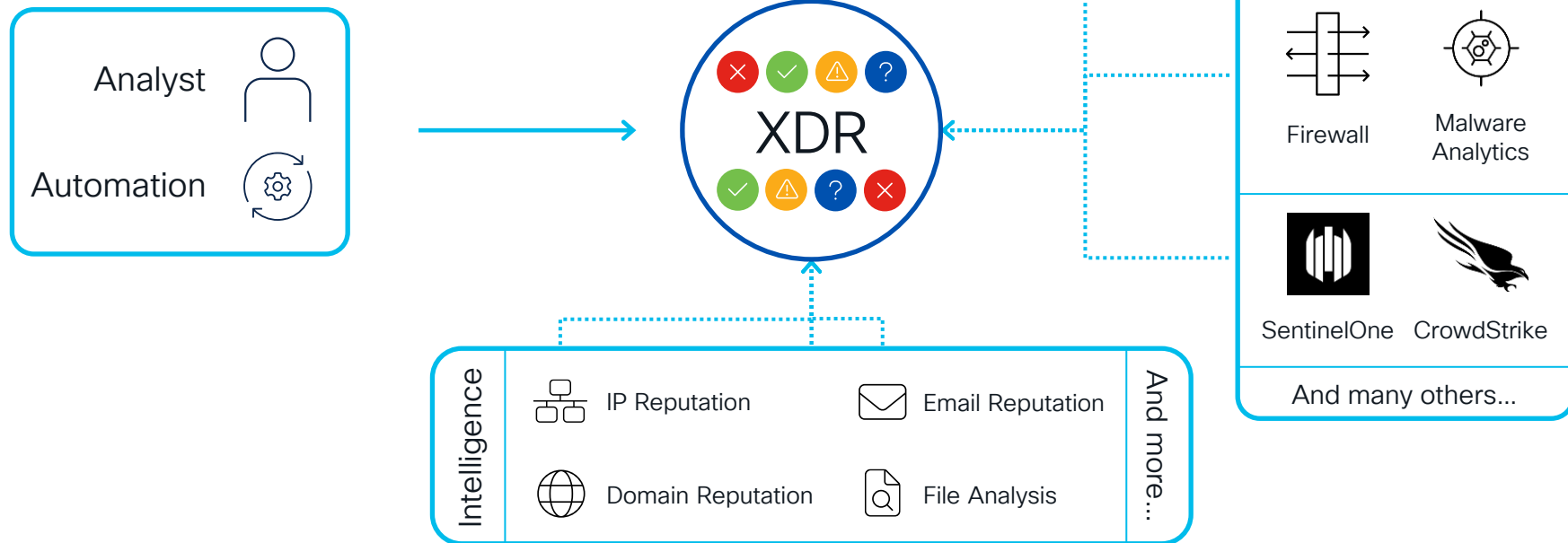
Investigation query integration and threat intel

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

INSPECT ^

POST /iroh/iroh-inspect/inspect return extracted observables from some raw text ^ 🔒

[required scopes:](#) inspect:read

Parameters Try it out

Name	Description
StrContent ★ required	
object (body)	<div>Example Value Model</div> <pre>{ "content": "string" }</pre> <div>Parameter content type</div> <div>application/json ▼</div>

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

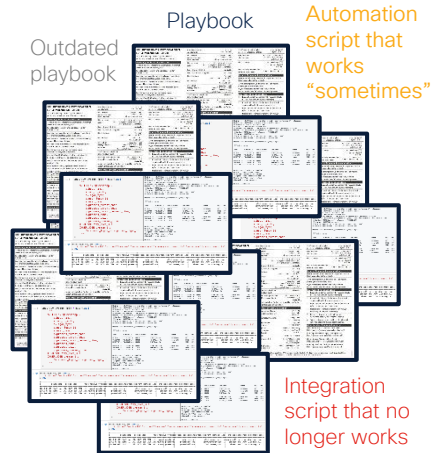


Scale

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

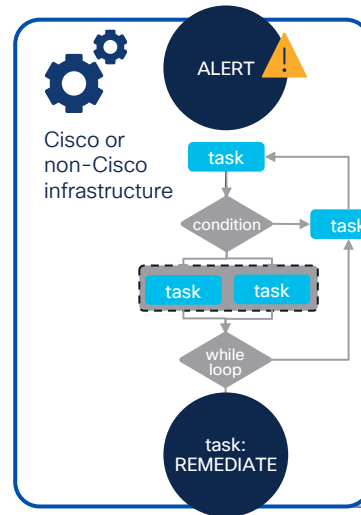
Maximising operational efficiency

Before: Repetitive, human-powered tasks



Solution: Orchestrating security across the full lifecycle

Pre-built or customisable workflows



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

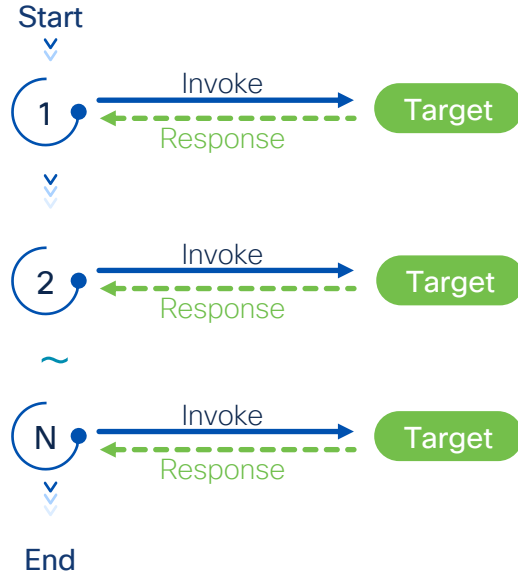
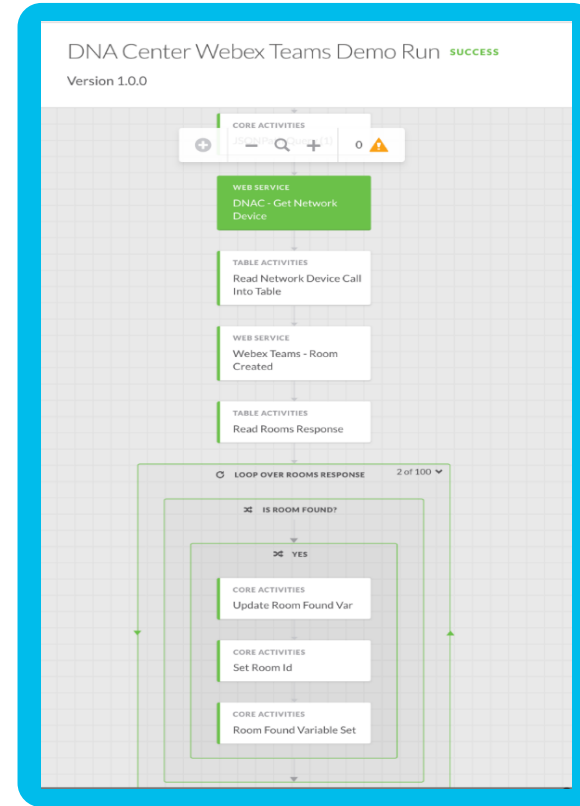
“

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



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 customisable.

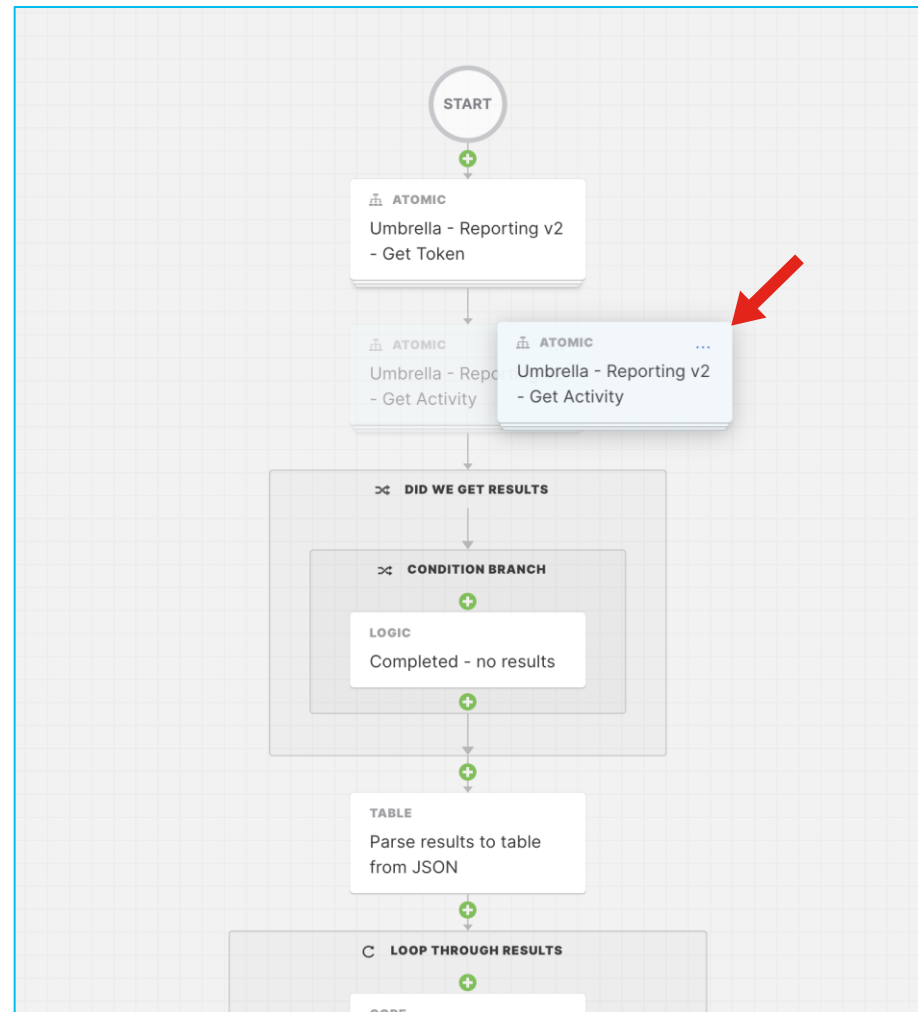
Remotes

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

What is a workflow?

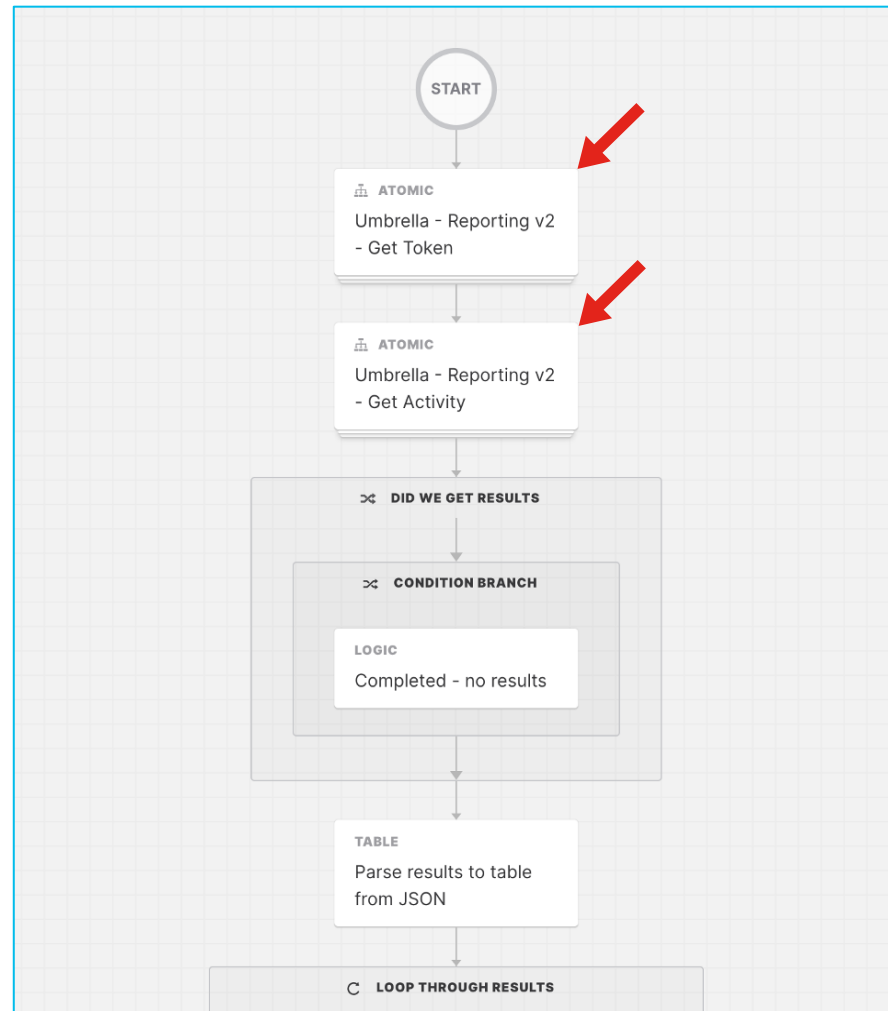
Simple or complex series of actions that accomplish a specific outcome.

