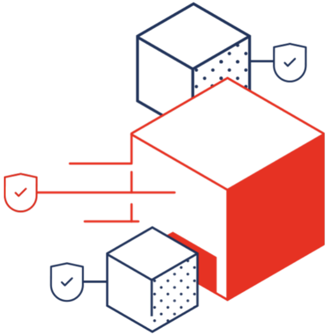
OpenShift - trendy v bezpečnost platformy a celého software delivery chain

David Bečvařík

Red Hat

The OpenShift platform vision:

A single hybrid-cloud platform for enterprises to build, deploy, run and manage intelligent applications securely at scale.

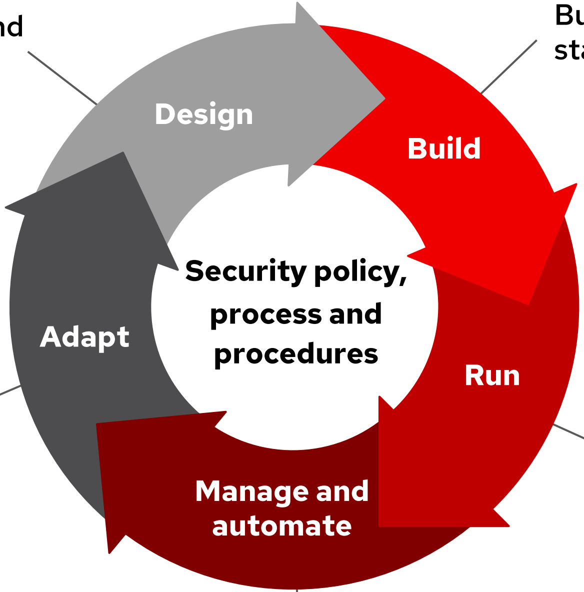


Red Hat

Security must be continuous and holistic

Identify security requirements and governance models

Built-in from the start; not bolted-on



FedRAMP

NIST National Institute of Standards and Technology U.S. Department of Commerce

CIS. Center for Internet Security

National Cyber Security Centre

PCI Security Standards Council

HIPAA Health Insurance Portability & Accountability Act

Revise, update, remediate as the landscape changes

Deploy to trusted platforms with enhanced security capabilities

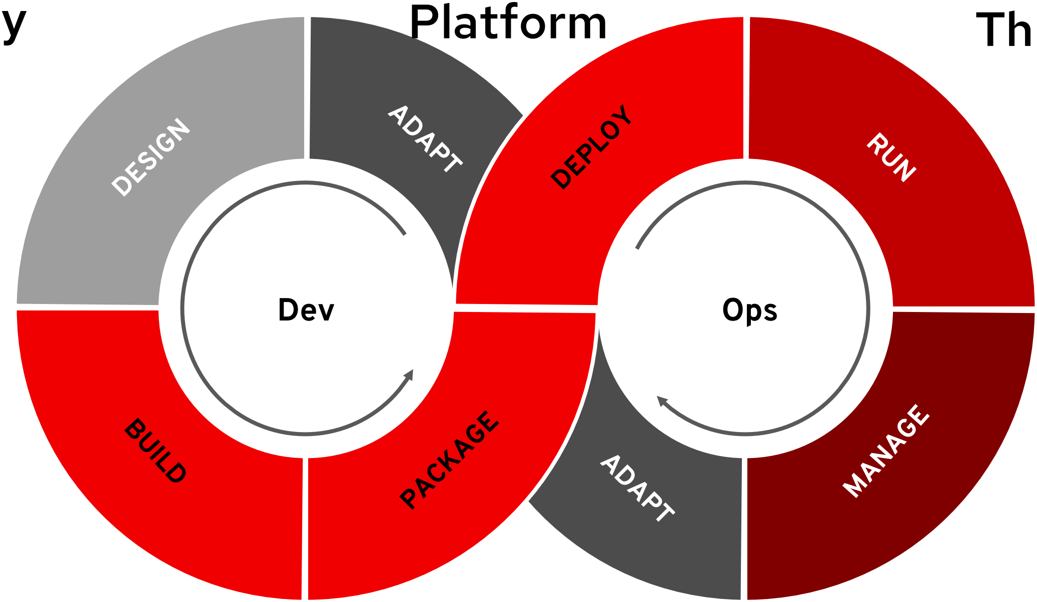
Automate systems for security and compliance

