Qualys Context Extended Detection and Response

Checkpoint Firewall

Data Mapping Guide

February 16, 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 Checkpoint Firewall 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** – Firewall
- **Device Vendor** – Checkpoint
- **Device Product** – Checkpoint Firewall
- **Supported Versions** – R80.20 (Splunk format)

Supported Formats

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

- **Syslog**
- **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 Context XDR.

deviceType – Firewall
deviceVendor – Checkpoint

Data Source Field	Qualys Context XDR QQL Tokens	Sample Values	Description
Syslog Time	receivedTime	8/4/2020 14:45	The time at which the log is received by SA system.
time	eventTime	1596566745	The time stamp when the log was created.
hostname	deviceName	IE11Win7	Hostname of the device where event is produced/logged
product	deviceType	Firewall	Product name
action	action	Accept	"Action of matched rule Possible values: 0 - Drop 1 - Reject 2 - Accept 3 - Encrypt 4 - Decrypt 17 - Authorize 18 - Deauthorize 30 - Bypass 33 - Block 34 - Detect 39 - Do not send 43 - Allow 46 - Ask User 61 - Extract Note: This field is not mandatory to every log"
layer_name	customString6	505BD-Middle Security	Layer name
layer_uuid	customString7	4a38eb87-498d-4c55-b70e-f6f82f86e835	Layer UUID
match_id	customString8	62	Mapping of matched rule to its matched application
parent_rule		0	Parent rule number, in case of inline layer
rule_action	action	Accept	Unknown rule action

Data Source Field	Qualys Context XDR QQL Tokens	Sample Values	Description
rule_uid		5befc758-0579-4acd-946c-b1fbbc303dc0	Access policy rule ID which the connection was matched on
ifdir	direction	inbound	Connection direction
ifname	sourceInterface	ethernet1/2, s1p2	The name of the Security Gateway interface, through which a connection traverses
logid		1	
loguid		{0x5f29acd9,0x2b,0xbfefca9b,0xd20627f9}	UUID of unified logs
origin	additionalIP	192.168.100.10	Name of the first Security Gateway that reported this event
originsicname	customString9	CN\=pridmzfw01,O\=prismvmfw02..2v3c7i	SIC name of the Security Gateway that generated this log
sequencenum	customNumber1	918	Number added to order logs with the same linux timestamp and origin
version	version	5	Applicationversion/deviceversion present in the log
nat_addtnl_rulenum		0	When matching 2 automatic rules, second rule match will be shown otherwise field will be 0
nat_rulenum		121	NAT rulebase first matched rule
xlatedport	natDestinationPort	0	Destination port after applying NAT
xlatedst	natDestinationIP	0.0.0.0	Destination ipv4 after applying NAT
xlatesport	natSourcePort	10692	Source port after applying hide NAT on source IP
xlatesrc	natSourceIP	192.168.100.10	Source ipv4 after applying NAT
dst	destinationIpv4	192.168.100.10	Destination IP
inzone	sourceZone	External	Indicates whether the source zone is internal or external

Data Source Field	Qualys Context XDR QQL Tokens	Sample Values	Description
outzone	destinationZone	DMZ	Indicates whether the destination zone is internal or external
proto	protocol	6	Protocol
s_port	sourcePort	57732	Source host port number
service	destinationPort	135	Protocol and destination port.
service_id	customString10	tcp_135	Service found on the connection (by destination port)
src	sourceIpv4	192.168.100.10	Client source IP address
Source Coordinates	geoSourceCoordinates	37.3526,-121.9541	Geo coordinates of the source IP for the audit log. can be part of enrichment
Destination Coordinates	geoDestinationCoordinates	34.164,-118.2387	Geo coordinates of the destination IP for the audit log. can be part of enrichment
Source Country	geoSourceCountry	United States, India	Country name of the source IP for the audit log. can be part of enrichment
Destination Country	geoDestinationCountry	United States, United Kingdom	Country name of the destination IP for the audit log. can be part of enrichment
Source City	geoSourceCity	Santa Clara, Kolkata	City name of the source IP for the audit log. can be part of enrichment
Destination City	geoDestinationCity	Glendale, New York	City name of the destination IP for the audit log. can be part of enrichment
Event Context	eventContext	remote-to-local, local-to-remote, local-to-local	Event Context, remote-to-local, local-to-local, local-to-remote

Data Source Field	Qualys Context XDR QQL Tokens	Sample Values	Description
flags	customString12		A 32-bit field that provides details on session. this field can be decoded by AND-ing the values with the logged value 0x80000000 —session has a packet capture (PCAP) 0x02000000 —IPv6 session 0x01000000 —SSL session was decrypted (SSL Proxy) 0x00800000 —the session was denied via URL filtering 0x00400000 —session has a NAT translation performed (NAT) 0x00200000 —user information for the session was captured via the captive portal (Captive Portal) 0x00080000 —X-Forwarded-For value from a proxy is in the source user field 0x00040000 —log corresponds to a transaction within a HTTP proxy session (Proxy Transaction) 0x00008000 —the session is a container page access (Container Page) 0x00002000 —session has a temporary match on a rule for implicit application dependency handling. Available in PAN-OS 5.0.0 and above. 0x00000800 —symmetric return was used to forward traffic for this session

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
deviceType	Firewall
deviceModel	
deviceVendor	Checkpoint
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
Drop	Drop
Reject	Deny
Accept	Accept
Encrypt	Encrypt
Decrypt	Decrypt
Authorize	Authorize
Deauthorize	Deauthorize
Bypass	Bypass
Block	Block
Detect	Detect
Do not send	Do not send
Allow	Allow
Ask User	Ask User
Extract	Extract

Data source field: dir

Source Values	Qualys Normalized Values
inbound	remote-to-local
outbound	local-to-remote