
cisco Live!
Let's go
#CiscoLive

The bridge to possible

Cisco XDR with Firewall

Adi Sankar, Technical Marketing Engineer

BRKSEC-2090

Cisco Webex App

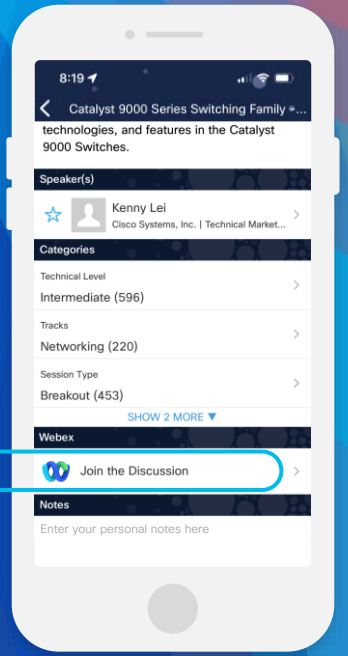
Questions?

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://ciscolive.ciscoevents.com/ciscolivebot/#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

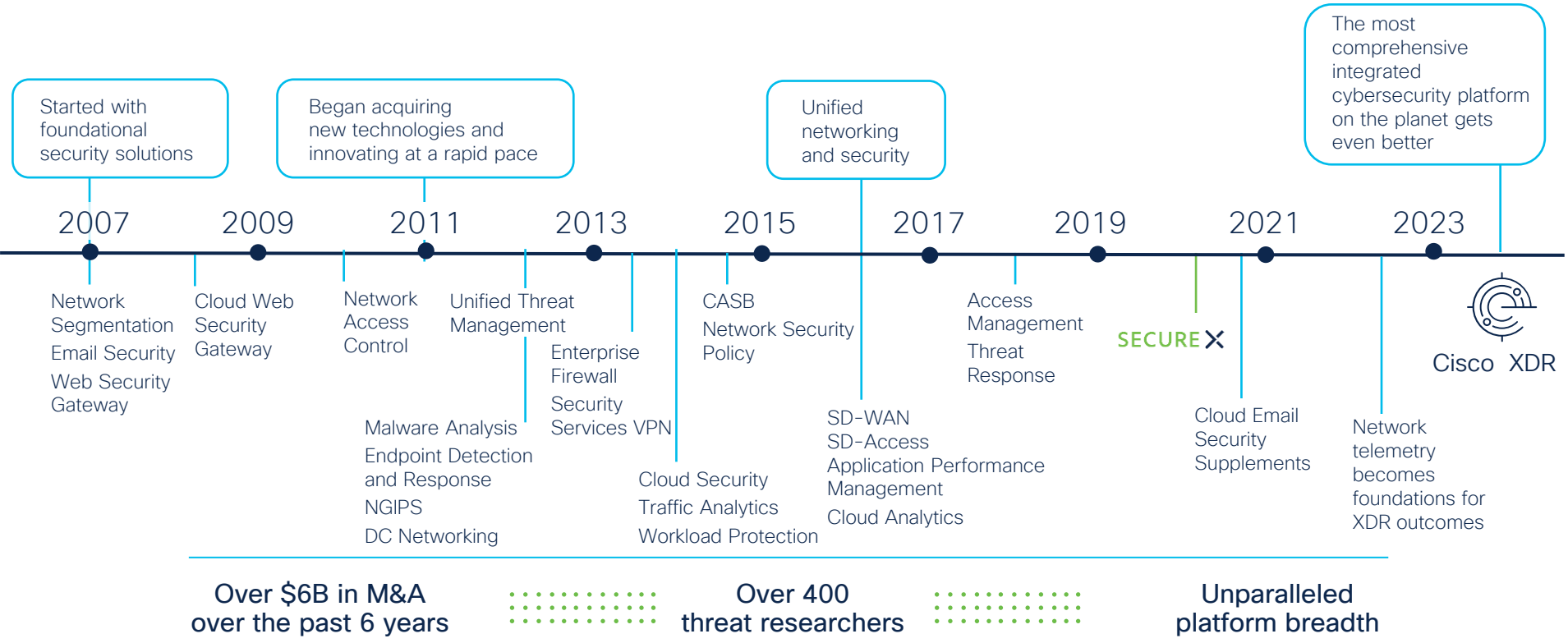
Agenda

- 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



Over $6B in M&A over the past 6 years

Over 400 threat researchers

Unparalleled platform breadth

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

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

Prioritize by Impact 2

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

3 Reduce Investigation Tim

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

Accelerate 4

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

Detect Sooner	Prioritize by Impact	Reduce Investigation Time	Accelerate Response	Extend Asset Context
Integrations	Correlated Events	Investigation	Prebuilt Playbooks	Integrations
Intelligence		Incident Manager		Account and Device Correlation
Machine Learning	Asset Insights	Threat Hunting	Automated Workflows	
		Automated Enrichment		

Analytics
Detections based on raw telemetry

Incidents
Security alerts, correlated, prioritized and enriched

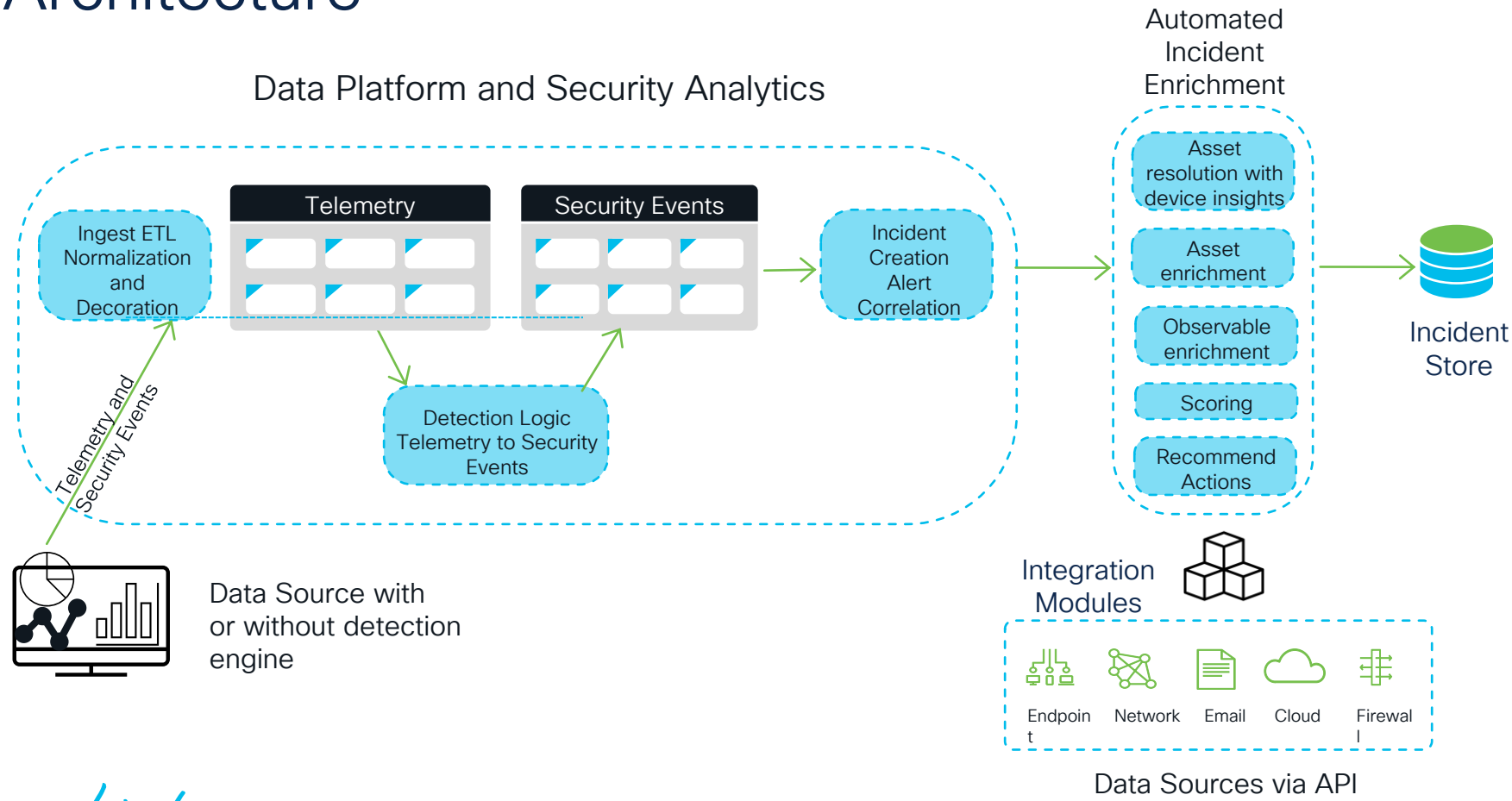
Integrations
built-in, pre-built or custom

Investigate
is at the core of the platform

Automate
drag-drop GUI for no/low code

Devices
device inventory with the contextual awareness

Architecture

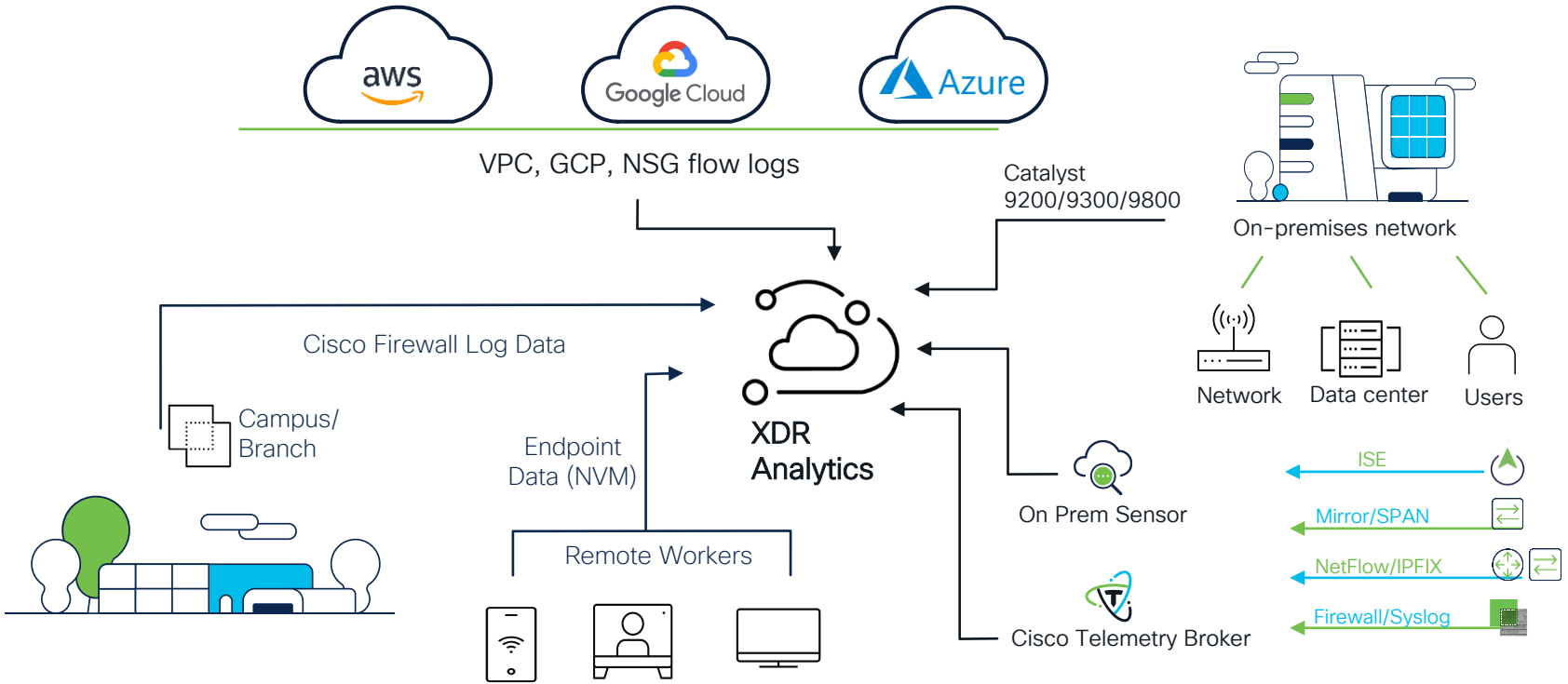


Overview Demo

XDR Analytics

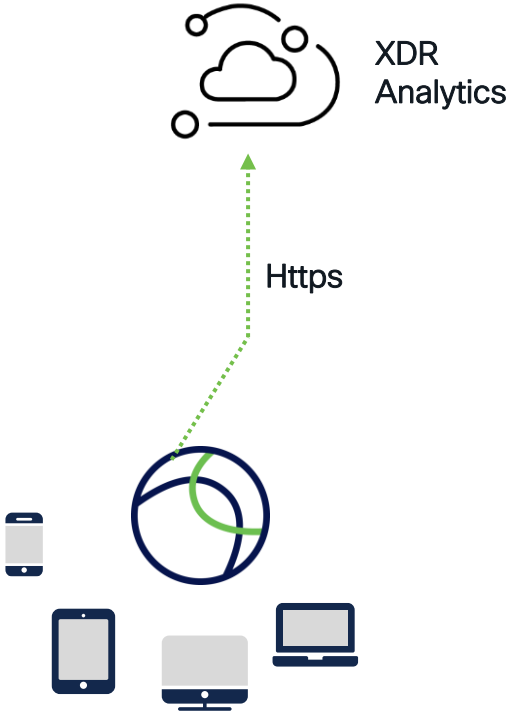
Raw Telemetry sources for XDR Analytics

Flexible ingest for dynamic environments

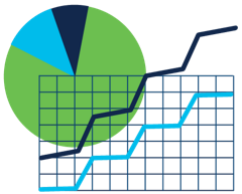


NVM Data to XDR anlaytics

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

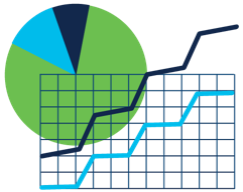
Firewall logging

- 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

IP address detected

Communicates with set of IPs

Classify roles
Dynamically assign roles to entities

Database server identified

Data stays within environment

36 day baseline
monitor and model behavior

Data access from regular location

Existing IP accesses database server

New external connection osbservation

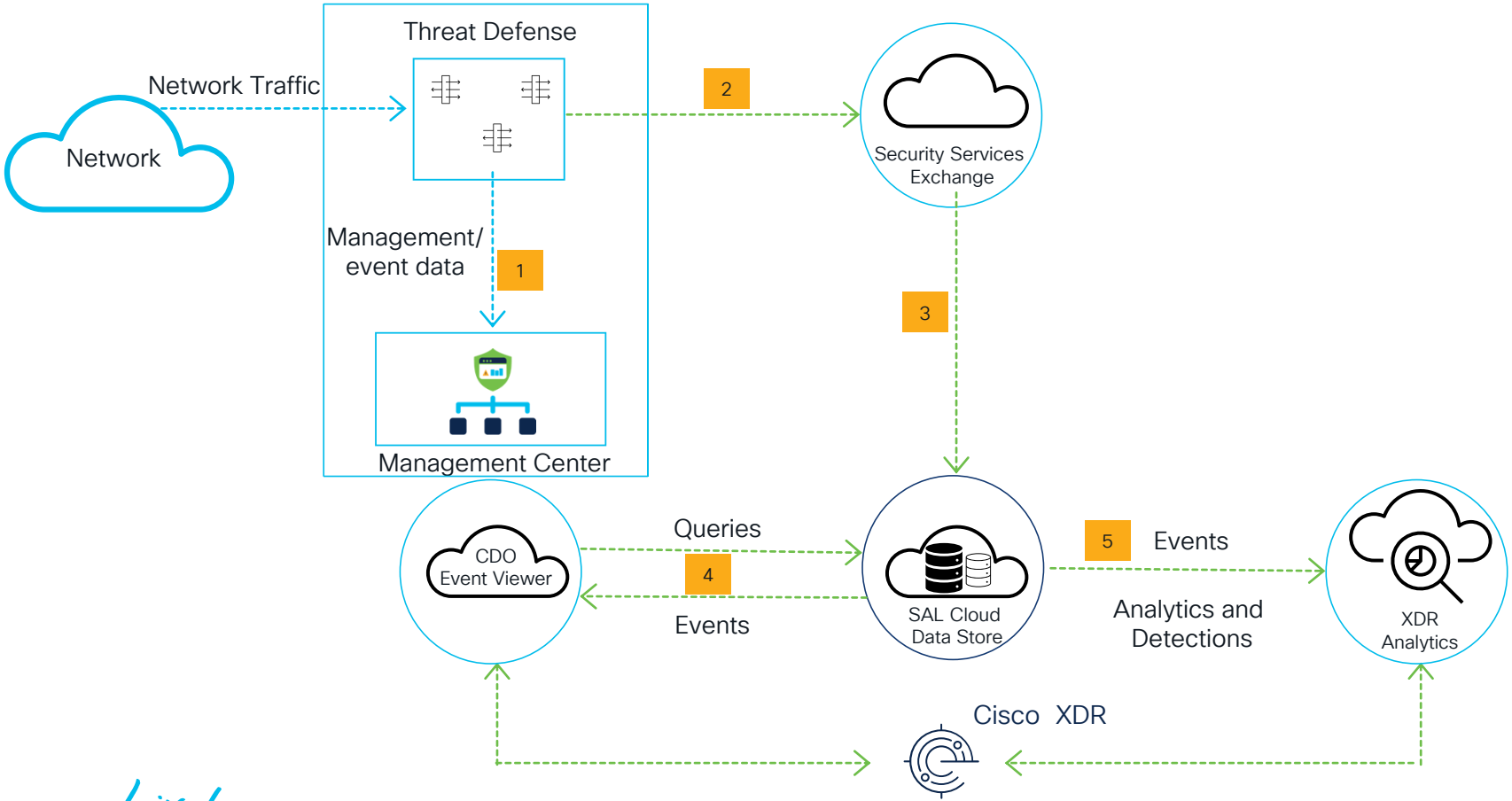
New high throughput connection

Alert triggers
for database exfiltration

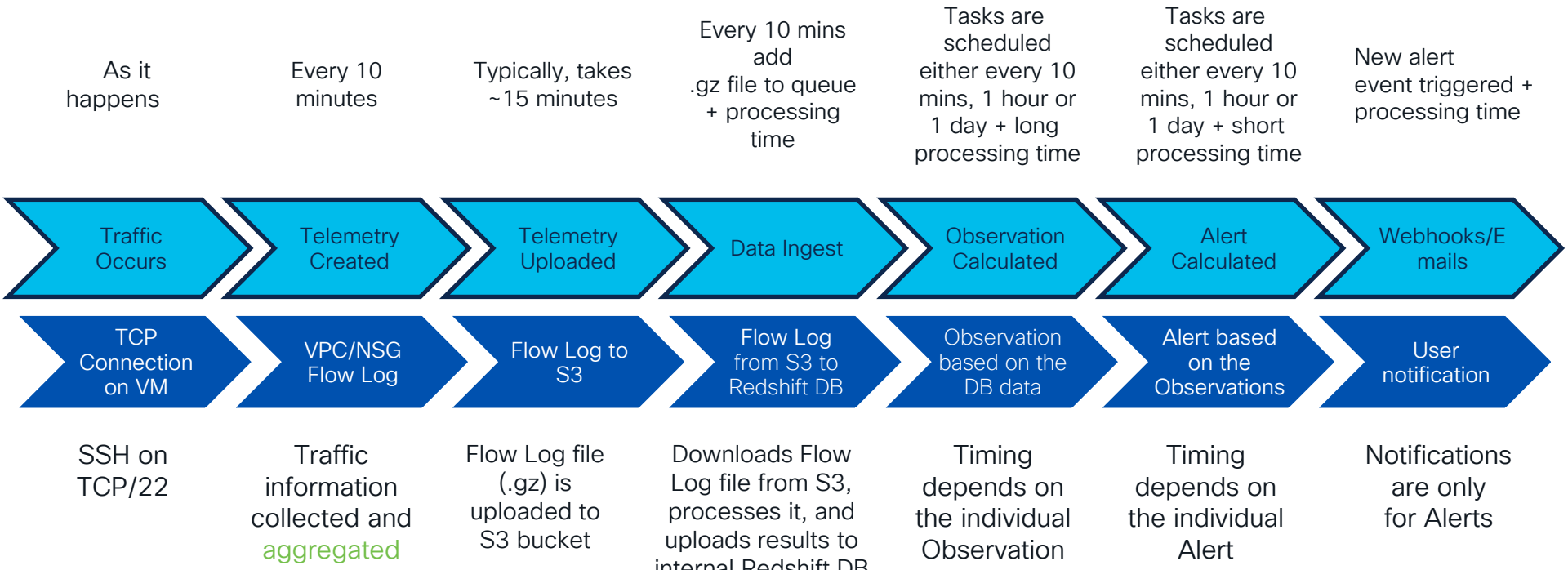
XDR Analytics detection and incident creation path

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

Eventing High Level Flow

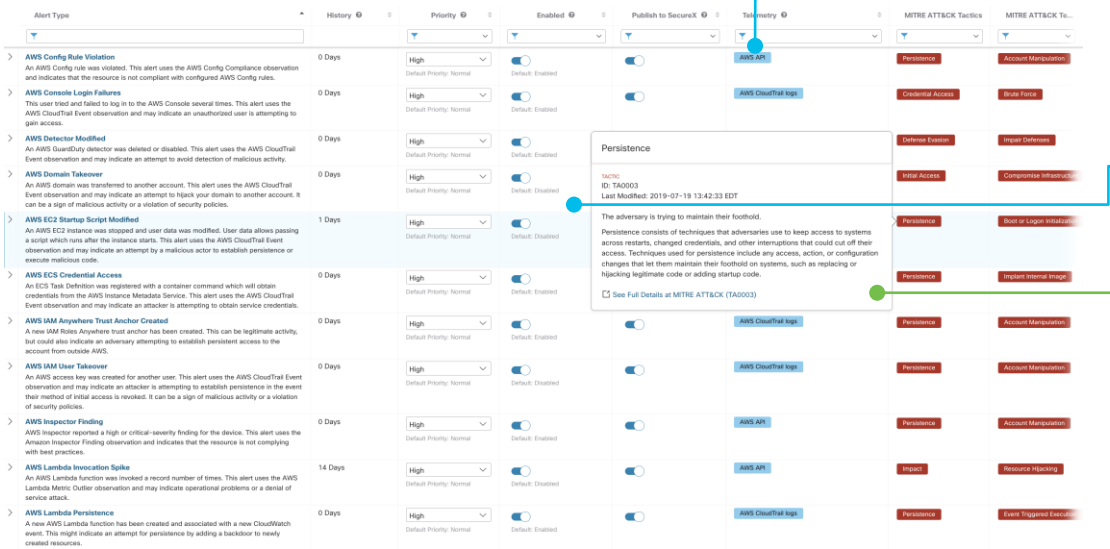


Flow Processing Fully Explained



Alerts with MITRE ATT&CK Tactics and Techniques

Single menu for all alert configuration



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

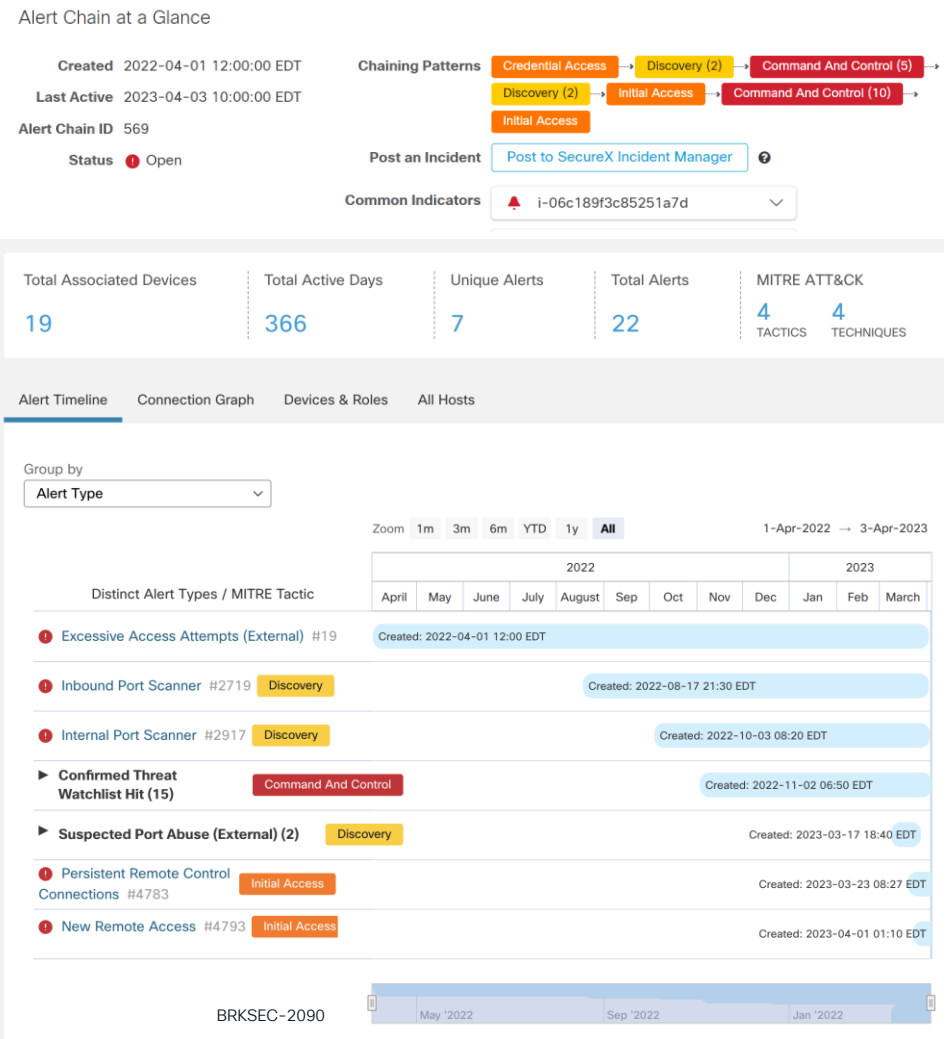
98%+ of XDR Analytics alerts are mapped to the MITRE ATT&CK framework

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



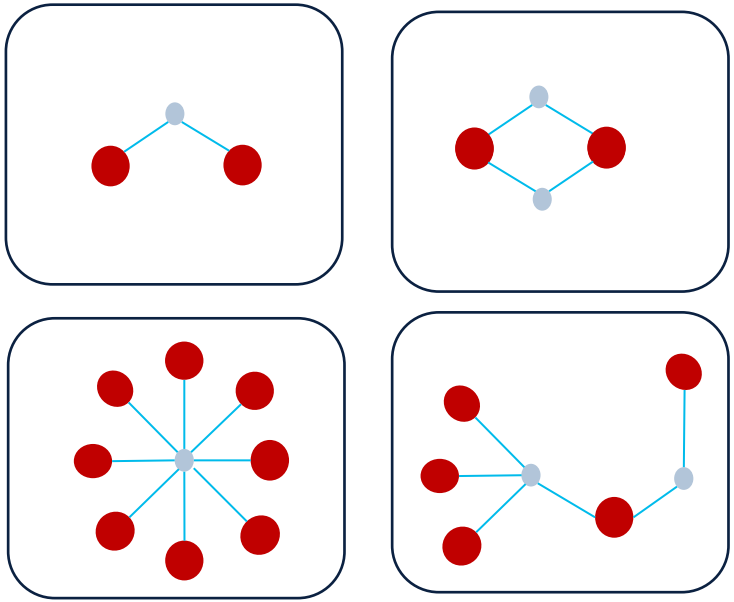
Chaining attacks based on common observables

Alert Sources

- NVM
- Firewall
- IPS, Malware
- Cloud Providers
- NetFlow

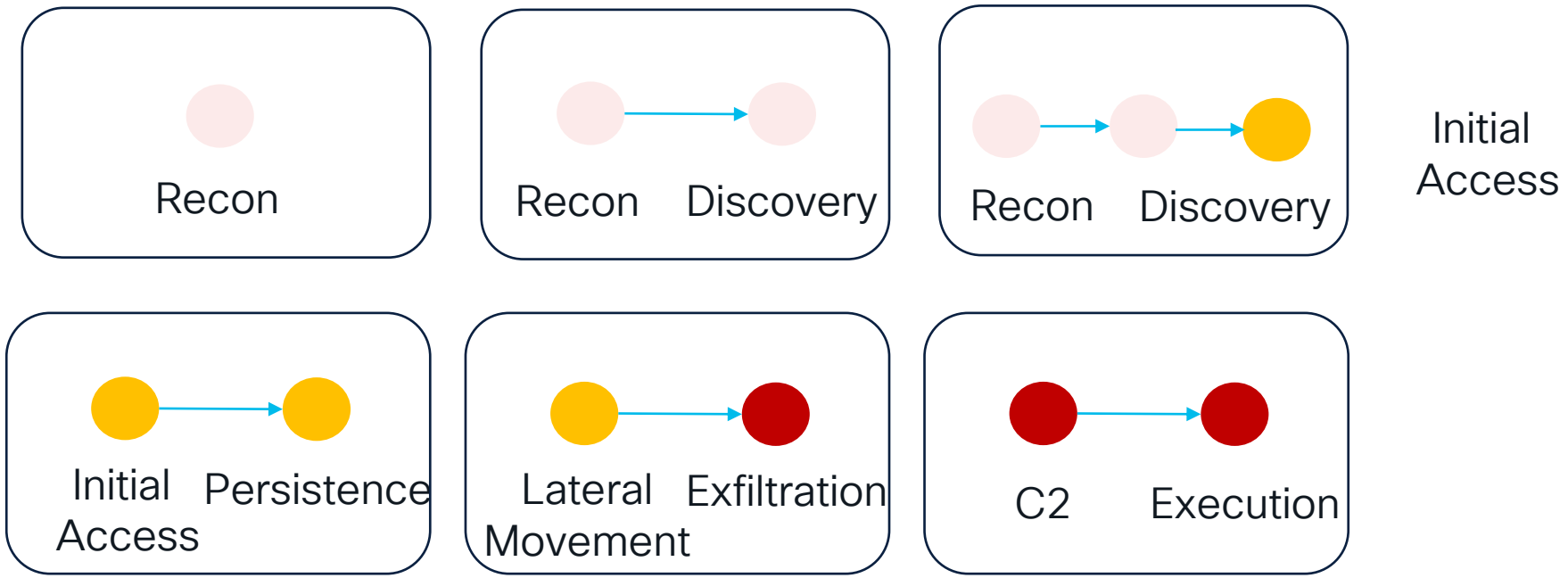
Observables

- IP Addresses
- Hostnames
- Devices
- Usernames
- AWS Resources
- CIDR
- Processes
- URLs
- ASNs