- 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



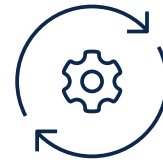
Response

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



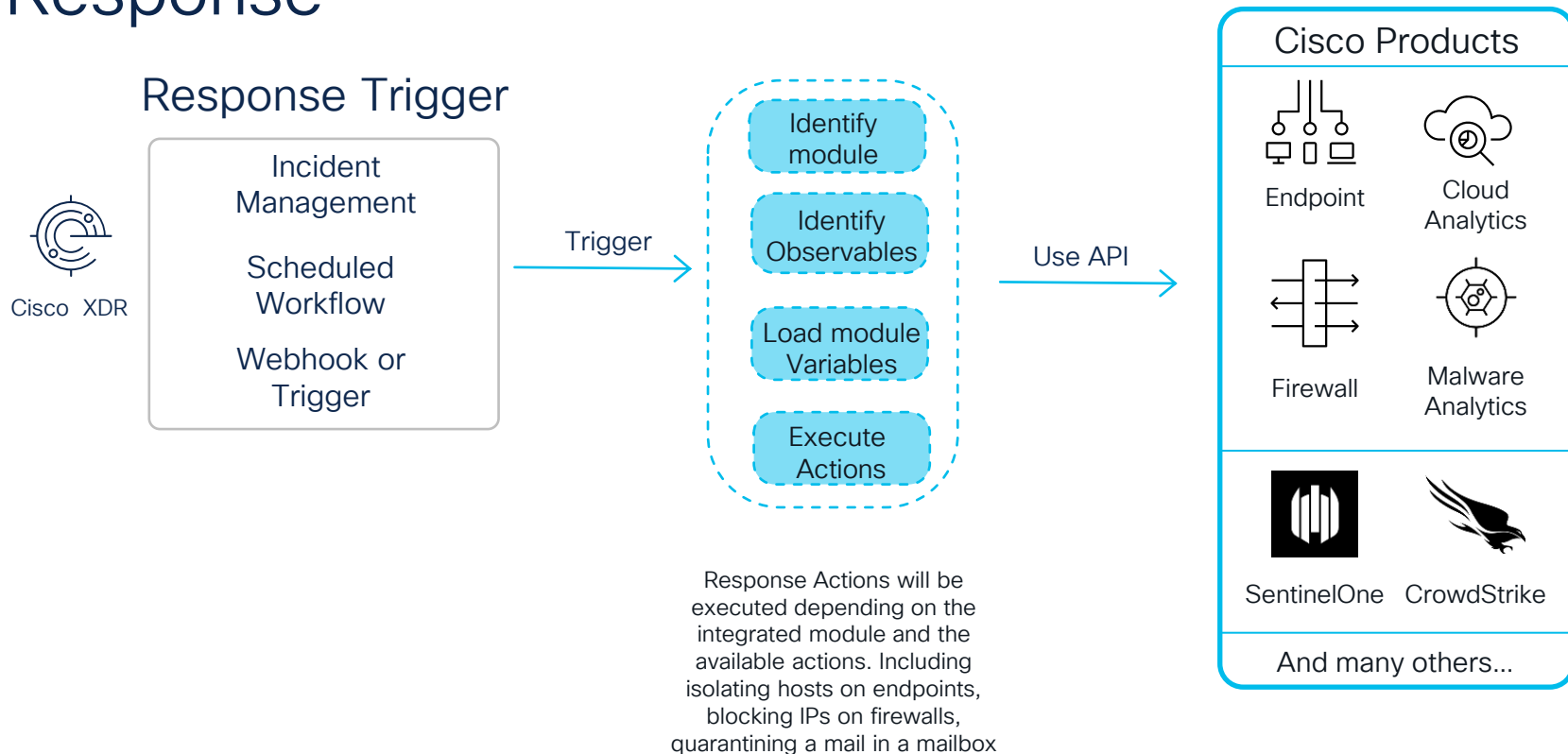
Eradicate



Recover

Identification	<div>▼ Identify Affected Hosts Add Note</div> <div>Add note with summary of findings on the investigations of hosts found with malicious indicators</div>
Containment	<div>▼ Contain Incident: Overview Add Note</div> <div>Overview of how to contain Indicators of Compromise to stop the spread of malicious activity</div>
Eradication	<div>^ Contain Incident: Assets Select</div> <div>Use asset-based containment to stop the spread of malicious activity.</div> <div>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.</div>
Recovery	<div>▼ Contain Incident: IPs Add Note</div> <div>Contain IP indicators of compromise to stop the spread of malicious activity</div>
	<div>▼ Contain Incident: Domains Select</div> <div>Contain domain indicators of compromise to stop the spread of malicious activity</div>
	<div>▼ Contain Incident: URLs Select</div> <div>Contain URL indicators of compromise to stop the spread of malicious activity</div>
	<div>Back Go to Eradication →</div>

Response



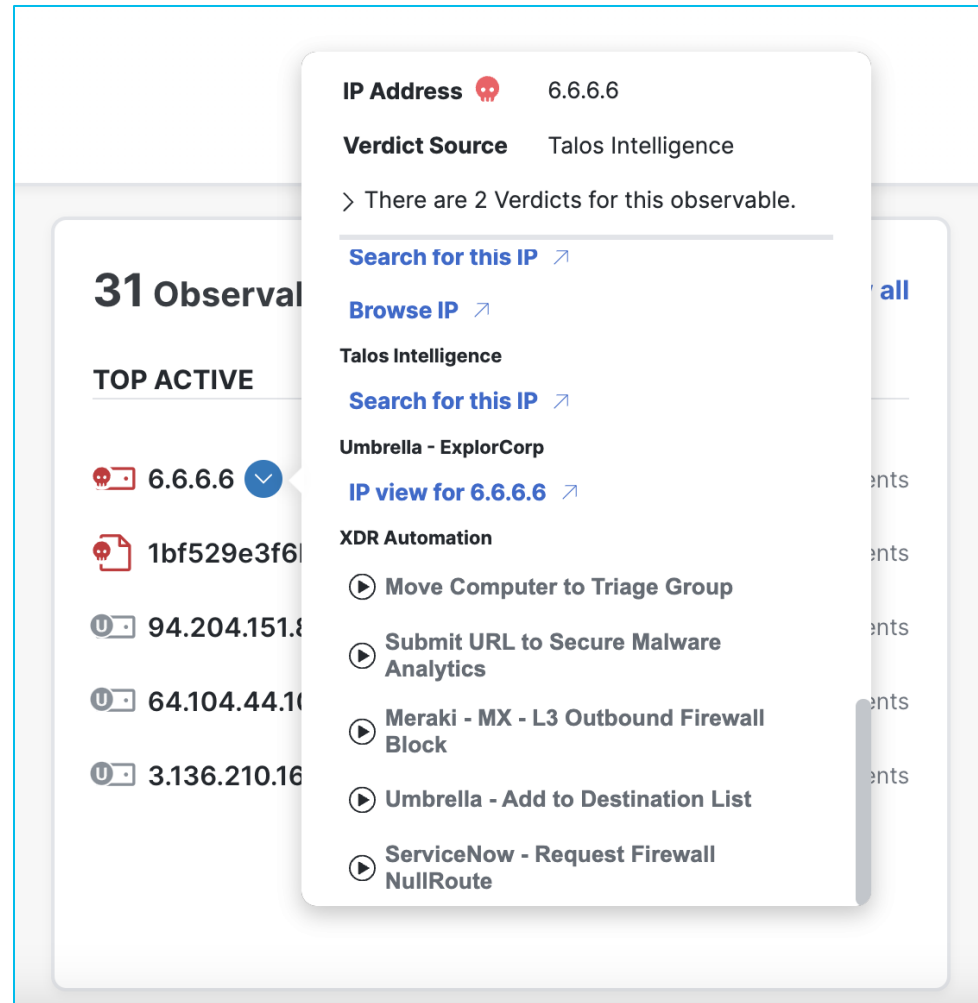
Pivot menu

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



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

Type

Q Search



Select



[Reset All](#)

