

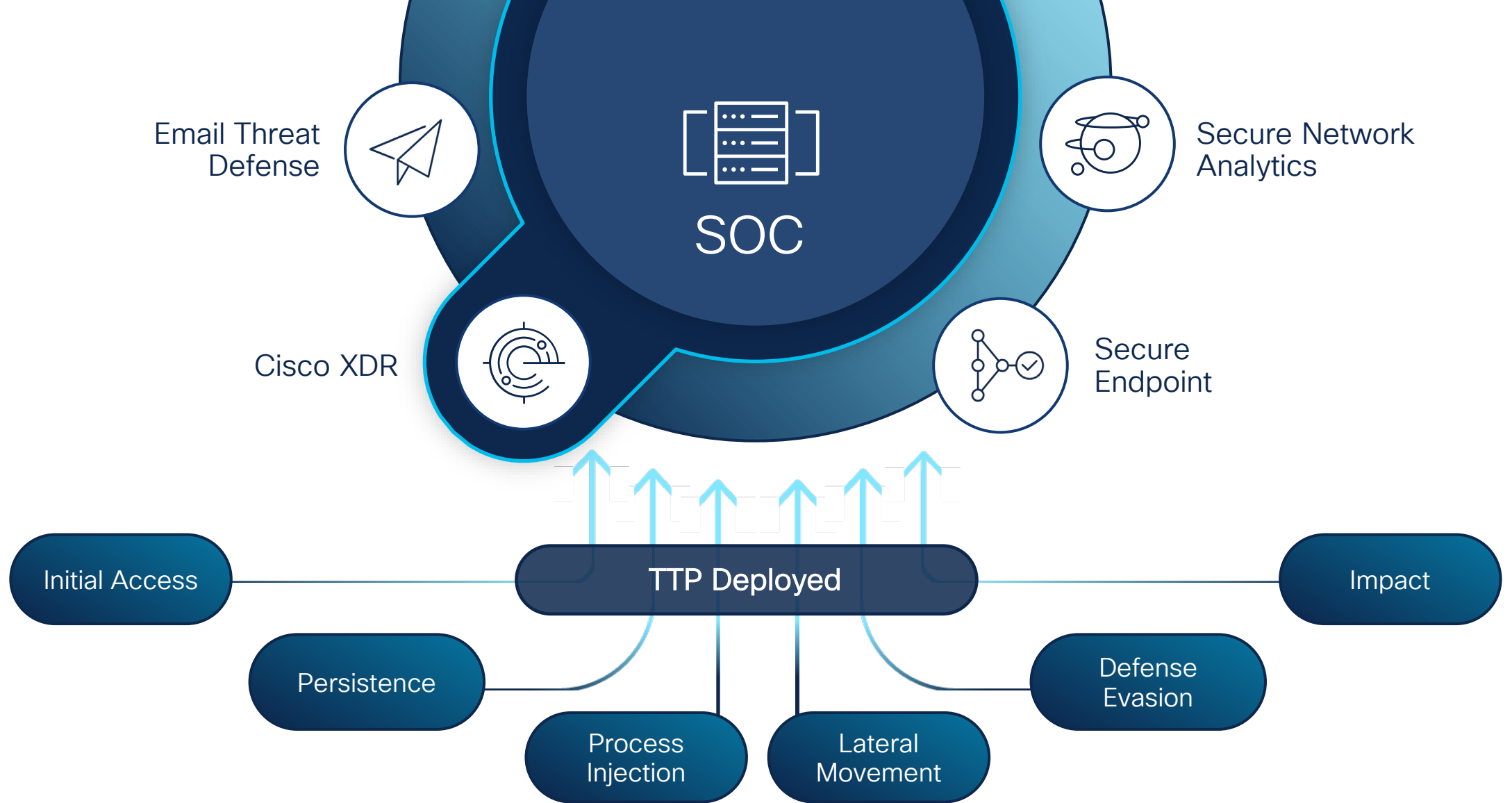
Security: Breach Protection

Tom Winburn – Security Engineer



Agenda

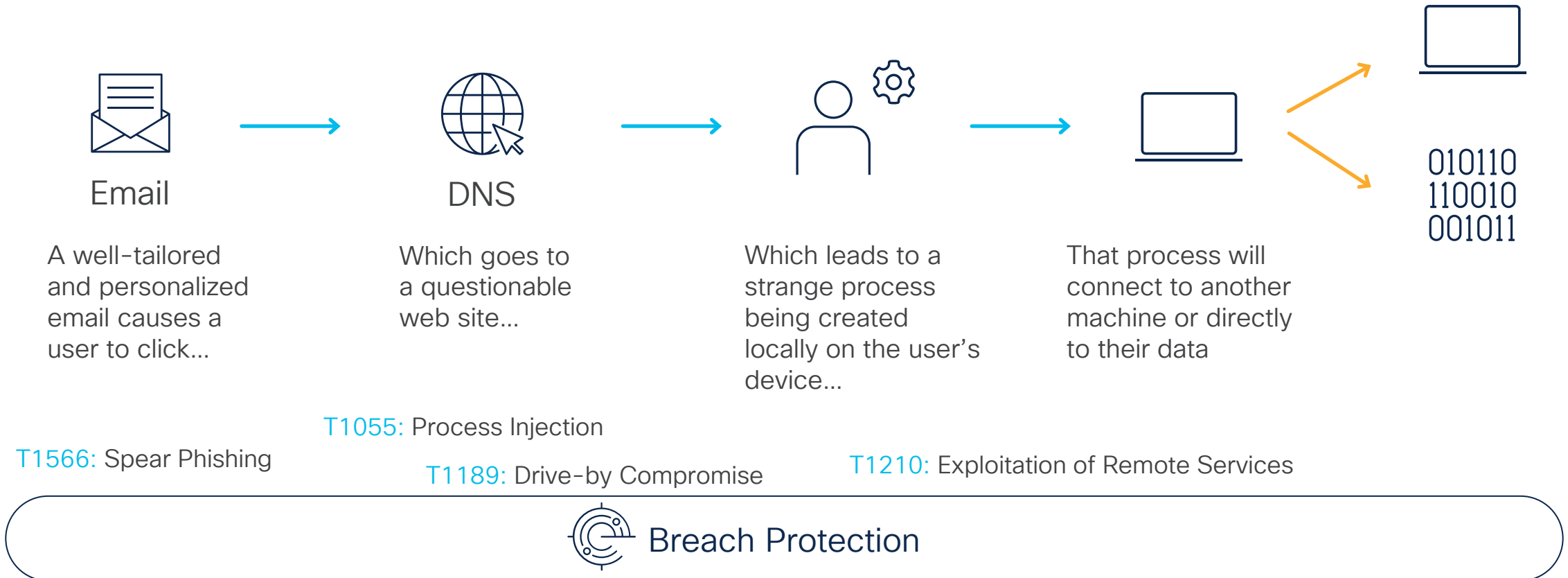
- Overview
- Extended Context
- Detections
- Response
- Resources



Organizations are struggling to detect and respond to sophisticated threats with multiple TTPs

Stop advanced threats like ransomware

Most attacks use a sequence like this...



Breach Protection 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 largest **material impacts** to our business?

3 Prioritize by Impact

Reduce Investigation Time

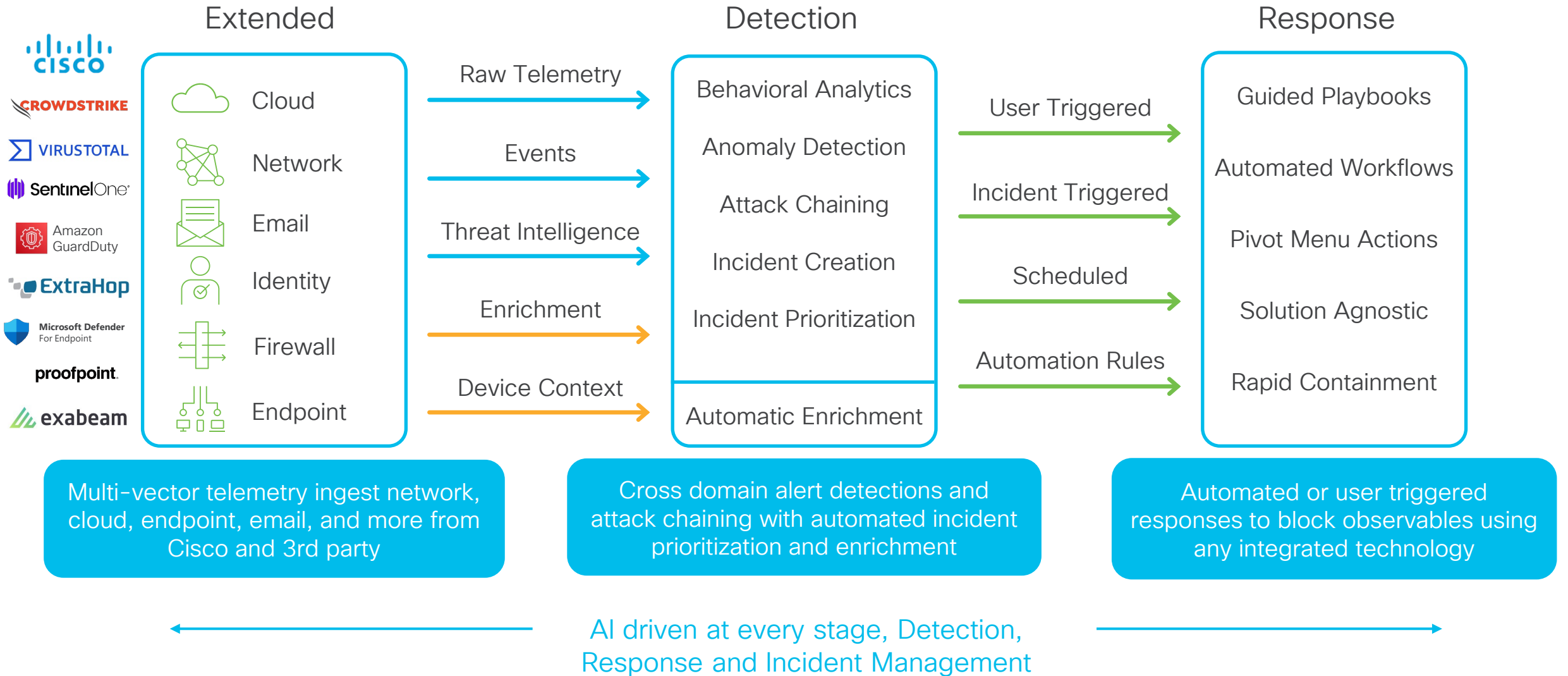
4

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

High level architecture



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.

