CISCO
SECURE

CISCO The bridge to possible

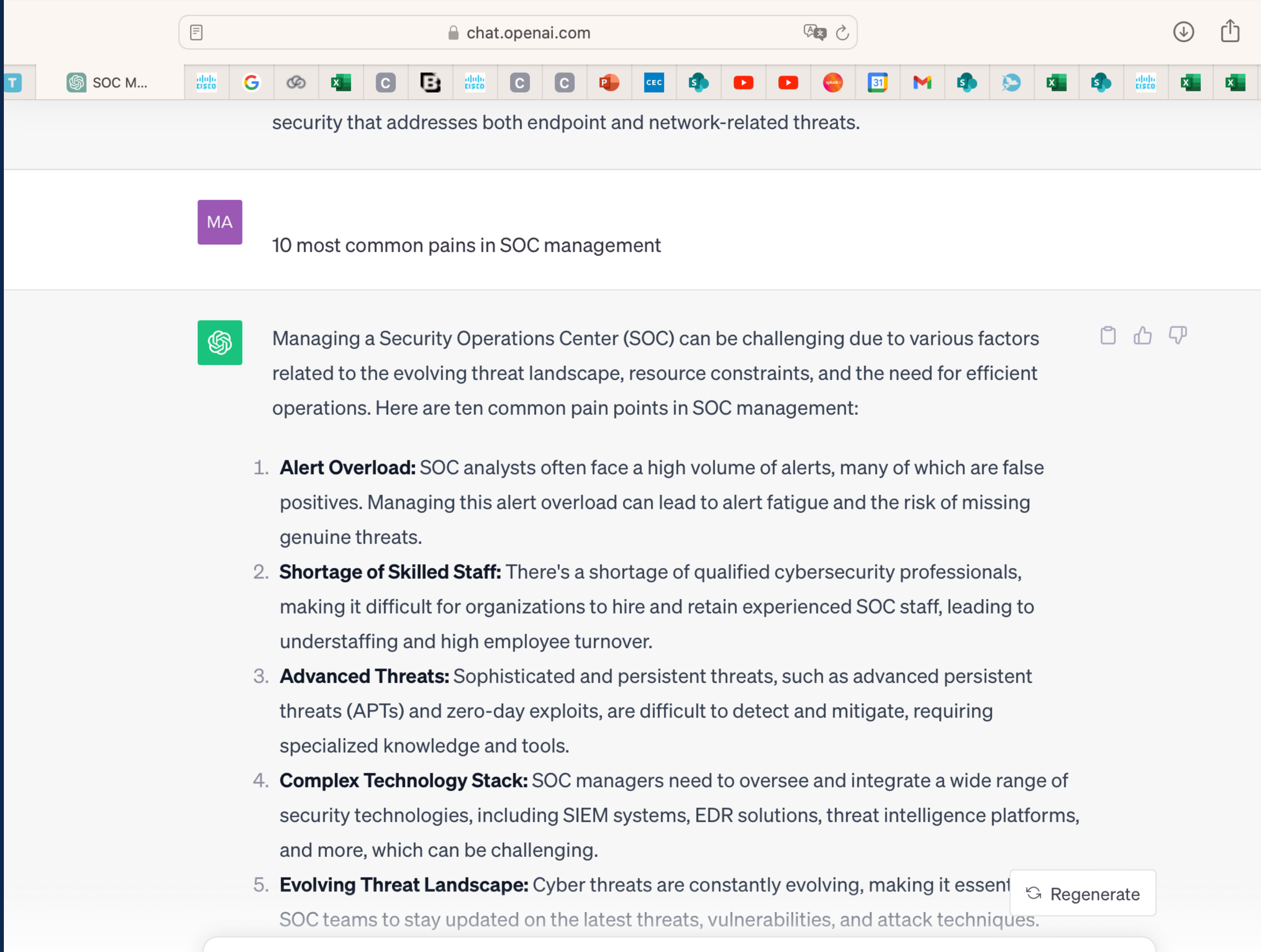
Cisco XDR

Tech Club

Jiří Tesař
TSA Security, jitesar@cisco.com
6.2.2024

SOC Management

Most common pains



security that addresses both endpoint and network-related threats.

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 essent SOC teams to stay updated on the latest threats, vulnerabilities, and attack techniques.

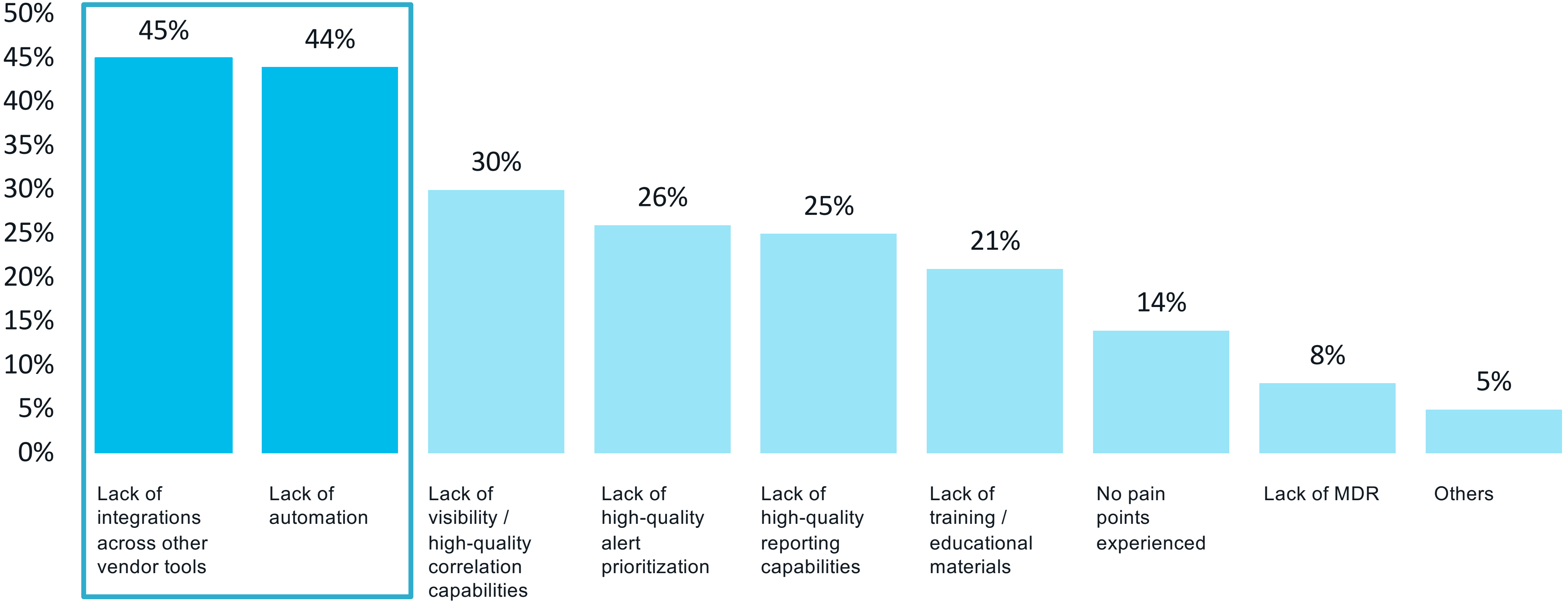
© 2023 Cisco and/or its affiliates. All rights reserved.

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**

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

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



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

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%

Cisco Secure Client

Cisco / Meraki (Networking)

Firewall Threat Defense (FTD)

Duo

Email Threat Defense (ETD)

Umbrella

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

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

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

IDC #US49731922 (September 2022)
Source: Future Enterprise Resiliency & Spending Survey - Wave 7, IDC, August 2022, n = 241; December 2021, n = 361

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

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

ANYTHING Detection and Response

EDR

ENDPOINT DETECTION AND RESPONSE

Endpoint installation agend needed.

NDR

NETWORK DETECTION AND RESPONSE

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

No agend needed

Behavioural analysis.

XDR

EXTENDED DETECTION AND RESPONSE

Correlation of different sources.

multi-vendor, cloud and on – premise.

Prioritztation of events based on business impact.

Automated response.

MDR

MANAGED DETECTION AND RESPONSE

Monitoring 24x7

Detection and Response Managed by vendor.

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

XDR vs SIEM

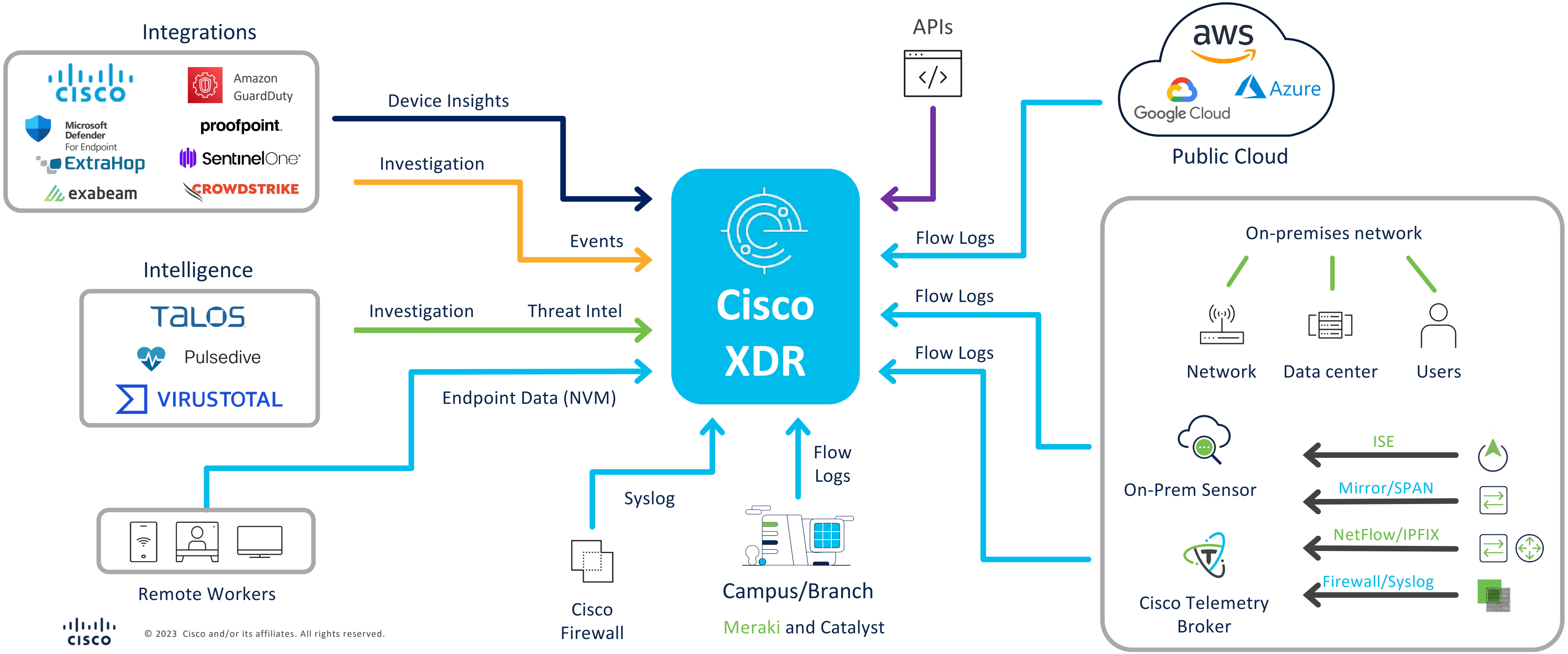
Key differences	SIEM	XDR
SCOPE OF DATA COLLECTION	collecting, analyzing, and correlating log and event data from a wide range of sources, such as firewalls, IDS/IPS, endpoints, and applications	goes beyond log and event data and also collects and analyzes endpoint data, network traffic, and cloud-based data in real time
DETECTION AND RESPONSE CAPABILITIES	Event correlation and reporting to generate alers	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.

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

Extended context

Telemetry sources for Cisco XDR

Flexible integration for existing infrastructure



Integrations

- Cisco
- Amazon GuardDuty
- Microsoft Defender For Endpoint
- proofpoint.
- ExtraHop
- SentinelOne
- exabeam
- CROWDSTRIKE

Device Insights

Investigation

Events

Intelligence

- TALOS
- Pulsedive
- VIRUSTOTAL

Investigation

Threat Intel

Endpoint Data (NVM)

Remote Workers

APIs

Cisco XDR

Flow Logs

Flow Logs

Flow Logs

Public Cloud

- aws
- Google Cloud
- Azure

On-premises network

- Network
- Data center
- Users

On-Prem Sensor

Cisco Telemetry Broker

ISE

Mirror/SPAN

NetFlow/IPFIX

Firewall/Syslog

Syslog

Cisco Firewall

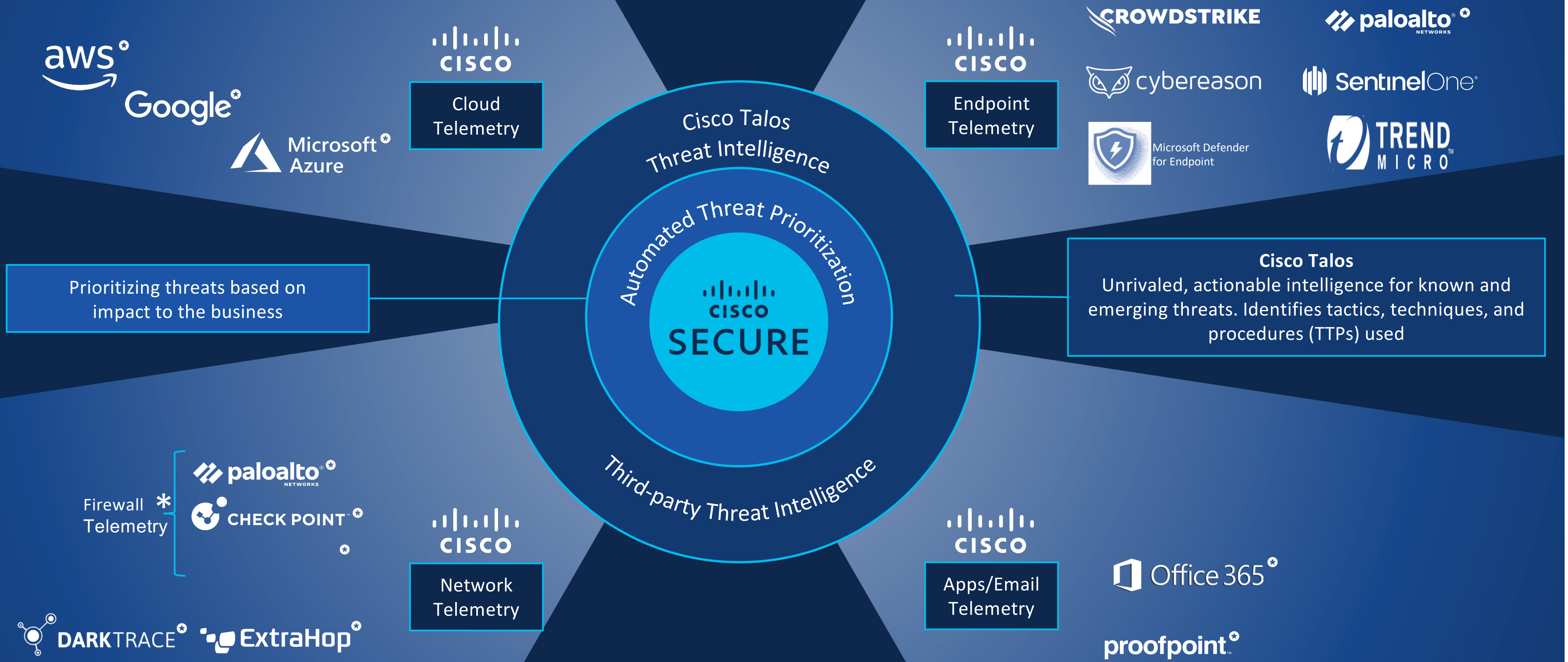
Flow Logs

Campus/Branch

Meraki and Catalyst

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

Strategic integrations to deliver customer outcomes



Cisco Talos Threat Intelligence

Automated Threat Prioritization

cisco SECURE

Third-party Threat Intelligence

Prioritizing threats based on impact to the business

Cisco Talos
Unrivaled, actionable intelligence for known and emerging threats. Identifies tactics, techniques, and procedures (TTPs) used

cisco Cloud Telemetry: aws ✪, Google ✪, Microsoft Azure ✪

cisco Endpoint Telemetry: CROWDSTRIKE, paloalto NETWORKS ✪, cybereason, SentinelOne, Microsoft Defender for Endpoint, TREND MICRO

cisco Network Telemetry: Firewall Telemetry * (paloalto NETWORKS ✪, CHECK POINT ✪, ✪), DARKTRACE ✪, ExtraHop ✪

cisco Apps/Email Telemetry: Office 365 ✪, proofpoint ✪

✪ Coming soon

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

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**

2 **Prioritize by Impact**

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**

4 **Accelerate Response**

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?

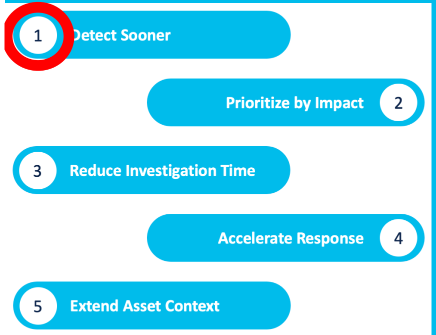
5 **Extend Asset Context**

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

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

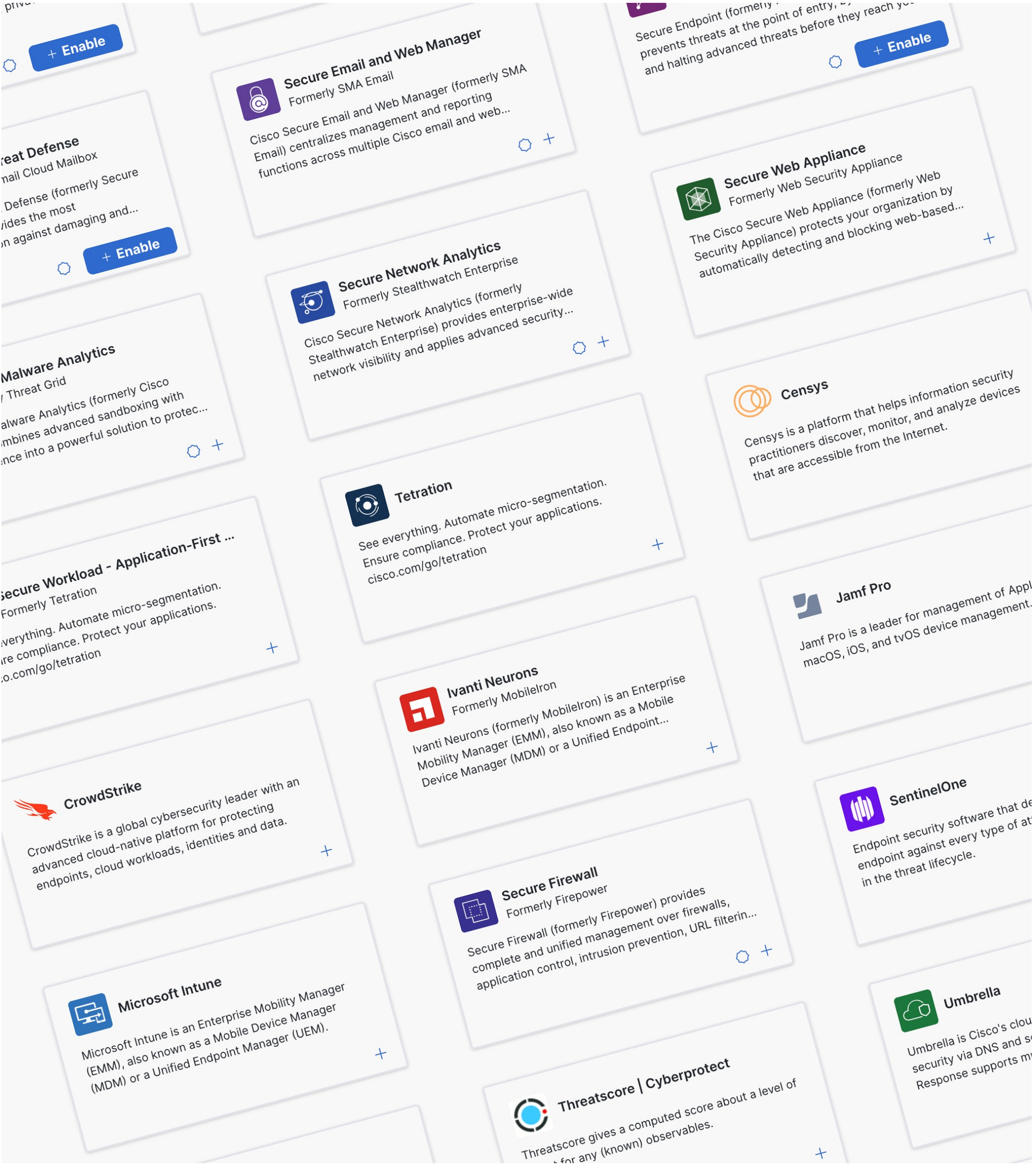

1 Detect Sooner

Prioritize by Impact 2

3 Reduce Investigation Time

Accelerate Response 4

5 Extend Asset Context


priva…

+ Enable

…reat Defense
…nail Cloud Mailbox
… Defense (formerly Secure
…vides the most
…n against damaging and...

