Webinar 23-06-2022

#CloudDevSecOps

Advanced Cluster Security: come si mette davvero al sicuro il cloud

Red Hat | par-tec

Eleonora Peruch
Solution Architect
Red Hat

Gabriele Torregrossa
DevOps Engineer
Par-Tec

Francesco Pignatelli
Giornalista
G11 Media

Red Hat | par-tec

Eleonora Peruch
Solution Architect
Red Hat

#CloudDevSecOps

Red Hat | par-tec

Advanced Cluster Security: come si mette davvero al sicuro il cloud

Red Hat
Advanced Cluster Security
for Kubernetes

DevSecOps with Red Hat Advanced Cluster Security for Kubernetes

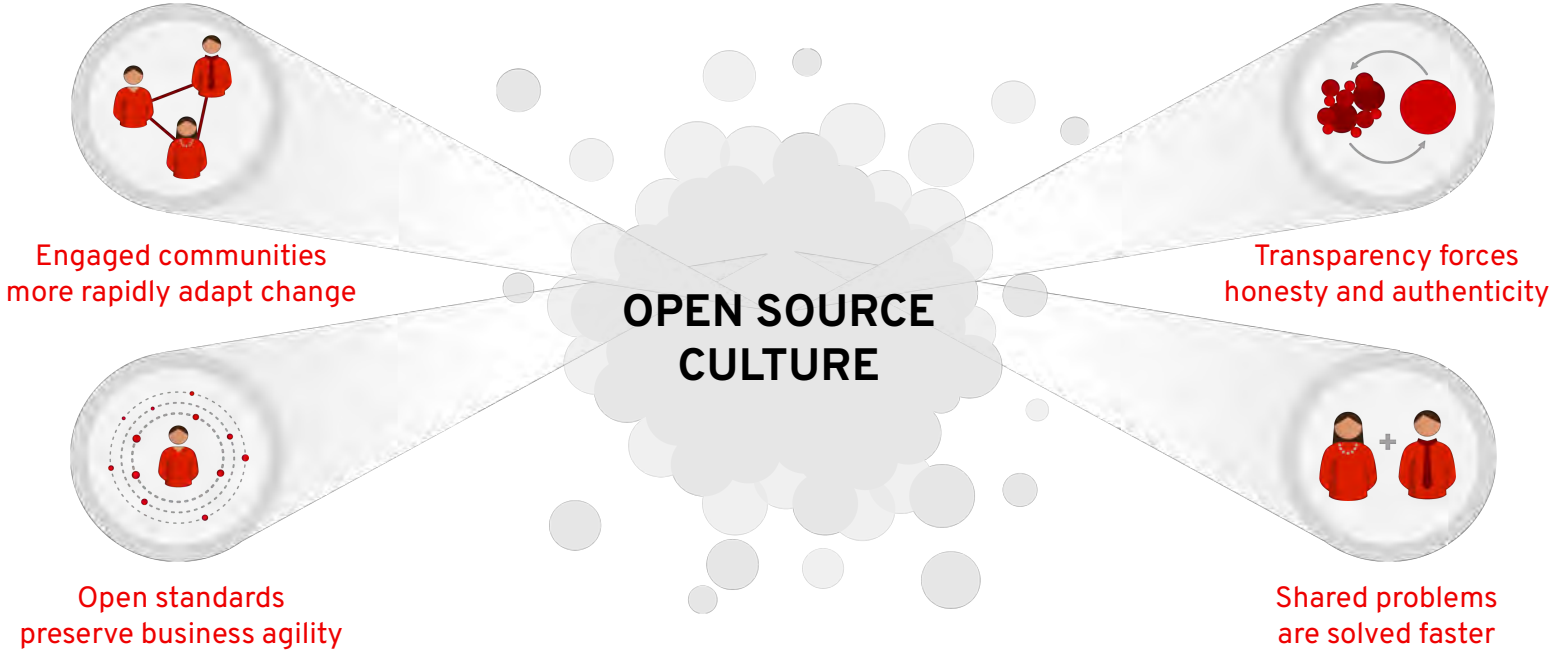
Eleonora Peruch
Red Hat Solution Architect

Agenda

1. Red Hat Hybrid Cloud Strategy
2. Continuous Security for Cloud-Native Applications
3. Product Overview
4. DevSecOps Examples