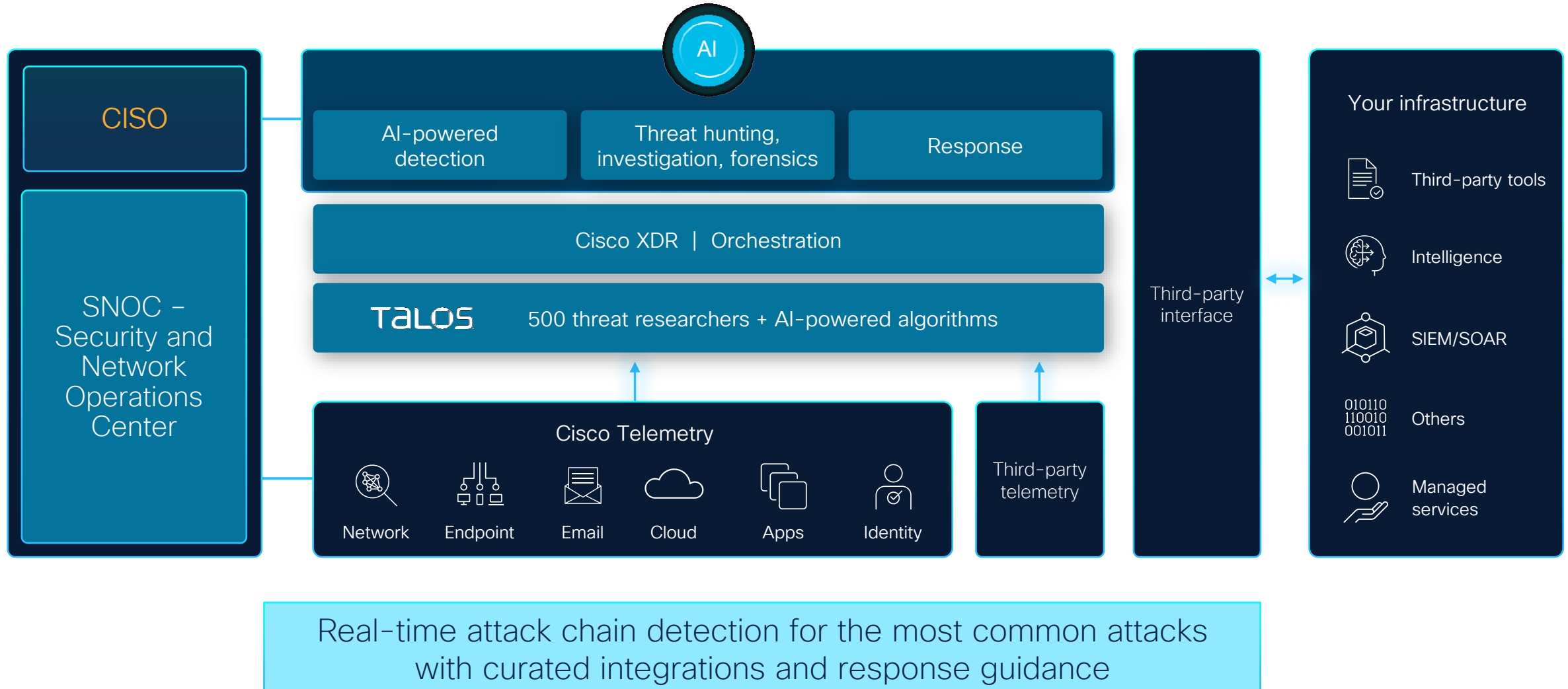


Interactive AI Assistance

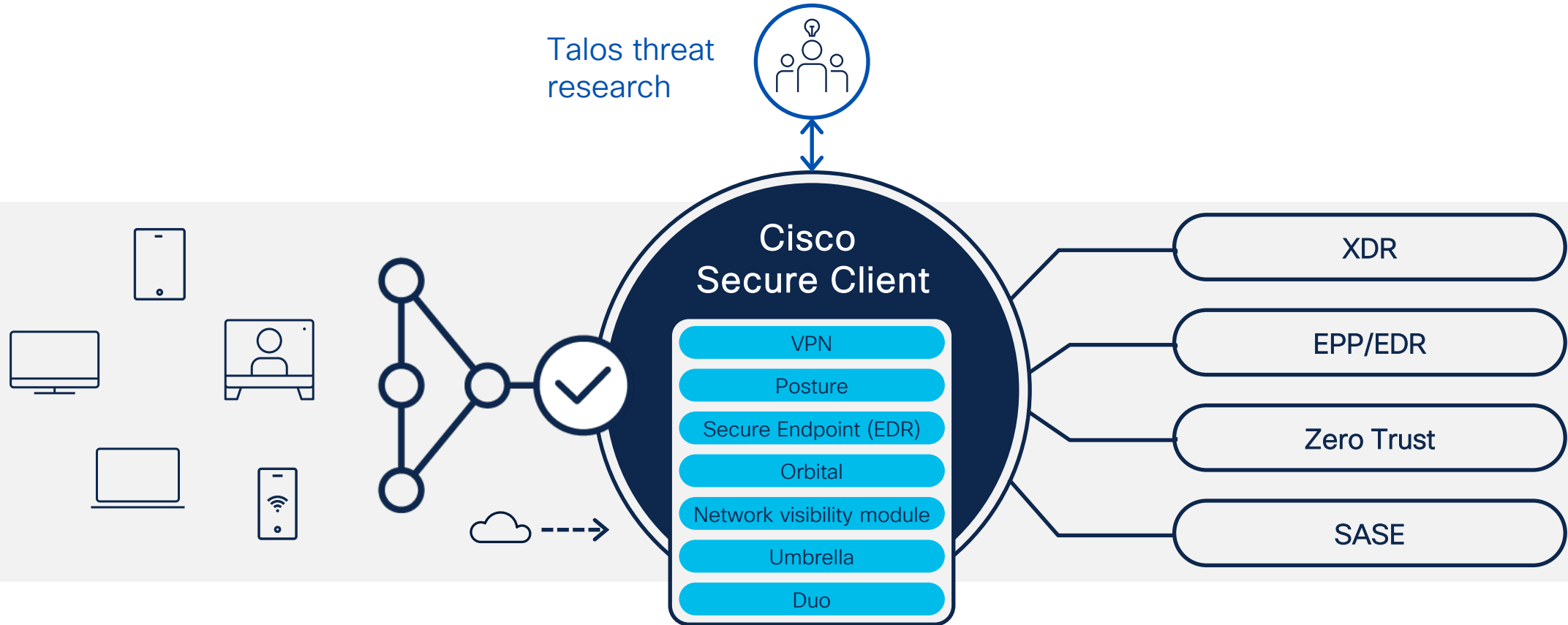
Achieve faster outcomes with interactive AI Assistant, a SOC analyst can invoke and interact with Assistant at any stage of an incident.

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

Cisco XDR: AI driven acceleration of the SNOOC

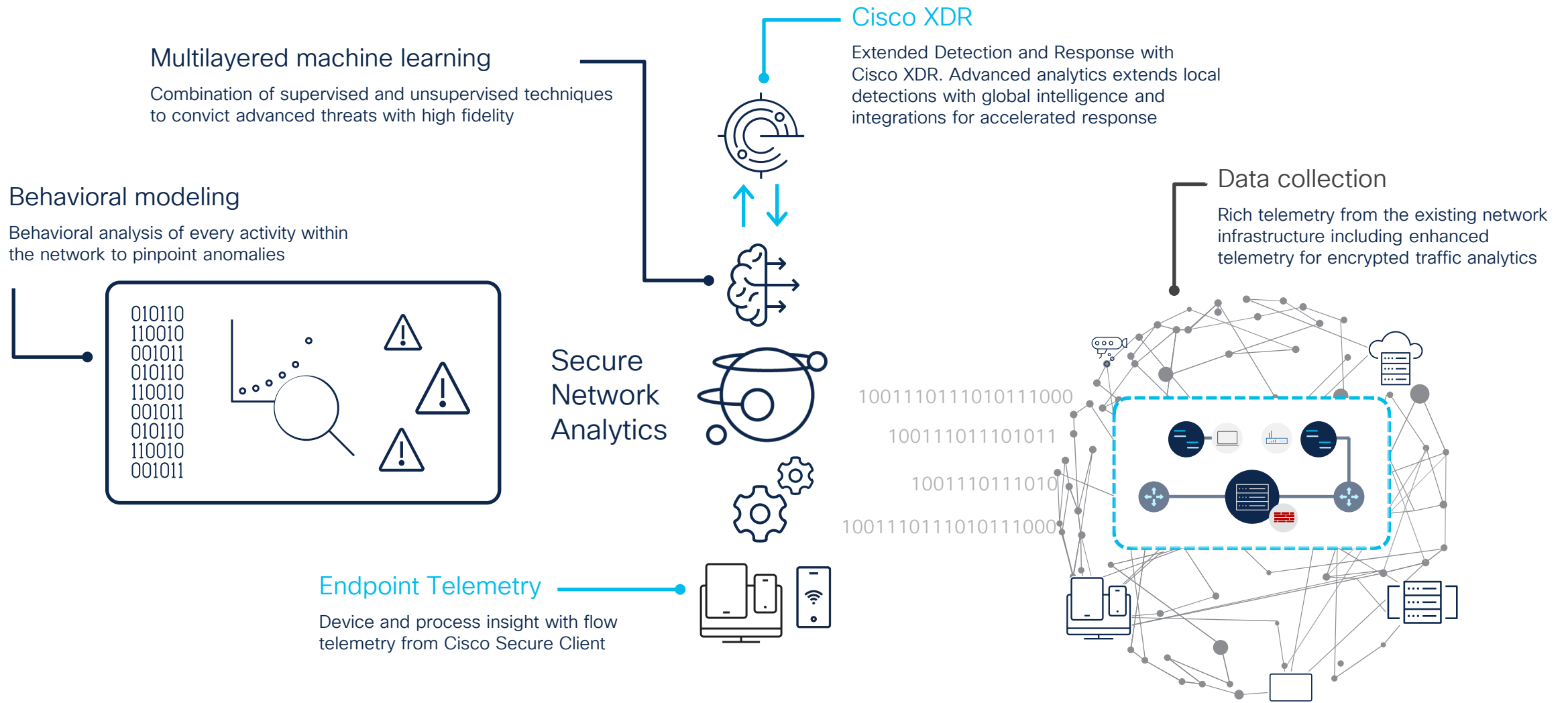


Redefined Endpoint Security



The Cisco secured endpoint is an integral component of the modern security stack

Network Analytics With Machine learning



Breach Protection

Correlated detections and automated responses

Detect

the most
sophisticated threats

Correlation of detections, threat intelligence enrichment and cross-domain telemetry to surface the most complex and multidimensional threats from skilled attackers

Act

on what truly
matters, faster

Application of advanced analytics to the collected and normalized evidence to produce correlated and prioritized detections of malicious activity

Elevate

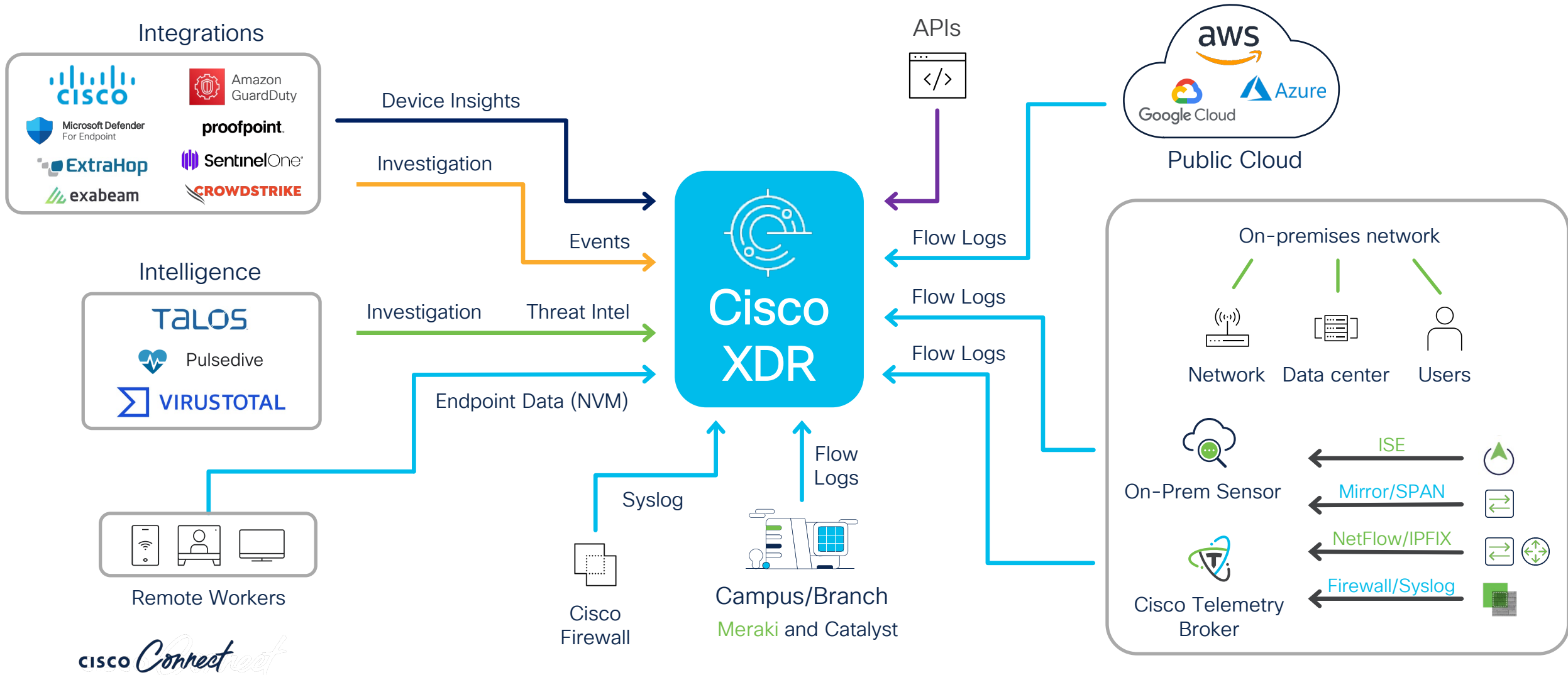
productivity with
automation

Guided responses across multiple control planes to quickly and effectively contain, mitigate, and eradicate the threat.

