Cisco XDR

The Future of IT Security Operations

Max Shantar, Cybersecurity Solutions Engineer CISSP, CRISC, MSc, CCNA, etc
Cisco Security

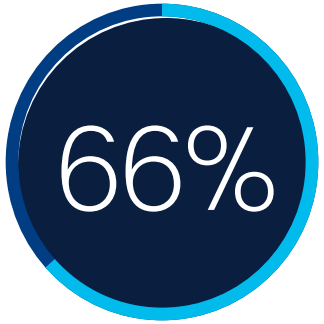
October 2025

AGENDA

1. Overview
2. Xtended Context
3. Detections
4. Response

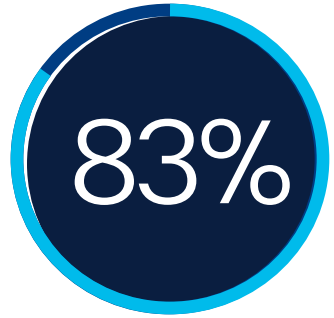
What are the challenges?

of attacks involve lateral movement from the entry point across the network [1]



of organizations were affected by ransomware in 2022 [2]

of security teams say critical alerts are being missed [3]



of the cyberattacks in 2023 were identity related [4]

Sources: Cybersecurity Insiders, 2022 Application Security Report (1); Sophos "The State of Ransomware", 2022 (2); Orca Security "Cloud Security Alert Fatigue Report", 2022(3); The State of the Identity Attack Surface -Osterman Research 2023(4)

What SecOps wants

"I want to have a correlated view of alerts across my environment."

"I need my security tools to help me work with speed, accuracy, and confidence."

"I want my team to remediate threats with guidance and automated playbooks."

Understanding the Alphabet Soup of Cybersecurity: XDR, MDR, NDR, and EDR

Attribution: AI Slop

EDR (Endpoint Detection and Response):
Focuses on detecting and responding to threats on endpoints like laptops and servers.

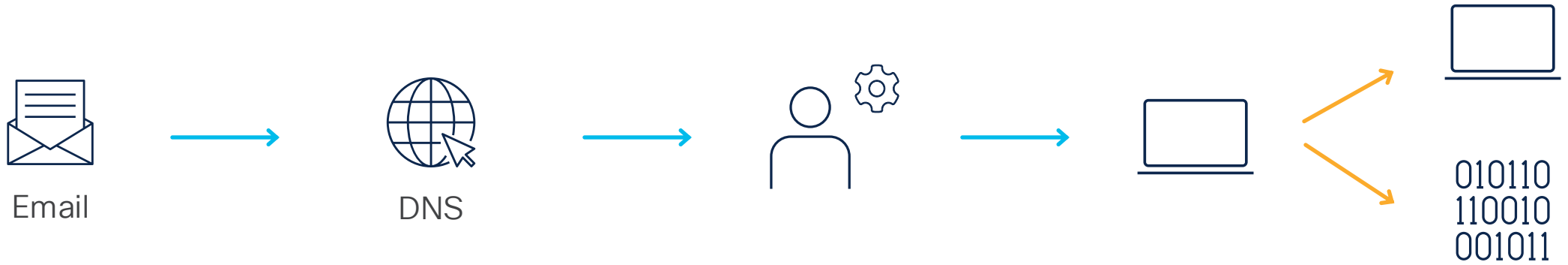
NDR (Network Detection and Response):
Monitors network traffic to detect suspicious activity.

XDR (Extended Detection and Response):
Integrates multiple security products (EDR, NDR, email, cloud, etc.) to provide a unified detection and response platform.

MDR (Managed Detection and Response):
A service that provides threat detection and response as an expert managed service.

Stop advanced threats like ransomware

Most attacks use a sequence like this...



A well-tailored and personalized email causes a user to click...

Which goes to a questionable web site...

Which leads to a strange process being created locally on the user's device...

That process will connect to another machine or directly to their data

T1566: Spear Phishing

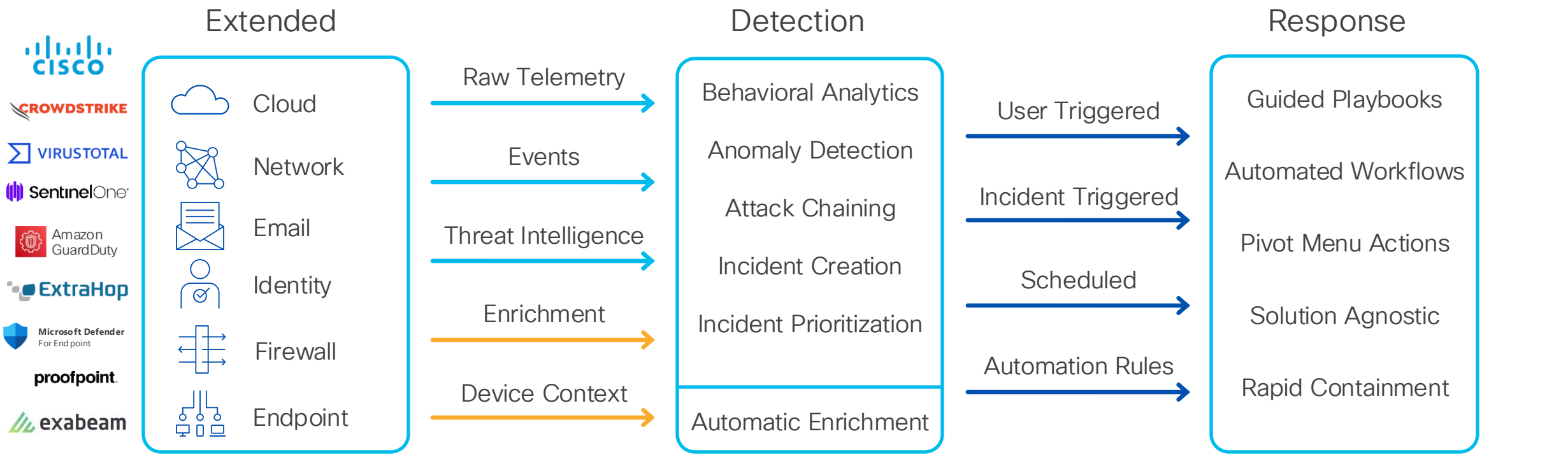
T1055: Process Injection

T1189: Drive-by Compromise

T1210: Exploitation of Remote Services

Cisco XDR

XDR High level architecture



Multi-vector telemetry ingest network, cloud, endpoint, email, and more from Cisco and 3rd party

Cross domain alert detections and attack chaining with automated incident prioritization and enrichment

Automated or user triggered responses to block observables using any integrated technology

AI driven at every stage, Detection, Response and Incident Management

Real world detections solved by Cisco XDR

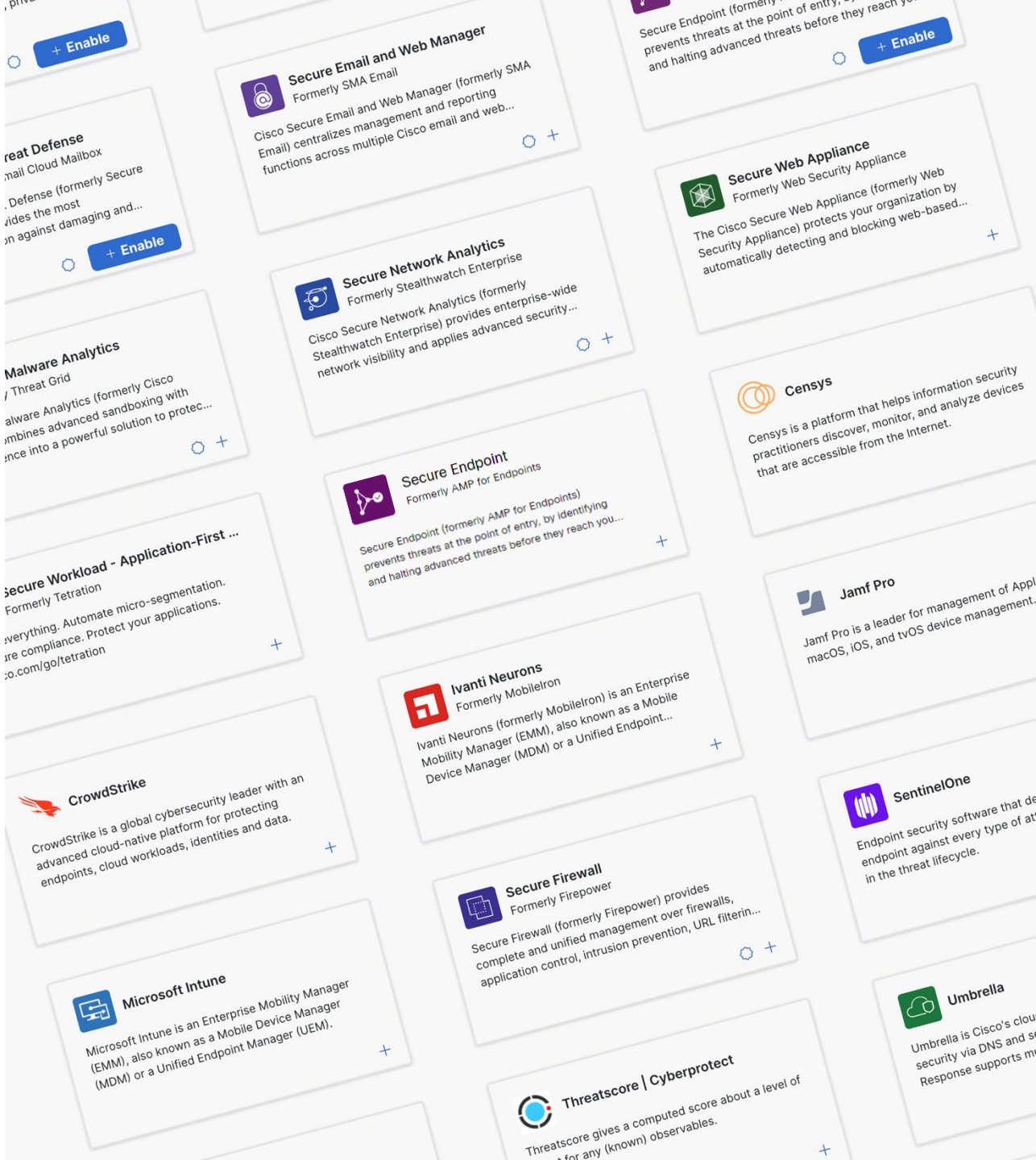
120+ alerts across 14 MITRE TTPs monitoring network telemetry

