



Qualys App for Splunk Enterprise with TA

User Guide
Version 1.11.4

March 28, 2024

Copyright 2021-2024 by Qualys, Inc. All Rights Reserved.

Qualys and the Qualys logo are registered trademarks of Qualys, Inc. All other trademarks are the property of their respective owners.

Qualys, Inc.
919 E Hillsdale Blvd
4th Floor
Foster City, CA 94404
1 (650) 801 6100



Table of Contents

About this guide.....	5
About Qualys	5
Qualys Support	5
Want to contact support	5
Get Started	6
Pre-requisites	6
Download and Install the App	6
Configure the App	8
VM Detection Data	10
Policy Compliance Data	13
WAS (Web Application Scanning) Findings Settings	14
Container Security Data Settings for Images	15
Container Security Data Settings for Containers	15
FIM data settings for events, ignored events and incidents	16
Endpoint Detection and Response Settings	17
Activity Log Settings	18
KnowledgeBase Settings	19
Secure Enterprise Mobility Settings	23
Policy Compliance Reporting Service Settings	24
Cyber Security Asset Management Settings	26
Certview Settings	28
Proxy Configuration	29
Preserve API Output	29
Kill Existing PID	30
Configure Data Sync	30
Enable the Data Feed to Start in Splunk	33
How to setup for a Search Head Cluster	33
How to index KB data into Splunk	34
How to get the RESULTS field indexed in host detection input	35
How to populate the Diagnosis, Consequence and Solution information in Splunk	35
View your Qualys Data in Splunk.....	36
Search Your Qualys Data	44
Search Container Security Data	45
Search FIM Data for Events and Incidents	49
Search EDR Data	51
Search Activity Log Data	52
Search Secure Enterprise Mobility Data	53
Search Policy Compliance Reporting Service Data	53
Search Cyber Security Asset Management Data	55

Search CertView Data	56
Event Types for Searching Your Apps Data.....	58
Event Types for VM Detection Data	58
Event Types for WAS Findings Data	58
Event Types for Policy Compliance Data	58
Event Types for Container Security Data for Images	58
Event Types for Container Security Data for Containers	59
Event Types for FIM Data for Events, Ignored Events, and Incidents	59
Event Types for Endpoint Detection and Response Data	59
Event Types for Activity Log Data	59
Event Types for Secure Enterprise Mobility	60
Event Types for Policy Compliance Reporting Service	60
Event Types for Cyber Security Asset Management	60
Event Types for CertView	60
App Management & Troubleshooting.....	61
APP Management	61
Troubleshooting	63
URL to the Qualys API Server	65
What's New	67

About this guide

Welcome to Qualys App for Splunk Enterprise with TA! This user guide describes how to install and use the Qualys Technology Add-on (TA) to see your Qualys data in Splunk.

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 www.qualys.com/support/

Want to contact support

Go to the support portal www.qualys.com/support/ and open a ticket with the following information:

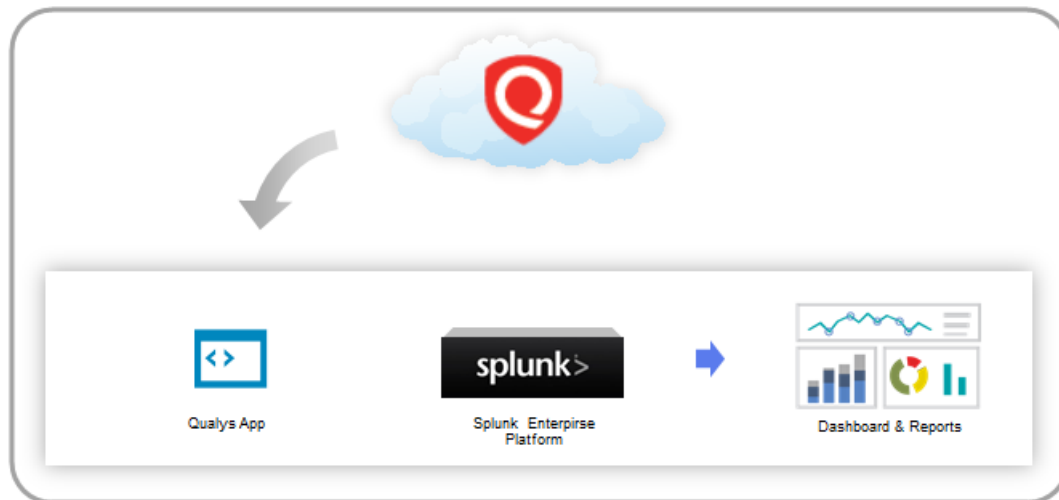
- Qualys TA version
- Visualization App version related to the issue, if any
- Complete TA and Splunk log for the time duration you had the issue

Get Started

Qualys App for Splunk Enterprise pulls (via the TA-QualysCloudPlatform) vulnerability and compliance detection data from your Qualys account and puts it in Splunk for easier searching and reporting.

The app uses Splunk's App Development framework and leverages existing Qualys APIs.

Qualys App for Splunk Enterprise solution



Pre-requisites

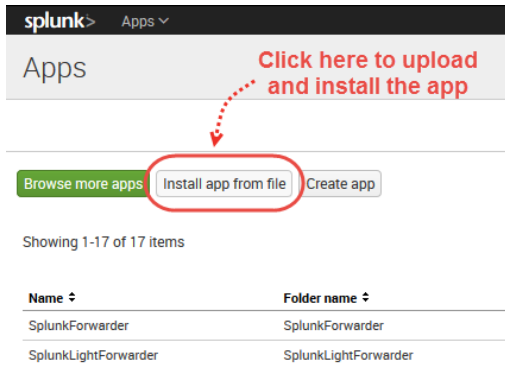
- A valid Qualys account with API access
- A Splunk Enterprise/Cloud account
- Computer with Linux

Download and Install the App

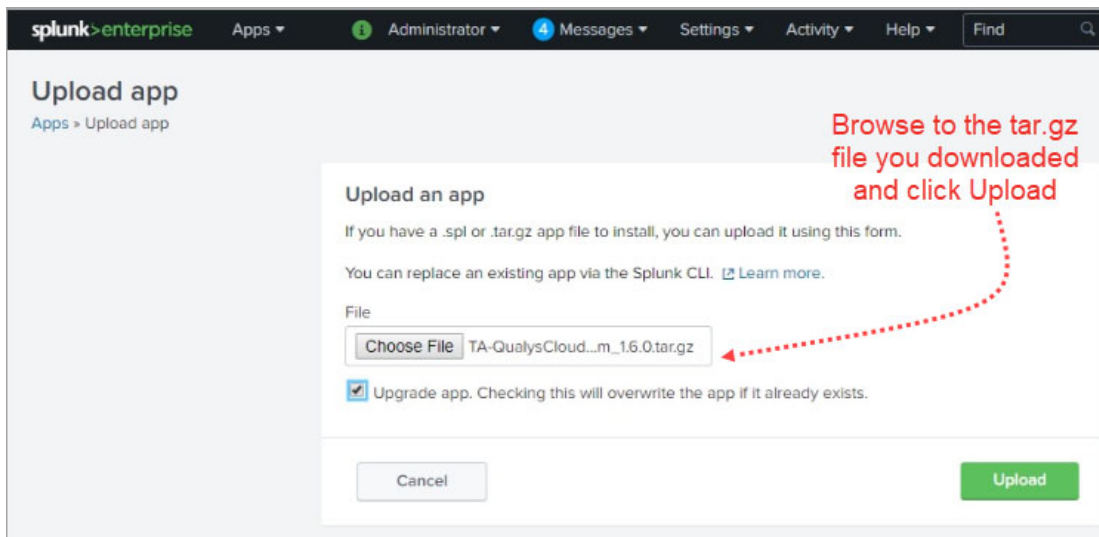
Download the latest version of Qualys Technology Add-on (TA) for Splunk by going to:

<https://splunkbase.splunk.com/app/2964/>

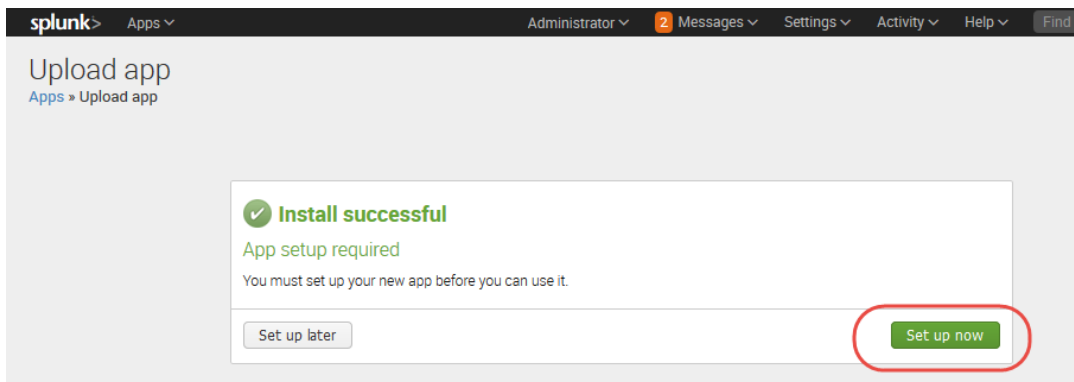
Upload the downloaded tar.gz file using the “Install app from file” option.



Browse to the file and click Upload.



You'll be prompted to restart Splunk. When you log back in, click the “Set up now” button.



Prefer to do this later? No problem. At any time go to the Apps list, find Qualys Technology Add-on for Splunk and click the “Set up” link under Actions.

Configure the App

Provide details for connecting to the Qualys API Server. Then configure settings for collecting VM, WAS, PC, FIM, EDR, CS detection data, Activity log, and KB Data. To access this page, go to Apps > Manage Apps > Qualys Technology Add-on for Splunk > Set up.

Note

If you are installing TA for the first time or upgrading your TA that has no configuration, then you must restart your Splunk once configurations in TA are saved successfully. You are required to restart Splunk only when you configure TA the first time. Restarting Splunk enables TA to reload the configurations from the app.conf file, which are modified after TA configuration.

If you are upgrading to TA 1.8.9, you have to again manually enter Qualys API credentials after the upgrade otherwise you won't be able to access the Qualys API server. Before entering the credentials, we recommend you to empty the cache of your browser and do a hard reload.

Configure This App

Qualys API Server

Note: The url should start with HTTPS.

Qualys Credentials

Username

Password

Confirm Password

Note: Leave username/password blank, if you have already set it up.

Client Certificate

API Timeout Settings

VM Detection Settings

WAS Findings Settings

Policy Compliance Settings

Container Security Settings for Images

Container Security Settings for Containers

FIM Settings for Events

FIM Settings for Ignored Events

FIM Settings for Incidents

Endpoint Detection and Response Settings

Activity Log Settings

Knowledge Base Settings

Secure Enterprise Mobility Settings

Policy Compliance Reporting Service Settings

Cyber Security Asset Management Settings

Certview Settings

Proxy Configuration

More Settings

Save

Cancel

Which URL do I enter for the Qualys API Server?

You'll enter the Qualys API Server URL for the Qualys Cloud Platform where your account is located. [Click here](#) if you need help finding the URL.

Which account credentials do I provide?

The username and password for the Qualys account you want to sync with Splunk. Note – If you return to TA Setup page at a later time, your saved credentials won't be visible. Do not enter credentials again as this will add another credential pair to the passwords.conf file and may cause issues when trying to pull data.

Note - If your TA version is 1.8.7 or higher, you do not have to remove the passwords.conf file to update TA credentials. Just update the credentials from the TA setup page without removing the passwords.conf file.

Can I authenticate using a client certificate?

Yes. Select “Use a Client certificate for authentication” and provide your PEM-encoded X.509 certificate (.pem file). You’ll also need to provide the certificate key (.key file) if it’s separate from the certificate, and enter a passphrase if the certificate/key file is encrypted.

Can I configure multiple Qualys instances via one Qualys TA App?

You can not create multiple Qualys instances using one Qualys TA app instance running on a Splunk instance. A single TA app instance does not support configuring multiple Qualys user accounts. The solution is to create multiple TA instance across multiple forwarders and configure one user account on each TA instance.

VM Detection Data

Configure settings for collecting VM detection data. Select one or more logging options to indicate the type of data you want to view in Splunk.

Enter API input parameters (in the Extra parameters field) for the Host Detection API to pull select vulnerability data from your Qualys account.

For example, only pull data for certain hosts by specifying ips=10.10.10.2-10.10.10.10.
[Refer to API user guides](#)

VM Detection Settings

☒ Log Host Summary events
 ☒ Log extra statistics in host summary (Breakdown of Vulnerability Count by (Severity and Type), by (Severity and Status)
 ☒ Log Individual Host Vulnerabilities
 ☒ Log host information with each detection (e.g. IP, OS, DNS, NetBios)

Host fields to log

ID,ASSET_ID,HOSTNAME,IP,IPV6,TRACKING_METHOD,DNS,NETBIOS,OS,LAST_SCAN_DATETIME,TAGS,N

Enter host XML tag names from API response to be logged in the event by a comma-separated. (e.g. ID,IP,TRACKING_METHOD,DNS)

Detection fields to log

QID,TYPE,PORT,PROTOCOL,SSL,STATUS,LAST_UPDATE_DATETIME,LAST_FOUND_DATETIME,FIRST_FOI

Enter detection XML tag names from API response to be logged in the event by a comma-separated. (e.g. QID,TYPE,PORT,PROTOCOL)

Max characters allowed in RESULTS field

0

Value 0 means TA won't truncate the RESULTS field. Non zero value means TA will truncate the RESULTS field at that length.

Extra parameters for Detection API

Enter as URL Query (e.g. a=1&b=string) or as JSON (e.g. {"a":1, "b": "string"}). Following parameters are NOT allowed:action, output_format, vm_processed_after, ids, suppress_duplicated_data_from_csv, max_days_since_last_vm_scan, max_days_since_vm_scan

☐ Load detection data using multiple threads (resource intensive)

Number of threads to use (between 1 and 10)

2

☐ TRURISK_SCORE, ACS, TRURISK_FACTORS for Host Asset API

Host List Detection Maximum API retry Count

0

Note: Host List Detection API will retry on failure till the configured number of times. Enter 0 for infinite retry and this feature applicable only in case of multithreading.

VM Detection - Advanced Settings

Host Ids

Enter comma-separated Host Ids to preserve VM Detection API response. (e.g. 12345,23445)

Note: In order to preserve the XML for the provided Host Ids, "Enable to preserve the XML/JSON files of API output" under "More Settings" should be disabled.

☐ Enable to preserve Host Asset API response.
 ☐ Enable full data pull always? If checked, TA will always do a full data pull. Leave unchecked for incremental pull.
 ☐ Enable .seed file generation? If checked, TA will only generate a .seed file instead of streaming data. You will have to explicitly import it later. Leave unchecked to let TA stream data into Splunk.

Directory path, where to generate the .seed file.

Why choose “Log host information with each detection”?

Choose this option if you want to log host information (IP, OS, DNS, NetBios) along with each detection.

Tell me about the “Host fields to log” and “Detection fields to log” fields

1) In the “Host fields to log” field, we show the default output fields that you will see for host assets on Splunk for VM events. You can add additional comma-separated host XML tag names such as “Asset_ID” returned in the Host List API response that you want to log in the event or remove any existing tag that you don't want to log.

11

2) In the “Detection fields to log” field, we show the default output fields that you will see for host detection on Splunk for VM events. You can add additional comma-separated detection XML tag names such as “AFFECT_EXPLOITABLE_CONFIG” and “AFFECT_RUNNING_KERNEL” returned in the Host List Detection response that you want to log in the event or remove any existing tag that you don't want to log.

Tell me about the “Max characters allowed in RESULTS” field

The “Max characters allowed in the RESULTS” field lets you specify how many maximum characters will appear in the Results field. This means if the number of characters exceeds the maximum allowed characters, then TA will truncate the excess characters after parsing the RESULTS field and append the message “[TRUNCATED XXX Characters]” in the Results field. The max length includes the characters in the appended message. The default value is zero which means TA won't truncate any characters while parsing and you will see the entire value in the RESULTS field in Splunk.

What values are shown in the “RESULT_TRUNCATED” field?

The “RESULT_TRUNCATED” field shows values based on whether the RESULT field is truncated by TA or Splunk.

- 1) The “RESULT_TRUNCATED” field is set to “0” if neither TA nor Splunk truncates the value in the Results field.
- 2) The “RESULT_TRUNCATED” field is set to “1” when Splunk truncates the RESULTS field. This happens if the truncation value set for the RESULTS field in the props.conf file in Splunk is greater than that set on the TA set up page. In this case, the difference between the truncation values set in the TA and Splunk is truncated by Splunk after TA truncates the RESULTS field as per the value specified in the “Max characters allowed in RESULTS” field.
- 3) The “RESULT_TRUNCATED” field is set to “2” if TA, after parsing the event, truncates the RESULTS field value and if the truncation value set for the RESULTS field in the props.conf file in Splunk is either the same or less than that set for the RESULTS field for VM on the TA set up page.

Note that if Splunk truncates the RESULTS field, then the message “[TRUNCATED XXX Characters]” in the Results field is not shown.

Tell me about TRURISK_SCORE, ACS, TRURISK_FACTORS for Host Asset API

We are now parsing TRURISK_SCORE, ACS, TRURISK_FACTORS and adding it into VM detection events. To get the TRURISK_SCORE, ACS, TRURISK_FACTORS, check the TRURISK_SCORE, ACS, TRURISK_FACTORS for Host Asset API checkbox provided under VM Detection Settings in TA setup page.

Tell me about Host List Detection Maximum API Retry Count

Host List Detection Maximum API retry count specified the number of times TA can retry the API call after any error occurs, except 429 Too Many Requests errors.

TA skips the API call after the maximum retry count exceeds and proceeds to pick the next Host IDs or Host ID range to pull the data.

Note: This feature is Applicable in the case of Multi threading only.

What are VM Detection-Advanced Settings?

To preserve the VM Detection API XMLs response exclusively for certain host IDs, you need to input those IDs into the **Host IDs** field in **TA-QualysCloudPlatform/tmp**. This field is used to save the response in TA-QualysCloudPlatform/tmp if it falls within the specified range. The system will save the response regardless of whether it exists or not.

The Host Asset API response XML can be preserve in **TA-QualysCloudPlatform/tmp** directory using **Enable to preserve Host Asset API response**.

Note: To preserve the XML for the Host Ids provided in the **Host IDs** field, you must disable the **Enable to preserve the XML/JSON files of API output** under **More Settings**. If **Enable to preserve the XML/JSON files of API output** under **More Settings** is enabled and you have provided the host Ids in **Host IDs** field, then all XMLs will be preserved along with the provided Host Ids.

How to configure directory path for the .seed file on Splunk Cloud?

Directory path for the .seed file on Splunk Cloud must start with \$SPLUNK_HOME/etc/apps/TA-QualysCloudPlatform/tmp. TA-QualysCloudPlatform shows an error while generating the .seed file if you configure any other path.

What are the event types for searching VM Detection data in Splunk?

Note that we provide default event types that you can use to search for VM detection data pulled in Splunk. See [Event Types for Searching Your Apps Data](#).

Policy Compliance Data

Choose one or more options to specify what posture data you want to fetch and index in Splunk for your policy. 1) Select “Log individual PC Compliance Posture events” to fetch posture info for all the host assets. 2) Select “Log Policy Summary”, to fetch policy summary information. These two options are selected by default. 3) Select “Log "All" details” to fetch full posture data. If the check box is not selected, we will show only basic details for your policy. 4) Select the “Add additional fields (REMEDIATION, RATIONALE, EVIDENCE, CAUSE_OF_FAILURE)” check box, to fetch and index full posture data and also data for these additional fields.

We use “policy_id” parameter to pull posture information. TA will first fetch all the policy IDs using the Compliance Policy List API and then for each policy_id, it fetches the posture information using the Compliance Posture Information API.

The “Number of posture info records per API request” option lets you specify the number of posture info records that will be returned per request for a single policy. The value in this field will be used for the “truncation_limit” parameter of the PC posture API request. If the requested list identifies more records than the truncation limit, then the XML output includes the <WARNING> element and the URL for making another request for the next batch of records.

The default value is 1000. If you specify 0, then TA will fetch all the posture information for a policy ID in a single output. We recommend paginated output if the posture info data is large.

Enter API input parameters (in the Extra parameters field) for the Posture Information API. For example, specify IDs of the hosts for which you want to collect the compliance posture information. [Refer to API user guides.](#)

Policy Compliance Settings
▼

***Note:** The PC feed does not pull the SCAP information.*

☒
Log individual PC Compliance Posture events

☒
Log Policy Summary

☐
Log "All" details (when unchecked, logs "Basic" details)

☐
Add additional fields (REMEDIATION, RATIONALE, EVIDENCE, CAUSE_OF_FAILURE)

☐
Enable multi-threading for PC Posture Information download

Number of threads to use for PC Posture Information (max 10)

2

Number of posture info records per API request

200

Extra parameters for Posture Information API

Note Enter as URL Query (e.g. a=1&b=string) or as JSON (e.g. [{"a":1, "b": "string"}]). Following parameters are NOT allowed: action, output_format, details, status_changes_since, policy_ids, show_remediation_info, cause_of_failure, include_dp_name, policy_id, truncation_limit

Note that we provide default event types that you can use to search for policy compliance data pulled in Splunk. See [Event Types for Searching Your Apps Data](#).

WAS (Web Application Scanning) Findings Settings

Configure WAS Finding settings to collect WAS data from your Qualys WAS account. You can choose to log individual findings and/or web application summary events.

Enter API input parameters (in the Extra parameters field) for the WAS Findings API to pull select data from your Qualys account. For example, specify Ids of web applications for which you want to view data. [Refer to API user guides](#)

WAS Findings Settings
▼

☒
Log Individual Findings

☒
Log Web App Summary events

Extra parameters to WAS Findings API

Enter as XML. (e.g. <filters><Criteria field="group" operator="IN">XSS, SQL, INFO</Criteria></filters>)

☐
Load WAS Findings data using multiple threads (resource intensive)

Number of threads to use (between 1 and 10)


2

Note that we provide default event types that you can use to search for WAS Findings data pulled in Splunk. See [Event Types for Searching Your Apps Data](#).

Container Security Data Settings for Images

Configure these settings to collect Container Security data for individual docker image vulnerabilities and summary of events for docker images.

Enter API input parameters (in the Extra parameters field) for the Docker Image Vulnerability API. This lets you pull only select vulnerability data for docker images from your Qualys account. For example, specify Ids of docker images for which you want to view vulnerability data. Go to the Container Security online help for API information.

Container Security Settings for Images 

☒ Log individual docker image vulnerability events

☒ Log docker image summary events

☐ Enable multi-threading to download docker image vulnerabilities

Number of threads to use for CS feed (max 10)

Page size

Extra filters for Docker Image API

Enter as Elastic Search Query (e.g. a:1 or b.c:string OR a:1 and b.c:string). Following parameters are NOT allowed: pageNumber, pageSize, updated

Note that we provide default event types that you can use to search for CS data for images data pulled in Splunk. See [Event Types for Searching Your Apps Data](#).

Container Security Data Settings for Containers

Configure these settings for collecting CS data for containers. Select one or more logging options to indicate whether you want to log and show individual vulnerabilities on a container and/or a summary of vulnerabilities found on a container. The Summary will include the total number of vulnerabilities with a break up of potential, confirmed and patchable vulnerabilities.

Enter API input parameters (in the Extra filters for Containers field) for the Container Vulnerability API. This lets you pull specific containers and their vulnerability data from your Qualys account. For example, if you want to download data only about running

containers that has severity 5 vulnerabilities, you would specify state:RUNNING and vulnerabilities.severity:5 in the Extra filters field. Go to [Container Security Online Help](#) for API information.

Container Security Settings for Containers

☒ Log individual docker container vulnerability events

☒ Log docker container summary events

☐ Enable multi-threading to download docker container vulnerabilities

Number of threads

Multi-threading is resource-intensive. Please set a value only between 2 to 10 (both inclusive).

Page size

Extra filters for Containers

Please refer Qualys UI help for search filter. Following parameters are NOT allowed: pageNo, pageSize, updated

Note that we provide default event types that you can use to search for CS data for containers data pulled in Splunk. See [Event Types for Searching Your Apps Data](#).

FIM data settings for events, ignored events and incidents

Configure FIM Settings for Events, Ignored Events and Incidents to collect FIM data for events, ignored events and incidents from your Qualys FIM account.

Enter API input parameters (in the Extra filters for FIM Events API, Extra filters for FIM Ignored Events API, Extra filters for FIM Incidents API) to specify what data (events, ignored events and incidents) will be pulled from your Qualys account.

For example, specify “action: rename” to pull all the events that are generated for this action.

FIM Settings for Events

Page size

Extra filters for FIM Events API

Enter as Elastic Search Query (e.g. a:1 or b.c:string OR a:1 and b.c:string). Following parameters are NOT allowed: pageNumber, pageSize, dateTime

FIM Settings for Ignored Events ▼

Page size

Extra filters for FIM Ignored Events API

Enter as Elastic Search Query (e.g. a:1 or b.c:string OR a:1 and b.c:string). Following parameters are NOT allowed: pageNumber, pageSize, dateTime

FIM Settings for Incidents

Page size

Extra filters for FIM Incidents API

Enter as Elastic Search Query (e.g. a:1 or b.c:string OR a:1 and b.c:string). Following parameters are NOT allowed: pageNumber, pageSize, dateTime

Note that FIM UI uses the user's local timezone while the Splunk-FIM integration uses UTC timezone by default. If you are trying to match results from UI to Splunk integration, you will need to match Qualys UI and Splunk Integration timezones.

Note

TA versions greater than 1.6.5 only work with FIM API version 2.0.2.0 and later and not with versions earlier than 2.0.2.0.

Note that we provide default event types that you can use to search for FIM events, ignored events, and incidents pulled in Splunk. See [Event Types for Searching Your Apps Data](#).

Endpoint Detection and Response Settings

Configure Endpoint Detection and Response (EDR) API settings to fetch the EDR data from your Qualys EDR Account.

- Choose Enable multi-threading to download EDR events to pull the EDR Events data in case of multithreading.

By default, this checkbox is disabled.

- Enter **Number of threads** to pull the EDR data.

You can select the number form 2 to 10.

- Enter **Page Size** to specify the number of records to be fetched in single API call.