Extended Context

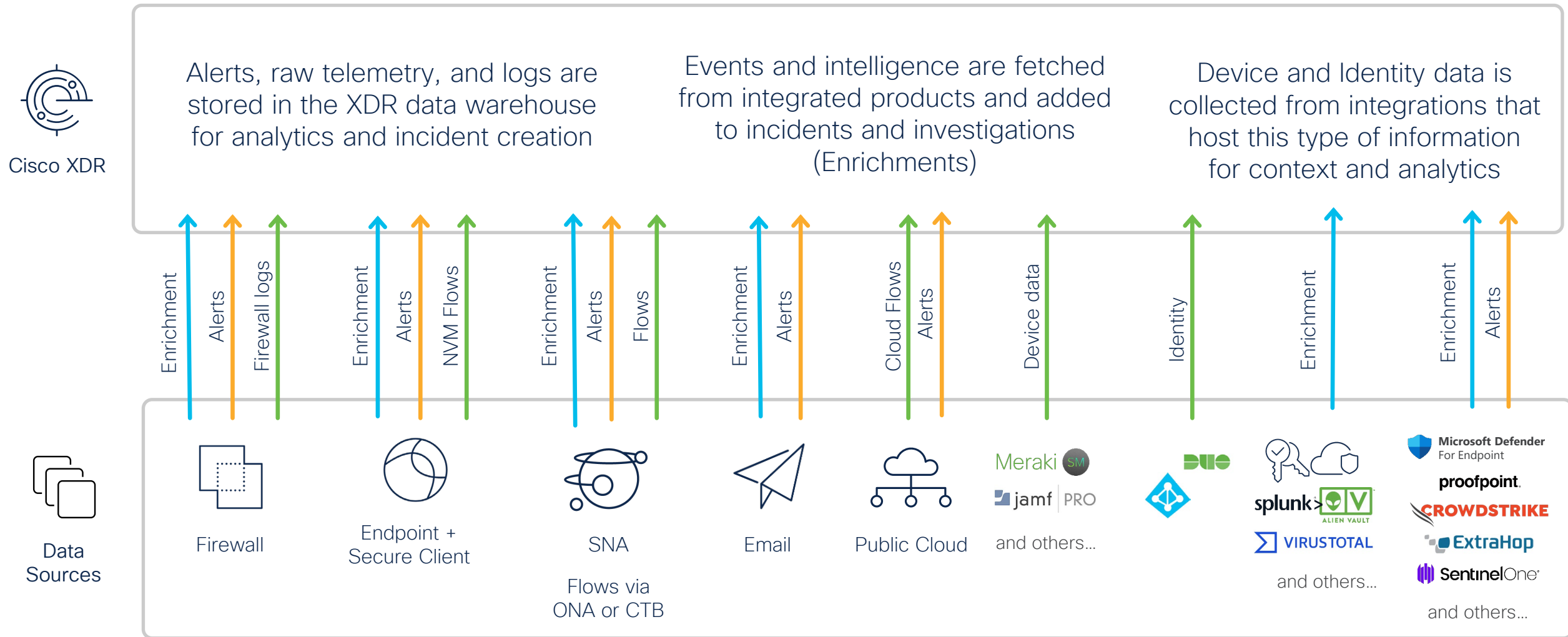
Telemetry Correlation with Cisco XDR

Flexible integration for existing infrastructure

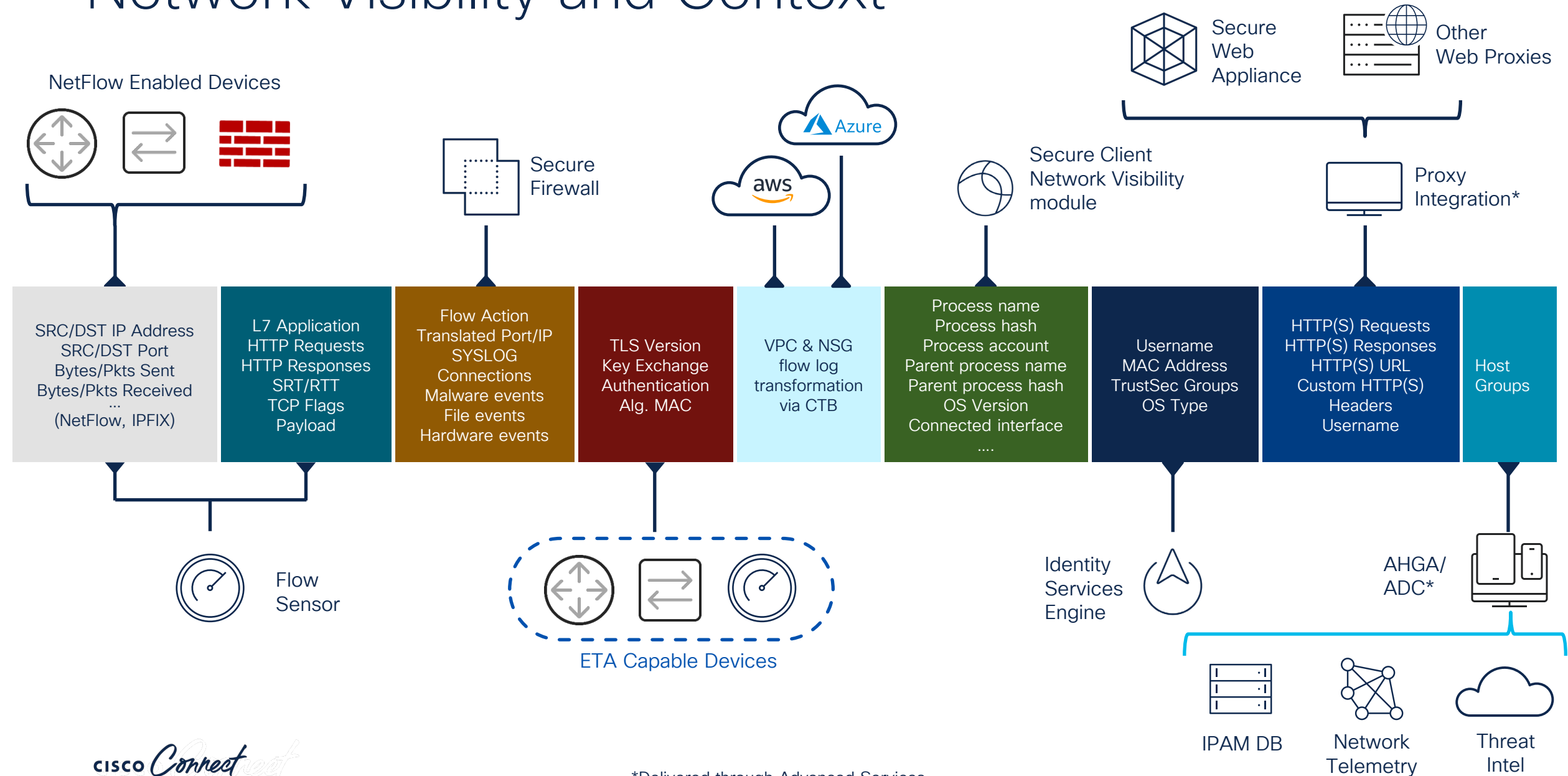


Extended context

Telemetry and enrichment



Network Visibility and Context

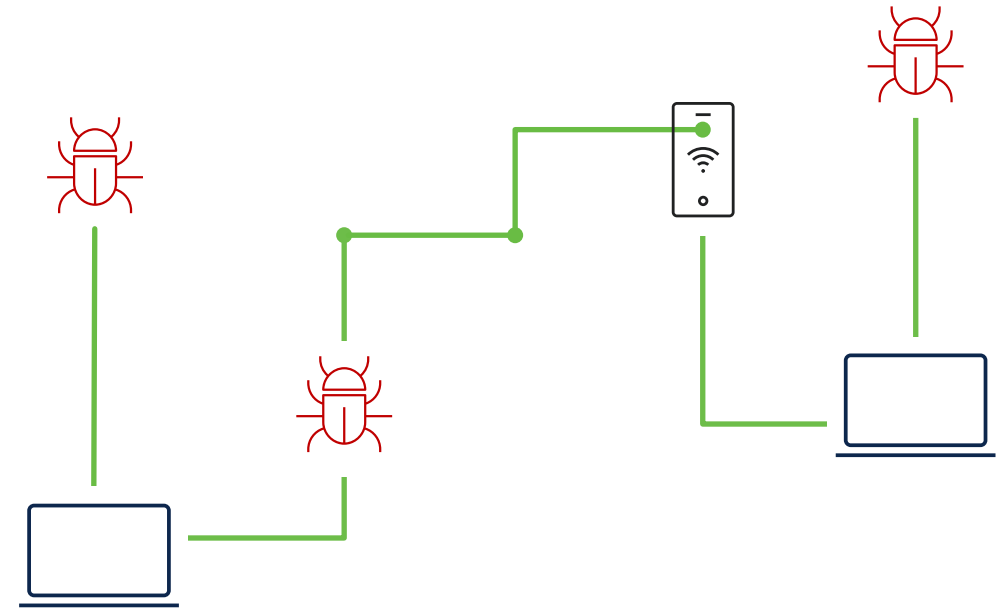


*Delivered through Advanced Services

Endpoint visibility and Context

Visibility into file activity:

- File transfer activity from one device to another
- View file execution, creations and movement actions
- Understand file execution details, parent process, arguments and commands
- View process communications to outside
- Behavior Indicators that detail attacker methods
- Real-time endpoint interrogation for confirmation, triage, and contextualization



Email contextual properties

Understand email by visualizing message, sender, and email relationships.

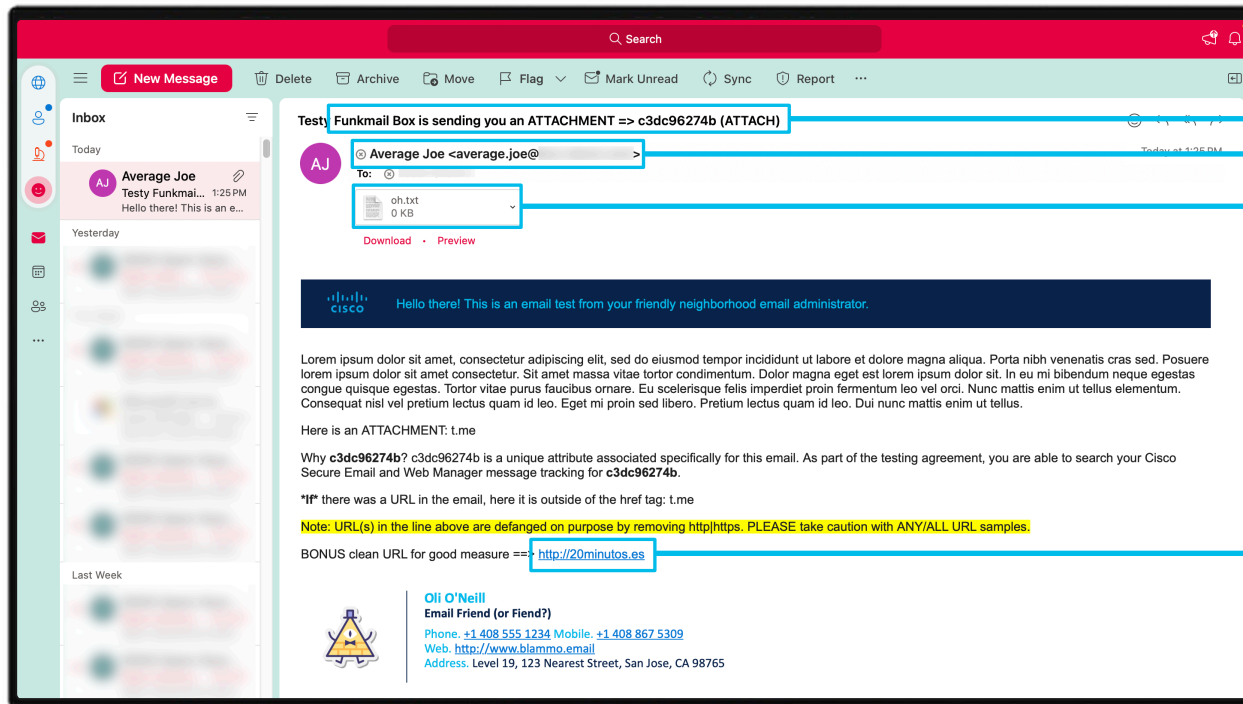
ETD and XDR uses context from email properties, such as:

- Email Subject
- Email Address(es)
- File Name/Attachment/SHA256
- URL(s)

And information from email headers:

- Sender IP
- Email Message ID

These email data points are synced into XDR as Observables.



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.

✓ XDR

- > Analytics
- > API Proxy
- ✓ Automation
 - > Instances
 - > Workflows
 - > Targets
 - > Variables
 - > Account Keys
 - > Events
 - > Tasks
 - > Webhooks
 - > Schemas
 - > Exchange

- > Events
- ✓ Investigate
 - > Enrich
 - ✓ Inspect

POST Inspect for observables

- > Private Intelligence
- > Response
- ✓ Modules
 - > Module Type
 - > Module Instance
- > Notifications
- > OAuth Clients
- > SSE
- > Users

POST Get Automation Token

POST Get Token

POST

https://visibility.{{amp_api_domain}}/iroh/iroh-inspect/in

Params Authorization Headers (8) Body Pre-request Script

none form-data x-www-form-urlencoded raw binary

```
1 {
2   ... "content": "This is a block of text with things li
3     suspicious. There may even be a file hash! 4a24
```

Body Cookies Headers (13) Test Results

Pretty Raw Preview Visualize JSON

```
1 [
2   {
3     "value": "192.168.1.1",
4     "type": "ip"
5   },
6   {
7     "value": "4a24048f81afbe9fb62e7a6a49adbd1faf41f",
8     "type": "sha256"
9   },
10  {
11    "value": "nlbmfsyplohyaicmxhum.com",
12    "type": "domain"
13  },
14  {
15    "value": "http://nlbmfsyplohyaicmxhum.com/post.",
16    "type": "url"
17  }
18 ]
```

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

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

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

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

Extended context

Enhanced detections with diverse intelligence

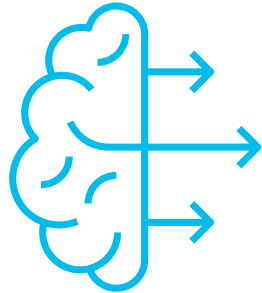
59.93.19.92 	Malicious	IP Addr...	2023-03-31T09:10:13.6... 2023-04-30T09:10:13.6...	TALOS IP B...	High
59.97.169.111 	Malicious	IP Addr...	2023-03-31T09:10:13.6... 2023-04-30T09:10:13.6...	TALOS IP B...	High
b0c57.binan... 	Malicious	Domain	2023-03-31T08:46:51.4... 2023-04-07T08:46:51....	ZeroDot1 C...	Medium

TALOS

 VIRUSTOTAL



Pulsedive



Others...

