

Cisco XDR

Tech Club

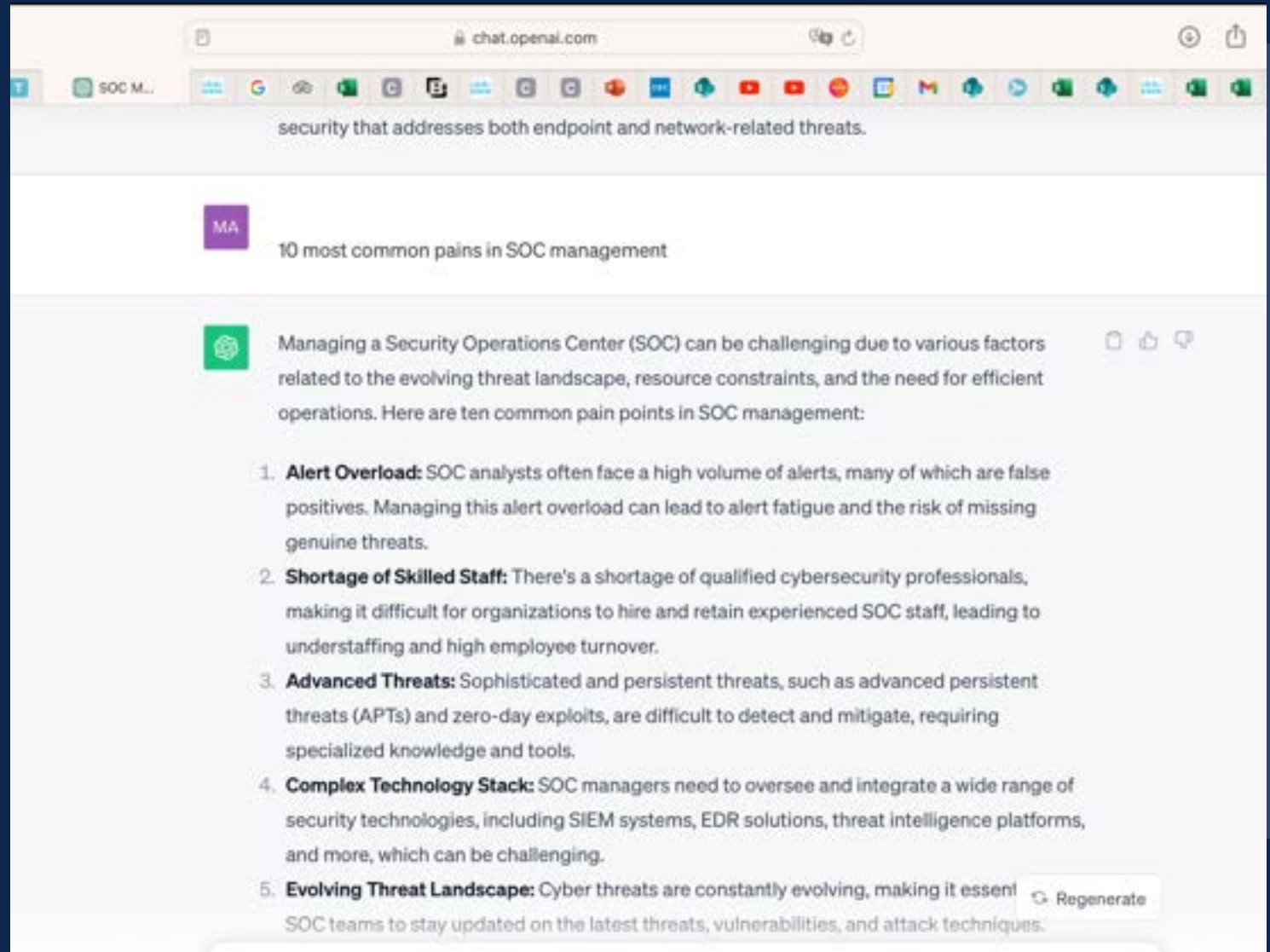
Jiří Tesař

TSA Security, jitesar@cisco.com

6.2.2024



Most common pains



chat.openai.com

security that addresses both endpoint and network-related threats.

MA

10 most common pains in SOC management

Managing a Security Operations Center (SOC) can be challenging due to various factors related to the evolving threat landscape, resource constraints, and the need for efficient operations. Here are ten common pain points in SOC management:

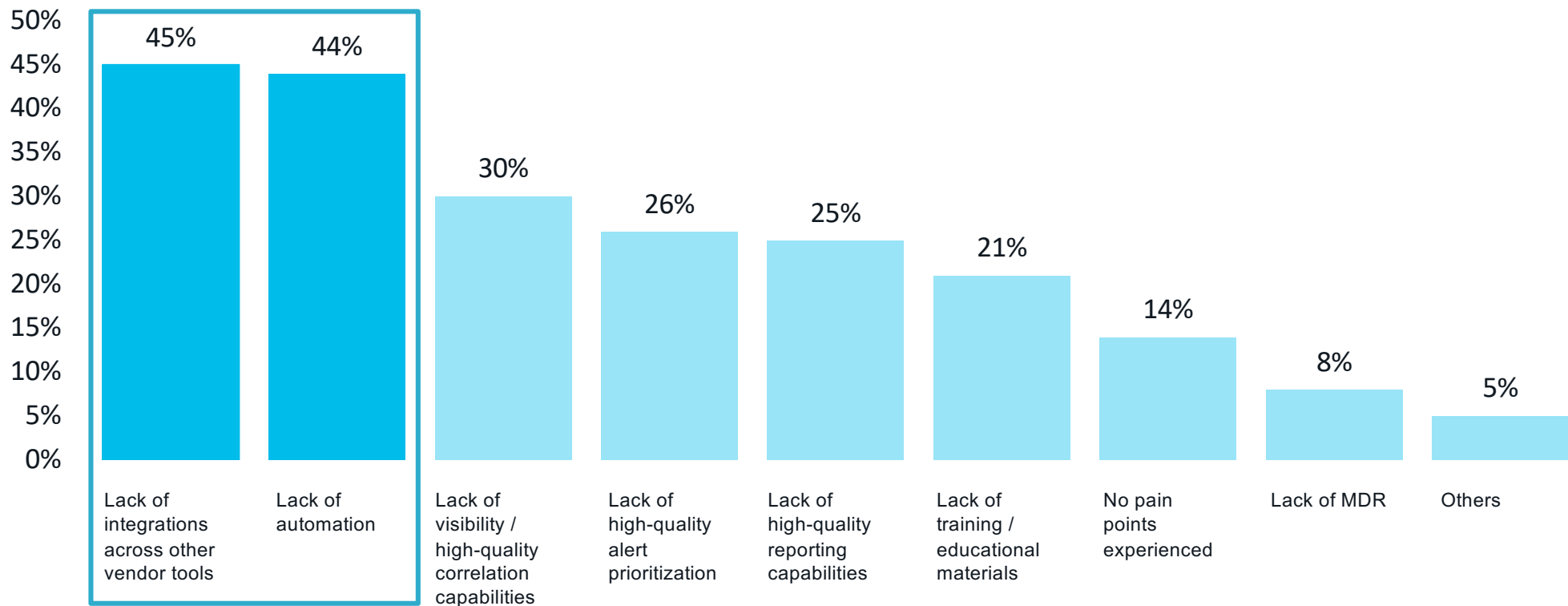
1. **Alert Overload:** SOC analysts often face a high volume of alerts, many of which are false positives. Managing this alert overload can lead to alert fatigue and the risk of missing genuine threats.
2. **Shortage of Skilled Staff:** There's a shortage of qualified cybersecurity professionals, making it difficult for organizations to hire and retain experienced SOC staff, leading to understaffing and high employee turnover.
3. **Advanced Threats:** Sophisticated and persistent threats, such as advanced persistent threats (APTs) and zero-day exploits, are difficult to detect and mitigate, requiring specialized knowledge and tools.
4. **Complex Technology Stack:** SOC managers need to oversee and integrate a wide range of security technologies, including SIEM systems, EDR solutions, threat intelligence platforms, and more, which can be challenging.
5. **Evolving Threat Landscape:** Cyber threats are constantly evolving, making it essential for SOC teams to stay updated on the latest threats, vulnerabilities, and attack techniques.

Regenerate

Most common pains









1. Alert Overload
2. Shortage of Skilled Staff
3. Advanced Threats
4. Complex Technology Stack
5. Evolving Threat Landscape
6. Budget Constraints
7. Regulatory Compliance
8. Incident Response Coordination
9. Retaining Talent
10. Legacy Systems

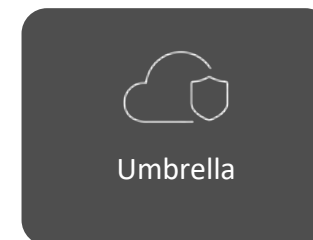
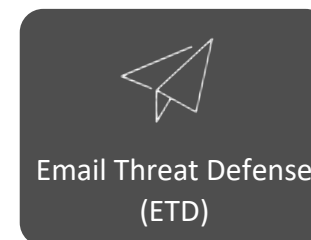
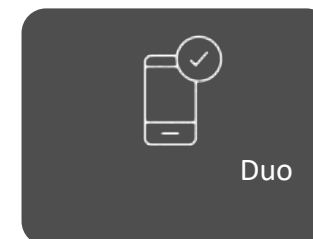
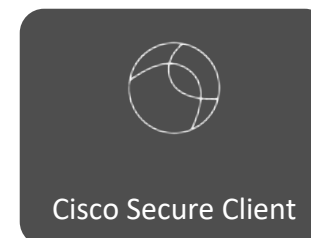
Lack of integration and automation are the most widespread pain points for existing XDR solutions



Telemetry data source importance

The top six data sources that customers believe are essential for an XDR are
Endpoint, Network, Firewall, Identity, Email, and DNS

Essential		
	Count	Share
 Endpoint	255	85.0%
 Network	226	75.3%
 Firewall	207	69.0%
 Identity	191	63.7%
 Email	179	59.7%
 DNS	140	46.7%
 Public Cloud	137	45.7%
 Non-Security Sources	36	12.0%



Definition of Extended Detection and Response (XDR)

Collection of telemetry from multiple security tools

Application of analytics to the collected and homogenized data to arrive at a detection of maliciousness

Response and remediation of that maliciousness

The Cisco approach to XDR

Detect more, act faster, elevate productivity, build resilience



Detect
the most sophisticated
threats

- Multi-vector detection: network, cloud, endpoint, email, and more
- Enriched incidents with asset insights, threat intel
- Optimized for multi-vendor environments



Act on
what truly matters,
faster

- Prioritize threats by greatest material risk
- Unified context to streamline investigations
- Evidence-backed recommendations



Elevate productivity

- Focus on what matters and filter out the noise
- Boost limited resources for maximum value
- Automate tasks and focus on, strategic tasks



Build
resilience

- Close security gaps
- Anticipate what's next through actionable intel
- Get stronger, everyday with continuous, quantifiable improvement

ANYTHING Detection and Response

EDR

ENDPOINT DETECTION AND RESPONSE

Endpoint installation agent
needed.

NDR

NETWORK DETECTION AND RESPONSE

Network detection and
response for north/south and
east/west traffic.

No agent needed

Behavioural analysis.

XDR

EXTENDED DETECTION AND RESPONSE

Correlation of different
sources.

multi-vendor, cloud and on –
premise.

Prioritization of events based
on business impact.

Automated response.

MDR

MANAGED DETECTION AND RESPONSE

Monitoring 24x7

Detection and Response
Managed by vendor.

