Qualys Context Extended Detection and Response

Palo Alto Firewall

Data Mapping Guide

February 18, 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 Palo Alto Firewall 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** – Firewall
- **Device Vendor** – Palo Alto
- **Device Product** – Palo Alto Firewall
- **Supported Versions** –
  Syslog- 7.1, 8.1.13, 9.0
  CEF- 7.1
  LEEF - 4.1

Supported Collectors

In Qualys Context XDR, you can configure to receive data from Palo Alto Firewall using the following collectors:

- **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 – Firewall
deviceVendor – Paloalto

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Receive Time	eventTime	2020/08/04 14:48:46	Time the log was received at the management plane.
Serial Number	externalId	119010205xx	Serial number of the firewall that generated the log.
Type	eventType	TRAFFIC	Specifies the type of log; value is TRAFFIC.
Threat/Content Type	eventSubType	end	"Subtype of traffic log; values are start, end, drop, and deny • Start—session started • End—session ended • Drop—session dropped before the application is identified and there is no rule that allows the session. • Deny—session dropped after the application is identified and there is a rule to block or no rule that allows the session."
Host	sourceHost	11XX-TXXX.corp.company.com	Hostname or IP address of the client machine. **NOTE: Duplication of 'sHost' key for fields (6) and (16). This field only comes in Config-type logs**.
Source Address	sourceIpv4	192.168.100.10	Original session source IP address.
Destination Address	destinationIpv4	192.168.100.10	Original session destination IP address.
NAT Source IP	natSourceIP	0.0.0.0	If Source NAT performed, the post-NAT Source IP address.
NAT Destination IP	natDestinationIP	0.0.0.0	If Destination NAT performed, the post-NAT Destination IP address.
Rule Name	policy	Allow_Internal_traffic	Name of the rule that the session matched.

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Source User	sourceUser	Johndoe	Username of the user who initiated the session. **NOTE: Duplication of 'sUsr' key for fields (12) and (25). This field only comes in Threat, Traffic and Hip Match-type logs**.
Destination User	destinationUser	Johndoe	Username of the user to which the session was destined.
Application	application	ping	Application associated with the session.
Machine name	sourceHost	114778-T470P$	Name of the user's machine. **NOTE: Duplication of 'sHost' key for fields (6) and (16). This field only comes in Hip Match-type logs**.
OS	osDetails	Windows 8, iOS	The operating system installed on the user's machine or device (or on the client system).
IPv6 Source Address	sourceIpv6	2001:db8:3333:4444:CCCC:DDDD:EEEE:FFFF	IPv6 address of the user's machine or device.
User Device Serial Number	deviceId	OD277000, EPC-23, ATLC-60A-290096	Serial number of the user's machine or device.
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	Command performed by the Admin; values are add, clone, commit, delete, edit, move, rename, set.

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Admin	sourceUser	Johndoe@corp	Username of the Administrator performing the configuration. **NOTE: Duplication of 'sUsr' key for fields (12) and (25). This field only comes in Config-type logs.**
Client	userAgentName	UNKNOWN, CHROME	Client used by the Administrator; values are Web and CLI
Result	outcome	Success, Failure	Result of the configuration action; values are Submitted, Succeeded, Failed, and Unauthorized
Configuration Path	customString10		The path of the configuration command issued; up to 512 bytes in length
Before Change Detail	oldFilePath	c:\opsdivfs03\operations_business_services\addbannerfop\addbannerfop.exe	It contains the full xpath before the configuration change.
After Change Detail	filePath	https://www(.)company(.)com/nri-services/nri-term-deposit.aspx, c:\opsdivfs03\operations_business_services \addbannerfop\addbannerfop.exe	It contains the full xpath after the configuration change.
Event ID	deviceEventId	ike-nego-p1-start	String showing the name of the event.
Object	object	pam_unix, System Statistics	Gateway_for_NY
Severity	deviceSeverity	informational	Severity associated with the event; values are informational, low, medium, high, critical.
Description	description	"IKE phase-1 negotiation is started as initiator, main mode. Initiated SA: 47.19.89.231[500]-65.203.132.18[500] cookie:1338534f1832dcb4:00000000000	Detailed description of the event, up to a maximum of 512 bytes.

