Container Security

Release Notes for Sensor

Version 1.19

September 8, 2022

Here's what's new in the Container Security Sensor!

SCA Scanning Now Supported

This Container Security Sensor release brings support for Software Composition Analysis (SCA) scanning of container images. An SCA scan discovers installed open source software and libraries, as well as associated vulnerabilities, present in your container images.

While evaluating security posture of container images it is important to identify all software packages present in the image. The SCA scan can be used to identify programming language-based software packages inside the image. In addition, metadata information for each image layer is also provided. The SCA scan detects packages for these programming languages: Java, Python, Go, Node.js, .NET.

SCA scanning is supported for all sensor types – General, Registry and CI/CD. It's supported for Docker Runtime only. SCA scanning is only supported when scanning container images. SCA scanning is not supported for Mac OS.

Prerequisites

- The SCA Scanning feature must be enabled for your subscription. Contact Qualys Support to have this feature enabled.
- Update your sensors to version 1.19 or later
- Relaunch your sensors with the parameter **--perform-sca-scan** to perform SCA scanning.

How it Works

SCA scanning is not performed by default. Users must enable SCA scanning using the new parameter **--perform-sca-scan**. The SCA scan is performed after a standard vulnerability scan (Static or Dynamic) on your container images. When the SCA scan completes, the sensor uploads the metadata information collected by the scan to the Qualys backend where posture evaluation is performed. You can view SCA scan data findings in the Container Security UI and API as part of image details. Vulnerability detections found by the SCA scan are presented as QIDs. Use filters to identify the scan type (SCA, Dynamic or Static) used to detect each vulnerability.

New Parameters

This release introduces 3 new parameters for SCA scanning.

Parameter	Description
--perform-sca-scan	(Optional) By default, SCA scanning is not performed. Use this parameter to enable SCA scanning for container images. When specified, the SCA scan will be performed after a standard vulnerability scan (Static or Dynamic). The SCA scan is attempted even when the vulnerability scan is not successful.
--disallow-internet-access-for-sca-scan	(Optional when --perform-sca-scan is specified) By default, SCA scans run in online mode. Use this parameter to disable Internet access for the SCA scan and run the scan in offline mode. Note - We recommend you run the SCA scan in online mode. Quality of software package enumeration for Java substantially degrades when the SCA scan is run in offline mode. The remote maven repository may need to be consulted for an accurate package detection. This can affect accuracy of the vulnerability posture of the image.
--sca-scan-timeout-in-seconds={value}	(Optional when --perform-sca-scan is specified) The default SCA scan command timeout is 5 minutes (300 seconds). Use this parameter to overwrite the default timeout with a new value specified in seconds. For example, you may need to increase the SCA scan timeout when scanning large container images to ensure the SCA scan has time to finish.

Sample Commands

To perform SCA scanning, you'll need to specify **--perform-sca-scan** as a command line parameter for "installsensor.sh" script or provide it as a command or args parameter when deploying a sensor. See details below.

Installsensor.sh Command

Specify **--perform-sca-scan** as a command line argument for installsensor.sh script.

```
sudo ./installsensor.sh ActivationId=<Activation id> CustomerId=<Customer id>
Storage=/usr/local/qualys/sensor/data -s --perform-sca-scan
```

In the following example, we'll enable SCA scanning, plus run the SCA scan in offline mode and increase the SCA scan timeout to 15 minutes (900 seconds).

```
sudo ./installsensor.sh ActivationId=<Activation id> CustomerId=<Customer id>
Storage=/usr/local/qualys/sensor/data -s --perform-sca-scan --disallow-
internet-access-for-sca-scan --sca-scan-timeout-in-seconds=900
```

Docker Run Command

Specify **--perform-sca-scan** as part of the Docker run command when deploying a sensor.

```
sudo docker run -d --restart on-failure -v
/var/run/docker.sock:/var/run/docker.sock:ro -v
/usr/local/qualys/sensor/data:/usr/local/qualys/qpa/data -e
ACTIVATIONID=<Activation id> -e CUSTOMERID=<Customer id> -e POD_URL=<POD
URL> --net=host --name qualys-container-sensor qualys/qcs-sensor:latest
--perform-sca-scan
```

Yaml Argument

Add **--perform-sca-scan** argument in args section of yaml, as shown below.

```
args: ["--k8s-mode", "--perform-sca-scan"]
```