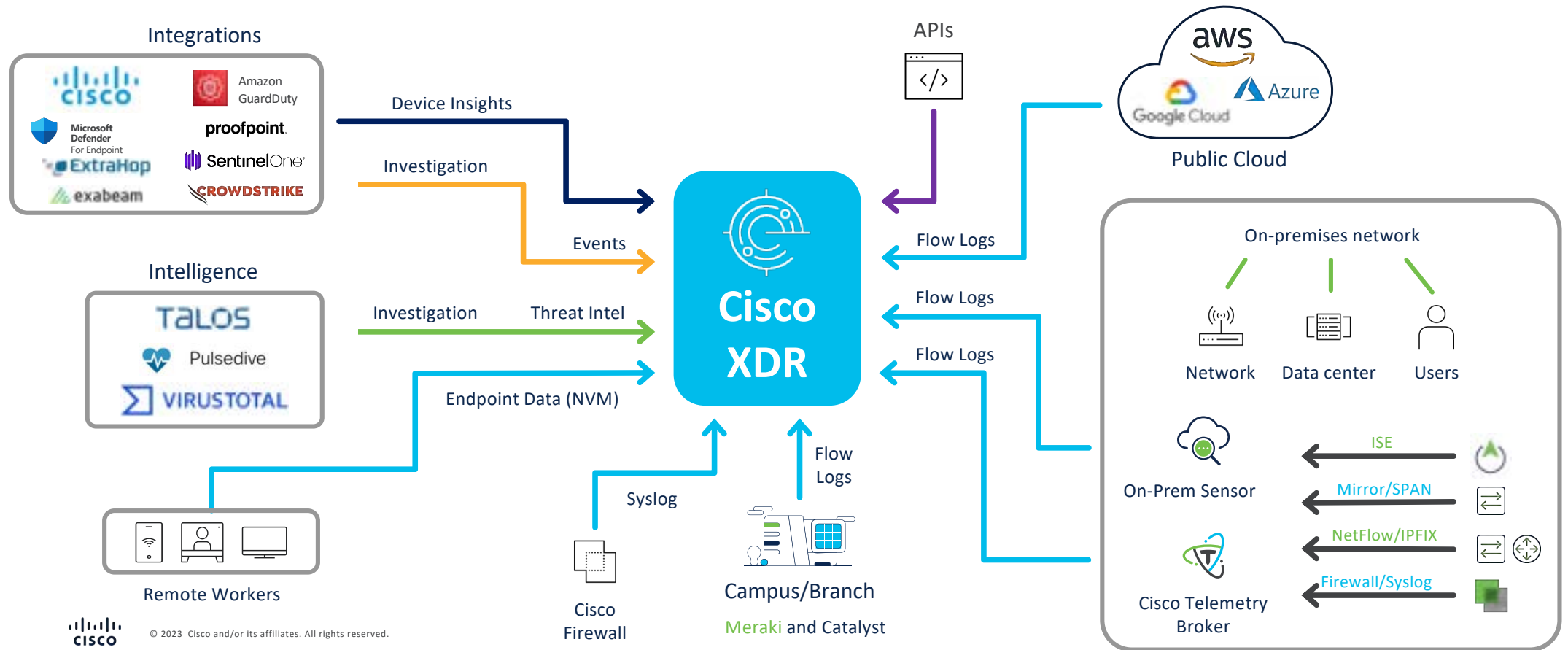
XDR vs SIEM

Key differences	SIEM	XDR
SCOPE OF DATA COLLECTION	collecting, analyzing, and correlating log and event data from a wide range of sources, such as firewalls, IDS/IPS, endpoints, and applications	goes beyond log and event data and also collects and analyzes endpoint data, network traffic, and cloud-based data in real time
DETECTION AND RESPONSE CAPABILITIES	Event correlation and reporting to generate alerts	advanced threat detection and automated response. Machine learning/AI + behavioral analytics to detect threats in real time.
DATA CORRELATION	Correlation rules and filters	Advanced analytics
ALERT MANAGEMENT	Large number of alerts, manually triaged and prioritize by analysts.	built-in intelligence to reduce alert fatigue and prioritize incidents based on their severity and potential impact
REAL TIME RESPONSE	provides information for incident investigation and reporting but often lacks real-time response capabilities	allows for real-time incident response, enabling automated actions to be taken immediately upon detection of a threat, thereby minimizing the time between detection and response.

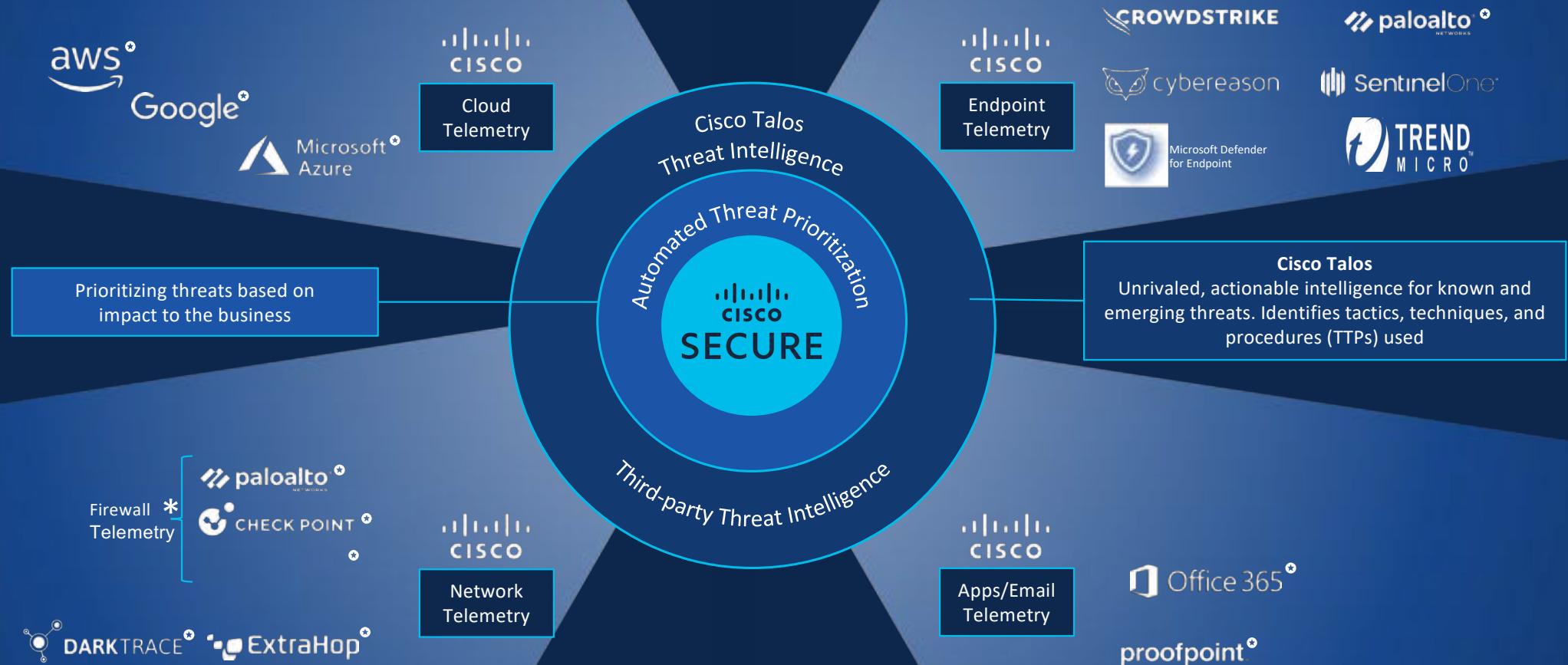
Extended context

Telemetry sources for Cisco XDR

Flexible integration for existing infrastructure



Strategic integrations to deliver customer outcomes



Business Needs



An XDR is an expression of business needs

Where are we **most exposed** to risk? How good are we at detecting attacks **early**?

1 Detect Sooner

Prioritize by Impact

2

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

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

3 Reduce Investigation Time

Accelerate Response

4

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

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

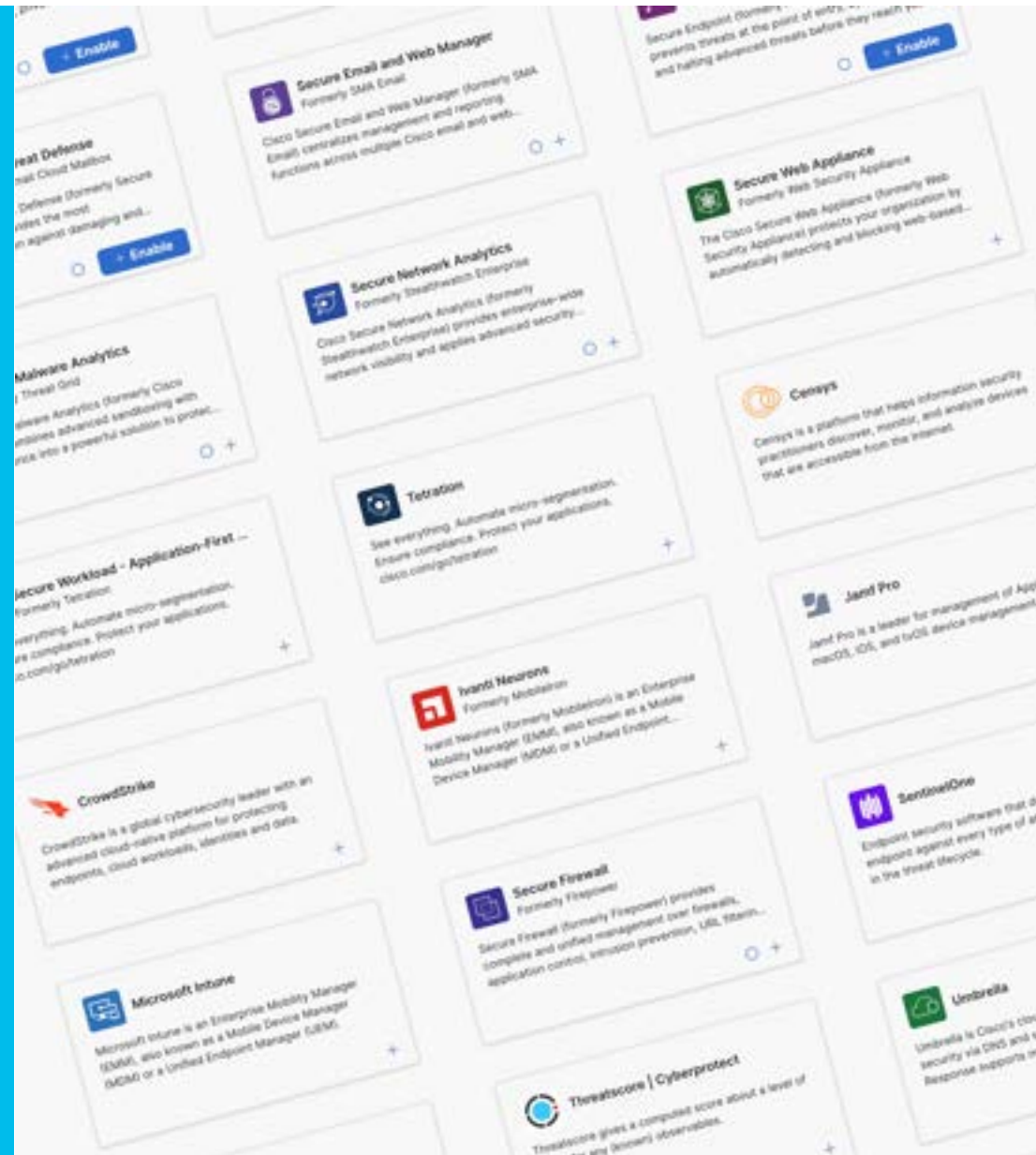
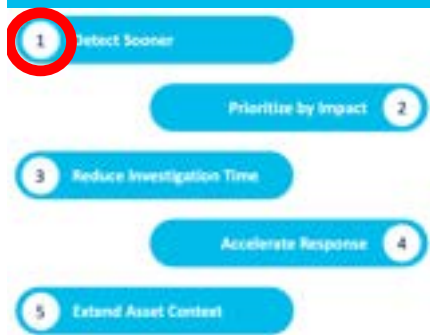
5 Extend Asset Context

Outcomes



1) Detect sooner

- Leverage integrations for faster detection and response
 - Now including CrowdStrike and SentinelOne
- Use intelligence from multiple integrated products
- Correlate alerts to detect slow or hidden attacks



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



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

Others...

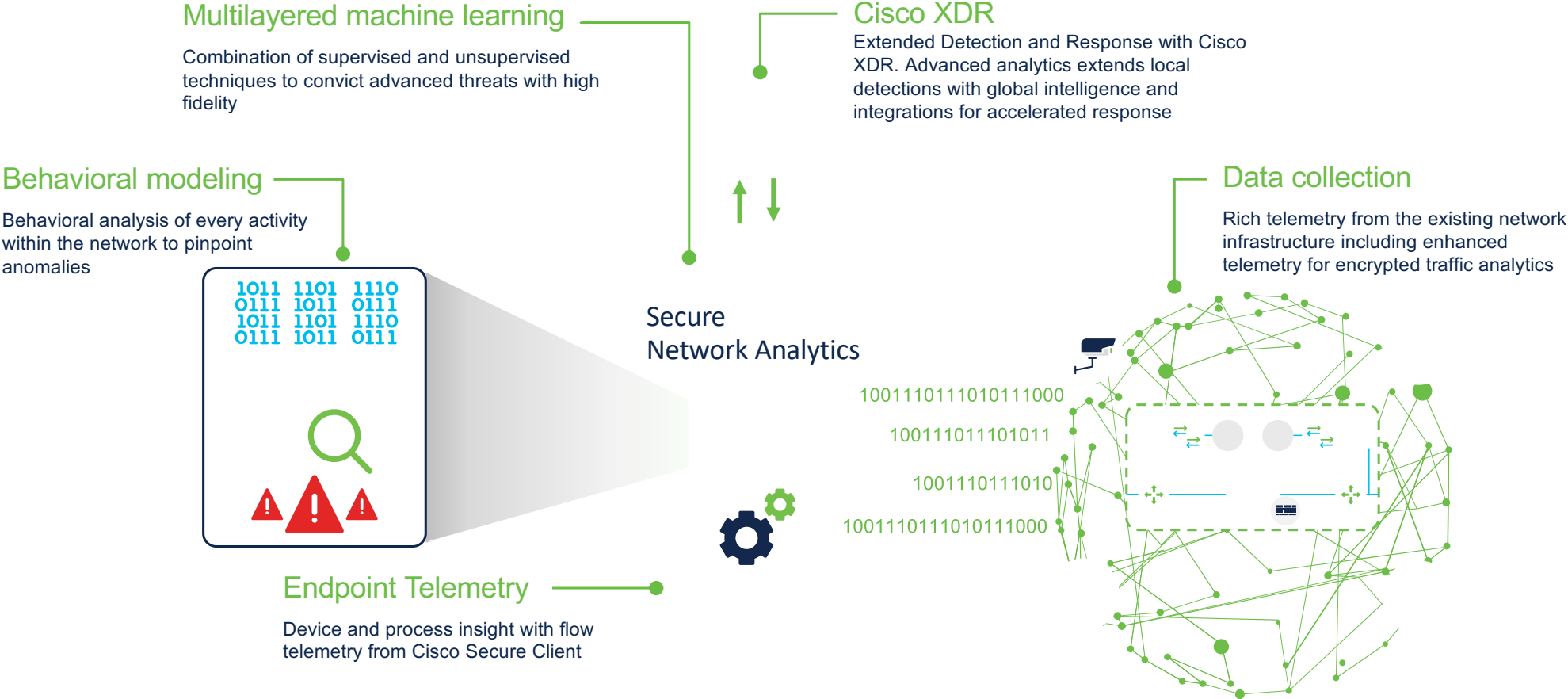
Judgements

Indicators

Feeds

Events

Secure Network Analytics



2) Prioritize by impact

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



Incidents

62 Incidents

33 New Incidents

8 Open

Search

62 matching results

Filters

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

Walk through incidents step by step

Progressive disclosure

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

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

Rich incident details

Incidents are enriched with data gathered from multiple sources including assets, indicators, observables and others. Associated MITRE ATT&CK tactics and techniques detailed with risk scoring

Priority **1000** Status **New**

Malicious Process and Suspicious SMB/RDP...

