Qualys Context XDR (Extended Detection and Response)

Cisco AMP Endpoint

Data Mapping Guide

April 13, 2022

Copyright 2022 by Qualys, Inc. All Rights Reserved.

Qualys and the Qualys logo are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

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 Extended 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 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 Cisco AMP Endpoint 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** – Cisco
- **Device Product** – Cisco AMP Endpoint
- **Supported Versions** – 5.4

Supported Collectors

In Qualys Context XDR, you can configure to receive data from Cisco AMP Endpoint using the following collectors:

- **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 – Endpoint
deviceVendor – Cisco

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
severity	deviceSeverity	Medium	Severity details for the event log as per the device which is producing the audit events
date	eventTime	2020-12-11T15:03:29+00:00	Time of the event
detection	risk	Trojan.Fochi.Agent.BA	virus name or the detection name form the event
start_timestamp	beginningTime	1607693448	Event/session start time
computer.hostname	sourceHost	131310MBP15	Hostname of the source machine (the machine who has generated this event as per the log audit)
computer.network_addresses.mac	sourceMac	00:08:20:83:53:D1	Mac address of the source machine (the machine who has generated this event as per the log audit)
computer.network_addresses.ip	sourceIpv4	192.168.100.10	IPv4 address of the source machine (the machine who has generated this event as per the log audit)
computer.network_addresses.mac	customString6	00:08:20:83:53:D1	
computer.network_addresses.ip	additionalIP	10.10.10.10	Additional IP if present in the log. e.g fwded event
computer.user	sourceUser	Johndoe@company.com	Username using/logged-in the source machine (the username present in the log audit as per the log audit logged by the device)

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
computer.external_ip	natSourceIP	192.168.100.10	Natted IP address of the source machine (the machine who has generated this event as per the log audit)
event_type	eventName	Policy Update	brief standard meaning of the message easy to read for Analyst
file.file_path	filePath	C:\\Users\\admin\\Downloads\\SpeedProInstaller.exe	Path of the file where file is present
file.file_name	fileName	psexec.exe	file name as present in the audit event
file.parent.process_id	processId	10516	processid if present in the event log
file.parent.disposition	outcome	Clean	Outcome of the event
file.parent.identity.sha1	sha1Hash	e57a32bc5f8ec856e2f3eaa368e6c5a964357f63	SHA1 hash value of the file
file.parent.identity.md5	md5Hash	f347f035e60cbe07c5f97711a2af21b5	MD5 hash value of the file
file.parent.identity.sha256	sha256Hash	e3d36d602ece84d4b3642133fe61ca821f5e3ffd9bf08a505a96cd4de127d56b	SHA256 hash value of the file
id	externalId	1.6077E+18	Associated ID given in the event by the event source.
detection_id	baseEventId	6.90495E+18	External ID given in the event by the event source.
event_type_id	deviceEventId	553648130	Event ID assigned by the device which is producing the audit events if present in the audit log
file_name	fileName	psexec.exe	file name as present in the audit event
vulnerabilities.name	application	Mozilla Firefox	name of the application used
vulnerabilities.score	cveRating	9.3	CVE criticality related to the CVE ID present in the event.

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
vulnerabilities.cve	cveId	CVE-2020-15663	CVE ID if present in the logs. (mainly applicable for IPS or Vulnerability scanner logs)
vulnerabilities.version	version	79	applicationversion/deviceversion present in the log
vulnerabilities.url	referrerUrl	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-15663	referred URL for the RequestURL.
cloud_ioc.description	reason	The WMI command tool (wmic.exe) is an interface to the Windows Management Instrumentation. It allows display and modification of local and remote computers, setting system variables and executing scripts. This instance is checking for the number of logical processors, and cores of the current machine. This is a common malware sandbox enumeration technique as sandboxes typically will only have a small number of processors and cores. If a small number is detected, the malware making the WMIC call will alter its behavior or exit without producing further malicious activity.	Connection status details
cloud_ioc.short_description	description	W32.WMIProcessCores.ioc	Rest of the fields from raw message
scan.malicious_detections	customString7	0	

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
start_date	beginningTime	2020-12-11T13:30:48+00:00	Event/session start time
tactics	customString8	"TA0002", "TA0008"	
techniques	customString9	"T1035", "T1077"	
Event Type	eventType	Event Logs	Type of the event. (E.g. TRAFFIC, SYSTEM)

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
deviceType	Endpoint
deviceModel	AMP
deviceVendor	Cisco
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: severity

Source Values	Qualys Normalized Values
Critical	Critical
High	Warning
Medium	Notice
Low	Informational