Qualys Context XDR (Extended Detection and Response)

KB

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 KB 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** – KnowledgeBase
- **Device Vendor** – Qualys
- **Device Product** – Qualys KB
- **Supported Versions** – Limited Support. Contact your TAM for further information.

Supported Formats

In Qualys Context XDR, you can configure to receive data from KB 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 – KnowledgeBase
deviceVendor – Qualys

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
QID	externalId	11	
VULN_TYPE	eventType	Vulnerability	
SEVERITY_LEVEL	deviceSeverity	2	Refer the severity table
	Severity	Minimum, Medium, Serious, Critical, Urgent	Based on deviceSeverity value.
TITLE	description	![CDATA[Hidden RPC Services]]	
CATEGORY	category	RPC	
LAST_SERVICE_MODIFICATION_DATETIME	updateTime	1999-01-01T08:00:00Z	
PUBLISHED_DATETIME	receivedTime	1999-01-01T08:00:00Z	
PATCHABLE	KB_Patchable	0	
SOFTWARE_LIST_SOFTWARE_PRODUCT	KB_SoftProduct	![CDATA[darxite]]	
SOFTWARE_LIST_SOFTWARE_VENDOR	KB_SoftVendor	![CDATA[darxite]]	

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
DIAGNOSIS	reason	![CDATA[Darxite is an system for retrieving and uploading files via FTP and HTTP where a daemon process sits in the background and downloads or uploads the files, while a number of client processes can control it and provide a user interface.]]	
CONSEQUENCE	KB_Consequence	![CDATA[Unauthorized users can build a list of RPC services running on the host. If they discover vulnerable RPC services on the host, they then can exploit them.]]	
SOLUTION	outcome	![CDATA[Firewalling the portmapper port or removing the portmapper service is not sufficient to prevent unauthorized users from accessing the RPC daemons. You should remove all RPC services that are not strictly required on this host.]]	
COMPLIANCE_LIST_COMPLIANCE_TYPE	KB_ComplianceType	HIPAA	
COMPLIANCE_LIST_COMPLIANCE_SECTION	KB_ComplianceSection	![CDATA[164.306 and 164.312]]	

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
COMPLIANCE_LIST_COMPLIANCE_DESCRIPTION	KB_ComplianceDescription	![CDATA[Insuring that Malware is not present on hosts addresses section(s) 164.306 and 164.312 requirements for securing critical system files and services and insuring system integrity.]]	
CVSS_BASE	KB_CVSSBase	5.0	
CVSS_TEMPORAL	KB_CVSSTemporal	3.6	
CVSS_VECTOR_STRING	KB_CVSSVector	CVSS:2.0/AV:N/AC:L/Au:N/C:P/I:N/A:N/E:U/RL:W/RC:UC	
PCI_FLAG	KB_PCIFlag	1	
DISCOVERY_REMOTE	KB_DiscoveryRemote	1	

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
DeviceType	KnowledgeBase
DeviceModel	KB
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