Display name

On/off

Description

Incident notifications to Webex



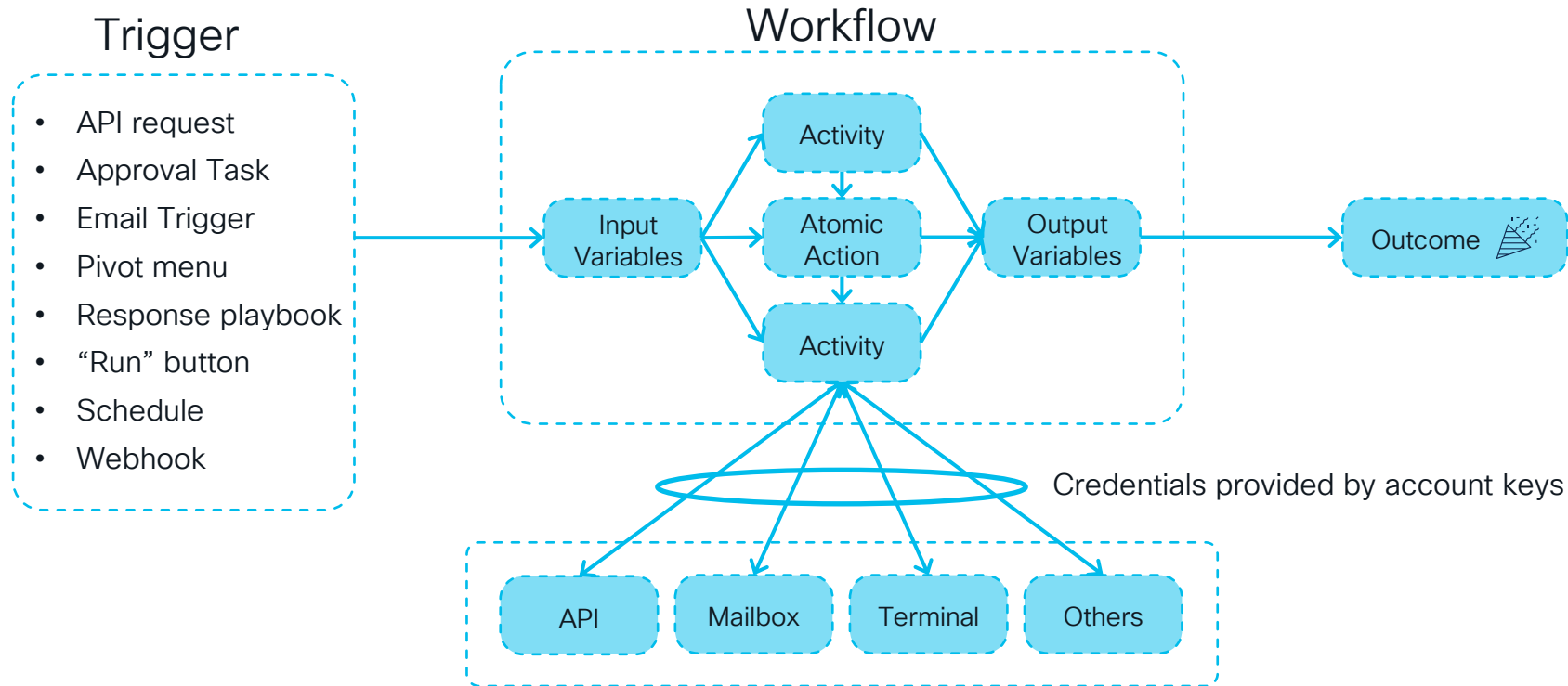
Check for Talos blog posts



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

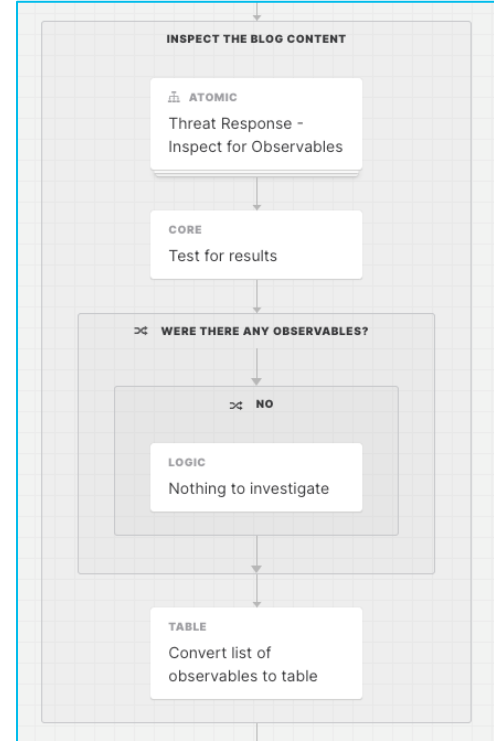


Automation, with the click of a button

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 displays the 'Exchange' section of a workflow ecosystem. At the top, a header reads 'Exchange' followed by a description: 'Exchange allows you to find and install workflows that have been approved by Cisco engineers and content providers.' Below this is a search bar with a magnifying glass icon and the text 'Search', and a category dropdown menu currently set to 'All'. The main content area is divided into two sections: 'Popular' and 'All Workflows'. The 'Popular' section features two workflow cards. The first card is titled 'Talos - Blog Post To SecureX Casebook' and includes an 'Xchange' icon. Its description states: 'Takes a Talos blog post, conducts an investigation into it using Cisco Threat Response, and then puts the results in a SecureX casebook. I...'. It has 'Learn More' and 'Installed' buttons. The second card is titled 'Threat Response Phishing Investigation' and also includes an 'Xchange' icon. Its description states: 'This workflow monitors a mailbox for incoming phishing reports. When an email is received, the workflow investigates its attachments and a...'. It has 'Learn More' and 'Install' buttons. The 'All Workflows' section features two more workflow cards. The first card is titled 'Azure AD - Get Blocked Sign-Ins (Locked...)' and includes an 'Xchange' icon. Its description states: 'This workflow checks for sign-ins that were blocked because the account was locked out in Microsoft Azure (error code 50053). If any result...'. It has 'Learn More' and 'Install' buttons. The second card is titled 'Azure AD - Get New Users' and includes an 'Xchange' icon. Its description states: 'This workflow checks for users that were created within the past X hours in Microsoft Azure (the timeframe is configurable). If any result...'. It has 'Learn More' and 'Install' buttons. A third card titled 'Duo - Investigate User' is partially visible at the bottom, also including an 'Xchange' icon.

Workflows and atomics

- Shows all the organisation'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 shows the 'All Workflows' tab with 28 workflows. The interface includes a search bar, filters for 'Ready State' and 'Category', and a 'Reset All' button. The workflow cards are arranged in a grid. Each card displays the workflow name, a brief description, a status indicator (e.g., 'Validated', 'Updated'), and a star icon for favoriting. The workflows shown include 'Umbrella - Search DNS Activity b...', 'Secure Firewall - Incident Monit...', 'Check for Umbrella Security Even...', 'Submit URL to Secure Malware Ana...', 'Talos - Get New Blog P...', and 'XDR - Contain Incident: Assets'.

The screenshot shows the 'All Workflows' tab with 28 workflows in a list view. The interface includes a search bar, filters for 'Ready State' and 'Category', and a 'Reset All' button. The workflow list is displayed with columns for 'Display name', 'Categories', 'Status', and 'Owner'.

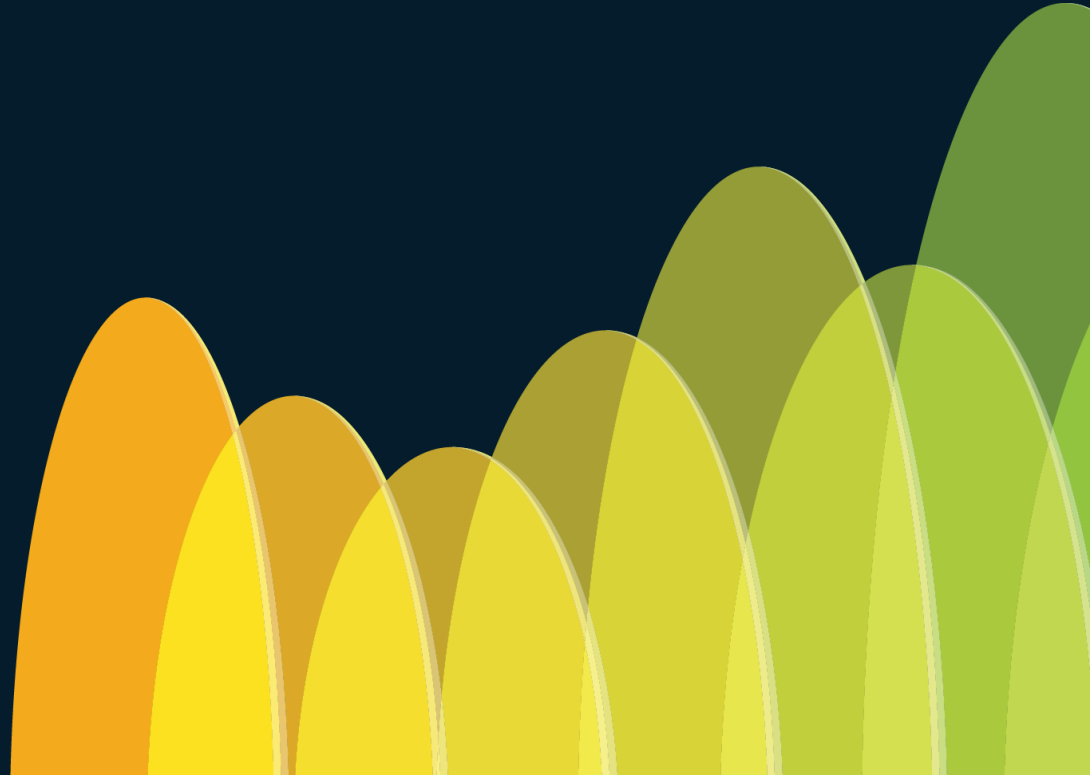
Display name	Categories	Status	Owner
Umbrella - Search DNS Activity b... This workflow searches and returns Cisco...		Validated	user@cisco.com
Secure Firewall - Incident Monit... This workflow fetches Cisco Secure Firewall...		Updated	user@cisco.com
Check for Umbrella Security Even... This workflow searches 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



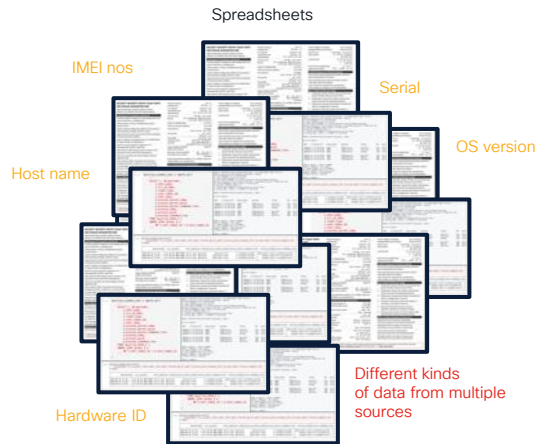
Configuration and management of Cisco Secure Client

Cloud-based management of Secure Client profiles and deployments

Gain contextual insights into your devices

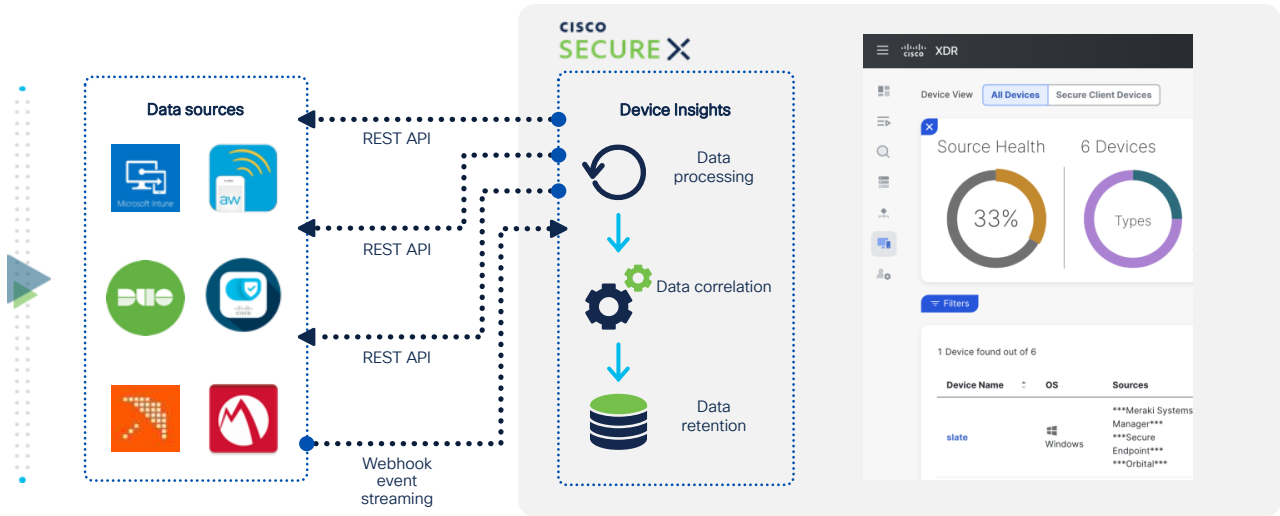
Before:

Multiple spreadsheets, no combined view of the denominator



Solution:

Comprehensive device inventory all in one place!



After:

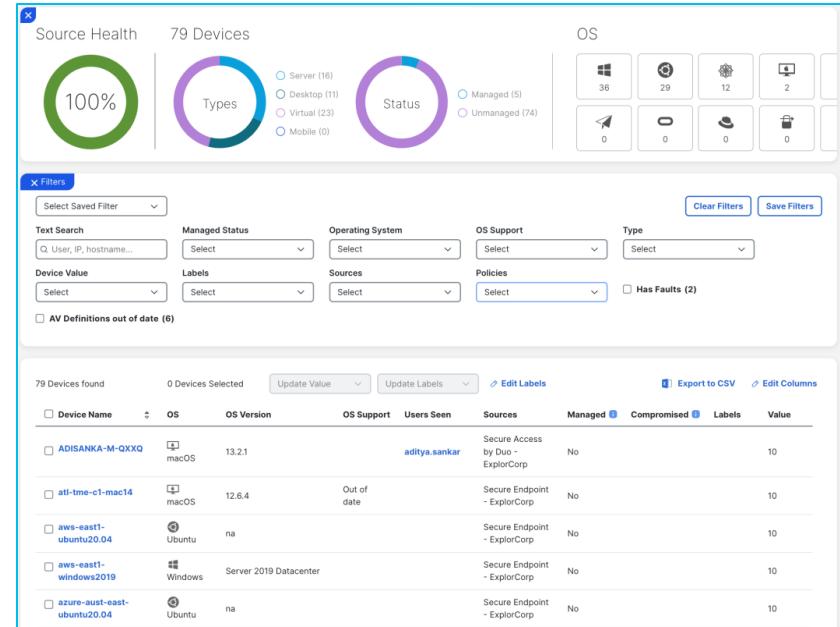
Gain unified visibility and contextual awareness to help you act on potential threats faster!

