Red Hat Summit

Connect

RED HAT ADVANCED CLUSTER SECURITY

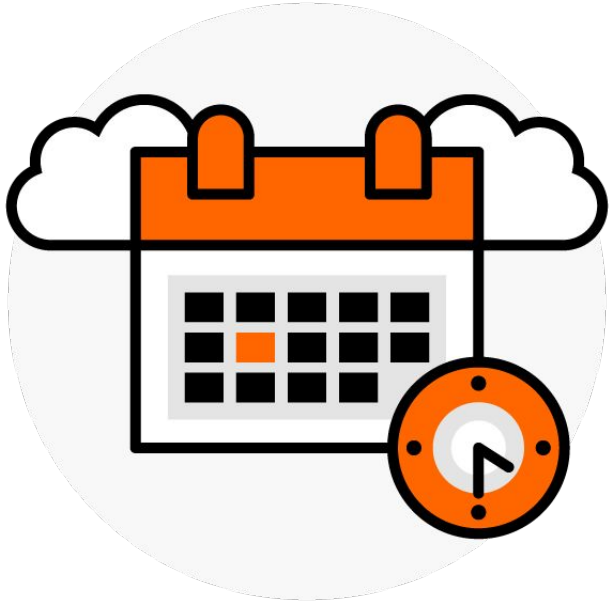
Gestire applicazioni cloud native in modo più sicuro

Gabriele Torregrossa
DevOps Engineer

par-tec

Red Hat | intel

Agenda



- Chi sono
- Concetto di sicurezza nel mondo Cloud
- Cos'è Red Hat Advanced Cluster Security (RHACS)
- RHACS Insights
- Thank you

Chi sono

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

Concetto di sicurezza nel mondo cloud

- Mantenere il passo con le vulnerabilità, i requisiti di conformità, gli strumenti e le modifiche architetturali delle tecnologie Cloud Native
- Riconsiderare la strategia di sicurezza tradizionale con rete perimetrale
- Estendere la sicurezza ad ogni livello dello stack dell'infrastruttura e dell'applicazione
- Attuare una difesa capillare, la cui efficacia sia legata ad una strategia di sicurezza su più livelli e che integra persone, processi e tecnologia

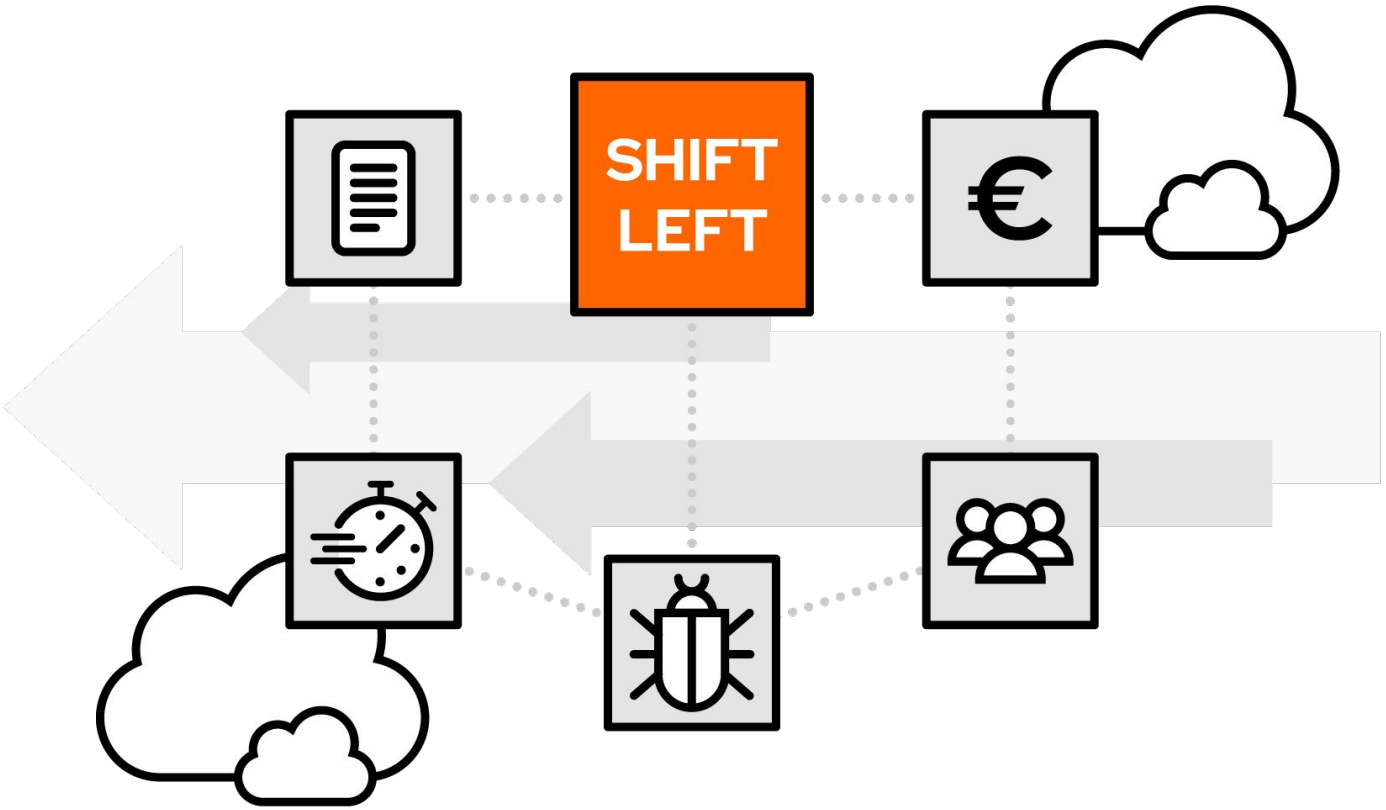
Cos'è Red Hat Advanced Cluster Security

- RHACS deriva da un'acquisizione Red Hat di StackRox
- Ha come obiettivo, la messa in sicurezza del ciclo dello sviluppo applicativo e dell' infrastruttura di esecuzione
- Monitora a livello infrastrutturale e applicativo le funzionalità native di Kubernetes
- Applica l'approccio di sicurezza "**zero trust execution**"
- RHACS è integrabile con ogni tipo di cluster Kubernetes

La storia del leone e della gazzella

Ogni giorno ...

Shift Left



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

Valutazione dei rischi per la sicurezza

- CIS Benchmarks
- HIPAA
- 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**

Gestione delle politiche di sicurezza

- Attività anomale
- Best pratices per DevOps
- Kubernetes
- Strumenti di rete
- Gestione dei pacchetti
- Privilegi
- Best practices di sicurezza
- 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

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

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**

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

Risposta alla violazioni

- CVEs
- DevOps best practices
- 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**

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**

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

Quindi, cos'è Red Hat Advanced Cluster Security?

Red Hat Summit

Connect

Thank you


linkedin.com/company/red-hat


facebook.com/redhatinc


youtube.com/user/RedHatVideos


twitter.com/RedHat

par-tec

Red Hat | intel