

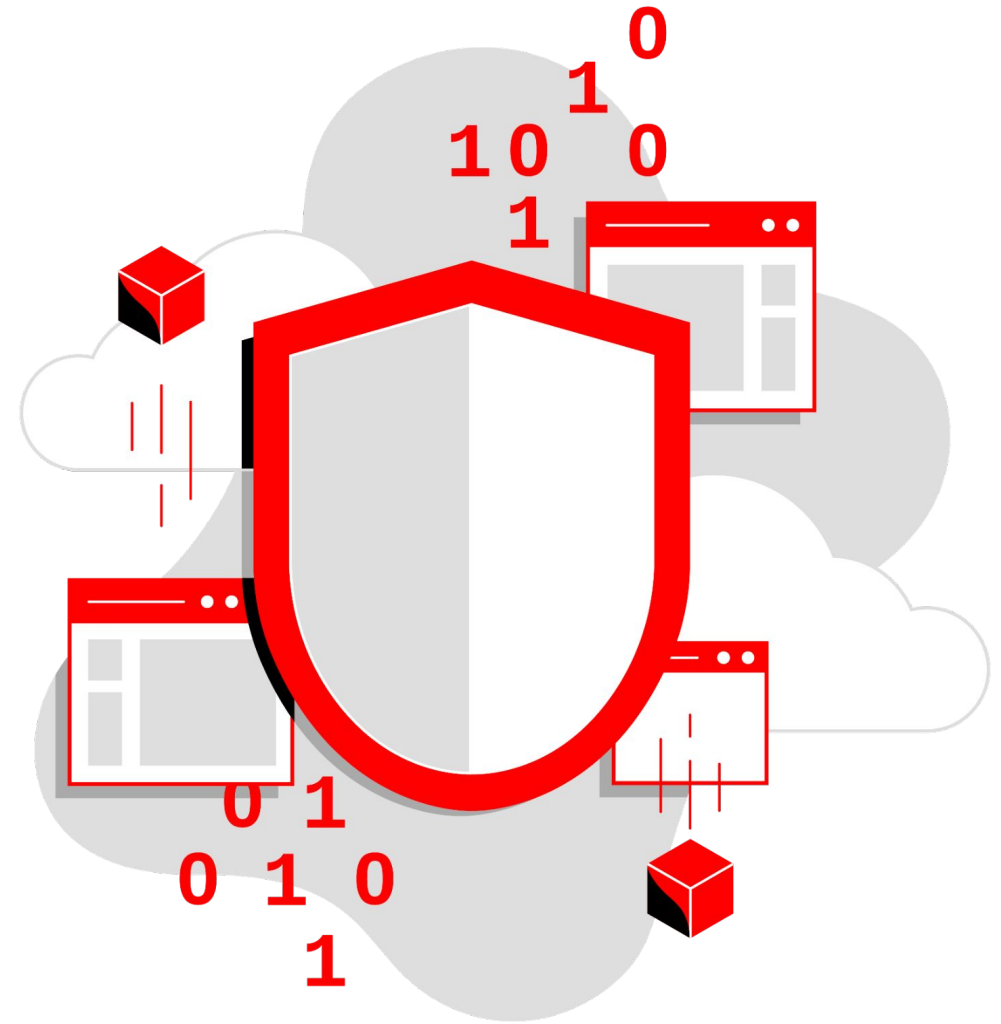


# Security Symposium

## 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



Enhance and extend

## Partner ecosystem

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

## Culture, process, and implementation

Red Hat Consulting | Red Hat Open Innovation Labs | Managed services & partner consulting | Managed services

## Red Hat Training and Certification

# 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

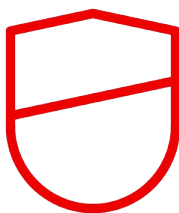
Automate security at every point in the lifecycle without sacrificing speed and agility.



## Security Expertise

Integrate security staff into the DevOps teams with a core responsibility for DevSecOps expertise and ownership.

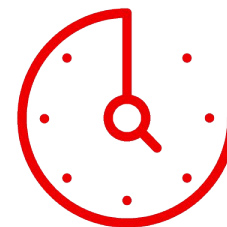
## Shared Goals / KPIs



Reduce Application security issues discovered in test and production



Percentage of deployments stopped due to failed policies



Time to fix security issues

# 9 DevSecOps Framework Categories

Application Analysis

Identity & Access Mgmt

Compliance

Network Controls

Data Controls

Runtime Analysis & Protection

Audit & Monitoring

Remediation

Platform Security

# 34 DevSecOps Framework Methods

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

# Partners & Use Cases


Partners Extend and Enhance Red Hat functionality to Secure the entire DevOps Lifecycle