+ Enable

…Malware Analytics
… Threat Grid
…alware Analytics (formerly Cisco
…mbines advanced sandboxing with
…nce into a powerful solution to protec...

…ecure Workload - Application-First ...
Formerly Tetration
…verything. Automate micro-segmentation.
…re compliance. Protect your applications.
…o.com/go/tetration

CrowdStrike
CrowdStrike is a global cybersecurity leader with an advanced cloud-native platform for protecting endpoints, cloud workloads, identities and data.

Microsoft Intune
Microsoft Intune is an Enterprise Mobility Manager (EMM), also known as a Mobile Device Manager (MDM) or a Unified Endpoint Manager (UEM).

Secure Email and Web Manager
Formerly SMA Email
Cisco Secure Email and Web Manager (formerly SMA Email) centralizes management and reporting functions across multiple Cisco email and web...

Secure Network Analytics
Formerly Stealthwatch Enterprise
Cisco Secure Network Analytics (formerly Stealthwatch Enterprise) provides enterprise-wide network visibility and applies advanced security...

Tetration
See everything. Automate micro-segmentation. Ensure compliance. Protect your applications. cisco.com/go/tetration

Ivanti Neurons
Formerly MobileIron
Ivanti Neurons (formerly MobileIron) is an Enterprise Mobility Manager (EMM), also known as a Mobile Device Manager (MDM) or a Unified Endpoint...

Secure Firewall
Formerly Firepower
Secure Firewall (formerly Firepower) provides complete and unified management over firewalls, application control, intrusion prevention, URL filterin...

Threatscore | Cyberprotect
Threatscore gives a computed score about a level of …t for any (known) observables.

Secure Endpoint (formerly … prevents threats at the point of entry, b… and halting advanced threats before they reach yo…

+ Enable

Secure Web Appliance
Formerly Web Security Appliance
The Cisco Secure Web Appliance (formerly Web Security Appliance) protects your organization by automatically detecting and blocking web-based...

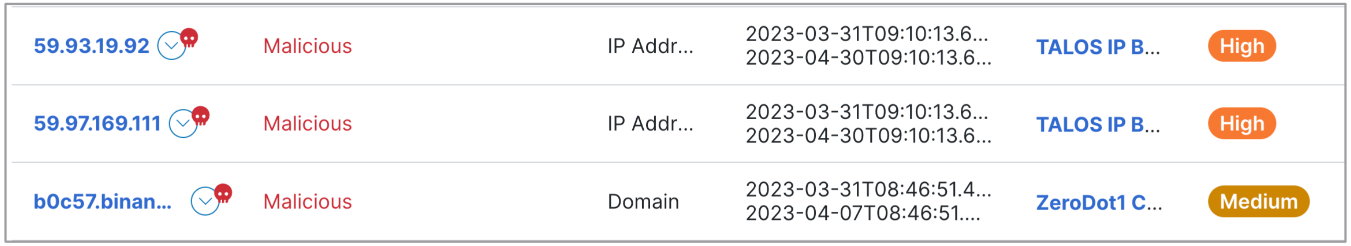
Censys
Censys is a platform that helps information security practitioners discover, monitor, and analyze devices that are accessible from the Internet.

Jamf Pro
Jamf Pro is a leader for management of Appl… macOS, iOS, and tvOS device management.

SentinelOne
Endpoint security software that de… endpoint against every type of at… in the threat lifecycle.

Umbrella
Umbrella is Cisco's clou… security via DNS and s… Response supports m…

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

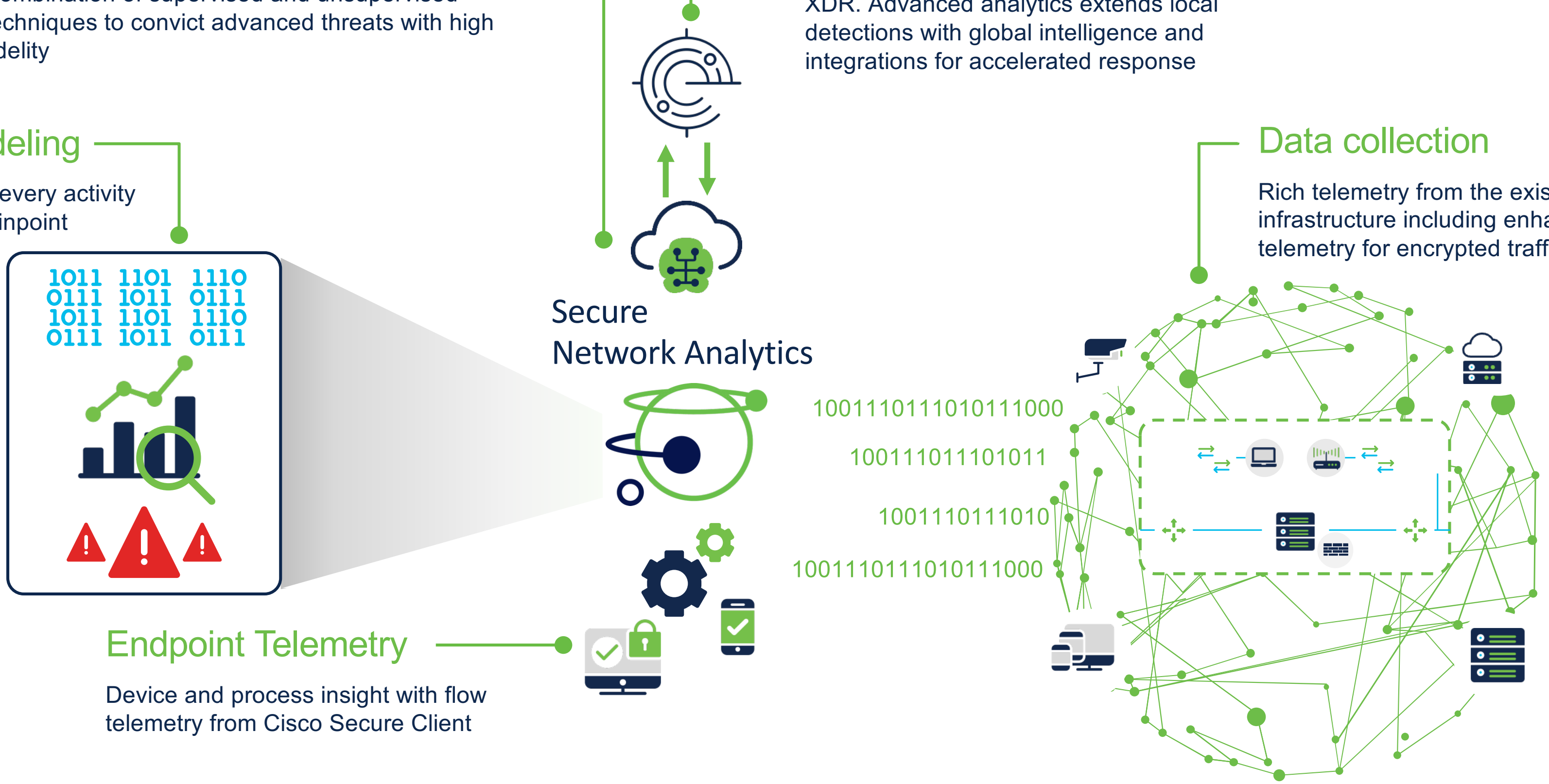
Indicators

Feeds

Events

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

Secure Network Analytics



Multilayered machine learning

Combination of supervised and unsupervised techniques to convict advanced threats with high fidelity

Behavioral modeling

Behavioral analysis of every activity within the network to pinpoint anomalies

Cisco XDR

Extended Detection and Response with Cisco XDR. Advanced analytics extends local detections with global intelligence and integrations for accelerated response

Data collection

Rich telemetry from the existing network infrastructure including enhanced telemetry for encrypted traffic analytics

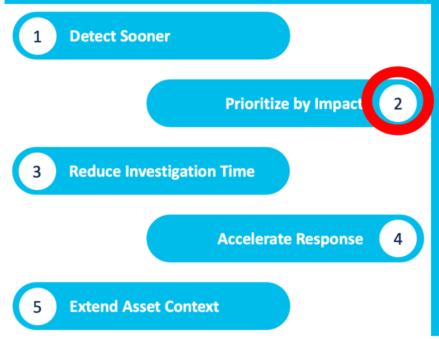
Endpoint Telemetry

Device and process insight with flow telemetry from Cisco Secure Client

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

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



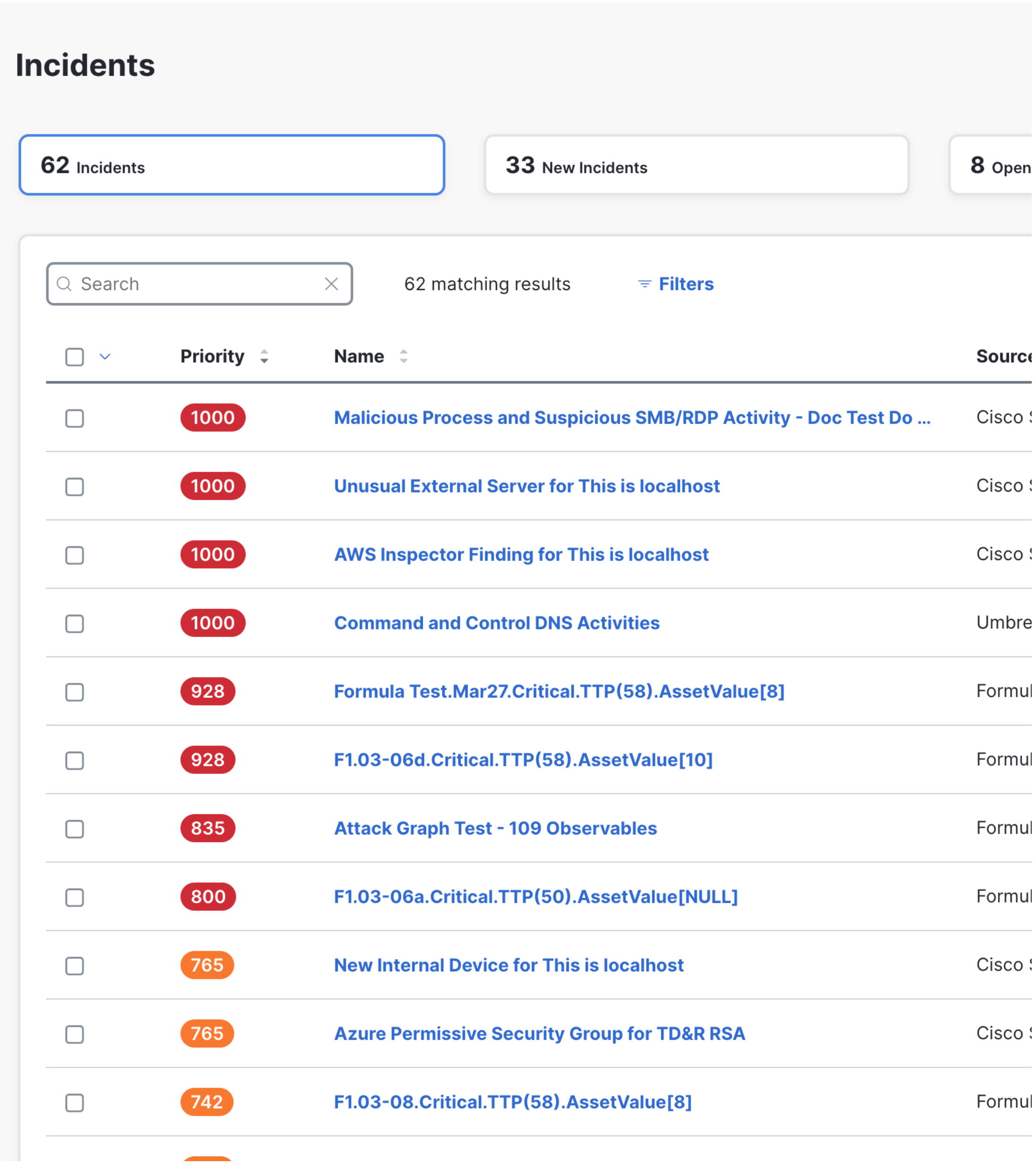
1 Detect Sooner

Prioritize by Impact 2

3 Reduce Investigation Time

Accelerate Response 4

5 Extend Asset Context



Incidents

62 Incidents

33 New Incidents

8 Open

Search

62 matching results

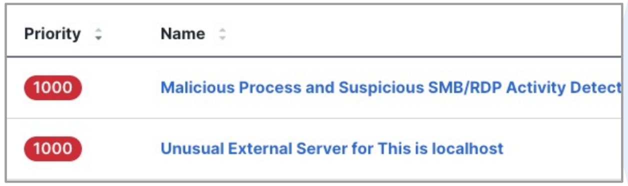
Filters

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

Walk through incidents step by step

Progressive disclosure

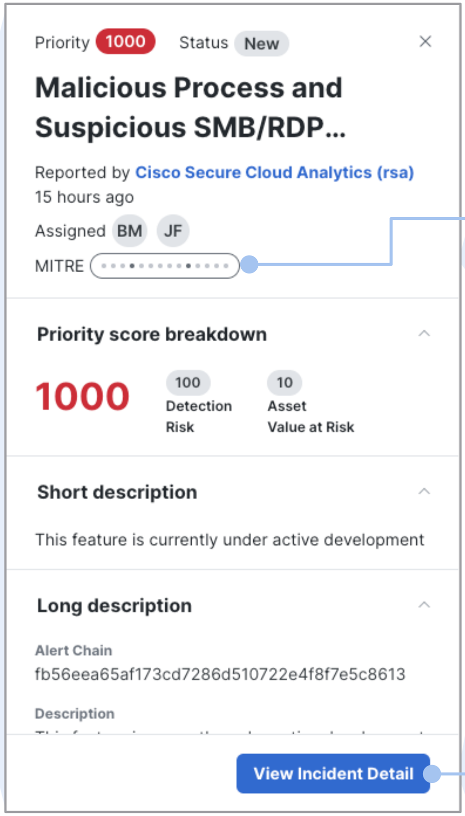
Looking into an incident is a progressive experience where the relevant data is revealed as needed without overwhelming the SOC analyst



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 BM JF

MITRE

Priority score breakdown

1000
100 Detection Risk
10 Asset Value at Risk

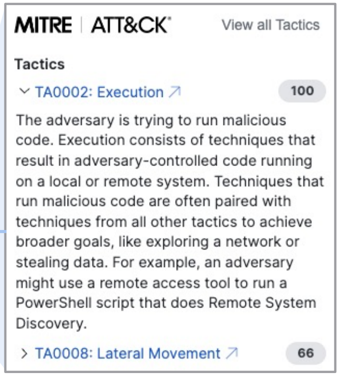
Short description

This feature is currently under active development

Long description

Alert Chain
fb56eea65af173cd7286d510722e4f8f7e5c8613

Description



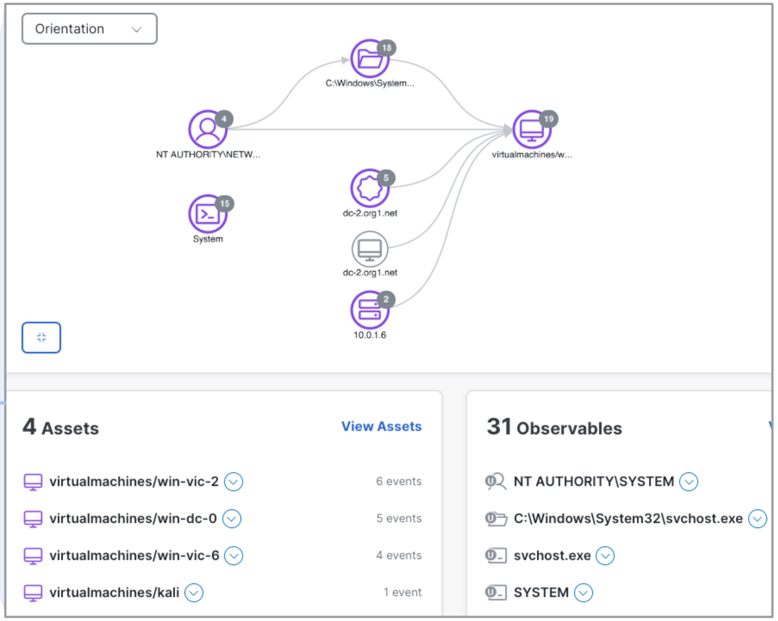
MITRE | ATT&CK View all Tactics

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



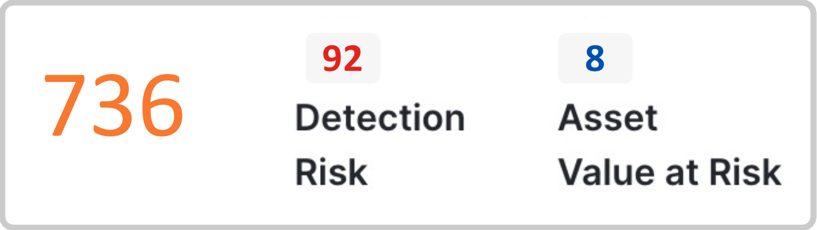
4 Assets View Assets

virtualmachines/win-vic-2	6 events
virtualmachines/win-dc-0	5 events
virtualmachines/win-vic-6	4 events
virtualmachines/kali	1 event

31 Observables

- NT AUTHORITY\SYSTEM
- C:\Windows\System32\svchost.exe
- svchost.exe
- SYSTEM

Identify the most impactful incidents based on risk



736

92 Detection Risk

8 Asset Value at Risk

Priority Score = Detection Risk x Asset Value

0-1000 | 0-100 | 0-10

The Incident total priority score used to prioritize incidents

Detection Risk composed of multiple values:

