



Automatisation de la sécurité

Maintenir l'ordre dans vos applications

Martin Sauvé
Architecte principal
msauve@redhat.com

BE SOCIAL #SECURITYSYMPOSIUM



“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



Et qu'est-ce qui a changé ?

”Shift-left” ?

PART VI—THE TECHNICAL PRACTICES OF INTEGRATING INFORMATION SECURITY, CHANGE MANAGEMENT, AND COMPLIANCE

Part VI Introduction

22 Information Security as Everyone’s Job, Every Day **23** Protecting the Deployment Pipeline and Integrating into Change Management and Other Security and Compliance Controls Conclusion to the DevOps Handbook: *A Call to Action*

Additional Material

Appendices Additional Resources Endnotes Index Acknowledgments Author Biographies



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.»

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.

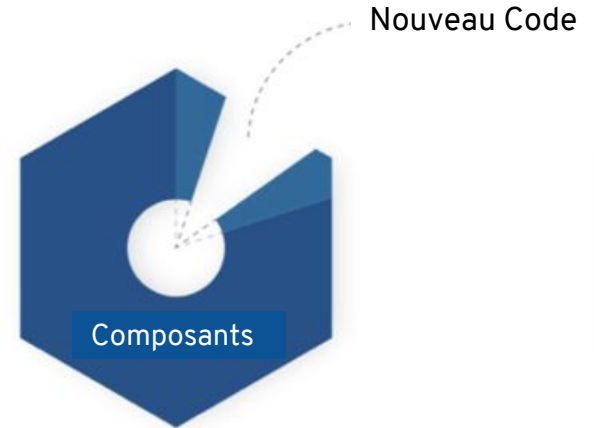
Défis:

- 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.

Les applications sont “assemblées”

... en utilisant des milliards de bibliothèques, 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.



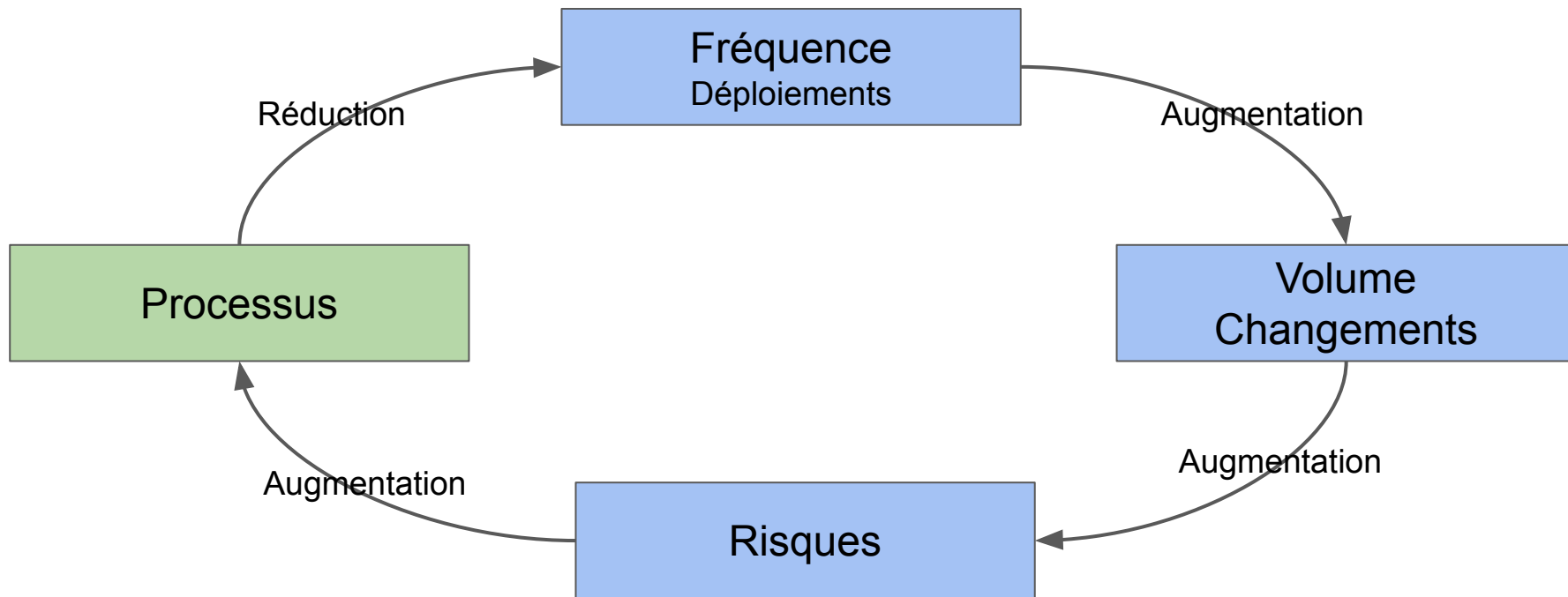
CHANGEMENTS DANS LES T.I.

