Automatisation de la sécurité

Maintenir l'ordre dans vos applications

Martin Sauvé
Architecte principal
msauve@redhat.com

“Depuis plus de 20 ans, la sécurité n’est considérée qu’à la toute fin du cycle de livraison”

Anonyme

Comment la sécurité est perçue par les DEVS et OPS ?

POURQUOI DevSecOps ?

- Les “puristes” de DevOps disent que la sécurité a toujours été intégrée à DevOps
- Avez-vous lu le livre ? La sécurité est au coeur de DevOps
- Pour les professionnels de DevOps: il faut automatiser et continuellement intégrer la sécurité dans le cycle de vie des applications

Red Hat

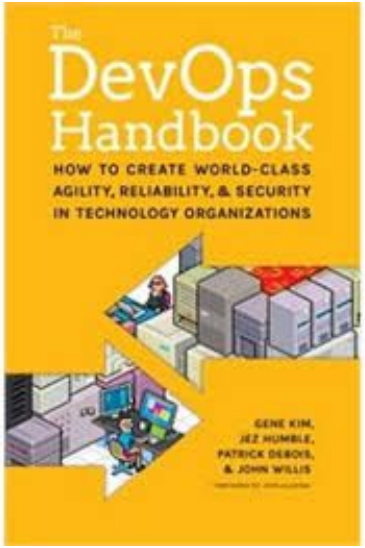
Source: IT Revolution, DevOps Enterprise abstract word cloud, 2014

Source: IT Revolution, DevOps Enterprise abstract word cloud, 2014

Source: IT Revolution, DevOps Enterprise abstract word cloud, 2014

Et qu’est-ce qui a changé ?

”Shift-left” ?



Red Hat

En demi-teinte....

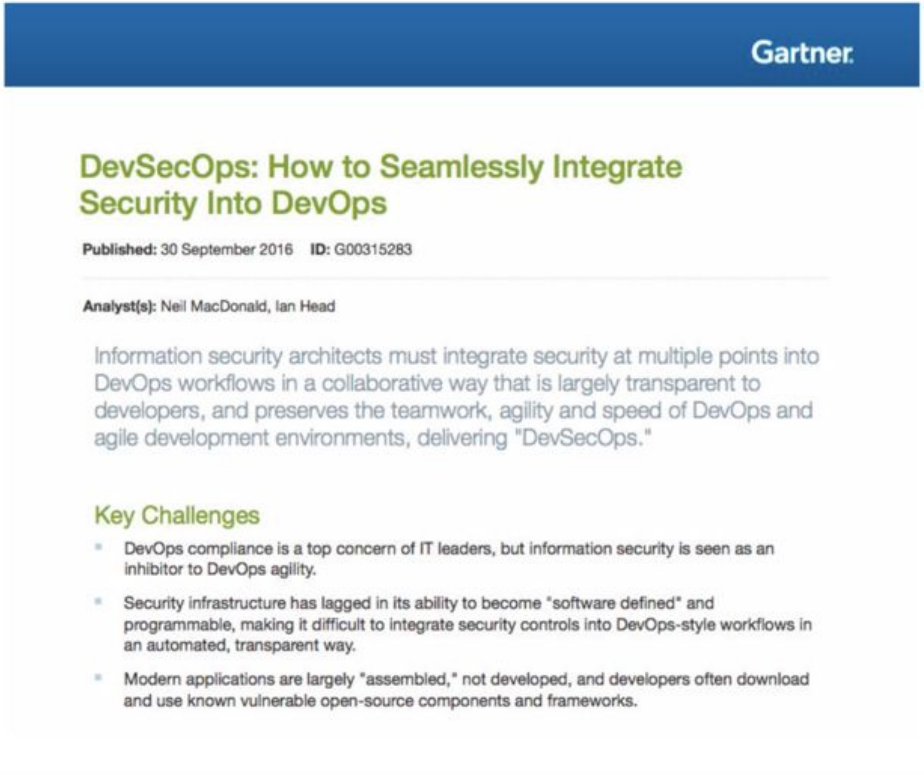
«Nous estimons que moins de 20% des architectes de sécurité ont adhéré à leurs initiatives DevOps pour intégrer de manière active et systématique la sécurité de l'information dans leurs initiatives DevOps; et encore moins ont atteint le degré élevé d'automatisation de la sécurité requis pour devenir DevSecOps.»

«D'ici 2019, plus de 70% des initiatives DevOps d'entreprise auront incorporé une analyse automatisée des vulnérabilités de sécurité et de la configuration des composants open source et des packages commerciaux, contre moins de 10% en 2016.»

DevSecOps: How to Seemlessly Integrate Security Into DevOps, Gartner Inc. September 2016

Red Hat

La sécurité - un obstacle à DevOps



Gartner

DevSecOps: How to Seamlessly Integrate Security Into DevOps

Published: 30 September 2016 **ID:** G00315283

Analyst(s): Neil MacDonald, Ian Head

Information security architects must integrate security at multiple points into DevOps workflows in a collaborative way that is largely transparent to developers, and preserves the teamwork, agility and speed of DevOps and agile development environments, delivering "DevSecOps."

Key Challenges

- DevOps compliance is a top concern of IT leaders, but information security is seen as an inhibitor to DevOps agility.
- Security infrastructure has lagged in its ability to become "software defined" and programmable, making it difficult to integrate security controls into DevOps-style workflows in an automated, transparent way.
- Modern applications are largely "assembled," not developed, and developers often download and use known vulnerable open-source components and frameworks.

Défis:

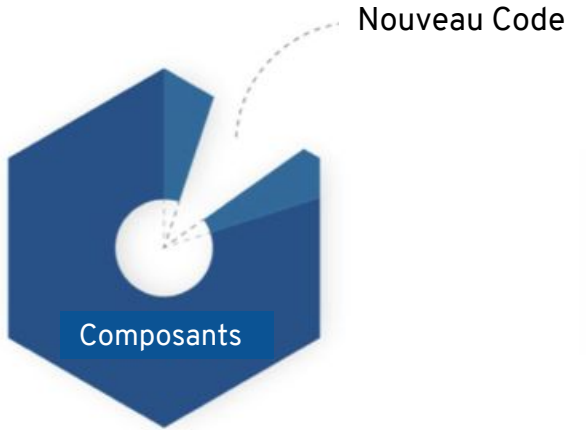
- L'infrastructure de sécurité a tardé à devenir «définie par le logiciel» et programmable, ce qui rend difficile l'intégration …
- Les applications modernes sont en grande partie «assemblées» et non développées, et les développeurs téléchargent et utilisent souvent des composants et des outils Open Source avec vulnérabilités connues.

Red Hat

Les applications sont “assemblées”

... en utilisant des milliards de librairies, cadres et utilitaires disponibles

- Toutes ne sont pas créées égales, certaines sont en bonne santé et d'autres non.
- **Toutes tournent mal avec le temps, ils vieillissent comme le lait, pas comme le vin**
- Les données montrent que les entreprises ont consommé en moyenne 229 000 composants logiciels par an, dont 17 000 présentaient une vulnérabilité connue.