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

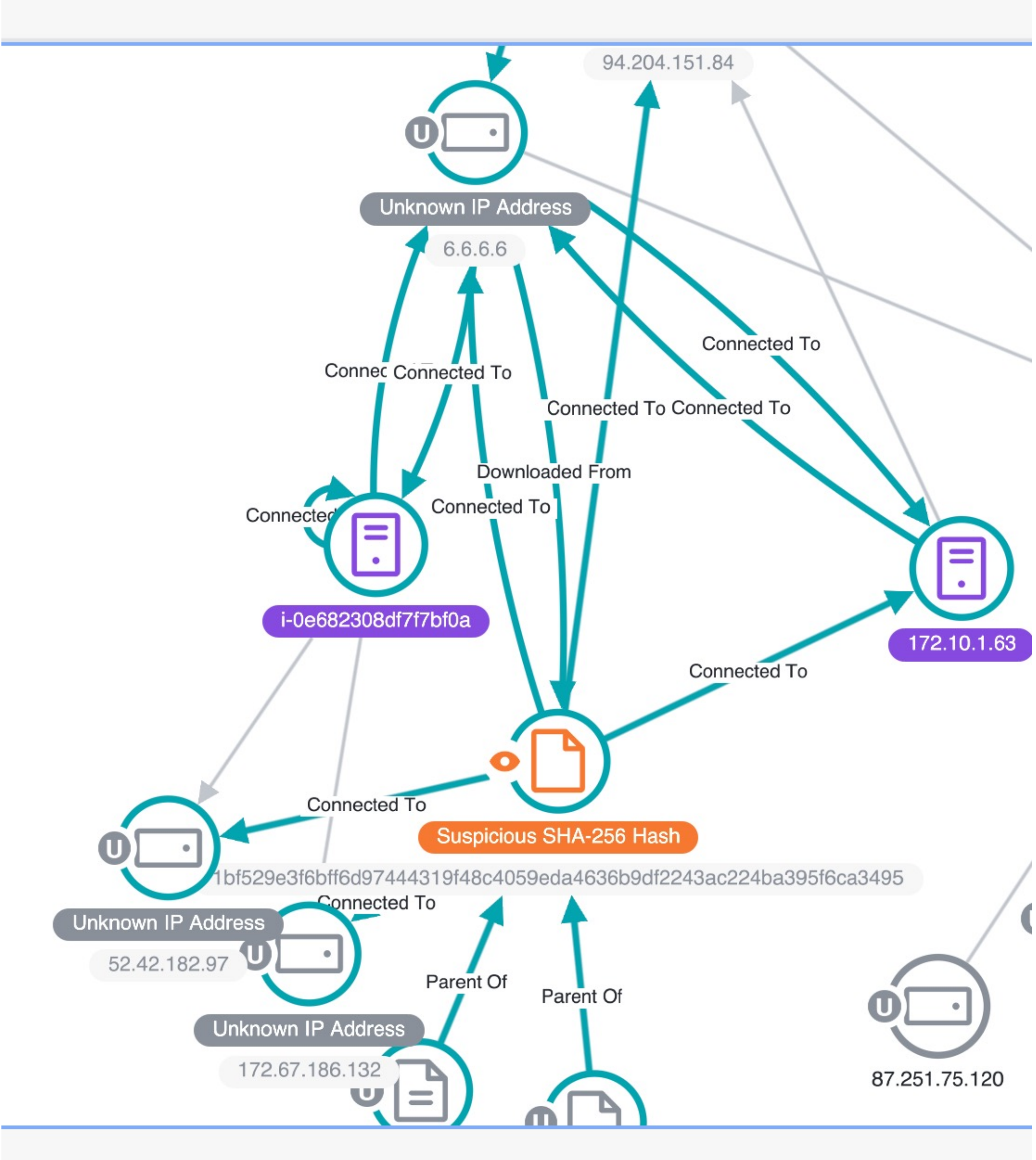
User Defined Asset Value represent the value of the asset involved in the incident

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

3) Reduce investigation time

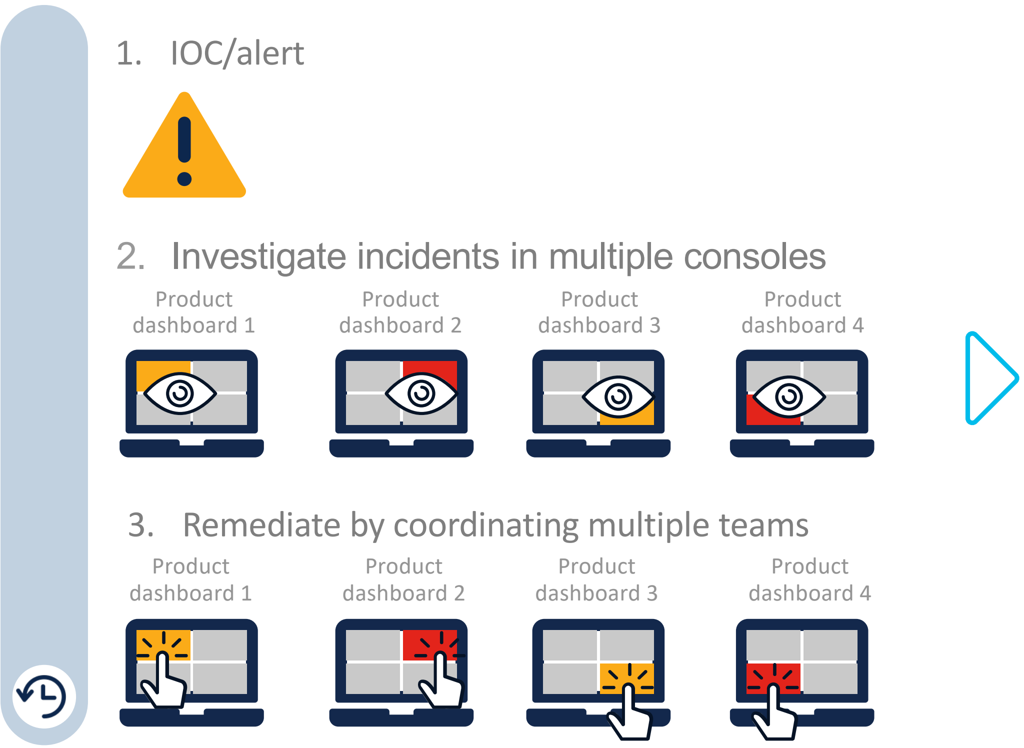
- Interactive, visual representations of incidents
- Event correlation and attack chaining to group related intelligence
- Automated enrichment for the most critical incidents, ensuring intelligence is gathered immediately

1 Detect Sooner
Prioritize by Impact 2
3 Reduce Investigation Time
Accelerate Response 4
5 Extend Asset Context



How true simplicity is experienced

Without XDR: 32 minutes

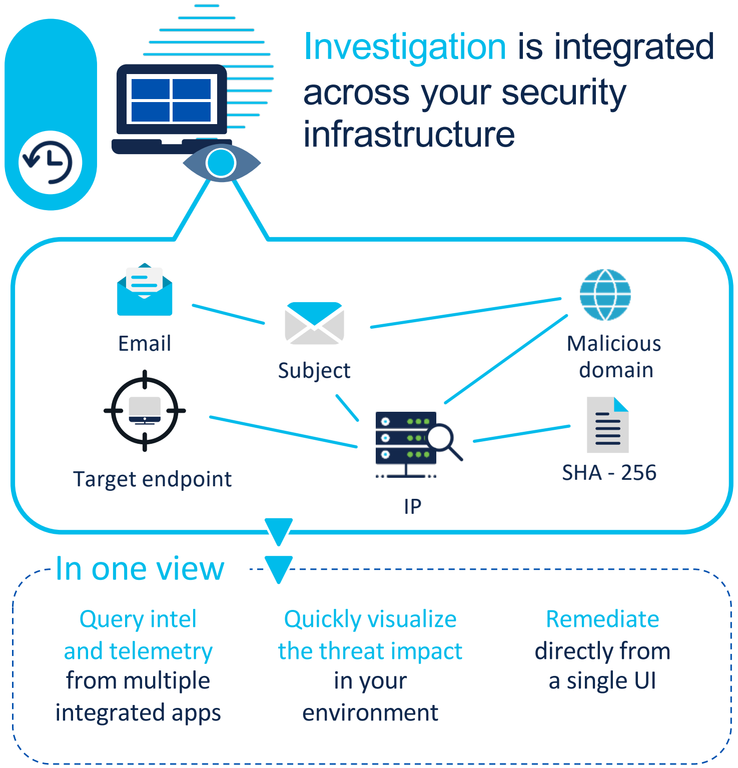


1. IOC/alert

2. Investigate incidents in multiple consoles

3. Remediate by coordinating multiple teams

With XDR: five minutes



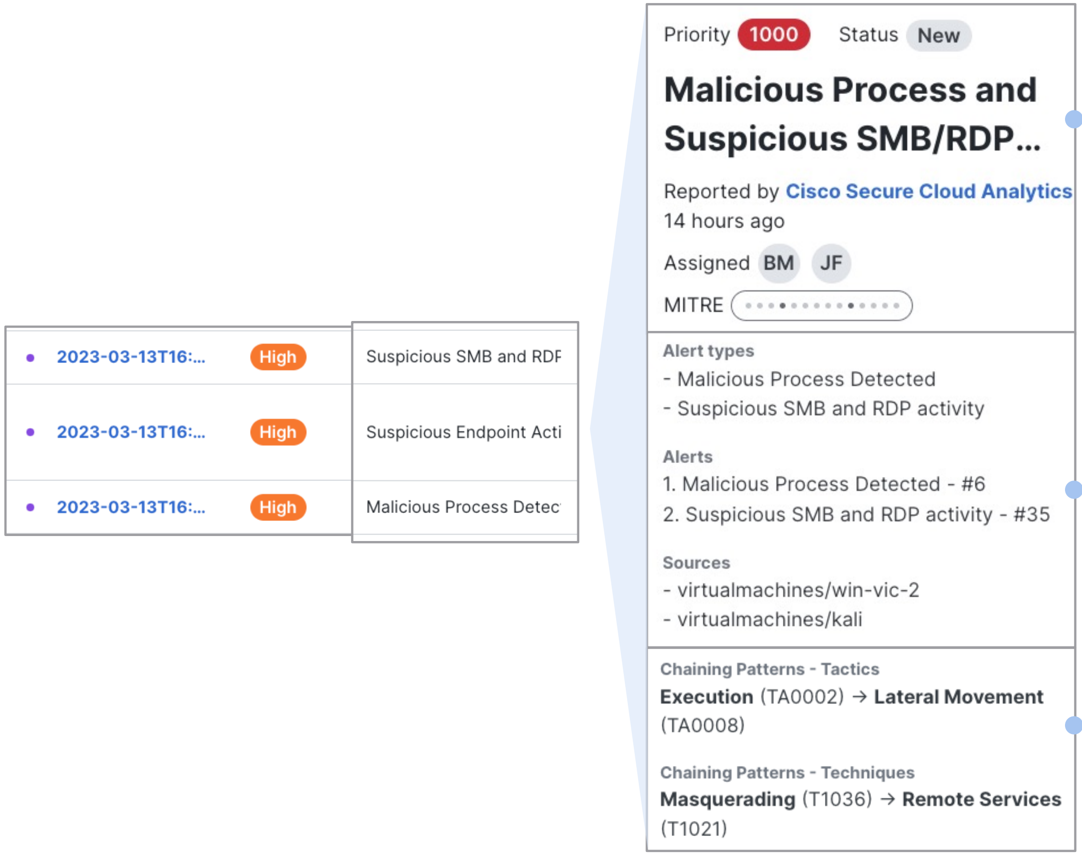
Investigation is integrated across your security infrastructure

In one view

- Query intel and telemetry from multiple integrated apps
- Quickly visualize the threat impact in your environment
- Remediate directly from a single UI

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

Confirm attacks sooner with alert correlation



•	2023-03-13T16:...	High	Suspicious SMB and RDF
•	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

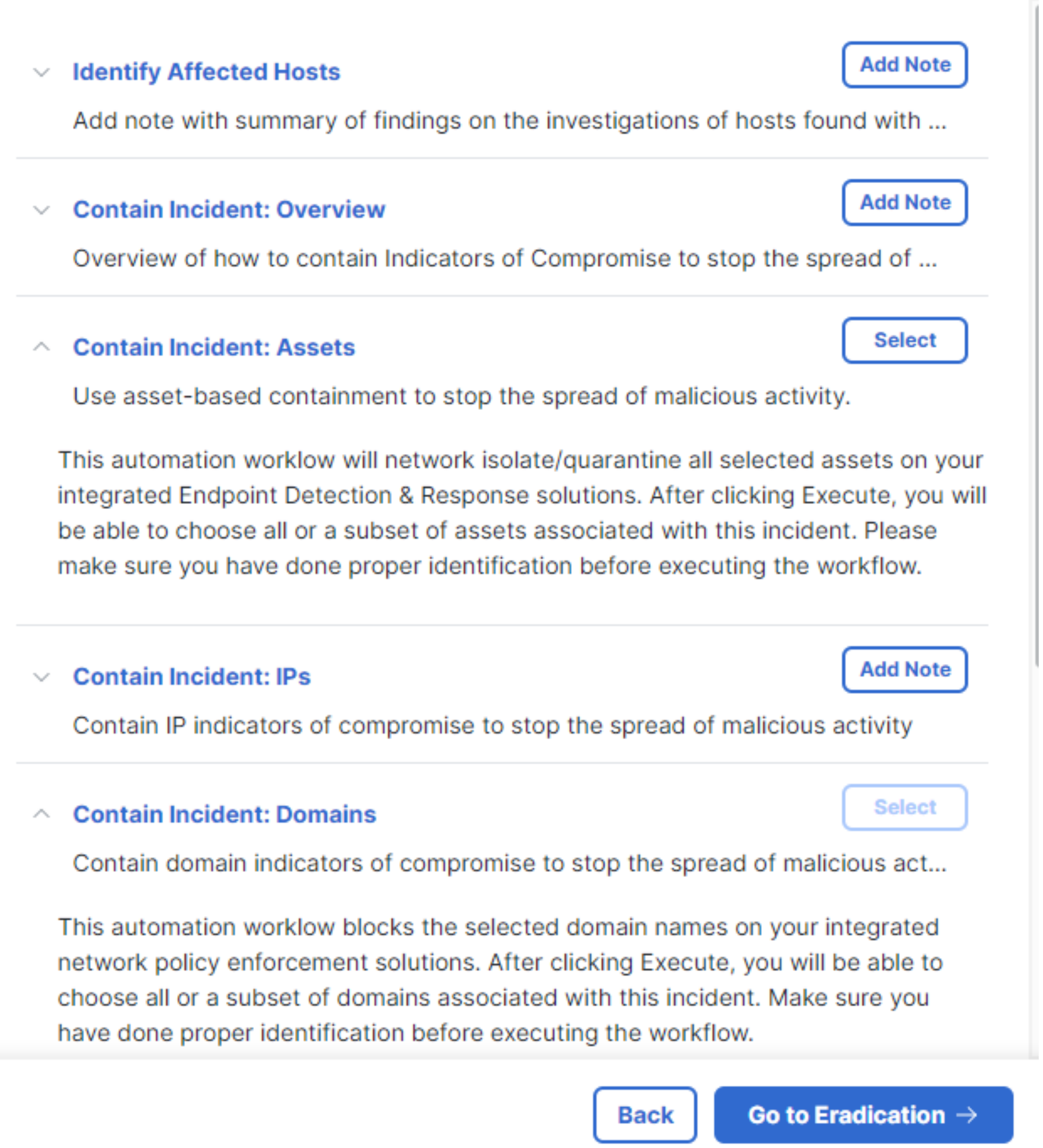
Using MITRE Tactics and Techniques to connect and revealing the attack chain

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

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

1 Detect Sooner
Prioritize by Impact 2
3 Reduce Investigation Time
Accelerate Response 4
5 Extend Asset Context



Identify Affected Hosts

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

Contain Incident: Overview

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

Contain Incident: Assets

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

This automation worklow 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

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

Contain Incident: Domains

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

This automation worklow 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.

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

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

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

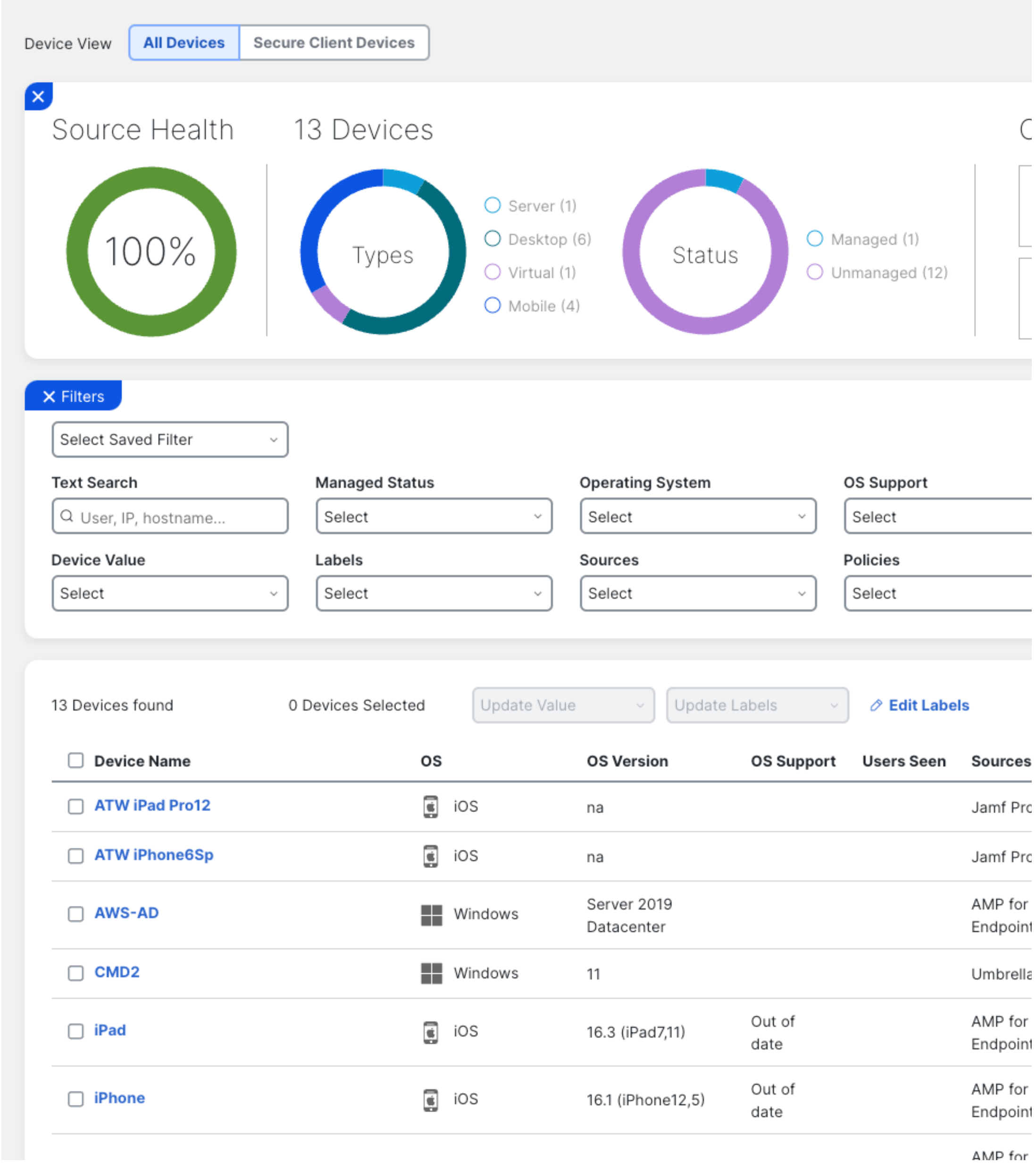
1 Detect Sooner

Prioritize by Impact 2

3 Reduce Investigation Time

Accelerate Response 4

5 Extend Asset Context



Device View **All Devices** Secure Client Devices

Source Health 100%

13 Devices

Types
○ Server (1)
○ Desktop (6)
○ Virtual (1)
○ Mobile (4)

Status
○ Managed (1)
○ Unmanaged (12)

✕ Filters

Select Saved Filter

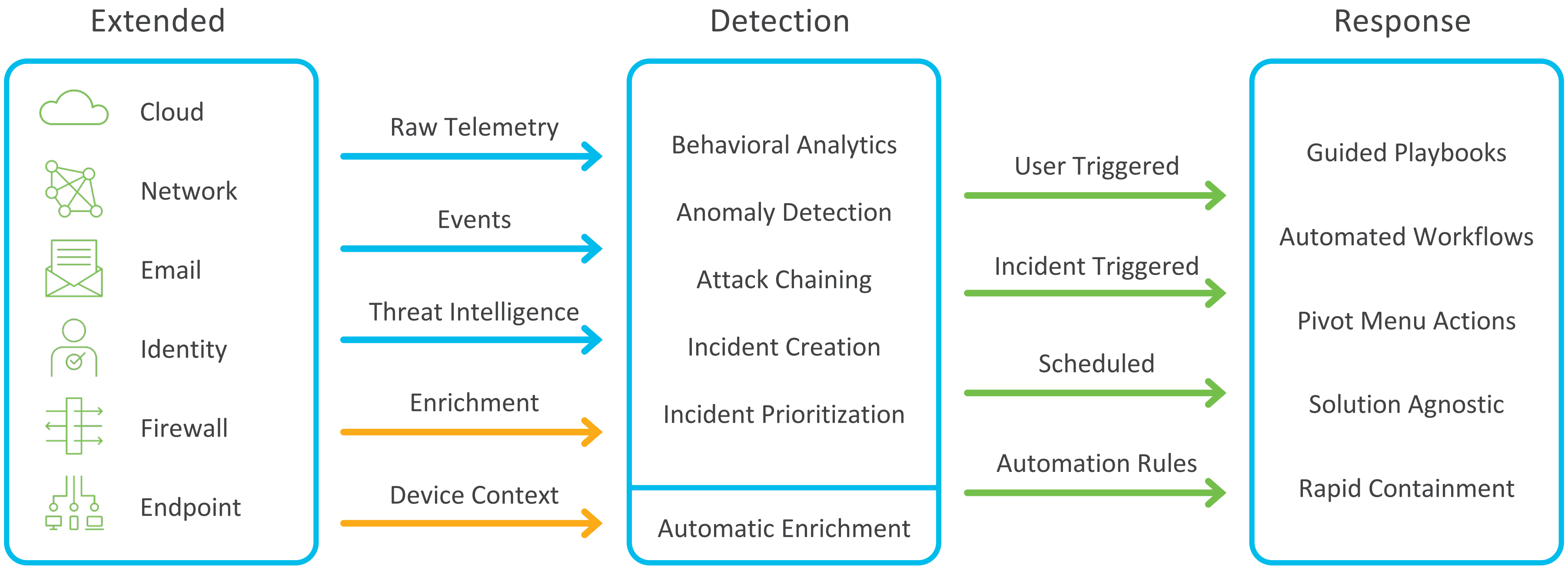
Text Search: User, IP, hostname...
Managed Status: Select
Operating System: Select
OS Support: Select
Device Value: Select
Labels: Select
Sources: Select
Policies: Select

