Tech’N’Talk - kube-bench

Liz Rice

@LizRice | @AquaSecTeam
The container lifecycle and security

<table>
<thead>
<tr>
<th>(1) Image Assurance</th>
<th>(2) Environment Hardening</th>
<th>(3) Protect Secrets</th>
<th>(4) Least Privileges Runtime</th>
<th>(5) Network Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Image Assurance</td>
<td>Environment Hardening</td>
<td>Protect Secrets</td>
<td>Least Privileges Runtime</td>
<td>Network Controls</td>
</tr>
</tbody>
</table>

Diagram:

1. Image
2. Registry
3. Container Engine
4. Host 1
5. Host 2

Network Controls

Diagram shows the flow from Image to Registry to Container Engine, indicating the lifecycle steps.
CIS Kubernetes Benchmark

- 200+ pages of best practices and tests
  - [https://www.cisecurity.org/benchmark/kubernetes/](https://www.cisecurity.org/benchmark/kubernetes/)
- Tests for workers, masters and federated nodes
kube-bench

- github.com/aquasecurity/kube-bench

- Open source (not just for Aqua Security customers!)

- Configurable tests

- JSON format output
Automating compliance

- CIS Docker
- PCI DSS

“Implement automated audit trails for all system components to reconstruct all actions taken by any individual with root or administrative privileges.”
OpenShift Origin security

Introduction

About This Guide
What Are Containers?
Container Security in OpenShift Origin

About This Guide

This guide provides a high-level walkthrough of the container security measures available in OpenShift Origin, including solutions for the host layer, the container and orchestration layer, and the build and application layer. This guide contains the following information:

• Why container security is important and how it compares with existing security standards.
Open issue for OpenShift config in kube-bench

https://github.com/aquasecurity/kube-bench/issues/23
Released today! manifesto

https://github.com/aquasecurity/manifesto

Store metadata alongside container images in registry
Get, list and put metadata associated with images
github.com/aquasecurity/kube-bench
github.com/aquasecurity/manifesto

@LizRice  |  @AquaSecTeam