Containers and Kubernetes need DevSecOps

Control Application Security

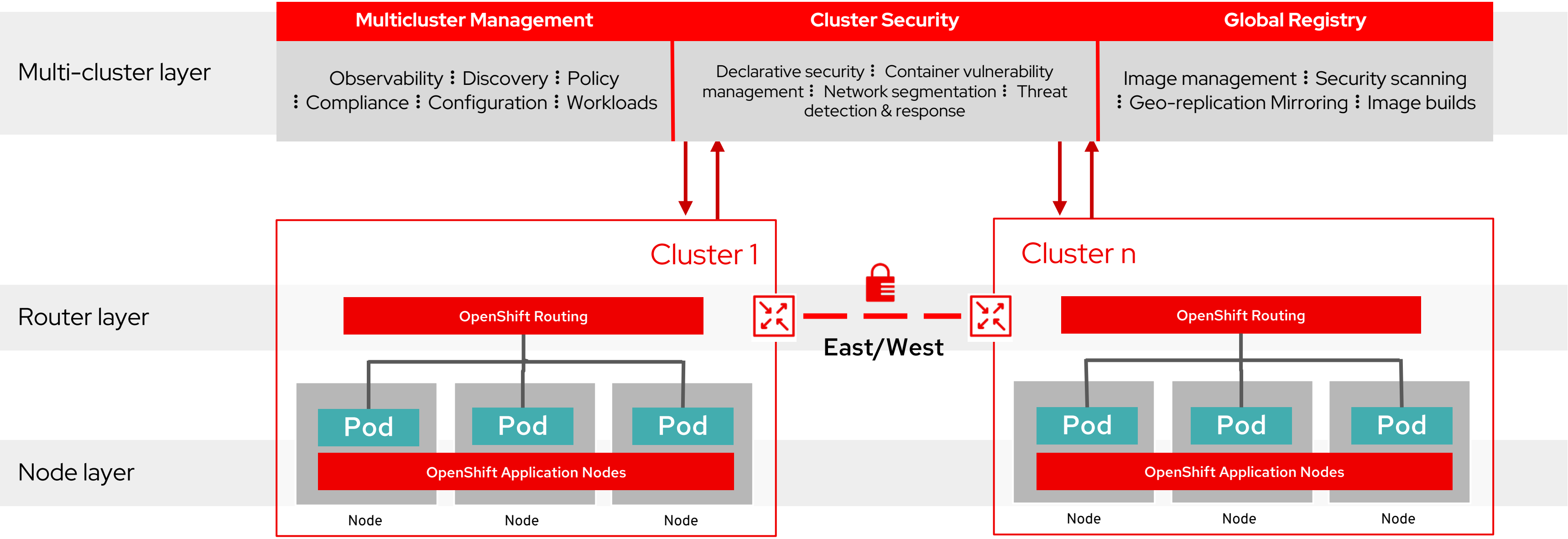
Protect the Platform

Detect & Respond to Runtime Threats



Red Hat OpenShift Platform Plus

Enabling Hybrid and Multi-Cloud Deployments


Multi-cluster layer
Multicluster Management
Observability ⁝ Discovery ⁝ Policy ⁝ Compliance ⁝ Configuration ⁝ Workloads
Cluster Security
Declarative security ⁝ Container vulnerability management ⁝ Network segmentation ⁝ Threat detection & response
Global Registry
Image management ⁝ Security scanning ⁝ Geo-replication Mirroring ⁝ Image builds
Router layer
Node layer
Cluster 1
OpenShift Routing
Pod
Pod
Pod
OpenShift Application Nodes
Node
Node
Node
East/West
Cluster n
OpenShift Routing
Pod
Pod
Pod
OpenShift Application Nodes
Node
Node
Node

Build: Control application security

Shift Security left

Best practices

Red Hat
UBI

- Use trusted sources for external content such as base images

Quay

- Use a trusted private registry to manage supply chain risk

OCP
Pipelines

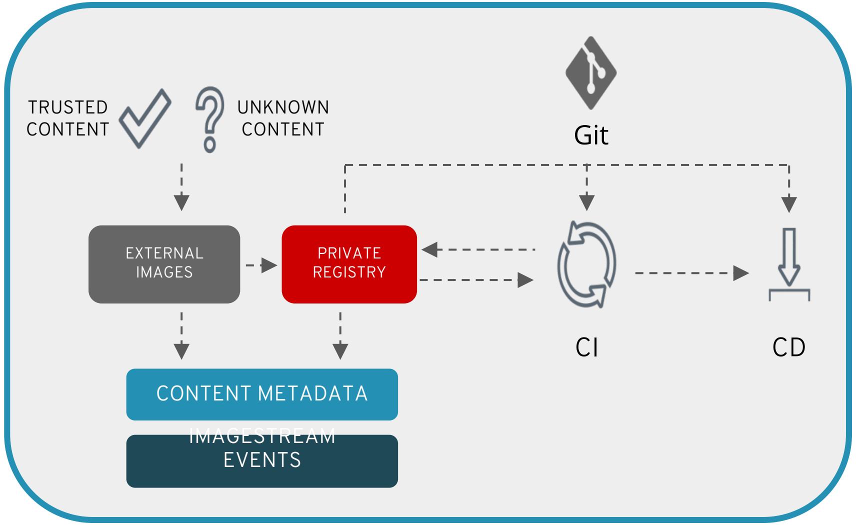
- Automate your CI/CD pipeline to enable rapid updates

