Qualys Context Extended Detection and Response

Trend Micro Deep Security Manager

Data Mapping Guide

January 14, 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 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 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 Trend Micro Deep Security Manager (DSM) fields and the Qualys data model.

Note: For the Trend Micro Deep Security Manager parser, we are ingesting logs with Linux Agent; hence source creation is happening differently. For ingesting the Trend Micro Deep Security Manager logs, you need to add a New Profile, go to the Qualys Context XDR UI, and navigate to **Configuration** > **Cloud Agent Profiles** > **Profiles**.

Device Details

- **Device Type** – Endpoint
- **Device Vendor** – Trend Micro
- **Device Product** – Trend Micro DSM
- **Supported Versions** – 20.x

Supported Formats

In Qualys Context XDR, you can configure the product to receive data from Trend Micro Deep Security Manager using the following formats:

- **JSON**

Data Field Mappings

This section provides a detailed mapping of the data source fields to the Qualys Context XDR.

deviceType – Endpoint
deviceVendor – Trend Micro

Mapping: AntiMalware

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
Device Vendor	deviceVendor	Trend Micro	Appliance vendor
Device Product	deviceModel	Deep Security Agent	Appliance product name
Device Version	version	20.0.0.5137	Appliance version
EventID	deviceEventId	4000000	Signature ID
cat	category	cat=Anti-Malware	Category. Example - Anti-Malware, AppControl, Firewall, Integrity Monitor, Intrusion Prevention, Log Inspection, Web Reputation
name	eventName	name=SPYWARE_KEYL_ACTIVE	Event name
desc	description	desc=SPYWARE_KEYL_ACTIVE	Event description. Anti-Malware uses the event name as the description.
sev	deviceSeverity	sev=6	The severity of the event. 1 is the least severe; 10 is the most severe.
cn1	deviceId	cn1=1	The agent computer's internal unique identifier.
cn2	fileSize	cn2=100	The size of the quarantine file.
cs3	object	cs3=C:\\Windows\\Temp\\2203538327.exe	The path of the spyware item. This field is only for spyware detection events.
cs4	ResourceType	cs4=10	Resource Type values:10=Files and Directories11=System Registry12=Internet Cookies13=Internet URL Shortcut14=Programs in Memory15=Program Startup

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
			Areas16=Browser Helper Object17=Layered Service Provider18=Hosts File19=Windows Policy Settings20=Browser23=Windows Shell Setting24=IE Downloaded Program Files25=Add/Remove Programs26=Servicesother=OtherFor example, if there's a spyware file named spy.exe that creates a registry run key to keep its persistence after system reboot, there will be two items in the spyware report: the item for spy.exe has cs4=10 (Files and Directories), and the item for the run key registry has cs4=11 (System Registry). This field is only for spyware detection events.
cs5	riskScore	cs5=25	Risk level values: 0=Very Low 25=Low 50=Medium 75=High 100=Very High This field is only for spyware detection events.
cs6	DockerInfo	cs6=ContainerImageName | ContainerName | ContainerID	The image name of the Docker container, container name, and container ID where the malware was detected.
filePath	filePath	filePath=C:\\Users\\Mei\\Desktop\\virus.exe	The location of the malware file.
act	action	act=Clean act=Clean	The action performed by the Anti-Malware engine. Possible values are: Deny, Access, Quarantine, Delete, Pass, Clean, Terminate, and Unspecified.

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
result	outcome	result=Deleted, result=Quarantined	The result of the failed Anti-Malware action.
msg	message	msg=Scheduled, msg=Realtime	The type of scan. Possible values are: Realtime, Scheduled, and Manual.
dvc	deviceIPAddress	dvc=10.1.144.199	The IPv4 address for cn1. Does not appear if the source is an IPv6 address or hostname. (Uses dvchost instead.)
dvchost	deviceName	dvchost=www.example.com dvchost=fe80::f018:a3c6:20f9:afa6%5	The hostname or IPv6 address for cn1. Does not appear if the source is an IPv4 address. (Uses dvc field instead.)
TrendMicroDsBehaviorType	eventType	BehaviorType=Threat-Detection	The type of behavior monitoring event detected.
TrendMicroDsTenantId	externalId	TrendMicroDsTenantId=0	Deep Security tenant ID
TrendMicroDsMalwareTarget	MalwareTarget	TrendMicroDsMalwareTarget=N/A TrendMicroDsMalwareTarget=C:\\Windows\\System32\\cmd.exe TrendMicroDsMalwareTarget=HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings TrendMicroDsMalwareTarget=Multiple	The file, process, or registry key (if any) that the malware was trying to affect. If the malware was trying to affect more than one, this field will contain the value "Multiple." Only suspicious activity monitoring and unauthorized change monitoring have values for this field.
TrendMicroDsMalwareTargetCount	count	TrendMicroDsMalwareTargetCount=3	The number of target files.

