Qualys Context Extended Detection and Response

Microsoft Windows Operating System

Data Mapping Guide

May 04, 2022

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100

Table of Contents

About this Guide **4**
About Qualys 4
Qualys Support 4
Overview **5**
Device Details 5
Supported Formats 5
Data Field Mappings **6**
Qualys Internal Fields 12
Field Value Mappings 12

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 Microsoft Windows Operating System 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** – Operating System
- **Device Vendor** – Microsoft
- **Supported Versions** – Windows 10

Supported Formats

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

- **JSON**

For information on configuring cloud agent profile for windows OS, refer to Configuring a Cloud Agent Profile 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 – Operating System
deviceVendor – Microsoft

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Computer	deviceName	131XXX-T.corp.company.com	Hostname of the device where event is produced/logged
logset	deviceSeverity	information	Severity details for the event log as per the device which is producing the audit events
reqClntApp	userAgent		The user agent associated with the request.
act	action	Sensitive Privilege Use	The action mentioned in the event.
EventID	externalId	4673	Associated ID given in the event by the event source.
keywords	eventType	Audit Failure	Type of the event. (E.g. TRAFFIC, SYSTEM)
cat	category		Category of the event log
SourcePort	sourcePort		The source port number. Valid port numbers are 0 - 65535.
osBuild	osDetails		OS Information of the asset
SubjectLogonId	winlogSubjectLogonId	0x1439fb	
ProcessID	processId	4	processid if present in the event log
winHost	winlogHostname	131XX-T4XX.corp.company.com	
SubjectUserSid/ UserSid	winlogSubjectSId	S-1-5-21-776561741-854245398-1417001333-35282	

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
SubjectDomainName/ UserName	winlogSubjectDomainName	CORP, NT AUTHORITY\\SYSTEM	
Guid	guid	54849625-5478-4994-a5ba-3e3b0328c30d	GUID from the event log
SubjectUserName	userName		Username present in the log apart from source and destination username
PrivilegeList	permissions	SeProfileSingleProcessPrivilege	file/user permissions from the event
winTrgtSrvrName	destinationHost		Hostname of the destination machine(the machine towards which this event is directed as per the log audit)
osVer	version		applicationversion/deviceversion present in the log
winlogEventId	deviceEventId		Event ID assigned by the device which is producing the audit events if present in the audit log
path	fileName		file name as present in the audit event
winKey	eventName	Audit Failure	brief standard meaning of the message easy to read for Analyst
Name	deviceEventId	Microsoft-Windows-Security-Auditing:4673	Event ID assigned by the device which is producing the audit events if present in the audit log
src	sourceHost		Hostname of the source machine (the machine who has generated this event as per the log audit)
filePath	filePath		Path of the file where file is present
EventData ProcessName	processName		processname if present in the event log

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
winTarUsername	destinationUser	Jsteven	Username using/logged-in the destination machine (the username presents in the log audit as per the log audit logged by the device)
RemoteUserID	destinationUserId	S-1-0-0	UserID using/logged-in the destination machine (the username present in the log audit as per the log audit logged by the device)
winTarDmn	destinationDomain		Domain name of the destination machine (the machine towards which this event is directed as per the log audit)
winHostName	winlogComputerName		
winUsername	sourceUser	Jsteven	Username using/logged-in the source machine (the username presents in the log audit as per the log audit logged by the device)
tags	tags		Used for QQL
deviceName	deviceModel	Windows	Model details of the device which is producing the audit events
collId	collectorId		Collector ID
srcCord	geoSourceCoordinates	["12.976230", "77.603290"]	Geo coordinates of the source IP for the audit log. can be part of enrichment
dstCord	geoDestinationCoordinates	["19.014410", "72.847940"]	Geo coordinates of the destination IP for the audit log. can be part of enrichment
srcGeoCountry	geoSourceCountry	India	country name of the source IP for the audit log. can be part of enrichment
dstGeoCountry	geoDestinationCountry	India	country name of the destination IP for the audit log. can be part of enrichment

