

The Cisco Live! logo, featuring the word "CISCO" in a dark blue, sans-serif font, followed by "Live!" in a dark blue, cursive script font.

CISCO *Live!*

The text "Let's go" in a large, dark blue, sans-serif font, positioned to the left of a bright white sunburst graphic that radiates across the right side of the image.

Let's go

#CiscoLiveAPJC



The bridge to possible

Accelerate your SOC

With Cisco XDR

Aaron T. Woland, CCIE #20113

Distinguished Engineer, Threat Detection & Response

loxx@cisco.com | [@aaronwoland](https://twitter.com/aaronwoland)

BRKSEC-1023



#CiscoLiveAPJC



\$ whoami



Cisco role: Distinguished Engineer,
Threat Detection & Response

Unofficial title:
“Cisco History Professor”

Experience: Old enough to wonder
how I have been doing this for ~30
years

Fun fact 1: Father of 5 daughters

Fun fact 2: Oldest works for Cisco
now! Youngest is 18 months!

Fun fact 3: Working through his
Cyber Security Master’s Degree
from SANS Institute (~04/24)

Sarcasm

*“If we can’t laugh
at ourselves,
Then we cannot
laugh at anything
at all”*



Cisco Webex App

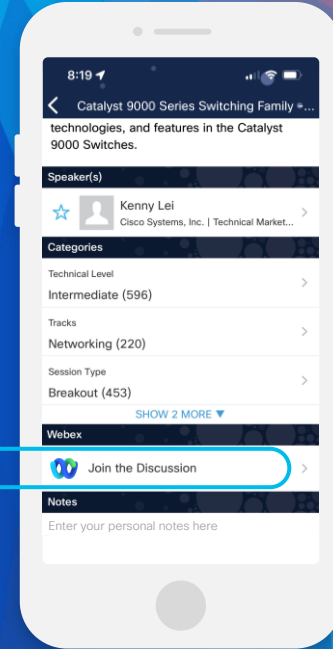
Questions?

Use Cisco Webex App to chat with the speaker after the session

How

- 1 Find this session in the Cisco Live Mobile App
- 2 Click “Join the Discussion”
- 3 Install the Webex App or go directly to the Webex space
- 4 Enter messages/questions in the Webex space

Webex spaces will be moderated by the speaker until December 22, 2023.



<https://ciscolive.ciscoevents.com/ciscolivebot/#BRKSEC-1023>

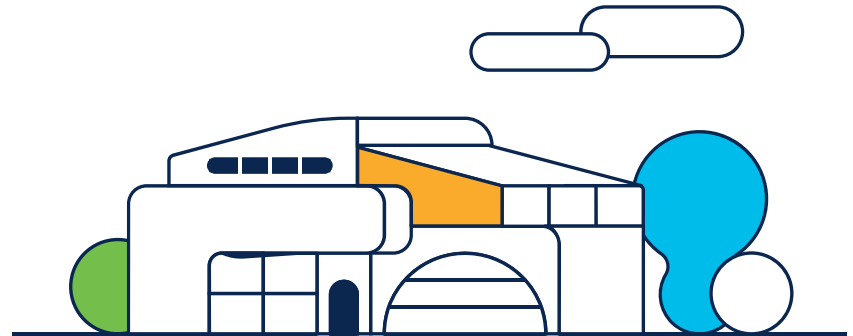
Please fill out the survey



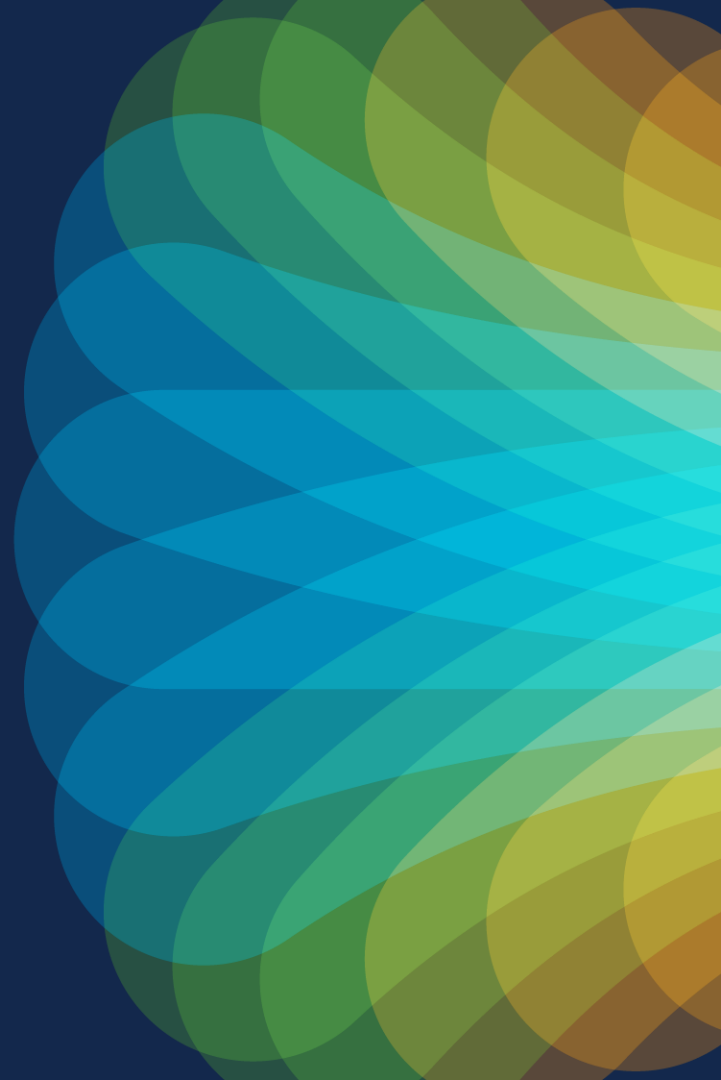
Drop your email in the comments – I WILL respond!

Agenda

- Intro to XDR
- Outcomes
- Features
- Resources



Intro to XDR



Protection isn't Enough

- The bad guys get through our defenses
- Require Detection & Response
 - Endpoint Detection & Response
 - Network Detection & Response
 - Email Detection & Response
 - Identity Threat Detection & Response



What is 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



We Are Here

Gartner®

Hype Cycle for Security Operations, 2022

Published 5 July 2022 • ID G00770249

HYPE CYCLE

PRIORITY MATRIX

Time To Plateau Will Be Reached:

< 2 yrs.

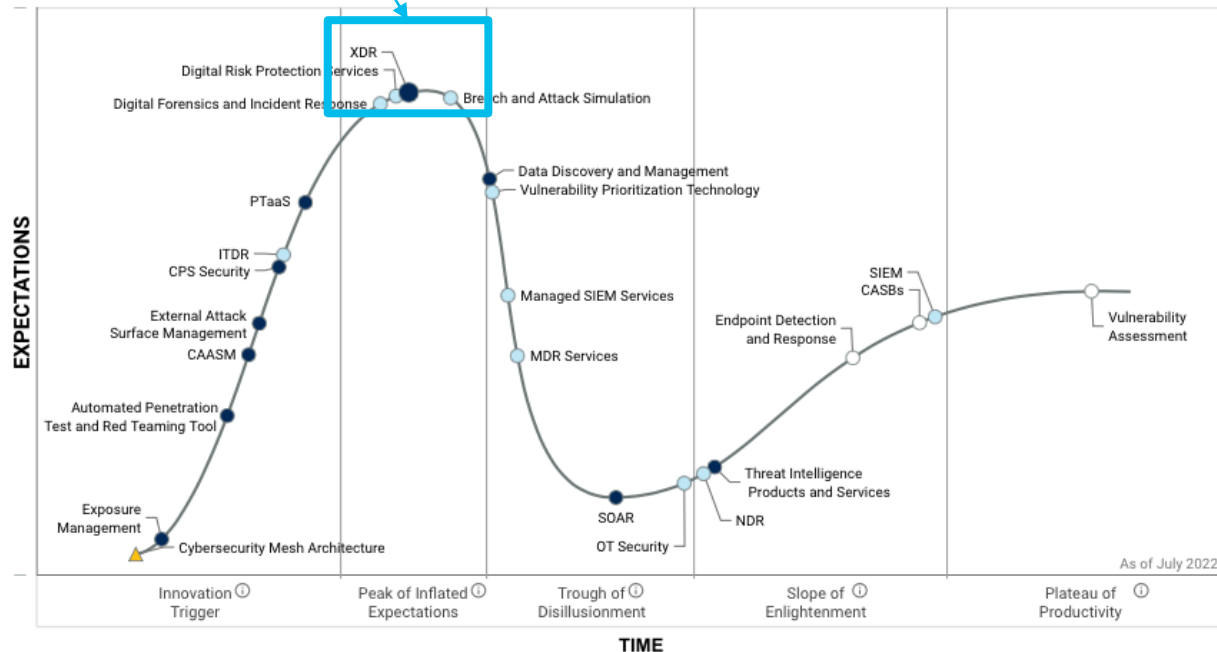
2-5 yrs.

5-10 yrs.

> 10 yrs.



XDR



Benefit Rating

High

Maturity

Early mainstream

Market Penetration

20% to 50% of target audience

Time to Plateau

5-10 yrs.