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

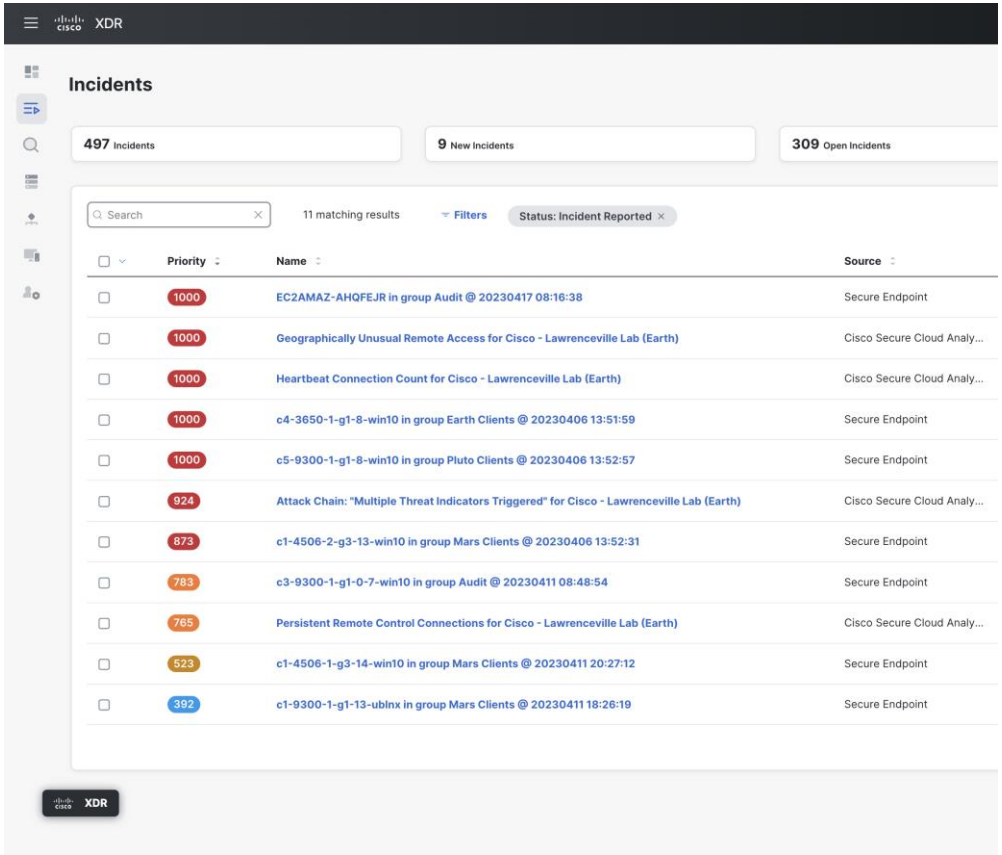


Incidents

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



Automatically Create Incidents

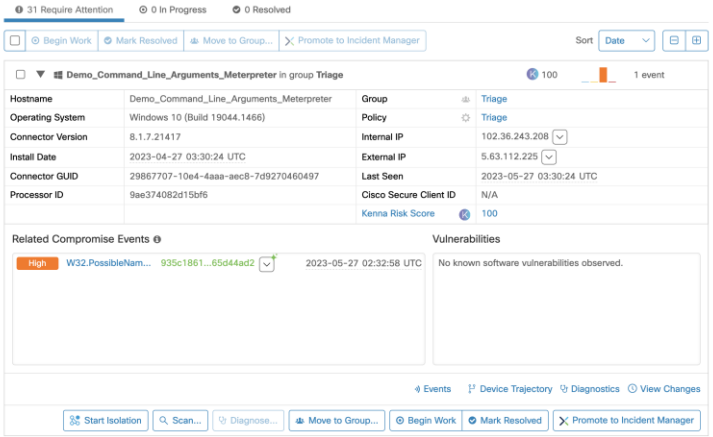
With Secure Endpoint

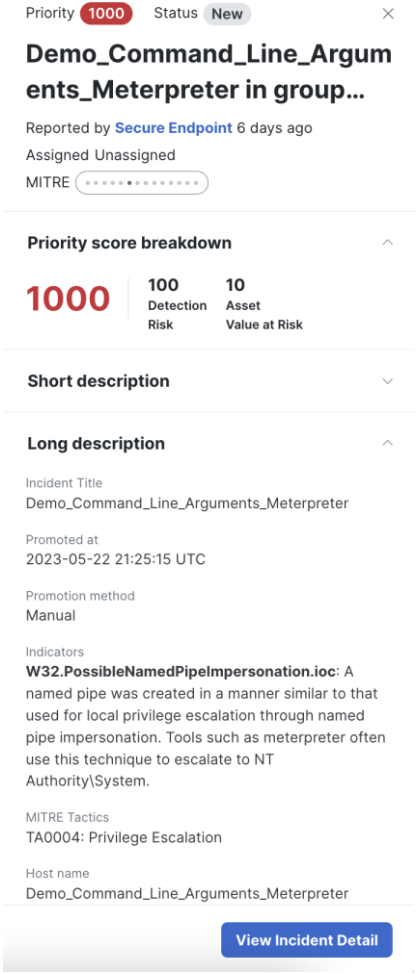
Secure Endpoint

Security events automatically create incidents in Incident Manager based on severity

Manually promote events as incidents from Secure Endpoint Inbox

Cisco XDR Incidents





Automatically Create Incidents

With XDR Analytics

XDR Analytics

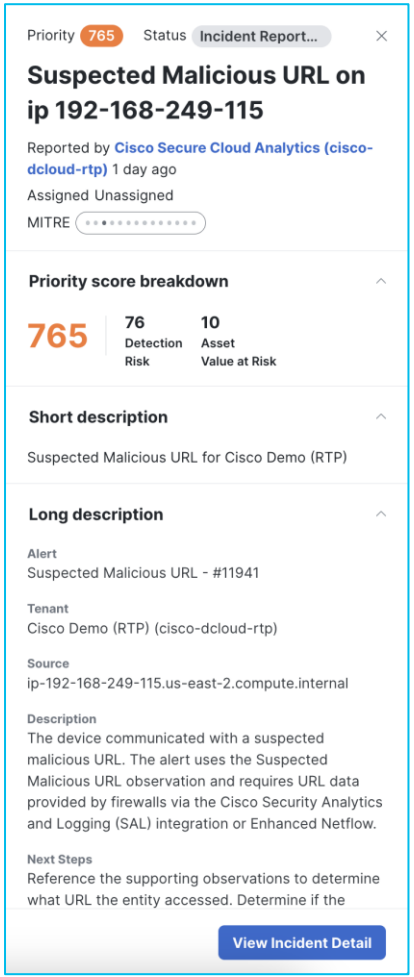
Create incidents automatically in Incident Manger as part of alert settings

Manually promote alerts as part of XDR Analytics alert workflow

Cisco XDR Incidents

Alert Type	History	Priority	Enabled	Publish to SecureX	Telemetry
= url					
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	Normal Default Priority: Normal	Default: Enabled		ETA
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	High Default Priority: Normal	Default: Enabled		ETA, 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	Normal Default Priority: Normal	Default: Disabled		Firewall, North-South

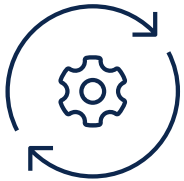
Configure severity and publication settings in Secure Cloud Analytics



Automatically Create Incidents

With Cisco XDR Automate

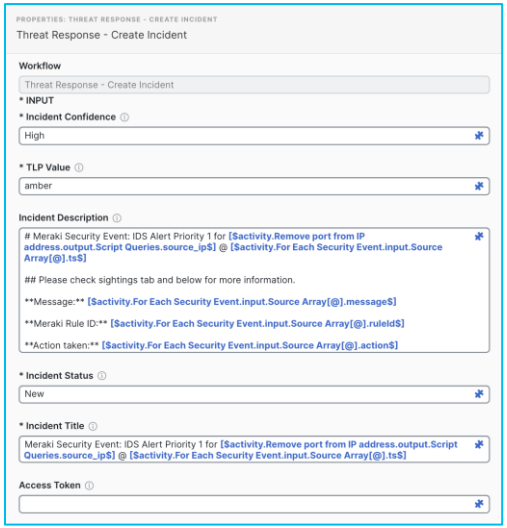
Cisco XDR Automate

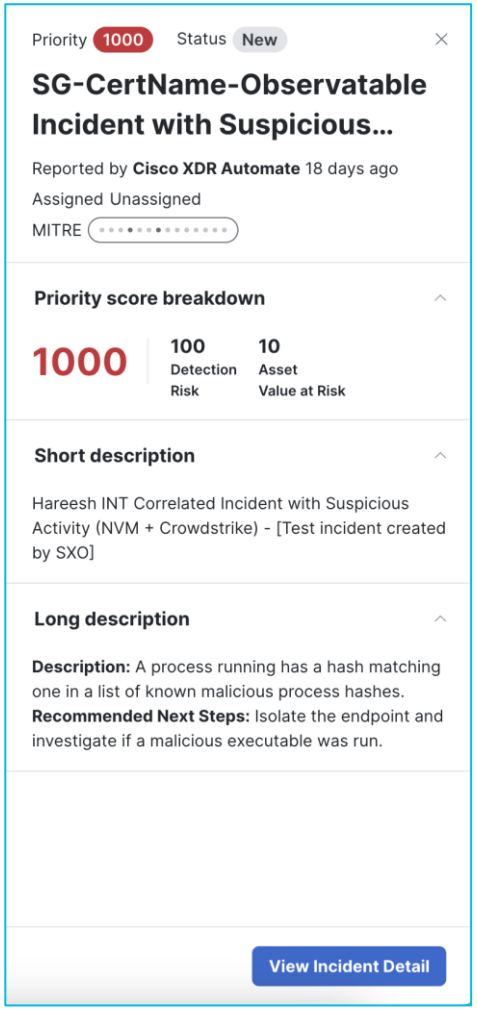


Workflow polls API on scheduled interval.

If detections is found incident is automatically created

Cisco XDR Incidents





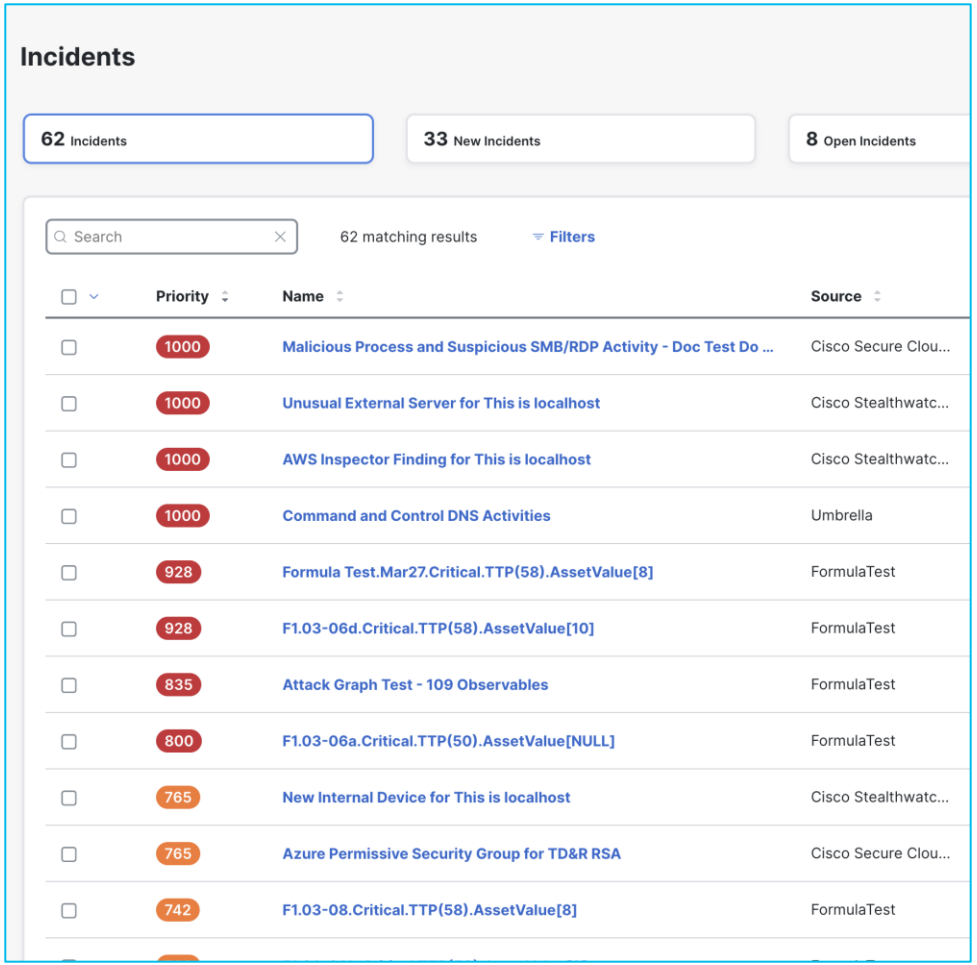
Prioritize by impact

- 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



Identify the most impactful incidents based on risk

1000

100	10
Detection Risk	Asset Value at Risk

Priority Score = Detection Risk x Asset Value

0-1000 | 0-100 | 0-10

The Incident total priority score used to prioritize incidents

Detection Risk composed of multiple values:

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

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

Walk through incidents step-by-step

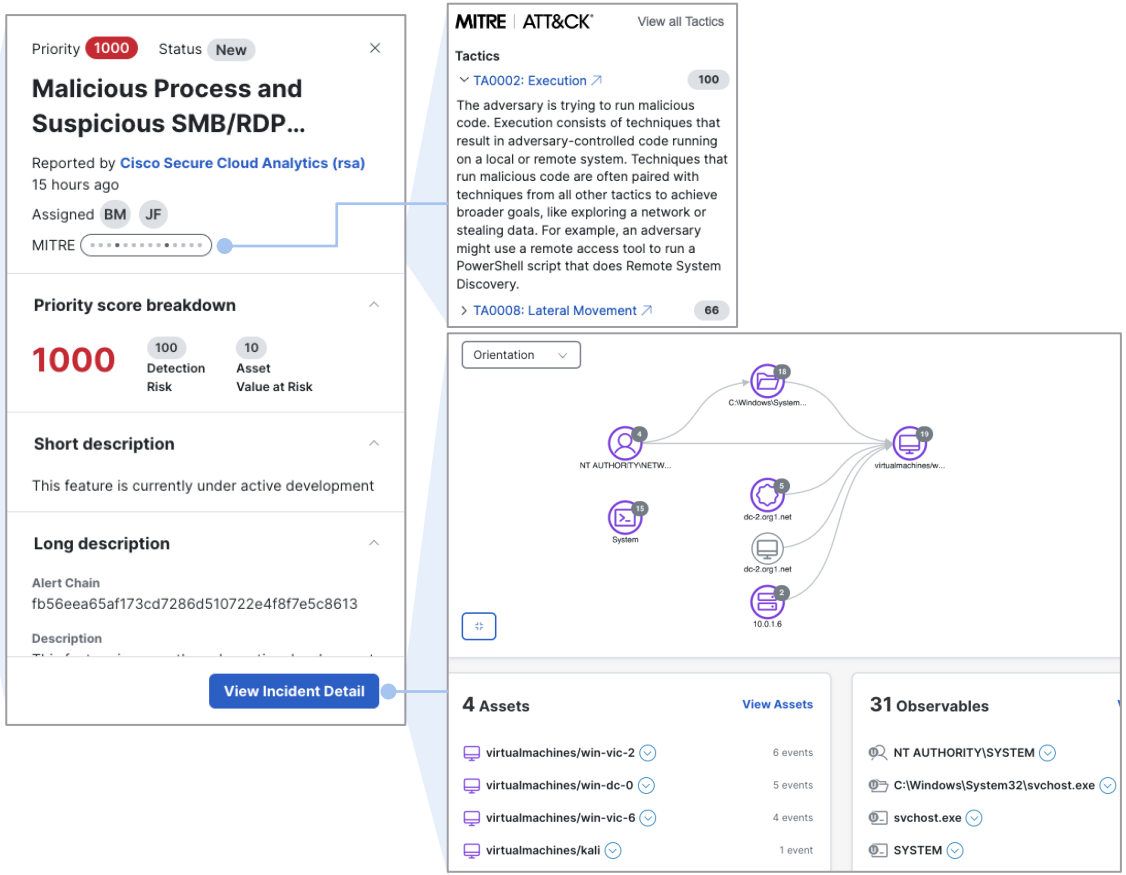
Progressive reveal of details

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

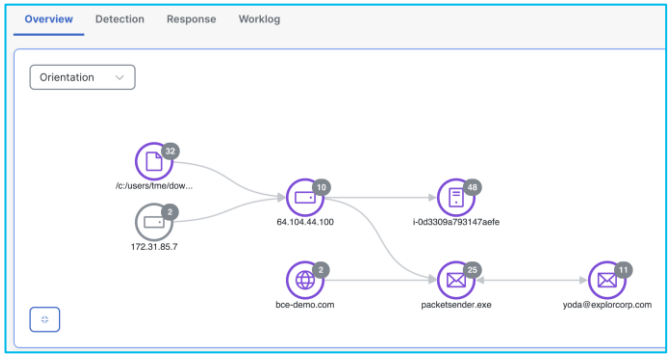
Priority	Name
1000	Malicious Process and Suspicious SMB/RDP Activity Detect
1000	Unusual External Server for This is localhost

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

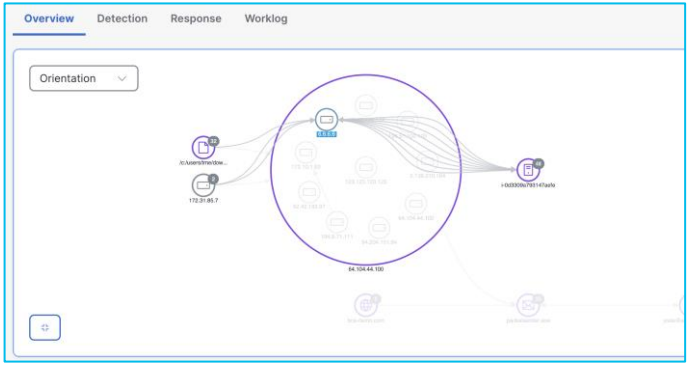


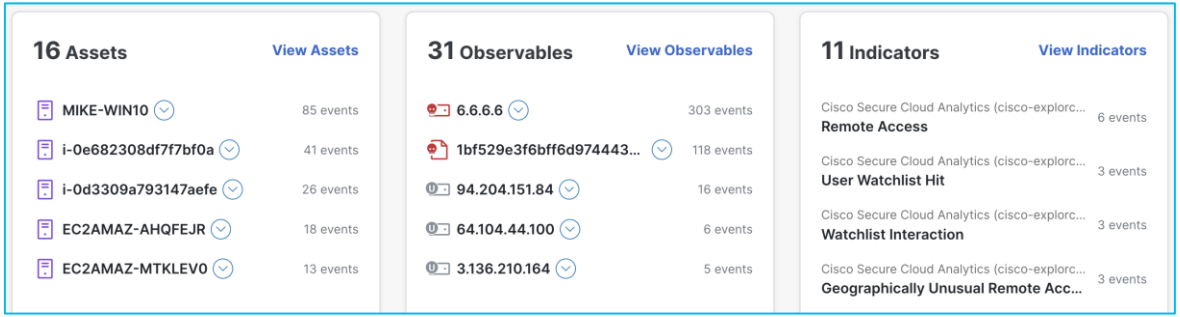
Walk through incidents step-by-step - Overview



Simplified Graphical view

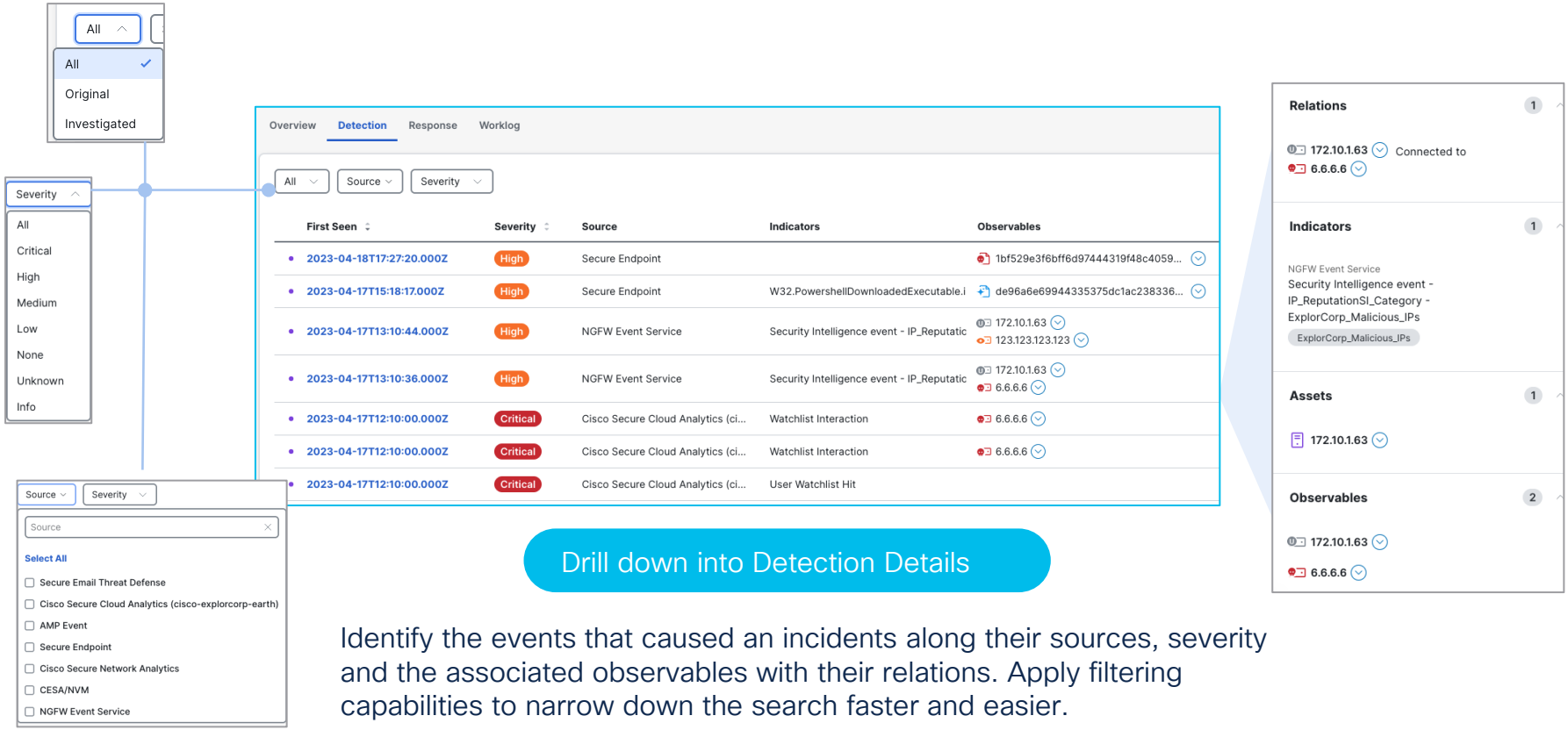
A simple yet powerful graph tool to identify observables and and their relations. Expand the view for additional details.





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.

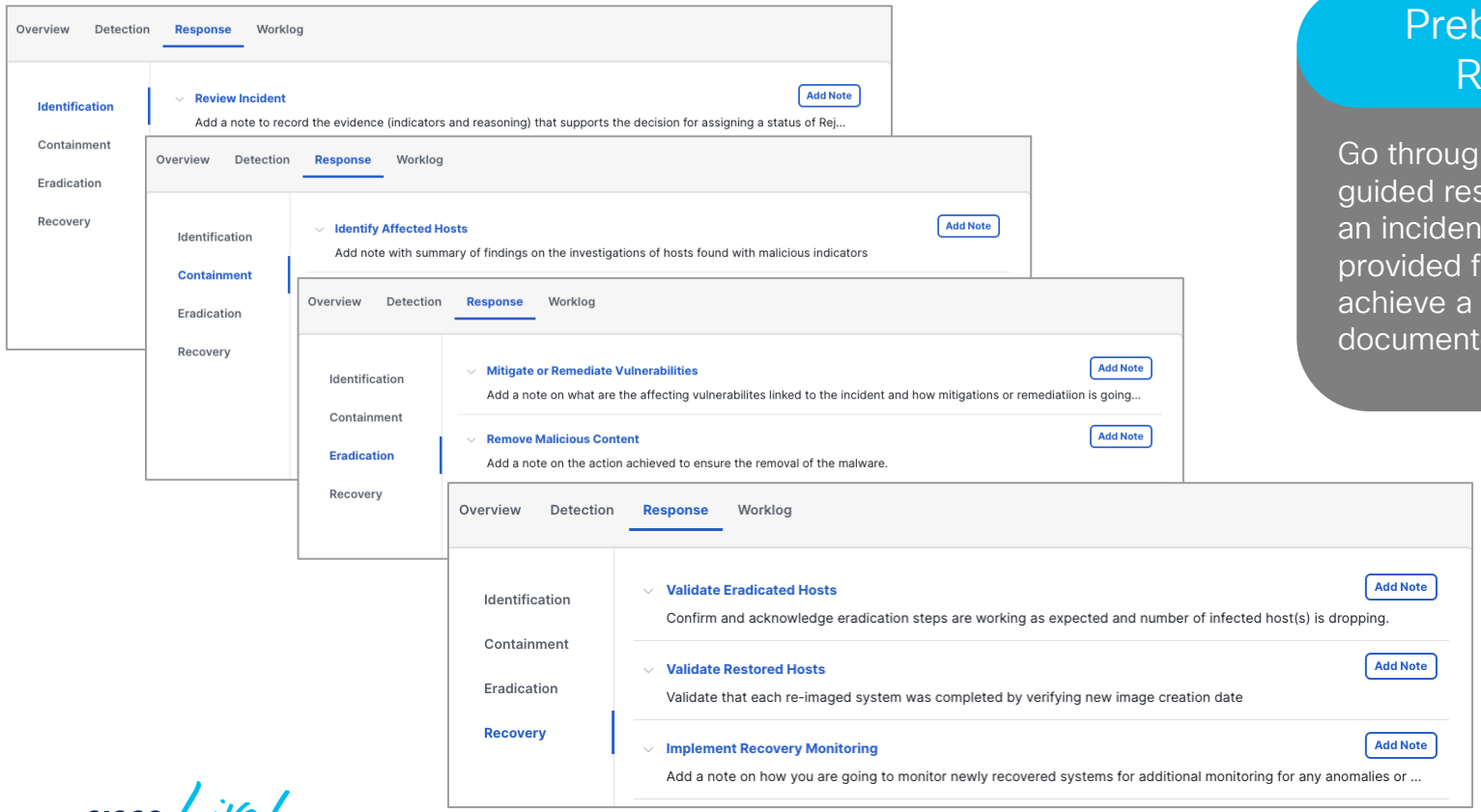
Walk through incidents step-by-step – Detection



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

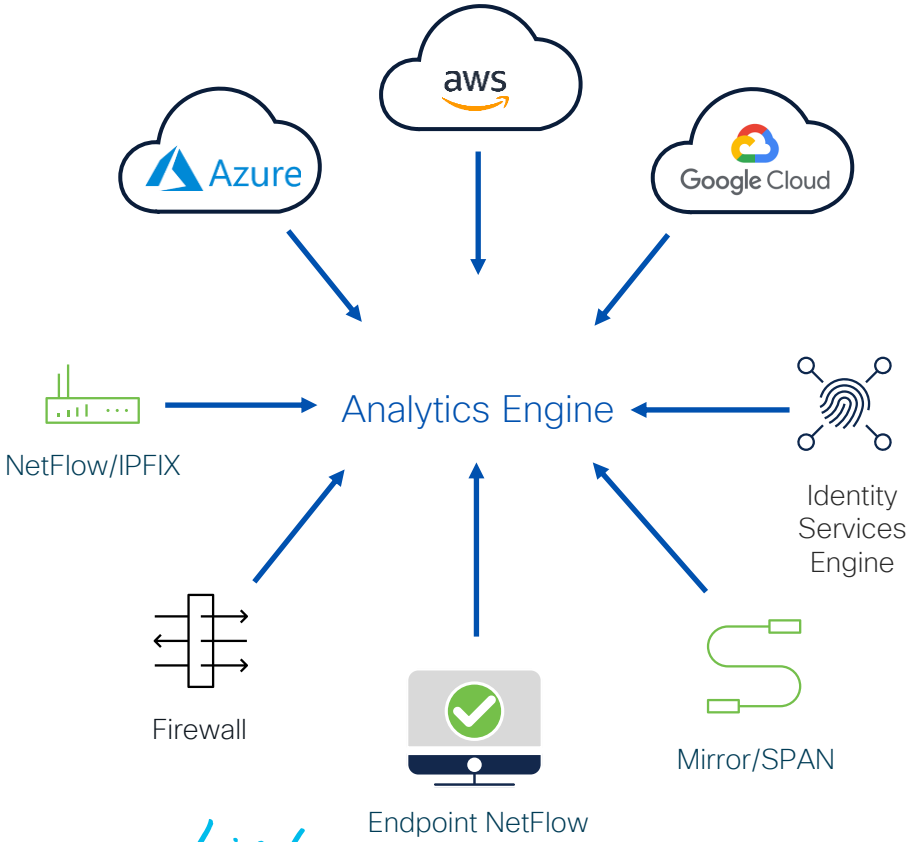


Prebuilt Guided Response

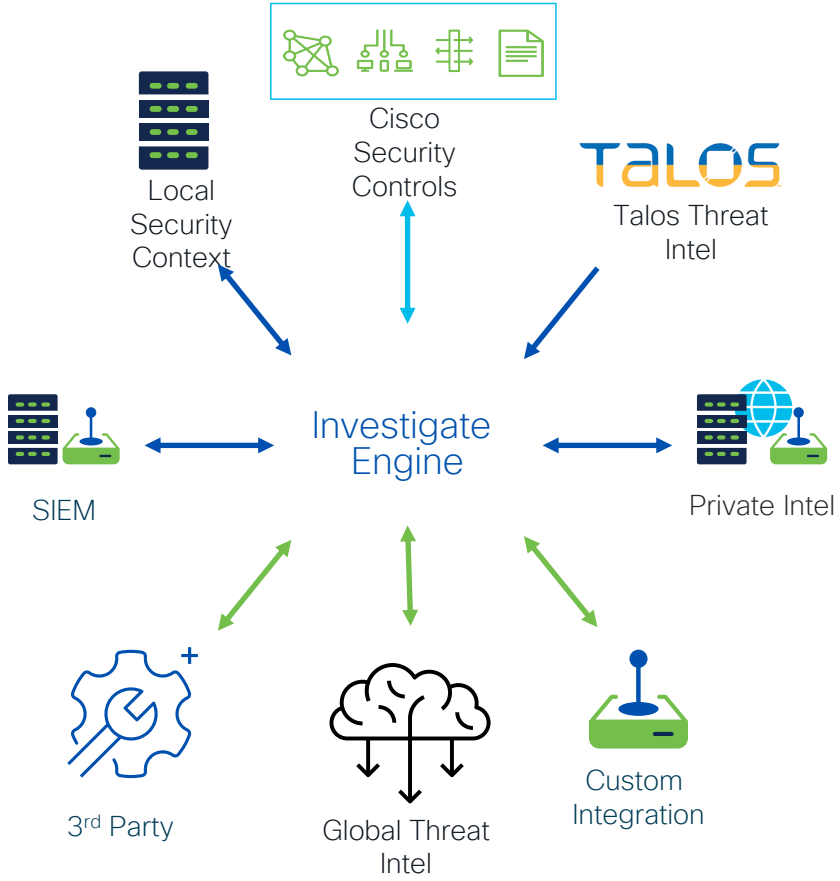
Go through a step-by-step guided response action for an incident using the provided flow of actions to achieve a faster and well documented response.