Red Hat Hybrid Cloud Strategy

Open Source fuels the Innovation



Red Hat Mission

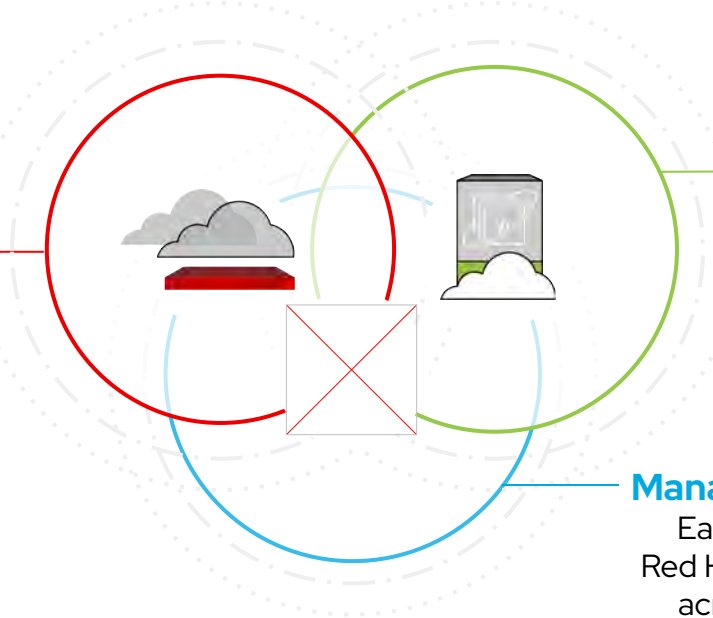
To be the catalyst in communities of customers contributors and partners creating better technology the open source way

Red Hat

The Three Pillars of Our Business

Open hybrid multi cloud & Edge

Red Hat's strategy and vision for its portfolio of software, tools, and services built in the open source development model and designed for future architectures that are open, secure, and agile across hybrid, multicloud.



Hybrid cloud infrastructure

Secure, scale, & manage foundations for traditional & cloud workloads across all environments

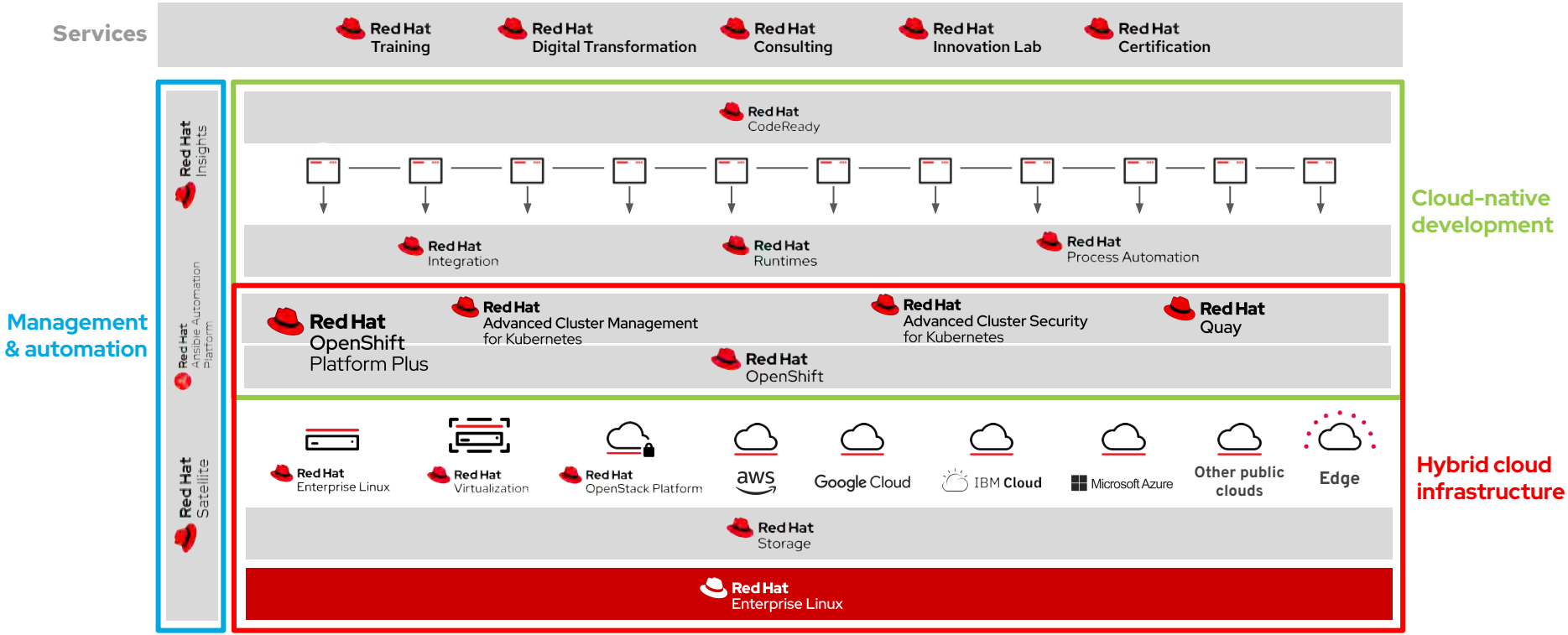
Cloud-native development

Develop, deploy, & manage any application, on any environment & give developers what they need to innovate

Management & automation

Easily & seamlessly manage Red Hat platforms and automate across hybrid environments

Red Hat Portfolio



Continuous Security for Cloud-Native Applications

Evolution of Security Challenges

Expanding the scope of security practices and instruments

"For those looking to secure complex environments, they need more than security features alone – there's a need for visibility across many environments, compliance management, threat detection, incident response, and much more."

