Qualys Context Extended Detection and Response

Teleport

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 Teleport fields and the Qualys data model.

Note: For the Teleport parser, we are ingesting logs with Linux Agent; hence source creation is happening differently. For ingesting the Teleport 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** – Teleport
- **Device Product** – Teleport IAM
- **Supported Versions** – 10.0

Supported Formats

In Qualys Context XDR, you can configure the product to receive data from Teleport IAM 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 – Teleport

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
event	eventType	cert.create	Event type
uid	externalId	30439cc7-eac1-427c-b3b6-f16e6e18b84a	A unique ID for the event log. Useful for deduplication.
code	deviceEventId	TC000I	Event code
time	eventTime	2022-09-12T14:43:32.093Z	Event Timestamp
cluster_name	cluster_name	teleauth.gov1.qualys.us	Teleport Cluster Name
user	userName	vdarji_fr	Teleport user name
login	sourceUser	vdarji_fr	OS login
sid	sessionId	4d8654e6-f454-4a4c-9afe-56479bc224bb	Session ID. Can be used to replay the session.
server_id	deviceId	8dae0cc3-7f1a-44d0-bcbe-07ce36616c0e	Unique server ID
server_hostname	deviceName	ac01.p01.iad02.qualys.com	Hostname of the Server.
server_addr	deviceIPAddress	10.245.3.21:3022	IP address of the Server.
server_labels.datacenter	region	us-east-1	Location where datacenter is present.
server_labels.hostname	deviceName	ac01.p01.iad02.qualys.com	Hostname of the Server.
addr.local	sourceIpv4	10.245.3.21:3022	Address of the SSH node
addr.remote	destinationIpv4	10.245.1.142:6100	Address of the connecting client (user)

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
session_recording	object	node	Entity that records the session.
cert_type	eventSubType	user	Certification type.
identity.user	userName	rdubey	User name.
identity.roles	permissions	"access", "editor", "auditor"	User role names
identity.logins	sourceUser	"abandal", "-teleport-internal-join"	Login user name.
identity.expires	endTime	2022-09-13T01:51:00.93134044Z	Expiry time in RFC8829 format
attributes.email	emailRecipient	vdarji@qualys.com	Email associated with the user.
attributes.isMemberOf	message	cn=psec,ou=groups,ou=identities,dc=gov,dc=qualys,dc=us	Directory tree information.
attributes.logins	sourceUser	vdarji_fr	Login user name.
attributes.groups	group	sa	Group name.
attributes.uid	sourceUserId	vdarji_fr	
url	requestUrl	file:///var/lib/teleport/log/records/multi/738d39f7-8961-4fb1-9bd1-23664ca860fc	URL Requested.
success	outcome	true false	Indicates successful/failure connection
connector	connector	new_saml_connector	Connector used for connection
participants	participants	rdubey	participants
session_start	beginningTime	2022-09-12T13:54:01.533954574Z	Session start time.

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
session_stop	endTime	2022-09-12T14:39:21.507880112Z	Session end time.
tx	outByte	12966	Bytes sent during the session.
rx	inByte	12918	Incoming bytes during the session.
db_name	db_name	test	Database/schema name
db_protocol	db_protocol	postgres	Database protocol
db_query	db_query	SELECT * FROM test	Query text
db_service	db_service	db2	Database service name
db_uri	db_uri	db2:5432	Database server endpoint
db_user	db_user	postgres	Database account name
db_query_parameters	db_query_parameters	"test-id", "2022-04-02 17:50:20-07", "{\"k\": \"v\"}"	Query parameters
identity.traits.email	emailRecipient	vdarji@qualys.com	Email associated with the user.
identity.traits.groups	group	sa	Group name.
identity.traits.isMemberOf	message	cn=psec,ou=groups,ou=identities,dc=gov,dc=qualys,dc=us	Directory tree information.
identity.traits.logins	sourceUser	vdarji_fr	Login user name.
identity.traits.uid	sourceUserId	vdarji_fr	Login user Id.
identity.traits.aws_role_arns	permissions	null	AWS role.
identity.traits.db_names	db_name	null	Database/schema name
identity.traits.db_users	db_user	null	Database account name

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
identity.traits.kubernetes_groups	group	null	kubernetes group name.
identity.traits.kubernetes_users	userName	null	kubernetes User name
identity.traits.windows_logins	accountName	null	Windows login name.
error	error	access to database denied	Connection error
message	message	access to database denied	Detailed error message
method	method	saml	Method used during authetication.
desktop_addr	sourceIpv4	192.168.1.206:3389	Windows host IP address.
desktop_labels.teleport.dev/dns_host_name	deviceName	WIN-I44F9TN11M3.teleport.example.com	Windows host name including domain name.
desktop_labels.teleport.dev/os	osDetails	Windows Server 2012 R2 Standard Evaluation	Windows host OS (Operating System) information.
desktop_labels.teleport.dev/os_version	version	6.3 (9600)	OS version.
desktop_labels.teleport.dev/windows_domain	sourceDomain	teleport.example.com	Windows domain name.
proto	protocol	tdp	Protocol name.
windows_desktop_service	deviceId	316a3ffa-23e6-4d85-92a1-5e44754f8189	Windows host service
windows_domain	sourceDomain	teleport.example.com	Windows domain name.

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
windows_user	accountName	administrator	Windows user name.
desktop_name	deviceName	WIN-I44F9TN11M3-teleport-example-com	Windows computer name.
length	outByte	4	Number of bytes sent
pid	processId	319267	Process Id
cgroup_id	connector	10863	Group Id
program	application	curl	Program name.
dst_port	destinationPort	80	Destination port number.
src_port	sourcePort	3389	Source port number.
src_addr	sourceIpv4	0.0.0.0	Source IP address.
dst_addr	destinationIpv4	216.58.194.206	Destination IP address.
version	version	4	Version number.
action	action	1	Action
mfa_device.mfa_device_name	deviceName	otp-device	MFA (Multifactor Authentication) device name.
mfa_device.mfa_device_uuid	participants	c5af73f3-9723-49a5-94d6-f6b3f0178bd0	MFA (Multifactor Authentication) device UUID.
mfa_device.mfa_device_type	category	TOTP	MFA (Multifactor Authentication) device type.
user_agent	userAgent	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/105.0.0.0 Safari/537.36	Agent through which the request was made.
name	sourceUser	rasoni_fr	User name.
expires	endTime	2022-09-12T12:46:16.301734501Z	MFA token expiry time.

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
roles	permissions	dbre	User role.

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
DeviceType	IAM
DeviceModel	Teleport
DeviceVendor	Teleport
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