Qualys Container Security

Release Notes for Sensor

Version 1.26
June 26, 2023

What's New?

Detecting Container Secrets

Container secrets are digital credentials providing identity authentication and authorizing access to privileged accounts, applications, and services. They can include passwords, API keys, and other credentials that are needed for applications to function properly. If these secrets are not properly secured, they can be accessed by unauthorized users, leading to malicious attacks. Therefore, discovering secrets is one of the important aspects of container security that organizations must prioritize to protect their sensitive data, meet compliance requirements, and reduce the risk of security incidents.

Starting this release, Container Security can now detect secrets within container images. For more information about secret detection, see Online Help: Detecting Container Secrets.

To collect the secrets data, you need to install the sensor with the following parameter:

Argument	Examples
--perform-secret-detection	• **Using docker run:** `docker run -d --restart on-failure --cpus=0.2 -v /var/run/docker.sock:/var/run/docker.sock:ro -v <client cert directory on the docker host>:/root/.docker -v /usr/local/qualys/sensor/data:/usr/local/qualys/qpa/data -e ACTIVATIONID=<Activation id> -e CUSTOMERID=<Customer id> -e POD_URL=<PODURL> -e DOCKER_TLS_VERIFY=1 -e DOCKER_HOST=<IPv4 or FQDN>:<port#> --net=host --name qualys-container-sensor qualys/qcs-sensor:latest --log-level 5 --perform-sca-scan` **`--perform-secret-detection`** • **Using installsensor.sh:** `sudo ./installsensor.sh ActivationId=<Activation id> CustomerId=<Customer id> Storage=/usr/local/qualys/sensor/data -s -c` **`--perform-secret-detection`** • **Using yaml file:** Add the "--perform-secret-detection" parameter to args: `args: ["--k8s-mode",` **`"--perform-secret-detection"`**`]`

Notes:

- Secret detection is supported only on:
  - **Sensors**: CICD and registry
  - **OS**: Linux
  - **Runtimes**: Docker, Containerd, and CRI-O
- In case of existing sensors, you need to reinstall the sensor with the `--perform-secret-detection` argument.
- The `--sca-scan-timeout-in-seconds` or `SCAScanTimeoutInSeconds` argument is now used for setting a timeout for both SCA and secret detection.
- Secret detection involves scanning the filesystem. It does not detect secrets that are stored as environment variables or passed as arguments within the image. Therefore, the performance of secret detection depends on the number of files present in the image.

For more information, see Sensor Deployment Guide.