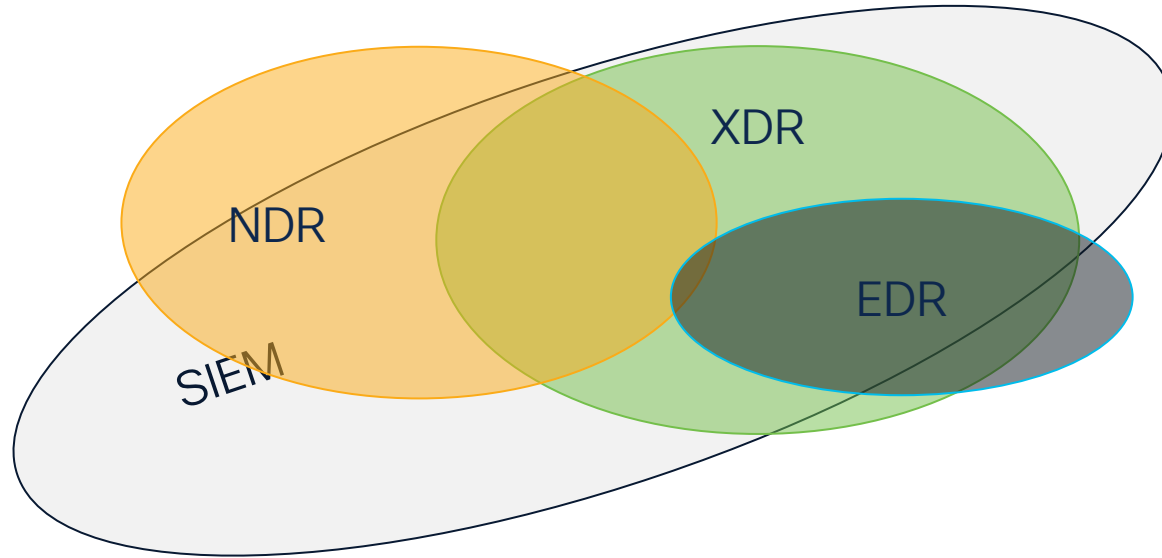
Definition

Extended detection and response (XDR) products are threat detection and incident response offerings that combine multiple security tools to meet more security operations needs. Primary functions include security analytics, alert correlation, incident response and incident response playbook automation.

Why This Is Important

XDR products can be seen as evolutions and amalgamations of some of the security operations tools that preceded them. However, XDR products have higher levels of integration, automation, ease of use, and focus on threat detection and incident response. They also include security controls for, among other things, endpoint detection and response (EDR), cloud access security brokers (CASBs),

Is XDR different than all the other things?



Shared use cases:

- Threat Detection
- Threat Hunting
- Forensics
- Response

*not to scale

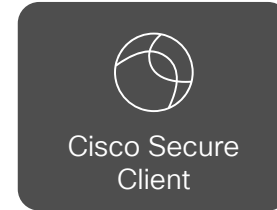
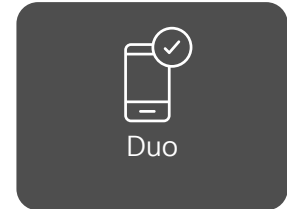
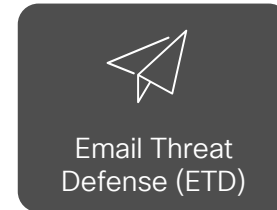
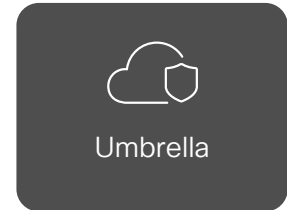
CISCO *Live!*

#CiscoLiveAPJC

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%



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



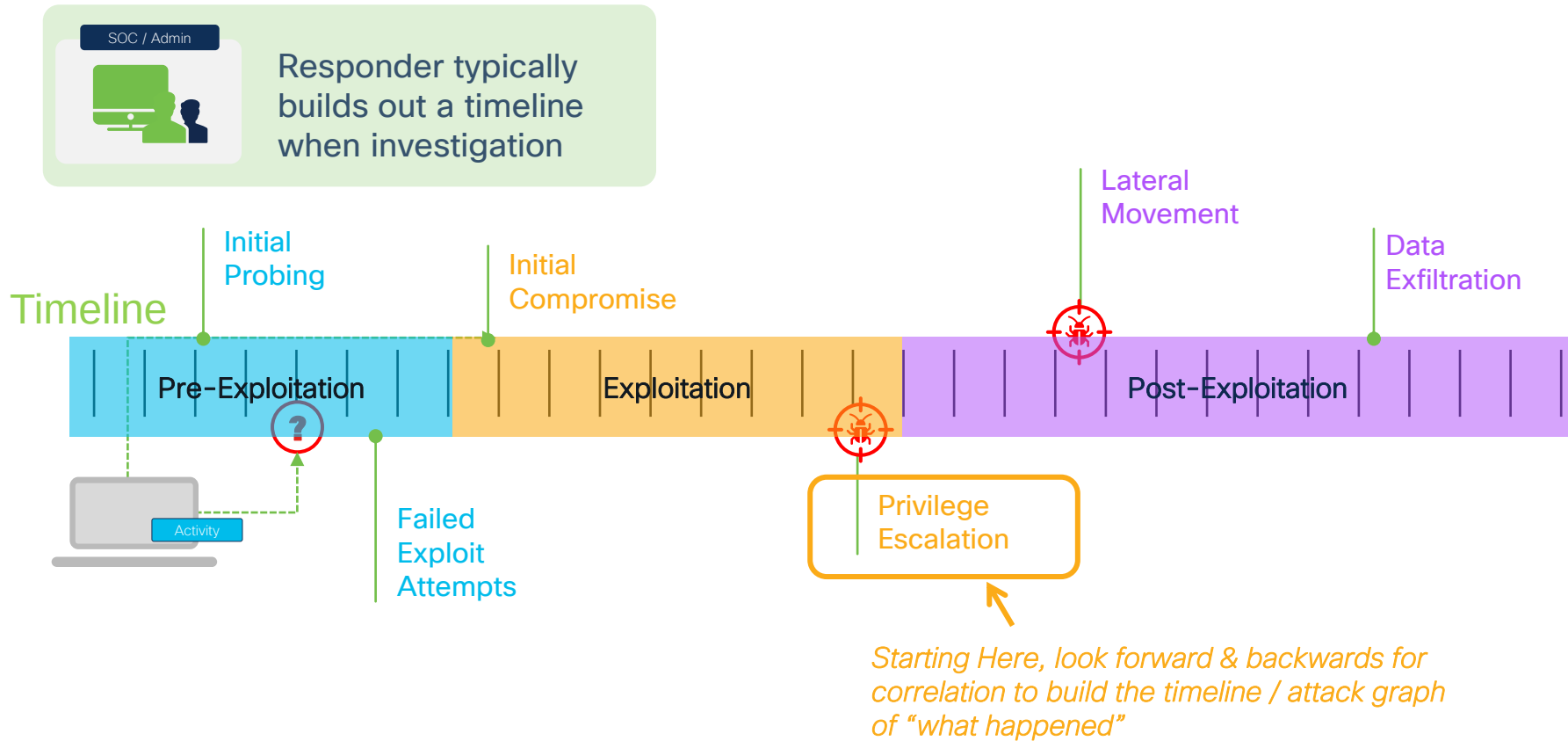
- Focus on what matters and filter out the noise
- Boost limited resources for maximum value
- Automate tasks and focus on, strategic tasks

Build resilience



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

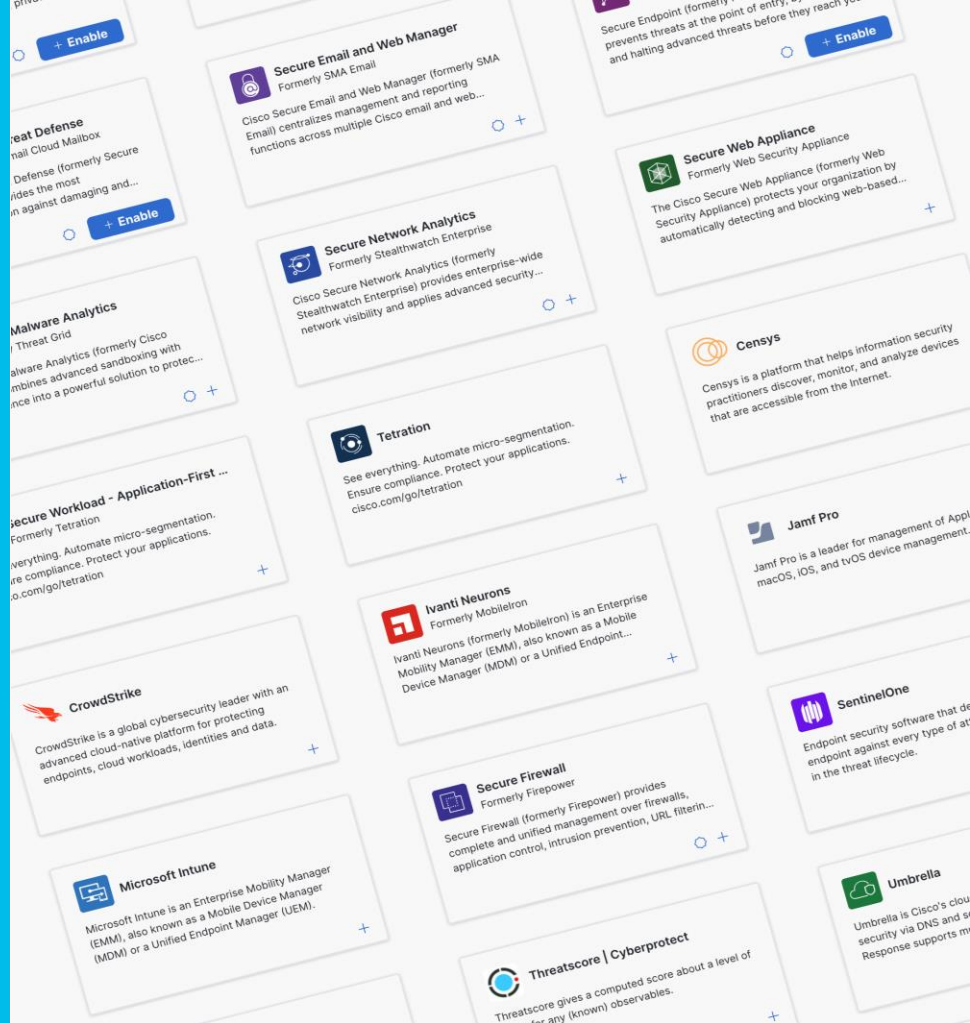
Investigation Timeline – what happened & when?