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:

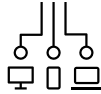
- What **types of devices** are connected to our network?
- What **users** have been accessing those devices?
- Where are those devices **located**?
- What **vulnerabilities** are associated with those devices?
- Which **security agents** are installed?
- Is our security software **up to date**?
- What **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



Normalise

Merge source-specific attributes into a common data schema



Deduplicate

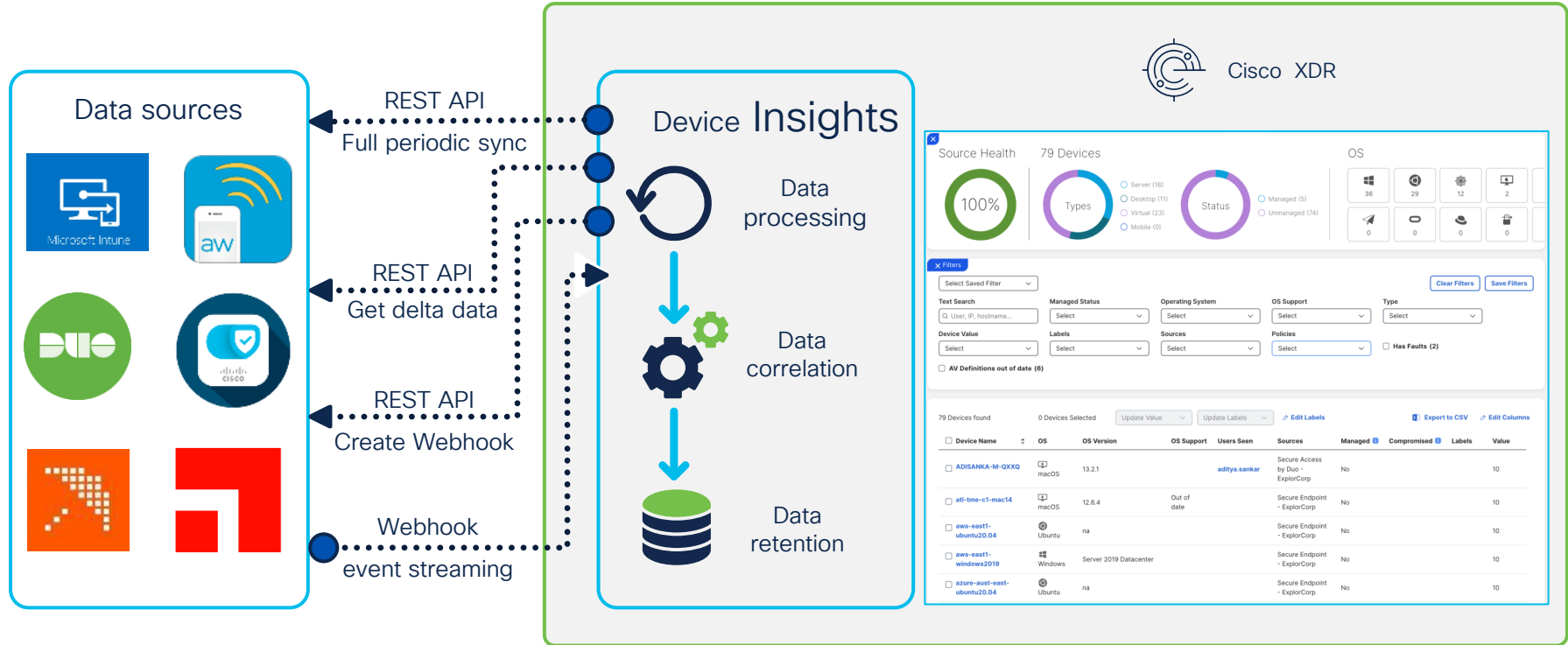
Remove duplicate or insignificant details from each record



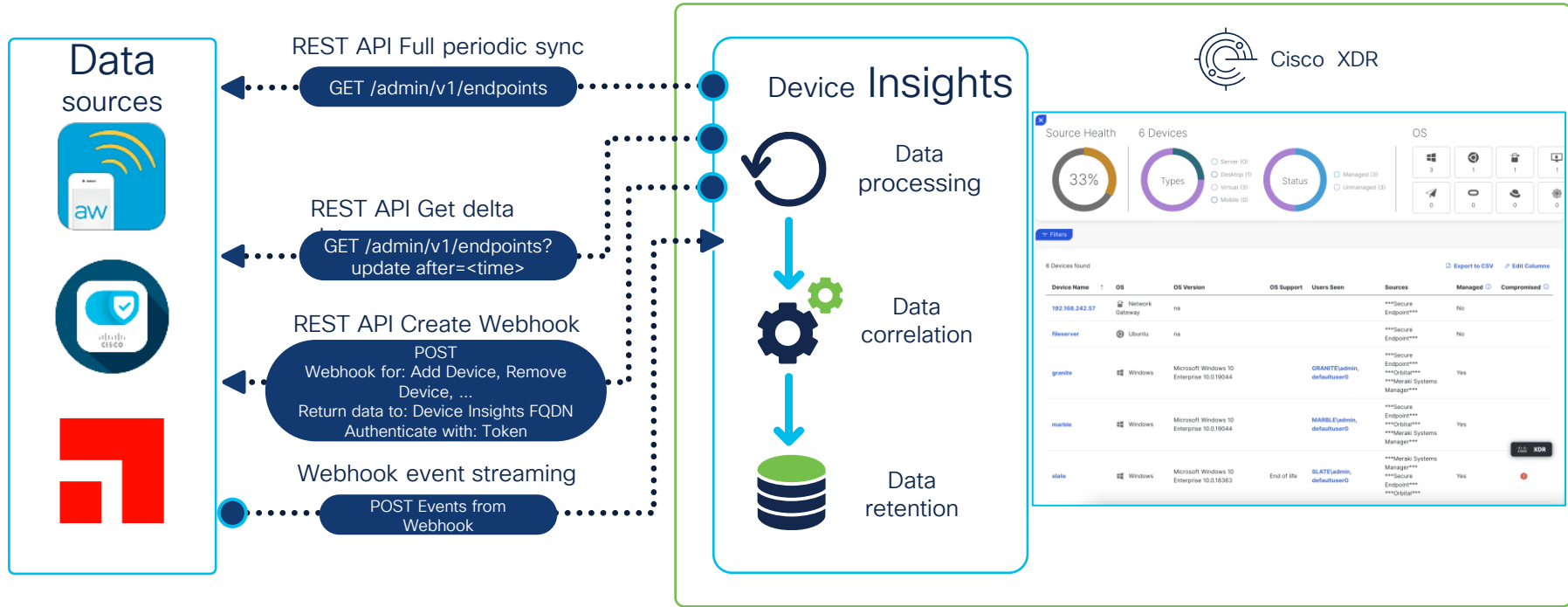
Correlate

Combine different records for the same device into one unified record

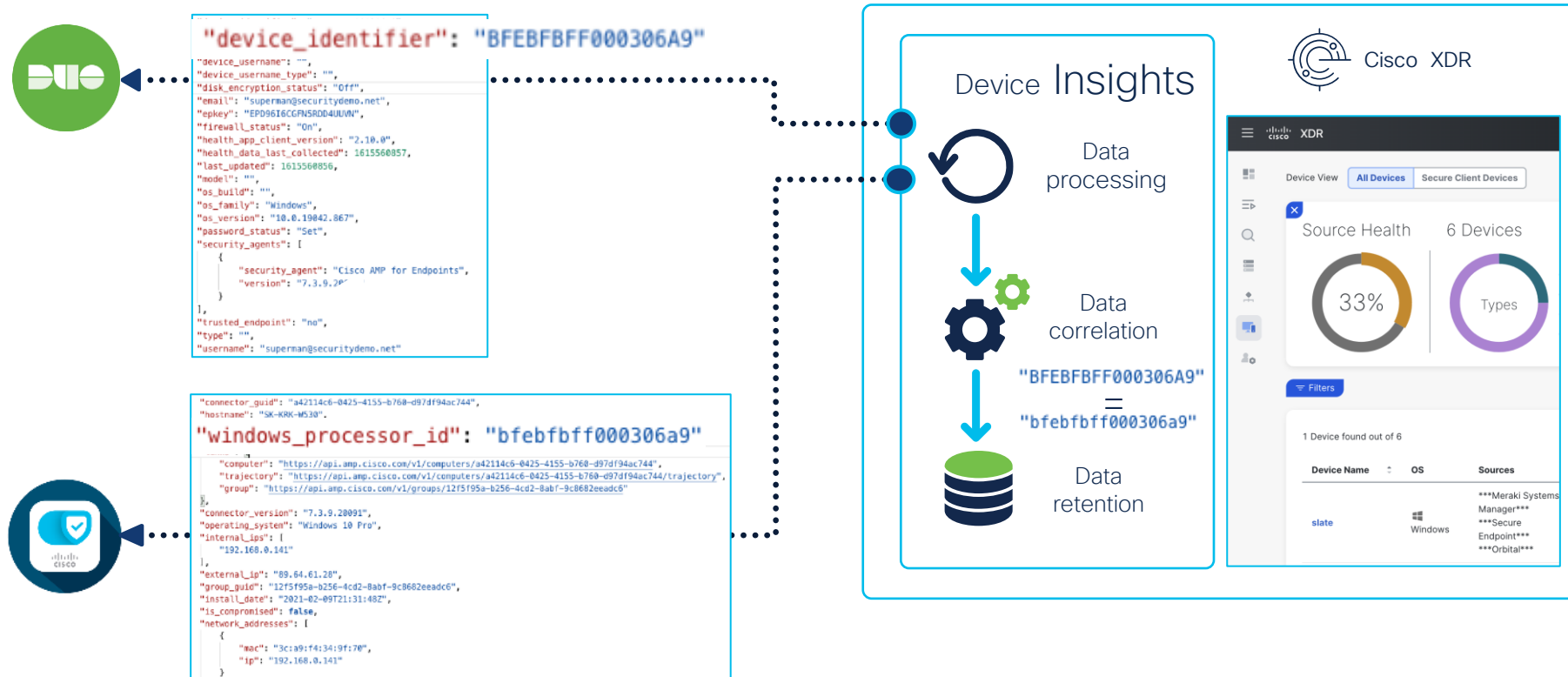
XDR Device Insights high level architecture



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 the Cisco Device Insights interface, showing details for three devices. Each device card includes a logo, name, and a list of 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:
- 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: 5.0.207
 - Reported OS: Windows
 - Reported OS Version: 10
 - Version:

[Open Cisco Umbrella Dashboard in New Window](#)
- 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
- Secure Client**
 - Last Seen: 2023-05-29T05:44:26.497Z
 - Deployment: Secure Client Deployment ExplorCorp
 - CSC Version: 5.0.02075
 - Secure Endpoint: 81.7.21417
 - 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
- Customisable 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 the Cisco Umbrella dashboard with three main device profile cards on the left and a detailed view of the 'Secure Client' on the right.

