Qualys Context XDR (Extended Detection and Response)

Cisco Meraki Network Device

Data Mapping Guide

April 22, 2022

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100

Table of Contents

About this Guide

Thank you for your interest in Extended Detection and Response (XDR). Qualys Context XDR expands the capabilities of the Qualys Cloud Platform to integrate data points from other Qualys products offer a unified view of your organization's security posture. Context XDR integrates data points (events/logs) from your enterprise's ecosystem that comprises of several heterogenous sources. This data is normalized, enriched and then categorized before storing it in the Qualys Context XDR data model. This unified database that holds data points from multiple security applications is then used to offer a 360° view of your organization's security posture — all from a single solution.

The Data Mapping Guides provide a list of the fields received through a data source and how these fields are mapped to the Context XDR data model.

About Qualys

Qualys, Inc. (NASDAQ: QLYS) is a pioneer and leading provider of cloud-based security and compliance solutions. The Qualys Cloud Platform and its integrated apps help businesses simplify security operations and lower the cost of compliance by delivering critical security intelligence on demand and automating the full spectrum of auditing, compliance, and protection for IT systems and web applications.

Founded in 1999, Qualys has established strategic partnerships with leading managed service providers and consulting organizations including Accenture, BT, Cognizant Technology Solutions, Deutsche Telekom, Fujitsu, HCL, HP Enterprise, IBM, Infosys, NTT, Optiv, SecureWorks, Tata Communications, Verizon and Wipro. The company is also a founding member of the Cloud Security Alliance (CSA). For more information, please visit www.qualys.com.

Qualys Support

Qualys is committed to providing you with the most thorough support. Through online documentation, telephone help, and direct email support, Qualys ensures that your questions will be answered in the fastest time possible. We support you 7 days a week, 24 hours a day. Access support information at http://www.qualys.com/support/.

Overview

Qualys Context Extended Detection and Response (XDR) can be configured to ingest data from several different data sources. Each data source has its own data points, and this Data Mapping Guide offers insight into how these data points are interpreted, normalized, and mapped in Qualys Context XDR.

This guide focuses on the data mapping between Cisco Meraki Network Device fields and the Qualys data model.

Note: For a complete list of sources that Qualys XDR supports, on the Qualys XDR UI, navigate to **Configuration** > **Data Collection** > **Catalog**. If the source you are looking for is not in the catalog, you can add a request for support using the **Not in the list?** card. Based on the requests coming in, Qualys will prioritize and attempt to add support at the earliest.

Device Details

- **Device Type** – Network Device
- **Device Vendor** – Cisco Meraki
- **Device Product** – Cisco Meraki Network Device
- **Supported Versions** – Limited Support – Contact your TAM for further information.

Supported Formats

In Qualys Context XDR, you can configure to receive data from Cisco Meraki Network Device using the following formats:

- **Syslog**

For information on configuring collectors, refer to the Deploying a Collector section in the Online Help.

Data Field Mappings

This section provides a detailed mapping of the data source fields to the Context XDR.

deviceType – Network Device
deviceVendor – Cisco Meraki

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
-	eventTime	1386337584	Time of the audit event log.
-	dvcHost	MX84	Metadata field
-	evtName	events,urls	Brief standard meaning of the message easy to read for Analyst
type	evtType	vpn_connectivity_change	Type of the event.
vpn_type	evtSubType	site-to-site	SubType of the event associated with EventType field.
peer_contact/ src	srcIpv4	10.10.10.100	IPv4 address of the source machine
sport	spt	51856	Port used on the source machine
connectivity	outcome	false	Outcome of the event
-	dscrp	Cellular connection down, failover to wan1	Description from the audit event log.
mac	sMac	A1:11:B2:XX:XX:XX	Mac address of the source machine
mac	dMac	3C:22:33:XX:XX:XX	Mac address of the destination machine
dst	dstIpv4	10.10.100.40:80	IPv4 address of the destination machine
dport	dpt	80	Port used on the destination machine
request	method	GET	Method used to Request the URL.
	reqUrl	http://www.meraki.com/	URL Requested in the event log
protocol	prt	udp	Protocol used to make/facilitate the request as present in the audit log

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
priority	dvcSeverity	2	Severity details for the event log as per the device which is producing the audit events
direction	dir	egress	Direction of the traffic or event
signature	dvcEventId	119:15:1	Event ID assigned by the device which is producing the audit events if present in the audit log
message	msg	EXPLOIT-KIT Multiple exploit kit single digit exe detection	Message from the audit event log.
sha256	sha256	275a021bbfb6489e54d471899f7db9d1663fc695ec2fe2a2c4538aabf651fd0f	SHA256 hash value of the file
pattern	act	allow	Action taken in the event log

Field Value Mappings

Data source field: device severity

Source Values	Qualys Normalized Values
1	Critical
2	Error
3	Warning
4	Informational

Data source field: outcome

Source Values	Qualys Normalized Values
true	Success
false	Failure

Data source field: action

Source Values	Qualys Normalized Values
allow	Allow
deny	Deny

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
customerId	d656b196-edb7-45e6-8485-3748a740d002
deviceType	Network Device
deviceModel	Meraki
deviceVendor	Cisco
collectorId	ae102769-bd05-415d-af3c-2cc59681cbab
eventSourceId	1ae639f0-0944-4cbc-81ef-87c040ca9eb2
eventId	d656b196-edb7-45e6-8485-3748a740d002
collectorReceivedTime	Jun 01, 2021 11:29:04 AM