

Red Hat
Summit

Connect

Bezpieczne przetwarzanie danych na platformie OpenShift

Jarosław Stakuń
Principal Solution Architect

jarek@redhat.com

Key security focus areas

Open Source Software lifecycle security

Shift security left

Cloud security posture management (CSPM)

Cloud workload protection (CWPP)

Secure supply chain

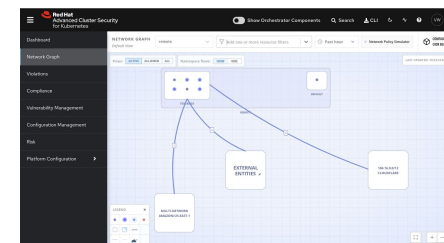
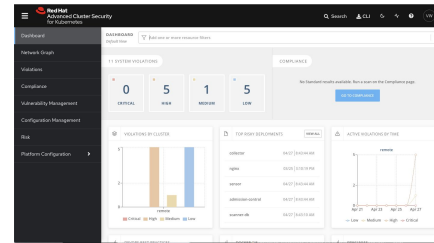
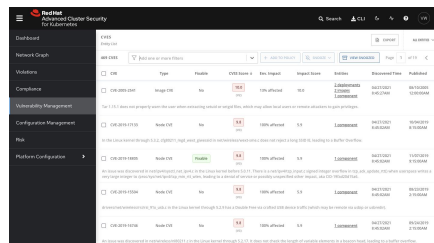
Secure infrastructure

Secure workloads

Extend scanning and compliance into development

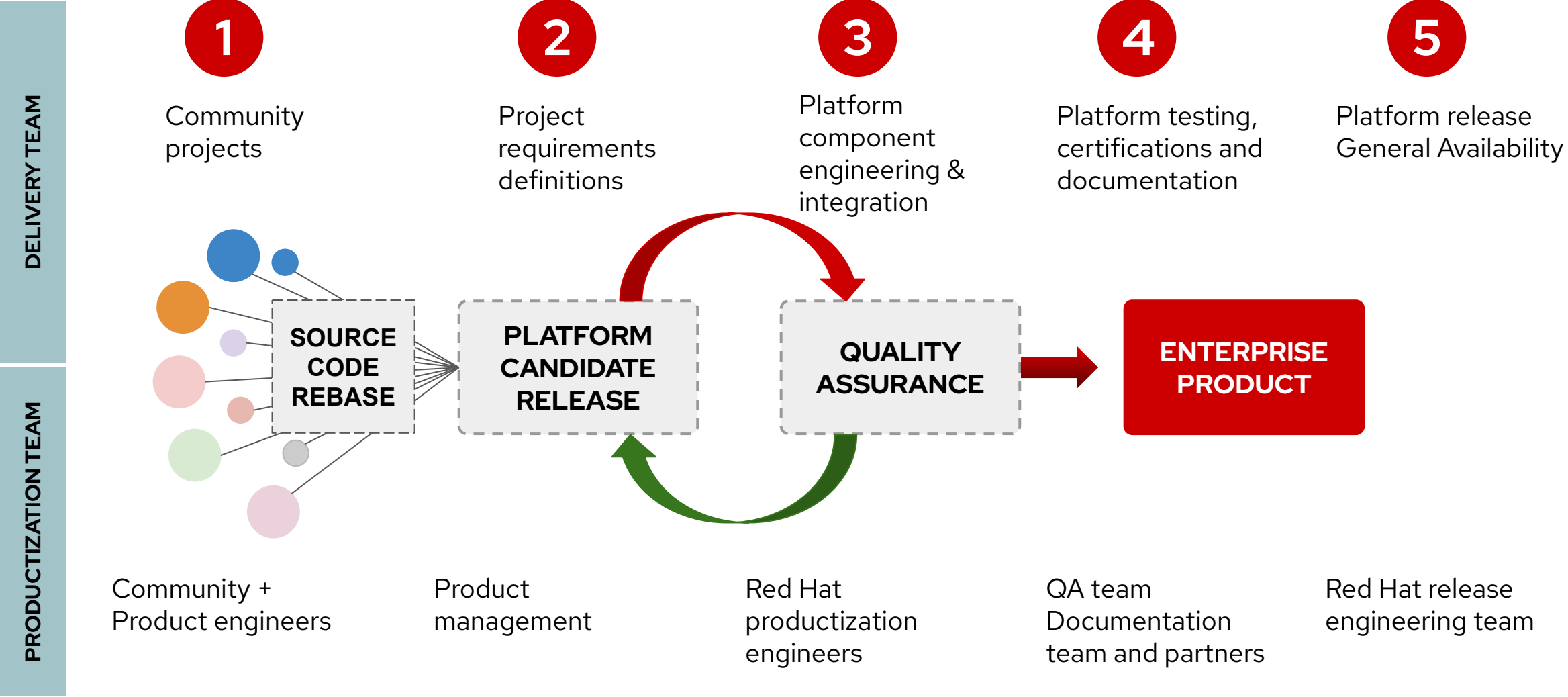
Leverage built-in Kubernetes CSPM to **identify and remediate risky configurations**

Maintain and enforce a **“zero-trust execution”** approach to workload protection



Bezpieczeństwo projektów open source i produktów Red Hat

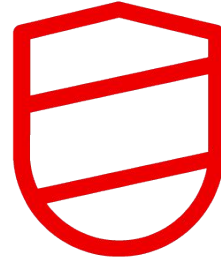
From Open Source Community Project To Enterprise Product



Open Source Development vs Distribution Model

Not vulnerable due to backporting

Security value of backports from Red Hat vs grabbing from upstream



CVE-2020-1967

Important OpenSSL

Vulnerability was introduced in OpenSSL version 1.1.1d which we did not ship

CVE-2021-3345

Critical libgcrypt

Vulnerability was introduced in libgcrypt version 1.9.0 which we did not ship

CVE-2021-20226

Important kernel

Vulnerable upstream code was not introduced in any version we shipped.

CVE-2020-8835

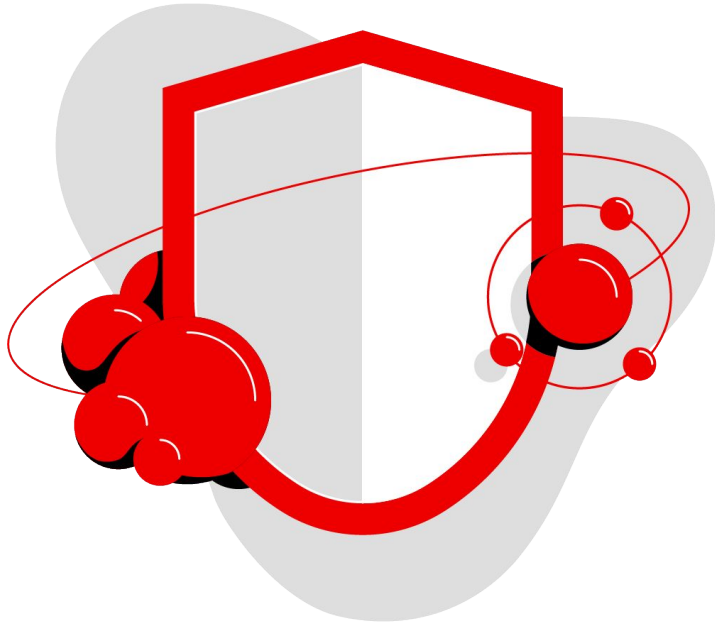
Important kernel

Vulnerable upstream code was not introduced in any version we shipped.

