Qualys Context Extended Detection and Response

Cisco Umbrella Proxy

Data Mapping Guide

February 18, 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 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 Umbrella Proxy 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** – Proxy
- **Device Vendor** – Cisco
- **Device Product** – Cisco Umbrella Proxy
- **Supported Versions** – Latest

Supported Collectors

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

- **Syslog / Cloud**

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 – Proxy
deviceVendor – Cisco

DNS logs

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Timestamp	eventTime	7/7/2020 8:12	When this request was made in UTC. This is different than the Umbrella dashboard, which converts the time to your specified time zone.
Policy Identity	policy	131596MBP16	The first identity that matched the request.
Identities	sourceHost	131596MBP16	All identities associated with this request.
InternalIp	sourceIpv4	192.168.100.10	The internal IP address that made the request.
ExternalIp	natSourceIP	64.39.96.133	The external IP address that made the request.
Action	action	Allowed	Whether the request was allowed or blocked.
QueryType	requestContext	1 (A)	The type of DNS request that was made. For more information, see Common DNS Request Types.
ResponseCode	outcome	NOERROR	The DNS return code for this request. For more information, see Common DNS return codes for any DNS service (and Umbrella).
Domain	requestUrlDomain	sharepoint.com	The domain that was requested.
Categories	objectCategory	Software/Technology,Business Services,Infrastructure,SaaS and B2B,Science and Technology,Application	The security or content categories that the destination matches. For category definitions, see Understanding Security Categories and Understanding Content Categories.

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Policy Identity Type	customString6	Anyconnect Roaming Client	The first identity type matched with this request. Available in version 3 and above.
Identity Types	instanceType	Anyconnect Roaming Client	The type of identity that made the request. For example, Roaming Computer, Network, and so on. Available in version 3 and above.
Blocked Categories	customString7	-	The categories that resulted in the destination being blocked. Available in version 4 and above.
SA Internal Field	eventType	dnslogs	Type of the event. (E.g. TRAFFIC, SYSTEM)

Proxy logs

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Timestamp	eventTime	7/7/2020 8:12	When this request was made in UTC. This is different than the Umbrella dashboard, which converts the time to your specified time zone.
Identities	sourceHost	114886-T480	All identities associated with this request.
InternalIp	sourceIpv4	192.168.100.10	The internal IP address that made the request.
ExternalIp	natSourceIP	64.39.96.133	The external IP address that made the request.
Destination IP	destinationIpv4	64.39.96.133	The destination IP requested.
Content Type	customString8	application/octet-stream	The type of web content, typically text/html.
Verdict	action	ALLOWED	Whether the destination was blocked or allowed.

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
URL	requestUrl	https://fp.msedge.net/conf/v1/asgw/fpconfig.min.json	The URL requested.
Referer	referrerUrl	-	The referring domain or URL.
userAgent	userAgent	-	The browser agent that made the request.
statusCode	status	200	The HTTP status code; should always be 200 or 201.
requestSize	inByte	2709	Request size in bytes.
responseSize	outByte	2320	Response size in bytes.
responseBodySize	customNumber1	-	Response body size in bytes.
SHA—SHA256	sha256Hash	c0ba8df26703805cd78e3b18d62426379cd755af007278fb8fa75d8e7359714c	hex digest of the response content.
Categories	objectCategory	Search Engines,Application	The security or content categories that the destination matches. For category definitions, see Understanding Security Categories and Understanding Content Categories.
AVDetections	detectionMethod	-	The detection name according to the antivirus engine used in file inspection.
PUAs	customString9	-	A list of all potentially unwanted application (PUA) results for the proxied file as returned by the antivirus scanner.
AMP Disposition	secondaryAction	UNKNOWN	The status of the files proxied and scanned by Cisco Advanced Malware Protection (AMP) as part of the Umbrella File Inspection feature; can be Clean, Malicious or Unknown.
AMP Malware Name	risk	-	If Malicious, the name of the malware according to AMP.
AMP Score	riskScore	0	The score of the malware from AMP. This field is not currently used and will be blank.

