Qualys Context Extended Detection and Response

VMware Cb Defense EDR

Data Mapping Guide

February 21, 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 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 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 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 XDR.

This guide focuses on the data mapping between VMware Cb Defense EDR 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** – Endpoint
- **Device Vendor** – VMware
- **Device Product** – VMware Cb Defense
- **Supported Versions** – Limited Support. Contact your TAM for further information.

Supported Formats

In Qualys XDR, you can configure the product to receive data from VMware Cb Defense EDR using the following formats:

- **Splunk**

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 XDR.

deviceType – EDR
deviceVendor – VMware

Object	Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
attribute	ruleName	eventName	Splunk - Suspicious logs	The security rule that was violated
attribute	eventTime	eventTime	1595932823797	Time of the event
attribute	eventDescription	description	Carbon Black has detected one or more threat indicator(s) on one of your devices.	Long textual description of the event as seen in the Carbon Black Cloud web console
attribute	Group	group	default	Policy group where device belongs
attribute	Device Email	emailRecipient	support@mycompany.com	Recipient of the email message as per log audit
attribute	Device Name	destinationHost	CORP\\114795-T470P	Name of the device that created this event
attribute	OS	osDetails	Windows 10 x64	OS type of device (Windows/OSX/Linux)
attribute	Indicators	objectCategory	ENUMERATE_PROCESSES(powershell.exe), MITRE_T1086_POWERSHELL(powershell.exe), BYPASS_POLICY(powershell.exe), FILELESS(powershell.exe), MITRE_T1057_PROCESS_DISCOVERY(powershell.exe),	Indicators that make up the threat
attribute	Severity	deviceSeverity	Monitored	The severity of the alert **Possible values**: MONITORED, THREAT, INFO, MINOR, SERIOUS, CRITICAL For Qualys normalized values, click here.

Object	Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
attribute	url	referrerUrl	https://dashboard.confer.net/investigate?s[searchWindow]=ALL&s[c][DEVICE_ID][0]=1910687&s[c][INCIDENT_ID][0]=8TIB8XFP&orgId=50	Referred URL for the RequestURL
attribute	type	eventType	THREAT	The event type. Use this field to determine which fields should be expected.
attribute	score	riskScore	3	Risk score from the event log
attribute	time	receivedTime	1595932870015	The time at which the log was received
attribute	summary	message	The application powershell.exe is executing a fileless script or command.	Additional field - future use
threatInfo.threatCause	actorProcessPPid	processId	18328-132404064237833975-0	PID of the actor process
threatInfo.threatCause	reason	reason	R_FILELESS	Description of the alert
threatInfo.threatCause	reputation	reputation	COMMON_WHITE_LIST	Reputation of the threat cause
threatInfo.threatCause	originSourceType	originSourceType	UNKNOWN	Source of the threat cause
threatInfo.threatCause	actorName	threatActorName	null	IP address of the threat actor
threatInfo.threatCause	threatCategory	riskType	NON_MALWARE	Threat category **Possible values**: UNKNOWN, NON_MALWARE, NEW_MALWARE, KNOWN MALWARE RISKY PROGRAM
threatInfo.threatCause	actor	sha256Hash | sourceIpv4	908b64b1971a979c7e3e8ce4621945cba84854cb98d76367b791a6e22b5f6d53	ID of the threat actor

Object	Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
threatInfo.threatCause	causeEventId	baseEventId	cd9b92dfd0be11eabf6cbdcb39782ce6	Event ID that triggered the event
threatInfo.threatCause	actorType	threatActorType	null	
threatInfo	incidentId	instanceId	8TIB8XFP	Instance ID for the cloud instance/asset
deviceInfo	externalIpAddress	natDestinationIP	64.39.96.133	IP address of the host as seen by the backend
deviceInfo	internalIpAddress	destinationIpv4	192.168.100.10	IP address of the endpoint as reported by the sensor
deviceInfo	targetPriorityType	targetPriorityType	LOW	Device priority as assigned via the policy **Possible values**: LOW, MEDIUM, HIGH, CRITICAL
deviceInfo	uemId	uemId	null	Unified Endpoint Management identifier assigned by VMware Workspace ONE Intelligence, only populated if the Workspace ONE integration is configured.

Qualys Internal Fields

Qualys XDR QQL Tokens	Sample Values
deviceType	Endpoint
deviceModel	Cbdefense
deviceVendor	VMware
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

Field Value Mappings

Data source field: deviceSeverity

Source Values	Qualys Normalized Values
Monitored	Debug
Threat	Warning
Info	Informational
Minor	Notice
Serious	Alert
Critical	Critical