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:

Orbital - ExplorCorp

- Last Seen: 2023-05-29T12:37:38.440Z
- Users: tme
- Local Users: Administrator, DefaultAccount, Guest, tme, WDAQUtilityAccount
- 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: 5.0.207
- Reported OS: Windows
- Reported OS Version: 10

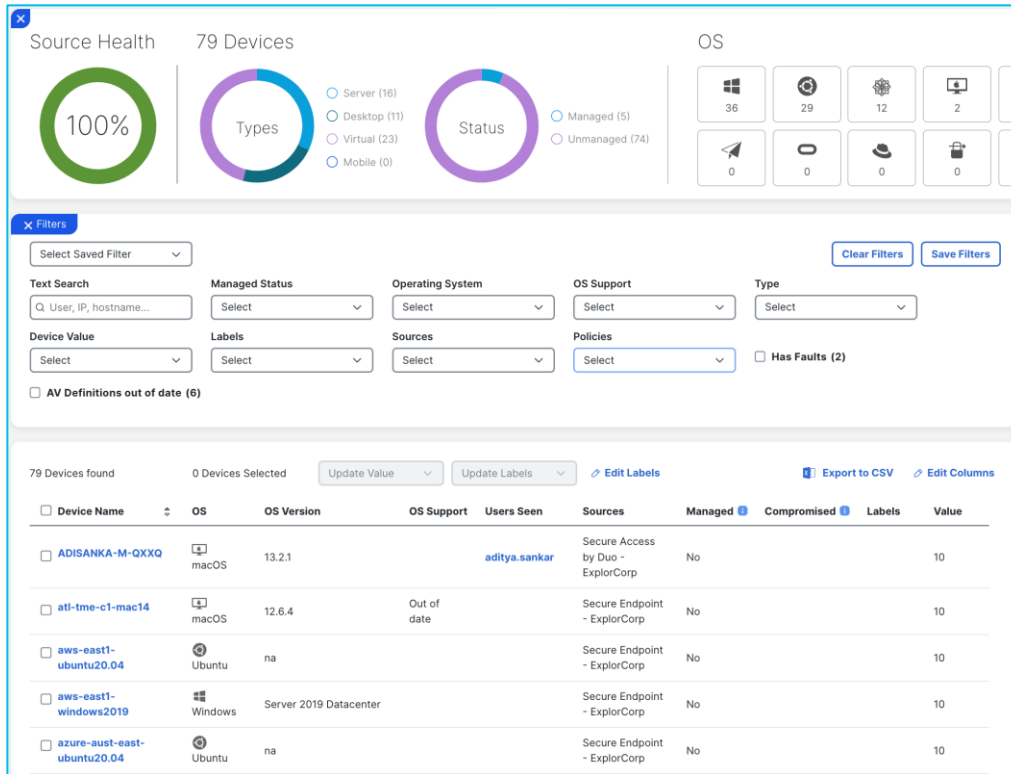
[Open Cisco Umbrella Dashboard in New Window](#)

Secure Client

- 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
- Last Seen: 2023-05-29T05:44:26.497Z
- Deployment: Secure Client Deployment ExplorCorp
- CSC Version: 5.0.02075
- Secure Endpoint Version: 8.1.7.21417
- Cloud Management Version: 1.0.1.400
- 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 UUID: cc2b22ab-57db-4051-932a-e5c4aa8f8b6b
- AC UUID: 68cca45cda768ff468753ec52f80bc18428fb048

[Device Events](#)

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 customised, 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

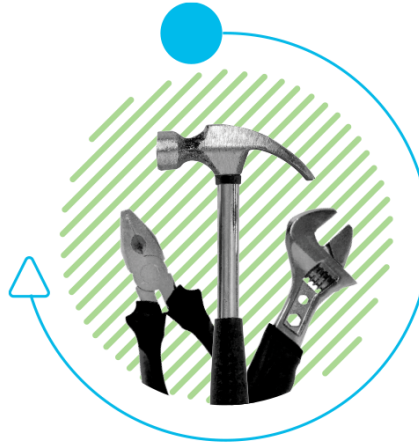
Cisco Secure Client: Security agent consolidation

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 displays the 'NVM to Direct XDR Deployment' configuration page. At the top, there are action buttons: 'Edit Name', 'Delete', 'Save', 'Full Installer', and 'Network Installer'. The interface is divided into two main sections for different versions of the deployment.

Top Section (Beta 1.0.1.400):

- Version dropdown: Beta (1.0.1.400)
- Cloud Management: NVM to Direct XDR CM (dropdown)
- Secure Endpoint: Choose a version (dropdown), Choose an Instance (dropdown), and Choose a Group (button).

Bottom Section (Beta 5.0.2810.0):

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

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. At the top, the profile name is 'NVM to Direct XDR CM', followed by links for 'Edit Name', 'Delete', 'Reset Changes', 'Cancel', 'Make A Copy', 'Save', and 'Download'. The settings are organized into four sections:

- Identity Service Settings:** Includes a toggle for 'Enable Debug Logging' which is currently disabled.
- Package Manager Service Settings:** Includes a 'Logging Level*' dropdown set to 'Error', a 'Check-in Interval*' dropdown set to '8 Hours', and a toggle for 'Notify User When Reboot Is Required' which is currently enabled.
- Cloud Management Service Settings:** Includes a 'Logging Level*' dropdown set to 'Error'.
- Product Update Window:** Includes a toggle for 'Enable Product Update Window' which is currently disabled. Below this toggle is a note: '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



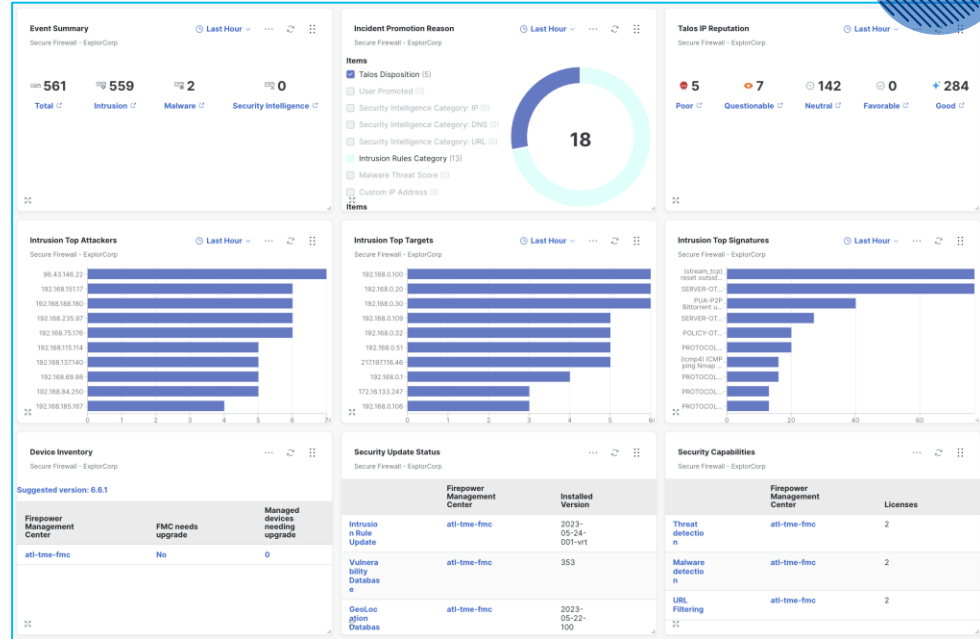
Agenda

- 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

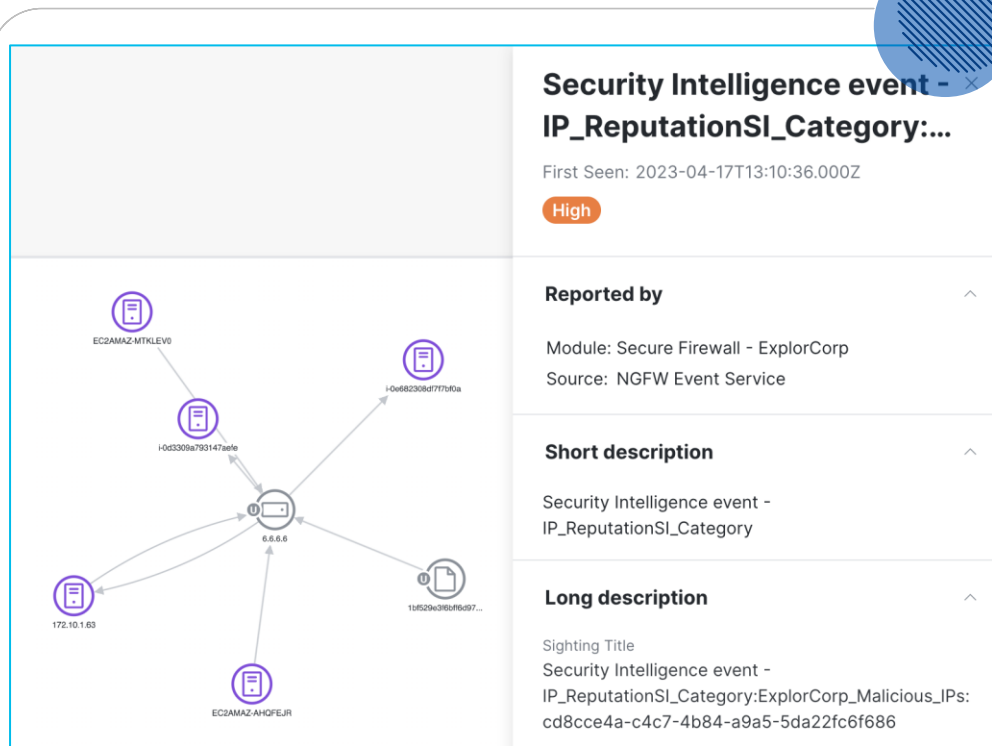
- Local IP sightings

Reference

- Pivot point to sighting event

Promote events

- Promote alerts from Analytics to incidents in XDR



Secure Firewall

Triage events

- See triaged network security events in the prioritised 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

The screenshot displays the Cisco Secure Cloud Analytics (cisco-dcloud-rtp) interface for a suspected malicious URL incident. The main header shows the incident title "Suspected Malicious URL on ip 192-168-249-115" with a status of "Unassigned" and a "View Investigation" button. Below the header, there's a navigation bar with tabs for "Overview", "Detection", "Response", and "Worklog". The "Overview" tab is active, showing a network diagram with nodes representing assets and observables. Below the diagram, there are three panels: "13 Assets", "4 Observables", and "7 Indicators", each with a "View all" link. The "Assets" panel lists assets like "marble", "granite", "slate", and "ip-172-16-133-37-us-east-2...". The "Observables" panel lists observables like "108.62.141.250", "OdSalc01c2706c8b66ba9...", "drinkfoodapp.com", and "http://drinkfoodapp.com/Ad...". The "Indicators" panel lists indicators like "Cisco Secure Cloud Analytics (cisco-dcloud-rtp) Watchlist Interaction", "Cisco Secure Cloud Analytics (cisco-dcloud-rtp) Watchlist Interaction", "Cisco Secure Cloud Analytics (cisco-dcloud-rtp) User Watchlist Hit", and "Cisco Secure Network Analytics Data_Exfiltration". On the right side, there's a sidebar with the incident title "Suspected Malicious URL on ip 192-168-249-115", a "Reported by" field, a "Assigned" field, a "MITRE" field, a "Priority score breakdown" section showing a score of 765 (76 Detection Risk, 10 Asset Value at Risk), a "Short description" field, and a "Long description" field. At the bottom right, there's a "View Incident Detail" button.

Never lose context with XDR Ribbon



The screenshot displays the Cisco XDR Casebook interface. The top navigation bar includes the Cisco logo, 'XDR CASEBOOK', and a search bar. The left sidebar shows a list of incidents, with 'Load RAT Grows Up-LU' selected. The main content area shows the details of this incident, including an overview, linked incidents, and a list of observables. The observables list includes 10 Domains, 10 SHA-256 hashes, and 9 URLs. The right sidebar shows a notes section with a link to the investigation.

Casebook

Search...