Quay scanner (registry)
Code Ready (IDE)
ACS scanner (CI)
KubeLinter (CI)

- Integrate security tools / gates in your pipeline to identify
  - Known vulnerabilities
  - Application misconfigurations

ACM

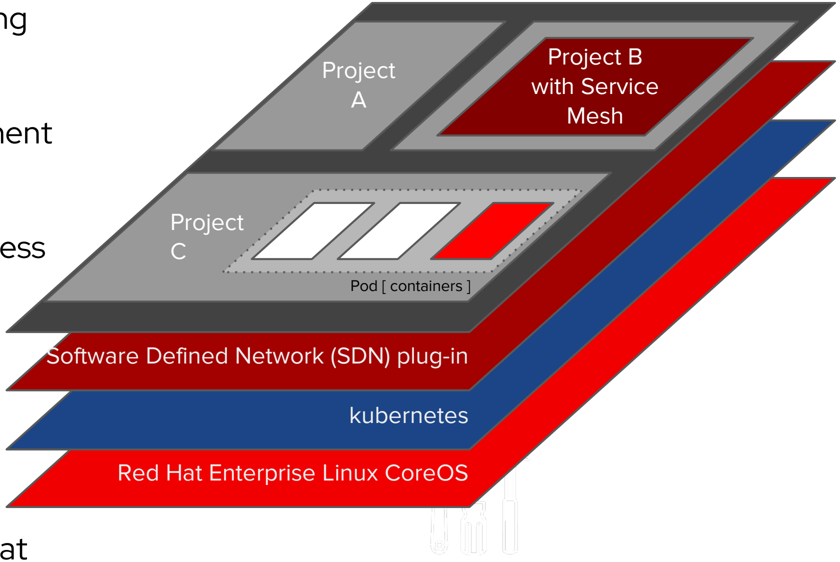
- Use policy-based deployment tools to manage application placement (e.g. locality)



Deploy: Protect the application platform

Best practices

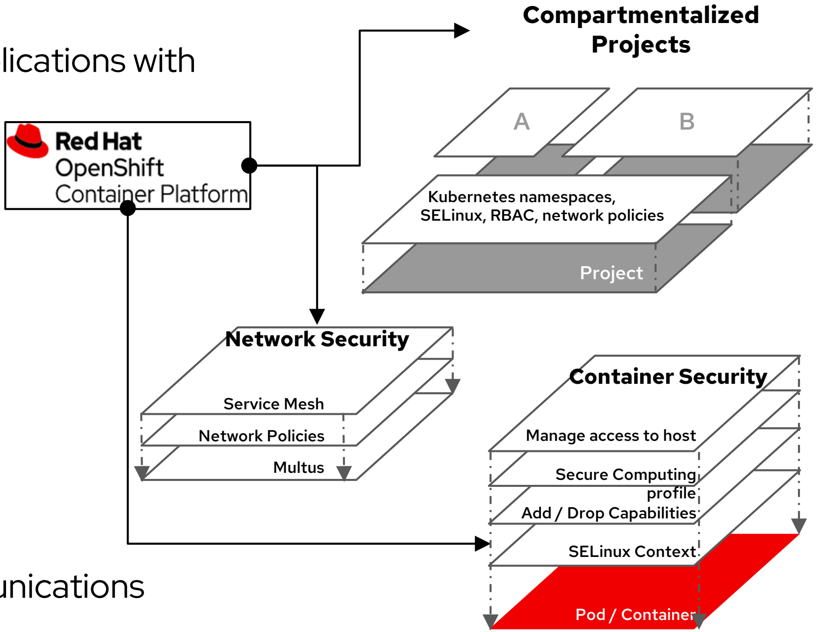
RHEL CoreOS	▶ Reduce attack surface with a container optimized operating system
OCP Operators ACM	▶ Use automated and policy-driven configuration management across your fleet
OCP RBAC ACS to monitor ACM to enforce	▶ Implement least privilege with fine-grained role based access control (RBAC)
OCP CAs Service mesh OCP IPSec RHCOS NBDE Encrypt etcd	▶ Encrypt platform data in transit and at rest
OCP Compliance Operator ACS ACM	▶ Use automated compliance, risk assessment and remediation solutions
OCP Security Context Constraints ACS	▶ Reduce deployment risk with admission control policies that • Minimize admission of privileged pods, pods with host capabilities • Prevent admission of pods with critical vulnerabilities


Project A
Project B with Service Mesh
Project C
Pod [containers]
Software Defined Network (SDN) plug-in
kubernetes
Red Hat Enterprise Linux CoreOS