The Value of Red Hat backporting policy:

- We don't require customers to upgrade to newest version but we backport patches to older versions
- We don't ship newest upstream versions hence we avoid being vulnerable to many CVE
- Less frequent upgrades

Red Hat offers authoritative security guidance and certifications

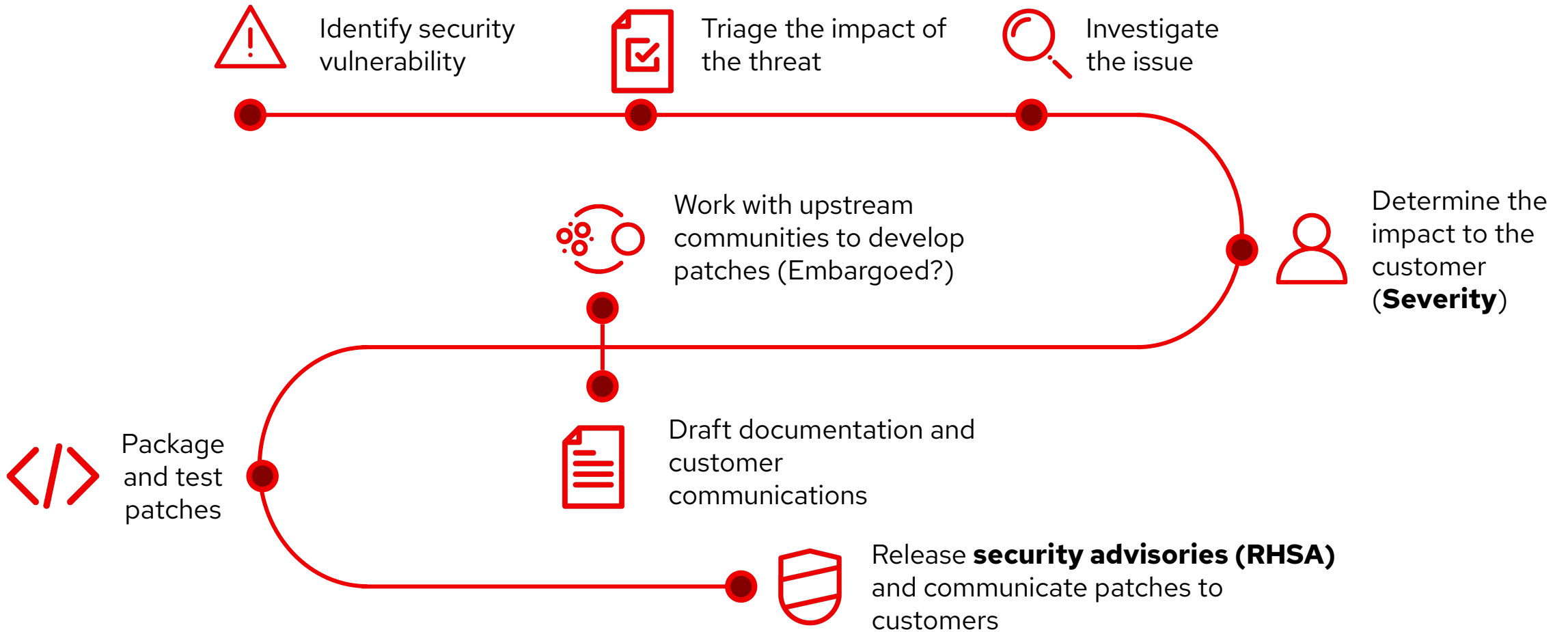


Address security concerns with Red Hat's dedicated Product Security team that **monitors, identifies, & addresses risks quickly.**

Receive **security patches (that Red Hat has created, tested, & delivered)** for all versions of Red Hat products during their supported life cycles.

Maintain compliance because Red Hat's products **meet government & commercial security standards.**

Customer security awareness workflow



Defensive security resources

The tools and expertise needed to safeguard your business

Red Hat Product Security Team

1596

CVEs reported
in 2021

1473

CVEs addressed
in 2021

1385

security advisories
released in 2021

46

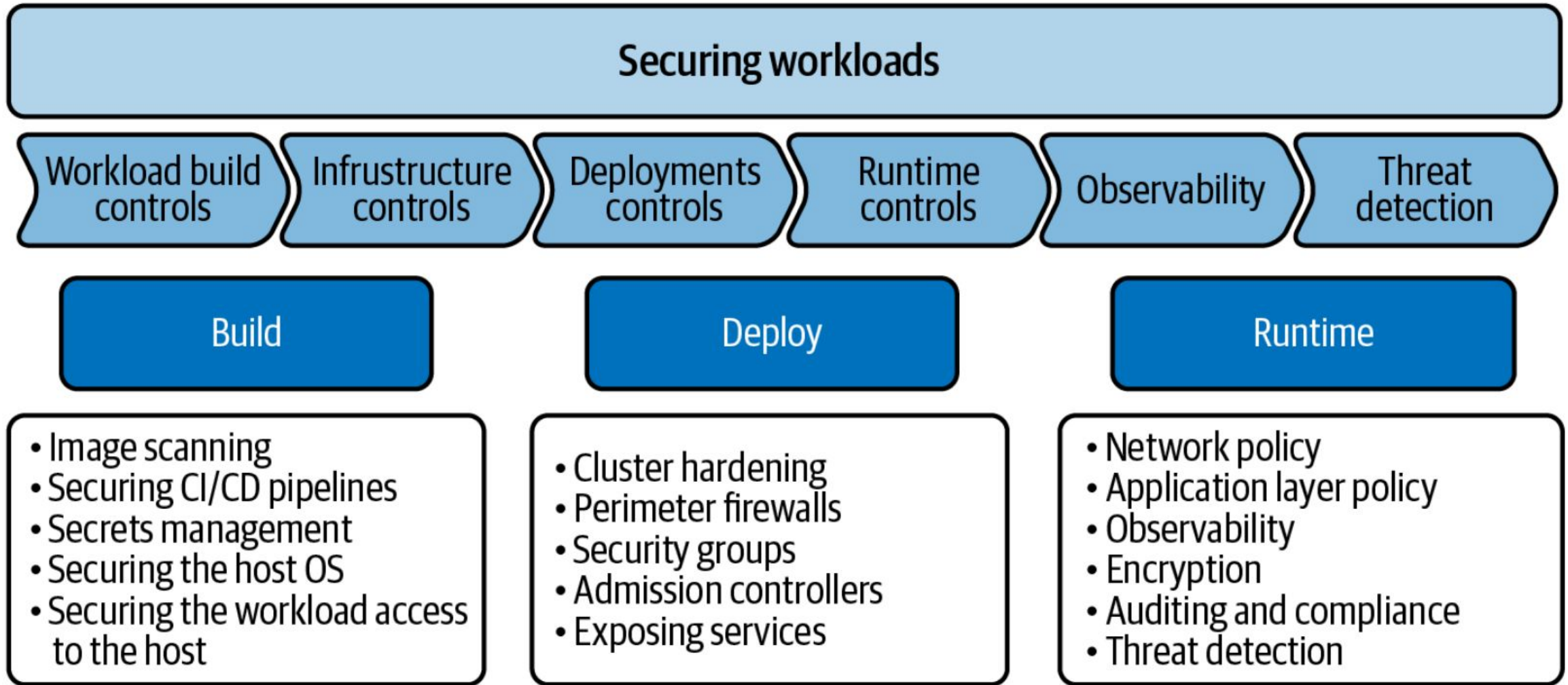
critical security advisories
released in 2021

01

application programming interface (API) to automate inspection of the Common Vulnerabilities and Exposures (CVE) database