Owned By Me

Owned By Others 1,495

CHEN TEST
1 Observable

Case 2023-05-28T17:57:40.000+03:00
1 Observable

Load RAT Grows Up-LU
29 Observables

Loda RAT Grows up
29 Observables

Loda RAT Growths up
29 Observables

Load RAT Grows Up-LU

Overview

Created May 25, 2023, 10:50:53 AM

Owner user210 dcloud_sxv2

Summary ...

Linked Incidents

No linked incidents...

Observables 29

Enter logs, IPs, domains, etc.

10 Domains 1 8 0 1

10 SHA-256 0 10 0 0

9 URLs 0 0 1 8

Notes

Talos Loda Rat Grows Up investigation

<https://blog.talosintelligence.com/loda-rat-grows-up/>

Run Investigation Link to Incident

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

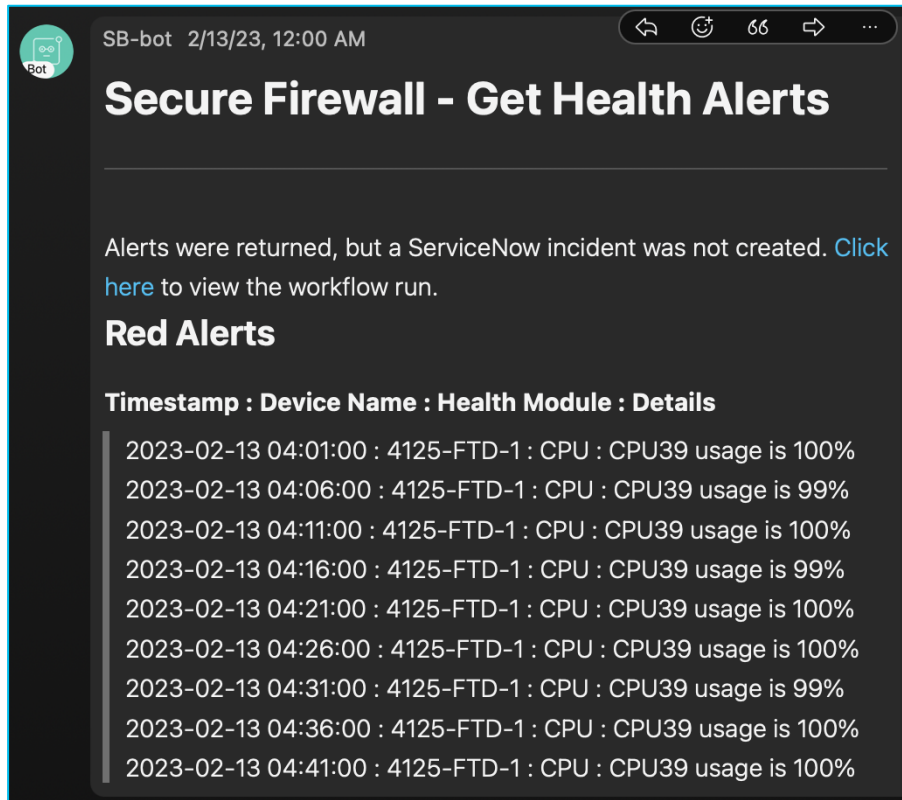
Firewall Incident automated investigation completed for promoted Incident *Security Intelligence event - URL_SI_Category:dcloud-SI-URL* involving internal host with IP [192.168.249.111](#)

- [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:
0d5a1c01c2706c8b66ba953dbe01f265d7d38e9b02aa41
bc4f62239e9acb8067
- 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.

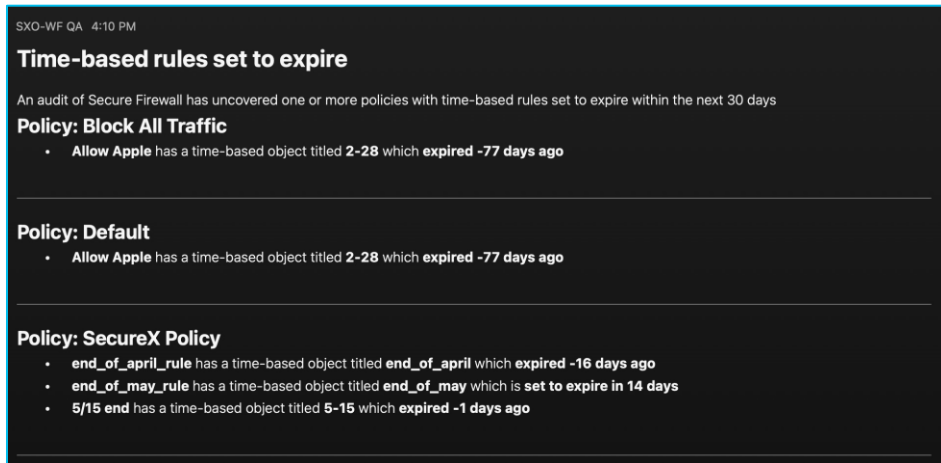
Red Alerts

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.

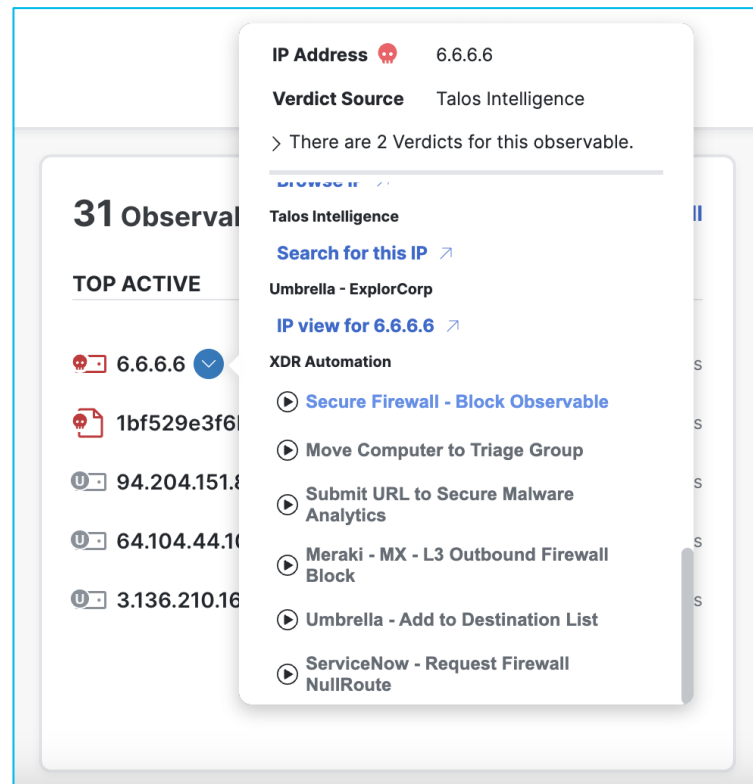
Solution: This orchestration workflow will check rules that have already expired or will expire soon and proactively notify you of which rules to review.



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.

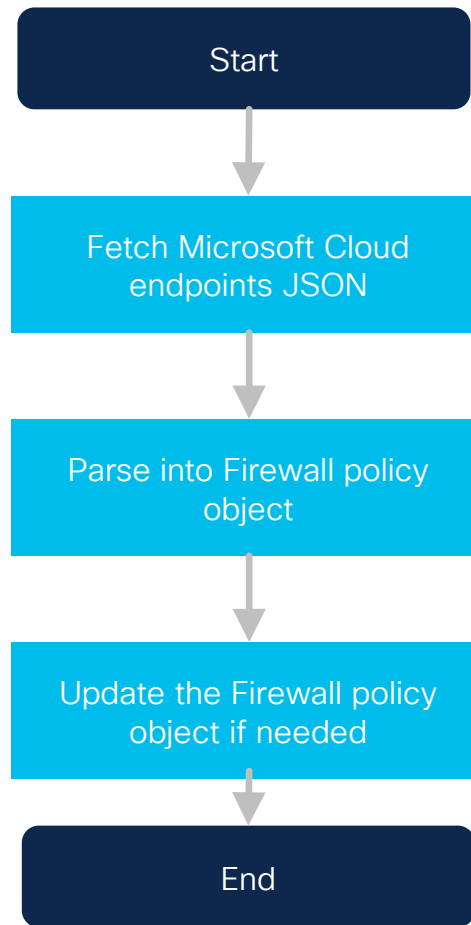
Solution: Using the pivot menu Adam can block the IP address at the click of a button from anywhere.



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

- 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

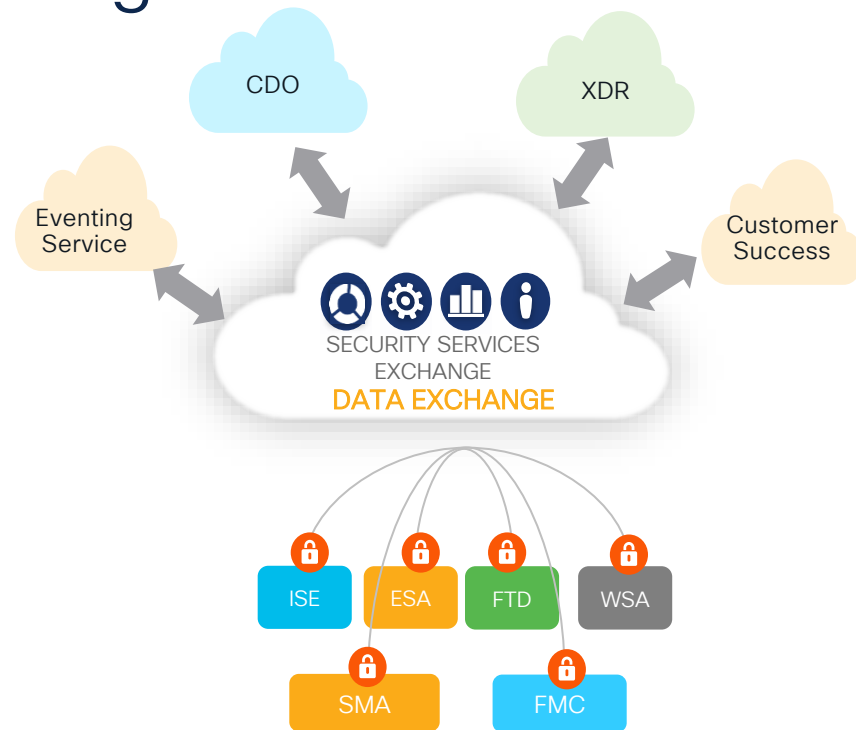
- Cisco Defense Orchestrator (CDO)
- XDR
- Cisco TAC
- Customer Success