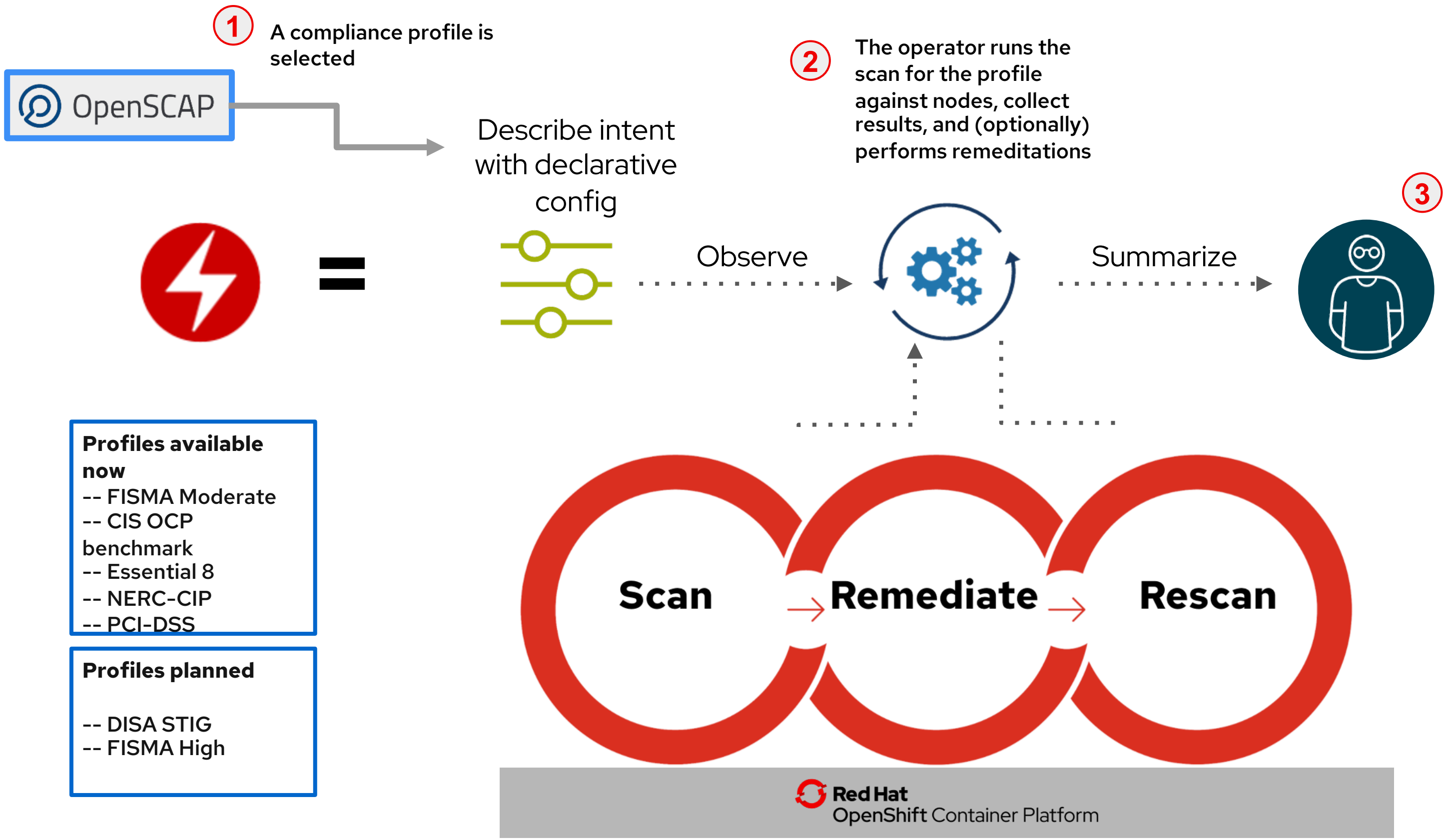
Run: Securing the container runtime

Best practices

- Minimize the impact of an attack by isolating running applications with
  - OCP ACS SELinux & Security Context Constraints
  - Kubernetes namespaces (Projects), RBAC
  - Network Policies for microsegmentation
- OCP ACM Use resource quotas to prevent resource exhaustion
- Manage application access and protect application data
  - Red Hat Single Sign On for user management
  - OCP Secure routes / ingress, 3Scale API Gateway
  - Service mesh to encrypt pod-to-pod traffic
  - Egress IPs / firewall
- OCP ACS ACM Monitor application metrics, logging and network communications
- ACS Automate threat detection and response
  - Alert or kill pods based on anomalous behavior
  - Detect privilege escalation and risky processes such as cryptomining



Openshift Compliance Operator for Continuous Compliance


OpenSCAP
Describe intent with declarative config
Observe
Summarize
Scan
Remediate
Rescan
Red Hat OpenShift Container Platform

1 A compliance profile is selected

2 The operator runs the scan for the profile against nodes, collect results, and (optionally) performs remeditations

3 Accreditors or Auditors can examine the scan results for compliance status, After review, if desired, remediations can be manually applied by the cluster-admin.