13 Devices found   0 Devices Selected   Update Value   Update Labels   Edit Labels

☐ Device Name	OS	OS Version	OS Support	Users Seen	Sources
☐ ATW iPad Pro12	iOS	na			Jamf Pr
☐ ATW iPhone6Sp	iOS	na			Jamf Pr
☐ AWS-AD	Windows	Server 2019 Datacenter			AMP for Endpoint
☐ CMD2	Windows	11			Umbrella
☐ iPad	iOS	16.3 (iPad7,11)	Out of date		AMP for Endpoint
☐ iPhone	iOS	16.1 (iPhone12,5)	Out of date		AMP for Endpoint
					AMP for

Features

High level architecture



Extended

- Cloud
- Network
- Email
- Identity
- Firewall
- Endpoint

Raw Telemetry

Events

Threat Intelligence

Enrichment

Device Context

Detection

- Behavioral Analytics
- Anomaly Detection
- Attack Chaining
- Incident Creation
- Incident Prioritization

Automatic Enrichment

User Triggered

Incident Triggered

Scheduled

Automation Rules

Response

- Guided Playbooks
- Automated Workflows
- Pivot Menu Actions
- Solution Agnostic
- Rapid Containment

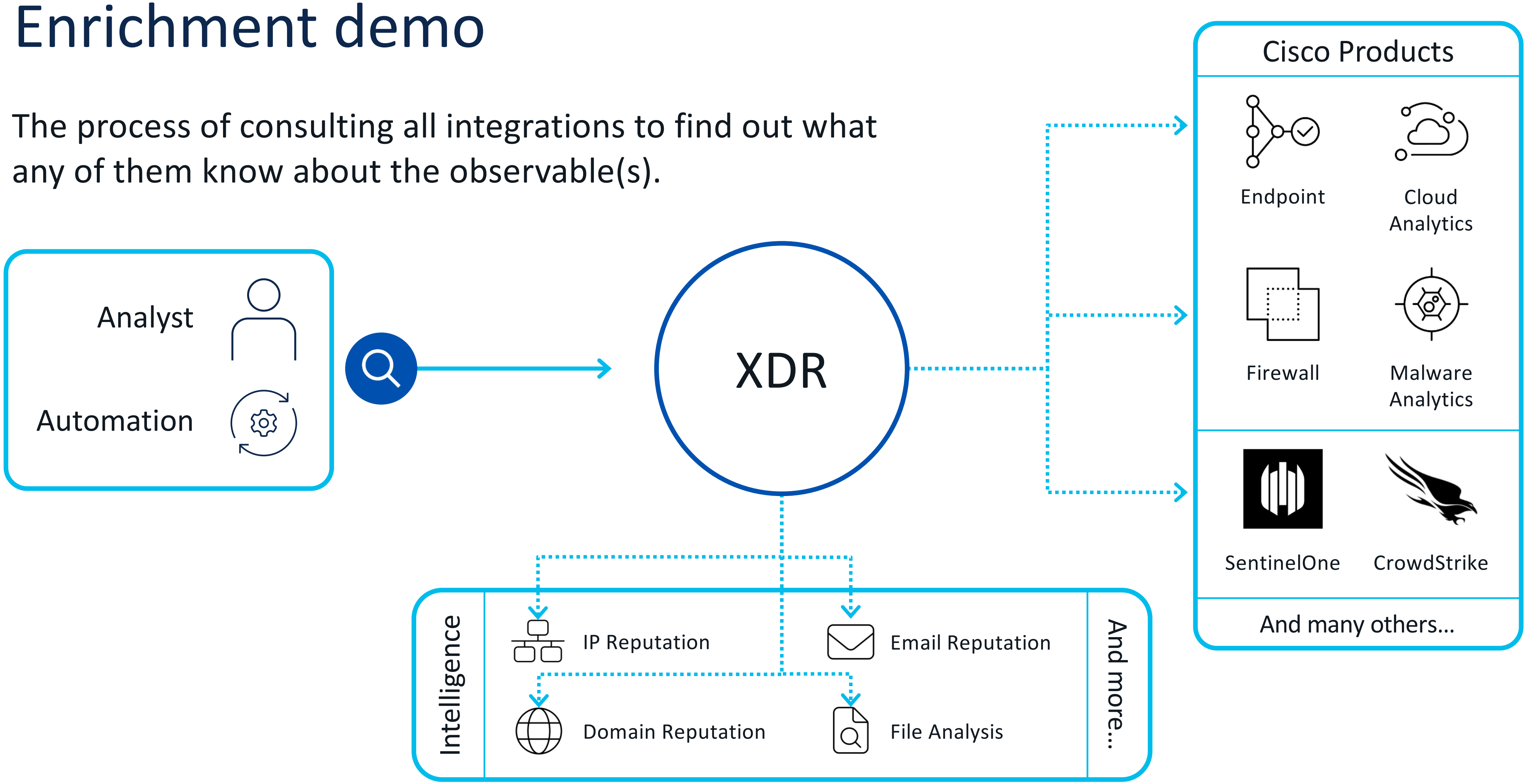
Multi-vector telemetry ingest network, cloud, endpoint, email, and more from Cisco and 3rd party

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).



Analyst

Automation

XDR

Cisco Products

Endpoint

Cloud Analytics

Firewall

Malware Analytics

SentinelOne

CrowdStrike

And many others...

Intelligence

IP Reputation

Email Reputation

Domain Reputation

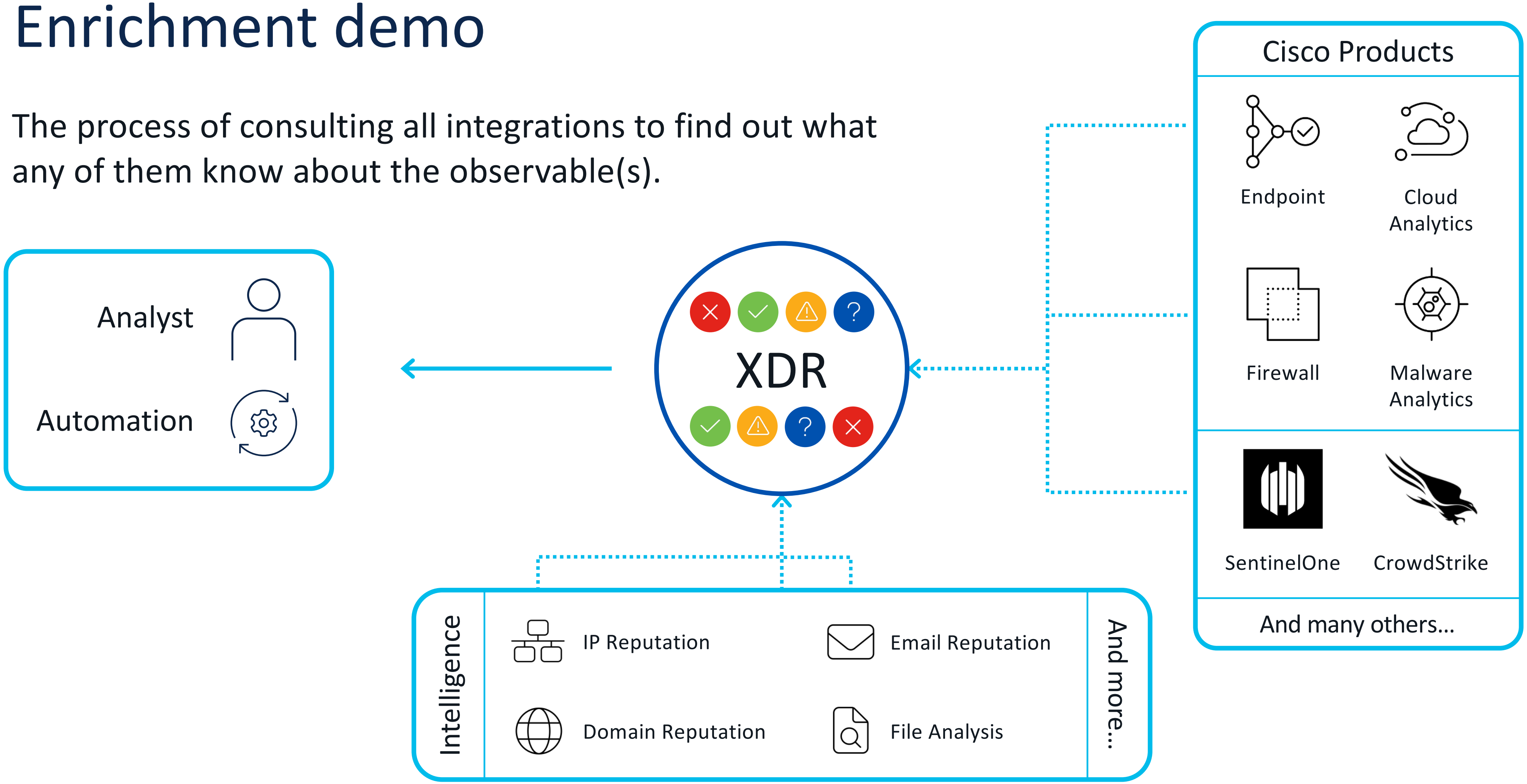
File Analysis

And more...

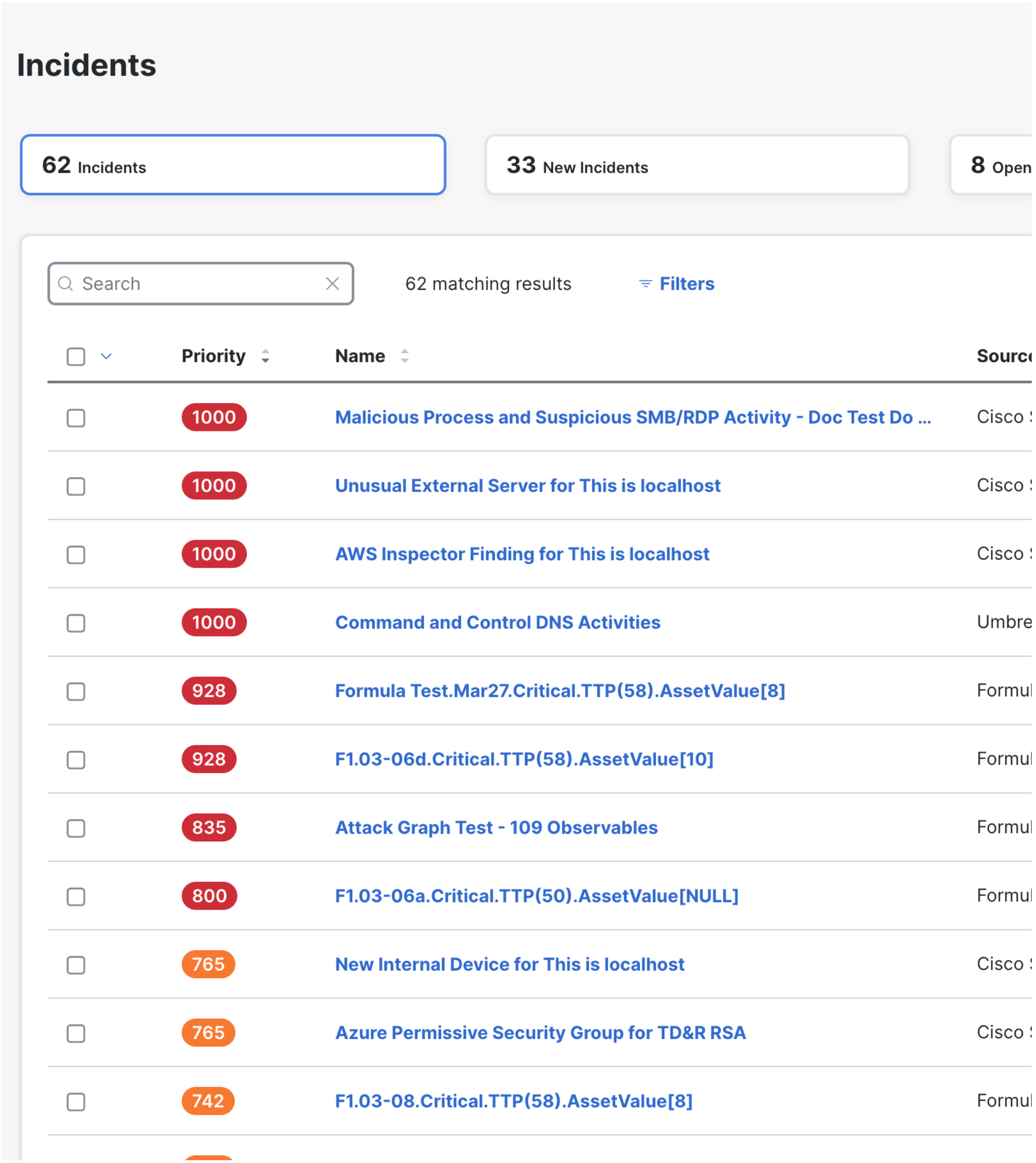
© 2023 Cisco and/or its affiliates. All rights reserved. Cisco Public

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

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

Incident response in four stages

Identify

Review the incident and confirm the findings

Contain

Act against impacted hosts, domains, files, etc.

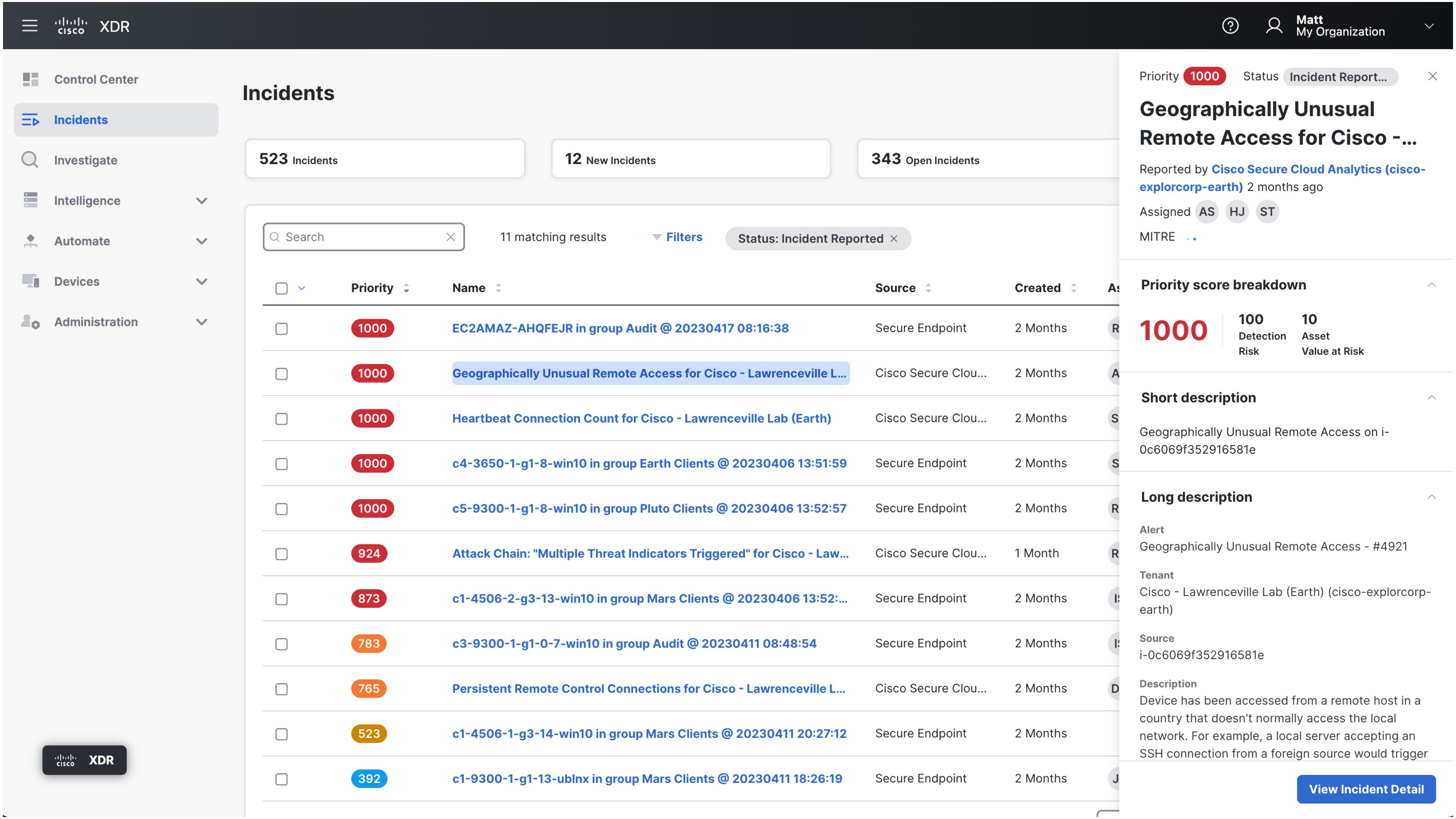
Eradicate

Remediate vulnerabilities and remove malicious content

Recover

Validate remediation and restore impacted services

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



Incidents

523 Incidents

12 New Incidents

343 Open Incidents

Search

11 matching results

Filters

Status: Incident Reported ×

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

10 Asset Value at Risk

Short description

Geographically Unusual Remote Access on i-0c6069f352916581e

Long description

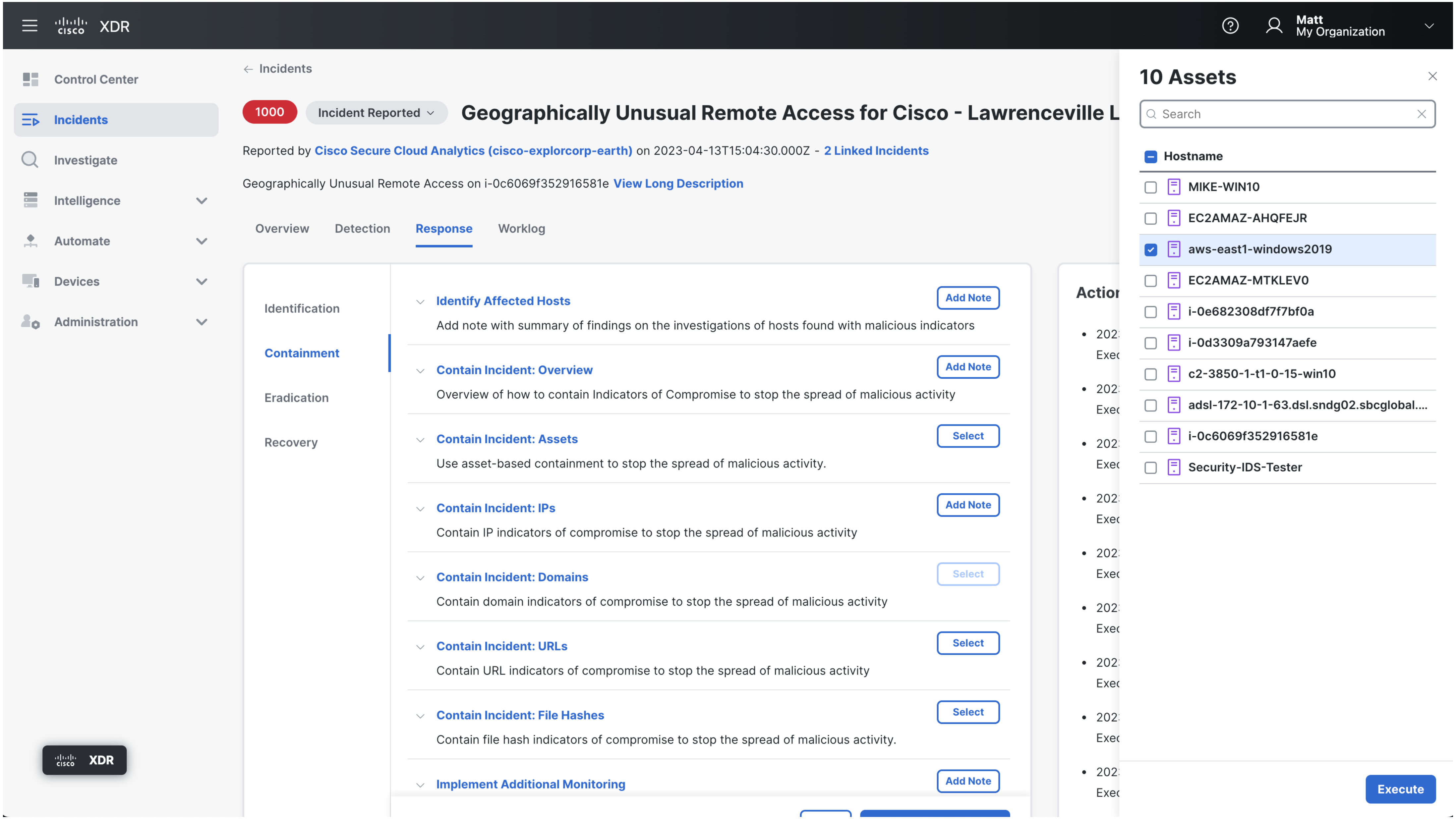
Alert
Geographically Unusual Remote Access - #4921