Red Hat

CHANGEMENTS DANS LES T.I.

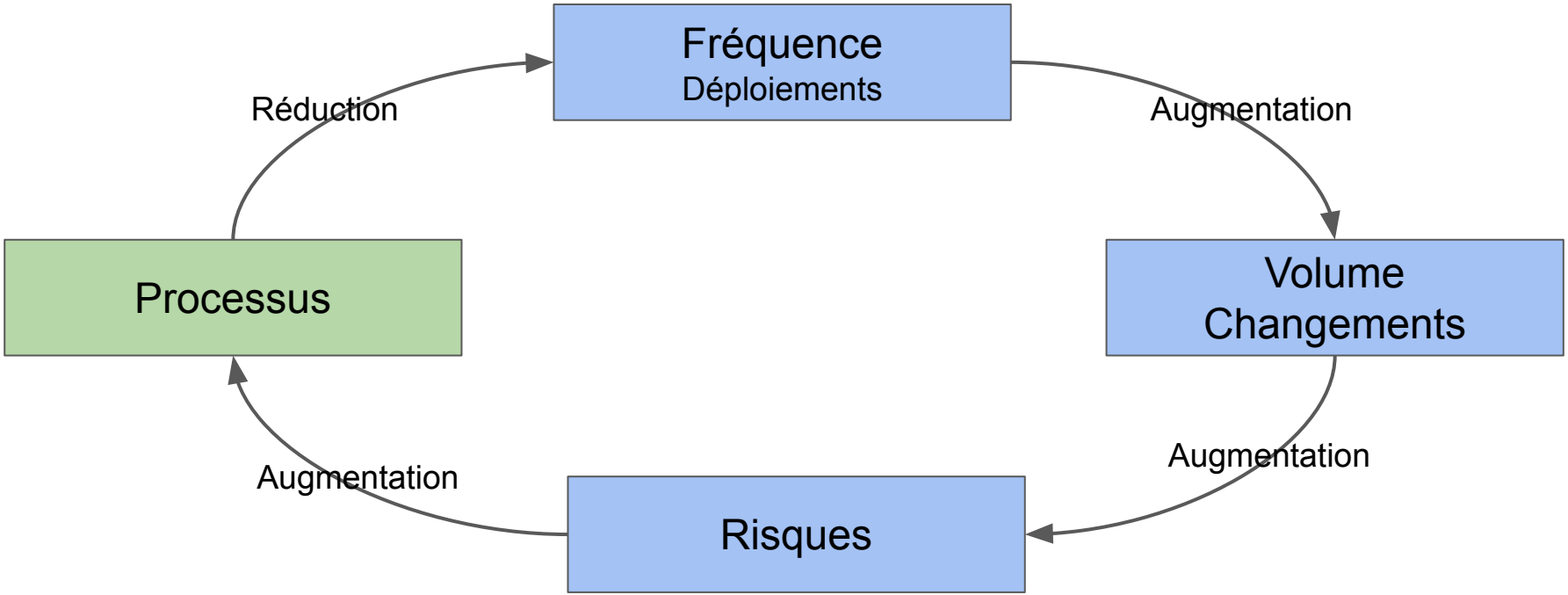
- Infonuagique
- DevOps
- Innovation du logiciel libre, explosion des outils et librairies
- Conteneurs
- Microservices
- Transformation Numérique
- Culture négligeant la sécurité

Red Hat

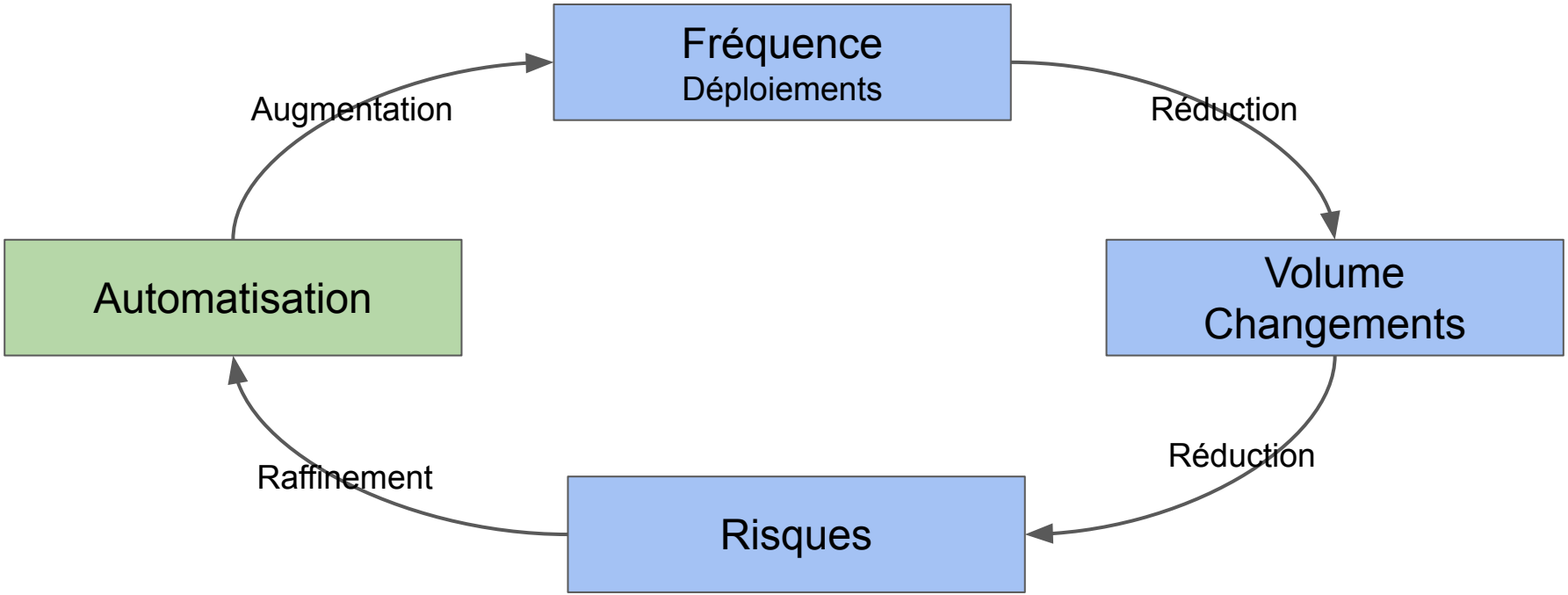
DevSecOps:

