Qualys App for Splunk Enterprise with TA
User Guide

November 15, 2019
# Table of Contents

About this guide......................................................................................................................... 4
About Qualys ................................................................................................................................. 4
Qualys Support ............................................................................................................................ 4

Get Started ................................................................................................................................. 5
Pre-requisites ............................................................................................................................... 5
Download and Install the App .................................................................................................... 5
Configure the App ....................................................................................................................... 7
  VM Detection Data ................................................................................................................. 8
  Policy Compliance Data ......................................................................................................... 9
  WAS Findings .......................................................................................................................... 10
  Container Security Data Settings for Images ................................................................. 10
  Container Security Data Settings for Containers ............................................................ 11
  FIM data settings for events, ignored events and incidents ................................................. 12
  Indication of Compromise (IOC) Settings ........................................................................ 12
  Proxy Configuration ............................................................................................................. 13
  Preserve API Output ............................................................................................................ 13
Configure Data Sync .................................................................................................................. 14
Enable the Data Feed to Start in Splunk .................................................................................. 16
How to setup for a Search Head Cluster .................................................................................. 16
How to get the RESULTS field indexed in host detection input ............................................ 17
How to populate the SOLUTION section in the KB lookup file ............................................... 17

View your Qualys Data in Splunk! .............................................................................................. 19
Search Your Qualys Data ........................................................................................................... 23
  Search Container Security Data ......................................................................................... 25
  Search FIM Data for Events and Incidents ....................................................................... 28
  Search IOC Data .................................................................................................................. 30

App Management & Troubleshooting ...................................................................................... 31
APP Management ..................................................................................................................... 31
Troubleshooting ......................................................................................................................... 32
URL to the Qualys API Server ................................................................................................. 33

What’s New ............................................................................................................................... 34
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/
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.

Pre-requisites

- A valid Qualys account with API access
- A Splunk Enterprise account
- Computer with MacOS or Linux
- A couple minutes for setup

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 and CS detection data.

**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 this 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.

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.

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. Download API user guides

Why choose “Log host information with each detection”?
This is recommended when you have more than 50,000 hosts in your Qualys account.
What are VM Detection-Advanced Settings?

The "Enable full data pull always?" option allows you to specify whether TA should do a full data pull or an incremental pull on each run. By default, this is not selected and TA does an incremental pull. Select the option to pull the full host detection data from Qualys account and put it on Splunk.

The "Enable .seed file generation?" option indicates to TA to generate a .seed file at the location specified by you for TA to stream host detection data into Splunk. You have the option to specify either directory path or file path. If you specify a directory path, TA creates a .seed file each time TA pulls data into Splunk. TA appends data in the same .seed file if you specify a file.

We strongly recommend you to get in touch with our support team if you want to change VM Detection-Advanced Settings.

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.

Policy Compliance Data

Configure settings for collecting PC data. For example, tell us whether you want to fetch all details or only basic details. Select basic details if you have a large amount of PC data. Additionally, you can choose to fetch individual compliance posture events for all hosts and/or a policy summary. You can also configure the number of policy IDs (1-10) to be fetched by the Posture API.

Enter API input parameters (in the Extra parameters field) for the Posture Information API. For example, specify Ids for the hosts for which you want to collect compliance posture information. Download API user guides
WAS Findings
Configure settings for collecting WAS data. 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. [Download API user guides](#)

---

Container Security Data Settings for Images
Configure settings for collecting CS data. Select one or more logging options to indicate whether you want to show individual image vulnerabilities and/or a 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 Data Settings for Containers

Configure 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 to 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 the Container Security online help for API information.
FIM data settings for events, ignored events and incidents

FIM Settings for Events, Ignored Events and Incidents sections are provided to help you configure the settings for collecting FIM data for events, ignored events and incidents.

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.

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.

Indication of Compromise (IOC) Settings

We have provided you IOC API settings that you can configure to fetch IOC data from your Qualys Account. Enter the API input parameters (in the Extra parameters to pass to Indication of Compromise API) to specify what IOC data (events) will be pulled 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 IOC API. These parameters are shown in the IOC settings. You can customize the API request by adding new parameters or modifying the existing parameters.
Proxy Configuration
Provide the proxy server IP address and credentials for Qualys API requests.

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.
Configure Data Sync

TA-QualysCloudPlatform pulls Qualys data and indexes it 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.

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.
For VM data, choose knowledge_base and host_detection.
For PC data, choose policy_posture_info.
For WAS data, choose knowledge_base and 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 IOC data choose ioc_events.

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.

What is the default schedule for data sync?
Data is pulled every day, starting 24 hours after install.

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 custom index to a Qualys metric?
While configuring a Qualys metric (data feed input), you can specify your own custom index under More Settings. TA when pulling the data for the metric will associate this index with the pulled data. To define an index for a metric, go to Settings > Advanced search > Search macros and click the event type for the metric. Type the index name as index="index name" in the Definition field. For example, index=was_new, where was_new is the name of the index.

Note that if you change the index for a metric then all the data that is pulled using this index will only appear in the search and Dashboard. The data that is pulled using the previous index will not appear in the search.
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.

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 any of these data inputs: host_detection, was_findings, policy_posture_info. Do NOT add the knowledge_base data input.

2) Use Deploer to push Qualys TA to all Search Heads. For reporting purposes you’ll also want to push these Qualys Apps to your Search Heads: Qualys VM App, Qualys PC App and Qualys WAS App.

3) Install Qualys TA on each Search Head. Go to Settings > Show All Settings and configure TA with your Qualys API credentials. On each Search Head add and enable only the knowledge_base data input. Do NOT add or enable any other data inputs on Search Heads.
How to get the RESULTS field indexed in host detection input

Skip the first 4 steps if the installed version of Qualys App for Splunk Enterprise is 1.4.1 or higher.