“Device downloaded data from an internal device that it doesn't communicate with regularly. Shortly after that, device uploaded a similar amount of data to an external device.”

“Device has been sending unusually large DNS packets. May indicate an attacker using the DNS protocol as a covert communications channel to exfiltrate data.”

“A device on the local network scanned (or was scanned by) a remote IP address.”

Extended context



Extended context

https://docs.xdr.security.cisco.com/Content/Administration/cisco-third-party-integrations-and-capabilities.htm

Integrations

XDR is as powerful as its integrations, and Cisco XDR has over 80+ integrations with a wide variety of products.

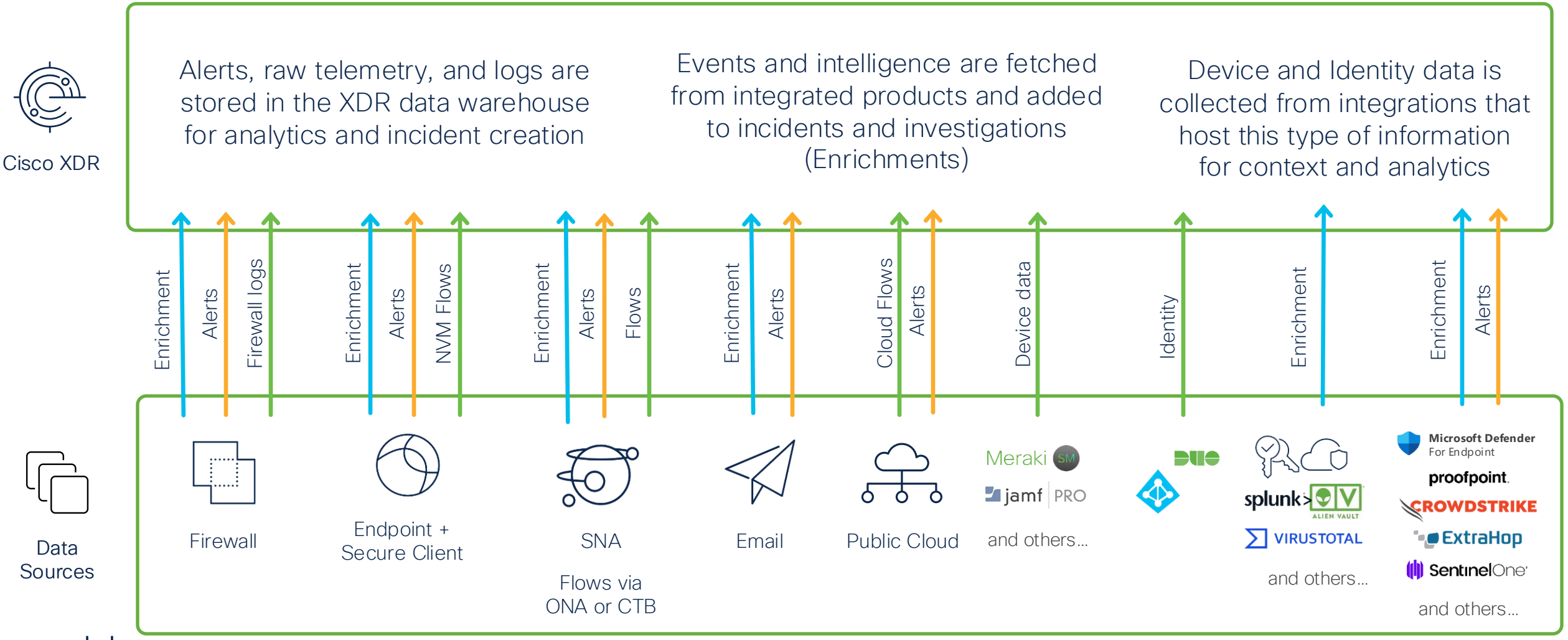
- Open platform with more third-party integrations than Cisco integrations.
- Mix of security products, intelligence sources, device managers, and more.
- Easy to enable or configure built on API-based communication with other products.
- Integrations can provide one or more capabilities including:
  - Detections and analytics
  - Threat Hunting and investigation
  - Asset Insights and Context
  - Automation and Response

Integration	Detection Analytics and Correlation	Threat Hunting and Investigation	Dashboard Tiles	Asset Insights and Context	Automation and Response	
					Controls and Responses	Security Operations Center (SOC) Automation
Cisco Vulnerability Management	No	No	No	No	No	Yes
Meraki	No	No	No	Yes	No	Yes
Orbital	No	Yes	Yes	Yes	No	Yes
Secure Cloud Analytics	Yes	Yes	Yes	No	No	Yes
Secure Email Appliance	No	Yes	Yes	No	No	Yes
Secure Email Threat Defense*	Yes	No	Yes	No	No	No
Secure Endpoint	Yes	Yes	Yes	Yes	Yes	Yes
Secure Firewall	No	Yes	Yes	No	Yes	Yes
Secure Malware Analytics	No	Yes	Yes	No	No	Yes
Secure Network Analytics	No	Yes	Yes	No	Yes	Yes
Secure Web Appliance	No	Yes	Yes	No	Yes	No
Secure Workload	No	No	Yes	No	No	No
Umbrella	No	Yes	Yes	Yes	Yes	Yes
Webex	No	No	No	No	No	Yes

Integration	Detection Analytics and Correlation	Threat Hunting and Investigation	Dashboard Tiles	Asset Insights and Context	Automation and Response	
					Controls and Responses	Security Operations Center (SOC) Automation
ExtraHop Reveal(x) 360	No	No	No	No	No	Yes
Ivanti Neurons	No	No	No	Yes	No	No
Jamf Pro	No	No	No	Yes	No	No
Jira Cloud	No	No	No	No	No	Yes
Microsoft Azure Active Directory - Users	No	No	No	Yes	No	No
Microsoft Defender for Endpoint*	Yes	Yes	No	Yes	Yes	Yes
Microsoft Defender for Office 365*	No	Yes	No	No	Yes	Yes
Microsoft Intune	No	No	No	Yes	No	No
Palo Alto Networks Cortex XDR	No	No	No	Yes	No	Yes
SentinelOne	No	Yes	No	Yes	Yes	Yes
ServiceNow	No	No	No	No	No	Yes
Slack	No	No	No	No	No	Yes