À la manière du logiciel libre

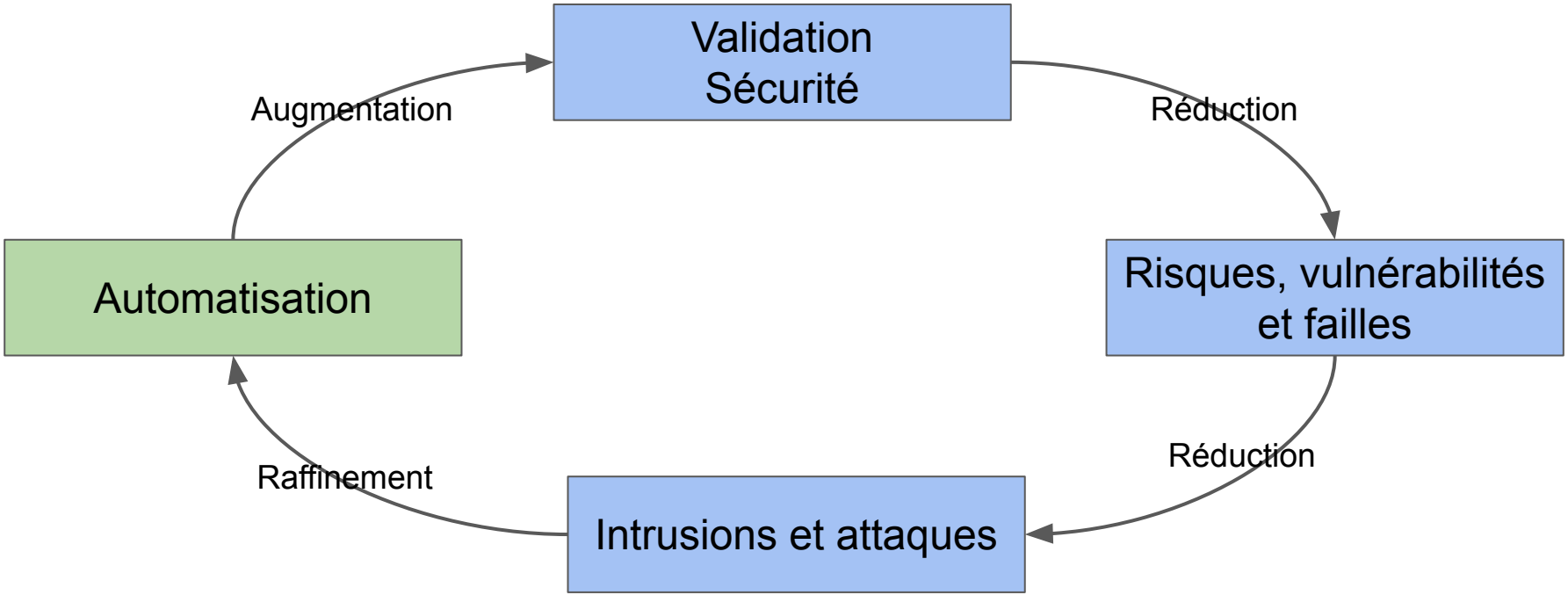
Approche Traditionnelle



Approche DevOps



Approche Dev(Sec)Ops



Gestion du risque par:

- ✓ Sécurité des actifs
- ✓ Sécurité des devs
- ✓ Sécurité des ops

Red Hat

Sécurité des actifs

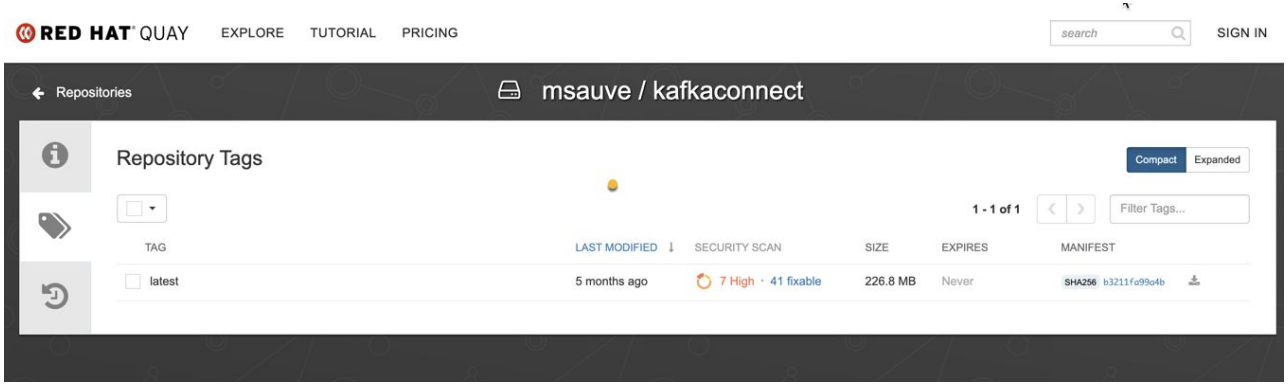
- Bâtir le code
  - Chaîne de déploiement
- Bâtir les actifs
  - Scripts, binaires, paquets (RPM), conteneurs, images...
  - Registres (conteneurs, services, applications)
  - Dépôts (librairies, hôtes)
  - Signer les actifs

Safe at Titan Missile Museum
https://upload.wikimedia.org/wikipedia/commons/5/59/Red_Safe%2C_Titan_Missile_Museum.jpg

Red Hat

Sécurité des actifs
Registre d'images

- Avez-vous besoin d'un registre privé ?
- Quelles métadonnées de sécurité sont disponible pour vos images ?
- Est-ce que les images sont mise-à-jour fréquemment dans votre registre ?
- Est-ce qu'il y a un contrôle des accès sur votre registre ? Qui peut pousser des images ?



Red Hat

Sécurité des actifs

SANTÉ - Indicateur de mise-à-jour

- Niveau de “fraîcheur” pour la sécurité des conteneurs.
- Surveiller le registre d'images pour mettre à jour automatiquement les images affectées
- Utilisez des politiques pour gérer ce qui peut être déployé: par exemple, si une image est inférieure à un certain degré de fraîcheur.

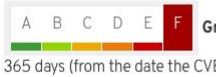
Grade A: This image has no missing Critical or Important security errata. It may be missing errata that fix Moderate or Low security flaws.

Grade B: This image may be missing Critical or Important security errata, but no missing Critical flaw is older than 7 days and no missing Important flaw is older than 30 days (from the date the CVE was first fixed in an erratum). It may be missing errata that fix Moderate or Low security flaws, of any age.

Grade C: This image may be missing Critical or Important security errata, but no missing Critical flaw is older than 30 days and no missing Important flaw is older than 90 days (from the date the CVE was first fixed in an erratum). It may be missing errata that fix Moderate or Low security flaws, of any age.

Grade D: This image may be missing Critical or Important security errata, but no missing Critical flaw is older than 90 days and no missing Important flaw is older than 365 days (from the date the CVE was first fixed in an erratum). It may be missing errata that fix Moderate or Low security flaws, of any age.

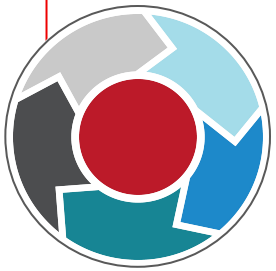
Grade E: This image may be missing Critical or Important security errata, but no missing Critical or Important flaw is older than 365 days (from the date the CVE was first fixed in an erratum). It may be missing errata that fix Moderate or Low security flaws, of any age.