Default: 1000 records, Maximum: 10000

Endpoint Detection and Response Settings
▼

☐ Enable multi-threading to download EDR events

Number of threads

Multi-threading is resource-intensive. Please set a value only between 2 to 10 (both inclusive).

Page size

Extra filters for Endpoint Detection and Response API

Enter as Elastic Search Query (e.g. a:1 or b.c:string OR a:1 and b.c:string).

EDR Maximum API retry count

Note: EDR API will retry on failure till the configured number of times. Enter 0 for infinite retry and this feature applicable only in case of multithreading.

- To pass to Indication of compromise API, enter API input parameters in the **Extra filters for Endpoint Detection and Response API** field to pull EDR data (events) from your Qualys account.

TA uses default parameters “type:file AND indicator.score>0) OR (type:process AND action:running)” in the API request to call EDR API. These parameters are shown in the EDR settings. You can customize the API request by adding new parameters or modifying the existing parameters

- Enter **EDR Maximum API retry count** to define number of times TA can retry the API call after any error occurs.

Note: To preserve the JSON File for EDR Events in case of multithreading **Enable debug logs** and **Enable to preserve the XML/JSON files of API output** under **More Settings** should be enabled. If **Enable debug logs** is disabled under **More Settings** parse the response on the fly.

Note that we provide default event types that you can use to search for EDR data pulled in Splunk. See [Event Types for Searching Your Apps Data](#).

Activity Log Settings

Configure Activity Log settings to fetch activities from your Qualys account. Enter the API input parameters (in the Extra parameters to pass to Activity Log API) to specify what Activity Log data (events) will be pulled from your Qualys account.

Activity Log Settings
▼

Extra parameters for Activity Log API

Note: Enter as URL Query (e.g. a=1&b=string) or as JSON (e.g. {"a":1, "b": "string"}). Following parameters are NOT allowed: action, output_format, since_datetime, until_datetime

Note that we provide default event types that you can use to search for Activity log data pulled in Splunk. See [Event Types for Searching Your Apps Data](#).

KnowledgeBase Settings

Configure Knowledge Base settings to fetch Solution, Consequence, and Diagnosis information in the KB data and enable or disable indexing KnowledgeBase (KB) data in Splunk. The check box “Index the KnowledgeBase...”, indicates whether TA after pulling the KnowledgeBase data will index the KnowledgeBase data in Splunk or write the data into a CSV file.

Knowledge Base Settings

- ☒ Log additional fields (SOLUTION, CONSEQUENCE, DIAGNOSIS)
- ☒ Index the knowledge base. CSV lookup file will NOT be created.

Note: This feature is helpful if you are using distributed setup.

When you select the check box and click Save, TA fetches the KB data and then indexes this data into Splunk. If you are on the distributed setup environment, we recommend you to select this option so that you can get the updated KnowledgeBase data on the Search Head and generate the KB CSV file from the Search Head.

If the check box is not selected, TA does not index the KB data and creates a KB CSV file. The CSV file will have KB data from 1999-01-01 till the current date. By default, this option is disabled.

After you enable the index KB data option, the KB data will be indexed in Splunk. Next, you need to generate the KB CSV lookup on the Search Head using the Splunk's scheduled saved searches feature. To generate KB CSV look up on the Search Head, you need to create a schedule save searches on the Search Head, and then create the KB CSV lookup definition. Creating “scheduled saved searches” and “KB CSV Lookup Definition” on the Search Head” are one-time activities that you need to perform when you enable KB indexing first time.

Note that we recommend these steps if you are using distributed Splunk setup & have enabled the index KB data option on the TA setup page.

If you disable the KB indexing option later, then disable the scheduled save searches and lookup definitions created for KB indexing. If you enable the KB indexing option after disabling, then just enable the scheduled save searches and lookup definitions created for KB indexing instead of creating them again.

Create scheduled saved searches on the Search Head

- 1) Go to **Settings > Searches, Reports, and Alerts**.

2) On the **Searches, Reports, and Alerts** page, click **New Report**.

3) On the **Create Report** screen, enter a title & description for the new report. For example, you can have a title: Generate KB CSV Lookup and a description: Generate KB CSV Lookup.

4) In the **Search** field, copy and paste this SPL and replace the {INDEX_NAME} with the actual index name which you have set for KnowledgeBase data input. The SPL will read the KB data for the specified fields using the specified index that has the Qualys KnowledgeBase source type and then write this data in the KB CSV output file.

```
index= {INDEX_NAME} sourcetype="qualys:knowledgebase" | table QID, SEVERITY,
VULN_TYPE, PATCHABLE, PCI_FLAG, TITLE, CATEGORY, PUBLISHED_DATETIME,
CVSS_BASE, CVSS_TEMPORAL, CVSS_VECTOR_STRING, CVSS_V3_BASE,
CVSS_V3_TEMPORAL, CVSS_V3_VECTOR_STRING, CVE, VENDOR_REFERENCE,
THREAT_INTEL_IDS, THREAT_INTEL_VALUES, BUGTRAQ_IDS | outputlookup
qualys_kb.csv
```

From TA v1.10.5 onwards, add the following SPL:

```
index= {INDEX_NAME} sourcetype="qualys:knowledgebase" | table
QID,SEVERITY,VULN_TYPE,PATCHABLE,PCI_FLAG,TITLE,CATEGORY,PUBLISHED_DATETIM
E,LAST_SERVICE_MODIFICATION_DATETIME,AUTHENTICATION,DISCOVERY_REMOTE,SU
PPORTED_MODULES,CVSS_BASE,CVSS_TEMPORAL,CVSS_VECTOR_STRING,CVSS_V3_BAS
E,CVSS_V3_TEMPORAL,CVSS_V3_VECTOR_STRING,CVE,VENDOR_REFERENCE,THREAT_IN
TEL_IDS,THREAT_INTEL_VALUES,BUGTRAQ_IDS | outputlookup qualys_kb.csv
```

Note: If you have selected the **Log additional fields (SOLUTION, CONSEQUENCE, DIAGNOSIS)** option in the Knowledge Base settings, then you must specify these fields in the SPL provided above.

5) In the **App** field, select the **Search & Reporting (search)** option to generate the KB CSV file under the directory: SPLUNK_HOME/etc/apps/search/lookups/.

- 6) Click **Save** to create the report. When you click **Save**, you will be navigated back to the **Searches, Reports, and Alerts** page.
- 7) On the **Searches, Reports, and Alerts** page, select **Search & Reporting (search)** from the app drop-down field.
- 8) Navigate to the report title that you have created, then click **Edit** to schedule the report.
- 9) Click **Edit** and select the **Edit Schedule** option.
- 10) On the **Edit Schedule** screen, select the **Schedule Report** check box.
- 11) From the **Schedule** drop-down field, select **Run on Cron Schedule**.
- 12) In the Cron Expression input field, enter the cron format to specify the cron schedule for running the report. For example, enter `*/2 * * * *` to schedule the cron after every 2 minutes.
- 13) In the **Time Range** field, select the **All time** option to pull all the index data.
- 14) Click **Save**.

Create KB CSV Lookup Definition on the Search Head

These steps let you access the KB CSV file data using the lookup.

- 1) Go to **Settings > Lookups** and on the **Lookups** page, click **Add New** in the Lookup definitions row to create lookup for KB CSV file.

Destination app: search

Name:

Type: File-based

Lookup file: geo_attr_countries.csv

Create and manage lookup table files.

☐ Configure time-based lookup

☐ Advanced options

Cancel Save

- 2) From the Destination app field, select the **search** option to select the destination app to be used for the lookup.
- 3) In the **Name** field, enter a name as `qualys_kb_lookup`.
- 4) From the **Type** field, select the **File-based** option.
- 5) From the **Lookup** file field, select the **qualys_kb.csv** option.
- 6) Click **Save** to create the KB CSV lookup.

What happens when you disable KB indexing option after enabling it first?

The KB CSV lookup file will be generated in **SPLUNK_HOME/etc/apps/TA-QualysCloudPlatform/lookups/directory**. So, the KB CSV file which is generated previously in **SPLUNK_HOME/etc/apps/search/lookups/directory**, is also present. It is possible that the

user may not receive updated data or may see a blank dashboard. To view updated data on the dashboard, remove the KB CSV file and disable scheduled saved searches from Splunk UI. To view the updated data on dashboard, follow these steps:

1. Remove the KB CSV file.

- Go to **Settings > Lookups > Lookup table files** and find **/opt/splunk/etc/apps/search/lookups/qualys_kb.csv** path.
- Click **Delete** from **Actions**.

2. Disable the scheduled saved searches.

- Go to **Settings > Searches, Reports, and Alerts**.
- Select the **Search & Reporting** (search) App and go to the **scheduled saved search** which you have created.
- Click **Edit** and **Disable** the scheduled saved search.

What happens when you enable the “index KnowledgeBase data” option?

When you enable indexing, TA determines if the KB data is getting indexed for the first time into Splunk or KB data has been indexed before. If TA determines that the KB data is indexed the first time, then the entire KB data from 1999-01-01 is pulled. TA pulls the entire data so that the KB data which you could see before upgrading TA will be available to you in the new version. On the other hand, if KB data has been indexed before, then TA uses the KB checkpoint date of the last run to pull the KB data.

How TA determines if the KB data is getting indexed for the first time?

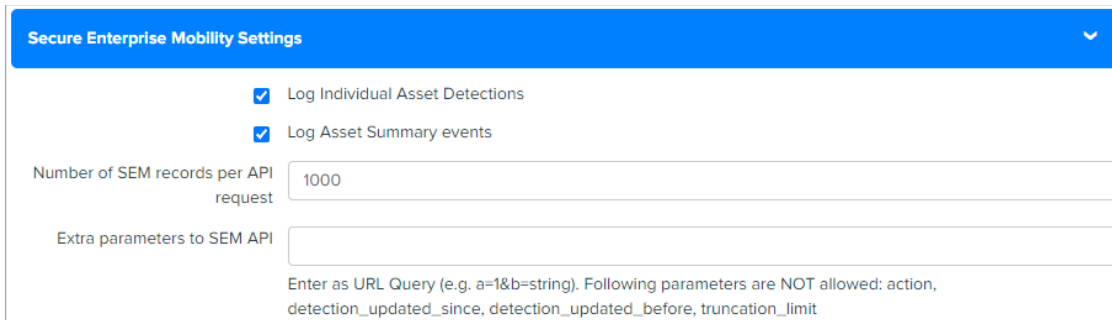
When you upgrade Splunk TA to 1.8.4 or later and choose to index the KB data into Splunk, TA will determine if the KB indexing option is enabled for the first time. TA does this by checking if the KB checkpoint file is empty and if the KB CSV file exists. Note that TA creates a KB CSV file when you upgrade Splunk TA to 1.8.4 or later. If TA finds these 2 conditions true, then TA will fetch the KB data from 1999-01-01, update the KB checkpoint file with the latest date time, and remove the KB CSV file from the lookup folder if it exists.

Later, if you delete the KB checkpoint file or clear the KB checkpoint file data, then before indexing the KB data, TA will check that the KB checkpoint file is empty and the KB CSV file doesn't exist. If these 2 conditions are found true, then TA will assume that the KB indexing option is enabled not for the first time. In this case, TA will use the start date provided on the KB input data form to pull the KB data from your Qualys account and update the KB checkpoint file with the latest date and time.

Note that if the index KB check box is not selected, TA will generate the KB CSV file but TA does not update the KB checkpoint file.

Secure Enterprise Mobility Settings

Configure Secure Enterprise Mobility (SEM) settings to fetch asset and asset detection data from your Qualys SEM account. The SEM settings section has options that enable you to 1) log the asset summary events, 2) log the individual asset detections, 3) set the number of records that will be fetched per API request (default limit is 1000), and 4) provide extra parameters, if any, for the SEM API. The default option is to log both the individual asset detections and the asset summary events. You can choose one or both options.



The screenshot shows a configuration window titled "Secure Enterprise Mobility Settings". It contains two checked checkboxes: "Log Individual Asset Detections" and "Log Asset Summary events". Below these is a text input field labeled "Number of SEM records per API request" with the value "1000". At the bottom is a text input field labeled "Extra parameters to SEM API". A note at the bottom states: "Enter as URL Query (e.g. a=1&b=string). Following parameters are NOT allowed: action, detection_updated_since, detection_updated_before, truncation_limit".

SEM data processing

We will use two dates to fetch the SEM data: the start date and current date. The start date is the date from which TA will pull the SEM data from your Qualys SEM account. TA will use the start date as the checkpoint date from the SEM checkpoint file if the file is available; else, it will use the start date from the data input page (Settings > Data Inputs > Add Data). This date is stored in the `detection_updated_since` parameter.

The second date is the current date in the YYYY-MM-DDTHH:MM:SSZ format. This date is stored in the `detection_updated_before` param.

TA will make a call to the asset list API with “`detection_updated_since`”, “`detection_updated_before`”, “`action=list`”, “`truncation_limit`” and extra params if any parameters to fetch all the SEM data available between the start date and current date in Splunk.

Note that if API response has a <WARNING> tag, TA makes a pagination call to pull the next data set.

Post-processing of SEM data

After receiving the SEM API response, we extract the asset ID from the <ASSET><ID></ID></ASSET> tag and create a new <ASSET_ID> tag for each of the <Detection> tag. The asset ID in the Detection tag helps the user identify the asset ID for a detection. We also remove the <DETECTION_LIST> tag from the <ASSET> tag and show the remaining asset information.

In the end, if more than one record is logged as an event in Splunk, then TA updates the checkpoint file with the value of `detection_updated_before` (i.e. current date of data input run). The checkpoint file is not updated if no records are found.

SEM Event types

TA logs the fetched SEM data into two event types: 1) Asset information (<ASSET></ASSET>) is logged into the “qualys_sem_asset_summary_event” event type in Splunk, and 2) Asset detection (<DETECTION></DETECTION>) is logged into the “qualys_sem_detection_event” event type.

Policy Compliance Reporting Service Settings

Configure the Policy Compliance Reporting Service (PCRS) settings to fetch the policy and the posture data from your subscribed Qualys PCRS account.

Policy Compliance Reporting Service Settings

☐ Add additional field evidence

☐ Do you want to truncate the evidence?

Number of threads for PCRS resolve host ids api (max 10)

Number of threads for PCRS posture streaming api(max 10)

PCRS Maximum API retry count

Note: PCRS API will retry on failure till the configured number of times. Enter 0 for infinite retry.

Number of Policy Ids to use for Resolve Host Ids API (max 10)

Host Ids Batch size for Posture Info Streaming API

PCRS Custom Policy Ids

Note: Enter comma seperated policy ids (e.g. 1234,4566). Leave blank to use Policy Ids from the Policy List API Response

PCRS custom policy operation (include/exclude) ☐ Include ☐ Exclude ☒ None

Note: Click "include" to use only the entered policy ids or click "exclude" to exclude the entered policy ids. Click "None" to use Policy Ids from the Policy List API Response.

The PCRS settings allows you to configure the following options.

Setting	Description
Add additional field evidence	Pull the evidence data for the posture information records. By default, this field is disabled.
Do you want to truncate the evidence?	<p>Truncate the evidence data. After you select the checkbox, only 100 lines are retained in the evidence data.</p> <p>Note: If there are policies with a large amount of evidence data, truncation should be enabled. Data fetching and ingesting for the policy id with large amounts of evidence would be affected due to data size.</p> <p>For example, if there is a policy id for which the evidence has 500 lines and if you enable the checkbox “Do you want to truncate the evidence?” then only 100 lines will be ingested for evidence data</p>
PCRS Maximum API retry count	Defines the number of times TA can retry the API call after any error occurs, except 429 Too Many Requests error. TA skips the API call after the maximum retry count exceeds and proceeds to pick the next Policy Ids to pull the data.

Setting	Description
Number of Policy Ids to use for Resolve Host Ids API (max 10)	Defines the number of policies considered for the subsequent Resolved Host API to pull the hosts associated to the respective policy Ids. The policy Ids are divided into multiple threads and data is pulled accordingly.
Host Ids Batch size for Posture Info Streaming API	Defines the number of Host Ids considered for the subsequent Posture Info Streaming API to pull the postures associated to the respective policy Ids.
PCRS Custom Policy Ids	Defines the Policy Ids if you want to pull or don't want to pull. If you want to provide more than one Policy Id, then provide comma separated values (for example, 1234, 4567). You need to check include/exclude setting to provide the Custom Policy Ids. - If you select the include setting, then Custom Policy Id/Ids which is/are provided are pulled by TA. - If you select the exclude setting, then Custom Policy Id/Ids which is/are provided are not pulled, but the remaining Policy Ids are pulled by the TA.
PCRS custom policy operation (include/exclude)	Select option to include or exclude the Policy Ids. By default, the None option is selected. If the default option is retained, you cannot provide any Policy Ids in PCRS Custom Policy Ids
Number of threads for PCRS resolve host Ids API (Max 10)	Defines the number of threads to use to pull Host Ids for Policy Ids. The minimum value is 2, and the maximum value is 10.
Number of threads for PCRS posture streaming API (Max 10)	Defines the number of threads to use to pull the posture data. The minimum value is 2, and the maximum value is 10.

Cyber Security Asset Management Settings

Configure the Cyber Security Asset Management Settings to fetch the asset details from your subscribed Qualys Cyber Security Asset Management account.

Cyber Security Asset Management Settings
▼

☒ Log User Accounts

☒ Log Open Ports

☒ Log File System Volume

☒ Log Network Interfaces

☒ Log Software (Separate event will be created for softwares)

☒ Log Tags

☒ Log Hardware

☒ Log Operating System

☐ Log Business App List Data (Separate event will be created for Business Apps)

☐ Exclude Unmanaged Assets

Page size (max 300)

Extra filters for CSAM API

Enter filter as JSON (e.g. [{"field": "fieldName", "operator": "operator", "value": "Value"}, {"field": "fieldName", "operator": "operator", "value": "Value"}]). Please refer the "Extra filters for CSAM API" description under Cyber Security Asset Management Settings in Qualys Splunk TA User Guide for search filter related details.

CSAM Maximum API retry count

Note: CSAM API will retry on failure till the configured number of times. Enter 0 for infinite retry.

You can configure the following settings in Cyber Security Asset Management Settings.

Setting	Description
Log User Accounts	Log the user account details when this checkbox is enabled. By default, this checkbox is selected.
Log Open Ports	Log the open ports details when this checkbox is enabled. By default, this checkbox is selected.
Log File System Volume	Log the file system volume details when this checkbox is enabled. By default, this checkbox is selected.
Log Network Interfaces	Log the network interface details when this checkbox is enabled. By default, this checkbox is selected.
Log Software (Separate event will be created for softwares)	Log the software details when this checkbox is enabled. Separate events will be created for software details. By default, this checkbox is selected.
Log Tags	Log the tag details when this checkbox is enabled. By default, this checkbox is selected.
Log Hardware	Log the hardware details when this checkbox is enabled. By default, this checkbox is selected.

Setting	Description
Log Operating System	Log the operating system details when this checkbox is enabled. By default, this checkbox is selected.
Log Business App List Data (Separate event will be created for Business Apps)	Log the user account details when this checkbox is enabled. Separate events are created for business app details. By default, this checkbox is unselected.
Exclude Unmanaged Assets	Excludes the unmanaged asset details when this checkbox is enabled. By default, this checkbox is unselected.
Page size (max 300)	Lets you specify the number of records to be fetched in single API call. The default value for page size is 100 records and maximum value is 300.
Extra filters for CSAM API	Lets you provide the extra filters, if any. Filter should be in following format {"filters": [{"field": "fieldName", "operator": "operator", "value": "Value"}, {"field": "fieldName", "operator": "operator", "value": "Value"}]}. For ex: {"filters": [{"field": "inventory.source", "operator": "EQUALS", "value": "IP"}, {"field": "operatingSystem", "operator": "EQUALS", "value": "Linux"}]}. For more information on supported fields and operators, refer to API user guide .
CSAM Maximum API retry count	Defines the number of times TA can retry the API call after any error occurs. TA stops the data input run after the maximum retry count exceeds and in checkpoint file it stores last seen asset details like last seen asset ID and asset last updated datetime and starts next run according to cron schedule and picks up last seen asset ID and asset last updated datetime from last run and pulls the remaining data.

Certview Settings

Configure the Certview Settings to fetch the asset details from your subscribed Qualys Certview account.

Certview Settings

Page size (max 200)

10

Extra filters for CertView API

Enter filter as JSON (e.g. [{"filters": [{"field": "fieldName", "value": "Value", "operator": "operator"}, {"field": "fieldName", "value": "Value", "operator": "operator"}]}]). Please refer the "Extra filters for CertView API" description under Certview Settings in Qualys Splunk TA User Guide for search filter related details.

CertView custom operation

☐ Include Fields
☐ Exclude Fields
☒ None

Note: Click "Include Fields" to include only the entered fields or click "Exclude Fields" to exclude the entered fields. Click "None" to use default API Response.

CertView Custom Fields

Note: Enter comma separated fields (e.g. abc,xyz).

Certview Maximum API retry count

0

Note: CertView API will retry on failure till the configured number of times. Enter 0 for infinite retry.

You can configure the following settings in CertView Settings

Setting	Description
Page size (max 200)	Specify the number of records to be fetched in single API call. Default: 10 records maximum: 200
Extra filters for CertView API	Provide the extra filters, if any. Filter should be in following format {"filters": [{"field": "fieldName", "value": "Value", "operator": "operator"}, {"field": "fieldName", "value": "Value", "operator": "operator"}]}. For ex: {"filters": [{"field": "inventory.source", "value": "IP", "operator": "EQUALS"}, {"field": "operatingSystem", "value": "Linux", "operator": "EQUALS"}]} For more information on this please refer to API user guide .
CertView custom operation	There are 3 options Include Fields: include only the entered fields Exclude Fields: exclude the entered fields None: use default API Response

Setting	Description
CertView Custom Fields	<p>User can either include or exclude fields based on the radio buttons selected in CertView custom operation, enter the field names comma separated in the Custom fields text box.</p> <p>Include Fields - Includes the specified parameters in the response. For example- ASSET_INTERFACES, VULNERABILITIES, SSL_PROTOCOLS, CIPHER_SUITES, ASSET_TAGS, EXTENSIVE_CERTIFICATE_INFO</p> <p>Exclude Fields - Exclude the specified parameters from the response. For example- certificate.certhash, certificate.keySize, asset.netbiosName, asset.uuid.</p> <p>For more information on include and exclude fields, refer to API user guide</p>
Certview Maximum API retry count	<p>Defines the number of times TA can retry the API call after any error occurs. TA stops the data input run after the maximum retry count exceeds, and in the checkpoint file, it stores the last seen certificate details like page number and certificate updated datetime and starts the next run according to the cron schedule and picks up page number and certificate updated datetime from last run and pulls the remaining data.</p>

Proxy Configuration

Provide the proxy server IP address and credentials for Qualys API requests.

Proxy Configuration

☐ Use a proxy Server for Qualys API requests

Proxy Server and credentials

(e.g. 10.10.10.2:8080 OR username:password@10.10.10.2:8080)

Preserve API Output

Select this check box to save the API output files in Splunk. By default, this check box is not selected. When checked, TA will preserve JSON/XML files of API output for all the modules for which TA is configured to pull the data from your Qualys cloud.

More Settings

☐ Enable debug logs

☐ Enable to preserve the XML/JSON files of API output

Kill Existing PID

Provide Existing PID and select the checkbox to kill PID. By default, this checkbox is not selected. When checked, TA kill the provided PID in next Cron Schedule.

Kill Existing PID
▼

☐
Enable the checkbox to kill below Process Id

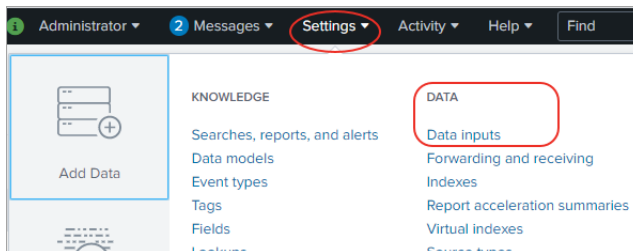
Enter Process Id to kill

Note: This feature is helpful when an earlier Process Id is stopped due to some reason but the process is actually not killed. So to kill the PID(Process Id) please give the PID number and enable the checkbox

Configure Data Sync

TA-QualysCloudPlatform pulls Qualys data and indexes in Splunk on a regular basis.

Scripts parse and convert the Qualys API output to Splunk friendly format (CIM-compliant in Splunk parlance).



Go to Settings (on the top menu) and select Data Inputs.

Then click the “Add new” link for the Qualys Technology Add-On, as shown below.

splunk> Apps ▼
Administrator ▼ 2 Messages ▼ Settings ▼ Activity ▼ Help ▼ Find

Data inputs

Local inputs

Set up data inputs from files and directories, network ports, and scripted inputs. If you want to set up forwarding and receiving between two Splunk instances, go to [Forwarding and receiving](#).

Type	Inputs	Actions
Files & directories Index a local file or monitor an entire directory.	6	Add new
HTTP Event Collector Receive data over HTTP or HTTPS.	0	Add new
TCP Listen on a TCP port for incoming data, e.g. syslog.	0	Add new
UDP Listen on a UDP port for incoming data, e.g. syslog.	0	Add new
Scripts Run custom scripts to collect or generate more data.	4	Add new
Qualys Technology Add-On Add-On for Qualys	1	Add new

Choose the Qualys metric (data feed input) you're interested in, specify when to start pulling data and how often. Then click Next. Repeat these steps for each metric you want.

Add Data

Select Source
Done

< Back
Next >

Files & Directories
Upload a file, index a local file, or monitor an entire directory.

HTTP Event Collector
Configure tokens that clients can use to send data over HTTP or HTTPS.

TCP / UDP
Configure the Splunk platform to listen on a network port.

Scripts
Get data from any API, service, or database with a script.

Systemd Journal Input for Splunk
This is the input that gets data from journald (systemd's logging component) into Splunk.

Qualys Technology Add-On
Add-On for Qualys

Splunk Secure Gateway
Initializes the Splunk Secure Gateway application to talk to mobile clients over websockets

Splunk Secure Gateway Mobile Alerts TTL
Cleans up storage of old mobile alerts

Splunk Secure Gateway Deleting Expired Tokens
Delete expired or invalid tokens created by Secure Gateway from

Qualys Metrics *

knowledge_base

Cron entry or Interval

This could be a cron format entry OR old style Interval between subsequent runs.

If you upgraded from version 1.1.0, it is recommended to change this to cron format for more control.