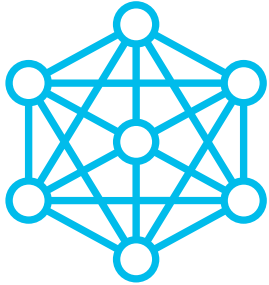
Outcomes

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



A vast ecosystem of integrations



Telemetry and Detections

Cisco XDR leverages multiple sources of telemetry and detections to achieve cross-product outcomes

Action and Response

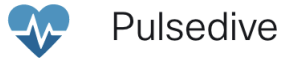
Multiple types of response actions are available across products such as network, endpoint, email, and others

Cisco and Third Party

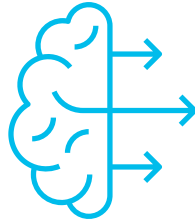
Leverage integrations with existing products, whether they are from Cisco or from a third party

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



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

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

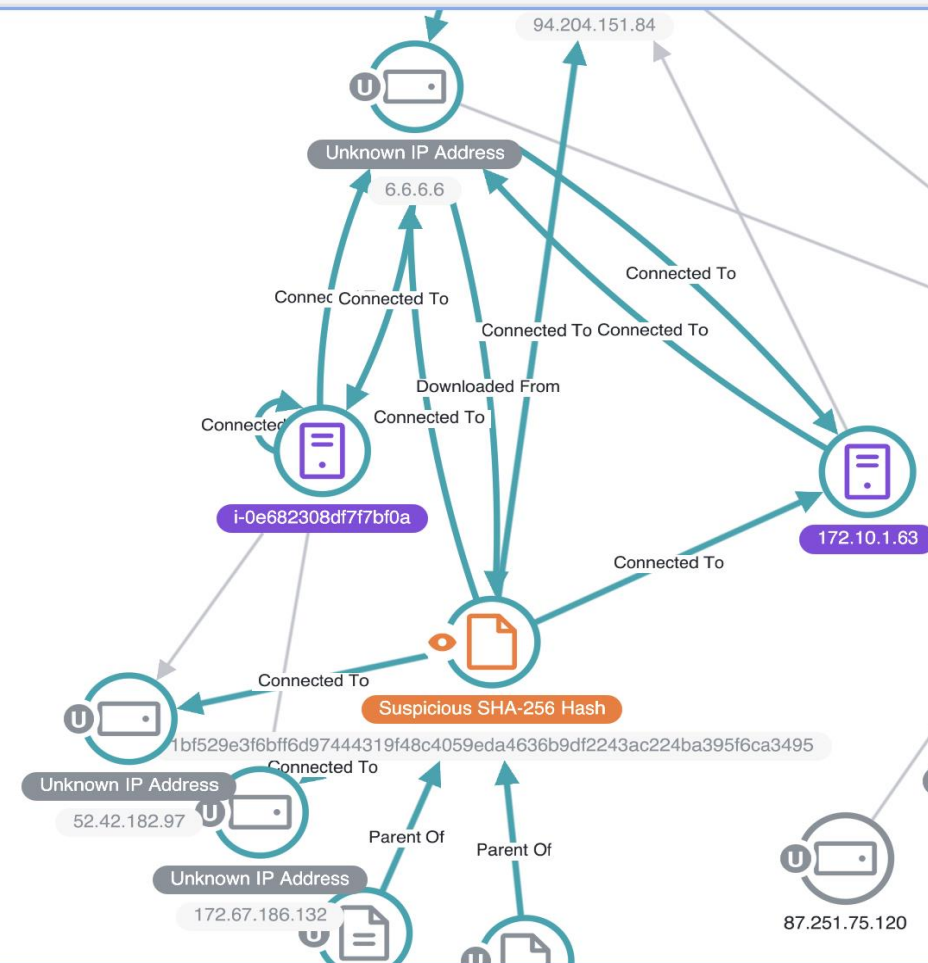
62 matching results

Filters

☐	Priority	Name	Source
☐	1000	Malicious Process and Suspicious SMB/RDP Activity - Doc Test Do ...	Cisco S
☐	1000	Unusual External Server for This is localhost	Cisco S
☐	1000	AWS Inspector Finding for This is localhost	Cisco S
☐	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 S
☐	765	Azure Permissive Security Group for TD&R RSA	Cisco S
☐	742	F1.03-08.Critical.TTP(58).AssetValue[8]	Formul

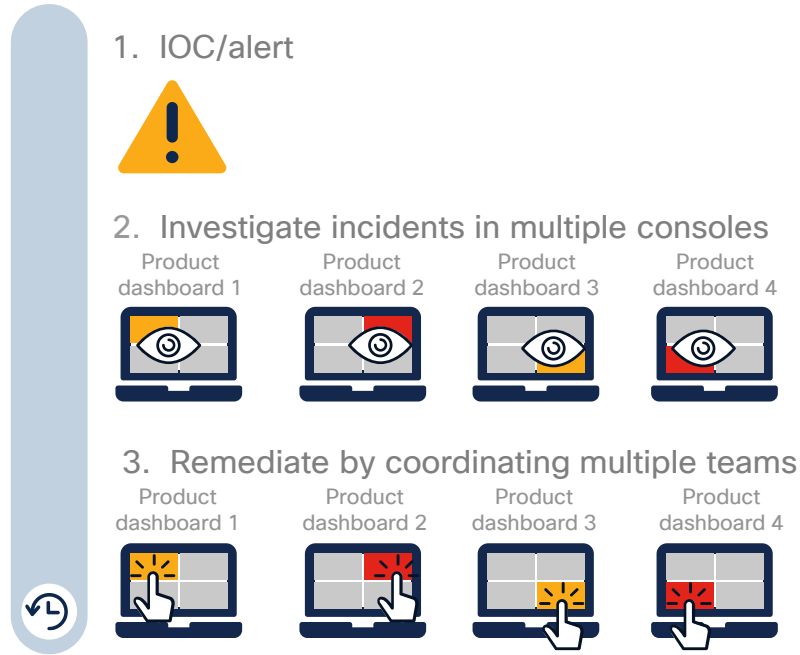
Reduce investigation time

- 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

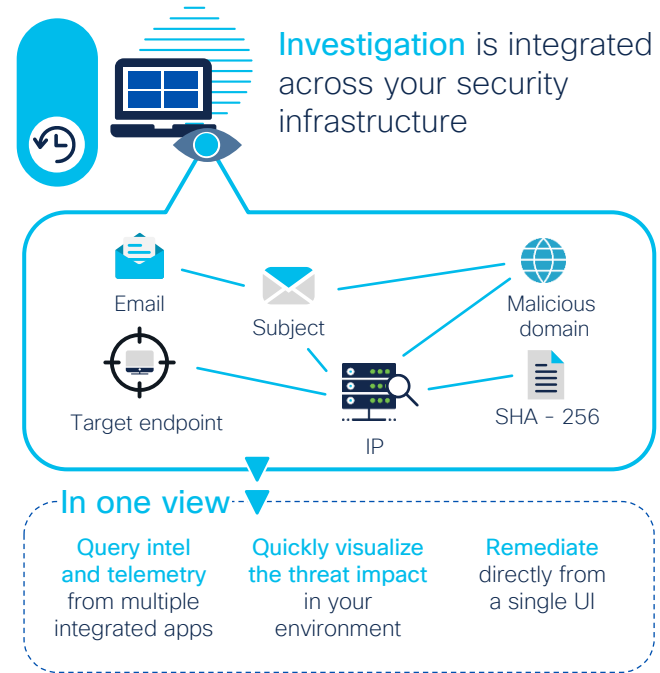


How true simplicity is experienced

Without XDR: 32 minutes



With XDR: five minutes



Confirm attacks sooner with alert correlation

• 2023-03-13T16:...	High	Suspicious SMB and 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 reveal the attack chain

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 →](#)

Powerful, flexible automation



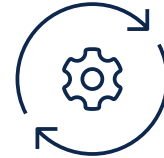
Response

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

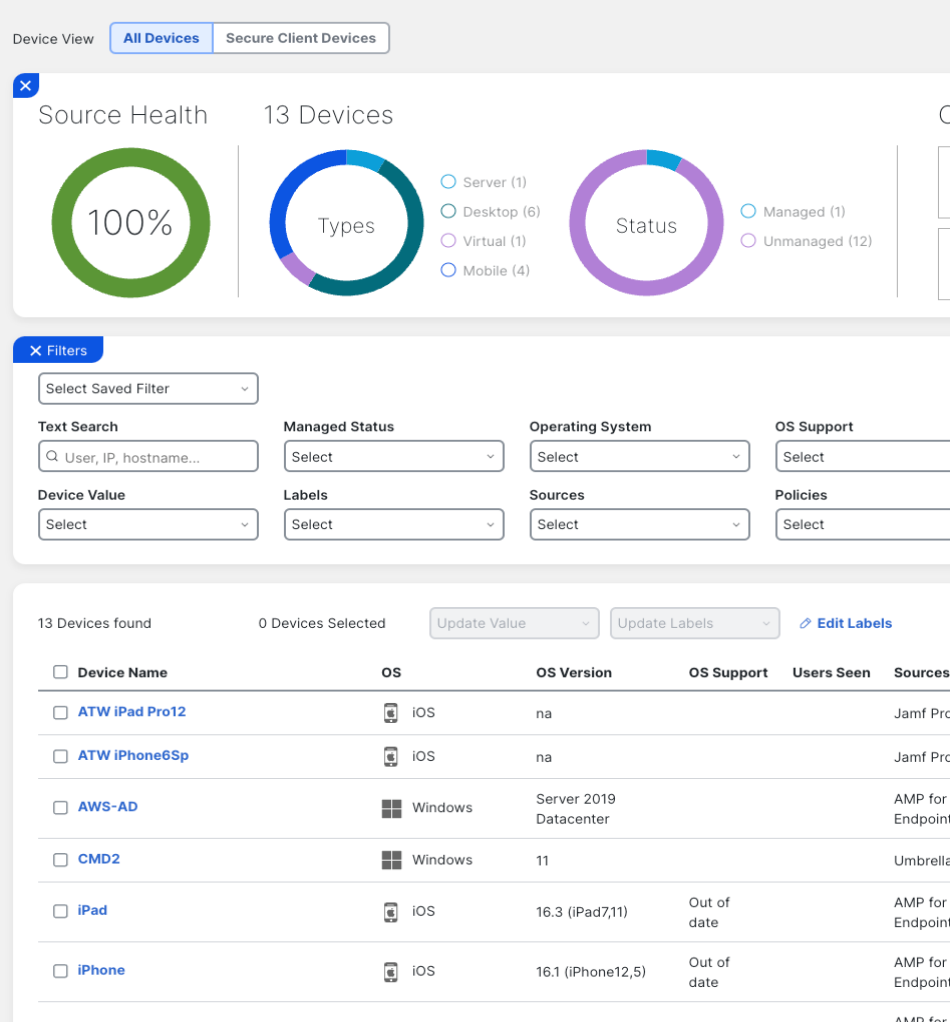


And more...

