

October 25, 2022

Building **DevSecOps** into AWS EKS using **Red Hat ACS**

Pathik Patel

Head of Cloud Security

Pathik Patel



@pathikpa – Twitter

With Informatica for past 6 years

Before that Netflix, Yahoo!

#Kubernetes, #python, #cryptography

Informatica @ a Glance

\$1.44B IN REVENUE

OFFERS INTELLIGENT DATA MANAGEMENT CLOUD (IDMC)

32 TRILLION TRANSACTION PER MONTH

MULTI-CLOUD OFFERINGS

My DevSecOps Opinion



Dev (development), Sec(security), Ops(operations) coming together and moving at same speed



Security is a shared responsibility



DevSecOps is a shared security mindset



Build guardrails for early feedback



Shiftleft gates to build secure code

DevSecOps Lifecycle



Plan & Develop

- Threat Modelling
- Pre-commit hooks
- Secure coding standards
- Peer Review



Code Commit

- SAST
- Dependency management
- Secure pipeline



Build & Test

- DAST
- Configurations scans
- Vulnerability scans
- Configuration validation



Ship & Deploy

- Security Smoke Tests
- Configuration Checks
- Pentest



Monitor

- Continuous Monitoring
- Vulnerability Scans

Tools of trade



AmazonEKS

Managed Kubernetes engine from AWS



Amazon ECR

Container registry offering hosted on AWS



Red Hat

Advanced Cluster
Security
for Kubernetes

Security configuration and monitoring tool

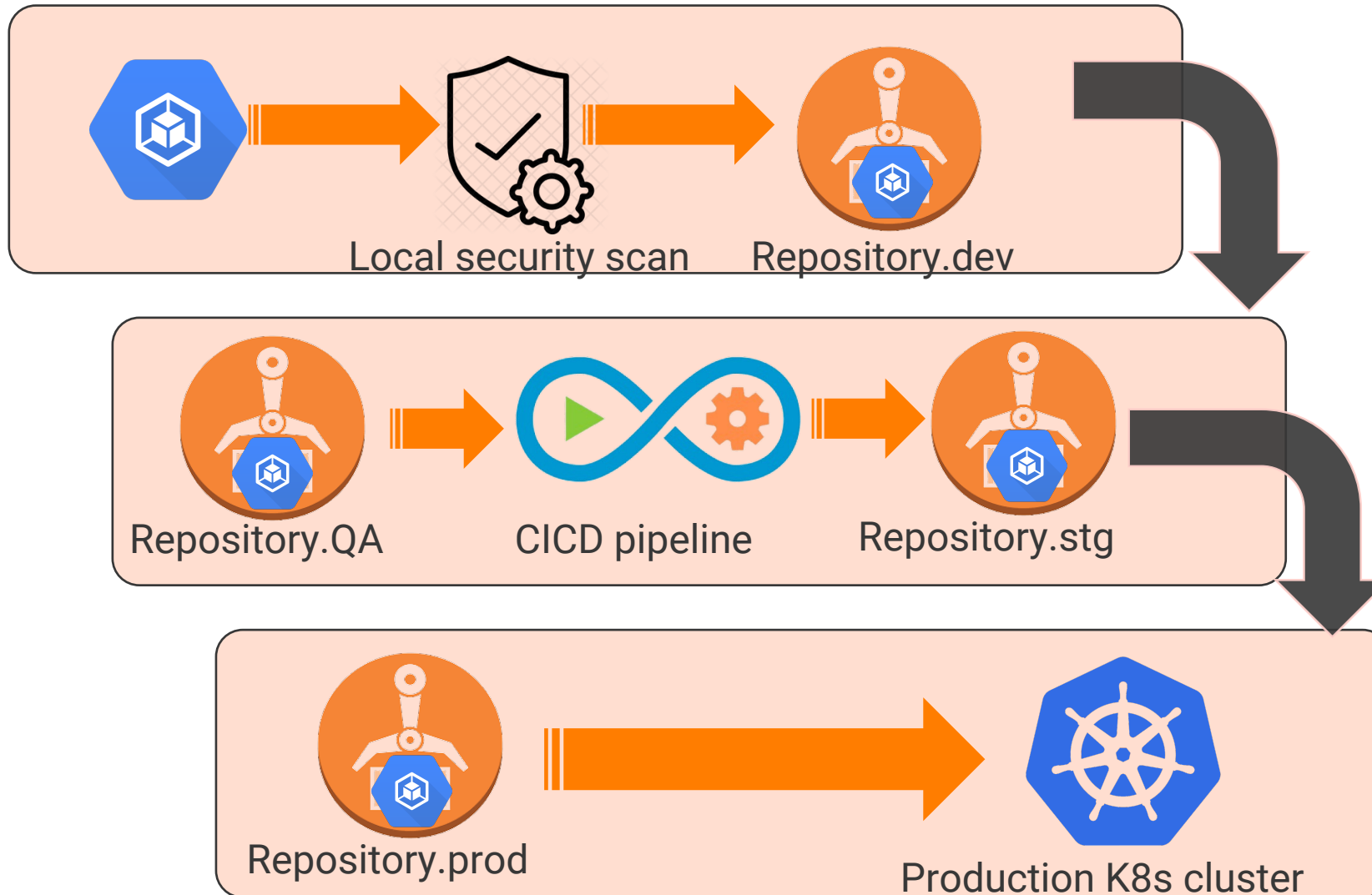


Ticketing and workflow management

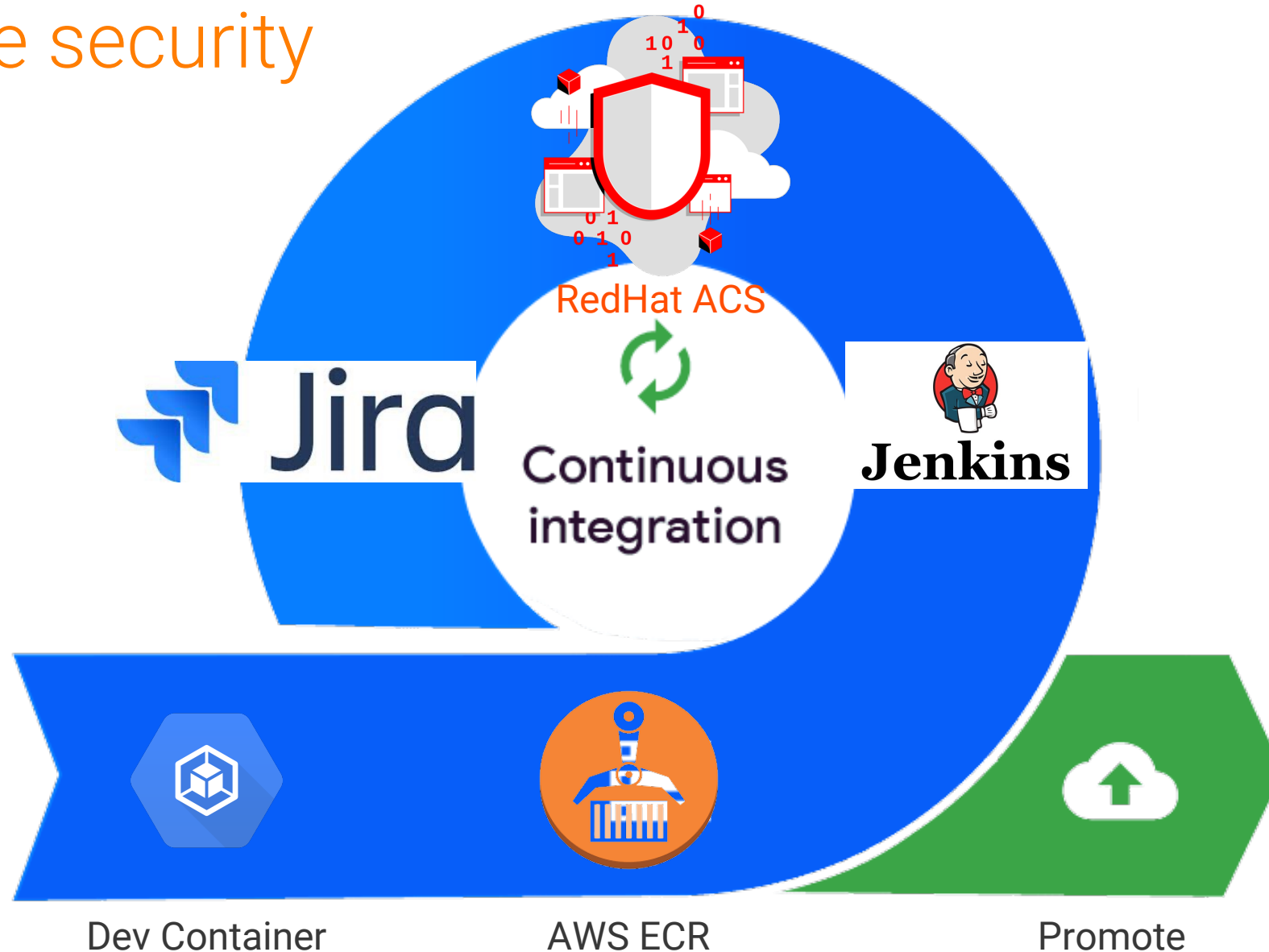
Best Practices

- Segregate your repositories
- Use distro-less container images
- Use admission controllers
- Enable Audit logs
- Consider build time and runtime security controls
- Adopt service mesh for optimal routing & encryption
- Implement CIS scans for container, worker node and clusters

