Qualys Context Extended Detection and Response

Atlassian Confluence

Data Mapping Guides

January 19, 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 Atlassian Confluence 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** – Application
- **Device Vendor** – Atlassian
- **Device Product** – Atlassian Confluence
- **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 Atlassian Confluence 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 – Application
deviceVendor – Atlassian

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
affectedObjects.id	destinationUserId	JIRAUSER10305	Affected object id.
affectedObjects.name	destinationUser	anksharma_fr	Affected object name.
auditType.action	eventName	User removed from group	Action performed by the user.
auditType.area	eventType	USER_MANAGEMENT	Area of the event.
auditType.category	category	group management	Category of the event.
author.id	sourceUserId	-1	Id of the user that actioned the event.
author.name	sourceUser	System	User that actioned the event.
author.type	objectCategory	System	User type that actioned the event.
author.uri	object	/secure/ViewProfile.jspa?name=ygavhane_fr	Accessed URI.
extraAttributes.name	eventSubType	Load balancer/proxy IP address	Extra attribute name from the event.
extraAttributes.value	additionalIP	10.246.21.61	Extra attributes value from the event.
method	method	Browser	
system	requestUrl	https://confluence.teleproxy.gov1.qualys.us	Accessed Url.
timestamp.epochSecond	eventTime	1663772682	Time at which audit event log occurred.

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
version	version	1.0	Jira platform REST API version
source	sourceIpv4	10.245.1.142	IP address of the source.
summary	eventName	Group created	Summary of the event.
category	category	group management	Category of the event.
created	eventTime	2022-11-04T20:16:41.298+0000	Time at which audit event log occurred.
objectItem.typeName	eventType	PROJECT	Object type name.
objectItem.parentId	externalId	10000	Object Id.
author.AccountId	sessionId	61f19ea778b7fd0072ededa3	Account Id of the user that actioned the event.
remoteAddress	destinationIpv4	165.193.18.163	IP address of the computer where the event was initiated from.
creationDate	eventTime	1667887305316	Creation date-time of the audit record, as a timestamp.
author.username	sourceUser	635fd44d01c2ff842c1955b0	User that actioned the event.
author.accountId	sourceUserId	635fd44d01c2ff842c1955b0	Account id of the user that actioned the event.
description	description		A long description of the event.
affectedObject.name	object	MySpace	Affected object id.
affectedObject.objectType	eventType	Space	Affected object name.

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
deviceType	Application
deviceModel	Confluence
deviceVendor	Atlassian Confluence
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