Qualys Context Extended Detection and Response

McAfee Network Security Platform IPS

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 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 McAfee Network Security Platform 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** – McAfee
- **Device Product** – McAfee Network Security Platform
- **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 McAfee Network Security Platform IPS using the following formats:

- **CVS**

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 – McAfee

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
SENSOR_ALERT_UUID	externalId	6821769483255275075	Associated ID given in the event by the event source.
ALERT_TYPE	category	Signature	Category of the event log
ATTACK_TIME	eventTime	2020-04-07 11:26:08 PDT	Device receipt time
ATTACK_NAME	eventName	"NETBIOS-SS: SMB Packets Parsing Buffer Overflow"	Specifies the name of the attack
ATTACK_ID	deviceEventId	0x4070e000	Event ID assigned by the device producing the audit events, if present in the audit log
ATTACK_SEVERITY	deviceSeverity	Medium	Displays the severity level as High, Medium, Low, or Informational. • For High severity, the score ranges between 7 and 9. • For Medium severity, the score ranges between 4 and 6. • For Low severity, the score ranges between 1 and 3. • For Informational severity, the score is 0. For information on Qualys normalized values, click here.
ATTACK_SIGNATURE	attackSignature	sig1	
ATTACK_CONFIDENCE	attackConfidence	Medium	
ADMIN_DOMAIN	destinationDomain	IE11Win7	Domain name of the destination machine (the machine towards which this event is directed as per the log audit)
SENSOR_NAME	deviceName	CSCC_Sensor	Device Host Name
INTERFACE	object	G0/2	Device Inbound Interface
SOURCE_IP	sourceIpv4	10.61.241.44	Source Address
SOURCE_PORT	sourcePort	57386	Source Port
DESTINATION_IP	destinationIpv4	10.60.51.102	Destination Address
DESTINATION_PORT	destinationPort	445	Destination Port

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
CATEGORY	eventType	Unknown	Displays the attack category. **Possible values**: • Exploit • DoS Learning Attack • DoS Threshold Attack • Reconnaissance Attack • Policy Violation • Malware **NOTE**: When you are working on Sensors prior to version 8.2, merge the IPS and reconnaissance attack settings from the Reconnaissance Attack Settings Merge Utility page. The reconnaissance attacks are not displayed in the Attack Definitions tab.
SUB_CATEGORY	eventSubType	brute-force	Displays the attack category. **Possible values**: • Exploit • DoS Learning Attack • DoS Threshold Attack • Reconnaissance Attack • Policy Violation • Malware **NOTE**: When you are working on Sensors prior to version 8.2, merge the IPS and reconnaissance attack settings from the Reconnaissance Attack Settings Merge Utilitypage. The reconnaissance attacks are not displayed in the Attack Definitions tab.
DIRECTION	direction	Inbound	Displays the direction of attack as Inbound, Outbound or Any.
RESULT_STATUS	action	Blocked	Specifies the action for the attack
DETECTION_MECHANISM	detectionMethod	signature	for sources like Web proxy and av and sandboxes--CAS MAA
APPLICATION_PROTOCOL	transportProtocol	N/A	Protocol used to make/facilitate the request as present in the audit log
NETWORK_PROTOCOL	protocol	udp	Displays the type of protocol
RELEVANCE	attackRelevance		
QUARANTINE_END_TIME	endTime	2019-03-20 12:06:47	Event/session end time
ALERT_ID	alertId		External Id
ATTACK_COUNT	count	1, 1025	Event Count

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
LAYER_7_DATA	reason	Null, Authentication Required	Connection status details
PROTECTION_CATEGORY	objectCategory	Business, Software/Hardware	Displays the protection category as Client Protection, Server Protection, Malware, Advanced Protection Options, or Network Protection.

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
deviceType	IPS
deviceModel	NSP
deviceVendor	McAfee
deviceHost	Metadata field
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: Severity

Source Values	Qualys Normalized Values
Medium	Warning
Low	Notice
Informational	Informational
Information	Informational
High	Error