Extended context

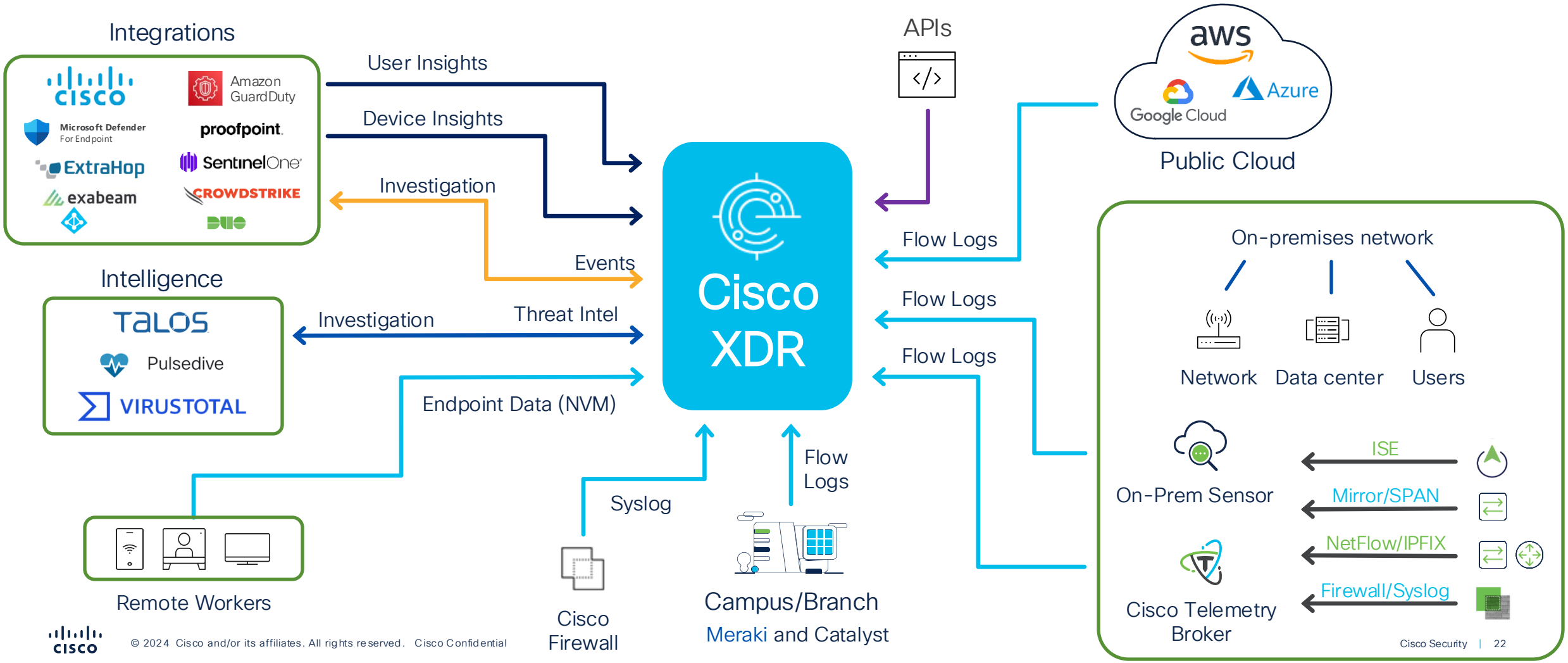
Telemetry and enrichment



Extended context

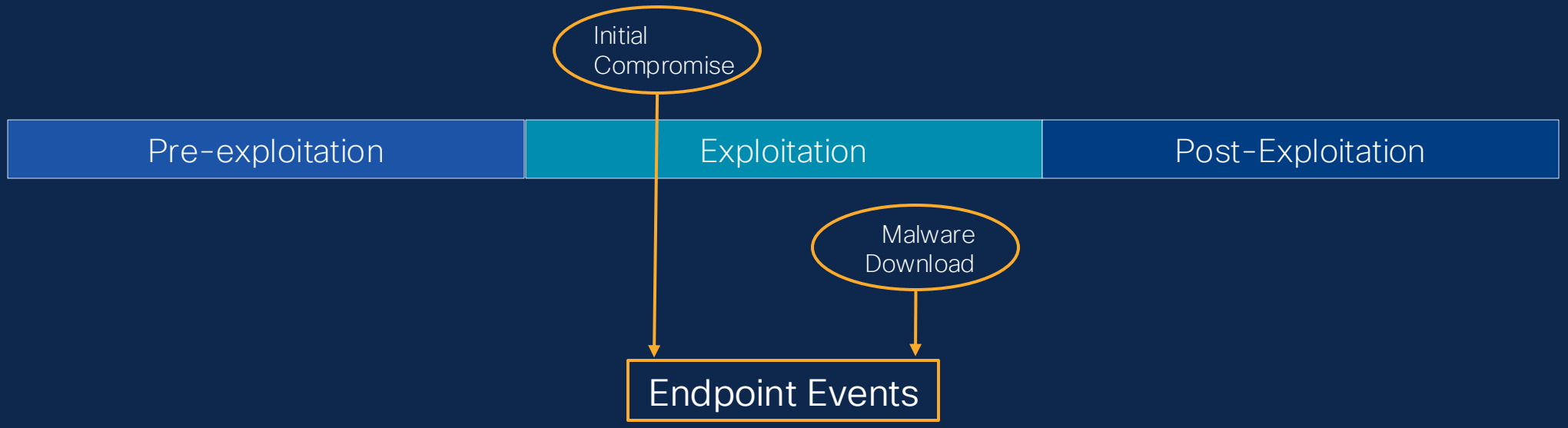
Telemetry sources for Cisco XDR

Flexible integration for existing infrastructure

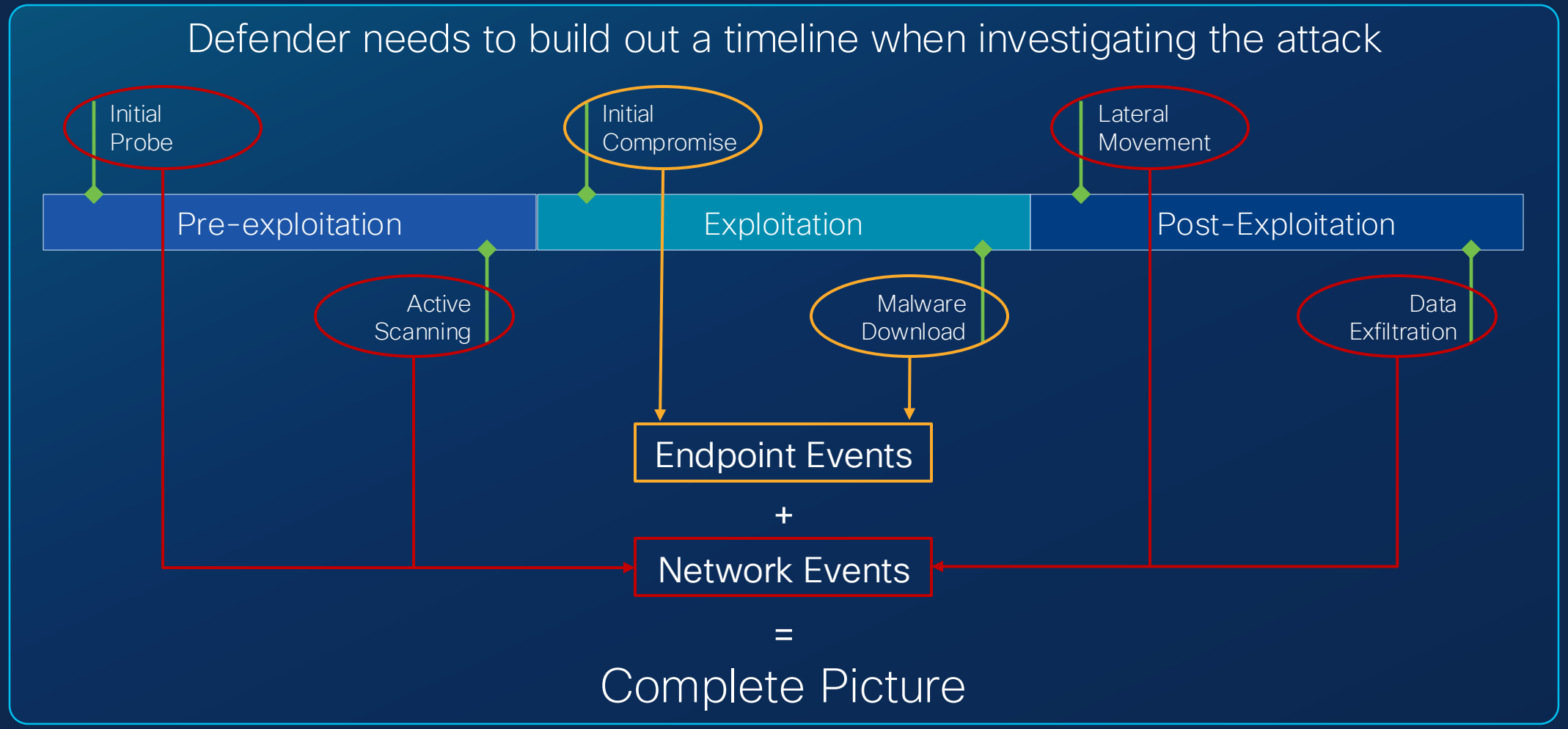


Endpoint telemetry alone is insufficient

Defender needs to build out a timeline when investigating the attack



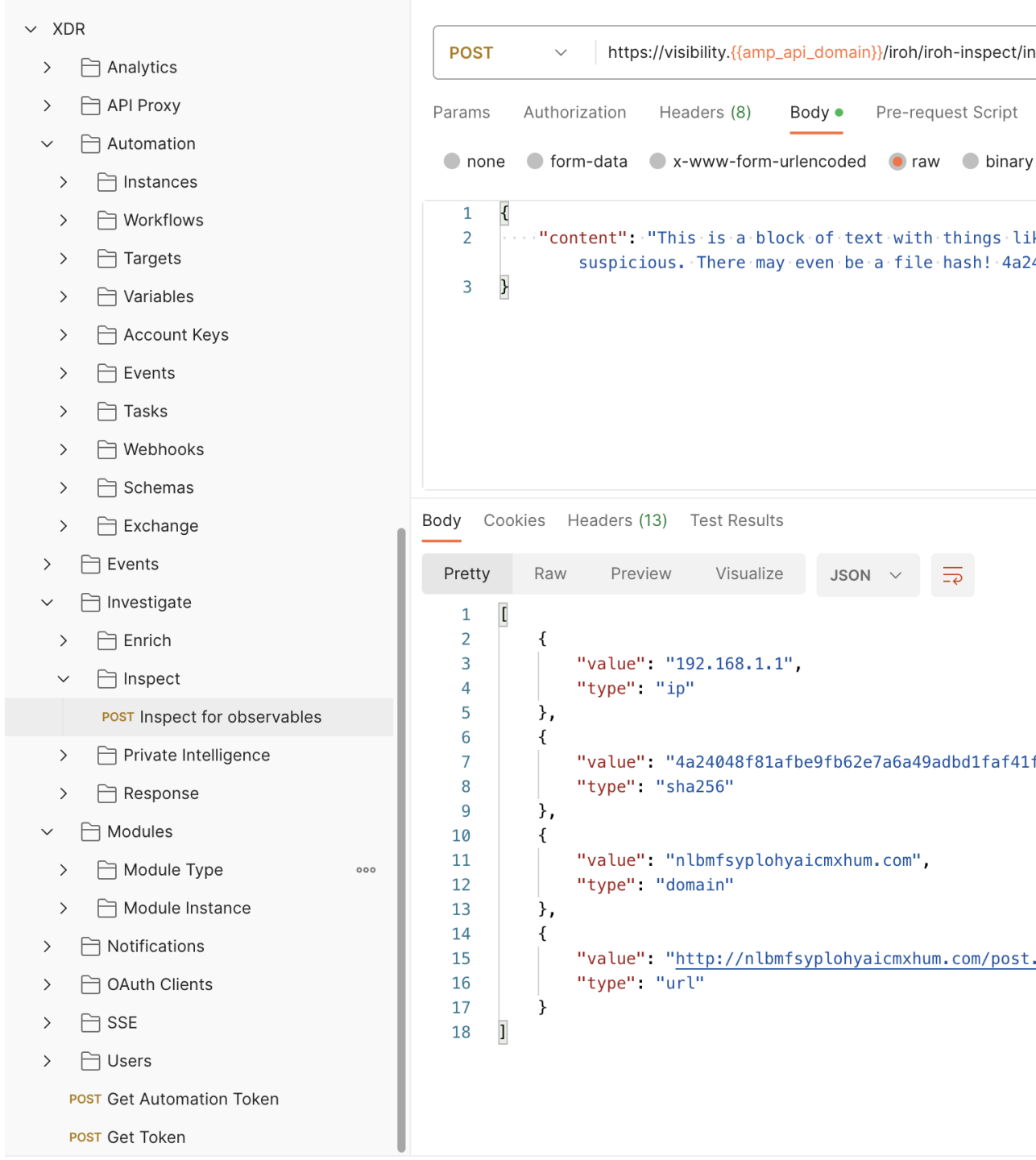
For complete visibility, you need the network



APIs are core to XDR

Cisco XDR has a wide variety of APIs that allow you to:

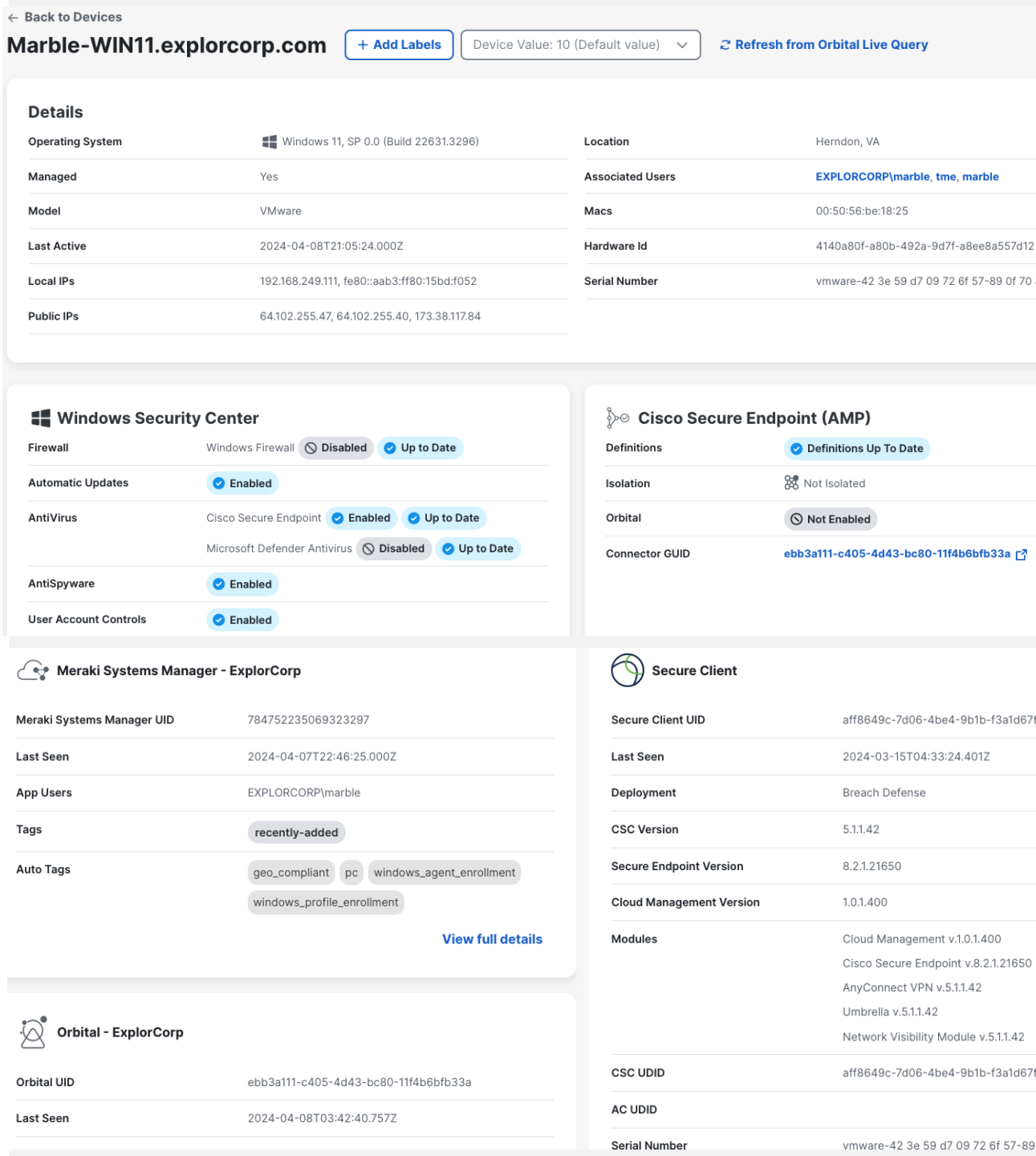
- Create and manage incidents and intelligence.
- Inspect content for observables and perform investigations.
- Communicate with integrated products and trigger response actions.



Devices

Extends the integration framework to collect data about device inventory and posture.

- Unique combination of data from security products and traditional device managers.
- Results in a unified asset inventory that can be used to provide context to investigations and meaningful reports.
- Each device has a single page of information about it, merged from all sources.
- Allows defining a device's "value" which is used when scoring XDR incidents.