DevSecOps na platformie OpenShift

Application Workloads Security

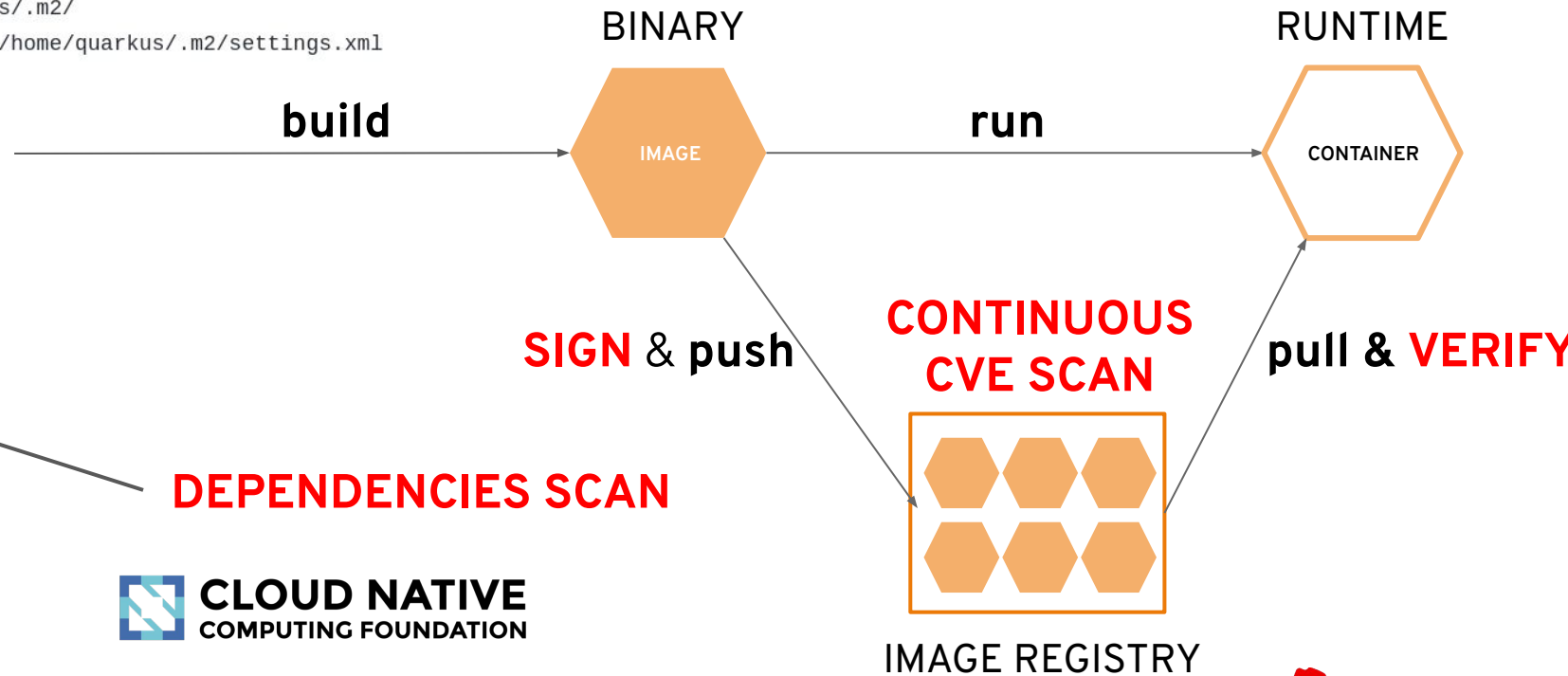


Secure containers build and run chain

Containerfile

BASE IMAGE

```
1 FROM quay.io/quarkus/ubi-quarkus-native-image:21.3.1-java11 AS build
2 ARG MAVEN_MIRROR_URL=https://repo1.maven.org/maven2/
3 RUN mkdir -p /home/quarkus/.m2
4 COPY --chown=quarkus:quarkus mvnw /code/mvnw
5 COPY --chown=quarkus:quarkus .mvn /code/.mvn
6 COPY --chown=quarkus:quarkus pom.xml /code/
7 COPY --chown=quarkus:quarkus settings.xml /home/quarkus/.m2/
8 RUN sed -i 's/MAVEN_MIRROR_URL/${MAVEN_MIRROR_URL}/g' /home/quarkus/.m2/settings.xml
9 USER quarkus
10 WORKDIR /code
11 COPY src /code/src
12 RUN ./mvnw package -DskipTests=true -Pnative
13
14 FROM quay.io/jstakun/ubi-micro-quarkus:latest
15 MAINTAINER Jaroslaw Stakun jstakun@redhat.com
16 LABEL quarkus-version=2.8.1.Final
17 WORKDIR /work/
18 COPY --from=build /code/target/*-runner /application
19 RUN chgrp 0 /application && chmod 110 /application
20 USER 1001
21 CMD /application
22 EXPOSE 8080
```

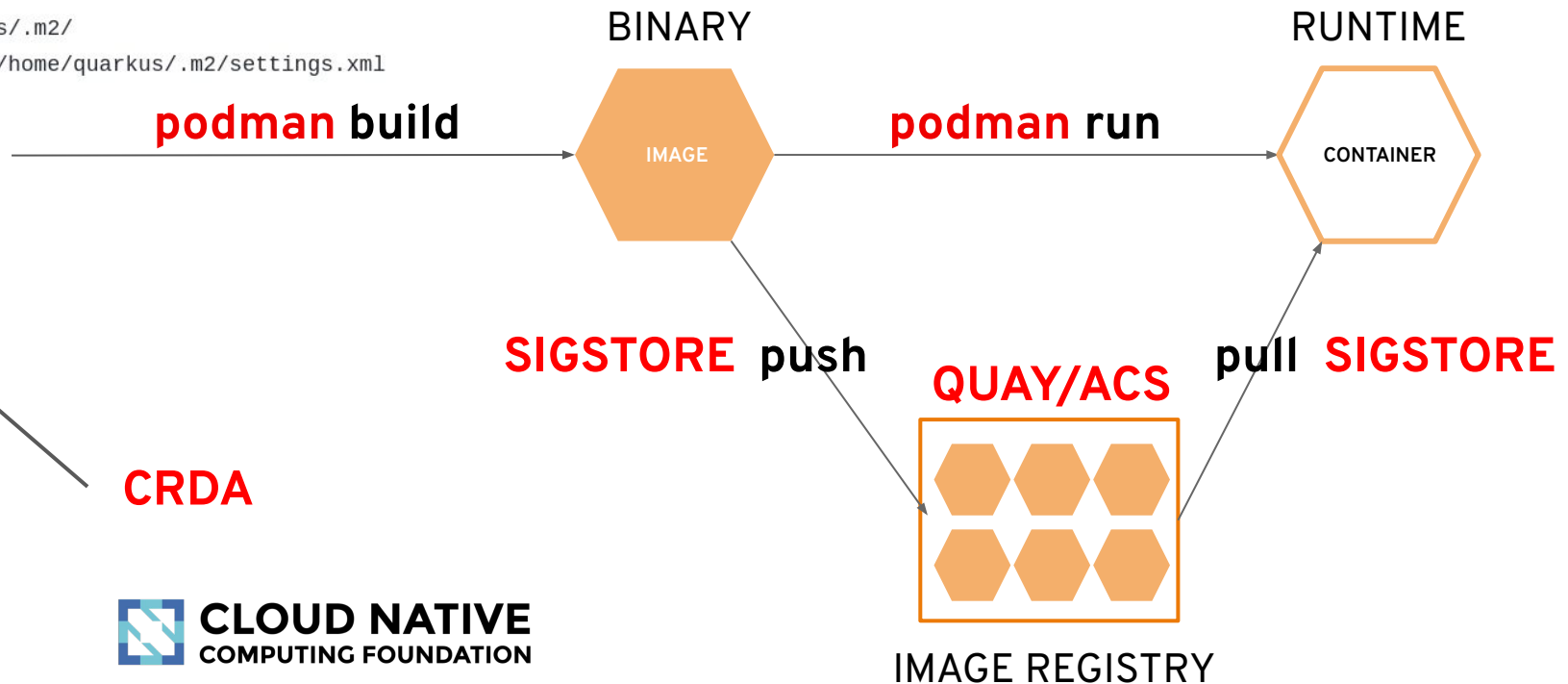


Secure containers build and run chain

Containerfile

RHEL, UBI

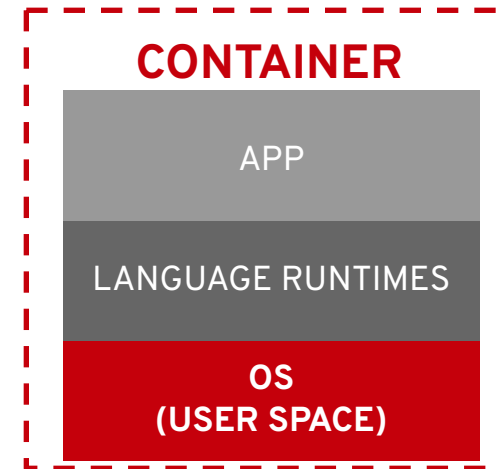
```
1 FROM quay.io/quarkus/ubi-quarkus-native-image:21.3.1-java11 AS build
2 ARG MAVEN_MIRROR_URL=https://repo1.maven.org/maven2/
3 RUN mkdir -p /home/quarkus/.m2
4 COPY --chown=quarkus:quarkus mvnw /code/mvnw
5 COPY --chown=quarkus:quarkus .mvn /code/.mvn
6 COPY --chown=quarkus:quarkus pom.xml /code/
7 COPY --chown=quarkus:quarkus settings.xml /home/quarkus/.m2/
8 RUN sed -i 's/MAVEN_MIRROR_URL/${MAVEN_MIRROR_URL}/g' /home/quarkus/.m2/settings.xml
9 USER quarkus
10 WORKDIR /code
11 COPY src /code/src
12 RUN ./mvnw package -DskipTests=true -Pnative
13
14 FROM quay.io/jstakun/ubi-micro-quarkus:latest
15 MAINTAINER Jaroslaw Stakun jstakun@redhat.com
16 LABEL quarkus-version=2.8.1.Final
17 WORKDIR /work/
18 COPY --from=build /code/target/*-runner /application
19 RUN chgrp 0 /application && chmod 110 /application
20 USER 1001
21 CMD /application
22 EXPOSE 8080
```



