Qualys Context Extended Detection and Response

Microsoft Defender for Identity

Data Mapping Guide

December 21, 2022

Qualys, Inc.
919 E Hillsdale Blvd
4th Floors
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 Defender for Identity 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** – Endpoint
- **Device Vendor** – Microsoft
- **Device Model** – Microsoft Defender for Identity
- **Supported Versions** – API version 1.0

Supported Formats

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

- **JSON**

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 – Endpoint
deviceVendor – Microsoft
Model – Microsoft Defender for Identity

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
activityGroupName	group		Name or alias of the activity group (attacker) this alert is attributed to.
azureTenantId	externalId	af96c4f2-8090-4d99-87f3-c6a583fba99d	Azure Active Directory tenant ID. Required.
category	eventType	RemoteExecution SecurityAlert	Category of the alert (for example, credentialTheft, ransomware, etc.).
closedDateTime	endTime		Time at which the alert was closed. The Timestamp type represents date and time information using ISO 8601 format and is always in UTC time. For example, midnight UTC on Jan 1, 2014 is 2014-01-01T00:00:00Z (supports update).
cloudAppStates.destinationServiceName	destinationServiceName		Cloud application/service name (for example "Salesforce", "DropBox", etc.).
cloudAppStates.destinationServiceIp	destinationServiceIp		Destination IP Address of the connection to the cloud application/service.
createdDateTime	beginningTime	2022-07-20T04:47:10.4631752Z	Time at which the alert was created by the alert provider. The Timestamp type represents date and time information using ISO 8601 format and is always in UTC time. For example, midnight UTC on Jan 1, 2014 is 2014-01-01T00:00:00Z. Required.

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
description	description	Administrator made 3 attempts to run commands remotely on WIN-TTAAPS4OJLN from WIN-2019 using 2 WMI methods,1 service.	Alert description.
eventDateTime	eventTime	2022-07-19T00:51:28.06773Z	Time at which the event(s) that served as the trigger(s) to generate the alert occurred. The Timestamp type represents date and time information using ISO 8601 format and is always in UTC time. For example, midnight UTC on Jan 1, 2014 is 2014-01-01T00:00:00Z. Required.
feedback	outcome	truePositive	Analyst feedback on the alert. Possible values are: unknown, truePositive, falsePositive, benignPositive. (supports update)
fileStates.fileHash.hashType	filehashtype	md5	File hash type. Possible values are: unknown, sha1, sha256, md5, authenticodeHash256, lsHash, ctph, peSha1, peSha256.
fileStates.fileHash.hashValue	filehashvalue	ec55d3e698d289f2afd663725127bace	Value of the file hash.
fileStates.name	fileName	mimikatz_trunk.7z	File name (without path).
fileStates.path	filePath	C:\Users\Surender\Downloads\mimikatz_trunk.7z	Full file path of the file/imageFile.
hostStates.fqdn	deviceName		Host FQDN (Fully Qualified Domain Name) (for example, machine.company.com).
hostStates.os	osDetails		Host Operating System. (For example, Windows10, MacOS, RHEL, etc.).
hostStates.privateIpAddress	privateIpAddress	192.168.1.2	Private (not routable) IPv4 or IPv6 address (see RFC 1918) at the time of the alert.

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
hostStates.publicIpAddress	publicIpAddress	216.24.35.125	Publicly routable IPv4 or IPv6 address (see RFC 1918) at time of the alert.
lastModifiedDateTime	updateTime	2022-07-20T04:47:24.9337067Z	Time at which the alert entity was last modified. The Timestamp type represents date and time information using ISO 8601 format and is always in UTC time. For example, midnight UTC on Jan 1, 2014 is 2014-01-01T00:00:00Z.
malwareStates.category	category	trojan	Provider-generated malware category (for example, trojan, ransomware, etc.).
malwareStates.family	riskType	wannacry	Provider-generated malware family (for example, 'wannacry', 'notpetya', etc.).
malwareStates.name	risk	Trojan:Win32/Powessere.H	Provider-generated malware variant name (for example, Trojan:Win32/Powessere.H).
networkConnections.applicationName	application	Facebook	Name of the application managing the network connection (for example, Facebook or SMTP).
networkConnections.destinationAddress	destinationIpv4 | destinationIpv6		Destination IP address (of the network connection).
networkConnections.destinationDomain	destinationDomain		Destination domain portion of the destination URL. (for example 'www.contoso.com').
networkConnections.destinationPort	destinationPort		Destination port (of the network connection).
networkConnections.destinationUrl	requestUrl		Network connection URL/URI string - excluding parameters. (for example 'www.contoso.com/products/default.html')