and

solve critical use cases

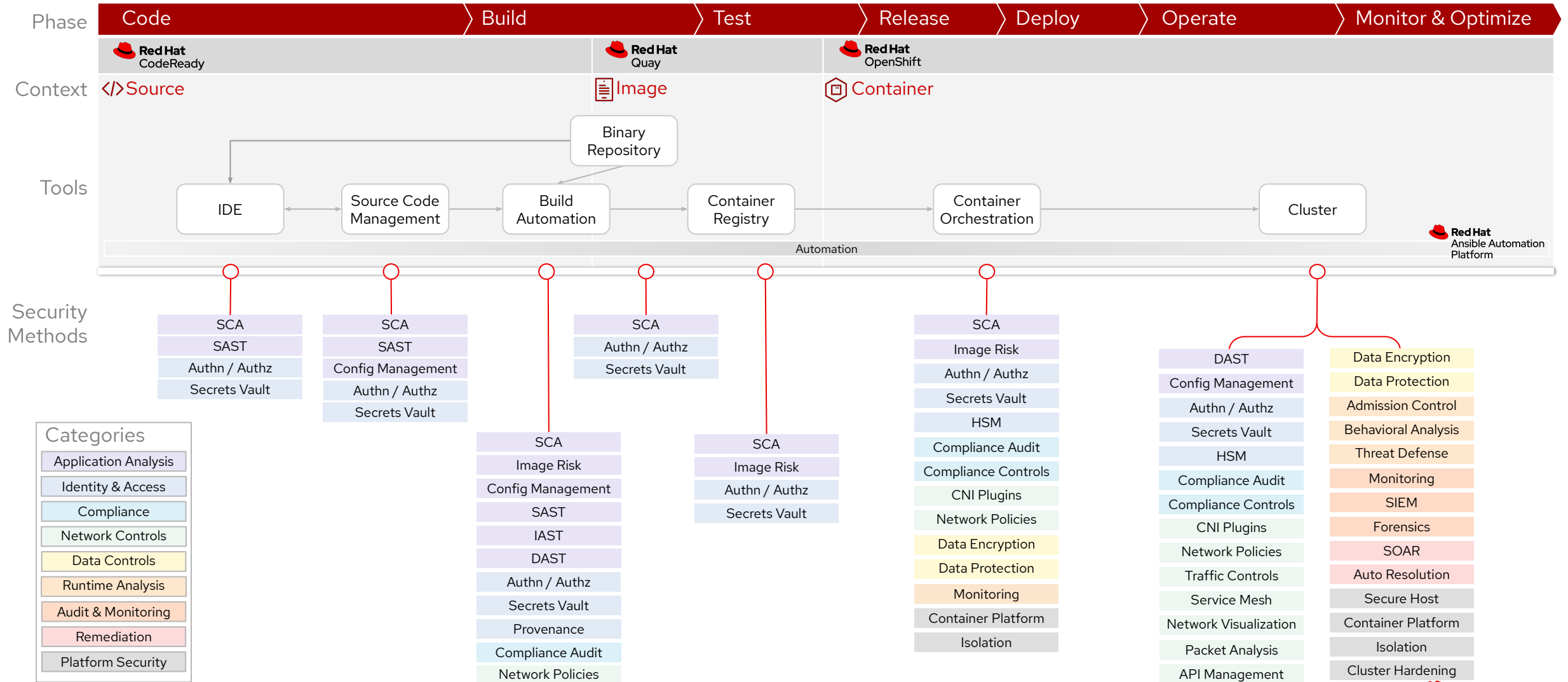
<b>Application Analysis</b> SAST, SCA, IAST, DAST, Config Mgmt, Image Risk	<b>Identity &amp; Access</b> Authn, Authz, Secrets Vault, HSM, Provenance
<b>Compliance</b> Regulatory Compliance Audit & Controls	<b>Network Controls</b> CNI, Policies, Traffic Controls, Service Mesh, Packet Analysis, API, Visualization
<b>Data Controls</b> Data Protection and Encryption	<b>Runtime Analysis</b> Admission Control, Behavioral, Threat Defense
<b>Audit &amp; Monitoring</b> Cluster Monitoring, SIEM, Forensics	<b>Remediation</b> SOAR, Automatic resolution



 <b>Red Hat Platform</b>
Secure Host, Container Platform, Namespace Isolation, k8s & Container Hardening

