Qualys Context Extended Detection and Response

HashiCorp Consul

Data Mapping Guides

January 27, 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 HashiCorp Consul fields and the Qualys data model.

Note: For the Hashicorp Consul parser, we are ingesting logs with Linux Agent; hence source creation is happening differently. For ingesting the Hashicorp Consul 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** – HashiCorp
- **Device Product** – HashiCorp Consul
- **Supported Versions** – 1.13.x.

Supported Formats

In Qualys Context XDR, you can configure the product to receive data from HashiCorp Consul 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 – HashiCorp

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
created_at	receivedTime	2020-12-08T12:30:29.196365-05:00	The timestamp value of when the event log was created.
event_type	eventType	audit	The type of event.
payload.id	processId	e4a20aec-d250-72c4-2aea-454fe8ae8051	Unique ID of the payload.
payload.version	version	1	Payload version.
payload.type	eventSubType	HTTPEvent	Payload type.
payload.timestamp	eventTime	2020-12-08T12:30:29.196206-05:00	The timestamp value of when the event occurred.
payload.auth.accessor_id	externalId	08f05787-3609-8001-65b4-922e5d52e84c	The accessor ID of the ACL token which issued the request.
payload.auth.description	description	Bootstrap Token (Global Management)	Description of the issued request.
payload.auth.create_time	beginningTime	2020-12-01T11:01:51.652566-05:00	The timestamp value when request was issued.
payload.request.operation	method	GET	The HTTP request type. i.e. GET
payload.request.endpoint	object	/v1/catalog/service/ssh	The Service name including endpoint.
payload.request.remote_addr	destinationIpv4	127.0.0.1:64015	IP address of the remote host.

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
payload.request.user_agent	userAgent	curl/7.54.0	User agent in use to make the request.
payload.request.host	sourceIpv4	127.0.0.1:8500	IP address of host making the request.
payload.stage	eventName	OperationStart	The agent status. i.e OperationStart, OperationComplete etc.
payload.response.status	status	200	The HTTP response status of the request.

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
deviceType	Application
deviceModel	Consul
deviceVendor	HashiCorp
deviceHost	el.xyz.com
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