Qualys Context Extended Detection and Response

Squid Proxy

Data Mapping Guide

February 21, 2022

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

Table of Contents

About this Guide **4**
About Qualys 4
Qualys Support 4
Overview **5**
Device Details 5
Supported Formats 5
Data Field Mappings **6**
Qualys Internal Fields 7

About this Guide

Thank you for your interest in Extended Detection, and Response (XDR). Qualys 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 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 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 XDR.

This guide focuses on the data mapping between Squid 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** – Squid
- **Device Product** – Squid Proxy
- **Supported Versions** – 4.8, 4.12

Supported Formats

In Qualys XDR, you can configure the product to receive data from Squid Proxy 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 XDR.

deviceType – Proxy
deviceVendor – Squid

Data Source Fields	Qualys XDR QQL Tokens	Sample Values	Description
EventTime	eventTime	Mar 18 05:53:42	The time at which the individual event occurred
ElapsedTime	duration	1	Time taken (in milliseconds) to process the request
SourceIP	sourceIpv4	64.39.96.133	IP address of the client
Status	status	200	Status of the request. For example, 200 OK, 400 PNF
Action	action	Forbidden	Type of action taken to process this request For a list of Qualys normalized values, click here.
OutByte	outByte	391	Number of bytes sent from appliance to client
Method	method	GET	Request method used from client to appliance
Scheme	scheme	http	Scheme from the 'log' URL
DeviceHost	destinationHost	www.xyz.com	Hostname from the 'log' URL. RDNS is used if the URL uses an IP address.
UriPath	requestUrl	/images/slrl_on.gif	Path from the 'log' URL. Does not include query
Query	requestUrl	-	Query from the 'log' URL
UserName	userName	-	Relative username of a client authenticated to the proxy (i.e., not fully distinguished)
Hierarchy	hierarchy	DIRECT	How and where the object was retrieved in the cache hierarchy
ServiceName	destinationServiceName		Service name on the destination machine (the machine that generated this event as per the log audit)
RequestClientApp	userAgent	Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)	Request header: User-Agent.
Category	category	TCP_HIT	Category of log - TCP-HIT, TCP-MISS
DestinationIP	destinationIpv4	192.168.100.10	IP address of the appliance on which the client established its connection
Domain	objectCategory	TRAVEL	example: Travel, Sports/Recreation/Hobbies
SourcePort	sourcePort	6352	Source port utilized by the session
DestinationPort	destinationPort	80	Destination port utilized by the session
Protocol	protocol	TCP	TCP, UDP

Qualys Internal Fields

Qualys XDR QQL Tokens	Sample Values
deviceType	Proxy
deviceModel	
deviceVendor	Squid
deviceHost	fproxyXXXX.eng.sjcXX.company.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
geoSourceCoordinates	37.3526,-121.9541
geoDestinationCoordinates	34.164,-118.2387
geoSourceCountry	United States, India
geoDestinationCountry	United States, United Kingdom
geoSourceCity	Santa Clara, Kolkata
geoDestinationCity	Glendale, New York