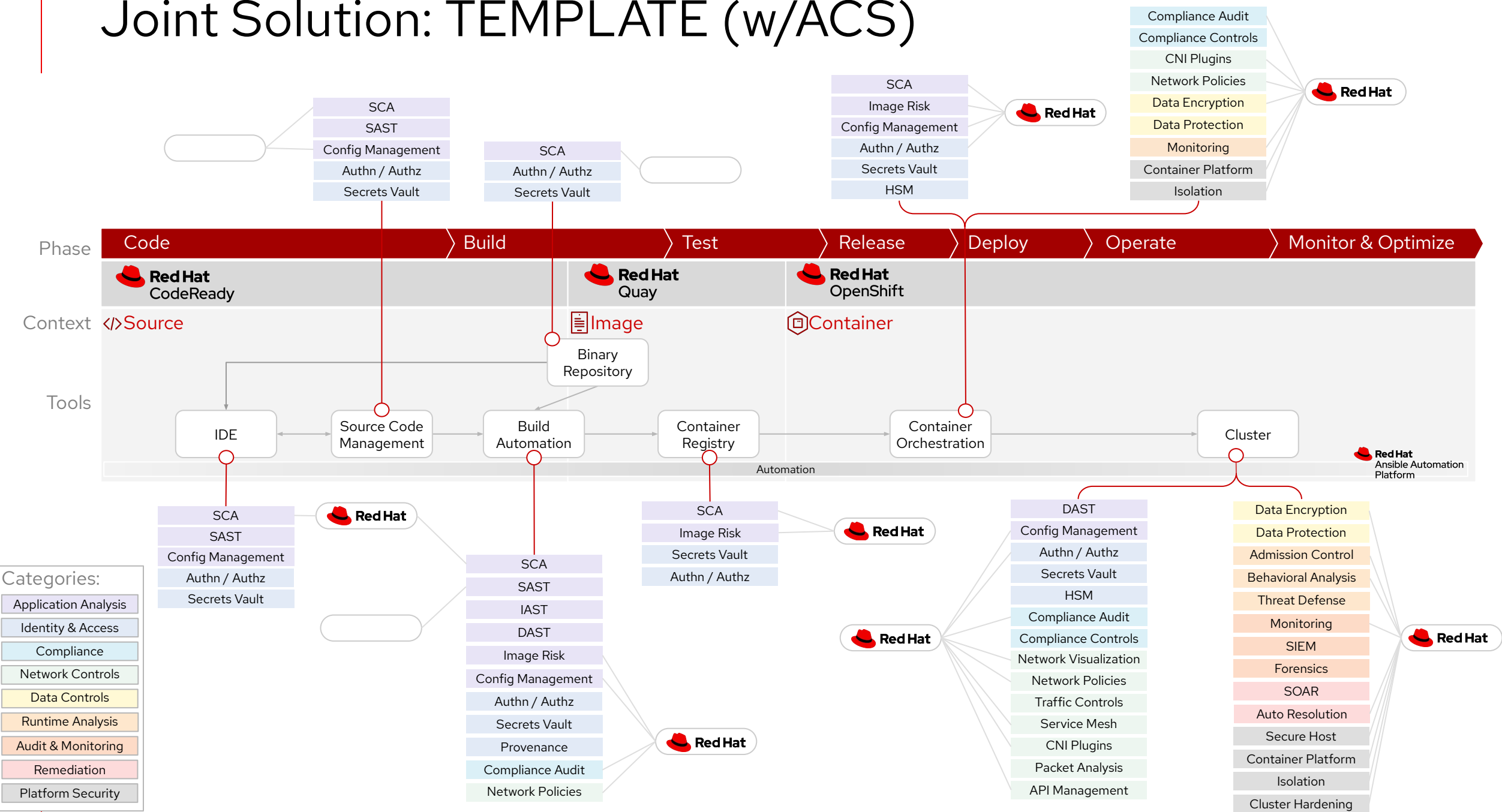


# DevSecOps Lifecycle and Security Methods

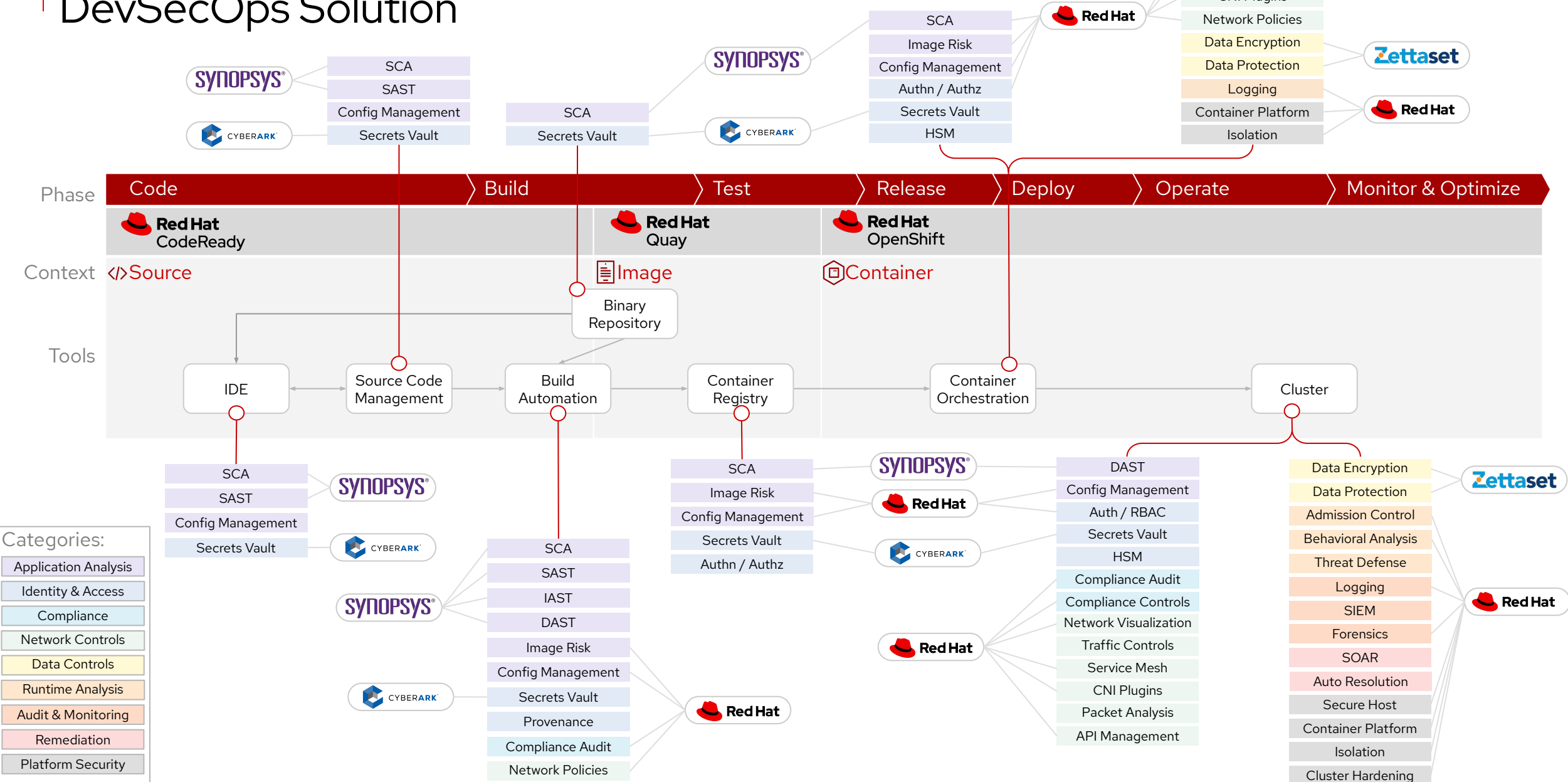




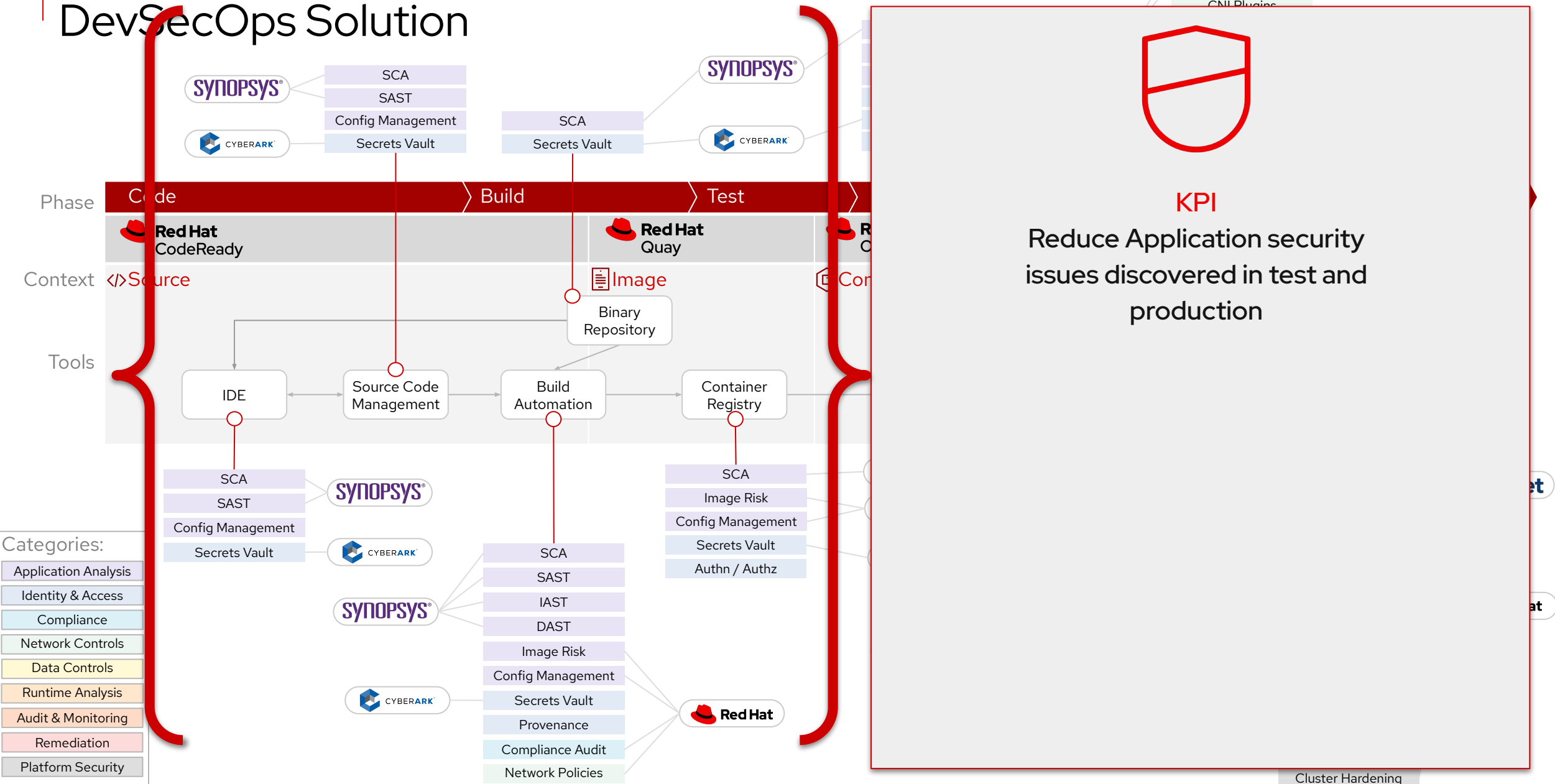
# Joint Solution: TEMPLATE (w/ACS)



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



# Red Hat, Zettaset, CyberArk, Synopsys DevSecOps Solution



PLR rox-pipeline-vg7o3u Failed

Actions ▾

[Details](#) [YAML](#) [Task Runs](#) [Logs](#) [Events](#)[Download](#) | [Download all task logs](#) | [Expand](#)

✓ image-scan

✗ image-check

image-check

✗ Image neilcar/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.

- Violations:

- 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-2015-5600 (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+deb8u4
- Fixable CVE-2016-10009 (CVSS 7.3) found in component 'openssh' (version 1:6.7p1-5+deb8u3), resolved by version 1:6.7p1-5+deb8u6
- Fixable CVE-2016-10012 (CVSS 7.8) found in component 'openssh' (version 1:6.7p1-5+deb8u3), resolved by version 1:6.7p1-5+deb8u6
- Fixable CVE-2016-10708 (CVSS 7.5) found in component 'openssh' (version 1:6.7p1-5+deb8u3), resolved by version 1:6.7p1-5+deb8u6