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

Source
i-0c6069f352916581e

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



← 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

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

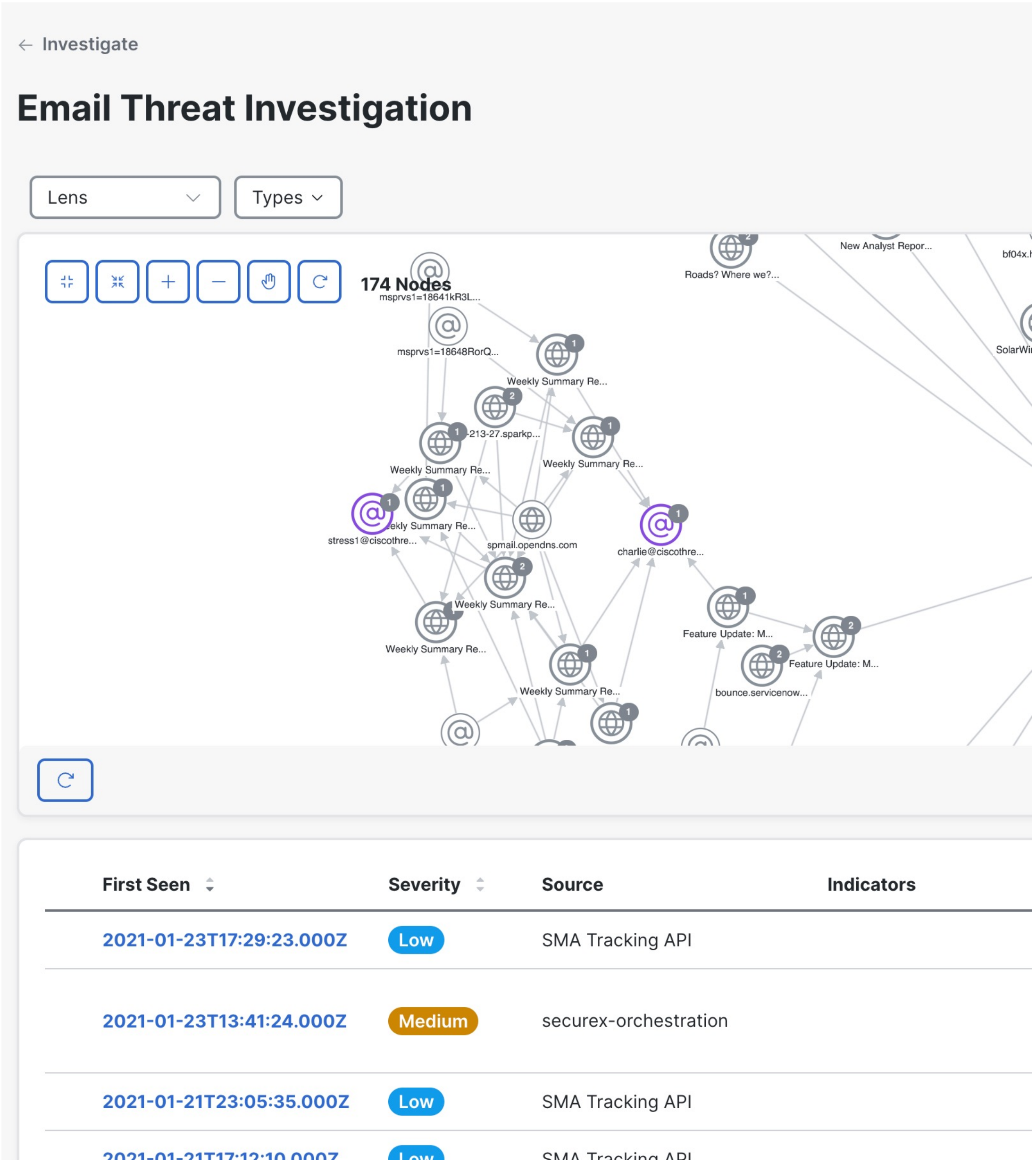
10 Assets

Search

Hostname
☐ MIKE-WIN10
☐ EC2AMAZ-AHQFEJR
☑ aws-east1-windows2019
☐ EC2AMAZ-MTKLEV0
☐ i-0e682308df7f7bf0a
☐ i-0d3309a793147aefe
☐ c2-3850-1-t1-0-15-win10
☐ adsl-172-10-1-63.dsl.sndg02.sbcglobal....
☐ i-0c6069f352916581e
☐ Security-IDS-Tester

Execute

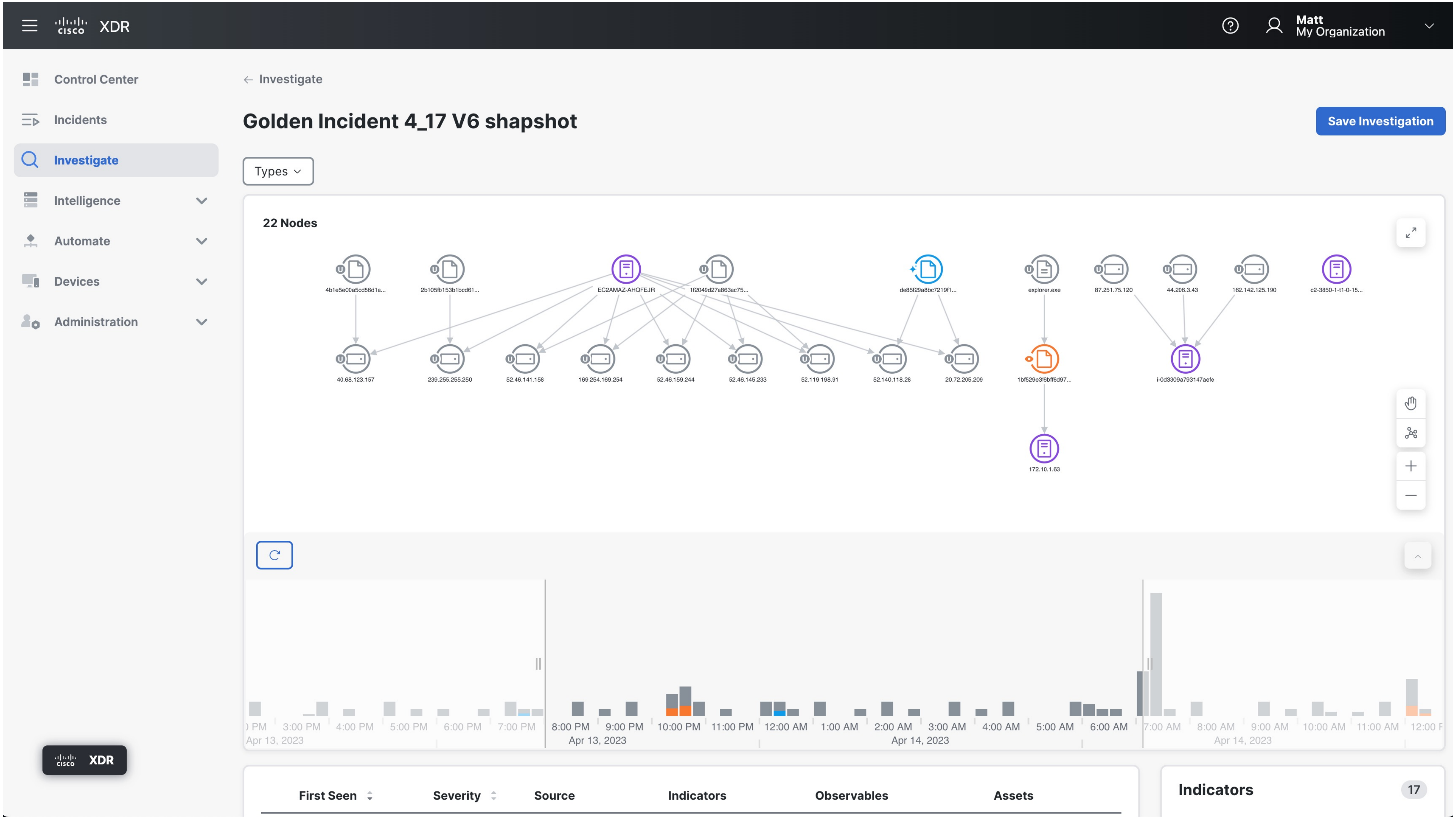
Investigate

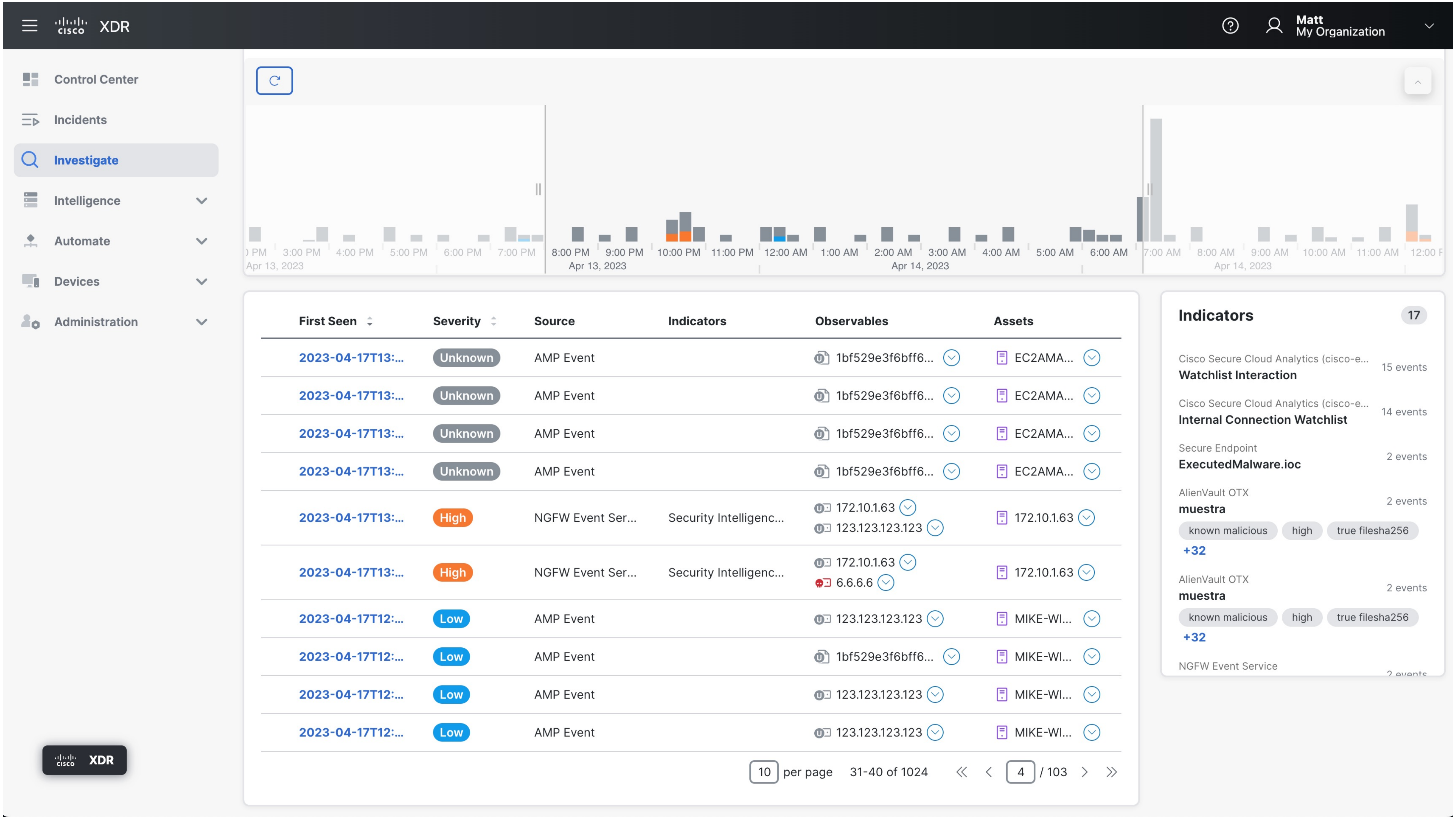


← Investigate

Email Threat Investigation

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	


XDR
Matt
My Organization
Control Center
Incidents
Investigate
Intelligence
Automate
Devices
Administration
Investigate
Golden Incident 4_17 V6 shapshot
Save Investigation
Types
22 Nodes
4b1e5e00a5cd56d1a...
2b105fb153b1bcd61...
EC2AMAZ-AHQFEJR
1f2049d27a863ac75...
de85f29a8bc7219f1...
explorer.exe
87.251.75.120
44.206.3.43
162.142.125.190
c2-3850-1-t1-0-15...
40.68.123.157
239.255.255.250
52.46.141.158
169.254.169.254
52.46.159.244
52.46.145.233
52.119.198.91
52.140.118.28
20.72.205.209
1bf529e3f6bff6d97...
i-0d3309a793147aefe
172.10.1.63
PM
3:00 PM
4:00 PM
5:00 PM
6:00 PM
7:00 PM
8:00 PM
9:00 PM
10:00 PM
11:00 PM
12:00 AM
1:00 AM
2:00 AM
3:00 AM
4:00 AM
5:00 AM
6:00 AM
7:00 AM
8:00 AM
9:00 AM
10:00 AM
11:00 AM
12:00
Apr 13, 2023
Apr 13, 2023
Apr 14, 2023
Apr 14, 2023
First Seen
Severity
Source
Indicators
Observables
Assets
Indicators
17
XDR



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-WI...
2023-04-17T12:...	Low	AMP Event		1bf529e3f6bff6...	MIKE-WI...
2023-04-17T12:...	Low	AMP Event		123.123.123.123	MIKE-WI...
2023-04-17T12:...	Low	AMP Event		123.123.123.123	MIKE-WI...

10 per page 31-40 of 1024 4 / 103

Indicators 17

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

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

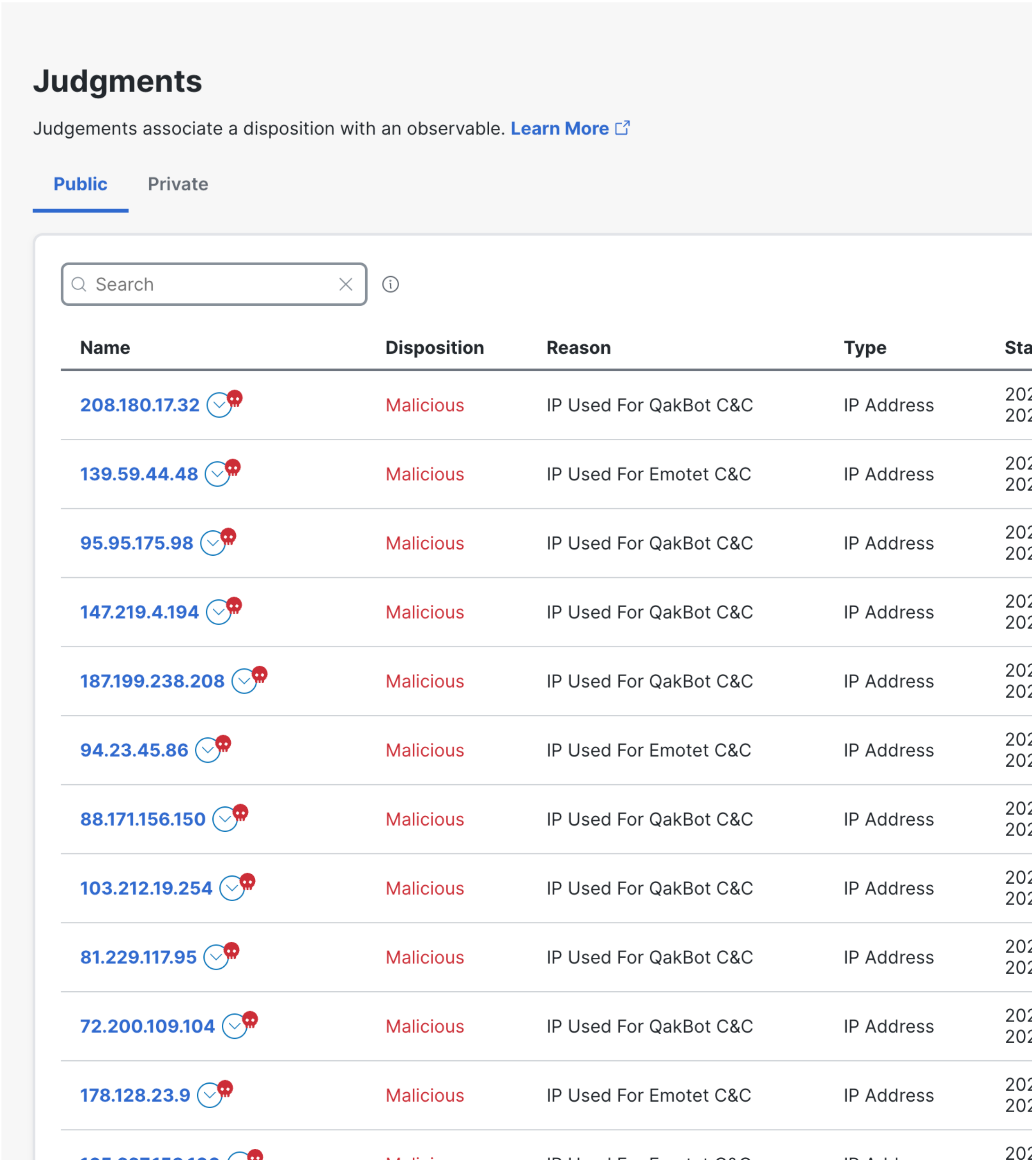
Secure Endpoint
ExecutedMalware.ioc 2 events