Red Hat Universal Base Image

The image for all your needs

- **Based on RHEL binaries**
- Made **available at no charge** by a new end user license agreement.
- Development
 - Minimal footprint (~90 to ~200MB)
 - Programming languages (Modularity & AppStreams)
 - Enables a single CI/CD chain
- Production
 - Supported as RHEL when running on RHEL
 - **Same Performance, Security & Life cycle as RHEL**
 - Can attach RHEL support subscriptions as RHEL
- 4 flavors : Micro, Minimal, Standard, Init



- Standardize Your own deps os image, certified & compliant
- **freely distribute to your teams, partners and contractors** that run image on the OS of their choice
- Once app built, and shipped as container in your Red Hat env:
 - it is secure & compliant
 - you get full support back

Source code dependencies analysis

The screenshot displays a VS Code interface with a 'Dependency Analytics Report' for a 'pom.xml' file. The report is divided into four main sections:

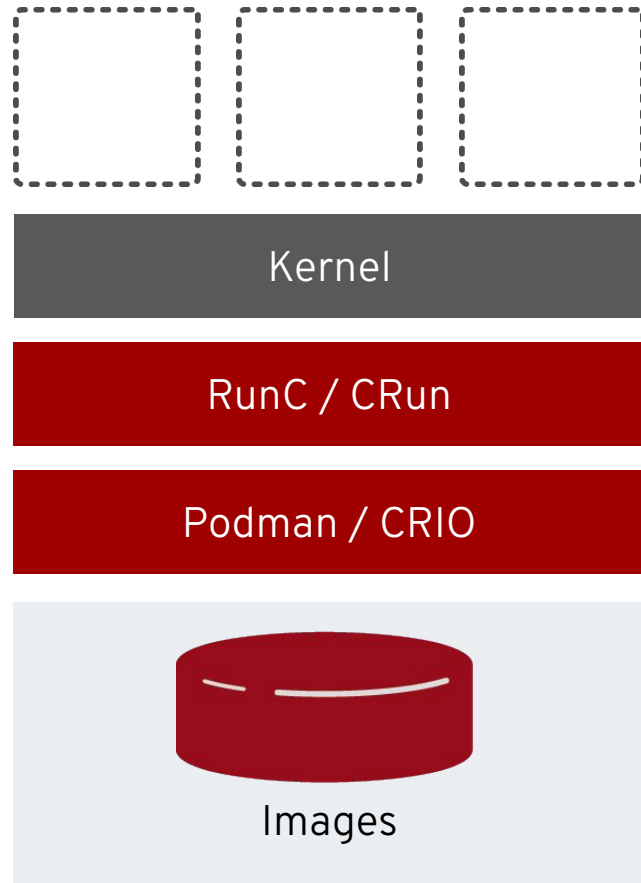
- Security Issues:** Shows 4 total vulnerabilities and 1 vulnerable dependency.
- Dependency Details:** Shows 2 analyzed dependencies, 58 transitive dependencies, and 0 unknown dependencies.
- Licenses:** Shows a suggested license of 'apache' with a score of 2.0, and 0 license conflicts, unknown licenses, or restrictive licenses.
- Add-ons:** Shows 3 total dependencies, 0 usage outliers, and 3 companion dependencies.

Below these sections, a table titled 'Dependencies with security issues in your stack' is shown, powered by Snyk. It lists 4 commonly known vulnerabilities and 0 unique to Snyk. The table has the following columns: #, Dependencies, # Direct Vulnerabilities, # Transitive Vulnerabilities, Highest CVSS Score, and Highest Severity Vulnerability.

#	Dependencies	# Direct Vulnerabilities	# Transitive Vulnerabilities	Highest CVSS Score	Highest Severity Vulnerability
#01	org.apache.logging.log4j:log4j-core	4	-	10/10	SNYK-JAVA-ORGAPACHELOGGING-LOG4J-2314720

The status bar at the bottom shows system metrics: 1 error, 0 warnings, 0 info, 0 previews, 1.49/6.06 GB memory usage (24%), and 254 m CPU usage. The editor shows line 1, column 1, UTF-8 encoding, 4 spaces, and XML file type.