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

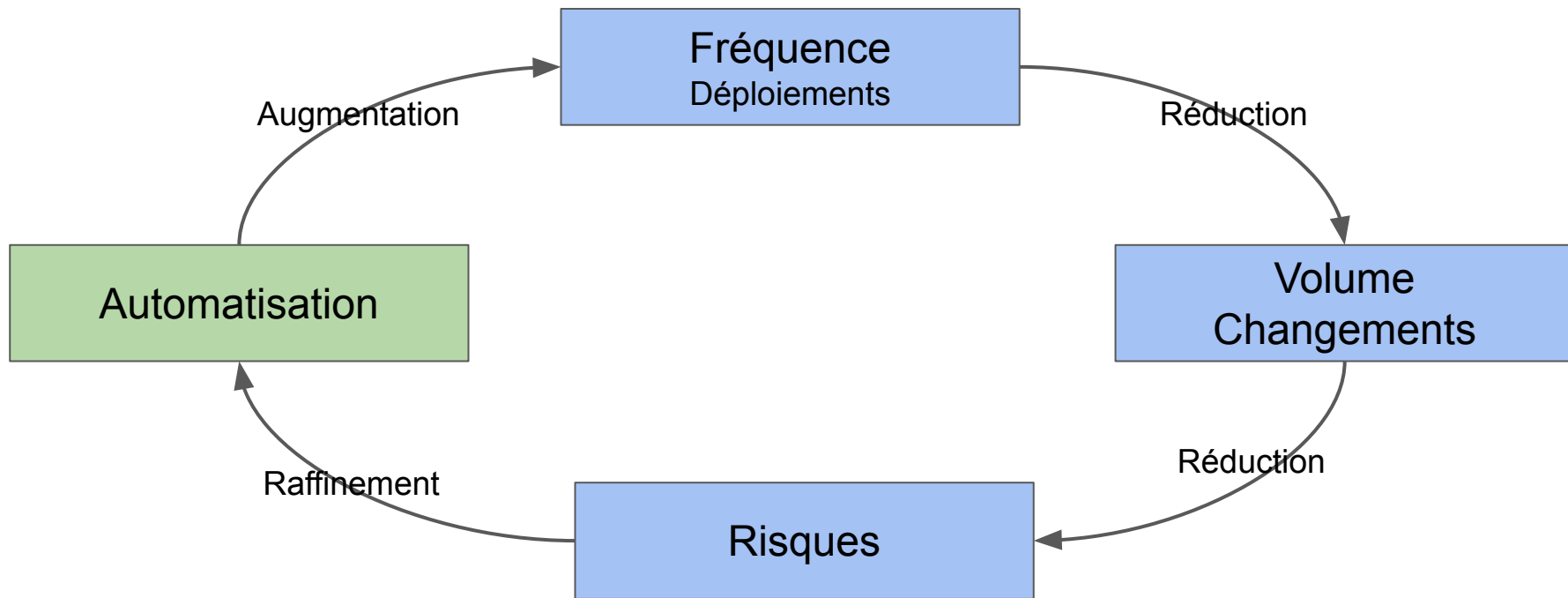


DevSecOps: À la manière du logiciel libre

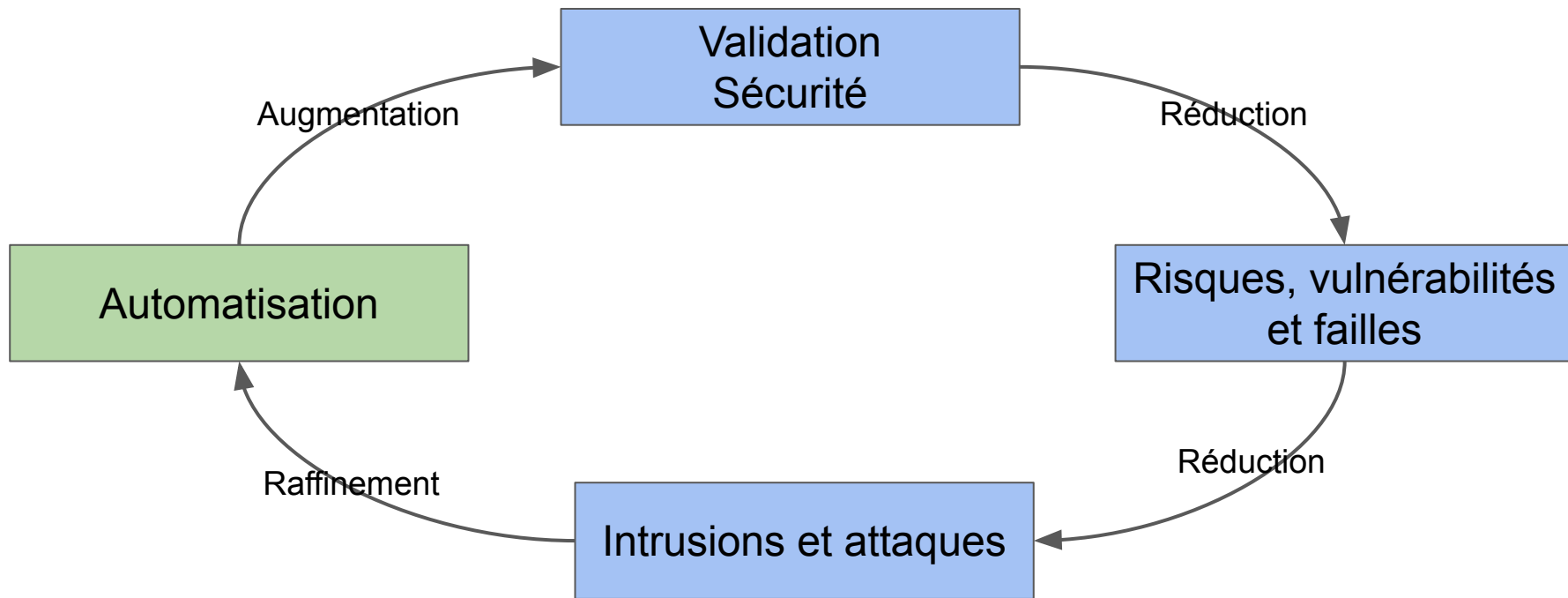
Approche Traditionnelle



Approche DevOps



Approche Dev(Sec)Ops



Gestion du risque par:



Sécurité des actifs



Sécurité des devs



Sécurité des ops

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



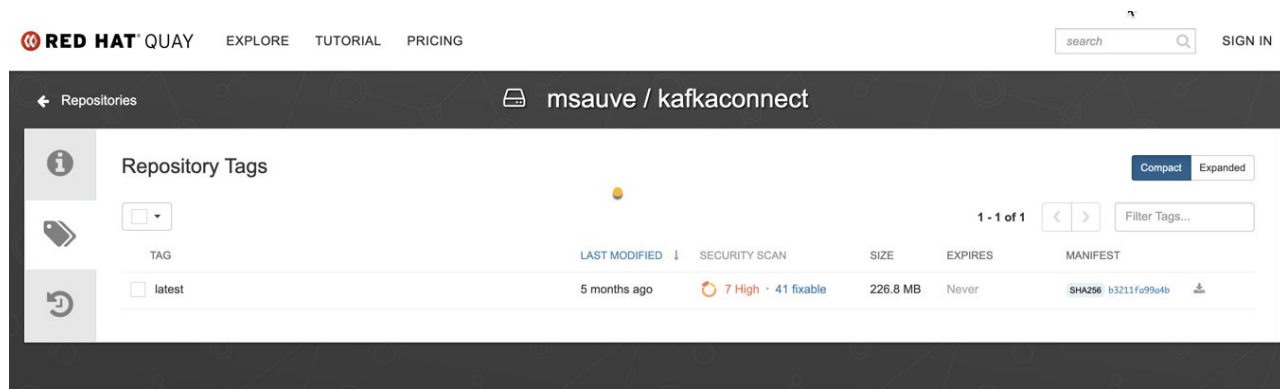
Safe at Titan Missile Museum

https://upload.wikimedia.org/wikipedia/commons/5/59/Red_Safe%2C_Titan_Missile_Museum.jpg

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 ?



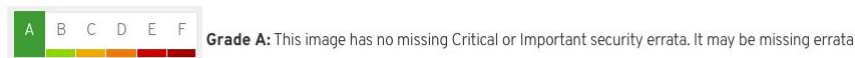
The screenshot displays the Red Hat Quay web interface. At the top, the navigation bar includes the Red Hat Quay logo, links for 'EXPLORE', 'TUTORIAL', and 'PRICING', a search bar, and a 'SIGN IN' button. The main content area is titled 'Repositories' and shows the path 'msauve / kafkaconnect'. Below this, there is a 'Repository Tags' section with a 'Compact' button and a 'Filter Tags...' input field. A table lists the available tags, with one tag 'latest' visible. The table columns are TAG, LAST MODIFIED, SECURITY SCAN, SIZE, EXPIRES, and MANIFEST.

TAG	LAST MODIFIED	SECURITY SCAN	SIZE	EXPIRES	MANIFEST
latest	5 months ago	7 High · 41 fixable	226.8 MB	Never	SHA256: b3211f993e4b

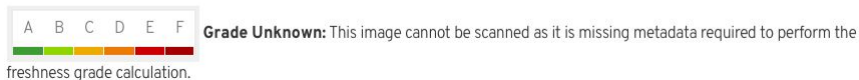
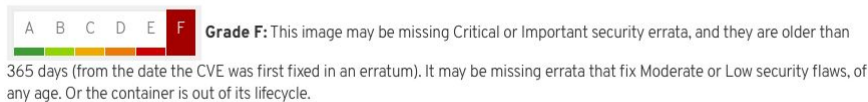
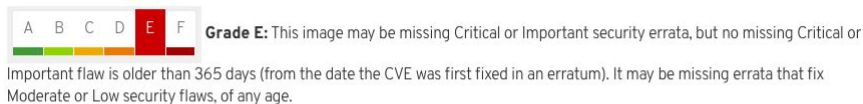
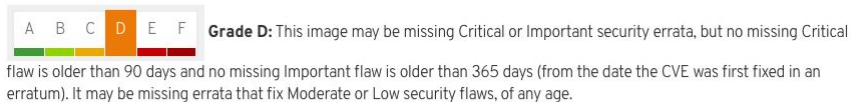
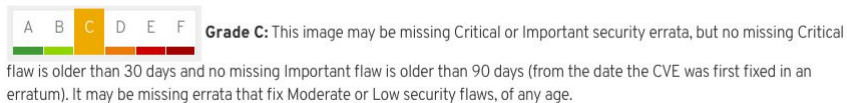
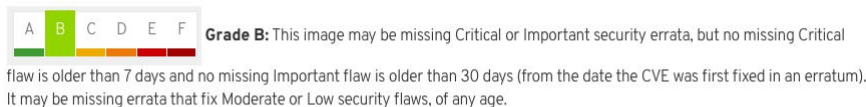
Sécurité des actifs

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.



that fix Moderate or Low security flaws.