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
srcGeoCity	geoSourceCity	Bengaluru	City name of the source IP for the audit log. can be part of enrichment
dstGeoCity	geoDestinationCity	Mumbai	City name of the destination IP for the audit log. can be part of enrichment
status	outcome	NA	outcome of the event
message	message		additional field - future use
substatus	winlogSubStatus		
TicketOptions	ticketOptions	0x40810000	
TicketEncryptionType	ticketEncryptionType	0x12	
ServiceName	destinationServiceName	WIN2008R2$	Service name on the destination machine (the machine who has generated this event as per the log audit)
ObjectName	object	C:\\Documents\\HBI Data.txt	group/policy/registry/domain change
AccessMask, AccessList	permissions	%%4484, 0x12019f	file/user permissions from the event
ShareName	filePath	*\\Documents	Path of the file where file is present
ShareLocalPath	filePath	\\??\\C:\\Documents	Path of the file where file is present
RelativeTargetName	fileName	Bginfo.exe	File name as present in the audit event
Application	destinationProcess	C:\\Windows\\System32\\rundll32.exe	Full path and the name of the executable for the new process
MandatoryLabel	winLogMandatoryLabel	S-1-16-8192	Token elevation is about User Account Control
TokenElevationType	winLogTokenElevationType	%%1938	SID of integrity label which was assigned to the new process.

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
ParentProcessName	sourceProcess	C:\\Windows\\explorer.exe	This useful field documents the name of the program that started this new process
ProcessName	processName	C:\\Windows\\System32\\lsass.exe	Full path and the name of the executable for the process
ImagePath	winLogImagePath	C:\Program Files\Cisco\AMP\endpointisolation\ancrcl64.sys	
TargetUserName	group	Administrators	The name of the group which members were enumerated
TargetDomainName	winLogTargetDomainName	Builtin	Group's domain or computer name
ObjectServer	winLogObjectServer	Security Account Manager	Contains the name of the Windows subsystem calling the routine
ObjectType	winLogObjectType	SAM_DOMAIN	The type or class of the object that was accessed
SettingType	winLogSettingType	Default Outbound Action	The name of the setting which was modified
SettingValue	winLogSettingValue	Block	New value of modified setting
ProfileChanged	group	Domain	The name of profile in which setting was changed. Possible values are: Public Domain Private
RuleID	winLogRuleId	{F2649D59-1355-4E3C-B886-CDD08B683199}	The unique identifier for modified firewall rule
RuleName	policy	Allow All Rule	The name of the rule that was modified

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
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
TargetLogonID	winLogTargetLogonId	0x139faf	Hexadecimal value that can help you correlate this event with recent events that might contain the same Logon ID
Process Command Line	command	"C:\\Windows\System32\WScript.exe"	Use the built in Windows tasklist command from a command prompt to display all processes, their PIDs, and a variety of other details.
Protocol	protocol	https, http, ftp, ssh, smb	protocol used in the event log
DestAddress	destinationIpv4	239.255.255.250	
DestPort	destinationPort	1900	
Source Address	sourceIpv4	10.113.107.133	
Direction	direction	Inbound, Outbound	
Mac	sourceMac	00:50:56:b0:c4:36	
message	eventName	The Windows Filtering Platform has blocked a packet.	
ChangeType	secondaryAction	Add	If there is additional action in the event log apart from the primary 'Action'.
CalloutName	object	NgcSock ALE Resource Release Callout V6	group/policy/registry/domain change
SubLayerName	object	OpenDNS ERC sublayer, Microsoft Corporation	group/policy/registry/domain change
ProviderContext Name	object	State Management Provider Context	group/policy/registry/domain change

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
ProviderName	object	Microsoft Corporation, ncrclsk transport provider	group/policy/registry/domain change

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
deviceType	Operating System
deviceVendor	Microsoft
deviceModel	Windows
customerId	d656b196-edb7-45e6-8485-3748a740d002
eventId	28e94ea8-0139-4614-9974-99b675cc7d5a
eventTime	May 14, 2021 12:54:05 PM

Field Value Mappings

Source Values	Qualys Normalized Values
critical	Alert
error	Error
warning	Warning
information	Informational
verbose	Debug