Integrations (Data Ingestion and API Enrichment)

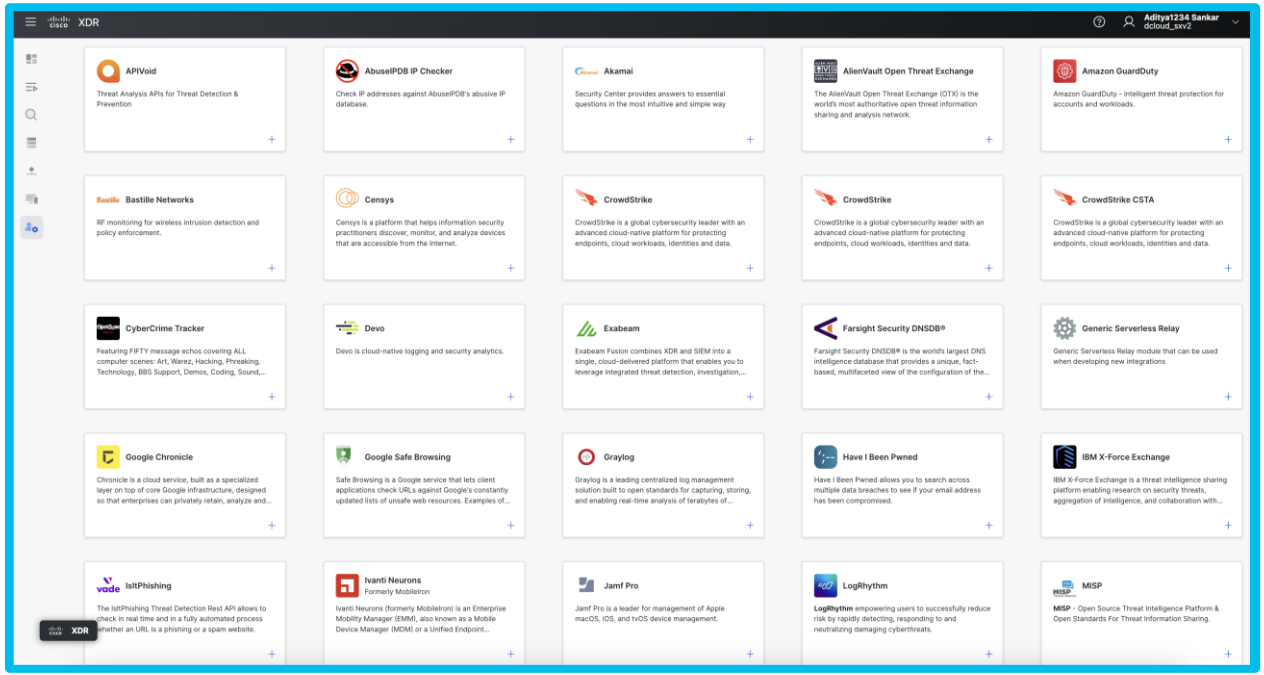
Data Ingestion



API Enrichment



Integrations for partner technologies



XDR Integrations API enrichment

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

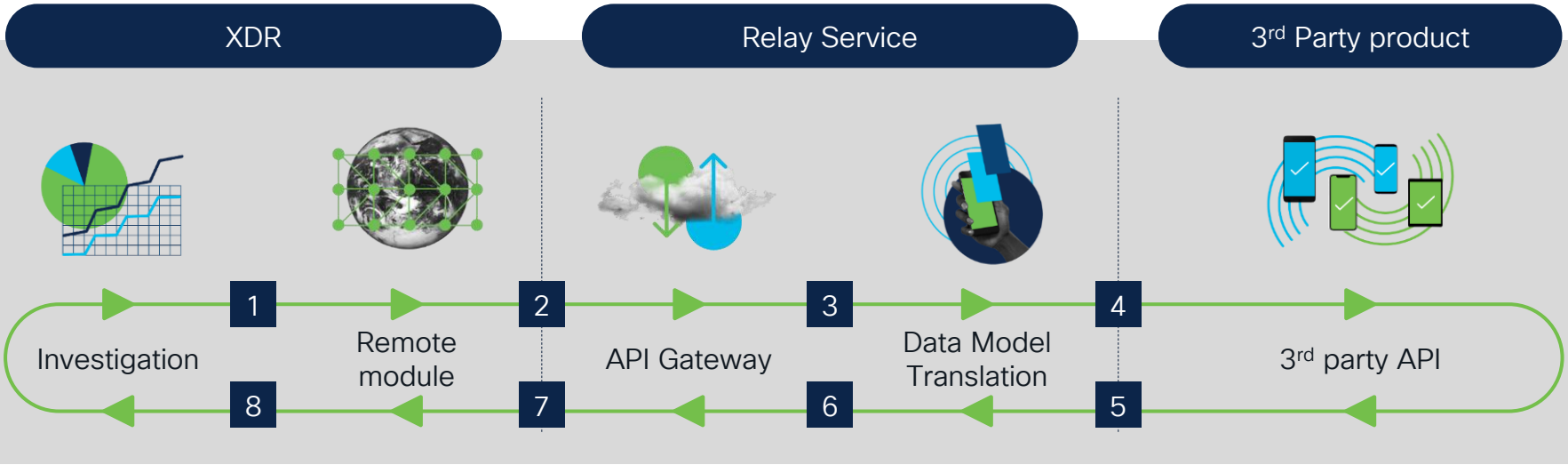
*Community/open source

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

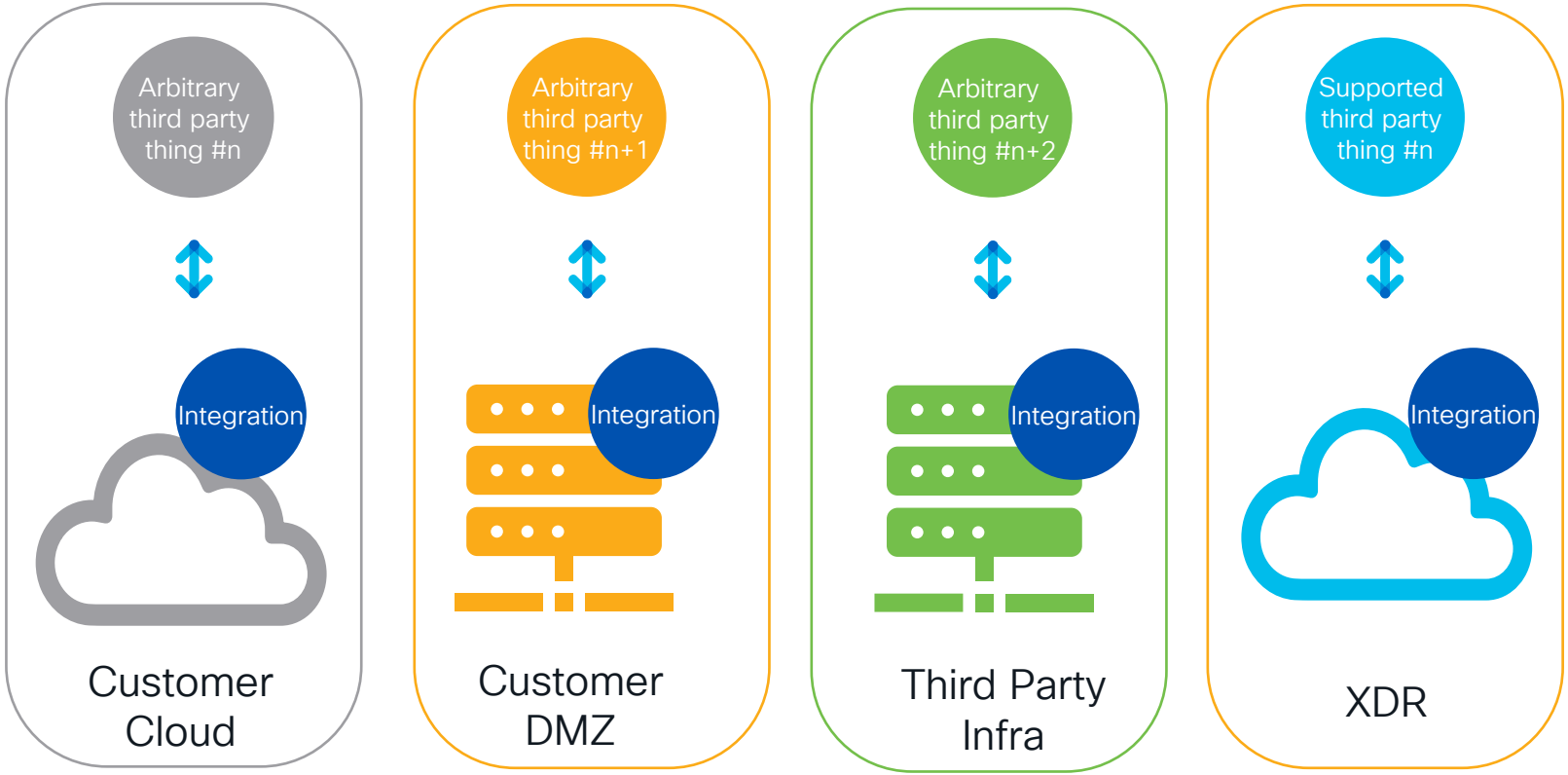
Relay API

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

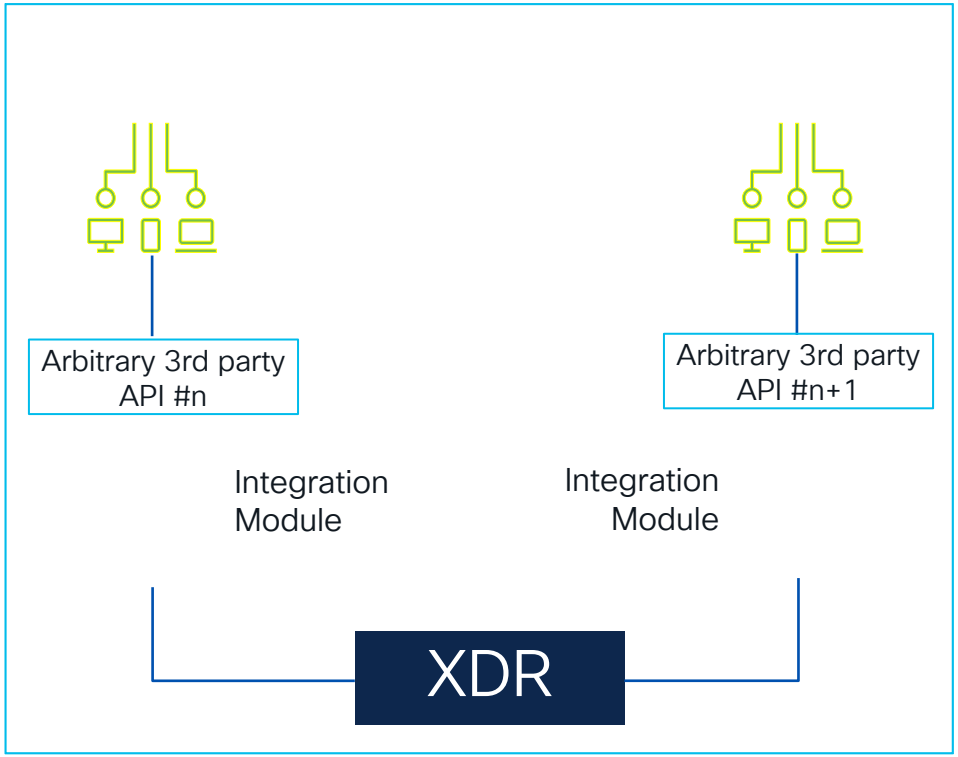
Bundle builder - http://cs.co/bundle-builder



Where do the relay servers live?



Integration Supported APIs



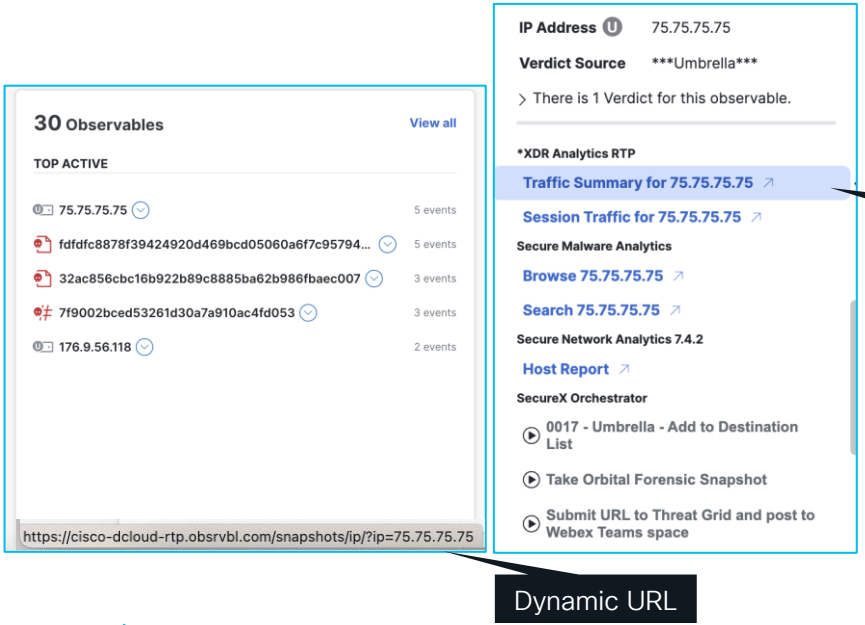

```
"supported-apis": [
        "health",
        "refer/observables",
        "observe/observables",
        "deliberate/observables"
        "observe/targets",
        "respond/trigger",
        "respond/observables",
        "tiles",
        "tiles/tile",
        "tiles/tile-data"
      ]
```

Integration Supported APIs

refer/observables

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

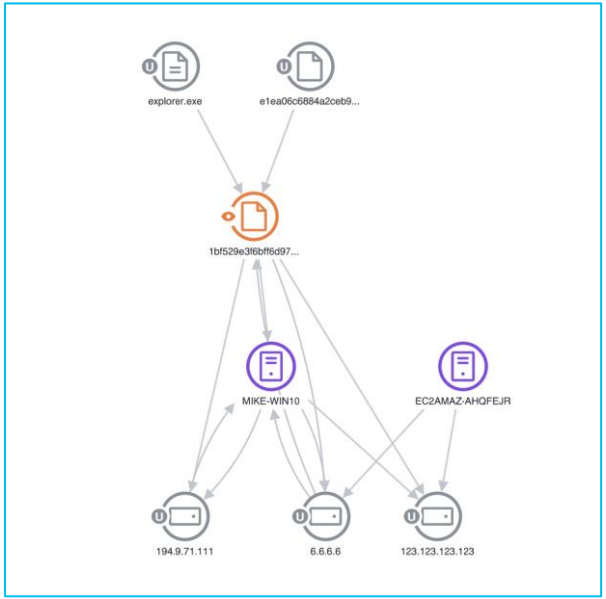
```
@enrich_api.route('/refer/observables',
methods=['POST'])
def refer_observables():
    token = get_jwt()
    observable = get_observables()
     json_refer = do_something_cool(url)
    return jsonify_data(json_refer)
```

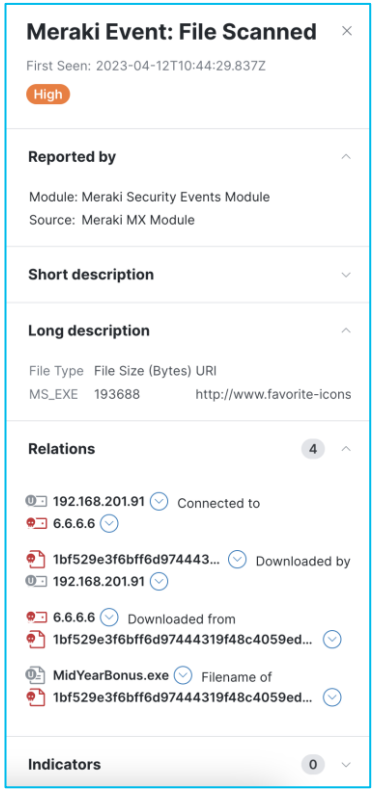


View the traffic summary for 75.75.75.75

Dynamic URL

Integration Supported APIs





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

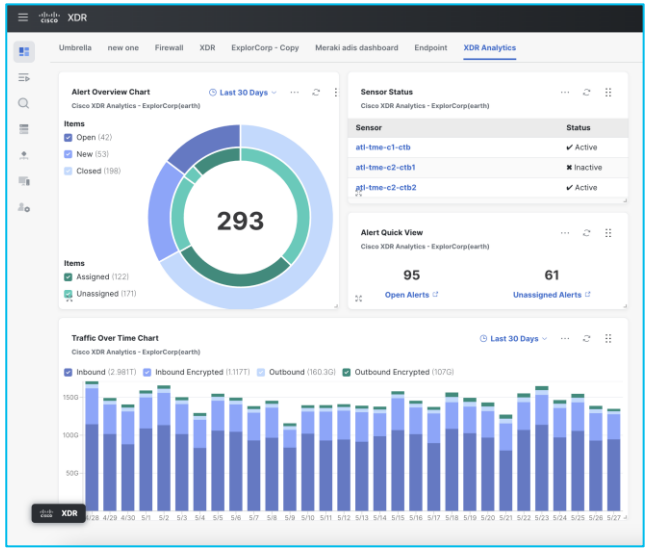
```
@enrich_api.route('/observe/observables', methods=['POST'])
def observe_observables():
    # Get JWT credentials and observables
    g.sightings = []
    # Iterate through observables and query sightings for each observable
    for observable in observables:
        response = query_sightings(observable['value'], 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()
```

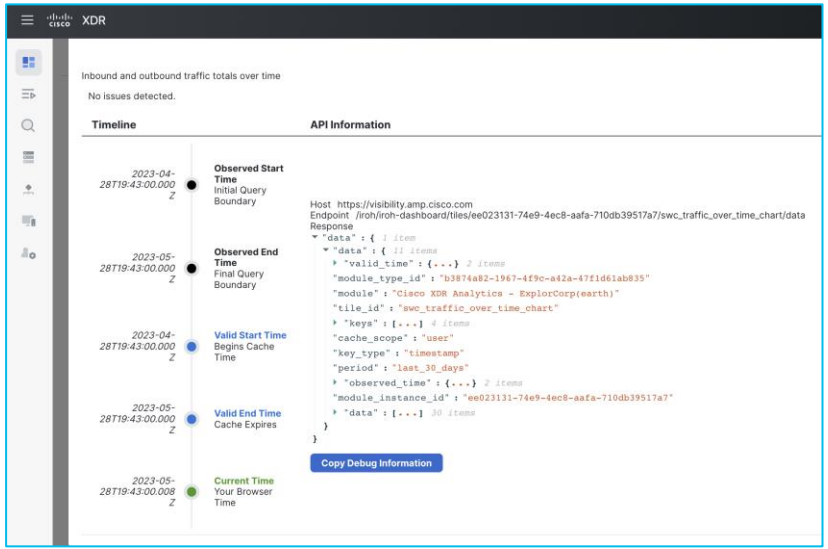
Integration Supported APIs

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

```python
@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({})
```

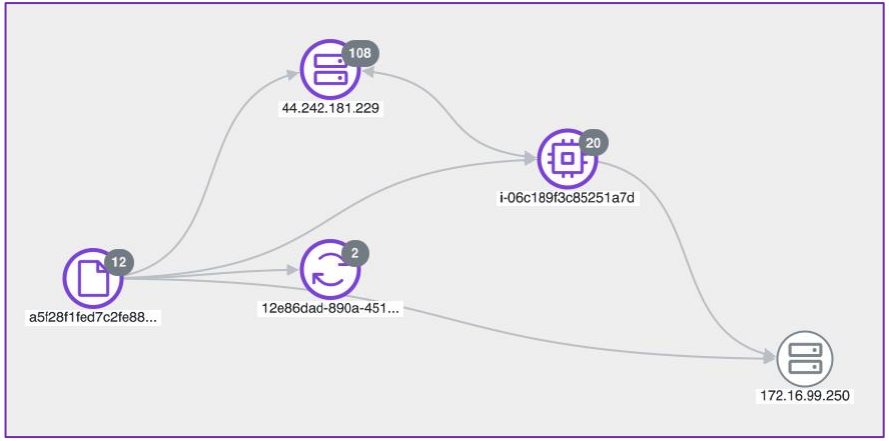


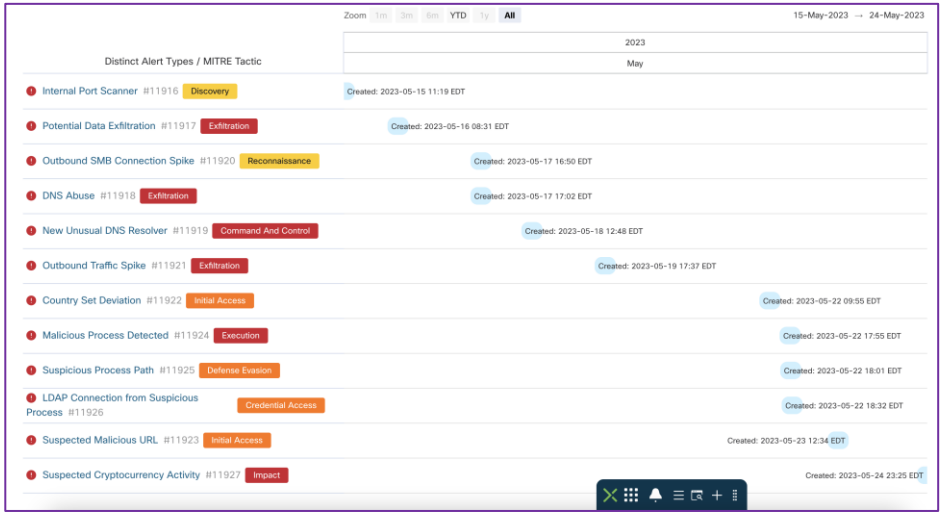


Investigate

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





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

Cloud security

Network firewall

Secure Web
Appliance

Have we seen these observables? Where?

Which endpoints connected to the domain/URL?

Response actions

Block destinations

Block files

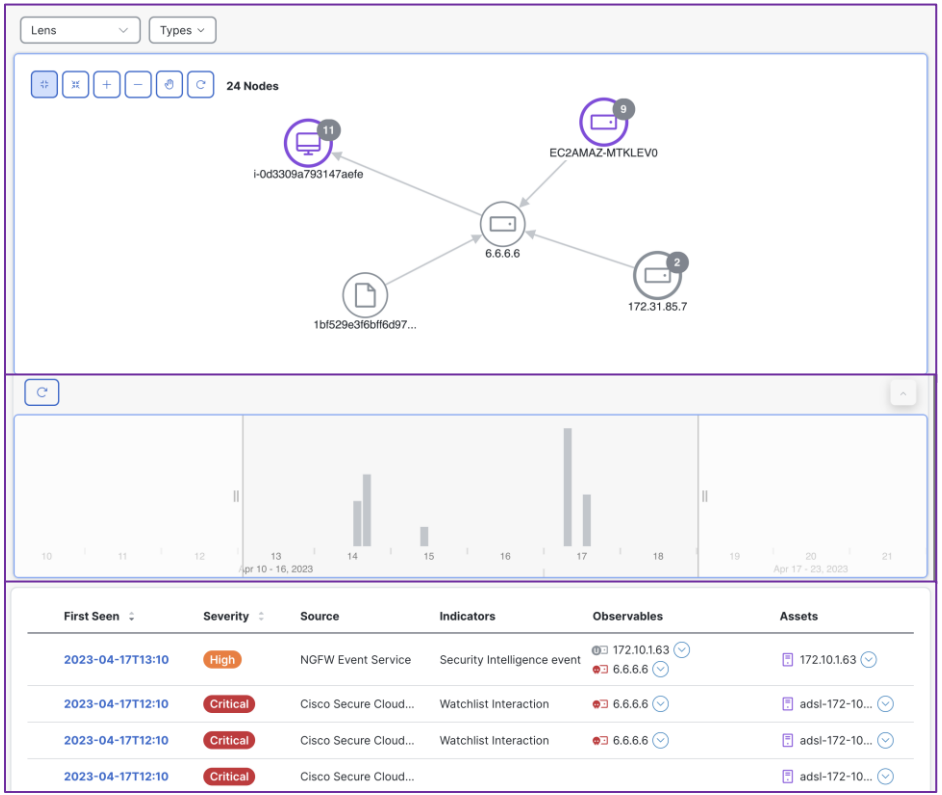
Isolate hosts

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
- 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

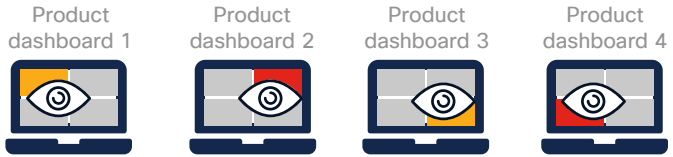


How true simplicity is experienced

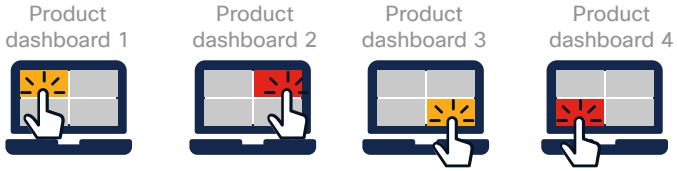
Without XDR: ~32 minutes

1. IOC/alert

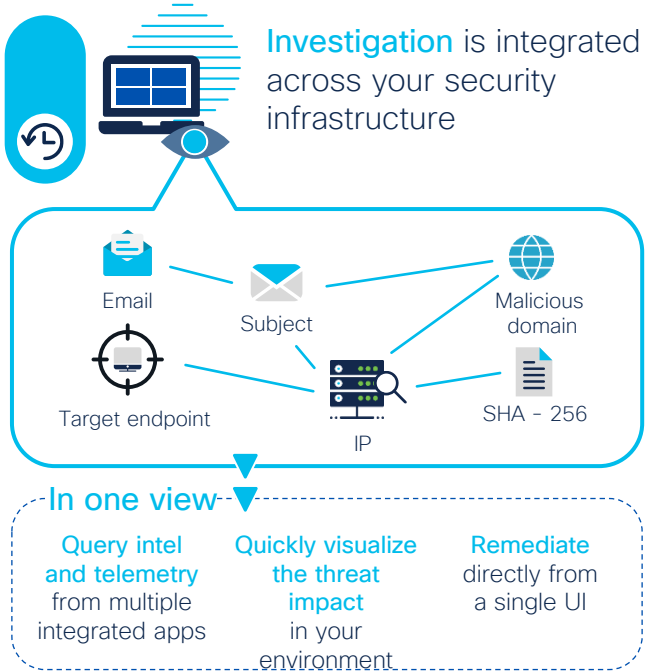
2. Investigate incidents in multiple consoles