Manage containers with Podman



Fast and lightweight

No daemons required

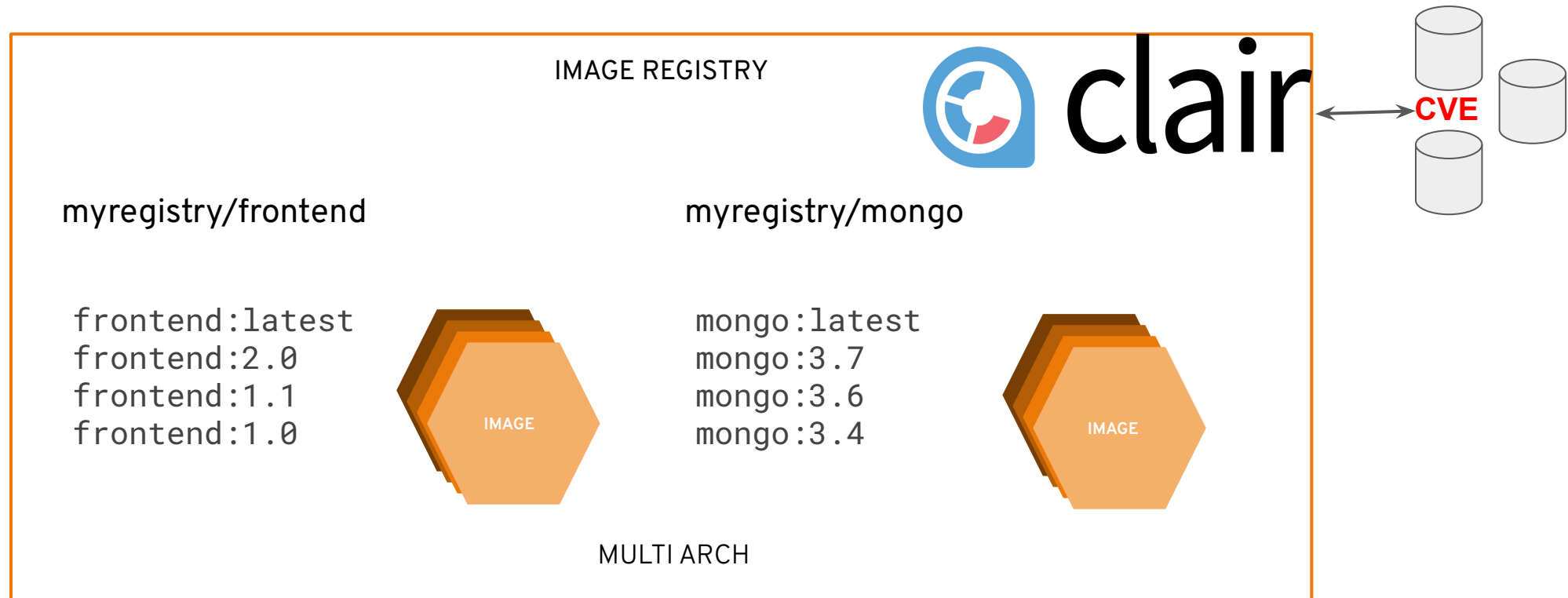
Advanced namespace isolation

Rootless operations for container run and build

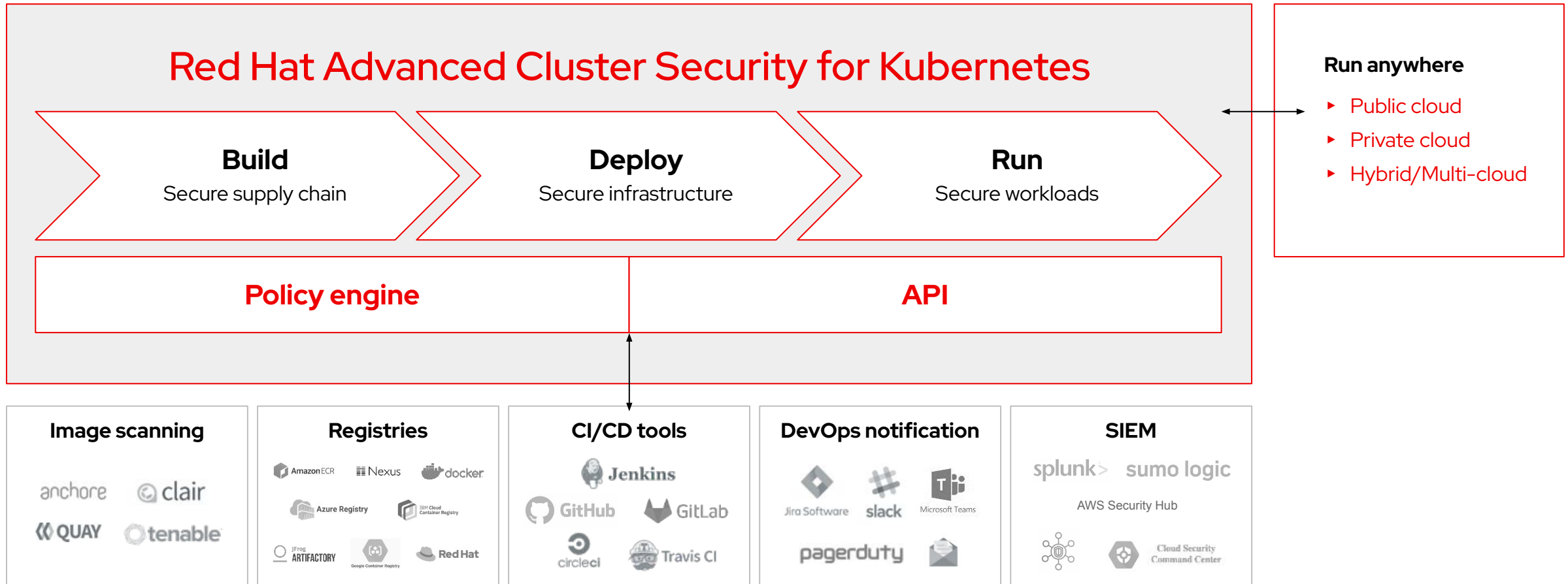
Open standards compliant

Creates and maintains any standard Open Containers Initiative (OCI) -compliant containers and pods