Grade F: This image may be missing Critical or Important security errata, and they are older than 365 days (from the date the CVE was first fixed in an erratum). It may be missing errata that fix Moderate or Low security flaws, of any age. Or the container is out of its lifecycle.

Grade Unknown: This image cannot be scanned as it is missing metadata required to perform the freshness grade calculation.

Red Hat



Chaîne d’approvisionnement sécurisée Red Hat

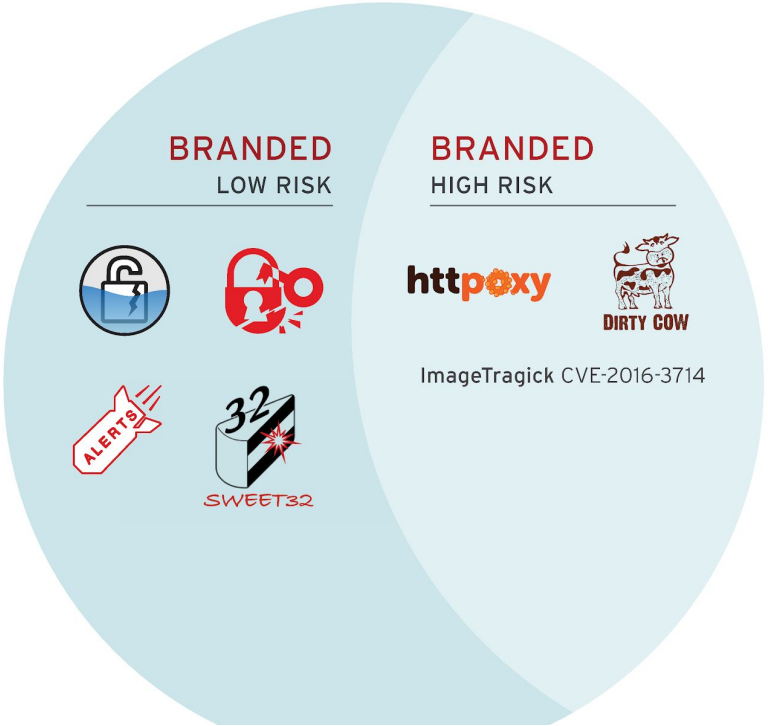
- Leadership dans les communautés
- Sélection des paquetages
- Inspection manuelle
- Inspection automatisée
- Directive pour les déploiements
- Source fiable

- Assurance qualité
- Certifications
- Signature
- Distribution
- Support
- Mise-à-jour et correctifs de sécurité

Red Hat

Red Hat: Gestion de la sécurité

Évaluation globale des risques, indépendamment du marketing



NOT BRANDED
HIGH RISK

- Kernel keychain overflow CVE-2016-0728
- glibc overflow CVE-2015-7547
- Samba DCE/RPC CVE-2015-5370
- Overcloud image password CVE-2016-4474
- JGroups auth bypass CVE-2016-2141
- Kernel challenge ack CVE-2016-5696
- BIND DoS CVE-2016-2776+

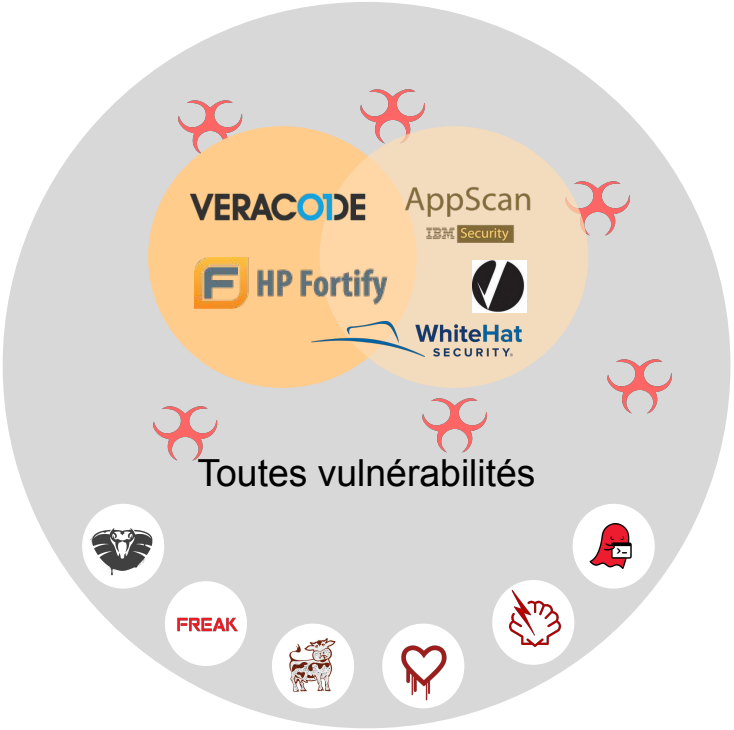
Red Hat

Sécurité du processus de développement

- Plusieurs déploiement en parallèle
- Code Source
  - Quel est la provenance?
  - De qui provient-il?
- Chaîne d'approvisionnement
  - Outils CI (e.g. Jenkins, Tekton)
  - Outils de tests
  - Outils de balayage (e.g. Black Duck, Sonatype)

Chaîne d'assemblage Boeing
https://upload.wikimedia.org/wikipedia/commons/c/c8/At_Boeing%27s_Everett_factory_near_Seattle_%289130160595%29.jpg

Le balayage des vulnérabilités en complément du SAST/DAST



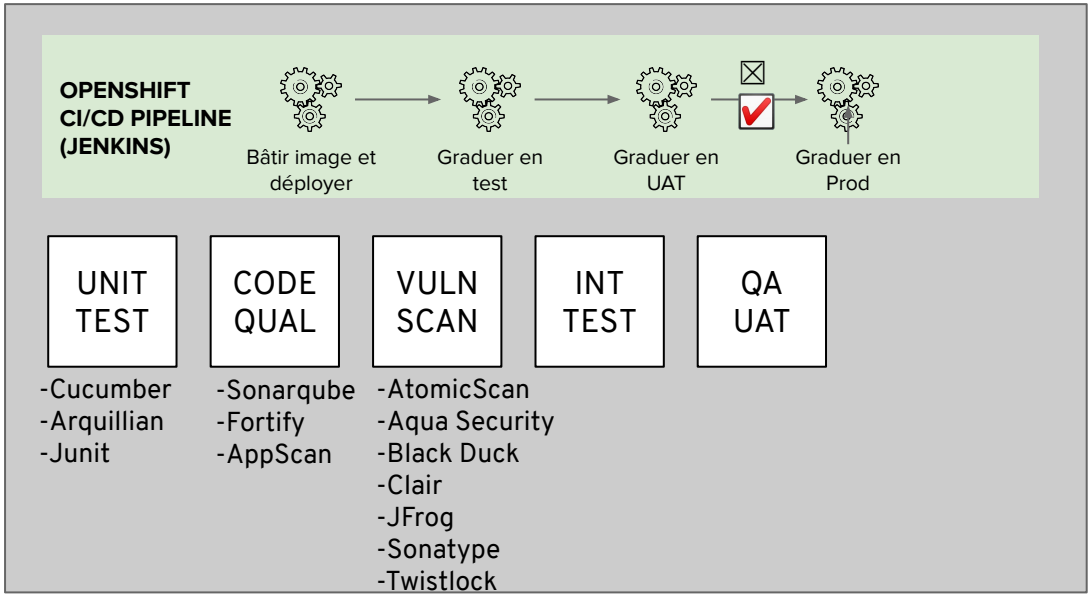
Analyse statique et dynamique
- Découverte des fautes de sécurités communes
- Focus sur votre code, pas l'upstream

