Container Security

Release Notes for Sensor

Version 1.6.0

September 15, 2020

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

Introducing Docker RBAC Support

With this release you can better control how the sensor authenticates to the docker daemon and what access controls the sensor is allowed.

By default, the sensor talks directly to the docker UNIX socket and uses unauthenticated access. Now we've added TCP/TLS socket support for additional security. When you enable TLS authentication on the sensor, the sensor will communicate with the docker daemon over TLS so the connection is secure and authenticated. During sensor installation, you'll include new parameters to enable TLS authentication and specify the TLS client certificate path (CA certificate filename, client certificate filename, docker client key filename).

Further, you can now control what actions the sensor can take through a docker Role Based Access Control (RBAC) policy. For this you can use the Open Policy Agent (OPA) docker plugin. With OPA, you'll create rego rules that define permissions for the sensor, for example only allow the sensor to delete containers that were created for scanning.

How to deploy:

1) Enable TLS authentication on the docker daemon. Please refer to https://docs.docker.com/engine/security/https/.

2) Deploy the Open Policy Agent (OPA) docker plugin. Please refer to https://www.openpolicyagent.org/docs/latest/docker-authorization/.

3) Create policy rego rules for Qualys user to define permissions.

4) Generate a client certificate for Qualys sensor.

5) Deploy the sensor so that it uses docker TLS socket. Please follow Qualys Container Security Sensor Deployment Guide for detailed instructions.