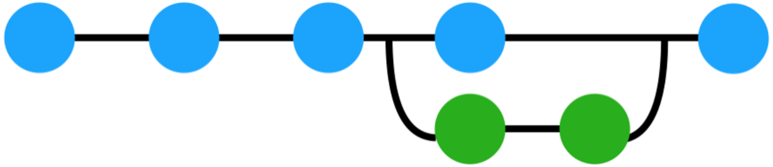
Profiles available now
-- FISMA Moderate
-- CIS OCP benchmark
-- Essential 8
-- NERC-CIP
-- PCI-DSS

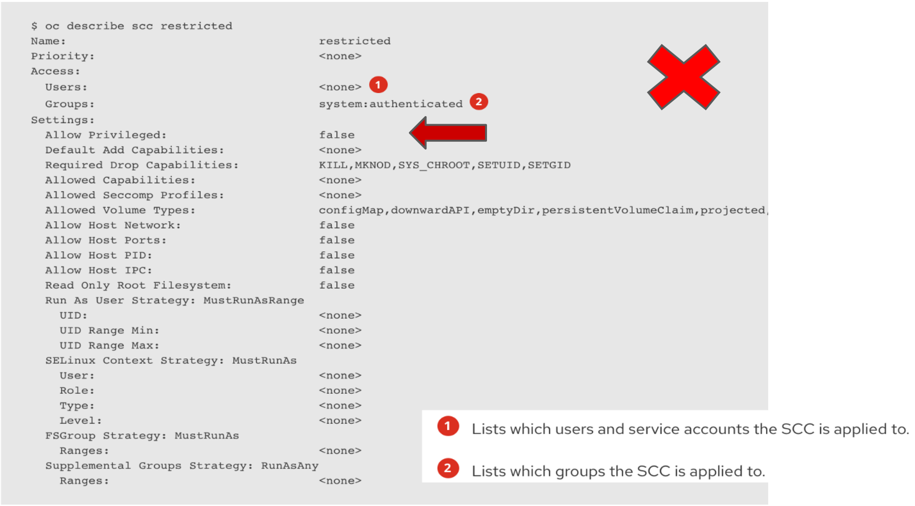
Profiles planned

-- DISA STIG
-- FISMA High

Policy-based deployment

- Allow list / block list to ensure pods are only deployed from approved registries
- Validate image signatures
- Automate principle of least privilege with Security Context Constraints
  - Automate allowed permissions for pods; if requested permissions are not allowed, the pod is not deployed
  - With the restricted SCC, pods cannot run as privileged, mount host directory volumes, or access the host network.
  - Admin can grant access to privileges when necessary.