Balayage des vulnérabilités
- Identification des dépendance vulnérables
- 3000+ divulgations en 2015
- 4000+ divulgations en 2016

Red Hat

Sécurité du processus de développement

- Intégration des tests de sécurité dans vos processus de CI et CD
- Utilisation de politiques automatisées pour signaler les builds avec problèmes



Red Hat

CODEREADY WORKSPACES

Une solution de développement collaborative native en conteneur qui s'exécute sous OpenShift sur site ou dans le cloud. Basé sur Eclipse Che

Espace de travail en conteneurs

Replicas standardisés des espaces de travail, pas de ‘ça fonctionnait sur mon poste”. Permet la collaboration et le travail en équipe

Intégrations DevOps

Référencez les espaces de travail du développeur pour tout problème, échec de la construction ou notification Git.

Protéger le code source

Accès complet au code source sans copie sur des ordinateurs portables difficiles à sécuriser.

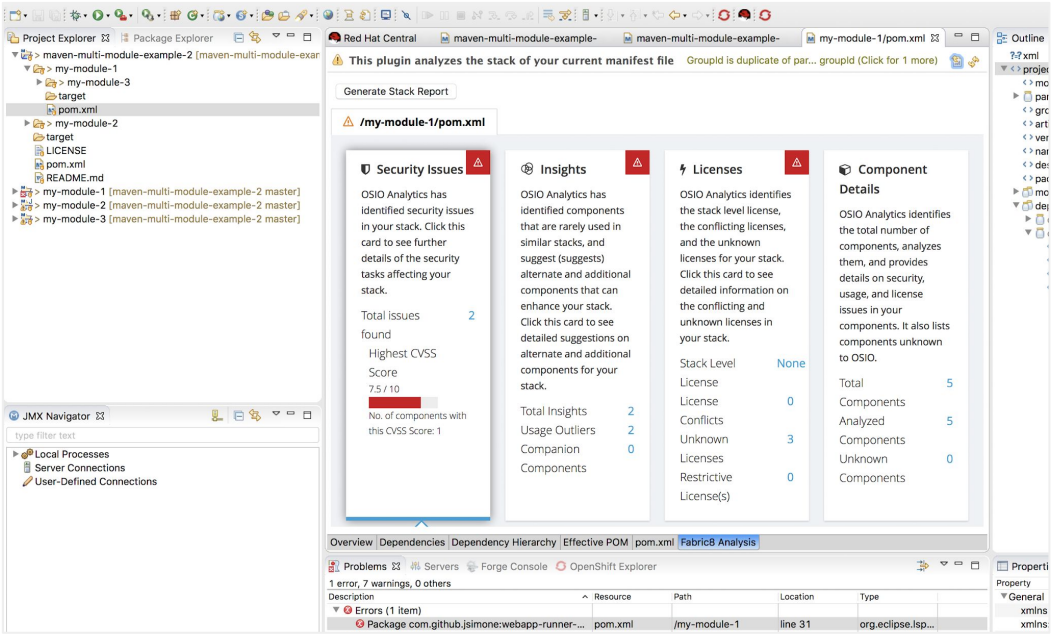
Sécurité intégrée: OpenShift et Red Hat Linux, avec des conteneurs de développement utilisant Red Hat Linux sécurisé.

Red Hat

Code Source - Analyse des dépendances

Le service d'analyse des dépendances fournit des avertissements de sécurité et de licence pour toutes les dépendances d'un projet, aidant ainsi les développeurs à résoudre les problèmes plus tôt dans le cycle.

- Découvre les CVEs dans tous les paquetages
- Découvre erreur de licence
- Supporté pour Java et Node
- Aide les développeurs à identifier les problèmes critiques tôt dans le cycle



Red Hat

Sécurité des opérations

Déploiement

- Registres de confiance
- Signature pour authentifier et authoriser les images
- Balayage d'images
- Politiques
- Évaluation en cours avec correctifs automatisés

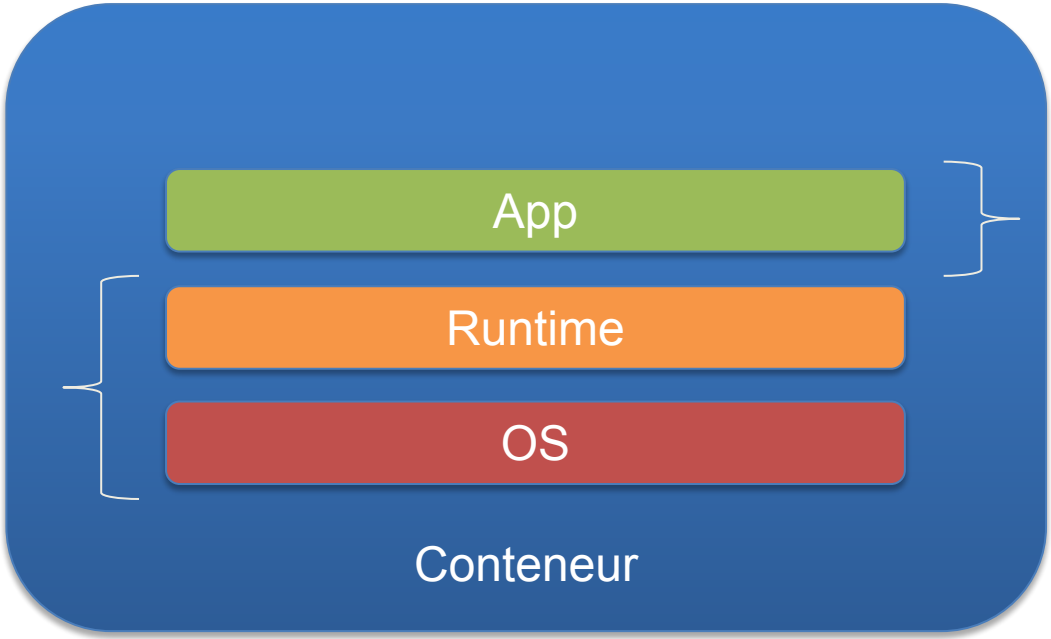
Mission Control - Apollo 13
https://c1.staticflickr.com/4/3717/9460197822_9f6ab3f30c_b.jpg