Reported by **Cisco Secure Cloud Analytics (rsa)**
15 hours ago

Assigned **RM** **JF**

MITRE **TA0003**

Priority score breakdown

1000

100
Detection
Risk

10
Asset
Value at Risk

Short description

This feature is currently under active development

Long description

Alert Chain
fb56eea65af173cd7286d510722e4f8f7e5c8613

Description

View Incident Detail

MITRE ATT&CK View all Tactics

Tactics

TA0003: Execution 100

TA0008: Lateral Movement 66

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

Orientation

```
graph LR; A1[NT AUTHORITY\SYSTEM] --- A2[C:\Windows\System32\svchost.exe]; A1 --- A3[svchost.exe]; A1 --- A4[SYSTEM]; A1 --- A5[10.0.1.8]; A2 --- A6[10.0.0.1]; A3 --- A6; A4 --- A6; A5 --- A6; A6[10.0.0.1] --- A7[10.0.0.1]; A7 --- A8[10.0.0.1]; A8 --- A9[10.0.0.1]; A9 --- A10[10.0.0.1]; A10 --- A11[10.0.0.1]; A11 --- A12[10.0.0.1]; A12 --- A13[10.0.0.1]; A13 --- A14[10.0.0.1]; A14 --- A15[10.0.0.1]; A15 --- A16[10.0.0.1]; A16 --- A17[10.0.0.1]; A17 --- A18[10.0.0.1]; A18 --- A19[10.0.0.1]; A19 --- A20[10.0.0.1]; A20 --- A21[10.0.0.1]; A21 --- A22[10.0.0.1]; A22 --- A23[10.0.0.1]; A23 --- A24[10.0.0.1]; A24 --- A25[10.0.0.1]; A25 --- A26[10.0.0.1]; A26 --- A27[10.0.0.1]; A27 --- A28[10.0.0.1]; A28 --- A29[10.0.0.1]; A29 --- A30[10.0.0.1]; A30 --- A31[10.0.0.1]; A31 --- A32[10.0.0.1]; A32 --- A33[10.0.0.1]; A33 --- A34[10.0.0.1]; A34 --- A35[10.0.0.1]; A35 --- A36[10.0.0.1]; A36 --- A37[10.0.0.1]; A37 --- A38[10.0.0.1]; A38 --- A39[10.0.0.1]; A39 --- A40[10.0.0.1]; A40 --- A41[10.0.0.1]; A41 --- A42[10.0.0.1]; A42 --- A43[10.0.0.1]; A43 --- A44[10.0.0.1]; A44 --- A45[10.0.0.1]; A45 --- A46[10.0.0.1]; A46 --- A47[10.0.0.1]; A47 --- A48[10.0.0.1]; A48 --- A49[10.0.0.1]; A49 --- A50[10.0.0.1]; A50 --- A51[10.0.0.1]; A51 --- A52[10.0.0.1]; A52 --- A53[10.0.0.1]; A53 --- A54[10.0.0.1]; A54 --- A55[10.0.0.1]; A55 --- A56[10.0.0.1]; A56 --- A57[10.0.0.1]; A57 --- A58[10.0.0.1]; A58 --- A59[10.0.0.1]; A59 --- A60[10.0.0.1]; A60 --- A61[10.0.0.1]; A61 --- A62[10.0.0.1]; A62 --- A63[10.0.0.1]; A63 --- A64[10.0.0.1]; A64 --- A65[10.0.0.1]; A65 --- A66[10.0.0.1]; A66 --- A67[10.0.0.1]; A67 --- A68[10.0.0.1]; A68 --- A69[10.0.0.1]; A69 --- A70[10.0.0.1]; A70 --- A71[10.0.0.1]; A71 --- A72[10.0.0.1]; A72 --- A73[10.0.0.1]; A73 --- A74[10.0.0.1]; A74 --- A75[10.0.0.1]; A75 --- A76[10.0.0.1]; A76 --- A77[10.0.0.1]; A77 --- A78[10.0.0.1]; A78 --- A79[10.0.0.1]; A79 --- A80[10.0.0.1]; A80 --- A81[10.0.0.1]; A81 --- A82[10.0.0.1]; A82 --- A83[10.0.0.1]; A83 --- A84[10.0.0.1]; A84 --- A85[10.0.0.1]; A85 --- A86[10.0.0.1]; A86 --- A87[10.0.0.1]; A87 --- A88[10.0.0.1]; A88 --- A89[10.0.0.1]; A89 --- A90[10.0.0.1]; A90 --- A91[10.0.0.1]; A91 --- A92[10.0.0.1]; A92 --- A93[10.0.0.1]; A93 --- A94[10.0.0.1]; A94 --- A95[10.0.0.1]; A95 --- A96[10.0.0.1]; A96 --- A97[10.0.0.1]; A97 --- A98[10.0.0.1]; A98 --- A99[10.0.0.1]; A99 --- A100[10.0.0.1];
```

4 Assets

virtualmachines/win-vic-2 6 events

virtualmachines/win-dc-0 5 events

virtualmachines/win-vic-8 4 events

virtualmachines/kali 1 event

View Assets

31 Observables

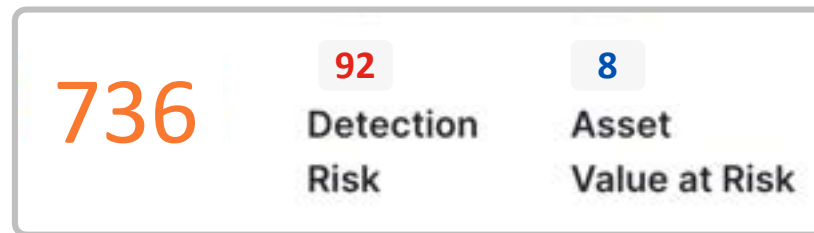
NT AUTHORITY\SYSTEM

C:\Windows\System32\svchost.exe

svchost.exe

SYSTEM

Identify the most impactful incidents based on risk



$$\begin{array}{ccccc} \text{Priority Score} & = & \text{Detection Risk} & \times & \text{Asset Value} \\ \text{0-1000} & & \text{0-100} & & \text{0-10} \end{array}$$

The Incident total priority score used to prioritize incidents

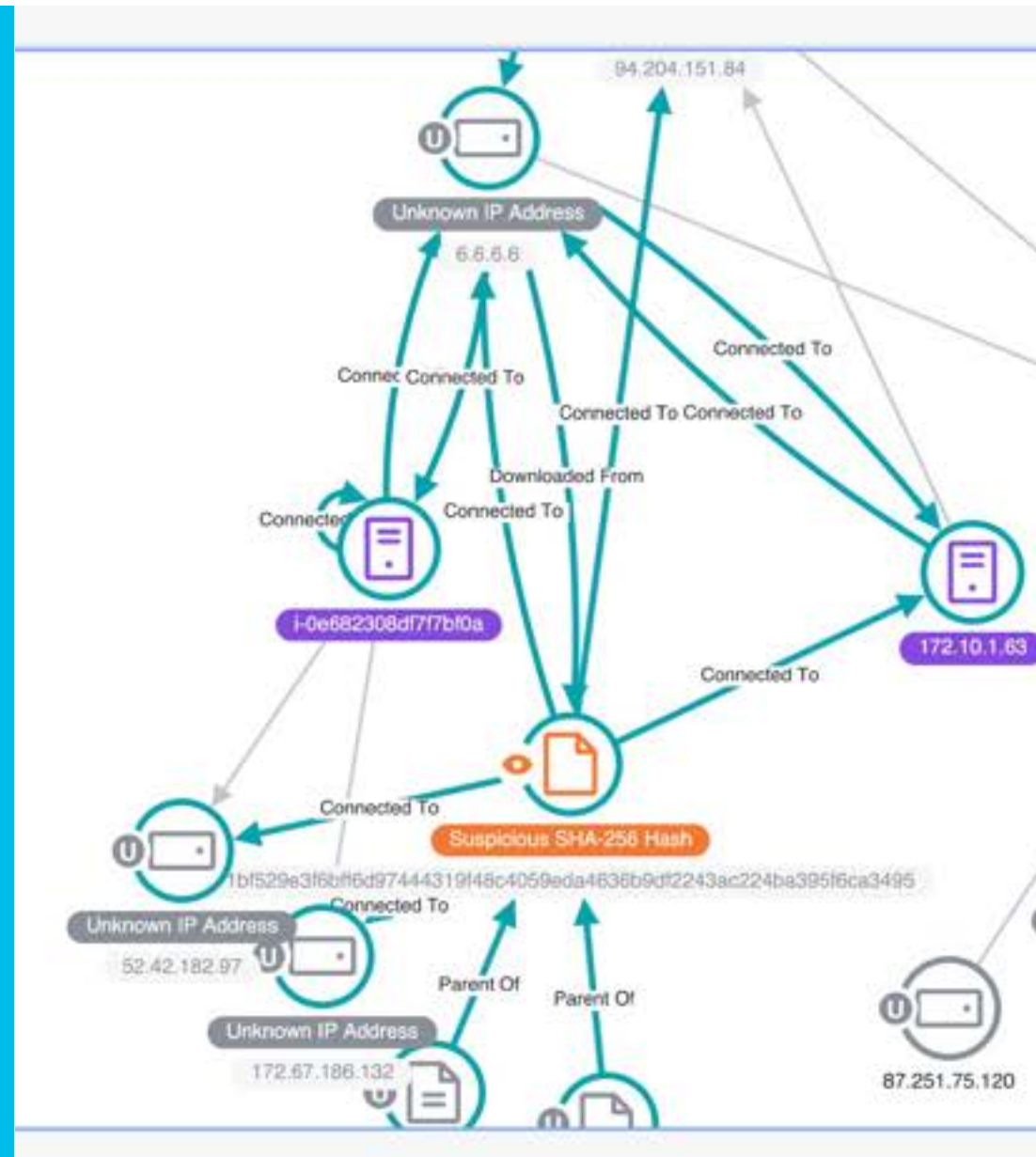
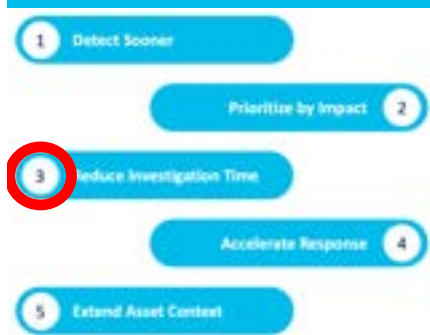
Detection Risk composed of multiple values:

