Qualys Context Extended Detection and Response

Trend Micro

Data Mapping Guides

January 22, 2023

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 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 Trend Micro 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** – Trend Micro
- **Device Product** – Trend Micro WS
- **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 Trend Micro using the following formats:

- **JSON**

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 – Trend Micro

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
logVer		CEF: 0	CEF format version
vendor	deviceVendor	Trend Micro	Appliance vendor
pname		Trend Micro Web Security	Appliance product name
pver	version	3.0.0.2042	Appliance version
eventid		100000	Signature ID
eventName	deviceEventId	Access Log	Description
severity		• 0: act=allow/analyze • 1: act=monitor/warn/override • 2: act=block	Risk level
rt	eventTime	Jul 05 2018 07:54:15 +0000	UTC timestamp
logType	eventType	Log type	1: Access Log
companyId	customString6	7800fcab-7611-416c-9ab4-721b7bd6b076	Company ID
adDomain	sourceDomain	trendmicro.com.cn	AD Domain
username | user	username	10.204.214.188	User name or client IP
groupName | group	Group	testgroup1	Group name
userDepartment | dep	customString7	finance department	User department

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
gatewayName | device	deviceName	on-premise-2051	Gateway name
app | application	protocol	• 1: HTTP • 2: HTTPS	Protocol used
transportBytes | traffic	totalBytes	Example: 221030	Body size of a request or response
dst	destinationIpv4 | destinationIpv6	Example: 54.231.184.240	Destination IP address of a request
src	sourceIpv4 | sourceIpv6	Example: 10.204.214.188	Source IP address of a request
upStreamSize | inbound	inByte	Example: 501	Upstream payload from Trend Micro Web Security to server, unit bytes
downStreamSize | outbound	outByte	Example: 220529	Downstream payload from server to Trend Micro Web Security, unit bytes
domainName | domain	requestUrlDomain	Example: clients4.google.com	URL domain
scanType	reason	• 0: Not match any rule • 1: Client certificate is required • 2: Untrusted server certificate • 10: Approved URLs/Blocked URLs • 13: Client not allowed • 14: Destination port not allowed • 15: Access to private address • 20: Web Reputation service • 30: True file type • 33: MIME type	Scan type

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
		- 34: File extension name - 40: Anti-malware - 41: Unscannable files - 45: Predictive machine learning - 50: Anti-botnet - 60: Application control - 70: Suspicious Object Analysis (Virtual Analyzer) - 90: Suspicious Object Filtering (Virtual Analyzer) - 100: Data loss prevention - 110: Ransomware	
policyName | policy	policy	default	Policy name
profileName | profile	customString8	default	Profile name
severity	deviceSeverity	- 0: WRS is disabled - 50: WRS security level=Low - 65: WRS security level=Medium - 80: WRS security level=high	WRS score threshold
principalName	SourceUser	Example: testuser@trendmicro.com.cn	Principal name
cat	category	Example: Search Engines/Portals	URL category
appName	application	Google	Application name
wrsScore | wrs	riskScore	81	WRS score
malwareType	riskType	1: Virus 2: Spyware 3: Joke	Malware type

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
		4: Trojan 5: Test_Virus 6: Packer 7: Generic 8: Other 9: Botnet	
malwareName	risk	Example: HEUR_OLEXP.B	Malware name
fname | filename	fileName	Example: sample_nice_dda_heurb_1177077.ppt-1	File name
filehash	sha1	Example: 3f21be4521b5278fb14b8f47afcabe08a17dc504	SHA-1
act | action	action	allow monitor block warn override analyze	Action
httpTrans	message	JSON format. Example:{"http_req":{ "method":"GET","scheme":"http","path":"index.html","host":www.sina.com.cn,"headers":{"header_1":"value_1", ...}},"http_response":{"status_code":"200","headers":{...} }}	HTTP transaction
method	method	Example: GET, PUT, POST	HTTP method
version | httpversion		Example: 1.1	HTTP version
path	FilePath	Example: example.html	HTTP request path
host	Destination Host	Example: client2.example.com	HTTP request host
status_code	status	Example: 200, 404, 503	HTTP response status code

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
scheme	protocol	Example: HTTP, HTTPS	HTTP or HTTPS protocol
url | RequestUrl	reqestUrl	Example: https://client2.example.com/example.html	Combination of scheme, host, and path
<http-request-header-name>_q	customString9	Example: User-Agent: Mozilla/5.0	HTTP request header field
<http-response-header-name>_s	customString10	Example: Content-Length: 348	HTTP response header field
user-agent		Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/101.0.4951.67 Safari/537.36	

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
DeviceType	Proxy
DeviceModel	Trend Micro WS
DeviceVendor	Trend Micro
DeviceHost	el.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