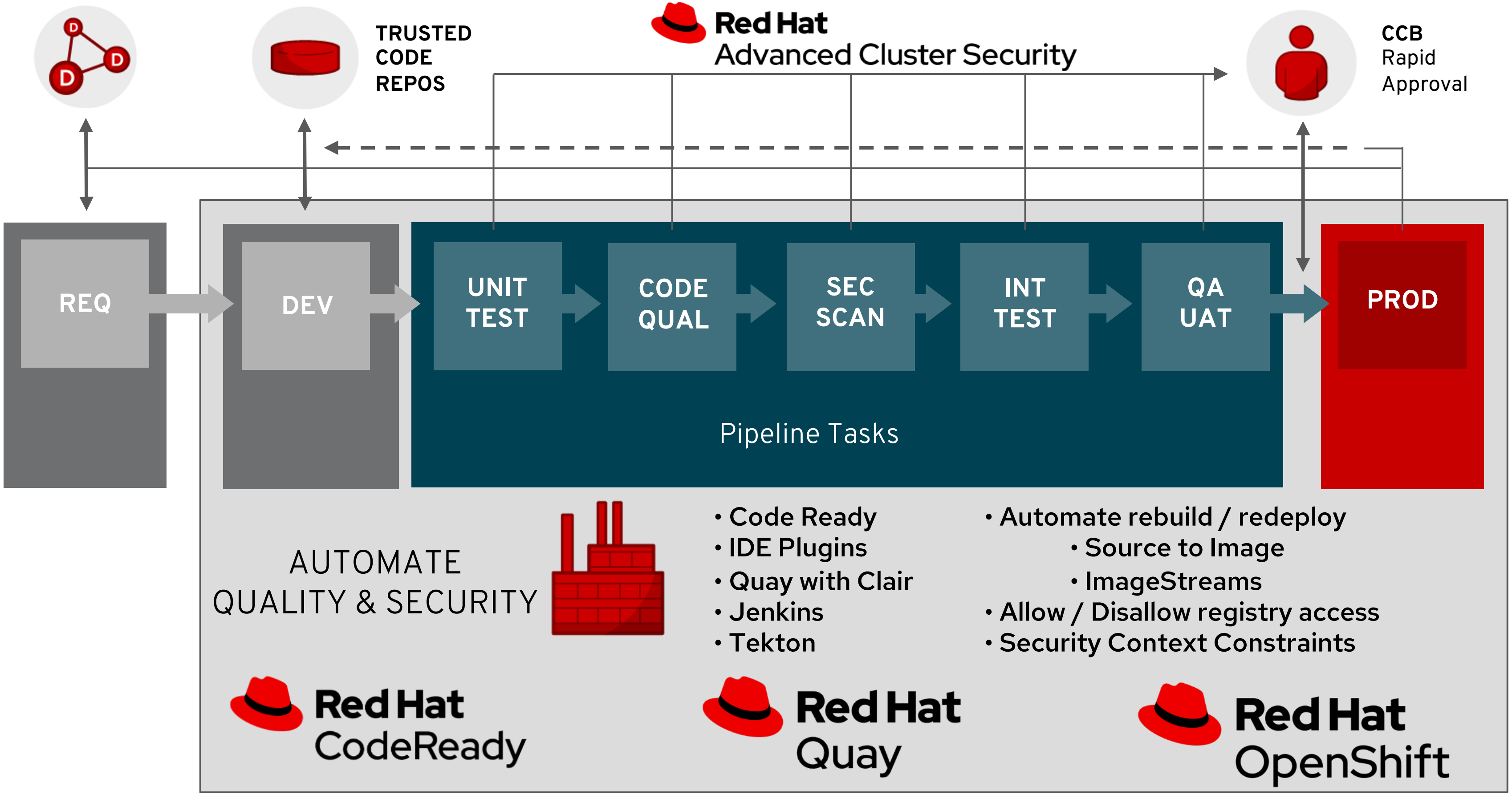


```
$ oc describe scc restricted
Name:                                   restricted
Priority:                               <none>
Access:
  Users:                                <none> [1]
  Groups:                               system:authenticated [2]
Settings:
  Allow Privileged:                     false
  Default Add Capabilities:             <none>
  Required Drop Capabilities:           KILL,MKNOD,SYS_CHROOT,SETUID,SETGID
  Allowed Capabilities:                 <none>
  Allowed Seccomp Profiles:             <none>
  Allowed Volume Types:                 configMap,downwardAPI,emptyDir,persistentVolumeClaim,projected,
  Allow Host Network:                   false
  Allow Host Ports:                     false
  Allow Host PID:                       false
  Allow Host IPC:                       false
  Read Only Root Filesystem:            false
  Run As User Strategy: MustRunAsRange
    UID:                                <none>
    UID Range Min:                      <none>
    UID Range Max:                      <none>
  SELinux Context Strategy: MustRunAs
    User:                               <none>
    Role:                               <none>
    Type:                               <none>
    Level:                              <none>
  FSGroup Strategy: MustRunAs
    Ranges:                             <none>
  Supplemental Groups Strategy: RunAsAny
    Ranges:                             <none>
```

[1] Lists which users and service accounts the SCC is applied to.

[2] Lists which groups the SCC is applied to.

The CI/CD pipeline for containers needs automation



TRUSTED CODE REPOS

Red Hat Advanced Cluster Security

CCB Rapid Approval

REQ

DEV

UNIT TEST

CODE QUAL

SEC SCAN

INT TEST

QA UAT

PROD

Pipeline Tasks

AUTOMATE QUALITY & SECURITY

- Code Ready
- IDE Plugins
- Quay with Clair
- Jenkins
- Tekton

- Automate rebuild / redeploy
  - Source to Image
  - ImageStreams
- Allow / Disallow registry access
- Security Context Constraints

Red Hat CodeReady

Red Hat Quay

Red Hat OpenShift

Hat

Red Hat Advanced Cluster Security: Use Cases

Security across the entire application lifecycle

Vulnerability Management

Protect yourself against known vulnerabilities in images and running containers

Security Configuration Management

Ensure your deployments are configured according to security best practices

Risk Profiling

Gain context to prioritize security issues throughout OpenShift and Kubernetes clusters