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
networkConnections.direction	direction		Network connection direction. Possible values are: unknown, inbound, outbound.
networkConnections.natDestinationAddress	natDestinationIP		Network Address Translation destination IP address.
networkConnections.natDestinationPort	natDestinationPort		Network Address Translation destination port.
networkConnections.natSourceAddress	natSourceIP		Network Address Translation source IP address.
networkConnections.natSourcePort	natSourceIP		Network Address Translation source port.
networkConnections.protocol	protocol		Network protocol. Possible values are: unknown, ip, icmp, igmp, ggp, ipv4, tcp, pup, udp, idp, ipv6, ipv6RoutingHeader, ipv6FragmentHeader, ipSecEncapsulatingSecurityPayload, ipSecAuthenticationHeader, icmpV6, ipv6NoNextHeader, ipv6DestinationOptions, nd, raw, ipx, spx, spxII.
networkConnections.sourceAddress	sourceIpv4 | sourceIpv6		Source (i.e. origin) IP address (of the network connection).
networkConnections.sourcePort	natSourcePort		Source (i.e. origin) IP port (of the network connection).
networkConnections.status	networkConnectionsStatus		Network connection status. Possible values are: unknown, attempted, succeeded, blocked, failed.
processes.accountName	processesAccountName	Amazon	User account identifier (user account context the process ran under) for example, AccountName, SID, and so on.
processes.commandLine	command	mimikatz.exe	The full process invocation commandline including all parameters.

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
processes.fileHash.hashType	filehashtype	md5	File hash type. Possible values are: unknown, sha1, sha256, md5, authenticodeHash256, lsHash, ctph, peSha1, peSha256.
processes.fileHash.hashValue	filehashvalue	ec55d3e698d289f2afd663725127bace	Value of the file hash.
processes.name	processName	mimikatz.exe	The name of the process' Image file.
processes.parentProcessId	parentProcessId		The Process ID (PID) of the parent process.
processes.parentProcessName	sourceProcess	cmd.exe	The name of the image file of the parent process.
processes.path	filePath	C:\Users\Surender\Downloads\mimikatz.exe	Full path, including filename.
processes.processId	processId		The Process ID (PID) of the process.
registryKeyStates.oldValueData	oldRegisteryKeyValue		Previous (i.e. before changed) registry key value data (contents).
registryKeyStates.oldValueName	oldRegisteryName		Previous (i.e. before changed) registry key value name.
registryKeyStates.operation	action		Operation that changed the registry key name and/or value. Possible values are: unknown, create, modify, delete.
registryKeyStates.processId	modifiedRegisteryProcessId		Process ID (PID) of the process that modified the registry key (process details will appear in the alert 'processes' collection).
registryKeyStates.valueData	modifiedRegisteryKeyValue		Current (i.e. changed) registry key value data (contents).
registryKeyStates.valueName	modifiedRegisteryKeyName		Current (i.e. changed) registry key value name
severity	deviceSeverity	medium	Alert severity - set by vendor/provider. Possible values are: unknown, informational, low, medium, high. Required.

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
status	status	inProgress	Alert lifecycle status (stage). Possible values are: unknown, newAlert, inProgress, resolved. (supports update). Required.
title	eventName	Remote code execution attempt	Alert title. Required.
userStates.aadUserId	guid		AAD User object identifier (GUID) - represents the physical/multi-account user entity.
userStates.accountName	accountName	Amazon	Account name of user account (without Active Directory domain or DNS domain) - (also called mailNickName).
userStates.domainName	sourceDomain	honeypot-vm	NetBIOS/Active Directory domain of user account (that is, domain\account format).
userStates.logonId	userlogonId		User sign-in ID.
userStates.logonIp	additionalIP	2.2.2.2	IP Address the sign-in request originated from.
userStates.logonLocation	userlogonLocation		Location (by IP address mapping) associated with a user sign-in event by this user.
userStates.logonType	userlogonType		Method of user sign in. Possible values are: unknown, interactive, remote Interactive, network, batch, service.
userStates.onPremisesSecurityIdentifier	sid	S-1-5-21-127386473-834194739-2516922971-500	Active Directory (on-premises) Security Identifier (SID) of the user.
userStates.userAccountType	useraccountType	administrator	User account type (group membership), per Windows definition. Possible values are: unknown, standard, power, administrator.

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
userStates.userPrincipalName	userName	Amazon@HONEYPOT-VM	User sign-in name - internet format: (user account name)@(user account DNS domain name).
vendorInformation.provider	serviceProvider		Specific provider (product/service - not vendor company); for example, WindowsDefenderATP.
vendorInformation.providerVersion	version		Version of the provider or subprovider, if it exists, that generated the alert. Required
vendorInformation.vendor	serviceProviderName		Name of the alert vendor (for example, Microsoft, Dell, FireEye). Required
vulnerabilityStates.cve	cveInfo		Common Vulnerabilities and Exposures (CVE) for the vulnerability.
vulnerabilityStates.severity	cveRating		Base Common Vulnerability Scoring System (CVSS) severity score for this vulnerability.
riskScore	riskScore		

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
deviceType	Endpoint
deviceVendor	Microsoft
deviceModel	Microsoft Defender for Identity
DeviceHost	
customerId	
CollectorId	
EventSourceId	
EventId	
CollectorReceivedTime	

Field Value Mappings

Data source field: dvcSeverity

Source Values	Qualys Normalized Values
medium	Medium
low	Low
informational	Informational
unknown	Unknown

Data source field: action

Source Values	Qualys Normalized Values
create	Create
modify	Modify
delete	Delete
high	High