Qualys Context Extended Detection and Response

TippingPoint IPS

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 TippingPoint 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** – TippingPoint
- **Device Product** – TippingPoint Endpoint Protection 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 TippingPoint Endpoint Protection IPS using the following format:

- **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 – IPS
deviceVendor – TippingPoint

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Internal Field	customerId	d656b196-edb7-45e6-8485-3748a740d002	Unique customer ID
Internal Field	eventId	d656b196-edb7-45e6-8485-3748a740d002	Unique event ID
Internal Field	CollectorReceivedTime	Jun 01, 2021 11:29:04 AM	Time when the log was received by the XDR system
Log generation time	eventTime	Apr 4, 2019, 3:11:49 PM	Time when the event occurred
Internal Field	deviceVendor	TippingPoint	Manufacturer of the device used in the event
Action Type	action	8	Action set to use. Valid values are restricted to allow, block, and trust. 7 is Permit, 8 is Block, 9 is P2P
Severity	deviceSeverity	2	The SEVERITY of the event. 0 is Normal, 1 is Low, 2 is Minor, 3 is Major, 4 is Critical
Internal Field	deviceModel	Threat Protection System	Device Model provides information like the device type and manufacturer
Signature ID	deviceEventId	23799	The number associated with the Signature in the protocol
Protocol	transportProtocol	HTTP, HTTPS, SMB, TLS, DNS	The protocol of signature, IP, SMB, HTTP, and so on
Signature Name	eventName	Obfuscated HTML Usage	User friendly name of Signature & Policy
Signature Protocol	protocol	TCP, UDP, ICMP	The protocol of captured traffic. Can be an explicit number or tcp, udp, or icmp
Source Address	sourceIpv4	192.168.100.10	Original session source IP address
Source Port	sourcePort	8080	The source port of the logged flow (TCP or UDP)
Destination Address	destinationIpv4	64.39.96.133	Original session destination IP address
Destination Port	destinationPort	39069	The destination port of the logged flow (TCP or UDP)
Hit Count	count	1	The number of times the firewall rule was applied
Source Zone Name	sourceZone	n/a	Zone Name of the Source address
Source Destination Name	destinationZone	n/a	Zone Name of the Destination address

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
VLAN	vlanId	0	The local VLAN that was targeted
Serial Number	externalId	CISCO_115439_D	The serial number of the IPS that generated the log
Category ID	tippingPointTaxonomyId	50269183	Category ID assigned to Signature
Category	category	0	Category associated with the session
Event timestamp in milliseconds	beginningTime	2019-04-04 14:55:33	Time stamp when the scan was started. yyyy-MM-dd HH:mm:ss
ID	ipsServer	ASVBUWB0083	ID of the IPS server
Domain	requestUrlDomain	AKAMAI.COM	The domain where the user is registered
Device Name	deviceId	tp00027757	The ID of the appliance
Internal Field	tags	IPS	Different tags for more details like device type, jdbc, parser details
Scan ID	scanId	1554264612	ID associated with the scan
Duration	duration	0	Session duration
Scan	reason	Scan started on selected drives and folders and all extensions.,,Command: Not a command scan (), Threats: 0,Infected: 0,Total files: 0,Omitted: 0,	Scan details
State	ipsState	Continue, Started	State of scan
Event timestamp in milliseconds	endTime	2019-04-04 14:52:48	Time when the scan ended
Rule	policy	Built-in rule	Policyname/rulename from the device
UserName	userName	None	User name
File Size	totalBytes	5903	File size in bytes
Source Application	sourceServiceName	SysPlant	Source application and Device control driver/service
Destination Application	destinationService	SysPlant	Destination application and Device control driver/service
Application	application	System	The subsystem or application that is providing the event data
Scanned Computer	computerName	CISCO-145212-L	Scanned computer
IP	additionalIP	10.200.174.158	IP associated with scan
Group	group	My Company\\COFMS	Group
Appliance host name	deviceName	VBINSEPMPRDAP01 , SMSIPS	Name of the device generating logs

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Internal Field	collectorId	f9d113fe-cac9-7656-82b6-882a2808461c	Unique collector ID to identify log source
Internal Field	geoSourceCordinates	["37.751", "-97.822"]	Source geo IP Coordinates ["latitude","longitude"]
Internal Field	geoDestinationCordinates	["57.751", "-97.672"]	Destination geo IP Coordinates ["latitude","longitude"]
Internal Field	geoSourceCountry	India	Source Country geolocation
Internal Field	geoDestinationCountry	United States	Destination Country geolocation
Internal Field	geoSourceCity	Mumbai	Source city geolocation
Internal Field	geoDestinationCity	Newyork	Destination city geolocation
Internal Field	eventContext	local-to-remote, remote-to-local	Context of Connection: Incoming/Outgoing
Status	outcome	Success, Failure	Status of event

Field Value Mappings

Data source field: dvcSeverity

Source Values	Qualys Normalized Values
0	Info
1	Notice
2	Warning
3	Error
4	Alert

Data source field: action

Source Values	Qualys Normalized Values
7	Allow
8	Block
9	P2P