Core Infrastructure Services

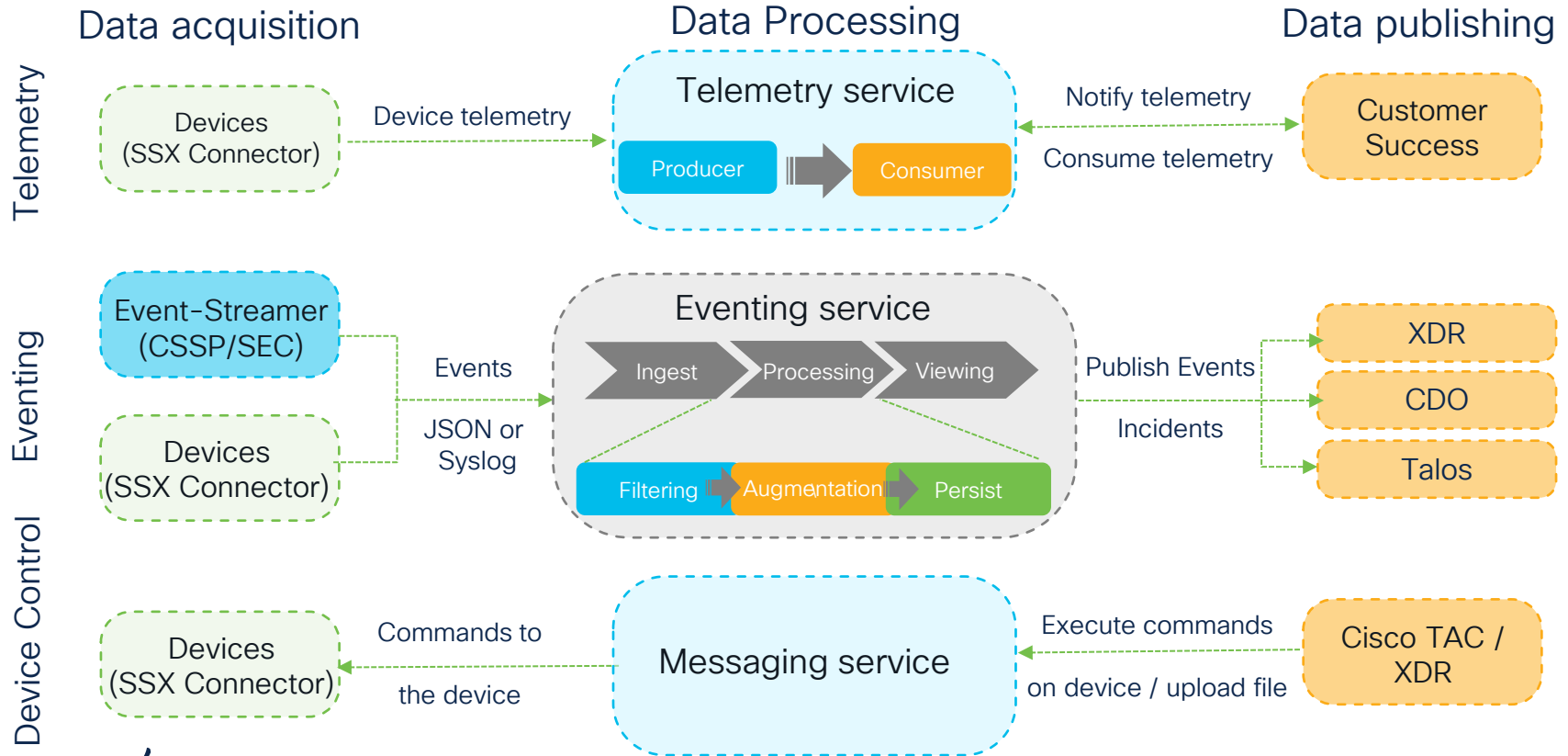
- Identity and Tenancy
- Secure device registration
- Application registration and discovery
- Data publishing

Device Connector / Agent

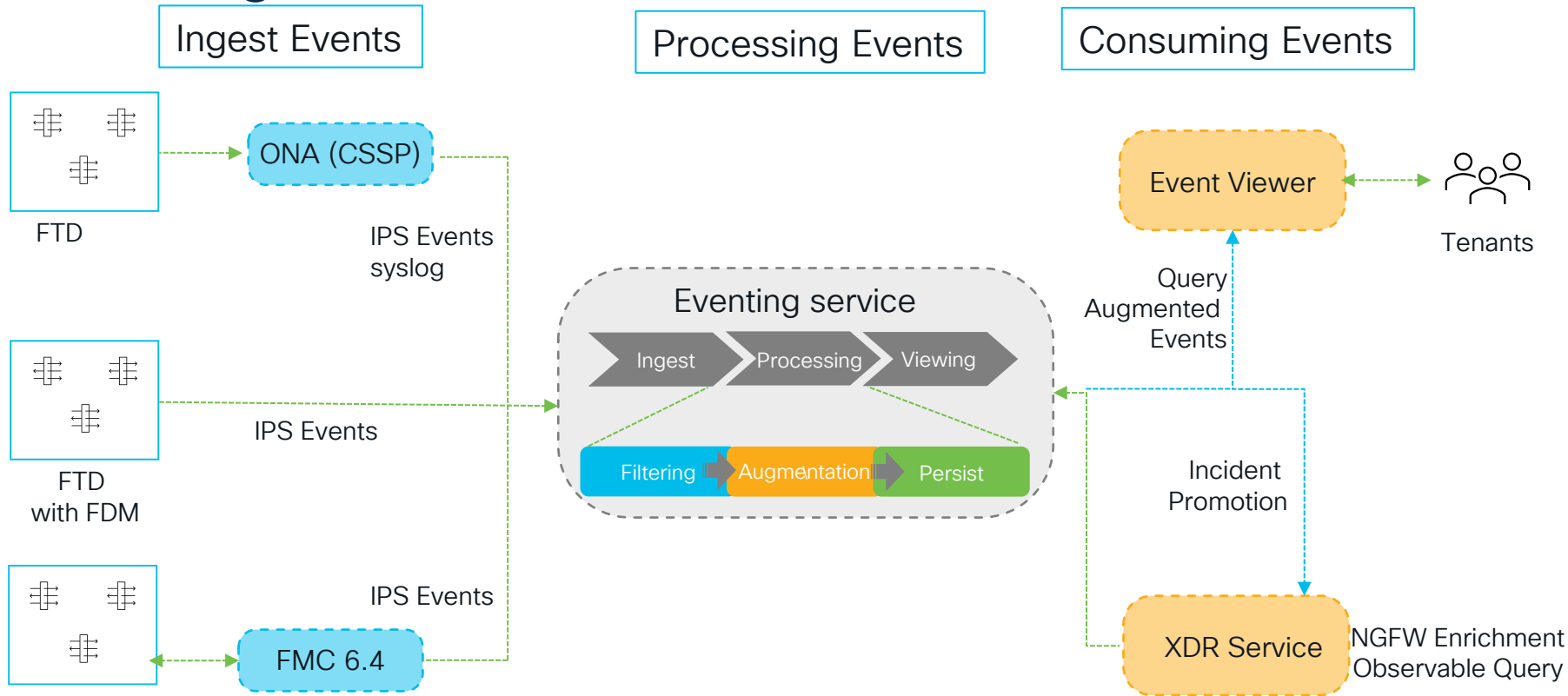
- Secure Bi-Directional Channel
- REST, CLI, WebSocket
- File Upload / Download
- Services Management
- Products: FMC, FTD*, ESA, WSA, SMA, ISE, SNA
- * = Events are SENT to SSX and stored for 7 days



