Qualys Context XDR (Extended Detection and Response)

SEM

Data Mapping Guide

February 13, 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 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 Context 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 Qualys SEM fields and the Qualys data model.

Note: For a complete list of sources that Qualys XDR supports, on the Qualys 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.

Device Details

- **Device Type** – Enterprise Mobility
- **Device Vendor** – Qualys
- **Device Product** – Qualys SEM
- **Supported Versions** – Limited Support. Contact your TAM for further information.

Supported Formats

In Qualys Context XDR, you can configure to receive data from SEM using the following formats:

- **Cloud**

Data Field Mappings

This section provides a detailed mapping of the data source fields to the Qualys Context XDR.

deviceType – Enterprise Mobility
deviceVendor – Qualys

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values
eventType	eventType	UPSERT
assetId	deviceId	219739
asset.name	deviceName	One Plus 7 pro
asset.created	beginningTime	1565340223048
asset.updated	updateTime	1565340223090
asset.assetType	category	HOST
asset.trackingMethod	SEM_TrackingMethod	SEM
asset.systemAttribute.system.biosDescription	SEM_BIOS_Dscrp	SEM mobile data
asset.systemAttribute.system.lastBoot	SEM_LastBoot	1546799400000
asset.systemAttribute.system.manufacturer	SEM_Manufacturer	One Plus
asset.systemAttribute.system.totalMemory	totalBytes	1024
asset.softwaresAttribute.software.name	processName	Secuirty patch
asset.softwaresAttribute.software.version	version	12.1
asset.softwaresAttribute.software.installedDate	SEM_SoftInstallDate	1546799400000
asset.softwaresAttribute.software.lastUpdated	SEM_SoftLastUpdate	1546799400000
asset.softwaresAttribute.software.isSystemApp	SEM_IsSystemApp	true
asset.softwaresAttribute.software.isEnterpriseApp	SEM_IsEnterpriseApp	true

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values
timestamp	eventTime	1565340700089
source	SEM_Source	HDS_SEM
subscriptionId	SEM_SubsID	3041

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
DeviceType	Enterprise Mobility
DeviceModel	SEM
DeviceVendor	Qualys
DeviceHost	compXX.pXX.cisco.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	6/1/2021 11:29