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. 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. ıılıılı cısco

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.

Until now.

ılıılı cısco

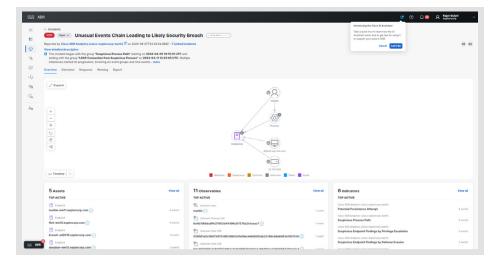
dede Moraki						Q Search Dashboard	0
 Olobal Overview Organization MX Demo ~ 	Security Center Mit Summary Mit Events XXX Receivers					Unusual Events Chain Leading to Likely Security Breach	
	59 incidents	1 New incidents	32 open incidents		O unassigned incid	by earth)	
Network AWS V	Q. Lastyne v) Saturn v) Moderns					1 few seconds ago Assigned to (BB) (BD)	
Secure Connect	Priority Name		Source ()	Created	Assigned	Priority score breakdown O	
> Network-wide	Malware Executed on MY-DEVICE-42	- Insident by Cisco XDR Automation	Cisco XDR Automation	1 day	(86) (90)	1000 Sop Detection So Asset	Asset Value at
Security & SD-WAN	5000 Suspicious Endpoint Behavior Sequer	ce Detected	Cisco XDR Analytics (cisco-explorcorp-earth)	2 days	85		
d Insight	Unusual Events Chain Leading to Like	Unusual Events Chain Leading to Likely Security Breach		3 days	(K)	Short description	
1. Organization	1000 Unusual Events Chain Leading to Like	Unusual Events Chain Leading to Likely Security Breach		3 days	(HJ)	This incident began with the group "Suspicious Process Path" starting on 2024-04-05 19:15:	
	Unusual Events Chain Leading to Like	Unusual Events Chain Leading to Likely Security Breach		Cisco XDR Analytics (cisco-explorcorp-earth) 7 days		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	
	Unusual Events Chain Leading to Like	Unusual Events Chain Leading to Likely Security Breach		Cisco XDR Analytics (cisco-explorcorp-earth) & days			
	1000 Progressive MITRE Mapped Suspiciou	Progressive MITRE Mapped Suspicious Endpoint Findings at Acme Unusual Events Chain Leading to Likely Security Breach		8 days		events in total. The security incident detailed he spanned over approximately six days, affecting several hosts within the controlled network. Not	cting
	Unusual Events Chain Leading to Like			Cisco XDR Analytics (cisco-explorcorp-earth) 8 days		the chain of events involved both suspicious pro activities and indications of defense evasion.	us proe
	1000 Unusual Events Chain Leading to Like	Unusual Events Chain Leading to Likely Security Breach		Cisco XDR Analytics (cisco-explorcorp-earth) 8 days			
	Malware Executed on MY-DEVICE-42	Malware Executed on MY*DEVICE+42 - Incident by Cisco XDR Automation		8 days		Long description	
	Endpoint Security Violation Involving	Endpoint Security Vielation Involving Multiple MITRE Tactics		8 days	(86)	Assets	
	1000 Security Incident - Multiple Suspiciou	Security Incident - Multiple Suspicious Endpoint Findings		9 days			
	Cascading Security Events Indicating	Cascading Security Events Indicating MALWARE Infiltration		10 days	(CM)	Observables	(B)
	Suspicious Endpoint Activities Linked	Suspicious Endpoint Activities Linked to Multiple MITRE Tectics		11 days	(CM)		
	1000 Suspicious Behaviors Detected on En	Suspicious Behaviors Detected on Endpoint Over 48 Hours		14 days	(BA)		
	Escalating Security Incident on Endpo	Escalating Security Incident on Endpoint by Various Tactics		Cisco XDR Analytics (cisco-explorcorp-earth) 14 days			
	5000 Suspicious Endpoint Dehavior Detecti	Suspicious Endpoint Dehavior Detection		Cisco XDR Analytics (cisco-explorcorp-earth) 15 days			
	1000 Sequential Suspisious Endpoint Activ	1000 Sequential Suspisious Endpoint Activities Detected		15 days	(88)	Helb () View Incident I	_

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...

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.



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

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 <u>www.cisco.com/go/xdr</u>.