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Blocked Categories	customString10	Anyconnect Roaming Client	The categories that resulted in the destination being blocked. Available in version 4 and above.
SA Internal Field	eventType	proxylogs	Type of the event. (E.g. TRAFFIC, SYSTEM)

IP logs

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Timestamp	eventTime	7/7/2020 8:12	When this request was made in UTC. This is different than the Umbrella dashboard, which converts the time to your specified time zone.
Identity	sourceHost	TheComputerName	All identities associated with this request.
Source IP	sourceIpv4	192.168.100.10	The IP of the computer making the request.
Source Port	sourcePort	55605	The port the request was made on.
Destination IP	destinationIpv4	64.39.96.133	The destination IP requested.
Destination Port	destinationPort	443	The destination port the request was made on.
Categories	objectCategory	Unauthorized IP Tunnel Access	Which security categories, if any, matched against the destination IP address/port requested.
SA Internal Field	eventType	iplogs	Type of the event. (E.g. TRAFFIC, SYSTEM)

Cloud Firewall

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Timestamp	eventTime	7/7/2020 8:12	When this request was made in UTC. This is different than the Umbrella dashboard, which converts the time to your specified time zone.
originId	customNumber2	[211039844]	The unique identity of the network tunnel.
Identity	sourceHost	Passive Monitor	All identities associated with this request.
Identity Types	instanceType	CDFW Tunnel Device	The type of identity that made the request. Should always be "CDFW Tunnel Device".
Direction	direction	OUTBOUND	The direction of the packet. It is destined either towards the internet or to the customer's network.
ipProtocol	protocol	1	The actual protocol of the traffic. It could be TCP, UDP, ICMP.
packetSize	customNumber3	84	The size of the packet that Umbrella CDFW received.
Source IP	sourceIpv4	192.168.100.10	The IP of the computer making the request.
Source Port	sourcePort	-	The port the request was made on.
Destination IP	destinationIpv4	64.39.96.133	The destination IP requested.
Destination Port	destinationPort	-	The destination port the request was made on.
dataCenter	availabilityZone	ams1.edc	The name of the Umbrella Data Center that processed the user-generated traffic.
ruleId	externalId	12	The ID of the rule that processed the user traffic.
Verdict	action	ALLOW	Whether the destination was blocked or allowed.
SA Internal Field	eventType	firewalllogs	Type of the event. (E.g. TRAFFIC, SYSTEM)

Intrusion Event Fields

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Timestamp		1/14/2021 9:31	Date and time the syslog message was sent from the device.
Host		IE11Win7.soc.sjc01.cisco.com	Device or interface from which the message was sent
Event Time	eventTime	1/14/2021 9:31	Time of the event
Device Name	deviceName	IE11Win7	Hostname of the device where event is produced/logged
Tag		SFIMS	When configuring a syslog alert response, you can specify the severity and facility associated with the syslog messages to ensure that they are processed properly by the syslog server. Facilities and severities are not displayed in the actual message that appears in the syslog, but are instead used to tell the system that receives the syslog message how to categorize it.
Secondary Device	secondaryDevice	sjc01-soc-ipss04	When device and the management console in picture
IP Address	sourceIpv4	192.168.100.10	IPv4 address of the source machine (the machine who has generated this event as per the log audit)
Port	sourcePort	44788	Port used on the source machine (the machine who has generated this event as per the log audit)
Event Name	eventName	New TCP Port	Brief standard meaning of the message easy to read for Analyst
Event Type	eventType	Discovery Event	Type of the event

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
deviceType	Proxy
deviceModel	Umbrella
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: Action

Source Values	Qualys Normalized Values
Allowed	Allow
Blocked	Block
ALLOWED	Allow
BLOCKED	Block

Data source field: Directory

Source Values	Qualys Normalized Values
OUTBOUND	Outbound
INBOUND	Inbound
PROXIED	Proxied
Proxied	Proxied