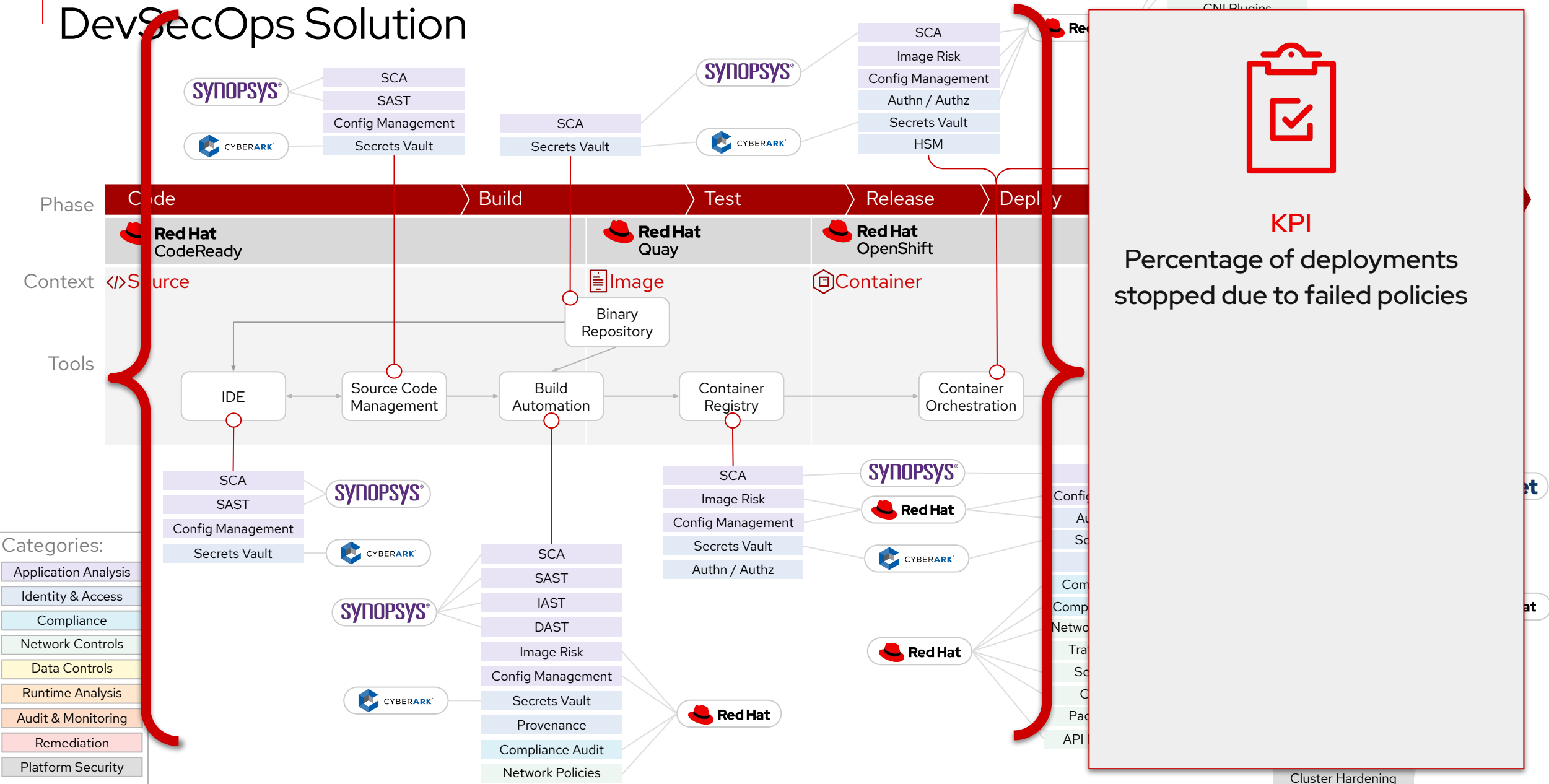
PLR rox-pipeline-vg7o3u Failed

Actions

Details YAML Task Runs Logs Events

	A	B	C	D	E	F	G	H	I
330	CVE-2016-4610	9.8	libxslt in Apple iC libxslt	1.1.28-2+deb8u	1.1.28-2+deb8u	RUN set -ex; apt-get update; apt-get install -y --no-install-recommends	autoconf	automake	bzip2 file g++ gcc imagemagick libbz2-dev libc6-dev lit
331	CVE-2019-1106	9.8	libxslt through 1. libxslt	1.1.28-2+deb8u	1.1.28-2+deb8u	RUN set -ex; apt-get update; apt-get install -y --no-install-recommends	autoconf	automake	bzip2 file g++ gcc imagemagick libbz2-dev libc6-dev lit
332	CVE-2016-4609	9.8	libxslt in Apple iC libxslt	1.1.28-2+deb8u	1.1.28-2+deb8u	RUN set -ex; apt-get update; apt-get install -y --no-install-recommends	autoconf	automake	bzip2 file g++ gcc imagemagick libbz2-dev libc6-dev lit
333	CVE-2016-7942	9.8	The XGetImage libx11	2:1.6.2-3	2:1.6.2-3+deb8u	RUN set -ex; apt-get update; apt-get install -y --no-install-recommends	autoconf	automake	bzip2 file g++ gcc imagemagick libbz2-dev libc6-dev lit
334	CVE-2016-7943	9.8	The XListFonts f libx11	2:1.6.2-3	2:1.6.2-3+deb8u	RUN set -ex; apt-get update; apt-get install -y --no-install-recommends	autoconf	automake	bzip2 file g++ gcc imagemagick libbz2-dev libc6-dev lit
335	CVE-2018-1460	9.8	An issue was dis libx11	2:1.6.2-3	2:1.6.2-3+deb8u	RUN set -ex; apt-get update; apt-get install -y --no-install-recommends	autoconf	automake	bzip2 file g++ gcc imagemagick libbz2-dev libc6-dev lit
336	CVE-2018-1459	9.8	An issue was dis libx11	2:1.6.2-3	2:1.6.2-3+deb8u	RUN set -ex; apt-get update; apt-get install -y --no-install-recommends	autoconf	automake	bzip2 file g++ gcc imagemagick libbz2-dev libc6-dev lit
337	CVE-2015-5297	9.8	An integer overfl pixman	0.32.6-3	0.32.6-3+deb8u	RUN set -ex; apt-get update; apt-get install -y --no-install-recommends	autoconf	automake	bzip2 file g++ gcc imagemagick libbz2-dev libc6-dev lit
338	CVE-2017-1462	9.8	ImageMagick 7.( imagemagick	8:6.8.9.9-5+deb	8:6.8.9.9-5+deb	RUN set -ex; apt-get update; apt-get install -y --no-install-recommends	autoconf	automake	bzip2 file g++ gcc imagemagick libbz2-dev libc6-dev lit
339	CVE-2017-1313	9.8	In ImageMagick imagemagick	8:6.8.9.9-5+deb	8:6.8.9.9-5+deb	RUN set -ex; apt-get update; apt-get install -y --no-install-recommends	autoconf	automake	bzip2 file g++ gcc imagemagick libbz2-dev libc6-dev lit
340	CVE-2017-1462	9.8	ImageMagick 7.( imagemagick	8:6.8.9.9-5+deb	8:6.8.9.9-5+deb	RUN set -ex; apt-get update; apt-get install -y --no-install-recommends	autoconf	automake	bzip2 file g++ gcc imagemagick libbz2-dev libc6-dev lit
341	CVE-2017-1503	9.8	ImageMagick ve imagemagick	8:6.8.9.9-5+deb8u10		RUN set -ex; apt-get update; apt-get install -y --no-install-recommends	autoconf	automake	bzip2 file g++ gcc imagemagick libbz2-dev libc6-dev lit
342	CVE-2017-1413	9.8	ImageMagick 7.( imagemagick	8:6.8.9.9-5+deb8u10		RUN set -ex; apt-get update; apt-get install -y --no-install-recommends	autoconf	automake	bzip2 file g++ gcc imagemagick libbz2-dev libc6-dev lit
343	CVE-2017-1462	9.8	ImageMagick 7.( imagemagick	8:6.8.9.9-5+deb	8:6.8.9.9-5+deb	RUN set -ex; apt-get update; apt-get install -y --no-install-recommends	autoconf	automake	bzip2 file g++ gcc imagemagick libbz2-dev libc6-dev lit
344	CVE-2019-1994	9.8	In ImageMagick imagemagick	8:6.8.9.9-5+deb	8:6.8.9.9-5+deb	RUN set -ex; apt-get update; apt-get install -y --no-install-recommends	autoconf	automake	bzip2 file g++ gcc imagemagick libbz2-dev libc6-dev lit