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

Code en
amont

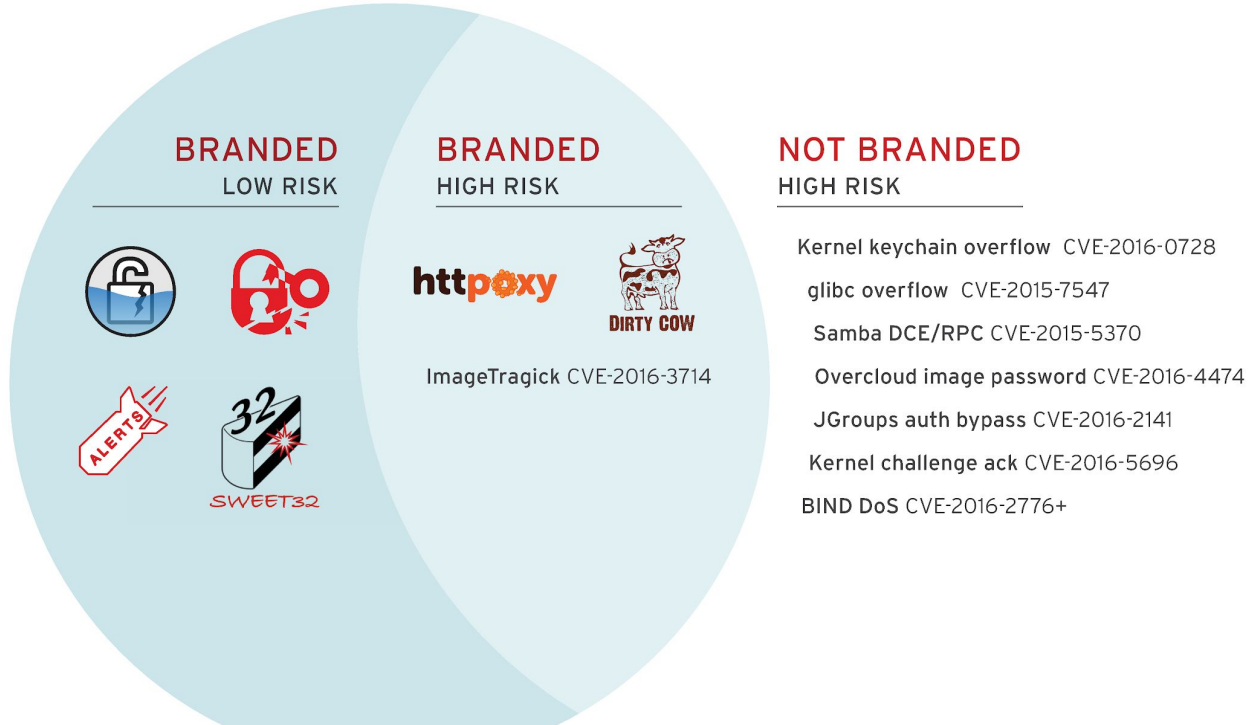
Projets de la
communauté

Produits
Red Hat

Clients
Red Hat

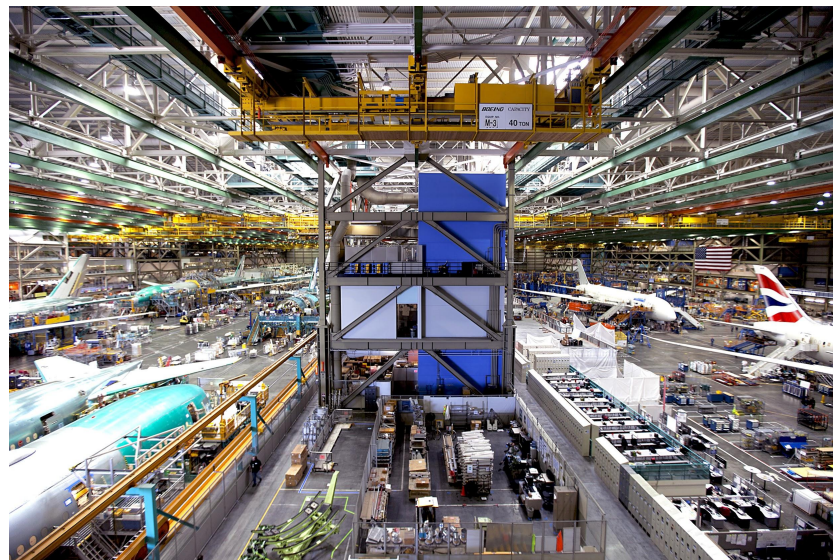
Red Hat: Gestion de la sécurité

Évaluation globale des risques, indépendamment du marketing



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)

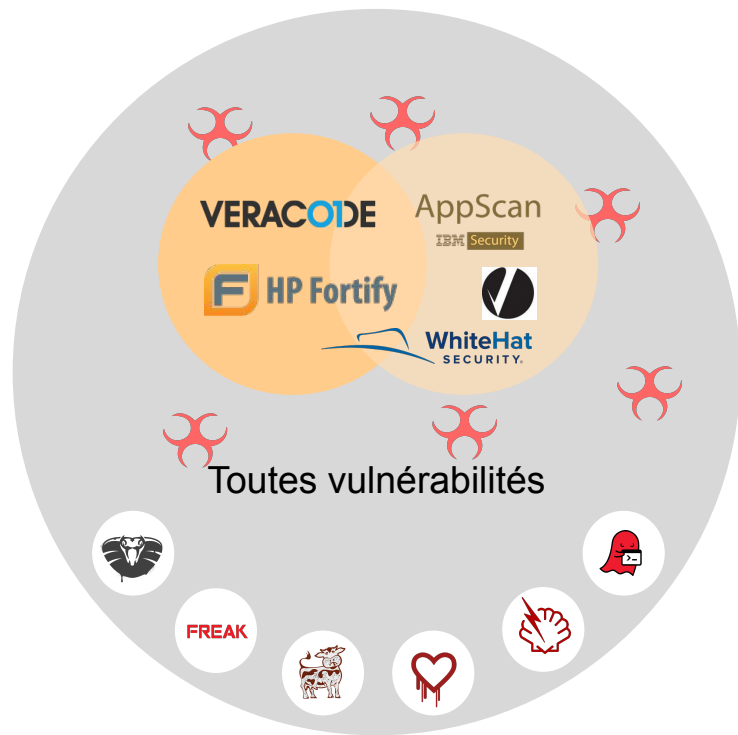


Chaîne d'assemblage Boeing

https://upload.wikimedia.org/wikipedia/commons/c/c8/At_Boeing%27s_Everett_factory_near_Seattle_%289130160595%29.jpg

Creative Commons

Le balayage des vulnérabilités en complément du SAST/DAST



Analyse statique et dynamique

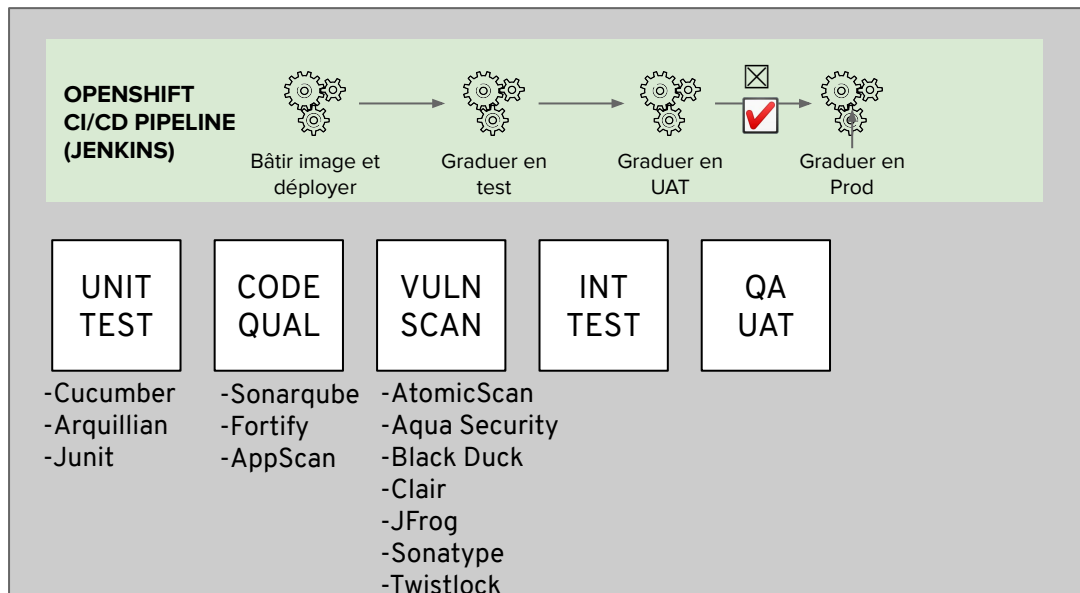
- Découverte des fautes de sécurité communes
- Focus sur votre code, pas l'upstream

Balayage des vulnérabilités

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

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



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



Référez 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.