451 Research, part of S&P Global Market Intelligence

Continuous Security: the NIST Five Functions

How to manage supply chain cybersecurity

NIST (National Institute of Standards and Technology) defined a Cybersecurity Framework that helps defining risk based cybersecurity outcomes, organized in a hierarchy of 5 core function, the **NIST Five Functions**:

- **Identify** the security environment, what we want to secure.
- **Protect** the identified environment with dedicated solutions (firewalls, waf, ecc)
- **Detect** anomalies and unusual behaviors.
- **Respond** to anomalies and threats (contain, investigate, ecc)
- **Recover** (turn off compromised systemd, restore, ecc).

https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

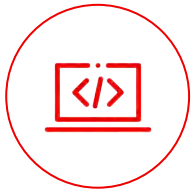
Benefits of a Kubernetes-native approach to security

Lower operational cost

DevOps and Security teams can use a common language and source of truth

Reduce operational risk

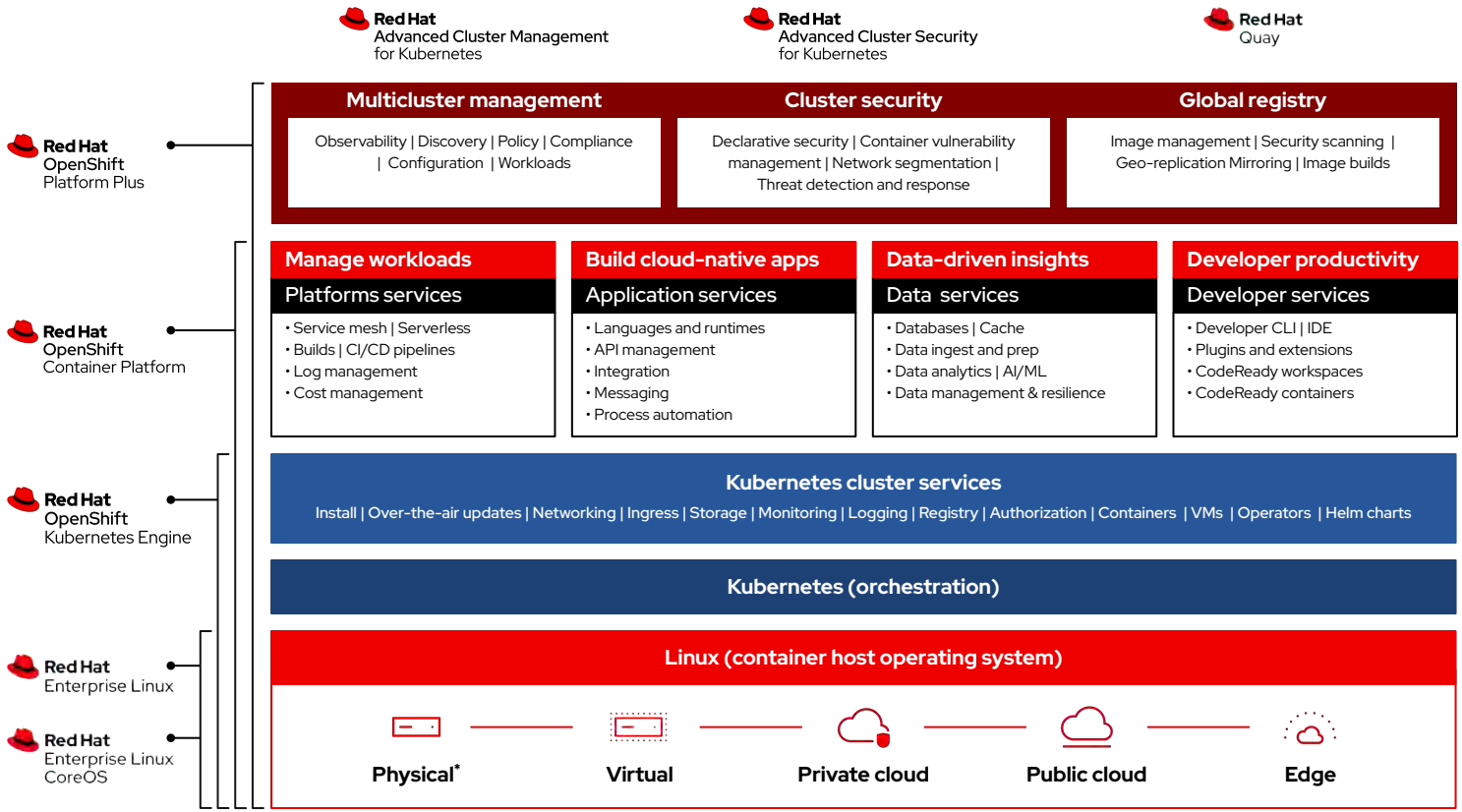
Ensure alignment between security and infrastructure to reduce application downtime