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
TrendMicroDsMalwareTargetType	MalwareTargetType	TrendMicroDsMalwareTargetType=N/A TrendMicroDsMalwareTargetType=Exploit TrendMicroDsMalwareTargetType=File System TrendMicroDsMalwareTargetType=Process TrendMicroDsMalwareTargetType=Registry	The type of system resource that this malware was trying to affect, such as the file system, a process, or Windows registry. Only suspicious activity monitoring and unauthorized change monitoring have values for this field.
TrendMicroDsProcess	sourceProcess	TrendMicroDsProcess= abc.exe	Process Name
TrendMicroDsFileMD5	md5Hash	TrendMicroDsFileMD5=1947A1BC0982C5871FA3768CD025453E	The MD5 hash of the file
TrendMicroDsFileSHA1	sha1Hash	TrendMicroDsFileSHA1=5AD084DDCD8F80FBF2EE3F0E4F812E812DEE60C1	The SHA1 hash of the file
TrendMicroDsFileSHA256	sha256Hash	TrendMicroDsFileSHA256=25F231556700749F8F0394CAABDED83C2882317669DA2C01299B45173482FA6E	The SHA256 hash of the file
TrendMicroDsRelevantDetectionNames	risk	TrendMicroDsRelevantDetectionNames=Ransom_CERBER.BZC;Ransom_CERBER.C;Ransom_CRYPNISCA.SM	Indicates the most likely type of threat contained in the file after Predictive Machine Learning compared the analysis to other known threats(separate by semicolon";")

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
TrendMicroDsCommandLine	command	TrendMicroDsCommandLine=/tmp/orca-testkit-sample/testsys_m64 -u 1000 -g 1000 -U 1000 -G 1000 -e cve_2017_16995 1 -d 4000000	The commands that the subject process executes
TrendMicroDsCve	cveId	TrendMicroDsCve=CVE-2016-5195,CVE-2016-5195,CVE-2016-5195	The CVE information, if the process behavior is identified in one of Common Vulnerabilities and Exposures.
TrendMicroDsMitre	MitreTIDs	TrendMicroDsMitre=T1068,T1068,T1068	The MITRE information, if the process behavior is identified in one of MITRE attack scenarios.
suser	sourceUser	suser=root	The user account name who triggered this event

Mapping: Application Control

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
Device Vendor	deviceVendor	Trend Micro	Appliance vendor
Device Product	deviceModel	Deep Security Agent	Appliance product name
Device Version	version	20.0.0.5137	Appliance version
EventID	deviceEventId	6001200	Signature ID
cat	category	cat=AppControl	Category. Example - Anti-Malware, AppControl, Firewall, Integrity Monitor, Intrusion Prevention, Log Inspection, Web Reputation
name	eventName	name=blocked	Event name

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
desc	description	desc=blocked	Event description. Anti-Malware uses the event name as the description.
sev	deviceSeverity	sev=6	The severity of the event. 1 is the least severe; 10 is the most severe.
cn1	deviceId	cn1=2	The agent computer's internal unique identifier.
cs1	reason	reason	The reason why application control performed the specified action, such as "notWhitelisted" (the software did not have a matching rule, and application control was configured to block unrecognized software).
cs2	sha1Hash	cs2=156F4CB711FDBD668943711F853FB6DA89581AAD	If it was calculated, the SHA-1 hash of the file.
cs3	md5Hash	cs3=4E8701AC951BC4537F8420FDAC7EFBB5	If it was calculated, the MD5 hash of the file.
act	action	act=blocked	The action performed by the Application Control engine. Possible values are: Blocked, Allowed.
dvc	deviceIPAddress	10.1.144.199	The IPv4 address for cn1. Does not appear if the source is an IPv6 address or hostname. (Uses dvchost instead.)
dvchost	deviceName	dvchost=www.example.com dvchost=fe80::f018:a3c6:20f9:afa6%5	The hostname or IPv6 address for cn1. Does not appear if the source is an IPv4 address. (Uses dvc field instead.)
suid	sourceUserId	suid=0	The account ID number of the user name.
suser	sourceUser	suser=root	The name of the user account that installed the software on the protected computer.