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

Extend asset context

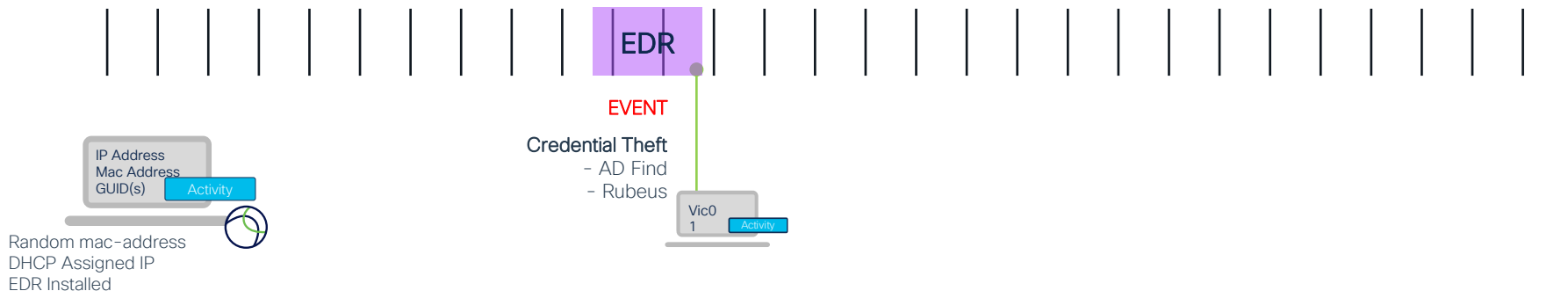
- Detailed asset information aggregated from multiple sources
- Combines asset inventory with security context
- Allows for more accurate incident prioritization based on asset value
- Distinguish between targets and assets



Features

Timeline from multiple sources

XDR Should Build out the Timeline

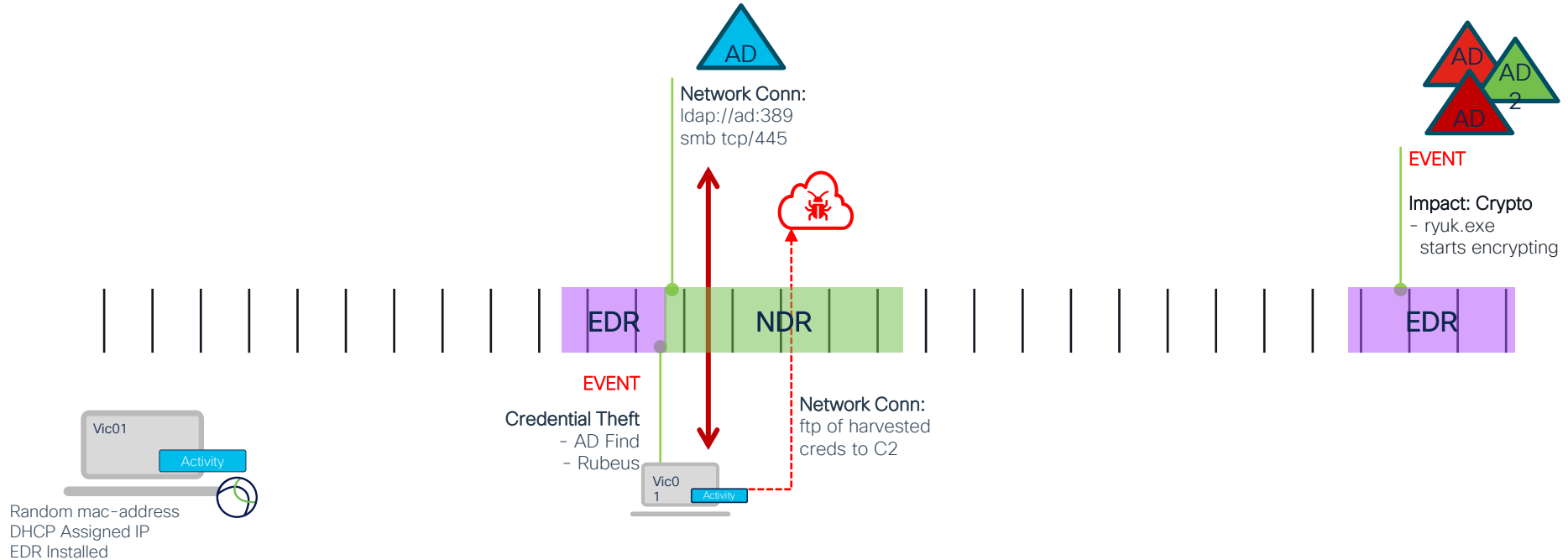


1. EDR event, detects Kerberoast attack to harvest credentials.
Is this enough information to act?



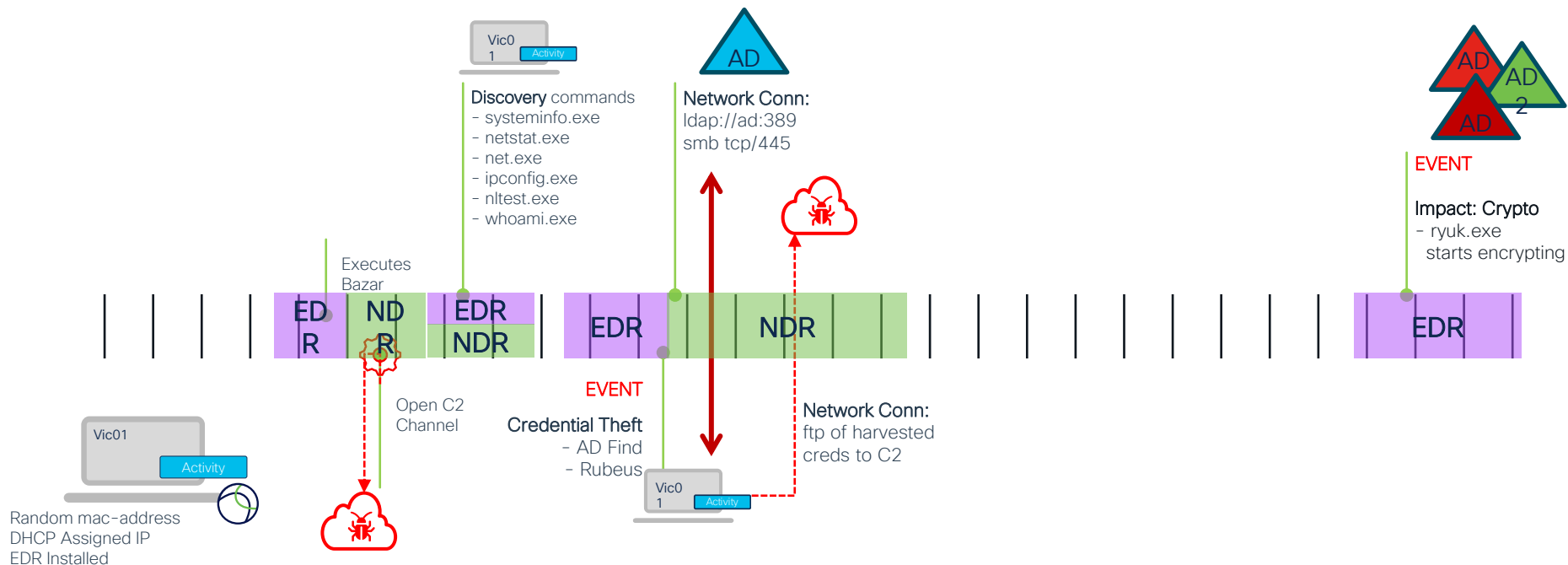
An XDR should be automatically looking for how the event happened.. Stitching together other key events that might not be as critical to generate an Alert!

