Demystifying DevSecOps practices and tooling in container environments

Neil Carpenter
Sr. Principal Solution Architect, Advanced Cluster Security

Dave Meurer
Global Principal Solutions Architect, Security ISVs
Comprehensive DevSecOps with Red Hat

Secure open hybrid cloud technologies

Red Hat
- Infrastructure
- Container and Kubernetes
- Automation and management
- Application development
- Hosted offerings

Partner ecosystem
- Certified containers and operators
- Secure the entire lifecycle
- Automate security operations center
- IBM collaboration

Enhance and extend

Culture, process, and implementation
Red Hat Consulting | Red Hat Open Innovation Labs | Managed services & partner consulting | Managed services

Red Hat Training and Certification

#securitysymposium
DevSecOps Culture

“Culture eats strategy for breakfast”

Training
Train developers on secure coding practices.
OWASP Top 10, CVE, CWE.

Risk Focus
Focus on Critical & High vulnerabilities. Trying to resolve every vulnerability is not practical and a time sink.

Speed and Accuracy Balance
Look for the most optimal balance of accuracy, speed, and efficiency in your environment.

Transparency
Eliminate silos. Promote collaboration and teamwork. Provide visibility into Ops tools. Transparency = Trust.

Shared Goals
Everyone is responsible for security. Define and measure KPIs throughout the pipeline.

Automate Security
Automate security at every point in the lifecycle without sacrificing speed and agility.

Security Expertise
Integrate security staff into the DevOps teams with a core responsibility for DevSecOps expertise and ownership.
Shared Goals / KPIs

- Reduce Application security issues discovered in test and production
- Percentage of deployments stopped due to failed policies
- Time to fix security issues
## DevSecOps Framework Categories

<table>
<thead>
<tr>
<th>Application Analysis</th>
<th>Identity &amp; Access Mgmt</th>
</tr>
</thead>
<tbody>
<tr>
<td>Compliance</td>
<td>Network Controls</td>
</tr>
<tr>
<td>Data Controls</td>
<td>Runtime Analysis &amp; Protection</td>
</tr>
<tr>
<td>Audit &amp; Monitoring</td>
<td>Remediation</td>
</tr>
</tbody>
</table>

**Platform Security**
<table>
<thead>
<tr>
<th>Application Analysis</th>
<th>Identity &amp; Access Mgmt</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAST, SCA, IAST, DAST, Config Management, Image Risk</td>
<td>Authn, Authz, Secrets Vault, HSM, Provenance</td>
</tr>
<tr>
<td>Compliance</td>
<td>Network Controls</td>
</tr>
<tr>
<td>Regulatory Compliance Audit, Compliance Controls/Remediation</td>
<td>CNI Plugins, Network Policies, Traffic Controls, Service Mesh, Visualization, Package Analysis, API Management</td>
</tr>
<tr>
<td>Data Controls</td>
<td>Runtime Analysis &amp; Protection</td>
</tr>
<tr>
<td>Data Protection and Encryption</td>
<td>Admission Controller, Application Behavior Analysis, Threat Defense</td>
</tr>
<tr>
<td>Audit &amp; Monitoring</td>
<td>Remediation</td>
</tr>
<tr>
<td>Cluster Monitoring, SIEM, Forensics</td>
<td>SOAR, Automatic resolution</td>
</tr>
<tr>
<td>Platform Security</td>
<td></td>
</tr>
<tr>
<td>Secure Host, Container Platform, Namespace, Isolation, k8s &amp; Container Hardening</td>
<td></td>
</tr>
</tbody>
</table>
Partners & Use Cases

Partners Extend and Enhance Red Hat functionality to Secure the entire DevOps Lifecycle and solve critical use cases

<table>
<thead>
<tr>
<th>Application Analysis</th>
<th>Identity &amp; Access</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAST, SCA, IAST, DAST, Config Mgmt, Image Risk</td>
<td>Authn, Authz, Secrets Vault, HSM, Provenance</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Compliance</th>
<th>Network Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Regulatory Compliance Audit &amp; Controls</td>
<td>CNI, Policies, Traffic Controls, Service Mesh, Packet Analysis, API, Visualization</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Data Controls</th>
<th>Runtime Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data Protection and Encryption</td>
<td>Admission Control, Behavioral, Threat Defense</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Audit &amp; Monitoring</th>
<th>Remediation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cluster Monitoring, SIEM, Forensics</td>
<td>SOAR, Automatic resolution</td>
</tr>
</tbody>
</table>

---

#securitysymposium

Red Hat Platform
Secure Host, Container Platform, Namespace Isolation, k8s & Container Hardening
DevSecOps Lifecycle and Security Methods

