# Qualys Context XDR (Extended Detection and Response)

## Oracle OCI VCN Flow

Data Mapping Guide

February 13, 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 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 Oracle OCI VCN Flow fields and the Qualys data model.

**Note**: For a complete list of sources that Qualys XDR supports, on the Qualys 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.

## Device Details

- **Device Type** – Cloud Infrastructure
- **Device Vendor** – Oracle
- **Device Product** – Oracle OCI VCN Flow
- **Supported Versions** – Limited Support. Contact your TAM for further information.

## Supported Formats

In Qualys Context XDR, you can configure to receive data from Oracle OCI VCN Flow using the following formats:

- **Cloud**

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** – Oracle

| Data Source Fields | Qualys Context XDR QQL Tokens | Sample Values | Description |
|---|---|---|---|
| data.action | action | ACCEPT | Type of record. Possible values:<br>ACCEPT: This record's traffic was accepted by the security lists.<br>REJECT: This record's traffic was rejected by the security lists. |
| data.bytesOut | outByte | 17114 | Number of bytes recorded in the capture window |
| data.destinationAddress | destinationIpv4 | 10.0.99.4 | IP address of the destination, either in IPv4 dot, or IPv6 colon notation. |
| data.destinationPort | destinationPort | 36266 | IANA port number of the destination. |
| data.endTime | endTime | 1598917970 | End time of the capture window in UNIX epoch seconds. |
| data.flowid | md5Hash | a6a73770 | Hash of key fields (source and destination addresses, ports, and protocol). |
| data.packets | packets | 250 | Number of packets recorded in the capture window. |
| data.protocol | Oracle_VCN_Data_Protocol | 6 | IANA protocol number. |
| data.protocolName | protocol | TCP | IANA name for protocol. |
| data.sourceAddress | sourceIpv4 | 123.0.0.1 | IP address of the source, either in IPv4 dot, or IPv6 colon notation. |
| data.sourcePort | sourcePort | 443 | IANA port number of the source. |

| Data Source Fields | Qualys Context XDR QQL Tokens | Sample Values | Description |
|---|---|---|---|
| data.startTime | beginningTime | 1598917969 | Start time of the capture window in Unix epoch seconds. |
| data.status | status | OK | Status of data capture window. Possible values:<br>OK<br>NODATA<br>SKIPDATA |
| data.version | version | 2 | Version of the flow log record schema. |
| id | externalId | abcdabcd-abcd-abcd-abcdabcdabcd | Random UUID, unique to each log entry. |
| oracle.compartmentid | Oracle_CompartmentId | ocid1.compartment.oc1.<region-id>.<unique-id> | OCID of the compartment the log group is in. |
| oracle.ingestedtime | receivedTime | 2020-08-31T23:53:54Z | Time the log was ingested by OCI Logging. |
| oracle.loggroupid | Oracle_LogGroupId | ocid1.loggroup.oc1.<region-id>.<unique-id> | OCID of the log group. |
| oracle.logid | Oracle_LogId | ocid1.log.oc1.<region-id>.<unique-id> | OCID of the log. |
| oracle.tenantid | Oracle_TenantId | ocid1.tenancy.oc1..<region-id>.<unique-id> | OCID of the tenant. |
| oracle.vniccompartmentocid | Oracle_VCN_VnicCompartmentoc_Id | ocid1.compartment.oc1..<region-id>.<unique-id> | OCID of the compartment to which the VNIC belongs. |
| oracle.vnicocid | Oracle_VCN_Vnicoc_Id | ocid1.vnic.oc1.<region-id>.<unique-id> | OCID of the VNIC. |
| oracle.vnicsubnetocid | Oracle_VCN_VnicSubnetoc_Id | ocid1.subnet.oc1.<region-id>.<unique-id> | OCID of the subnet to which the VNIC belongs. |
| time | eventTime | 2020-08-31T23:52:35Z | Same as startTime. |

| Data Source Fields | Qualys Context XDR QQL Tokens | Sample Values | Description |
|---|---|---|---|
| type | eventType | com.oraclecloud.vcn.flowlogs.DataEvent | Category of log: DataEvent, QualityEvent.NoData, or QualityEvent.SkipData. |

## Qualys Internal Fields

| Qualys Context XDR QQL Tokens | Sample Values |
|---|---|
| DeviceType | Cloud Infra |
| DeviceModel | Oracle OCI VCN |
| DeviceVendor | Oracle |
| DeviceHost | - |
| 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 |