Qualys Context Extended Detection and Response

Cisco OpenDNS Proxy

Data Mapping Guide

February 18, 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 Qualys 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 OpenDNS Proxy fields and the Qualys data model.

Note: For a complete list of sources that Qualys Context XDR supports, on the Qualys Context 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** – Proxy
- **Device Vendor** – Cisco
- **Device Product** – Cisco OpenDNS
- **Supported Versions** – Limited Support – Contact your TAM for further information.

Supported Formats

In Qualys Context XDR, you can configure the product to receive data from Cisco OpenDNS 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 Qualys Context XDR.

deviceType – Proxy
deviceVendor – Cisco

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
timestamp	eventTime	09-06-2020 11:28	The date and time when this request was made in UTC. This is different than the Umbrella dashboard, which converts the time to your specified time zone
mostGranularIdentity	policy	Johndoe@company.com	The first identity that matched the request.
identities	sourceHost	(Johndoe@company.com), HK - 1,TB-HKG-00014	All identities associated with this request.
internalIp	sourceIpv4	192.168.100.10	The internal IP address that made the request
externalIp	natSourceIP	64.39.96.133	The external IP address that made the request.
action	action	Allowed	The type of change made, such as Create, Update, or Delete
queryType	requestContext	1 (A)	The type of DNS request that was made. For more information, see Common DNS Request Types.
responseCode	outcome	NOERROR	The DNS return code for this request. For more information, see Common DNS return codes for any DNS service (and Umbrella).
domain	requestUrlDomain	xyz.com	The domain that was requested.
categories	objectCategory	Software/Technology	The security or content categories that the destination matches. For category definitions, see Understanding Security Categories and Understanding Content Categories.
mostGranularIdentityType	identityType	AD Users	
identityTypes	instanceType	AD Users,Networks, Roaming Computers	The type of identity that made the request. For example, Roaming Computer, Network, and so on. Available in version 3 and above.
blockedCategories	blockedCategories	File Storage	The categories that resulted in the destination being blocked.

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
evtName	eventName	NTP Server Unreachable, Invalid TCP flag combination, Proxy logs, Policy Update, session closed	Brief standard meaning of the message easy to read for Analyst
Source Coordinates	geoSourceCoordinates	37.3526,-121.9541	Geo coordinates of the source IP for the audit log. can be part of enrichment
Destination Coordinates	geoDestinationCoordinates	34.164,-118.2387	Geo coordinates of the destination IP for the audit log. can be part of enrichment
Source Country	geoSourceCountry	India	Country name of the source IP for the audit log. can be part of enrichment
Destination Country	geoDestinationCountry	United states	Country name of the destination IP for the audit log. can be part of enrichment
Source City	geoSourceCity	Mumbai	City name of the source IP for the audit log. can be part of enrichment
Destination City	geoDestinationCity	New York	City name of the destination IP for the audit log. can be part of enrichment
Event Context	eventContext	remote-to-local, local-to-remote, local-to-local	Event Context, remote-to-local, local-to-local, local-to-remote

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
deviceType	DNS
deviceModel	OpenDNS
deviceVendor	Cisco
deviceHost	xyz.com
customerId	d656b196-edb7-45e6-8485-3748a740d002
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