Qualys Context XDR (Extended Detection and Response)

Qualys Endpoint

Data Mapping Guide

April 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 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 Qualys Endpoint fields and the Qualys data model.

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

Supported Formats

In Qualys Context XDR, you can configure to receive data from Qualys Endpoint 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 Context XDR.

deviceType – Endpoint
deviceVendor – Qualys

Data Source Fields			Qualys XDR QQL Tokens	Sample Values	Description
dateTime			eventTime	2021-12-03T00:50:26.663+0000	Time of the event
process					
	processName		destinationProcess	rundll32.exe	Process name on the destination machine (the machine who has generated this event as per the log audit)
	fullPath		filePath	C:\\Windows\\System32\\rundll32.exe	Path of the file where file is present
	parentProcessName		sourceProcess	svchost.exe	Process name on the source machine (the machine who has generated this event as per the log audit)
	userName		sourceUser	PATCH11\\Administrator	Username using/logged-in the source machine (the username present in the log audit as per the log audit logged by the device)
	processFile				
		moduleName	fileName	rundll32.exe	File name as present in the audit event
		md5	md5Hash	f68af942fd7ccc0e7bab1a2335d2ad26	MD5 hash value of the file
		size	fileSize	71168	File size as present in the audit event

Data Source Fields			Qualys XDR QQL Tokens	Sample Values	Description
eventSource			detectionMethod	EDR	“EventSource” is a key field to indicate detection engine
indicator2					
	sha256		sha256Hash	11064e9edc605bd5b0c0a505538a0d5fd7de53883af342f091687cae8628acd0	SHA256 hash value of the file
	score		riskScore	0	riskscore from the event log
	threatName		risk	Win32.Trojan.Generic	Virus name or the detction name form the event
	familyName		riskType	Trojan.Generic	Risk type or virus type/family
	category				
	verdict		reputation	KNOWN	Reputation score of the entity (User/Host etc.) as per mentioned in the audit log
type			eventType	PROCESS	Type of the event. (E.g. PROCESS, FILE)
customerId			customerId	3d86e9fe-ea41-d2bb-83c6-467111409204	ID of the customer in Qualys ecosystem to uniquely identify a customer.
action			action	TERMINATED	Action taken in the event log
id			baseEventId	RTP_df3fbfd6-ed74-344a-8e1d-69aaee9e77de_3-12-2021	External ID given in the event by the event source.
asset					

Data Source Fields			Qualys XDR QQL Tokens	Sample Values	Description
	agentId		customString6	6da80da8-0fd2-42f5-a09b-9fa51a458883	
	fullOSName		osDetails	Microsoft Windows 10 Pro 10.0.18362 Build 18362	OS Information of the asset
	hostName		deviceHost	Patch11	Metadata field
file					
	fullPath		filePath	C:\\Users\\Administrator\\Desktop\\DB Browser for SQLite\\Qt5Network.dll	Path of the file where file is present
	md5		md5Hash	f695b4ec06c6d164e71742dc52cf45bd	MD5 hash value of the file
	fileType		fileType	dll	Type of the file from the event
	size		fileSize	1053304	File size as present in the audit event
mutex					
	mutexName		object	\\Sessions\\2\\BaseNamedObjects\\__DDrawCheckExclMode__	group/policy/registry/domain change
actor					
	userId		sourceUserId	S-1-5-21-968202812-1357026296-468998715-500	UserID using/logged-in the source machine (the username present in the log audit as per the log audit logged by the device)
	processId		processId	1596	processid if present in the event log
	processName		processName	mmc.exe	processname if present in the event log

Data Source Fields			Qualys XDR QQL Tokens	Sample Values	Description
	imageFullPath		filePath	C:\\Windows\\system32\\mmc.exe	Path of the file where file is present
registry					
	key		object	HKU\\S-1-5-21-968202812-1357026296-468998715-500\\Software\\Microsoft\\Windows\\CurrentVersion\\Internet Settings	group/policy/registry/domain change
	value		customString9	<local>	
network					
	protocol		protocol	TCP	Protocol used in the event log
	localIP		sourceIpv4	10.115.97.232	IPv4 address of the source machine (the machine who has generated this event as per the log audit)
	localPort		sourcePort	54798	Port used on the source machine (the machine who has generated this event as per the log audit)
	remoteIP		destinationIpv4	10.115.27.54	IPv4 address of the destination machine (the machine who has generated this event as per the log audit)
	remotePort		destinationPort	3128	Port used on the destination machine (the machine who has generated this event as per the log audit)

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
deviceType	Endpoint
deviceModel	EDR
deviceVendor	Qualys
deviceHost	Patch11
customerId	2104c860-925a-4572-9ae6-e4c9c6b8fdab
collectorId	e22ca2cf-26db-4974-b226-d155f22ebfc6
eventSourceId	69608d8a-4088-4c6d-be0c-f3d5108f25d6
eventId	c664ac73-0e9b-46d8-98f0-bf0dae79ae09
collectorReceivedTime	Sep 14, 2021 11:29:04 AM

Field Value Mappings

Data source field: EventName

eventType	eventName
PROCESS	EDR Process Event
FILE	EDR File Event
MUTEX	EDR Mutex Event
REGISTRY	EDR Registry Event
NETWORK	EDR Network Event

Data source field: severity

EDR		XDR
riskScore	**Severity (EDR)**	**severity(enriched)**
10	Critical	Alert
7-9	High	Critical
4-6	Medium	Error
1-3	Low	Warning
0	Clean	Informational

Data source field: action

Source Values	Qualys Normalized Values
CREATED	Created
RUNNING	Running
TERMINATED	Terminated
DELETED	Deleted
WRITE	Write
ESTABLISHED	Established
CLOSED	Closed