Old style intervals are still supported for backward-compatibility purpose. Old Format: 'w'd'h'm's', where ' ' is any positive number. For example: 12h to run after 12 hours since last run. You can omit the letter if value is 0.

Note - API rate limit according to your API tier will be applicable.

Start Date

For fim_events, fim_ignored_events, and fim_incidents Qualys Metrics - date to start data pull from should be in UTC in ISO 8601 format: "YYYY-MM-DDThh:mm:ss.msZ". Ex: 2017-01-01T00:00:00.000Z

For sem_detection Qualys Metrics - date to start data pull from should be in UTC in ISO 8601 format: "YYYY-MM-DDThh:mm:ssZ". Default value is "2021-01-26T00:00:00Z".

For other Qualys Metrics - date to start data pull from should be in UTC in ISO 8601 format: "YYYY-MM-DDThh:mm:ssZ". Default value is "1999-01-01T00:00:00Z".

For knowledge_base, 'Start Date' field is applicable only if 'Index the knowledge base' is enabled on the TA setup page.

For host_detection, this value refers to the host scanned date.

For was_findings, this value refers to the last tested date.

For VM data, choose knowledge_base and host_detection. You need to create 2 data inputs. One for knowledgebase and another for host detection.

For PC data, choose policy_posture_info.

For WAS data, choose knowledge_base and was_findings. You need to create 2 data inputs. One for knowledgebase and another for was findings.

For CS image data, choose cs_image_vulns.

For CS container data, choose cs_container_vulns.

For FIM events data, choose fim_events.

For FIM ignored events data, choose fim_ignored_events.

For FIM incidents data, choose fim_incidents.

For EDR data, choose edr_events.

For Activity Log data, choose activity_log.

For SEM data, choose sem_detection.

For PCRS data, choose pcrs_posture_info.

For CSAM data, choose cyber_security_asset_management.

For CertView data, choose `certview_certificates`.

Tip – When setting the interval, keep in mind your Qualys scanning schedule. If you're scanning weekly, you don't need to sync data daily.

Does the script pull all data or deltas only?

The first time a script runs it pulls all data from your Qualys account. After that it pulls only the changes.

Qualys data is added to Splunk

You'll notice each scan has a separate entry in Splunk. If you purge hosts using your Qualys account the data is not removed from Splunk.

How to assign a custom index to an event type?

From TA v1.7.1 onwards, we are not supporting macro definition for indexes.

Specify a custom index from UI

Go to Settings > Event types and from the App drop-down select Qualys Technology Add-On for Splunk. Navigate to the event type that you want to update. Click the event type and update the search string to specify `index=<name of the custom index>`.

Specify a custom index from CLI

To set custom index, copy the `eventtype.conf` file from `$SPLUNK_HOME/etc/apps/TA-QualysCloudPlatform/default/` to `$SPLUNK_HOME/etc/apps/TA-QualysCloudPlatform/local/` and update the search string of the required event type to specify `index=<name of the custom index>`. Then restart Splunk.

Enable the Data Feed to Start in Splunk

Return to Settings > Data Inputs > Qualys Technology Add-On. You'll see each of the Qualys metrics you selected. Make sure you enable these.

The screenshot shows the Splunk interface for the Qualys Technology Add-On. The breadcrumb trail is Settings > Data Inputs > Qualys. A red dotted arrow points to the 'Enable' button in the 'Status' column of the table, with the text 'Click here to enable each data feed'.

Qualys Metrics	Cron entry or Interval	Start Date	Status	Actions
cs_container_vulns	45 14 28 8 *	1999-01-01T00:00:00Z	Disabled	Enable Clone Delete
cs_image_vulns	49 14 28 8 *	1999-01-01T00:00:00Z	Disabled	Enable Clone Delete
fim_events	02 18 28 8 *	2019-01-01T00:00:00Z	Enabled	Disable Clone Delete
fim_ignored_events	51 10 27 8 *	2019-01-01T00:00:00Z	Disabled	Enable Clone Delete
fim_incidents	06 11 27 8 *	2019-01-01T00:00:00Z	Disabled	Enable Clone Delete
host_detection	35 12 27 8 *	2019-01-01T00:00:00Z	Disabled	Enable Clone Delete
edr_events	13 14 26 8 *	2019-08-23T00:00:00Z	Disabled	Enable Clone Delete
knowledge_base	22 15 28 8 *	1999-01-01T00:00:00Z	Disabled	Enable Clone Delete
policy_posture_info	11 13 27 8 *	2018-01-01T00:00:00Z	Disabled	Enable Clone Delete
was_findings	36 17 28 8 *	2019-07-01T00:00:00Z	Enabled	Enable Clone Delete
sem_detection	2m	2021-01-26T00:00:00Z	Enabled	Enable Clone Delete

Once you enable data feeds, check the \$SPLUNK_HOME/etc/apps/TA-QualysCloudPlatform/tmp directory on your search head to see the XML files begin to download. Depending on how much data there is, it can take from hours to days to download the first data set.

Note that for all FIM data inputs, choose a date equal to or greater than 2017-01-01T00:00:00.000Z.

How to setup for a Search Head Cluster

- 1) Install Qualys TA on your Forwarder. Depending on the type of data you want to ingest, add and enable all or any of these data inputs: host_detection, was_findings, policy_posture_info.
- 2) Use Deployer to push Qualys visualization apps.
- 3) On each Search Heads, manually configure the event types. To add event types, go to Settings > Event types. On the Event types page, click New Event Type. In the Add new page, provide the search string for the new event type and click Save.

How to index KB data into Splunk

We support indexing of the KnowledgeBase (KB) data in Splunk so that the Splunk TA users on the distributed setup environment can get the updated KnowledgeBase data on the Search Head from the Heavy Forwarder.

On the TA set up page, we added a KnowledgeBase Settings section that has a check box “Index the KnowledgeBase. CSV lookup...”.

Knowledge Base Settings
▼

☒
Log additional fields (SOLUTION, CONSEQUENCE, DIAGNOSIS)

☒
Index the knowledge base. CSV lookup file will NOT be created.

The check box indicates whether to index the KnowledgeBase data in Splunk or to write the data into a CSV file. When you select the check box and click Save, TA will fetch the KB data and index the KB data in Splunk. If the check box is not selected, TA does not index the KB data into Splunk and creates a CSV file. The CSV file will have KB data from 1999-01-01.

<div style="background-color: #f0f0f0; padding: 5px; margin-bottom: 5px;"> Files & Directories Upload a file, index a local file, or monitor an entire directory. </div> <div style="background-color: #f0f0f0; padding: 5px; margin-bottom: 5px;"> HTTP Event Collector Configure tokens that clients can use to send data over HTTP or HTTPS. </div> <div style="background-color: #f0f0f0; padding: 5px; margin-bottom: 5px;"> TCP / UDP Configure the Splunk platform to listen on a network port. </div> <div style="background-color: #f0f0f0; padding: 5px; margin-bottom: 5px;"> Scripts Get data from any API, service, or database with a script. </div> <div style="background-color: #f0f0f0; padding: 5px; margin-bottom: 5px;"> Systemd Journal Input for Splunk This is the input that gets data from journald (systemd's logging component) into Splunk. </div> <div style="background-color: #f0f0f0; padding: 5px; margin-bottom: 5px;"> Qualys Technology Add-On Add-On for Qualys > </div> <div style="background-color: #f0f0f0; padding: 5px; margin-bottom: 5px;"> Splunk Secure Gateway Initializes the Splunk Secure Gateway application to talk to mobile clients over websockets </div> <div style="background-color: #f0f0f0; padding: 5px; margin-bottom: 5px;"> Splunk Secure Gateway Mobile Alerts TTL Cleans up storage of old mobile alerts </div> <div style="background-color: #f0f0f0; padding: 5px; margin-bottom: 5px;"> Splunk Secure Gateway Deleting Expired Tokens Delete expired or invalid tokens created by Secure Gateway from Splunk </div> <div style="background-color: #f0f0f0; padding: 5px;"> Splunk Secure Gateway Role Based Notification Manager Used for sending mobile alerts to users by role </div>	<div style="margin-bottom: 10px;"> Qualys Metrics * knowledge_base </div> <div style="margin-bottom: 10px;"> Cron entry or Interval <p style="font-size: 0.8em; margin-top: 5px;"> This could be a cron format entry OR old style Interval between subsequent runs. If you upgraded from version 11.0, it is recommended to change this to cron format for more control. Old style intervals are still supported for backward-compatibility purpose. Old Format: 'w*d'h'm's', where * is any positive number. For example: 12h to run after 12 hours since last run. You can omit the letter if value is 0. Note - API rate limit according to your API tier will be applicable. </p> </div> <div style="margin-bottom: 10px;"> Start Date <p style="font-size: 0.8em; margin-top: 5px;"> For fim_events, fim_ignored_events, and fim_incidents Qualys Metrics - date to start data pull from should be in UTC in ISO 8601 format: "YYYY-MM-DDThh:mm:ss.msZ". Ex: 2017-01-01T00:00:00.000Z For sem_detection Qualys Metrics - date to start data pull from should be in UTC in ISO 8601 format: "YYYY-MM-DDThh:mm:ssZ". Default value is "2021-01-26T00:00:00Z". For other Qualys Metrics - date to start data pull from should be in UTC in ISO 8601 format: "YYYY-MM-DDThh:mm:ssZ". Default value is "1999-01-01T00:00:00Z". </p> <div style="border: 2px solid red; padding: 2px; font-size: 0.8em; margin-bottom: 5px;"> For knowledge_base, 'Start Date' field is applicable only if 'Index the knowledge base' is enabled on the TA setup page. </div> <p style="font-size: 0.8em; margin-top: 5px;"> For host_detection, this value refers to the host scanned date. For was_findings, this value refers to the last tested date. For cs_image_vulns, this value refers to image scan date. </p> </div> <div> More settings <input type="checkbox"/> </div>
--	--

On the Settings > Data Inputs > Add Data page for Qualys technology add on, we added the information that for knowledge_base “Start Date” field is applicable only if the “Index the KnowledgeBase. CSV lookup...” option is enabled for the Knowledge Base settings on the TA set up page.

After you enable the index KB data option, you need to generate KB CSV lookup on the Search Head. See [KnowledgeBase Settings](#).

How to get the RESULTS field indexed in host detection input

Update optional parameters on the TA setup page to include “show_results=1”. Already have optional parameters listed? Simply append this with an ‘&’ sign, for example “show_tags=1&show_results=1”.

How to populate the Diagnosis, Consequence and Solution information in Splunk

Go to the KnowledgeBase Settings section on the TA setup page and select the “Log additional fields (SOLUTION, CONSEQUENCE, DIAGNOSIS)” check box. TA will fetch the Diagnosis, Consequence, and Solution fields from Qualys cloud in the KB data. Search the KB data in Splunk to view information related to these fields.

View your Qualys Data in Splunk

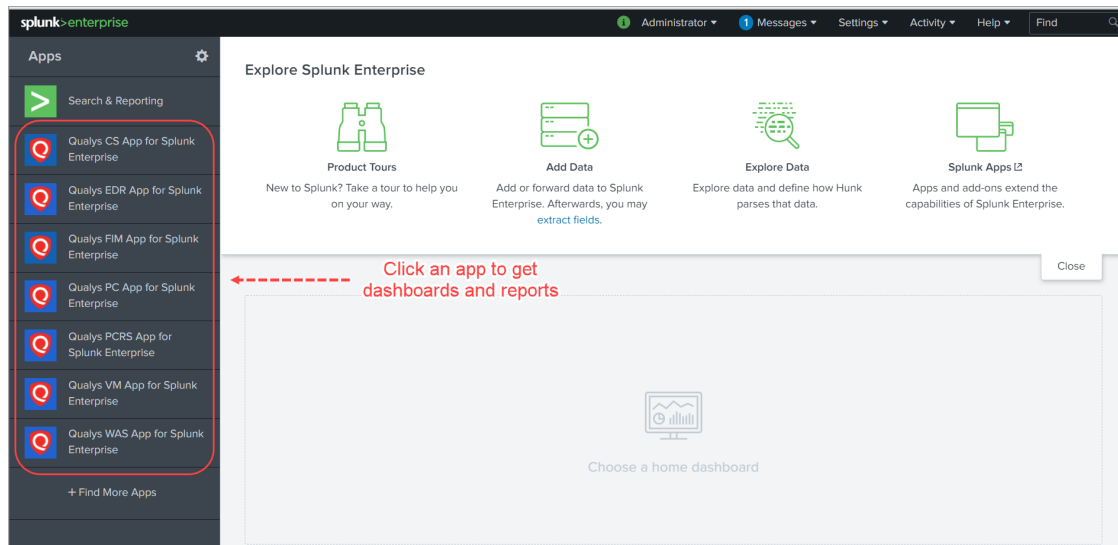
We provide additional apps that make use of the data collected by the TA. You'll get dashboards and reports, and you'll be able to easily search your data.

Simply download and install these apps. There is no setup needed!

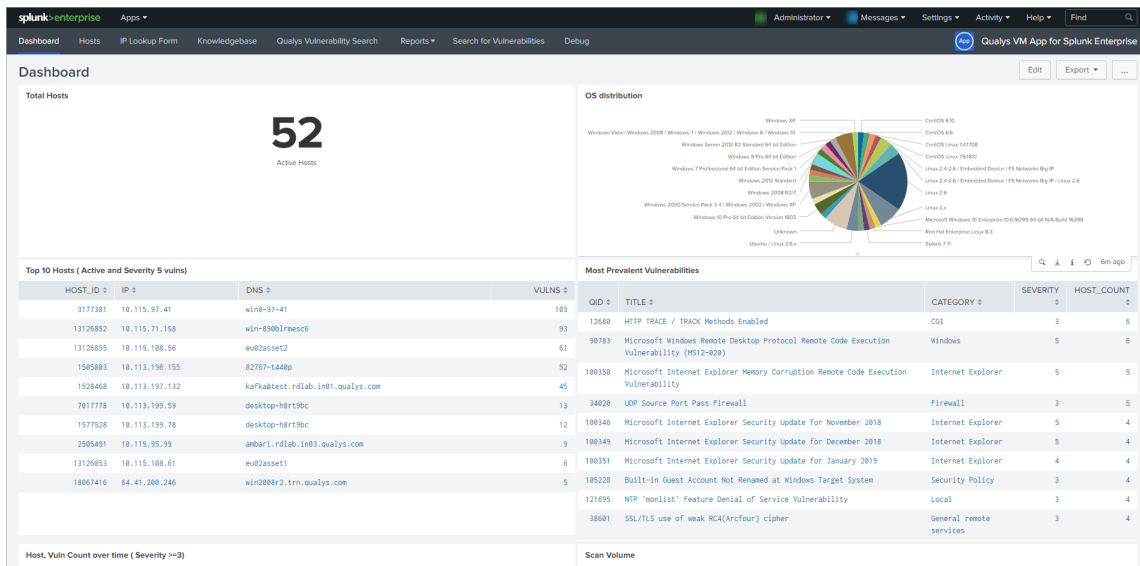
- Qualys VM App for Splunk Enterprise
- Qualys PC App for Splunk Enterprise
- Qualys WAS App for Splunk Enterprise
- Qualys CS App for Splunk Enterprise
- Qualys FIM App for Splunk Enterprise
- Qualys EDR App for Splunk Enterprise
- Qualys PCRS App for Splunk Enterprise
- Qualys CSAM App for Splunk Enterprise
- Qualys Certview App for Splunk Enterprise

Once installed, you'll see new apps on your Splunk Home page.

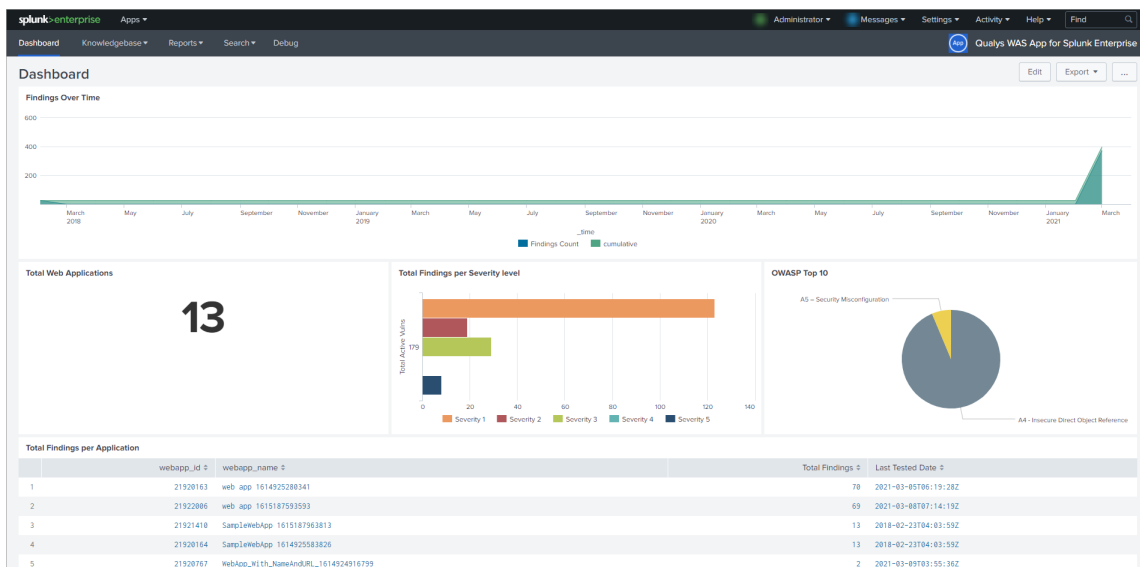
Click any app on your Home page to view data.



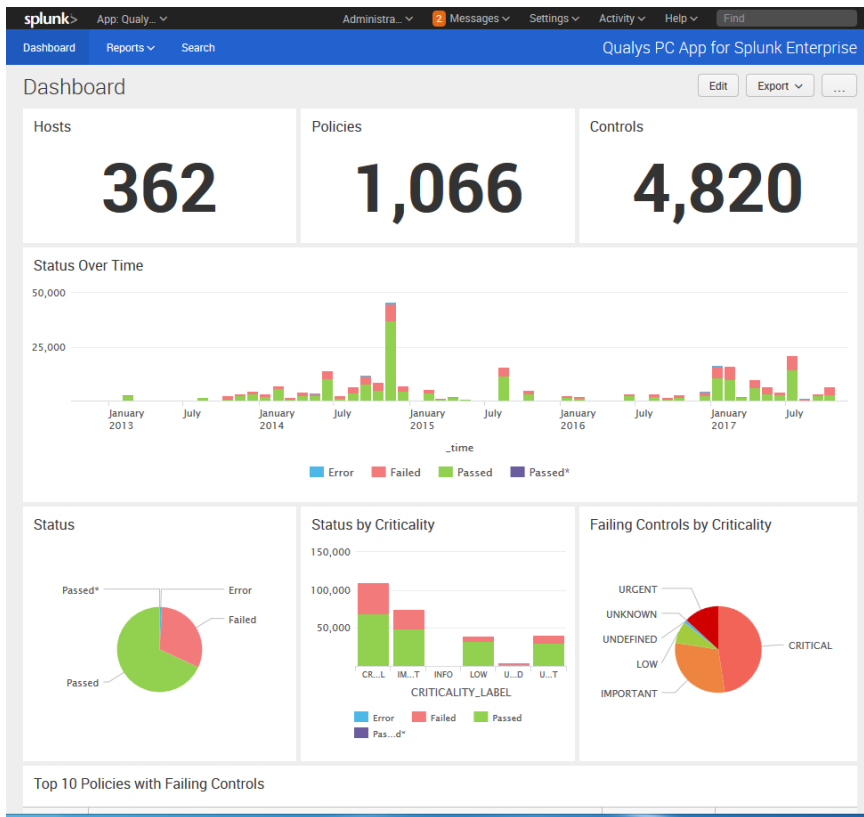
Sample VM Dashboard



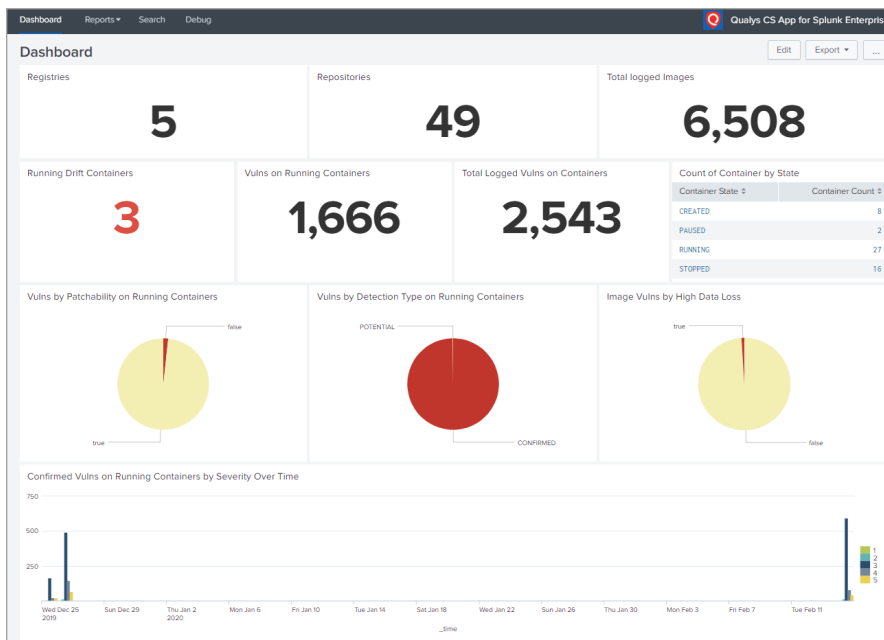
Sample WAS Dashboard



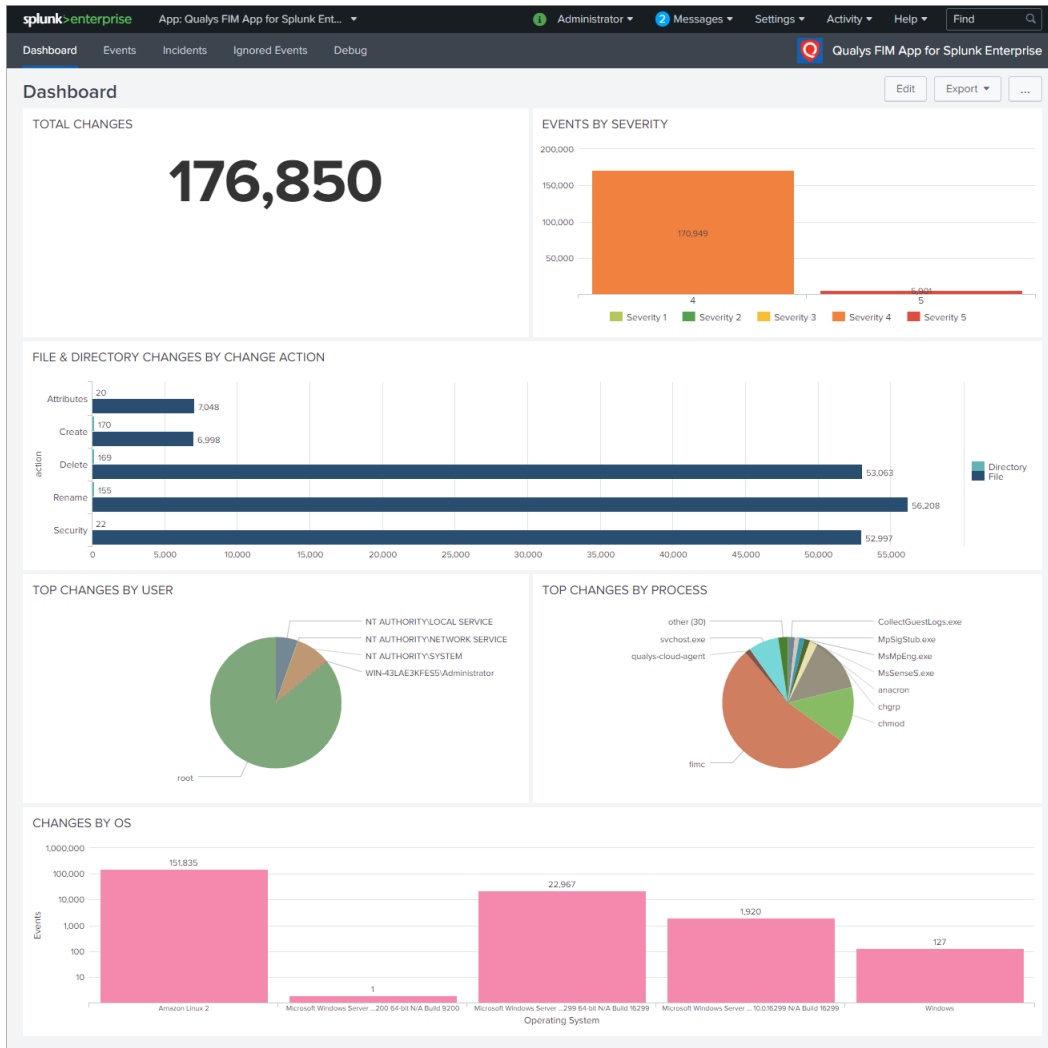
Sample PC Dashboard



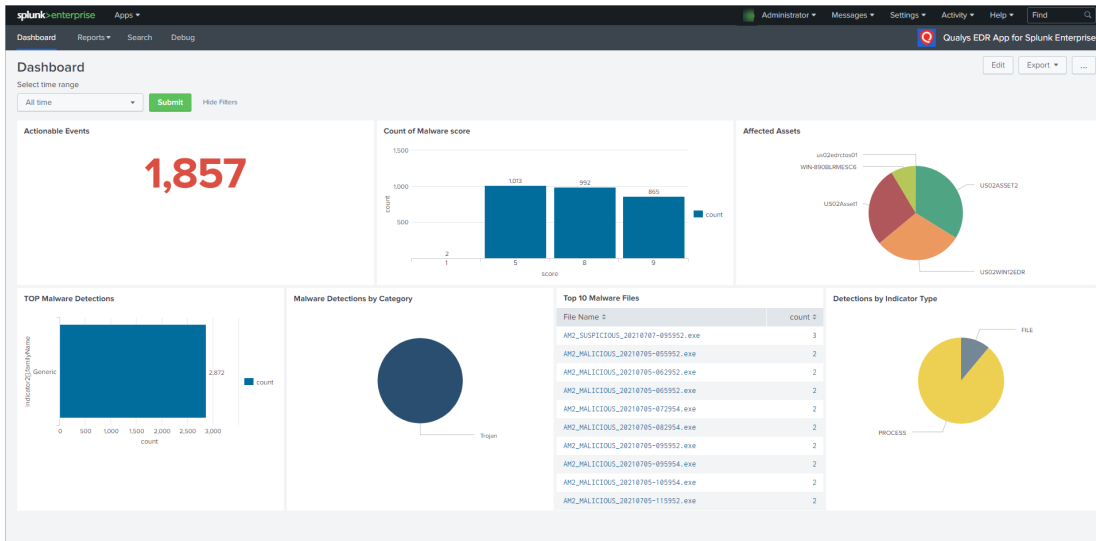
Sample CS Dashboard



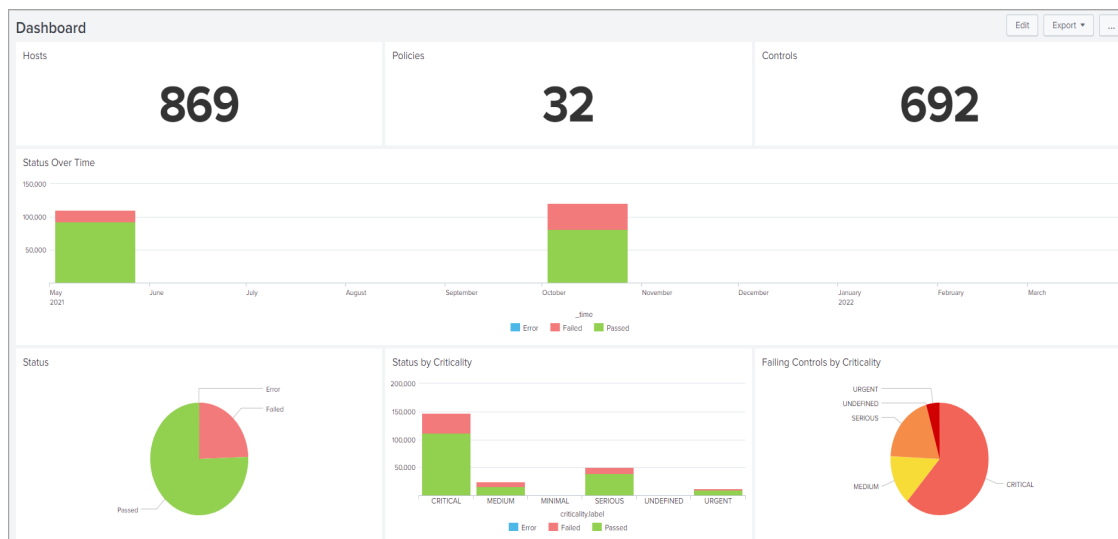
Sample FIM Dashboard



Sample EDR Dashboard



Sample PCRS Dashboard



Top 10 Policies with Failing Controls			
Policy Id	Policy Title	No. of Failed Controls	Last Evaluated DateTime
116482	CIS_Benchmark_For_Oracle_Linux_7_v2.1.0	38816	2021-12-02T22:04:08Z
91477	Redhat 6	18384	2021-12-02T22:12:11Z
116481	CRM-Reproduce	792	2021-12-02T22:05:38Z
144888	Email_notification	248	2022-01-11T07:05:08Z
4989786	Unit Manager policy for streaming posture API -- edited by manager	68	2022-03-25T15:00:00Z
4207711	Regression_FullScan_SDC_UDC	44	2022-03-29T03:54:45Z
116480	l_host	12	2021-12-02T22:04:45Z
4886889	Aruba OS OCA Policy	10	2022-03-29T03:54:44Z
4207851	Regression_SDC+UDC+DNS+AgCT-includePCAgent-withException	8	2022-03-29T03:54:46Z
4847696	COMPLIANCE POLICY 10.18	8	2022-03-29T03:54:42Z