An image registry contains all versions of an image

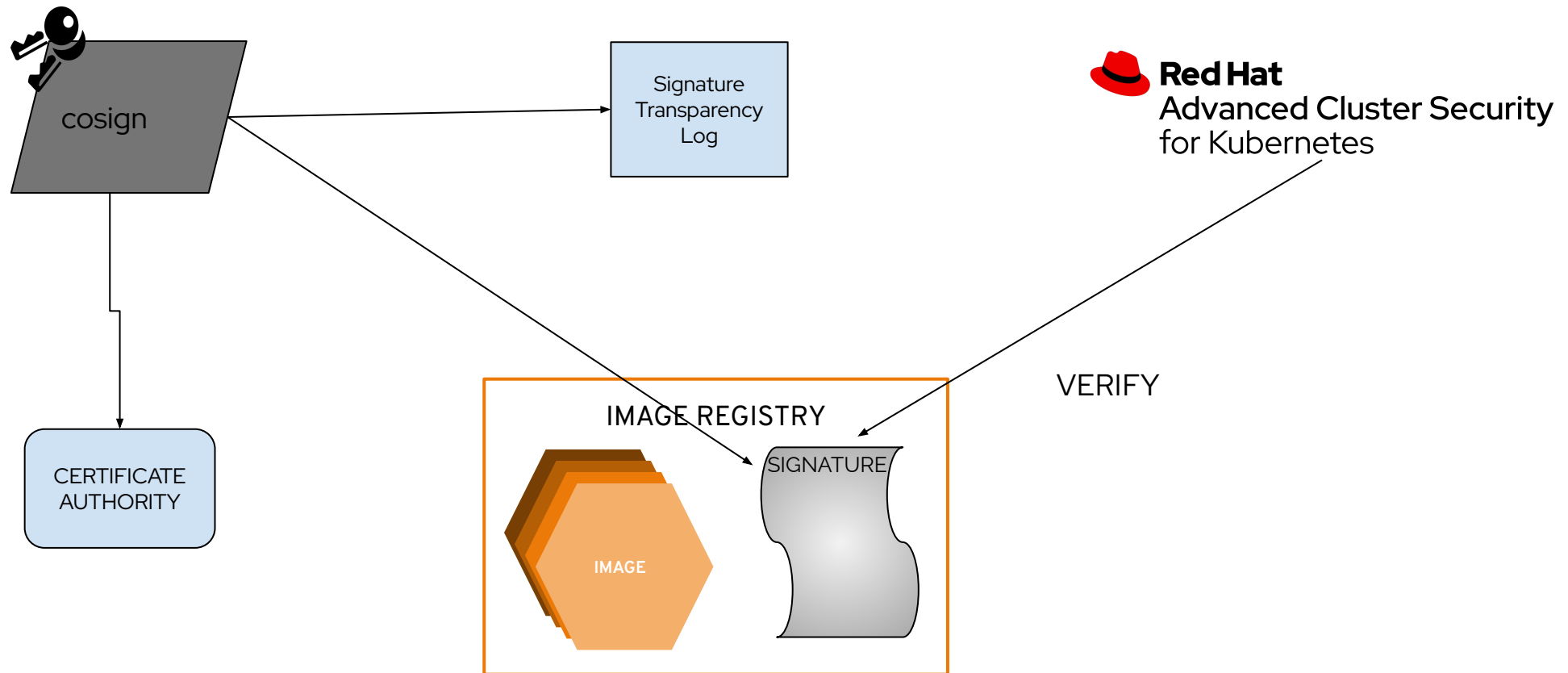


Kubernetes-native security platform

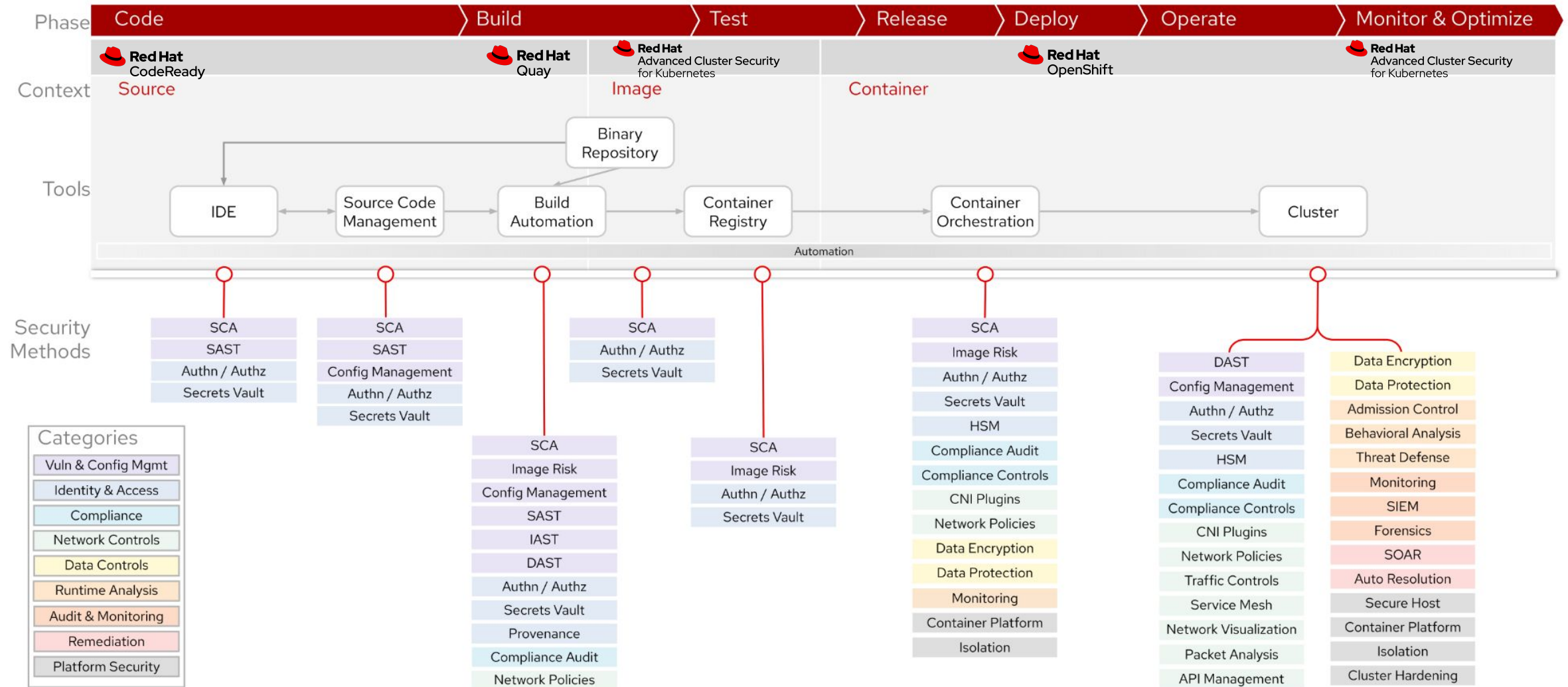


Sigstore cosign

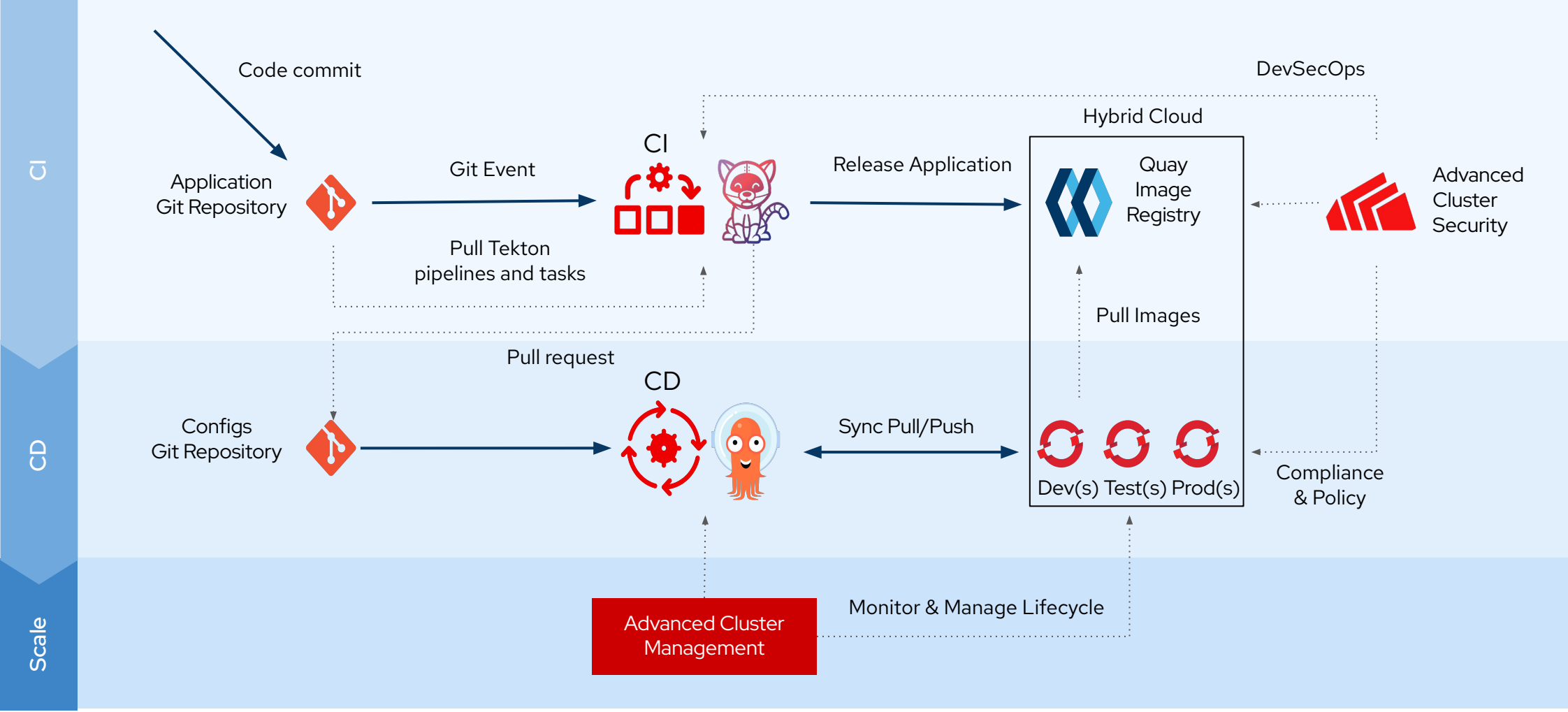
·f· sigstore



DevSecOps Application Pipeline Framework



DevSecOps Application Delivery with OpenShift

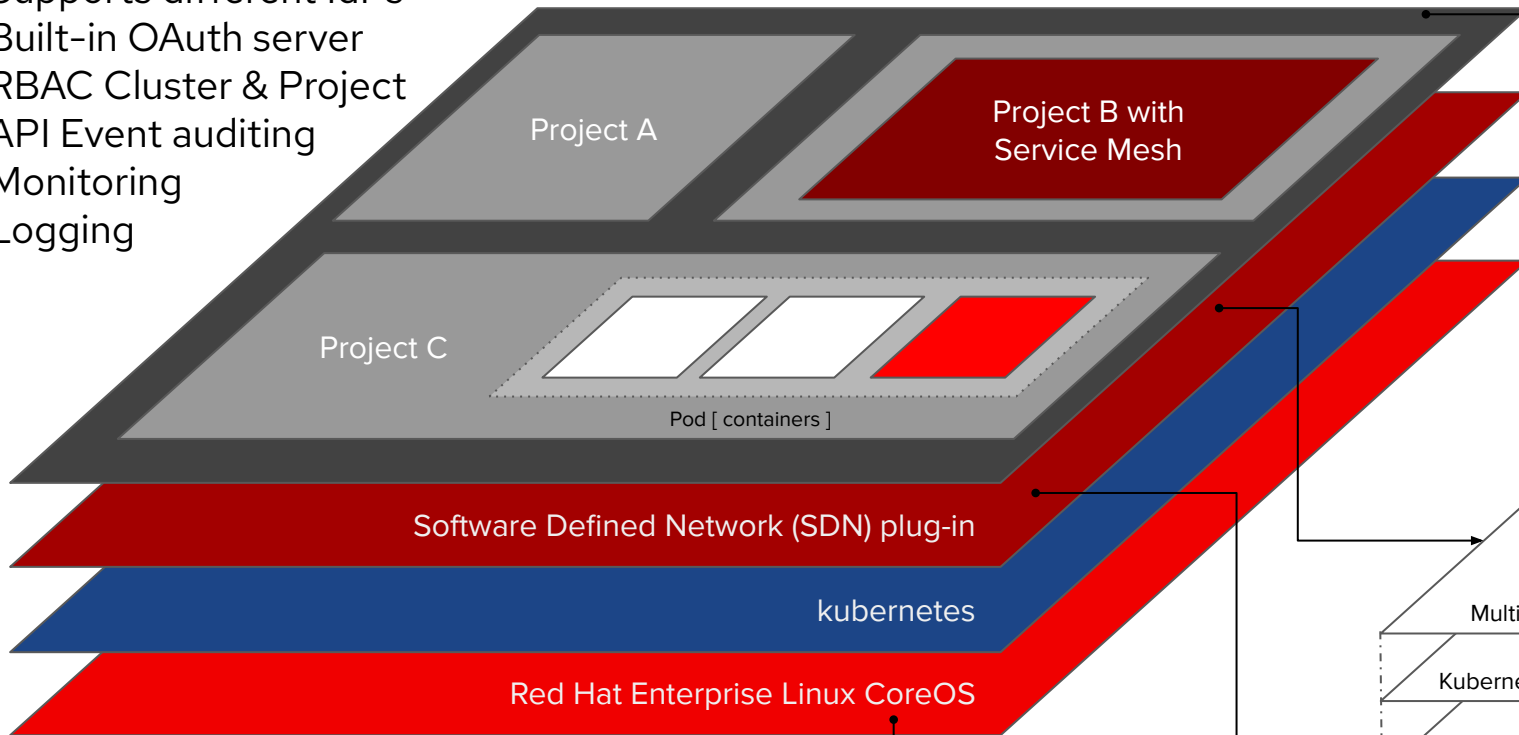


Bezpieczna Platforma Kontenerowa

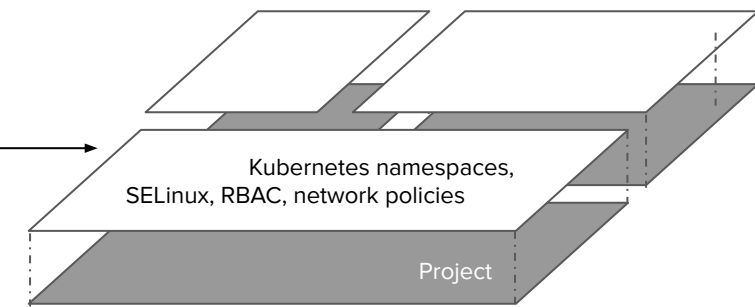
OpenShift Defense in Depth

OpenShift Container Platform

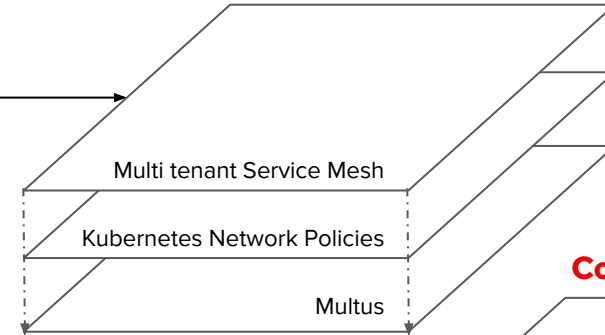
- Supports different IdPs
- Built-in OAuth server
- RBAC Cluster & Project
- API Event auditing
- Monitoring
- Logging