Increase developer productivity

Leverage Kubernetes to seamlessly provide guardrails supporting developer velocity

Product Overview



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

StackRox is now part of Red Hat

Red Hat
Advanced Cluster Security
for Kubernetes

Available as part of Red Hat OpenShift Platform Plus

Available as a standalone product

- Supporting Red Hat OpenShift, Amazon EKS, Google GKE, Azure AKS
- Existing StackRox customers supported as-is

Kubernetes is the standard for application innovation…

Red Hat OpenShift

- Microservices architecture
- Declarative definition
- Immutable infrastructure

…and Kubernetes-native security is increasingly critical

Red Hat
Advanced Cluster Security for Kubernetes

- Secure supply chain
- Secure infrastructure
- Secure workloads

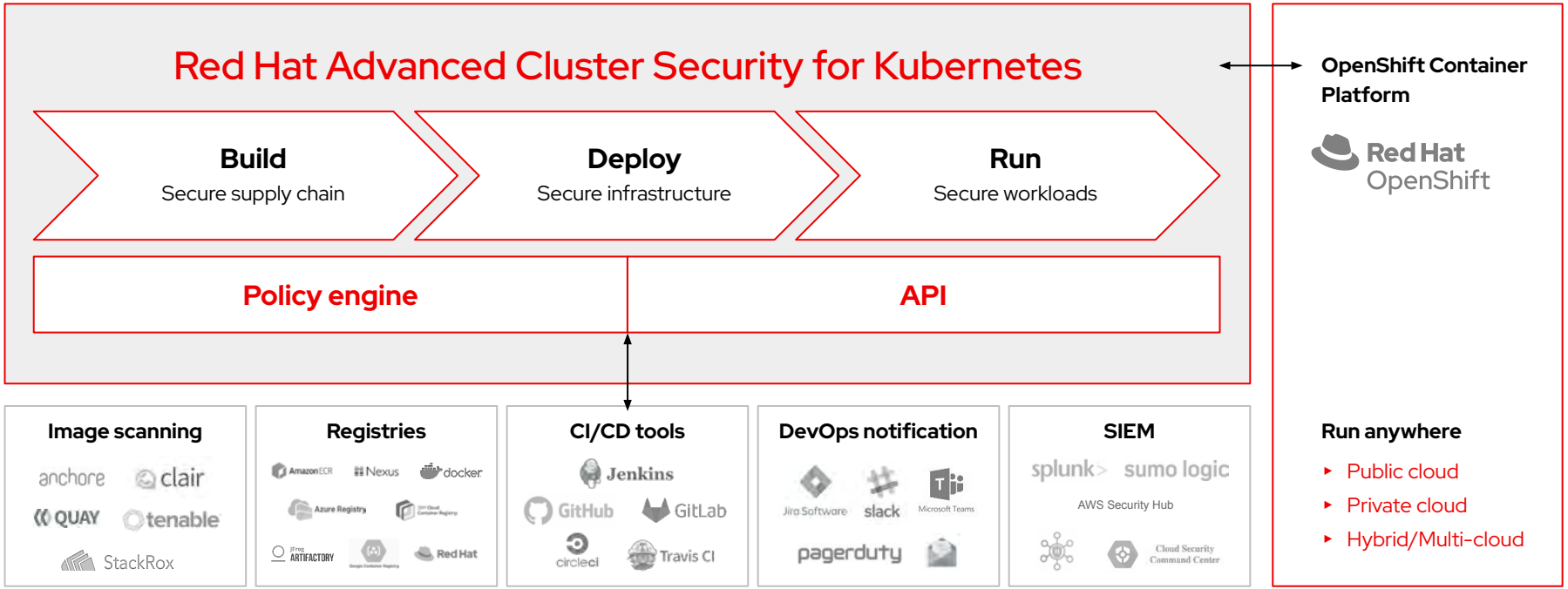
DevOps → DevSecOps → Security

Red Hat Advanced Cluster Security for Kubernetes

A cloud workload protection platform and cloud security posture management to enable you to “shift left”

Shift left	Cloud security posture management (CSPM)	Cloud workload protection (CWPP)
Secure supply chain	Secure infrastructure	Secure workloads
Extend scanning and compliance into development (DevSecOps)	Leverage built-in Kubernetes CSPM to identify and remediate risky configurations	Maintain and enforce a “zero-trust execution” approach to workload protection

RHACS Integration and Focus



Red Hat Advanced Cluster Security: Use Cases

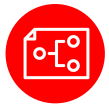
Security across the entire application lifecycle