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

The screenshot displays the Maven dependency analysis results for a multi-module project. The central panel shows four main sections:

- Security Issues:** OSIO Analytics has identified security issues in your stack. Total Issues found: 2. Highest CVSS Score: 7.5 / 10. No. of components with this CVSS Score: 1.
- Insights:** OSIO Analytics has identified components that are rarely used in similar stacks, and suggest alternate and additional components that can enhance your stack. Total Insights: 2, Usage Outliers: 2, Companion: 0, Components: 0.
- Licenses:** OSIO Analytics identifies the stack level license, the conflicting licenses, and the unknown licenses for your stack. Stack Level: None, License: 0, Conflicts: 3, Unknown: 3, Restrictive License(s): 0.
- Component Details:** OSIO Analytics identifies the total number of components, analyzes them, and provides details on security, usage, and license issues in your components. Total Components: 5, Analyzed Components: 5, Unknown Components: 0.

The 'Problems' window at the bottom shows a warning: "Groupid is duplicate of par... groupid (Click for 1 more)".

Sécurité des opérations

Déploiement

- Registres de confiance
- Signature pour authentifier et autoriser 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

Balayage des vulnérabilités - Clair

The screenshot displays the Quay Security Scanner interface. At the top, the Quay logo and navigation links (Repositories, Tutorial, Docs, Blog) are visible. The user is logged in as 'Quay User'. The main content area shows a summary for a specific image: 'exmample/nginx' with ID '99009dfc5e95'. A donut chart indicates that 55 vulnerabilities were detected, with 15 patches available. The chart is divided into five segments: 40% (grey), 16% (orange), 16% (yellow), 13% (light yellow), and 15% (dark grey). A legend on the right lists the severity levels: 9 High-level, 9 Medium-level, 7 Low-level, 22 Negligible-level, and 8 Unknown-level vulnerabilities. Below the chart, a table titled 'Image Vulnerabilities' lists specific CVEs, their severity, the affected package, current version, and fixed version. Two vulnerabilities are shown: CVE-2016-2108 (High severity) for the 'openssl' package, and CVE-2016-3191 (High severity) for the 'pcre3' package. The interface also includes a search filter and a checkbox for 'Only show fixable' vulnerabilities.

QUAY Repositories Tutorial Docs Blog

exmample/nginx 99009dfc5e95

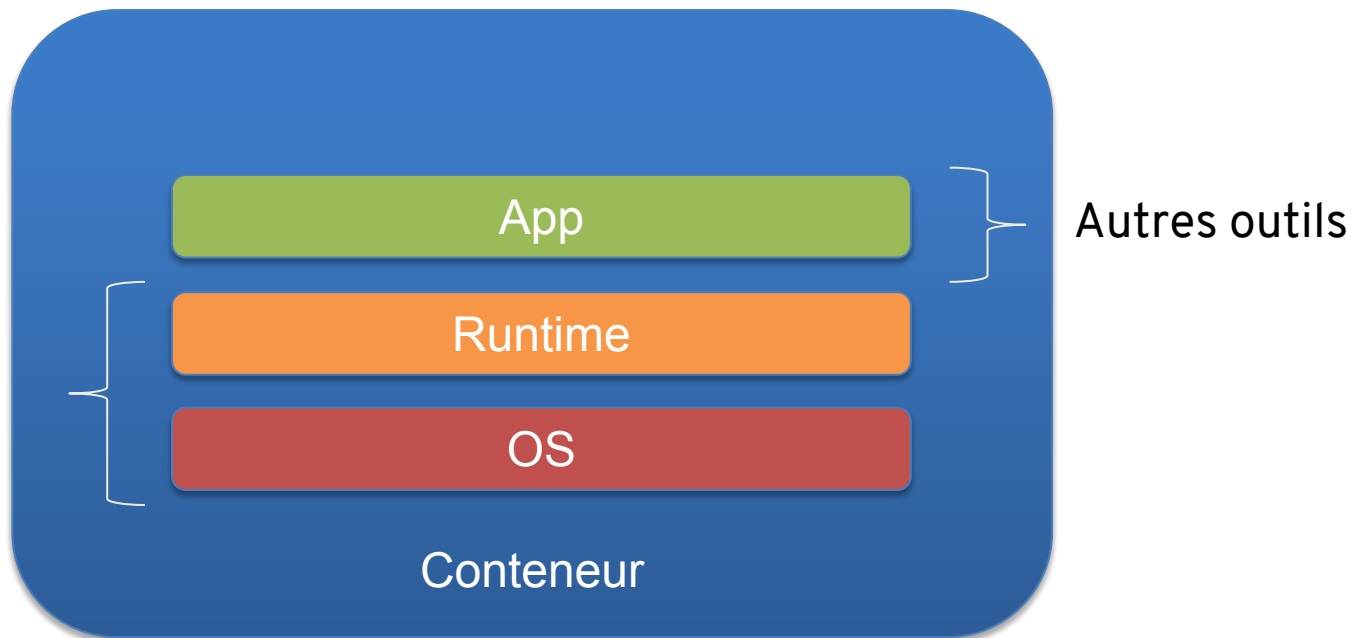
Quay Security Scanner has detected **55** vulnerabilities.
Patches are available for **15** vulnerabilities.

