Qualys Context Extended Detection and Response

ClamAV

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 ClamAV fields and the Qualys data model.

Note: For the ClamAV parser, we are ingesting logs with Linux Agent; hence source creation is happening differently. For ingesting the ClamAV 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** – Endpoint
- **Device Vendor** – ClamAV
- **Device Product** – ClamAV Endpoint
- **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 ClamAV 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 – Endpoint
deviceVendor – ClamAV

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
EventTime	eventTime	1569865553705	Event time is the time at which the individual event occurred
DeviceModel	deviceVendor	ClamAV	Manufacturer of the device used in the event.
DeviceType	deviceType	Endpoint	Device Model provides information manufacturer.
	dvcName	elsmastercer01.p02.ams01.qualys.com	Hostname of the device where event is produced/logged.
	prcsName	clamd	Process name on the source machine.
	fileName	/usr/share/clamav-testfiles/clam.bz2.zip	File Name that is being scanned or that is infected.
	risk	ClamAV-Test-File	Threat Name
	action	FOUND	Action performed by ClamAV
	eventName	Database status OK	Event Name.