Qualys Context Extended Detection and Response

Nexus Repository

Data Mapping Guides

January 19, 2023

Copyright 2023 by Qualys, Inc. All Rights Reserved.

Qualys and the Qualys logo are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

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 Nexus Repository fields and the Qualys data model.

Note: For the Nexus Repository parser, we are ingesting logs with Linux Agent; hence source creation is happening differently. For ingesting the Nexus Repository logs, you need to add a New Profile, go to the Qualys Context XDR UI, and navigate to **Configuration** > **Cloud Agent Profiles** > **Profiles**.

Device Details

- **Device Type** – Application
- **Device Vendor** – Sonatype
- **Device Product** – Nexus Repository
- **Supported Versions** – 3.42.0

Supported Formats

In Qualys Context XDR, you can configure the product to receive data from Nexus Repository using the following formats:

- **JSON**

Data Field Mappings

This section provides a detailed mapping of the data source fields to the Qualys Context XDR.

deviceType – Application
deviceVendor – Sonatype

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
timestamp	eventTime	2022-09-22 09:20:00,003+0000	The date and time this event occurred
nodeId	instanceId	A197748D-40F545C3-66A237DC-33ADCB88-88D40BCF	The nodeId of the instance (used to correlate audit logs across multiple instances)
	sourceUser	*UNKNOWN	username
	sourceIpv4	10.246.21.23	host
domain	sourceDomain	tasks	Functional area of the system
type	eventType	finished	Action performed in this domain
context	eventName	Storage facet cleanup	Identifying details of the event
thread	object	quartz-10-thread-20	Thread name of the event initiator. Thread name can help correlate related log lines from other log files.
attributes.schedule	description	Cron{properties={schedule.clientTimeZone=UTC, schedule.startAt=2022-08-26T13:05:42.543Z, schedule.cronExpression=0 */10 * * * ?, schedule.type=cron}}	Description about the schedule time
attributes..name	processName	Storage facet cleanup	Name of the event
attributes.id	externalId	bc682c78-9a33-4bec-90d1-c54dac4cebfb	
attributes.typeName	eventName	Storage facet cleanup	Type of the event occured

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
attributes.lastRunState.endState	status	OK	Status of the event
attributes..updated	updateTime	2022-08-26T13:05:42.543Z	Date and time when the event is updated
attributes..message	message	Reclaim storage for deleted repositories	Message from the audit event log
attributes.lastRunState.runDuration	duration	2	Time taken for the event to complete
attributes..created	beginningTime	2022-08-26T13:05:42.543Z	Date and time when the event get triggered
attributes.repository.name	application	docker-fedramp-high-repo	Repository service used in the event
attributes.format	category	docker	Category of the event log
attributes.name	eventName	v2/-/blobs/sha256:c5574fcbe7ea8a9f75e5fbad701eb668bcf201415a0e40ddd4d7021abdb3382c	Identifying details of the event
attributes.type	eventSubType	proxy	Type of the action performed domain
attributes.failureReasons	reason	"INCORRECT_CREDENTIALS"	Reason if the event fails
attributes.wasSuccessful	outcome	false	True/false based on the success of the event
attributes.userId	sourceUserId	admin	UserId logged in the machine
attributes.remoteIp	destinationIpv4	10.246.21.22	IP address of the destination machine

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
attributes.userAgent	userAgent	Mozilla/5.0 (Windows NT 10.0; Win64; x64; rv:68.0) Gecko/20100101 Firefox/68.0	Agent used browser
attributes.path	filePath	/service/rapture/session	Destination path where the event occurred

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
deviceType	Application
deviceModel	Nexus Repository
deviceVendor	Sonatype
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