- 9 High-level vulnerabilities.
- 9 Medium-level vulnerabilities.
- 7 Low-level vulnerabilities.
- 22 Negligible-level vulnerabilities.
- 8 Unknown-level vulnerabilities.

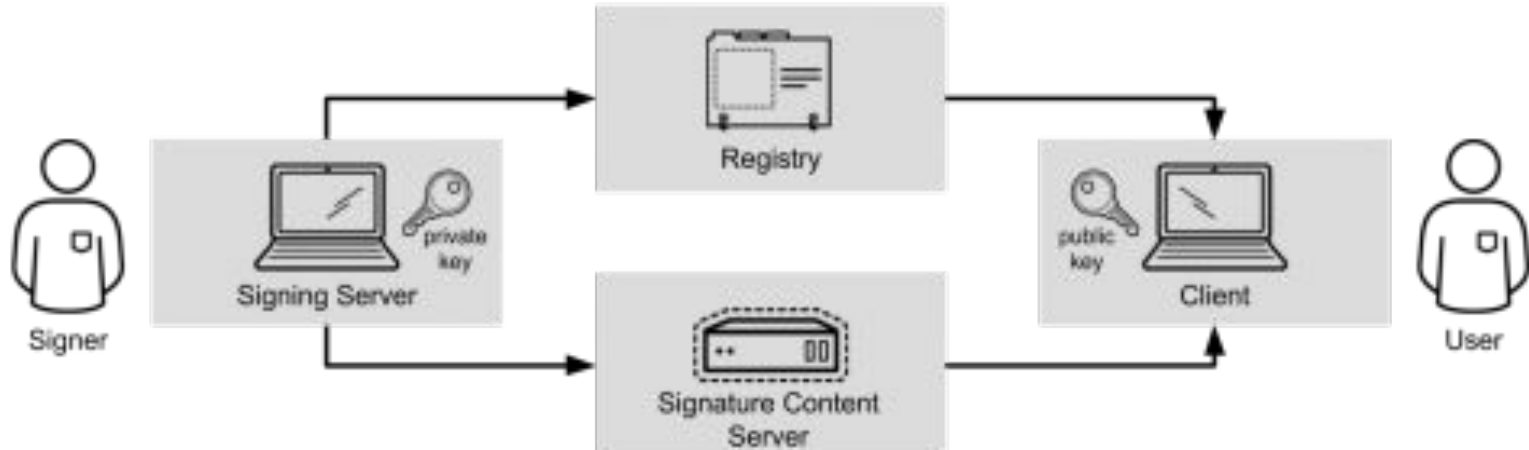
Image Vulnerabilities Only show fixable

CVE	SEVERITY ↓	PACKAGE	CURRENT VERSION	FIXED IN VERSION	INTRODUCED IN IMAGE
> CVE-2016-2108	10 / 10	openssl	1.0.1k-3+deb8u4	1.0.1k-3+deb8u5	RUN opt-key adv --keyserver hkp...
> CVE-2016-3191	High	pcre3	2:8.35-3.3+deb8u2	2:8.35-3.3+deb8u3	ADD file:b5391cb13172fb513dbfca...