345	CVE-2017-1453	9.8	ImageMagick 7.( imagemagick	8:6.8.9.9-5+deb	8:6.8.9.9-5+deb	RUN set -ex; apt-get update; apt-get install -y --no-install-recommends	autoconf	automake	bzip2 file g++ gcc imagemagick libbz2-dev libc6-dev lit
346	CVE-2015-9290	9.8	In FreeType befo freetype	2.5.2-3+deb8u2	2.5.2-3+deb8u3	RUN set -ex; apt-get update; apt-get install -y --no-install-recommends	autoconf	automake	bzip2 file g++ gcc imagemagick libbz2-dev libc6-dev lit
347	CVE-2017-1693	9.8	parser.c in libxm libxml2	2.9.1+dfsg1-5+d	2.9.1+dfsg1-5+d	RUN set -ex; apt-get update; apt-get install -y --no-install-recommends	autoconf	automake	bzip2 file g++ gcc imagemagick libbz2-dev libc6-dev lit
348	CVE-2017-7375	9.8	A flaw in libxm libxml2	2.9.1+dfsg1-5+d	2.9.1+dfsg1-5+d	RUN set -ex; apt-get update; apt-get install -y --no-install-recommends	autoconf	automake	bzip2 file g++ gcc imagemagick libbz2-dev libc6-dev lit
349	CVE-2017-7376	9.8	Buffer overflow in libxm libxml2	2.9.1+dfsg1-5+d	2.9.1+dfsg1-5+d	RUN set -ex; apt-get update; apt-get install -y --no-install-recommends	autoconf	automake	bzip2 file g++ gcc imagemagick libbz2-dev libc6-dev lit
350	CVE-2016-4448	9.8	Format string vu libxm libxml2	2.9.1+dfsg1-5+deb8u4		RUN set -ex; apt-get update; apt-get install -y --no-install-recommends	autoconf	automake	bzip2 file g++ gcc imagemagick libbz2-dev libc6-dev lit
351	CVE-2019-1245	9.8	file_copy_fallbac glib2.0	2.42.1-1	2.42.1-1+deb8u	RUN set -ex; apt-get update; apt-get install -y --no-install-recommends	autoconf	automake	bzip2 file g++ gcc imagemagick libbz2-dev libc6-dev lit
352	CVE-2018-1642	9.8	In GNOME GLib glib2.0	2.42.1-1	2.42.1-1+deb8u	RUN set -ex; apt-get update; apt-get install -y --no-install-recommends	autoconf	automake	bzip2 file g++ gcc imagemagick libbz2-dev libc6-dev lit
353	CVE-2016-9539	9.8	tools/tiffcrop.c in tiff	4.0.3-12.3+deb8u4		RUN set -ex; apt-get update; apt-get install -y --no-install-recommends	autoconf	automake	bzip2 file g++ gcc imagemagick libbz2-dev libc6-dev lit
354	CVE-2017-9117	9.8	In LibTIFF 4.0.7, tiff	4.0.3-12.3+deb8u4		RUN set -ex; apt-get update; apt-get install -y --no-install-recommends	autoconf	automake	bzip2 file g++ gcc imagemagick libbz2-dev libc6-dev lit
355	CVE-2017-7546	9.8	PostgreSQL ver: postgresql-9.4	9.4.12-0+deb8u	9.4.13-0+deb8u	RUN set -ex; apt-get update; apt-get install -y --no-install-recommends	autoconf	automake	bzip2 file g++ gcc imagemagick libbz2-dev libc6-dev lit
356	CVE-2014-9939	9.8	ihex.c in GNU Bi binutils	2.25-5+deb8u1		RUN set -ex; apt-get update; apt-get install -y --no-install-recommends	autoconf	automake	bzip2 file g++ gcc imagemagick libbz2-dev libc6-dev lit
357	CVE-2017-7614	9.8	elflink.c in the Bi binutils	2.25-5+deb8u1		RUN set -ex; apt-get update; apt-get install -y --no-install-recommends	autoconf	automake	bzip2 file g++ gcc imagemagick libbz2-dev libc6-dev lit
358	CVE-2018-1269	9.8	finish_stab in ste binutils	2.25-5+deb8u1		RUN set -ex; apt-get update; apt-get install -y --no-install-recommends	autoconf	automake	bzip2 file g++ gcc imagemagick libbz2-dev libc6-dev lit
359	CVE-2009-3546	9.3	The _gdGetColo libwmf	0.2.8.4-10.3+deb8u2		RUN set -ex; apt-get update; apt-get install -y --no-install-recommends	autoconf	automake	bzip2 file g++ gcc imagemagick libbz2-dev libc6-dev lit
360	CVE-2017-7544	9.1	libxif through 0. libxif	0.6.21-2	0.6.21-2+deb8u	RUN set -ex; apt-get update; apt-get install -y --no-install-recommends	autoconf	automake	bzip2 file g++ gcc imagemagick libbz2-dev libc6-dev lit