1) Open <TA DIR>/bin/qualysModule/splunkpopulator/detectionpopulator.py and find class HostDetectionPopulator.

2) In this class, find _process_root_element(self, elem) method.

3) In this method, add “RESULTS” to the end of the HostDetectionPopulator.detection_fields_to_log list. This is a list of fields to parse from the detection tag. This will tell the code to parse the XML tag and output it while printing the event data. As a best practice, be sure to also include a comment describing why you’re editing the list.

4) Save the file and restart Splunk.

5) 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”.

Note - RESULTS in host detection API output could be multi-line text. As we set KV_MODE = auto for hostDetection input in props.conf, we are not sure how Splunk will treat the events when RESULTS field is multi-line text. It may or may not consider the multi-line text to be the part of same single event. The newline character might confuse Splunk’s event detection.

How to populate the SOLUTION section in the KB lookup file

You’ll need to edit the kbpopulator.py script used to populate the KB lookup file. The KB lookup file is: SPLUNK_HOME/etc/apps/TA-QualysCloudPlatform/lookups/qualys_kb.csv

1) Go to SPLUNK_HOME/etc/apps/TA-QualysCloudPlatform. Use this command:

cd /opt/splunk/etc/apps/TA-QualysCloudPlatform

2) Backup this file:

SPLUNK_HOME/etc/apps/TA-QualysCloudPlatform/bin/qualysModule/splunkpopulator/kbpopulator.py

3) Open kbpopulator.py and do the following:

Find this line and remove # from the beginning of the line (uncomment it):

# QID_EXTRA_FIELDS_TO_LOG = ["VULN_TYPE", "PATCHABLE", "PCI_FLAG", "TITLE", "CATEGORY", "DIAGNOSIS", "CONSEQUENCE", "SOLUTION", "PUBLISHED_DATETIME"]

Find this line and add # to the beginning of the line (comment it out):

QID_EXTRA_FIELDS_TO_LOG = ["VULN_TYPE", "PATCHABLE", "PCI_FLAG", "TITLE", "CATEGORY", "PUBLISHED_DATETIME"]

The 2 lines should look like this when you’re done:
QID_EXTRA_FIELDS_TO_LOG = ["VULN_TYPE", "PATCHABLE", "PCI_FLAG", "TITLE", "CATEGORY", "DIAGNOSIS", "CONSEQUENCE", "SOLUTION", "PUBLISHED_DATETIME"]

# QID_EXTRA_FIELDS_TO_LOG = ["VULN_TYPE", "PATCHABLE", "PCI_FLAG", "TITLE", "CATEGORY", "PUBLISHED_DATETIME"]

4) Save your changes to kbpopulator.py.

5) Let the knowledgebase input run according to your schedule or run it immediately using this command:

cd SPLUNK_HOME/etc/apps/TA-QualysCloudPlatform

SPLUNK_HOME/bin/splunk cmd python /bin/run.py -k -s <your Qualys API server> -u <your Qualys API username> -p <your Qualys API password>
View your Qualys Data in Splunk!

We provide additional apps that make use of the data collected by the TA app. 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 IOC 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.
View your Qualys Data in Splunk!

Sample VM Dashboard

Sample WAS Dashboard
View your Qualys Data in Splunk!

Sample PC Dashboard

Sample CS Dashboard
Sample FIM Dashboard

176,850
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.

**QIDs by Category**

![QIDs by Category](image)

**Host Distribution by OS**

![Host Distribution by OS](image)
Scan Volume

Time since Last Scan
Search Container Security Data

CS data is in JSON format. TA indexes CS events 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
sourcetype="qualys:cs:csimageinfo"|search repo{}.registry="docker.io"
Sample JSON query to search images with a specific vulnerability severity count

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

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

Sample query to search for FIM ignored events

eventtype="qualys_ignored_fim_event"
Sample query to search for FIM incidents

eventtype="qualys_fim_incident"
Search IOC Data

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

**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 will delete all the XML files related to the chosen data input(s), except those belonging to currently running TA processes.

Example 1: Help

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

Example 2: Delete Host Detection and WAS Findings XML

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

Example 3: Delete XML files belonging to all data inputs

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

Looking for logs?
Qualys logs are populated in Splunk’s index “_internal”. Use this search to find logs:
index=_internal source="/opt/splunk/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.

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="/opt/splunk/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/2.0/fo/asset/host/vm/detection/ API call, then check that the host_detection input was added and enabled.
- If not enabled, please enable it.
- If enabled, and you still don’t see any records for the VM detection 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="/opt/splunk/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 will now pull the data from the date configured in Data Input Settings for the respective Qualys module.
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).
What’s New

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.

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 IOC events 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.
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.

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

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 HOSTSYMMARY 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="184.54.89.105", TRACKING_METHOD="IP", NETWORK_ID=0,
DNS="185.89.184.184.bc.googleusercontent.com", LAST_SCAN_DATE_TIME="2018-09-18T12:06:35Z",
LAST_VM_SCANNED_DATE=2018-09-18T11:59:44Z, LAST_VM_SCANNED_DURATION=371s, 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=100339320, IP="172.16.5.4", TRACKING_METHOD="AGENT", NETWORK_ID=0,
TYPE="POTENTIAL", SSL="0", STATUS="FIXED", FIRST_FOUND_DATE_TIME="2018-09-19T02:43:34Z",
TYPE="POTENTIAL", SSL="0", STATUS="FIXED", FIRST_FOUND_DATE_TIME="2018-09-19T02:43:34Z",
FIXED_DATE_TIME="2018-09-19T02:43:34", 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).
What's New

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.