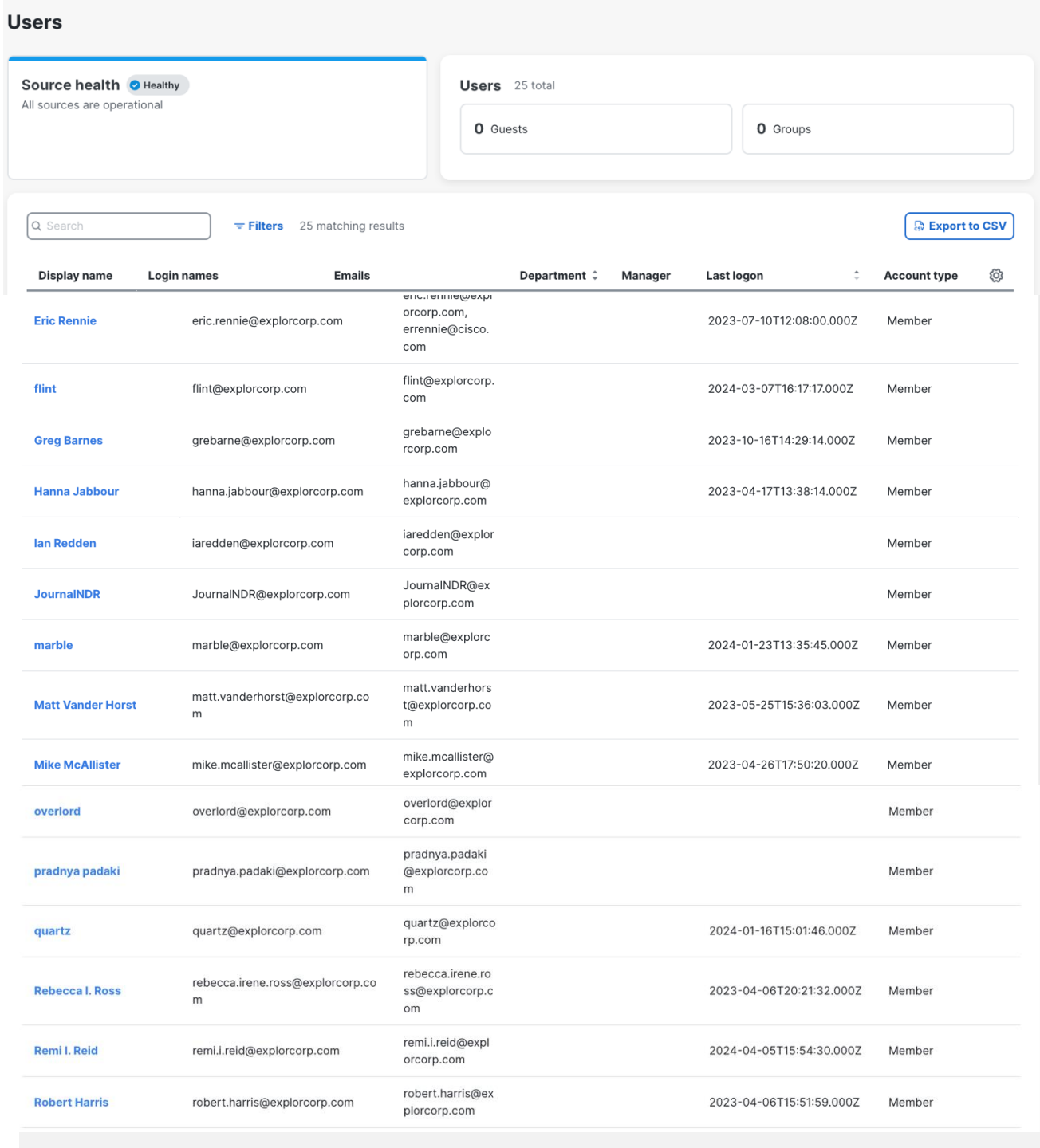


Extended context

Identity

Leverage the integration framework to collect data about user inventory and posture.

- Results in a unified asset inventory that can be used to provide context to investigations and meaningful reports.
- Each user has a single page of information about it, merged from all sources.
- Allow User and Device data association with detections and incidents



Extended context

Supported sources for XDR Devices and Identity

Duo Access
Duo Beyond

Secure Endpoint

Umbrella (DNS)
Windows / macOS

Meraki SM

Secure Client

Orbital

Duo

Third Party

CrowdStrike

SentinelOne

Microsoft
Intune

Jamf Pro

Ivanti Neurons
(formerly MobileIron)

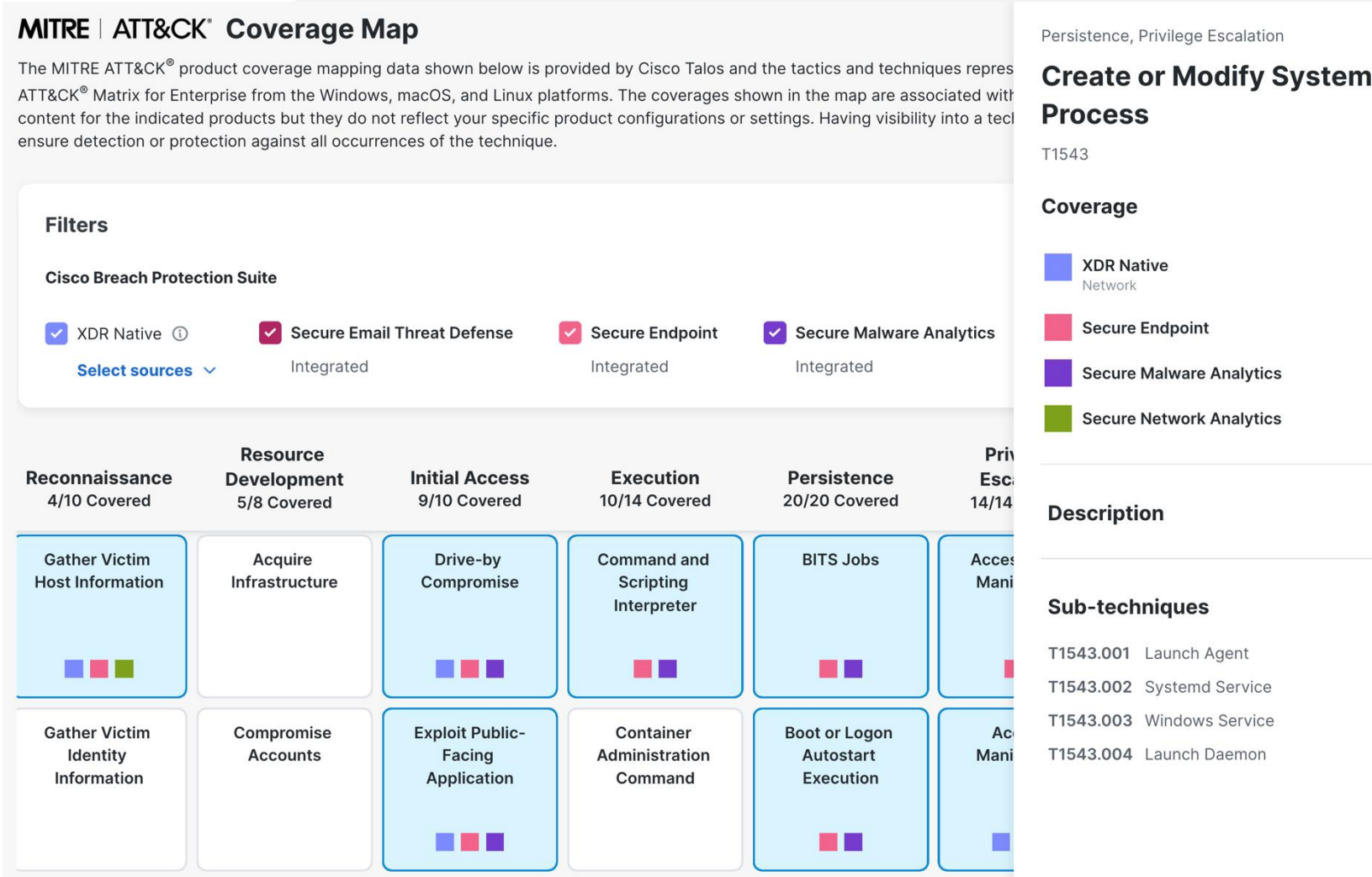
VMware
Workspace ONE
(formerly Airwatch)

