Qualys Context Extended Detection and Response

Cisco SourceFire IPS

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 Cisco SourceFire IPS 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** – IPS
- **Device Vendor** – Cisco Sourcefire
- **Device Product** – Sourcefire
- **Supported Versions** – 5.4.11, 6.0.0

Supported Formats

In Qualys Context XDR, you can configure the product to receive data from Cisco SourceFire IPS 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 – IPS
deviceVendor – Cisco Sourcefire

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Received Time	receivedTime	01-08-2004 14:59	The time at which the log is received by XDR system
Device Name	deviceName	cisco-ipsxx	Name or IP address of a device on your monitored network
Event Time	eventTime	May 14, 2021 12:54:05 PM	Time of the event
Secondary Device	secondaryDevice	ipss06	When device and the management console in picture
Detection Engine	detectionEngine	Primary Detection Engine (f99f39fc-490b-11e4-906f-d90d4b28607a)	
Device Id	deviceId	lb6_inline	deviceid of the device where event is produced/logged if present in event log
Generator id	generatorId	1	Generator ID; the ID of the component that generated the event.
Device Event Id	deviceEventId	31289	Event ID assigned by the device which is producing the audit events if present in the audit log
Revision Number	revisionNumber	5	The version of the signature that was used to generate the event.
Message	eventName	SERVER-WEBAPP /etc/passwd file access attempt	Message generated by an event, determined by the rule, decoder, or preprocessor that triggered it
Classification	eventType	Attempted Administrator Privilege Gain	Type of the event
User	sourceUser	Unknown	Username using/logged-in the source machine (the username present in the log audit as per the log audit logged by the device)
Application	application	Unknown, VPN, Facebook, HTTP	Name of an application
Client	userAgent	Web browser	user_agent used to request the URL
App Protocol	transportProtocol	HTTP	Protocol used to make/facilitate the request as present in the audit log

Data Source Fields	Qualys Context XDR QQL Tokens	Sample Values	Description
Interface Ingress	sourceInterface	s1p2	Interface name on the source machine (the machine that generated this event as per the log audit)
Interface Egress	destinationInterface	s1p1	Interface name on the destination machine (the machine that generated this event as per the log audit)
Security Zone Ingress	sourceZone	cisco-ipsXX-sX	Zone or group of the source machine (the machine that generated this event as per the log audit)
Security Zone Egress	destinationZone	cisco-ipsXX-sX	Zone or group of the destination machine (the machine that generated this event as per the log audit)
Context	sourcefireContext	Unknown	
Priority	eventPriority	Priority: 1 [DeviceSeverity earlier]	Priority high, low Estimated urgency of an event
Protocol	protocol	TCP	The name or number of the transport protocol used in the connection
SourceIP	sourceIpv4	192.168.100.10	IPv4 address of the source machine (the machine who has generated this event as per the log audit)
SourcePort	sourcePort	80	Port used on the source machine (the machine that generated this event as per the log audit)
Destination IP	destinationIpv4	64.39.96.133	IPv4 address of the destination machine (the machine that generated this event as per the log audit)
Destination Port	destinationPort	59358	Port used on the destination machine (the machine that generated this event as per the log audit)
Source Coordinates	geoSourceCoordinates	37.3526,-121.9541	Geo coordinates of the source IP for the audit log. can be part of enrichment
Destination Coordinates	geoDestinationCoordinates	34.164,-118.2387	Geo coordinates of the destination IP for the audit log. can be part of enrichment
Source Country	geoSourceCountry	India	Country name of the source IP for the audit log. can be part of enrichment
Destination Country	geoDestinationCountry	United states	Country name of the destination IP for the audit log. can be part of enrichment
Source City	geoSourceCity	Mumbai	City name of the source IP for the audit log. can be part of enrichment
Destination City	geoDestinationCity	New York	City name of the destination IP for the audit log. can be part of enrichment
Event Context	eventContext	remote-to-local, local-to-remote, local-to-local	Event Context, remote-to-local, local-to-local, local-to-remote

Qualys Internal Fields

Qualys Context XDR QQL Tokens	Sample Values
deviceType	IPS
deviceModel	Sourcefire
deviceVendor	Cisco Sourcefire
deviceHost	elsaltxx.xyz.com
customerId	d656b196-edb7-45e6-8485-3748a740d002
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