Top 10 Least Compliant Hosts			
Host Id	Host IP	Host DNS	No. of Failed Controls
127545864		1-1-1-37.bogus.tld	186
127547705		1-1-1-0.bogus.tld	97
127547706		1-1-1-1.bogus.tld	97
127547707		1-1-1-2.bogus.tld	97
127547708		1-1-1-3.bogus.tld	97
127547709		1-1-1-4.bogus.tld	97
127547726		1-1-1-5.bogus.tld	97
127547727		1-1-1-6.bogus.tld	97
127547728		1-1-1-7.bogus.tld	97
127547731		1-1-1-8.bogus.tld	97

Policies Not Evaluated in Last 10 Days		Q	↓	↑	18m ago
Last Evaluated DateTime	Policy Title				
2021-08-05 11:05:10	PC_AgentData				
2021-09-22 11:45:23	PC_RHEL7_Data				
2021-09-22 11:58:25	PC_Agent_CentOS7				
2021-09-30 12:55:54	Best Practice Controls for Malware/Ransomware Prevention				
2021-09-30 12:55:57	Compensating Controls for Reducing Risk of Vulnerabilities Leveraged by Fireeye Red team tools				
	Security Configuration and Compliance Policy for Zoom Client on Windows Remote Endpoints				
2021-09-30 12:55:58	Minimum Security Hygiene for Windows Remote Endpoints				
	Minimum Security Hygiene for Mac OS X Remote Endpoints				
2021-09-30 12:55:59	Security Configuration and Compliance Policy for Zoom Client on Mac OS X Remote Endpoints				
	Security Hygiene Controls for Reducing Risk of SolarWinds Orion Compromise (SUNBURST/Solorigate)				
2021-12-03 03:34:08	CIS_Benchmark_For_Oracle_Linux_7_v2.1.0				
2021-12-03 03:34:45	l_host				
2021-12-03 03:35:38	CRM-Reproduce				
	Redhat 1 asset				

« Prev 1 2 3 Next »

Note: The following image displays the time taken to ingest the events.

splunk>enterprise Apps Administrator Messages Settings Activity Help Find

Dashboard Reports Search **Debug** Qualys PCRS App for Splunk Enterprise

Debug Edit Export ...

Select one or more log Types PID

All time Error X Hide Filters

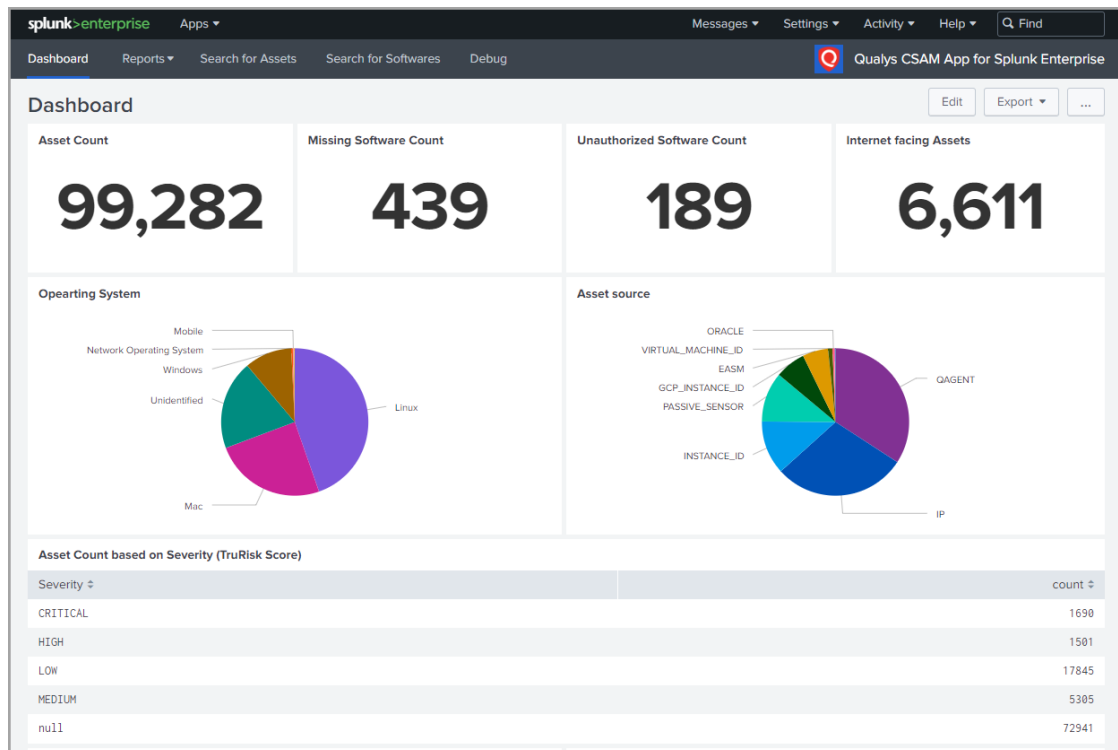
Policy Compliance Reporting Service log

Search did not return any events.

Policy Compliance Reporting Service Time taken

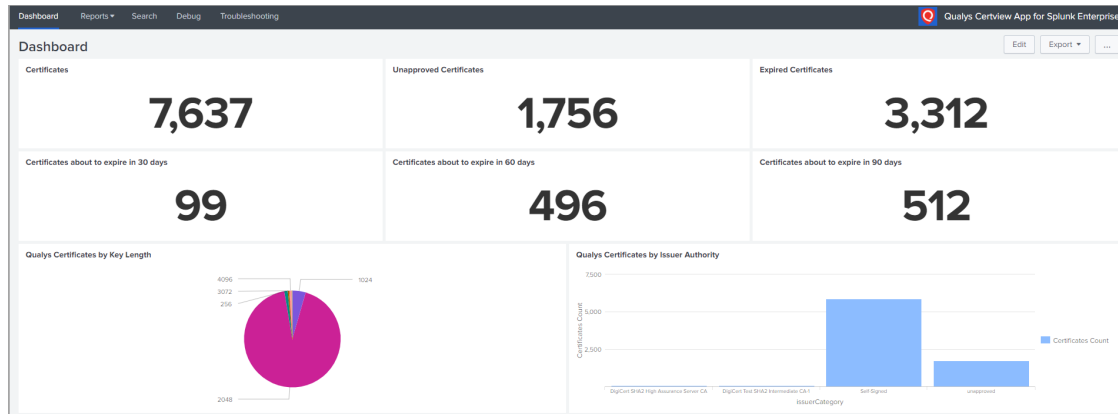
i	Time	Event
>	3/21/22 3:59:19.000 PM	TA-QualysCloudPlatform (pcrs.posture_info): 2022-03-21 15:59:19 PID=1329475 [MainThread] INFO: Qualys PCRS Populator finished.
		host = lxagubu source = /opt/splunk/var/log/splunk/ta_QualysCloudPlatform.log sourcetype = ta_QualysCloudPlatform-too_small
>	3/21/22 3:59:19.000 PM	TA-QualysCloudPlatform (pcrs.posture_info): 2022-03-21 15:59:19 PID=1329475 [MainThread] INFO: PCRS input logged 1194 entries.
		host = lxagubu source = /opt/splunk/var/log/splunk/ta_QualysCloudPlatform.log sourcetype = ta_QualysCloudPlatform-too_small
>	3/21/22 3:58:33.000 PM	TA-QualysCloudPlatform (pcrs.posture_info): 2022-03-21 15:58:33 PID=1329475 [MainThread] INFO: Qualys PCRS Populator started.
		host = lxagubu source = /opt/splunk/var/log/splunk/ta_QualysCloudPlatform.log sourcetype = ta_QualysCloudPlatform-too_small

Sample CSAM Dashboard





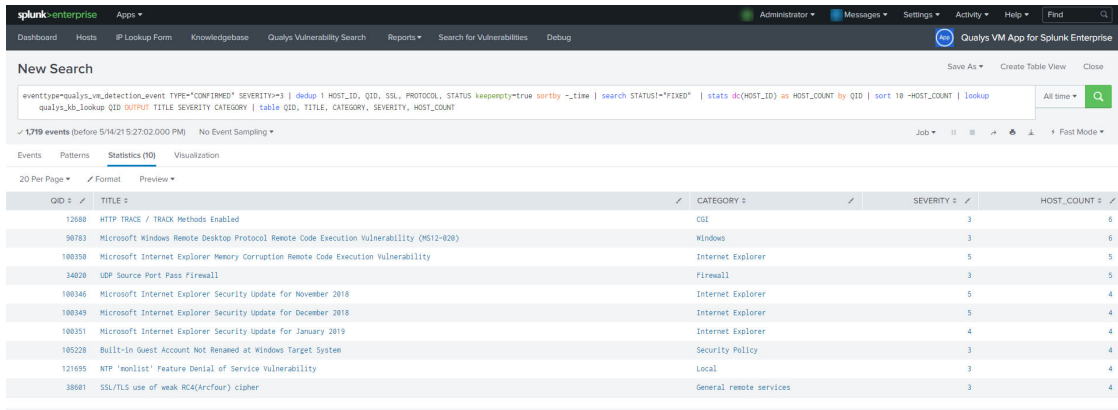
Sample Certview Dashboard



Search Your Qualys Data

Choose Search & Reporting on the Splunk Home page. Then enter your search query in the search field. Here are some sample search queries to get you started.

Most Prevalent Vulnerabilities



New Search Save As Create Table View Close

eventtype=qualys_vuln_detection_event TYPE="CONFIRMED" SEVERITY=3 | dedup 1 HOST_ID, QID, SSL, PROTOCOL, STATUS keepkeys=true sortby _time | search STATUS!="FIXED" | stats dc(HOST_ID) as HOST_COUNT by QID | sort 10 -HOST_COUNT | lookup qualys_vuln_lookup QID OUTPUT TITLE SEVERITY CATEGORY | table QID, TITLE, CATEGORY, SEVERITY, HOST_COUNT

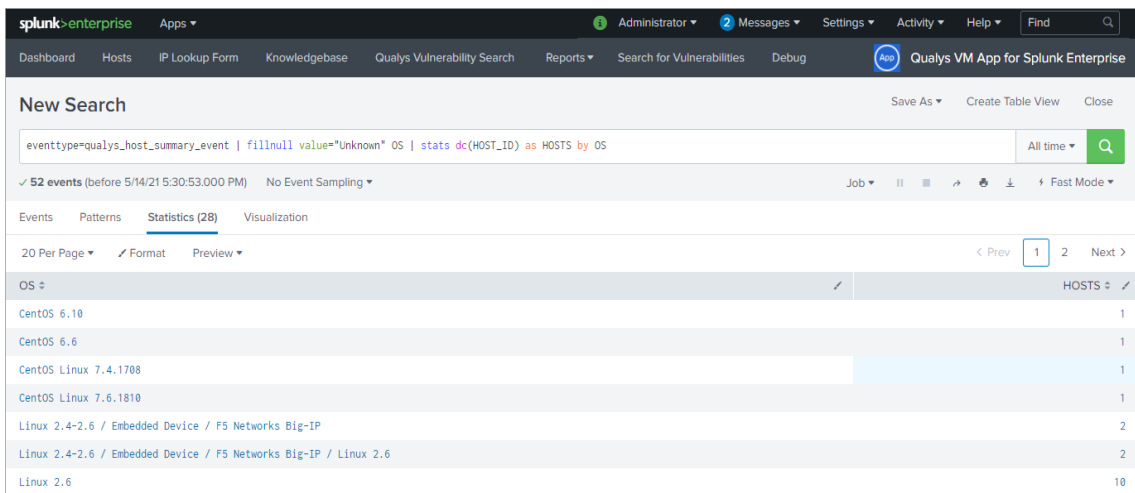
✓ 1719 events (before 5/14/21 5:27:02.000 PM) No Event Sampling

Events Patterns **Statistics (10)** Visualization

20 Per Page Format Preview

QID	TITLE	CATEGORY	SEVERITY	HOST_COUNT
12688	HTTP TRACE / TRACK Methods Enabled	CGI	3	6
90783	Microsoft Windows Remote Desktop Protocol Remote Code Execution Vulnerability (MS12-028)	Windows	3	6
108358	Microsoft Internet Explorer Memory corruption Remote Code Execution Vulnerability	Internet Explorer	5	5
34028	UDP Source Port Pass Firewall	Firewall	3	5
100346	Microsoft Internet Explorer Security Update for November 2018	Internet Explorer	5	4
100349	Microsoft Internet Explorer Security Update for December 2018	Internet Explorer	5	4
100351	Microsoft Internet Explorer Security Update for January 2019	Internet Explorer	4	4
105228	Built-in Guest Account Not Renamed at Windows Target System	Security Policy	3	4
121695	HTTP 'onlist' Feature Denial of Service Vulnerability	Local	3	4
38081	SSL/TLS use of weak RC4(Arcfour) cipher	General remote services	3	4

Host Distribution by OS



New Search Save As Create Table View Close

eventtype=qualys_host_summary_event | fillnull value="Unknown" OS | stats dc(HOST_ID) as HOSTS by OS

✓ 52 events (before 5/14/21 5:30:53.000 PM) No Event Sampling

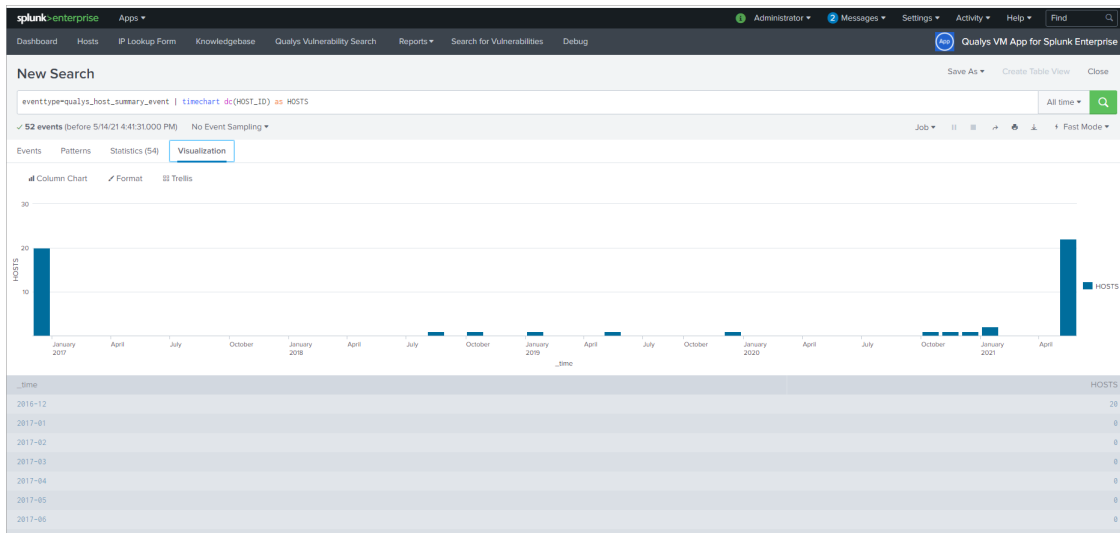
Events Patterns **Statistics (28)** Visualization

20 Per Page Format Preview

< Prev 1 2 Next >

OS	HOSTS
CentOS 6.10	1
CentOS 6.6	1
CentOS Linux 7.4.1708	1
CentOS Linux 7.6.1810	1
Linux 2.4-2.6 / Embedded Device / F5 Networks Big-IP	2
Linux 2.4-2.6 / Embedded Device / F5 Networks Big-IP / Linux 2.6	2
Linux 2.6	10

Scan Volume



Hosts not Scanned in more than 30 days

The screenshot shows a Splunk search interface with the following details:

- Search Query:** `eventtype=qualys_host_summary_event | where _time<relative_time(now(),~-30d86400) | debug HOST_ID | eval Last_Scanned=if(Last_Scanned, "Y", "N") | stats list(DNG) as "Host Name", list(OS) as OS by Last_Scanned, IP | sort by Last_Scanned`
- Results:** 30 events (before 5/14/21 8:59:54.000 PM). No Event Sampling.
- Visualization:** A table view showing the results of the search. The table has columns for `Last_Scanned`, `IP`, `Host Name`, and `OS`. The data shows a list of hosts that have not been scanned in more than 30 days.

Last_Scanned	IP	Host Name	OS
2016-12-23 15:32:14	64.41.200.231	demo01.s82.sjc01.qualys.com	Windows 2000 Service Pack 3-4 / Windows 2003 / Windows XP
2016-12-23 15:37:19	64.41.200.233	demo03.s82.sjc01.qualys.com	Linux 2.4-2.6 / Embedded Device / FS Networks Blg-IP
2016-12-23 15:37:20	64.41.200.235	demo05.s82.sjc01.qualys.com	Solaris 9-10
2016-12-23 15:37:21	64.41.200.242	demo12.s82.sjc01.qualys.com	Linux 2.4-2.6 / Embedded Device / FS Networks Blg-IP / Linux 2.6
2016-12-23 15:37:22	64.41.200.243	demo13.s82.sjc01.qualys.com	Ubuntu / Linux 2.6.x
2016-12-23 15:37:23	64.41.200.244	demo14.s82.sjc01.qualys.com	Linux 2.4-2.6 / Embedded Device / FS Networks Blg-IP / Linux 2.6
2016-12-23 15:37:24	64.41.200.245	demo15.s82.sjc01.qualys.com	Linux 2.4-2.6 / Embedded Device / FS Networks Blg-IP / Linux 2.6
2016-12-23 15:37:24	64.41.200.247	trn-win7.trn.qualys.com	Windows 2008 R2/7
2016-12-23 15:37:25	64.41.200.248	demo18.s82.sjc01.qualys.com	Windows Vista / Windows 2008 / Windows 7 / Windows 2012 / Windows 8 / Windows 10
2016-12-23 15:37:25	64.41.200.249	demo19.s82.sjc01.qualys.com	Windows Vista / Windows 2008 / Windows 7 / Windows 2012 / Windows 8 / Windows 10
2016-12-23 15:37:27	64.41.200.250	demo20.s82.sjc01.qualys.com	Ubuntu / Linux 2.6.x
2016-12-23 15:38:59	64.41.200.234	demo04.s82.sjc01.qualys.com	Linux 2.4-2.6 / Embedded Device / FS Networks Blg-IP
2016-12-23 15:38:59	64.41.200.238	demo08.s82.sjc01.qualys.com	Windows 2000 Service Pack 3-4 / Windows 2003 / Windows XP
2016-12-23 15:41:03	64.41.200.241	demo11.s82.sjc01.qualys.com	Linux 2.6
2016-12-23 15:47:46	64.41.200.246	demo16.s82.sjc01.qualys.com	Windows Vista / Windows 2008 / Windows 7 / Windows 2012 / Windows 8 / Windows 10
2016-12-23 15:58:58	64.41.200.237	demo07	Windows XP
2016-12-23 15:51:51	64.41.200.236	demo06.s82.sjc01.qualys.com	Linux 2.6

Search Container Security Data

CS data is in JSON format. TA indexes CS ev ents in a structured format. You can search the CS data in Splunk using DOT notation.

Use these event types to search for different types of container data: `cs_image_info_event` to search for vulnerabilities of images, `qualys_cs_container_details`, `qualys_cs_container_vuln` to search for container data and `qualys_cs_container_vuln_summary` to search for container vulnerabilities.

For more information on creating search queries to filter CS data, refer to the [Splunk Search Reference](#).

Sample JSON query to filter images matching a registry object in a repo list

eventtype="cs_image_info_event"

The screenshot shows the Splunk Search interface. At the top, the search bar contains the query `eventtype="cs_image_info_event"`. Below the search bar, it indicates 89 events from 5/13/21 8:30:00.000 PM to 5/14/21 9:16:50.000 PM. The interface includes tabs for Events (89), Patterns, Statistics, and Visualization. A timeline visualization is shown with green bars representing events. Below the timeline, a table displays the search results. The table has columns for Time and Event. The first result is for 5/14/21 10:05:34.000 AM. The event data is a JSON object containing various fields related to a container image scan.

Time	Event
5/14/21 10:05:34.000 AM	<pre>{ "associatedContainersCount": 1, "associatedHostsCount": 1, "compliance": { "failCount": 2, "passCount": 1 }, "created": "2021-05-12T11:34:56Z", "imageId": "b1ee5de3d743", "instrumentationState": "null", "instrumentedFrom": "44869d2070b0ff6c51ed4b6d67a45e7f2c180ce01e37fc80458231a9737c977", "isDockerHubOfficial": false, "isInstrumented": false, "lastComplianceScanDate": "1620986503576", "lastFoundOnHost": { "registryId": "1620934017496" }, "lastVidScanDate": "1620934017496", "repo": { "digests": ["b1ee5de3d74316d16bf7116790685fe50800dccc8dc5bfac33d668571123c7e0"], "scanErrorCode": null, "scanStatus": "SUCCESS", "scanType": "DYNAMIC", "sha": "b1ee5de3d74316d16bf7116790685fe50800dccc8dc5bfac33d668571123c7e0", "size": 440040442, "source": ["b1ee5de3d74316d16bf7116790685fe50800dccc8dc5bfac33d668571123c7e0"] } }</pre>

Sample JSON query to search images with a specific vulnerability severity count

eventtype="cs_image_info_event" "vulnerabilities.severity2Count"="2"

The screenshot shows the Splunk Search interface. At the top, the search bar contains the query: `eventtype="cs_image_info_event" "vulnerabilities.severity2Count"="2"`. The search results are displayed in a table view, showing a single event from May 7, 2021, at 10:05:37:000 AM. The event details are as follows:

Time	Event
5/7/21 10:05:37:000 AM	<pre>{ "associatedContainersCount": 0, "associatedHostsCount": 0, "compliance": { "errorCount": 0, "failCount": 0, "passCount": 0 }, "created": "2021-03-28T12:48:26Z", "imageId": "e38ca8a339e7", "instrumentationState": null, "instrumentedFrom": null, "isDockerHubOfficial": false, "isInstrumented": false, "lastComplianceScanDate": null, "lastFoundOnHost": null, "lastVesScanDate": "1620381937362", "registryUuid": ["+"], "repo": ["+"], "repoDigests": ["+"], "scanErrorCode": null, "scanStatus": "SUCCESS", "scanType": "DYNAMIC", "sha": "e38ca8a339e752f80e71835ed8a4fe983927fe5efdb930b8eb83360e233a04", "size": 407404459, "source": ["+"], "type": "IMAGE_INFO" }</pre>

The interface also includes a sidebar with field lists (SELECTED FIELDS, INTERESTING FIELDS) and a timeline visualization at the top.

