Qualys Context Extended Detection and Response

Netbox

Data Mapping Guides

January 23, 2023

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100

Table of Contents

About this Guide 4

About Qualys 4

Qualys Support 4

Overview 5

Device Details 5

Supported Formats 5

Data Field Mappings 6

Qualys Internal Fields 9

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 Netbox fields and the Qualys data model.

Note: For a complete list of sources that Qualys Context XDR supports, on the Qualys Context 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. Based on the requests coming in, Qualys will prioritize and attempt to add support at the earliest.

Device Details

- **Device Type** – Infrastructure Monitoring
- **Device Vendor** – Netbox
- **Device Product** – Netbox Infrastructure Monitoring
- **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 Netbox Infrastructure Monitoring using the following formats:

- **JSON**

For information on configuring collectors, refer to the Deploying a Collector section in the Online Help.

Data Field Mappings

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

deviceType – Infrastructure Monitoring
deviceVendor – Netbox

		Sample Values	Description
affectedObject.name	object	MySpace	Affected object id.
affectedObject.objectType	eventType	Space	Affected object name.

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
id	instanceId	294861	ID of the instance
display	message	ipam | VLAN group John created by anonymous@qualys.com	Event display message
time	eventTime	2022-01-14T17:59:35.586923Z	The time at which the event occurred
user_id	sourceUserId	209	ID of the source user
user_username	userName	anonymous@qualys.com	Username
user_name	sourceUser	anonymous@qualys.com	
request_id	sessionid	fbe39048-f2dd-4166-9e6e-354d8faef1a1	
action_label	action	Created	Action taken by the device
changed_object_type	objectCategory	ipam.vlangroup	Category the object belongs to
changed_object_id	customString6	5	

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
changed_object_url	requestUrl	https://netbox01.eng.in03.qualys.com/api/ipam/vlan-groups/5/	URL requested
changed_object_name	object	John	
prechange_data_name	customString7	vcn01-eng-in03_Non-EVC-CL01-NoSPIN	
prechange_data_site	customString8	10	
prechange_data_tags	customString9	Synced, "vCenter", "vcn01-eng-in03"	
prechange_data_type	customString10	2	
prechange_data_group	customString11		
prechange_data_group_name	customString12	24	
prechange_data_created	customString13	"2021-06-06"	
prechange_data_last_updated	customString14	2021-06-06T19:31:14.194Z	
prechange_data_mac_address	customString15		
prechange_data_primary_ip4	customString16		
prechange_data_primary_ip6	customString17		

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
postchange_data_name	customString18	John	
postchange_data_tags	customString19	"Synced", "vCenter", "vcn01-eng-in03", "Orphaned"	
postchange_data_created	beginningTime	"2022-01-14"	
postchange_data_description	description	1	Description of the event
postchange_data_last_updated	updateTime	2022-01-14T17:59:35.581Z	Time the event was updated
postchange_data_ssid	customString20	1	
postchange_data_auth_psk	customString21		
postchange_data.auth_type	eventType		
postchange_data.auth_cipher	eventSubType		
postchange_data_domain	sourceDomain	1	
postchange_data_group_name	group	John	
posthange_data_mac_address	sourceMac		

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
postchange_data_primary_ip4	sourceIpv4		IP(v4) Address of the source
postchange_data_primary_ip6	sourceIpv6		IP(v6) Address of the source

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
deviceType	Infrastructure Monitoring
deviceModel	Netbox
deviceVendor	Digital Ocean
deviceHost	
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