The Need to Shift Left and What It Means to Security

Alex Mandernack
Security Solution Architect
Product Management
Qualys, Inc
Traditional World

Each app team builds their own image (CentOS v1, v2, v3)

PenTest report to Dev (t0+1Mo)
- Dev team dealing with out of date findings
- Not machine readable
- Repeated work across apps 1, 2, 3 (OS level vulns)
- Not doing it often enough due to cost, efficient reasons

Deploy application (1, 2, 3)

Scan in production (VM, WAS, PC etc.)
- Findings for app 1, 2, 3
- Separate patching workflows for running production workloads (v1, v2, v3)

Inefficiencies, slows things down, no standardization across teams, repetition in security workflows
The Driver: Scale, Elasticity & DevOps Pipeline

aws

containerd
docker
cri-o
openshift
kubernetes
Can Security Teams do Better?
Shifting Security to the Left

- Developers and security teams must think about security, sooner
- Get security tools into the process earlier
- Automate! Leverage API’s, CI plugins
- Golden images
- Scan in the CI pipeline
  - Vulnerability gates in the pipeline
  - Vulnerability information at the fingertips of Dev
The New Role of the Security Team

- Must not be a roadblock
- Provide security tooling that is self-service for DevOps, Dev
  - CI Plugins
  - APIs
  - Scripting
- Verify and audit the process
  - Dashboards/live data
  - Trending
Shift Left with Qualys!

Build base hardened OS Golden Image (to be used by multiple teams)

Rebuild with fixes from issues identified from staging

Dev teams use Golden Image and build app on top

Rebuild with fixes from issues identified from staging

Deploy
- Qualys VM, WAS, PC active scans
- Find less stuff due to standardization, shift left

CI/CD Scan
- Jenkins VM
- Jenkins PC

CI/CD Scan + Gate
- Jenkins VM
- Jenkins WAS
- Jenkins PC

Golden Image

Build/Load Application

Runtime
Qualys Jenkins Plugin

Available on the Jenkins Marketplace
- Vulnerability Management
- Container Security
- Web Application Scanning
- API Security
Secure the CI Pipeline
Jenkins Vulnerability Management Plugin
Jenkins WAS Plugin
Jenkins Container Security Plugin

BUILD REPORT - e8d112ff7588

Build Status: Failed
Image ID: e8d112ff7588
Size: 828 MB

Build Summary
The vulnerabilities count by severity for image e8d112ff7588 exceeded one of the configured threshold values:
Configured: Severity 1 > 0, Severity 2 > 0, Severity 3 > 0, Severity 4 > 0, Severity 5 > 0.

INSTALLED SOFTWARE

<table>
<thead>
<tr>
<th>Name</th>
<th>Installed Version</th>
<th>Fixed In Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>libmagickwand-dev</td>
<td>8.6.9.7.4+dfsg-11+deb9u3</td>
<td>8.6.9.7.4+dfsg-11+deb9u4</td>
</tr>
<tr>
<td>libmagickwand-6-headers</td>
<td>8.6.9.7.4+dfsg-11+deb9u3</td>
<td>8.6.9.7.4+dfsg-11+deb9u4</td>
</tr>
<tr>
<td>libmagickcore-dev</td>
<td>8.6.9.7.4+dfsg-11+deb9u3</td>
<td>8.6.9.7.4+dfsg-11+deb9u4</td>
</tr>
<tr>
<td>libmagickcore-6-headers</td>
<td>8.6.9.7.4+dfsg-11+deb9u3</td>
<td>8.6.9.7.4+dfsg-11+deb9u4</td>
</tr>
<tr>
<td>imagemagic-6.q16</td>
<td>8.6.9.7.4+dfsg-11+deb9u3</td>
<td>8.6.9.7.4+dfsg-11+deb9u4</td>
</tr>
</tbody>
</table>
Demo
Qualys GitHub

Automation scripts

Reporting scripts

Open Source community

https://github.com/Qualys
Thank you

Alex Mandernack
amandernack@qualys.com