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
TrendMicroDsTenantId	externalId	TrendMicroDsTenantId=0	Deep Security tenant ID
fileHash	sha256Hash	fileHash=E3B0C44298FC1C149AFBF4C8996FB92427AE41E4649B934CA495991B7852B855	The SHA 256 hash that identifies the software file.
filePath	filePath	filePath=/bin/my.jar	The location of the malware file.
fsize	fileSize	fsize=16	The file size in bytes.
repeatCount	count	repeatCount=4	The number of occurrences of the event. Non-aggregated events have a value of 1. Aggregated events have a value of 2 or more.

Mapping: Firewall

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
Device Vendor	deviceVendor	Trend Micro	Appliance vendor
Device Product	deviceModel	Deep Security Agent	Appliance product name
Device Version	version	20.0.0.5137	Appliance version
EventID	deviceEventId	6001200	Signature ID
cat	category	cat=Firewall	Category. Example - Anti-Malware, AppControl, Firewall, Integrity Monitor, Intrusion Prevention, Log Inspection, Web Reputatio
name	eventName	name=blocked	Event name
desc	description	desc=blocked	Event description. Anti-Malware uses the event name as the description.
sev	deviceSeverity	sev=6	The severity of the event. 1 is the least severe; 10 is the most severe.

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
act	action	act=Log. act=Deny	The action performed by the Firewall engine.
cn1	deviceId	cn1=2	The agent computer's internal unique identifier.
cnt	count	cnt=8	The number of times this event was sequentially repeated.
dstMAC	destinationMac	dmac= 00:0C:29:2F:09 :B3	MAC address of the destination computer's network interface.
dstPort	destinationPort	dpt=135	(For TCP and UDP protocol only) Port number of the destination computer's connection or session.
dst	destinationIpv4	dst=192.168.1. 102 dst=10.30.128. 2	IP address of the destination computer.
in	inByte	in=137 in=21	(For inbound connections only) Number of inbound bytes read.
out	outByte	out=216 out=13	(For outbound connections only) Number of outbound bytes read.
proto	protocol	proto=tcp proto=udp proto=icmp	Name of the transport protocol used.
srcMAC	sourceMac	smac= 00:0E:04:2C:02 :B3	MAC address of the source computer's network interface.
srcPort	sourcePort	spt=1032 spt=443	(For TCP and UDP protocol only) Port number of the source computer's connection or session.
src	sourceIpv4	src=192.168.1. 105 src=10.10.251. 231	The packet's source IP address at this event.
TrendMicroDs FrameType	FrameType	TrendMicroDs FrameType=IP TrendMicroDs FrameType=A RP TrendMicroDs FrameType=R	Connection ethernet frame type.

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
		evARP TrendMicroDsFrameType=NetBEUI	
dvc	deviceIPAddress	10.1.144.199	The IPv4 address for cn1. Does not appear if the source is an IPv6 address or hostname. (Uses dvchost instead.)
dvchost	deviceName	dvchost=www.example.com dvchost=fe80::f018:a3c6:20f9:afa6%5	The hostname or IPv6 address for cn1. Does not appear if the source is an IPv4 address. (Uses dvc field instead.)
TrendMicroDsTenantId	externalId	TrendMicroDsTenantId=0	Deep Security tenant ID
in	inByte	in=137 in=21	(For inbound connections only) Number of inbound bytes read.
out	outByte	out=216 out=13	(For outbound connections only) Number of outbound bytes read.
proto	protocol	proto=tcp proto=udp proto=icmp	Name of the transport protocol used.

Mapping: Integrity Monitor

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
Device Vendor	deviceVendor	Trend Micro	Appliance vendor
Device Product	deviceModel	Deep Security Agent	Appliance product name
Device Version	version	20.0.0.5137	Appliance version
EventID	deviceEventId	6001200	Signature ID
cat	category	cat=Integrity Monitor	Category. Example - Anti-Malware, AppControl, Firewall, Integrity

