Qualys Context Extended Detection and Response

Microsoft Sysmon

Data Mapping Guide

May 08, 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 Microsoft Sysmon 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** – Application
- **Device Vendor** – Microsoft
- **Device Model** – Sysmon
- **Supported Versions** – Contact your TAM for further information.

Supported Formats

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

- **JSON**

For information on configuring cloud agent profile for Windows OS, refer to the 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 – Application
deviceVendor – Microsoft
Model – Sysmon

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Provider Name	deviceEventId	Microsoft-Windows-Sysmon:5	Identifies the provider that logged the event.
EventID			The identifier that the provider used to identify the event.
Version	version	3	Contains the version number of the event's definition.
Channel	eventType	Microsoft-Windows-Sysmon/Operational	The channel to which the event was logged.
ProcessID	processId	6184	Contains information about the process and thread that logged the event.
SystemTime	eventTime	2022-03-28T06:31:40.495Z	The time stamp identifies when the event was logged.
EventRecord ID	baseEventId	10470	The record number assigned to the event when it was logged.
Level	deviceSeverity	information	Contains the severity level of the event.
Computer	deviceHost	win10-security	The name of the computer on which the event occurred.
UserID	SourceUser	SYSTEM	Identifies the user that logged the event.
	eventName	Sysmon service state changed	The brief standard meaning of the message is easy to read for Analyst
	action	Process terminated (rule: ProcessTerminate)	Action taken in the event log
	outcome	Success	Outcome of the event
Description	description	ServiceHub.TestWindowStoreHost.exe	Description of the image associated with the main process (child)

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
ProcessId	processId	1524	Process ID is used by the OS to identify the created process (child)
Image	processName/destinationProcess	C:\\Program Files (x86)\\Microsoft Visual Studio\\2019\\Community\\Common7\\ServiceHub\\Hosts\\ServiceHub.Host.CLR.AnyCPU\\ServiceHub.TestWindowStoreHost.exe	The file path of the process being spawned/created. Considered also the child or source process.
OriginalFileName	fileName	ServiceHub.TestWindowStoreHost.exe	OriginalFileName from the PE header
CommandLine	command	C:\\Program Files (x86)\\Microsoft Visual Studio\\2019\\Community\\Common7\\ServiceHub\\Hosts\\ServiceHub.Host.CLR.AnyCPU\\ServiceHub.TestWindowStoreHost.exe\" \"desktopClr$TestWindowStoreHost\" \"net.pipe://1385681B06960414BDDED6C74F0D5D5786059\" \"/TelemetrySession:{\"\"\"IsOptedIn\"\"\":true,\"\"\"HostName\"\"\":\"\"\"Dev14\"\"\",\"\"\"AppInsightsInstrumentationKey\"\"\":\"\"\"f144292e-e3b2-4011-ac90-20e5c03fbce5\"\"\",\"\"\"AsimovInstrumentationKey\"\"\":\"\"\"AIF-312cbd79-9dbb-4c48-a7da-3cc2a931cb70\"\"\",\"\"\"AppId\"\"\":1001,\"\"\"UserId\"\"\":\"\"\"64098f91-19ca-4818-8e81-2d081fba3d64\"\"\",\"\"\"Id\"\"\":\"\"\"65f4d865-1df0-4e47-8b24-18b5f5d1123f\"\"\",\"\"\"ProcessStartTime\"\"\":637840454737777844}	Arguments that were passed to the executable associated with the main process.