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
		00000."	
Source Zone	sourceZone	CPPIB_Internal	Zone the session was sourced from.
Destination Zone	destinationZone	VPN	Zone the session was destined to.
Inbound Interface	sourceInterface	ethernet1/2	Interface that the session was sourced from.
Outbound Interface	destinationInterface	tunnel.1	Interface that the session was destined to.
Session ID	sessionId	74796	An internal numerical identifier applied to each session.
Repeat Count	count	1	Number of sessions with same Source IP, Destination IP, Application, and Subtype seen within 5 seconds.
Source Port	sourcePort	0	Source port utilized by the session.
Destination Port	destinationPort	0	Destination port utilized by the session.
NAT Source Port	natSourcePort	0	Post-NAT source port.
NAT Destination Port	natDestinationPort	0	Post-NAT destination port.
Flags	customString12	0x100019	"32-bit field that provides details on session; this field can be decoded by AND-ing the values with the logged value: 0x80000000—session has a packet capture (PCAP) 0x40000000—option is enabled to allow a client to use multiple paths to connect to a destination host 0x20000000—file is submitted to WildFire for a verdict 0x10000000—enterprise credential submission by end user detected 0x08000000— source for the flow is an allow list and not subject to recon protection 0x02000000—IPv6 session 0x01000000—SSL session is decrypted (SSL Proxy)

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
			0x00800000—session is denied via URL filtering 0x00400000—session has a NAT translation performed 0x00200000—user information for the session was captured through Captive Portal 0x00100000—application traffic is on a non-standard destination port 0x00080000 —X-Forwarded-For value from a proxy is in the source user field 0x00040000—log corresponds to a transaction within a http proxy session (Proxy Transaction) 0x00020000—Client to Server flow is subject to policy based forwarding 0x00010000—Server to Client flow is subject to policy based forwarding 0x00008000—session is a container page access (Container Page) 0x00002000—session has a temporary match on a rule for implicit application dependency handling.Available in PAN-OS 5.0.0 and above. 0x00000800—symmetric return is used to forward traffic for this session 0x00000400—decrypted traffic is being sent out clear text through a mirror port 0x00000100—payload of the outer tunnel is being inspected"
Protocol	protocol	icmp	IP protocol associated with the session.
Action	action	allow	Action taken for the session; values are alert, allow, deny, drop, drop-all-packets, reset-client, reset-server, reset-both, block-url. • alert—threat or URL detected but not blocked • allow— flood detection alert • deny—flood detection mechanism activated and deny traffic based on configuration • drop— threat detected and associated session was dropped • reset-client —threat detected

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
			and a TCP RST is sent to the client • reset-server —threat detected and a TCP RST is sent to the server • reset-both —threat detected and a TCP RST is sent to both the client and the server • block-url —URL request was blocked because it matched a URL category that was set to be blocked • block-ip—threat detected and client IP is blocked • random-drop—flood detected and packet was randomly dropped • sinkhole—DNS sinkhole activated • syncookie-sent—syncookie alert • block-continue (URL subtype only)—a HTTP request is blocked and redirected to a Continue page with a button for confirmation to proceed • continue (URL subtype only)—response to a block-continue URL continue page indicating a block-continue request was allowed to proceed • block-override (URL subtype only)—a HTTP request is blocked and redirected to an Admin override page that requires a pass code from the firewall administrator to continue • override-lockout (URL subtype only)—too many failed admin override pass code attempts from the source IP. IP is now blocked from the block-override redirect page • override (URL subtype only)—response to a block-override page where a correct pass code is provided and the request is allowed