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

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

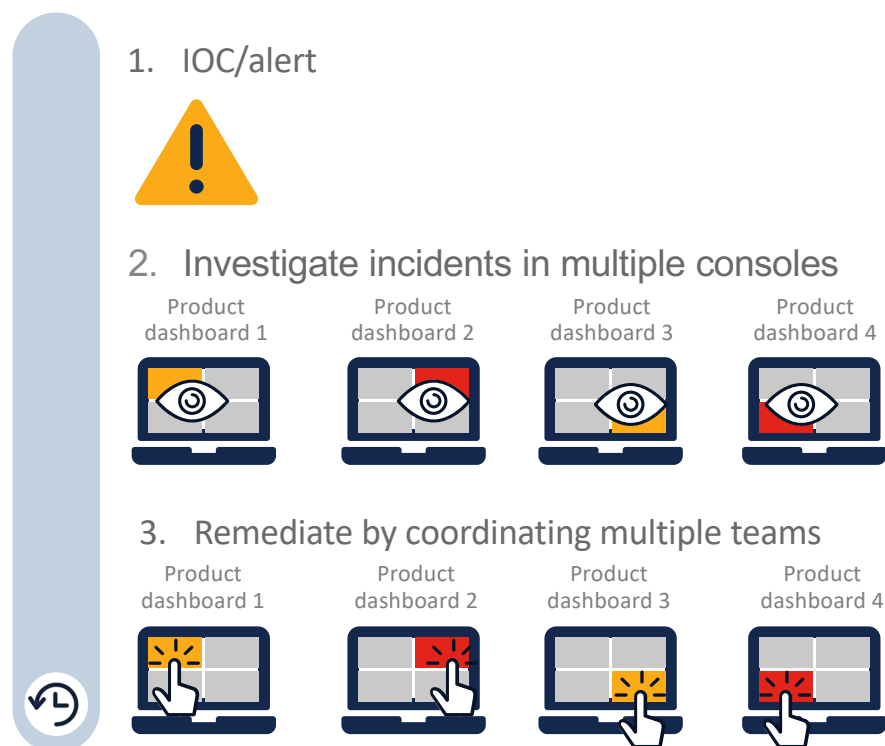
3) Reduce investigation time

- Interactive, visual representations of incidents
- Event correlation and attack chaining to group related intelligence
- Automated enrichment for the most critical incidents, ensuring intelligence is gathered immediately

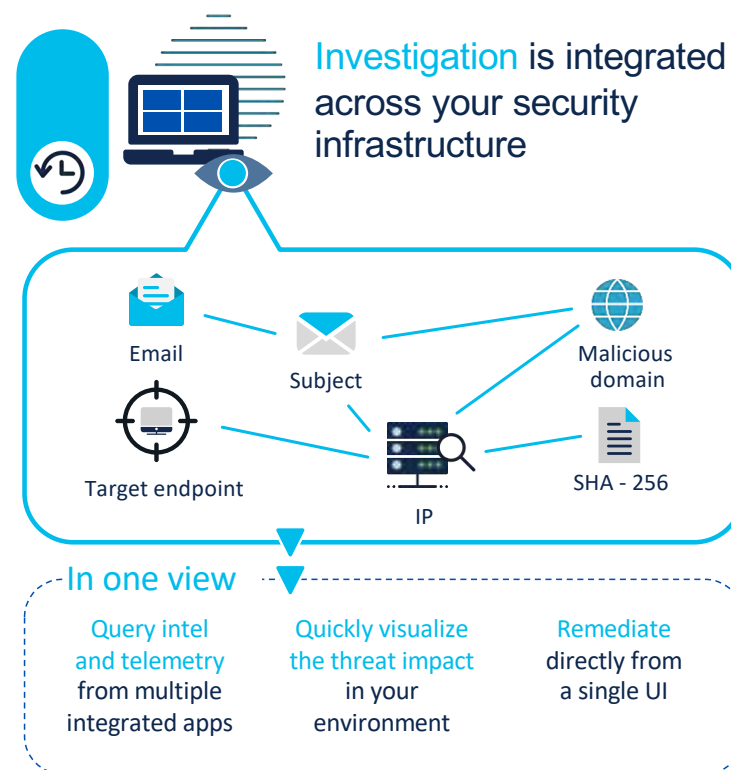


How true simplicity is experienced

Without XDR: 32 minutes



With XDR: five minutes



Confirm attacks sooner with alert correlation

• 2023-03-13T16:...	High	Suspicious SMB and RDP
• 2023-03-13T16:...	High	Suspicious Endpoint Acti
• 2023-03-13T16:...	High	Malicious Process Detec

Priority **1000** Status **New**

Malicious Process and Suspicious SMB/RDP...

Reported by **Cisco Secure Cloud Analytics**
14 hours ago

Assigned **BM** **JF**

MITRE

Alert types

- Malicious Process Detected
- Suspicious SMB and RDP activity

Alerts

1. Malicious Process Detected - #6
2. Suspicious SMB and RDP activity - #35

Sources

- virtualmachines/win-vic-2
- virtualmachines/kali

Chaining Patterns - Tactics

Execution (TA0002) → Lateral Movement (TA0008)

Chaining Patterns - Techniques

Masquerading (T1036) → Remote Services (T1021)

Correlate alerts through time

Automatically create new incidents from correlated alerts over time, reveal the bigger picture of a multi-stage attack

Mapping the Attack Chain

Using MITRE Tactics and Techniques to connect and revealing the attack chain

4) Accelerate response

- Ability to respond throughout the interface
- Simplified response workflows available from within incidents
- Broad set of workflows to achieve a variety of outcomes



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 →](#)

Orchestration Workflows

Powerful, flexible automation



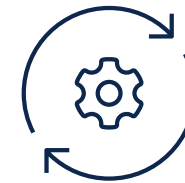
Response

Analyst triggers a workflow from within the incident manager or a pivot menu



Automation rules

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

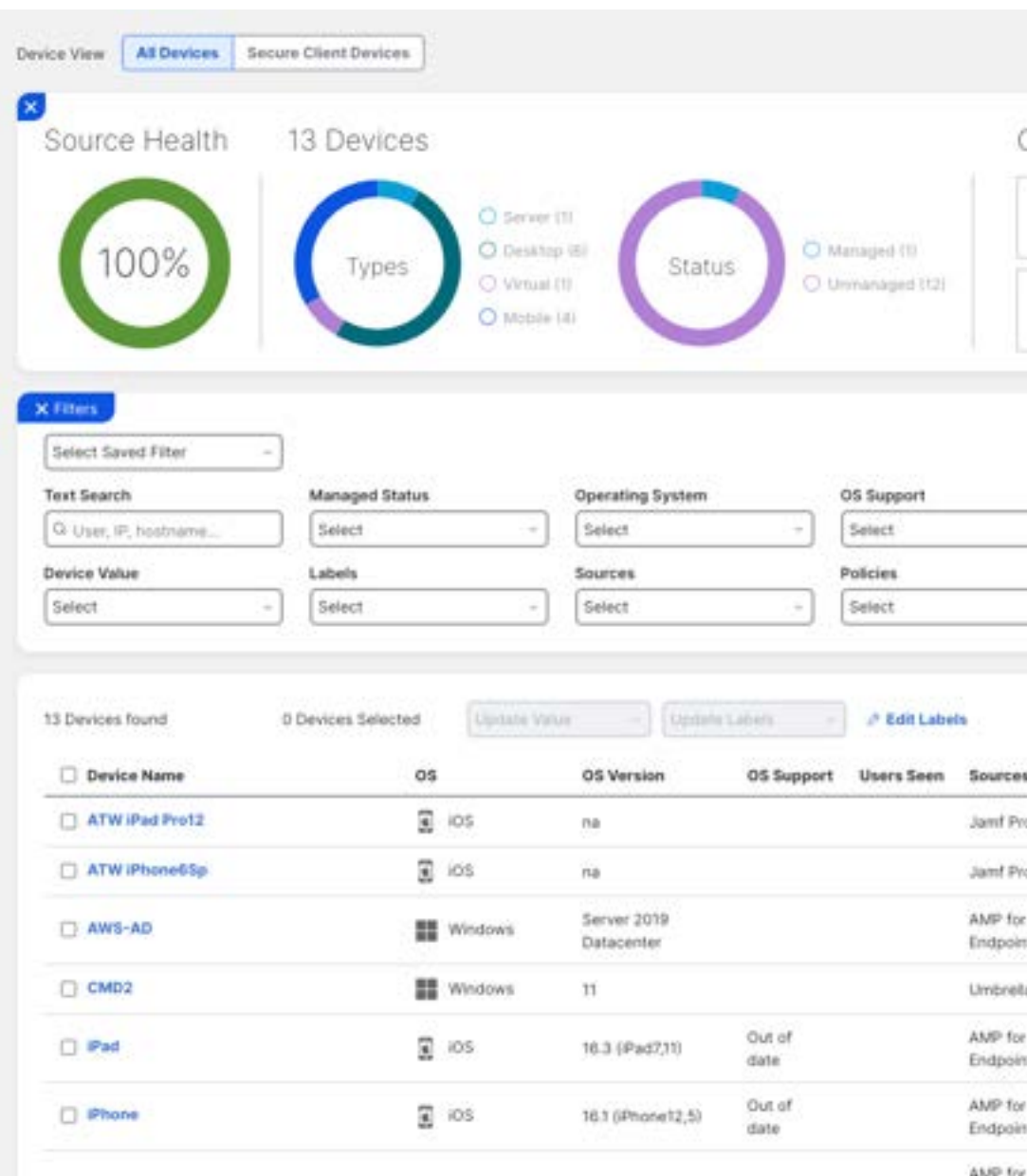
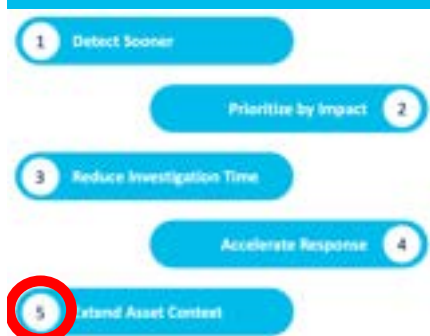


And more...

Workflows triggered by users, APIs, webhooks, schedules, and more

5) Extend asset context

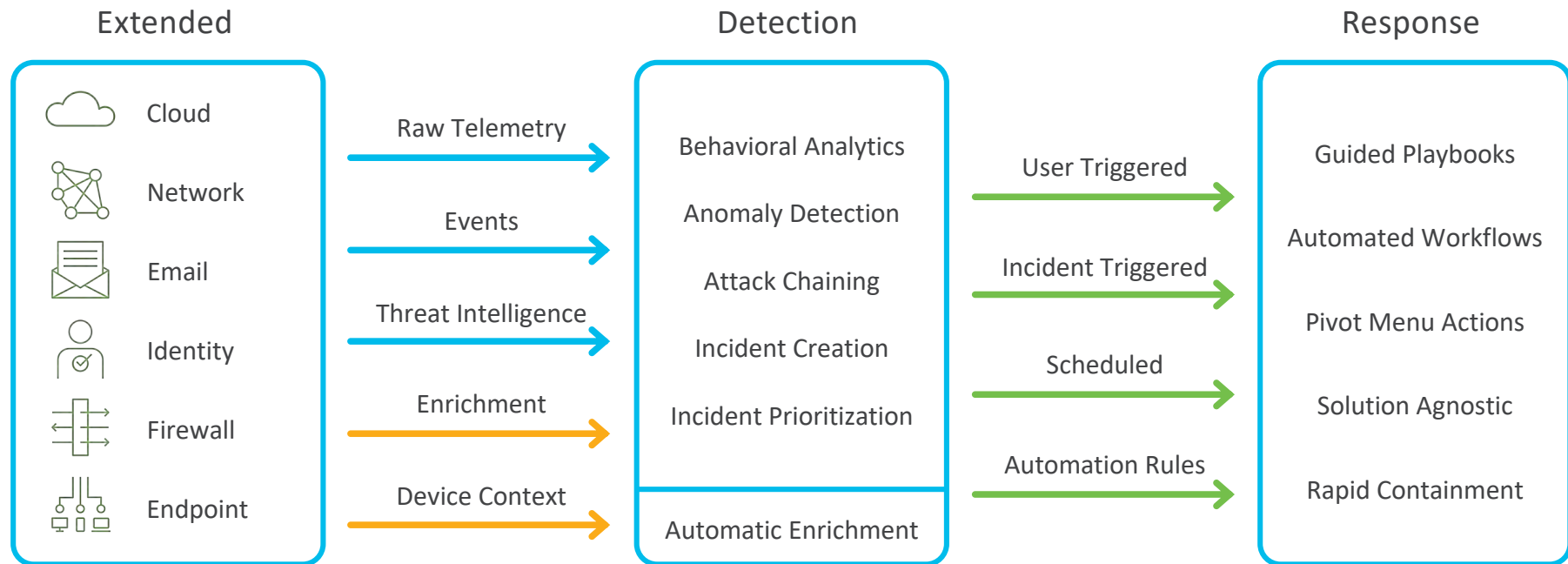
- Detailed asset information aggregated from multiple sources
- Combines asset inventory with security context
- Allows for more accurate incident prioritization based on asset value
- Distinguish between targets and assets



