



Cisco XDR

The Future of IT Security Operations

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

October 2025



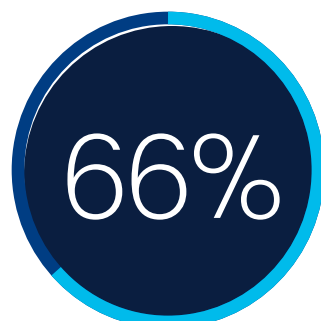
AGENDA

- 1 Overview
- 2 **X**tended Context
- 3 **D**etections
- 4 **R**esponse

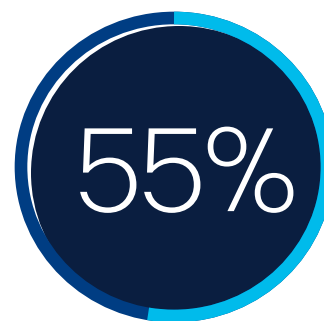
What are the challenges?



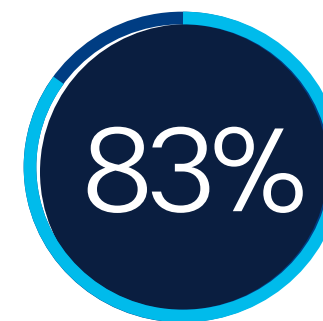
of attacks involve lateral movement from the entry point across the network¹



of organizations were affected by ransomware in 2022²

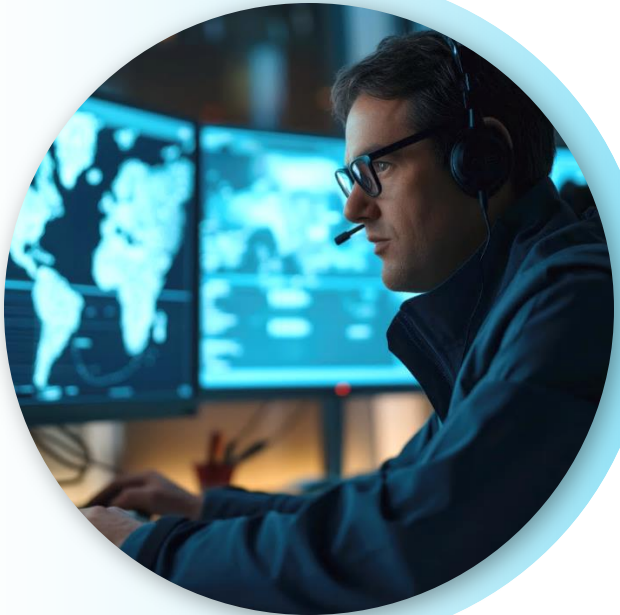


of security teams say critical alerts are being missed³



of the cyberattacks in 2023 were identity related⁴

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):

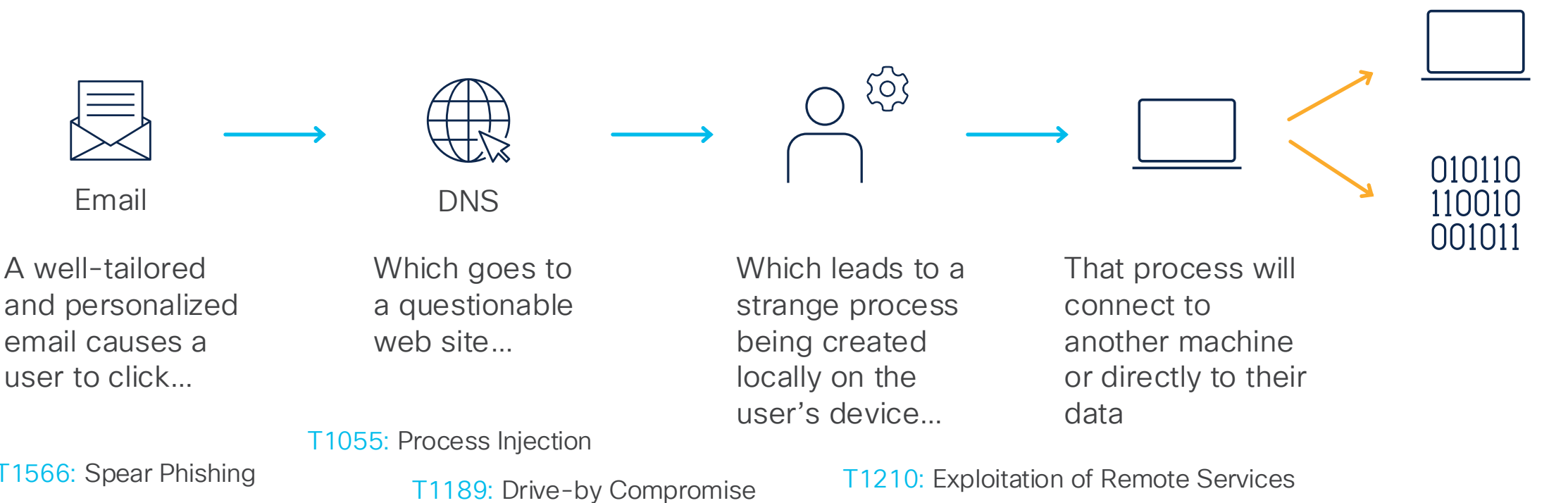
Integrates multiple security products (EDR, NDR, email, cloud, etc.) to provide a unified detection and response platform.

MDR (Managed Detection and Response):

A service that provides threat detection and response as an expert managed service.