3. Remediate by coordinating multiple teams

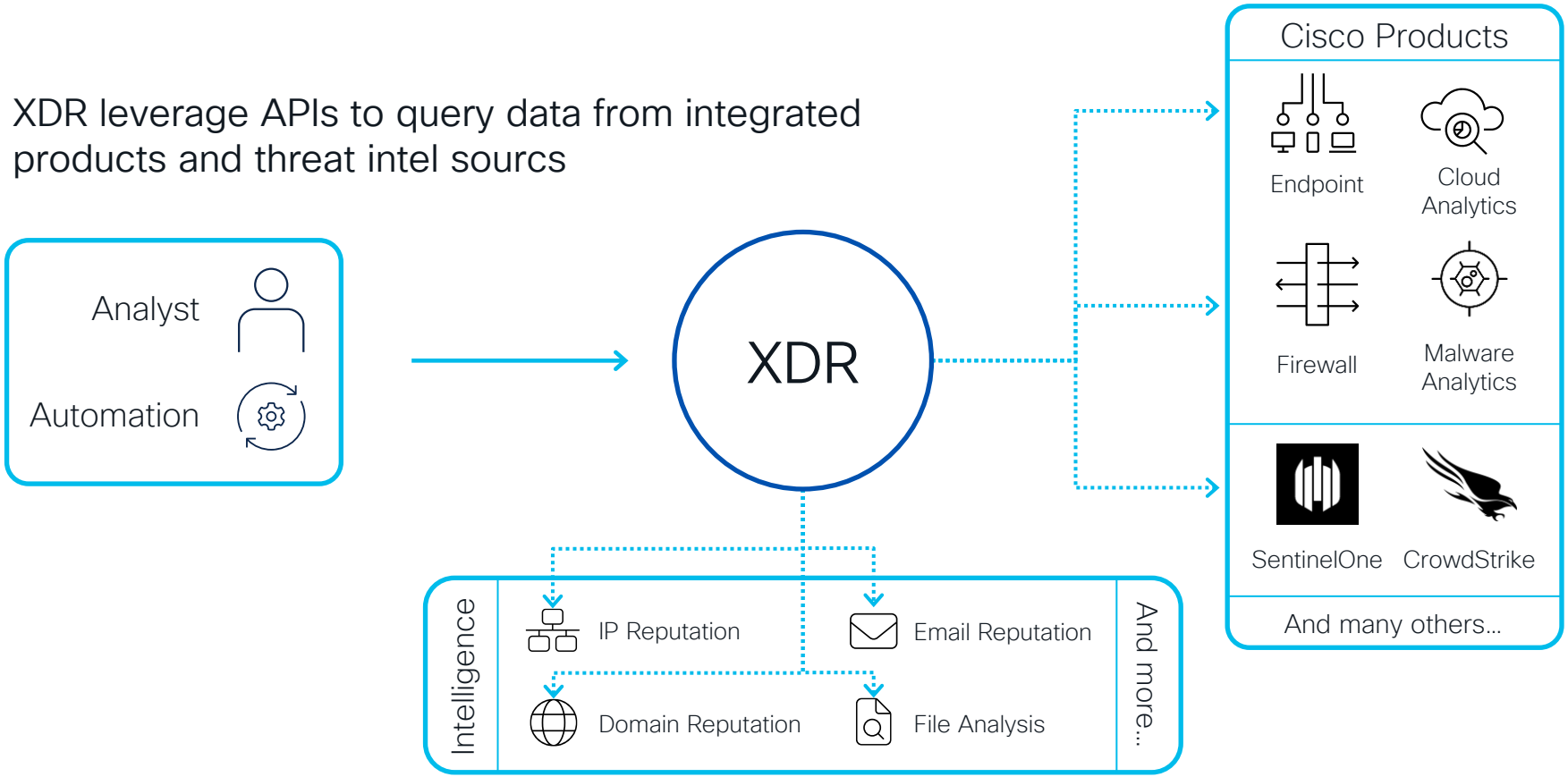


With XDR: five minutes



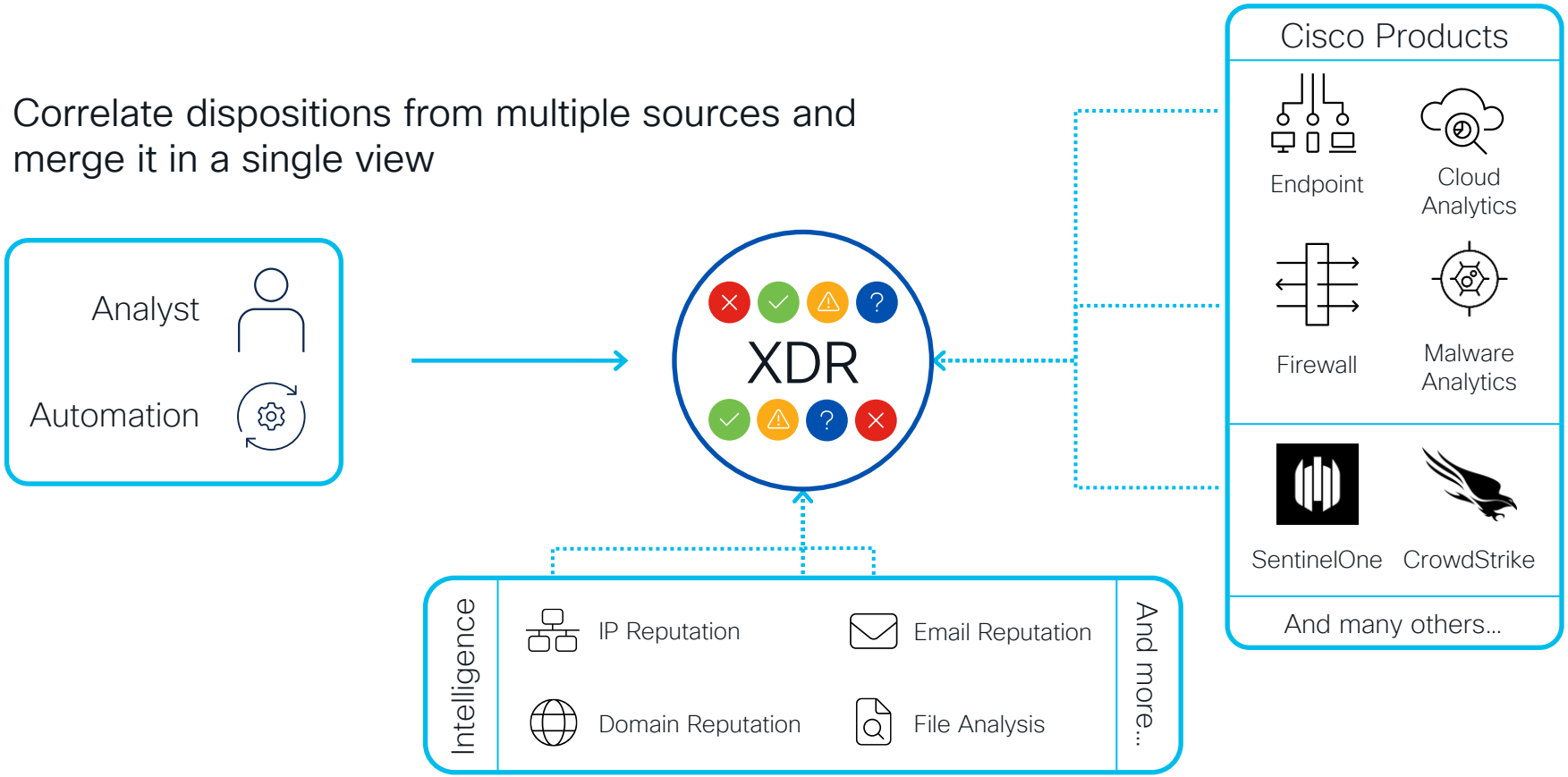
Investigation query integration and threat intel

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

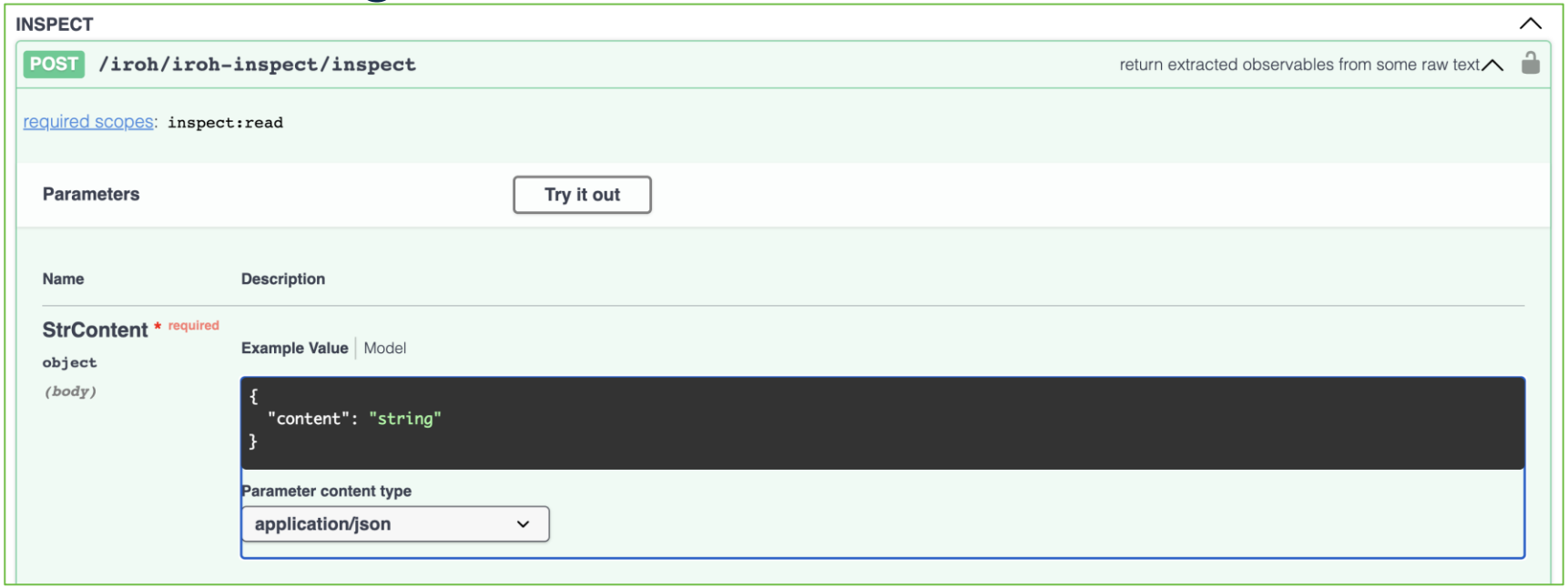


Correlate and merge information

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



XDR Investigate API's



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.

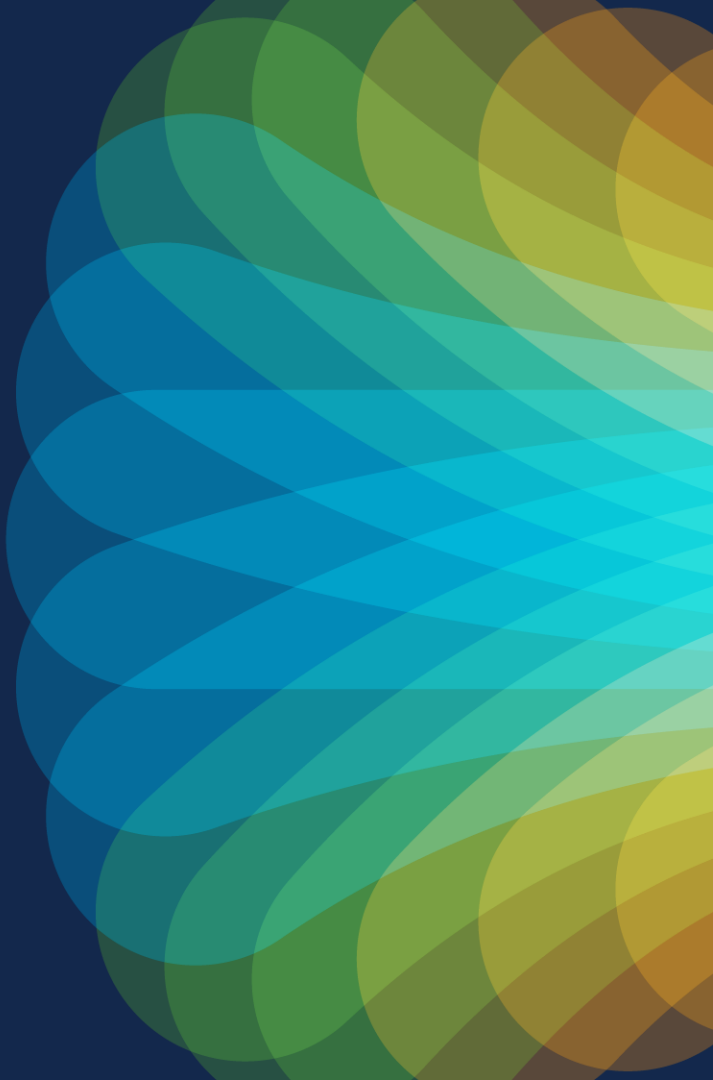
```
{
"content":
"some_string_containing_6.6.6.6_observables"
}
```

