Qualys Container Security
Comprehensive Security for the ever-changing Container Stack

Asif Awan
CTO, Container Security, Qualys, Inc.
Agenda

Container Advantages
Container Deployments
Visibility & Control Challenges
Qualys Container Security Solution
Demo
Q&A
Everybody Loves Containers

Portability

Agility

Density
Container Deployments
Deployment Scenario #1

Use Case

1. Shrinking infrastructure, as organizations continue migration to the cloud
2. Containers deployed within Virtual Machines
3. But organizations still have the overhead and costs of the hypervisor and virtual machines
Use Case

1. The orchestration battle ends with Kubernetes winning 80% of the market
2. But organizations struggle to scale their own Kubernetes clusters
Deployment Scenario #3

**Use Case**

1. Container-as-a-Service and Orchestration-as-a-Service adoption accelerate container adoption
2. Now where do you put security?
Container Lifecycle Challenges

**Build**
- What's in the images?
- Vulnerabilities?
- OSS license exposure?
- Solution disruptive to my CI Pipeline?
- Scanning report integrated with bug tracking?

**Ship**
- Registry scanning?
- Enforce compliance?
- Vulnerability, package and license-based rules?
- Vulnerability impact notifications?

**Run**
- How to protect host?
- Container engine configured correctly?
- Container orchestration configured correctly?
- Runtime app visibility?
- Runtime app protection?
Qualys Container Security
Qualys Container Security

- Host Protection
- CIS Benchmarks
- Protection for container infrastructure stack

- Scanning & Compliance
- Accurate insight and control of container images

- Visibility & Protection
- Automated analysis and enforcement of container behavior
Demo
### Image Details: php

<table>
<thead>
<tr>
<th>Detail</th>
<th>Compliance Sunburst</th>
<th>Vulnerability Sunburst</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scan Date</td>
<td>2018-11-12T23:47:19.2Z</td>
<td></td>
</tr>
<tr>
<td>Scan Status</td>
<td>done</td>
<td></td>
</tr>
<tr>
<td>Registry</td>
<td>5be9e64b9d30760001014780</td>
<td></td>
</tr>
<tr>
<td>Image Tags</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Compliance</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Layers</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Total Vulnerabilities: 273

<table>
<thead>
<tr>
<th>Package</th>
<th>CVE</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td>util-linux 2.29.2-1+deb9u1</td>
<td>CVE-2016-2779</td>
<td>High</td>
</tr>
<tr>
<td>tar 1.29b-1.1</td>
<td>CVE-2006-2541</td>
<td>Negligible</td>
</tr>
<tr>
<td>systemd 232-25+deb9u4</td>
<td>CVE-2018-6954</td>
<td>High</td>
</tr>
<tr>
<td>systemd 232-25+deb9u4</td>
<td>CVE-2018-1049</td>
<td>Medium</td>
</tr>
<tr>
<td>systemd 232-25+deb9u4</td>
<td>CVE-2013-4392</td>
<td>Negligible</td>
</tr>
</tbody>
</table>
Top 10 Containers and Images by Activity

Containers

<table>
<thead>
<tr>
<th>Name</th>
<th>Anomalies</th>
</tr>
</thead>
<tbody>
<tr>
<td>location: aws-east-1</td>
<td></td>
</tr>
<tr>
<td>host: prod-domain-291</td>
<td></td>
</tr>
<tr>
<td>host: prod-load286</td>
<td></td>
</tr>
<tr>
<td>service: oracle</td>
<td></td>
</tr>
<tr>
<td>service: systemd</td>
<td></td>
</tr>
<tr>
<td>service: sshd</td>
<td></td>
</tr>
<tr>
<td>service: java</td>
<td></td>
</tr>
<tr>
<td>host: prod-spp-257</td>
<td></td>
</tr>
<tr>
<td>host: prod-web-291</td>
<td></td>
</tr>
</tbody>
</table>
Process /usr/sbin/httpd was blocked from executing /bin/sh. Severity: High

Raw log:

<table>
<thead>
<tr>
<th>Process</th>
<th>Process ID</th>
<th>Call</th>
<th>Arguments</th>
<th>Action</th>
<th>Time</th>
</tr>
</thead>
</table>

Processes executing /usr/sbin/httpd:

- /usr/sbin/httpd

Processes accessing /usr/sbin/httpd:

- /usr/sbin/httpd
Thank You

Asif Awan
aawan@qualys.com