# Red Hat, Zettaset, CyberArk, Synopsys DevSecOps Solution



```
vi pod.yaml
apiVersion: v1
kind: Pod
metadata:
  name: security-context-demo
spec:
  securityContext:
    runAsUser: 1000
    runAsGroup: 3000
    fsGroup: 2000
  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
~
~
~
-- INSERT --
```

```
vi pod.yaml

apiVersion: v1
kind: Pod
metadata:
  name: security-context-demo
spec:
  securityContext:
    runAsUser: 1000
    runAsGroup: 3000
    fsGroup: 2000
  volumes:
  - name: sec-ctx-vol
    emptyDir: {}
  containers:
  - name: sec-ctx-demo
    image: busybox
    resources:
      requests:
        memory: "64Mi"
        cpu: "250m"
    command: [ "sh", "-c", "sleep 300s" ]
    volumeMounts:
    - name: sec-ctx-vol
      mountPath: /data/demo
    securityContext:
      allowPrivilegeEscalation: true
      readOnlyRootFilesystem: true
      runAsUser: 1000
      runAsGroup: 3000
      fsGroup: 2000
  
```

-- INSERT --

```
→ 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/management-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/management-resources-containers/#requests-and-limits for details.)

Error: found 3 lint errors
→ tmp
```

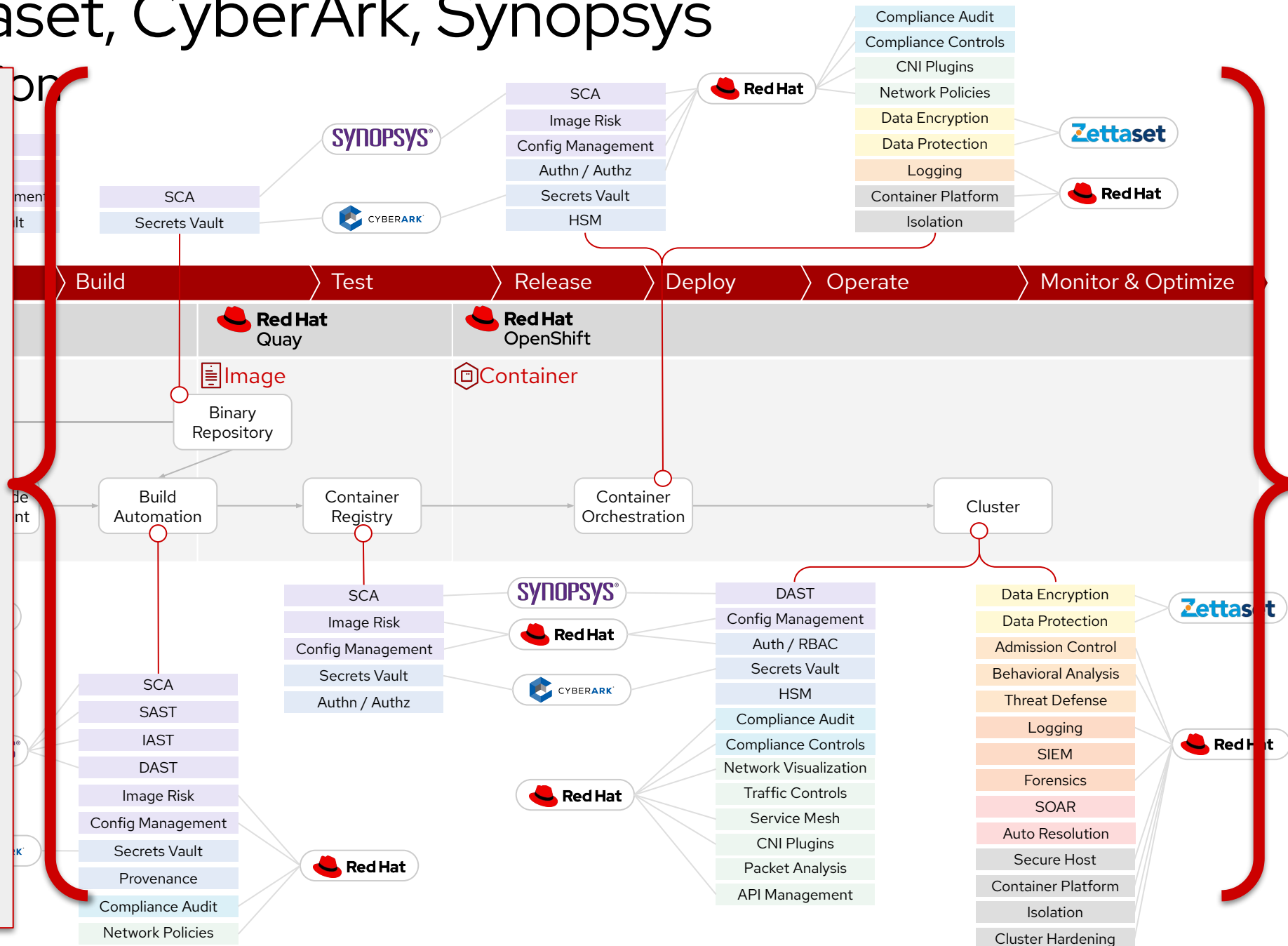


# Red Hat, Zettaset, CyberArk, Synopsys



KPI

Time to fix security issues



RISK

Default View

Add one or more resource filters

+ CREATE POLICY

32 DEPLOYMENTS

Page 1 of 1

<>

Name	Created	Cluster	Namespace	Priority
<div><div></div>tekton-triggers-webhook</div>	05/24/2021   12:03:50PM	production	openshift-pipelines	8
<div><div></div>reporting</div>	05/24/2021   11:59:37AM	production	medical	9
<div><div></div>tekton-triggers-controller</div>	05/24/2021   12:03:52PM	production	openshift-pipelines	11
<div><div></div>concourse-ci-postgresql</div>	06/04/2021   9:03:12AM	production	default	15
<div><div></div>tekton-pipelines-controller</div>	05/24/2021   12:03:14PM	production	openshift-pipelines	16
<div><div></div>tekton-operator-proxy-webhook</div>	05/24/2021   12:03:20PM	production	openshift-pipelines	17
<div><div></div>concourse-ci-web</div>	06/04/2021   9:03:12AM	production	default	18
<div><div></div>puppet-master</div>	05/24/2021   11:59:30AM	production	operations	21
<div><div></div>proxy</div>	05/24/2021   11:59:38AM	production	medical	24