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
2 events

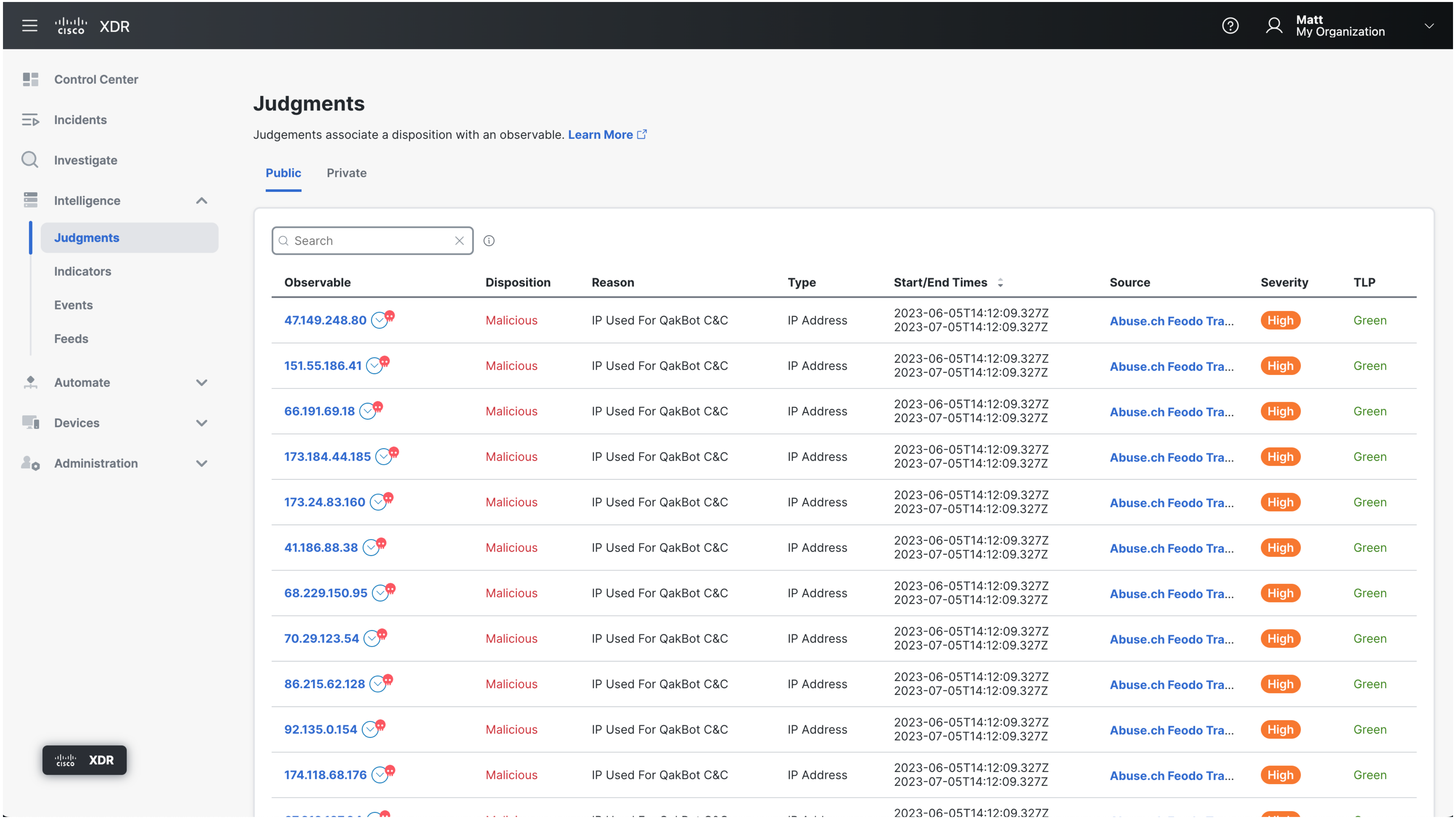
Intelligence



Judgments

Judgements associate a disposition with an observable. **Learn More**

Name	Disposition	Reason	Type	Sta
208.180.17.32	Malicious	IP Used For QakBot C&C	IP Address	202 202
139.59.44.48	Malicious	IP Used For Emotet C&C	IP Address	202 202
95.95.175.98	Malicious	IP Used For QakBot C&C	IP Address	202 202
147.219.4.194	Malicious	IP Used For QakBot C&C	IP Address	202 202
187.199.238.208	Malicious	IP Used For QakBot C&C	IP Address	202 202
94.23.45.86	Malicious	IP Used For Emotet C&C	IP Address	202 202
88.171.156.150	Malicious	IP Used For QakBot C&C	IP Address	202 202
103.212.19.254	Malicious	IP Used For QakBot C&C	IP Address	202 202
81.229.117.95	Malicious	IP Used For QakBot C&C	IP Address	202 202
72.200.109.104	Malicious	IP Used For QakBot C&C	IP Address	202 202
178.128.23.9	Malicious	IP Used For Emotet C&C	IP Address	202 202



Judgments

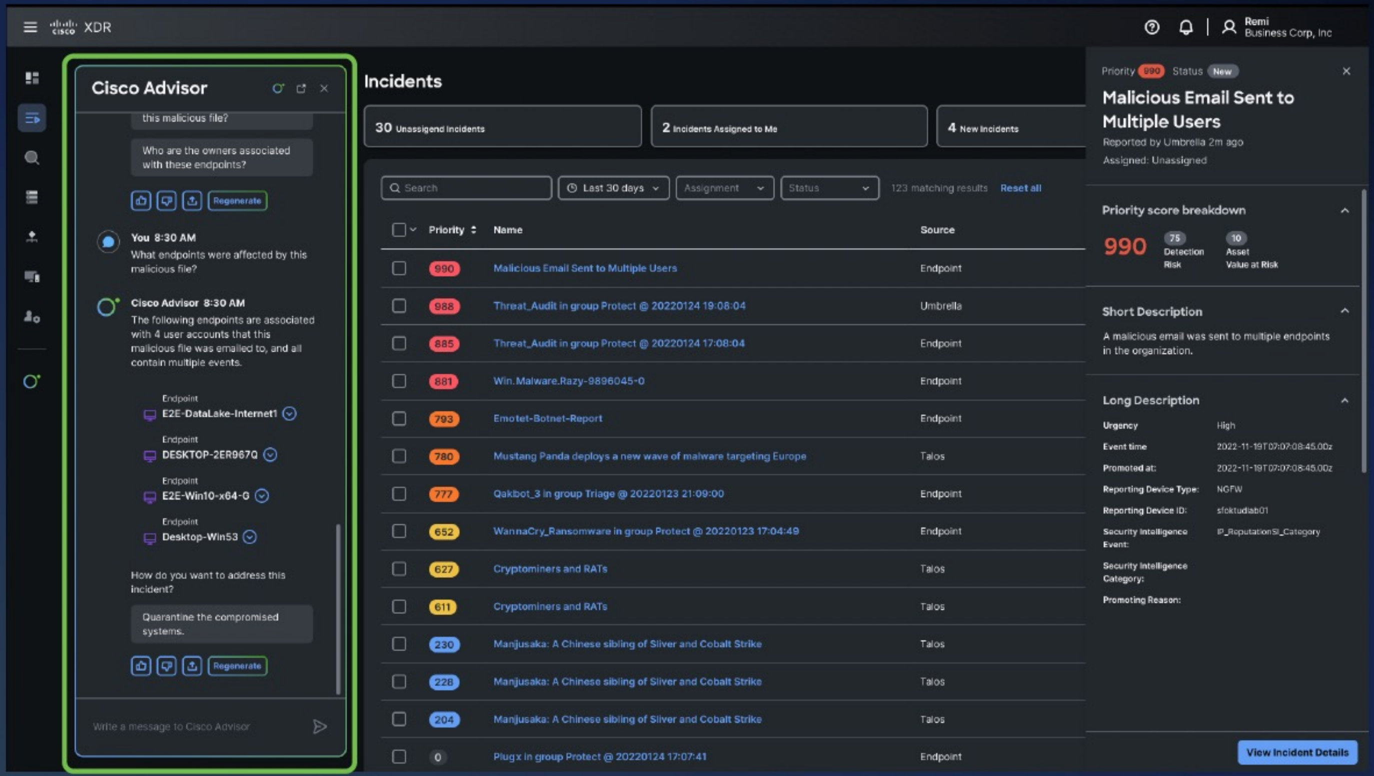
Judgements associate a disposition with an observable. **Learn More**

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



this malicious file?

Who are the owners associated with these endpoints?

You 8:30 AM
What endpoints were affected by this malicious file?

Cisco Advisor 8:30 AM
The following endpoints are associated with 4 user accounts that this malicious file was emailed to, and all contain multiple events.

Endpoint
E2E-DataLake-Internet1

Endpoint
DESKTOP-2ER967Q

Endpoint
E2E-Win10-x64-G

Endpoint
Desktop-Win53

How do you want to address this incident?

Quarantine the compromised systems.

Incidents

30 Unassigend Incidents
2 Incidents Assigned to Me
4 New Incidents

123 matching results

☐	Priority	Name	Source
☐	990	Malicious Email Sent to Multiple Users	Endpoint
☐	988	Threat_Audit in group Protect @ 20220124 19:08:04	Umbrella
☐	885	Threat_Audit in group Protect @ 20220124 17:08:04	Endpoint
☐	881	Win.Malware.Razy-9896045-0	Endpoint
☐	793	Emotet-Botnet-Report	Endpoint
☐	780	Mustang Panda deploys a new wave of malware targeting Europe	Talos
☐	777	Qakbot_3 in group Triage @ 20220123 21:09:00	Endpoint
☐	652	WannaCry_Ransomware in group Protect @ 20220123 17:04:49	Endpoint
☐	627	Cryptominers and RATs	Talos
☐	611	Cryptominers and RATs	Talos
☐	230	Manjusaka: A Chinese sibling of Sliver and Cobalt Strike	Talos
☐	228	Manjusaka: A Chinese sibling of Sliver and Cobalt Strike	Talos
☐	204	Manjusaka: A Chinese sibling of Sliver and Cobalt Strike	Talos
☐	0	Plugx in group Protect @ 20220124 17:07:41	Endpoint

Priority 990 Status New

Malicious Email Sent to Multiple Users

Reported by Umbrella 2m ago
Assigned: Unassigned

Priority score breakdown

990 · 75 Detection Risk · 10 Asset Value at Risk

Short Description

A malicious email was sent to multiple endpoints in the organization.

Long Description

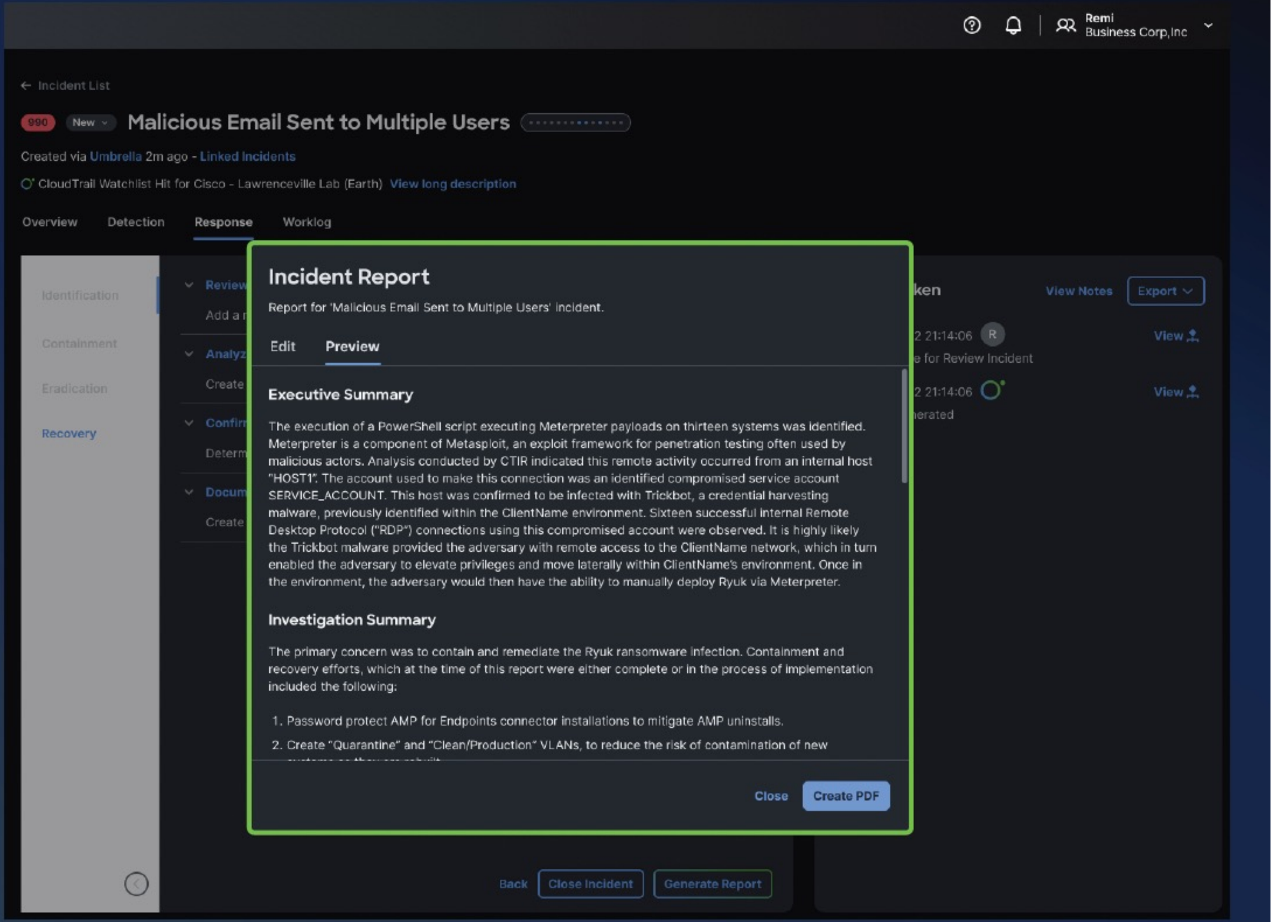
Urgency	High
Event time	2022-11-19T07:07:08:45.00z
Promoted at:	2022-11-19T07:07:08:45.00z
Reporting Device Type:	NGFW
Reporting Device ID:	sfcktudlab01
Security Intelligence Event:	IP_ReputationSI_Category
Security Intelligence Category:	
Promoting Reason:	

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

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



Incident Report

Report for 'Malicious Email Sent to Multiple Users' incident.

Executive Summary

The execution of a PowerShell script executing Meterpreter payloads on thirteen systems was identified. Meterpreter is a component of Metasploit, an exploit framework for penetration testing often used by malicious actors. Analysis conducted by CTIR indicated this remote activity occurred from an internal host "HOST1". The account used to make this connection was an identified compromised service account SERVICE_ACCOUNT. This host was confirmed to be infected with Trickbot, a credential harvesting malware, previously identified within the ClientName environment. Sixteen successful internal Remote Desktop Protocol ("RDP") connections using this compromised account were observed. It is highly likely the Trickbot malware provided the adversary with remote access to the ClientName network, which in turn enabled the adversary to elevate privileges and move laterally within ClientName's environment. Once in the environment, the adversary would then have the ability to manually deploy Ryuk via Meterpreter.

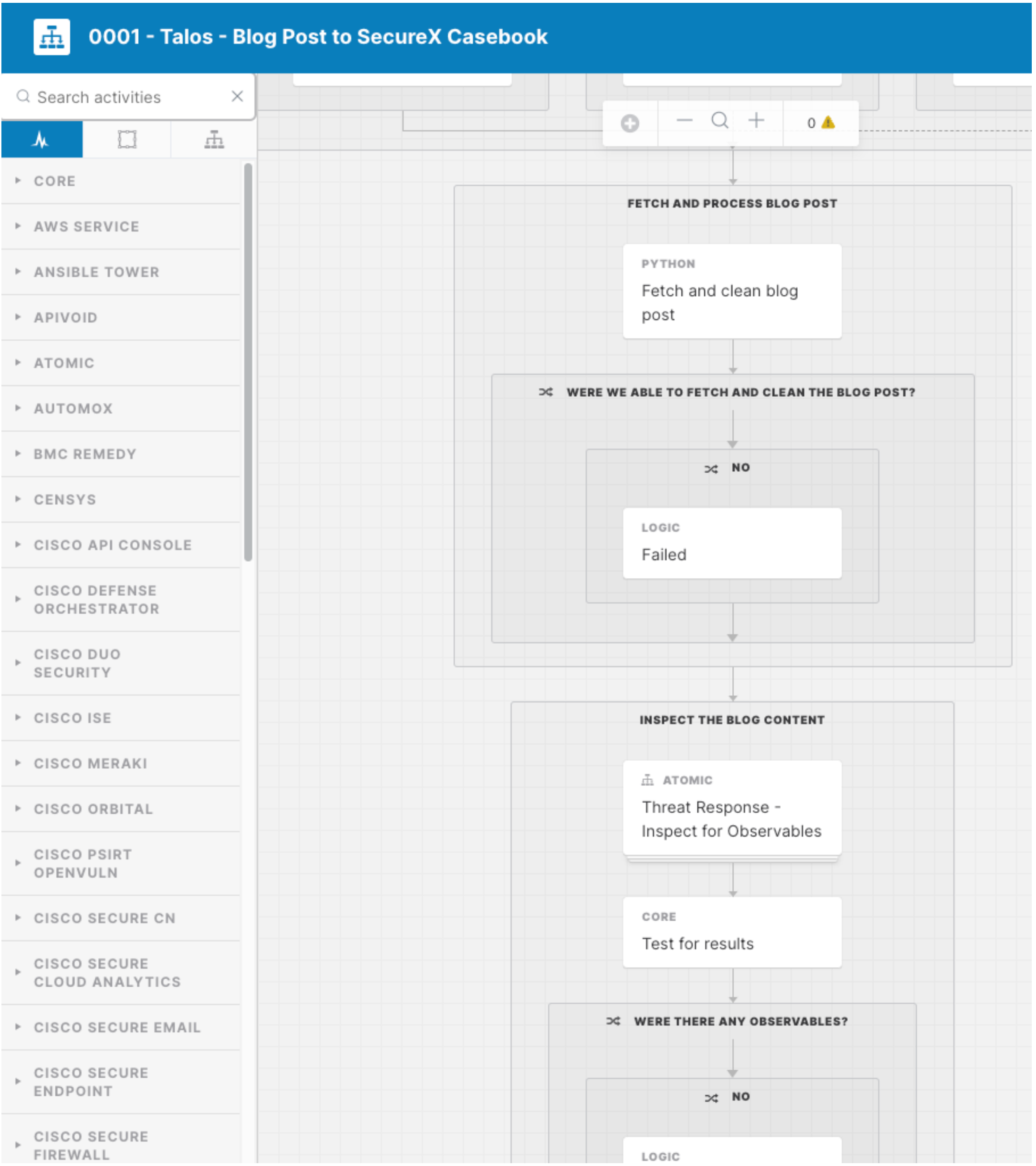
Investigation Summary

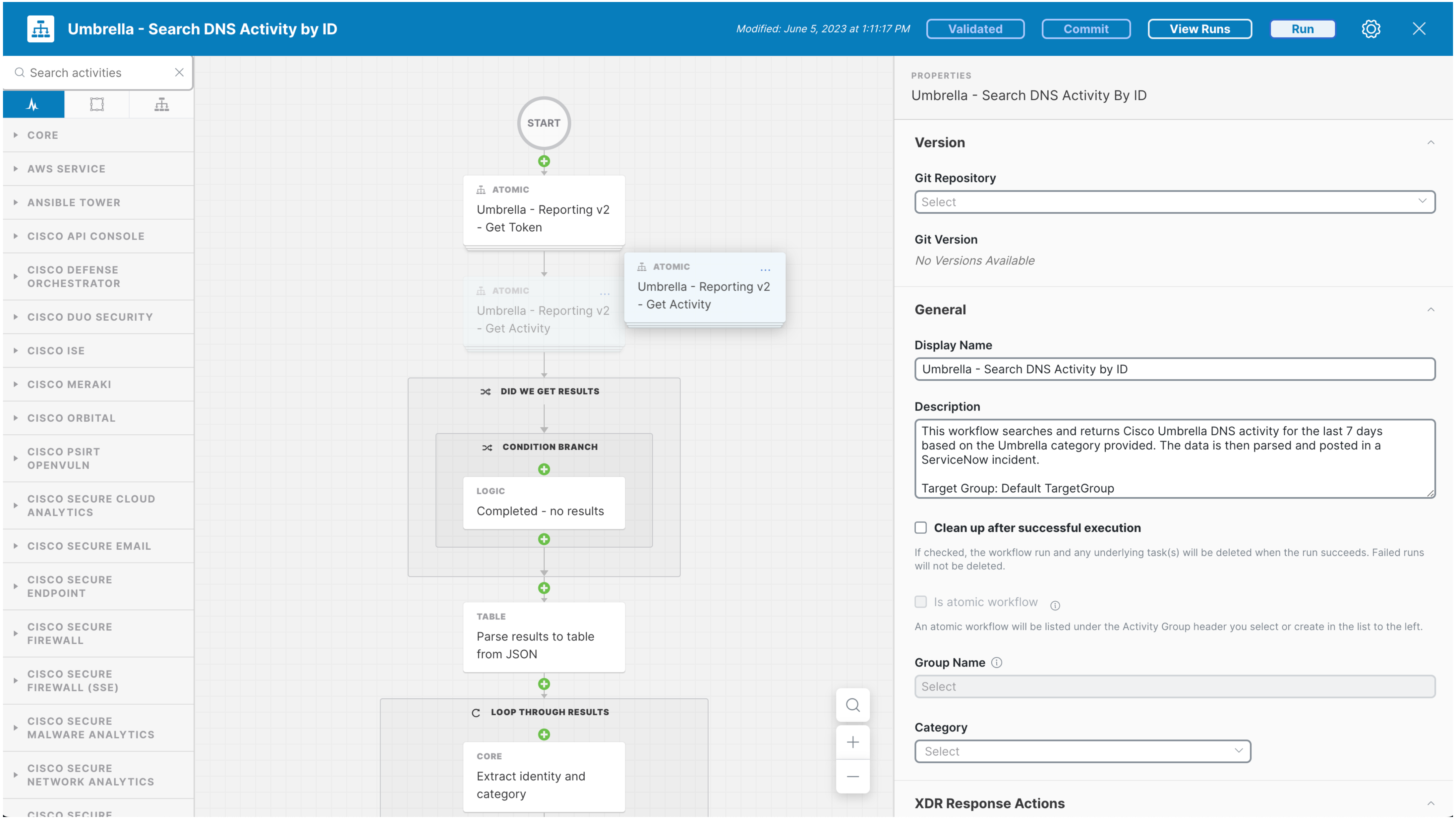
The primary concern was to contain and remediate the Ryuk ransomware infection. Containment and recovery efforts, which at the time of this report were either complete or in the process of implementation included the following:

