Qualys Context Extended Detection and Response

Check Point SmartDefense IPS

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 Check Point SmartDefense IPS 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** – IPS
- **Device Vendor** – Check Point
- **Device Product** – Check Point SmartDefense IPS
- **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 Check Point SmartDefense IPS using the following formats:

- **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 – IPS
deviceVendor – Checkpoint

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Syslog Time	receivedTime	Aug 4 14:59:26	The time at which the log is received by XDR system.
time	eventTime	1596567565	The time stamp when the log was created
hostname	deviceName	prismvmfw02	Hostname of the device where event is produced/logged
severity	deviceSeverity	Medium	Threat severity determined by ThreatCloud **Possible values**: 0 - Informational 1 - Low 2 - Medium 3 - High 4 – Critical Refer to this section for Qualys normalized values for this field.
confidence_level	reputation	High	Confidence level determined by ThreatCloud
product	deviceType	IPS	Product name
alert	action	alert	Alert level of matched rule (for connection logs)
action	action	Detect	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. Refer to this section for Qualys normalized values for this field.
ifdir	direction	inbound	Connection direction Refer to this section for Qualys normalized values for this field.
ifname	sourceInterface	eth2	The name of the Security Gateway interface, through which a connection traverses

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
loguid	externalId	{0x0,0x0,0x0,0x0}	UUID of unified logs
origin	additionalIP	10.44.254.12	Name of the first Security Gateway that reported this event
originsicname	ipsOrigicSicName	CN\=prmdmzfw01,O\=prismvmfw02..2v3c7i	SIC name of the Security Gateway that generated this log
sequencenum	ipsSequenceNumber	3	Number added to order logs with the same Linux timestamp and origin
version	version	5	Application/device version present in the log
attack	category	Malformed Packet	Name of the vulnerability category in case of a host vulnerability or network vulnerability
attack_info	eventName	Invalid TCP flag combination	Description of the detected malicious action.
dst	destinationIpv4	114.143.186.91	Destination IP
industry_reference	cveId	CAN-2002-1071	CVE registry entry
performance_impact	performanceImpact	1	Protection performance impact
protection_id	protectionId	PacketSanity	Protection malware id
protection_name	eventType	Packet Sanity	Specific signature name of the attack
protection_type	eventSubType	anomaly	Type of protection used to detect the attack
proto	protocol	6	Protocol
s_port	sourcePort	49915	Source host port number
service	destinationPort	61380	Protocol and destination port
smartdefense_profile	policy	Default_Protection_2df2f915b4001bd5	IPS profile responsible for the decision about the action
src	sourceIpv4	96.70.22.17	Client source IP address
streaming_engine	reason	Potential network configuration problem detected	Connection status details
sub_policy_name	ipsLayerName	245CR-Internet_New Security	Layer name
suppressed_logs	suppressedLogs	8	Sum of aggregated malicious connections
total_logs	count	5	Total count of the event logs in case they are aggregated
tcp_flags	tcpFlags	FIN-SYN-RST-PUSH-ACK-URG	TCP packet flags (SYN, ACK, etc.,)
Source Coordinates	geoSourceCoordinates	["45.8491", "-119.7143"]	Geo coordinates of the source IP for the audit log. can be part of enrichment

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Destination Coordinates	geoDestination Cordinates	["36.6544", "-78.3752"]	Geo coordinates of the destination IP for the audit log. can be part of enrichment
Source Country	geoSourceCountry	India	Country name of the source IP for the audit log. can be part of enrichment
Destination Country	geoDestination Country	United States	Country name of the destination IP for the audit log. can be part of enrichment
Source City	geoSourceCity	Mumbai	City name of the source IP for the audit log. can be part of enrichment
Destination City	geoDestination City	Boydton	City name of the destination IP for the audit log. can be part of enrichment
Event Context	eventContext	local to remote, remote to local	Event Context, remote-to-local, local-to-local, local-to-remote

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
deviceType	IPS
deviceVendor	Checkpoint
deviceModel	Smartdefense
customerId	d656b196-edb7-45e6-8485-3748a740d002
collectorId	ae102769-bd05-415d-af3c-2cc59681cbab
eventSourceId	75a20062-417a-4ed9-81e2-25c261af8bfd
eventId	d656b196-edb7-45e6-8485-3748a740d002
collectorReceivedTime	Jun 21, 2021 01:29:04 AM
deviceHost	XYZ-IND-APS

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: ifdir

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

Data source field: dvcSeverity

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