Features



High level architecture



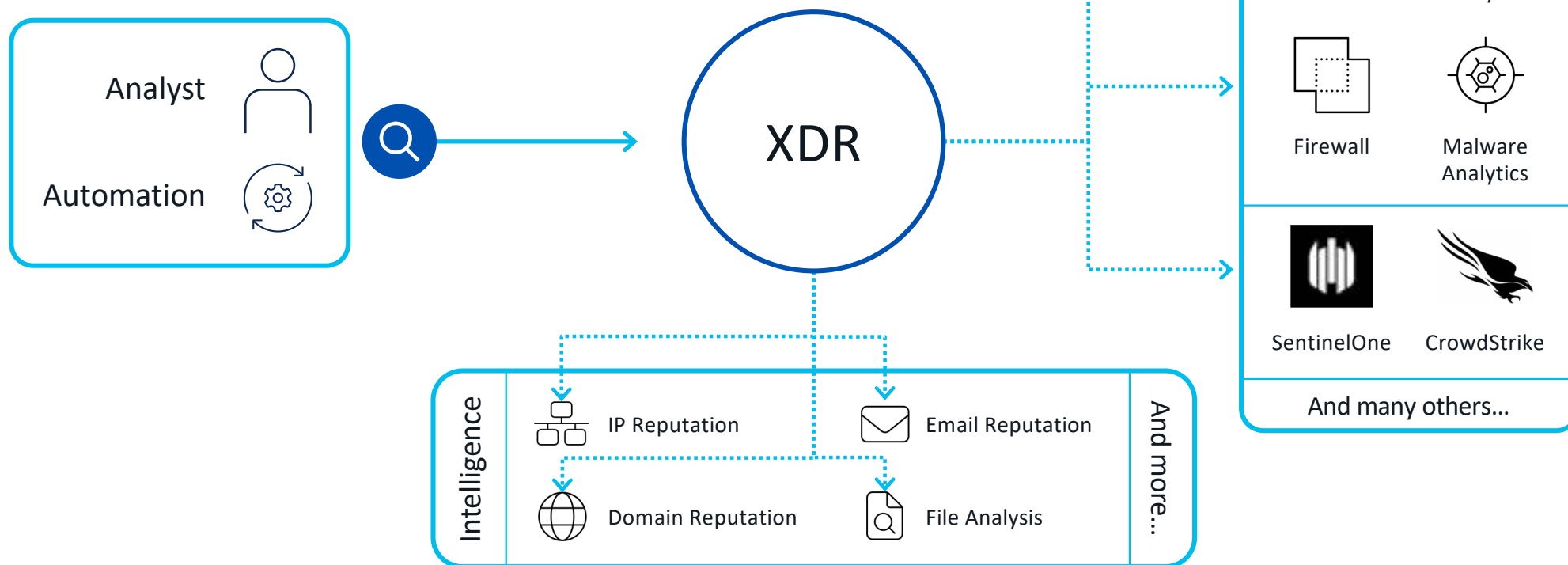
Multi-vector telemetry ingest network, cloud, endpoint, email, and more from Cisco and 3rd party

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

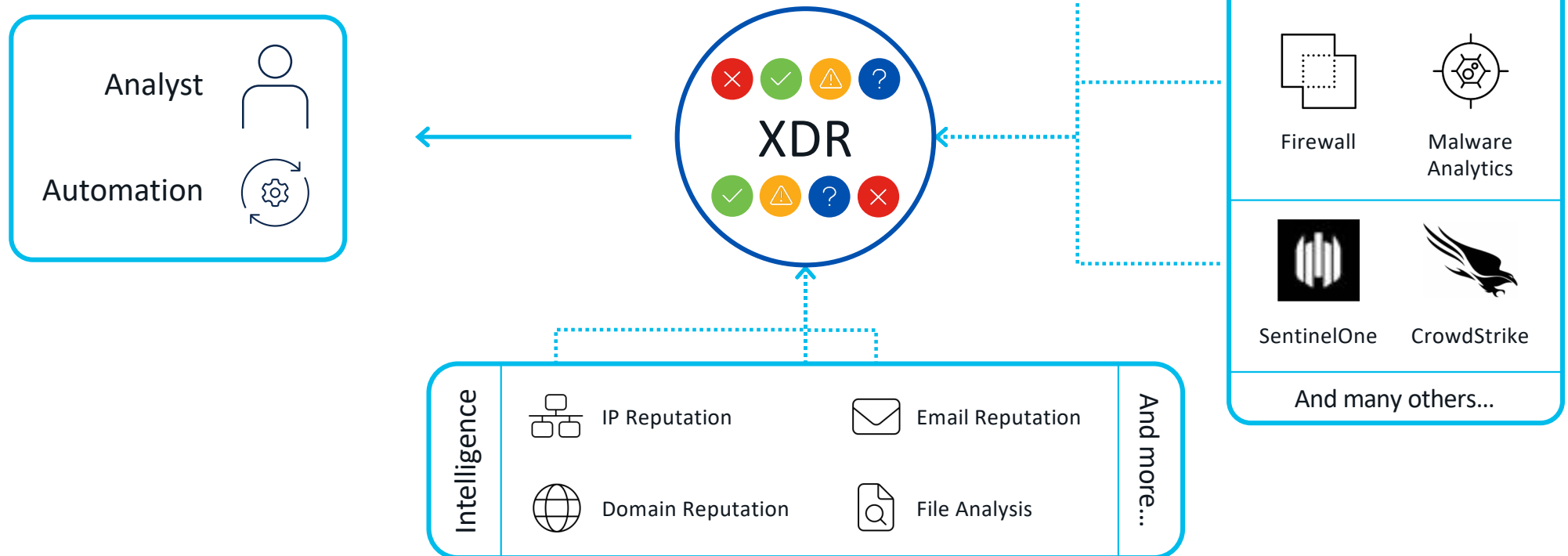
Enrichment demo

The process of consulting all integrations to find out what any of them know about the observable(s).



Enrichment demo

The process of consulting all integrations to find out what any of them know about the observable(s).



Incident manager

Incidents

62 Incidents

33 New Incidents

8 Open

Search

62 matching results

Filters

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

Incident response in four stages

Identify



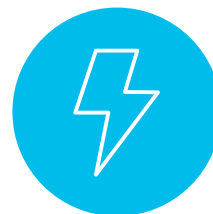
Review the incident and confirm the findings

Contain



Act against impacted hosts, domains, files, etc.

Eradicate



Remediate vulnerabilities and remove malicious content

Recover



Validate remediation and restore impacted services

Control Center

Incidents

Investigate

Intelligence

Automate

Devices

Administration

Incidents

523 Incidents

12 New Incidents

343 Open Incidents

Search

11 matching results

Filters

Status: Incident Reported

<input type="checkbox"/>	Priority	Name	Source	Created	As
<input type="checkbox"/>	1000	EC2AMAZ-AHQFEJR in group Audit @ 20230417 08:16:38	Secure Endpoint	2 Months	R
<input type="checkbox"/>	1000	Geographically Unusual Remote Access for Cisco - Lawrenceville L...	Cisco Secure Clou...	2 Months	A
<input type="checkbox"/>	1000	Heartbeat Connection Count for Cisco - Lawrenceville Lab (Earth)	Cisco Secure Clou...	2 Months	S
<input type="checkbox"/>	1000	c4-3650-1-g1-8-win10 in group Earth Clients @ 20230406 13:51:59	Secure Endpoint	2 Months	S
<input type="checkbox"/>	1000	c5-9300-1-g1-8-win10 in group Pluto Clients @ 20230406 13:52:57	Secure Endpoint	2 Months	R
<input type="checkbox"/>	924	Attack Chain: "Multiple Threat Indicators Triggered" for Cisco - Law...	Cisco Secure Clou...	1 Month	R
<input type="checkbox"/>	873	c1-4506-2-g3-13-win10 in group Mars Clients @ 20230406 13:52:...	Secure Endpoint	2 Months	E
<input type="checkbox"/>	783	c3-9300-1-g1-0-7-win10 in group Audit @ 20230411 08:48:54	Secure Endpoint	2 Months	E
<input type="checkbox"/>	765	Persistent Remote Control Connections for Cisco - Lawrenceville L...	Cisco Secure Clou...	2 Months	D
<input type="checkbox"/>	523	c1-4506-1-g3-14-win10 in group Mars Clients @ 20230411 20:27:12	Secure Endpoint	2 Months	J
<input type="checkbox"/>	392	c1-9300-1-g1-13-ublnx in group Mars Clients @ 20230411 18:26:19	Secure Endpoint	2 Months	J

Priority 1000 Status Incident Report...

Geographically Unusual Remote Access for Cisco - ...

Reported by Cisco Secure Cloud Analytics (cisco-explorcorp-earth) 2 months ago

Assigned AS HJ ST

MITRE

Priority score breakdown

1000

100
Detection
Risk10
Asset
Value at Risk

Short description

Geographically Unusual Remote Access on i-
Oc6069f352916581e

Long description

Alert
Geographically Unusual Remote Access - #4921

Tenant
Cisco - Lawrenceville Lab (Earth) (cisco-explorcorp-earth)

Source
i-Oc6069f352916581e

Description
Device has been accessed from a remote host in a country that doesn't normally access the local network. For example, a local server accepting an SSH connection from a foreign source would trigger

View Incident Detail

Control Center

Incidents

Investigate

Intelligence

Automate

Devices

Administration

Incidents

1000

Incident Reported

Geographically Unusual Remote Access for Cisco - Lawrenceville L

Reported by Cisco Secure Cloud Analytics (cisco-explorcorp-earth) on 2023-04-13T15:04:30.000Z - 2 Linked Incidents

Geographically Unusual Remote Access on i-0c6069f352916581e [View Long Description](#)

Overview Detection **Response** Worklog

Identification

Containment

Eradication

Recovery

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

10 Assets

Search

Hostname

- ☐ MIKE-WIN10
- ☐ EC2AMAZ-AHQFEJR
- ☒ aws-east1-windows2019
- ☐ EC2AMAZ-MTKLEVO
- ☐ i-0e682308df7f7bf0a
- ☐ i-0d3309a793147ae0e
- ☐ c2-3850-1-t1-0-15-win10
- ☐ adsl-172-10-1-63.dsl.sndg02.sbcglobal...
- ☐ i-0c6069f352916581e
- ☐ Security-IDS-Tester

Action

- 202 Exec
- 202 Exec
- 202 Exec
- 202 Exec
- 202 Exec
- 202 Exec
- 202 Exec
- 202 Exec
- 202 Exec