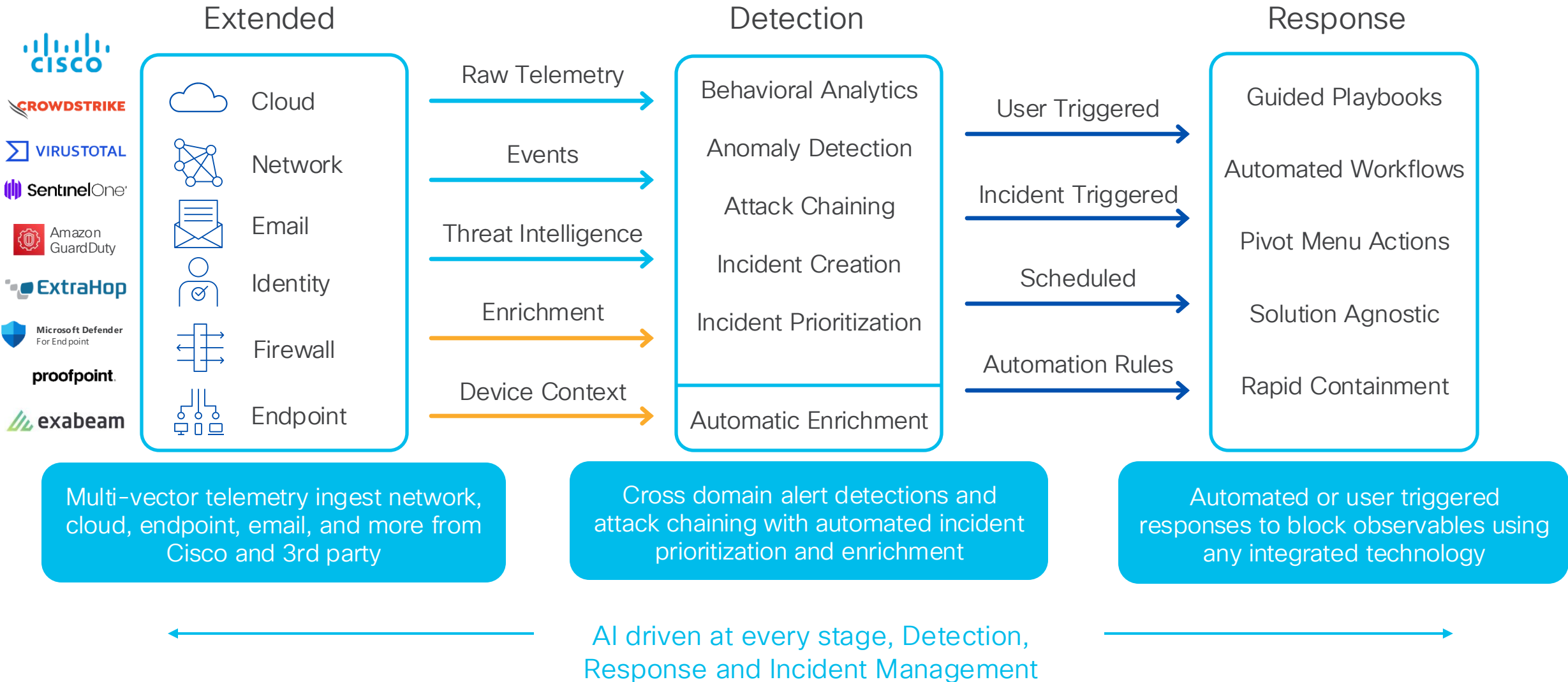
Stop advanced threats like ransomware

Most attacks use a sequence like this...



 Cisco XDR

XDR High level architecture



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.”

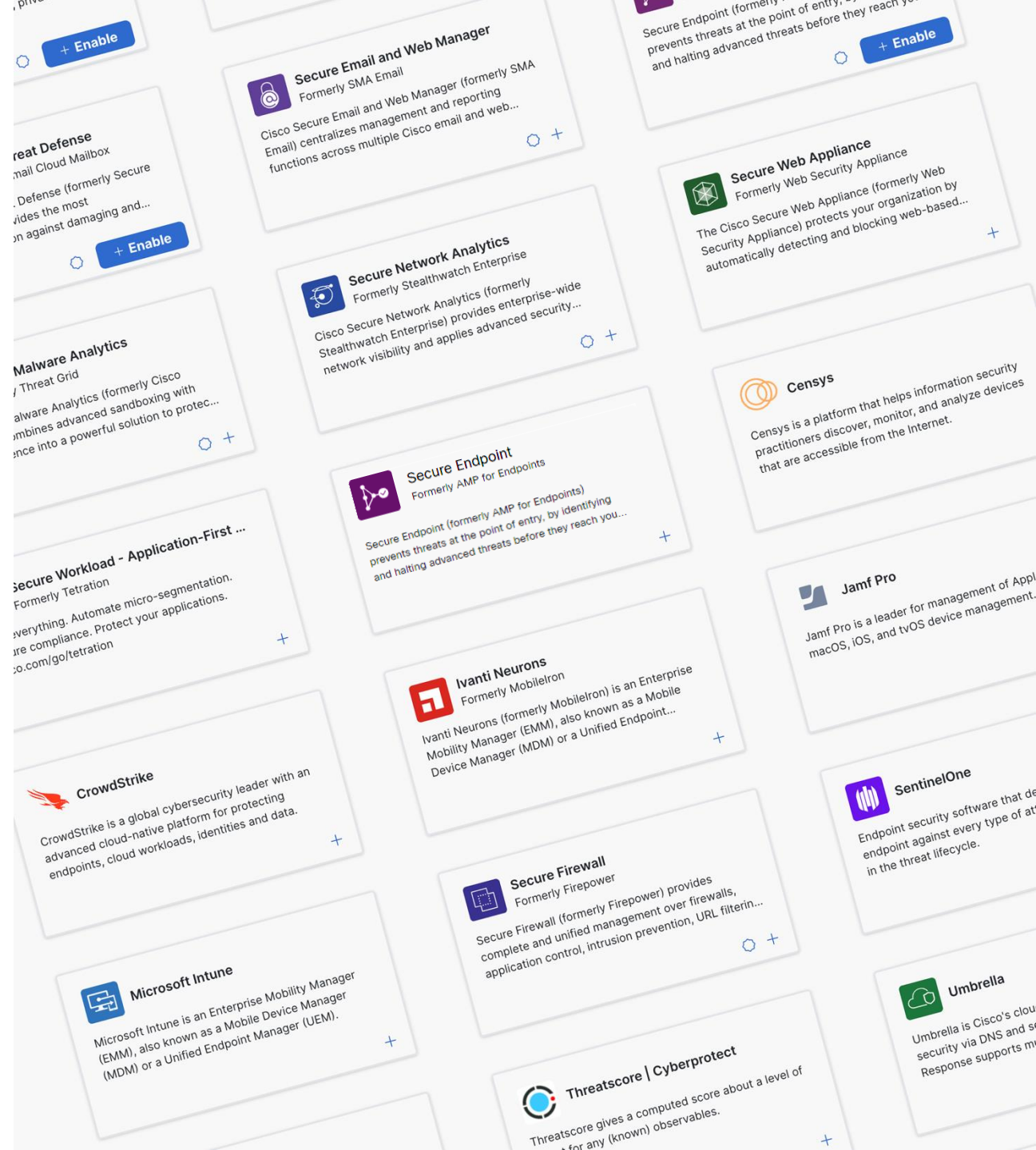


“Device has been sending unusually large DNS packets. May indicate an attacker using the DNS protocol as a covert communications channel to exfiltrate data.”