Red Hat

Balayage des vulnérabilités - Clair

Red Hat

Conteneur: plusieurs couches

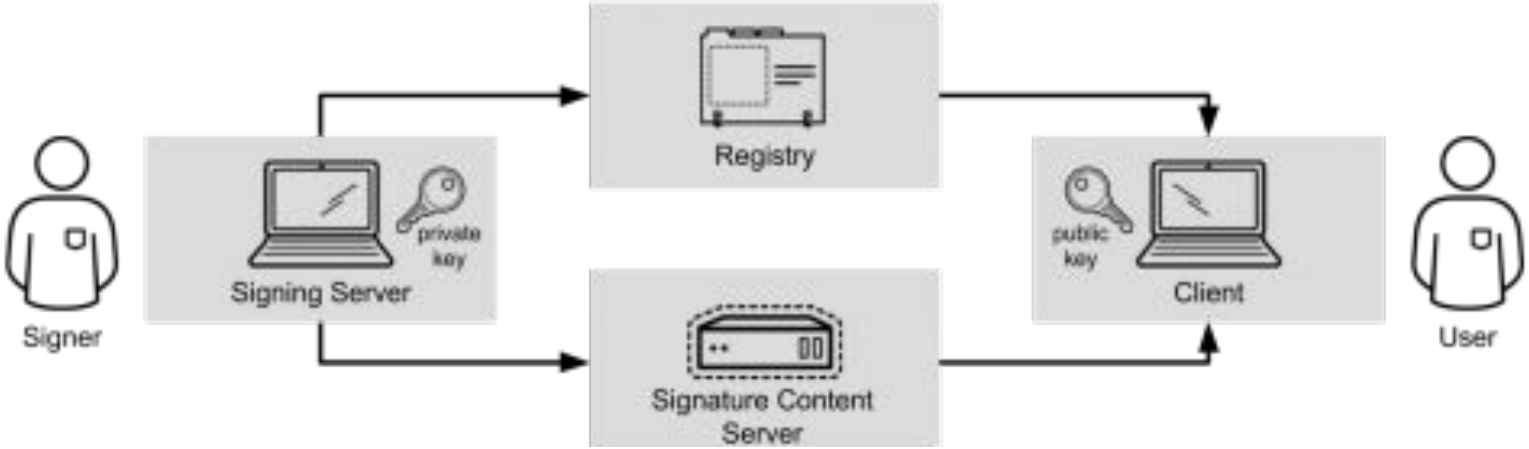


RED HAT QUAY

clair

Red Hat

Signature d’images



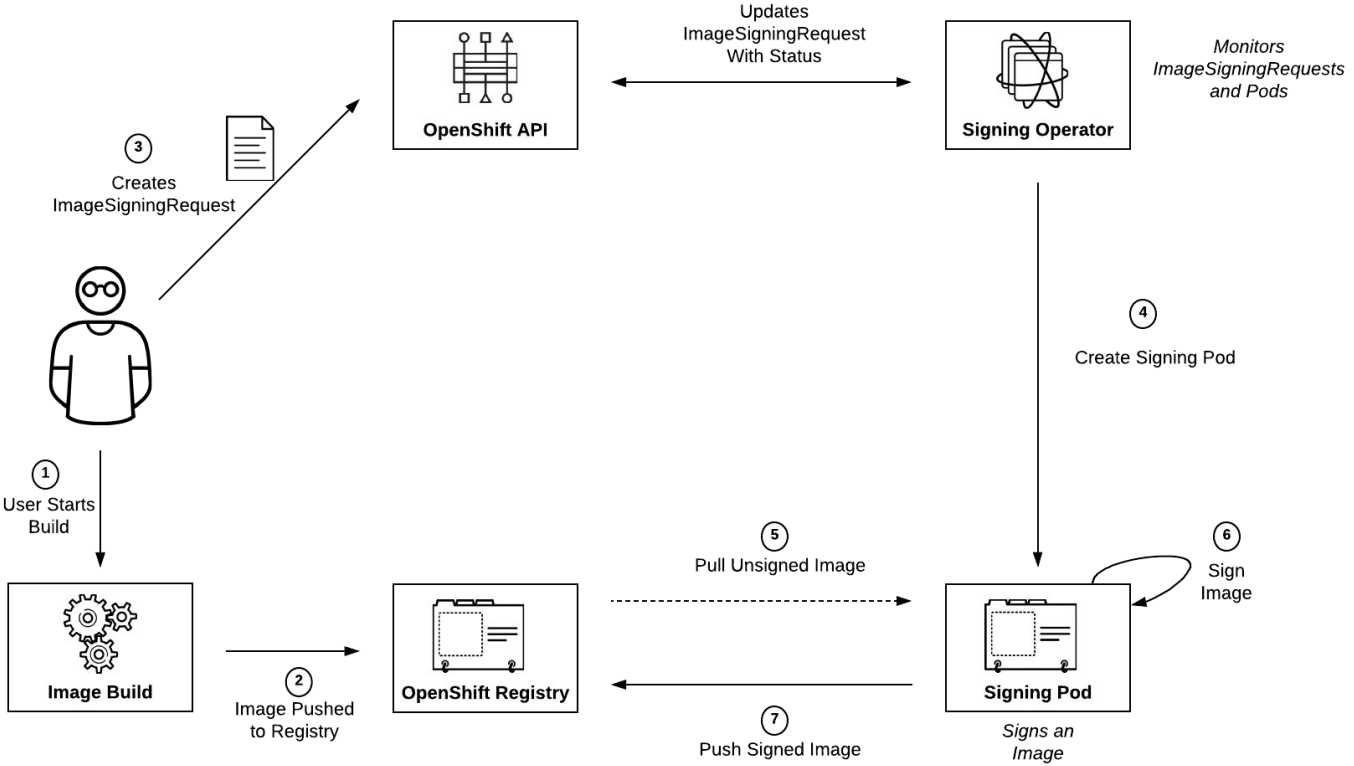
Vérification de la source de l’image

Indépendant du registre

Support de plusieurs signatures

Appliquer des politiques de signatures au niveau du nœud via une politique