<div><div></div>tekton-pipelines-webhook</div>	05/24/2021   12:03:14PM	production	openshift-pipelines	25
<div><div></div>openshift-pipelines-operator</div>	05/24/2021   12:02:39PM	production	openshift-operators	29
<div><div></div>wordpress</div>	05/24/2021   11:59:35AM	production	frontend	31
<div><div></div>tekton-triggers-core-</div>	05/24/2021   12:03:50PM	production	openshift-pipelines	32

Reporting

RISK INDICATORS

DEPLOYMENT DETAILS

PROCESS DISCOVERY

VIEW DEPLOYMENT IN NETWORK GRAPH

Policy Violations

Fixable CVSS >= 7 (severity: High)

No resource requests or limits specified (severity: Medium)

90-Day Image Age (severity: Low)

Docker CIS 4.1: Ensure That a User for the Container Has Been Created (severity: Low)

Latest tag (severity: Low)

Ubuntu Package Manager in Image (severity: Low)

Image Vulnerabilities

Image "quay.io/rhacs-demo/reporting:latest" contains 137 CVEs with CVSS scores ranging between 2.1 and 10.0

Service Configuration

Secrets rhacs-demo-pull-secret are used inside the deployment

No capabilities were dropped

## RISK

Default View



## 32 DEPLOYMENTS

## Name

☐ tekton-triggers-webhook☒ reporting☐ tekton-triggers-controller☐ concourse-ci-postgresql☐ tekton-pipelines-controller☐ tekton-operator-pr-webhook☐ concourse-ci-web☐ puppet-master☐ proxy☐ tekton-pipelines-webhook☐ openshift-pipelines-operator☐ wordpress☐ tekton-triggers-core

## Dockerfile.reporting M X

demo &gt; demo-images &gt; Dockerfile.reporting &gt; USER

You, seconds ago

1 FROM debian:10

2

3 USER reporting

4

5 COPY --from=netflow /bin/entrypoint /bin/entrypoint

6

7 RUN chmod +x /bin/entrypoint

8

9 RUN touch /reporting

10

You, seconds ago • Uncommitted changes

05/24/2021 | 12:02:39PM production openshift-operators 29

05/24/2021 | 11:59:35AM production frontend 31

## Service Configuration

Secrets rhacs-demo-pull-secret are used inside the deployment

No capabilities were dropped

# 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.



[linkedin.com/company/red-hat](https://linkedin.com/company/red-hat)



[youtube.com/user/RedHatVideos](https://youtube.com/user/RedHatVideos)



[facebook.com/redhatinc](https://facebook.com/redhatinc)



[twitter.com/RedHat](https://twitter.com/RedHat)