“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

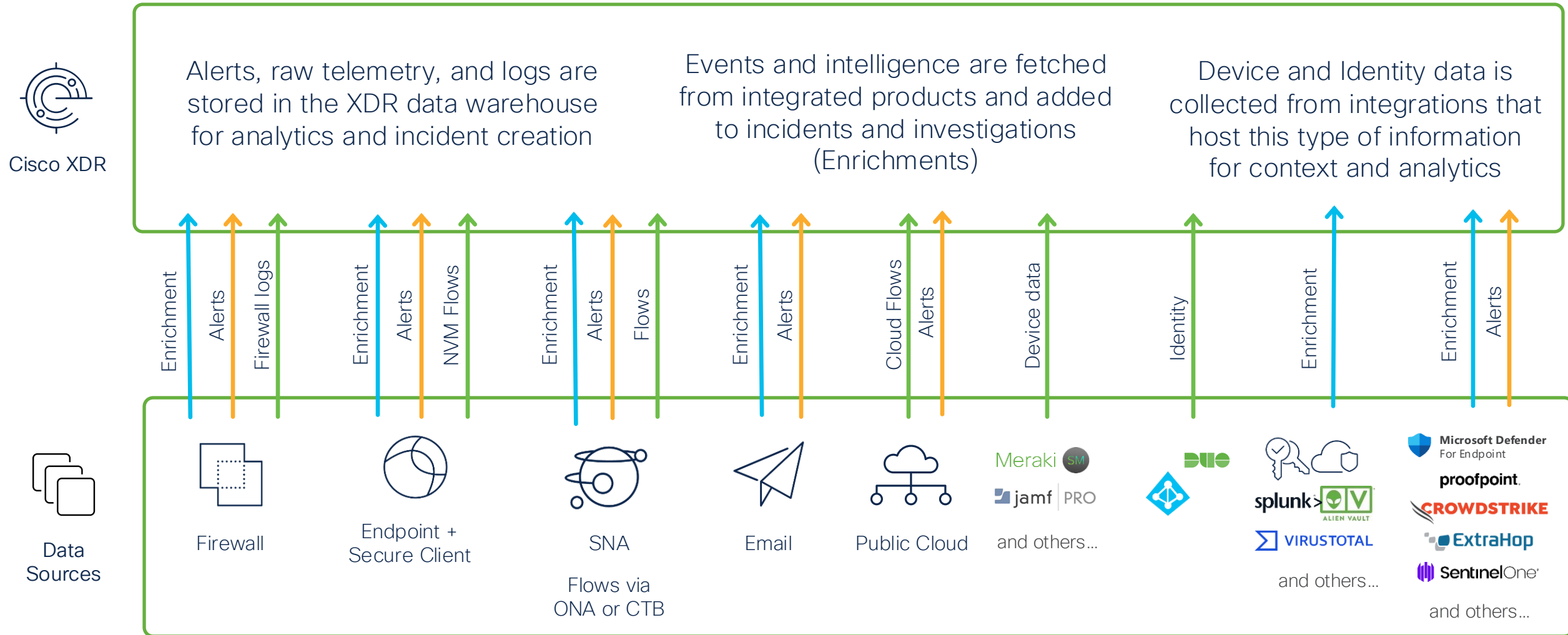
Integration	Detection Analytics and Correlation	Threat Hunting and Investigation	Dashboard Tiles	Asset Insights and Context	Automation and Response	
					Controls and Responses	Security Operations Center (SOC) Automation
Cisco Vulnerability Management	No	No	No	No	No	Yes
Meraki	No	No	No	Yes	No	Yes
Orbital	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