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
			• block (Wildfire only)—file was blocked by the firewall and uploaded to Wildfire
URL/Filename	fileName/requestUrlDomain	google.com, nist.gov	"Field with variable length. A Filename has a maximum of 63 characters. A URL has a maximum of 1023 characters The actual URI when the subtype is url **NOTE:** • **File name or file type when the subtype is file** • **File name when the subtype is virus** • **File name when the subtype is wildfire-virus** • **File name when the subtype is wildfire** • **URL or File name when the subtype is vulnerability if applicable"**
Threat ID	customString13		"Palo Alto Networks identifier for the threat. It is a description string followed by a 64-bit numerical identifier in parentheses for some Subtypes: 8000 – 8099— scan detection 8500 – 8599— flood detection 9999— URL filtering log 10000 – 19999 —spyware phone home detection 20000 – 29999 —spyware download detection 30000 – 44999 —vulnerability exploit detection 52000 – 52999— filetype detection 60000 – 69999 —data filtering detection"
Category	category	phish, 0, TCP_TUNNEL, AAA, Malformed Packet, malware	For URL Subtype, it is the URL Category; For WildFire subtype, it is the verdict on the file and is either 'malicious', 'phishing', 'grayware', or 'benign'; For other subtypes, the value is 'any'.
Direction	direction	Inbound, Outbound, client-to-	"Indicates the direction of the attack, client-to-server or server-to-client:

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
		server, server-to-client	0—direction of the threat is client to server 1—direction of the threat is server to client"
Bytes	totalBytes	78	Number of total bytes (transmit and receive) for the session.
Bytes Sent	outByte	78	Number of bytes in the client-to-server direction of the session.
Bytes Received	inByte	0	Number of bytes in the server-to-client direction of the session.
Packets	packets	1	Number of total packets (transmit and receive) for the session.
Start Time	beginningTime	2020/08/04 14:48:34	Time of session start.
Elapsed Time	duration	0	Elapsed time of the session.
Category	requestURL	any	URL category associated with the session (if applicable).
Content Type	requestContext	1 (A)	"Applicable only when Subtype is URL. Content type of the HTTP response data. Maximum length 32 bytes."
File Digest	md5Hash/sha1Hash/sha256Hash	e57a32bc5f8ec856e2f3eaa368e6c5a964357f63	The file digest string shows the binary hash of the file sent to be analyzed by the WildFire service. **NOTE: Calculate the hash value and map to sha1, md5 or sha256 hash fields.**
User Agent	userAgent	Chrome/88.0.4324.182 Safari/537.36,10.231.128.238	The User Agent field specifies the web browser that the user used to access the URL, for example Internet Explorer. This information is sent in the HTTP request to the server.
File Type	fileType	Images, url, attachment	Specifies the type of file that the firewall forwarded for WildFire analysis.
X-Forwarded-For	additionalIP	10.10.X.X	The X-Forwarded-For field in the HTTP header contains the IP address of the user who requested the web page. It allows you to identify the IP address of the user, which is useful particularly if

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
			you have a proxy server on your network that replaces the user IP address with its own address in the source IP address field of the packet header.
Referer	referrerURL	https://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2020-15663, https://threatinsight.proofpoint.com/0fef6787-d8ee-d631-92d4-95270f81185c/threat/email/2a19c088833758ef1032692f550f7758d9500c7c6bacc9b9d9803be4d701c499	The Referer field in the HTTP header contains the URL of the web page that linked the user to another web page; it is the source that redirected (referred) the user to the web page that is being requested.
Sender	emailSender	XYZ@company.com	Specifies the name of the sender of an email that WildFire determined to be malicious when analyzing an email link forwarded by the firewall.
Subject	emailSubject	Dashboards deployment, Orderconfirmation for delivery	Specifies the subject of an email that WildFire determined to be malicious when analyzing an email link forwarded by the firewall.
Recipient	emailRecipient	abc@company.com	Specifies the name of the receiver of an email that WildFire determined to be malicious when analyzing an email link forwarded by the firewall.
Packets Sent	packetsOut	1	Number of client-to-server packets for the session.
Packets Received	packetsIn	0	Number of server-to-client packets for the session.
Session End Reason	reason	aged-out	"The reason a session terminated. If the termination had multiple causes, this field displays only the highest priority reason. The possible session end reason values are as follows, in order of priority (where the first is highest): threat—The firewall detected a threat