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
User	sourceUser/destinationUser	WIN10-SECURITY\\Administrator	Name of the account that created the process (child). It usually contains domain name and username.
LogonId	destinationUserId	0x42e660a	Login ID of the user who created the new process. Value that can help you correlate this event with others that contain the same Logon ID
TerminalSessionId	sessionId	2	ID of the session the user belongs to
IntegrityLevel	customString6	High	There are four integrity levels, low, medium, high, and system. It is not possible for a process with a lower integrity level to open a handle with full access to a process with a higher integrity level.
Hashes	sha1Hash/sha256Hash/md5Hash	263E0DB5FEAE3197DD608C9D810973DB623587E2DC944FDAFAFF47FD189840F4	Full hash of the file with the algorithms in the HashType field
ParentImage	sourceProcess	C:\\Program Files (x86)\\Microsoft Visual Studio\\2019\\Community\\Common7\\ServiceHub\\controller\\Microsoft.ServiceHub.Controller.exe	File path that spawned/created the main process

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
ParentCommandLine	customString7	C:\\Program Files (x86)\\Microsoft Visual Studio\\2019\\Community\\Common7\\ServiceHub\\controller\\Microsoft.ServiceHub.Controller.exe\" \"6e79eeee5b491ef4c95138b06251ef14c4b1bb5dce9ea3855fbade82821aaa9d//\\\\devenv.exe.config\" /TelemetrySession:{\"\"\"IsOptedIn\"\"\":true,\"\"\"HostName\"\"\":\"\"\"Dev14\"\"\",\"\"\"AppInsightsInstrumentationKey\"\"\":\"\"\"f144292e-e3b2-4011-ac90-20e5c03fbce5\"\"\",\"\"\"AsimovInstrumentationKey\"\"\":\"\"\"AIF-312cbd79-9dbb-4c48-a7da-3cc2a931cb70\"\"\",\"\"\"AppId\"\"\":1001,\"\"\"UserId\"\"\":\"\"\"64098f91-19ca-4818-8e81-2d081fba3d64\"\"\",\"\"\"Id\"\"\":\"\"\"65f4d865-1df0-4e47-8b24-18b5f5d1123f\"\"\",\"\"\"ProcessStartTime\"\"\":637840454737777844}	Arguments which were passed to the executable associated with the parent process.
ParentUser	sourceUser	WIN10-SECURITY\\Administrator	Name of the account that created the parent process. It usually contains domain name and username
TargetFilename	filePath	C:\\Users\\Adam Joe\\AppData\\Roaming\\Microsoft\\Teams\\Session Storage\\LOG	Full path name of the file
CreationUtcTime	fileModificationTime/fileCreateTime	2022-03-22 22:01:17.969	New creation time of the file
PreviousCreationUtcTime	fileCreateTime	2022-03-22 22:01:17.969	Previous creation time of the file

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Protocol	protocol	tcp	Protocol being used for the network connection
SourceIp	sourceIpv4/sourceIpv6	10.20.12.15	Source IP address that made the network connection
SourceHostname	sourceHost	DESKTOP-HRS9VRH.hsd1.ca.comcast.net	DNS name of the host that made the network connection
SourcePort	sourcePort	49714	Source port number
DestinationIp	destinationIpv4/destinationIpv6	23.1.25.244	IP address destination
DestinationHostname	destinationHost	www.xyz.com	DNS name of the host that is contacted
DestinationPort	destinationPort	443	Destination port number
State	action	Stopped	Sysmon service state
ImageLoaded	customString8	C:\Windows\System32\ole32.dll	File path of the driver loaded
Signed	customString9	true	Is the driver loaded signed
SourceImage	sourceProcess	<unknown process>	File path of the source process that created a thread in another process
TargetImage	destinationProcess	C:\\Windows\\system32\\svchost.exe	File path of the target process
StartAddress	customString10	0x00007FFA15F3B9F0	New thread start address
StartModule	customString11	C:\\Windows\\System32\\KERNELBASE.dll	Start module determined from thread start address mapping to PEB loaded module list

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
StartFunction	customString12	CtrlRoutine	Start function is reported if exact match to function in image export tables
SourceUser	sourceUser	NT AUTHORITY\\SYSTEM	Name of the account for which process that started the remote thread
TargetUser	destinationUser	NT AUTHORITY\\SYSTEM	Name of the account for which process the thread was started in
Device	customString13	\Device\HarddiskVolume2	Target device
GrantedAccess	permission	0x1fffff	The access flags (bitmask) associated with the process rights requested for the target process