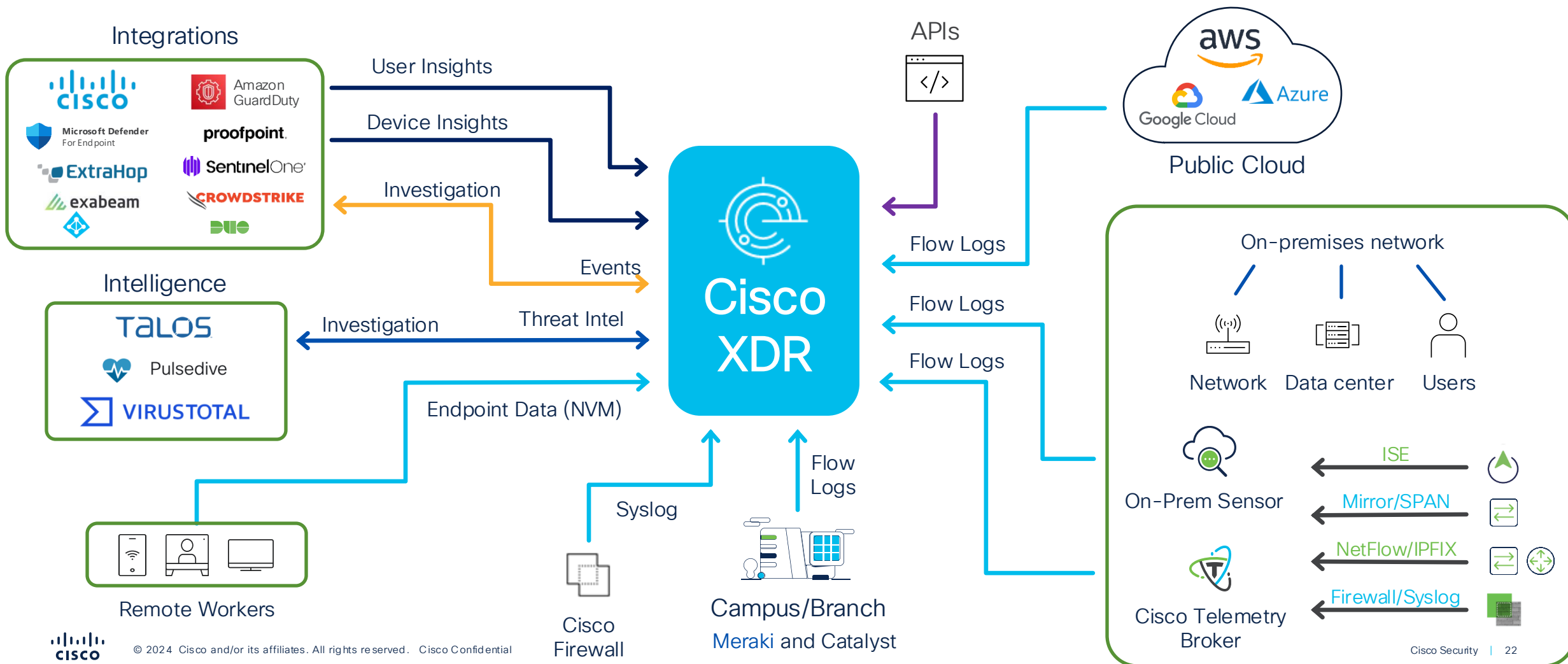
Telemetry and enrichment



Extended context

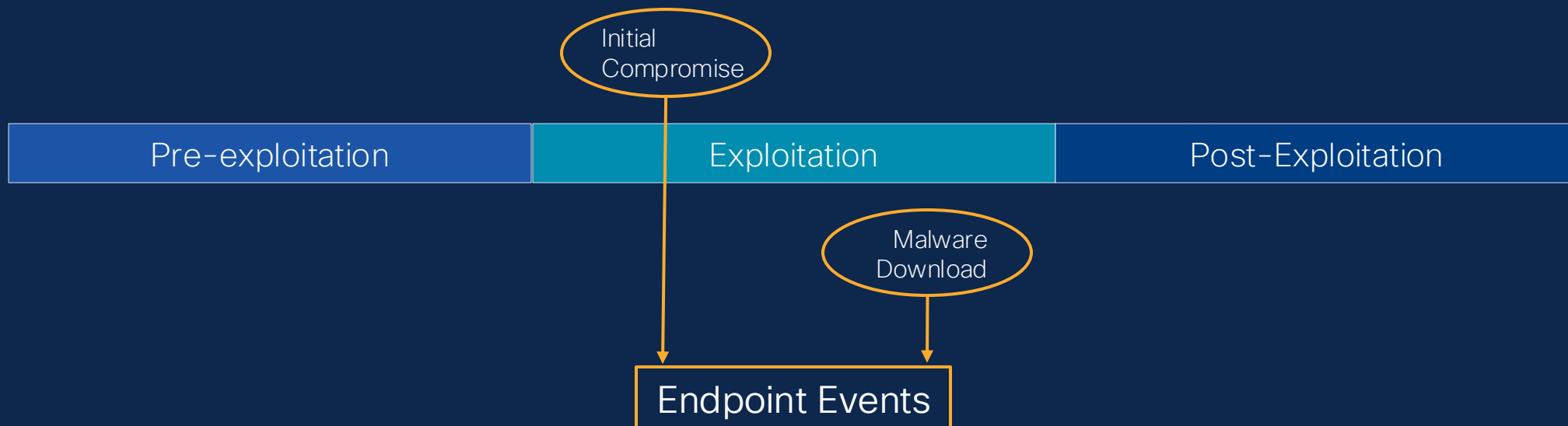
Telemetry sources for Cisco XDR

Flexible integration for existing infrastructure

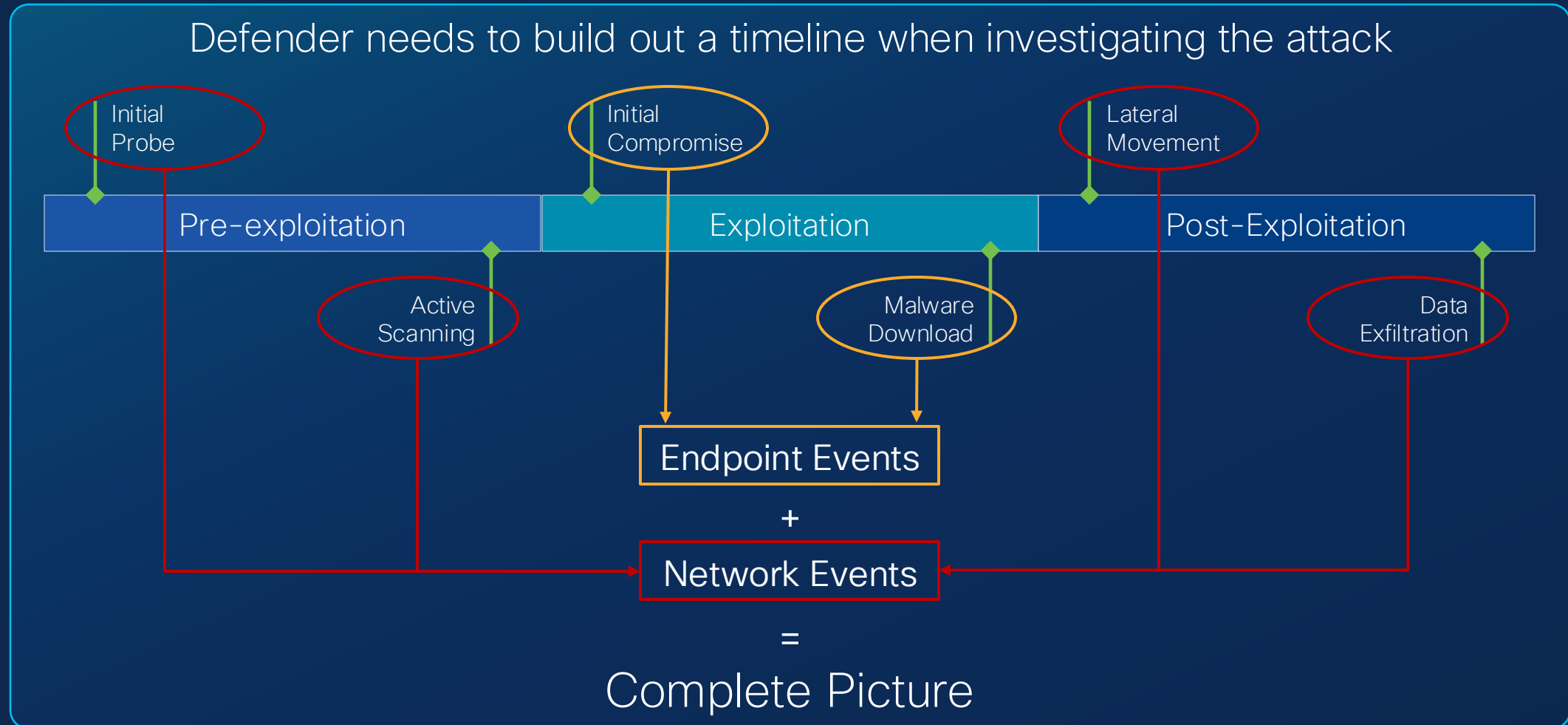


Endpoint telemetry alone is insufficient

