

Container Security

Release Notes for Sensor

Version 1.3.0

July 26, 2019

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

Static scanning of Docker images

The sensor will perform static scanning for docker images as a fallback mechanism to current dynamic scanning in case docker images does not have a shell. Static scanning will not be performed on Docker container or Docker images having a shell.

Static scanning collects the list of installed software from the Docker image file system to find vulnerabilities in the Docker images. The installed software list is retrieved from the Package manager metadata files. Package managers supported are RPM, DPKG and Alpine.

Static scanning for Docker images without shell is disabled by default and you can enable it by contacting Qualys Support.

Fixed Issue

- Fixed an issue where the sensor was trying to rescan docker images/containers that do not have a shell, resulting in scan failure. Now you can enable static scanning for such images/containers.
- Fixed an issue where upon extracting the Container Sensor tar file, the Container Sensor home directory had access permission 755 instead of 700, which resulted into denying SSH access.