Conteneur: plusieurs couches



Signature d'images



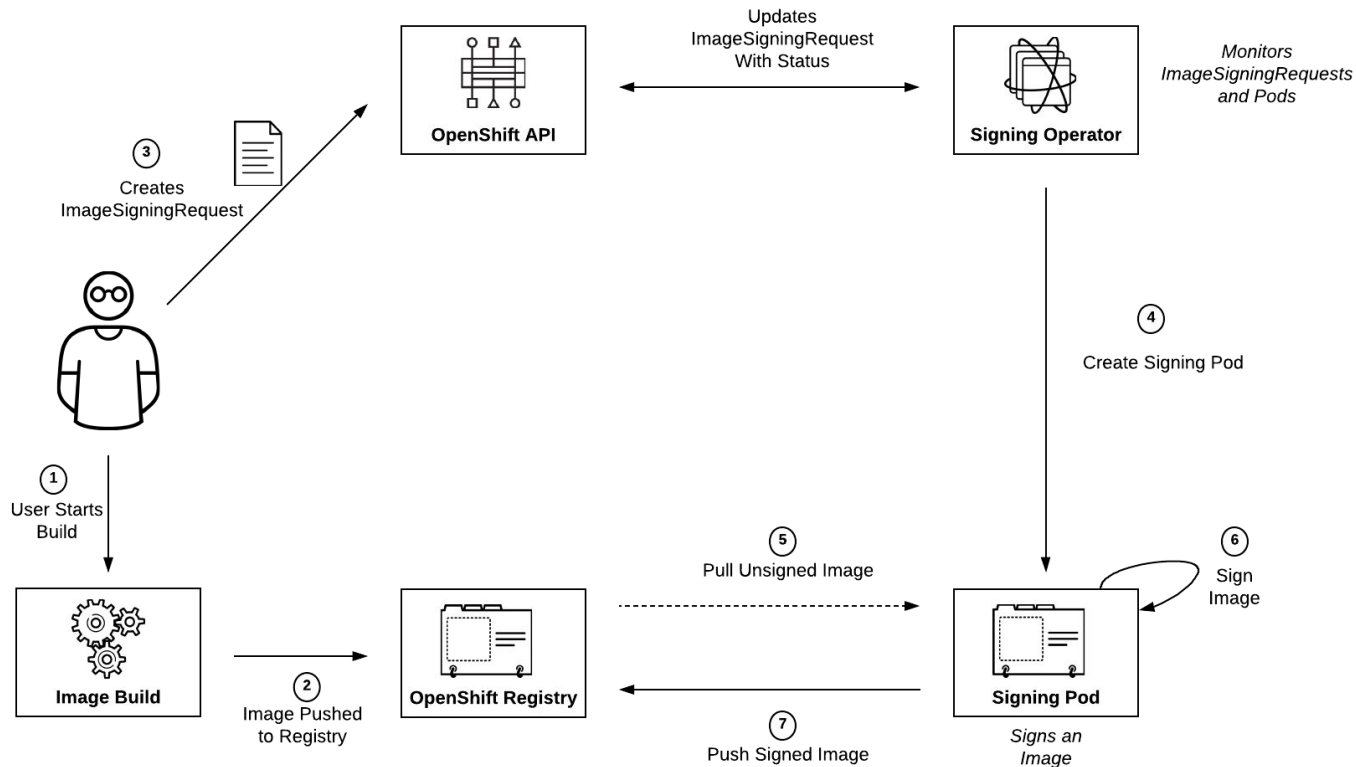
Vérification de la source de l'image

Support de plusieurs signatures

Indépendant du registre

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

Example: Signature d'Images



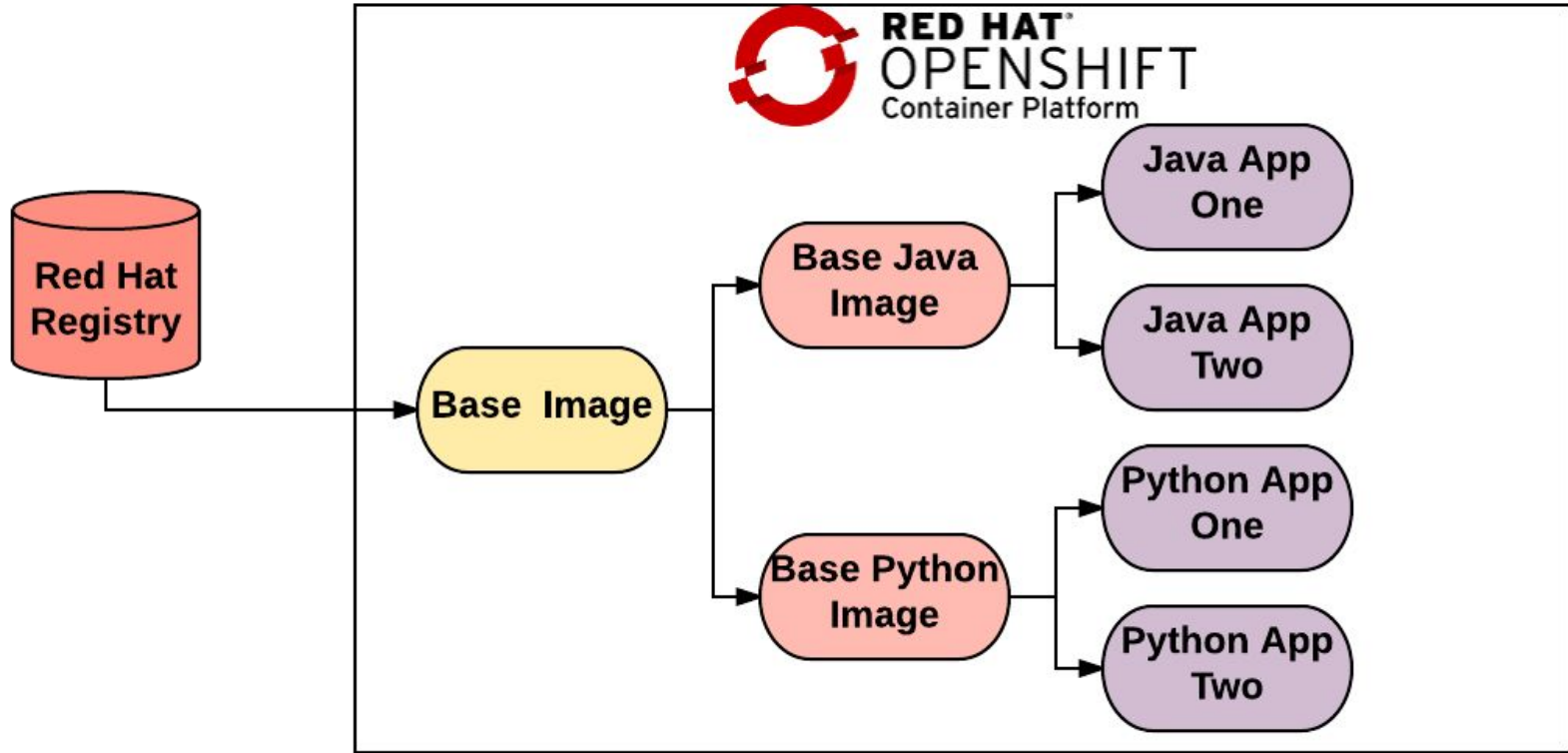
CUSTOM RESOURCE DEFINITIONS

