Qualys Context XDR (Extended Detection and Response)

Smokescreen Decoy

Data Mapping Guide

May 05, 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 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 Smokescreen Decoy 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** – Decoy
- **Device Vendor** – Smokescreen
- **Device Product** – Smokescreen Decoy
- **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 Smokescreen Decoy 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 – Decoy
deviceVendor – Smokescreen

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
timestamp	eventTime	1569865553705	Epoch time for the time at which the event occurs
timestamp_string	beginningTime	2019-02-16T10:49:36+00:00	Time when the log was sent at the management plane
EndTime	endTime	2/16/2019 16:19:36	Time when the log was received at the management plane
appliance	ApplianceID	AXIAIRRU01	The ID of the appliance
attacker	sourceUserId	ab-npc1-d1a176	The ID of the attacker
type	eventType	network | shares | ssh	Services being used
sub_type	eventSubType	tcp | icmp | user_connect | version	Protocol used for the services
decoy_ip	destinationIpv4	10.101.0.44	The IP of the decoy that was attacked
protocol	protocol	tcp | ICMP	IP protocol associated with the session
target_port	destinationPort	445	The destination port of the logged flow (TCP or UDP), that was targeted
attacker_hostname	sourceHost	AB-NPC1-D1A176	Hostname of the attacker
attacker_ip	sourceIpv4	10.101.11.208	IP address of the attacker
username	userName	cwip1961	Local or domain username
decoy_id	deviceId	minwifimgmt2	Decoy device ID
domain	requestUrlDomain	AXISB	The domain where the user is registered
version	version	SSH-2.0-PuTTY_Release_0.60	Version of the SSH protocol in use

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
customerId	d656b196-edb7-45e6-8485-3748a740d002
deviceType	Decoy
deviceVendor	Smokescreen
collectorId	ae102769-bd05-415d-af3c-2cc59681cbab
eventId	d656b196-edb7-45e6-8485-3748a740d002
tags	Decoy
deviceName	AXIAIRRU01
geoSourceCoordinates	["45.8491", "-119.7143"]
geoDestinationCoordinates	["36.6544", "-78.3752"]
geoSourceCountry	United States
geoDestinationCountry	United States
geoSourceCity	Boardman
geoDestinationCity	Boydton
eventContext	local to remote, remote to local