Microsoft Defender
for Endpoint

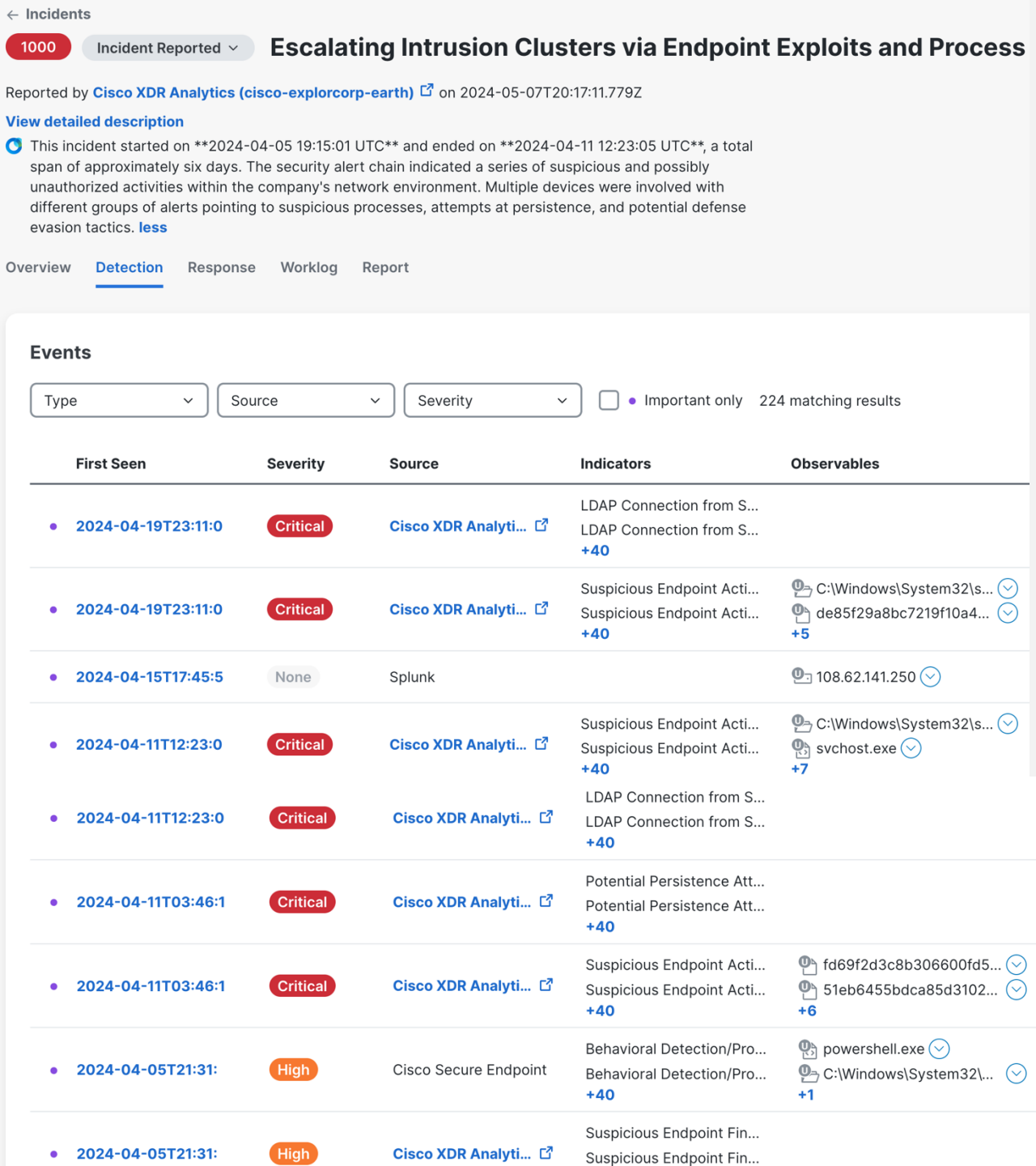
Microsoft
Azure AD

MITRE Coverage Map

- Mapping to Tactics and Techniques to Cisco Products XDR, Secure Email Threat Defense, Secure Endpoint, Secure Network Analytics and Secure Malware analytics
- Visibility on the coverage provided by each product for each tactic and technique.
- Allow faster identification of gaps and of possible routes to close these gaps
- Non-Cisco product integrations are planned in future updates

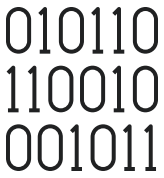


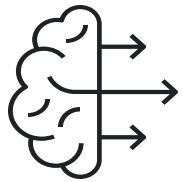
Detections



Detections

XDR Analytics detections from raw telemetry





Behavioral analytics

- Machine learning techniques for suspicious activity detections
- Endpoint NVM detections
- Anomaly detection through statistical learning
- 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

Machine Learning

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

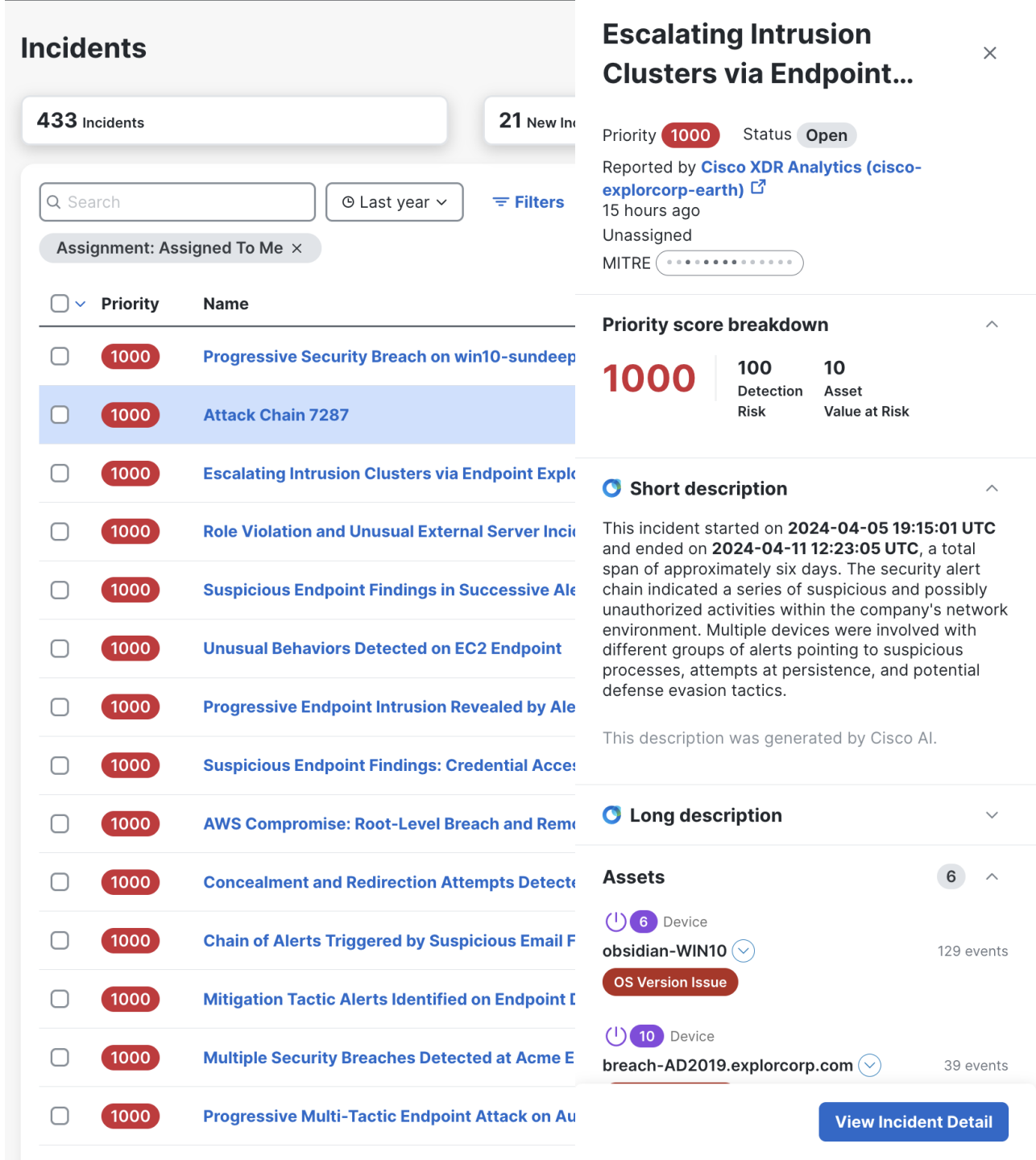
Talos threat intel

- Malware classification
- Knowledge and correlation of global campaigns to local threats
- Threatening IP, URL, and domain communication detections

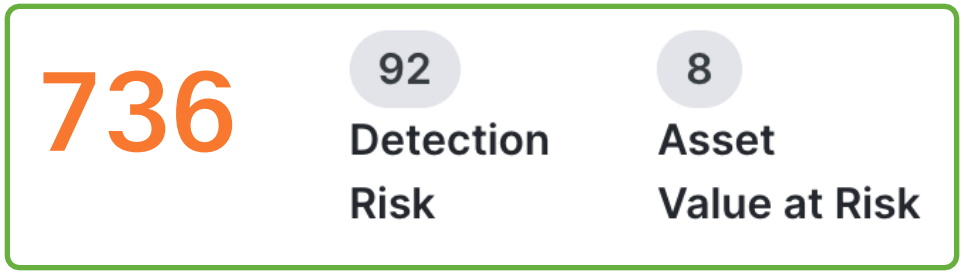
Incidents

Prioritized list of incidents based on detections from integrated products that enables analysts to quickly decide what to investigate first.

- Various options for sorting and filtering.
- Source indicates which product the incident originated from.
- Assignees and status can be changed right from the incident list.
- The drawer shows a summary of the selected incident including key information such as source, assignees, and MITRE tactics and techniques.



