Qualys App for QRadar 1.0.1 - User Guide

About the application

If you have a Qualys subscription and API access, you can use the Qualys App for QRadar to ingest your Qualys VM detections into QRadar and visualize them on a single page. Install the app, configure, and schedule the sync. The Qualys App will continue pulling your detection delta so you will always see updated reports. Want to visualize historical data? Just use date-time pickers given in the Qualys App and see useful reports.

How to install

1. Login to your QRadar and go to "Admin" tab.
2. Click on "Extensions Management".
3. Click "Add" button and upload the extension ZIP file. Please **refer this link** to get zip of Qualys App for QRadar 1.0.1.
4. Confirm whether you want to replace/skip any existing contents with those coming from of extension, and click "Install" button.
5. After installation is successfully completed, refresh your QRadar user interface.
6. You should now see a new tab "Qualys App for QRadar" in top menu.

> **Application Dependencies**
> This application has following dependencies. These are installed by QRadar's application management while spinning up the application container.
>
> 1. vixie-cron
> 2. python-crontab-2.1.1.tar.gz
>
> The `vixie-cron` is installed using `yum install` command, where as `python-crontab-2.1.1` is installed using `pip` command.

How to configure

Prerequisites

To use this extension, you need followings.

1. A valid Qualys subscription.
2. API access to Qualys VM module.
3. Knowledgebase access, if you want to enable Knowledgebase input.
4. QRadar should have Internet access, and your Qualys API server should be reachable from QRadar.

Manual Steps

Attention Please!
You need to carry following steps manually, right after you install the app and **BEFORE** you start using it.

Add Log Source Event Mapping

Skip this section if already done for app version 1.0.0

1. Go to Admin > DSM Editor.
2. In "Select Log Source Type", search and select "Qualys LEEF".
3. In the popup that opens, go to "Event Mappings".
4. Notice existing mappings. You would probably have only 2 entries. You need to have one for Qualys.
5. Click on + to add a new. This opens another popup "Create a new Event Mapping".
6. In this popup, set Event ID as "Qualys" (without quotes) and Category as "Qualys" (again, without quotes).
7. Click on "Choose Event" link.
8. The "Event Categorizations" popup, click "Create New" button.
9. Set values as follows.
   ```
   Name: Qualys Information
   Description: Qualys Information
   Log Source Type: Qualys LEEF
   High Level Category: System
   Low Level Category: Information
   Severity: 2
   ```
10. Click "Save" button. This will take you back to "Event Categorizations" popup.
11. Click and select the newly created entry which is shown in "Search Results" table.
12. Click "Ok" button. This takes you back to "Create a new Event Mapping" popup.
13. Click "Create" button. This takes you back to "Qualys LEEF" popup - Event Mappings tab.
14. Confirm that now you have 3 entries, including Event ID "Qualys" - Category "Qualys".
15. Finally, click "Save" button and close the popup window.

Enable "Last Scan Datetime" Parsing

Skip this section if already done for app version 1.0.0

1. Go to Admin > DSM Editor.
2. In "Select Log Source Type", search and select "Qualys LEEF".
3. In the popup that opens, go to "Properties".
4. In the list of properties, search and open "Last Scan Datetime".
5. In the Property Configuration > Expression section, click "Edit".
6. Notice the "Enabled" field. It may be in disabled state (tick grayed out). Continue if its in disabled state.
7. Tick the "Enabled" field. It changes color.
8. Click "OK" button on Expression section.
9. Click "Save" button and close the popup window.

Update Log Source Identifier in Log Source

Skip this section if already done for app version 1.0.0

1. Login to your QRadar box as root user, and follow the instructions given here to connect to Qualys App for QRadar's command line.
2. Using `ifconfig` command, find out IP address of this docker container. Note it down, as you need to use it in subsequent steps.
3. On your console UI, Go to Admin > Data Sources > Log Sources.
4. In the popup that opens, select log source with name "Qualys" and click "Edit" button. You should now see "Edit a log source" section.
5. In "Log Source Identifier" field, the default value will be `qualysapp`. Edit and change it to IP address you noted in step 2.
6. Click "Save".

