Qualys Context Extended Detection and Response

Arbor-APS DDoS

Data Mapping Guide

February 14, 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 Arbor-APS DDoS 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** – DDoS
- **Device Vendor** – Arbor
- **Device Product** – Arbor-APS
- **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 Arbor-APS DDoS using the following format:

- **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 – DDoS
deviceVendor – Arbor

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
CustomerId	customerId	d656b196-edb7-45e6-8485-3748a740d002	Unique customer ID
EventId	eventId	d656b196-edb7-45e6-8485-3748a740d002	Unique event ID
EventTime	eventTime	1569865553705	Epoch time for the time when the event occurred
ReceivedTime	receivedTime	Aug 13 14:08:31	Time stamp when event occurred
DeviceName	deviceName	APS arbor-networks-aps	Data source on which the session was logged
DeviceType	deviceType	DDOS	Type of device
DeviceModel	deviceVendor	Arbor	Name of the device manufacturer
Action	action	Blocked Host	Action taken for the session
SourceIP	sourceIpv4	192.168.100.10 | 00:08:20:83:53:D1	Original session source IP address (IPV4 or IPV6)
Reason	reason	Invalid Packets DNS Rate Limiting Blacklisted Hosts Filter List Blocked Countries ICMP Flood Detection Malformed HTTP Filtering Block Malformed SIP Traffic	Built-in countermeasures designed to detect and automatically engage on specific types of attacks based on the vendors deep experience and knowledge of the attack landscape.
IPProtocol	transportProtocol	UDP, TCP	Principal communications protocol in the Internet protocol suite for relaying datagrams across network boundaries
DestinationPort	destinationPort	53	Port numbers used to determine what protocol the incoming traffic should be directed to
Protocol	protocol	DOMAIN, HTTPS, MICROSOFT-DS	TCP/UDP Protocol associated with the session
DestinationIP	destinationIpv4	192.168.100.10 | 00:08:20:83:53:D1	Original session destination IP address (IPv4 or IPv6)

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
SourcePort	sourcePort	34944	The source port of the logged flow. Registered and Dynamic Port numbers (1024-65535)
URL	requestUrl	https://APS/summary/	The URL address that can be accessed to view event data for this data source (maximum of 512 characters).
Tags	tags	DDOS	
CollectorId	collectorId	ae102769-bd05-415d-af3c-2cc59681cbab	Unique collector ID to identify log source
GeoSourceCordinates	geoSourceCoordinates	["12.976230", "77.603290"]	The latitude, longitude of the source
GeoDestainationCordinates	geoDestinationCoordinates	["19.014410", "72.847940"]	The latitude, longitude of the destination
GeoSourceCountry	geoSourceCountry	India	Source Country name
GeoDestinationCountry	geoDestinationCountry	India	Destination Country name
GeoSourceCity	geoSourceCity	Bengaluru	Source City name
GeoDestinationCity	geoDestinationCity	Mumbai	Destination City name
EventContext	eventContext	local to remote, remote to local	Event Context

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
deviceType	DDoS
deviceModel	APS
deviceVendor	Arbor
deviceHost	el.xyz.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 14, 2021 11:29:04 AM

Field Value Mappings

Data source field: action

Source Values	Qualys Normalized Values
Blocked Host	Block