Qualys Context Extended Detection and Response

GreenRADIUS

Data Mapping Guides

January 27, 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 GreenRocket Security fields and the Qualys data model.

Note: For the GreenRADIUS parser, we are ingesting logs with Linux Agent; hence source creation is happening differently. For ingesting the GreenRADIUS 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** – GreenRocket Security
- **Device Product** – GreenRADIUS
- **Supported Versions** – v4.8.8.8

Supported Formats

In Qualys Context XDR, you can configure the product to receive data from Cisco IOS 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 – GreenRocket Security

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
source	deviceName	grsgrva	The source that generated the log event.
product_id	deviceId	GreenRADIUS	The product ID. i.e. GreenRADIUS.
event	eventType	AUTH	The event type.
user	sourceUser	vmscan002@corp.qualys.com	The username, in user@domain format.
token_type	eventSubType	Temporary token	The type of token.
token_id	externalId		The public ID of the token.
status	outcome	Success	The authentication status.
details	description	Successful with Temporary token	The authentication status details.
authentication_source	object	RADIUS	The entity that verify authentication.
nas_id	processName	sshd	NAS ID
authenticating_endpoint	destinationIpv4	172.16.240.114	IP address of Authenticating Endpoint.
authenticating_agent	additionalIP	172.16.239.50	IP address of Authenticating Agent.
web_request_source_ip	sourceIpv4	172.18.0.5	IP address of machine initiating web request.

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
DeviceType	IAM
DeviceModel	GreenRADIUS
DeviceVendor	GreenRocket Security
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