Execute

XDR

Investigate

Investigate

Email Threat Investigation

Lens

Types



174 Nodes



First Seen

Severity

Source

Indicators

2021-01-23T17:29:23.000Z

Low

SMA Tracking API

2021-01-23T13:41:24.000Z

Medium

securex-orchestration

2021-01-21T23:05:35.000Z

Low

SMA Tracking API

2021-01-21T17:12:10.000Z

Low

SMA Tracking API

Control Center

Incidents

Investigate

Intelligence

Automate

Devices

Administration

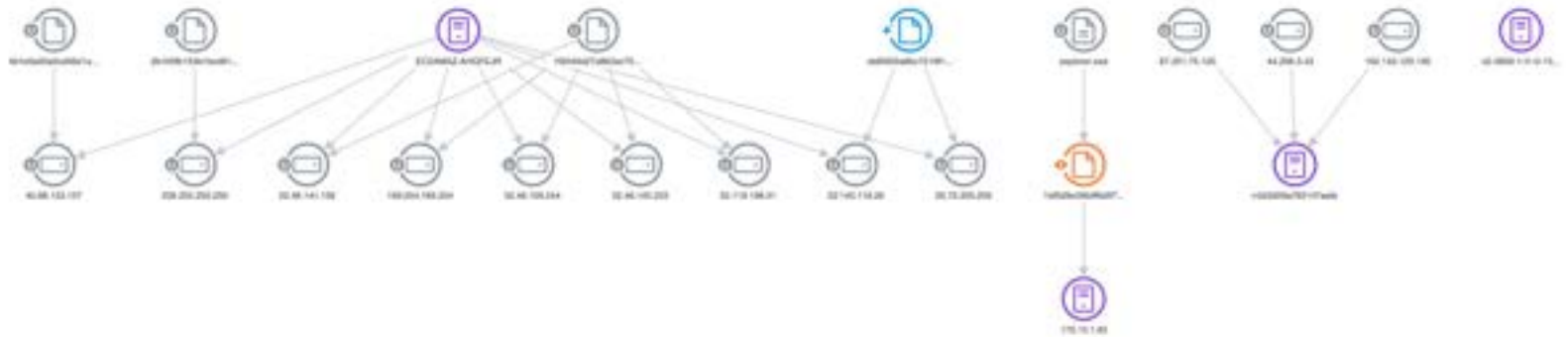
← Investigate

Golden Incident 4_17 V6 shapshot

Save Investigation

Types ▾

22 Nodes



First Seen ▾

Severity ▾

Source

Indicators

Observables

Assets

Indicators

17

XDR

Control Center

Incidents

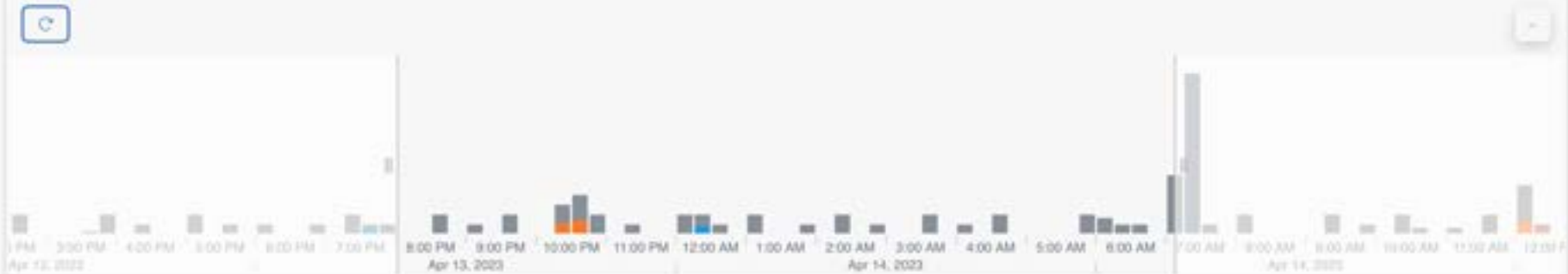
Investigate

Intelligence

Automate

Devices

Administration



First Seen	Severity	Source	Indicators	Observables	Assets
2023-04-17T13:...	Unknown	AMP Event		1bf529e3f6bff6...	EC2AMA...
2023-04-17T13:...	Unknown	AMP Event		1bf529e3f6bff6...	EC2AMA...
2023-04-17T13:...	Unknown	AMP Event		1bf529e3f6bff6...	EC2AMA...
2023-04-17T13:...	Unknown	AMP Event		1bf529e3f6bff6...	EC2AMA...
2023-04-17T13:...	High	NGFW Event Ser...	Security Intelligenc...	172.10.1.63 123.123.123.123	172.10.1.63
2023-04-17T13:...	High	NGFW Event Ser...	Security Intelligenc...	172.10.1.63 6.6.6.6	172.10.1.63
2023-04-17T12:...	Low	AMP Event		123.123.123.123	MIKE-WL...
2023-04-17T12:...	Low	AMP Event		1bf529e3f6bff6...	MIKE-WL...
2023-04-17T12:...	Low	AMP Event		123.123.123.123	MIKE-WL...
2023-04-17T12:...	Low	AMP Event		123.123.123.123	MIKE-WL...

Indicators

17

Cisco Secure Cloud Analytics (cisco-e...
Watchlist Interaction 15 events

Cisco Secure Cloud Analytics (cisco-e...
Internal Connection Watchlist 14 events

Secure Endpoint
ExecutedMalware.loc 2 events

AlienVault OTX
muestra 2 events
 known malicious high true filesha256
 +32

AlienVault OTX
muestra 2 events
 known malicious high true filesha256
 +32

NGFW Event Service 1 events











Intelligence

Judgments

Judgements associate a disposition with an observable. [Learn More](#)

Public

Private

Name	Disposition	Reason	Type	Status
208.180.17.32 	Malicious	IP Used For QakBot C&C	IP Address	2019-01-01
139.59.44.48 	Malicious	IP Used For Emotet C&C	IP Address	2019-01-01
95.95.175.98 	Malicious	IP Used For QakBot C&C	IP Address	2019-01-01
147.219.4.194 	Malicious	IP Used For QakBot C&C	IP Address	2019-01-01
187.199.238.208 	Malicious	IP Used For QakBot C&C	IP Address	2019-01-01
94.23.45.86 	Malicious	IP Used For Emotet C&C	IP Address	2019-01-01
88.171.156.150 	Malicious	IP Used For QakBot C&C	IP Address	2019-01-01
103.212.19.254 	Malicious	IP Used For QakBot C&C	IP Address	2019-01-01
81.229.117.95 	Malicious	IP Used For QakBot C&C	IP Address	2019-01-01
72.200.109.104 	Malicious	IP Used For QakBot C&C	IP Address	2019-01-01
178.128.23.9 	Malicious	IP Used For Emotet C&C	IP Address	2019-01-01

Control Center

Incidents

Investigate

Intelligence

Judgments

Indicators

Events

Feeds

Automate

Devices

Administration

Judgments

Judgements associate a disposition with an observable. [Learn More](#)

Public

Private

Search

Observable	Disposition	Reason	Type	Start/End Times	Source	Severity	TLP
47.149.248.80	Malicious	IP Used For QakBot C&C	IP Address	2023-06-05T14:12:09.327Z 2023-07-05T14:12:09.327Z	Abuse.ch Feodo Tra...	High	Green
151.55.186.41	Malicious	IP Used For QakBot C&C	IP Address	2023-06-05T14:12:09.327Z 2023-07-05T14:12:09.327Z	Abuse.ch Feodo Tra...	High	Green
66.191.69.18	Malicious	IP Used For QakBot C&C	IP Address	2023-06-05T14:12:09.327Z 2023-07-05T14:12:09.327Z	Abuse.ch Feodo Tra...	High	Green
173.184.44.185	Malicious	IP Used For QakBot C&C	IP Address	2023-06-05T14:12:09.327Z 2023-07-05T14:12:09.327Z	Abuse.ch Feodo Tra...	High	Green
173.24.83.160	Malicious	IP Used For QakBot C&C	IP Address	2023-06-05T14:12:09.327Z 2023-07-05T14:12:09.327Z	Abuse.ch Feodo Tra...	High	Green
41.186.88.38	Malicious	IP Used For QakBot C&C	IP Address	2023-06-05T14:12:09.327Z 2023-07-05T14:12:09.327Z	Abuse.ch Feodo Tra...	High	Green
68.229.150.95	Malicious	IP Used For QakBot C&C	IP Address	2023-06-05T14:12:09.327Z 2023-07-05T14:12:09.327Z	Abuse.ch Feodo Tra...	High	Green
70.29.123.54	Malicious	IP Used For QakBot C&C	IP Address	2023-06-05T14:12:09.327Z 2023-07-05T14:12:09.327Z	Abuse.ch Feodo Tra...	High	Green
86.215.62.128	Malicious	IP Used For QakBot C&C	IP Address	2023-06-05T14:12:09.327Z 2023-07-05T14:12:09.327Z	Abuse.ch Feodo Tra...	High	Green
92.135.0.154	Malicious	IP Used For QakBot C&C	IP Address	2023-06-05T14:12:09.327Z 2023-07-05T14:12:09.327Z	Abuse.ch Feodo Tra...	High	Green
174.118.68.176	Malicious	IP Used For QakBot C&C	IP Address	2023-06-05T14:12:09.327Z 2023-07-05T14:12:09.327Z	Abuse.ch Feodo Tra...	High	Green
				2023-06-05T14:12:09.327Z			

SOC- AI Assistance

Cisco Advisor

- AI Chatbot that uses natural language processing to provide insightful answers, practical advice and actionable steps
- Optimizes and recommends next steps and remediation tactics

The screenshot displays the Cisco Advisor interface, which is a SOC- AI Assistance tool. It features a chatbot window on the left and a list of incidents on the right.

Cisco Advisor Chatbot Window:

- Header:** Cisco Advisor
- Input:** "Who are the owners associated with this incident?"
- Response:** "New 8:30 AM: What endpoints were affected by this incident?"
- Response:** "Cisco Advisor 8:30 AM: The following endpoints are associated with 4 user accounts that the malicious file was emailed to, and on certain multiple events."
- Incidents:**
 - Incident: 620-End-user Microsoft
 - Incident: 600KTOP-1039070
 - Incident: 620-End-user v14
 - Incident: 600KTOP-1039070
- Footer:** "How do you want to address this incident?"

Incidents List:

Priority	Name	Source
High	Malicious Email Sent to Multiple Users	Endpoint
High	Threat_Avail in group Protect @ 20230124 10:30:04	Endpoint
High	Threat_Avail in group Protect @ 20230124 10:30:04	Endpoint
High	Win_Microsoft.Policy @ 20230124 10:30:04	Endpoint
High	Endpoint_Burned_Report	Endpoint
High	Microsoft_Policy_Reports a new wave of malware targeting Windows	File
High	Service_A in group Protect @ 20230124 10:30:04	Endpoint
High	Internal_Org_Businesses in group Protect @ 20230124 10:30:04	Endpoint
High	Organizations and MSOs	File
High	Organizations and MSOs	File
High	Organizations: A Chinese attack of Windows and Linux RHEL	File
High	Organizations: A Chinese attack of Linux and Linux RHEL	File
High	Organizations: A Chinese attack of Linux and Linux RHEL	File
High	Page in group Protect @ 20230124 10:30:04	Endpoint

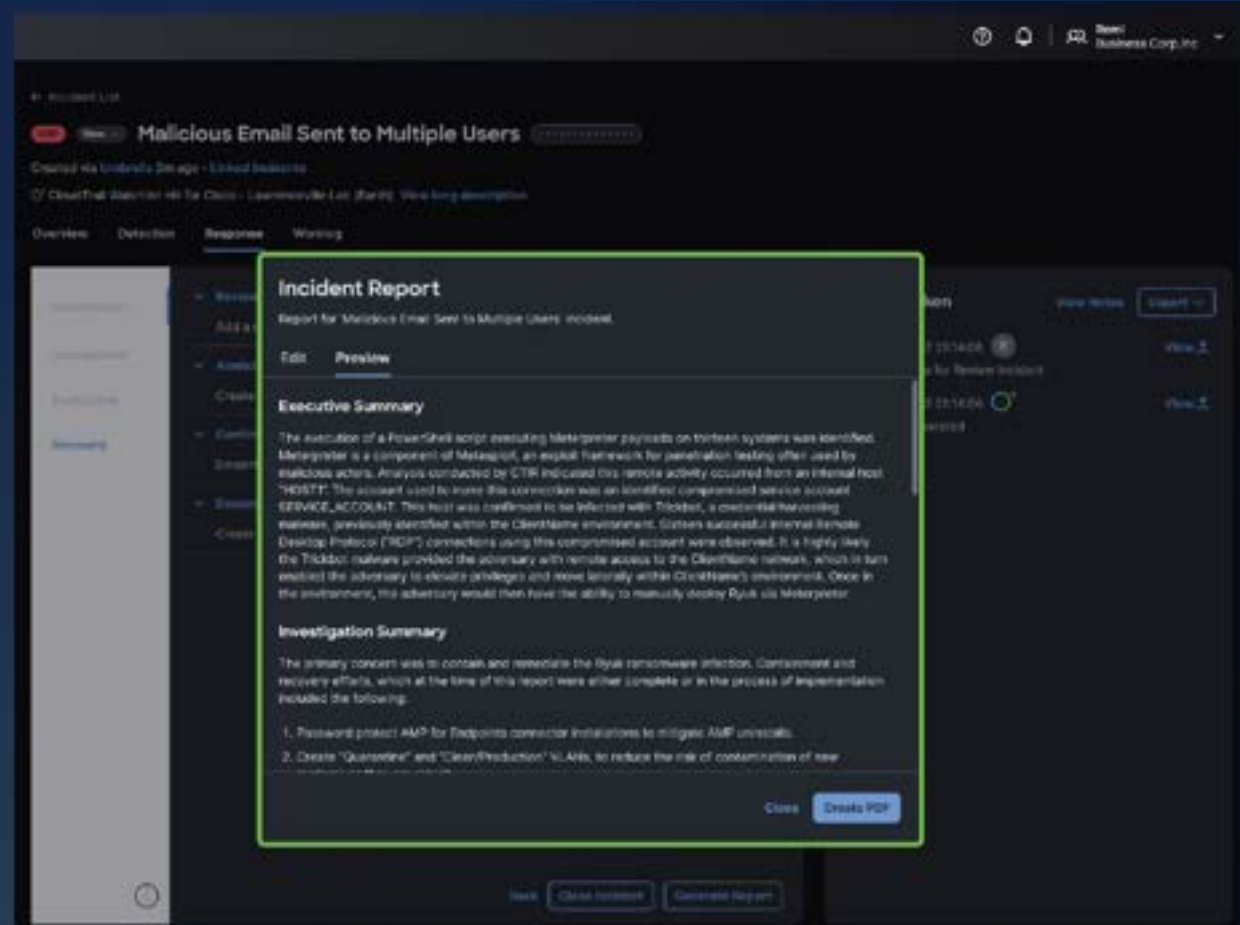
Incident Details Panel (Right):

- Header:** Malicious Email Sent to Multiple Users
- Reported by:** User
- Assigned to:** User
- Priority:** High
- Score:** 990
- Short Description:** A malicious email was sent to multiple endpoints in the organization.
- Long Description:** [Detailed description of the incident]
- Tags:** [List of tags]
- Event Date:** 2023-01-24 10:30:04
- Prevalence:** 2023-01-24 10:30:04
- Reporting Source Type:** [Type]
- Reporting Source ID:** [ID]
- Security Intelligence:** [Source]
- Security Intelligence Category:** [Category]
- Prevalence Reason:** [Reason]