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

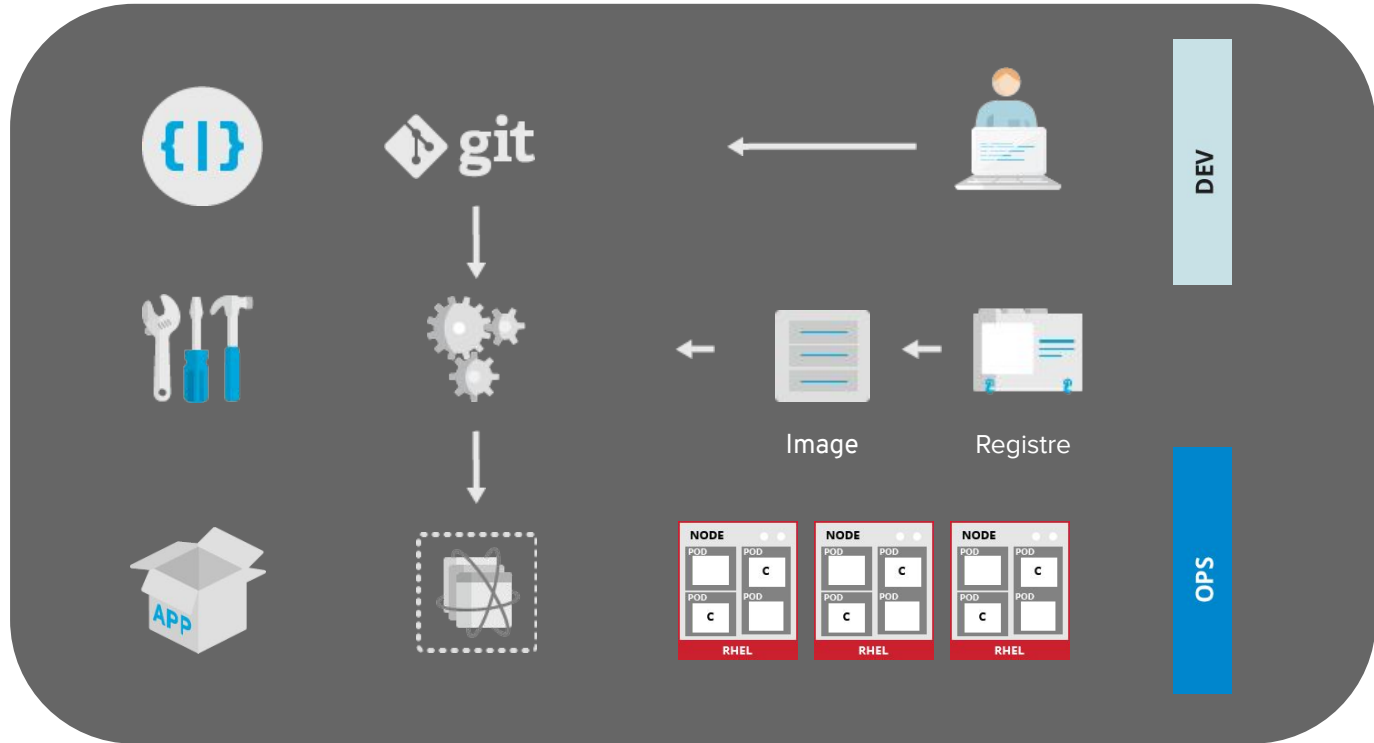


Construction en cascade



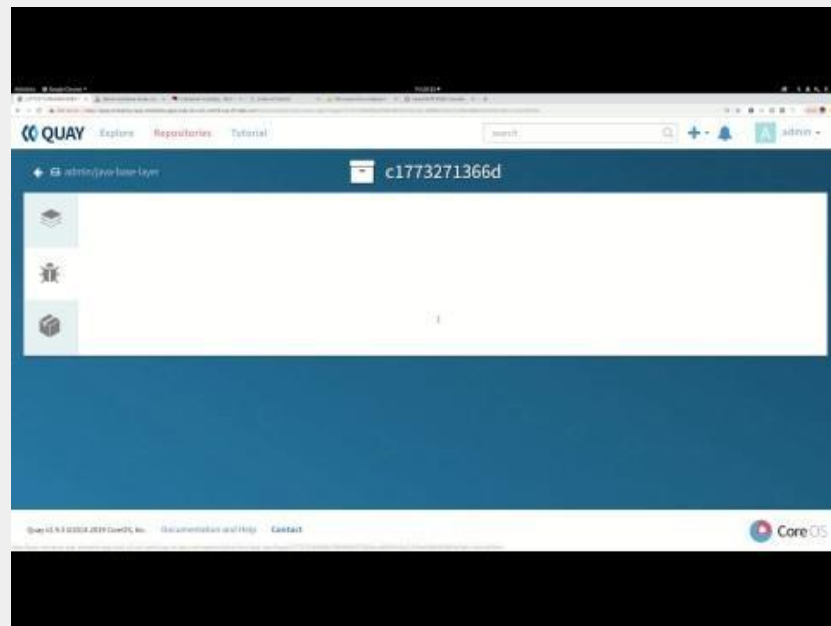
Sécurité en continue

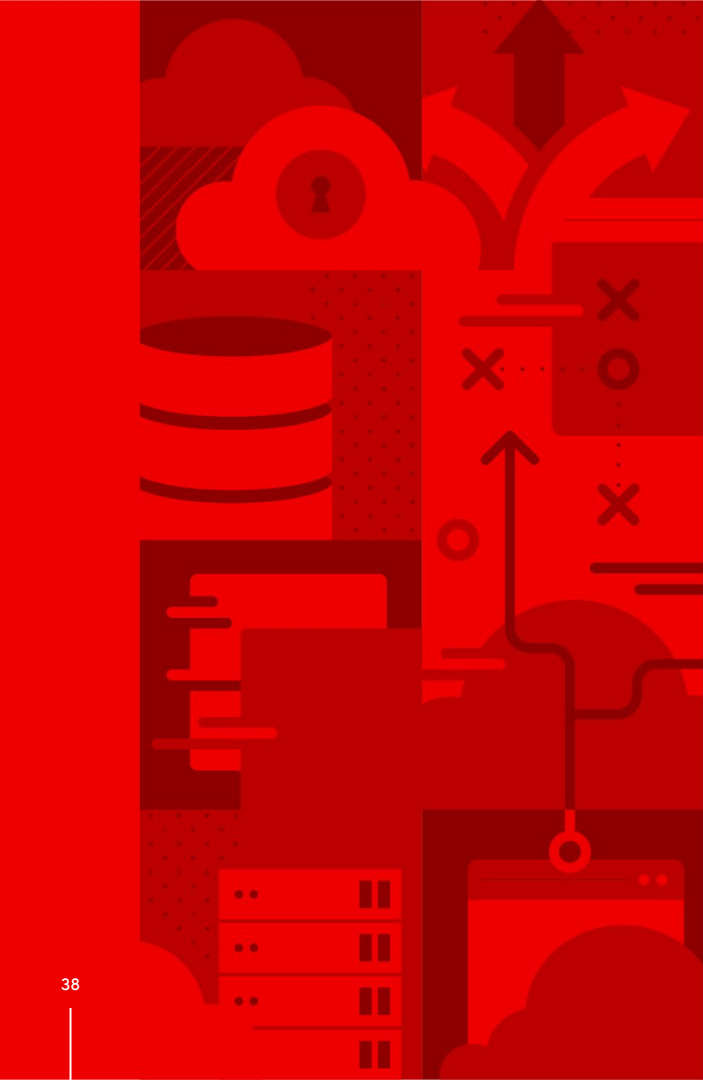
Continuous Integration / Continuous Deployment / Continuous Security



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

Demo





Questions

Merci!