Vulnerability Management

Protect yourself against known vulnerabilities in images and running containers

Configuration Management

Ensure your deployments are configured according to security best practices

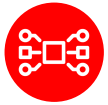


Risk Profiling

Gain context to prioritize security issues throughout OpenShift and Kubernetes clusters

Visibility

Comprehensive visibility into your cloud-native infrastructure



Network Segmentation

Apply and manage network isolation and access controls for each application

Compliance

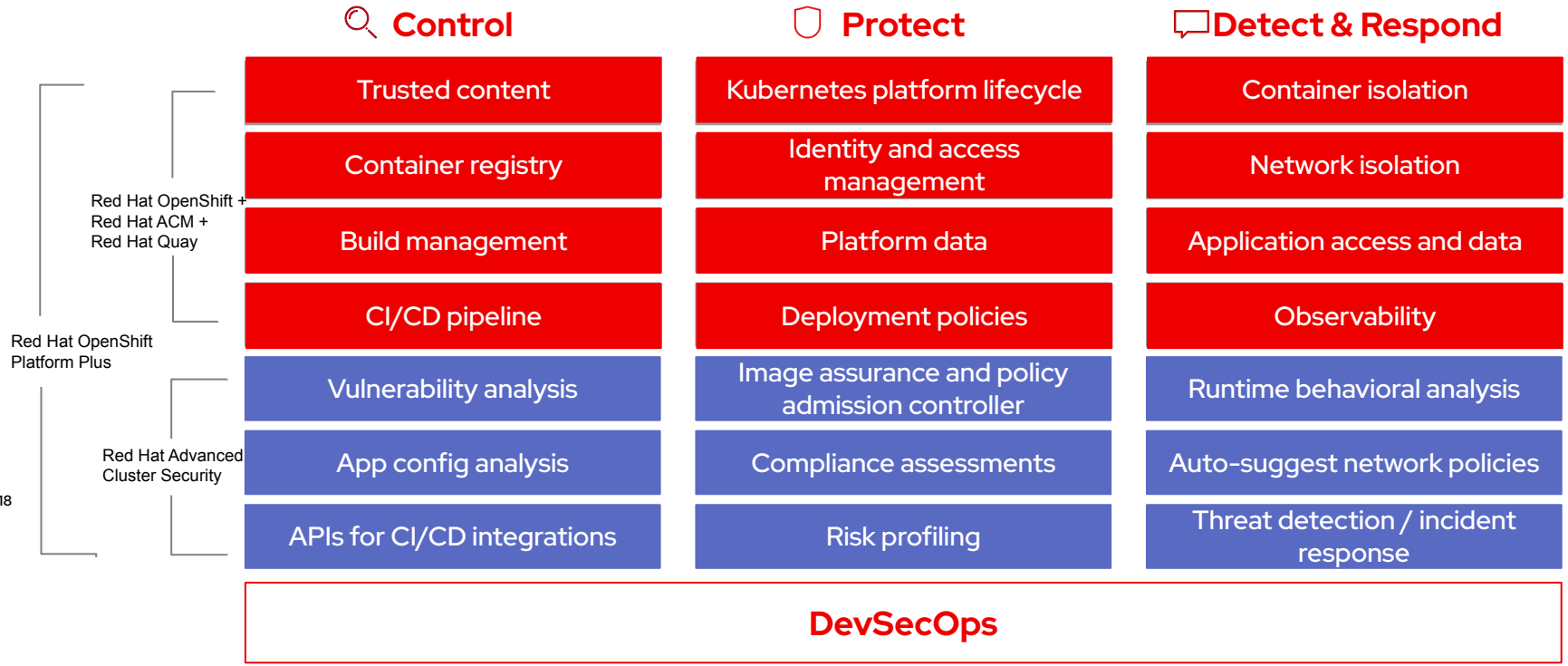
Meet contractual and regulatory requirements and easily audit against them

Detection and Response

Carry out incident response to address active threats in your environment

Enabling DevSecOps

Integrate vulnerability and configuration analysis into the CI/CD pipeline.

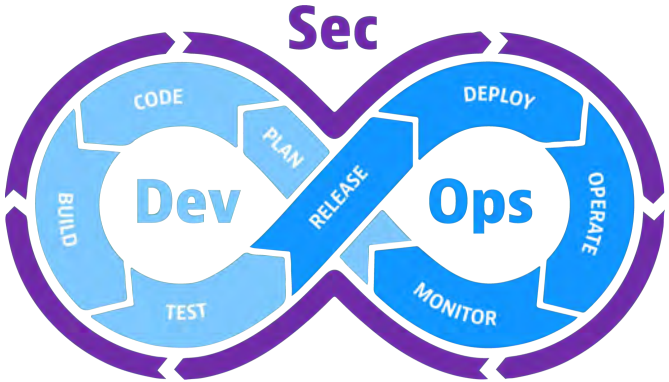

Control
Protect
Detect & Respond
Trusted content
Kubernetes platform lifecycle
Container isolation
Container registry
Identity and access management
Network isolation
Red Hat OpenShift + Red Hat ACM + Red Hat Quay
Build management
Platform data
Application access and data
CI/CD pipeline
Deployment policies
Observability
Red Hat OpenShift Platform Plus
Vulnerability analysis
Image assurance and policy admission controller
Runtime behavioral analysis
Red Hat Advanced Cluster Security
App config analysis
Compliance assessments
Auto-suggest network policies
APIs for CI/CD integrations
Risk profiling
Threat detection / incident response
DevSecOps