1. Password protect AMP for Endpoints connector installations to mitigate AMP uninstalls.
2. Create "Quarantine" and "Clean/Production" VLANs, to reduce the risk of contamination of new

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

Automation


0001 - Talos - Blog Post to SecureX Casebook
Search activities
0
CORE
AWS SERVICE
ANSIBLE TOWER
APIVOID
ATOMIC
AUTOMOX
BMC REMEDY
CENSYS
CISCO API CONSOLE
CISCO DEFENSE ORCHESTRATOR
CISCO DUO SECURITY
CISCO ISE
CISCO MERAKI
CISCO ORBITAL
CISCO PSIRT OPENVULN
CISCO SECURE CN
CISCO SECURE CLOUD ANALYTICS
CISCO SECURE EMAIL
CISCO SECURE ENDPOINT
CISCO SECURE FIREWALL
FETCH AND PROCESS BLOG POST
PYTHON
Fetch and clean blog post
WERE WE ABLE TO FETCH AND CLEAN THE BLOG POST?
NO
LOGIC
Failed
INSPECT THE BLOG CONTENT
ATOMIC
Threat Response - Inspect for Observables
CORE
Test for results
WERE THERE ANY OBSERVABLES?
NO
LOGIC



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 | CISCO

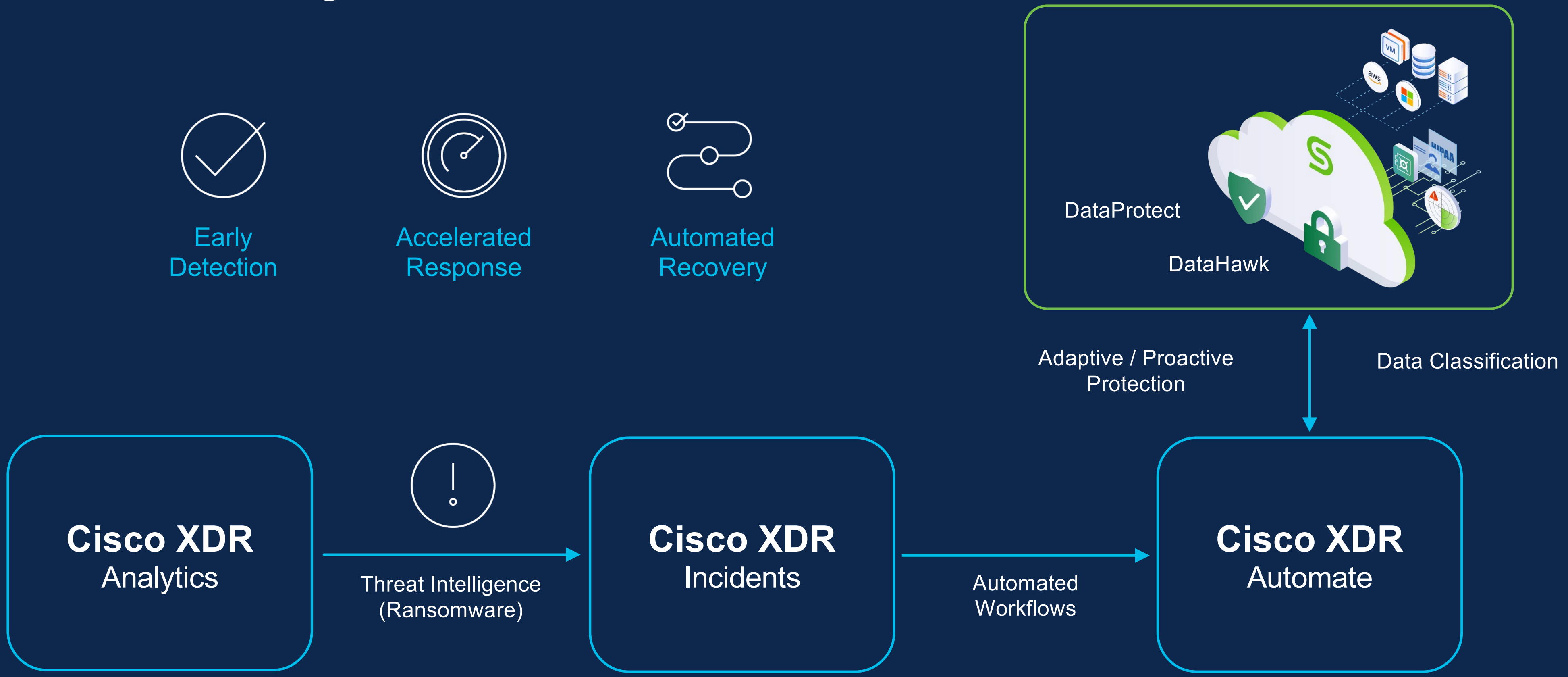
© 2023 Cisco and/or its affiliates. All rights reserved.

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

Early Detection

Accelerated Response

Automated Recovery



DataProtect

DataHawk

Adaptive / Proactive Protection

Data Classification

Cisco XDR
Analytics

Threat Intelligence (Ransomware)

Cisco XDR
Incidents

Automated Workflows

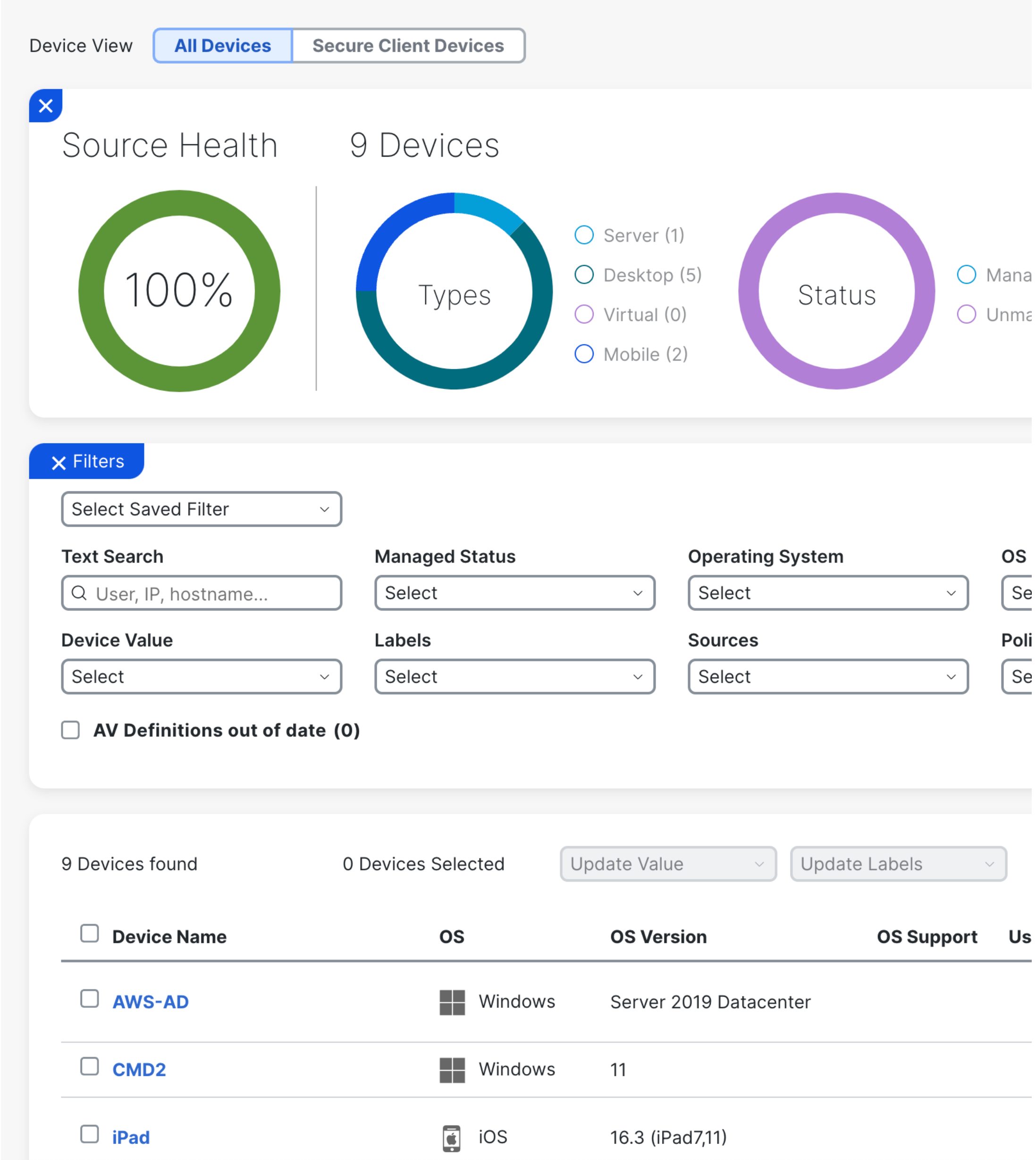
Cisco XDR
Automate

CISCO SECURE

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

* Includes Cohesity as the first data protection solution provider

Devices



Text Search: User, IP, hostname...

Managed Status: Select

Operating System: Select

OS: Se

Device Value: Select

Labels: Select

Sources: Select

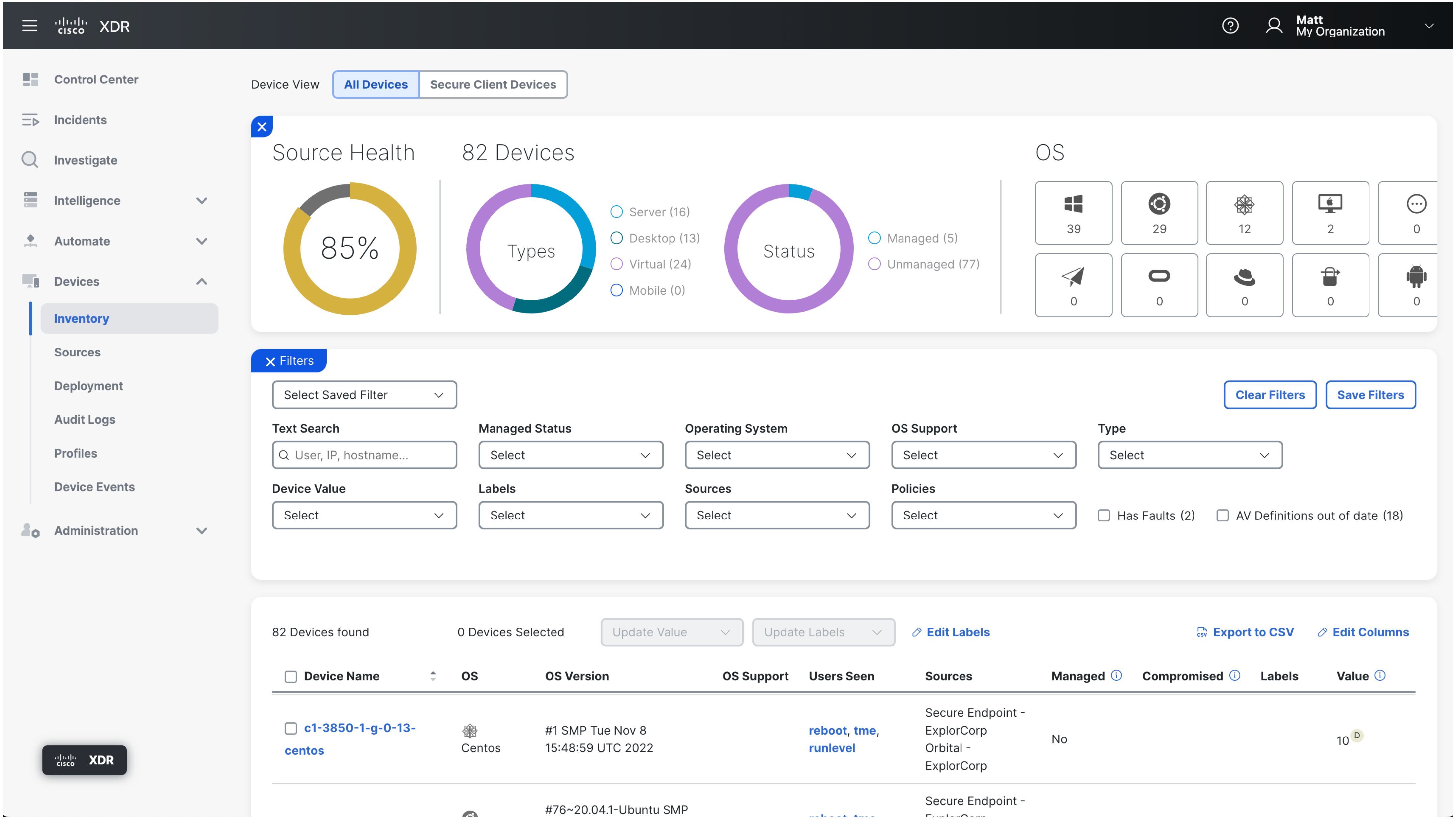
Poli: Se

☐ **AV Definitions out of date (0)**

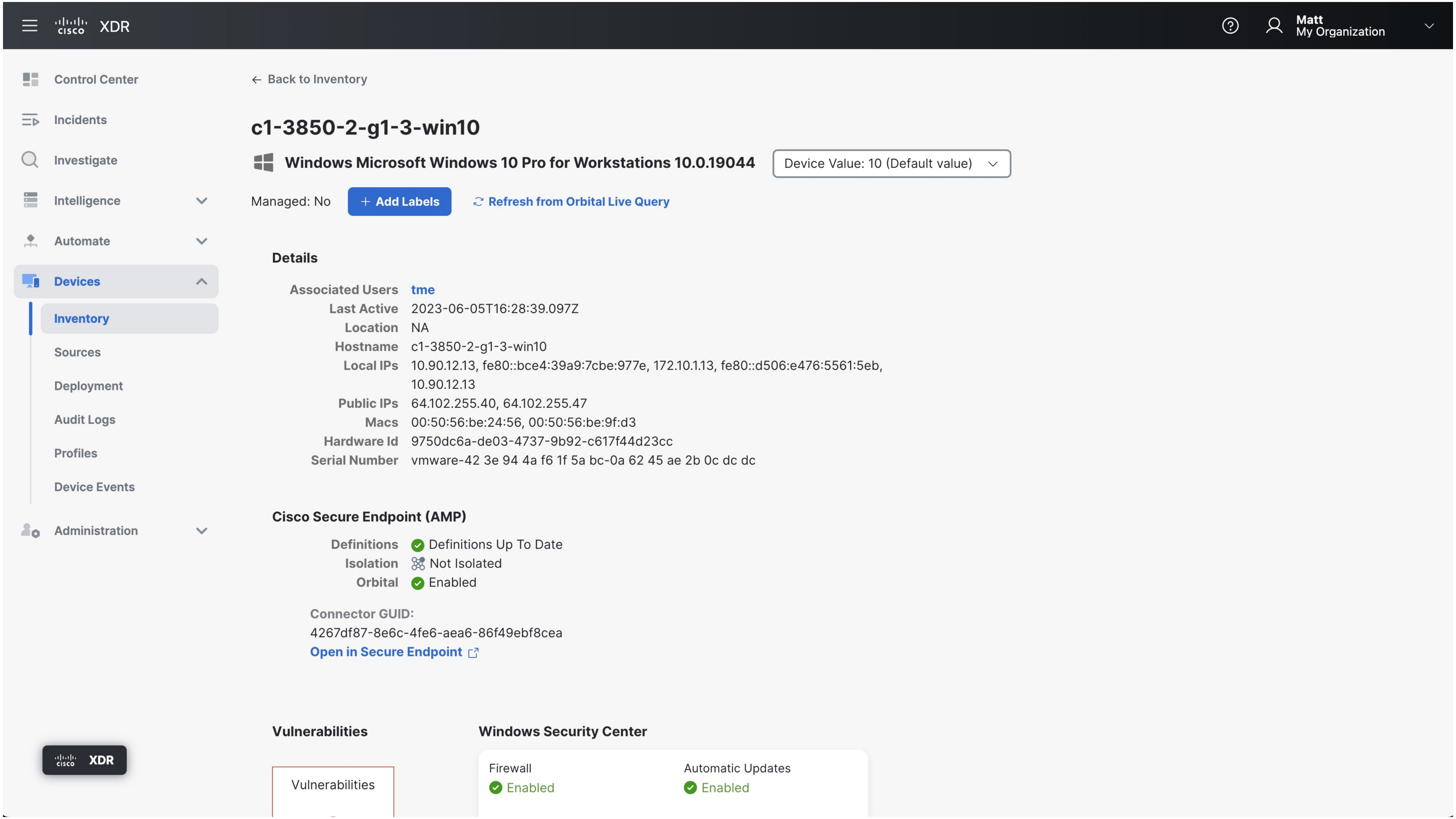
9 Devices found

0 Devices Selected

☐	Device Name	OS	OS Version	OS Support	Us
☐	AWS-AD	Windows	Server 2019 Datacenter		
☐	CMD2	Windows	11		
☐	iPad	iOS	16.3 (iPad7,11)		



☐ Device Name	OS	OS Version	OS Support	Users Seen	Sources	Managed	Compromised	Labels	Value
☐ 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 D
		#76~20.04.1-Ubuntu SMP			Secure Endpoint -				



c1-3850-2-g1-3-win10

Windows Microsoft Windows 10 Pro for Workstations 10.0.19044

Device Value: 10 (Default value)

