Qualys Context Extended Detection and Response

OpenSearch SearchAnalytics

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 OpenSearch SearchAnalytics 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** – SearchAnalytics
- **Device Vendor** – OpenSearch
- **Device Product** – OpenSearch WAF
- **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 OpenSearch SearchAnalytics 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 – SearchAnalytics
deviceVendor – OpenSearch

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description

Field	CES Label	Sample Values	Description
audit_format_version		4	the audit log message format vesion
audit_category	category	INDEX_EVENT	The audit log category. FAILED_LOGIN, MISSING_PRIVILEGES, BAD_HEADERS, SSL_EXCEPTION, OPENSEARCH_SECURITY_INDEX_ATTEMPT, AUTHENTICATED, or GRANTED_PRIVILEGES.
audit_node_id		FmhBprUxQzS4YVNTMTMAzQ	the ID of the node where the event was generated
audit_node_name	deviceHost	athm01	the name of the node where the event was generated
audit_node_host_address	destination IP	10.245.4.153	the host address of the node where the event was generated.
audit_node_host_name	Destination Host	10.245.4.153	the host name of the node where the event was generated
audit_request_origin		REST	The layer from which the event originated, either TRANSPORT or REST
audit_request_effective_user	SourceUser	admin	The username that failed to authenticate
audit_rest_request_path	object		the REST endpoint URI
audit_rest_request_headers.User-Agent	userAgent		
audit_rest_request_headers.Referrer	referrerUrl		
audit_rest_request_headers.Version	version		

Field	CES Label	Sample Values	Description
audit_request_initiating_user	SourceUser		The user that initiated the request. Only logged if it differed from the effective user
audit_trace_task_id	sessionId	FmhBprUxQzS4YVNTMTMAzQ:2798640	the ID of the request
audit_transport_headers		_opendistro_security_remotecn": "athena_opensearch	the headers of the request, if any.
audit_transport_request_type		PutMappingRequest	the type of request (IndexRequest)
audit_trace_resolved_indices		fim_k8s-2022.09.26	the resolved index name(s) affected by the request. only logged if resolved_indices is true
audit_request_privilege	permissions	• indices:data/write/bulk* • indices:data/write/delete • indices:data/write/index • indices:data/write/update	The required privilege of the request (indices:data/read/search) reference:https://opensearch.org/docs/latest/security-plugin/access-control/permissions/

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
deviceType	
deviceModel	OpenSearch
deviceVendor	OpenSearch
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