Steps

1. Login to your QRadar and go to "Admin" tab.
2. Scroll to "Plug-ins" section and click on "Qualys App Settings". A pop-up window would open.
3. Use "Qualys API" tab to configure your Qualys credentials.
    a. Enter your Qualys API server, username and password in appropriate fields.
4. Use "Host Detection" tab to configure and enable Host Detection input.
    a. **You must enable this input in order to use this extension.**
    b. To enable this input, tick the checkbox in front of "Enable Host Detection fetch".
    c. In "Host Detection Cron Schedule" field, write a valid cron entry (time part only). Your input will run according to this schedule. Please refer here for more information on cron.
        i. This is a mandatory field.
        ii. It is advised to keep this in sync with your scanning schedules. For example, if you run yours once a day, schedule this input to run once a day.
    d. *Optional:* In "Start Date-Time" field, enter the date from which you wish to fetch the VM detection data. The date/time is specified in YYYY-MM-DD[THH:MM:SSZ] format (UTC/GMT), like “2007-07-01” or “2007-01-25T23:12:00Z”.
        i. You may leave this field blank.
        ii. When left blank, it defaults to 1999-01-01T00:00:00Z.
    e. *Optional:* If you want to provide any extra parameters to Host Detection API, set them in "Extra API Parameters" field, in valid JSON format. Please refer Qualys API Quick Reference Guide to know API parameters.
        i. You may leave this field blank.
5. Use "Knowledgebase" tab to configure and enable Knowledgebase input.
    a. A copy of Qualys knowledgebase is bundled with this extension. If you wish to keep it updated, please enable this input.
    b. To enable this input, tick the checkbox in front of "Enable Knowledgebase fetch".
    c. In "Knowledgebase Cron Schedule" field, write a valid cron entry (time part only). Your input will run according to this schedule. Please refer here for more information on cron.
        i. This is a mandatory field.
        ii. You might not want to run this every day. Once a week is also OK.
    d. *Optional:* If you want to provide any extra parameters to Knowledgebase API, set them in "Extra API Parameters" field, in valid JSON format. Please refer Qualys API Quick Reference Guide to know API parameters.
        i. You may leave this field blank.

How it works

What happens after configuration

Once you configure and enable Host Detection input, application bundled with this extension will start fetching your VM detection data.

For first run, it might take some time depending on your scan volume. After that, subsequent pulls are incremental ones - fetching only new/changed data.

How data gets into QRadar

Whenever it runs (based on the cron schedule you set), it makes outbound API call to Qualys, transforms the XML response it receives into LEEF format and sends it to QRadar over syslog.

Using Log Source provided with this extension, QRadar then puts this data into Ariel database - events table.

How to use

Summary

When you click "Qualys App for QRadar" tab in top menu, you see a summary dashboard provided by this app. It renders following reports.

1. Confirmed vulnerabilities over time
2. Count of Active Hosts
3. Detections by Severity
4. Detections by Status
5. Detections by Type
6. Hosts Not Scanned in Last 30 Days
7. Top 10 Vulnerabilities

By default, these reports are based on detection data in last 3 months. To change it, please use "Start Date-Time" and "End Date-Time" and click on "Search" button. When you click it, all the reports are updated according to new date-time range.

Knowledgebase

Application has a default copy of knowledgebase bundled with it. This menu shows you some visualizations about current knowledgebase copy. If you have enabled knowledgebase input, this copy will be kept up-to-date.

It also shows knowledgebase in tabular format.

Raw Data

Sometimes, you may be interested in seeing the raw data. This extension provides a saved search for this. Follow steps given below to use it.

1. Go to "Log Activity" tab and click "Search" > "New Search" link.
2. In "Saved Searches" section:
    a. Search "Qualys Host Detection Events".
    b. Click "Load' button.
3. Notice the AQL loaded in "Advanced Search" section.
4. Click "Search" button.

You might want to change the date-time range to widen/shorten your search span.

You can also execute your own AQL queries to find more appropriate data. Please refer to fields in "Qualys LEEF" log source to know about Qualys fields.

Host Detection Input Logs

While running, host detection input sends its log to QRadar over syslog. To see them, you can use a "Qualys:HostDetection Logs" saved search provided with this app.

Follow same steps as mentioned above, but for "Qualys:HostDetection Logs" saved search.

Troubleshooting

In case your application isn't bringing in your VM detection data, please go through the list given below.

1. Make sure that application dependencies got installed correctly.
2. Make sure you have correctly configured this app.
    a. Make sure you do have correct API and access permissions.
    b. Your credentials are correct.
    c. You have enabled host detection input.
    d. Cron schedule entry is valid one.
    e. If you have set start date-time, its complies with Qualys required format.
    f. If you have set extra parameters, make sure:
        i. the JSON is valid one.
        ii. all parameters mentioned there are valid ones.
3. Make sure your QRadar do have Internet access and is able to reach your Qualys API server.
4. Check the Host Detection input logs as mentioned in section above.

Support

In case above mentioned troubleshooting steps don't provide you any useful information and you need more help, please contact Qualys support at support@qualys.com