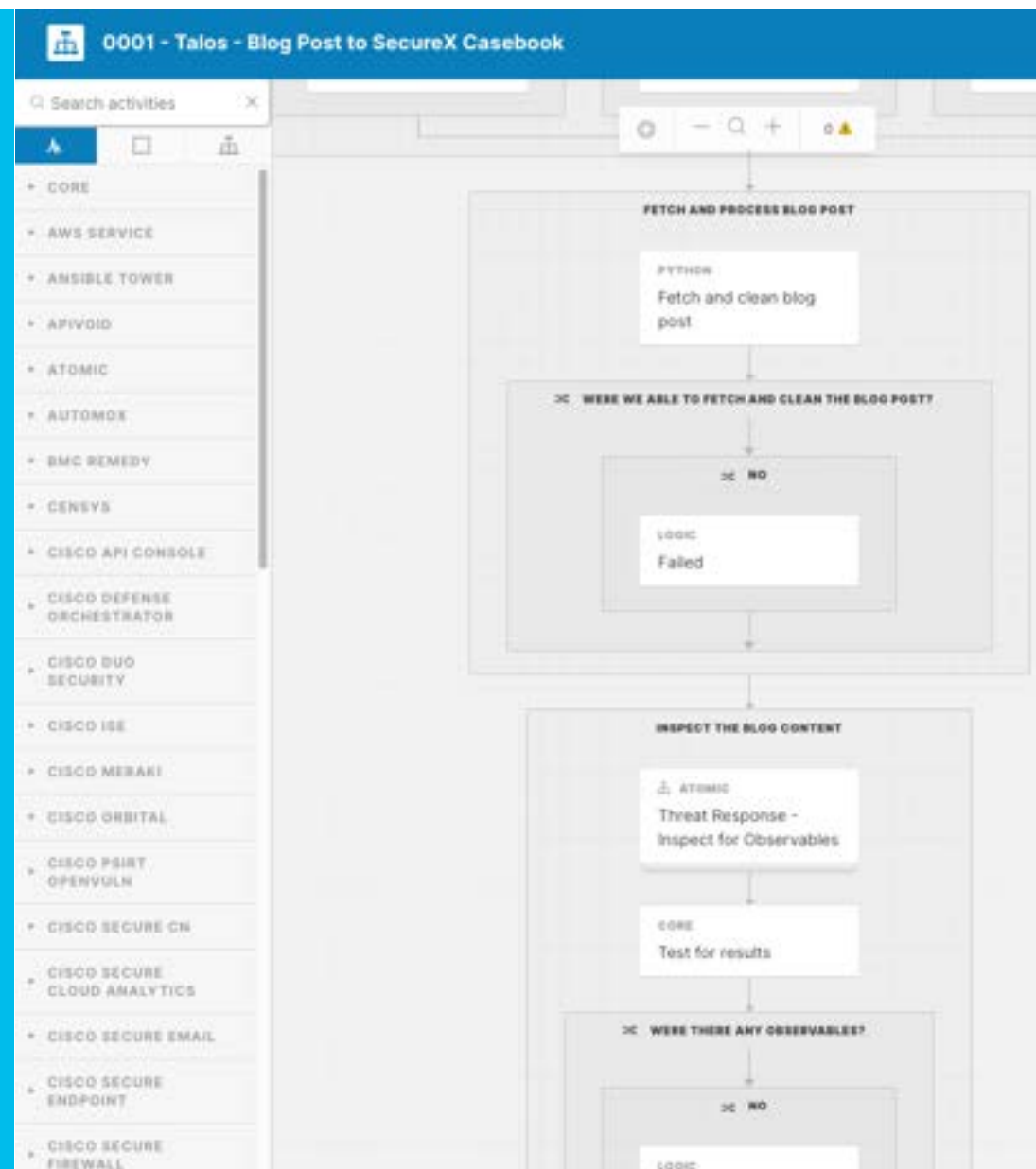
SOC- AI Assistance

Incident Summary Reporting

- As the incident is resolved, save time by allowing generative AI to draft the post-mortem incident summary report
- Export to .pdf to share with external stakeholders



Automation





Search activities



- CORE
- AWS SERVICE
- ANSIBLE TOWER
- CISCO API CONSOLE
- CISCO DEFENSE ORCHESTRATOR
- CISCO DUO SECURITY
- CISCO ISE
- CISCO MERAKI
- CISCO ORBITAL
- CISCO PSIRT OPENVULN
- CISCO SECURE CLOUD ANALYTICS
- CISCO SECURE EMAIL
- CISCO SECURE ENDPOINT
- CISCO SECURE FIREWALL
- CISCO SECURE FIREWALL (SSE)
- CISCO SECURE MALWARE ANALYTICS
- CISCO SECURE NETWORK ANALYTICS
- richa senise



PROPERTIES

Umbrella - Search DNS Activity By ID

Version

Git Repository

Select

Git Version

No Versions Available

General

Display Name

Umbrella - Search DNS Activity by ID

Description

This workflow searches and returns Cisco Umbrella DNS activity for the last 7 days based on the Umbrella category provided. The data is then parsed and posted in a ServiceNow incident.

Target Group: Default TargetGroup

☐ Clean up after successful execution

If checked, the workflow run and any underlying task(s) will be deleted when the run succeeds. Failed runs will not be deleted.

☐ Is atomic workflow

An atomic workflow will be listed under the Activity Group header you select or create in the list to the left.

Group Name

Select

Category

Select

XDR Response Actions

Recovery

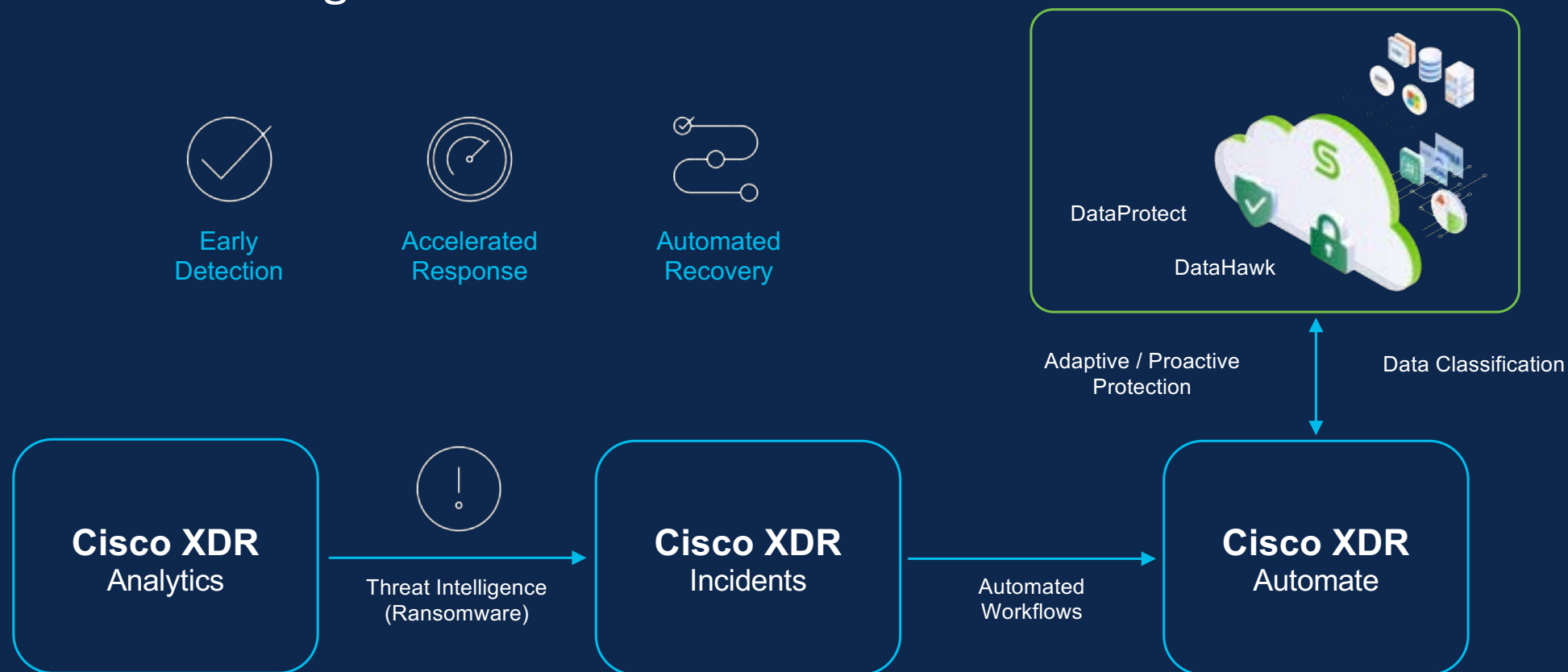
XDR+R



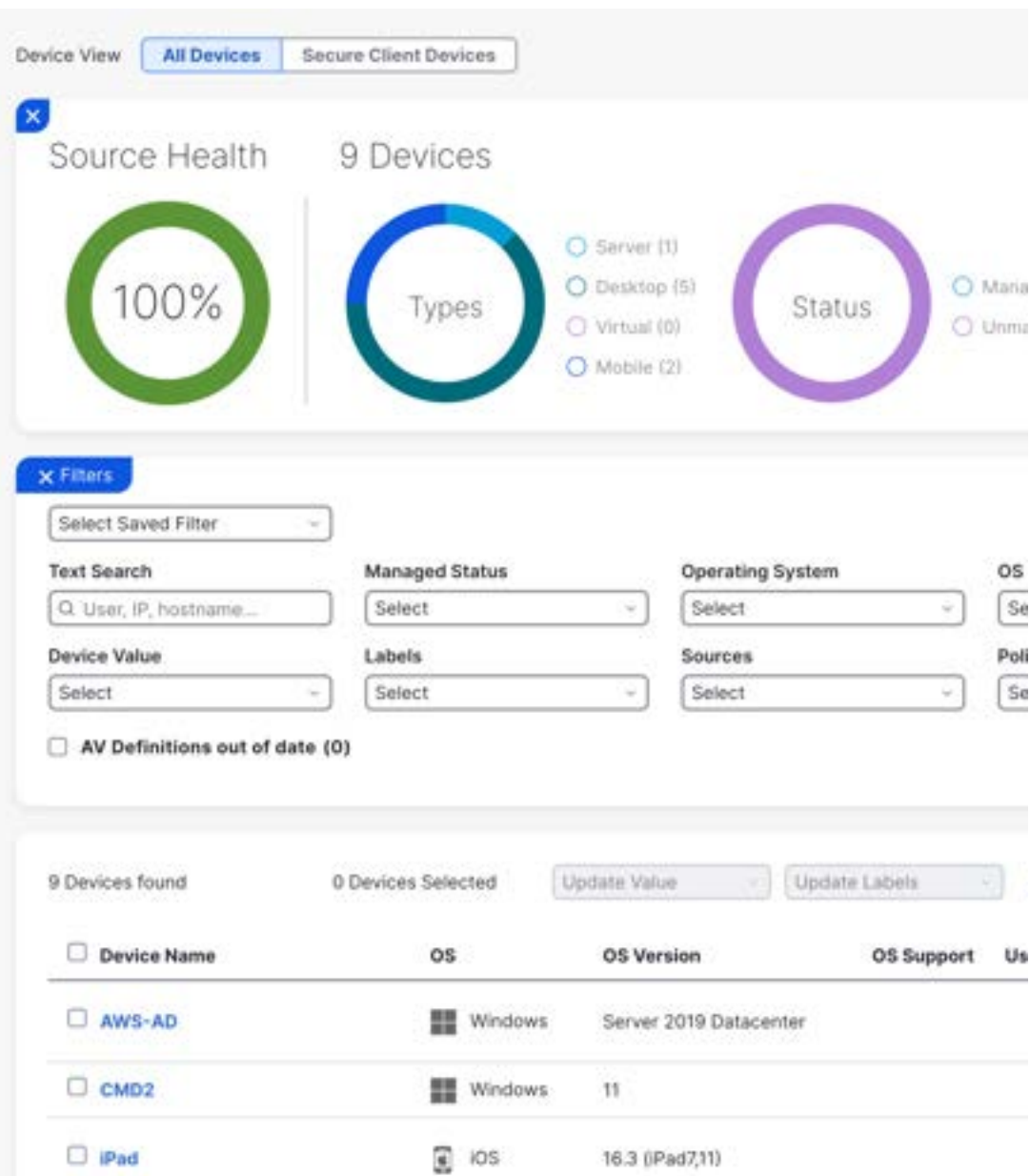
COHESITY



Full Cycle Automated Threat Response and Recovery* Cohesity and Cisco XDR Integration



Devices



Control Center

Incidents

Investigate

Intelligence

Automate

Devices

Inventory

Sources

Deployment

Audit Logs

Profiles

Device Events

Administration

Device View

All Devices

Secure Client Devices



Source Health

82 Devices



☐ Server (16)
☐ Desktop (13)
☐ Virtual (24)
☐ Mobile (0)



☐ Managed (51)
☐ Unmanaged (77)

OS



Filters

Select Saved Filter

Clear Filters

Save Filters

Text Search

Q User, IP, hostname...