DevSecOps Examples

DevSecOps: the future of digital innovation

"Secure DevOps practices - also known as DevSecOps - is critical for enterprises that must rapidly develop and deploy digital innovations. The ability to quickly create, deploy, and iterate high-quality software will be a core business requirement by 2023."

IDC, DevSecOps: A Framework for the Future of Digital Innovation, April 2020

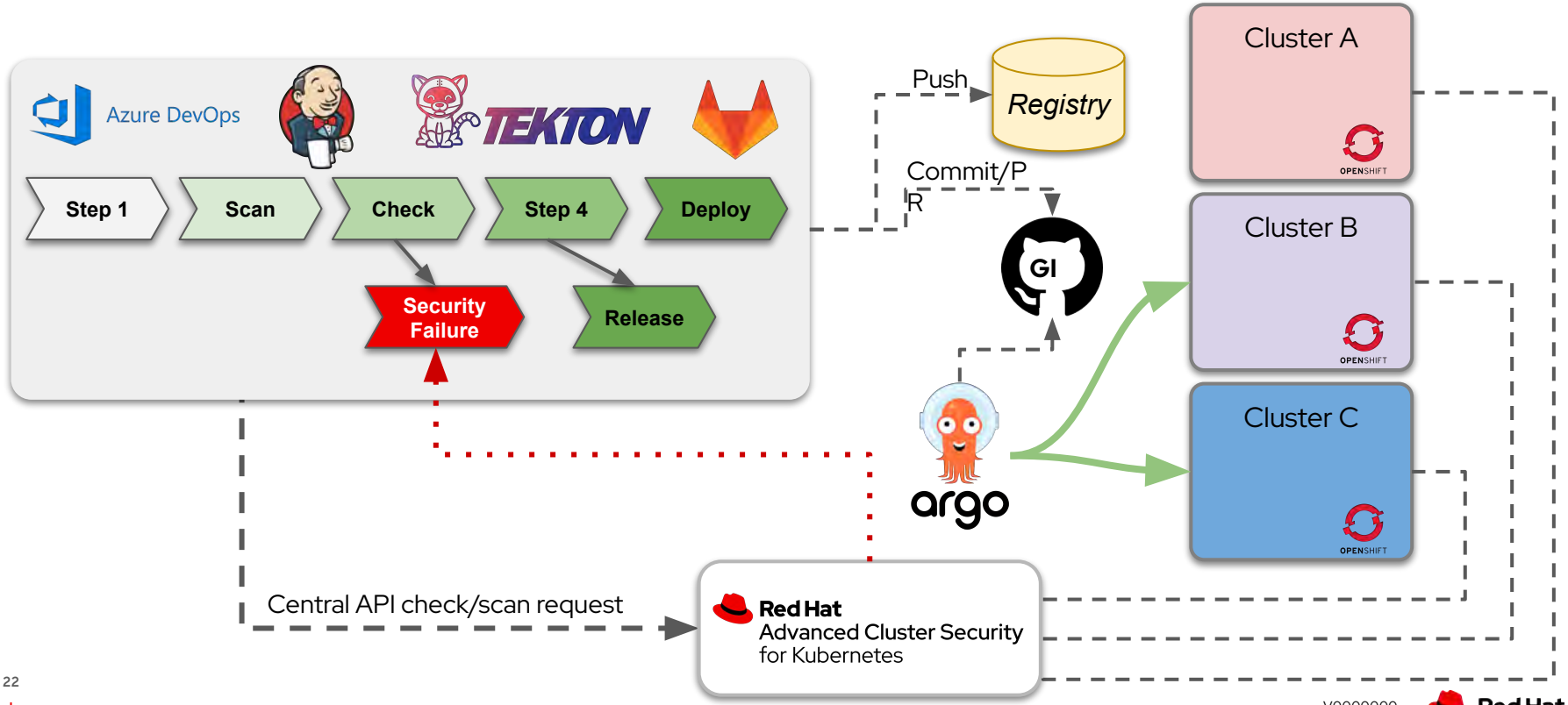


Shift Left Security Testing

Red Hat Advanced Cluster Security for Kubernetes supports integration with many different CI tools to implement a **shift left** approach where potential vulnerabilities and risk are scanned and identified a the beginning of the toolchain.