**Phase**
- **Code**
- **Build**
- **Test**
- **Release**
- **Deploy**
- **Operate**
- **Monitor & Optimize**

**Context**
- Source
- Binary Repository

**Tools**
- IDE
- Source Code Management
- Build Automation
- Container Registry
- Container Orchestration
- Cluster

**Security Methods**
- SCA
- SAST
- Authn / Authz
- Secrets Vault
- Image Risk
- Config Management
- SAST
- IASt
- DAST
- Authn / Authz
- Secrets Vault
- Compliance Audit
- Network Policies
- Compliance Controls
- CNI Plugins
- Network Policies
- Data Encryption
- Data Protection
- Monitoring
- Container Platform
- Isolation

**Categories**
- Application Analysis
- Identity & Access
- Compliance
- Network Controls
- Data Controls
- Runtime Analysis
- Audit & Monitoring
- Remediation
- Platform Security

**#securitysymposium**
Red Hat, ACS, Zettaset, CyberArk, Synopsys
DevSecOps Solution

Phase
- Code
- Build
- Test
- Release
- Deploy
- Operate
- Monitor & Optimize

Context
- Source

Tools
- IDE
- Source Code Management
- Build Automation
- Container Registry
- Container Orchestration
- Cluster

Categories:
- Application Analysis
- Identity & Access
- Compliance
- Network Controls
- Data Controls
- Runtime Analysis
- Remediation
- Audit & Monitoring
- Platform Security

Red Hat, ACS, Zettaset, CyberArk, Synopsys
DevSecOps Solution

Synopsys
- SCA
- SAST
- Secret Management
- Secrets Vault

CyberArk
- SCA
- SAST
- Secret Management
- Secrets Vault

Red Hat
- SCA
- Image Risk
- Config Management
- Secrets Vault
- Authn / Authz

Zettaset
- Compliance Audit
- Data Encryption
- Data Protection
- Network Controls
- Admission Control
- Behavioral Analysis
- Threat Defense
- Logging
- SIEM
- Forensics
- SOAR
- Auto Resolution
- Secure Host
- Container Platform
- Isolation
- Cluster Hardening

CI/CD
- Config Management
- Secrets Vault
- Provenance
- Compliance Audit
- Network Policies

Container Orchestration
- DAST
- IAST
- SAST
- Config Management
- Secrets Vault
- Authn / Authz

Build Automation
- Source Code Management
- Build
- Container Registry
- Container Orchestration
- Cluster

Image
- Binary Repository

Cluster
- Packet Analysis
- Compliance Controls
- Traffic Controls
- Service Mesh
- CNI Plugins
- Packet Analysis
- API Management

Red Hat
- CodeReady
- Image Quay
- OpenShift

Source
- Cluster Hardening
- Network Visualization
- Remedia
- Audit & Monitoring
- Platform Security

Target
- Container
- Network Policies
- Image Risk
- SCA
- Secrets Vault
- Compliance Audit
- Authn / Authz
- Secrets Vault
- Authn / RBAC
- Compliance Controls
- Data Encryption
- Data Protection
Red Hat, Zettaset, CyberArk, Synopsys DevSecOps Solution

KPI
Reduce Application security issues discovered in test and production

Categories:
- Application Analysis
- Identity & Access
- Compliance
- Network Controls
- Data Controls
- Runtime Analysis
- Audit & Monitoring
- Remediation
- Platform Security
**Image Check**

- Image melcar/docker-test:0.1.214 failed policy 'Fixable CVSS >= 7' (policy enforcement caused failure)

  - Description:
    - Alert on deployments with fixable vulnerabilities with a CVSS of at least 7
  
  - Rationale:
    - Known vulnerabilities make it easier for adversaries to exploit your application. You can fix these high-severity vulnerabilities by updating to a newer version of the affected component(s).

    This is policy SEC-9918-001, which specifies that builds cannot be promoted until this issue is resolved.

  - Remediation:
    - Use your package manager to update to a fixed version in future builds or speak with your security team to mitigate the vulnerabilities.