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
CallTrace	customString14	C:\\Windows\\SYSTEM32\\ntdll.dll+9e664|C:\\Windows\\System32\\KERNELBASE.dll+8e73|C:\\Windows\\System32\\KERNELBASE.dll+767e|C:\\Windows\\System32\\KERNELBASE.dll+7226|C:\\Windows\\System32\\KERNEL32.DLL+1c7b4|C:\\Users\\Adam Joe\\Downloads\\SysmonSimulator-Latest.exe\\SysmonSimulator.exe+1946|C:\\Users\\Adam Joe\\Downloads\\SysmonSimulator-Latest.exe\\SysmonSimulator.exe+3007|C:\\Users\\Adam Joe\\Downloads\\SysmonSimulator-Latest.exe\\SysmonSimulator.exe+36a0|C:\\Windows\\System32\\KERNEL32.DLL+17034|C:\\Windows\\SYSTEM32\\ntdll.dll+52651	Stack trace of where open process is called. Included is the DLL and the relative virtual address of the functions in the call stack right before the open process call
TargetObject	object	HKU\\S-1-5-21-698767444-2437629069-3382640457-1000\\SOFTWARE\\Microsoft\\Windows NT\\CurrentVersion\\AppCompatFlags\\Compatibility Assistant\\Store\\C:\\Program Files (x86)\\Microsoft\\Edge\\Application\\msedge.exe	Complete path of the registry key
EventType	eventSubType	SetValue	CreateKey or DeleteKey

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
NewName	customString15	\REGISTRY\MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce\BadWolf	New name of the registry key
Configuration	filePath	C:\\Users\\Adam Joe\\Downloads\\SysmonSimulator-Latest.exe\\sysmonconfig-export.xml	File path of the Sysmon config file being updated
ConfigurationFileHash	sha1Hash/sha256Hash/md5Hash	A2A6F2E3011A0747247719BA958FBC4C10EDD9526130CF660F28C95C1C9F3D9A	Hash (SHA1) of the Sysmon config file being updated
PipeName	customString16	\\sysmontestnamedpipe	Name of the pipe created
Operation	action	Created	WMI Event filter operation
EventNamespace	customString17	\"root\\\\cimv2\"	Event Namespace of the WMI class
Name	customString18	\"ServiceFilter\	Name of the created filte
Query	customString19	\"select * from __instanceModificationEvent within 5 where targetInstance isa 'win32_Service'\"	WMI query tied to the filter
Type	customString20	Log File	Type of event consumer
Destination	destinationProcess	\"C:\\\\Log.log\"	Process executed by the consumer

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Consumer	customString21	CommandLineEventConsumer.Name=\"BotConsumer23\"	Consumer to bind
Filter	customString22	__EventFilter.Name=\"BotFilter82\"	Filter to bind to the Consumer
QueryName	customString23	wpad	DNS name that was queried
QueryStatus	status	9003	Query result status code
QueryResults	message		Results of the query
IsExecutable	customString24	true	Boolean statement whether the file is
Archived	customString25	true	Boolean statement whether the file was stored in the configured archive folder
Session	sessionId	2	Terminal Session ID

ClientInfo	user=sourceUser
	hostname=sourceHost
		user: WIN2019\admin
		hostname: EndPoint342
			Username and hostname of the originating RDP host, if capturable

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
deviceType	Application
deviceVendor	Microsoft
deviceModel	Sysmon
DeviceHost	w19-ex-111.Win2019.local
customerId	d656b196-edb7-45e6-8485-3748a740d002
CollectorId	ae102769-bd05-415d-af3c-2cc59681cbab
EventSourceId	69608d8a-4088-4c6d-be0c-f3d5108f25d6
EventId	d656b196-edb7-45e6-8485-3748a740d002
CollectorReceivedTime	9/14/2021 11:29

Field Value Mappings

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