XDR Investigate API's


```
[
  {
    "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

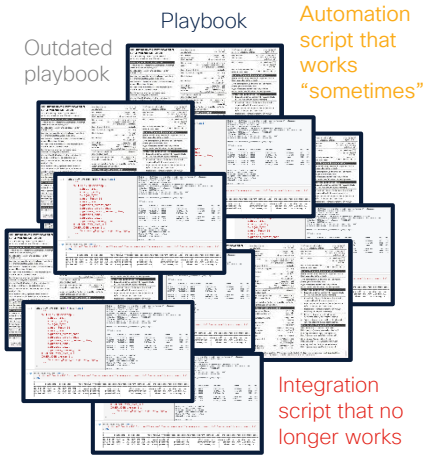
Unique turnkey approach to quickly integrate with other systems and solutions to expand your toolbox

Scale

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

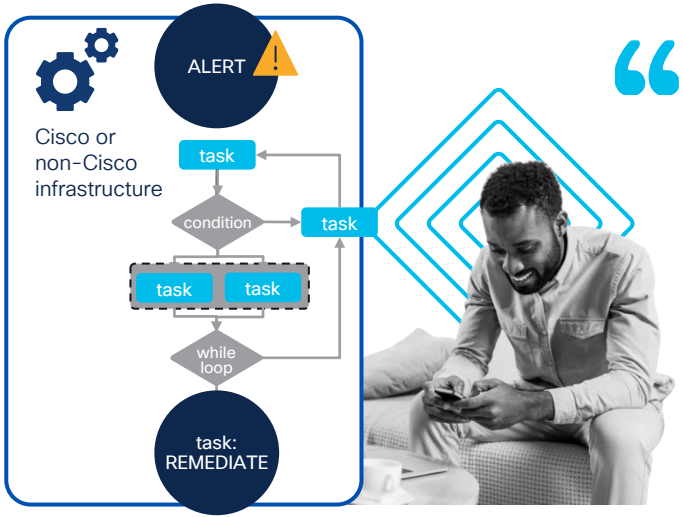
Maximizing operational efficiency

Before: Repetitive, human-powered tasks



Solution: Orchestrating security across the full lifecycle

Pre-built or customizable workflows



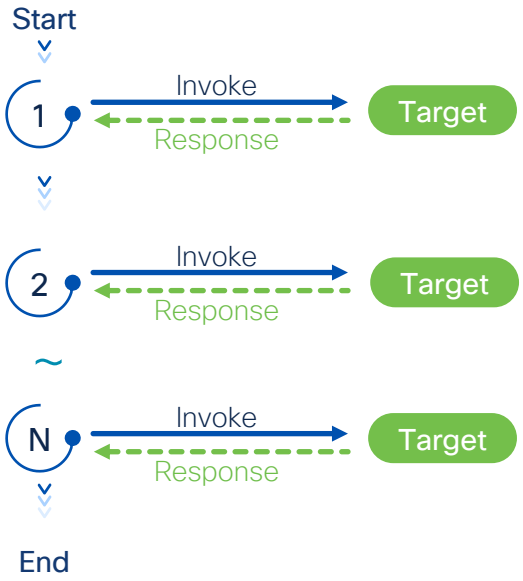
After: I combined 9 tasks across 3 security tools, 2 infrastructure systems, and 3 teams in one keystroke!

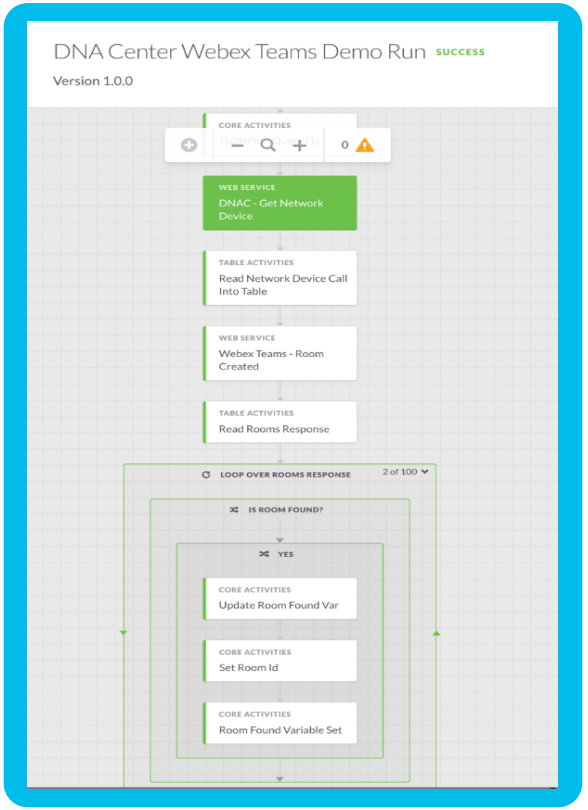
"I make automated playbook changes in minutes with a drag-drop interface

We have never communicated faster: Our approvals are automated

My top 5 most frustrating tasks have all be automated

XDR Automate





Core concepts

FYI

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.

FYI

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.

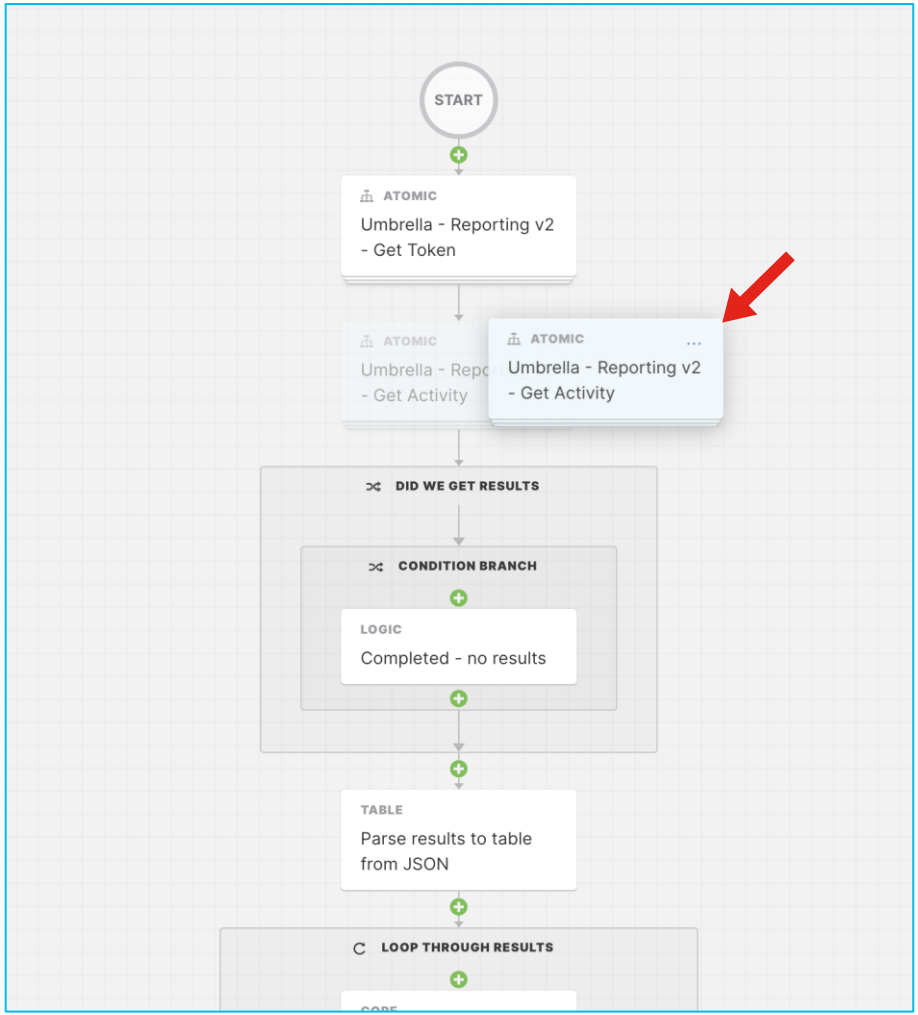
Remotes

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

What is a workflow?

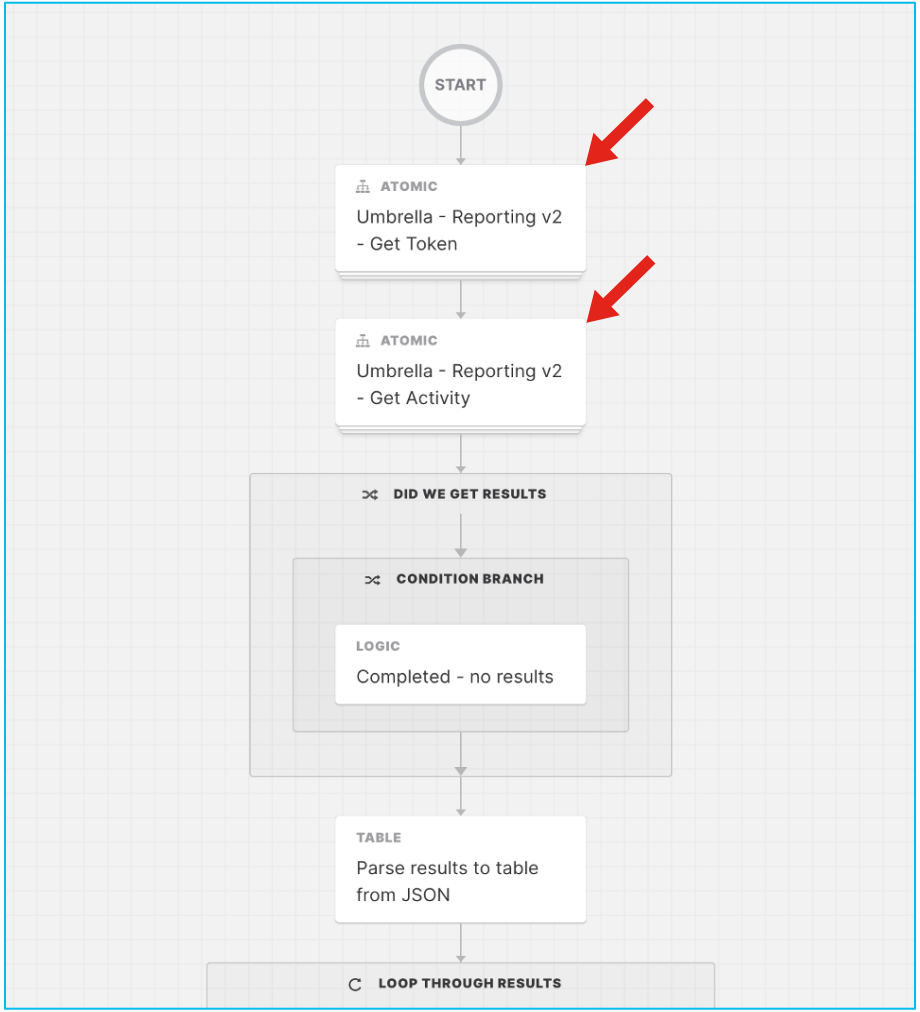
Simple or complex series of actions that accomplish a specific outcome.

- 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

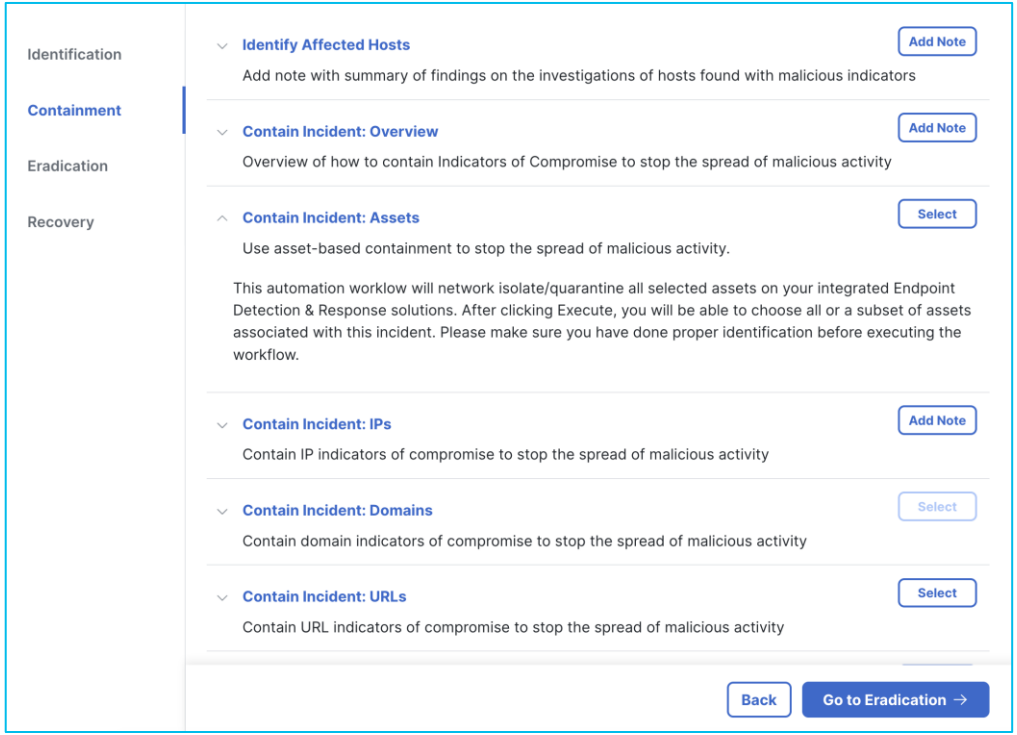
An incident matches a pre-defined rule and a workflow is triggered

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



Response

Response Trigger

Cisco XDR

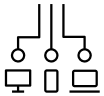
- Incident Management
- Scheduled Workflow
- Webhook or Trigger

Trigger

- Identify module
- Identify Observables
- Load module Variables
- Execute Actions

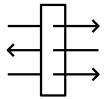
Use API

Cisco Products

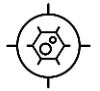


Endpoint

Cloud Analytics



Firewall



Malware Analytics

SentinelOne

CrowdStrike

And many others...

Response Actions will be executed depending on the integrated module and the available actions. Including isolating hosts on endpoints, blocking IPs on firewalls, quarantining a mail in a mailbox

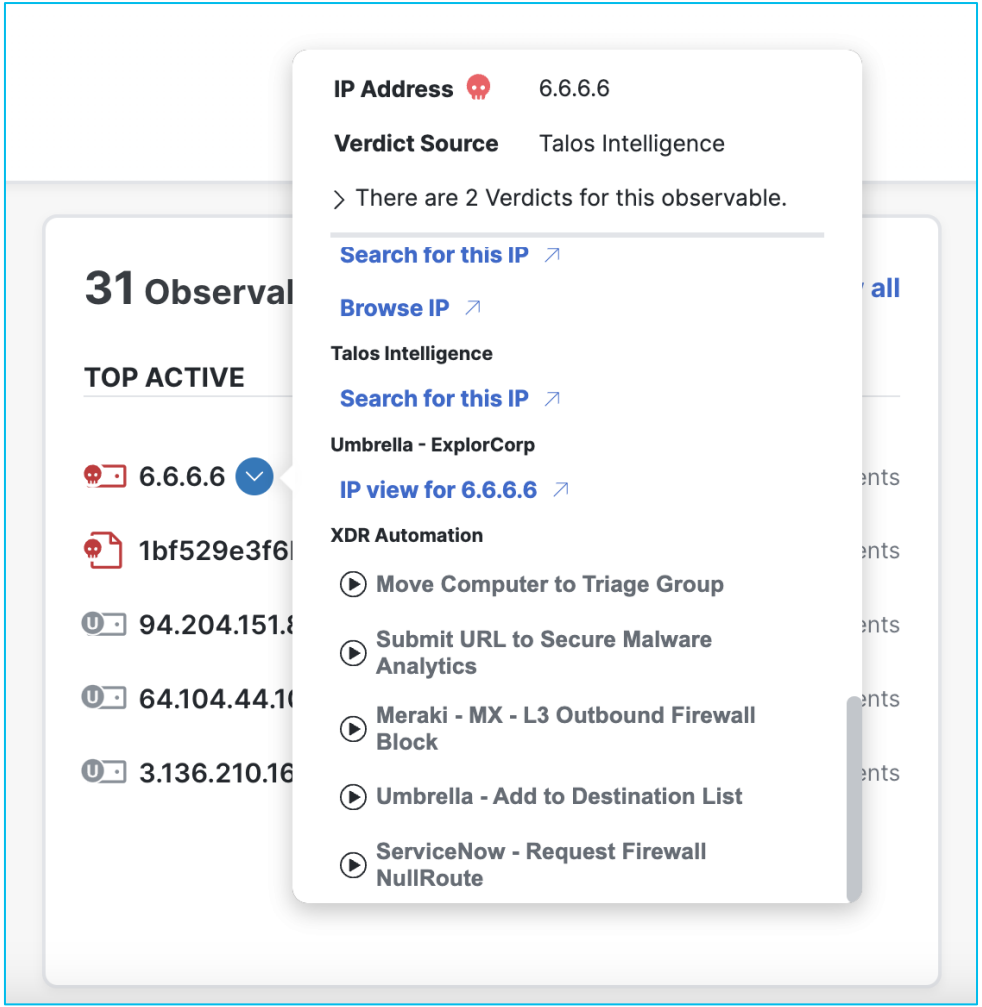
Pivot menu

Accessed by clicking the icon next to an observable:

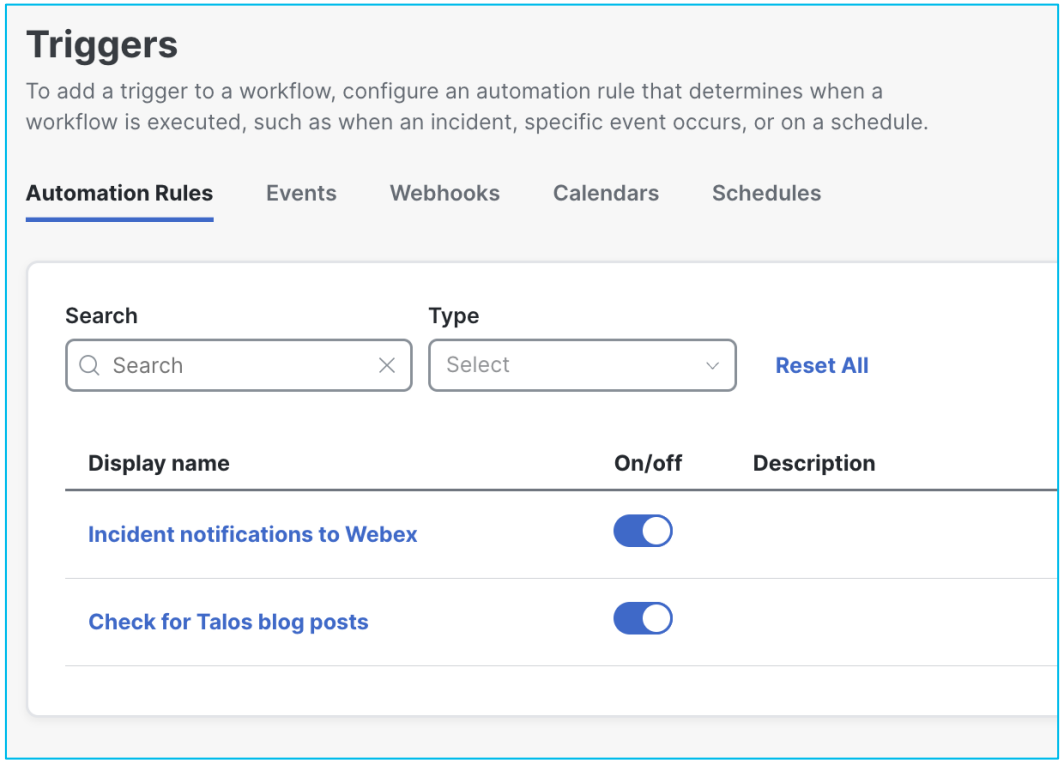
- During investigations
- In the incident manager
- While using the XDR ribbon

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



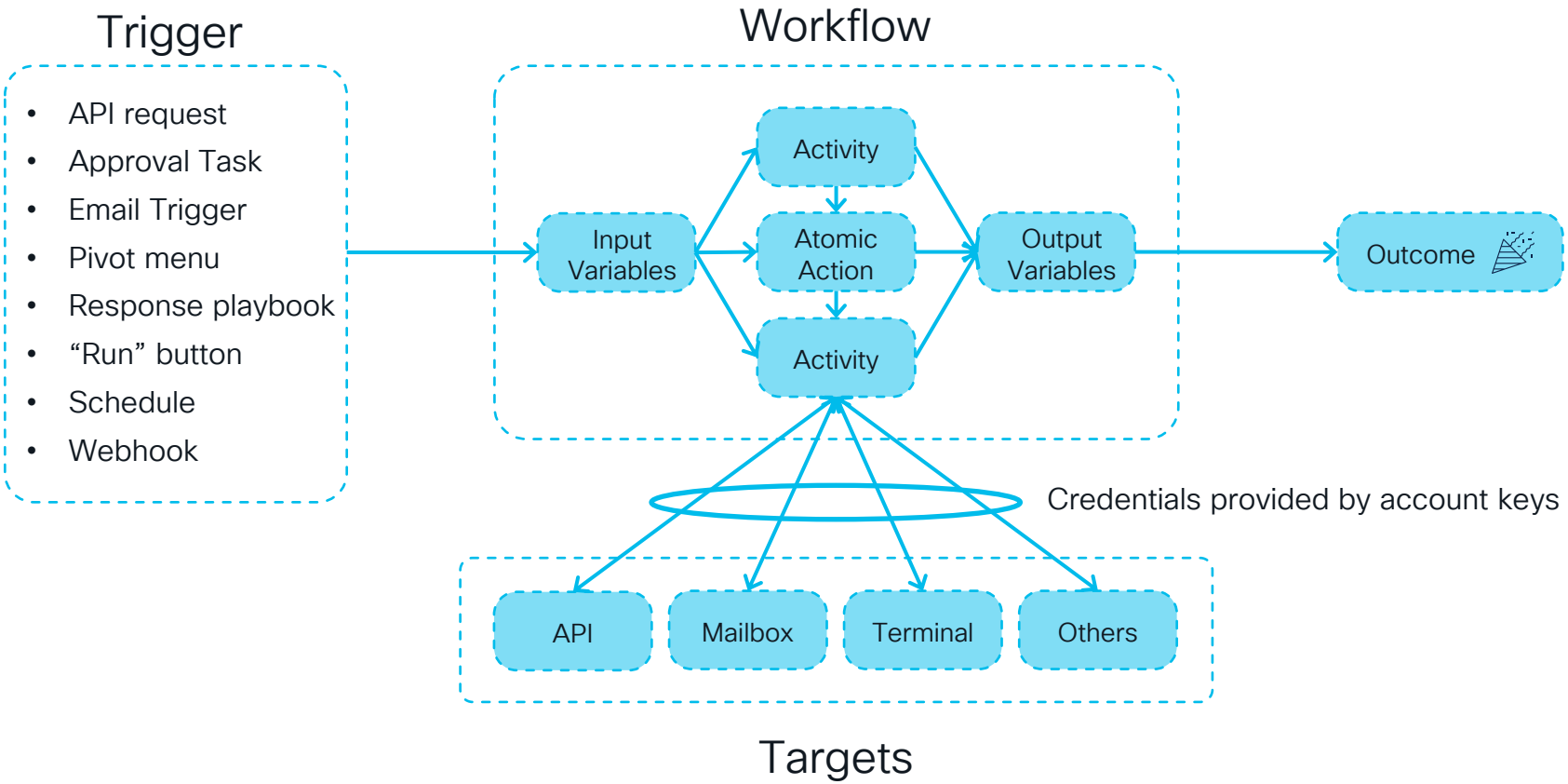
Automation rules



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

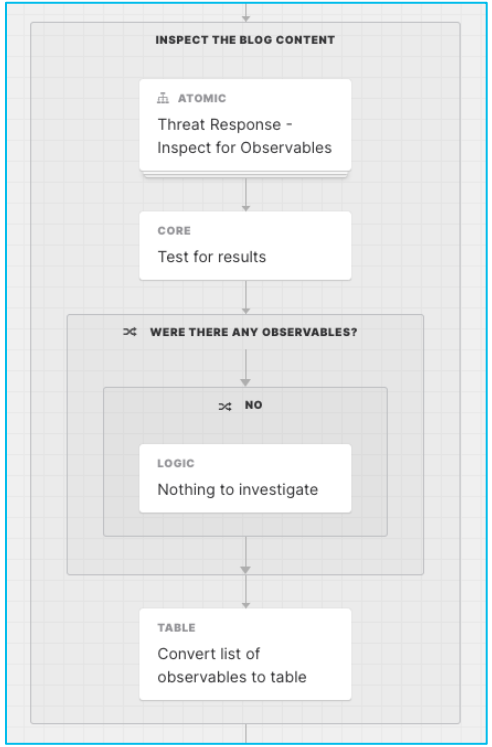


Automation, with the click of a button

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

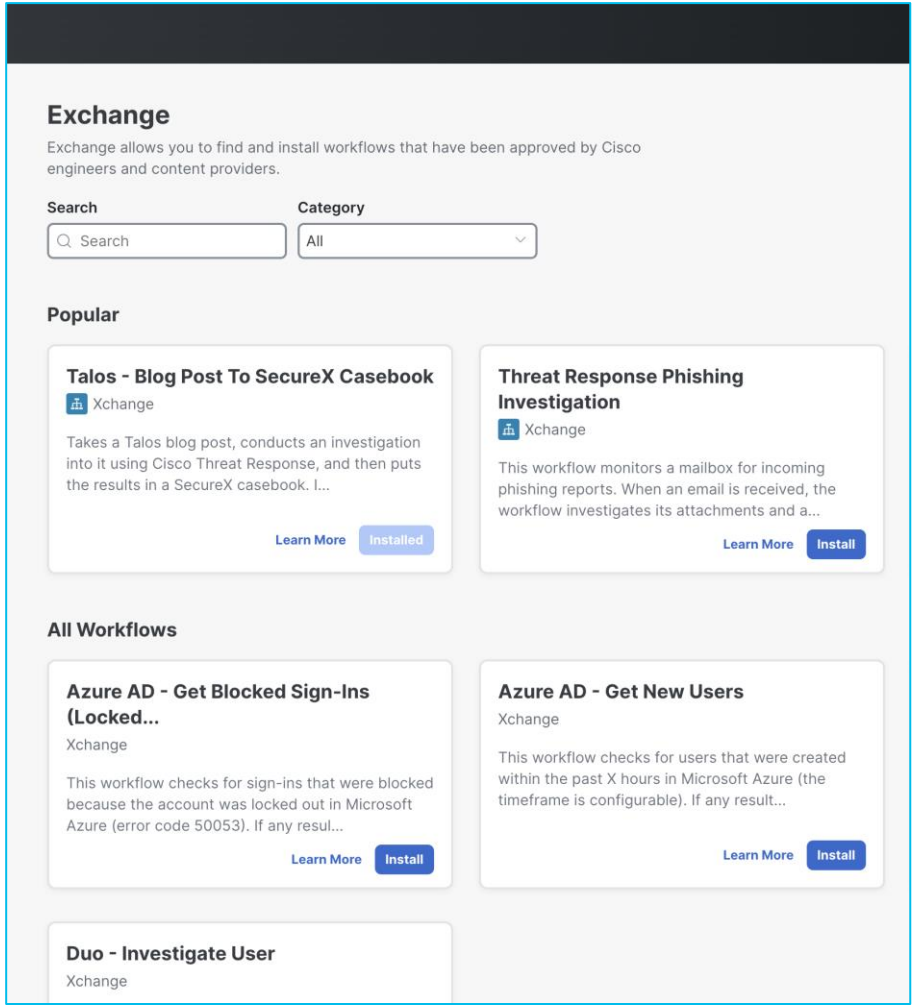


Exchange

Workflow ecosystem designed for discovering and importing content

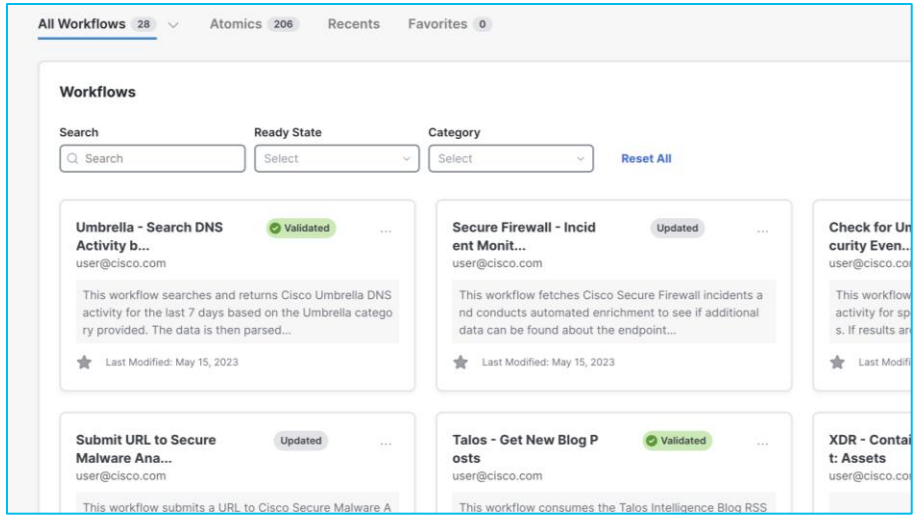
- Streamlined workflow installation process from within the orchestration console.
- Offers a searchable workflow index to find content easier
- Configuration wizard helps user configure the required targets/account keys upon installation

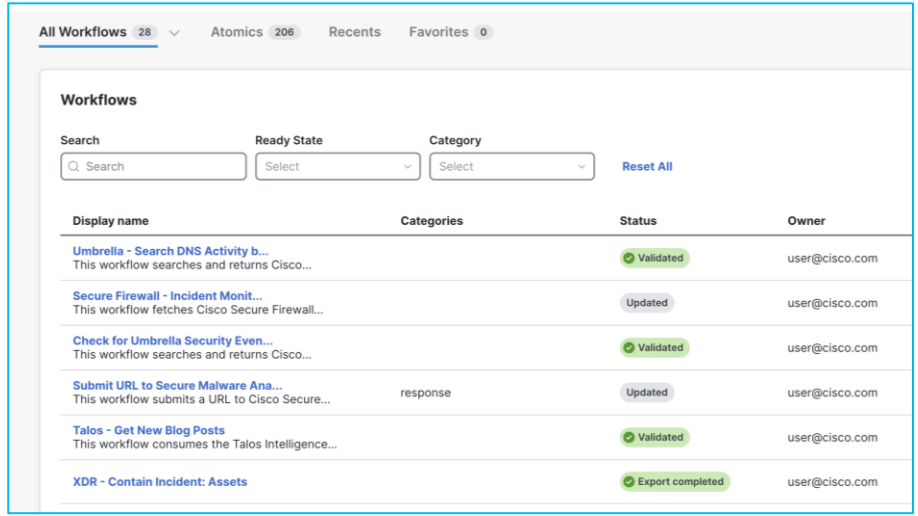
Benefits: Users can start automating with Orchestration in under 15 minutes – Getting value of XDR Orchestration is streamlined



Workflows and atomics