XDR Should Build out the Timeline



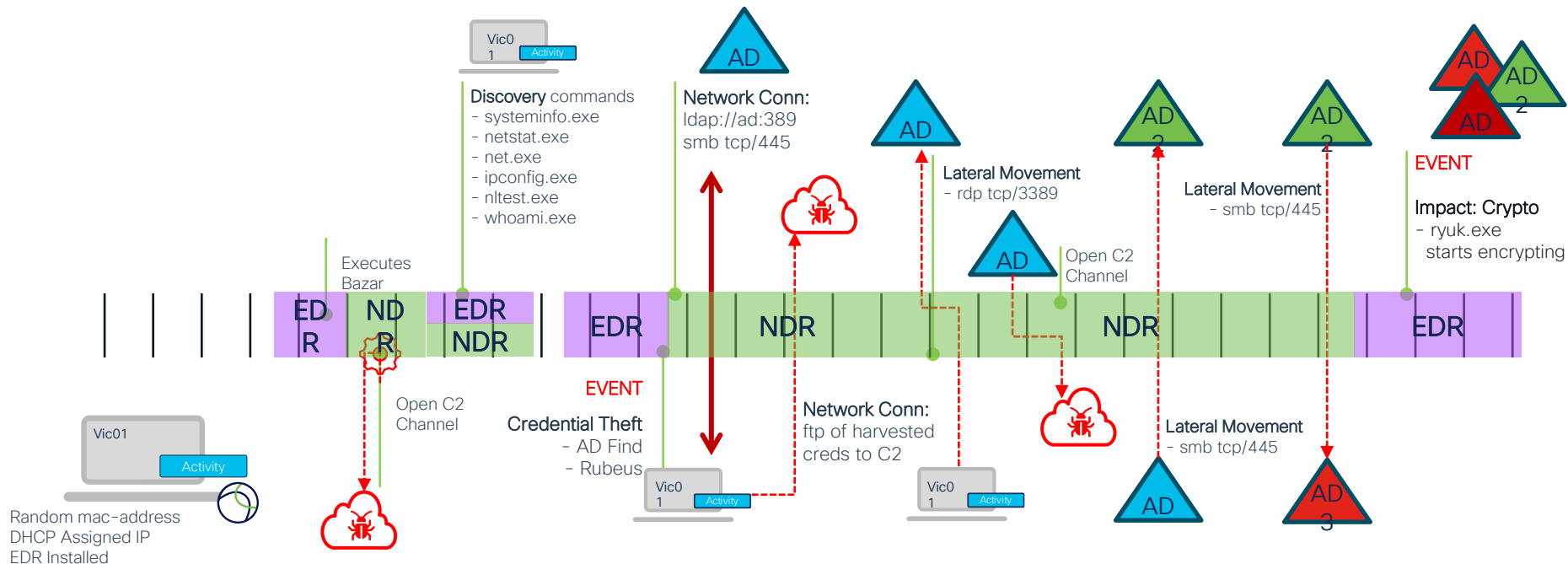
2. NDR: Endpoint Vic01 connected via LDAP & SMB to the AD server for the kerberoast to be successful
3. NDR: Endpoint Vic01 sent the harvested creds out to the C2 server
4. EDR: First System (AD) was Ransomed! How did this happen?

XDR Should Build out the Timeline



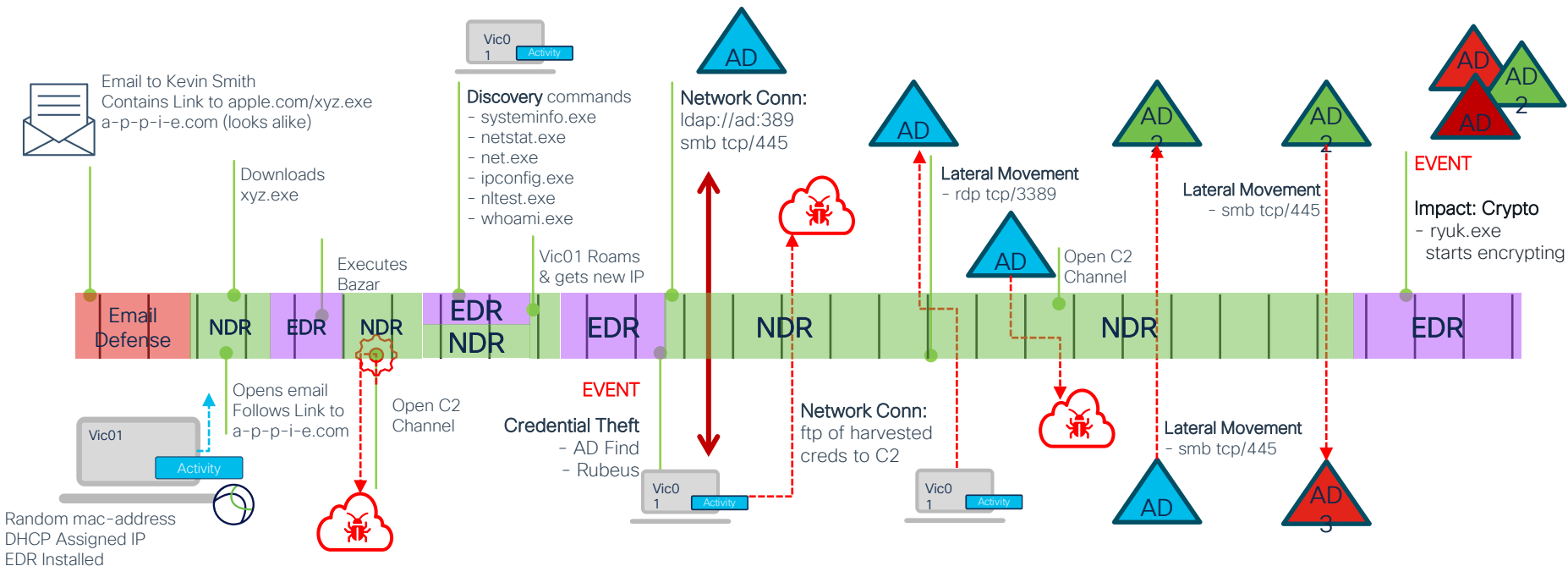
5. EDR: Endpoint Vic01 was sending out discovery commands previously, what else was seen for Vic01?
6. EDR: Endpoint Vic01 Executed an unknown binary before those commands were run
7. NDR / DNS / Proxy: XYZ on Vic01 was communicating encrypted TLS w/ a potentially risky site before the commands

XDR Should Build out the Timeline



8. NDR: Vic01 does first lateral move to AD via RDP
9. NDR: AD Establishes C2 channel
10. NDR: AD moves laterally to other AD servers via SMB

XDR Should Build out the Timeline



11. Vic01 had roamed & gotten a new IP Address (so much more important than you know)
12. Bazar executable XYZ was downloaded by Kevin Smith
13. Kevin Smith received an email w/ a look-alike domain in the URL & he clicked it to download that executable