Identify the most impactful incidents based on risk



Priority Score = **Detection Risk** x **Asset Value**

0–1000 | 0–100 | 0–10

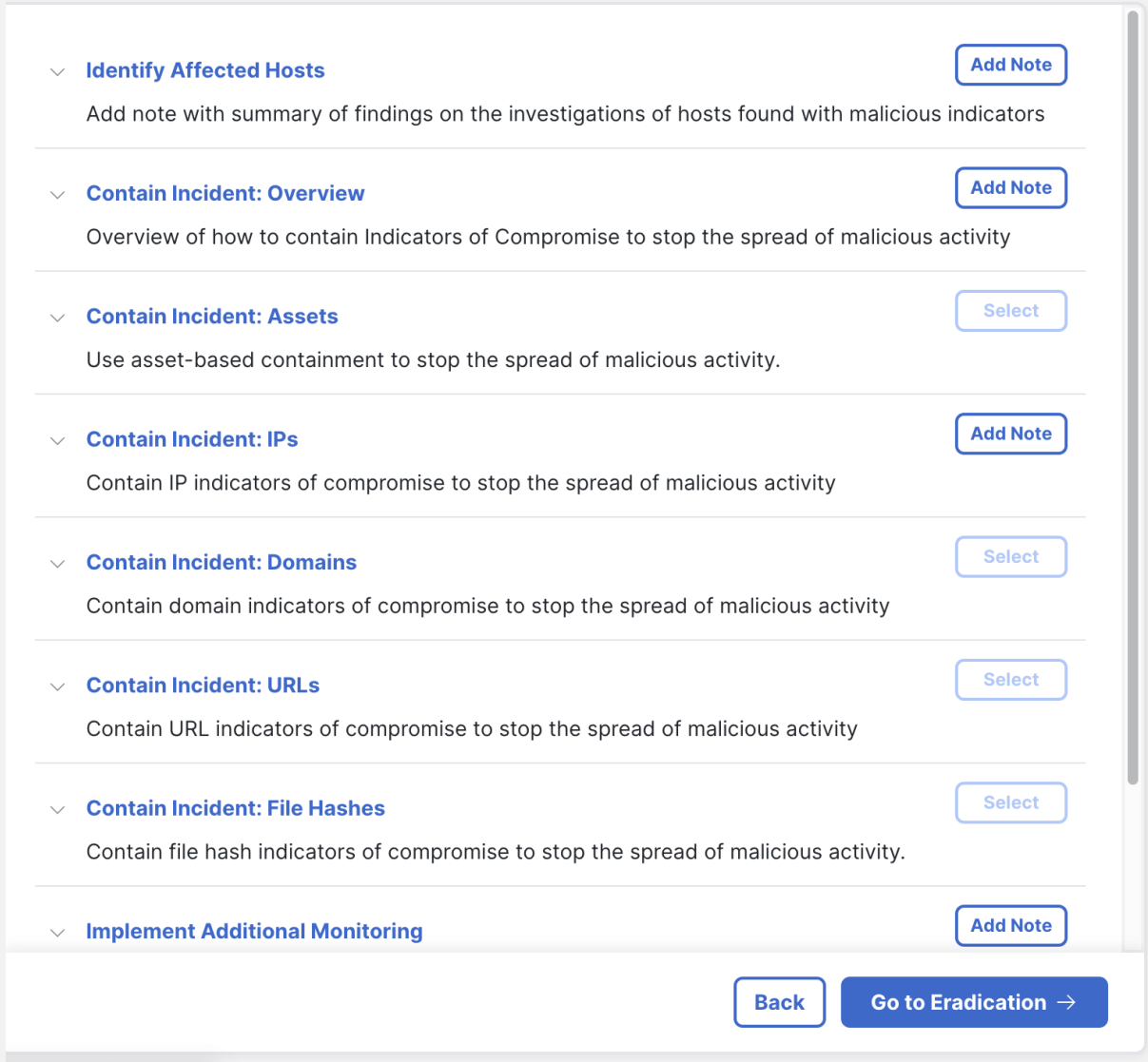
The Incident total priority score used to prioritize incidents

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

Response



Incident response in four stages

Identify

Review the incident and confirm the findings

Contain

Act against impacted hosts, domains, and files

Eradicate

Mitigate or remediate vulnerabilities and remove malicious content

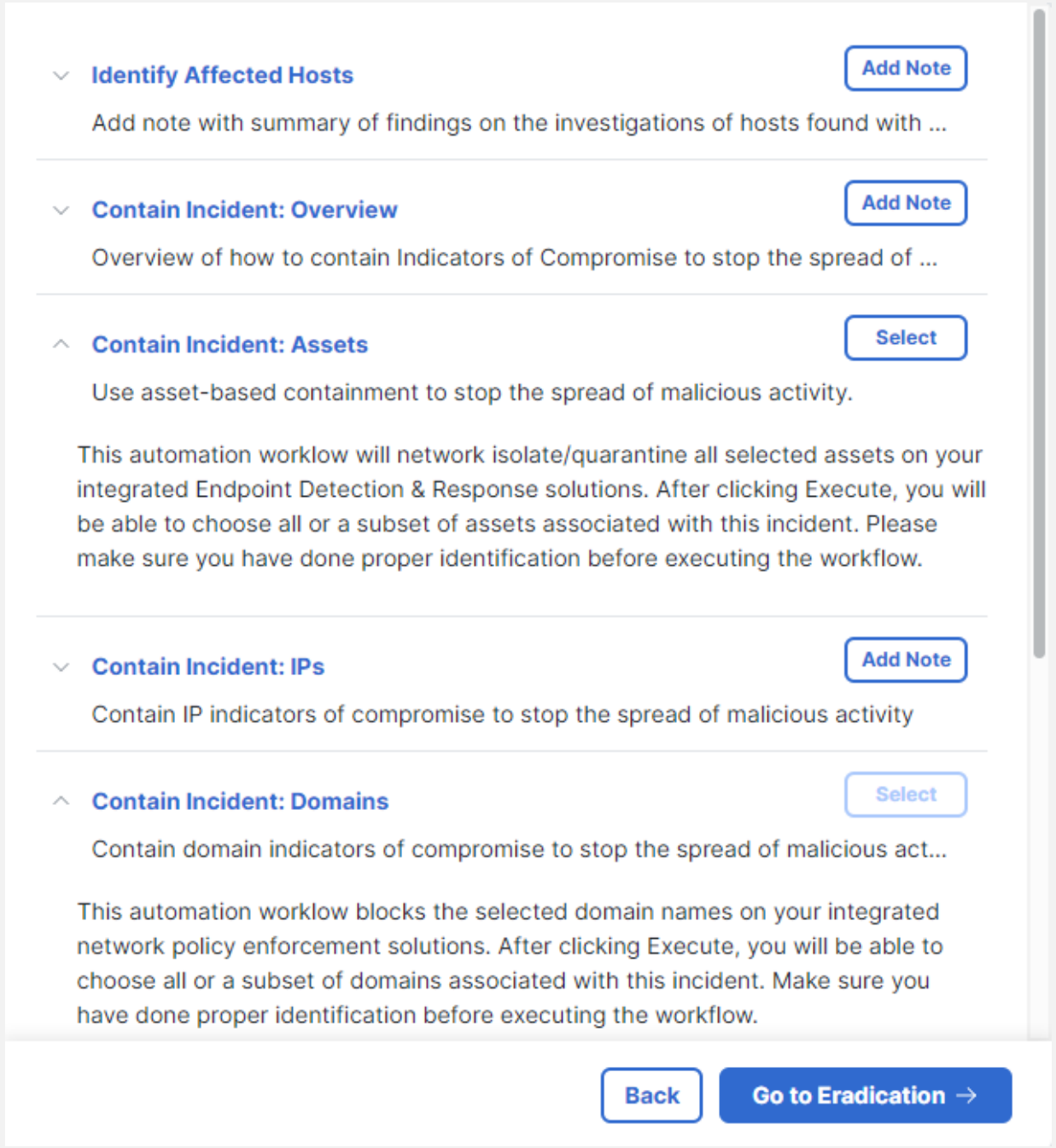
Recover

Validate remediation steps and restore impacted services

Response playbooks

Bring the ability to take immediate response actions into the incident manager.

- Powered by out of the box XDR Automation workflows.
- Create customized playbooks and apply them where needed
- Broken down into four stages:
  - Identify
  - Contain
  - Eradicate
  - Recover