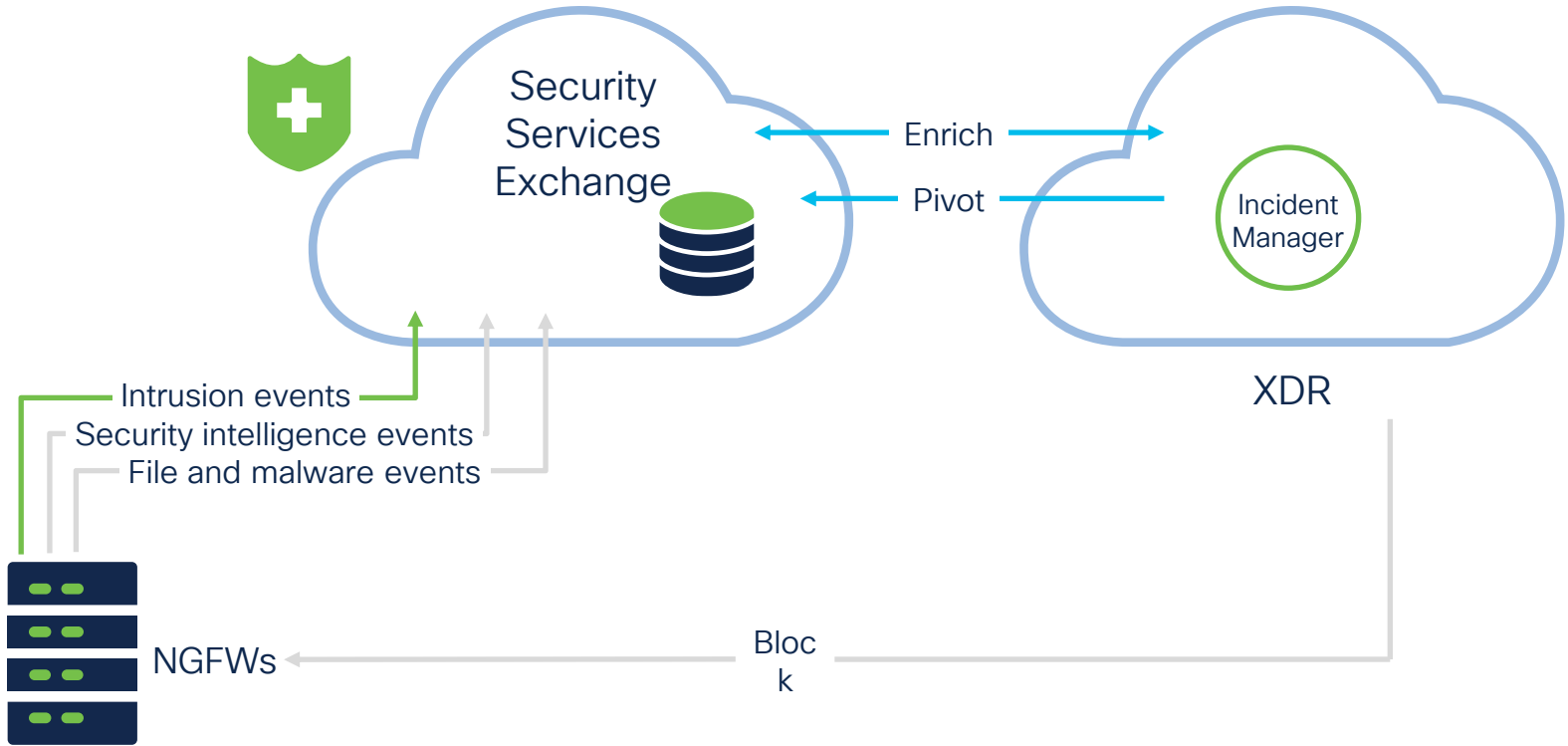
Supported Data pipelines



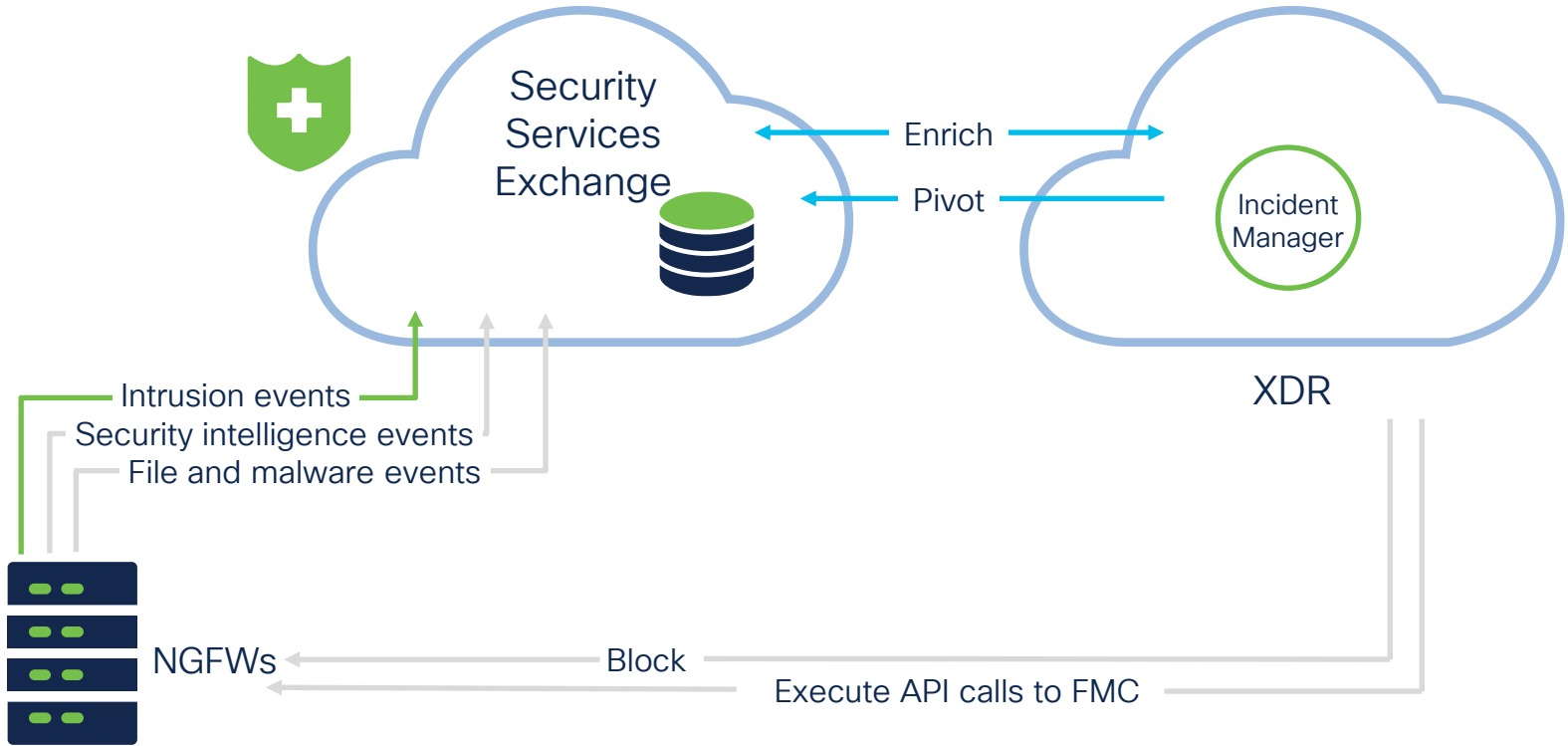
Eventing Service



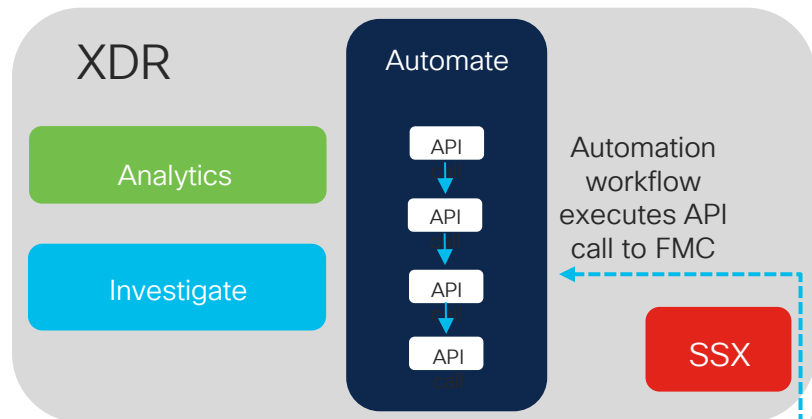
Secure Firewall



Secure Firewall



Cloud to on-prem API Proxy

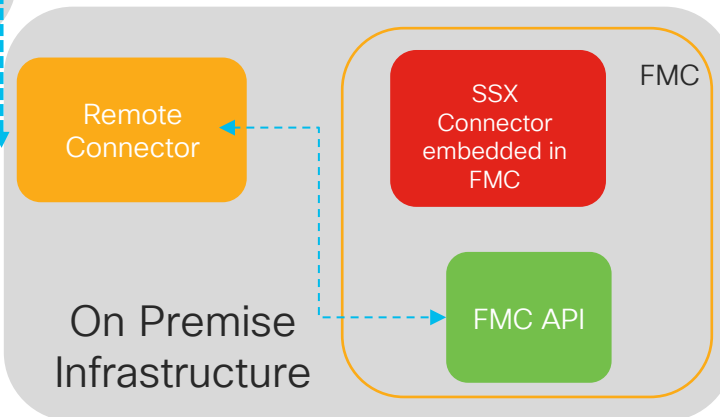


API call is sent to orchestration remote based on target configuration

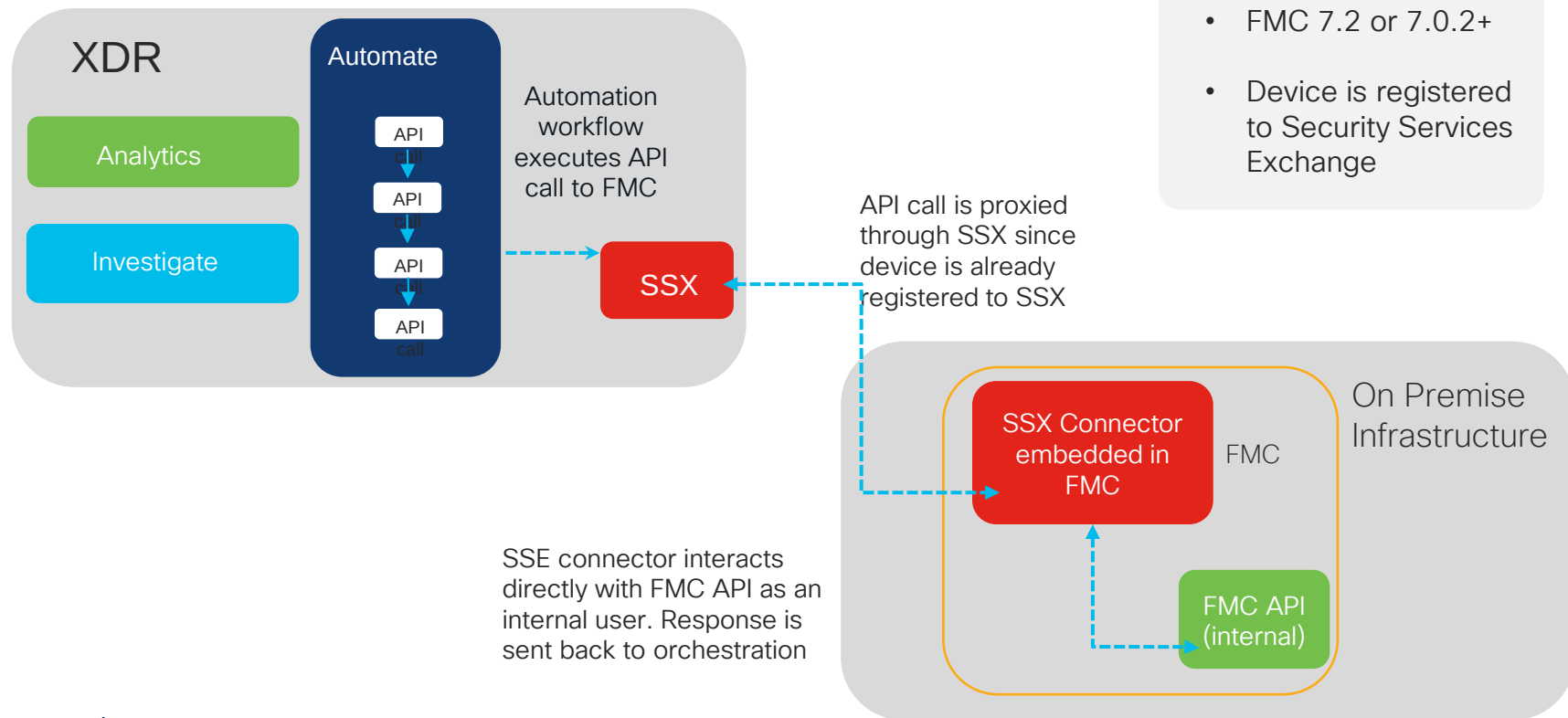
Authenticate to API as an external user and execute API call. Response is sent back through orchestration remote

Requirements

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



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__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

device-id * 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 steps, each with a green arrow pointing to a specific configuration element:

- Step 1: Cloud Region** - A dropdown menu is set to 'us-east-1 (US Region)'. A green arrow points from the step number to the dropdown.
- Step 2: SecureX Enablement** - A green checkmark indicates 'SecureX is enabled for US Region'. A green arrow points from the step number to the checkmark.
- Step 3: Event Configuration** - Under 'Send events to the cloud', the 'Intrusion events', 'File and malware events', and 'Connection Events' checkboxes are checked. A green arrow points from the step number to the 'Intrusion events' checkbox.
- Step 4: Orchestration** - Under 'Enable SecureX Orchestration', the checkbox is checked. A dropdown menu for 'Assigned Role' is set to 'Administrator'. A green arrow points from the step number to the dropdown.

At the bottom of the page, there is a navigation bar with icons for XDR, Automation, and other features.

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 Malware Analytics**
Formerly Threat Grid

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	7.2.3	Registered	10.90.12.236 atl-tme-fmc-log.cisco.com	10.90.12.236
atl-tme-fp4100-1	7.2.0	Registered	10.90.12.210 atl-tme-fp4100-1 (FMC managed)	10.90.12.210
atl-tme-fp4100-2	7.2.0	Registered	10.90.12.220 atl-tme-fp4100-2 (FMC managed)	10.90.12.220
atl-tme-ftd-log	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.

Save

1 Add Firewall module

2 Save the module

Firewall and XDR Demo



Agenda

- 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

- 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://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

START

Monday, June 5 | 1:00 p.m.

BRKSEC-1639

An Introduction to Risk-Based Vulnerability Management

Monday, June 5 | 3:00 p.m.

BRKMER-2003

Meraki with Secure Network Analytics and XDR: Threat Detection for the Rest of Us

Monday, June 5 | 4:00 p.m.

BRKSEC-1023

Accelerate your SOC with Cisco XDR

Tuesday, June 6 | 1:00 p.m.

BRKSEC-2084

Seeing is Believing: Unlocking XDR Outcomes with Visibility

Tuesday, June 6 | 2:30 p.m.

BRKSEC-2101

Malware Execution As A Service: a Deep Dive into CSMA Advanced File Analysis

Wednesday, June 7 | 10:30 a.m.

BRKSEC-2095

Cisco XDR with Email: Protect, Analyze and Evolve the SMTP Conversation

Wednesday, June 7 | 1:00 p.m.

BRKSEC-2113

Cisco XDR - Making sense of the Solution and how it's a Security Productivity Tool

Thursday, June 8 | 9:30 a.m.

BRKSEC-2178

Extended Detection with Cisco XDR: Security analytics across the enterprise

Thursday, June 8 | 10:30 a.m.

BRKSEC-2931

Building, Proving, and Extending Detections in Secure Analytics

Thursday, June 8 | 1:00 p.m.

BRKSEC-3116

Automating your Cisco XDR Workflows: from Threat Hunting, to Finding and Confirming Incidents, to Responding!

FINISH

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!

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

 **Mission:-** 3.8 - SOC Life Simplified with XDR

 **Section:-** 3 - Blue Team powered by Cisco Secure

BETA TESTING

 Available Actions for this Mission

Other Associated CTF Portals: [ctf23-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).

Overall Difficulty: Easy	Recommended For: SecOps
Time to Complete: 01H:00M	Mission Author: 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 3rd party ED, NDR, firewall, and email solutions.**



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

Keynote Deep Dives

Wednesday
10:30am – 11:30am



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

Level 1
Room 106



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

Level 2
Room 204



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

Level 2
Room 203



Securing User to
Application and
Everything in
Between

Level 2
Melbourne Room 2



Unlocking
Digital Resilience
through Unified
Observability

The HUB
Centre Stage

Complete Your Session Evaluations



Complete a minimum of 4 session surveys and the Overall Event Survey to claim a **Cisco Live T-Shirt**.



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



Continue your education



- Visit the Cisco Stand for related demos
- Book your one-on-one Meet the Expert meeting
- Attend the interactive education with DevNet, Capture the Flag, and Walk-in Labs
- Visit the On-Demand Library for more sessions at www.CiscoLive.com/on-demand



Thank you

CISCO *Live!*

#CiscoLiveAPJC

CISCO *Live!*

GO BEYOND

#CiscoLiveAPJC