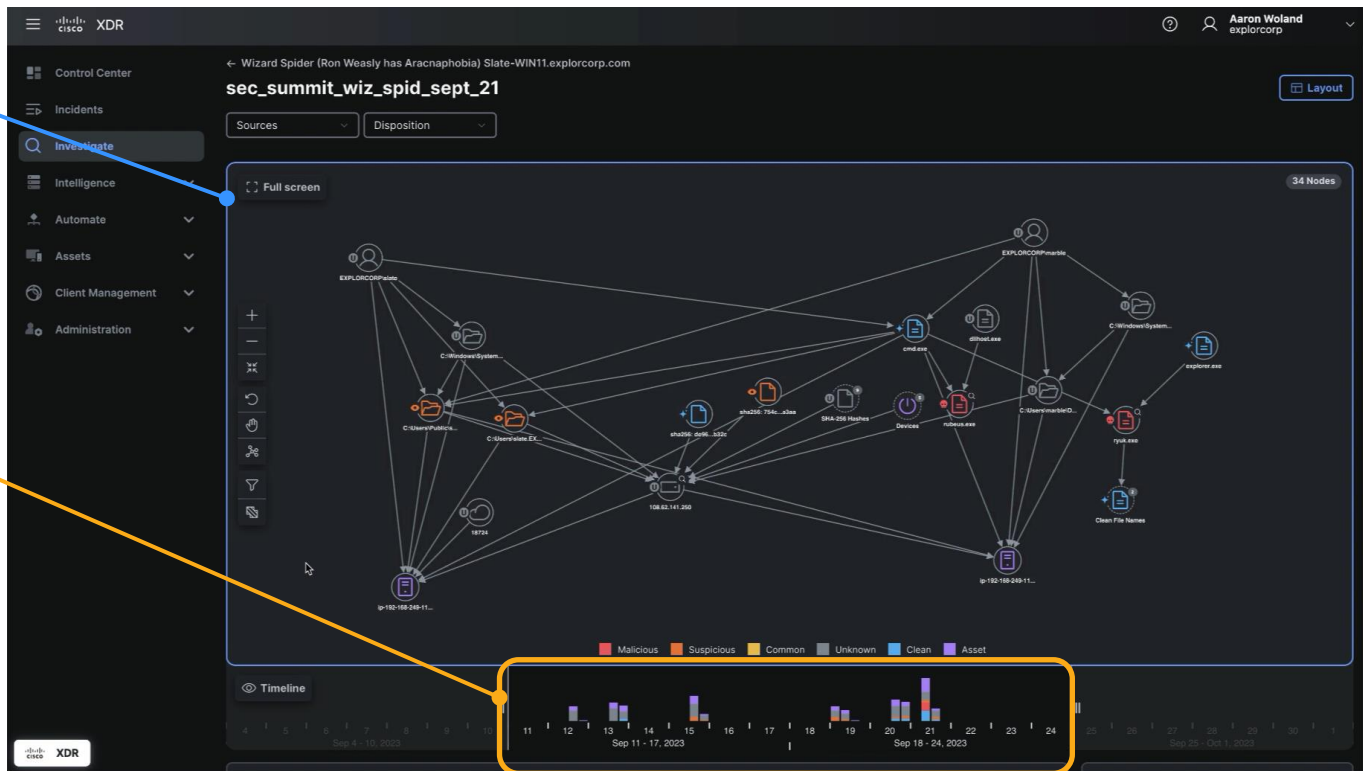
Timeline in Cisco XDR

Interactive Graph

Interactive Graph displays & groups the entities involved in the incident

Timeline

Interactive: drag it, select a portion, zoom in & out





Control Center



Incidents



Investigate



Intelligence



Automate



Assets



Client Management



Administration

← Wizard Spider (Ron Weasley has Aracnaphobia) Slate-WIN11.explorcorp.com

sec_summit_wiz_spid_sept_21

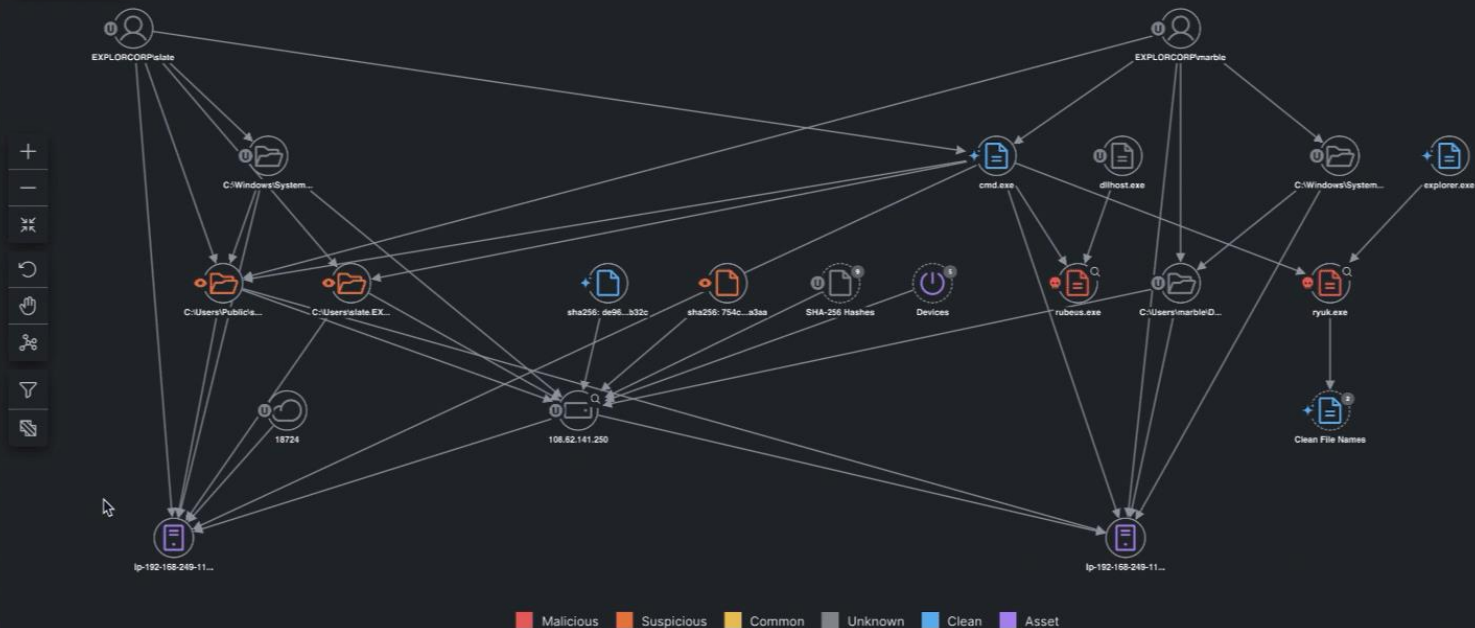
Layout

Sources

Disposition

Full screen

34 Nodes



Timeline

4 5 6 7 8 9 10
Sep 4 - 10, 202311 12 13 14 15 16 17
Sep 11 - 17, 202318 19 20 21 22 23 24
Sep 18 - 24, 202325 26 27 28 29 30 1
Sep 25 - Oct 1, 2023

Incident manager

Incidents

62 Incidents

33 New Incidents

8 Open

Search

62 matching results

Filters

☐	Priority	Name	Source
☐	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]	Formu
☐	928	F1.03-06d.Critical.TTP(58).AssetValue[10]	Formu
☐	835	Attack Graph Test - 109 Observables	Formu
☐	800	F1.03-06a.Critical.TTP(50).AssetValue[NULL]	Formu
☐	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]	Formu

Incident manager



Centralized incident management

Incidents from a wide portfolio of products, all in one place



Automated prioritization

Risk- and asset-based prioritization, so you know what to investigate first



Built-in response workflows

Automated actions that make resolving an incident simpler and faster

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 Detected
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

View Incident Detail

MITRE ATT&CK View all Tactics

Tactics

TA0002: Execution 100

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

TA0008: Lateral Movement 66

Orientation

```
graph LR
    NT[NT AUTHORITY\SYSTEM] --- C[C:\Windows\System...]
    C --- VM2[virtualmachines/win-vic-2]
    C --- VM0[virtualmachines/win-dc-0]
    C --- VM6[virtualmachines/win-vic-6]
    C --- VMK[virtualmachines/kali]
    VM2 --- DC1[dc-2.org1.net]
    VM0 --- DC2[dc-2.org1.net]
    VM6 --- DC2
    VMK --- DC2
    DC1 --- IP[10.0.1.6]
    DC2 --- IP
    IP --- NT
    IP --- C
    IP --- VM2
    IP --- VM0
    IP --- VM6
    IP --- VMK
```

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

$$\text{Priority Score} = \text{Detection Risk} \times \text{Asset Value}$$

0-1000 0-100 0-10

The 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 represents the value of the assets involved in the incident

523 Incidents

523 Incidents

12 New Incidents

343 Open Incidents

Search

11 matching results

Filters

Status: Incident Reported ×

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

- Control Center
- Incidents
- Investigate
- Intelligence
- Automate
- Devices
- Administration

← Incidents

1000 Incident Reported ▾

Geographically Unusual Remote Access for Cisco - Lawrenceville Lab ...

View Investigation

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

AS HJ ST

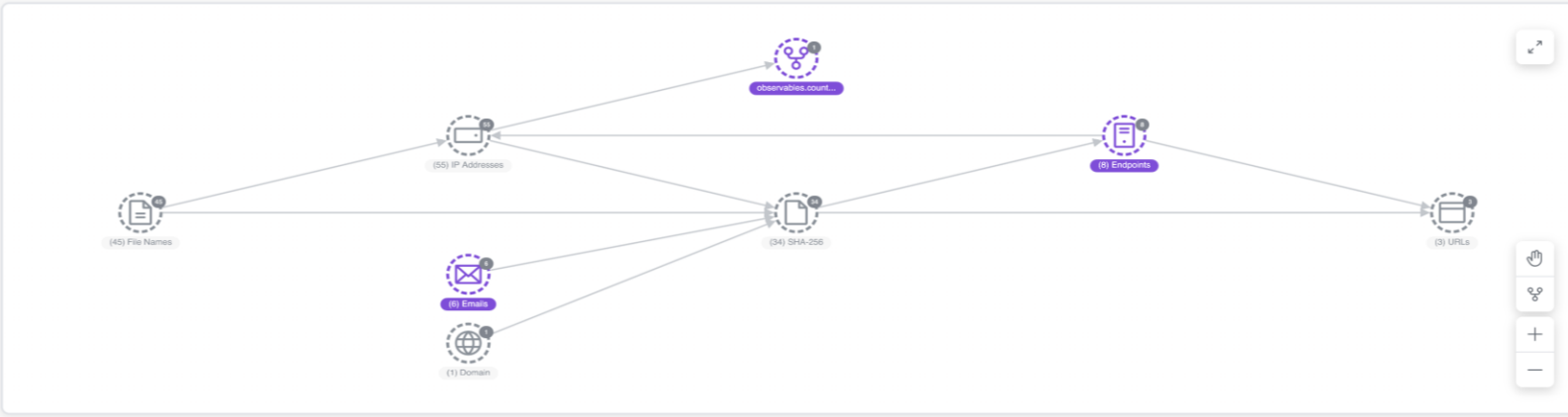
Geographically Unusual Remote Access on i-0c6069f352916581e [View Long Description](#)

Overview

Detection

Response

Worklog



19 Assets [View all](#)

TOP ACTIVE

172.31.81.151

1,098 events

MIKE-WIN10

368 events

EC2AMAZ-AHQFEJR

250 events

41 Observables [View all](#)

TOP ACTIVE

200.75.2.138

13,991 events

196.221.71.221

10,778 events

189.164.140.152

7,084 events

33 Indicators [View all](#)

TOP ACTIVE

Cisco Secure Cloud Analytics (cisco-explorcorp-earth)
Internal Connection Watchlist

14 events

Cisco Secure Network Analytics
Port Scan

13 events

1000

Incident Reported ▾

Geographically Unusual Remote Access for Cisco - Lawrenceville Lab ...

QUESTION

[View Investigation](#)

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

Type Source Severity

☒ Important only

First Seen	Severity	Source	Indicators	Observables	Assets
2023-04-17T15:18:17.000Z	High	Secure Endpoint	W32.PowershellDownloadedEx...	de96a6e69944335375dc1ac2...	EC2AMAZ-AHQFEJR
2023-04-17T13:10:44.00...	High	NGFW Event Service	Security Intelligence event - IP...	172.10.1.63 123.123.123.123	172.10.1.63
2023-04-17T13:10:36.00...	High	NGFW Event Service	Security Intelligence event - IP...	172.10.1.63 6.6.6.6	172.10.1.63
2023-04-17T12:10:00.00...	Critical	Cisco Secure Cloud Analyti...	Watchlist Interaction	6.6.6.6	adsl-172-10-1-63.d...
2023-04-17T12:10:00.00...	Critical	Cisco Secure Cloud Analyti...	Watchlist Interaction	6.6.6.6	adsl-172-10-1-63.d...
2023-04-17T12:10:00.00...	Critical	Cisco Secure Cloud Analyti...	User Watchlist Hit		adsl-172-10-1-63.d...
2023-04-17T12:10:00.00...	Critical	Cisco Secure Cloud Analyti...	Watchlist Interaction	6.6.6.6	adsl-172-10-1-63.d...
2023-04-17T12:10:00.00...	Critical	Cisco Secure Cloud Analyti...	Watchlist Interaction	6.6.6.6	adsl-172-10-1-63.d...
2023-04-17T10:21:25.000Z	High	Cisco Secure Network Anal...	Port Scan	196.221.71.221 172.31.89.198	
2023-04-17T10:06:33.00...	High	Cisco Secure Network Anal...	Port Scan	200.75.2.138 172.31.89.198	

- 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-0d3309a793147aefe
- ☐ 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

Execute



Incident response in four stages

Identify



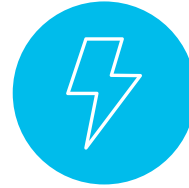
Review the incident and confirm the findings

Contain



Act against impacted hosts, domains, files, etc.