Defender needs to build out a timeline when investigating the attack



For complete visibility, you need the network

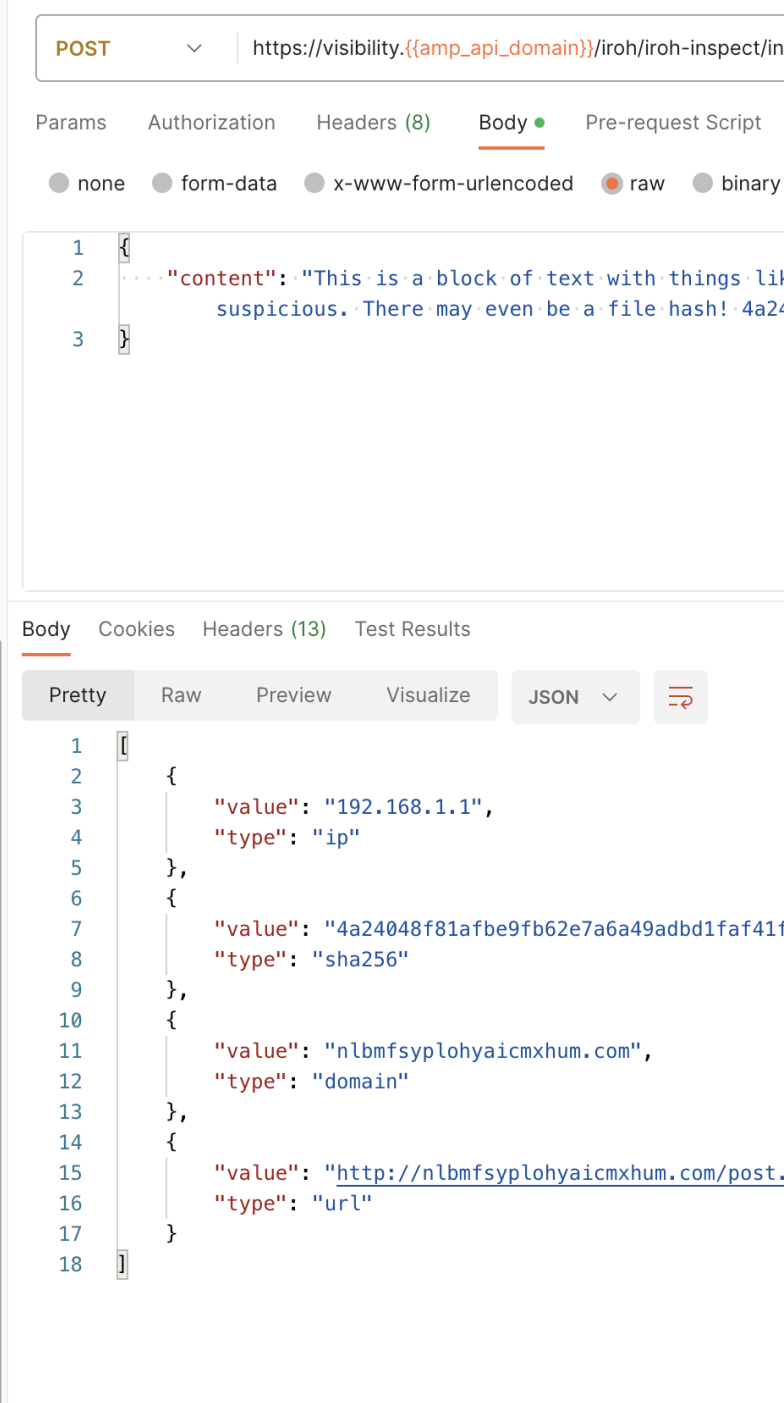
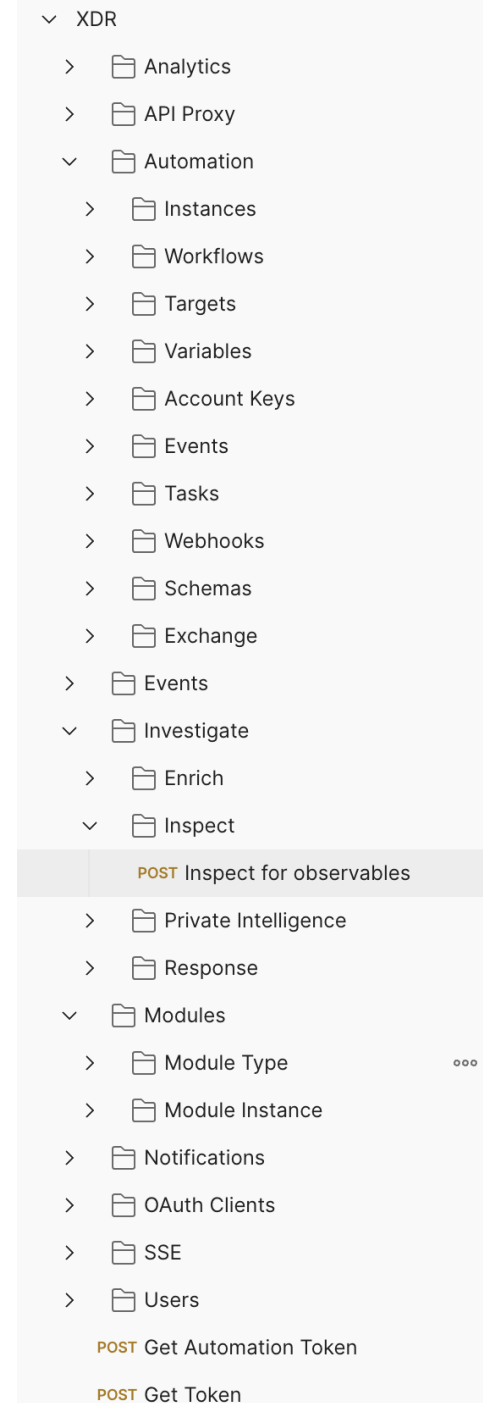


Extended context

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.



Extended context

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.

