Cisco XDR + Meraki MX Native Network Integration

The Power of the SNOC: Security and Network Operations Unified

Cisco XDR excels at connecting and correlating data and telemetry from every tool deployed across diverse security stacks, so defenders detect more, act decisively, and elevate productivity. It's the fastest, easiest way to integrate threat detection, investigation, and response (TDIR) into your security posture and eliminate most, if not all, security operations (SecOps) gaps. But it hasn't addressed the blind spot that continues to challenge organizations of all sizes, which is the one between security and network operations.

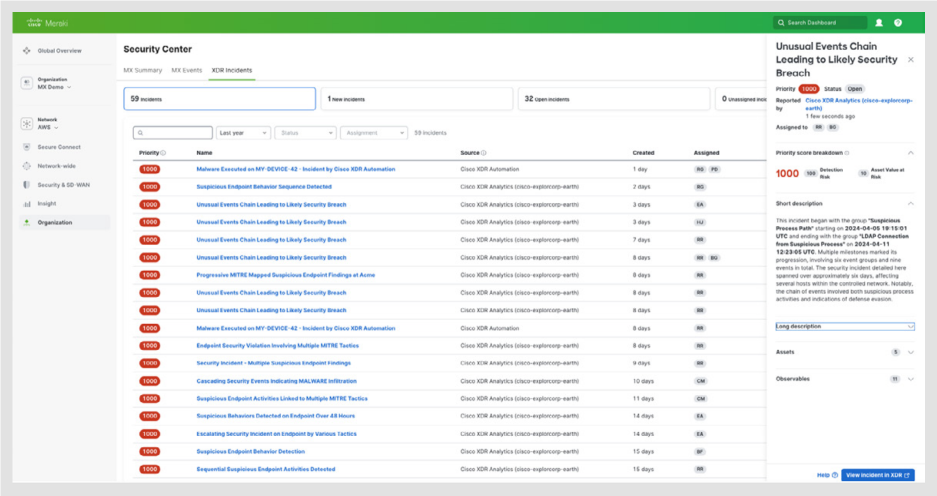
Until now.

Through our native integration for the Cisco Meraki MX portfolio with Cisco XDR, we have given rise to the Security and Network Operations Center (SNOC). This creates a bi-directional advantage for security and network operations, giving security analysts valuable TDIR insights from the network, eliminating that blind spot, and allowing network administrators to proactively monitor emerging threats within their environment.

Benefits

Enhanced threat detection: Meraki log data seamlessly integrates with Cisco XDR to significantly improve the early detection of suspicious activities and threats. An endpoint security finding alone may not provide enough information to assess its impact. But when Cisco XDR links it with a corresponding network alert, the incident can be marked as high priority and managed accordingly.

Unified visibility, simplified operations: With just one click, Cisco XDR can be integrated into the Meraki dashboard, providing network admins with a mirrored view of XDR Incidents. This gives network admins an early warning of developing threats that could impact the network availability and uptime, so they can assign incidents to their security counterparts or adjust the event status.



Security Center

MX Summary | MX Events | XDR Incidents

59 Incidents | 1 New incidents | 32 Open incidents | 0 Unassigned incid

Last year | Status | Assignment | 59 Incidents

Priority	Name	Source	Created	Assigned
1000	Malware Executed on MY-DEVICE-42 - Incident by Cisco XDR Automation	Cisco XDR Automation	1 day	RG PD
1000	Suspicious Endpoint Behavior Sequence Detected	Cisco XDR Analytics (cisco-explorcorp-earth)	2 days	RG
1000	Unusual Events Chain Leading to Likely Security Breach	Cisco XDR Analytics (cisco-explorcorp-earth)	3 days	EA
1000	Unusual Events Chain Leading to Likely Security Breach	Cisco XDR Analytics (cisco-explorcorp-earth)	3 days	HJ
1000	Unusual Events Chain Leading to Likely Security Breach	Cisco XDR Analytics (cisco-explorcorp-earth)	7 days	RR
1000	Unusual Events Chain Leading to Likely Security Breach	Cisco XDR Analytics (cisco-explorcorp-earth)	8 days	RR BG
1000	Progressive MITRE Mapped Suspicious Endpoint Findings at Acme	Cisco XDR Analytics (cisco-explorcorp-earth)	8 days	RR
1000	Unusual Events Chain Leading to Likely Security Breach	Cisco XDR Analytics (cisco-explorcorp-earth)	8 days	RR
1000	Unusual Events Chain Leading to Likely Security Breach	Cisco XDR Analytics (cisco-explorcorp-earth)	8 days	RR
1000	Malware Executed on MY-DEVICE-42 - Incident by Cisco XDR Automation	Cisco XDR Automation	8 days	RR
1000	Endpoint Security Violation Involving Multiple MITRE Tactics	Cisco XDR Analytics (cisco-explorcorp-earth)	8 days	RR
1000	Security Incident - Multiple Suspicious Endpoint Findings	Cisco XDR Analytics (cisco-explorcorp-earth)	9 days	RR
1000	Cascading Security Events Indicating MALWARE Infiltration	Cisco XDR Analytics (cisco-explorcorp-earth)	10 days	CM
1000	Suspicious Endpoint Activities Linked to Multiple MITRE Tactics	Cisco XDR Analytics (cisco-explorcorp-earth)	11 days	CM
1000	Suspicious Behaviors Detected on Endpoint Over 48 Hours	Cisco XDR Analytics (cisco-explorcorp-earth)	14 days	EA
1000	Escalating Security Incident on Endpoint by Various Tactics	Cisco XDR Analytics (cisco-explorcorp-earth)	14 days	EA
1000	Suspicious Endpoint Behavior Detection	Cisco XDR Analytics (cisco-explorcorp-earth)	15 days	BF
1000	Sequential Suspicious Endpoint Activities Detected	Cisco XDR Analytics (cisco-explorcorp-earth)	15 days	RR