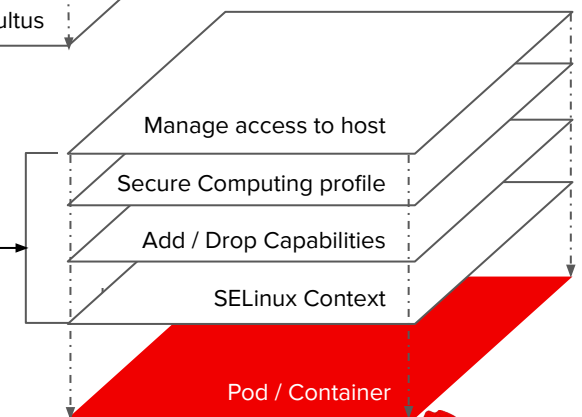
Multi tenant (Isolated) Projects



Network Security



Container Security



Security Context Constraints (Kubernetes Admission Controller)

Red Hat Universal Base Image
containers can leverage RHEL
FIPS capabilities

Red Hat CoreOS

- Minimized attack surface
- Controlled Immutability
- SELinux on by default
- Kernel namespaces and Cgroups
- CRI-O container runtime, Kubelet
- Auditd for host-level audit
- FIPS enablement
- RHCOS volume encryption



OpenShift secures against CVEs



Red Hat
Customer Portal

CVE-2021-30465

Public on May 19, 2021

“Customers of OpenShift have **SELinux enabled in enforcing mode in every host** across all clusters. Therefore, It is expected that customers **have a reduced impact from this issue...**”



Red Hat
Customer Portal

CVE-2020-8554

Public on December 6, 2020

“OpenShift Container Platform (OCP) includes a builtin externalIP admission plugin, which **restricts the use** of Service externalIPs to those configured by a cluster-admin. In OCP4 all externalIP ranges are **disabled by default.**”



Red Hat
Customer Portal

CVE-2020-14386

Public on September 2, 2020

“CAP_NET_RAW capability **disabled by default**, then only a privileged user can trigger this bug..”



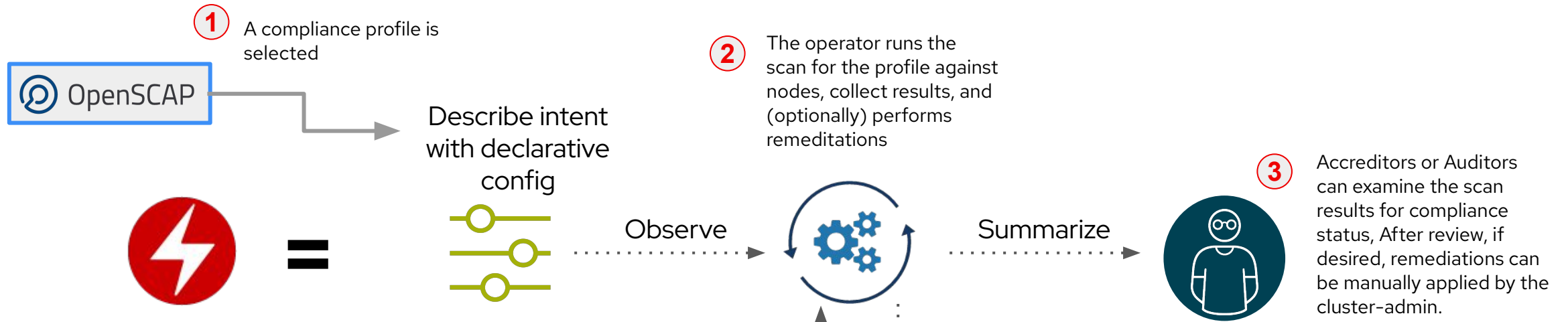
Red Hat Product Security

Red Hat Product Security

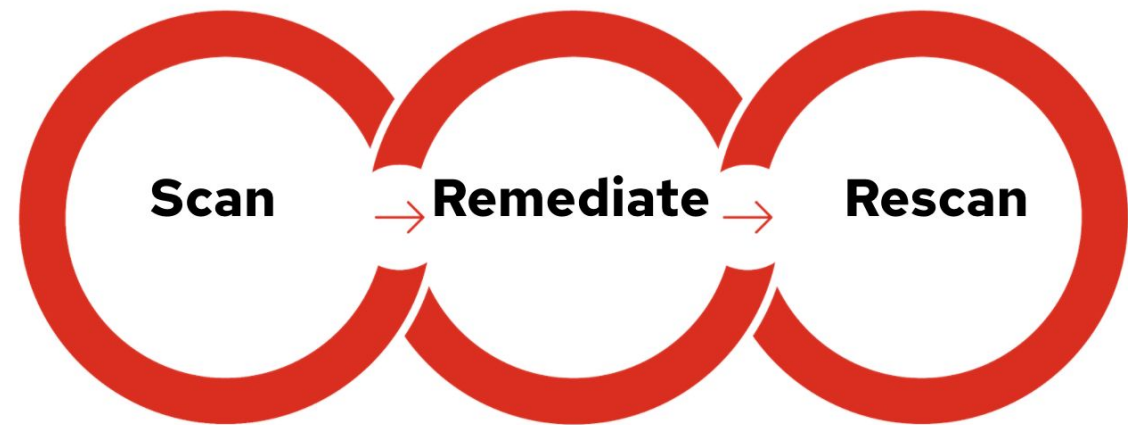
<https://access.redhat.com/security> @RedHatSecurity



Openshift Compliance Operator for Continuous Compliance



- Profiles available now**
- FISMA Moderate
 - CIS OCP benchmark
 - Essential 8
 - NERC-CIP
 - PCI-DSS
- Profiles planned**
- DISA STIG
 - FISMA High



Wykrywanie i reagowanie na zagrożenia w działających aplikacjach

Central security dashboard

2 Clusters 5 Nodes 170 Violations 76 Deployments 42 Images 25 Secrets

Last updated 7/21/2022 at 12:21 PM

Dashboard

Review security metrics across all or select resources

Resources: All clusters ▼ All namespaces ▼

170 policy violations by severity

[View all](#)



Most recent violations with critical severity

iptables Executed in Pr...	proxy	07/11/2022 9:45:15PM
Apache Struts: CVE-2...	backend-atlas	07/11/2022 7:46:19PM
Apache Struts: CVE-2...	mastercard-proc...	07/11/2022 7:46:19PM

Images at most risk

[Options](#) ▼

[View all](#)

Images	Risk priority	Critical CVEs	Important CVEs
ultra-current... ard-processor	1	54 fixable	91 fixable
ultra-current... s/asset-cache	1	54 fixable	91 fixable
ultra-current... x/asset-cache	1	0 fixable	26 fixable
ultra-current... isa-processor	1	54 fixable	91 fixable
ultra-current... backend-atlas	1	54 fixable	91 fixable
ultra-current... rox/jump-host	2	0 fixable	17 fixable

Deployments at most risk

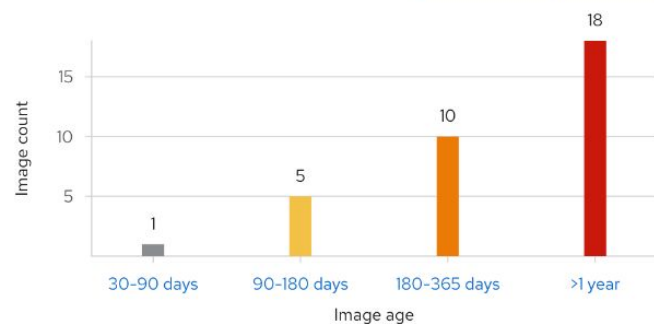
[View all](#)