← Back to Devices

Marble-WIN11.explorcorp.com

+ Add Labels

Device Value: 10 (Default value) ▾

Refresh from Orbital Live Query

Details

Operating System	Windows 11, SP 0.0 (Build 22H2.3296)	Location	Herndon, VA
Managed	Yes	Associated Users	EXPLORCORP\marble, tme, marble
Model	VMware	Macs	00:50:56:be:18:25
Last Active	2024-04-08T21:05:24.000Z	Hardware Id	4140a80f-a80b-492a-9d7f-a8ee8a557d12
Local IPs	192.168.249.111, fe80::aab3:ff80:15bd:f052	Serial Number	vmware-42 3e 59 d7 09 72 6f 57-89 0f 70
Public IPs	64.102.255.47, 64.102.255.40, 173.38.117.84		

Windows Security Center

Firewall

Windows Firewall

Disabled

Up to Date

Automatic Updates

Enabled

AntiVirus

Cisco Secure Endpoint

Enabled

Up to Date

Microsoft Defender Antivirus

Disabled

Up to Date

AntiSpyware

Enabled

User Account Controls

Enabled

Cisco Secure Endpoint (AMP)

Definitions

Definitions Up To Date

Isolation

Not Isolated

Orbital

Not Enabled

Connector GUID

ebb3a111-c405-4d43-bc80-11f4b6bfb33a

Meraki Systems Manager - ExplorCorp

Meraki Systems Manager UID

784752235069323297

Last Seen

2024-04-07T22:46:25.000Z

App Users

EXPLORCORP\marble

Tags

recently-added

Auto Tags

geo_compliant

pc

windows_agent_enrollment

windows_profile_enrollment

View full details

Orbital - ExplorCorp

Orbital UID

ebb3a111-c405-4d43-bc80-11f4b6bfb33a

Last Seen

2024-04-08T03:42:40.757Z

Secure Client

Secure Client UID

aff8649c-7d06-4be4-9b1b-f3a1d67f

Last Seen

2024-03-15T04:33:24.401Z

Deployment

Breach Defense

CSC Version

5.1.1.42

Secure Endpoint Version

8.2.1.21650

Cloud Management Version

1.0.1.400

Modules

Cloud Management v.1.0.1.400

Cisco Secure Endpoint v.8.2.1.21650

AnyConnect VPN v.5.1.1.42

Umbrella v.5.1.1.42

Network Visibility Module v.5.1.1.42

CSC UDID

aff8649c-7d06-4be4-9b1b-f3a1d67f

AC UDID

Serial Number

vmware-42 3e 59 d7 09 72 6f 57-89

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

Users

Source health Healthy

All sources are operational

Users 25 total

0 Guests

0 Groups

Q Search

Filters 25 matching results

Export to CSV

Display name	Login names	Emails	Department	Manager	Last logon	Account type
Eric Rennie	eric.ennie@explorcorp.com	eric.ennie@explorcorp.com, errennie@cisco.com			2023-07-10T12:08:00.000Z	Member
flint	flint@explorcorp.com	flint@explorcorp.com			2024-03-07T16:17:17.000Z	Member
Greg Barnes	grebarne@explorcorp.com	grebarne@explorcorp.com			2023-10-16T14:29:14.000Z	Member
Hanna Jabbour	hanna.jabbour@explorcorp.com	hanna.jabbour@explorcorp.com			2023-04-17T13:38:14.000Z	Member
Ian Redden	iaredden@explorcorp.com	iaredden@explorcorp.com				Member
JournalNDR	JournalNDR@explorcorp.com	JournalNDR@explorcorp.com				Member
marble	marble@explorcorp.com	marble@explorcorp.com			2024-01-23T13:35:45.000Z	Member
Matt Vander Horst	matt.vanderhorst@explorcorp.com	matt.vanderhorst@explorcorp.com			2023-05-25T15:36:03.000Z	Member
Mike McAllister	mike.mcallister@explorcorp.com	mike.mcallister@explorcorp.com			2023-04-26T17:50:20.000Z	Member
overlord	overlord@explorcorp.com	overlord@explorcorp.com				Member
pradnya padaki	pradnya.padaki@explorcorp.com	pradnya.padaki@explorcorp.com				Member
quartz	quartz@explorcorp.com	quartz@explorcorp.com			2024-01-16T15:01:46.000Z	Member
Rebecca I. Ross	rebecca.irene.ross@explorcorp.com	rebecca.irene.ross@explorcorp.com			2023-04-06T20:21:32.000Z	Member
Remi I. Reid	remi.i.reid@explorcorp.com	remi.i.reid@explorcorp.com			2024-04-05T15:54:30.000Z	Member
Robert Harris	robert.harris@explorcorp.com	robert.harris@explorcorp.com			2023-04-06T15:51:59.000Z	Member