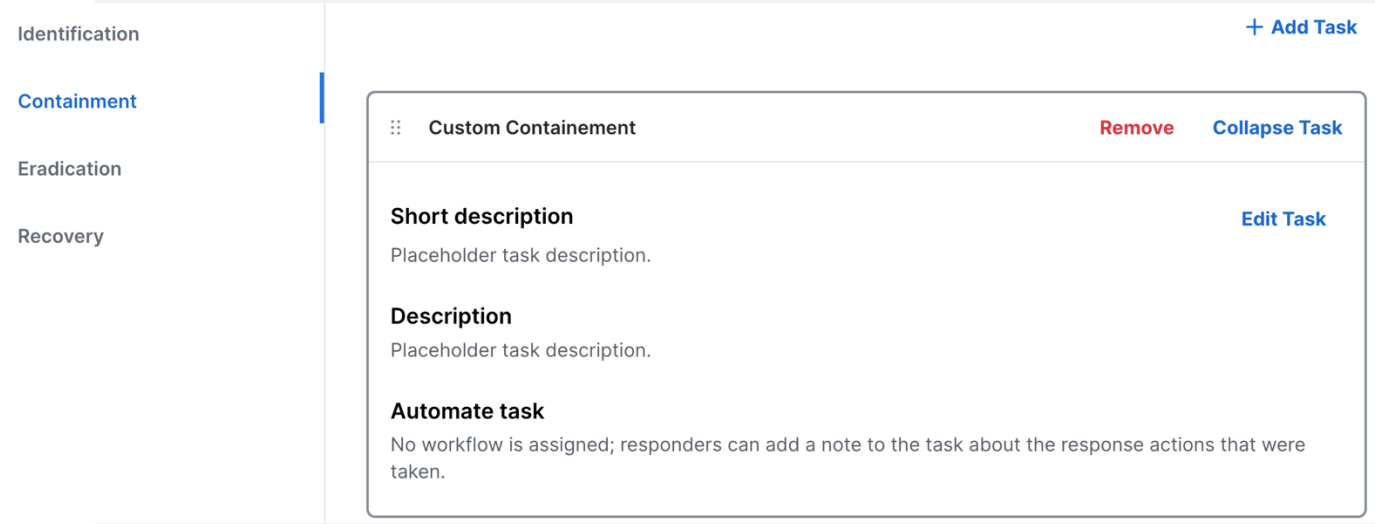


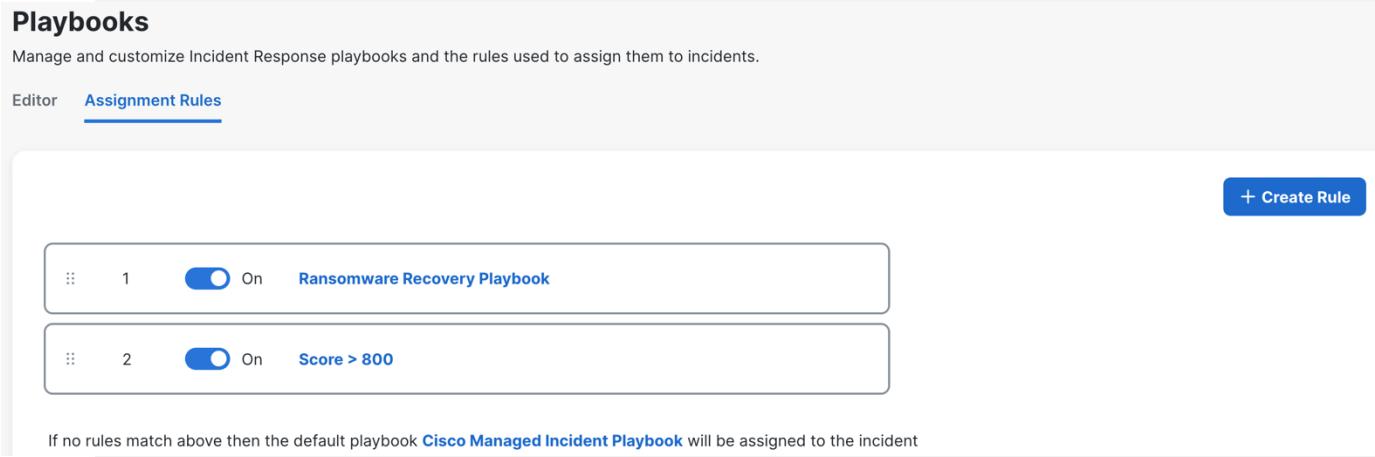
Custom Play Books

Provide the ability to create customized playbooks.

- Create customized playbooks provides the ability to respond to incidents with a customized actions based on use case.

- Dynamically assign playbooks using rules to link playbooks to incidents based on specific conditions.

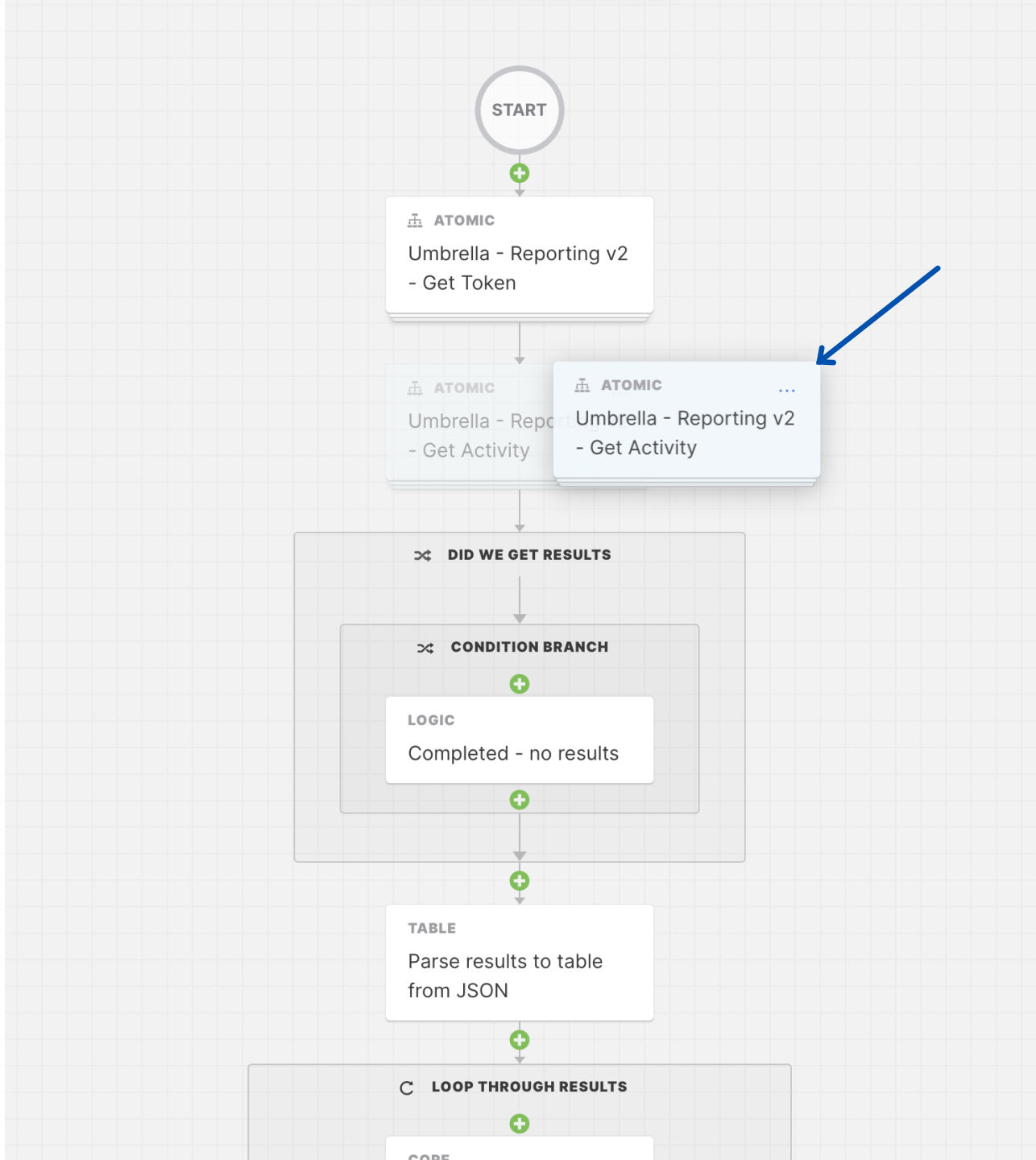




XDR Automation

A “no to low code” drag and drop editor that allows you to build simple or complex workflows.

- Powers the playbook feature in the incident manager using out of the box workflows.
- Pre-written workflows are available for import from Cisco.
- Wide variety of use cases that are not limited to security or XDR-related outcomes.



AI driven at every stage

Threat Detections

Unearthing hidden threats with machine learning technique that finds suspicious activities using advanced algorithms

Native language processing detects spear phishing and advanced email attack

AI Summarization and reporting

AI summarizes incident alerts, events in a human readable and comprehensible format which makes it easier for a SOC analyst to understand and handle the attack from start to end.

Enhance Decision Making with AI generated multi-layer incident reports with tailored information at each level from executive summaries to event lists in a single view.

Interactive AI Assistance

Achieve faster outcomes with interactive AI Assistant, a SOC analyst can invoke and interact with Assistant at any stage of an incident.

AI Assistant supports the SOC analyst with incident management providing clarity, summarization, guided responses and tailored recommendations.

An XDR is as good as its outcomes

How good are we at detecting attacks early?

1 Detect Sooner

Extend Asset Context 2

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

Where are we most exposed to risk? Are we prioritizing the attacks that represent the greatest material impacts to our business?

3 Prioritize by Impact

Reduce Investigation Time 4

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

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

5 Accelerate Response

Live Demo

Easy to buy tiers for Cisco XDR

Cisco XDR Essentials

Full-featured XDR
+
Native integration of the full Cisco security portfolio
+
Talos and third-party threat intelligence enrichment

Cisco XDR Advantage

All features in Essentials
+
Integrations with extensive list of third-party tools

Cisco XDR Premier

All features in Advantage
+
Managed extended detection & response (MXDR) delivered by Cisco CX

Buy **a la carte** or as a part of the **Breach Protection Suite**.