Thanks to this agnostic approach, RHACS can be integrated with **Azure DevOps**, **Tekton**, **Jenkins, CircleCI**, **GigLab**, **GitHub**, **Google Function**, and many other CI solutions.

Shift Left + GitOps



https://github.com/stackrox/contributions.git

Thank you


linkedin.com/company/red-hat


youtube.com/user/RedHatVideos


facebook.com/redhatinc


twitter.com/RedHat

Gabriele Torregrossa
DevOps Engineer
Par-Tec

#CloudDevSecOps

Red Hat | par-tec

Advanced Cluster Security: come si mette davvero al sicuro il cloud

RED HAT ADVANCED CLUSTER SECURITY

LA SOLUZIONE ALLE SFIDE DI SICUREZZA NEL DEVSECOPS

Gabriele Torregrossa
DevOps Engineer

par-tec

Gabriele Torregrossa

DevOps Engineer

COSA FACCIO

- DevOps
- DevSecOps
- Software Development
- Cloud O&M

Le mie certificazioni

- Red Hat Delivery Specialist - Container Platform Deployment
- Red Hat Sales Engineer Specialist - Container Platform
- Red Hat Sales Specialist - Hybrid Cloud Infrastructure
- Dynatrace Associate

par-tec

CHI SIAMO

Agendo come system integrator, Par-Tec supporta le aziende italiane nella realizzazione di servizi digitali moderni, efficienti e sicuri mediante la fornitura di soluzioni, servizi professionali e formazione di altissima qualità.

Infrastruttura IT, cloud enablement, applicazioni verticali per il mercato finanziario, industria 4.0, privacy compliance e formazione sono solo alcune delle aree governate dai nostri centri di competenza distribuiti tra Milano, Roma, Pistoia e Pomezia.

Il **Gruppo Par-Tec** è una realtà che comprende **oltre 200 professionisti** e include 4 aziende oltre alla capogruppo:

par-tec
beyond the IT domain

Swing, specializzata nella fornitura di servizi e consulenza IT in materia di conformità alle normative di Banca d'Italia per il mercato degli intermediari finanziari.

Fine Tuning - Consulenza Integrata, esperta nello sviluppo di applicazioni web-based e nell'integrazione di soluzioni di social & web intelligence e digital analytics.

Faberbee, una startup focalizzata nel R&D e nell'implementazione di soluzioni basate su Blockchain e Distributed Ledger Technology in diversi ambiti, quali il Contract Management.

Lightstreamer, che sviluppa l'omonimo prodotto per il real-time data push adottato con successo da importanti realtà in tutto il mondo.

OFFERTA

La nostra offerta è la sintesi di 20 anni di esperienza maturata nei settori telco e finance.

Il nostro approccio al mercato comprende quattro diverse modalità di delivery:

- Solution Delivery
- Professional Services
- Par-Tec Control Center
- On-premise Managed Services

TECHNOLOGY SOLUTIONS

- Cloud, DevOps e IT Automation
- Database
- System & Software Engineering
- IT Operations

FINANCIAL SERVICES SOLUTIONS

- Trading On-line
- Multichannel Banking
- Informativa Finanziaria
- Quality Assurance

INDUSTRIA 4.0

- Industrial IoT
- Messaging Protocols
- Blockchain
- Predictive Analytics

SECURITY

- Regulatory Compliance
- Identity Governance
- Infrastructure Security
- Information Security

ADVANCED & PREDICTIVE ANALYTICS

- AddToBuild

EDUCATIONAL

- E-learning
- Formazione in aula
- Blended learning

ALCUNI NOSTRI CLIENTI

IN ITALIA

ALL'ESTERO

RHACS INSIGHTS

- Gestione della conformità in base agli standard del settore
- Valutazione dei rischi per la sicurezza
- Gestione delle politiche di rete e delle vulnerabilità
- Risposta alle violazioni
- Gestione della salute del cluster
- Sistema centralizzato di ricerca
- Integrazione SSO
- Integrazione con sistemi di notificazione per gli allarmi e per i backup

CONFORMITÀ AGLI STANDARD DI SETTORE

- CIS Benchmarks
- HIPAA
- NIST Special Publication 800-53
- NIST Special Publication 800-190
- PCI DSS

- Valutare la conformità infrastrutturale
- Rafforzare il Docker Engine
- Rafforzare l'Orchestrator di Kubernetes
- Ottenere una visualizzazione dettagliata dello stato di conformità

par-tec

VALUTAZIONE DEI RISCHI PER LA SICUREZZA

- Valutazione del rischio per ambiente
- Classificazione dei rischi
- Dettaglio sulle vulnerabilità
- Configurazione dei rischi
- Gestione delle attività di runtime
- Indicatori del rischio

RHACS valuta i rischi all'interno del nostro ambiente classificandoli.

