Qualys Context Extended Detection and Response

Symantec Endpoint Protection

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

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 Symantec Endpoint Protection 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** – Endpoint
- **Device Vendor** – Symantec
- **Device Product** – Symantec Endpoint Protection
- **Supported Versions** – 14

Supported Formats

In Qualys Context XDR, you can configure to receive data from Symantec Endpoint Protection 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 – Endpoint
deviceVendor – Symantec

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Timestamp	receivedTime	2019-03-20 12:32:57	Time stamp when the scan was reported
Action	category	Warning|Info|Error	Action taken for the session. Possible values are: Warning, info and error
Device ID	deviceId	ttu-268369	ID of the device on which the scan was performed
Hostname	deviceName	SYLINK	The hostname of the SEP on which the session was logged
Rule_Name	reason	User permitted application list	Reasons for whilelisting Possible values: • Not on the permitted application list • Symantec permitted application list • Administrator permitted application list • User permitted application list
Role	symantecState	Completed|Started	Started and completed are the roles configured for the SEP
Duration (seconds)	duration	467	The elapsed time of the session
User1	sourceUser	SYSTEM	User who was logged in when scan started
User2	destinationUser	SYSTEM	User who was logged in when scan stopped
Destination	destinationIpv4	10.161.28.137	The IP address of the remote computer that was being scanned
Domain	destinationDomain	TTU	SEP domain name
IP Address	additionalIP	129.118.130.140	The IP address that pertains to the event
Certificate issuer	certificateIssuer		The certificate's issuer
Certificate thumbprint	certificatePrint		The certificate's thumbprint
Signing timestamp	certificateSigningTime	0	The certificate's signature timestamp
Log Risk	scanType	Scheduled scan	Log risk action description
Group	group	My Company\Operations Division\PCs\Engineering_Services	Client group name in the SEPM
Risk name	risk	Tracking Cookies	This is related to SONAR

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Occurrences	count	1	The number of sessions with same Source IP, Destination IP, Application, and Subtype seen within 5 seconds
Actual action	action	Details pending	Action taken for the session
Requested action	secondaryAction	Quarantined	Requested action by policy
Secondary action	secondaryActualAction	Deleted	Secondary actions can be similar to action taken on the risk
Begin	beginningTime	2019-03-20 12:32:57	Time stamp when the scan was started. yyyy-MM-dd HH:mm:ss
End	endTime	2019-03-20 12:06:47	Time stamp when the scan ended. yyyy-MM-dd HH:mm:ss
Last update time	updateTime	2019-03-20 12:32:57	The time on the server when the event is logged into the system or updated in the system. yyyy-MM-dd HH:mm:ss
User	sourceUser	bpohl	SEPM admin name
Source computer	sourceHost	11XXX-TXXX.corp.company.com	Computer name where this event occurred
Computer	sourceUserId	MC293981-375-09	ID of the environment from which the scan has been done
Source IP	sourceIpv4		Original session source IP address
Disposition	reputation	Good	Disposition: Good / Bad / Unknown / Not available.
Download site	requestUrl	null	The site from where the file was downloaded
Downloaded by	sourceProcess	null	The creator process of the dropper threat. Default is "".
Confidence	message	Reputation was not used in this detection.	Confidence associate with the session
URL Tracking Status	outcome	Success/Failure	Status of the connection
Application hash	sha1Hash		The hash for this application
Application name	application		Name of the application
Application version	version		Version of the application
Size (bytes)	totalBytes	13509	Number of total bytes for the session
Category set	eventType	Security risk	The category set in the session
Category type	eventSubType	Trackware	The category type in the session
Internal Fields	tags	SEP	Different tags for more details like device type, jdbc, parser details
File	filePath	'c:\program files\microsoft office\root\office16\outlook.exe'	file path
Internal Fields	geoSourceCoordinates		Source geo IP Coordinates ["latitude","longitude"]

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Internal Fields	geoDestination Coordinates		Destination geo IP Coordinates ["latitude","longitude"]
Internal Fields	geoSourceCountry		Source Country geolocation
Internal Fields	geoDestination Country		Destination Country geolocation
Internal Fields	geoSourceCity		Source city geolocation
Internal Fields	geoDestination City		Destination city geolocation
Internal Fields	eventContext		Context of Connection : Ingoing/Outgoing
Description	description		Description

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
deviceType	Endpoint
deviceModel	Endpoint Protection
deviceVendor	Symantec
deviceHost	TB-HXX-00XX
customerId	d656b196-edb7-45e6-8485-3748a740d002
collectorId	ae102769-bd05-415d-af3c-2cc59681cbab
eventSourceId	1ae639f0-0944-4cbc-81ef-87c040ca9eb2
eventId	d656b196-edb7-45e6-8485-3748a740d002
eventTime	May 14, 2021 12:54:05 PM
collectorReceivedTime	Jun 01, 2021 11:29:04 AM

Field Value Mappings

Data source field: dvcSeverity

Source Values	Qualys Normalized Values
Info	Informational
Error	Error
Warning	Warning