Qualys Context XDR (Extended Detection and Response)

Microsoft Azure Directory Audit

Data Mapping Guide

February 13, 2023

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 Microsoft Azure Directory Audit 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.

Device Details

- **Device Type** – Cloud Infrastructure
- **Device Vendor** – Microsoft
- **Device Product** – Microsoft Azure Directory Audit
- **Supported Versions** – Limited Support. Contact your TAM for further information.

Supported Formats

In Qualys Context XDR, you can configure to receive data from Microsoft Azure Directory Audit using the following formats:

- **Cloud**

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 – Cloud Infrastructure
deviceVendor – Microsoft

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
category/metadata	eventName	RoleManagement/ AzureADSignIns	Brief standard meaning of the message easy to read for Analyst
result/errorCode	outcome	success	Outcome of the event
resultReason/failureReason	reason	Microsoft.Online.DirectoryServices.DirectoryValueNotFoundException	Reason for the audit event log to occur.
activityDisplayName	eventType	Triggered PIM alert	Type of the event.
activityDateTime /createdDateTime	eventTime	2022-03-09T20:25:40.1332226Z, 2022-03-09T20:42:10Z	Date and time (UTC) the sign-in was initiated.
loggedByService	sourceServiceName	PIM/Core Directory	Service name on the source machine(the machine who has generated this event as per the log audit)
operationType	eventSubType	ActivateAlert	SubType of the event associated with EventType field.
displayName / appDisplayName	application	Azure Credential Configuration Endpoint Service, Microsoft Azure Signup Portal	App name displayed in the Azure Portal.
servicePrincipalName	application	Microsoft Approval Management	Name of the application used
id/ userId	sourceUserId	86729171-9d9c-47e2-a3ec-1c646a77a824	User principal name of the user that initiated the sign-in.
userPrincipalName	sourceUser	qualysthreatsandbox@08bvt.onmicrosoft.com	ID of the user that initiated the sign-in.

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
ipAddress	sourceIpv4	20.190.132.106	IP address of the client used to sign in.
displayName	object	Azure AD Directory Roles	Name of the policy
type	objectCategory	Other/Policy	URL categorization of the URL in event log. (Primarily used for URL categorization)
userPrincipalName	destinationuser	null	Username using/logged-in the destination machine(the username present in the log audit as per the log audit logged by the device)
displayName/appliedConditionalAccessPolicies	customArray1	AccountEnabled	Indicates the property name of the target attribute that was changed.
oldValue	customArray2	null	Indicates the previous value (before the update) for the property.
newValue	customArray3	TRUE	Indicates the updated value for the property.
id	externalId	01e6c214-37c6-4c30-84bc-35c1f2cc9001	Unique ID representing the sign-in activity.
clientAppUsed	userAgent	Browser	Identifies the client used for the sign-in activity.
isInteractive	AzureADIsInteractive	TRUE	Indicates if a sign-in is interactive or not.

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
riskDetail	AzureADRiskDetail	none	Provides the 'reason' behind a specific state of a risky user, sign-in or a risk event. The possible values are: none, adminGeneratedTemporaryPassword, userPerformedSecuredPasswordChange, userPerformedSecuredPasswordReset, adminConfirmedSigninSafe, aiConfirmedSigninSafe, userPassedMFADrivenByRiskBasedPolicy, adminDismissedAllRiskForUser, adminConfirmedSigninCompromised, unknownFutureValue. The value none means that no action has been performed on the user or sign-in so far.
riskLevelAggregated	riskScore	none	Aggregated risk level. The possible values are: none, low, medium, high, hidden, and unknownFutureValue. The value hidden means the user or sign-in was not enabled for Azure AD Identity Protection.
riskState	AzureADriskState	none	Reports status of the risky user, sign-in, or a risk event. The possible values are: none, confirmedSafe, remediated, dismissed, atRisk, confirmedCompromised, unknownFutureValue.
riskEventTypes	AzureADriskEventType	maliciousIPAddress	Risk event types associated with the sign-in. The possible values are: unlikelyTravel, anonymizedIPAddress, maliciousIPAddress, unfamiliarFeatures, malwareInfectedIPAddress, suspiciousIPAddress, leakedCredentials, investigationsThreatIntelligence, generic, and unknownFutureValue.
resourceDisplayName	AzureADresDispName	Microsoft Graph	Name of the resource the user signed into.

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
additionalDetails	message	MFA requirement satisfied by claim in the token	Provides additional details on the sign-in activity
deviceId	deviceId		Refers to the UniqueID of the device used for signing in.
displayName	deviceName		Refers to the name of the device used for signing in.
operatingSystem	osDetails	MacOs	Indicates the operating system name and version used for signing in.
browser	userAgent	Chrome 98.0.4758	Indicates the browser information of the used for signing in.
isCompliant	AzureADisCompliant	FALSE	Indicates whether the device is compliant.
isManaged	AzureADisManaged	FALSE	Indicates whether the device is managed.
trustType	AzureADtrustType	Workplace Joined	Provides information about whether the signed-in device is Workplace Joined, AzureAD Joined, Domain Joined.
city	geoSourceCity	Hayward	Provides the city where the sign-in originated. This is calculated using latitude/longitude information from the sign-in activity.
countryOrRegion	geoSourceCountry	US	Provides the country code info (2 letter code) where the sign-in originated. This is calculated using latitude/longitude information from the sign-in activity.
geoCoordinates	geoSourceCoordinates	**	Provides the latitude, longitude and altitude where the sign-in originated.

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
DeviceType	Cloud Infrastructure
DeviceModel	Azure Active Directory
DeviceVendor	Microsoft
DeviceHost	-
CustomerId	d656b196-edb7-45e6-8485-3748a740d002
CollectorId	ae102769-bd05-415d-af3c-2cc59681cbab
EventSourceId	1ae639f0-0944-4cbc-81ef-87c040ca9eb2
EventId	d656b196-edb7-45e6-8485-3748a740d002
CollectorReceivedTime	6/1/2021 11:29