Qualys Context Extended Detection and Response

Cloudfare Audit

Data Mapping Guides

January 19, 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 Cloudfare Audit 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** – Cloud Infrastructure
- **Device Vendor** – Cloudfare
- **Device Product** – Cloudfare Audit
- **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 Cloudfare Audit 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 – Cloud Infrastructure
deviceVendor – Cloudfare

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
action.result	outcome	true	Whether the action was successful.
action.type	eventType	token_revoke	Type of action taken.
actor.email	emailSender	srai@qualys.com	Email of the actor.
actor.id	sourceUserId	95e2bd719dda45ab65f0d6403f1b6c06	Unique identifier of the actor in Cloudflare's system.
actor.ip	sourceIpv4 | sourceIpv6	115.110.247.173	Physical network address of the actor.
actor.type	category	user	Type of user that started the audit trail.
id	externalId	a76eb835-02cf-456c-b986-4dbed7cb3b77	Unique identifier of an audit log.
interface	objectCategory	API	Entry point or interface of the audit log.
newValue	customString6		Contains the new value for the audited item.
oldValue	customString7		Contains the old value for the audited item.
owner.id	destinationUserId	95e2bd719dda45ab65f0d6403f1b6c06	The identifier of the user that was acting or was acted on behalf of. If a user did the action themselves, this value will be the same as the ActorID.
resource.id	customString8	95e2bd719dda45ab65f0d6403f1b6c06	Unique identifier of the resource within Cloudflare's system.

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
resource.type	object	account	The type of resource that was changed.
when	eventTime	2022-09-20T12:17:20Z	When the change happened.
metadata.new_token_status	customString9	deleted	Status of the new token.
metadata.old_token_status	customString10	active	Status of the old token.
metadata.token_name	eventName	Edit zone DNS	Token name.
metadata.token_tag		fb144d2f1a8158a26dbe60a71cf8d084	
metadata.zone_name	sourceDomain	srai.workers.dev	Name of the zone.
metadata.subdomain	customString11	srai	Name of the sub domain.
metadata.name	eventName	SSL	Event Name.
metadata.old_value	-	flexible	
metadata.type	-	crypto	
metadata.value	-	full_strict	
metadata.cf-ray	-	749ef3c9014485d2-BOM	
action.info	description	Backup pack issued for certificate pack	Action description.
newValueJson.certificate_authority	certificateAuthority	lets_encrypt	Certificate authority name.

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
newValueJson.authority	certificateAuthority	google	Certificate authority name.
newValueJson.certificates.issuer	certificateIssuer	LetsEncrypt	The issuer of the certificate.
newValueJson.issuer	certificateIssuer	google	The issuer of the certificate.
newValueJson.created_at	certificateSigningTime	2022-09-14T06:04:28.215786Z	Timestamp value when certificate was created/issued.
newValueJson.certificates.issued_on	certificateSigningTime	2022-09-14T17:54:32Z	Timestamp value when certificate was created/issued.
newValueJson.certificates.expires_on	endTime	2022-12-13T05:07:47Z	Timestamp value when certificate gets expired.
newValueJson.expires_on	endTime	2022-12-13T05:07:47Z	Timestamp value when certificate gets expired.
newValueJson.certificates.modified_on	updateTime	2022-09-14T06:07:49.536759Z	Timestamp value when certificate was modified.
newValueJson.modified_on	updateTime	2022-09-14T06:04:29.727271Z	Timestamp value when certificate was modified.
newValueJson.hosts	sourceHost	"*.srai.workers.dev", "srai.workers.dev"	Host name.
newValueJson.certificates.fingerprint_sha256	sha256Hash	5a19dbd02935cebfbd7866489888eb1b65de1cbd537be77e20cea54104015be0	SHA256 hash value.
newValueJson.certificat	sha1Hash	5a19dbd02935cebfbd7866489888eb1b65de1cbd537be7	SHA1 hash value.

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
es.fingerprint_sha1		7e20cea54104015bee	
newValueJson.certificates.fingerprint_md5	md5Hash	5a19dbd02935cebfbd7866489888eb1b65de1cbd537be77e20cea5410401535	MD5 hash value.
newValueJson.certificates.status	customString12	active	New Certificate Status.
newValueJson.status	customString12	active	New Certificate Status.
oldValueJson.certificates.status	customString13	pending_validation	Old Certificate Status.
oldValueJson.status	customString13	pending_validation	Old Certificate Status.

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
deviceType	Cloud Infrastucture
deviceModel	Cloudflare
deviceVendor	Cloudflare
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 01, 2021 11:29:04 AM