Qualys Context Extended Detection and Response

Akamai WAF

Data Mapping Guides

February 14, 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 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 Akamai WAF 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** – WAF
- **Device Vendor** – Akamai
- **Device Product** – Akamai WAF
- **Supported Versions** – Limited Support – Contact your TAM for further information.

Supported Formats

In Qualys Context XDR, you can configure the product to receive data from Akamai WAF using the following formats:

- **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 – WAF
deviceVendor – Akamai

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
asn	asnNumber	11734	Autonomous system number (ASN) is a unique number that's available globally to identify an autonomous system.
method	method	GET	The method of the incoming request, assuming an HTTP request. For example: GET, POST, PUT, and HEAD.
qur	requestUrl	haiku630498=..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2F..%2Fetc%2Fpasswd%00.htm	The client request's full query string
start	beginningTime	1553005153	A string representation of the epoch time when the edge server initiated the connection for the request.
path	filePath	/nri-services/nri-term-deposit.aspx	The path used in the incoming URI from the client, not including query strings
protocol	protocol	HTTP/1.1	The protocol of the transaction being monitored. Currently HTTP or HTTPS.
requestHeaders	requestHeader	Accept: text/html,application/xhtml xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8	The value of the Content-Type header in the client request.

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
responseHeaders	responseHeader	Accept: text/html,application/xhtml xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8\r\nAccept-Language: en-US\r\nCookie: _ga=GA1.3.695480917.1552998798; _gat=1; _gid=GA1.3.1096444416.1552998798; ARRAffinity=f5c22f173e05bd926484cc276c72ec1329224d563635c7e9dd436c0e270becda; ASP.NET_SessionId=zs452p4ha5af42053l24e3wf\r\nUpgrade-Insecure-Requests: 1\r\nUser-Agent: Mozilla/5.0 (X11; Linux x86_64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/61.0.3163.100 Electron/2.0.9 Safari/537.36\r\nHost: www.akamai.com\r\nAccept-Encoding: gzip, deflate\r\nConnection: close\r\nContent-Length: 0\r\n", "responseHeaders": "Server: AkamaiGHost\r\nMime-Version: 1.0\r\nContent-Type: text/html\r\nContent-Length: 332\r\nExpires: Tue, 19 Mar 2019 14:19:13 GMT\r\nDate: Tue, 19 Mar 2019 14:19:13 GMT\r\nConnection: close\r\n	The value of the Content-Length header in the client response.
port	sourcePort	443	The port number of the incoming client request
bytes	totalBytes	332	The content bytes served in the client response
host	destination Host	www.akamai.com	The hostname of the server
tls	tlsVersion	tls1.2	TLS version, if applicable

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
status	status	403	The count of requests that resulted in 2xx, 3xx, 4xx, and 5xx error codes
type	sourceHost	akamai_siem	Characterizes the source of this report data
ruleSelectors	ruleSelectors	REQUEST_COOKIES_NAMES:DECLARE/**/@x/**/char(9)	Identifies the location in the request that triggered each rule
ruleMessages	message	Anomaly Score Exceeded for Command Injection	The message reported by each triggered rule
ruleTags	ruleTags	AKAMAI/POLICY/CMD_INJECTION_ANOMALY	Represents a set of categories for the triggered rule
clientIP	sourceIpv4	209.134.60.114	The IP address of the requesting client
ruleActions	action	deny	Identifies whether the request was aborted (deny) or allowed to pass with a warning logged (alert)
rules	policy	CMD-INJECTION-ANOMALY	A series of identifiers for rules within the configuration that triggered for this request
ruleData	ruleData	DECLARE/**/@x	User-supplied values that led each rule to trigger, typically suspect text that appears somewhere in the request, or a specified Client Reputation score
version	version	1.0	The version of the protocol. For example, 1.0 or 1.1.
Internal Fields	tags	Akamai	Different tags for more details like device type, jdbc, parser details

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
deviceType	WAF
deviceModel	
deviceVendor	Akamai
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
geoSourceCoordinates	37.3526,-121.9541
geoDestinationCoordinates	34.164,-118.2387
geoSourceCountry	United States, United Kingdom
geoDestinationCountry	United States, United Kingdom
geoSourceCity	Santa Clara, Kolkata
geoDestinationCity	Glendale, New York