Qualys Context Extended Detection and Response

Cisco IOS

Data Mapping Guides

January 22, 2023

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 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 Cisco IOS 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** – Operating System
- **Device Vendor** – Cisco
- **Device Product** – Cisco IOS
- **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 Cisco IOS 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 – Operating System
deviceVendor – Cisco

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
Event Time	eventTime	Sep 15 14:13:51	Time of the event
Host	deviceHost	192.168.100.10	Metadata field
Description	description	Device supports the following 4 cipher(s)	Rest of the fields from raw message
Device Severity	deviceSeverity	6	Severity details for the event log as per the device which is producing the audit events
Device Event ID	deviceEventId	%FW-6-DROP_PKT	Event ID assigned by the device which is producing the audit events if present in the audit log
Event Type	eventType	DROP_PKT	Type of the email Recipient

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
DeviceType	Operating System
DeviceModel	IOS
DeviceVendor	Cisco
DeviceHost	10.220.40.1
CustomerId	2104c860-925a-4572-9ae6-e4c9c6b8fdab
CollectorId	e22ca2cf-26db-4974-b226-d155f22ebfc6
EventSourceId	69608d8a-4088-4c6d-be0c-f3d5108f25d6
EventId	c664ac73-0e9b-46d8-98f0-bf0dae79ae09
CollectorReceivedTime	Sep 14, 2021 11:29:04 AM