Qualys Context Extended Detection and Response

Blue Coat Proxy

Data Mapping Guide

February 16, 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 Blue Coat Proxy 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** – Proxy
- **Device Vendor** – Blue Coat
- **Device Product** – Blue Coat Proxy
- **Supported Versions** – Limited Support – Contact your TAM for further information.

Supported Formats

In Qualys Context XDR, you can configure to receive data from Blue Coat Proxy 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 – Proxy
deviceVendor – Blue Coat

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
CustomerId	customerId	d656b196-edb7-45e6-8485-3748a740d002	Unique customer ID
EventTime	eventTime	1569865553705	The time at which the individual event occurred
EventId	eventId	d656b196-edb7-45e6-8485-3748a740d002	Unique event ID
DeviceModel	deviceVendor	BlueCoat	Manufacturer of the device used in the event
DeviceType	deviceType	Proxy	Type of device producing the audit events
Duration	receivedTime	2005-05-04 17:16:22	Time stamp when event occurred
ElapsedTime	duration	1	Time taken (in milliseconds) to process the request
SourceIP	sourceIpv4	45.14.1.98	IP address of the client
Status	status	200	Status of the request. For example, 200 OK, 400 PNF
Action	action	PROXIED	Type of action taken to process this request
OutByte	outByte	391	Number of bytes sent from appliance to client
InByte	inByte	339	Number of bytes sent from client to appliance
Method	method	GET	Request method used from client to appliance
Scheme	scheme	http	Scheme from the 'log' URL
DeviceHost	destinationHost	www.southwest.com	Hostname from the 'log' URL. RDNS is used if the URL uses an IP address.
UriPath	requestUrl	/images/slrl_on.gif	Path from the 'log' URL. Does not include query
Query	requestUrl	-	Query from the 'log' URL
UserName	userName	-	Relative username of a client authenticated to the proxy (i.e. not fully distinguished)
VirusDetails	riskType	-	Details of a virus if one was detected
Hierarchy	hierarchy	DIRECT	How and where the object was retrieved in the cache hierarchy
ServiceName	destinationServiceName		Service name on the destination machine (the machine that has generated this event as per the log audit)
SupplierName	requestUrlDomain	63.169.44.100	Name of the upstream host (not available for a cache hit)
ProtocolCode	protocolCode	none	ICAP error code

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
ConnectionType	connectionType	image/gif	Used to identify a type of data uploaded on internet. It is used so software can know how to handle the data. It serves the same purpose on the Internet that file extensions do on Microsoft Windows. E For example, text/html,image/gif
RequestClientApp	userAgent	"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)"	Request header: User-Agent.
ErrorDetails	reason	-	ICAP error details
Category	category	TCP_HIT	Category of log - TCP-HIT, TCP-MISS
VirusId	risk	-	Identifier of a virus if one was detected
DestinationIP	destinationIpv4	192.16.170.42	IP address of the appliance on which the client established its connection
SiteName	siteName	SG-HTTP-Service	Service used to process the transaction
Domain	objectCategory	TRAVEL	example: Travel, Sports/Recreation/Hobbies
DeviceName	deviceName		Host name of the device where event is produced/logged
CollectorId	collectorId	ae102769-bd05-415d-af3c-2cc59681cbab	Unique collector ID to identify log source
GeoSourceCoordinates	geoSourceCoordinates	[52.090830, 5.122220]	Geographical coordinates of source in latitude and longitude
GeoDestinationCoordinates	geoDestinationCoordinates	[36.174970, -115.137220]	Geographical coordinates of destination in latitude and longitude
GeoSourceCountry	geoSourceCountry	Netherlands	Source country name
GeoDestinationCountry	geoDestinationCountry	United States	Destination country Name
GeoSourceCity	geoSourceCity	Utrecht	Source city name
GeoDestinationCity	geoDestinationCity	Las Vegas	Destination city name
EventContext	eventContext	local to remote, remote to local	Context of connection: Ingoing / Outgoing
SourcePort	sourcePort		Source port utilized by the session
DestinationPort	destinationPort		Destination port utilized by the session
Protocol	protocol		TCP, UDP

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Tags	tags	proxy	Different tags for more details like device type, jdbc, parser details

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
deviceType	Proxy
deviceModel	Bluecoat Proxy
deviceVendor	Bluecoat
deviceHost	DC2-PA-XXX.npi.int
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