- Use public and private sources of intelligence to achieve better threat identification.
- Create and customize your own feeds based on your environment and needs.

Judgements

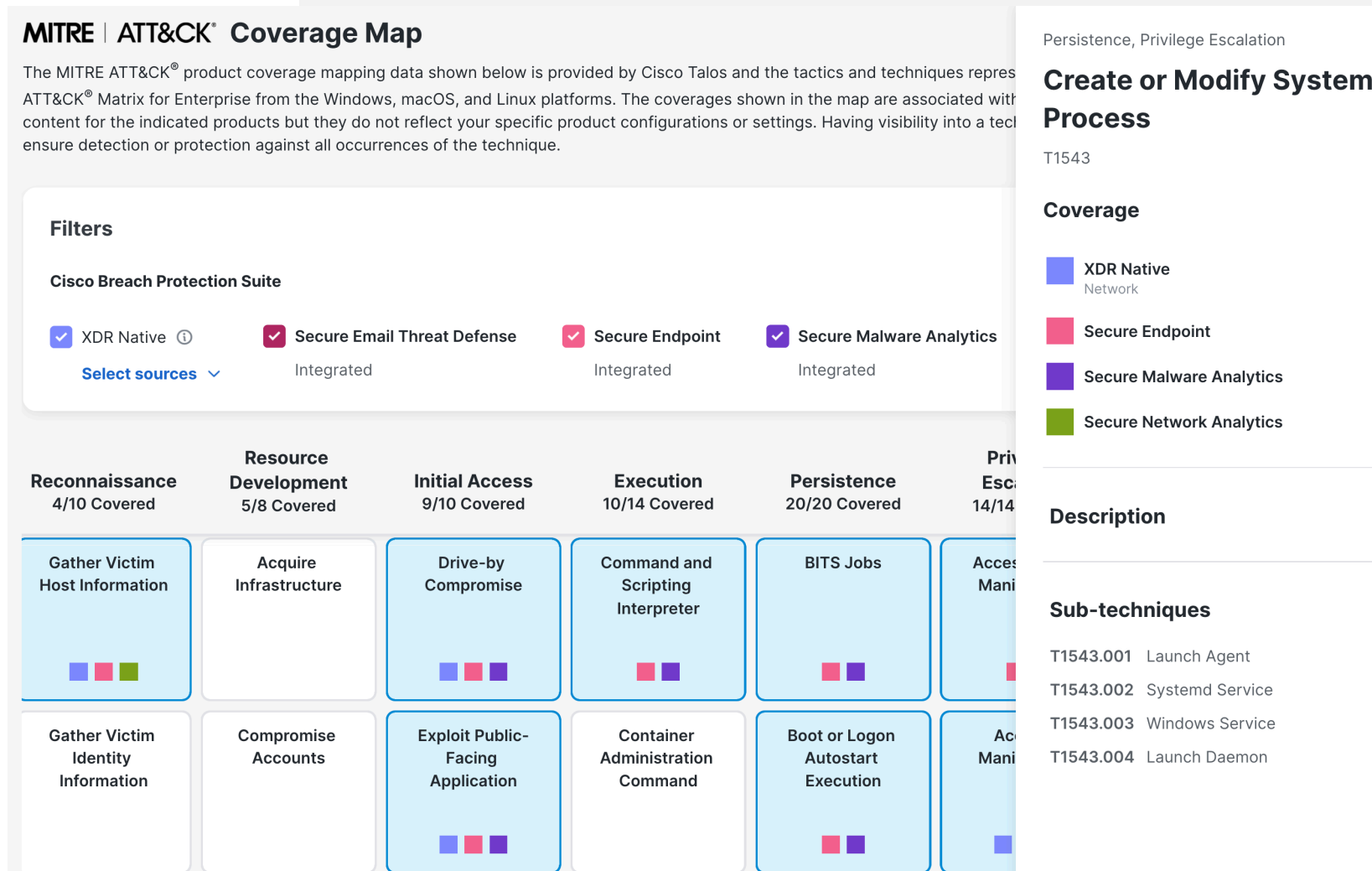
Indicators

Feeds

Events

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

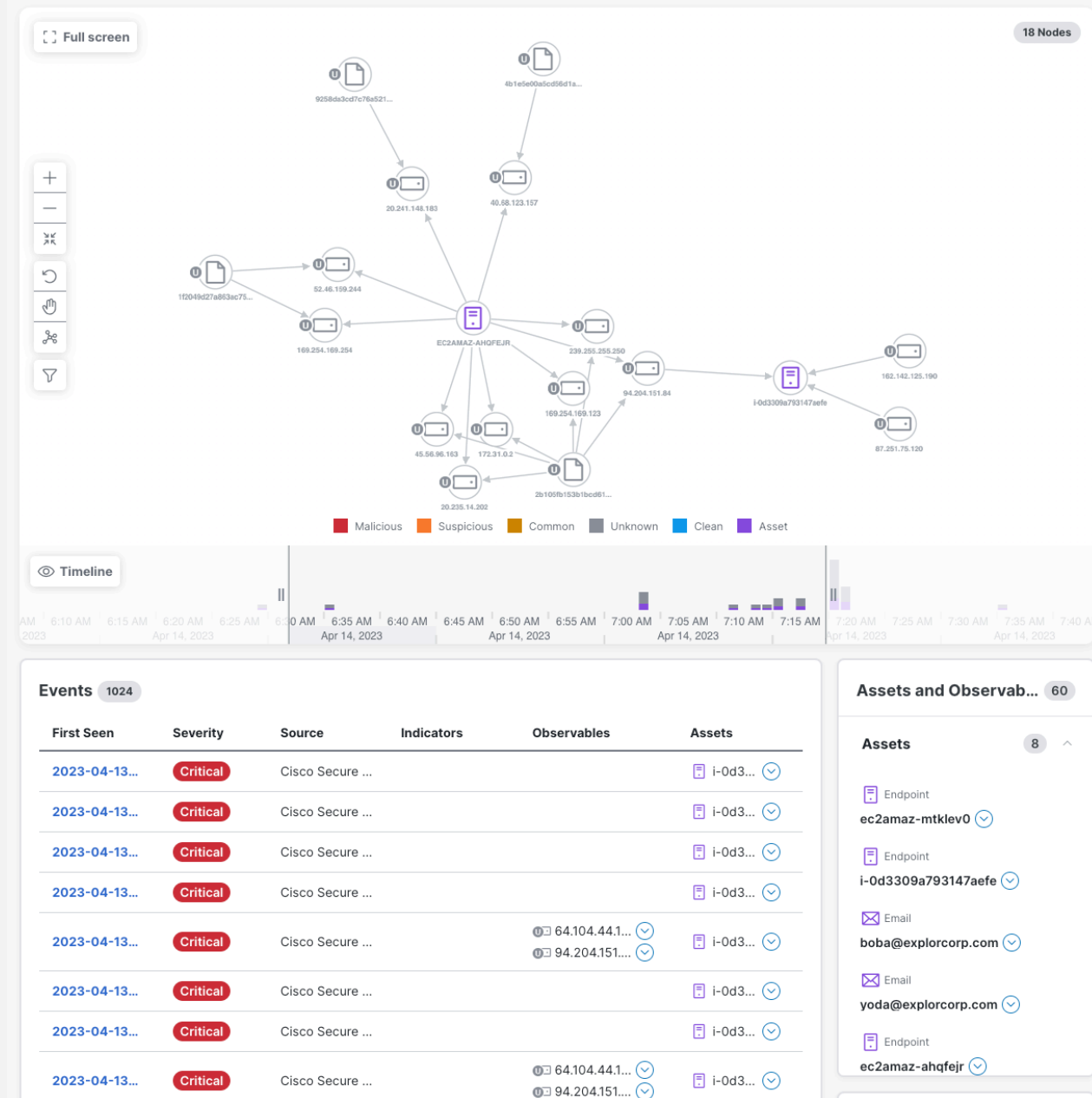


Example of investigating a previous incident

Investigate

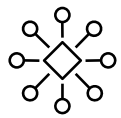
One place to investigate across all your integrated products

- Interactive visualization of observables and how they relate to each other.
- Classification of “targets” versus “assets”.
- Built-in response actions via pivot menus.
- Dynamic timeline to filter events by a date/time range.
- Color-coded observables clearly identify dispositions.
- Investigations can be saved to share or to view later.



Investigate with intelligence, context and response

Global Intelligence



Endpoint security
Malware intelligence
Internet intelligence



VirusTotal and other
third parties

Are these observables
suspicious or malicious?

Local security context



Endpoint security



Email security



Analytics

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



Cloud security



Network firewall



Secure Web
Appliance

Response actions

Block destinations

Block files

Isolate hosts

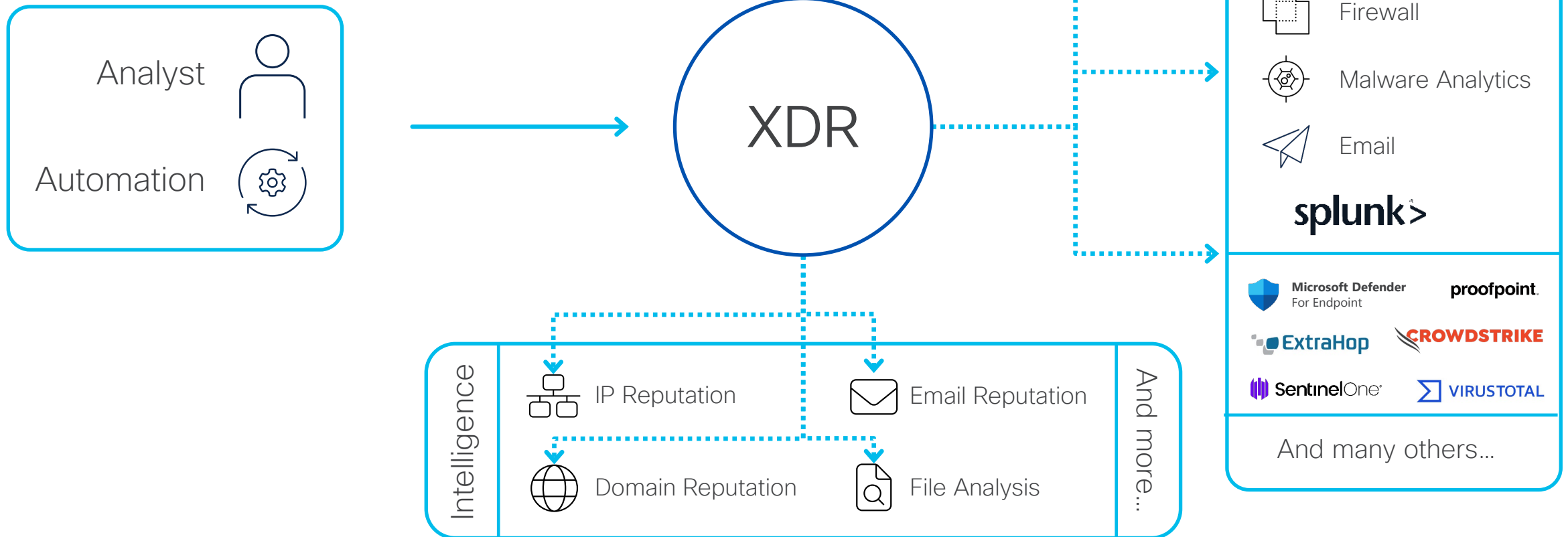
What can I do about
it right now?