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
			Monitor, Intrusion Prevention, Log Inspection, Web Reputation
name	eventName	name=Microsoft Windows - System file modified	Event name
desc	description	name=Microsoft Windows - System file modified	Event description. Anti-Malware uses the event name as the description.
sev	deviceSeverity	sev=6	The severity of the event. 1 is the least severe; 10 is the most severe.
act	action	act=created act=deleted	The action detected by the integrity rule. Can contain: created, updated, deleted or renamed.
cn1	deviceId	cn1=2	The agent computer's internal unique identifier.
filePath	filePath	filePath=C:\WINDOWS\system32\drivers\etc\hosts	The integrity rule target entity. May contain a file or directory path, registry key, etc.
suser	sourceUser	suser=WIN-038M7CQDHIN\Administrator	Account of the user who changed the file being monitored.
sproc	sourceProcess	sproc=C:\\Windows\\System32\\notepad.exe	The name of the event's source process.
msg	message		(For "renamed" action only) A list of changed attribute names. If "Relay via Manager" is selected, all event action types include a full description.
oldfilePath	oldFilePath	oldFilePath=C:\WINDOWS\system32\logfiles\ds_agent.log	(For "renamed" action only) The previous integrity rule target entity to capture the rename action from the previous target entity to the new, which is recorded in the filePath field.

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
dvc	deviceIPAddress	10.1.144.199	The IPv4 address for cn1. Does not appear if the source is an IPv6 address or hostname. (Uses dvchost instead.)
dvchost	deviceName	dvchost=www.example.com dvchost=fe80::f018:a3c6:20f9:afa6%5	The hostname or IPv6 address for cn1. Does not appear if the source is an IPv4 address. (Uses dvc field instead.)
TrendMicroDsTenantId	externalId	TrendMicroDsTenantId=0	Deep Security tenant ID

Mapping: Intrusion Prevention

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
Device Vendor	deviceVendor	Trend Micro	Appliance vendor
Device Product	deviceModel	Deep Security Agent	Appliance product name
Device Version	version	20.0.0.5137	Appliance version
EventID	deviceEventId	6001200	Signature ID
cat	category	cat=Integrity Monitor	Category. Example - Anti-Malware, AppControl, Firewall, Integrity Monitor, Intrusion Prevention, Log Inspection, Web Reputation
name	eventName	name=Microsoft Windows - System file modified	Event name
desc	description	name=Microsoft Windows - System file modified	Event description. Anti-Malware uses the event name as the description.
sev	deviceSeverity	sev=6	The severity of the event. 1 is the least severe; 10 is the most severe.

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
act	action	act=Block	(IPS rules written before Deep Security version 7.5 SP1 could additionally perform Insert, Replace, and Delete actions. These actions are no longer performed. If an older IPS Rule is triggered which still attempts to perform those actions, the event will indicate that the rule was applied in detect-only mode.)
cn1	deviceId	cn1=2	The agent computer's internal unique identifier.
cnt	count	cnt=8	The number of times this event was sequentially repeated.
cs1	eventType	cs1=Drop_data	(Optional) A note field which can contain a short binary or text note associated with the payload file. If the value of the note field is all printable ASCII characters, it will be logged as text with spaces converted to underscores. If it contains binary data, it will be logged using Base-64 encoding.
dstMAC	destinationMac	dmac= 00:0C:29:2F:09:B3	MAC address of the destination computer's network interface.
dstPort	destinationPort	dpt=80 dpt=135	(For TCP and UDP protocol only) Port number of the destination computer's connection or session.
dst	destinationIpv4	dst=192.168.1.10 2 dst=10.30.128.2	IP address of the destination computer.
xff	additionalIP	xff=192.168.137.1	The IP address of the last hub in the X-Forwarded-For header. This is typically originating IP address, beyond the proxy that may exist. See also the src field. To include xff in events, enable the "1006540 - Enable X-Forwarded-For HTTP Header Logging" Intrusion Prevention rule.
in	inByte	in=137 in=21	(For inbound connections only) Number of inbound bytes read.

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
out	outByte	out=216 out=13	(For outbound connections only) Number of outbound bytes read.
proto	protocol	proto=tcp proto=udp proto=icmp	Name of the transport protocol used.
srcMAC	sourceMac	smac= 00:0E:04:2C:02:B3	MAC address of the source computer's network interface.
srcPort	sourcePort	spt=1032 spt=443	(For TCP and UDP protocol only) Port number of the source computer's connection or session.
src	sourceIpv4	src=192.168.1.105 src=10.10.251.231	The packet's source IP address at this event.
TrendMicroDsFrameType	FrameType	TrendMicroDsFrameType=IP TrendMicroDsFrameType=ARP TrendMicroDsFrameType=RevARP TrendMicroDsFrameType=NetBEUI	Connection ethernet frame type.
dvc	deviceIPAddress	10.1.144.199	The IPv4 address for cn1. Does not appear if the source is an IPv6 address or hostname. (Uses dvchost instead.)
dvchost	deviceName	dvchost=www.example.com dvchost=fe80::f018:a3c6:20f9:afa6%5	The hostname or IPv6 address for cn1. Does not appear if the source is an IPv4 address. (Uses dvc field instead.)
TrendMicroDsTenantId	externalId	TrendMicroDsTenantId=0	Deep Security tenant ID