Deployment	Resource location	Risk priority
visa-processor	in "production / payments"	1
backend-atlas	in "production / backend"	2
calico-node	in "production / kube-system"	3
asset-cache	in "production / frontend"	4
mastercard-processor	in "production / payments"	5
monitor	in "production / frontend"	6

34 Aging images

[Options](#) ▼

[View all](#)



Policy violations by category

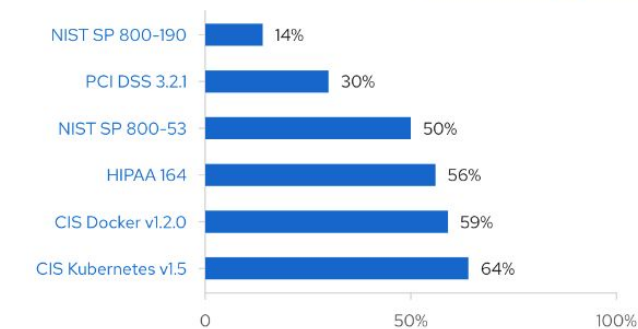
[Options](#) ▼



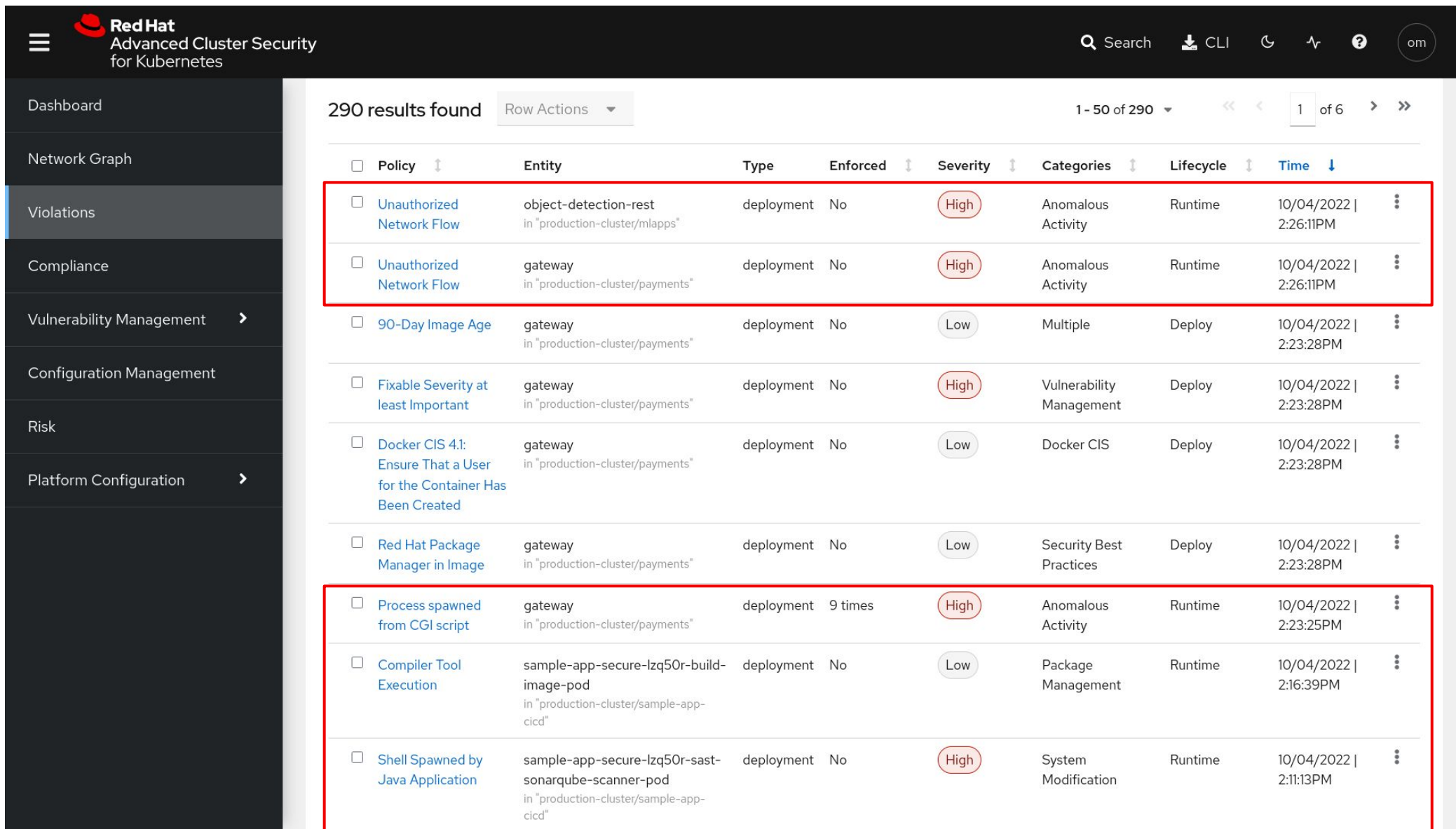
Compliance by standard

[Options](#) ▼

[View all](#)



Runtime threat detection & remediation



The screenshot displays the Red Hat Advanced Cluster Security for Kubernetes interface. The left sidebar contains navigation options: Dashboard, Network Graph, Violations (selected), Compliance, Vulnerability Management, Configuration Management, Risk, and Platform Configuration. The main content area shows a table of 290 results found, with the first page displaying 50 results. The table columns are: Policy, Entity, Type, Enforced, Severity, Categories, Lifecycle, and Time. Two rows are highlighted with red boxes: 'Unauthorized Network Flow' (High severity) and 'Process spawned from CGI script' (High severity).

Policy	Entity	Type	Enforced	Severity	Categories	Lifecycle	Time
<input type="checkbox"/> Unauthorized Network Flow	object-detection-rest in "production-cluster/mlapps"	deployment	No	High	Anomalous Activity	Runtime	10/04/2022 2:26:11PM
<input type="checkbox"/> Unauthorized Network Flow	gateway in "production-cluster/payments"	deployment	No	High	Anomalous Activity	Runtime	10/04/2022 2:26:11PM
<input type="checkbox"/> 90-Day Image Age	gateway in "production-cluster/payments"	deployment	No	Low	Multiple	Deploy	10/04/2022 2:23:28PM
<input type="checkbox"/> Fixable Severity at least Important	gateway in "production-cluster/payments"	deployment	No	High	Vulnerability Management	Deploy	10/04/2022 2:23:28PM
<input type="checkbox"/> Docker CIS 4.1: Ensure That a User for the Container Has Been Created	gateway in "production-cluster/payments"	deployment	No	Low	Docker CIS	Deploy	10/04/2022 2:23:28PM
<input type="checkbox"/> Red Hat Package Manager in Image	gateway in "production-cluster/payments"	deployment	No	Low	Security Best Practices	Deploy	10/04/2022 2:23:28PM
<input type="checkbox"/> Process spawned from CGI script	gateway in "production-cluster/payments"	deployment	9 times	High	Anomalous Activity	Runtime	10/04/2022 2:23:25PM
<input type="checkbox"/> Compiler Tool Execution	sample-app-secure-lzq50r-build-image-pod in "production-cluster/sample-app-cicd"	deployment	No	Low	Package Management	Runtime	10/04/2022 2:16:39PM
<input type="checkbox"/> Shell Spawned by Java Application	sample-app-secure-lzq50r-sast-sonarqube-scanner-pod in "production-cluster/sample-app-cicd"	deployment	No	High	System Modification	Runtime	10/04/2022 2:11:13PM

Network communication monitoring

Red Hat Advanced Cluster Security for Kubernetes

Dashboard
Network Graph
Violations
Compliance
Vulnerability Management
Configuration Management
Risk
Platform Configuration

production-cluster | Namespaces 1 | Add one or more deployment filters | Past hour

Flows: ACTIVE | ALLOWED | ALL | LAST UPDATED: 03:19:34PM

Namespace flows: SHOW | HIDE

sentiment-analysis-rest-git Deployment | Flows | Network Policies | Details

NETWORK FLOWS | BASELINE SETTINGS

1 ACTIVE FLOW | Page 1 of 1

Add one or more resource filters

Entity	Traffic	Type	Namespace	Port	Protocol	State
1 Anomalous Flow						
<input type="checkbox"/>	gateway	Egress	Deployment	payments	8080	TCP Active
0 Baseline Flows						
No baseline flows.						

LEGEND

EXTERNAL ENTITIES

Demo

Red Hat
Summit

Connect

Thank you



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



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



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



twitter.com/RedHat