Eradicate



Remediate vulnerabilities and remove malicious content

Recover



Validate remediation and restore impacted services

Investigate

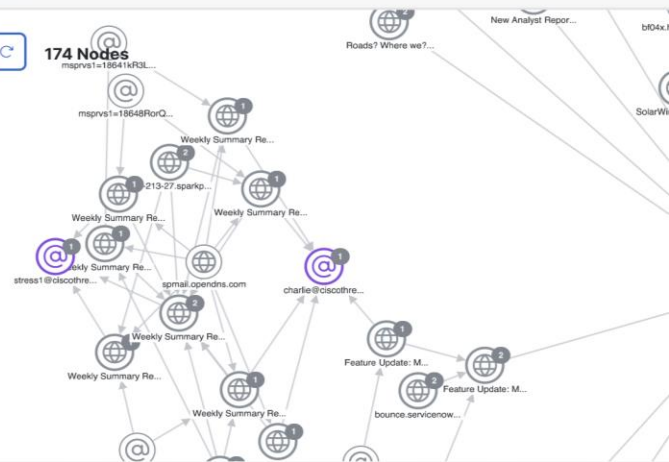
Email Threat Investigation

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

Investigate



One place to investigate across products

Aggregated intelligence from all your integrated products



Interactive visualization of investigation elements

Drag, drop, and inspect the results of your investigation



Built-in response actions

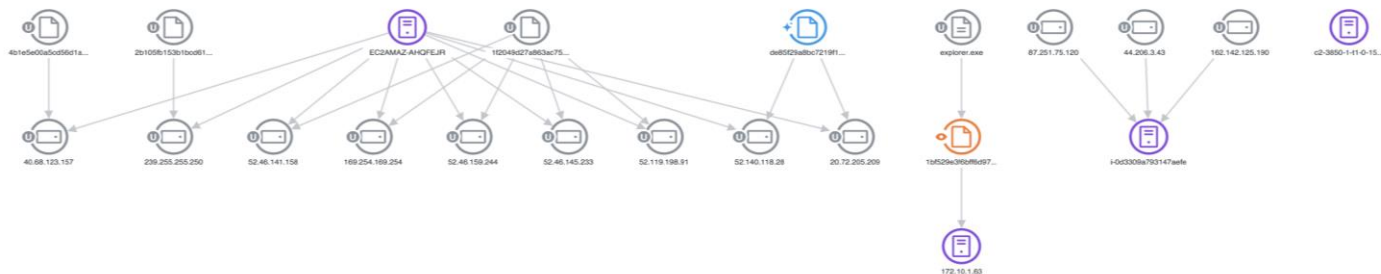
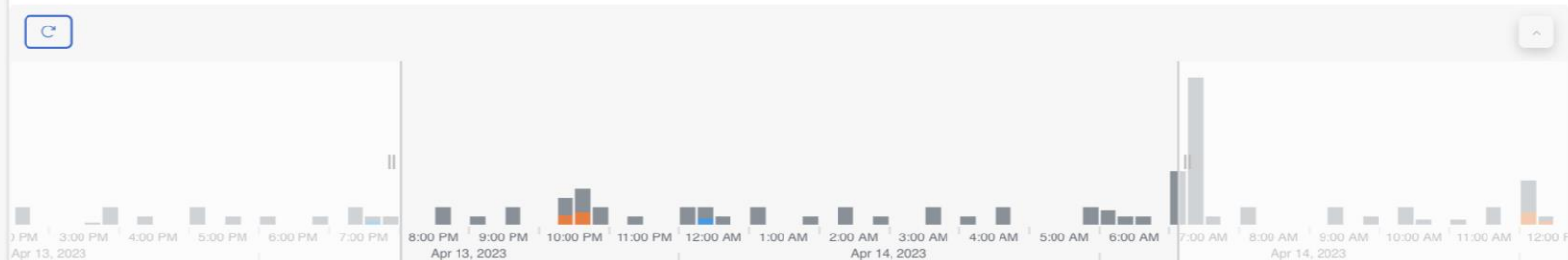
Take action right from an investigation, no cross-launching into other products required

Golden Incident 4_17 V6 shapshot

Save Investigation

Types ▾

22 Nodes

First Seen Severely 

Source

Indicators

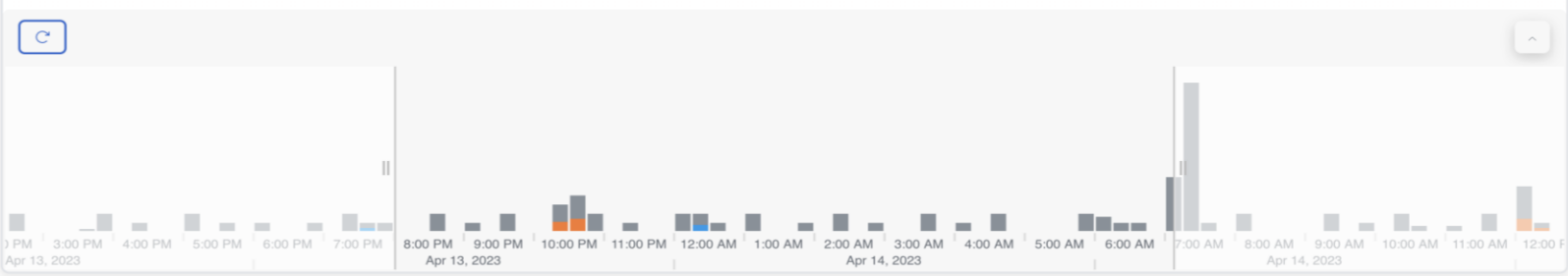
Observables

Assets

Indicators

17

- 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-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...

Indicators 17

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

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

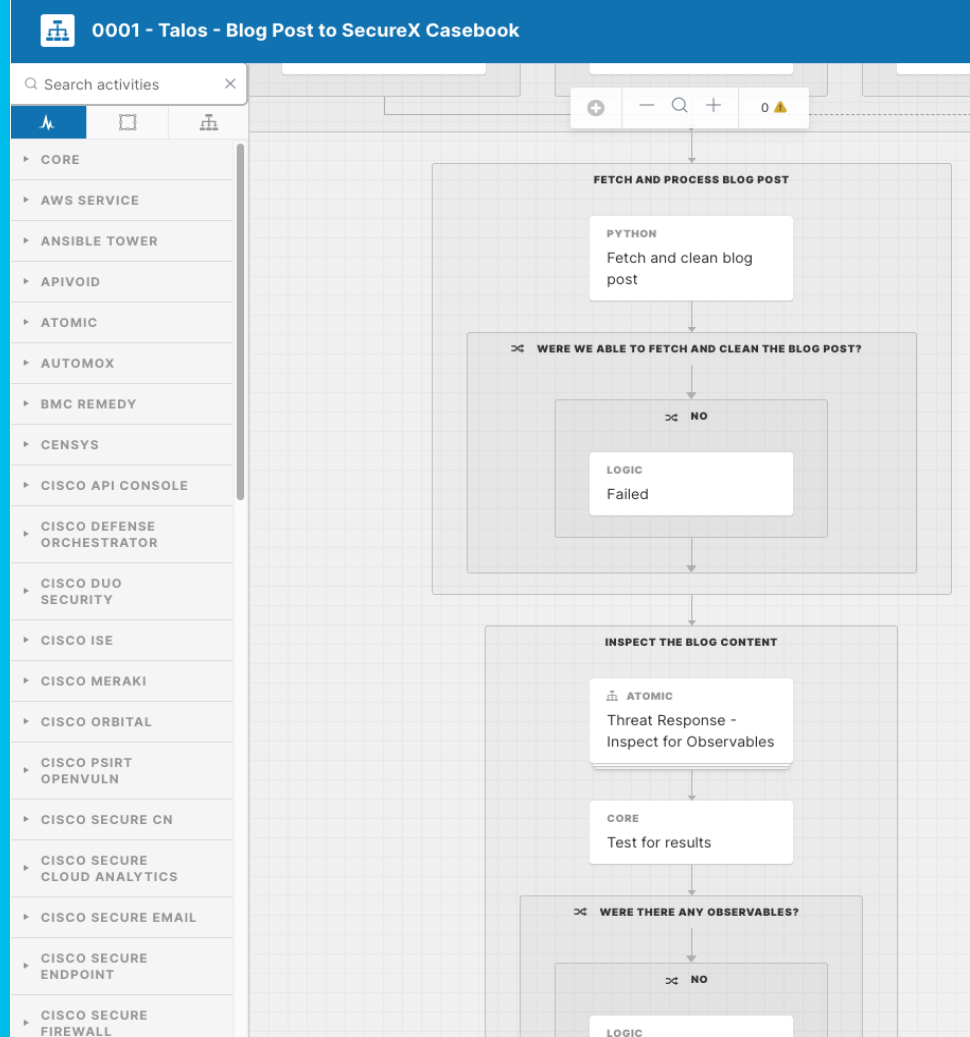
Secure Endpoint
ExecutedMalware.ioc 2 events

AlienVault OTX
muestra 2 events
known malicious high true filesa256
+32

AlienVault OTX
muestra 2 events
known malicious high true filesa256
+32

NGFW Event Service 2 events

Automation



Automation



Drag and drop, "no-to-low code" workflow builder

Simple workflow editor that works without writing a single line of code



Accelerates how you investigate and respond

Automate how your analysts investigate and respond



Out of the box workflows from Cisco

Popular use cases built in, more available for import from Cisco



Search activities



CORE

AWS SERVICE

ANSIBLE TOWER

CISCO API CONSOLE

CISCO DEFENSE
ORCHESTRATOR

CISCO DUO SECURITY

CISCO ISE

CISCO MERAKI

CISCO ORBITAL

CISCO PSIRT
OPENVULNCISCO SECURE CLOUD
ANALYTICS

CISCO SECURE EMAIL

CISCO SECURE
ENDPOINTCISCO SECURE
FIREWALLCISCO SECURE
FIREWALL (SSE)CISCO SECURE
MALWARE ANALYTICSCISCO SECURE
NETWORK ANALYTICS

CISCO SECURE



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

Devices

Device View

All DevicesSecure Client Devices

×

Source Health

9 Devices

100%

Types

Server (1)

Desktop (5)

Virtual (0)

Mobile (2)

Status

Managed (1)

Unmanaged (8)

×

Filters

Select Saved Filter

Text Search

Q User, IP, hostname...