Sample JSON query to search vulnerabilities on running containers

eventtype=qualys_cs_container_vuln [search eventtype=qualys_cs_container_details state=RUNNING | dedup containerId | fields + containerId]

The screenshot shows the Splunk Search interface with the following details:

- Search Bar:** Contains the query `eventtype=qualys_cs_container_vuln [search eventtype=qualys_cs_container_details state=RUNNING | dedup containerId | fields + containerId]`.
- Results:** Shows 5,586 events. The search is set to "All time".
- Visualizations:** A bar chart is displayed at the top, showing event counts over time.
- Fields List:**
 - SELECTED FIELDS:** host 1, source 1, sourcetype 1.
 - INTERESTING FIELDS:** authType, category, containerId, customerSeverity, cveids, cvssInfo, cvssInfo, discoveryType, firstFound, lastFound, patchAvailable, port, product, published, qid, result, risk, severity, sha, software, status, supportedBy.
- Event Details:** A sample event is shown with the following fields:
 - `authType: [{}]`
 - `category: Debian`
 - `containerId: ac815c95f1e7`
 - `customerSeverity: 3`
 - `cveids: [{}]`
 - `cvssInfo: [{}]`
 - `cvssInfo: [{}]`
 - `discoveryType: [{}]`
 - `firstFound: 2020-10-01T13:28:45Z`
 - `lastFound: 2020-10-01T13:28:45Z`
 - `patchAvailable: true`
 - `port: null`
 - `product: [{}]`
 - `published: null`
 - `qid: 177338`
 - `result: "table col=3"`
 - `risk: 10`
 - `severity: 3`
 - `sha: ac815c95f1e7b22d6ef315fffb866d824a1e76d47aaf2e81367eef83dc6`
 - `software: [{}]`
 - `status: null`
 - `supportedBy: [{}]`

You can use Debug option to view debug information for one or more data input parameters

The screenshot shows the Splunk Debug interface with the following details:

- App:** Qualys CS App for Splunk Enterprise.
- Search Bar:** Contains the query `eventtype=qualys_cs_container_vuln [search eventtype=qualys_cs_container_details state=RUNNING | dedup containerId | fields + containerId]`.
- Debug Options:**
 - Select one or more data input Types:** Containers x, Images x.
 - Select one or more log Types:** Error x, Warning x, Info x, Debug x.
 - Select time range:** All time.
- Container Security log:**

Time	Event
22/01/2019 04:30:08.000	TA-QualysCloudPlatform: 2019-01-22 04:30:08 PID=20984 [MainThread] INFO: TA-QualysCloudPlatform (cs_container_vulns) - Qualys CS Container Populator finished.
22/01/2019 04:30:08.000	TA-QualysCloudPlatform: 2019-01-22 04:30:08 PID=20984 [MainThread] INFO: TA-QualysCloudPlatform (cs_container_vulns) - Total time taken to pull the data is 0:00:05.097241.
22/01/2019 04:30:08.000	TA-QualysCloudPlatform: 2019-01-22 04:30:08 PID=20984 [MainThread] INFO: TA-QualysCloudPlatform (cs_container_vulns) - Container Populator logged 0 vulnerabilities.
22/01/2019 04:30:08.000	TA-QualysCloudPlatform: 2019-01-22 04:30:08 PID=20984 [MainThread] INFO: TA-QualysCloudPlatform (cs_container_vulns) - Container Populator logged 0 containers.
22/01/2019 04:30:08.000	TA-QualysCloudPlatform: 2019-01-22 04:30:08 PID=20984 [Thread-2] INFO: TA-QualysCloudPlatform (cs_container_vulns) - inbound queue exiting.
22/01/2019 04:30:08.000	TA-QualysCloudPlatform: 2019-01-22 04:30:08 PID=20984 [Thread-2] INFO: TA-QualysCloudPlatform (cs_container_vulns) - inbound idsetQueue empty.
22/01/2019 04:30:08.000	TA-QualysCloudPlatform: 2019-01-22 04:30:08 PID=20984 [Thread-1] INFO: TA-QualysCloudPlatform (cs_container_vulns) - inbound queue exiting.

Search FIM Data for Events and Incidents

FIM events, Ignored events and incidents ingested in splunk can be searched using their eventtype. Further, user can search them using SPL of desired filters.

Here are some sample queries for searching FIM data in Splunk.

Sample query to search for FIM events

eventtype="qualys_fim_event"

The screenshot shows the Splunk Search interface. The search bar contains the query `eventtype="qualys_fim_event"`. Below the search bar, it indicates 552 events were found for the time range 6/24/19 3:30:00.000 PM to 6/25/19 4:08:37.000 PM. The results are displayed in a table with columns for Time and Event. The first event is shown with a time of 6/25/19 4:08:24.000 PM and an action of Rename.

Time	Event
6/25/19 4:08:24.000 PM	{ [-] action: Rename actor: { [+] }

Sample query to search for FIM ignored events

eventtype="qualys_ignored_fim_event"

The screenshot shows the Splunk Search interface. The search bar contains the query `eventtype="qualys_ignored_fim_event"`. Below the search bar, it indicates 16 events were found for the time range 6/24/19 3:30:00.000 PM to 6/25/19 4:00:32.000 PM. The results are displayed in a table with columns for Time and Event. The first event is shown with a time of 6/25/19 3:58:12.000 PM and an action of Delete.

Time	Event
6/25/19 3:58:12.000 PM	{ [-] action: Delete actor: { [+] }

Sample query to search for FIM incidents

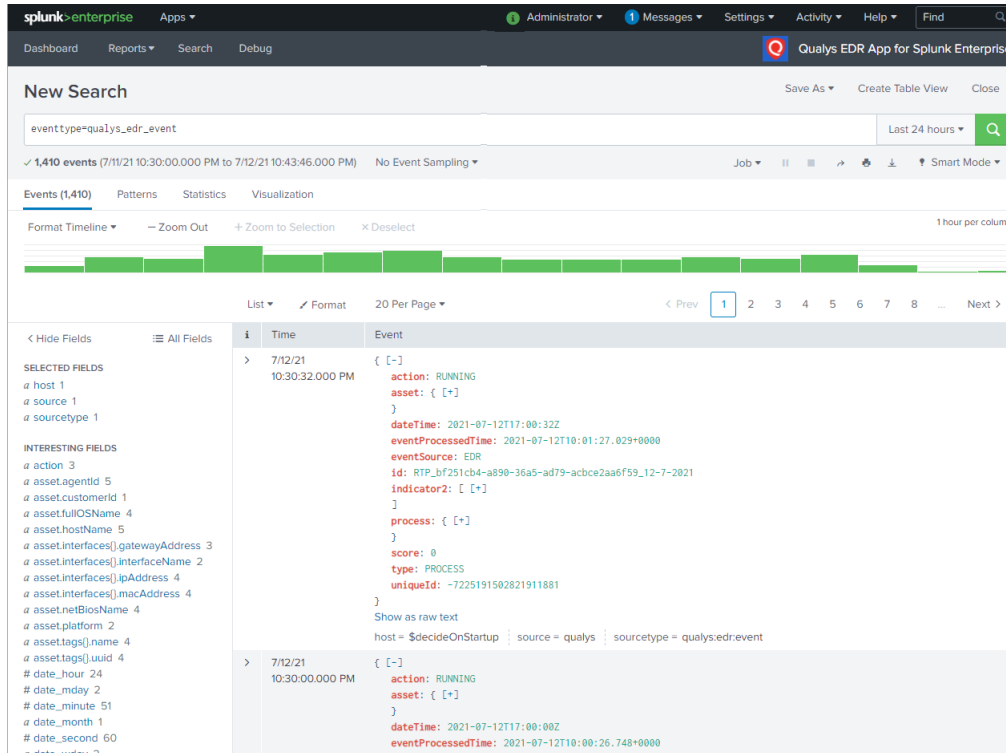
eventtype="qualys_fim_incident"

The screenshot displays the Splunk Search & Reporting interface. At the top, the navigation bar includes 'Search', 'Metrics', 'Datasets', 'Reports', 'Alerts', and 'Dashboards'. The 'Search' tab is active, showing a 'New Search' window. The search query 'eventtype="qualys_fim_incident"' is entered in the search bar, and the time range is set to 'Last 24 hours'. Below the search bar, a status bar indicates '1 event (6/24/19 3:30:00.000 PM to 6/25/19 4:00:44.000 PM)'. The 'Events (1)' tab is selected, showing a single event. The event details are displayed in a table with columns for 'Time' and 'Event'. The event is a FIM incident from 6/25/19 at 3:58:14.000 PM. The event data includes fields such as approvalDate, approvalStatus, approvalType, assignDate, changeType, comment, createdBy, customerId, deleted, dispositionCategory, filterFromDate, filterToDate, filters, id, lastUpdatedBy, marked, markupStatus, name, reviewers, and splunk_event_type.

Time	Event
6/25/19 3:58:14.000 PM	{ [-] approvalDate: 2019-03-29T14:58:13.376+0000 approvalStatus: UNAPPROVED approvalType: MANUAL assignDate: 2019-03-29T14:55:45.133+0000 changeType: MANUAL comment: dfbsadfgasg createdBy: { [+] } customerId: a6df6808-8c45-eb8c-e040-10ac13041e17 deleted: false dispositionCategory: PATCHING filterFromDate: 2019-02-01T05:00:00.000+0000 filterToDate: 2019-03-01T04:59:59.999+0000 filters: [[+]] id: e4ffcac4-c75b-46aa-8eac-fcd260bf286d lastUpdatedBy: { [+] } marked: true markupStatus: COMPLETED name: Services.exe Incident reviewers: [[+]] splunk_event_type: FIM_INCIDENT

Search EDR Data

You can search for specific EDR events that TA has pulled in Splunk from your Qualys account. Use `eventtype="qualys_edr_event"` or create your own SPL search query to filter the data.



The screenshot shows the Splunk Enterprise interface with the 'Qualys EDR App for Splunk Enterprise' loaded. A new search is being performed with the query `eventtype=qualys_edr_event`. The search results show 1,410 events. The interface includes a timeline visualization at the top and a list view below. The list view shows two events, both occurring on 7/12/21 at 10:30:00 PM. The first event is a 'RUNNING' action for an asset, with fields like `dateTime`, `eventProcessedTime`, `eventSource`, `id`, `indicator2`, `process`, `score`, `type`, and `uniqueId`. The second event is also a 'RUNNING' action for an asset, with fields like `dateTime` and `eventProcessedTime`.

Time	Event
7/12/21 10:30:32.000 PM	<pre>{ action: RUNNING asset: { } dateTime: 2021-07-12T17:00:32Z eventProcessedTime: 2021-07-12T10:01:27.029+0000 eventSource: EDR id: RTP_bf251cb4-a890-36a5-ad79-acbce2aa6f59_12-7-2021 indicator2: [] process: { } score: 0 type: PROCESS uniqueId: ~7225191502821911881 }</pre>
7/12/21 10:30:00.000 PM	<pre>{ action: RUNNING asset: { } dateTime: 2021-07-12T17:00:00Z eventProcessedTime: 2021-07-12T10:00:26.748+0000 }</pre>

Search Activity Log Data

You can search for specific Activity Log events that TA has pulled in Splunk from your Qualys account. Use `eventtype="qualys_activity_log_event"` or create your own SPL search query to filter the data.

The screenshot shows the Splunk Search interface. At the top, the header includes the Splunk logo, 'App: Search & Reporting', and a user profile for 'Administrator'. Below the header is a navigation bar with tabs for Search, Analytics, Datasets, Reports, Alerts, and Dashboards. The 'Search' tab is active, and the 'New Search' section shows the search query `eventtype="qualys_activity_log_event"`. Below the query bar, it indicates '13 events (before 7/16/20 12:32:30.000 PM)' and 'No Event Sampling'. The 'Events (13)' tab is selected, and a timeline view shows a bar for '8 events at 6 PM on Tuesday, July 14, 2020'. Below the timeline, a table view displays the search results. The table has columns for 'Time' and 'Event'. The first event is a login attempt on 7/15/20 at 10:59:16.000 AM. The event details are shown in a JSON-like format, including fields like Action, Date, Details, Module, User IP, User Name, and User Role. The event details are: `{ [-] Action: login Date: 2020-07-15T05:29:16Z Details: API: /msp/about.php Module: auth User IP: 103.216.98.78 User Name: qualys_qb59 User Role: Reader }`. Below the event details, there is a 'Show as raw text' link and a summary bar showing `host = localhost.localdomain | source = qualys | sourcetype = qualys:activityLog`.

Time	Event
7/15/20 10:59:16.000 AM	<pre>{ [-] Action: login Date: 2020-07-15T05:29:16Z Details: API: /msp/about.php Module: auth User IP: 103.216.98.78 User Name: qualys_qb59 User Role: Reader }</pre> <p>Show as raw text</p> <p>host = localhost.localdomain source = qualys sourcetype = qualys:activityLog</p>

Search Secure Enterprise Mobility Data

You can search for specific Secure Enterprise Mobility (SEM) events that TA has pulled in Splunk from your Qualys account. Use `eventtype="qualys_sem_asset_summary_event"` to fetch the asset information and `eventtype="qualys_sem_detection_event"` to fetch the asset detection information. You can create your own SPL search query to filter the data.

The Sample search shows asset information for asset summary event.

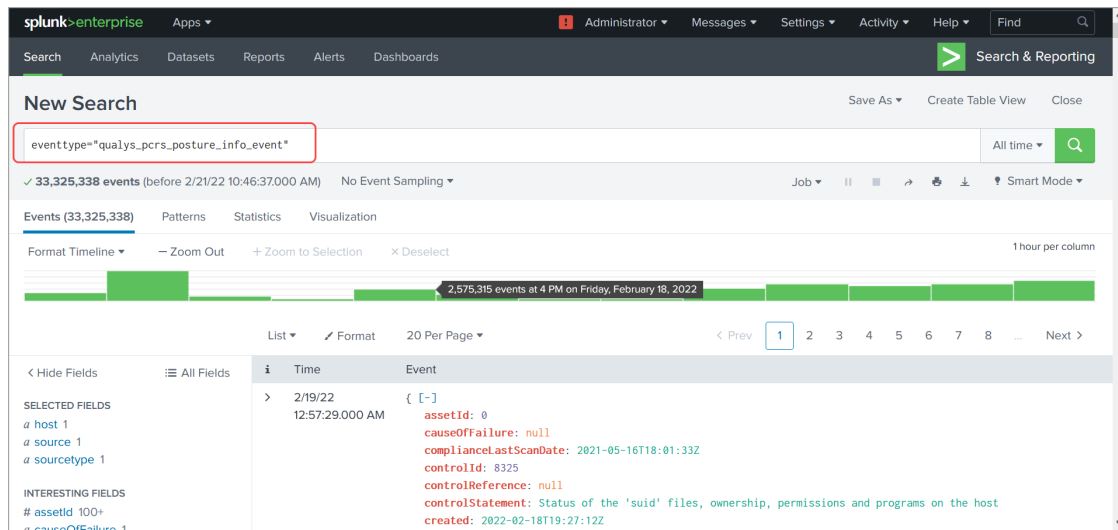
The screenshot shows the Splunk Search & Reporting interface. The search bar contains the query `eventtype="qualys_sem_asset_summary_event"`. The results are displayed in a table with columns for Time and Event. The table shows several events, including asset summary events for various devices like iPhones and Androids.

Time	Event
10/25/21 6:47:13.000 AM	<ASSET>=ID=2958/<ID=ASSET_FRIENDLY_NAME=sahirrao_iPhone_8_3_2021_10_46_AM_105_Apple/<ASSET_FRIENDLY_NAME>=OS=IOS/<OS=OS_VERSION=15.0/<OS_VERSION>=ASSET_STATUS=Enrolled/<ASSET_STATUS>=LAST_SEEN=2021-10-05 09:31:43/<LAST_SEEN>=OWNERSHIP=Corporate - Owned/<OWNERSHIP>=MODEL_NAME=IPhone 12/<MODEL_NAME>=MODEL_NUMBER=IPhone 12/<MODEL_NUMBER>=MANUFACTURER=Apple/<MANUFACTURER>=USER_NAME=sahirrao@qualysintegration.onmicrosoft.com/<USER_NAME>=</ASSET>
10/25/21 6:47:13.000 AM	<ASSET>=ID=2958/<ID=ASSET_FRIENDLY_NAME=sahirrao_iPhone_8_3_2021_11_10_AM_105_Apple/<ASSET_FRIENDLY_NAME>=OS=IOS/<OS=OS_VERSION=12.5.4/<OS_VERSION>=ASSET_STATUS=Enrolled/<ASSET_STATUS>=LAST_SEEN=2021-10-05 09:31:43/<LAST_SEEN>=OWNERSHIP=Corporate - Owned/<OWNERSHIP>=MODEL_NAME=IPhone 6/<MODEL_NAME>=MODEL_NUMBER=IPhone 6/<MODEL_NUMBER>=MANUFACTURER=Apple/<MANUFACTURER>=USER_NAME=sahirrao@qualysintegration.onmicrosoft.com/<USER_NAME>=</ASSET>
10/25/21 6:47:13.000 AM	<ASSET>=ID=2957/<ID=ASSET_FRIENDLY_NAME=sahirrao_AndroidForWork_8_3_2021_12_29_PM_Android4_Google/<ASSET_FRIENDLY_NAME>=OS=Android/<OS=OS_VERSION=9/<OS_VERSION>=ASSET_STATUS=Enrolled/<ASSET_STATUS>=LAST_SEEN=2021-10-05 09:31:43/<LAST_SEEN>=OWNERSHIP=Corporate - Owned/<OWNERSHIP>=MODEL_NAME=Pixel 2/<MODEL_NAME>=MODEL_NUMBER=Pixel 2/<MODEL_NUMBER>=MANUFACTURER=Google/<MANUFACTURER>=USER_NAME=sahirrao@qualysintegration.onmicrosoft.com/<USER_NAME>=</ASSET>
10/25/21 6:47:13.000 AM	<ASSET>=ID=2956/<ID=ASSET_FRIENDLY_NAME=sahirrao_AndroidForWork_7_10_2021_4_09_AM_Android4_Google/<ASSET_FRIENDLY_NAME>=OS=Android/<OS=OS_VERSION=9/<OS_VERSION>=ASSET_STATUS=Enrolled/<ASSET_STATUS>=LAST_SEEN=2021-10-05 09:31:43/<LAST_SEEN>=OWNERSHIP=Corporate - Owned/<OWNERSHIP>=MODEL_NAME=Pixel 2/<MODEL_NAME>=MODEL_NUMBER=Pixel 2/<MODEL_NUMBER>=MANUFACTURER=Google/<MANUFACTURER>=USER_NAME=sahirrao@qualysintegration.onmicrosoft.com/<USER_NAME>=</ASSET>
10/25/21 6:47:13.000 AM	<ASSET>=ID=2959/<ID=ASSET_FRIENDLY_NAME=sahirrao_iPhone_8_5_2021_5_18_AM_105_Apple/<ASSET_FRIENDLY_NAME>=OS=IOS/<OS=OS_VERSION=14.1/<OS_VERSION>=ASSET_STATUS=Enrolled/<ASSET_STATUS>=LAST_SEEN=2021-10-05 09:31:43/<LAST_SEEN>=OWNERSHIP=Employee - Owned/<OWNERSHIP>=MODEL_NAME=IPhone 12/<MODEL_NAME>=MODEL_NUMBER=IPhone 12/<MODEL_NUMBER>=MANUFACTURER=Apple/<MANUFACTURER>=USER_NAME=sahirrao@qualysintegration.onmicrosoft.com/<USER_NAME>=</ASSET>

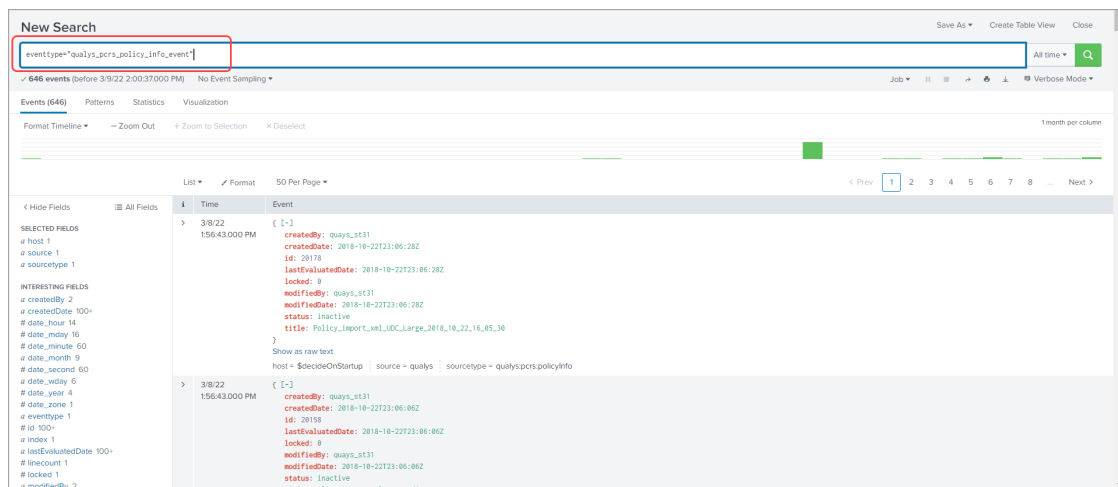
Search Policy Compliance Reporting Service Data

You can search for specific Policy Compliance Reporting Service (PCRS) events that TA has pulled in Splunk from your Qualys account. Use `eventtype="qualys_pcrs_posture_info_event"` to fetch the number of posture events, `eventtype="qualys_pcrs_policy_info_event"` to fetch the policy information and `eventtype="qualys_pcrs_policy_summary"` to fetch the policy summary. You can create your own SPL search query to filter the data.

The sample search shows posture info event.



The sample search shows policy info event.



The sample search shows policy summary.

New Search Save As Create Table View Close

eventtype="qualys_pcrs_policy_summary" All time Q

✓ 2 events (before 3/9/22 1:35:14.000 PM) No Event Sampling Job || + - Smart Mode

Events (2) Patterns Statistics Visualization

Format Timeline → Zoom Out + Zoom to Selection x Deselect 1 millisecond per column

List ✓ Format 20 Per Page

Hide Fields	All Fields	i	Time	Event
SELECTED FIELDS # host 1 # source 1 # sourcetype 1	INTERESTING FIELDS # eventtype 1 # FAILED 2 # index 1 # linecount 1 # NUMBER_OF_CONTROLS 2 # PASSED 2 # POLICY_ID 2 # punct 1 # splunk_server 1 # timestamp 1		3/9/22 12:53:37.000 PM	<pre>[-] FAILED: 73392 NUMBER_OF_CONTROLS: 441881 PASSED: 368489 POLICY_ID: 95473 } Show as raw text host = \$decideOnStartup source = qualys sourcetype = qualys:pcrs:policy_summary</pre>
			3/9/22 12:53:37.000 PM	<pre>[-] FAILED: 24432 NUMBER_OF_CONTROLS: 147181 PASSED: 122669 POLICY_ID: 92474 } Show as raw text host = \$decideOnStartup source = qualys sourcetype = qualys:pcrs:policy_summary</pre>

+ Extract New Fields

Search Cyber Security Asset Management Data

You can search for specific Cyber Security Asset Management (CSAM) assets that TA has pulled in Splunk from your Qualys account. Use below eventtypes

eventtype="qualys_csam_assets" to fetch the asset data,

eventtype="qualys_csam_businessApps" to business app data and

eventtype="qualys_csam_softwares" to fetch the software data.

You can create your own SPL search query to filter the data. The sample search shows CSAM assets.

New Search Save As Create Table View Close

eventtype="qualys_csam_assets" All time Q

✓ 88,212 events (before 10/16/23 3:57:52.000 PM) No Event Sampling Job || + - Fast Mode

Events (88,212) Patterns Statistics Visualization

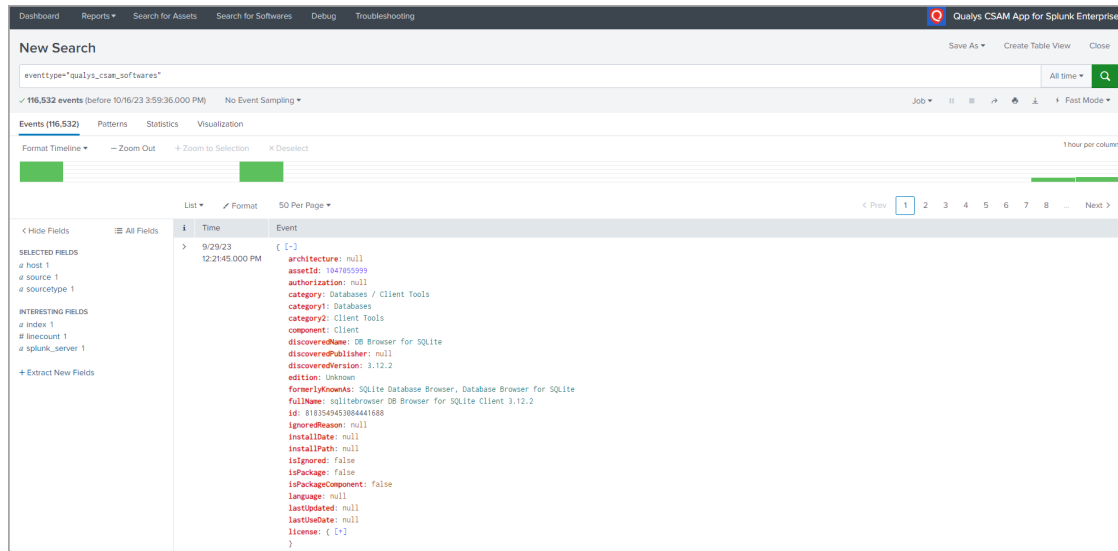
Format Timeline → Zoom Out + Zoom to Selection x Deselect 1 hour per column

List ✓ Format 50 Per Page < Prev 1 2 3 4 5 6 7 8 ... Next >

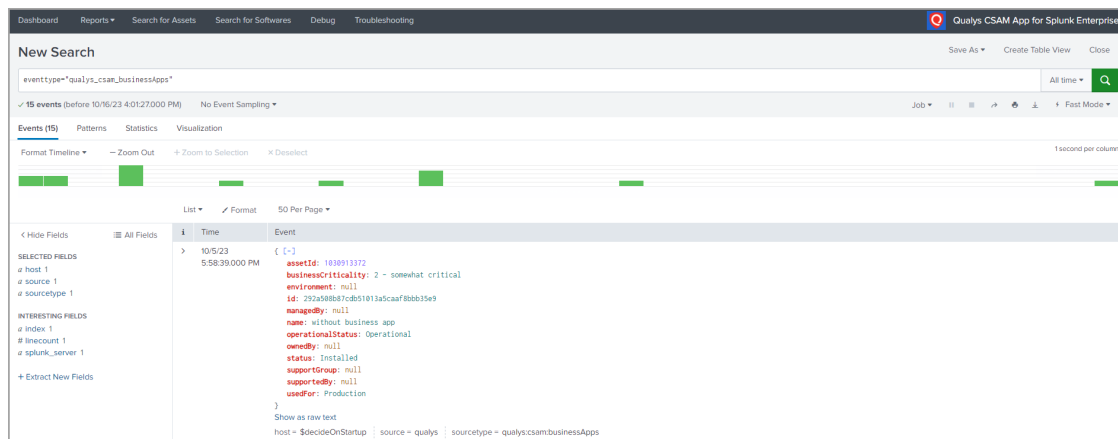
Hide Fields	All Fields	i	Time	Event
SELECTED FIELDS # host 1 # source 1 # sourcetype 1	INTERESTING FIELDS # index 1 # linecount 1 # splunk_server 1		9/29/23 12:21:49.000 PM	<pre>[-] activity: { [-] } address: agent: { [+] } agentId: null asn: null assetId: 1048920090 assetName: 5736418723812140778 assetType: HOST assetUUID: e782ef97-0b3e-41ff-aaaf-4ccfd2e8bde8 assignedLocation: null biosAssetTag: biosDescription: null biosSerialNumber: businessAppListData: null businessInformation: null cloudProvider: { [-] } container: { [+] } cpuCount: 0 createdDate: 2023-09-28T10:51:54.000Z criticality: { [+] } }</pre>

+ Extract New Fields

The sample search shows CSAM software assets.