Mapping: Log Inspection

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
Device Vendor	deviceVendor	Trend Micro	Appliance vendor
Device Product	deviceModel	Deep Security Agent	Appliance product name
Device Version	version	20.0.0.5137	Appliance version
EventID	deviceEventId	6001200	Signature ID
cat	category	cat=Log Inspection	Category. Example - Anti-Malware, AppControl, Firewall, Integrity Monitor, Intrusion Prevention, Log Inspection, Web Reputation
name	eventName	name=Microsoft Windows Events	Event name
desc	description	name=Multiple Windows Logon Failures	Event description. Anti-Malware uses the event name as the description.
sev	deviceSeverity	sev=6	The severity of the event. 1 is the least severe; 10 is the most severe.
cn1	deviceId	cn1=2	The agent computer's internal unique identifier.
cs1	eventType	cs1=Multiple Windows audit failure events	The Log Inspection sub-rule which triggered this event.
duser	destinationUser	duser=(no user) duser=NETWORK SERVICE	Details of the Log Inspection event. May contain a verbose description of the detected log event.
fname	fileName	fname=Application fname=C:\Program Files\CMS\logs\server0.log	The Log Inspection rule target entity. May contain a file or directory path, registry key, etc.
msg	message	msg=WinEvtLog: Application: AUDIT_FAILURE(20187): pgEvent: (no user): no domain:	

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
		SERVER01: Remote login failure for user 'xyz'	
shost	sourceHost	shost=webserver01.corp.com	Source computer hostname.
src	sourceIpv4	src=192.168.1.105 src=10.10.251.231	Source computer IP address.
dvc	deviceIPAddress	dvc=10.1.144.199	The IPv4 address for cn1. Does not appear if the source is an IPv6 address or hostname. (Uses dvchost instead.)
dvchost	deviceName	dvchost=www.example.com dvchost=2001:db8::5	The hostname or IPv6 address for cn1. Does not appear if the source is an IPv4 address. (Uses dvc field instead.)
TrendMicroDsTenantId	externalId	TrendMicroDsTenantId=0	Deep Security tenant ID

Mapping: Web Reputation

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
Device Vendor	deviceVendor	Trend Micro	Appliance vendor
Device Product	deviceModel	Deep Security Agent	Appliance product name
Device Version	version	20.0.0.5137	Appliance version
EventID	deviceEventId	6001200	Signature ID
cat	category	cat=Web Reputation	Category. Example - Anti-Malware, AppControl, Firewall, Integrity Monitor, Intrusion Prevention, Log Inspection, Web Reputation

Data Source Fields	Qualys Context XDR QQL Labels	Sample Values	Description
name	eventName	name=Microsoft Windows Events	Event name
desc	description	name=Multiple Windows Logon Failures	Event description. Anti-Malware uses the event name as the description.
sev	deviceSeverity	sev=6	The severity of the event. 1 is the least severe; 10 is the most severe.
cn1	deviceId	cn1=2	The agent computer's internal unique identifier.
request	requestUrl	request=http://www.example.com/index.php	The URL of the request.
msg	message	msg=WinEvtLog: Application: AUDIT_FAILURE(20187): pgEvent: (no user): no domain: SERVER01: Remote login failure for user 'xyz'	
dvc	deviceIPAddress	dvc=10.1.144.199	The IPv4 address for cn1. Does not appear if the source is an IPv6 address or hostname. (Uses dvchost instead.)
dvchost	deviceName	dvchost=www.example.com dvchost=2001:db8::5	The hostname or IPv6 address for cn1. Does not appear if the source is an IPv4 address. (Uses dvc field instead.)
TrendMicroDsTenantId	externalId	TrendMicroDsTenantId=0	Deep Security tenant ID

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
deviceType	Endpoint
deviceModel	Deep Security Manager
deviceVendor	Trend Micro
deviceHost	el.xyz.com
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	Jun 01, 2021 11:29:04 AM