Managed: No

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

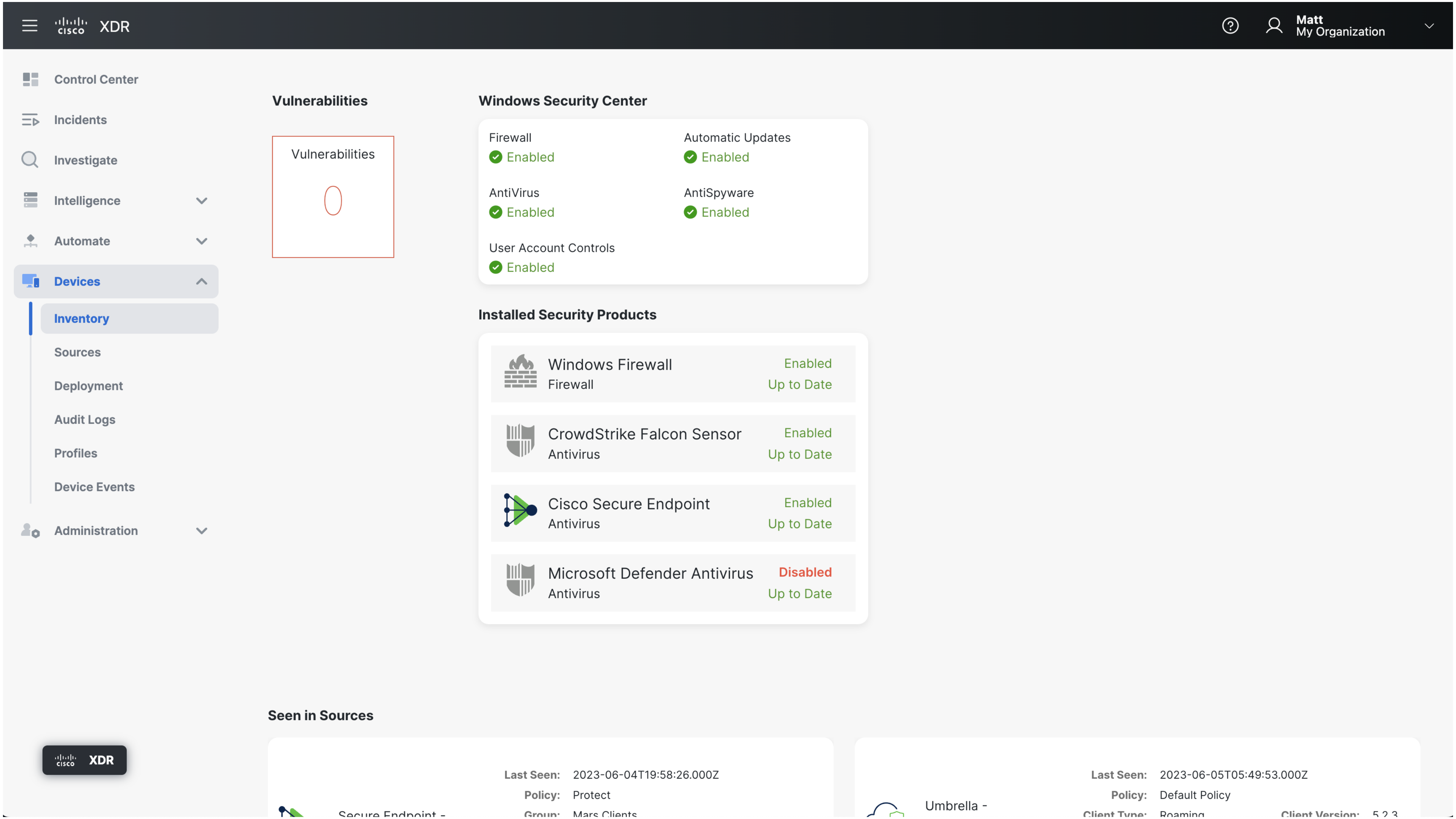
Connector GUID:
4267df87-8e6c-4fe6-aea6-86f49ebf8cea

Vulnerabilities

Vulnerabilities

Windows Security Center

Firewall	Automatic Updates
✓ Enabled	✓ Enabled



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

Secure Endpoint -

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

Policy: Protect

Group: Mars Clients

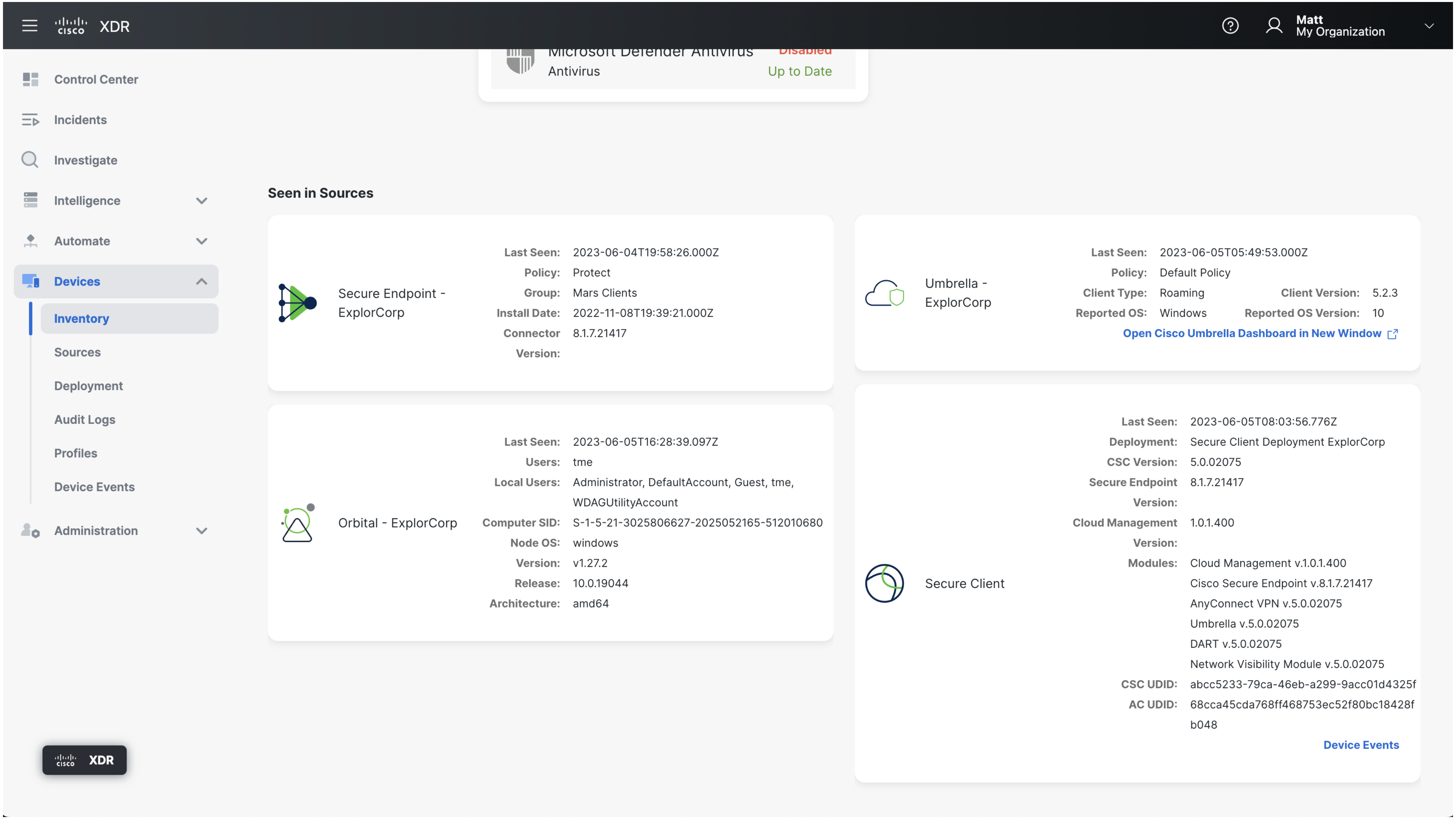
Umbrella -

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

Policy: Default Policy

Client Type: Roaming

Client Version: 5.2.3



Microsoft Defender Antivirus Disabled
Antivirus 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 Version: 8.1.7.21417

Orbital - ExplorCorp

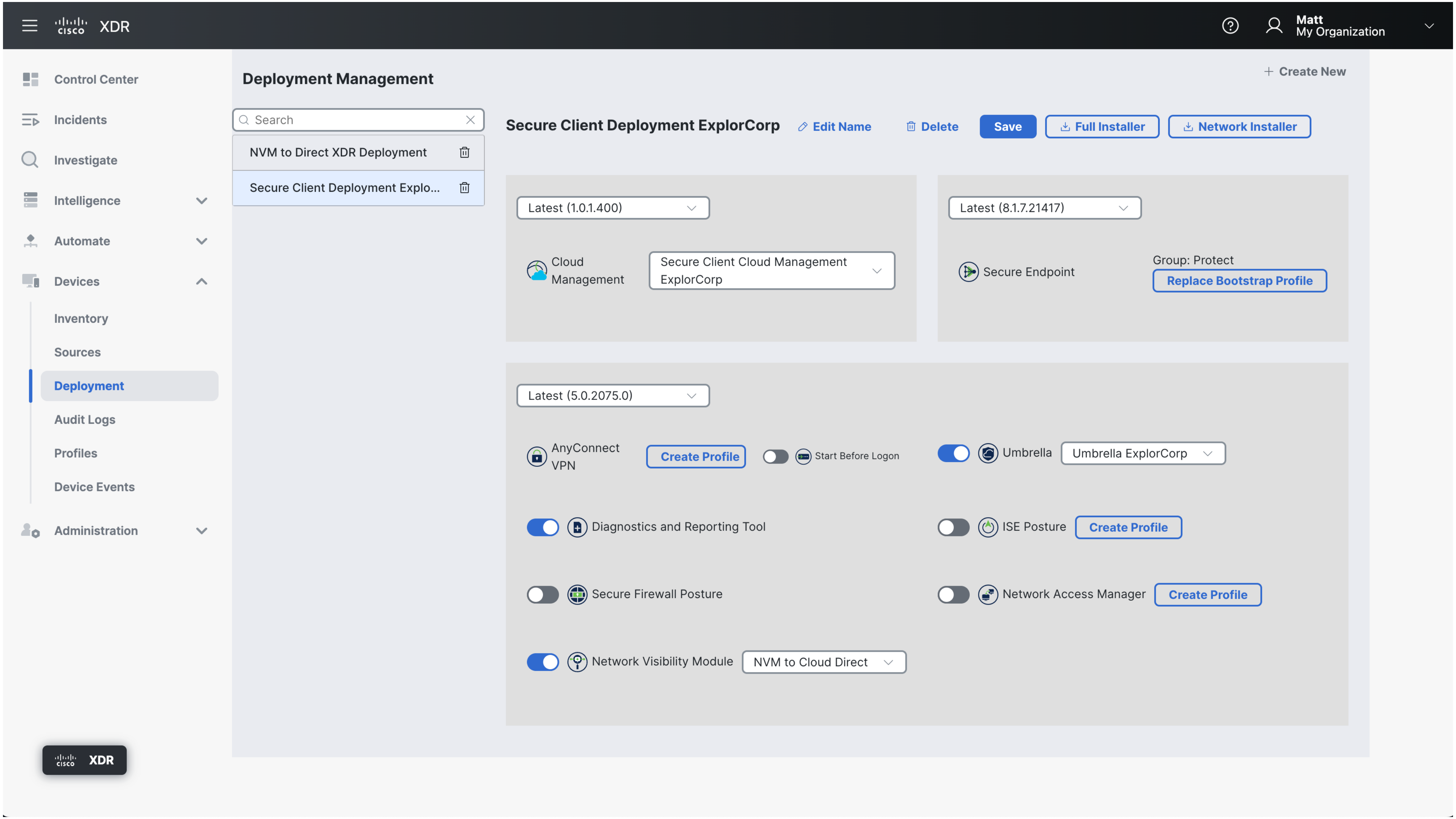
Last Seen: 2023-06-05T16:28:39.097Z
Users: tme
Local Users: Administrator, DefaultAccount, Guest, tme, WDAGUtilityAccount
Computer SID: S-1-5-21-3025806627-2025052165-512010680
Node OS: windows
Version: v1.27.2
Release: 10.0.19044
Architecture: amd64

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

Secure Client

Last Seen: 2023-06-05T08:03:56.776Z
Deployment: Secure Client Deployment ExplorCorp
CSC Version: 5.0.02075
Secure Endpoint Version: 8.1.7.21417
Cloud Management Version: 1.0.1.400
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: 68cca45cda768ff468753ec52f80bc18428fb048
Device Events



Deployment Management

NVM to Direct XDR Deployment

Secure Client Deployment Explo...

Secure Client Deployment ExplorCorp

Latest (1.0.1.400)

Cloud Management: Secure Client Cloud Management ExplorCorp

Latest (8.1.7.21417)

Secure Endpoint — Group: Protect

Latest (5.0.2075.0)

AnyConnect VPN

Start Before Logon

Umbrella: Umbrella ExplorCorp

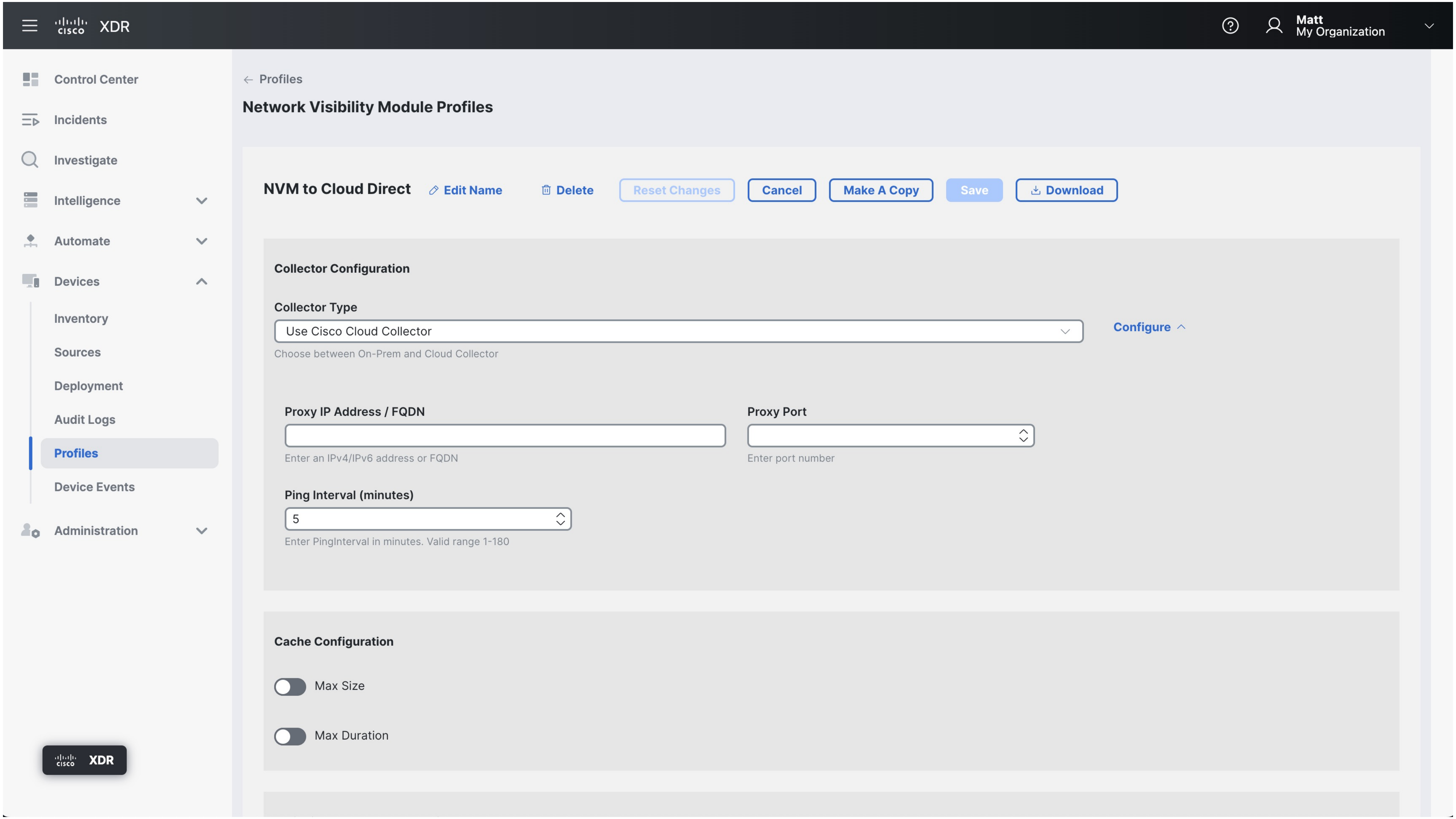
Diagnostics and Reporting Tool

ISE Posture

Secure Firewall Posture

Network Access Manager

Network Visibility Module: NVM to Cloud Direct



Network Visibility Module Profiles

NVM to Cloud Direct

Collector Configuration

Collector Type: Use Cisco Cloud Collector

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): 5

Enter PingInterval in minutes. Valid range 1-180

Cache Configuration

○ Max Size

○ Max Duration

One more thing…

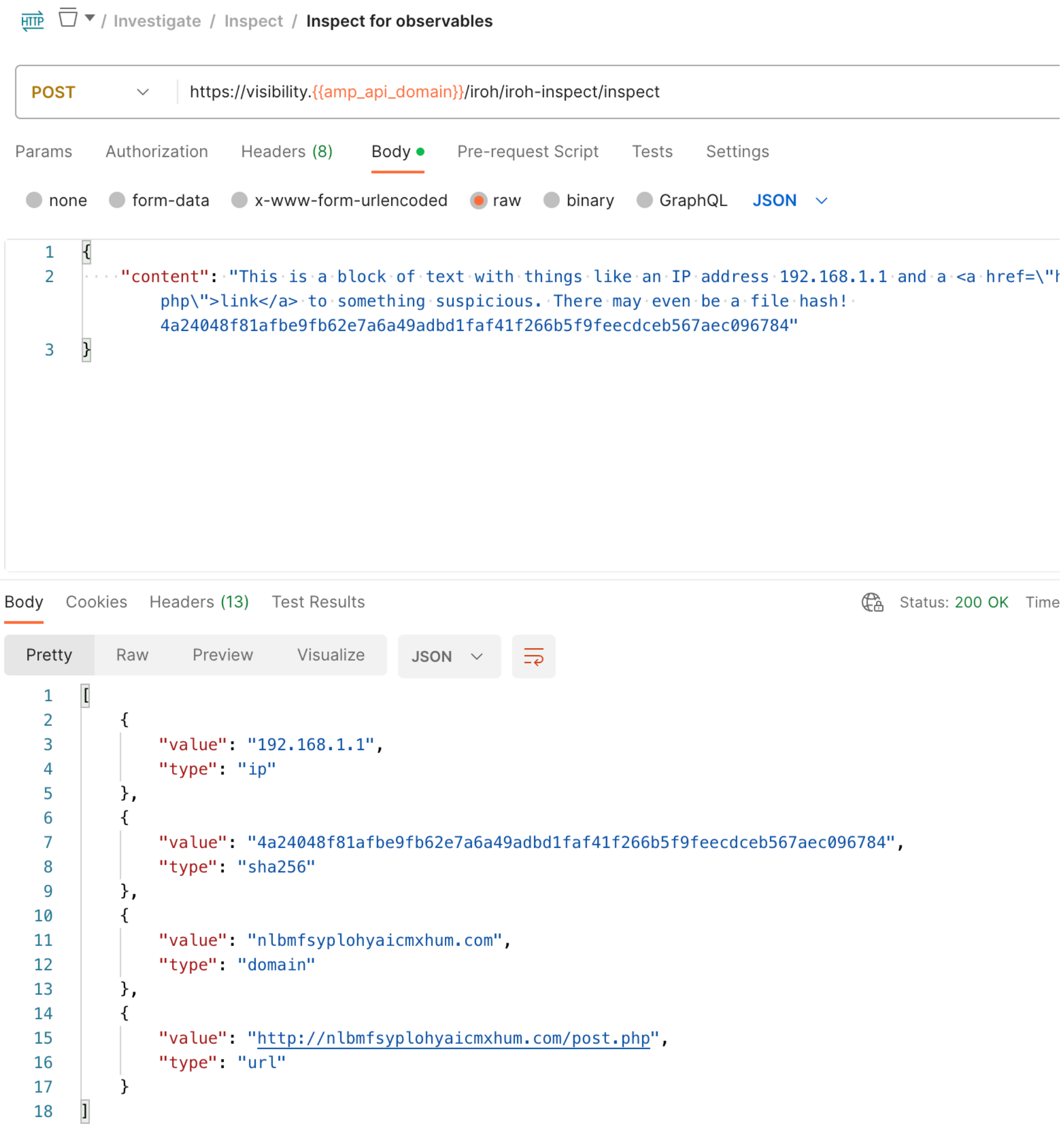
XDR has a robust set of APIs!

- 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

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

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…



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

```
{
    "content": "This is a block of text with things like an IP address 192.168.1.1 and a <a href=\"
        php\">link</a> to something suspicious. There may even be a file hash!
        4a24048f81afbe9fb62e7a6a49adbd1faf41f266b5f9feecdceb567aec096784"
}
```

```
[
    {
        "value": "192.168.1.1",
        "type": "ip"
    },
    {
        "value": "4a24048f81afbe9fb62e7a6a49adbd1faf41f266b5f9feecdceb567aec096784",
        "type": "sha256"
    },
    {
        "value": "nlbmfsyplohyaicmxhum.com",
        "type": "domain"
    },
    {
        "value": "http://nlbmfsyplohyaicmxhum.com/post.php",
        "type": "url"
    }
]
```

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

SECURE

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

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**

© 2023 Cisco and/or it

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

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

https://cisco.com/go/xdr

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

The bridge to possible

Děkuji za pozornost

Q & A