Network Segmentation

Apply and manage network isolation and access controls for each application

Compliance

Meet contractual and regulatory requirements and easily audit against them

Detection and Response

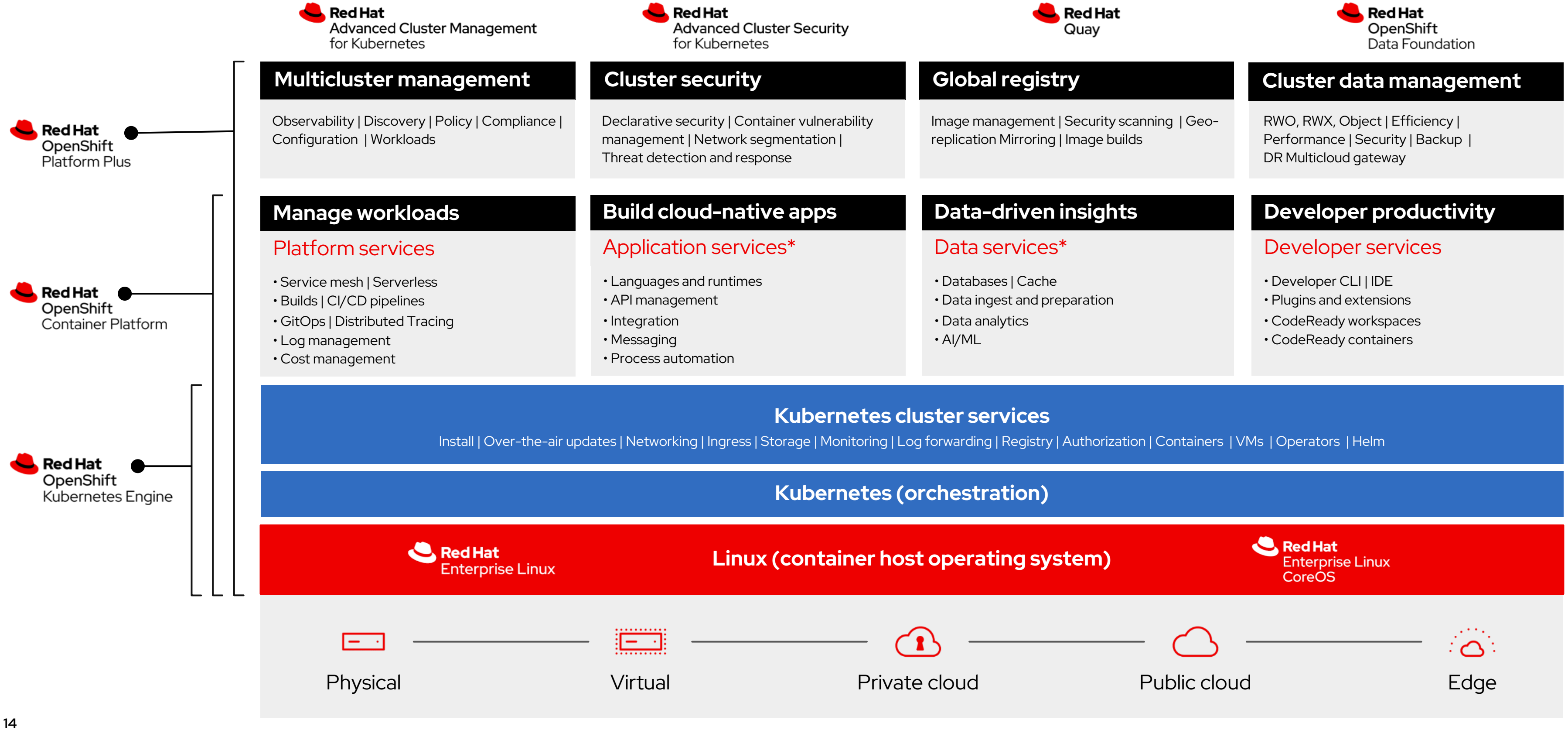
Carry out incident response to address active threats in your environment

OpenShift delivers continuous security

	Control	Protect	Detect & Respond
ACM	Application Lifecycle and Locality	Fleet Management	Fleet Observability & Alerts
ACS	Vulnerability analysis	Policy admission controller	Runtime behavioral analysis
	App config analysis	Compliance assessments	Auto-suggest network policies
	APIs for CI/CD integrations	Risk profiling	Threat detection / incident response
OCP	Trusted content	Kubernetes platform lifecycle	Container isolation
	Container registry	Identity and access management	Network isolation
	Build management	Protect platform data	Protect application access and data
	CI/CD pipeline	Deployment policies	Observability
	BUILD	DEPLOY	RUN

DevSecOps

Red Hat open hybrid cloud platform



Red Hat OpenShift Platform Plus

Red Hat OpenShift Container Platform

Red Hat OpenShift Kubernetes Engine

Red Hat Advanced Cluster Management for Kubernetes

Multicluster management

Observability | Discovery | Policy | Compliance | Configuration | Workloads

Red Hat Advanced Cluster Security for Kubernetes

Cluster security

Declarative security | Container vulnerability management | Network segmentation | Threat detection and response

Red Hat Quay

Global registry

Image management | Security scanning | Geo-replication Mirroring | Image builds

Red Hat OpenShift Data Foundation

Cluster data management

RWO, RWX, Object | Efficiency | Performance | Security | Backup | DR Multicloud gateway

Manage workloads

Platform services

- Service mesh | Serverless
- Builds | CI/CD pipelines
- GitOps | Distributed Tracing
- Log management
- Cost management

Build cloud-native apps

Application services*

- Languages and runtimes
- API management
- Integration
- Messaging
- Process automation

Data-driven insights

Data services*

- Databases | Cache
- Data ingest and preparation
- Data analytics
- AI/ML

Developer productivity

Developer services

- Developer CLI | IDE
- Plugins and extensions
- CodeReady workspaces
- CodeReady containers

Kubernetes cluster services

Install | Over-the-air updates | Networking | Ingress | Storage | Monitoring | Log forwarding | Registry | Authorization | Containers | VMs | Operators | Helm

Kubernetes (orchestration)

Red Hat Enterprise Linux

Linux (container host operating system)

Red Hat Enterprise Linux CoreOS

Physical

Virtual

Private cloud

Public cloud

Edge

* Red Hat OpenShift® includes supported runtimes for popular languages/frameworks/databases. Additional capabilities listed are from the Red Hat Application Services and Red Hat Data Services portfolios.