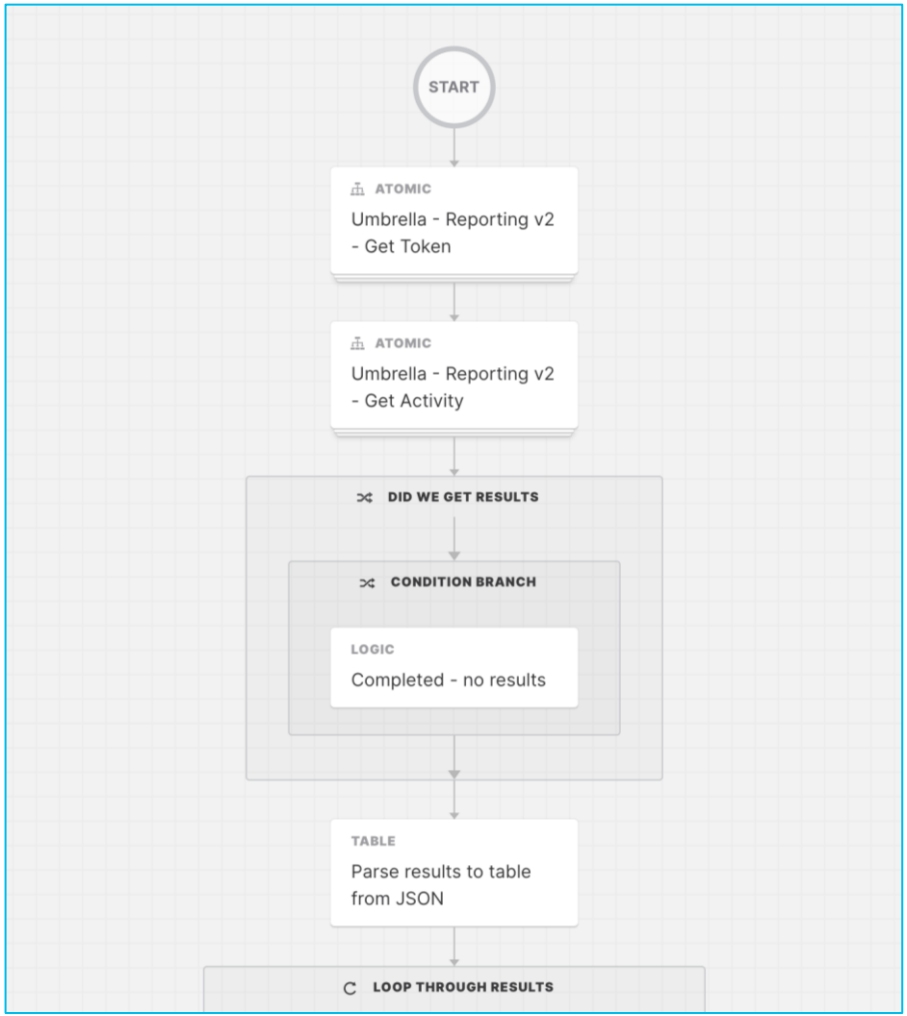
- Shows all the organization's installed workflows and atomic actions
- Card view (default) or list view
- Tabs for workflows, atomics, recent workflows, and favorited workflows.
- Workflows can be favorited by clicking the star icon on their tile or list row
- Workflows can be searched





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

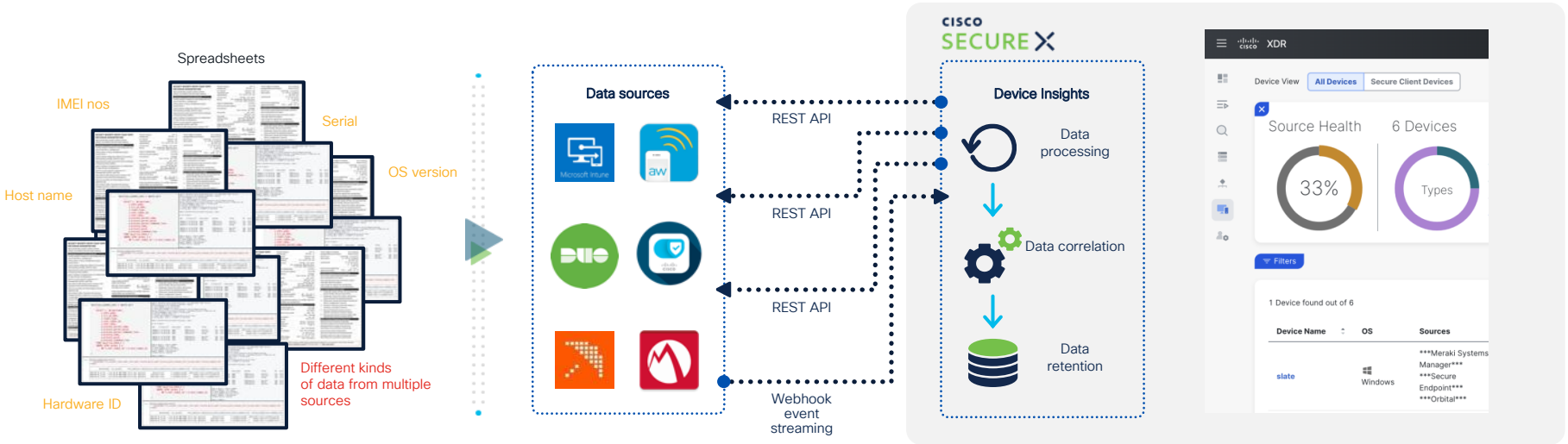
Configuration and management of Cisco Secure Client
Cloud-based management of Secure Client profiles and deployments

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!

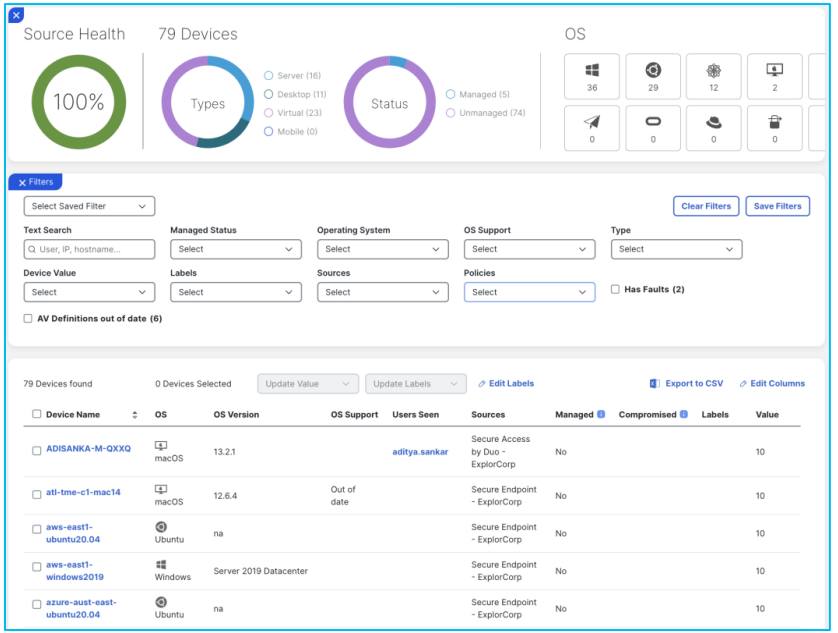


What is Device Insights?

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.

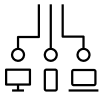
With Device Insights, you'll be able to answer these all-important questions:

- 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

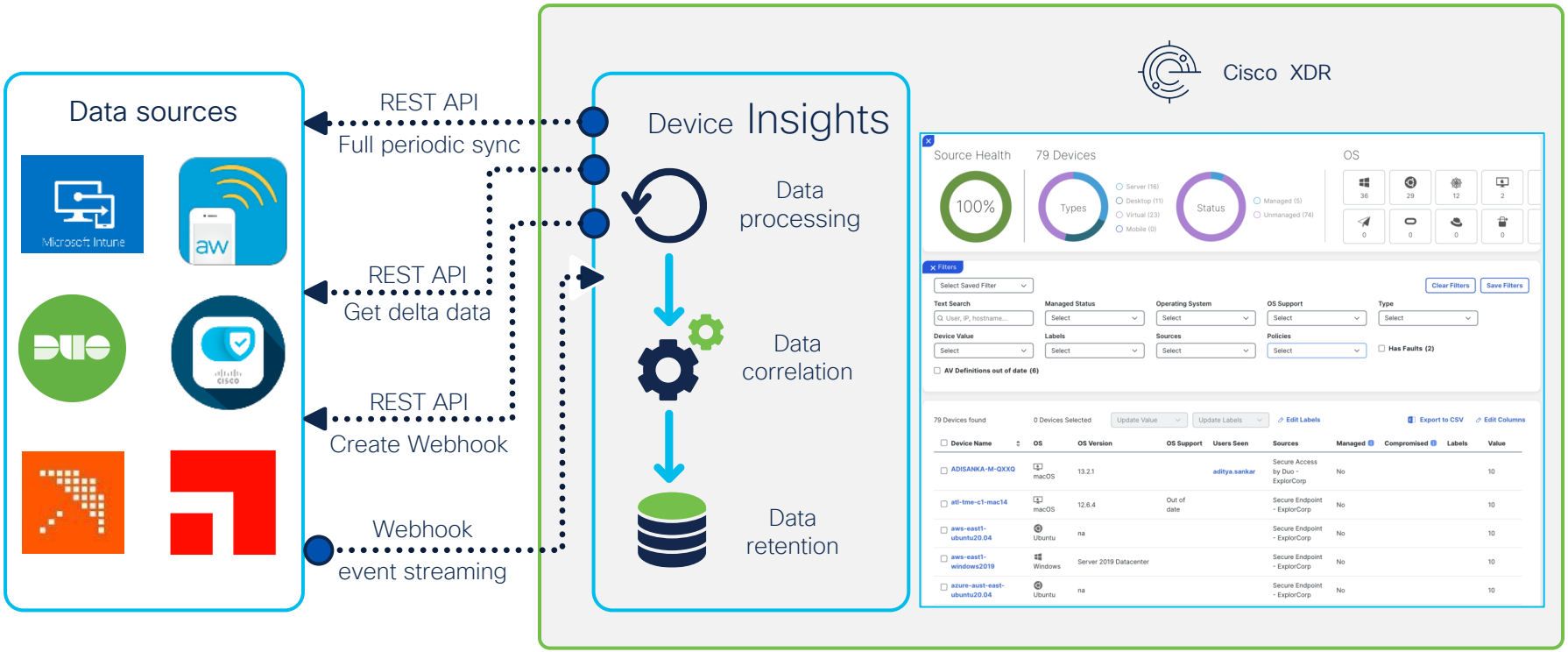
Deduplicate

Remove duplicate or insignificant details from each record

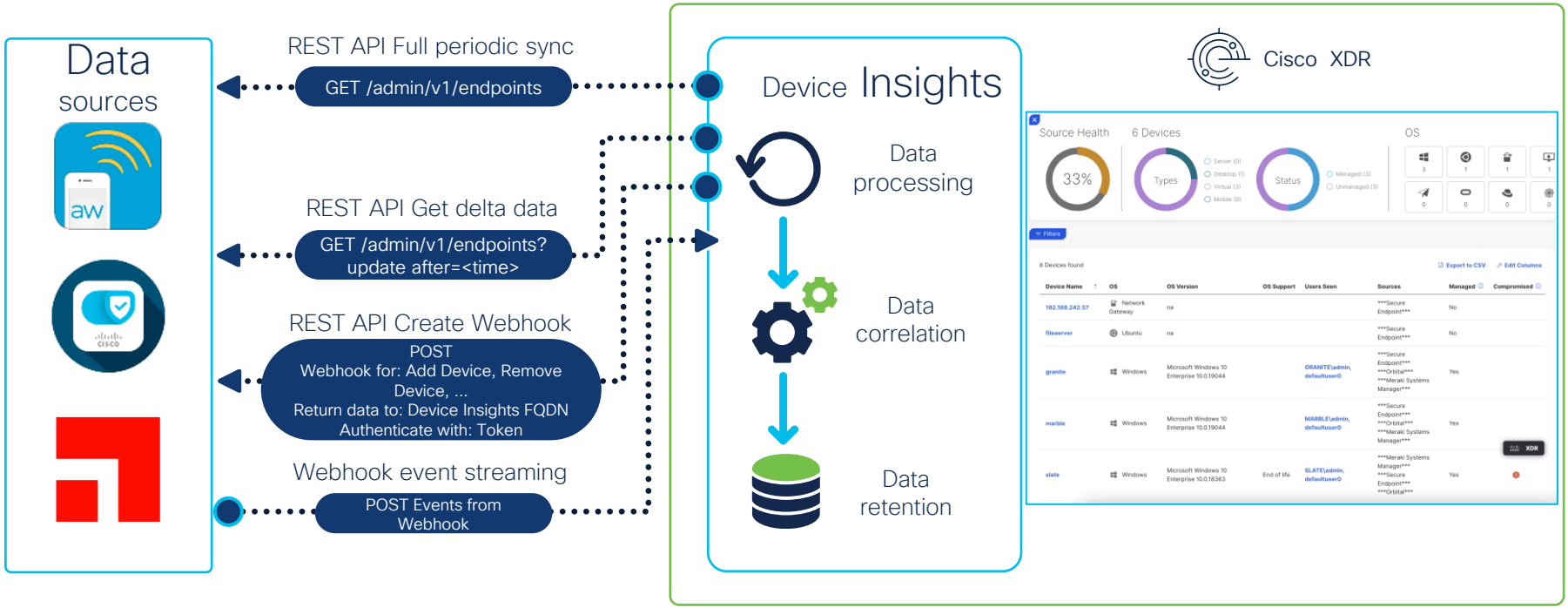
Correlate

Combine different records for the same device into one unified record

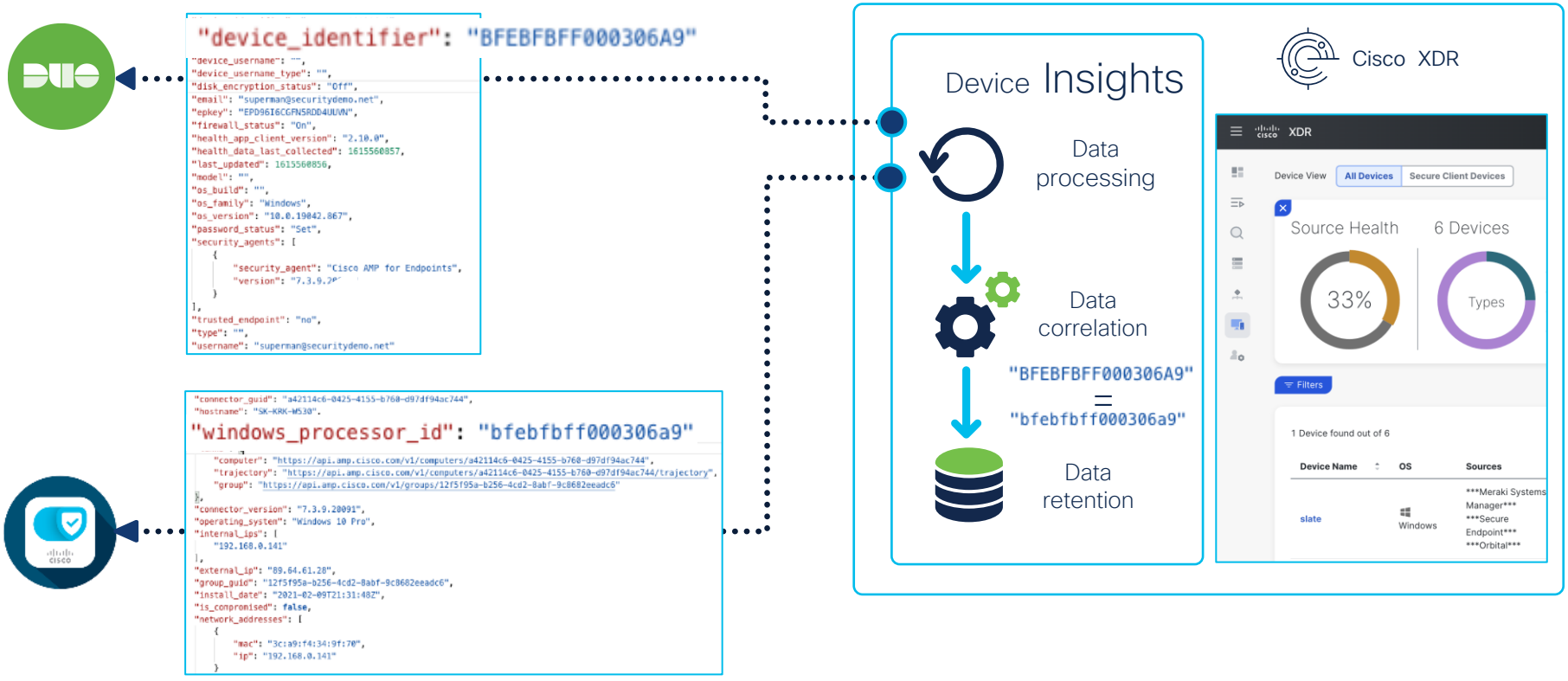
XDR Device Insights high level architecture



Communication methods - examples



Data merging example (simplified)

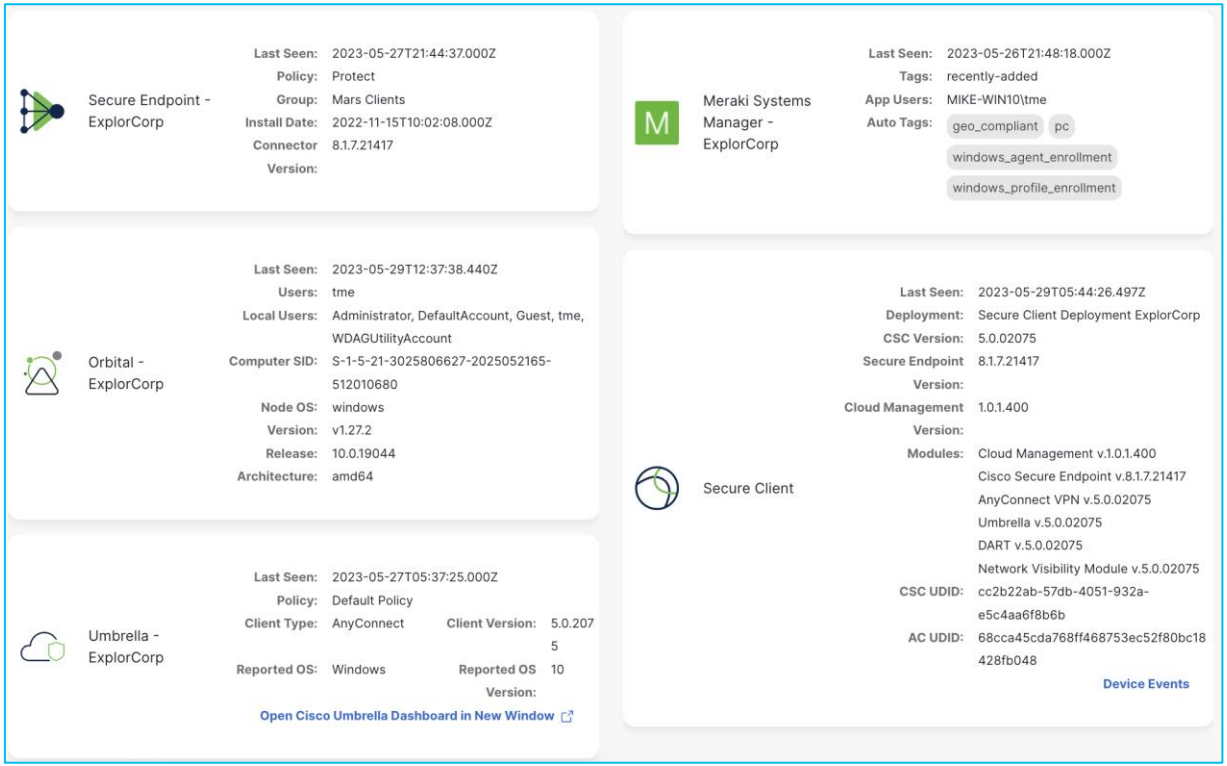


Data merging priorities

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.

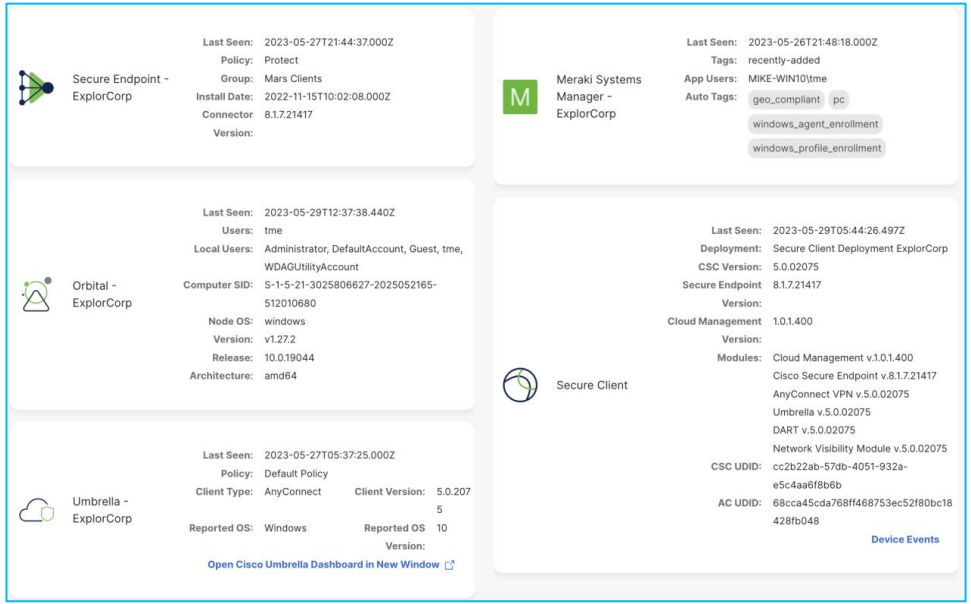
When there is a possibility to match on multiple attributes, Device Insights sets the priority based on the list shown below to ensure we have obtained the best possible match

- Hardware ID
- Serial
- MAC
- IMEI
- Hostname

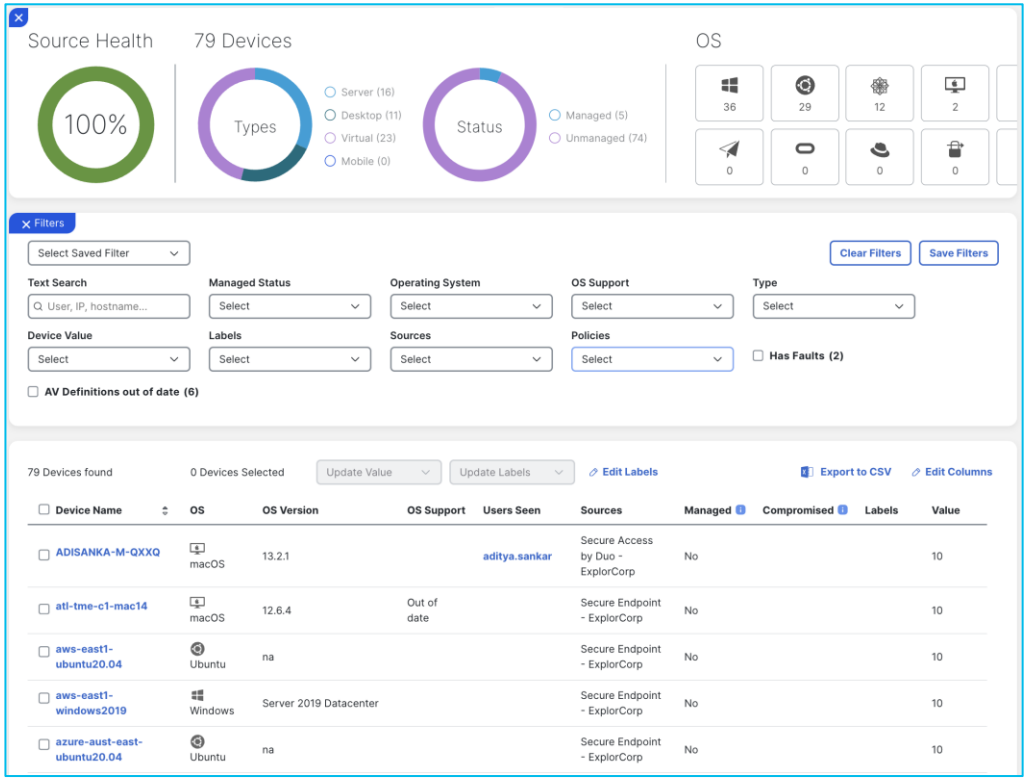


Next-level asset resolution and inventory

- 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



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

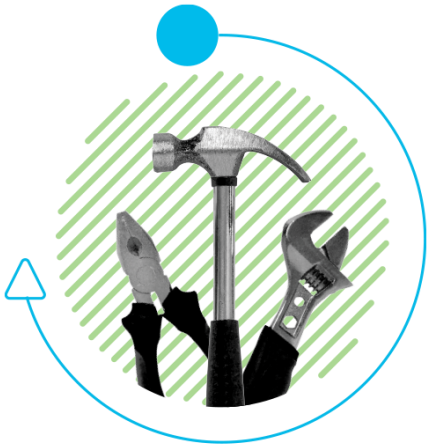
Cisco Secure Client: Security agent consolidation

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



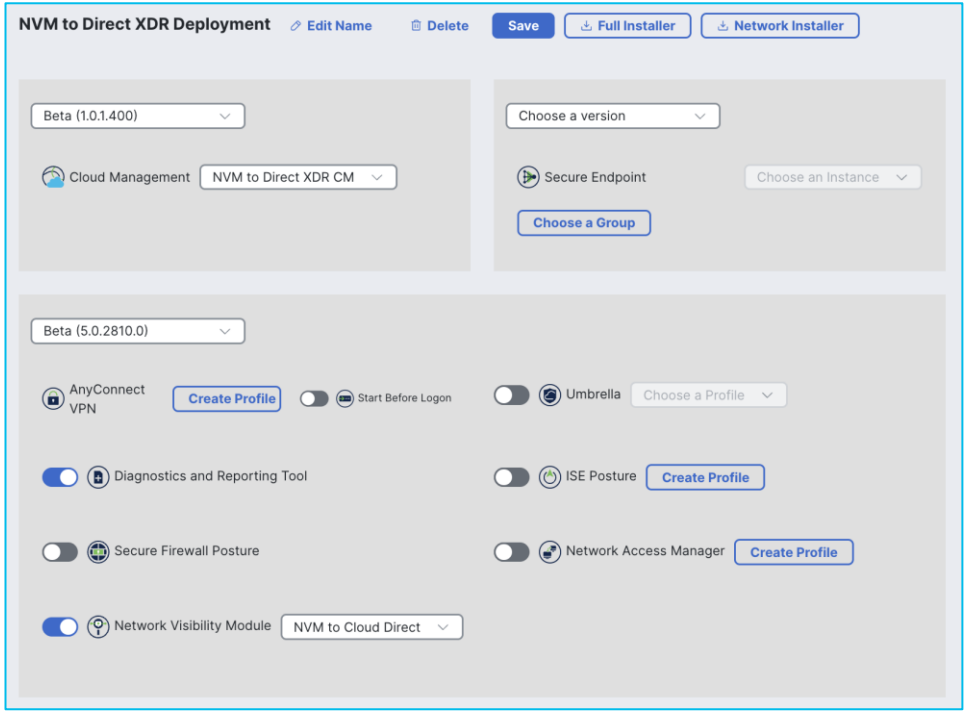
ISE Posture performs endpoint posture assessment

Umbrella Roaming Security module adds DNS-layer security

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

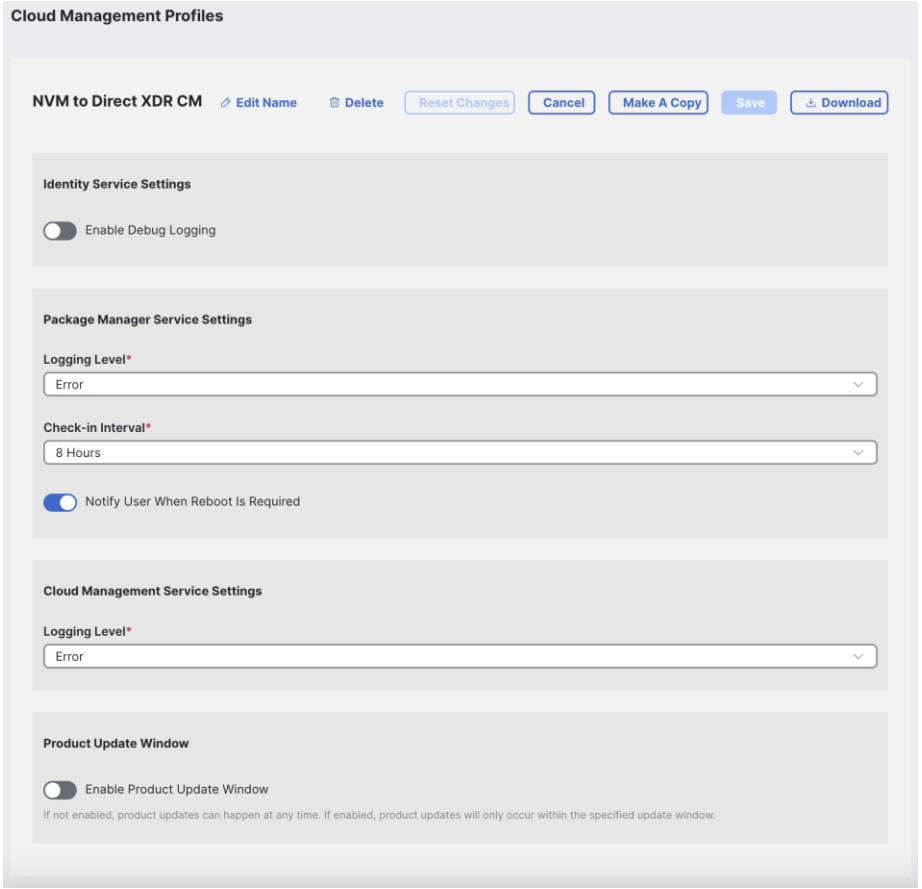
Deployments

- 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



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



Incident Response Demo

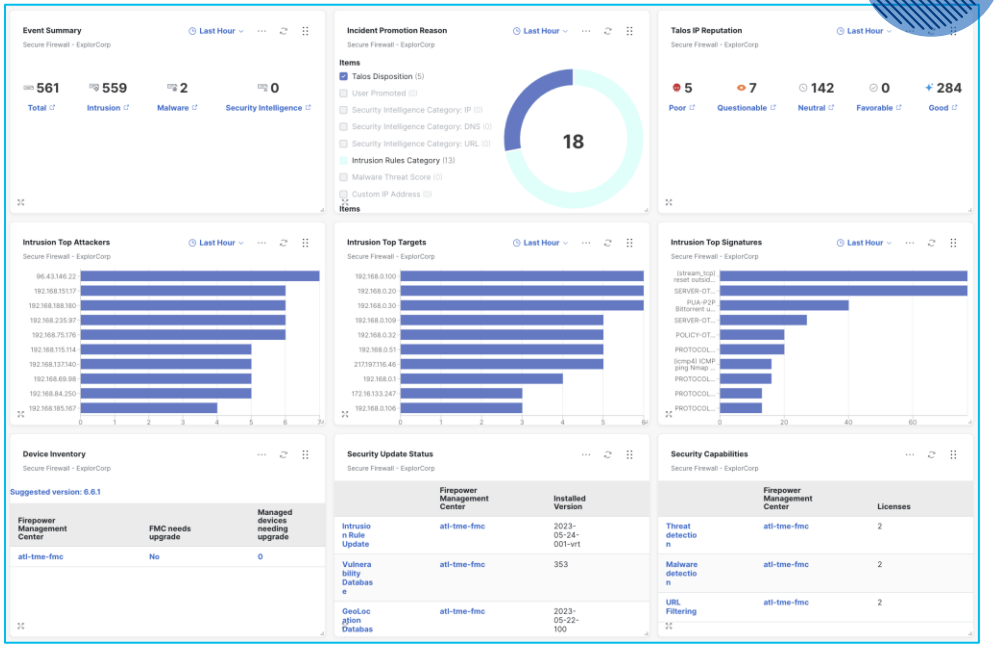
Agenda

- 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

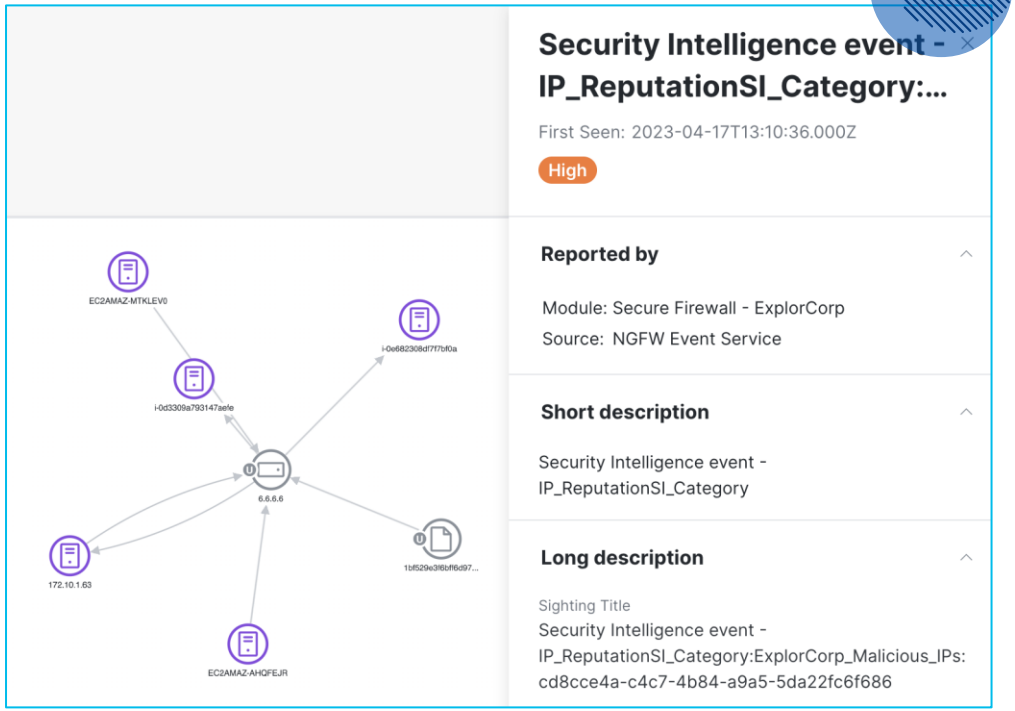
- Local IP sightings

Reference

- Pivot point to sighting event

Promote events

- Promote alerts from Analytics to incidents in XDR



Secure Firewall

Triage events

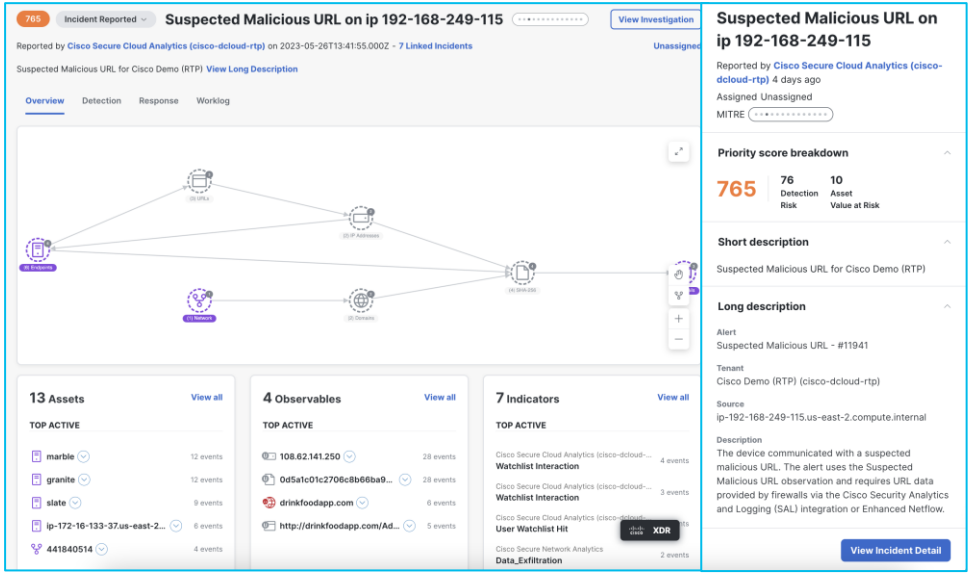
- See triaged network security events in the prioritized incidents list.

Incident management

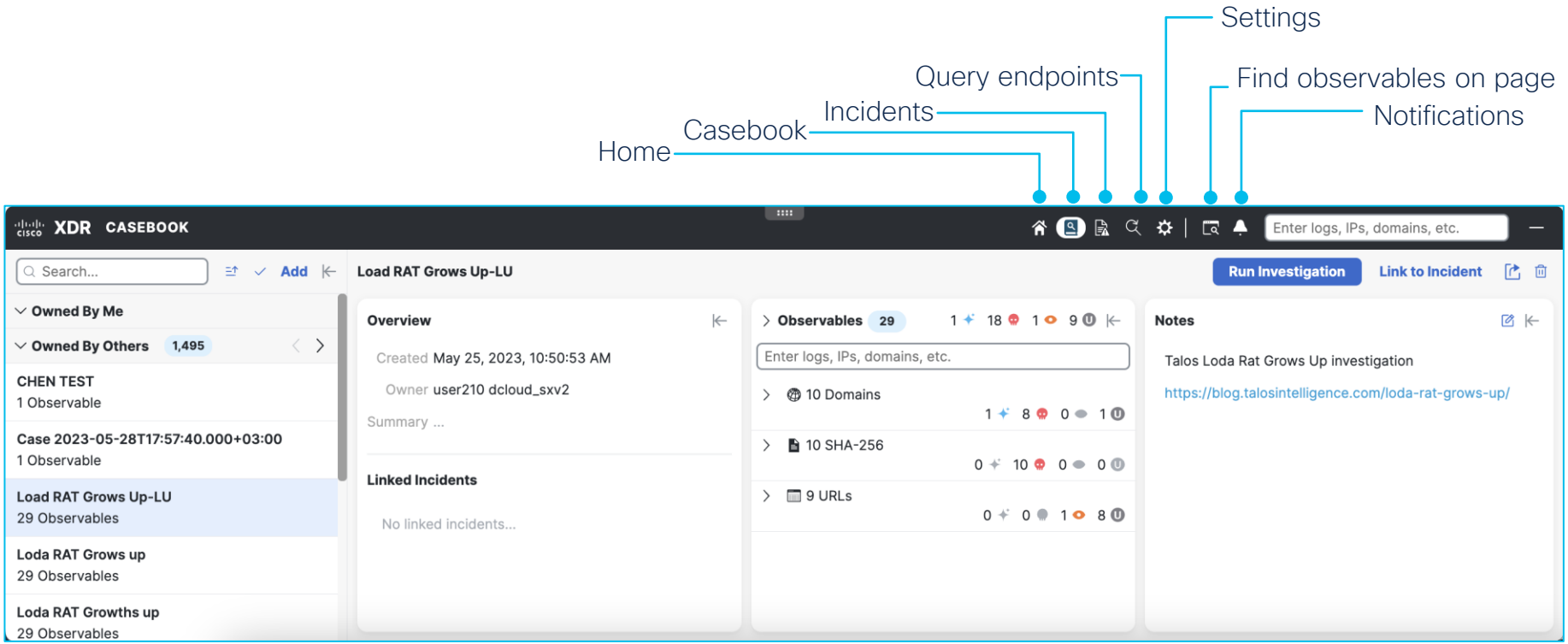
- Assign to others, change status, link incidents or add notes

Maintain context

- View incidents in the XDR ribbon or the browser extension



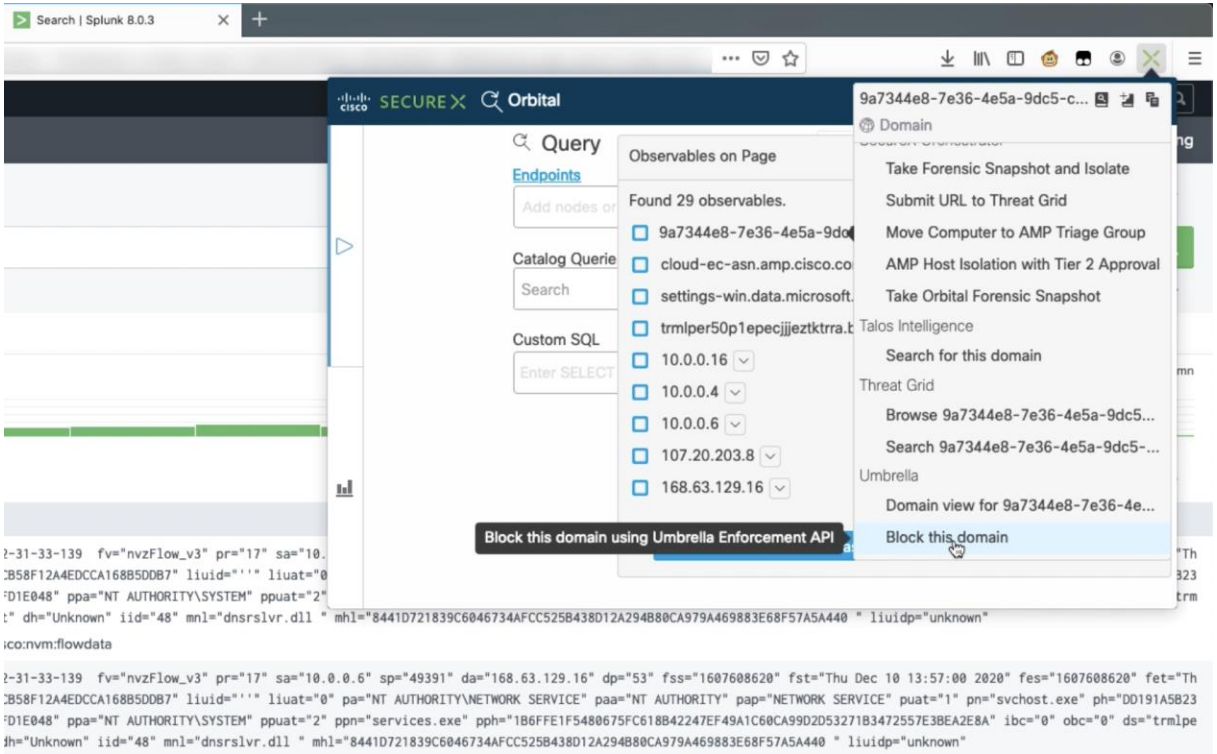
Never lose context with XDR Ribbon



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

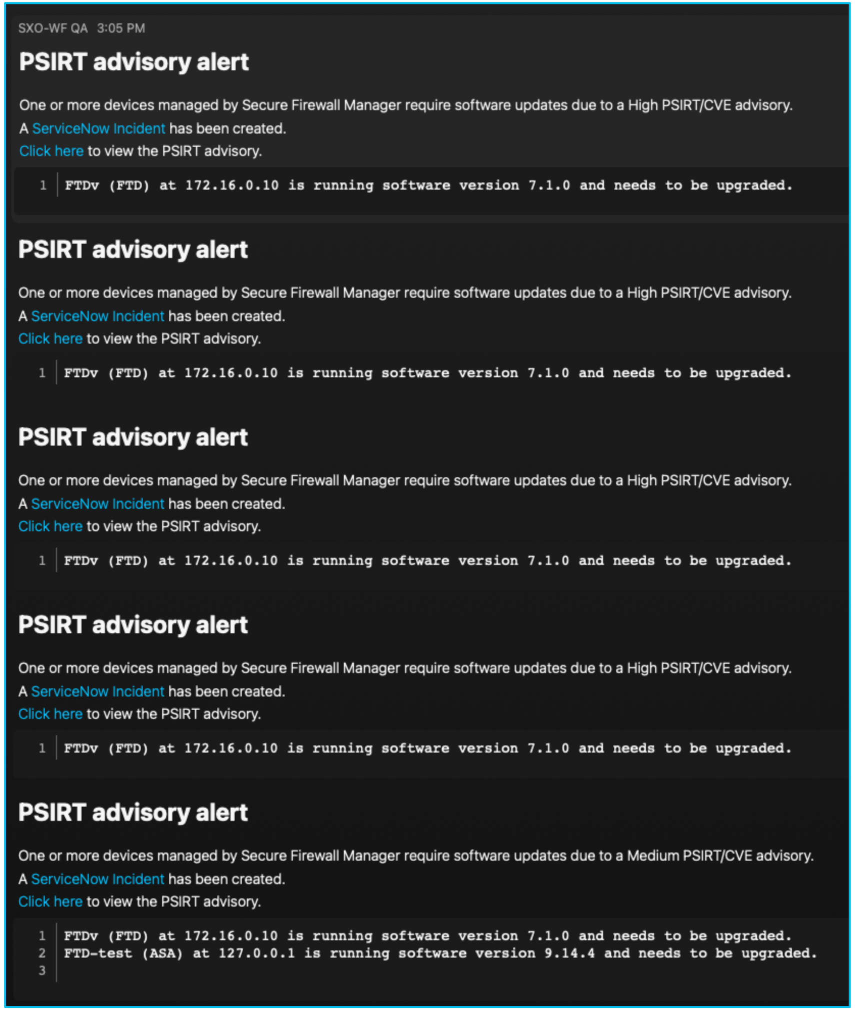
XDR browser extension



PSIRT Impact Monitoring

