



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.

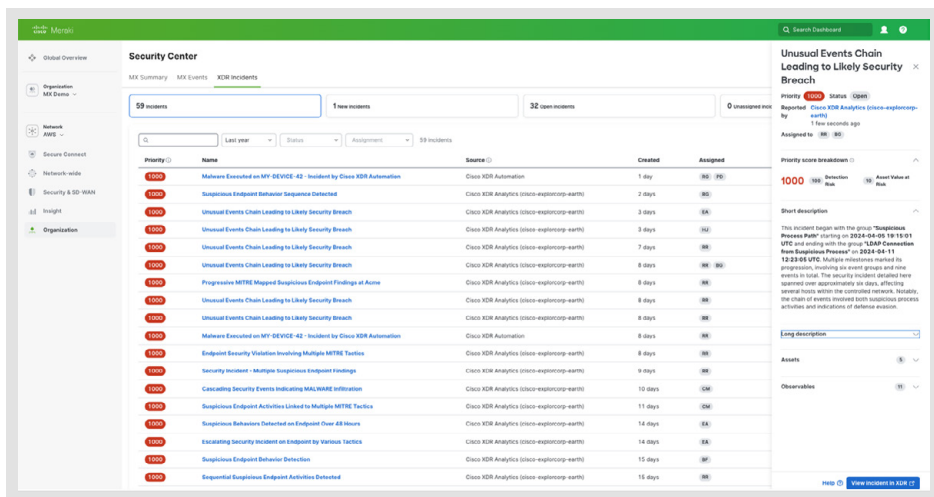
Benefits

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.

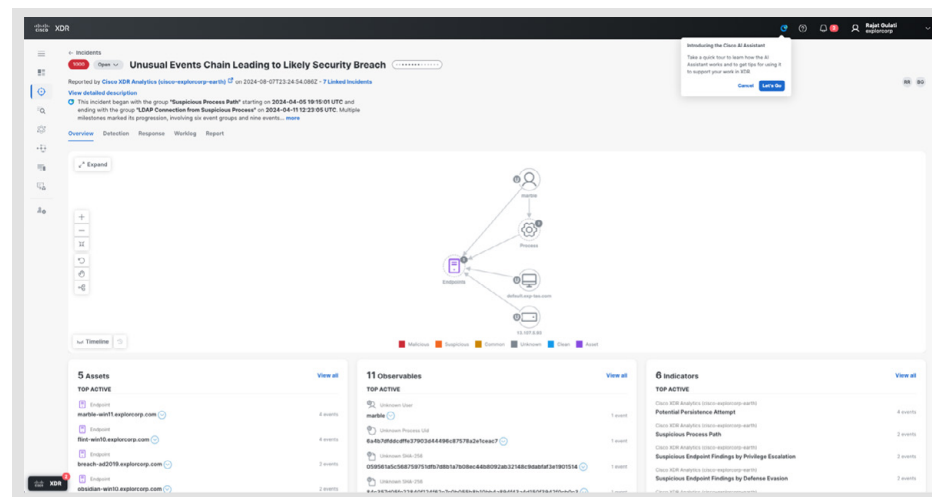
Unified visibility, simplified operations:

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.



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.