- Fixable CVE-2015-5297 (CVSS 9.8) found in component 'pixman' (version 0.32.6-3), resolved by version 0.32.6-3+deb8u1
- Fixable CVE-2015-5608 (CVSS 8.5) found in component 'openssh' (version 1:6.7p1-5+deb8u3), resolved by version 1:6.7p1-5+deb8u6
- Fixable CVE-2015-8947 (CVSS 7.6) found in component 'harfbuzz' (version 0.9.35-2), resolved by version 0.9.35-2+deb8u1
- Fixable CVE-2015-9290 (CVSS 9.8) found in component 'freetype' (version 2.5.2-3+deb8u2), resolved by version 2.5.2-3+deb8u3
- Fixable CVE-2015-9381 (CVSS 8.8) found in component 'freetype' (version 2.5.2-3+deb8u2), resolved by version 2.5.2-3+deb8u2
- Fixable CVE-2016-10009 (CVSS 7.3) found in component 'openssh' (version 1:6.7p1-5+deb8u3), resolved by version 1:6.7p1-5+deb8u3
- Fixable CVE-2016-10012 (CVSS 7.8) found in component 'openssh' (version 1:6.7p1-5+deb8u3), resolved by version 1:6.7p1-5+deb8u3
- Fixable CVE-2016-10708 (CVSS 7.5) found in component 'openssh' (version 1:6.7p1-5+deb8u3), resolved by version 1:6.7p1-5+deb8u3
apiVersion: v1
kind: Pod
metadata:
  name: security-context-demo
spec:
  securityContext:
    runAsUser: 10000
    runAsGroup: 30000
    fsGroup: 20000
volumes:
- name: sec-ctx-vol
  emptyDir: {}
containers:
- name: sec-ctx-demo
  image: busybox
  resources:
    requests:
      memory: "64Mi"
      cpu: "250m"
  command: [ "sh", "-c", "sleep 1h" ]
  volumeMounts:
- name: sec-ctx-vol
  mountPath: /data/demo
  securityContext:
    allowPrivilegeEscalation: false
```bash
tmp kube-linter lint pod.yaml

KubeLinter 0.2.2

pod.yaml: (object: <no namespace>/security-context-demo /V1, Kind=Pod) container "sec-ctx-demo" does not have a read-only root file system (check: no-read-only-root-fs, remediation: Set readOnlyRootFilesystem to true in the container securityContext.)

pod.yaml: (object: <no namespace>/security-context-demo /V1, Kind=Pod) container "sec-ctx-demo" has cpu limit 0 (check: unset-cpu-requirements, remediation: Set CPU requests and limits for your container based on its requirements. Refer to https://kubernetes.io/docs/concepts/configuration/manage-resources-containers/#requests-and-limits for details.)

pod.yaml: (object: <no namespace>/security-context-demo /V1, Kind=Pod) container "sec-ctx-demo" has memory limit 0 (check: unset-memory-requirements, remediation: Set memory requests and limits for your container based on its requirements. Refer to https://kubernetes.io/docs/concepts/configuration/manage-resources-containers/#requests-and-limits for details.)

Error: found 3 lint errors
```
Red Hat, Zettaset, CyberArk, Synopsys

**KPI**

**Time to fix security issues**
<table>
<thead>
<tr>
<th>Name</th>
<th>Created</th>
<th>Cluster</th>
<th>Namespace</th>
<th>Priority</th>
</tr>
</thead>
<tbody>
<tr>
<td>tekton-triggers-webhook</td>
<td>05/24/2021 12:03:50PM</td>
<td>production</td>
<td>openshift-pipelines</td>
<td>8</td>
</tr>
<tr>
<td>reporting</td>
<td>05/24/2021 12:03:50PM</td>
<td>production</td>
<td>medical</td>
<td>9</td>
</tr>
<tr>
<td>tekton-triggers-controller</td>
<td>06/04/2021 12:03:50PM</td>
<td>production</td>
<td>openshift-pipelines</td>
<td>11</td>
</tr>
<tr>
<td>concourse-ci-postgresql</td>
<td>06/04/2021 12:03:50PM</td>
<td>production</td>
<td>default</td>
<td>15</td>
</tr>
<tr>
<td>tekton-pipelines-controller</td>
<td>05/24/2021 12:03:50PM</td>
<td>production</td>
<td>openshift-pipelines</td>
<td>16</td>
</tr>
<tr>
<td>tekton-operator-proxy-webhook</td>
<td>05/24/2021 12:03:50PM</td>
<td>production</td>
<td>openshift-pipelines</td>
<td>17</td>
</tr>
<tr>
<td>concourse-ci-web</td>
<td>06/04/2021 12:03:50PM</td>
<td>production</td>
<td>default</td>
<td>18</td>
</tr>
<tr>
<td>puppet-master</td>
<td>05/24/2021 12:03:50PM</td>
<td>production</td>
<td>operations</td>
<td>21</td>
</tr>
<tr>
<td>proxy</td>
<td>05/24/2021 12:03:50PM</td>
<td>production</td>
<td>medical</td>
<td>24</td>
</tr>
<tr>
<td>tekton-pipelines-webhook</td>
<td>05/24/2021 12:03:50PM</td>
<td>production</td>
<td>openshift-pipelines</td>
<td>25</td>
</tr>
<tr>
<td>openshift-pipelines-operator</td>
<td>05/24/2021 12:03:50PM</td>
<td>production</td>
<td>openshift-operators</td>
<td>29</td>
</tr>
<tr>
<td>wordpress</td>
<td>05/24/2021 12:03:50PM</td>
<td>production</td>
<td>frontend</td>
<td>31</td>
</tr>
</tbody>
</table>
FROM debian:10

USER reporting

COPY --from-netflow /bin/entrypoint /bin/entrypoint

RUN chmod +x /bin/entrypoint

RUN touch /reporting
Thank you

Red Hat is the world’s leading provider of enterprise open source software solutions. Award-winning support, training, and consulting services make Red Hat a trusted adviser to the Fortune 500.