Promoting your images



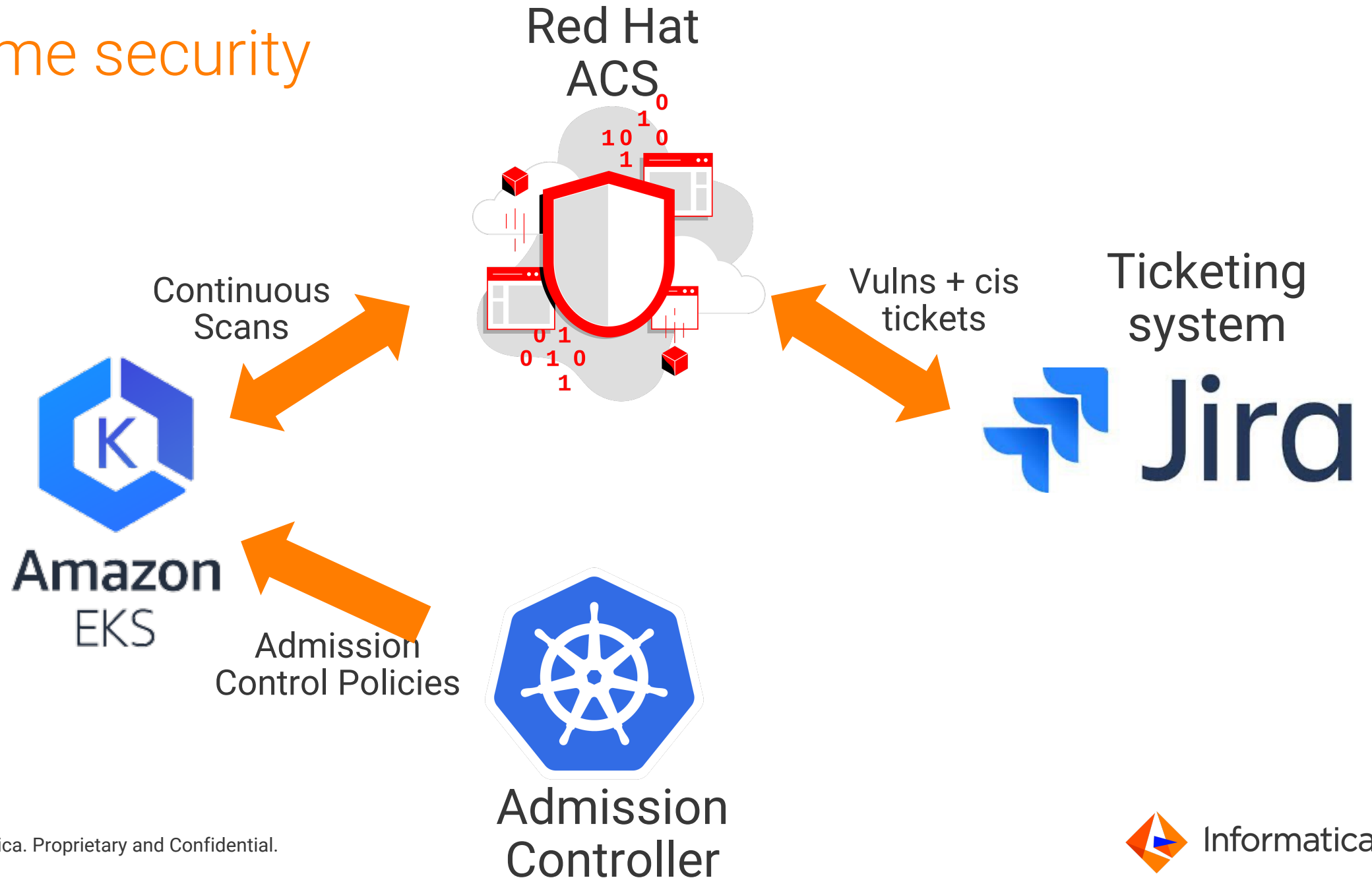
Build time security



Build secure images

- **Distro-less** images will save you lot of pain
- **Remove** package managers, unused utilities (e.g. network, filesystem)
- **Encourage** developers to scan while building image
- **Integrate** ACS with Jenkins CICD for continuous feedback during build time
- **Scan** at dev time and promote to QA
- **Scan** in CI pipeline and promote to staging
- **Block** build system from using non-compliant repositories
- **Allow** only from approved labeled repositories