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

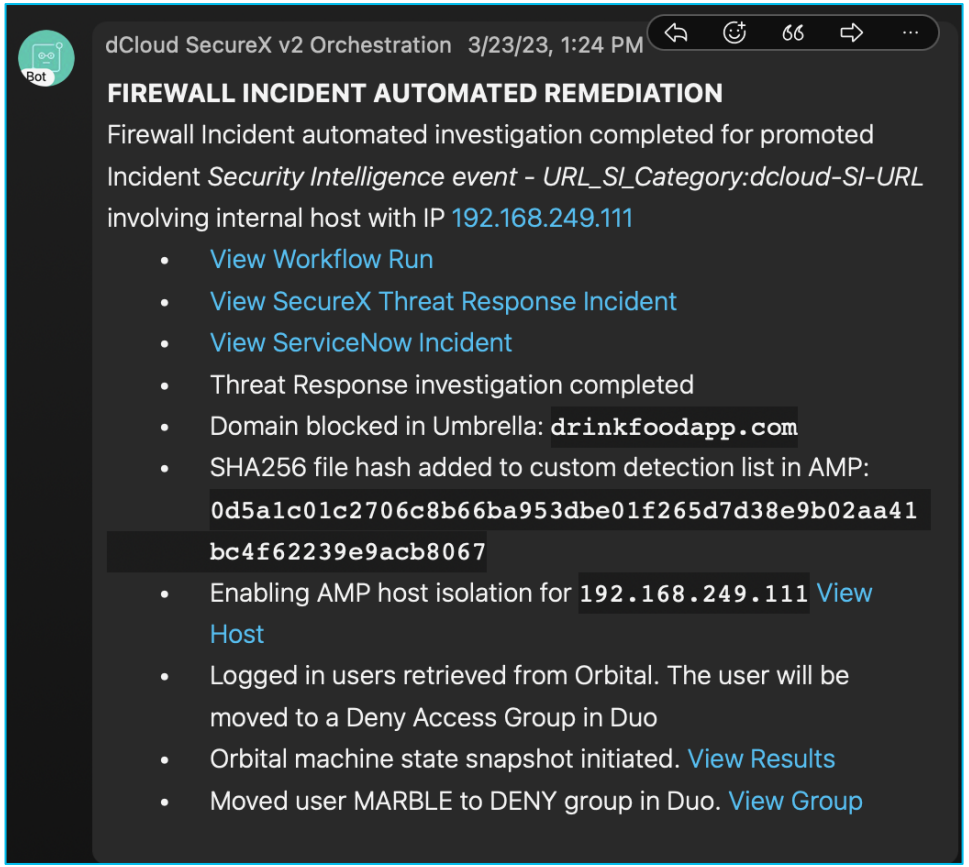
Solution: This orchestration workflow will check for new PSIRTs then compare your devices version and notify you if any vulnerable devices were found.



Impact Red Remediation

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

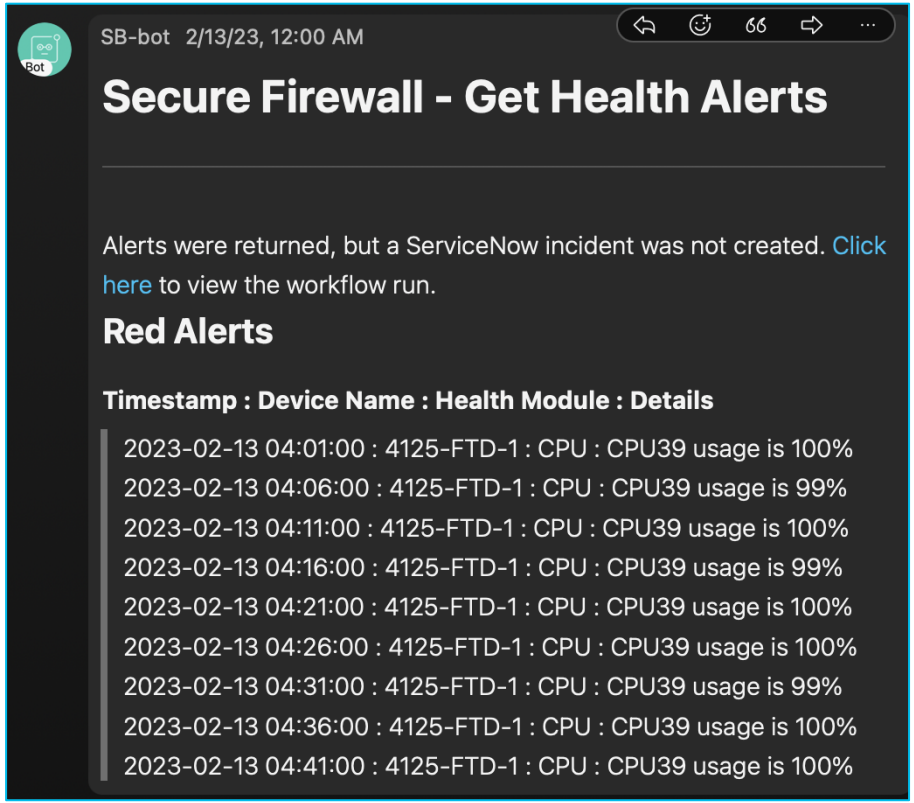
Solution: An XDR orchestration workflow investigates the event and waits for approval. Once approval is granted, automated remediation at the DNS, application, and endpoint level are taken.



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.

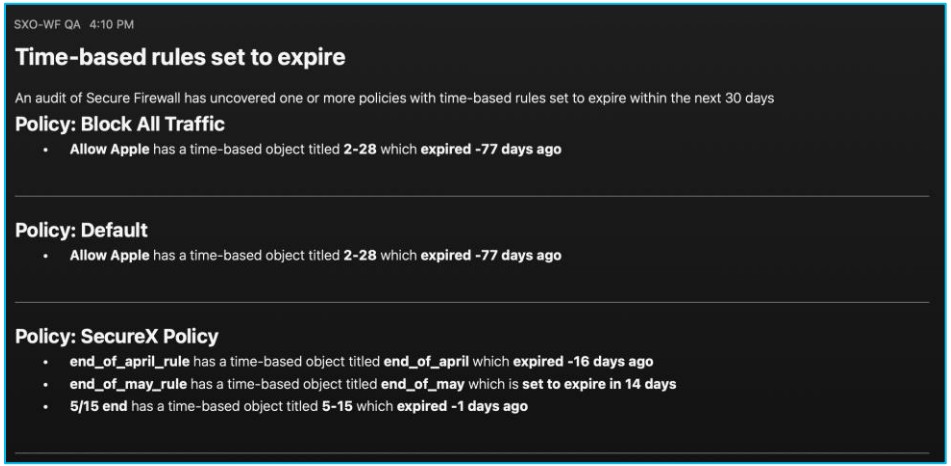
Solution: This orchestration workflow will check for health alerts from your devices and proactively notify via Webex teams, Slack, or email.



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.

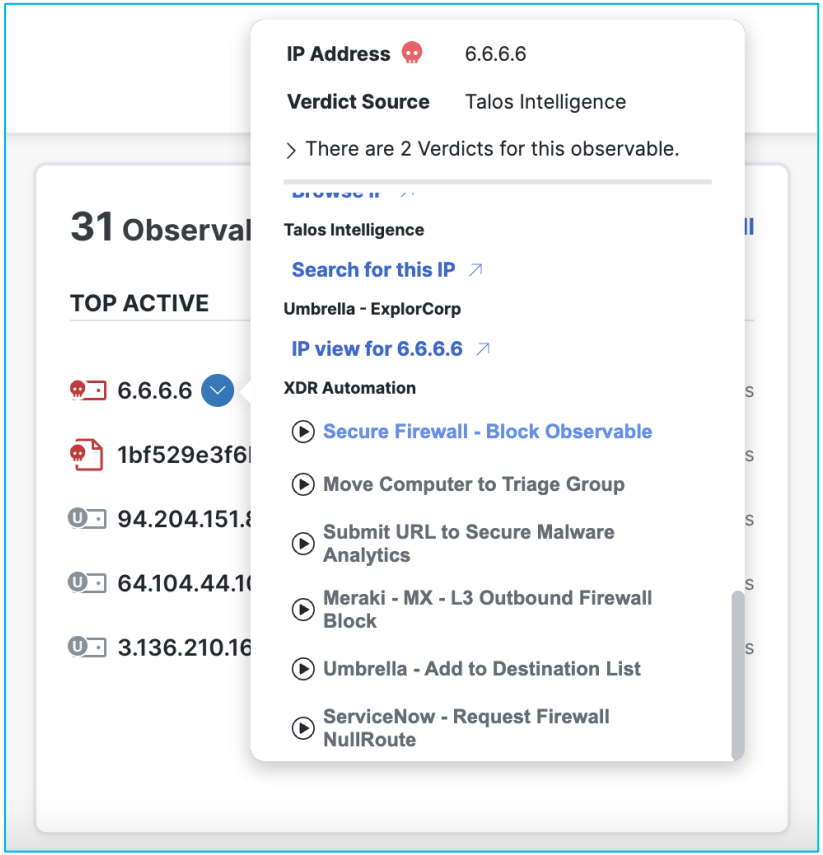
Solution: This orchestration workflow will check rules that have already expired or will expire soon and proactively notify you of which rules to review.



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.

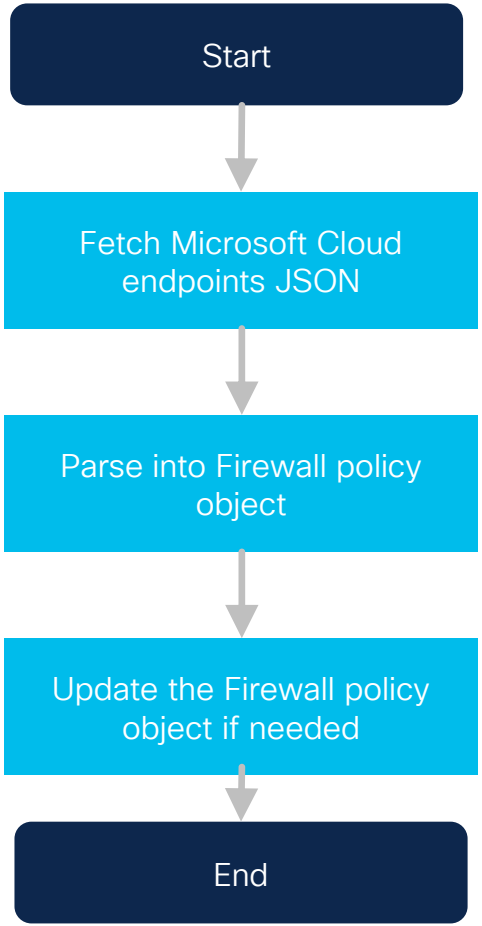
Solution: Using the pivot menu Adam can block the IP address at the click of a button from anywhere.



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

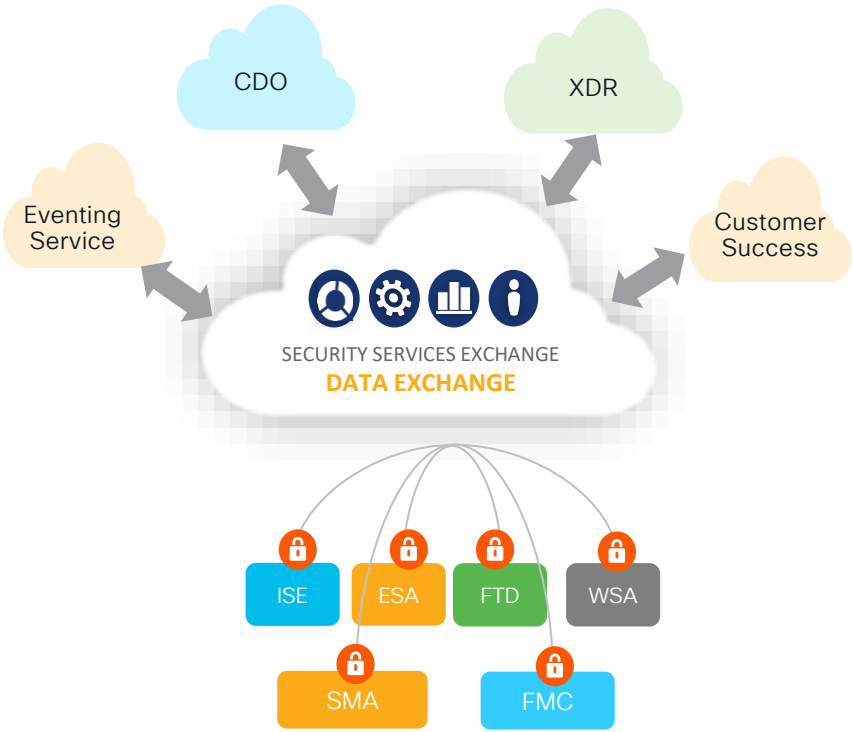
- Cisco Defense Orchestrator (CDO)
- XDR
- Cisco TAC
- Customer Success

Core Infrastructure Services

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

Device Connector / Agent

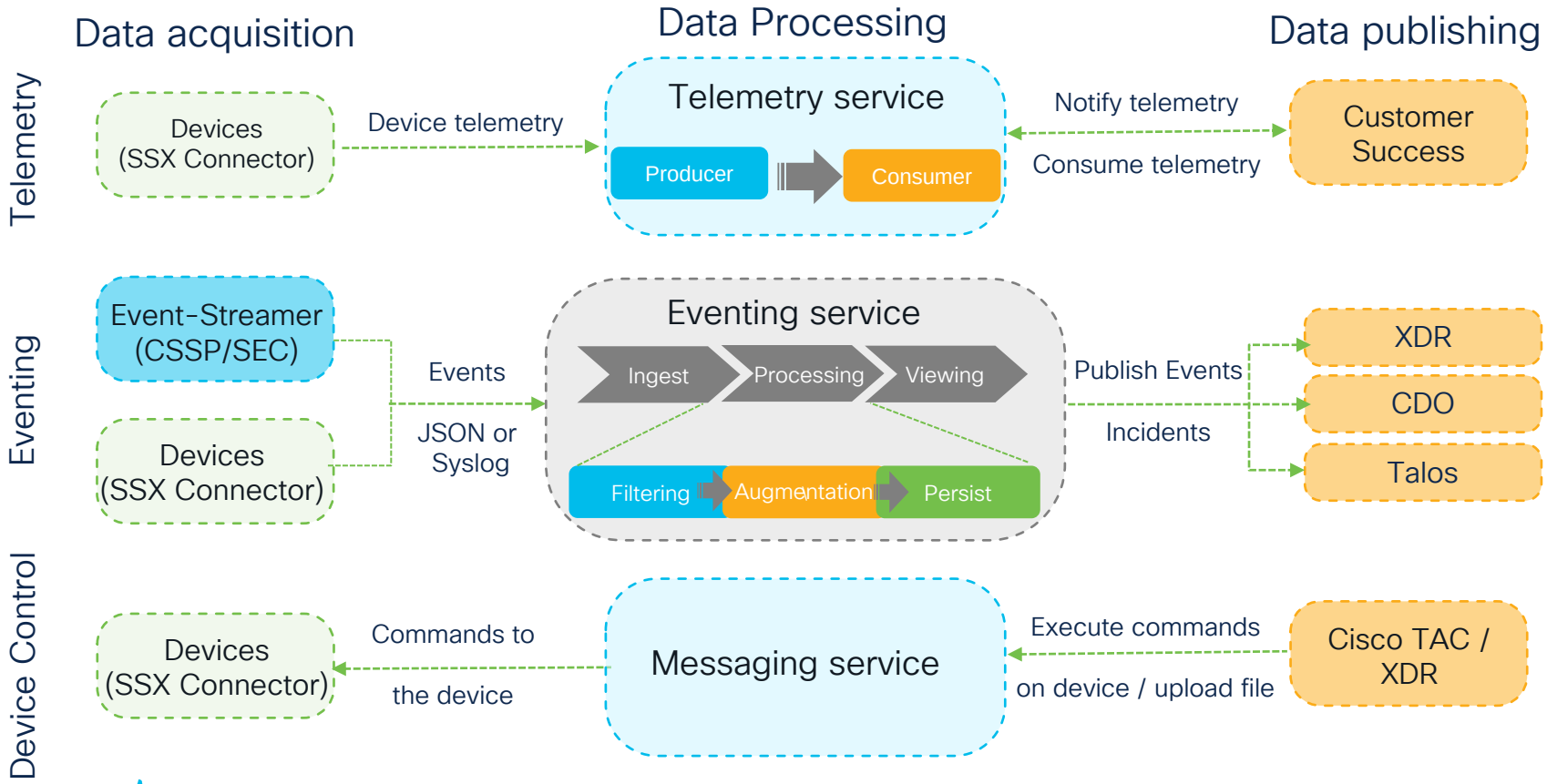
- Secure Bi-Directional Channel
- REST, CLI, WebSocket
- File Upload / Download
- Services Management
- Products: FMC, FTD*, ESA, WSA, SMA, ISE, SNA
- * = Events are SENT to SSX and stored for 7 days



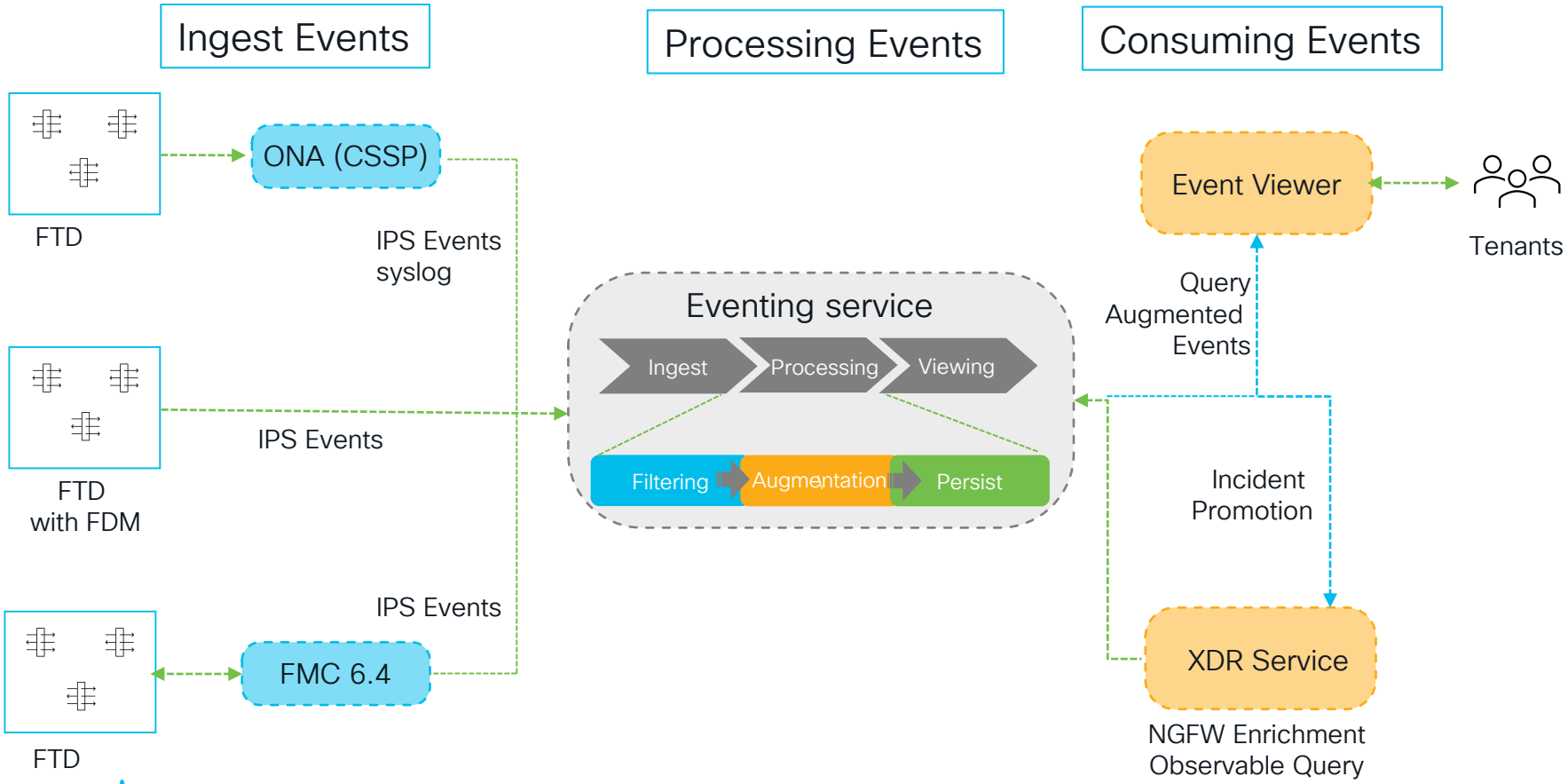
SSX Core Functions

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

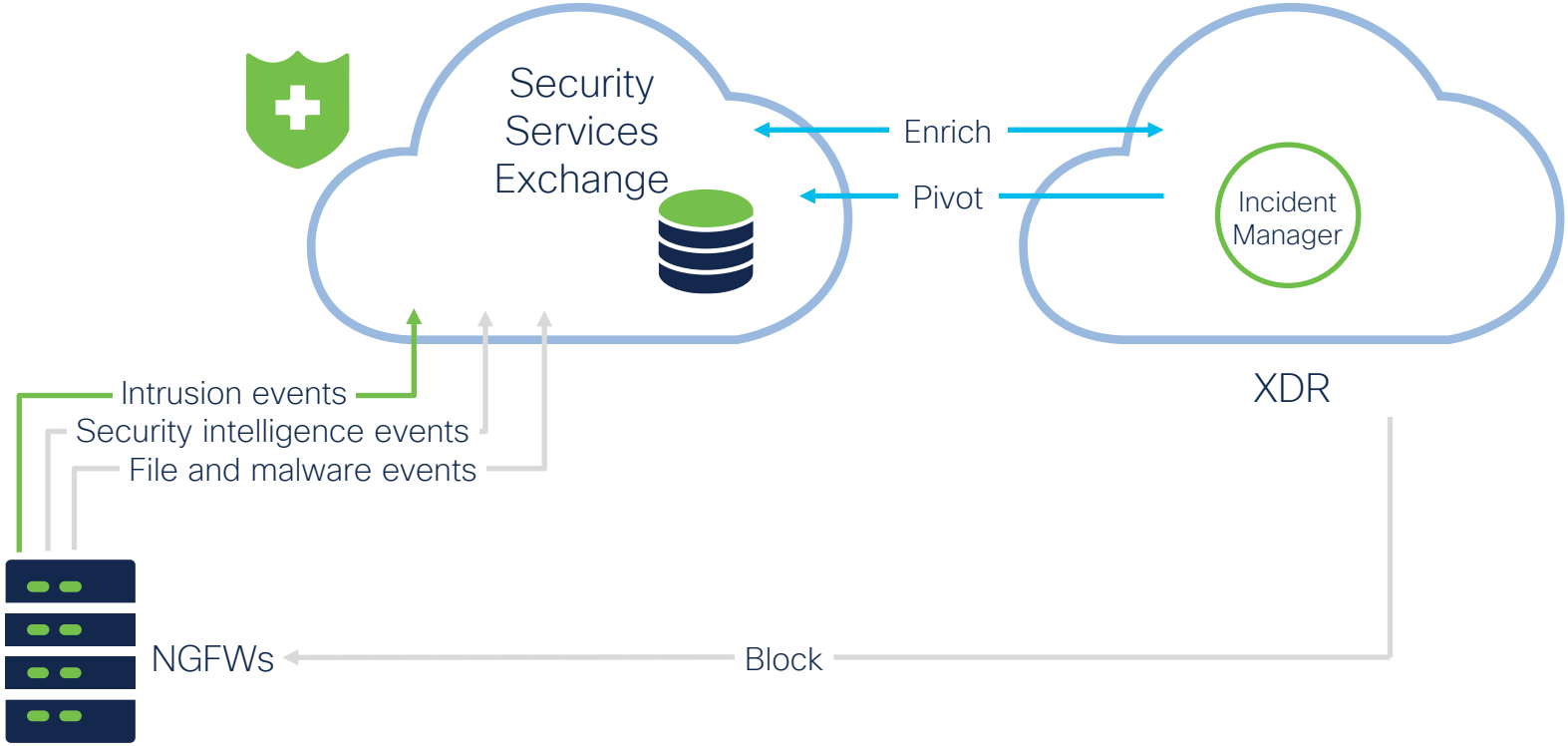
Supported Data pipelines



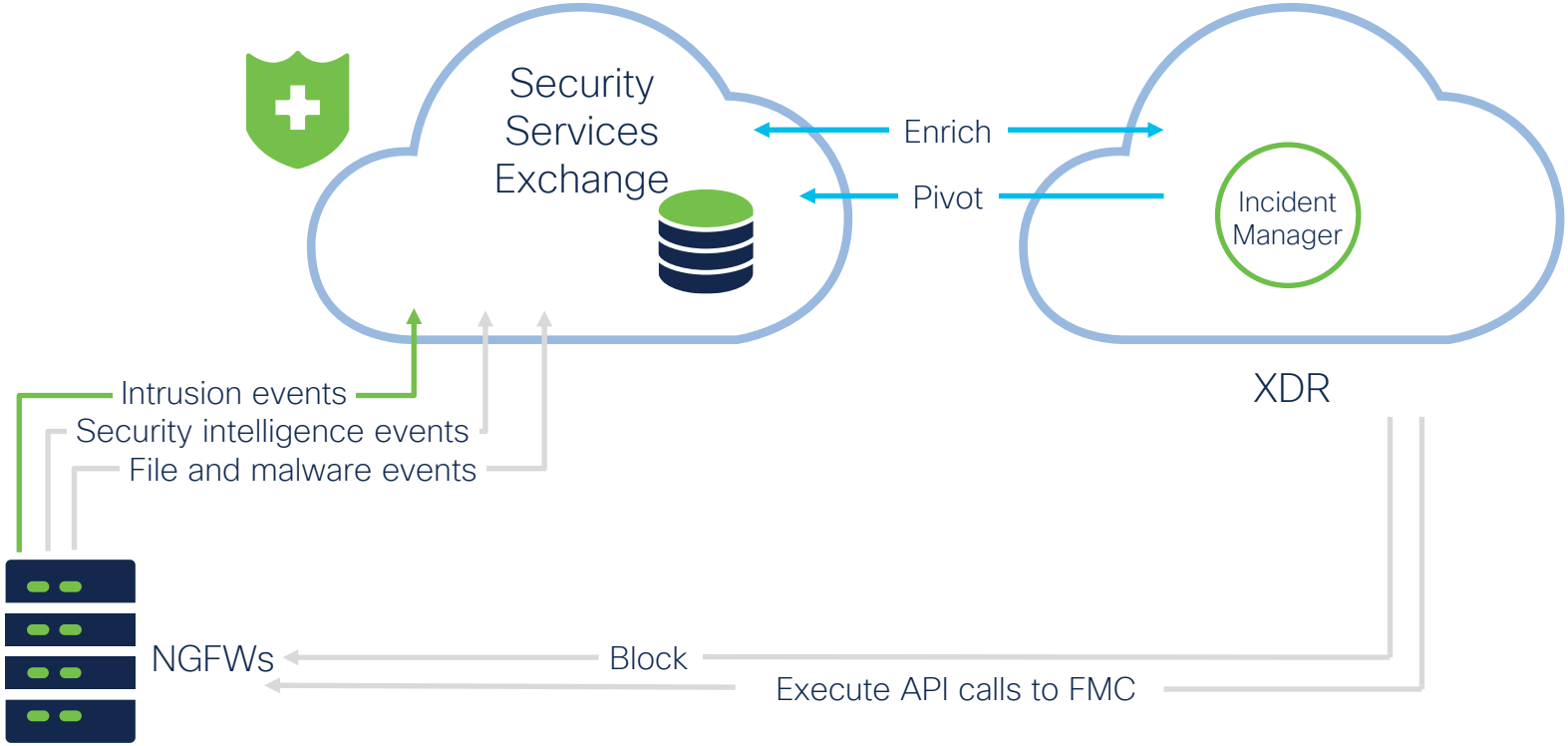
Eventing Service



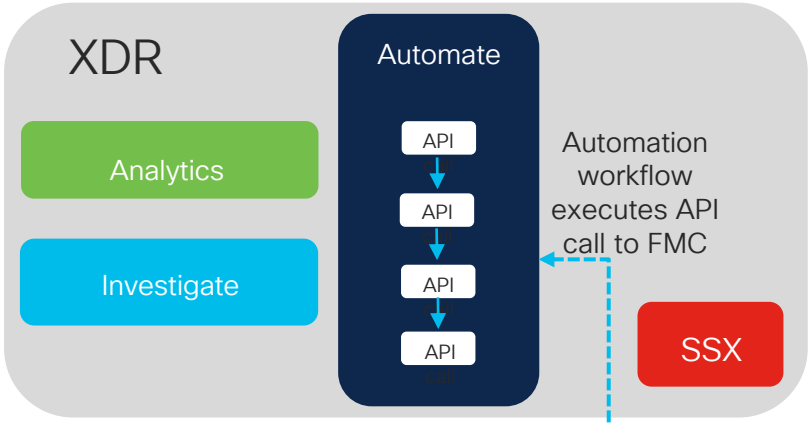
Secure Firewall



Secure Firewall



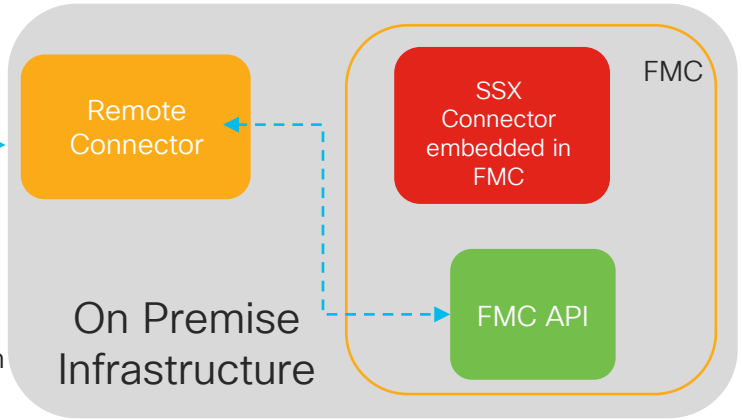
Cloud to on-prem API Proxy



Requirements

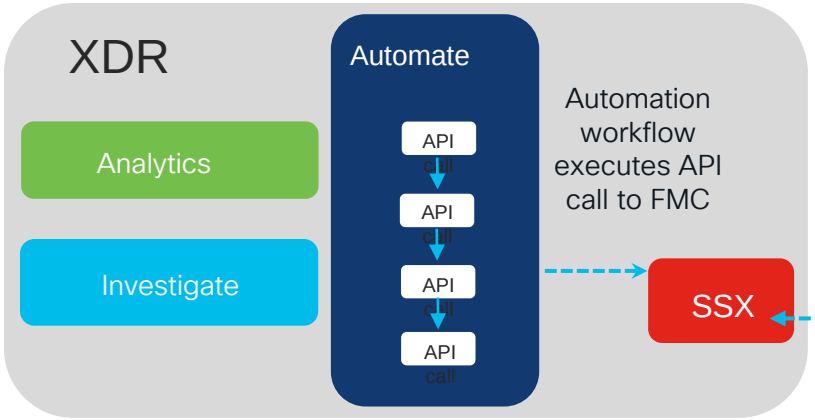
- Any FMC version
- Remote appliance deployed in vCenter
- Outbound access on TCP 8883

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

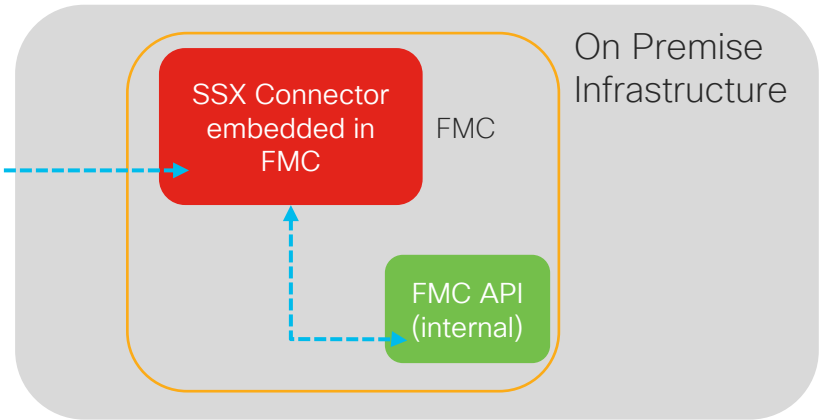
Cloud to on-prem API Proxy



Requirements

- FMC 7.2 or 7.0.2+
- Device is registered to Security Services Exchange

API call is proxied through SSX since device is already registered to SSX



SSE connector interacts directly with FMC API as an internal user. Response is sent back to orchestration

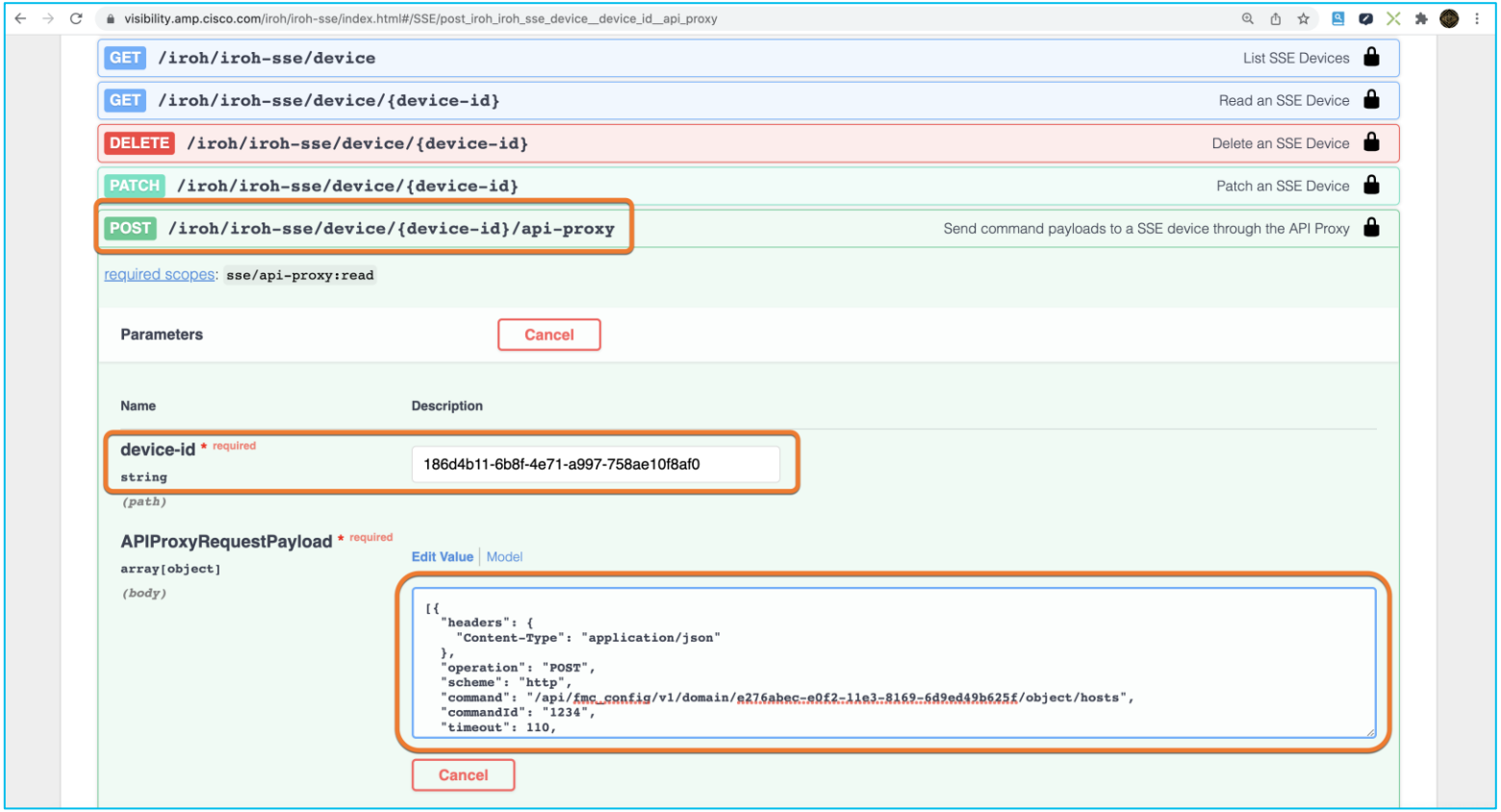
XDR + FMC + Orchestration Remote VM

- 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.



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

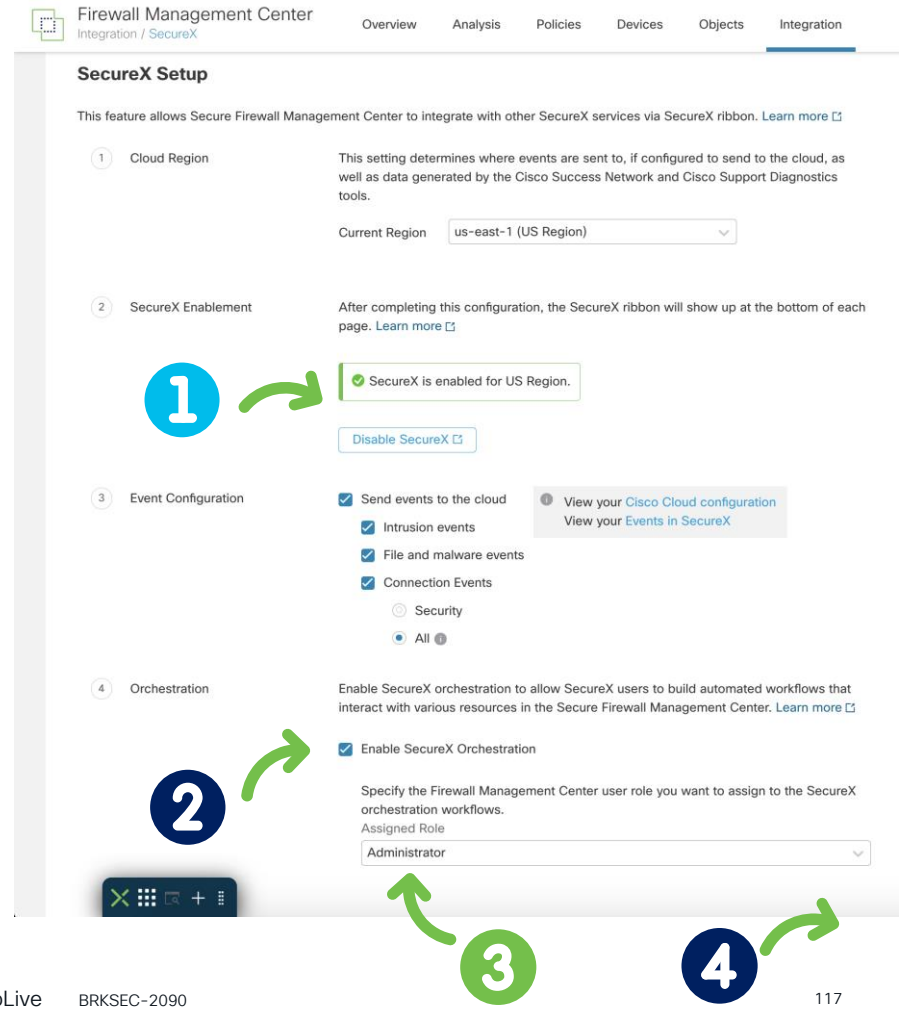
```
[{
  "headers": {
    "Content-Type": "application/json"
  },
  "operation": "POST",
  "scheme": "http",
  "command": "/api/fmc_config/v1/domain/e276abec-e0f2-
11e3-8169-6d9ed49b625f/object/hosts",
  "commandId": "1234",
  "timeout": 110,
  "body": {
            "type": "Host",
          "value":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

