Qualys Context XDR (Extended Detection and Response)

Snare Operating System

Data Mapping Guide

April 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 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 Snare Operating System fields and the Qualys data model.

Note: For a complete list of sources that Qualys XDR supports, on the Qualys 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** – Operating System
- **Device Vendor** – Snare
- **Device Product** – Snare Operating System
- **Supported Versions** – 5.5.1.7
    - Windows Vista
    - Windows 7

Supported Formats

In Qualys Context XDR, you can configure to receive data from Snare Operating System using the following formats:

- **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 Context XDR.

deviceType – Operating System
deviceVendor – Snare

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Event Log Type	category	MSWinEventLog	Fixed value of 'MSWinEventLog'
Criticality	deviceSeverity	0	This is determined by the Alert level given to the audit policy by the user and is a number between 0 and 4
LogName	eventType	Security	This is the Windows Event Log from which the event record was derived. In the above example, the event record was derived from the 'security' event log.
Snare Event Counter	baseEventCount	635	Based on the internal Snare event counter. Rotates at 'MAXDWORD'.
DateTime	eventTime	Wed Feb 16 04:51:05 2022	This is the date time stamp of the event record.
EventID	externalId	4689	This is the Windows Event ID.
SourceName	deviceEventId	Microsoft-Windows-Security-Auditing:4689	This is the Source of the Windows Event Log from which the event record was derived.
UserName	sourceUser	SNARE01\Administrator	This is the Window's user name.
EventLogType	message	Success Audit	This can be anyone of 'Success Audit', 'Failure Audit', 'Error', 'Information', or 'Warning'.
ComputerName	deviceHost	snare01	This is the Windows computer name.
CategoryString	eventSubType	Process Termination	This is the category of audit event, as detailed by the Windows event logging system.
DataString	eventName	A process has exited.	This contains the data strings.

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
ExpandedString	description	Subject: Security ID: S-1-5-21-2957414253-2395456600-4194264932-500 Account Name: Administrator Account Domain: SNARE01 Logon ID: 0x338d8 Process Information: Process ID: 0xbe0 Process Name: C:\Windows\System32 undll32.exe	This contains the expanded data strings.
Security ID	winlogSubjectSId	S-1-5-21-2957414253-2395456600-4194264932-500	
Account Name	userName	Administrator	
Account Domain	winlogSubjectDomainName	SNARE01	
Logon ID	customString6	0x338d8	
Process ID	processId	0xbe0	
Process Name	processName	C:\Windows\System32 undll32.exe	
New Process Name	destinationProcess	C:\\Windows\\System32\\rundll32.exe	The full path and the name of the executable for the new process
Sub Status	winlogSubStatus		
Status	winlogStatus		
Mandatory Label	winLogMandatoryLabel	S-1-16-8192	SID of integrity label which was assigned to the new process.
Token Elevation Type	winLogTokenElevationType	%%1938	Token elevation is about User Account Control

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Logon Type	winLogonType		
Ticket Options	ticketOptions	0x40810000	
Ticket Encryption Type	ticketEncryptionType	0x12	
Service Name	destinationServiceName	WIN2008R2$	Service name on the destination machine (the machine that has generated this event as per the log audit)
Object Name	object	C:\\Documents\\HBI Data.txt	group/policy/registry/domain change
Access Mask	permissions	0x12019f	file/user permissions from the event
Share Name	filePath	*\\Documents	Path of the file where file is present
Share Local Path	filePath	\\??\\C:\\Documents	Path of the file where file is present
Relative Target Name	fileName	Bginfo.exe	File name as present in the audit event
Parent Process Name	sourceProcess	C:\\Windows\\explorer.exe	This useful field documents the name of the program that started this new process
Image Path	winLogImagePath	C:\Program Files\Cisco\AMP\endpointisolation\ancrcl64.sys	
Target User Name	group	Administrators	The name of the group which members were enumerated
Target Domain Name	winLogTargetDomainName	Builtin	Group's domain or computer name
Object Server	winLogObjectServer	Security Account Manager	Contains the name of the Windows subsystem calling the routine
Object Type	winLogObjectType	SAM_DOMAIN	The type or class of the object that was accessed

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Setting Type	winLogSettingType	Default Outbound Action	The name of the setting which was modified
Setting Value	winLogSettingValue	Block	New value of modified setting
Profile Changed	group	Domain	The name of profile in which setting was changed. Possible values are: Public Domain Private
Rule ID	winLogRuleId	{F2649D59-1355-4E3C-B886-CDD08B683199}	The unique identifier for modified firewall rule
Rule Name	policy	Allow All Rule	The name of the rule that was modified
Properties	winLogProperties	%%1537 {bf967a86-0de6-11d0-a285-00aa003049e2}	First part is the type of access that was used. Typically has the same value as Accesses field. Second part is a tree of GUID values of Active Directory classes or property sets, for which operation was performed
Target Logon ID	winLogTargetLogonId	0x139faf	Hexadecimal value that can help you correlate this event with recent events that might contain the same Logon ID
category	category	Object Access	the name of auditing Category which subcategory was changed.
Privileges	permissions	SeSecurityPrivilege	The list of user privileges which were requested.
Workstation Name	sourceHost	XDUO-NODE01	Machine name from which a logon attempt was performed.
Source Network Address	sourceIpv4	10.113.107.192	IP address of machine from which logon attempt was performed.
Source Port	sourcePort	53434	Source port which was used for logon attempt from remote machine.

Field Value Mappings

Data source field: device severity

Source Values	Qualys Normalized Values
0	Critical
1	Error
2	Warning
3	Informational
8	Debug

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
customerId	d656b196-edb7-45e6-8485-3748a740d002
deviceType	Operating System
deviceModel	SnareWin
deviceVendor	Snare
deviceHost	snare01
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