Qualys Context XDR (Extended Detection and Response)

Ubuntu UnixOperatingSystem

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 Ubuntu UnixOperatingSystem 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. Based on the requests coming in, Qualys will prioritize and attempt to add support at the earliest.

Device Details

- **Device Type** – UnixOperatingSystem
- **Device Vendor** – Linux
- **Device Product** – Ubuntu UnixOperatingSystem
- **Supported Versions** – 22.04, 20.04, 18.04

Supported Formats

In Qualys Context XDR, you can configure to receive data from Ubuntu UnixOperatingSystem 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 – UnixOperatingSystem
deviceVendor – Linux

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
timestamp	eventTime	Nov 4 15:47:00	Time of the event
hostname	sourceHost	Ubuntu-2204	hostname of the device where event is produced/logged
eventName	eventName	UFW AUDIT	hostname of the device where event is produced/logged
Incoming interface	sourceInterface	ens33	Source interface of the device where event is produced/logged
Outgoing interface	destinationInterface	ens31	Destination interface of the device where event is produced/logged
Source Mac	sourceMac	00:0c:29:4c:52:1f:00:0c:29:f1:7e:4b:08:00	Source Mac ID of the device where event is produced/logged
Source IP	sourceIpv4	192.168.1.11	Source IP of the device where event is produced/logged
Destination IP	destinationIpv4	192.168.1.246	Destination IP of the device where event is produced/logged
Length	totalBytes	0	Length of the total bytes of the device where event is produced/logged
Protocol	protocol	TCP	Protocol of the device where event is produced/logged
Source Port	sourcePort	10837	Source port number of the device where event is produced/logged
Destination Port	destinationPort	80	Destination port number of the device where event is produced/logged
TCP Windows Size	fileSize	512	TCP windows size the device where event is produced/logged

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
deviceType	UnixOperatingSystem
deviceModel	Unix
deviceVendor	Linux
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	Jun 01, 2021 11:29:04 AM