** Disaster recovery, volume and multicloud encryption, key management service, and support for multiple clusters and off-cluster workloads requires OpenShift Data Foundation Advanced

Security Partners by Use Case

Partners extend and enhance Red Hat functionality

Application Analysis

SAST, SCA, IAST, DAST, Image Risk

- paloalto NETWORKS
- SYNOPSYS
- aqua
- anchore
- NeuVector
- snyk
- sysdig
- Red Hat Advanced Cluster Security

Identity & Access Mgmt

Auth, RBAC, Secrets Vault, Provenance, HSM

- IBM IAM
- CYBERARK
- THALES

Compliance

Regulatory Compliance, PCI-DSS, GDPR

- aqua
- SYNOPSYS
- TIGERA
- anchore
- Red Hat Advanced Cluster Security
- NeuVector
- sysdig
- paloalto NETWORKS

Network Controls

CNI Plugins, Policies, Traffic Controls, Service Mesh

- aqua
- TIGERA
- Red Hat Advanced Cluster Security
- sysdig
- paloalto NETWORKS

Data Controls

Data Protection and Encryption

- IBM Guardium
- Zettaset
- THALES

Runtime Analysis & Protection

RASP, Production Analysis

- aqua
- sysdig
- paloalto NETWORKS
- anchore
- NeuVector
- Red Hat Advanced Cluster Security

Audit & Monitoring

Logging, Visibility, Forensics

- sysdig
- NeuVector
- Red Hat Advanced Cluster Security
- aqua
- paloalto NETWORKS

Remediation

SOAR, Automatic resolution

- snyk
- paloalto NETWORKS
- IBM Resilient

Red Hat Platform Security

Secure Host, Container Platform, Namespace Isolation, k8s & Container Hardening

OpenShift 4: Automated Configuration and Lifecycle Management

Dramatically simplified for the Hybrid Cloud

Machines

Machines are complex for ops

↓

Make machines easy
(like containers)

Configuration

Config change is risky

↓

Make config management
and config change
easy and safe

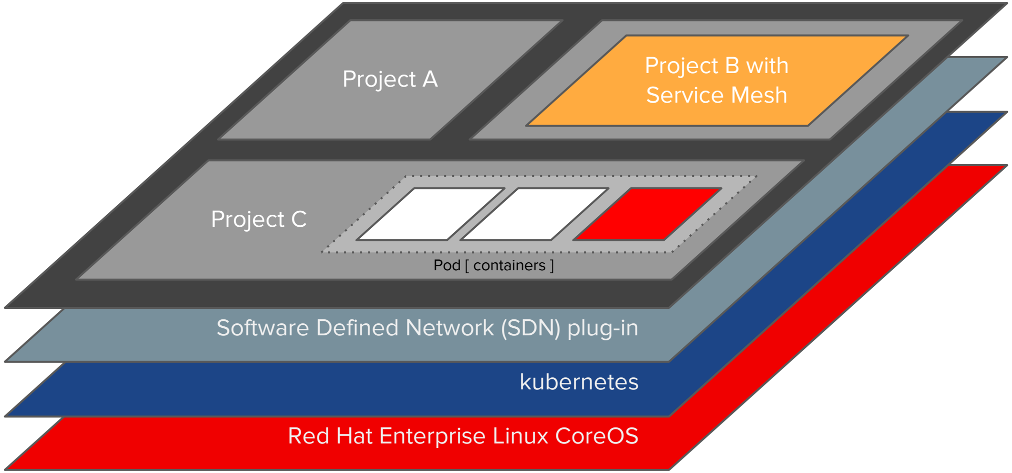
Lifecycle

Software lifecycle is hard

↓

Automate software
lifecycle on Kube

Red Hat OpenShift: Defense in Depth


Project A
Project B with Service Mesh
Project C
Pod [containers]
Software Defined Network (SDN) plug-in
kubernetes
Red Hat Enterprise Linux CoreOS

1. Automated configuration and operations
2. Integrated node management, including host OS
3. Protect data at rest, data in transit
4. Authentication and authorization
5. OOTB deploy policies manage workload privileges
6. Network security and segmentation
7. Automated compliance and remediation
8. Automated application deployment (e.g. locality to meet GDPR)
9. Runtime behavioral analysis and vulnerability management
10. Security policies and event response

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

youtube.com/user/RedHatVideos

facebook.com/redhatinc

twitter.com/RedHat