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

Extended context

Enrichment and investigation

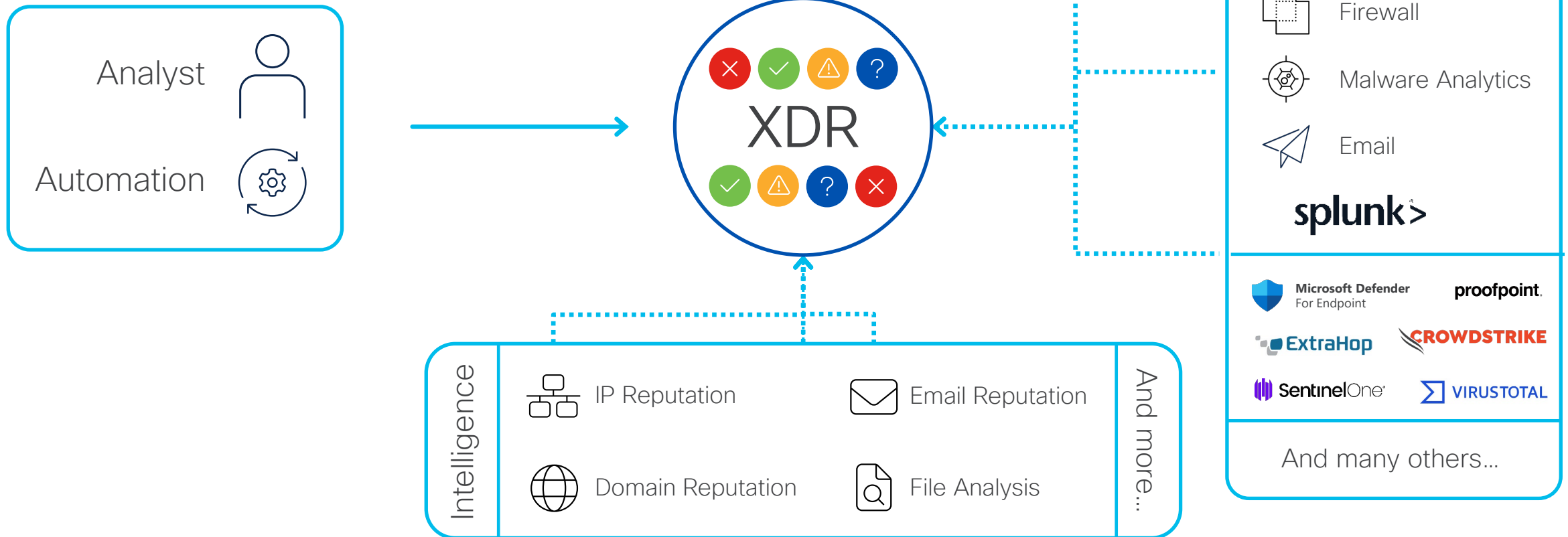
XDR leverage APIs to query data from integrated products and threat intel sources



Extended context

Enrichment and investigation

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



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 ▾

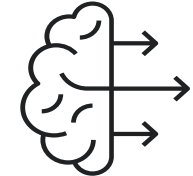
☐ Important only

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

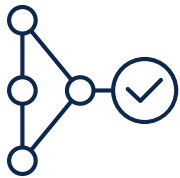
Machine Learning

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

Talos threat intel

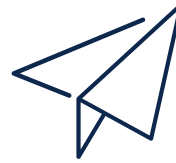
- Malware classification
- Knowledge and correlation of global campaigns to local threats
- Threatening IP, URL, and domain communication detections

XDR Analytics detections from event telemetry



Endpoint Detections

- Command and Control
- Credential Access
- Defense evasion
- Discovery and Execution
- Lateral Movement
- Persistence and Privilege Escalation



Email Detections

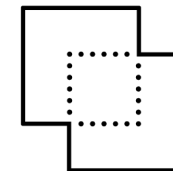
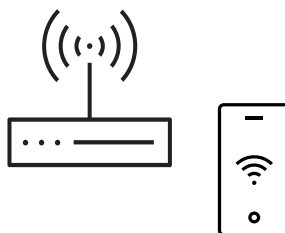
- Initial Access
- Phishing & Spear Phishing
- Scam Emails
- Malware in Attachments
- Business Email Compromise



Network Detections

- Lateral Movement
- Data Exfiltration
- Data Movement
- Network Discovery
- Behavioral Traffic Change

Comprehensive protection through detections



Public Cloud Detections

- 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...

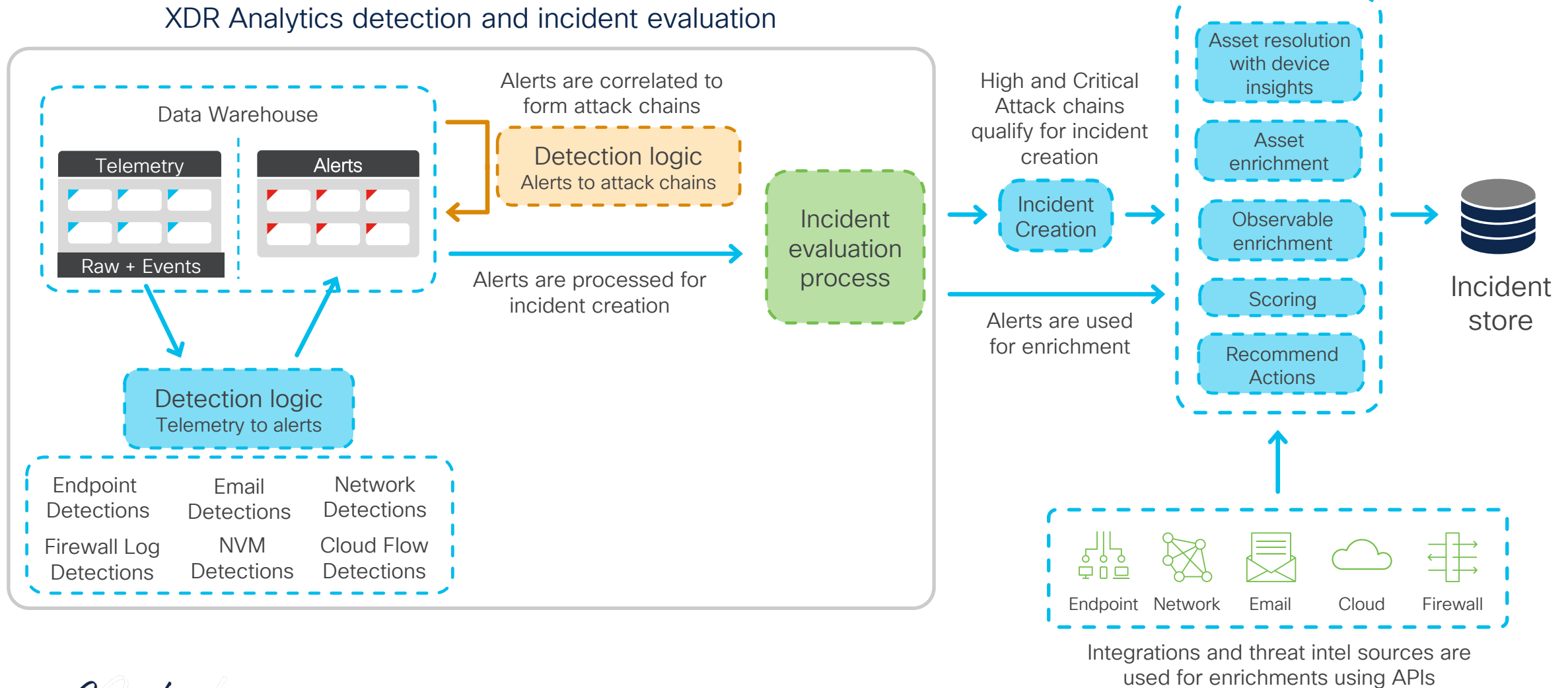
Network and Endpoint Detections

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

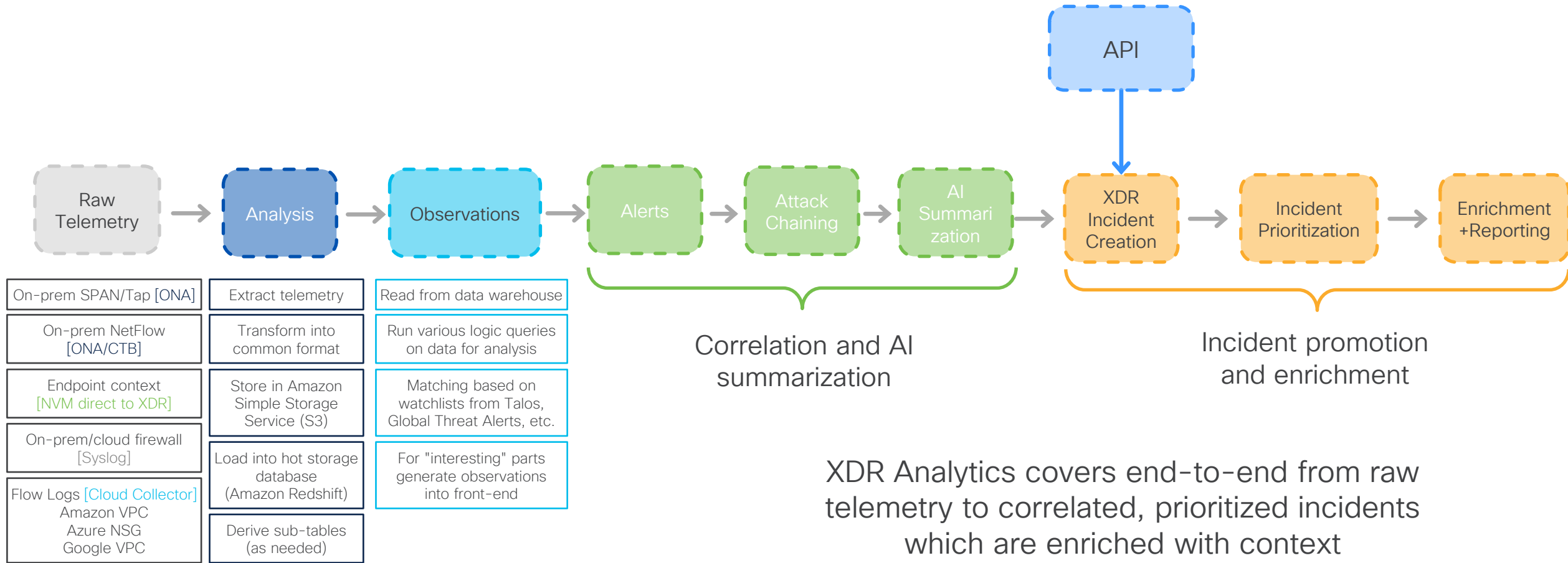
Firewall Analytics

- 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-premises detections

Detection architecture



XDR Analytics detection and incident creation path



Correlation with attack chaining

- Alerts from XDR and integrated products are correlated prior to becoming XDR incidents.
- Alerts with common indicators are combined into attack chains.
- New alerts are also appended to incidents as they occur over time.
- Analysts can also link incidents together for manual correlation.
- Attack chain are summarized with Gen AI

Attach Chain source of incidents

← Incidents

1000

Incident Reported ▾

Escalating Intrusion Clusters via Endpoint Exploits and Process Mis

Reported by [Cisco XDR Analytics \(cisco-explorcorp-earth\)](#) on 2024-05-07T20:53:37.498Z

[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 i... [more](#)

[Overview](#)

[Detection](#)

[Response](#)

[Worklog](#)

[Report](#)

Expand

+

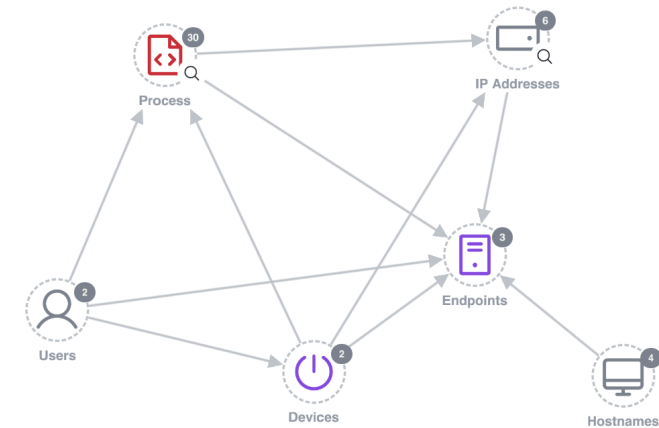
−

⌕

↺

⌕

⌕



6 Assets

[View all](#)

TOP ACTIVE

Device
obsidian-WIN10
OS Version Issue

129 events

Device
breach-AD2019.explorcorp.com
OS Version Issue

39 events

134 Observables

[View all](#)

