Qualys Context XDR (Extended Detection and Response)

Linux UnixOperatingSystem

Data Mapping Guide

April 22, 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 Linux UnixOperatingSystem fields and the Qualys data model.

Note: For a complete list of sources that Qualys XDR supports, on the Qu
navigate to **Configuration** > **Data Collection** > **Catalog**. If the source you
not in the catalog, you can add a request for support using the **Not in the**
on the requests coming in, Qualys will prioritize and attempt to add supp
earliest.

Device Details

- **Device Type** – UnixOperatingSystem
- **Device Vendor** – Linux
- **Device Product** – Linux UnixOperatingSystem
- **Supported Versions** – CentOS 7.9.2009

Supported Formats

In Qualys Context XDR, you can configure to receive data from Linux UnixOperatingSystem 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 Qualys Context XDR.

deviceType – UnixOperatingSystem
deviceVendor – Linux

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
EventTime	eventTime	2021-02-26T05:49:45+00:00	Time of the event
DeviceName	deviceName	elsalt01.cisco.com	hostname of the device where event is produced/logged
Process Name	processName	sshd	process name on the source machine
Process ID	processId	22645	processid if present in the event log
EventName	eventName	session closed	brief standard meaning of the message easy to read for Analyst
Source IP	sourceIpv4	172.20.8.50	IPv4 address of the source machine (the machine who has generated this event as per the log audit)
Source Port	sourcePort	54724	Port used on the source machine (the machine who has generated this event as per the log audit)
Session Id	application	sudo:session, QWEB	name of the application used
Message	message	TTY=pts/1 ; PWD=/home/ansible_vault-prod	additional field - future use
Source User	sourceUser	root, john	Username using/logged-in the source machine (the username present in the log audit as per the log audit logged by the device)

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Command	command	COMMAND=/bin/sh -c echo BECOME-SUCCESS-wjrhkjfgyoaxpqgbeadjrglxqtjwtjkv ; /usr/bin/python /home/ansible_vault-prod/.ansible/tmp/ansible-tmp-1614318573.58-18670-216485457090170/AnsiballZ_file.py	This filed captures the 'command' used in the audit log
Destination IP	destinationIpv4	172.16.146.51	IPv4 address of the destination machine (the machine who has generated this event as per the log audit)
OutByte	outByte	13449	Traffic in Bytes sent by the user as present in the event
InByte	inByte	368371	Traffic in Bytes received by the user as present in the event
TotalBytes	totalBytes	40003044	Total Bytes value as present in the event
Duration	duration	5	time field. e.g. session duration, scan duration, attack duration
EventType	eventType	auth	Type of the event. (E.g. TRAFFIC, SYSTEM)
Action	action	try	Action taken in the event log
Outcome	outcome	Login failed	Outcome of the event
DeviceSeverity	deviceSeverity	WARN	Severity details for the event log as per the device which is producing the audit events
Received Time	receivedTime	2021-02-26T08:03:52.326Z	The time at which the log is received by SA system.
Host	destinationHost	dist3.cisco.com:443	Hostname of the destination machine (the machine towards which this event is directed as per the log audit)

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Status	status	200	HTTP status codes
Method	method	CONNECT	Method used to Request the URL.
Destination Host	destinationHost	public.apps.cisco.com:443	Hostname of the destination machine (the machine towards which this event is directed as per the log audit)
Duration	duration	31	time field. e.g. session duration, scan duration, attack duration
Category	category	TCP_TUNNEL	Category of the event log
Content Type	contentType	text/html	
username	sourceUser	-	Username using/logged-in the source machine (the username present in the log audit as per the log audit logged by the device)
Peer Status	peerStatus	HIER_DIRECT	
Object	object	pam_unix	group/policy/registry/domain change
User	UserName	root	Username present in the log apart from source and destination username
Session Id	sessionId	782	session id from the event log
acct	sourceUser	root	Records a user's account name.
addr	sourceIpv4	10.0.200.205	Records the IPv4 or IPv6 address. This field usually follows a hostname field and contains the address the host name resolves to.
cgroup	group		Records the path to the cgroup that contains the process at the time the Audit event was generated.

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
cmd	command	yum update	Records the entire command line that is executed. This is useful in case of shell interpreters where the exe field records, for example, /bin/bash as the shell interpreter and the cmd field records the rest of the command line that is executed, for example helloworld.sh --help.
comm	fileName	systemd	Records the command that is executed. This is useful in case of shell interpreters where the exe field records, for example, /bin/bash as the shell interpreter and the comm field records the name of the script that is executed, for example helloworld.sh.
exe	filePath	/usr/lib/systemd/systemd	Records the path to the executable that was used to invoke the analyzed process.
exit	sysCallExitCode	0	Records the exit code returned by a system call. This value varies by system call. You can interpret the value to its human-readable equivalent with the following command: ausearch --interpret --exit exit_code
filetype	fileType		Records the type of the file.
hostname	sourceHost	10.119.209.58/localhost	Records the host name.
id	destinationUserId	root	Records the user ID of an account that was changed.
key	policy	(null)	Records the user defined string associated with a rule that generated a particular event in the Audit log.
msg	eventType(eventtime:baseevtid)	audit(10/24/2019 13:01:07.661:67)	Records a time stamp and a unique ID of a record, or various event-specific <name>=<value> pairs provided by the kernel or user space applications.

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
obj	object		Records the SELinux context of an object. An object can be a file, a directory, a socket, or anything that is receiving the action of a subject.
perm	permissions		Records the file permission that was used to generate an event (that is, read, write, execute, or attribute change)
pid	processId	1	The pid field semantics depend on the origin of the value in this field. In fields generated from user-space, this field holds a process ID.
ppid	sourceProcess	13565	Records the Parent Process ID (PID).
proto	protocol	tcp	Records the networking protocol that was used. This field is specific to Audit events generated by iptables.
res	outcome	success	Records the result of the operation that triggered the Audit event.
ses	sessionId	unset	Records the session ID of the session from which the analyzed process was invoked.
success	sysCallSuccess	yes	Records whether a system call was successful or failed.
syscall	sysCall	272	Records the type of the system call that was sent to the kernel.
uid	sourceUserId	root	Records the real user ID of the user who started the analyzed process.
type	eventName	SERVICE_STOP	
op	action/application	destroy	
direction	direction	from-server	

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
customerId	d656b196-edb7-45e6-8485-3748a740d002
deviceType	UnixOperatingSystem
deviceModel	Unix
deviceVendor	Linux
deviceHost	compXX.pXX.cisco.com
collectorId	ae102769-bd05-415d-af3c-2cc59681cbab
eventSourceId	75a20062-417a-4ed9-81e2-25c261af8bfd
eventId	d656b196-edb7-45e6-8485-3748a740d002
collectorReceivedTime	Jun 15, 2021 11:29:04 AM

Field Value Mappings

Data source field: Severity

Source Values	Qualys Normalized Values
INFO	Informational
debug	Debug
WARN	Warning
error	Error
warning	Warning
eror	Error
info	Informational

Data source field: outcome

Source Values	Qualys Normalized Values
Login failed	Login Failed
Logout	Logout
failed	Failure
fail	Failure
success	Success

Data source field: action

Source Values	Qualys Normalized Values
terminate	Terminate
login	Login
start	Start
destroy	Destroy