- È possibile creare politiche di sicurezza personalizzate
- Vengono fornite schede di indicatori del rischio
- Sezioni panoramiche
- Possiamo aggiungere **tag** di processo e **baseline**

par-tec

GESTIONE DELLE POLITICHE DI SICUREZZA

- Attività anomale
- Best pratice per DevOps
- Kubernetes
- Strumenti di rete
- Gestione dei pacchetti
- Privilegi
- Best practices di sicurezza
- Modifiche di sistema
- Gestione delle vulnerabilità

RHACS fornisce delle policy di sicurezza di base pronte all'uso.

È possibile definire criteri e policy da applicare ai nostri ambienti.

Le dashboard ci forniranno una panoramica completa dello stato dei rischi dell'infrastruttura.

par-tec

GESTIONE DELLE POLITICHE DI RETE

- Network graph
- Network policy simulator
- Network policy generator

RHACS semplifica questa gestione, attraverso tre componenti:

Il **Network graph**, che fornisce visibilità e controllo sulle connessioni consentite;

Il **Network policy simulator**, per verificare eventuali effetti collaterali nell'applicazione di nuove politiche;

Il **Network policy generator**, per applicare policy specifiche basate sull' analisi dei flussi in ingresso.

par-tec

GESTIONE DELLE VULNERABILITÀ

- Images
- Clusters
- Namespaces
- Deployments
- Components
- CVEs
- Policies

RHACS fornisce strumenti per identificare, visualizzare e gestire le vulnerabilità.

Ci vengono fornite inoltre delle **Top List** tra cui: le **politiche violate più frequentemente** e i **componenti più a rischio**.

Un componente molto importante è la scheda **Dockerfile**, che mostra tutti i livelli di rischio all'interno di ciascun layer.

par-tec

RISPOSTA ALLA VIOLAZIONI

- CVEs
- DevOps best practice
- Build ad alto rischio
- Deployment pratices
- Comportamenti sospetti in fase di esecuzione
- Default out of the box security policies
- Policies customization

Le policy integrate e personalizzate di **RHACS** monitorano componenti e comportamenti all'interno del nostro ambiente

RHACS notifica quando avviene una violazione di una policy

È possibile analizzare tutte le violazioni all'interno di una vista

Si possono utilizzare **commenti** e **tag**

SISTEMA CENTRALIZZATO DI RICERCA

- Ricerca globale
- Ricerca con auto completamento
- Ricerche avanzate
- Ricerca categorizzata
- Paginazione delle ricerche

RHACS ha un sistema di ricerca e filtraggio centralizzato.

La ricerca è basata su coppie di parametri:

- **attributo**, che Identifica il tipo di risorsa da cercare
- **termine di ricerca**, che trova la risorsa corrispondente

Ad esempio **namespace: web-server**

par-tec

INTEGRAZIONE CON SSO

- Okta Identity Cloud
- Google Workspace
- Gestione RBAC
- Autenticazione PKI

RHACS può essere integrato con diversi identity provider basati su **SAML 2.0**, **OAuth 2.0** e **OIDC** o tramite **PKI**.

Il controllo degli accessi è basato sui ruoli (**RBAC**) basati sui permessi.

I permessi predefiniti includono:

- **Administrator**: accesso completo
- **Analyst**: accesso in lettura
- **Continuous Integration**: accesso machine-to-machine per la CI

È possibile creare dei ruoli associando i permessi a delle risorse specifiche (e.g. ruolo "**Analyst per il namespace web-server**")

GESTIONE DELLA SALUTE DEL CLUSTER

- Salute del cluster
- Definizione delle vulnerabilità
- Images integrate
- Sistemi di notifica integrati
- Backup integrati
- Salute dei componenti

RHACS fornisce una Dashboard con le informazioni relative allo stato del Cluster.

A ciascun componente viene assegnato un attributo qualitativo che ne definisce lo stato, nello specifico:

Healthy > Degraded > Unhealthy > Uninitialized

Vengono fornite metriche su: **lo stato dei servizi**, **i sensori**, **i rischi di vulnerabilità** e **l'integrazione con i servizi esterni**.

par-tec

INTEGRAZIONE PER ALLARMI E BACKUP

- Slack
- Webhooks
- PagerDuty
- Sumo Logic
- Syslog
- Google Cloud SCC
- Splunk
- Jira
- Email

È possibile integrare **RHACS** con piattaforme e software per la gestione di backup e segnalazione degli errori.

Può essere utilizzato anche in processi di Continuous Integration (CI), per gestire backup su Google Cloud Storage o Amazon S3.

Si integra con vari scanner di terze parti per il controllo delle vulnerabilità

par-tec

GRAZIE PER L'ATTENZIONE

 www.par-tec.it

 info@par-tec.it

 Milano: +39 02 667321

 Roma: +39 06 98269600

par-tec

Q&A

Eleonora Peruch
Solution Architect
Red Hat

Gabriele Torregrossa
DevOps Engineer
Par-Tec

Francesco Pignatelli
Giornalista
G11 Media

Red Hat | par-tec

undici media