Qualys Context Extended Detection and Response

HashiCorp Vault

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 HashiCorp Vault fields and the Qualys data model.

Note: For the HashiCorp Vault parser, we are ingesting logs with Linux Agent; hence source creation is happening differently. For ingesting the HashiCorp Vault 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** – IAM
- **Device Vendor** – HashiCorp
- **Device Product** – HashiCorp Vault
- **Supported Versions** – v.1.11.x

Supported Formats

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

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
time	eventTime	2022-09-22T16:01:59.2754117Z	Timestamp when the request is generated
type	eventType	response	Log entry type; there are currently just two types, request and response
auth.client_token	HashiCorp_Vault_client_token	hmac-sha256:cea805e955310099f47fcd89af2043458afef82d4598c91baef18d87b7f98223	HMAC of the client's token ID
auth.accessor	HashiCorp_Vault_accessor	hmac-sha256:c79f127c2745ddc6490812f17476350e52bdd9e5e4f36d40e61a998a093a70cb	HMAC of the client token accessor
auth.display_name	eventSubType	token	Display name set by the auth method role or explicitly at secret creation time
auth.policies	policy	["default", "sudo"]	List of policies associated with the client_token
auth.entity_id	externalId	hmac-sha256:2fced7e2c77266f5079d733bea71dc8c8413d3838584ca9d0f4867271df7a220	Token entity identifier
request.id	deviceEventId	b2f72168-6cba-1bab-808a-72d9304b82f8	Unique request identifier
request.operation	eventName	read	Type of operation which corresponds to path capabilities and is expected to be one of: create, read, update, delete, or list

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
request.path	filePath	auth/token/lookup-self	The requested Vault path for operation
request.remote_address	sourceIpv4	172.17.0.1	The IP address of the client making the request
request.remote_port	spt	13442	The port of the client making the request
request.wrap_ttl	HashiCorp_Vault_wrap_ttl	5s or 10m	This displays configured wrapped TTL value as numeric string
error	HashiCorp_Vault_error	permission denied	Error occurred with the request
response.auth.display_name	eventSubType	token	
response.auth.policies	policy	["default", "sudo"]	
response.data.creation_time	beginningTime	1523307682	Timestamp of the token’s creation
response.data.expire_time	endTime	2023-12-23T05:01:22.8929692Z	Token expiry time
response.data.issue_time	receivedTime	2018-04-09T21:01:22.8929624Z	Token issued time
response.data.meta		{ "loglevel": "hmac-sha256:eac4a7deb2df94609ab14ae48b9edea81d91de51be1dd59df6ca6852537227c5", "remote": "hmac-sha256:aa2d1dd64d4468bbd9c6b0ca275cdffb7473a2d91b5f42a047161620245fcc79", "surf": "hmac-sha256:8b29af9294da23c72de8d8d847ccebd450d978af5565807d0c9922b6b2e92988" }	

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
response.data.num_uses	count	0	If the token is limited to a number of uses, that value will be represented here

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
deviceType	IAM
deviceModel	Vault
deviceVendor	HashiCorp
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