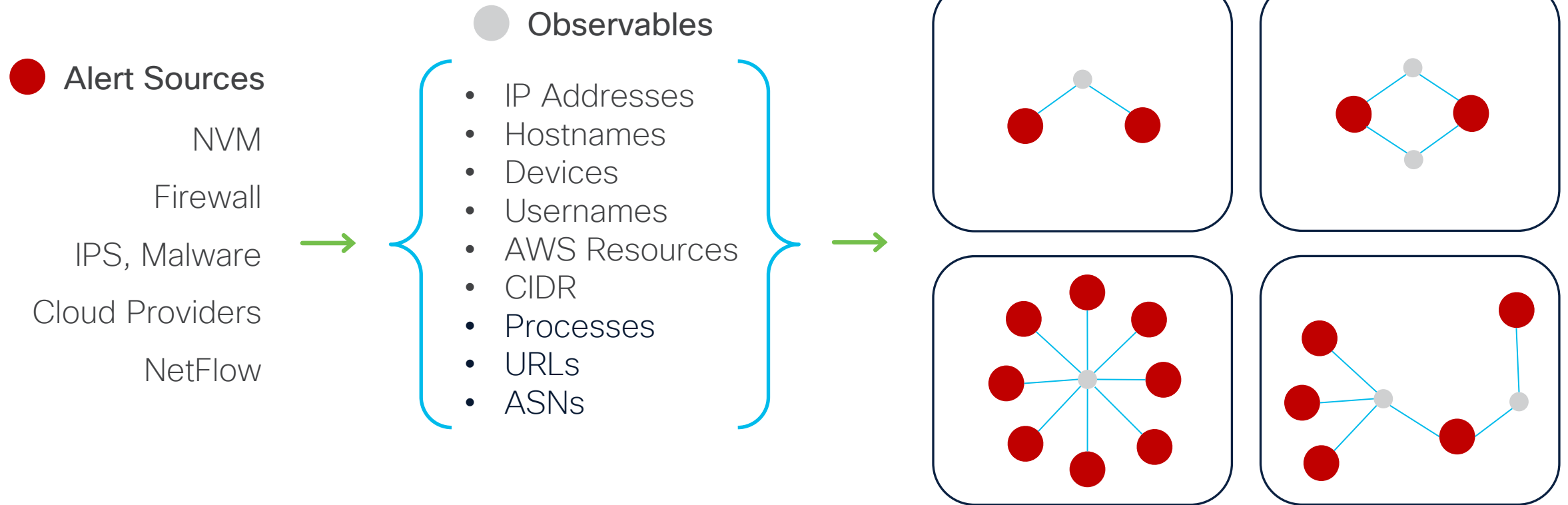
TOP ACTIVE

Malicious SHA-256
e415af393d9182435cc088e211babb40dae11bfbdd... 102 events

Unknown File Name
DefenderUpgradeExec.exe 98 events

Unknown File Path
\\?C:\Users\obsidian\AppData\Local\Temp\Defender... 98 events

Chaining attacks based on common observables

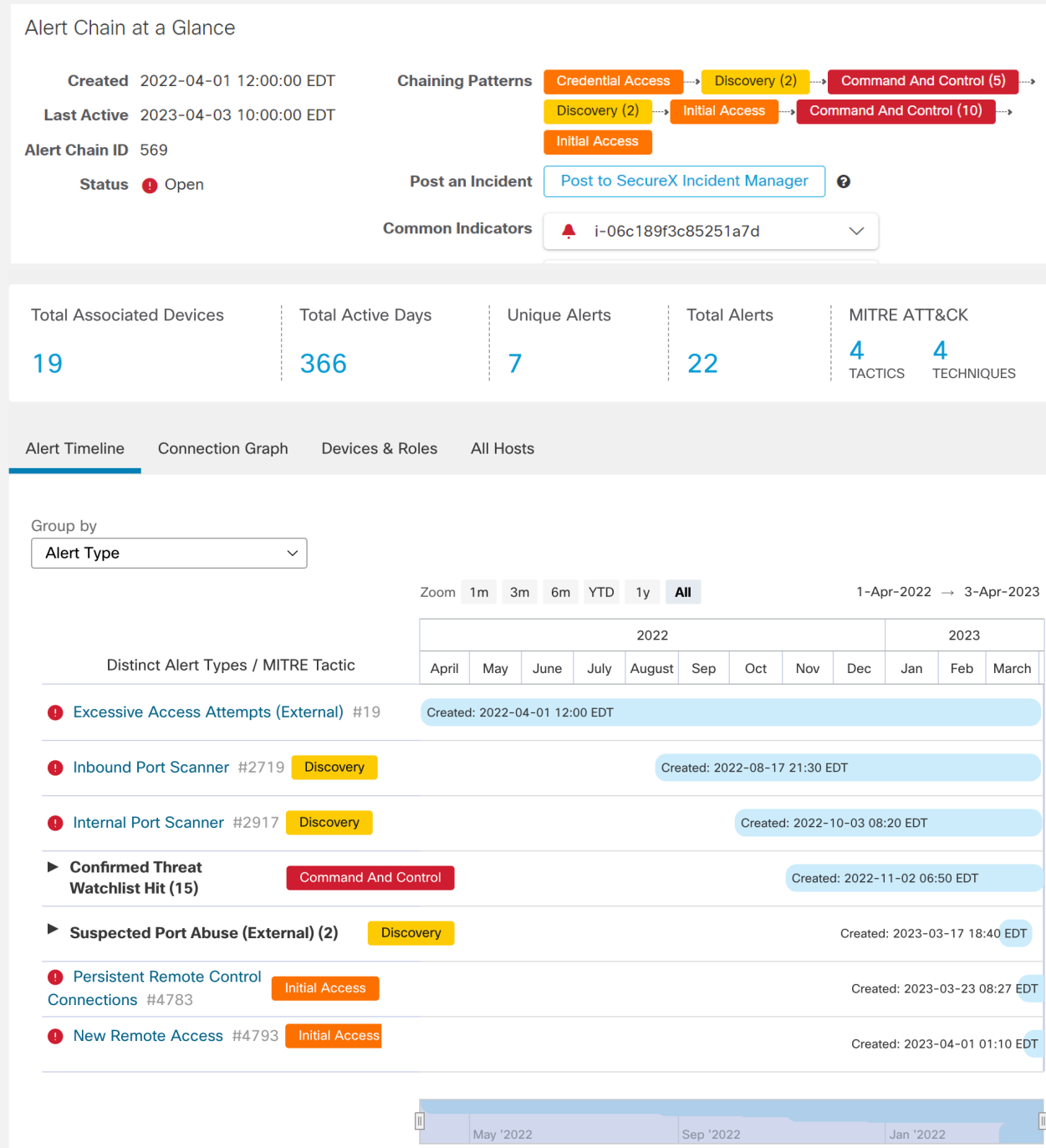


Leverage common observables to relate alerts coming from multiple sources and with different threat vectors in one attack chain.

Attack chains

Attack Chains correlate related alerts based on common indicators to show the entire attack

- Mapped to the MITRE ATT&CK framework.
- Chains are summarized with AI for better and simplified Incident comprehension.
- Alerts are correlated over time, revealing the bigger picture of a multi-stage attack.
- Alert activity is plotted on a timeline.
- Visualization is provided by the alert connection graph.



Incident creation

- Incidents are created from:
 - XDR Analytics alerts and security events correlated into attack chains
 - Manual event promotion from within XDR Analytics
 - API calls to XDR
- New incidents are assigned a priority score and are automatically enriched if their risk score is above 500
- Events discovered in enrichments that are relevant to an incident are added to that incident

Escalating Intrusion Clusters via Endpoint...

Priority 1000

Status Incident Report...

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

OS Version Issue

129 events

10 Device

breach-AD2019.explorcorp.com

39 events

View Incident Detail

Created

XDR Analytics (cisc...)

11 Hours

XDR Analytics (cisc...)

12 Hours

XDR Analytics (cisc...)

15 Hours

XDR Analytics (cisc...)

16 Hours

XDR Analytics (cisc...)

16 Hours

XDR Analytics (cisc...)

16 Hours

XDR Analytics (cisc...)

17 Hours

XDR Analytics (cisc...)

17 Hours

XDR Analytics (cisc...)

17 Hours

XDR Analytics (cisc...)

17 Hours

XDR Analytics (cisc...)

18 Hours

XDR Analytics (cisc...)

19 Hours

XDR Analytics (cisc...)

21 Hours

XDR Analytics (cisc...)

1 Day

XDR Analytics (cisc...)

1 Day

XDR Analytics (cisc...)

2 Days

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 Incidents

🕒 Last year ▾

≡ Filters

Assignment: Assigned To Me ×

<input type="checkbox"/> ▾	Priority	Name
<input type="checkbox"/>	1000	Progressive Security Breach on win10-sundee
<input type="checkbox"/>	1000	Attack Chain 7287
<input type="checkbox"/>	1000	Escalating Intrusion Clusters via Endpoint Expl
<input type="checkbox"/>	1000	Role Violation and Unusual External Server Inci
<input type="checkbox"/>	1000	Suspicious Endpoint Findings in Successive Al
<input type="checkbox"/>	1000	Unusual Behaviors Detected on EC2 Endpoint
<input type="checkbox"/>	1000	Progressive Endpoint Intrusion Revealed by Ale
<input type="checkbox"/>	1000	Suspicious Endpoint Findings: Credential Acce
<input type="checkbox"/>	1000	AWS Compromise: Root-Level Breach and Rem
<input type="checkbox"/>	1000	Concealment and Redirection Attempts Detect
<input type="checkbox"/>	1000	Chain of Alerts Triggered by Suspicious Email F
<input type="checkbox"/>	1000	Mitigation Tactic Alerts Identified on Endpoint I
<input type="checkbox"/>	1000	Multiple Security Breaches Detected at Acme E
<input type="checkbox"/>	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	10
Detection Risk	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

Incident enrichment provides incident context

← Incidents

1000 Incident Reported ▾ Escalating Intrusion Clusters via Endpoint Exploits and Process Misuse

Reported by Cisco XDR Analytics (cisco-explorcorp-earth) on 2024-05-01T18:04:17.505Z - 6 Linked Incidents

[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 i... [more](#)

Overview Detection Response Worklog Report [View Investigation](#)

Events

1 Type ⓘ Source Severity ⓘ Important only 206 matching results [Reset all](#)

Investigated x

First Seen	Severity	Source	Indicators	Observables	Assets
2024-04-15T17:45:58.018Z	None	Splunk		108.62.141.250	192.168.249.116
2024-04-05T19:17:21.000Z	Critical	Cisco XDR Analytics (cisco...)	Suspicious Endpoint Activity Suspicious Endpoint Activity +40	calculator.exe powershell.exe +6	6 obsidian-WIN10
2024-04-05T19:15:01.000Z	Critical	Cisco XDR Analytics (cisco...)	Suspicious Endpoint Activity Suspicious Endpoint Activity +40	calculator.exe powershell.exe +6	flint-win10.explorcorp.com
2024-04-05T17:36:25.000Z	Unknown	Secure Endpoint		13161dcf64451b93efb294bcf1f9453... calculator.exe +3	6 obsidian-WIN10
2024-04-05T17:36:25.000Z	Unknown	Secure Endpoint		13161dcf64451b93efb294bcf1f9453... /c:/windows/system32/dumpwebcred... +3	6 obsidian-WIN10
2024-04-05T17:30:16.000Z	Unknown	Secure Endpoint		e415af393d9182435cc088e211babb... DefenderUpgradeExec.exe +1	6 obsidian-WIN10
2024-04-05T17:30:16.000Z	Unknown	Secure Endpoint		e415af393d9182435cc088e211babb... DefenderUpgradeExec.exe +1	6 obsidian-WIN10

- XDR incidents are automatically enriched when they are created.
- Enrichment uses Cisco integrations, third-party integrations, public intelligence, private intelligence, and endpoint data to add context to incidents.
- Judgments are automatically provided to analysts to help them make more informed incident response decisions with fewer steps.

Incident AI summarization

Short description

This incident transpired from **2024-04-05 19:15:01 UTC** to **2024-04-05 21:31:03 UTC**, showed the progression of suspicious activities across multiple devices in the network, leading to potential security breaches. Alerts were grouped under distinct categories such as "Suspicious Process Path", "Suspicious Endpoint Findings by Defense Evasion", "Suspicious Endpoint Findings by Privilege Escalation", and "Potential Persistence Attempt" implying a strategic escalation of hostile activities. Multiple stages of the attack pattern consisted of the execution of suspicious processes, evasion tactics, privilege escalation, and persistent attempts to maintain network access.

Short Description

Incidents are summarized with a short description that provides a high-level overview of the attack end to end

Long Description

Long descriptions provide detailed history of the attack based on the events timeline; the attack is described in a human readable format without compromising on the details.

Simplified Alert Analysis with AI incident summarization elevating an Analyst proficiency

Long description

Initially, at **2024-04-05 19:15:01 UTC**, two alerts were generated under the "Suspicious Process Path" group from hosts **flint-win10.explorcorp.com** and **obsidian-win10.explorcorp.com**. This group was triggered due to suspicious processes executed from unusual directories and connected to an external IP address **"108.62.141.250"**.

Shortly after at **2024-04-05 20:49:37 UTC**, a single alert from host **breach-ad2019.explorcorp.com** was generated under two distinct groups — "Suspicious Endpoint Findings by Defense Evasion" and "Suspicious Endpoint Findings by Privilege Escalation". These alerts pointed to suspicious behaviors mapped to Defense Evasion and Privilege Escalation tactics of the MITRE ATT&CK framework.

Following that, two more alerts were raised at **2024-04-05 20:52:05 UTC** under the "Potential Persistence Attempt" from the same sources. These alerts were triggered due to detected persistence mechanisms such as running applications from network shares and establishing background processes used for network access.

Afterward, at **2024-04-05 21:31:03 UTC**, another set of two alerts emerged from the **flint-win10.explorcorp.com** host. They were classified under the groups of "Suspicious Endpoint Findings by Defense Evasion" and "Suspicious Endpoint Findings by Privilege

Incident details through progressive disclosure

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, such as assets, indicators, and observables, from multiple sources. Associated MITRE ATT&CK tactics and techniques are displayed and factored into the incident priority score.

AWS Compromise: Root-Level Breach and Remote...