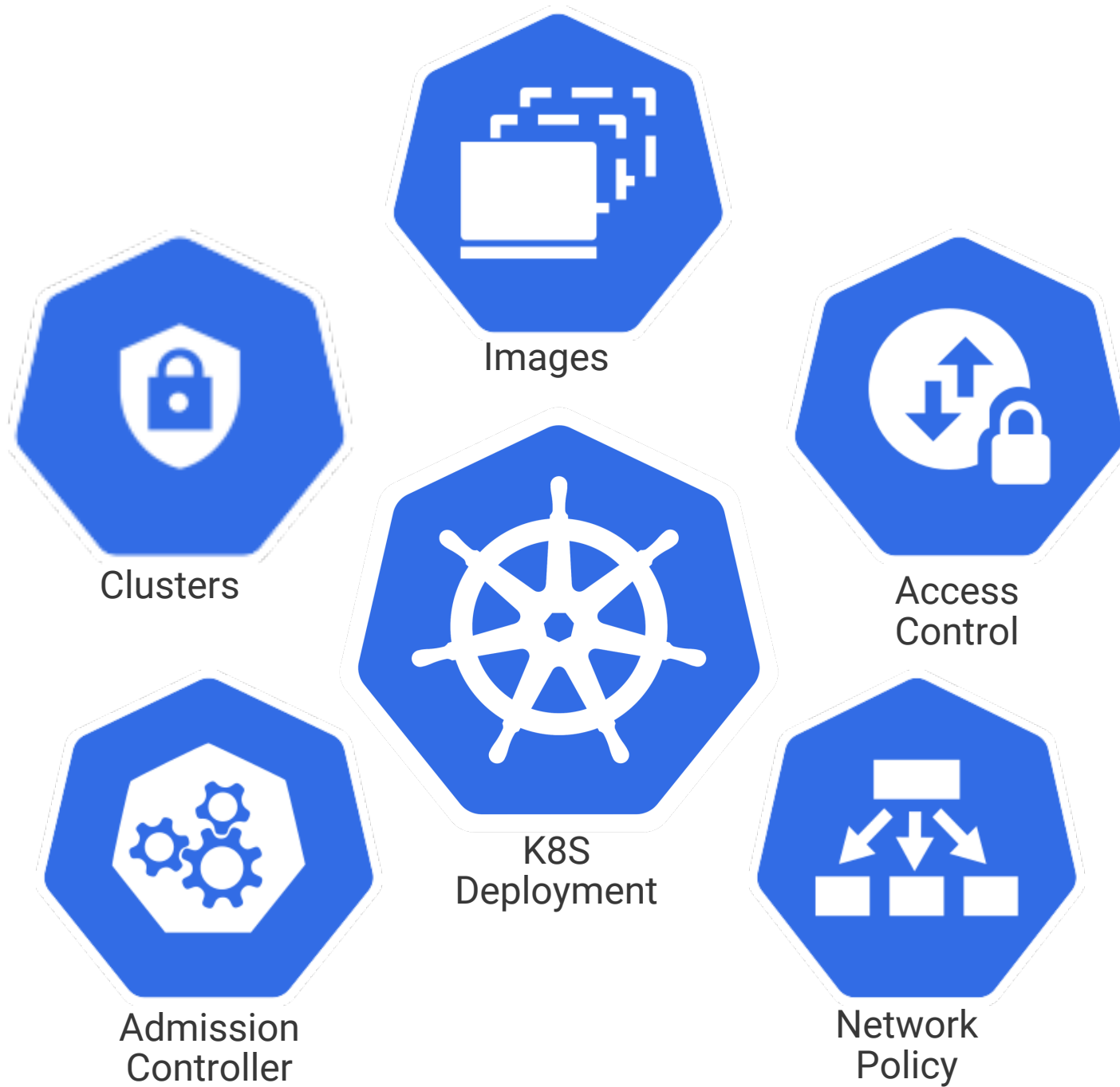
Run time security



Secure your runtime

- Enforce **NameSpace** usage to
 - Build out segregation between products, business units
 - Enforce RBAC to allow access within namespace only
 - Create network policies and segmentation
- Use **Admission Controller** to
 - Enforce company wide guardrails
 - Implement PodSecurityPolicies(PSP)
 - Protect your API server
 - Enforce repository usage
- **Monitor configurations** to
 - Detect CIS compliance failures
 - Rogue container processes
 - Enforce RBAC

Risk Lens



Risk based evaluation

RISK
De 11748 Deployments

Add one or more resource filters

+ CREATE POLICY

11748 DEPLOYMENTS
Please add a filter to narrow down your results.

Page 1 of 235

Vault-Consul-Consul-Server

Name
Created
Cluster
Namespace
Priority

RISK INDICATORS
DEPLOYMENT DETAILS
PROCESS DISCOVERY

infa-spin-sidecar

02/07/2022 | 8:01:55PM

spin2-prod-uswest2-kube-controlplane-sensor

spinnaker

8

vault-consul-consul-server

10/13/2020 | 8:40:41AM

cloudtrust-shrd-aks-prod-jpeast

ha-vault-ichsnttprod-jpeast

12

vault-consul-consul-server

07/08/2019 | 2:40:07PM

ichsprod1-useast1-kube-controlplane

ha-vault-prod-useast1

12

jenkins

07/10/2019 | 3:28:22PM

spin2-prod-uswest2-kube-controlplane-sensor

jenkins

14

spin-rosc

07/11/2019 | 2:32:29PM

spin2-prod-uswest2-kube-controlplane-sensor

spinnaker

15

spin-rosc

10/17/2022 | 9:25:10PM

spin2-prod-uswest2-kube-controlplane-sensor

spin-k8s-prod

15

Policy Violations

Fixable CVSS >= 7 (severity: High)

Process with UID 0 (severity: High)

Secret Mounted as Environment Variable (severity: High)

Untrusted Images (severity: High)

90-Day Image Age (severity: Medium)

Container using read-write root filesystem (severity: Medium)

Docker CIS 4.1: Ensure That a User for the Container Has Been Created

Take Aways

- Define guard rails and document
- Codify guard rails using Red Hat ACS
- Provide early feedback to developers
- K8s amplifies your problems (1000s of containers)
- Build automation to report

Questions??

Thank you

ppatel@informatica.com