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



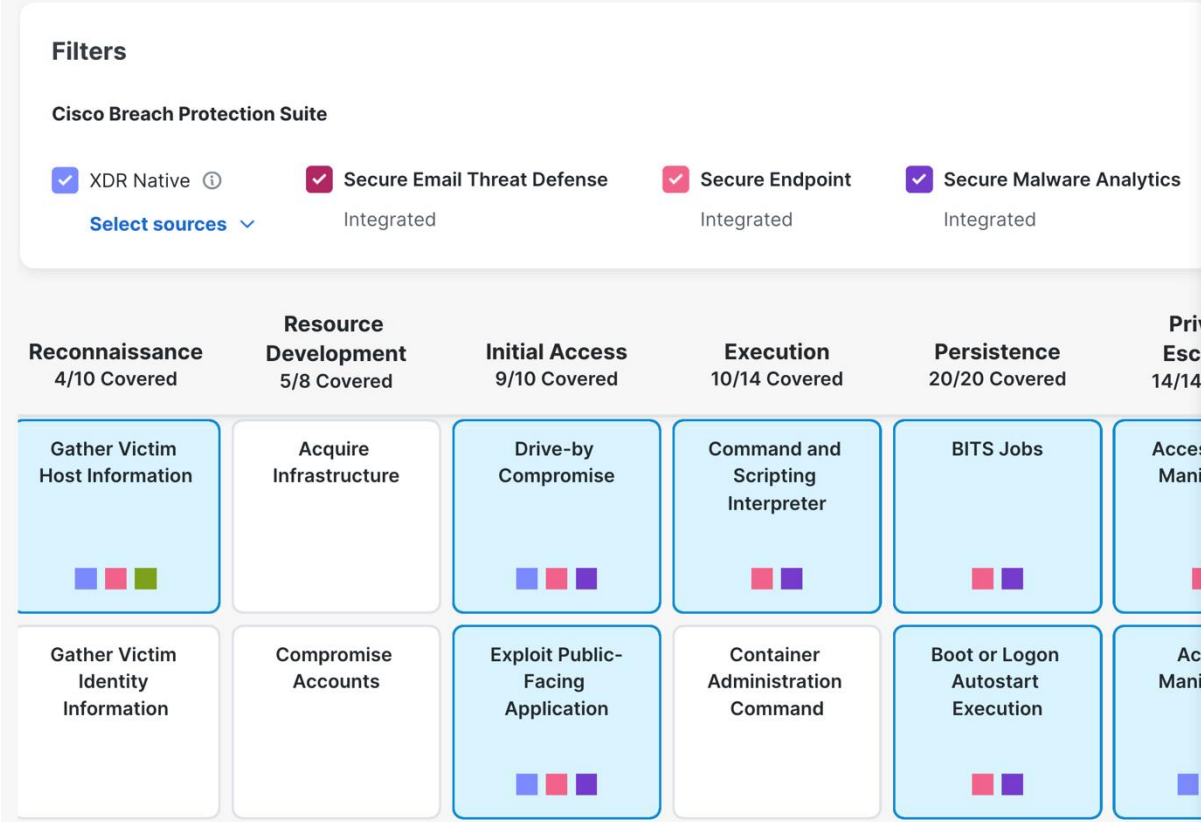
Microsoft
Azure AD

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

MITRE | ATT&CK® Coverage Map

The MITRE ATT&CK® product coverage mapping data shown below is provided by Cisco Talos and the tactics and techniques represent the ATT&CK® Matrix for Enterprise from the Windows, macOS, and Linux platforms. The coverages shown in the map are associated with content for the indicated products but they do not reflect your specific product configurations or settings. Having visibility into a technique ensures detection or protection against all occurrences of the technique.



Persistence, Privilege Escalation

Create or Modify System Process

T1543

Coverage

- XDR Native Network
- Secure Endpoint
- Secure Malware Analytics
- Secure Network Analytics

Description

Sub-techniques

- T1543.001 Launch Agent
- T1543.002 Systemd Service
- T1543.003 Windows Service
- T1543.004 Launch Daemon

Detections

Reported by [Cisco XDR Analytics \(cisco-explorcorp-earth\)](#) on 2024-05-07T20:17:11.779Z

[View detailed description](#)

This incident started on **2024-04-05 19:15:01 UTC** and ended on **2024-04-11 12:23:05 UTC**, a total span of approximately six days. The security alert chain indicated a series of suspicious and possibly unauthorized activities within the company's network environment. Multiple devices were involved with different groups of alerts pointing to suspicious processes, attempts at persistence, and potential defense evasion tactics. [less](#)

Overview Detection Response Worklog Report

Events

Type ▾

Source ▾

Severity ▾

☐ Important only

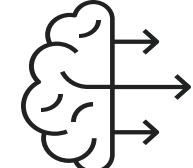
224 matching results

First Seen	Severity	Source	Indicators	Observables
• 2024-04-19T23:11:0	Critical	Cisco XDR Analyti... ↗	LDAP Connection from S... LDAP Connection from S... +40	
• 2024-04-19T23:11:0	Critical	Cisco XDR Analyti... ↗	Suspicious Endpoint Acti... Suspicious Endpoint Acti... +40	 C:\Windows\System32\s... ⌵  de85f29a8bc7219f10a4... ⌵ +5
• 2024-04-15T17:45:5	None	Splunk		 108.62.141.250 ⌵
• 2024-04-11T12:23:0	Critical	Cisco XDR Analyti... ↗	Suspicious Endpoint Acti... Suspicious Endpoint Acti... +40	 C:\Windows\System32\s... ⌵  svchost.exe ⌵ +7
• 2024-04-11T12:23:0	Critical	Cisco XDR Analyti... ↗	LDAP Connection from S... LDAP Connection from S... +40	
• 2024-04-11T03:46:1	Critical	Cisco XDR Analyti... ↗	Potential Persistence Att... Potential Persistence Att... +40	
• 2024-04-11T03:46:1	Critical	Cisco XDR Analyti... ↗	Suspicious Endpoint Acti... Suspicious Endpoint Acti... +40	 fd69f2d3c8b306600fd5... ⌵  51eb6455bdca85d3102... ⌵ +6
• 2024-04-05T21:31:	High	Cisco Secure Endpoint	Behavioral Detection/Pro... Behavioral Detection/Pro... +40	 powershell.exe ⌵  C:\Windows\System32\... ⌵ +1
• 2024-04-05T21:31:	High	Cisco XDR Analyti... ↗	Suspicious Endpoint Fin... Suspicious Endpoint Fin...	



XDR Analytics detections from raw telemetry

010110
110010
001011



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.

Incidents

433 Incidents

21 New Inc

Search

Last year

Filters

Assignment: Assigned To Me

☐	Priority	Name
☐	1000	Progressive Security Breach on win10-sundee
☐	1000	Attack Chain 7287
☐	1000	Escalating Intrusion Clusters via Endpoint Expl
☐	1000	Role Violation and Unusual External Server Inci
☐	1000	Suspicious Endpoint Findings in Successive Ale
☐	1000	Unusual Behaviors Detected on EC2 Endpoint
☐	1000	Progressive Endpoint Intrusion Revealed by Ale
☐	1000	Suspicious Endpoint Findings: Credential Acce
☐	1000	AWS Compromise: Root-Level Breach and Rem
☐	1000	Concealment and Redirection Attempts Detect
☐	1000	Chain of Alerts Triggered by Suspicious Email F
☐	1000	Mitigation Tactic Alerts Identified on Endpoint T
☐	1000	Multiple Security Breaches Detected at Acme E
☐	1000	Progressive Multi-Tactic Endpoint Attack on Au

Escalating Intrusion Clusters via Endpoint...

Priority 1000 Status Open
Reported by Cisco XDR Analytics (cisco-explorcorp-earth) 15 hours ago
Unassigned
MITRE

Priority score breakdown

1000
100 Detection Risk
10 Asset Value at Risk

Short description

This incident started on 2024-04-05 19:15:01 UTC and ended on 2024-04-11 12:23:05 UTC, a total span of approximately six days. The security alert chain indicated a series of suspicious and possibly unauthorized activities within the company's network environment. Multiple devices were involved with different groups of alerts pointing to suspicious processes, attempts at persistence, and potential defense evasion tactics.

This description was generated by Cisco AI.