The sample search shows CSAM business application.




Search CertView Data

You can search for specific CertView data that TA has pulled in Splunk from your Qualys account. Use following eventtype


`eventtype="qualys_certview_certificates"` to fetch the certificate information.

You can create your own SPL search query to filter the data.

The sample search shows Certview certificates.

Dashboard Reports Search Debug Troubleshooting  Qualys Certview App for Splunk Enterprise

New Search Save As Create Table View Close

eventtype="qualys_certview_certificates" All time 

✓ 51,332 events (before 10/16/23 4:25:59.000 PM) No Event Sampling Job Format Fast Mode

Events (51,332) Patterns Statistics Visualization

Format Timeline Zoom Out Zoom to Selection Deselect 1 hour per column

List Format 50 Per Page Prev 1 2 3 4 5 6 7 8 Next

	Time	Event
<div>< Hide Fields</div> <div>≡ All Fields</div> <div>SELECTED FIELDS</div> <div>• host 1</div> <div>• source 1</div> <div>• sourcetype 1</div> <div>INTERESTING FIELDS</div> <div>• index 1</div> <div>• linecount 1</div> <div>• splunk_server 1</div> <div>+ Extract New Fields</div>	> 10/16/23 11:54:40.000 AM	{ [-] assetCount: 1 assets: { [-] } } certHash: 03f64b5c71f15c04e0ff0b00fda7bd136db9a2a1f0970996230f6a97acc14 createdDate: 2023-10-16T06:07:39.000+00:00 dn: CN=www10e1511e4d extendedValidation: false id: 19072013 imported: false instanceCount: 1 issuer: { [-] } } issuerCategory: Self-Signed keySize: 2048 lastFound: 1697433450000 selfSigned: true serialNumber: 151a306a0be1f6804353abc027cde355 signatureAlgorithm: SHA256withRSA sources: { [-] } } subject: { [-] } } updateDate: 2023-10-16T06:07:39.000+00:00 validFrom: 1697261960000 validFromDate: 2023-10-14T05:39:28.000+00:00

Event Types for Searching Your Apps Data

Here is the list of default event types for Qualys Apps. You can use these event types when searching your Apps data in Splunk.

Note - If the customer has used custom index then replace {INDEX_NAME} with custom index name else replace with main.

Event Types for VM Detection Data

- Event Type Name - qualys_vm_detection_event

Search Query - index={INDEX_NAME} (sourcetype="qualys:hostDetection" OR sourcetype="qualys_vm_detection") "HOSTVULN"

- Event Type Name - qualys_host_summary_event

Search Query - index={INDEX_NAME} (sourcetype="qualys:hostDetection" OR sourcetype="qualys_vm_detection") "HOSTSUMMARY"

Event Types for WAS Findings Data

- Event Type Name - qualys_was_finding_event

Search Query - index={INDEX_NAME} sourcetype="qualys:wasFindings" "WAS_FINDING"

- Event Type Name - qualys_was_summary_event

Search Query - index={INDEX_NAME} sourcetype="qualys:wasFindings" "WAS_SUMMARY"

Event Types for Policy Compliance Data

- Event Type Name - qualys_policy_info_event

Search Query - index={INDEX_NAME} sourcetype="qualys:pc:policyInfo" "POLICY_INFO"

- Event Type Name - qualys_posture_info_event

Search Query - index={INDEX_NAME} sourcetype="qualys:pc:postureInfo" "POSTURE_INFO"

- Event Type Name - qualys_policy_summary_event

Search Query - index={INDEX_NAME} sourcetype="qualys:pc:postureInfo" "POLICY_SUMMARY"

Event Types for Container Security Data for Images

- Event Type Name - cs_image_info_event

Search Query - index={INDEX_NAME} sourcetype="qualys:cs:csimageinfo" "IMAGE_INFO"

- Event Type Name - cs_vuln_info_event

Search Query - index={INDEX_NAME} sourcetype="qualys:cs:csimagevulninfo"
"VULN_INFO"

- Event Type Name - cs_vuln_summary_event

Search Query - index={INDEX_NAME} sourcetype="qualys:cs:csimagevulninfo"
"VULN_SUMMARY"

Event Types for Container Security Data for Containers

- Event Type Name - qualys_cs_container_details

Search Query - index={INDEX_NAME} sourcetype="qualys:cs:container"
"CONTAINER_DETAILS"

- Event Type Name - qualys_cs_container_vuln

Search Query - index={INDEX_NAME} sourcetype="qualys:cs:containerVuln"
type=CONTAINER_VULN

- Event Type Name - qualys_cs_container_vuln_summary

Search Query - index={INDEX_NAME} sourcetype="qualys:cs:containerVuln"
type=CONTAINER_VULN_SUMMARY

Event Types for FIM Data for Events, Ignored Events, and Incidents

- Event Type Name - qualys_fim_event

Search Query - index={INDEX_NAME} sourcetype="qualys:fim:event"
splunk_event_type=FIM_EVENT

- Event Type Name - qualys_ignored_fim_event

Search Query - index={INDEX_NAME} sourcetype="qualys:fim:ignored_event"
splunk_event_type=FIM_IGNORED_EVENT

- Event Type Name - qualys_fim_incident

Search Query - index={INDEX_NAME} sourcetype="qualys:fim:incident"
splunk_event_type=FIM_INCIDENT

Event Types for Endpoint Detection and Response Data

- Event Type Name - qualys_edr_event

Search Query - index={INDEX_NAME} source="qualys"
sourcetype="qualys:ioc:ioceventinfo" OR sourcetype="qualys:edr:event"

Event Types for Activity Log Data

- Event Type Name - qualys_activity_log_event

Search Query - index={INDEX_NAME} sourcetype="qualys:activityLog"

Event Types for Secure Enterprise Mobility

- Event Type Name - qualys_sem_asset_summary_event

Search Query - index={INDEX_NAME} sourcetype="qualys:sem:asset_summary"

- Event Type Name - qualys_sem_detection_event

Search Query - index={INDEX_NAME} sourcetype="qualys:sem:detection"

Event Types for Policy Compliance Reporting Service

- Event Type Name - qualys_pcrs_policy_info_event

Search Query - index={INDEX_NAME} sourcetype="qualys:pcrs:policyinfo"

- Event Type Name - qualys_pcrs_policy_summary

Search Query - index={INDEX_NAME} sourcetype="qualys:pcrs:policy_summary"

- Event Type Name - qualys_pcrs_posture_info_event

Search Query - index={INDEX_NAME} sourcetype="qualys:pcrs:postureinfo"

Event Types for Cyber Security Asset Management

- Event Type Name - qualys_csam_assets

Search Query - index={INDEX_NAME} sourcetype="qualys:csam:assets"

- Event Type Name - qualys_csam_businessApps

Search Query - index={INDEX_NAME} sourcetype="qualys:csam:businessApps"

- Event Type Name - qualys_csam_softwares

Search Query - index={INDEX_NAME} sourcetype="qualys:csam:softwares"

Event Types for CertView

- Event Type Name - qualys_certview_certificates

Search Query - index={INDEX_NAME} sourcetype="qualys:certview:certificates"

App Management & Troubleshooting

APP Management

How to Remove the app

1) Stop Qualys App for Splunk Enterprise:

```
$SPLUNK_HOME/bin/splunk stop
```

2) Remove Qualys App for Splunk Enterprise:

```
$SPLUNK_HOME/bin/splunk remove app TA-QualysCloudPlatform -auth  
username:password
```

Note: To remove the TA app from Splunk cloud, raise a ticket with Splunk Support.

Utility script to Clean up Left-over XML and PID Files

You'll sometimes see orphan XML files in the TA-DIR/tmp directory when TA has errors, for example while calling the API, getting the response stream or parsing the API response. While running the utility, you can provide command line options to specify data input(s) for the XML files to be cleaned up. The utility deletes all the XML files related to the chosen data input(s), except those belonging to currently running TA processes.

Example 1: Help: Use the below command to understand how utility script can be used for specific data inputs

```
my-user@my-host:$SPLUNK_HOME/etc/apps/TA-QualysCloudPlatform#  
$SPLUNK_HOME/bin/splunk cmd python ./bin/cleanup.py --help
```

Example 2: Delete Host Detection and WAS Findings XML

```
my-user@my-host:$SPLUNK_HOME/etc/apps/TA-QualysCloudPlatform#  
$SPLUNK_HOME/bin/splunk cmd python ./bin/cleanup.py --hd --was
```

Example 3: Delete XML files belonging to all data inputs

```
my-user@my-host:$SPLUNK_HOME/etc/apps/TA-QualysCloudPlatform#  
$SPLUNK_HOME/bin/splunk cmd python ./bin/cleanup.py --all
```

Know important file paths in Splunk

File	Path
Index	\$SPLUNK_HOME/etc/apps/TA-QualysCloudPlatform/default/eventtype.conf
KB lookup	\$SPLUNK_HOME/etc/apps/TA-QualysCloudPlatform/lookups/qualys_kb.csv
API Credential	\$SPLUNK_HOME/etc/apps/TA-QualysCloudPlatform/local/passwords.conf
Qualys TA Configuration	\$SPLUNK_HOME/etc/apps/TA-QualysCloudPlatform/local/qualys.conf
Qualys TA log	\$SPLUNK_HOME/var/log/splunk/ta_QualysCloudPlatform.log
Check point	\$SPLUNK_HOME/var/lib/splunk/modinputs/qualys

Troubleshooting

Looking for logs?

Qualys logs are populated in Splunk's index "_internal". Use this search to find logs:

```
index=_internal source="$SPLUNK_HOME/var/log/splunk/ta_QualysCloudPlatform.log"
```

Troubleshooting the setup

- Be sure to enter the proper [API Server URL](#) for the configuration.
- Verify you can reach the API from the Splunk Search Head where you installed Qualys App for Splunk Enterprise (no firewall or other infrastructure).
- Be sure the Qualys user account you're using to connect has API access. Edit the user account in the Qualys UI and select the API access check box in the user settings. Don't see this option? Reach out to Qualys Support or your Technical Account Manager.

Updated TA Setup Page does not reflect

If you are not able to see the updated TA Setup page, then clear the Cache and perform a hard Reload to view the changes.

Check that API calls are being made

In the Splunk setup where failing account is used, run the following search to see if API calls are being made to Qualys APIs:

```
index=_internal source="$SPLUNK_HOME/var/log/splunk/ta_QualysCloudPlatform.log"
("/api/2.0/fo/asset/host/vm/detection/" OR "/api/2.0/fo/knowledge_base/vuln/" OR
"/api/2.0/fo/compliance/posture/info/" OR "/qps/rest/3.0/search/was/finding")
```

Check that data feed is enabled

If you don't see any entry for the API call, then check that the data input was added and enabled.

- If not enabled, please enable it.
- If enabled, and you still don't see any records for the API call, please check the TA installation directory. If you find the host_detection.pid file in the installation directory, delete it.

Note that you should see entries for the /api/2.0/fo/knowledge_base/vuln/ API call.

Check error logs

If everything is fine (inputs added and enabled; API calls are made) and you still don't have data, please check "_internal" index for errors logged for TA-QualysCloudPlatform.

Run the following search and provide error logs to Qualys Support:

```
index=_internal source="$SPLUNK_HOME/var/log/splunk/ta_QualysCloudPlatform.log"
ERROR:
```

Delete the checkpoint file and pull the data again for a Qualys module

Navigate to \$SPLUNK_HOME/var/lib/splunk/modinputs/qualys/. Delete the checkpoint file of the desired module. For example, Delete 'host_detection' file for module Host Detection and initiate the pull once again. TA now pulls the data from the date configured in Data Input Settings for the respective Qualys module.

qualys.py is running even after the data input is disabled or Splunk is restarted

This issue is seen mostly on Ubuntu OS, that has default shell set to 'dash'. To fix this issue, set the default shell from 'dash' to 'bash'.

Steps to change the Ubuntu configuration:

- 1) ~# debconf-show dash
* dash/sh: true
- 2) ~# debconf-set-selections <<< "dash dash/sh string false"
- 3) ~# debconf-show dash
* dash/sh: false
- 4) ~# dpkg-reconfigure -f noninteractive dash

Removing 'diversion of /bin/sh to /bin/sh.distrib by dash'

Adding 'diversion of /bin/sh to /bin/sh.distrib by bash'

Removing 'diversion of /usr/share/man/man1/sh.1.gz to /usr/share/man/man1/sh.distrib.1.gz by dash'

Adding 'diversion of /usr/share/man/man1/sh.1.gz to /usr/share/man/man1/sh.distrib.1.gz by bash'

- 5) ~# debconf-show dash
* dash/sh: false

How to switch python interpreter for Python3?

- 1) Goto the path - \$SPLUNK_HOME/etc/system/local/server.conf
- 2) Add the python.version=python3 under [general].

```
[general]
serverName = localhost.localdomain
pass4SymmKey = $7$Z03cCfEXoKvcETwaVM2FccRz6Wge4vUY0MEuycaGvZWzibpIg2rt2w==
python.version = python3
```

- 3) Restart the Splunk.

Blank dashboard for the KnowledgeBase data

Perform these steps to identify and troubleshoot the issue:

- Check whether the correct index is used in the SPL added for the scheduled saved search.

- In case you disabled indexing after enabling it earlier, then check whether the scheduled saved search is also disabled as it is running for the index in which data is not updated.
- Go to the Settings > Lookups > Lookup table files and on the Lookup table files page select "All" from the App drop-down field. Check `qualys_kb.csv` is generated for which app. On enabling the indexing, the file should be present for 'search' app and on disabling the indexing, the file should be present for 'TA-QualysCloudPlatform' app. If `qualys_kb.csv` is present for any other app, then you should delete the file for that app else you may get to see blank KnowledgeBase dashboard.

Working logic of VM And PCRS Maximum API retry count in VM Detection Settings And Policy Compliance Reporting Service Settings

VM Detection Settings

- If TA receives the expected 429 Client Error: Too Many Requests while running `host_detection` data input, the retry count increases, regardless of the maximum retry limit set in the TA setup page under VM Detection settings.
- If the TA encounters an error other than 429 Client Error: Too Many Requests, the configured maximum retry limit is considered, and the number of retry counts matches the configured value of Host List Detection maximum API retry count on the TA setup page, the Host Ids or Host Id range for that specific API request is skipped, and it proceeds further.

Policy Compliance Reporting Service Settings



- If TA receives a 429 Client Error: Too Many Requests while running `pcrs_posture_info` data input, the retry count increases, regardless of the maximum retry limit configured in the TA setup page under PCRS settings.
- If TA encounters an error other than 429 Client Error: Too Many Requests, the configured maximum retry limit is considered, and the number of retry counts matches the configured value of PCRS maximum API retry count on the TA setup page, the batch size for that specific API request is skipped, and it proceeds further.

URL to the Qualys API Server

The Qualys API URL you should use for API requests depends on the Qualys platform where your account is located.

Click [here](#) to identify your Qualys platform and get the API URL.

You can easily find the API server URL for your account. Log in to your Qualys account and go to Help > About. You'll see this information under Security Operations Center (SOC).

AboutLaunch Help

General Information >
Identified Services >
Identified OS >
Additional References >

General Information

Qualys Web Service

Application Version:	8.9.0.2-2
Online Help Version:	8.9.29-1
SCAP Module Version:	1.2

Qualys External Scanners

Security Operations Center (SOC):	64.39.96.0/20 (64.39.96.1-64.39.111.254)
Scanner Version:	9.0.29-1
Vulnerability Signature Version:	2.3.492-2
Scanner Services	3.0.12-1

Qualys Scanner Appliances

Security Operations Center (SOC):	- qualysguard.qualys.com:443
	- qualysapi.qualys.com:443
	- dist01.sjdc01.qualys.com:443
	- nochohost.sjdc01.qualys.com:443
	- scanservice1.qualys.com:443
	- all in 64.39.96.0/20

What's New

New Feature in 1.11.4

With this release, we have enhanced Endpoint Detection and Response Settings in TA setup page.

We have added following options:

- Checkbox for Enable multi-threading to download EDR events
- Number of threads field for multithreading to pull EDR events in lesser time
 - Loop for each date range to get the counts with the count API. If a date range contains events, then the start date of the data range is the checkpoint date.
 - Again divide the data range with newer checkpoint date as per provided thread for example, $18\text{hr}/10 = 1.8\text{ hr}$. In this way 10 threads are running to pull the 1.8 hr data each.
- The EDR API are changed to `/ioc/events/searchAfter`
 - First API call do not have any value for the searchAfter parameter.
 - For next API calls pass searchaftervalues from the response header of previous request to searchAfterValues field of input parameter.
 - The searchAfter parameter values are from previous request's header.

For details, refer to [Endpoint Detection and Response Settings](#) section.

Note: Checkpoint files are individually created for each thread under the `edr_events_cp_folder`, containing their respective date ranges. Additionally, a checkpoint file is generated for the input `edr_event` data. These files facilitate comparison between the checkpoint files of each thread and the main checkpoint file, enabling the selection of the latest date range to initiate the next data pull.

New Feature in 1.11.3

With the new release, we have enhanced the functionality of **Host IDs** field under **VM Detection - Advanced Settings** in **VM Detection Settings** in TA setup page.

For more details, refer to What are [What are VM Detection-Advanced Settings?](#) section.

New Feature in 1.11.2

With this release, we have added the following enhancements:

- We have added **Host List Detection Maximum API retry count** field under **VM Detection Settings** in TA setup

For more details, refer to [Tell me about Host List Detection Maximum API Retry Count](#).

- We have added **Kill Existing PID** in TA Setup. If an earlier process ID (PID) has been stopped for some reason, but the process itself has not been killed, you can use the following steps to kill the PID. First, provide the PID number and then enable the checkbox. This allows you to kill the PID and proceed with a new PID in the next cron schedule. To kill existing PID, you need to enter PID manually under Kill Existing PID on TA Setup.

New Feature in 1.11.1

With the new release, we have added **Host IDs** field and **Enable to preserve Host Asset API response** checkbox under **VM Detection - Advanced Settings** in VM Detection Settings in TA setup page.

For more details, refer to [What are VM Detection-Advanced Settings?](#)

New Feature in 1.11.0

The Qualys Splunk TA 1.11.0 requires a minimum supported version of Splunk v8.x.

Integration of the Qualys Cyber Security Asset Management with Splunk TA

We have now integrated Qualys Cyber Security Asset Management (CSAM) with Splunk TA. You can now configure the TA app to fetch your CSAM data from your Qualys account.

CSAM fetches data continuously in the following manner:

- 1) Once you enable the data input, it pulls the count API to get total number of assets which is updated after asset last updated datetime.
- 2) Then it calls search API to pull all the assets as per asset last updated datetime and specified parameters.

We added a new Cyber Security Asset Management Settings section on the TA setup page where you can specify:

- Log User Accounts
- Log Open Ports
- Log File System Volume
- Log Network Interfaces
- Log Software
- Log Tags
- Log Hardware
- Log Operating System
- Log Business App List Data
- Exclude Unmanaged Assets
- Page size
- Extra filters for CSAM API

- CSAM Maximum API retry count

For details, refer to [Cyber Security Asset Management Settings](#).

We also added a new Qualys Metrics **cyber_security_asset_management** that you can use to create a cron job to pull your CSAM data.

Integration of the Qualys CertView with Splunk TA

We have now integrated Qualys Certview with Splunk TA. You can now configure the TA app to fetch your Certview data from your Qualys account.

CertView fetches data continuously. Once you enable the data input, it pulls the certificates which is updated after certificate updated datetime.

We added a new Certview Settings section on the TA setup page where you can specify:

- Page size
- Extra filters for CertView API
- CertView custom operation
- CertView Custom Fields
- Certview Maximum API retry count

For details, refer to [Certview Settings](#) section.

We also added a new Qualys Metrics **certview_certificates** that you can use to create a cron job to pull your Certview data.

Minimum supported Splunk version for Qualys Splunk TA 1.11.0 is Splunk v8.x

From this release we are not removing qualys_kb.csv file from the search/lookups automatically if user disables KB indexing option after enabling it first as per Splunk's recommendation. Users need to remove it manually. For more details, refer to [What happens when you disable KB indexing option after enabling it first?](#)

New Feature in 1.10.15

With this release, we have added following enhancements:

Parsing Newly Added Fields for following APIs in Splunk TA

Host List API

- LAST_ACTIVITY
- LAST_BOOT
- SERIAL_NUMBER
- HARDWARE_UUID
- FIRST_FOUND_DATE
- AGENT_STATUS
- CLOUD_AGENT_RUNNING_ON

Host List Detection API

- UNIQUE_VULN_ID

To get the UNIQUE_VULN_ID, add UNIQUE_VULN_ID in Detection fields to log under VM Detection Settings in TA setup page.

Renaming ARS Field Names to TRURISK

The fields ARS and ARS_FACTORS are changed to TRURISK_SCORE and TRURISK_SCORE_FACTORS respectively.

New Feature in 1.10.14

In TA setup page under the Policy Compliance Reporting Service Settings, we have removed **Do you want to enable SSL Certificate Verification?** checkbox. Now SSL certificate verification is enabled by default for PCRS. In a recent policy change, Splunk no longer allows disabling SSL certificates to ensure secure connections.

If there is an error with the SSL certificate for PCRS data input, ensure that your API connection is secured with SSL.

New Feature in 1.10.12

We fixed an issue where the user faced data missing in Splunk TA when making the API call. The issue of parsing blank spaces in the streaming posture data for PCRS data input has been resolved.

New Feature in 1.10.11

With the new release, we have extended our support to CIM-5.x for CS and SEM data input.

We have fixed the issue where TA encounters an error if an XML tag had a blank value for host detection input data.

New Feature in 1.10.10

We fixed the issue for the TruRisk factors parsing in the **host_detection** data input. It was not parsing in the previous version.

New Feature in 1.10.9

With the new release, we have added following enhancements:

Introduced Parallelism into PCRS Data Input:

- We introduced two separate multi-threads, ResolveHostThread and PostureStreamingThread, to call the Resolve Host Ids API and the Posture Streaming API.

ResolveHostThread can select a batch of policies, the batch size defined in the number of policy Ids to use for the Resolve Host Ids API field, and each thread ResolveHostThread-1, ResolveHostThread-2, ResolveHostThread-3, and so on, can make the Resolve Host Id API call.

The Resolve Host Ids can be added to the Host Id queue once the thread completes the pull. The PostureStreamingThread can immediately pick it. Each thread PostureStreamingThread-1, PostureStreamingThread-2, PostureStreamingThread-3, etc., can make the Resolve Posture Streaming API call.

As a result, the Resolve Host Id API and Posture Streaming API can pull data in parallel, and data pull can be faster compared to the previous method.

Parsing isIgnored Field for WAS Findings:

We are now parsing the isIgnored tag and ingesting it into WAS finding events.

- A few minor bug fixes are made.

New Feature in 1.10.8

With the new release, we have added below enhancements:

Parsing TruRisk Fields for Host Detection:

We are now parsing **ARS**, **ACS** and **ARS_FACTORS** and adding it into VM detection events. To get the **ARS**, **ACS** and **ARS_FACTORS**, check the **ARS**, **ACS** and **ARS_FACTORS for Host Asset API** checkbox provided under VM Detection Settings in TA setup page.

We are parsing **QDS** and **QDS_FACTORS** and adding it into VM detection events. To get the **QDS**, add "QDS" in "Detection fields to log" add "show_qds=1" in the extra parameter under VM Detection. To get the **QDS_FACTORS**, add "QDS_FACTORS" in "Detection fields to log" and add "show_qds_factors=1".

Parsing HOSTNAME field for Host Detection:

We are now parsing HOSTNAME and adding it into VM Detection Events.

New Settings under Policy Compliance Reporting Service

We have introduced the following settings under Policy Compliance Reporting Service settings on the TA setup page:

- Do you want to truncate the evidence?
- Do you want to enable SSL Certificate Verification?
- Number of threads to use for PCRS (max 10)
- PCRS Maximum API retry count
- PCRS Custom Policy Ids
- PCRS custom policy operation (include/exclude)

For more details, refer to the [Policy Compliance Reporting Service Settings](#) section.

New Feature in 1.10.7

With the new release, we have added the support for Truncation Limit under Policy Compliance Reporting Service Settings in TA setup page.

For more details, refer to **Policy Compliance Reporting Service Settings** section.

New Feature in 1.10.6

With the new release, we have added **Host Ids Batch size for Posture Info Streaming API** field under Policy Compliance Reporting Service Settings in TA setup page.

For more details, refer to **Policy Compliance Reporting Service Settings** section.

We are parsing CLOUD_PROVIDER_TAGS and adding in the VM events in CLOUD_PROVIDER_TAGS_name1 = val1, CLOUD_PROVIDER_TAGS_name2 = val2... format.