Example: Signature d'Images



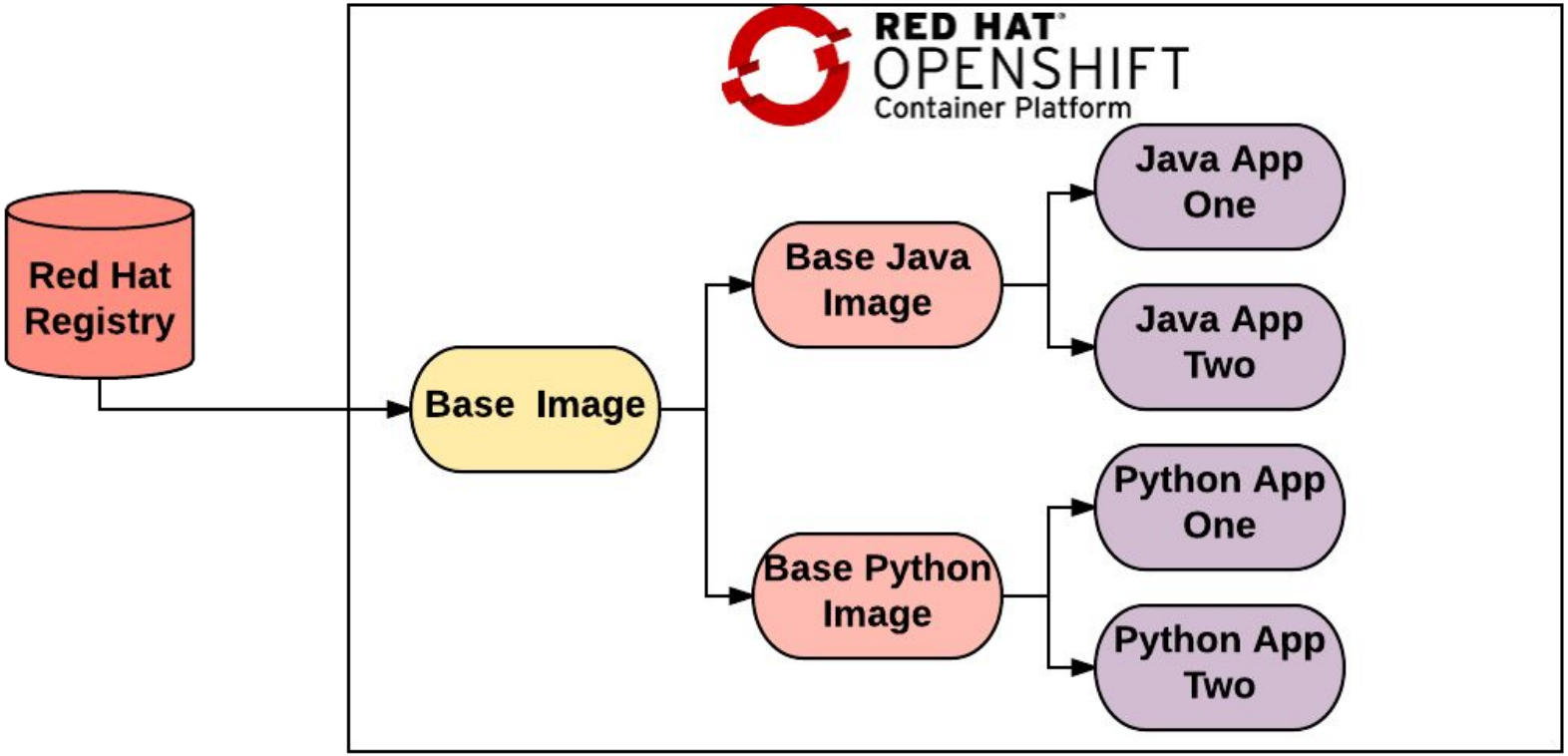
Red Hat

CUSTOM RESOURCE DEFINITIONS

Les “Custom Resource Definitions (CRD’s)” permettent aux utilisateurs d’étendre les capacités OpenShift et de définir leurs propres ressources

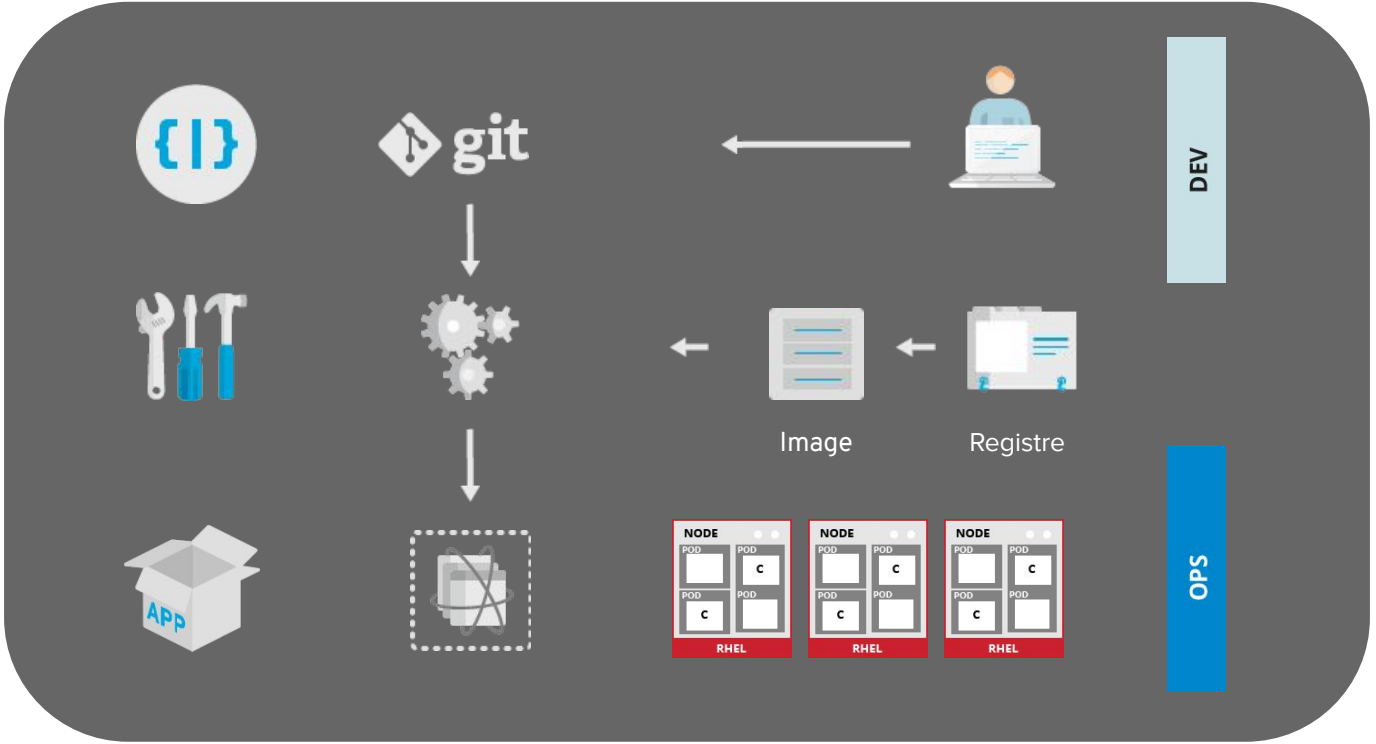
L'opérateur de signature d'image surveille les ressources ImageSigningRequest et prend action en fonction de l'état défini