Long description

Assets

6 Device
obsidian-WIN10 129 events
OS Version Issue
10 Device
breach-AD2019.explorcorp.com 39 events

View Incident Detail

Identify the most impactful incidents based on risk

736

92

Detection
Risk

8

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 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

▼ Identify Affected Hosts

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

Add Note

▼ Contain Incident: Overview

Overview of how to contain Indicators of Compromise to stop the spread of malicious activity

Add Note

▼ Contain Incident: Assets

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

Select

▼ Contain Incident: IPs

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

Add Note

▼ Contain Incident: Domains

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

Select

▼ Contain Incident: URLs

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

Select

▼ Contain Incident: File Hashes

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

Select

▼ Implement Additional Monitoring

Add Note

Back

Go to Eradication →

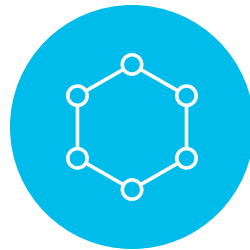
Incident response in four stages

Identify



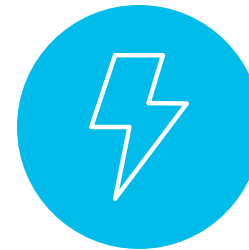
Review the incident and confirm the findings

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

▼ Identify Affected Hosts

[Add Note](#)

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

▼ Contain Incident: Overview

[Add Note](#)

Overview of how to contain Indicators of Compromise to stop the spread of ...

^ Contain Incident: Assets

[Select](#)

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

This automation workflow will network isolate/quarantine all selected assets on your integrated Endpoint Detection & Response solutions. After clicking Execute, you will be able to choose all or a subset of assets associated with this incident. Please make sure you have done proper identification before executing the workflow.

▼ Contain Incident: IPs

[Add Note](#)

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

^ Contain Incident: Domains

[Select](#)

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

This automation workflow blocks the selected domain names on your integrated network policy enforcement solutions. After clicking Execute, you will be able to choose all or a subset of domains associated with this incident. Make sure you have done proper identification before executing the workflow.

[Back](#)[Go to Eradication →](#)

Response

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.

Identification

Containment

Eradication

Recovery

+ Add Task

Custom Containment

Remove

Collapse Task

Short description

Placeholder task description.

Edit Task

Description

Placeholder task description.

Automate task

No workflow is assigned; responders can add a note to the task about the response actions that were taken.

Playbooks

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

Editor Assignment Rules

+ Create Rule

1

On

Ransomware Recovery Playbook

2

On

Score > 800

If no rules match above then the default playbook **Cisco Managed Incident Playbook** will be assigned to the incident

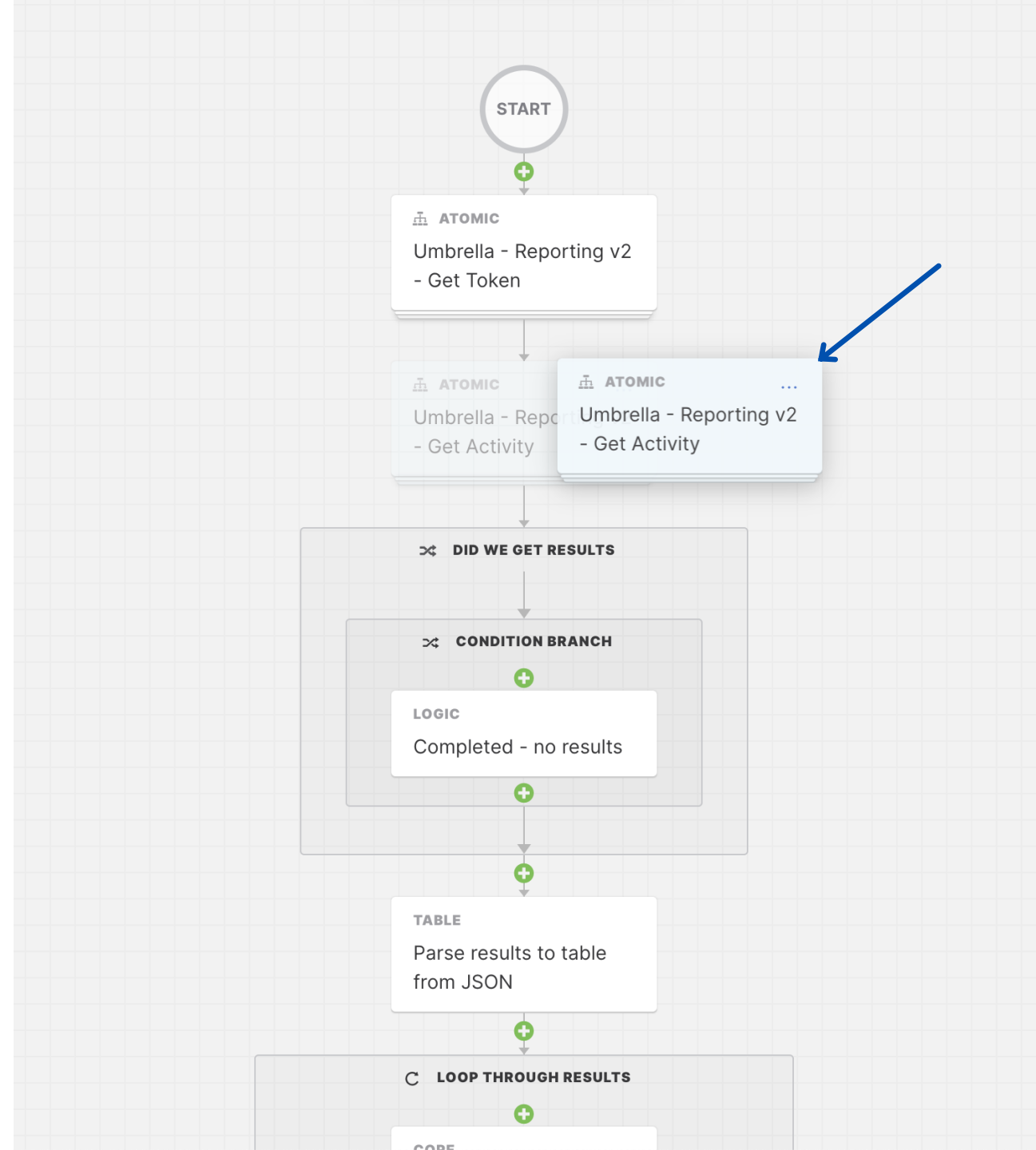
© 2024 Cisco and/or its affiliates. All rights reserved. Cisco Confidential

Response

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.