Managed Status

Select

Operating System

Select

OS Support

Select

Type

Select

Device Value

Select

Labels

Select

Sources

Select

Policies

Select

☐ Has Faults (2)

☐ AV Definitions out of date (18)

82 Devices found

0 Devices Selected

Update Value

Update Labels

Edit Labels

Export to CSV

Edit Columns

<input type="checkbox"/> Device Name	OS	OS Version	OS Support	Users Seen	Sources	Managed	Compromised	Labels	Value
<input type="checkbox"/> c1-3850-1-g-0-13-centos	Centos	#1 SMP Tue Nov 8 15:48:59 UTC 2022		reboot, tme, runlevel	Secure Endpoint - ExplorCorp Orbital - ExplorCorp	No			10
		#76~20.04.1-Ubuntu SMP			Secure Endpoint -				

Control Center

Incidents

Investigate

Intelligence

Automate

Devices

Inventory

Sources

Deployment

Audit Logs

Profiles

Device Events

Administration

[← Back to Inventory](#)

c1-3850-2-g1-3-win10

Windows Microsoft Windows 10 Pro for Workstations 10.0.19044

Device Value: 10 (Default value) ▾

Managed: No

[+ Add Labels](#)[Refresh from Orbital Live Query](#)

Details

Associated Users [tme](#)
Last Active 2023-06-05T16:28:39.097Z
Location NA
Hostname c1-3850-2-g1-3-win10
Local IPs 10.90.12.13, fe80::bce4-39a9-7cbe-977e, 172.10.1.13, fe80::d506:e476:5561:5eb,
10.90.12.13
Public IPs 64.102.255.40, 64.102.255.47
Macs 00:50:56:be:24:56, 00:50:56:be:9f:d3
Hardware Id 9750dc6a-de03-4737-9b92-c617f44d23cc
Serial Number vmware-42 3e 94 4a f6 1f 5a bc-0a 62 45 ae 2b 0c dc dc

Cisco Secure Endpoint (AMP)

Definitions Definitions Up To Date
Isolation Not Isolated
Orbital Enabled

Connector GUID:
4267df87-8e6c-4fe6-aea6-86f49ebf8cea
[Open in Secure Endpoint](#)

Vulnerabilities

Vulnerabilities

Windows Security Center

Firewall

Enabled

Automatic Updates

Enabled

Control Center

Incidents

Investigate

Intelligence

Automate

Devices

Inventory

Sources

Deployment

Audit Logs

Profiles

Device Events

Administration

Vulnerabilities

Vulnerabilities

0

Windows Security Center

Firewall

Enabled

Automatic Updates

Enabled

AntiVirus

Enabled

AntiSpyware

Enabled

User Account Controls

Enabled

Installed Security Products



Windows Firewall
Firewall

Enabled
Up to Date



CrowdStrike Falcon Sensor
Antivirus

Enabled
Up to Date



Cisco Secure Endpoint
Antivirus

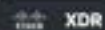
Enabled
Up to Date



Microsoft Defender Antivirus
Antivirus

Disabled
Up to Date

Seen in Sources





Cisco Secure Endpoint

Last Seen: 2023-06-04T19:58:26.000Z

Policy: Protect

Owner: Matt's Clients



Umbrella

Last Seen: 2023-06-05T05:49:53.000Z

Policy: Default Policy

Client Type: Browser

Client Version: 4.2.3

Control Center

Incidents

Investigate

Intelligence

Automate

Devices

Inventory

Sources

Deployment

Audit Logs

Profiles

Device Events

Administration



Microsoft Defender Antivirus
Antivirus

Disabled
Up to Date

Seen in Sources



Secure Endpoint -
ExplorCorp

Last Seen: 2023-06-04T19:58:26.000Z
 Policy: Protect
 Group: Mars Clients
 Install Date: 2022-11-08T19:39:21.000Z
 Connector: 8.1.7.21417
 Version:



Umbrella -
ExplorCorp

Last Seen: 2023-06-05T05:49:53.000Z
 Policy: Default Policy
 Client Type: Roaming Client Version: 5.2.3
 Reported OS: Windows Reported OS Version: 10
[Open Cisco Umbrella Dashboard in New Window](#)



Orbital - ExplorCorp

Last Seen: 2023-06-05T16:28:39.097Z
 Users: tme
 Local Users: Administrator, DefaultAccount, Guest, tme, WDAGUtilityAccount
 Computer SID: S-1-5-21-3025806627-2025052165-512010680
 Node OS: windows
 Version: v1.27.2
 Release: 10.0.19044
 Architecture: amd64



Secure Client

Last Seen: 2023-06-05T08:03:56.776Z
 Deployment: Secure Client Deployment ExplorCorp
 CSC Version: 5.0.02075
 Secure Endpoint: 8.1.7.21417
 Version:
 Cloud Management: 1.0.1.400
 Version:
 Modules: Cloud Management v.1.0.1.400
 Cisco Secure Endpoint v.8.1.7.21417
 AnyConnect VPN v.5.0.02075
 Umbrella v.5.0.02075
 DART v.5.0.02075
 Network Visibility Module v.5.0.02075
 CSC UDID: abcc5233-79ca-46eb-a299-9acc01d4325f
 AC UDID: 68cca45cda768ff468753ec52f80bc18428f
 b048

[Device Events](#)


XDR

- Control Center
- Incidents
- Investigate
- Intelligence
- Automate
- Devices
 - Inventory
 - Sources
 - Deployment
 - Audit Logs
 - Profiles
 - Device Events
- Administration

Deployment Management

+ Create New

Search

NVM to Direct XDR Deployment

Secure Client Deployment Explo...

Secure Client Deployment ExplorCorp

Edit Name

Delete

Save

Full Installer

Network Installer

Latest (1.0.1.400)

Cloud Management

Secure Client Cloud Management ExplorCorp

Latest (8.1.7.21417)

Secure Endpoint

Group: Protect

Replace Bootstrap Profile

Latest (5.0.2075.0)

AnyConnect VPN

Create Profile

Start Before Login

Umbrella

Umbrella ExplorCorp

Diagnostics and Reporting Tool

ISE Posture

Create Profile

Secure Firewall Posture

Network Access Manager

Create Profile

Network Visibility Module

NVM to Cloud Direct

Control Center

Incidents

Investigate

Intelligence

Automate

Devices

Inventory

Sources

Deployment

Audit Logs

Profiles

Device Events

Administration

← Profiles

Network Visibility Module Profiles

NVM to Cloud Direct

[Edit Name](#)

[Delete](#)

[Reset Changes](#)

[Cancel](#)

[Make A Copy](#)

[Save](#)

[Download](#)

Collector Configuration

Collector Type

Use Cisco Cloud Collector

[Configure](#)

Choose between On-Prem and Cloud Collector

Proxy IP Address / FQDN

Enter an IPv4/IPv6 address or FQDN

Proxy Port

Enter port number

Ping Interval (minutes)

Enter Ping interval in minutes. Valid range 1-180

Cache Configuration

☒ Max Size

☐ Max Duration


XDR

One more thing...

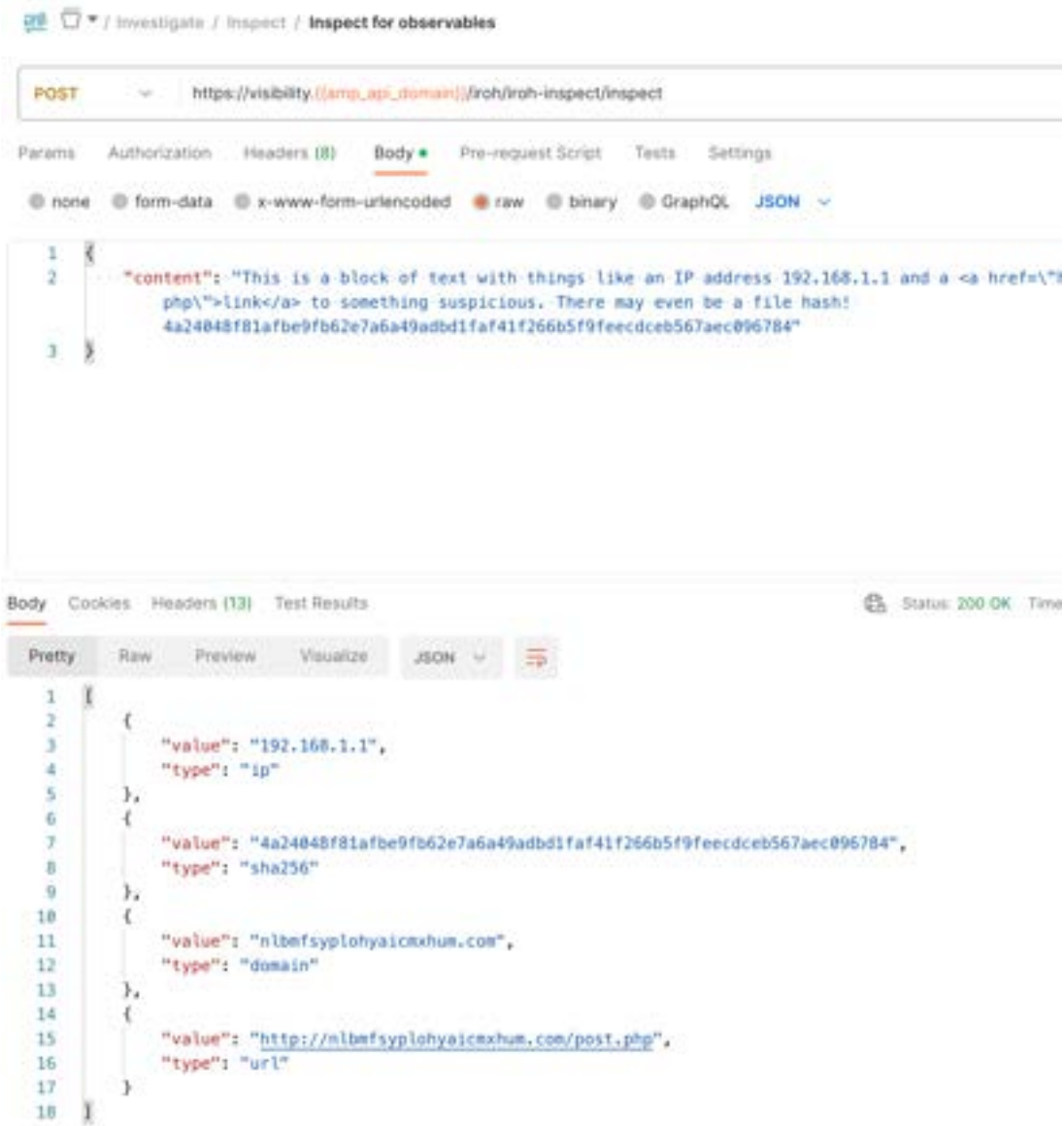


XDR has a robust set of APIs!

- We have APIs for:
 - Threat intelligence
 - Private and public databases of threat intel
 - Investigation
 - Inspect content for observables
 - Enrich data using your integrated products
 - Response
 - Act on observables you know to be dangerous
 - Automation
 - Trigger workflows in XDR to do just about anything you want

XDR Inspect API

- Takes an arbitrary block of text and extracts observables from it
- Simple and easy way to extract things to investigate from content like emails, blog posts, threat intel websites, and more...



Commercial



Easy to buy tiers for Cisco XDR

Cisco XDR Essentials

Full featured XDR

Native integration of the Cisco security portfolio enabling analysts to detect and respond to the most sophisticated threats, plus a repository for data ingest and retention

Cisco XDR Advantage

Cisco XDR ESS

+

Commercially supported and curated integrations with select third-party security solutions

Cisco XDR Premier

Cisco XDR Adv

+

Cisco Secure Managed Detection and Response MDR

+

Cisco Talos Incident Response

+

Cisco Technical Security Assessment

XDR Premier

Number of users licensed

of Hours

Available Services

100 - 499

Up
to 20 Hours

- Intel on demand: **5+ hrs**
- Breach Susceptibility Workshop: **5+ hrs**
- Organization Digital Footprint Assessment: **10+ hrs**

500 - 2.999

20-80 Hours

- All the above, plus:
- Emergency Incident Response: **40+ hrs**
 - Security Design Thinking Workshop: **20+ hrs**
 - Pen testing: **40+ hrs**
 - Threat Modelling: **40+ hrs**
 - Configuration and Build Review: **40+ hrs**
 - IR Plan: **50+ hrs**
 - IR Playbooks: **50+ hrs**
 - Tabletop Exercise: **50+ hrs**

3,000 - 9,999

80-160 Hours

- All the above, plus:
- Security Architecture Assessment: **80+ hrs**
 - IR Readiness Assessment: **80+ hrs**
 - Compromise Assessment: **80+ hrs**
 - Cyber Range: **80+ hrs**
 - Proactive Threat Hunting: **100+ hrs**

10,000 +

>160 Hours

- All the above, plus:
- Red Teaming: **160+ hrs**
 - Purple Teaming: **160+ hrs**
 - Security Operations Assessment: **160+ hrs**

Resources



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](#)
- <https://docs.xdr.security.cisco.com/Content/Administration/cisco-third-party-integrations-and-capabilities.htm>

Cisco XDR on Cisco.com



© 2023 Cisco and/or its affiliates. All rights reserved. Cisco





<https://cisco.com/go/xdr>

Děkuji za pozornost

Q & A