Priority **1000** Status **Open**

Reported by [Cisco XDR Analytics \(cisco-explorcorp-earth\)](#) 21 days ago

Assigned **AS** **HJ** **RR** +1

MITRE

Priority score breakdown

1000

100	10
Detection Risk	Asset Value at Risk

Short description

This incident started on the 13th of October, 2023 at 15:12:29 UTC and ended on the 27th of February, 2024 at 00:35:44 UTC. The key concern was the repeated use of the AWS root account, coupled with frequent, uncharacteristic remote access alerts associated with several devices. AWS logging was impaired and deleted, suggesting a possible attempt at covering malicious activities. IP addresses related to the breach were flagged as suspicious, indicative of a security compromise.

This description was generated by Cisco AI.

Long description

Assets

Endpoint	1524	17 events
Endpoint	i-08bacd4bbafe3c184	10 events

[View Incident Detail](#)

MITRE ATT&CK

View all Tactics

Tactics

TA0002: Execution 100

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

TA0008: Lateral Movement 66

MITRE ATT&CK Mapping

Incidents are mapped to MITRE ATT&CK framework Tactic categories to highlight which attack stages the detections fall under, providing a quick view and link to a common language for the SOC

Expand

7 Assets [View all](#)

TOP ACTIVE

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

134 Observables

TOP ACTIVE

Malicious SHA-256	e415af393d9182435cc088e211babb40dae11bfbdd...
Unknown File Name	DefenderUpgradeExec.exe
Unknown File Path	\\?C:\Users\obsidian\AppData\Local\Temp\Defender...

Detections

Incident: Overview

Simplified graphical view

A simple yet powerful graph tool to identify observables and their relations.

Key incident details

An overview of all Incident aspects: assets involved in the incident, relevant observables with their dispositions, and related indicators, all in one view.

← Incidents

1000

Incident Reported ▾

Escalating Intrusion Clusters via Endpoint Exploits and Pro

Reported by [Cisco XDR Analytics \(cisco-explorcorp-earth\)](#) on 2024-05-01T18:04:17.505Z - [6 Linked Incidents](#)

[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 i... [more](#)

[Overview](#)

[Detection](#)

[Response](#)

[Worklog](#)

[Report](#)

↗ Expand

+

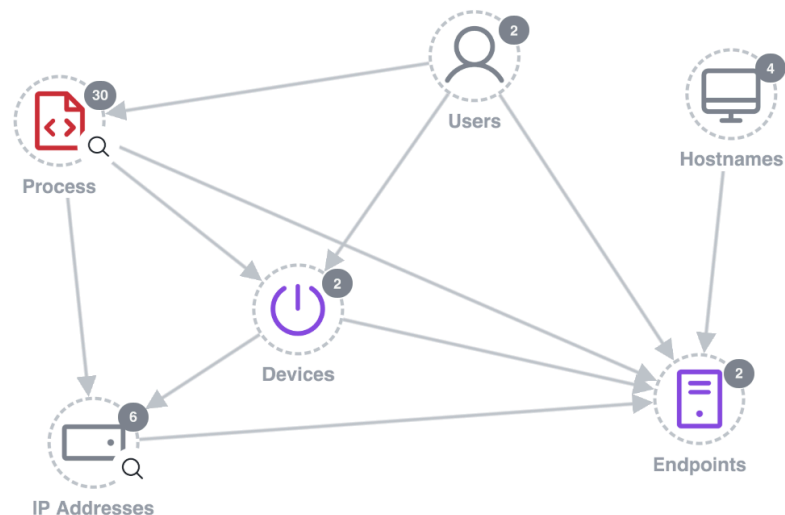
—

⌕

↺

👉

👤



7 Assets

[View all](#)

TOP ACTIVE

🔌 6 Device

obsidian-WIN10

OS Version Issue

129 events

134 Observables

[View all](#)

TOP ACTIVE

🔴 Malicious SHA-256

e415af393d9182435cc088e211babb40dae... 102 events

📄 Unknown File Name

Incident: Detection

Detailed events

Identify the events that caused an incidents along with their sources, severities, and associated observables.

Flexible filtering

Filter detections based on their type, which integrated product they came from, or their severity. Use the “Important only” toggle to see the most critical detections.

Focus on importance

An important event can a target or indicator of first encounter, has high/critical severity or contains MITRE ATT&CK data.



← Incidents

1000

Incident Reported ▾

Escalating Intrusion Clusters via Endpoint Ex

Reported by Cisco XDR Analytics (cisco-explorcorp-earth) ↗ on 2024-05-01T18:04:17.505Z - 6 Linked Incidents

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 i... [more](#)

Overview

Detection

Response

Worklog

Report

Events

Type ▾

Source ▾

Severity ▾

✓

Important only

29 ma

Important Only ×

First Seen	Severity	Source	Indicators
<div>•</div> <div>2024-04-19T23:11:00</div>	<div>Critical</div>	<div>Cisco XDR Analytic... ↗</div>	<div>LDAP Connection from Su...</div> <div>LDAP Connection from Su...</div> <div>+40</div>
<div>•</div> <div>2024-04-19T23:11:00</div>	<div>Critical</div>	<div>Cisco XDR Analytic... ↗</div>	<div>Suspicious Endpoint Activ...</div> <div>Suspicious Endpoint Activ...</div> <div>+40</div>
<div>•</div> <div>2024-04-15T17:45:58</div>	<div>None</div>	<div>Splunk</div>	
<div>•</div> <div>2024-04-11T12:23:05</div>	<div>Critical</div>	<div>Cisco XDR Analytic... ↗</div>	<div>Suspicious Endpoint Activ...</div> <div>Suspicious Endpoint Activ...</div> <div>+40</div>

Incident: Response

Built-in and custom playbooks

Contextual playbooks provide a step-by-step, guided response for incidents. Cisco provides built-in playbooks that follows the SANS PICERL incident response model. You can create and apply your own playbooks.

Powered by automation

Many actions in the playbook are powered by native XDR Automation workflows. These workflows take actions based on which products you have integrated accelerating how you respond.



← Incidents

1000 Incident Reported ▾

Escalating Intrusion Clusters via Endpoints

Reported by Cisco XDR Analytics (cisco-explorcorp-earth) on 2024-05-08T22:05:45.678Z

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 i... more

Overview Detection Response Worklog Report

Cisco Managed Incident Playbook ⓘ

Published April 10, 2024 at 6:45:51 PM

Identification

Containment

Eradication

Recovery

▾ Contain Incident: Assets

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

Execute

▾ Contain Incident: IPs

Contain IP indicators of compromise to stop the spread of malicio...

Add Note

▾ Contain Incident: Domains

Contain domain indicators of compromise to stop the spread of m...

Execute

▾ Contain Incident: URLs

Contain URL indicators of compromise to stop the spread of malic...

Execute

▾ Contain Incident: File Hashes

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

Execute

▾ Implement Additional Monitoring

Add Note

12 Items

×

Q Search

Select All

☐ 6 Device

obsidian-WIN10

129 events

OS Version Issue

☒ 10 Device

breach-AD2019.explorcorp.com

39 events

OS Version Issue

☐ Endpoint

flint-win10.explorcorp.com

39 events

☐ Endpoint

quartz-win10.explorcorp.com

6 events

☐ Unknown Hostname

breach-ad2019.explorcorp.com

6 events

☐ 10 Device

fileserver

5 events

☐ Endpoint

marble-win11.explorcorp.com

5 events

☐ Unknown Hostname

explorcorp.com

2 events

Execute

Detections

Incident: Worklog

Collaboration

View work already completed for the incident, post notes with important details, and collaborate with your team.

Auditing

See a history of actions taken, including the execution of automated response actions in the response playbook.

← Incidents

1000

Incident Reported ▾

Escalating Intrusion Clusters via Endpoint Exploits and Pr...

Unassigned

Reported by [Cisco XDR Analytics \(cisco-explorcorp-earth\)](#) on 2024-05-08T22:05:45.678Z

[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 i... [more](#)

Overview

Detection

Response

Worklog

Report

[View Investigation](#)

Notes

Audit Log

Sort by: Newest ▾

[Add Note](#)

Created by: Automation Workflow

2024-05-09T00:55:18.068Z

[RESPONSE TASK] Contain Incident: Assets

[XDR - Contain Incident: Assets](#) started by remi.i.reid@explorcorp.com failed:

Created by: Automation Workflow

2024-05-09T00:55:06.772Z

[RESPONSE TASK] Contain Incident: Assets

Workflow: [XDR - Contain Incident: Assets](#) started by remi.i.reid@explorcorp.com

Created by: Automation Workflow

2024-05-08T23:46:15.463Z

Incident Report

Downloadable Incident report

Provide a complete report of the incident including:

- **Executive Summary** : summary of the incident, when it occurred, what devices and which users were affected..
- **Incident Summary** : summarizes the incident with technical details and information on how it was handled.
- **Event Summary** : summary of all actions on each device including connection to destination, process executions and others
- **Timeline of events**: list of events by timeline on each device affected by the incident



← Incidents

1000

Incident Reported ▾

Escalating Intrusion Clusters via Endpoint Exploits and Process Mis...

Unassigned

Reported by Cisco XDR Analytics (cisco-explorcorp-earth) on 2024-05-08T22:05:45.678Z

[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 i... [more](#)

Overview

Detection

Response

Worklog

Report

View Investigation

Incident Report

▼ Executive Summary

Created by Cisco AI on May 8, 2024 at 11:49:29 PM

Edit

^ Incident Summary

Created by Cisco AI on May 8, 2024 at 11:50:34 PM

Edit

On April 5, 2024, the user **administrator** accessed the device **obsidian-WIN10** and executed the process **powershell.exe** . The device **fileserver** established connections with the IP **108.62.141.250** and the endpoint **flint-WIN10.explorcorp.com** . The device **obsidian-WIN10** was also connected to multiple endpoints including **Quartz-WIN10.explorcorp.com** , **Marble-WIN11.explorcorp.com** , and **flint-WIN10.explorcorp.com**.

The device **obsidian-WIN10** executed several processes including **pscp.exe** , **plink.exe** , **powershell.exe** , **calculator.exe** , **taskhostw.exe** , **svsystemsettings.exe** , **sihost.exe** , **sdxhelper.exe** , and **crossdeviceservice.exe** . The device **obsidian-WIN10** also connected to the IP addresses **108.62.141.250** and **108.62.141.151**.

The endpoint **flint-WIN10.explorcorp.com** was connected to multiple IP addresses including **52.109.6.4** , **23.62.165.109** , **52.113.194.132** , and **108.62.141.250** . The endpoint **flint-WIN10.explorcorp.com** was also connected to hostnames **fa000000138.resources.office.net** , **ecs.office.com** , and **mrodevicemgr.officeapps.live.com**.

The incident was promoted on May 8, 2024, by **explorcorp** and several remediation actions were taken by **Remi I. Reid** including changing the status, adding assignees, executing workflows for Document and Notify, Confirm Incident, Contain Incident: File Hashes, Identify Vulnerabilities, and Contain Incident: Assets.

The products used in the analysis of the incident were **ServiceNow** , **Cisco XDR Analytics (cisco-explorcorp-earth)** , **Secure Endpoint** , **Splunk** , and **Cisco Secure Endpoint** . The incident involved 6 devices and affected several user accounts including **granite** , **slate** , **obsidian** , **files** , **evals-team-da** , **marble** , **krbtgt** , **judy** , **flint** , **coal** , **limestone** , **bill** , **quartz** , **vendor-da** , and **tme**.

↻ Regenerate

▼ Event Summary

Edit

Robust native response options



Pivot menus

Act on an observable from various places within XDR and other Cisco Secure products



Incident playbooks

Built in Guided, four stage process for incident response, Bring your own playbook and apply it when needed



Automation

Simple or complex workflows that can investigate and respond at machine speed

▼ **Identify Affected Hosts** [Add Note](#)

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

▼ **Contain Incident: Overview** [Add Note](#)

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

▼ **Contain Incident: Assets** [Select](#)

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

▼ **Contain Incident: IPs** [Add Note](#)

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

▼ **Contain Incident: Domains** [Select](#)

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

▼ **Contain Incident: URLs** [Select](#)

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

▼ **Contain Incident: File Hashes** [Select](#)

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

▼ **Implement Additional Monitoring** [Add Note](#)

[Back](#) [Go to Eradication →](#)

Response

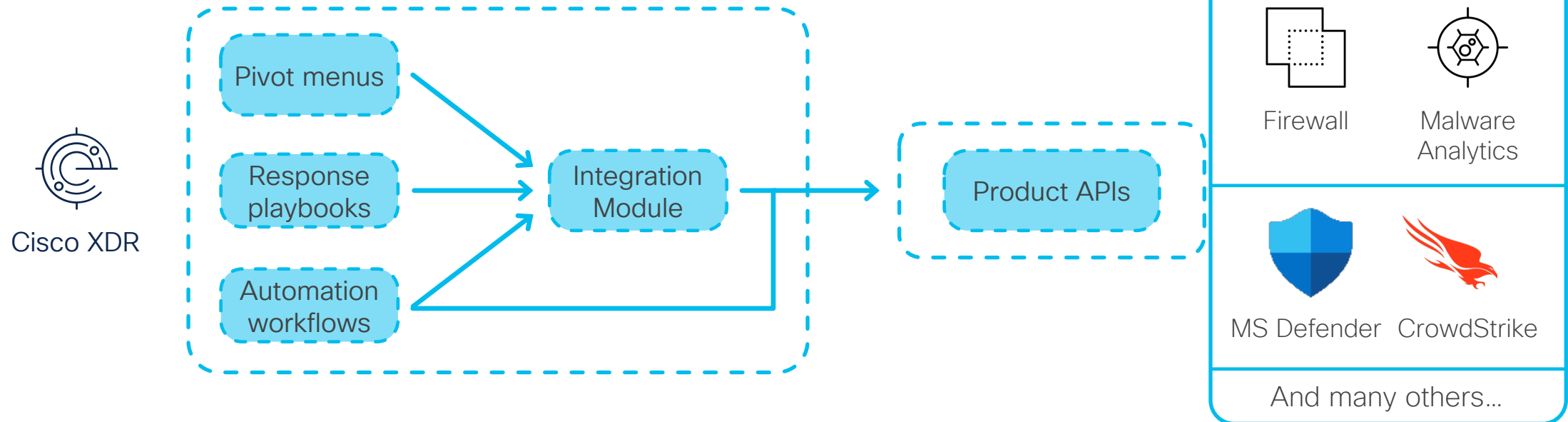
Architecture

Wide variety of actions

Isolate hosts, block IPs on firewalls, block hostnames in DNS, quarantine messages in a mailbox, and more...