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
			associated with a reset, drop, or block (IP address) action. policy-deny—The session matched a security rule with a deny or drop action. decrypt-cert-validation—The session terminated because you configured the firewall to block SSL forward proxy decryption or SSL inbound inspection when the session uses client authentication or when the session uses a server certificate with any of the following conditions: expired, untrusted issuer, unknown status, or status verification time-out. This session end reason also displays when the server certificate produces a fatal error alert of type bad certificate, unsupported_certificate, certificate_revoked, access_denied, or no_certificate_RESERVED (SSLv3 only). decrypt-unsupport-param—The session terminated because you configured the firewall to block SSL forward proxy decryption or SSL inbound inspection when the session uses an unsupported protocol version, cipher, or SSH algorithm. This session end reason is displays when the session produces a fatal error alert of type unsupported_extension, unexpected_message, or handshake_failure. decrypt-error—The session terminated because you configured the firewall to block SSL forward proxy decryption or SSL inbound inspection when firewall resources or the hardware security module (HSM) were unavailable. This session end reason is also displayed when you configured the firewall to block SSL traffic that has SSH errors or that produced any fatal error alert other than those listed for the decrypt-cert-validation and decrypt-unsupport-param end reasons. tcp-rst-from-client—The client sent a TCP reset to the server. tcp-rst-from-server—The server sent a

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
			TCP reset to the client. resources-unavailable—The session dropped because of a system resource limitation. For example, the session could have exceeded the number of out-of-order packets allowed per flow or the global out-of-order packet queue. tcp-fin—Both hosts in the connection sent a TCP FIN message to close the session. tcp-reuse—A session is reused and the firewall closes the previous session. decoder—The decoder detects a new connection within the protocol (such as HTTP-Proxy) and ends the previous connection. aged-out—The session aged out. unknown—This value applies in the following situations: Session terminations that the preceding reasons do not cover (for example, a clear session all command). For logs generated in a PAN-OS release that does not support the session end reason field (releases older than PAN-OS 6.1), the value will be unknown after an upgrade to the current PAN-OS release or after the logs are loaded onto the firewall. In Panorama, logs received from firewalls for which the PAN-OS version does not support session end reasons will have a value of unknown. n/a—This value applies when the traffic log type is not end."
Virtual System Name	customString11		The name of the virtual system associated with the session; only valid on firewalls enabled for multiple virtual systems.
Device Name	deviceName	PRNFWVPN01	The hostname of the firewall on which the session was logged.
HTTP Method	method	GET, POST	Describes the HTTP Method used in the web request. Only the following methods are logged: Connect, Delete, Get, Head, Options, Post, Put.

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Threat Category	objectCategory	Unauthorized IP Tunnel Access, Business, Software/Hardware	Describes threat categories used to classify different types of threat signatures.
UUID for rule	customString14	a55e3cb5-e324-44a1-b807-a448727fce52	The UUID that permanently identifies the rule.
	receivedTime	Aug 4 14:48:47	
IMSI	customString8		International Mobile Subscriber Identity (IMSI) is a unique number allocated to each mobile subscriber in the GSM/UMTS/EPS system. IMSI shall consist of decimal digits (0 through 9) only and maximum number of digits allowed are 15
IMEI	CustomString9		International Mobile Equipment Identity (IMEI) is a unique 15 or 16 digit number allocated to each mobile station equipment

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
deviceType	Firewall
deviceModel	PA
deviceVendor	Paloalto
deviceHost	el.xyz
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