Managed Status

Select

Operating System

Select

Device Value

Select

Labels

Select

Sources

Select

☐ AV Definitions out of date (0)

9 Devices found

0 Devices Selected

Update Value

Update Labels

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

BRKSEC-1023

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

66

Devices



Extensive visibility into your devices

Combined inventory from both security and device management products



Provides asset context to investigations

Differentiate between a generic target and an asset that belongs to you



Configuration and management of Cisco Secure Client

Cloud-based management of Secure Client profiles and deployments

Supported sources



Duo Access
Duo Beyond



Secure Endpoint



Umbrella (DNS)
Windows / macOS



Meraki SM



Secure Client



Orbital

Third Party



CrowdStrike



SentinelOne



Microsoft Intune



Jamf Pro



Ivanti Neurons
(formerly MobileIron)



VMware
Workspace ONE
(formerly Airwatch)

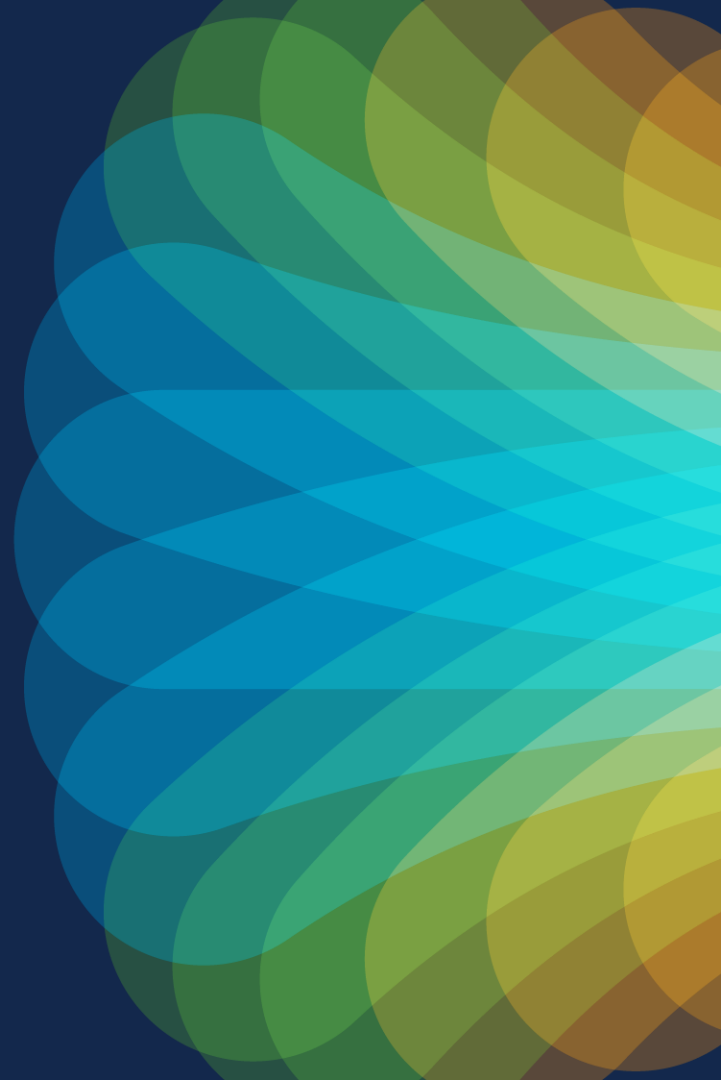
One more
thing...



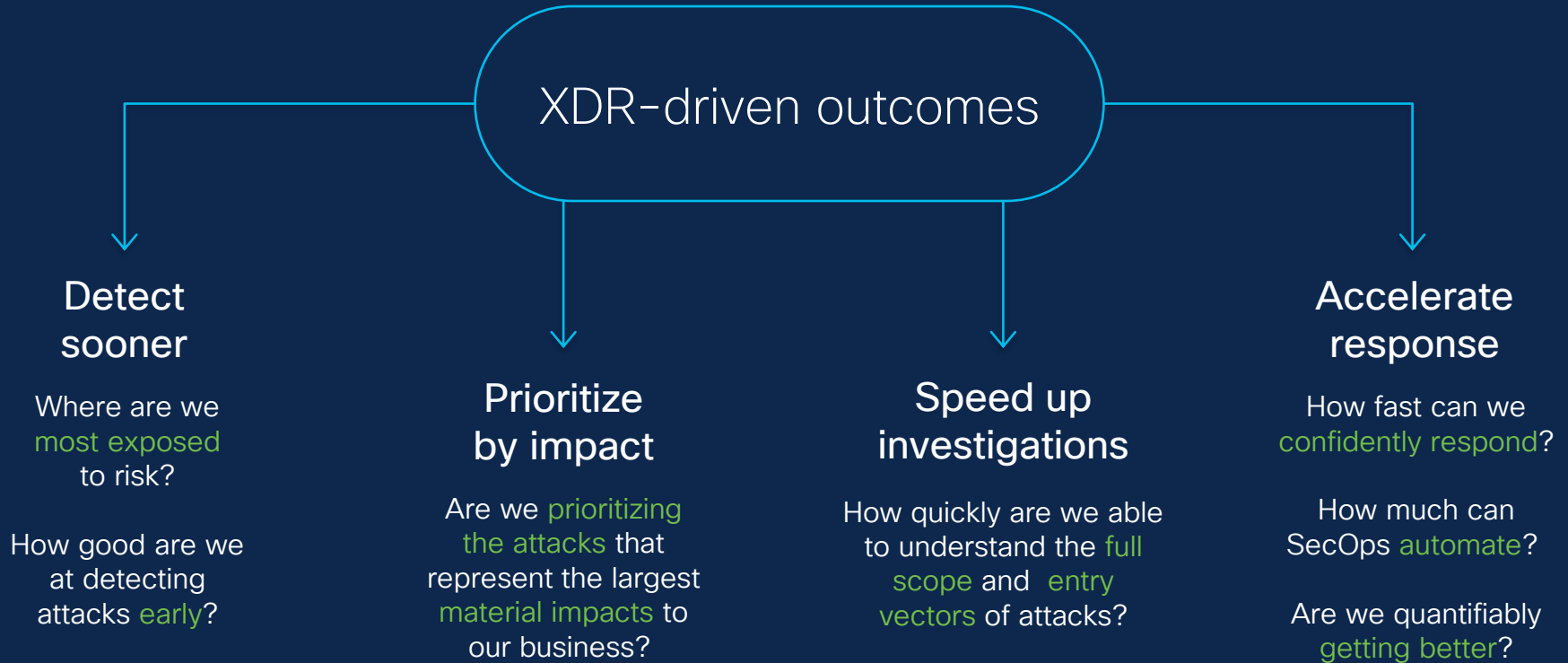
XDR has a robust set of APIs!

- 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

To summarize



Shift the focus to outcomes



Stop advanced threats like ransomware

Most attacks use a sequence like this...



Email



DNS



010110
110010
001011

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

Which goes to a questionable web site...

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

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

T1055: Process Injection

T1566: Spear phishing

T1189: Drive-by Compromise

T1570: Lateral Tool Transfer

T1087: Account Discovery: Domain Account

T1048: System Network Connections Discovery

Vendor A

Vendor C

Vendor E

Vendor G

Vendor D

Quickly position teams to achieve incremental XDR milestones

Integrate

Consolidate solutions and technology with an integrated platform



Orchestrate

Enable prioritized detection and response using AI & ML



Optimize

Evolve, and fine tune security by proactively executing against that baseline



Unify

Build an ecosystem that aggregates, enriches data and telemetry from all part of your environment



Automate

Automate detection and response workflows that require minimal human intervention



Resources

Other XDR sessions



Matthew Robertson
Distinguished TME

Extended Detection with
Cisco XDR: Security
analytics across the
enterprise

BRKSEC-2178

Wednesday @ 4:00 PM



Aaron Woland
Distinguished TME

Cisco's Unified Agent:
Cisco Secure Client.
Bringing AMP,
AnyConnect, Orbital &
Umbrella together

BRKSEC-2834

Thursday @ 9:00 AM



Aaron Woland
Distinguished TME

Cisco XDR - Making sense
of the Solution and how it's
a Security Productivity Tool

BRKSEC-2113

Friday @ 1:30 PM



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

Participating in user research gives you a place to share your thoughts and experiences to influence the future of Cisco Secure products.

- You'll hear from us at most once every 90 days.
- Participation is completely optional, and you can opt out at any time.



CISCO *Live!*

Did you know?

You can have a
one-on-one session with
a technical expert!

Visit Meet the Expert in The HUB
to meet, greet, whiteboard & gain
insights about your unique questions
with the best of the best.



Meet the Expert Opening Hours:

Tuesday	3:00pm – 7:00pm
Wednesday	11:15am – 7:00pm
Thursday	9:30am – 4:00pm
Friday	10:30am – 1:30pm

Capture the Flag

The Hub in the World of Solutions

Tuesday	9:00 a.m. – 5:30 p.m.
Wednesday	8:00 a.m. – 5:30 p.m.
Thursday	8:00 a.m. – 5:30 p.m.
Friday	9:00 a.m. – 1:30 p.m.

Learn Technology using your problem-solving skills and ignite your competitive spirit with our immersive and educational Capture the Flag – Gamified Hands-on Labs!

Now you can earn **Cisco Continuing Education Credits** by playing select Capture the Flag Missions at Cisco Live. Redeem them to renew your Cisco Certifications!



Session Surveys

We would love to know your feedback on this session!

- Complete a minimum of four session surveys and the overall event surveys to claim a Cisco Live T-Shirt



Getting started

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 Buyer's Guide](#)

[Cisco XDR on Cisco.com](#)





The bridge to possible

Thank you

CISCO *Live!*

#CiscoLiveAPJC

The background of the slide is a vibrant, abstract graphic. It features a large, stylized cloud shape on the left side, composed of overlapping, semi-transparent layers of orange, red, and yellow. To the right of the cloud, a bright, multi-colored sunburst or starburst pattern radiates from a central point, with rays extending towards the right edge of the frame. The colors in the sunburst transition through a spectrum from blue and purple on the left to yellow and orange on the right. The overall effect is energetic and celebratory.

cisco *Live!*

Let's go

#CiscoLiveAPJC