Unusual Events Chain Leading to Likely Security Breach

Priority 1000 Status Open

Reported by Cisco XDR Analytics (cisco-explorcorp-earth)
1 few seconds ago

Assigned to RR BG

Priority score breakdown

1000 100 Detection Risk 10 Asset Value at Risk

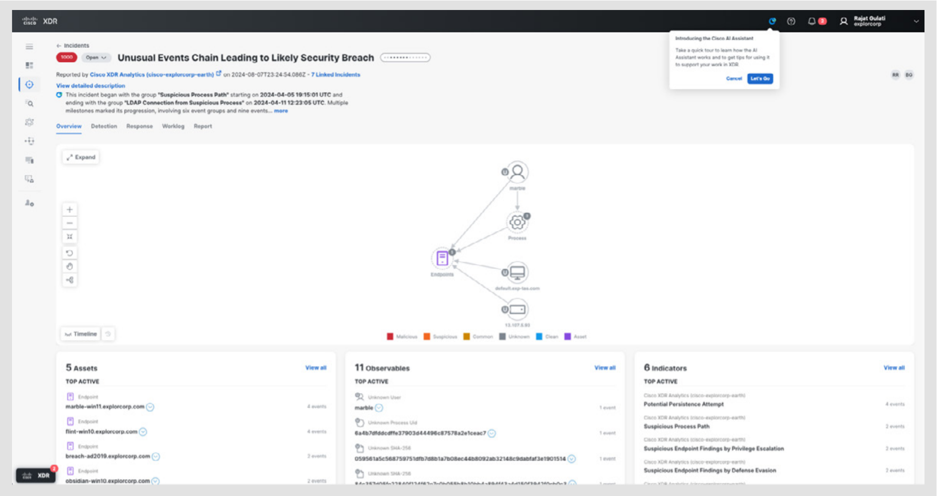
Short description

This incident began with the group **"Suspicious Process Path"** starting on **2024-04-05 19:15:01 UTC** and ending with the group **"LDAP Connection from Suspicious Process"** on **2024-04-11 12:23:05 UTC**. Multiple milestones marked its progression, involving six event groups and nine events in total. The security incident detailed here spanned over approximately six days, affecting several hosts within the controlled network. Notably, the chain of events involved both suspicious process activities and indications of defense evasion.

Long description

Assets 5

Observables 11



← Incidents

1000 Open Unusual Events Chain Leading to Likely Security Breach

Reported by Cisco XDR Analytics (cisco-explorcorp-earth) on 2024-08-07T23:24:54.086Z - 7 Linked Incidents

View detailed description

This incident began with the group **"Suspicious Process Path"** starting on **2024-04-05 19:15:01 UTC** and ending with the group **"LDAP Connection from Suspicious Process"** on **2024-04-11 12:23:05 UTC**. Multiple milestones marked its progression, involving six event groups and nine events... more

Introducing the Cisco AI Assistant

Take a quick tour to learn how the AI Assistant works and to get tips for using it to support your work in XDR

5 Assets — View all

TOP ACTIVE

Endpoint
marble-win11.explorcorp.com — 4 events

Endpoint
flint-win10.explorcorp.com — 4 events

Endpoint
breach-ad2019.explorcorp.com — 2 events

Endpoint
obsidian-win10.explorcorp.com — 2 events

11 Observables — View all

TOP ACTIVE

Unknown User
marble — 1 event

Unknown Process Uid
6a4b7dfddcdffe37903d44496c87578a2e1ceac7 — 1 event

Unknown SHA-256
059561a5c568759751dfb7d8b1a7b08ec44b8092ab32148c9dabfaf3e1901514 — 1 event

6 Indicators — View all

TOP ACTIVE

Cisco XDR Analytics (cisco-explorcorp-earth)
Potential Persistence Attempt — 4 events

Cisco XDR Analytics (cisco-explorcorp-earth)
Suspicious Process Path — 2 events

Cisco XDR Analytics (cisco-explorcorp-earth)
Suspicious Endpoint Findings by Privilege Escalation — 2 events

Cisco XDR Analytics (cisco-explorcorp-earth)
Suspicious Endpoint Findings by Defense Evasion — 2 events

Administrators have access to Cisco XDR Incidents directly within the Meraki Dashboard.

When the "View incident in XDR" button is clicked in the Meraki dashboard...

...the administrator is taken to the Incident view within Cisco XDR.

Sharp Focus, Clear and Timely Action

Most of the extended detection and response (XDR) solutions available today take an endpoint-focused approach to security. But more than half of the devices in most environments can't run endpoint agents and many threats don't originate on an endpoint. While some tools have evolved to collect data from email, firewall, and identity products, they still fail to account for the connective tissue linking these disparate security control points: The Network. As a result, security and network admins alike get a blurry, incomplete view of what's going on in their environments.

Through this native integration with Meraki devices, Cisco XDR can uniquely leverage network connection data to fill in the blanks between security events. This provides security analysts with enhanced visibility into lateral movement beyond what EDR-based solutions can deliver, helping them track the progression of an attack for more informed and timely actions.

For network admins, this one-click integration within the Meraki Dashboard reveals early warning signs of suspicious incidents so they can assign the task to security analysts for further investigation, rather than the old model of waiting for 'Breaking News' from their security counterparts.

Seize the Power of the SNOC today

Are your security and network teams struggling to fill the gap where security meets the network with hidden, unfocused, and incomplete information? Cisco XDR, with its native Meraki MX network integration, can close that gap so your teams realize the power of secure network operations. To learn more, visit www.cisco.com/go/xdr.