Qualys Context Extended Detection and Response

Microsoft Windows DNS

Data Mapping Guide

February 18, 2022

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 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 Microsoft Windows DNS 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** – DNS
- **Device Vendor** – Microsoft
- **Device Product** – Microsoft Windows DNS
- **Supported Versions** – win2k12 10.0 (14393)

Supported Formats

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

- **Syslog**

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 – DNS
deviceVendor – Microsoft

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Timestamp	eventTime	6/18/2020 4:05:21 PM	Date and time fields
ThreadId	customString6	11DC	Hex numerical thread id as an integer value
Context	category	PACKET	Uppercase context field as a string
Internal packet identifier	externalId	000002356CAD6070	Hex numerical internal packet identifier as a long value
UDP/TCP indicator	protocol	UDP	Uppercase UDP/TCP indicator as a string
Send/Receive indicator	direction	Snd/Rcv	Send/Receive indicator as a string
Remote IP	sourceIpv4	192.168.100.10	Remote IP as an IPADDR-type value
Xid(hex)	customString7	7a80	Xid hex numerical field as a long value

Query/Respon se	action	R = Response
		blank = Query
			Query/Response values to 0/1 integers (a true/false condition in queries)

Opcode	secondaryAction	Q = Standard Query
		U = Update
		N = Notify
		? = Unknown
			Opcode field values as a string

Flags (hex)	customString8	a081	Flags hex numerical field as an integer value

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description

Flags (char codes)	customString9	A DR
		A = Authoritative Answer
		T = Truncated Response
		D = Recursion Desired
		R = Recursion Available
			Flags char codes fields to separate string columns

ResponseCode	outcome	NXDOMAIN	Response Code field as a string
Question Type	eventType	A/PTR	Question Type uppercase field as a string
Question Name (Domain)	destinationDomain	.cloudflare-dns.com.	Question Name field with the domain name labels into an ARRAY
Source Coordinates	geoSourceCoordinates	37.3526,-121.9541	Geo coordinates of the source IP for the audit log. can be part of enrichment
Destination Coordinates	geoDestinationCoordinates	34.164,-118.2387	Geo coordinates of the destination IP for the audit log. can be part of enrichment
Source Country	geoSourceCountry	India	Country name of the source IP for the audit log. can be part of enrichment
Destination Country	geoDestinationCountry	United states	Country name of the destination IP for the audit log. can be part of enrichment
Source City	geoSourceCity	Mumbai	City name of the source IP for the audit log. can be part of enrichment
Destination City	geoDestinationCity	New York	City name of the destination IP for the audit log. can be part of enrichment
Event Context	eventContext	remote-to-local, local-to-remote, local-to-local	Event Context, remote-to-local, local-to-local, local-to-remote

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Event Name	eventName	DNS debug logs	brief standard meaning of the message easy to read for Analyst
Severity	severity	Informational	XDR severity assigned to this log audit

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values	Description
deviceType	DNS	Type of the device which is producing the audit events
deviceModel	Microsoft DNS	Device Model provides information like the device type and manufacturer.
deviceVendor	Microsoft	Manufacturer of the device used in the event.
deviceHost	elsaltxx.xyz.com	The hostname of the firewall on which the session was logged.
customerId	d656b196-edb7-45e6-8485-3748a740d002	The Customer ID is a unique identification number given to every Customer
collectorId	ae102769-bd05-415d-af3c-2cc59681cbab	Unique id of collector , to identify log source.
eventSourceId	1ae639f0-0944-4cbc-81ef-87c040ca9eb2	Event Source ID
eventId	d656b196-edb7-45e6-8485-3748a740d002	The event ID is the unique ID given to every event
collectorReceivedTime	Jun 01, 2021 11:29:04 AM	Received time of the collector