To get the CLOUD_PROVIDER_TAGS, add "CLOUD_PROVIDER_TAGS" in "host fields to log" field and add "show_cloud_tags=1" in the extra parameter under VM Detection

Settings in TA setup page.

Also, some minor improvements in logging are made.

New Feature in 1.10.5

We are now compatible with SPLUNK v9.0 and minor improvements added are as follows:

- Parsing ASSET_ID tag and adding in VM events:

With the new release, we are parsing ASSET_ID tag and adding it to the VM events.

To get the ASSET_ID, add "show_asset_id=1" in the extra parameter under VM Detection Settings in TA setup page.

- Additional fields added to the KB CSV File are as follows:

- AUTHENTICATION
- DISCOVERY_REMOTE
- LAST_SERVICE_MODIFICATION_DATETIME
- SUPPORTED_MODULES

- Parsing IPV6 tag and adding in VM events:

With the new release, TA parses the IPV6 tag (if its present in XML) and ingests into VM events. If the tag is not present, then IPV6 field will not be present in the event ingested to Splunk. If tag is present but value is empty/null/None, then empty string will be present in the event.

i	Time	Event
>	8/13/22 12:51:38.000 PM	HOSTSUMMARY: HOST_ID=43267, IPV6="2601:f0f1:f666:247c::a73:7c96", TRACKING ED_DATE="2022-08-13T07:21:26Z", LAST_VH_SCANNED_DURATION="268", SEVERITY_1 INITIAL_FIXED=0, POTENTIAL_NEW=0, CONFIRMED_NEW=0, CONFIRMED_1=0, POTENTIAL =0, _SEVERITY_3=10, CONFIRMED_SEVERITY_3=1, CONFIRMED_SEVERITY_3=2, CONF

VM Detection Settings

☒ Log Host Summary events

☒ Log extra statistics in host summary (Breakdown of Vulnerability Count by (Severity and Type), by (Severity and Status)

☒ Log Individual Host Vulnerabilities

☒ Log host information with each detection (e.g. IP, OS, DNS, NetBios)

Host fields to log

ID,ASSET_ID,IP,IPV6,TRACKING_METHOD,DNS,NETBIOS,OS,LAST_SCAN_DATETIME,TAGS,NETWORK_ID,

Enter host XML tag names from API response to be logged in the event by a comma-separated. (e.g. ID,IP,TRACKING_METHOD,DNS)

New Feature in 1.10.4

In TA v1.10.4, we included a new parameter in the VM detection API call that is **"detection_updated_since"**. This parameter will filter out the QID whose status does not change since the datetime mentioned with this parameter.

New Feature in 1.10.2

The new release comes with improvements in logging and minor enhancements in utility script.

New Feature in 1.10.1

Integration of the Qualys Policy Compliance Reporting Service with Splunk TA

We have now integrated Qualys Policy Compliance Reporting Service (PCRS) with Splunk TA. You can now configure the TA app to fetch your PCRS data from your Qualys account.

The PC APIs also pull the posture data, but due to hindrances such as CPU usage, memory consumption, and time consumption to pull the complete information, we introduced PCRS for TA apps.

PCRS improves the data fetching of the huge data on the Qualys Cloud. Fetching data in PCRS is quicker for the accounts with millions of assets and postures.

PCRS fetches data continuously in the following manner:

- 1) Once you enable the data input, it will first pull the number of Policy IDs to the subscription ID.

- 2) Divides the Policy IDs into threads and starts pulling the associated hosts.
- 3) Calls the posture data for all the hosts associated to the policy IDs.

We added a new Policy Compliance Reporting Service Settings section on the TA setup page where you can specify:

- Add additional field evidence
- Add the number of policy Ids that can be used in Resolve Host Id API.

For more details, refer to [Policy Compliance Reporting Service Settings](#) section.

The screenshot shows the 'Policy Compliance Reporting Service Settings' section. It includes a checkbox labeled 'Add additional field evidence' which is currently unchecked. Below this is a text input field labeled 'Number of Policy Ids to use for Resolve Host Ids API (max 10)' with the value '2' entered.

We also added a new Qualys Metrics “pcrs_posture_info” that you can use to create a cron job to pull your PCRS data.

The screenshot shows the 'Add Data' interface in Splunk Enterprise. On the left, under 'Files & Directories', the 'Qualys Technology Add-On' is highlighted with a red box. On the right, the 'Qualys Metrics' dropdown menu is open, showing a list of metrics. The 'pcrs_posture_info' metric is highlighted with a red box. Below the metrics list, the 'Start Date' field is visible, with a note indicating the format for the date should be in UTC in ISO 8601 format: "YYYY-MM-DDThh:mm:ss.msZ".

New Feature in 1.9.0

Integration of the Qualys Secure Enterprise Mobility with Splunk TA

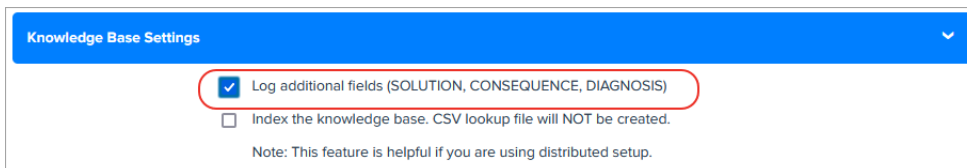
With this release, we integrated Qualys Secure Enterprise Mobility (SEM) with Splunk TA. You can now configure TA app to fetch your SEM data from your Qualys account.

On the TA setup page, we added a new Security Enterprise Mobility Settings section where you can specify: 1) the SEM data that you want to fetch from your account, 2) the number of records that you want to fetch per API request, and 3) extra params, if any. See [Secure Enterprise Mobility Settings](#).

We also added a new Qualys Metrics “sem_detection” that you can use to create a corn job to pull your SEM data. The start date for Qualys Metrics should be in “YYYY-MM-DDThh:mm:ssZ” and cannot be less than the default date “2021-01-26T00:00:00Z”.

View Diagnosis, Consequence, and Solution information in KB data in Splunk

We added a new check box in the KnowledgeBase Settings section on the TA setup page. When you select this check box, TA will fetch the Diagnosis, Consequence, and Solution information in the Splunk along with the other KB data. When you search for the KB data in Splunk, the new Diagnosis, Consequence, and Solution columns will show the information in the respective columns.



Improvements in 1.8.9

Indication of Compromise (IOC) App rebranded as Endpoint Detection and Response (EDR)

With this release, Indication of Compromise (IOC) App will be known as Endpoint Detection and Response (EDR) in Qualys TA. Because of this change, we replaced all the instances of IOC on TA UI (labels, IOC data input), log messages with EDR.

If you are using IOC data input and choose to upgrade to TA 1.8.9, we will show you a warning message in the TA log for IOC data input. The warning message will inform that IOC data input is deprecated and you need to manually configure the EDR data input from the Splunk UI.

If you are using IOC data input and if you enable the new EDR data input, we check if IOC data checkpoint is available or not. After the check, If we find IOC checkpoint file and do not find EDR check point file then TA will rename the IOC checkpoint file to the EDR checkpoint file and consider IOC checkpoint as the start date to fetch the data for the EDR data input.

If both the IOC and EDR checkpoint is available then TA will fetch the data from the EDR checkpoint file and ignore the IOC checkpoint file.

We removed the event types of IOC data input. The new event type name for EDR data input is "qualys_edr_event". For backward compatibility that is to make the older IOC data available in Splunk along with the EDR data, we have merged the IOC and EDR source types into a EDR event type. When you use the EDR event type, we will fetch older IOC data for IOC data input and latest EDR data for EDR data input.

Note

As IOC App is deprecated, you need to manually add EDR and remove the IOC data input.

Issues Fixed

TA setup changes for Qualys API credentials

We had an issue where the users using multiple technology add ons of different organizations were unable to configure username and password from the TA setup page.

We fixed this issue by setting TA-QualysCloudPlatform-Api as realm name for Qualys API credentials in the passwords.conf file.

The realm name was not set in previous releases. Now you can update the username and password from the TA setup page only if the user with "TA-QualysCloudPlatform-Api" realm name exists in the passwords.conf file.

Note that this means if you are upgrading to TA 1.8.9, you have to again manually enter Qualys API credentials after the upgrade otherwise you wont be able to access the Qualys API server. Before entering the credentials, we recommend you to empty the cache of your browser and do a hard reload.

We will create a new entry for the username with the realm name in the passwords.conf file. This user name with realm name will be used to fetch data from your Qualys account.

Add milliseconds in checkpoint file for FIM data inputs

We fixed an issue where TA was not able to fetch FIM data because checkpoint date or start date is till seconds, whereas FIM supports date in the milliseconds (YYYY-MM-DDThh:mm:ss.msZ) format. To fix this issue, we now check the checkpoint or start date and add milliseconds to it if the checkpoint date is till seconds.

Fixed incomplete API response XML file issue for Policy Compliance

We fixed an issue where for Policy Compliance module, TA was unable to fetch data for PC data input and showed an error message if the PC API returns incomplete data or XML file.

To fix this issue, now when TA will receive incomplete data or XML file, it will save this file as error file and will make the PC API call again to fetch the data from your Qualys account.

Fixed 400 bad request issue for Container Security

We fixed an issue where due to limitation of elastic search for Container Security data input if the page size is not equally divisible 10000 then the CS API was throwing 400 bad Request error. We have updated the logic so that elastic search limitation of 10000 is not violated when fetching CS data.

Improvements in 1.8.8

TA to support date format in milliseconds for FIM data input

As FIM now supports date in milliseconds format, TA will also accept date format with milliseconds to fetch FIM events, ignored events, and incident data. Due to this change, on the Data Input page, the start date to pull FIM data should be in UTC in ISO 8601 format: "YYYY-MM-DDThh:mm:ss.msZ".

If the Start Date field is blank, then we set the default start date to 1999-01-01T00:00:00Z and pull the data from this date. But as FIM requires milliseconds in the date format, we will now show an invalid date format message if you leave the Start Date empty for any of the FIM Qualys Metrics. For FIM Qualys Metrics, you need to manually enter the Start Date in UTC in ISO 8601 format: "YYYY-MM-DDThh:mm:ss.msZ".

We added this information on the Data Inputs screen (Settings > Data Inputs > Qualys Technology Add-On).

Note that if you are upgrading to TA 1.8.8 and you have already added FIM data inputs, then edit the data inputs as per the new date/time format and save it again to let the data input run successfully.

Improvements in 1.8.7

Updated CS containers and CS images API Version to 1.3

We updated CS Container and CS Image API version from 1.2 to 1.3 for CS container and CS image data inputs.

From this version onwards, use in the CS API request:

- SHA value of the image (imageSha) instead of image ID (imageId) to fetch the image details
- SHA value of the container (containerSha) instead of container ID (containerId) to fetch the container details.
- the pageNumber parameter instead of PageNo parameter to fetch the page with the specified number.

Reset the username and password from the TA setup page

We made an improvement where earlier if a user with two Qualys API accounts on a Qualys platform tried to switch between accounts by changing the Qualys API credentials from the TA setup page, then the password.conf file was required to be removed.

Now, as per the new flow, you do not have to remove the password.conf file while setting the Qualys API credentials from the TA setup page. When you enter the username on the TA setup page, we check if the username already exists in the password.conf file. If the username already exists then we only update the password.

If the username specified on the TA setup page does not exist in the password.conf file, then we fetch the old username from the password.conf file. If the old username is not blank in the file, then we delete the old credentials and add the new username and password specified on the TA setup page. In the case of a new user, we add the new username and password specified on the TA setup page.

Show Splunk restart message when saving settings on TA setup page first time

We will now show a message to “restart the Splunk to load all settings” after you save the settings on the TA setup page for the first time. Earlier, when the user was saving the TA setup form the first time and was not restarting the Splunk, then on the data input and event types pages, the TA set up form was shown instead of the respective forms.

Added DISA STIG SV values to PC Data Input

Policy Posture API response now has <REFERENCE> tag shown under <GLOSSARY>. We will show the value of the <REFERENCE> tag in Splunk when you search Policy Posture data using the posture info event. The value for the tag will be blank if the <REFERENCE> tag has no value.

Improvements in 1.8.6

Change in processing logic of PC data input

Prior to this release, PC data input was using the “policy_ids” parameter to pull posture information. With this release, we will use the “policy_id” instead of the “policy_ids” parameter to pull the posture information. As per the new logic, TA will first fetch all the policy IDs using the Compliance Policy List API and then for each policy_id, it will fetch the posture information using the Compliance Posture Information API.

As a result of this change, on the TA setup page, we removed the “Number of POLICY IDs to use for PC Posture Information (max 10)” option and added the “Number of posture info records per API request” option for PC posture API request. The value in this field will be used for the “truncation_limit” parameter of the PC posture API request and define how many posture info records will be returned per request. If the requested list identifies more records than the truncation limit, then the XML output includes the <WARNING> element and the URL for making another request for the next batch of records.

The default value is 1000. If you want to fetch all the posture information in a single output then specify 0. Paginated output is recommended if the posture info data is large.

Policy Compliance Settings

Note: The PC feed does not pull the SCAP information.

- ☒ Log individual PC Compliance Posture events
- ☒ Log Policy Summary
- ☐ Log "All" details (when unchecked, logs "Basic" details)
- ☐ Add additional fields (REMEDIATION, RATIONALE, EVIDENCE, CAUSE_OF_FAILURE)
- ☐ Enable multi-threading for PC Posture Information download

Number of threads to use for PC Posture Information (max 10):

Number of posture info records per API request:

Extra parameters for Posture Information API:

Note Enter as URL Query (e.g. a=1&b=string) or as JSON (e.g. {"a":1, "b": "string"}). Following parameters are NOT allowed: action, output_format, details, status_changes_since, policy_ids, show_remediation_info, cause_of_failure, include_dp_name, policy_id, truncation_limit

Change in XML input file parsing logic for performance improvement

We changed the parsing logic for the XML input files to improve the processing time of XML files. TA now does not load the full XML input file in the Splunk memory which was making the system slow and causing the XML processing to take longer time. To improve the performance, TA now parses the XML file line by line or tag by tag.

Improvements in 1.8.5

Added three new fields in the VM Detection Setting section on the TA set up page

We have added three new fields: “Host fields to log”, “Detection fields to log”, and “Max characters allowed in RESULTS field” in the VM Detection Settings section on the TA Set up page.

1) “Host fields to log” shows default output values for host assets. You can add additional comma-separated host XML tag names such as “Asset_ID” returned in the Host List API response that you want to log into the event or remove any existing tag that you don't want to log.

2) “Detection fields to log” shows default output fields for host detection. You can add additional comma-separated detection XML tag names such as “AFFECT_EXPLOITABLE_CONFIG” and “AFFECT_RUNNING_KERNEL” returned in the Host List Detection response that you want to log in the event or remove any existing tag that you don't want to log.

3) Max characters allowed in the RESULTS field lets you specify how many maximum characters will appear in the Results field. This means if the number of characters exceeds the maximum allowed characters, then TA will truncate the excess characters after parsing the RESULTS field and append the message “[TRUNCATED XXX Characters]” in the RESULTS field.

```
> 2/23/21 10:59:44.000 AM HOSTVULN: HOST_ID=346787379, IP="172.16.52.17", TRACKING_METHOD="AGENT", NETWORK_ID="0", OS="Ubuntu Linux 18.04.4", DNS="closenpvm.isw5zgahnqnetfakcx.bpr1n2he.cx.internal.cloudapp.net", LAST_SCAN_DATETIME="2021-02-23T05:29:44Z", LAST_VM_SCANNED_DATE="2021-02-23T04:54:15Z", SEVERITY=2, QID="115968", TYPE="INFO", FIRST_FOUND_DATETIME="2020-08-27T17:00:47Z", LAST_FOUND_DATETIME="2021-02-23T04:54:15Z", TIMES_FOUND="1047", IS_DISABLED="0", RESULT_TRUNCATED="2", RESULTS="root daemon bin sys sync games man ip mail news uucp proxy www-data backup list irc gnats nobody systemd-network systemd-resolve syslog messagebus _apt lxd uuid dnsmaq land [TRUNCATED 58 Characters]"
host = $decideOnStartup source = qualys sourcetype = qualys:hostDetection
```

The “RESULT_TRUNCATED” field now shows values based on whether the RESULT field is truncated by the TA or Splunk.

1) RESULT_TRUNCATED is “0” if neither TA nor Splunk truncates the RESULTS field/raw event.

2) RESULT_TRUNCATED value is “1” if the RESULTS field is truncated by Splunk. Note that if Splunk truncates the RESULTS field then the message “[TRUNCATED XXX Characters]” in the Results field is not shown.

```
> 2/26/21      HOSTVULN: HOST_ID=13126853, IP="10.115.108.61", NETWORK_ID="0", OS="Windows 10 Pro 64 bit Edition Version 2004", DN
2:16:14.000 PM S="eu02asset1", LAST_SCAN_DATETIME="2021-02-26T08:46:14Z", LAST_VM_SCANNED_DATE="2021-02-26T08:45:45Z", SEVERITY=3,
QID="105237", TYPE="INFO", FIRST_FOUND_DATETIME="2020-10-31T20:08:51Z", LAST_FOUND_DATETIME="2021-02-26T08:45:45Z",
TIMES_FOUND="654", IS_DISABLED="0", RESULT_TRUNCATED="1", RESULTS="\SAMR S-1-15-3-8 8 access-allowed standard_read
read_extended_attributes read_data synchronize write_data write_extended_attributes write_attributes read_attribute
s \SAMR Everyone 0 access-allowed standard_read read_extended_attributes read_data synchronize write_data write_ext
ended_attributes write_attributes read_attributes \SAMR AnonymousLogon 7 access-allowed standard_read read_extended
_attributes read_data synchronize write_data write_extended_attributes write_attributes read_attributes \SAMR Admin
istrators 544 access-allowed append_data execute standard_write_dac standard_r

host = $decideOnStartup | source = qualys | sourcetype = qualys:hostDetection
```

3) RESULT_TRUNCATED value is “2” if the RESULTS field is truncated by TA. Note that if TA truncates the RESULTS field then the message “[TRUNCATED XXX Characters]” in the Results field is shown.

Improvements in 1.8.4

Added option to index the KB data in Splunk

With this release, we now support indexing of the KnowledgeBase (KB) data in Splunk so that the Splunk TA users on the distributed setup environment can get the updated KnowledgeBase data on the Search Head from the Heavy Forwarder and generate the KB CSV file.

On the TA setup page, we added a KnowledgeBase Settings section that has a check box “Index the KnowledgeBox...”.

Knowledge Base Settings

- ☒ Log additional fields (SOLUTION, CONSEQUENCE, DIAGNOSIS)
- ☒ Index the knowledge base. CSV lookup file will NOT be created.

The check box indicates whether to index the KnowledgeBase data in Splunk or to write the data into a CSV file. When you select the check box and click Save, TA will fetch the KB data and index the KB data in Splunk. If the check box is not selected, TA does not index the KB data into Splunk and creates a CSV file.

The CSV file will have KB data from 1999-01-01.

<p>Files & Directories Upload a file, index a local file, or monitor an entire directory.</p> <p>HTTP Event Collector Configure tokens that clients can use to send data over HTTP or HTTPS.</p> <p>TCP / UDP Configure the Splunk platform to listen on a network port.</p> <p>Scripts Get data from any API, service, or database with a script.</p> <p>Systemd Journal Input for Splunk This is the input that gets data from journald (systemd's logging component) into Splunk.</p> <p>Qualys Technology Add-On Add-On for Qualys</p> <p>Splunk Secure Gateway Initializes the Splunk Secure Gateway application to talk to mobile clients over websockets</p> <p>Splunk Secure Gateway Mobile Alerts TTL Cleans up storage of old mobile alerts</p> <p>Splunk Secure Gateway Deleting Expired Tokens Delete expired or invalid tokens created by Secure Gateway from Splunk</p> <p>Splunk Secure Gateway Role Based Notification Manager Used for sending mobile alerts to users by role</p>	<p>Qualys Metrics * knowledge_base</p> <p>Cron entry or Interval <input type="text"/></p> <p>This could be a cron format entry OR old style Interval between subsequent runs.</p> <p>If you upgraded from version 1.1.0, it is recommended to change this to cron format for more control.</p> <p>Old style intervals are still supported for backward-compatibility purpose. Old Format: "w*d*h*m*s", where " " is any positive number. For example: 12h to run after 12 hours since last run. You can omit the letter if value is 0.</p> <p>Note - API rate limit according to your API tier will be applicable.</p> <p>Start Date <input type="text"/></p> <p>For fim_events, fim_ignored_events, and fim_incidents Qualys Metrics - date to start data pull from should be in UTC in ISO 8601 format: "YYYY-MM-DDThh:mm:ss.msZ". Ex: 2017-01-01T00:00:00.000Z</p> <p>For sem_detection Qualys Metrics - date to start data pull from should be in UTC in ISO 8601 format: "YYYY-MM-DDThh:mm:ssZ". Default value is "2021-01-26T00:00:00Z".</p> <p>For other Qualys Metrics - date to start data pull from should be in UTC in ISO 8601 format: "YYYY-MM-DDThh:mm:ssZ". Default value is "1999-01-01T00:00:00Z".</p> <p>For knowledge_base, 'Start Date' field is applicable only if 'index the knowledge base' is enabled on the TA setup page.</p> <p>For host_detection, this value refers to the host scanned date. For was_findings, this value refers to the last tested date. For cs_image_vulns, this value refers to image scan date.</p> <p>More settings <input type="checkbox"/></p>
--	---

On the Settings > Data Inputs > Add Data page for Qualys technology add on, we added the information that for knowledge_base "Start Date" field is applicable only if "index the knowledge base" is enabled on the TA set up page.

After you enable the index KB data option, you need to generate KB CSV lookup on the Search Head. See [KnowledgeBase Settings](#).

CS image label Information now available in CS events

You will now see the CS label information along with the CS image vulnerabilities in CS events for images in Splunk. TA uses a new API "/csapi/v1.2/images/<imageId>" to fetch the CS label and image vulnerability information. TA uses the label key to fetch the label information and the "vulnerabilities" key to fetch the vulnerability information. The image vulnerabilities & label information will be available in cs_vuln_info_event event type.

The new API does not provide image vulnerability summary information in the response. TA generates vulnerability summary information with the help of severity and patch availability fields of vuln summary information. All this vulnerability summary information will be available in the cs_vuln_summary_event event type.

Improvements in 1.8.3

We have fixed these issues in 1.8.3.

Issues Fixed

-We fixed an issue where the check box selection values for "log host summary events" and "Log Individual Host Vulnerabilities" options in the TA set up > VM Detection settings section was read from the app configuration file instead of qualys.conf file.

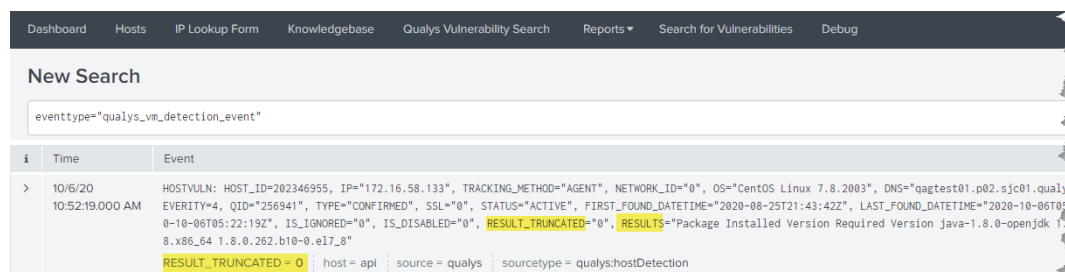
- We fixed an issue where TA was logging “VM host summary events for host detection” in Splunk even though the user had configured to exclude the VM host summary events on the TA setup page.
- We fixed an issue where WAS summary events weren't fetched for all the threads when the WAS data was fetched using multiple threads. Now when the WAS data is fetched in the multi-thread mode, TA logs events in Splunk from all the threads.
- We fixed an issue where TA throws an error and terminates the WAS API call when the WAS data input is fetched using multiple threads and the web application IDs are not distributed appropriately to each thread. To fix this error, we have changed the logic of distribution for web application IDs between the threads so that web application IDs are appropriately distributed.

Improvements in 1.8.2

Enhancements to VM Detection Event

With this release, we have moved the **Result** field in the VM Detection event to the end of the event. When the Result field is placed before the other event fields, Splunk, at the time of processing the VM Detection event data, truncates all the fields after the Results field if the size of the event exceeds the truncation limit. To avoid truncation of fields, we have added the Results field at the end of the event. Now only the values in the results field will be truncated, if the event size exceeds the truncation limit.

We have added a **RESULT_TRUNCATED** field before the "Results" field in the event to inform you that the event is truncated or not. **RESULT_TRUNCATED** = 1 means event is truncated and **RESULT_TRUNCATED** = 0 means event is not truncated. You can search for truncated and non truncated events using this field.



i	Time	Event
>	10/6/20 10:52:19.000 AM	HOSTVULN: HOST_ID=202346955, IP="172.16.58.133", TRACKING_METHOD="AGENT", NETWORK_ID="0", OS="CentOS Linux 7.8.2003", DNS="aagtest01.p02.sjc01.qualys.com", EVERITY=4, QID="256941", TYPE="CONFIRMED", SSL="0", STATUS="ACTIVE", FIRST_FOUND_DATETIME="2020-08-25T21:43:42Z", LAST_FOUND_DATETIME="2020-10-06T05:00-10-06T05:22:19Z", IS_IGNORED="0", IS_DISABLED="0", RESULT_TRUNCATED=0 , RESULTS ="Package Installed Version Required Version java-1.8.0-openjdk 1.8.x86_64 1.8.0.262.b10-0.e17_8"

TA will also remove the leading and trailing white spaces from the Results field after TA fetches VM detection data from your Qualys account using the Host List Detection API.

Splunk reads the truncate value from the **props.conf** file in the TA in “global/local” directory. If this file is removed from the app “global/local” directory, then TA will read the truncate value from the **global props.conf** file in Splunk. TA never truncates the event data while sending it to Splunk. Splunk automatically truncates the event if the size of the event exceeds the truncate limit set in the props.conf or global props.conf file.

Note

The VM Detection event shows the Results field when **show_results** is set to 1 in the “Extra Parameters” fields in VM Detection Settings on the TA setup page. If this parameter is not set, then none of these changes will have any impact on the VM Detection Event data.

