Qualys Context Extended Detection and Response

ForgeRock

Data Mapping Guides

January 22, 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 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 ForgeRock fields and the Qualys data model.

Note: For the ForgeRock parser, we are ingesting logs with Linux Agent; hence source creation is happening differently. For ingesting the ForgeRock Logs, you need to add a New Profile, go to the Qualys Context XDR UI, and navigate to **Configuration** > **Cloud Agent Profiles** > **Profiles**.

Device Details

- **Device Type** – IAM
- **Device Vendor** – ForgeRock
- **Device Product** – ForgeRock
- **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 ForgeRock using the following formats:

- **JSON**

Data Field Mappings

This section provides a detailed mapping of the data source fields to the Qualys Context XDR.

deviceType – IAM
deviceVendor – ForgeRock

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
timestamp	eventTime	9/24/2021 3:50	Time of the event
client.ip	sourceIpv4	64.39.96.133	
client.port	sourcePort	39488	Source Port
server.ip	destination Ipv4	0.0.0.0	Destination IP
server.port	destination Port	636	Destination Port
eventName	eventName	DJ-LDAP	
request.protocol	protocol	LDAPS	
request.dn	distinguishedName	ou=events,ou=cluster,dc=openidm,dc=forgerock,dc=io	Distinguished Name
request.scope	searchScope	one	
request.filter	searchFilter	(&(fr-idm-json:caseIgnoreJsonQueryMatch:=/instanceId eq \"node1\")(objectClass=uidObject)(objectClass=fr-idm-generic-obj))	
request.connId	baseEventId	339280	Connection Number
request.operation	eventType	SEARCH	Common REST operation taken on the object; for example, UPDATE, DELETE, or ACTION.
transaction Id	externalId	90398517-8504-4eb7-9692-4dc77f29ad74-8214078	Specifies the UUID of the transaction, which identifies an

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
			external request when it comes into the system boundary
userId	sourceUserId	uid=admin	
response.nentries	count	0	
response.statusCode	status		Specifies the response status code
response.status	outcome	Normally, SUCCESSFUL, FAILED, or null.	
response.elapsedTime	elapsedTime		Specifies the time to execute the access event, usually in millisecond precision.
http.request.method	method	GET, POST, PUT	Specifies the HTTP method requested by the client.
http.request.path	requestUrl	https://openam.example.com:8443/openam/json/realms/root/authenticate	Specifies the path of the HTTP request

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
DeviceType	IAM
DeviceModel	LDAP
DeviceVendor	ForgeRock
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