Construction en cascade



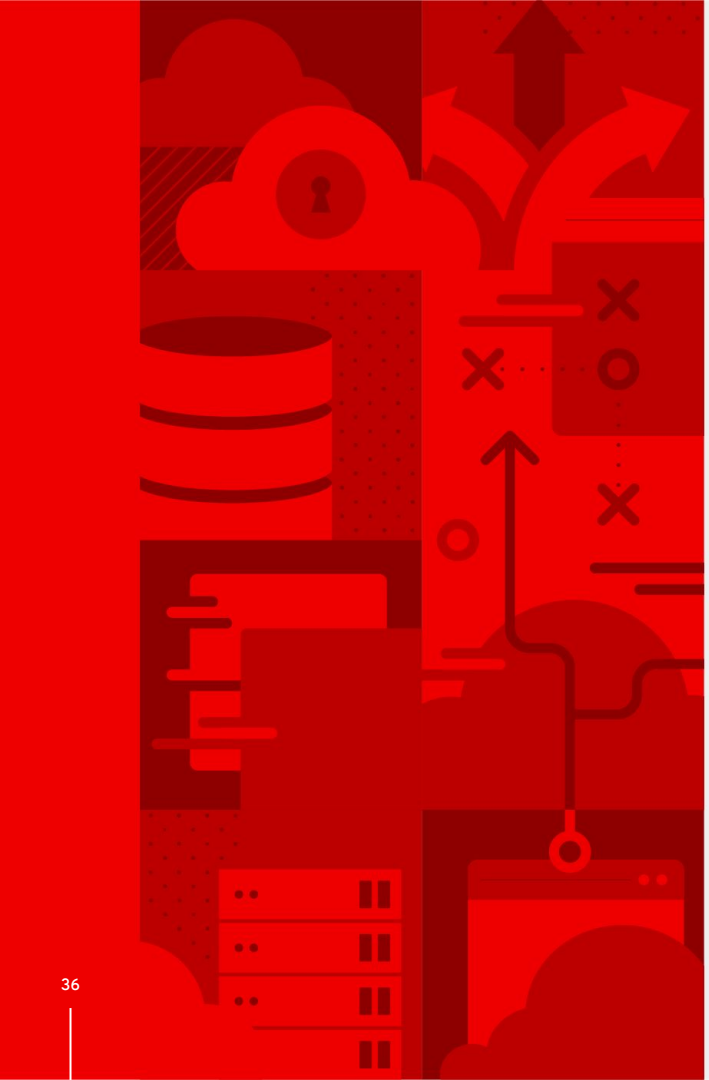
Sécurité en continue

Continuous Integration / Continuous Deployment / Continuous Security



La sécurité est en fonction du temps: reconstruisez et redéployez au besoin

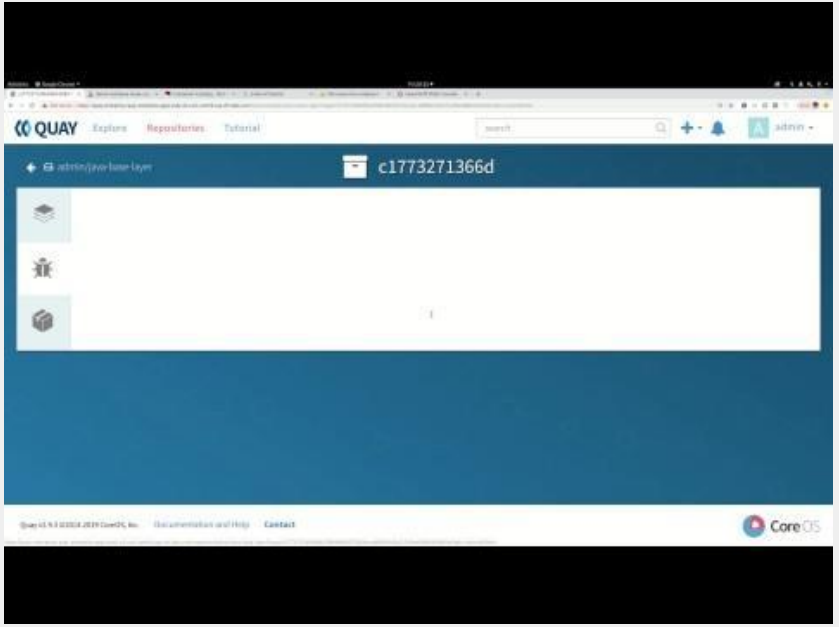
Red Hat



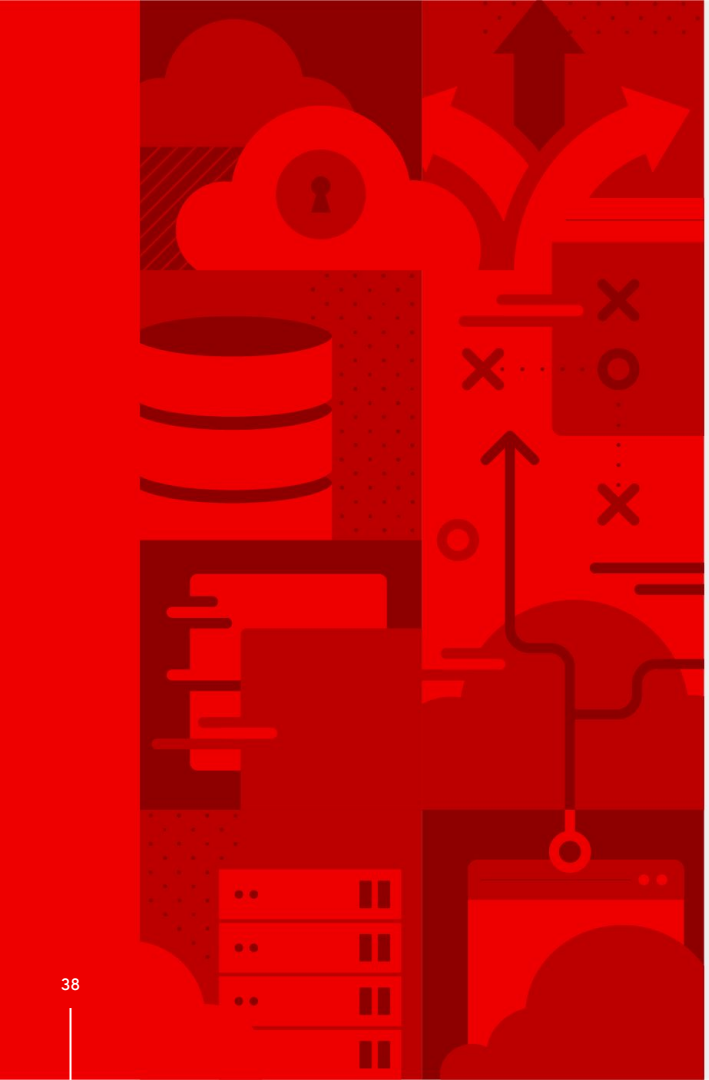
Demo

Red Hat

Demo


QUAY
Explore
Repositories
Tutorial
admin
c1773271366d
CoreOS

Red Hat



Questions

Red Hat

Merci!