Sample Response

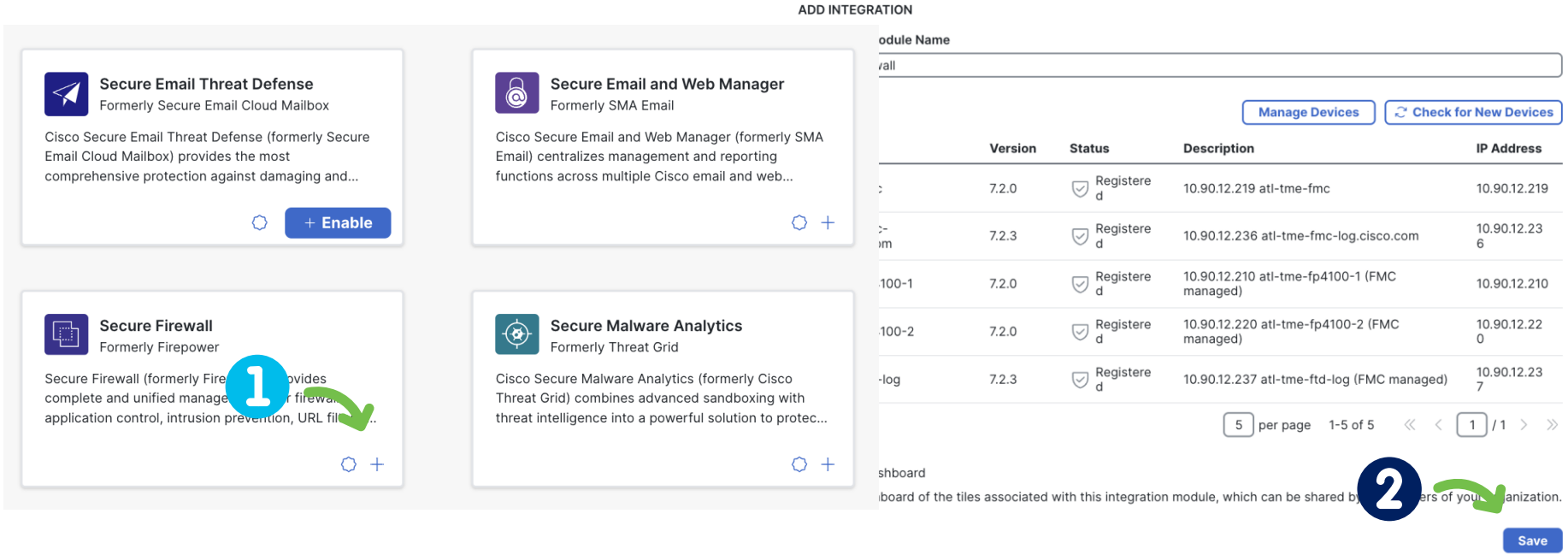

```
{
  "data": [
    {
      "headers": {…},
      "operation": "POST",
      "scheme": "http",
      "command": "/api/fmc_config/v1/domain/e276abec-e0f2-11e3-8169-
6d9ed49b625f/object/hosts",
      "commandId": "1234",
      "body": {
        "description": "Host created from XDR Automate",
        "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



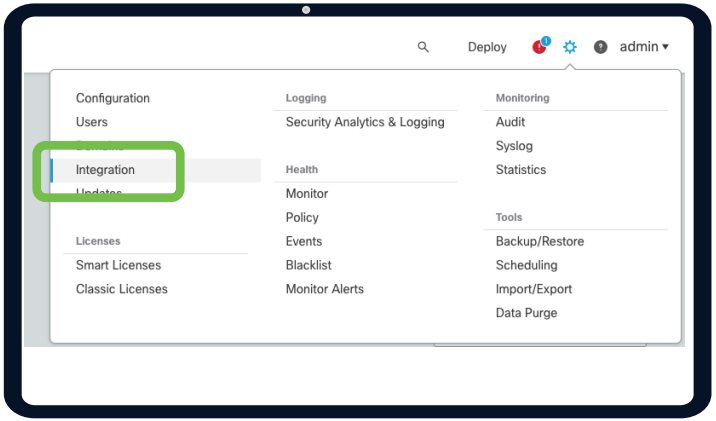
Configure the integration

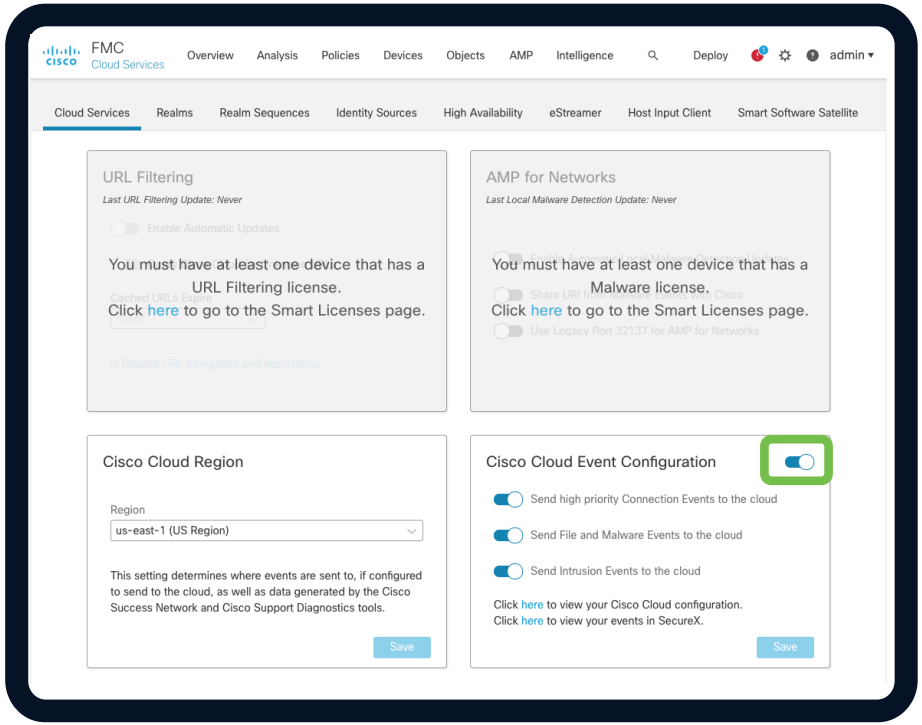


1 Add Firewall module

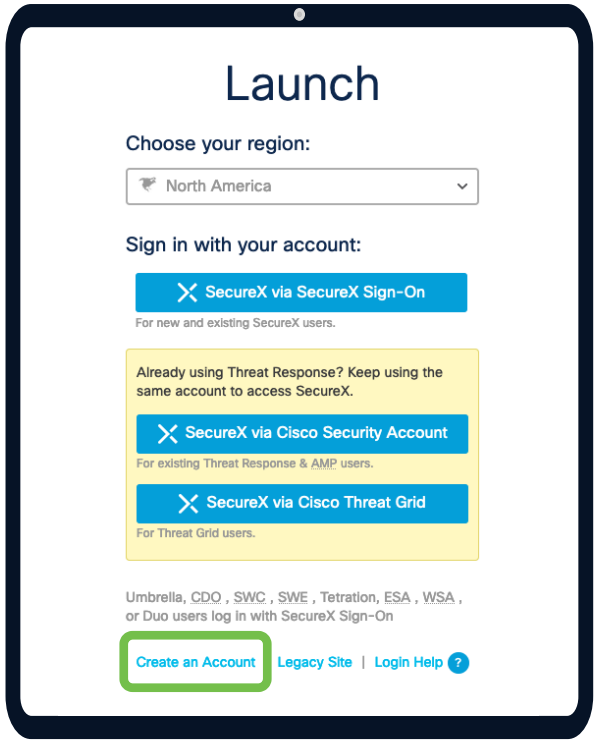
2 Save the module

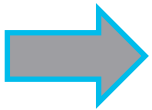
Enable Cloud Event Configuration

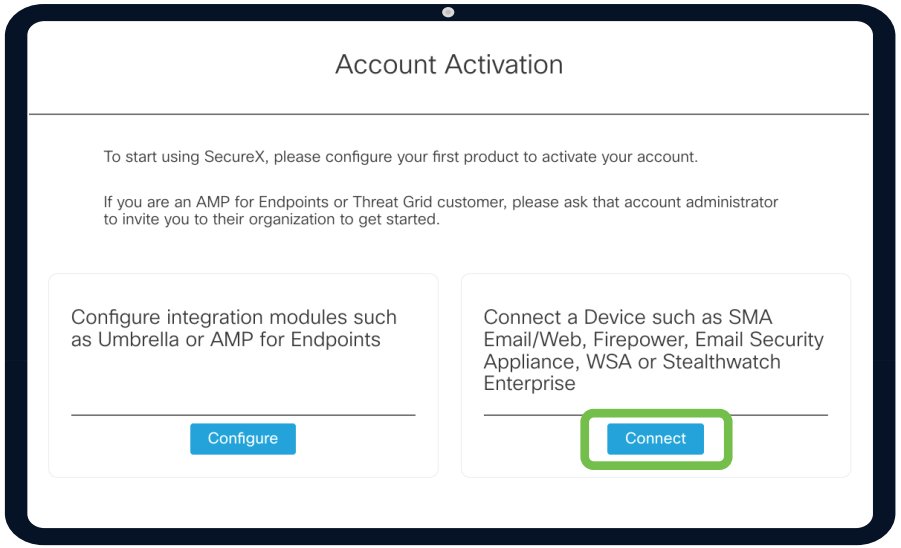




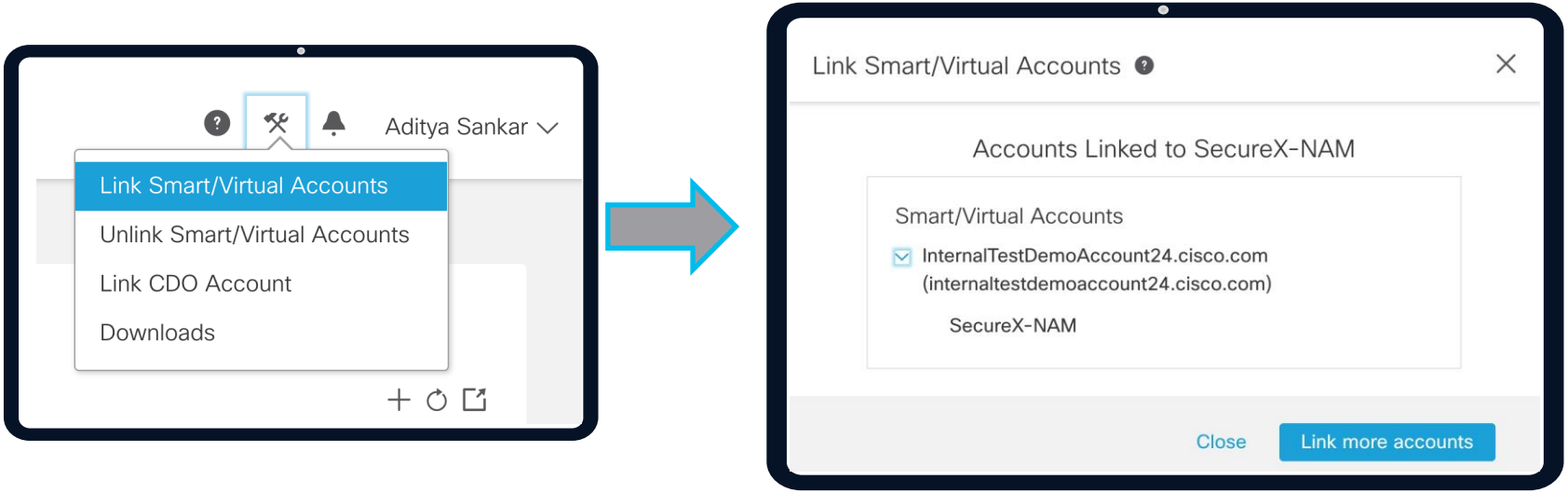
Sign up for XDR



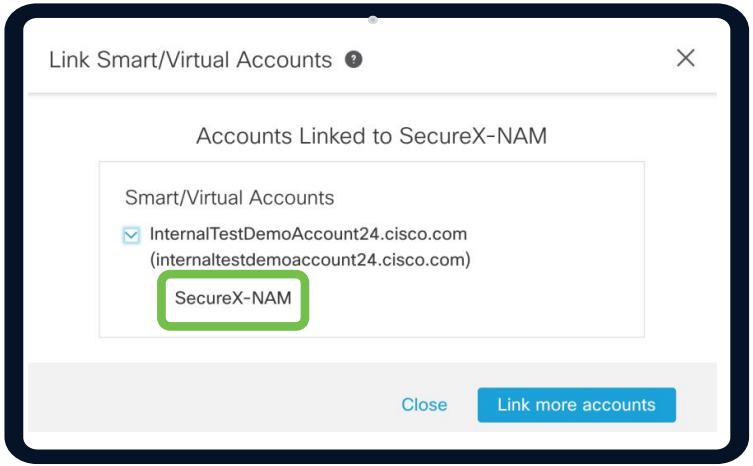


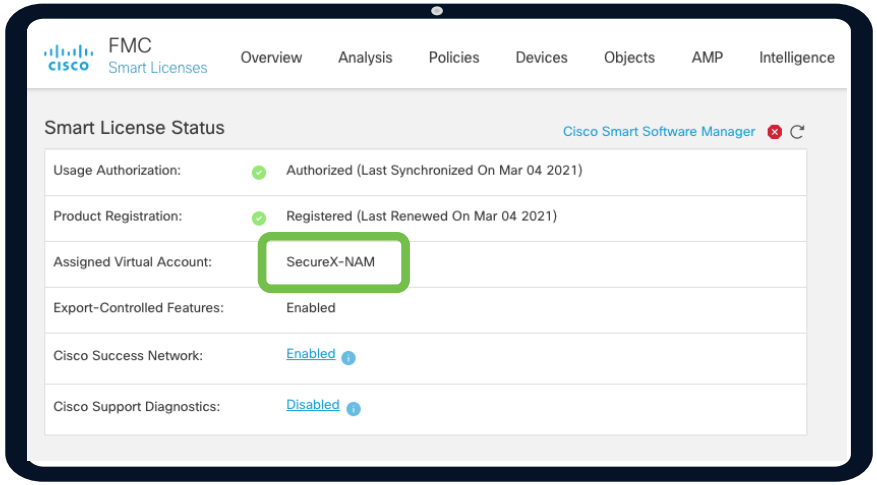


Link Smart License Account to SSX



Devices are onboarded to XDR





Full configuration video at cs.co/XDR_videos

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.

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

FINISH

Thursday, June 8 | 1:00 p.m.
BRKSEC-3116
Automating your Cisco XDR Workflows: from Threat Hunting, to Finding and Confirming Incidents, to Responding!

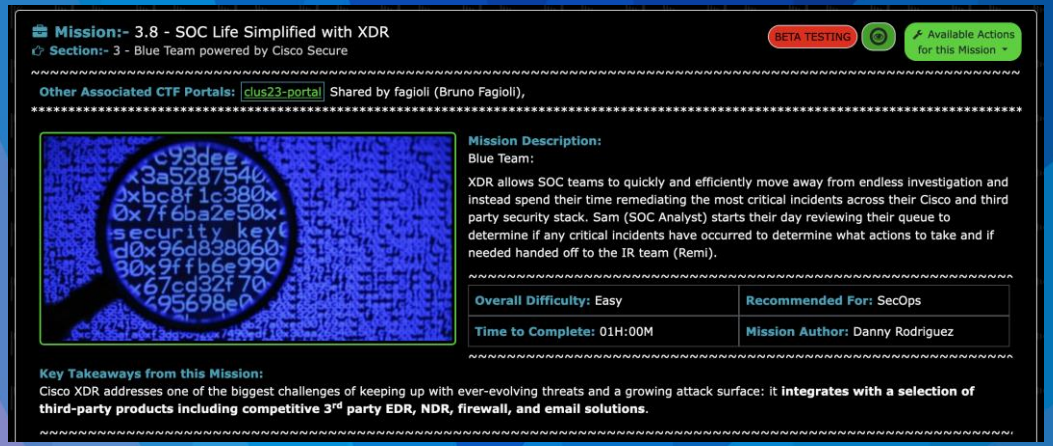
cisco Live!
Las Vegas, NV | June 4-8, 2023

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!

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



cisco Live!

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

CISCO DEVNET

Want to learn more about developing with XDR?

Visit us in the DevNet Zone!

Demo Booth	Theater Session
Tuesday from 9:30 AM to 5 PM	DEVNET-1083 Tuesday at 1 PM

cisco Live!

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

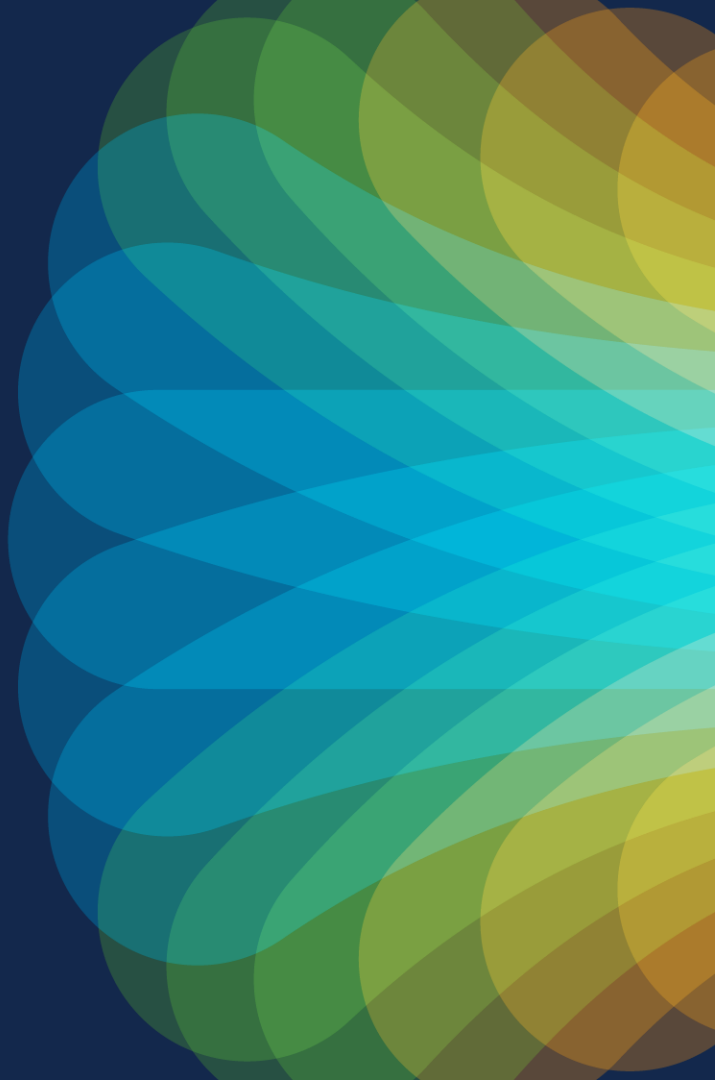
Complete your Online Session Evaluation

Continue your education

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

The bridge to possible

Thank you



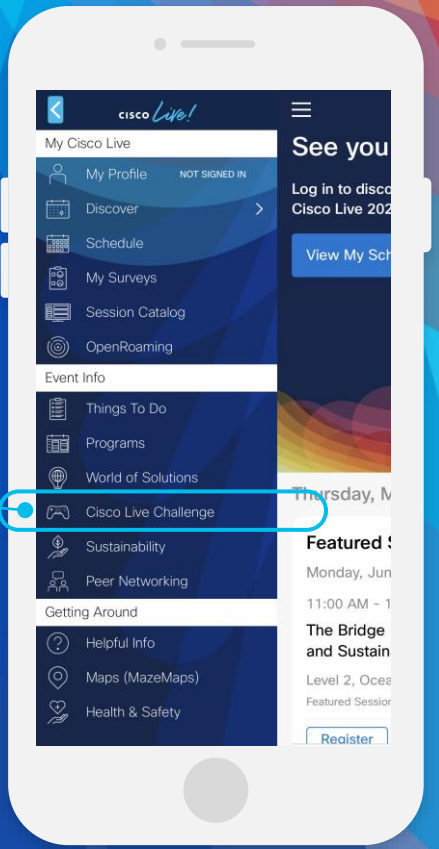
Cisco Live
Challenge

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:




cisco Live!
Let's go
#CiscoLive