Improvements in 1.8.1

Cleanup Script to remove API output files for Activity Log

We added the “Activity Log” data input in the cleanup script to remove the API output files from the /tmp directory.

Issue Fixed

We fixed the byte string issue for the host detection data pulled in Splunk for versions above 8.x.x which uses Python 3 interpreter.

Improvements in 1.8.0

Added a new data input - Activity Log

We added a new data input “Activity Log” to TA to let you pull activity logs from your Qualys Account. To access data input page, go to Settings > Data > Data Inputs > Qualys Technology Add-On. Click Add and from Qualys Metrics drop-down, select activity_log.

Page size field added for data inputs

We added Page size field for these data inputs to let you specify the number of records to be fetched in single API call. The default value for page size is 1000 records, but you can change the value.

- Container Security Data Settings for Images
- Container Security Data Settings for Containers
- FIM settings for events
- FIM settings for ignored events
- FIM settings for incidents
- Indication of Compromise (IOC)

Redesigned TA setup form

We have redesigned TA setup form to make TA 1.8.0 Splunk cloud compatible as per the SplunkAppInspect tool suggestion and improve the user experience.

The screenshot shows the 'TA-QualysCloudPlatform' configuration page in the Splunk web interface. The page has a dark header with 'splunk>enterprise' and navigation links for Apps, Administrator, Messages, Settings, Activity, and Help. The main content area is titled 'Configure This App' and contains the following sections:

- Qualys API Server:** A text input field with the value 'https://qualysapi.qualys.com'. A note below states: 'Note: The url should start with HTTPS.'
- Qualys Credentials:** Three text input fields for Username, Password, and Confirm Password. A note below states: 'Note: Leave username/password blank, if you have already set it up.'
- Client Certificate:** A blue header with a dropdown arrow. Below it is a checkbox labeled 'Use a Client certificate for authentication'. If checked, there are four text input fields: 'Path to client CA certificate', 'Path to client CA certificate key', 'Passphrase for client CA certificate', and 'Confirm Passphrase'.
- API Timeout Settings:** A section with a right-pointing arrow.
- VM Detection Settings:** A section with a right-pointing arrow.

Issues Fixed

We have fixed the proxy server validation issue in this release.

You can now update Qualys's password in the TA setup form without removing the password.conf file & restarting Splunk.

We now log the error in TA log if the CRON format of data input is invalid.

Improvements in 1.7.1

We made these improvements in 1.7.1

- TA is now compatible with both Python v2.7 and v3.7. See [How to switch python interpreter for Python3?](#)
- Container Security APIs now support the API gateway. Private cloud provider can use the gateway URL to connect to and fetch CS data from Qualys Cloud platform.

TA v1.7.1 no longer supports macro definition for indexes

Due to a known issue with Splunk, the user was getting a 255 error on the distributed Search Head setup. We have used macros for the ease of handling indexes and event types.

But in case of the distributed setup, macros definition was not getting expanded and as a result, the user was getting error on dashboard or while searching with event types.

To resolve this issue, the Splunk team has suggested not to use macros till further notice from them. See [How to assign a custom index to an event type?](#)

Improvements in 1.6.7

Policy Compliance data to show additional fields

You can now view REMEDIATION, RATIONALE, EVIDENCE and CAUSE_OF_FAILURE information in the compliance posture data for your policy.

Events (1)	Patterns	Statistics	Visualization				
Format Timeline ▾	Zoom Out	Zoom to Selection	DeSelect	1 millisecond per column			
		List ▾	Format ▾	20 Per Page ▾			
< Hide Fields	▣ All Fields	I Time	Event				
SELECTED FIELDS	> 19/10/18 POSTURE_INFO: POLICY_ID="844587", HOST_ID="155411113", HOST_IP="64.41.200.243", HOST_DNS="demo3.012.sjc81.qualys.com", CONTROL_ID="1073", CONTROL_STATEMENT="status of the 'Maximum Password Age' setting (expiration) / Accounts having the 'password never expires' flag set", CRITICALITY_LABEL="URGENT", SROZ_VALEN="3", RATIONALNTE_TECHNOLOGY_ID="43" , RATIONALNTE_TEXT="One characteristic that makes 'user identification via password a secure/reliable solution is setting a 'password expiration' requirement. Each time a new password is created, replacing one that has been in place for a given period of time, this reduces the difficulty of breaking a password via brute-force to its maximum level; it can also help ensure that a compromised 'back account with a password that has expired is then closed. While no 'secure maximum' for limiting the use of a password has been agreed upon, ninety (90) days is considered to be the maximum allowed for most enterprise organizations. However, this tactic must be used along with other passive security factors, such as increasing the complexity of the password set-point by requiring mixed-alph and/or special characters, to further increase the difficulty of breaking any password by brute-force attacks." , TECHNOLOGY_ID="sa", TECHNOLOGY_NAME="Centos 6.x", STATUS="failed", POSTURE_MODIFIED_DATE="1918-11-09T08:48:22Z", REMARKS="To specify password maximum for new accounts, with the file '/etc/logos/nfs.nfs' and add or correct the following line, replacing [DAYS] appropriately: PASS_MAX_AGE= [DAYS] the job requirement is 60 * CAUSE OF FAILURE=PASSWORD=1;NOT CAUSE OF FAILURE=PASSWORD=0" , CAUSE OF FAILURE="UNEXPECTED="99999", EVIDENCE_DPO_NAME="nfs.secan.system.loginfofs-max-password-days", EVIDENCE="Expected Value(s) = 1-365 / Current Value(s) = 99999 == LastUpdated:2019-06-17T04:21:45Z, EVIDENCE_CURRENT_VALUE="12704-06-17T04:21:45Z" host = qualys-virtual-machine source = qualys sourcetype = qualyscp.postureinfo						
INTERESTING FIELDS	> CONTROL_ID 1 a index 1 a source 1 a sourcetype 1						
+ Extract New Fields							

To pull this data in Splunk, go to the TA setup page and in the “Policy Compliance Settings” section, select the “Add additional fields (REMEDIATION, RATIONALE, EVIDENCE, CAUSE_OF_FAILURE)” check box.

Policy Compliance Settings

Note: The PC feed does not pull the SCAP information.

☒ Log individual PC Compliance Posture events

☒ Log Policy Summary

☒ Log "All" details (when unchecked, logs "Basic" details)

☒ Add additional fields (REMEDIATION, RATIONALE, EVIDENCE, CAUSE_OF_FAILURE)

☐ Enable multi-threading for PC Posture Information download

Number of threads to use for PC Posture Information (max 10)

2

Issues Fixed

We fixed an issue where last evaluated date was not shown as the event date for the policy. Now if the policy has last evaluated date then we will show this date as the event date.

✓ 18 events (before 3/18/20 5:00:54.000 PM) No Event Sampling ▼

Events (18) Patterns Statistics Visualization

List ▼ Format 20 Per Page ▼

< Hide Fields	≡ All Fields	i	Time	Event
SELECTED FIELDS a host 1 a source 1		>	3/18/20 10:25:18.000 AM	POLICY_INFO: POLICY_ID="845427", POLICY_TITLE="Riz", LAST_EVALUATED_DATETIME="2020-03-18T04:55:18Z" LAST_MODIFIED_DATETIME="2020-03-18T04:55:46Z", CREATED_BY="quays_rc70", STATUS="active", IS_LOCKED="0" host = quays-virtual-machine source = quays sourcetype = quays:pc:policyinfo

Improvements in 1.6.6

TA to use “updated” dateTime to download Container and Images data in Splunk

The new version of Container Security API uses a new parameter: “updated” to address the issue with mismatch count between Qualys UI and Splunk.

In TA 1.6.6, we now use the new parameter “updated” instead of “created” to ensure that all the Container and Images that were updated in particular duration gets synced in Splunk.

Improved Logging

We have now improvised logging to print exception messages and avoid logging empty messages.

Masked Passwords

Previously, the password was in plain text. But, we now mask passwords in proxy authentication.

Improved parsing for Host Detection RESULTS

We have improvised Host Detection RESULTS section to address the issue of parsing RESULTS in upper case.

Retry Interval

We have introduced a new configuration 'retry_interval_seconds' to retry same API request after configured interval, in case any error occurs while calling APIs.

Steps to configure 'retry_interval_seconds':

-edit qualys.conf file from below location:

<Splunk_Home>/etc/apps/TA-QualysCloudPlatform/local/qualys.conf

-add below line to qualys.conf file

```
retry_interval_seconds =<time_in_seconds>
```

Improvements in 1.6.5

TA to use “processedTime” for downloading FIM Data in Splunk

The new version 2.0.2.0 of FIM API has a new parameter “processedTime” to address the time lag issues with uploading the events on the Qualys portal by FIM agents.

In TA 1.6.5, we now use the new parameter “processedTime” instead of “dateTime” to ensure that all the FIM events that are generated in a particular duration are pulled in Splunk.

Due to this change, TA 1.6.5 will work only with FIM API version 2.0.2.0 and later and not with versions earlier than 2.0.2.0.

Improvements in 1.6.4

KnowledgeBase data to show BUGTRAQ_ID field

In Splunk, we will now show a new field “BUGTRAQ_ID” in KnowledgeBase data that is pulled from Qualys. This information is shown for QIDs that has “BUGTRAQ_ID” available.

FIM events to show event generated time in search results

When you search for FIM events in Splunk, the Time column in search results will now show you the time when the FIM event occurred as reported in your Qualys account. Earlier the time shown was the time when the event is pulled in Splunk.

New Search		
eventtype="qualys_fim_event"		
✓ 28,444 events (11/5/19 11:30:00.000 AM to 11/12/19 12:29:27.000 PM) No Event Sampling ▼		
List ▼ Format 20 Per Page ▼		
< Hide Fields	Time	Event
SELECTED FIELDS a host 1 a source 1 a sourcetype 1 INTERESTING FIELDS a action 5 a actorImagePath 40 a actorProcess 32 # actorProcessID 100+ a actorUserID 6 a actorUserName 7 a assetAgentID 14 a assetAgentVersion 3 a assetAssetType 1 a assetCreated 11 a assetEc2 1 # assetHostID 14 a assetInterfaces().address 26 a assetInterfaces().hostname 14 a assetInterfaces().interfaceName 7 a assetInterfaces().macAddress 13 a assetLastCheckedIn 57 a assetLastLoggedOnUser 3 a assetName 14	11/8/19 10:20:47.332 PM	<pre>{ [-] action: Delete actor: { [-] } asset: { [-] } changedAttributes: null class: Disk customerId: a6fddbd7-47f5-da87-8125-2a7054b3db53 dateTime: 2019-11-08T16:50:47.332+0000 fullPath: \Device\HarddiskVolume3\Clean\Aegis\Airports\frsdk.cfg-e2f63632-0202-425f-9ce8-df074e2cc2e3.bak id: 12b53652-536c-3883-855e-ecce7ee7e20fe incidentId: null name: frsdk.cfg-e2f63632-0202-425f-9ce8-df074e2cc2e3.bak newContent: null oldContent: null platform: WINDOWS profiles: [[-]] severity: 5 splunk_event_type: FIM_EVENT type: File }</pre> Show as raw text host = localhost source = qualys sourcetype = qualys:fim:event

Improvements in 1.6.3

Error on saving proxy server credentials

Fixed an issue where the TA user was getting an error when saving proxy server credentials required for authentication to the proxy server on the Qualys App set up page. Now the credential details are getting saved.

KnowledgeBase Data not populating in the solution section of the KB lookup file

We fixed an issue where the solution section in the KB lookup file (qualys_kb.csv) was not getting populated due to a failure in parsing of KnowledgeBase data. The parsing error occurred because the parameters "Threat_INTEL_IDs" and "Threat_INTEL_VALUES" were not found in the KB lookup file. We have added these two parameters in the KB lookup file.

Handle XML parsing error for WAS data

We fixed an issue where TA used to parse the WAS XML response file that had XML parsing errors. Now when TA will receive WAS data that contains parsing errors, it will not parse the file and request Qualys API server to resend the response file. TA will keep on requesting the WAS data from API server till it receives the data contains no parsing errors.

Certificate authentication failure when connecting to Qualys API server

We fixed an issue where authentication to the Qualys API server was getting failed when the user tried to connect to the API server via the proxy server using the certificate.

New Enhancements in 1.6.2

We have made the following enhancements in 1.6.2 release. TA can now:

- Pull EC2 metadata in host detection events using the extra parameter. For example, {"host_metadata": "ec2", "host_metadata_fields": "region,accountId,instanceId"}.
- Pull "cwe" information in Qualys WAS events.
- Retry the request that failed due to corrupted response XML.

New Features in 1.6.1

You can now configure Qualys App for Splunk Enterprise to pull IOCEvents data in Splunk from your Qualys account. We added a new Qualys metric (data input feed) "ioc_events" that you need to configure and enable for pulling the IOC events from your Qualys account. A new event type "ioc_info_event" is added for searching pulled IOC events in Splunk.



You can now preserve API output files in Splunk using the "Enable to preserve the XML/JSON files of API output" option. This option is available on the Qualys app setup page. By default, this check box will not be selected.

Preserve API Output

☒ Enable to preserve the XML/JSON files of API output

Added FIM Dashboard

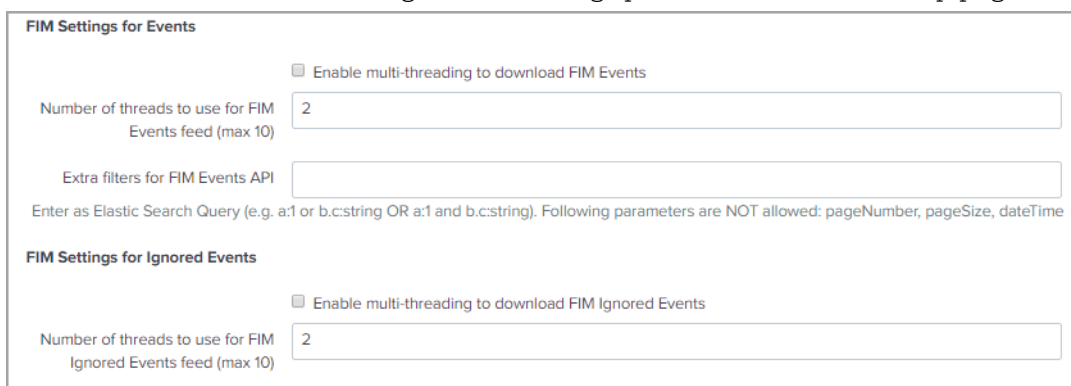
We have also added a FIM dashboard to give you a graphical analysis of your FIM data pulled from your Qualys Account. You will see graphical data for total number changes, events by severity, file and directory changes by change action, and top changes by OS, user and process.

Multithreading not supported for FIM

We removed multithreading support for FIM as the new APIs (FIM API Version 2.0) do not support multithreading.

New Feature in 1.5.0

Qualys App for Splunk Enterprise can now pull FIM data for events, ignored events and incidents from your Qualys Account. On the TA set up page, you will now see 3 new sections: FIM Settings for Events, Ignored Events and Incidents. Specify configuration settings in these sections for collecting FIM data. Next, enable the FIM data feeds to pull the FIM data based on the configuration settings provided on the TA set up page.



The screenshot shows a configuration page for FIM (File Integrity Monitoring) settings. It is divided into two main sections: 'FIM Settings for Events' and 'FIM Settings for Ignored Events'.

FIM Settings for Events:

- There is a checkbox labeled 'Enable multi-threading to download FIM Events' which is currently unchecked.
- Below it is a text input field labeled 'Number of threads to use for FIM Events feed (max 10)' with the value '2' entered.
- Below that is another text input field labeled 'Extra filters for FIM Events API' which is empty.
- Below the filter field is a note: 'Enter as Elastic Search Query (e.g. a:1 or b.c:string OR a:1 and b.c:string). Following parameters are NOT allowed: pageNumber, pageSize, dateTime'.

FIM Settings for Ignored Events:

- There is a checkbox labeled 'Enable multi-threading to download FIM Ignored Events' which is currently unchecked.
- Below it is a text input field labeled 'Number of threads to use for FIM Ignored Events feed (max 10)' with the value '2' entered.

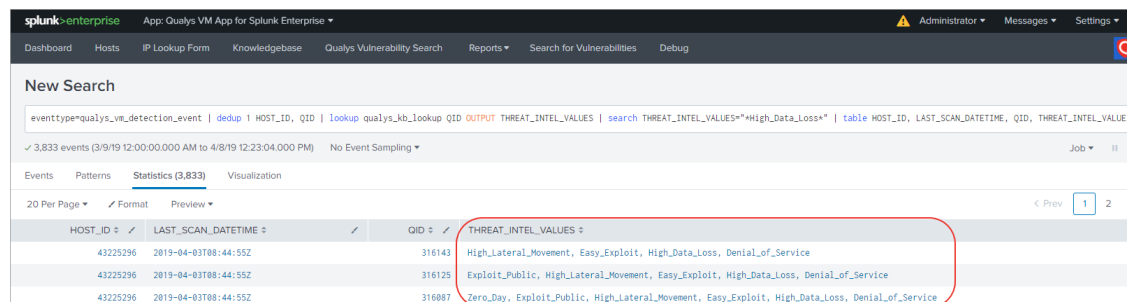
New Features and Fixed Issues in 1.4.1

View Qualys Real-time Threat Indicators (RTIs) for vulnerabilities

We are now sending the Qualys Real-time Threat Indicators (RTIs) data in the data input for the Knowledge_base metric. Only, the user account with Threat Protection subscription can view this information for vulnerabilities found in the host based scans. You can set up your dashboard to monitor vulnerabilities for various threat level values.

The sample search shows vulnerabilities for which threat value is High_Data_Loss.

```
eventtype=qualys_vm_detection_event | dedup 1 HOST_ID, QID | lookup qualys_kb_lookup
QID OUTPUT THREAT_INTEL_VALUES | search
THREAT_INTEL_VALUES="*High_Data_Loss*" | table HOST_ID, LAST_SCAN_DATETIME,
QID, THREAT_INTEL_VALUES
```



HOST_ID	LAST_SCAN_DATETIME	QID	THREAT_INTEL_VALUES
43225296	2019-04-03T08:44:55Z	316143	High_Lateral_Movement, Easy_Exploit, High_Data_Loss, Denial_of_Service
43225296	2019-04-03T08:44:55Z	316125	Exploit_Public, High_Lateral_Movement, Easy_Exploit, High_Data_Loss, Denial_of_Service
43225296	2019-04-03T08:44:55Z	316087	Zero_Day, Exploit_Public, High_Lateral_Movement, Easy_Exploit, High_Data_Loss, Denial_of_Service

Support for arf_kernel filters parameter for VM host detection

We now support “arf_kernel filters” parameter to identify vulnerabilities found on running or non-running Linux kernels.. You can update the optional parameter to include the arf_kernel parameter in VM Detection Settings on the TA setup page.

Set show_results=1 to view TCP/UDP port information

We have fixed an issue where the user was unable to view the open TCP/UDP ports information in the HOSTSYMMMARY events. To view the information, update optional parameters in VM Detection Settings on the TA setup page to include “show_results=1”.

Newline character removed from the port data in vulnerability data feed

We have fixed an issue where whitespace and newline characters in the port data in the Results tag in the vulnerability data feed fetched from the Qualys Server were introducing new events when imported in Splunk. Now, we have fixed this issue by removing these characters from the vulnerability data feed before importing it in Splunk.

Enable CVSS scoring in your account to view CVSS scores for vulnerabilities

We have fixed an issue where Splunk was showing an error for missing CVSS data when importing KnowledgeBase API response in Splunk TA. This issue was occurring for the user accounts that have CVSS Scoring not enabled for their subscriptions. As a result, the KnowledgeBase API response does not have CVSS data for vulnerabilities. To Enable CVSS Scoring in your Qualys account, go to "Reports > Setup > CVSS > Enable CVSS" and click "save".

Now, Splunk does not show missing CVSS data error if you do not enable CVSS scoring for your subscription. In this case, Splunk will show no CVSS metrics scores for vulnerabilities in the Splunk KnowledgeBase.

New Feature in 1.4.0

TA now supports ingesting Container Security data

Qualys App for Splunk Enterprise can now pull vulnerability information for docker image and container in Container Security from your Qualys account. TA pulls CS data based on the configuration information you have provided in the Container Security Settings for Images and Containers. CS data is in JSON format.

New Feature in 1.3.4

New information added in HOSTSUMMARY and HOSTVULN events

Added NETWORK_ID, LAST_VM_SCANNED_DATE and LAST_VM_SCANNED_DURATION information in HOSTSUMMARY.

```
HOSTSUMMARY: HOST_ID=227520646, IP="104.154.89.105", TRACKING_METHOD="IP", NETWORK_ID="0",
DNS="105.89.154.104.bc.googleusercontent.com", LAST_SCAN_DATETIME="2018-09-18T12:06:35Z",
LAST_VM_SCANNED_DATE="2018-09-18T11:59:44Z", LAST_VM_SCANNED_DURATION="371", SEVERITY_1=5,
SEVERITY_2=3, INFO=5, CONFIRMED=3, POTENTIAL=0, NEW=0, ACTIVE=3, FIXED=0, RE-OPENED=0, _SEVERITY_1=5,
ACTIVE_SEVERITY_2=3, INFO_SEVERITY_1=5, CONFIRMED_SEVERITY_2=3, TOTAL_VULNS=8
```

Added LAST_FIXED_DATETIME, TIMES_FOUND, IS_IGNORED, IS_DISABLED information in HOSTVULN.

```
HOSTVULN: HOST_ID=190339320, IP="172.16.5.4", TRACKING_METHOD="AGENT", NETWORK_ID="0",
OS="Ubuntu Linux 14.04.5", DNS="wordpress", LAST_SCAN_DATETIME="2018-09-19T0
2:47:26Z", LAST_VM_SCANNED_DATE="2018-09-19T02:43:34Z", SEVERITY=3, QID="370845",
TYPE="POTENTIAL", SSL="0", STATUS="FIXED", FIRST_FOUND_DATETIME="2018-04-10T23:36
:56Z", LAST_FOUND_DATETIME="2018-07-09T17:36:54Z", TIMES_FOUND="438", LAST_TEST_
DATETIME="2018-09-19T02:43:34Z", LAST_UPDATE_DATETIME="2018-09-19T02:47:26Z", LAST_
FIXED_DATETIME="2018-07-09T23:15:12Z", IS_IGNORED="0", IS_DISABLED="0"
```

New Features in 1.3.3

New Basic option for fetching policy posture compliance data

You can now specify to Posture API to fetch only basic details of the policy posture compliance data for policy IDs. This option is for policy IDs with large posture compliance data. Keep the “Log All details (when unchecked, logs “Basic” details)” check box deselected in the Policy Compliance Settings for the API to get basic details.

Configure total number of policy IDs to be fetched

You can now configure in the Policy Compliance Settings the total number of policy IDs to be fetched by the Posture API. The valid number range is 1 to 10. Set this value low for policy IDs with large policy posture compliance data.

New Features in 1.3.1

Introducing new data input for Policy Compliance

TA is now able to pull and ingest Policy Compliance posture information! The TA Setup page includes new Policy Compliance configuration settings. The extra parameters option accepts API parameters for Posture Information API (`/api/2.0/fo/compliance/posture/info/` with `action=list`). When pulling policies information, Posture API parameter `policy_ids` becomes the parameter `ids` for Policy detail API call.

Support for using client certificates to call API

Now you can specify a client certificate in TA so that TA uses it while making API calls. A new section has been added to the TA setup page for this.

New utility script to clean up left-over XML and PID files

This new script is useful for cleaning up orphan XML files in the `TA-DIR/tmp` directory. While running the utility, you can provide command line options to specify data inputs for the XML files to be cleaned up. The utility will delete all the XML files for the chosen data inputs, except those belonging to currently running TA processes.

Additional Improvements 1.3.1

Update to Host List Detection API

You'll now see the parameter `vm_processed_after` in TA logs. With Qualys 8.9, we 1) changed the way we report host scan time so it's based on when a scan finished, not when the scan started. 2) Introduced new parameters to filter the Host List VM Detection API by scan end dates and processed dates. The `vm_processed_after` parameter is used to filter the list to only show hosts with vulnerability scan results processed after a certain date and time.

Setup page save fails if there are any validation errors

TA will try to validate inputs given on the TA setup page. If validation fails, it will NOT save any details, but raise a `ValueError`. This results in a generic error message in the Splunk UI. You can see a more detailed error message given by TA in `splunkd.log`.

When installed on Search Head, do not run data inputs other than knowledge base

Checks were added to the code (with help from the Splunk team) to ensure that TA will only run the knowledgebase data input when TA is installed on a Search Head, even when other data inputs have been added and enabled. In other words, TA will not run host detection, WAS findings and PC posture information data inputs when installed on Search Head.

Log error messages given by Qualys API

If the Qualys API responds back with an error (in response body), TA will now log the error message in the TA log for troubleshooting. This way you'll know if there's an API reason for not getting data (e.g. Rate Limit exceeded).

PID repeat issue resolved

TA writes PID in .pid file for every input run. This file is deleted at the end of the run. TA uses this pid file to check if any process with the PID is running. If it finds any such process, TA will check if the process is running qualys.py then only will it terminate itself, else TA will run the qualys.py script for the scheduled input.

Configurable API Timeout period

By default, the API timeout period is 300 seconds. If this value is not adequate you can set a different timeout value on the TA setup page.

Display API parameters not allowed by TA

To avoid operational problems, API parameters that are not allowed by TA are now clearly listed for each Extra API parameter field on the TA setup page.

Log the index name being used in each run

To help with troubleshooting, TA will now log the name of the index where data from each run will go into. This is the same index name as selected by the user while adding/updating the data input.

Display data input name in each log entry

There are some common execution paths for all data inputs in TA, and they write some log entries. When multiple data inputs are running at the same time, it becomes hard to identify which log entry was written for which data input. To fix this, TA will have a mention of data input it is running for in each log entry it writes. This way, one can grep all the log entries belonging to a particular data input. This would be useful if you are troubleshooting subsequent runs of the same data input.

Avoid unnecessary call to msp/about.php each time Splunk invokes modular input

Splunk invokes TA's entry point script every 60 seconds. On each invocation, the code checks for the Qualys version by making a msp/about.php API call. This call was being made irrespective of whether the current time matched the configured cron/time interval. To avoid unnecessary calls, TA will first check if now is the time for any input to run. If yes, the API call is made. If no, the API call is not made.