Qualys Context Extended Detection and Response

Grafana Audit

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 Grafana Audit 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** – Grafana
- **Device Product** – Grafana Audit
- **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 Grafana Audit 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 – Grafana

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
timestamp	eventTime	2021-11-12T22:12:36.144795692Z	The date and time the request was made, in coordinated universal time (UTC) using the RFC3339 format.
user.userId	sourceUserId	1	ID of the Grafana user that made the request.
user.orgId	customString6	1	Current organization of the user that made the request.
user.orgRole	permissions	Admin	Current role of the user that made the request.
user.name	sourceUser	admin	Name of the Grafana user that made the request.
user.tokenId	externalId	1	ID of the user authentication token.
action	action	create	The request action. For example, create, update, or manage-permissions.
result.statusType	outcome	success	If the request action was successful, success. Otherwise, failure.
result.statusCode	status	200	HTTP status of the request.
result.failureMessage	message		HTTP error message.
resources[x].id	deviceId	1	ID of the resource.
resources[x].type	eventType	api-key	The type of the resource that was logged: alert, alert-notification, annotation, api-key, auth-

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
			token, dashboard, datasource, fold er, org, panel, playlist, report, team , user, or version.
requestUri	object	/api/auth/keys	Request URI.
ipAddress	sourceIpv4	127.0.0.1	IP address that the request was made from.
userAgent	userAgent	Mozilla/5.0 (X11; Linux x86_64; rv:94.0) Gecko/20100101 Firefox/94.0	Agent through which the request was made.
grafanaVer sion	version	8.3.0-pre	Current version of Grafana when this log is created.

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
deviceType	Application
deviceModel	Grafana Audit
deviceVendor	Grafana
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
deviceType	Application