Qualys Context XDR (Extended Detection and Response)

Forcepoint Proxy

Data Mapping Guide

March 11, 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 Collectors... 5

Data Field Mappings 6

Qualys Internal Fields 8

Field Value Mappings 8

Data source field: Action 8

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 Forcepoint 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** – Forcepoint
- **Device Product** – Forcepoint Proxy
- **Supported Versions** – Limited Support – Contact your TAM for further information.
-

Supported Collectors

In Qualys Context XDR, you can configure to receive data from Forcepoint Proxy using the following collectors:

- **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 – Forcepoint

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
id	externalId	3	
FWIP	deviceIPAddress	10.231.143.34	The IP address of the proxy (on-premises data) or the SIEMConnector IP address (hybrid data)
timestamp	eventTime	1613984348	The Forcepoint DLP timestamp for the forensic data
dispostion_code	deviceEventId	1048	The numeric code associated with the action (e.g., category permitted, file type blocked) applied to the request
client_ip	sourceIpv4	10.231.128.238	IPv4 or IPv6 address of the client (requesting) machine
destination_ip	destinationIpv4	2.19.62.181	Translated IPv4 or IPv6 address of the destination machine (resolved by DNS from the requested URL)
Protocol	protocol	https	The protocol name (custom or defined in the Master Database)
URI	requestUrl	https://cdn.odc.officeapps.live.com	Full requested URL. Does not include protocol or port
Port	sourcePort	443	Integer representing the TCP port of the origin server
ResponseSize	outByte	15547	
RequestSize	inByte	17942	
sourceServer	deviceName	LogServer8.4ForForcePoint	IP address (in integer format) of the server that originated the message, either Content Gateway or Network Agent
File Type Code	fileType	Images	The Content Type value from the request header (for example, image/gif)

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
ID	baseEventId	A795187637C64752955C33C0D3A36201	
User Agent	userAgent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML%2C like Gecko) Chrome/88.0.4324.182 Safari/537.36, 10.231.128.238	Contents of the User-Agent HTTP header, if present
client	sourceHost	10.231.128.238/wgbaero523.kn.cisco.local	
policyNames	policy	GLOBAL-no-auth	The name of the policy or policies that could be applied to the request. (Multiple policies may be found, for example, for a user who belongs to multiple groups.)
roleId		8	A number associated with the delegated administration role in which the policy applied to the request was created. The identifier for the Super Administrator role is 8.
User Path	customString6	LDAP://gbltndc001.cisco.local OU=Users,OU=LTN,OU=AS,DC=CISCO,DC=LOCAL/Aldridge\	Contains NameSpace, Domain, and UserName information for the user to whom the policy was applied.
	sourceDomain	LOCAL	Pick up LOCAL from CustomString6(30)
UserID	sourceUser	Luke	
Disposition reference Description	eventName	Category permitted, not set	

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
SA Internal Fields	severity	Informational	
Disposition reference Summary	action	Permitted	Permitted or Blocked, based on the value of dispositionNumber

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
deviceType	Proxy
deviceModel	Websense
deviceVendor	Forcepoint
deviceHost	
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

Field Value Mappings

Data source field: Action

Source Values	Qualys Normalized Values
Permitted	Allow
Blocked	Block