Qualys Context Extended Detection and Response

Proofpoint TAP Email

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 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 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 Proofpoint TAP Email 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** – Email
- **Device Vendor** – Proofpoint
- **Device Product** – Proofpoint Targeted Attack Protection (TAP)
- **Supported Versions** – 8.15.0

Supported Formats

In Qualys Context XDR, you can configure the product to receive data from Proofpoint TAP Email using the following formats:

- **Syslog**

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 – Email
deviceVendor – Proofpoint

Object	Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Attribute	Device Vendor	deviceHost	ProofpointTAP	Author of the Targeted Attack Protection service
Attribute	Event Type (MSGID)	deviceEventId	MSGBLK, MSGDLV, CLKPER, CLKBLK	The MSGID identifies the type of message
Attribute	Severity	deviceSeverity	Warning, Informational, Alert	Severity details for the event log as per the device generating the events. For Qualys normalized values, click here.
Attribute	Description	eventName	A message containing a threat was delivered by PPS.	Brief standard meaning of the message for easy reading
Attribute	Action	action	delivered, quarantined, permitted, blocked	Action taken in the event log For Qualys normalized values, click here.
Attribute	messageTime	eventTime	2020-09-21T01:30:32Z	Time when the message was delivered to the user or quarantined by PPS
Attribute	messageID	baseEventId	20200920183016.714AC13965AB9143@admin.com	Message-ID extracted from the headers of the email message. It can be used to look up the associated message in PPS and is not unique.
Attribute	recipient	emailRecipient	Johndoe@company.com	An array containing the email addresses of the recipients
Attribute	sender	emailSender	no_reply@XYZ.com	The email address of the sender. The user-part is hashed. The domain-part is cleartext.
Attribute	senderIP	sourceIpv4	64.39.96.133	The IP address of the sender
Attribute	phishScore	riskScore	100	The phish score of the message. Higher scores indicate higher certainty.
Attribute	spamScore	spamScore	100	The spam score of the message. Higher scores indicate higher certainty.
threatsInfoMap	threatStatus	outcome	active	The current state of the threat **Possible values**: • active • expired • false positive • cleared For Qualys normalized values, click here.

Object	Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
threatsInfoMap	classification	category	phish	The threat category of the malicious URL **Possible values**: • Malware • Phish • Spam
threatsInfoMap	threatUrl	referrerURL	https://threatinsight(.)proofpoint(.)com/0fef6787-d8ee-d631-92d4-95270f81185c/threat/email/14e7dcc85a196b70f067dbf8f060aa24d4fae948ba423711d63ac5cdeedea60e\	A link to the entry on the TAP Dashboard for the particular threat.
threatsInfoMap	threatTime	beginningTime	2020-09-12T00:11:36.000Z	Time when Proofpoint identified the URL as a threat
threatsInfoMap	threat	requestURL | sha256Hash | message	roundcubenewupdatesnet(.)web(.)app/	Artifact condemned by Proofpoint. The malicious URL, hash of the attachment threat, or email address of the impostor sender.
threatsInfoMap	campaignID	campaignId	cefa140d-38ac-462e-81f5-c877a28c8749	An identifier for the campaign of which the threat is a member, if available at the time of the query. Threats can be linked to campaigns even after these events are retrieved.
threatsInfoMap	threatType	riskType	url	Specifies the threat was an attachment, URL, or message type
threatsInfoMap	threatID	externalId	b809370506c9c29ccac60717caf72cf49a51459f4425d4ca3a26978412e4a3b8	The unique identifier associated with this threat. It can be used to query the forensics and campaign endpoints.
Attribute	malwareScore	riskScore	0	The malware score (0-100) of the message. Higher scores indicate higher certainty.
Attribute	impostorScore	impostorScore	75.0	The impostor score (0-100) of the message. Higher scores indicate higher certainty.
Attribute	cluster	provider	Company_hosted	The name of the PPS cluster that processed the message
Attribute	subject	emailSubject	null	The subject line of the message, if available

Object	Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Attribute	quarantineFolder	filePath	Phish	The name of the folder that contains the quarantined message. This appears only for messagesBlocked events.
Attribute	quarantineRule	quarantineRule	module.spam.rule.inbound_phish_definite	The name of the rule that quarantined the message. This appears only for messagesBlocked events.
Attribute	policyRoutes	policy	default_inbound, tap_group	The policy routes that the message matched during processing by PPS. Comma-delimited
Attribute	modulesRun	detectionMethod	access, smtpsrv, av, zerohour, spf, sandbox, spam, batv, pdr	The list of PPS modules that processed the message
Attribute	messageSize	totalBytes	3560	The size in bytes of the message, including headers and attachments
Attribute	fromAddress	fromEmailAddress	no_reply@XYZ.com	The email address contained in the From: header, excluding friendly name
Attribute	completelyRewritten	rewriteStatus	FALSE	The rewrite status of the message. **Possible values**: • true - all instances of URL threats within the message were successfully rewritten • false - at least one instance of the threat URL was not rewritten • na - the message did not contain any URL-based threats
messageParts	disposition	emailDisposition	inline	• inline - the messagePart is a message body • attached - the messagePart is an attachment
messageParts	md5	md5Hash	3f7b6a40741ddf4d098b5e770a89a810	The MD5 hash of the messagePart contents
messageParts	filename	fileName	text.html	The filename of the messagePart

Object	Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
messageParts	sandboxStatus	sandboxStatus	null	The verdict returned by the sandbox during the scanning process. **Possible values**: • **unsupported** - the messagePart is not supported by Attachment Defense and was not scanned • **clean** - the sandbox returned a clean verdict • **threat** - the sandbox returned a malicious verdict • **prefilter** - the messagePart contained no active content, and was therefore not sent to the sandboxing service • **uploaded** - the message was uploaded by PPS to the sandboxing service, but did not yet have a verdict at the time the message was processed • **inprogress** - the attachment had been uploaded and was awaiting scanning at the time the message was processed • **uploaddisabled** - the attachment was eligible for scanning but was not uploaded because of PPS policy.
messageParts	contentType	contentType	text/html	The true, detected Content-Type of the messagePart. This may differ from the oContentType value.
threatsInfoMap	threatID(2)	threatId2	200900e0954fdb4e44ea4de42ebdfe8c872885ae230235ed6a0c960cba965b6d	Additional identifier associated with the threat.

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
deviceType	Email
deviceModel	TAP
deviceVendor	Proofpoint
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
Warning	Warning
Informational	Informational
Alert	Alert

Data source field: action

Source Values	Qualys Normalized Values
delivered	Delivered
quarantined	Quarantined
permitted	Allow
blocked	Block

Data source field: outcome

Source Values	Qualys Normalized Values
active	Active
expired	Expired
falsepositive	False Positive
cleared	Cleared