Dynamic Response

Response actions can be automated or user-initiated



Pivot menu

Can be triggered for observables from various parts of XDR, including within investigations and incidents. Allow you to take actions such as:

- Creating a judgement
- Adding the observable to a case
- Linking out to other products to view additional information
- Taking a response action via an integrated product
- List of contextual response workflows which can be immediately executed by the user using XDR Automation

Orientation



1 Asset

 10.150.0.2**IP Address**  10.150.0.2

Secure Endpoint - ExplorCorp

[Search for this IP](#)

Secure Network Analytics - ExplorCorp 741

[Host Report](#)

Secure Network Analytics - ExplorCorp 742

[Host Report](#)

XDR Automation

 Submit URL to Secure Malware Analytics Duo - Block User Meraki - MX - L3 Outbound Firewall Block

1 Observable

 170.210.208

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.

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.

Edit Task

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

Incident response in four stages

Identify



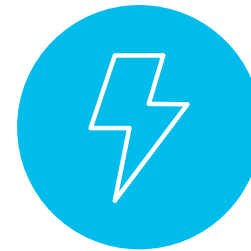
Review the incident and confirm the findings

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

Automation rules

Allow various types of events to cause workflows to run.

- **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 new 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 URL.

Triggers

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

Automation Rules

Events

Webhooks

Calendars

Schedules

Search

Q Search



Type

Select



[Reset All](#)

Display name

On/off

Type

Owner

Hourly Workflow



Schedule

user@cisco.com

Incoming Webhook



Webhook

user@cisco.com

Incident Notification



Incident

user@cisco.com

Response

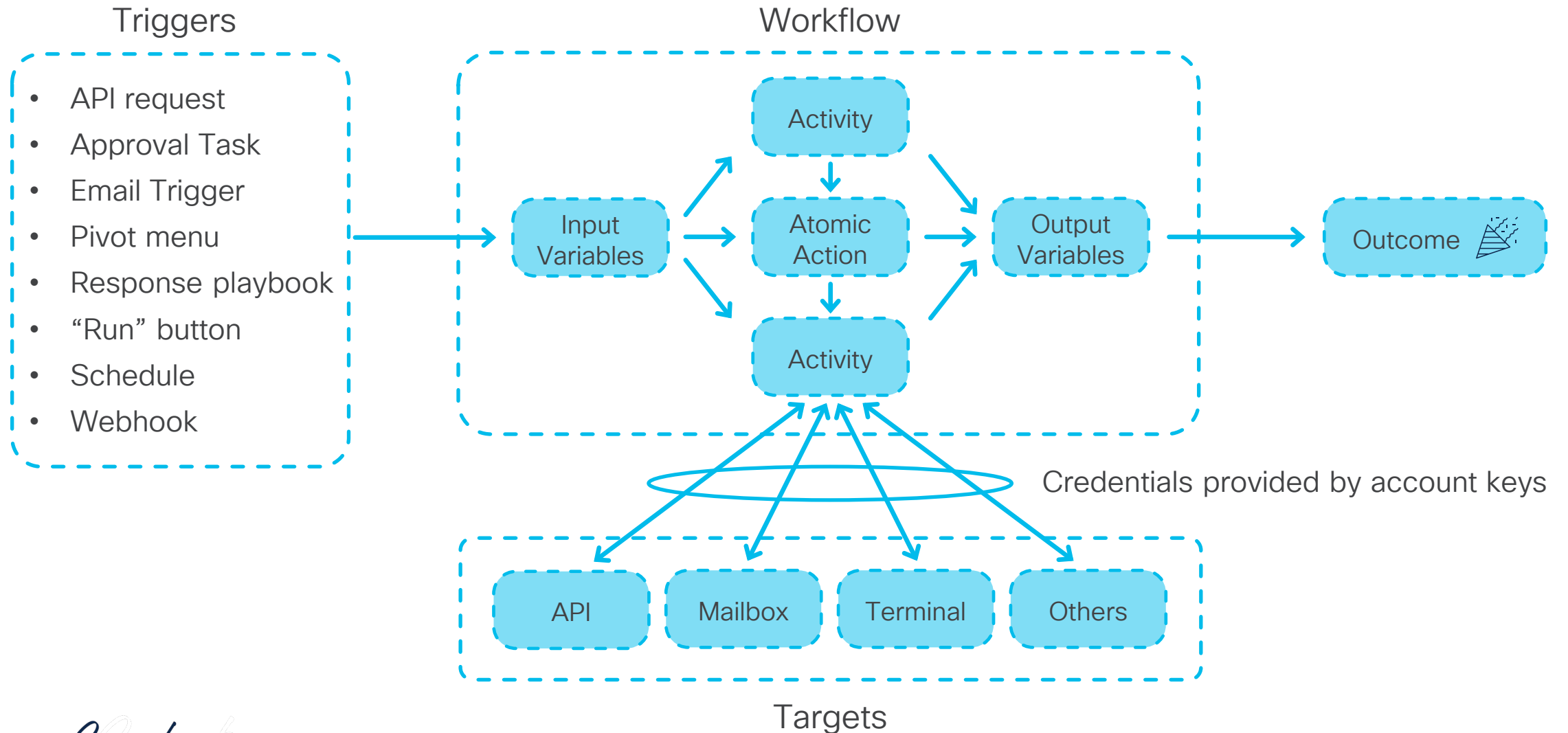
XDR Automation

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.



Workflow diagram



Response

Ransomware Recovery

Achieve automated ransomware recovery leveraging XDR automation, rule-based triggering and Cohesity integration.

- Restore a device to its previous known good state before infection.
- Automate snapshot taking and recovery for devices to their known good state.
- Reduce downtimes and time for recovery with end-to-end automation

[← Incidents](#)


1000

Open ▾

Escalating Intrusion Clusters via Endpoint Exploits and Process M

Reported by [Cisco XDR Analytics \(cisco-explorcorp-earth\)](#) [↗](#) on 2024-04-09T20:09:19.858Z - [5 Linked Incidents](#)

[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 i... [more](#)

[Overview](#) [Detection](#) [Response](#) [Worklog](#) [Report](#)

[Notes](#) [Audit Log](#)

Created by: Automation Workflow

2024-04-09T20:09:28.743Z

[AUTOMATION RULE]

[Cohesity - Identify Restore Point for Affected Virtual Machines](#) [↗](#) started by [Score greater than 800](#) [↗](#)

Introducing Cisco XDR 2.0

Clear verdict. Decisive action. AI speed.

Instant Attack Verification

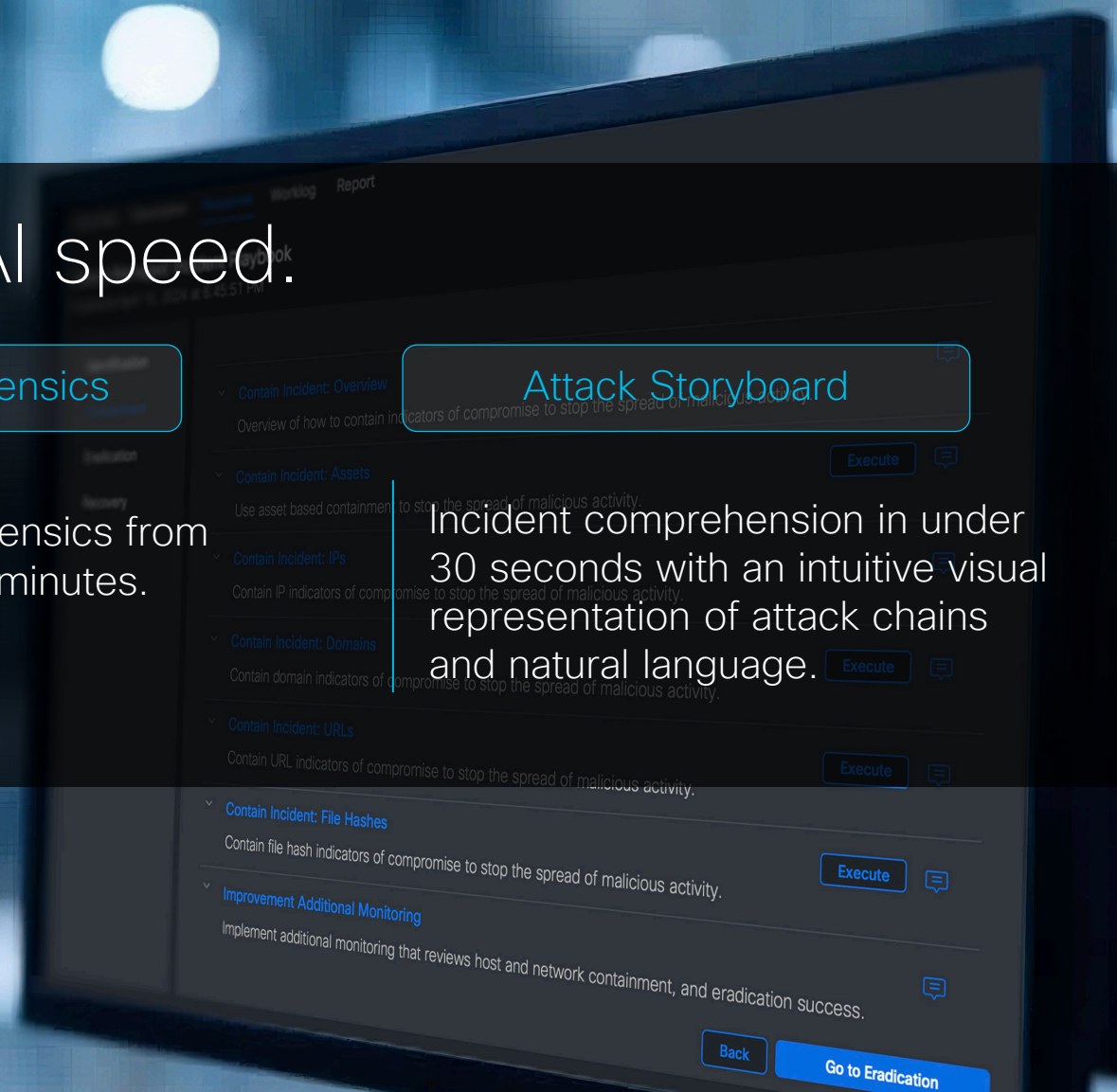
Multi-agent, agentic AI to quickly confirm threats, enabling decisive, automated response

Automated Forensics

Market leading forensics from every endpoint in minutes.

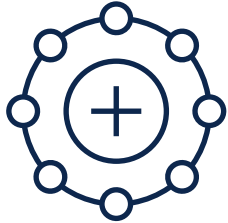
Attack Storyboard

Incident comprehension in under 30 seconds with an intuitive visual representation of attack chains and natural language.



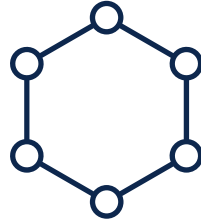
Summary

Why Cisco Breach Protections



Faster detections

Detect threats sooner with advanced analytics and a unique attack chaining capability that provides end-to-end attack correlation with automated incident prioritization based on risk and threat risk.



Simplified investigation

Simplified investigation using automated incident enrichment and event correlation. Empowering the SOC to quickly identify the source of a threat, its impact, and relevant resources like assets across integrated products.



Rapid containment

Contain threats with robust, automated response actions while keeping track of who did what right within the incident. Various places to initiate a response from an investigation, incident, or the Ribbon.

Resources

Where can you learn more about Cisco XDR?

- [Cisco XDR At a Glance](#)
- [An XDR Primer: The Promise of Simplifying Security Operations Position Paper](#)
- [Cisco XDR: Security Operations Simplified eBook](#)
- [Five Ways to Experience XDR eBook](#)
- [Cisco XDR Overview Video](#)
- [XDR Instant Demo](#)
- [Threat Hunting Workshop](#)

Cisco XDR on Cisco.com





Thank you