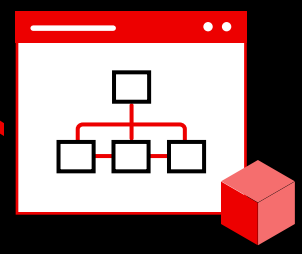
Red Hat
OpenShift
Platform Plus

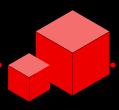
Créer une usine logicielle pour le DevSecOps

Un guide pour lancer votre projet DevSecOps

Sommaire



Protégez votre entreprise avec le DevSecOps



Un nombre croissant d'entreprises adoptent le développement d'applications **cloud-native**, les **conteneurs** et les **microservices** pour innover et réussir leur **transformation numérique**. Dans le cadre de cette transformation, nombre d'entre elles utilisent Kubernetes pour l'orchestration des conteneurs afin de prendre en charge les opérations cloud-native. Puisque les **clusters Kubernetes** peuvent s'étendre sur des hôtes dans des environnements sur site et cloud, Kubernetes représente la plateforme idéale pour héberger des applications cloud-native qui nécessitent une mise à l'échelle rapide et une exploitation résiliente.

Néanmoins, tout cela pose de nouveaux défis, notamment en matière de sécurité et de gestion à grande échelle. En effet, 50 % des responsables informatiques interrogés citent la cybersécurité comme l'une des trois priorités technologiques[1].

L'adoption d'approches et de pratiques DevSecOps peut vous aider à intégrer la sécurité dans vos applications, dans vos processus et dans votre plateforme afin de mieux protéger votre entreprise.

Ce livre numérique fournit des conseils et présente les éléments à prendre en compte pour établir une stratégie DevSecOps réussie au sein de votre entreprise sur la base de Red Hat® OpenShift® et d'autres technologies Red Hat.

Une application cloud-native, qu'est-ce que c'est ?

Une **application cloud-native** se compose de services plus petits, indépendants et faiblement couplés.

Le DevOps et le DevSecOps, qu'est-ce que c'est ?

Le modèle **DevOps** est une approche de la culture informatique, de l'automatisation et de la conception de plateformes qui se concentre sur l'augmentation de la valeur ajoutée et l'optimisation de la réactivité des entreprises grâce à une distribution plus rapide, automatisée et efficace des services. La méthode **DevSecOps** correspond à l'expansion de la culture collaborative DevOps pour intégrer la sécurité à l'ensemble du cycle de vie des applications. Le DevSecOps regroupe les individus, processus et technologies, et rend ainsi la sécurité omniprésente dans les environnements distribués.

Grâce à l'approche DevSecOps, la sécurité devient une responsabilité partagée et appliquée par toutes les équipes. Elle n'est plus seulement un ensemble de tâches confié à une seule équipe à la fin du développement et du déploiement des applications. Les équipes de sécurité, de développement et d'exploitation travaillent main dans la main et partagent leurs connaissances, leurs commentaires, les leçons à retenir et les informations importantes. Le DevSecOps permet d'intégrer la sécurité dès le début du développement des applications et du déploiement de l'infrastructure, améliorant ainsi la protection et diminuant les risques.

88 %

des entreprises interrogées utilisent Kubernetes comme orchestrateur de conteneurs, et 74 % l'utilisent en production[2].

74 %

des entreprises interrogées ont déjà lancé un projet DevSecOps[2].

1 Flexera, « 2021 Flexera State of Tech Spend Report », janvier 2021.

2 Red Hat, « Rapport sur l'état de la sécurité de Kubernetes », 2021.

Objectifs de l'approche DevSecOps

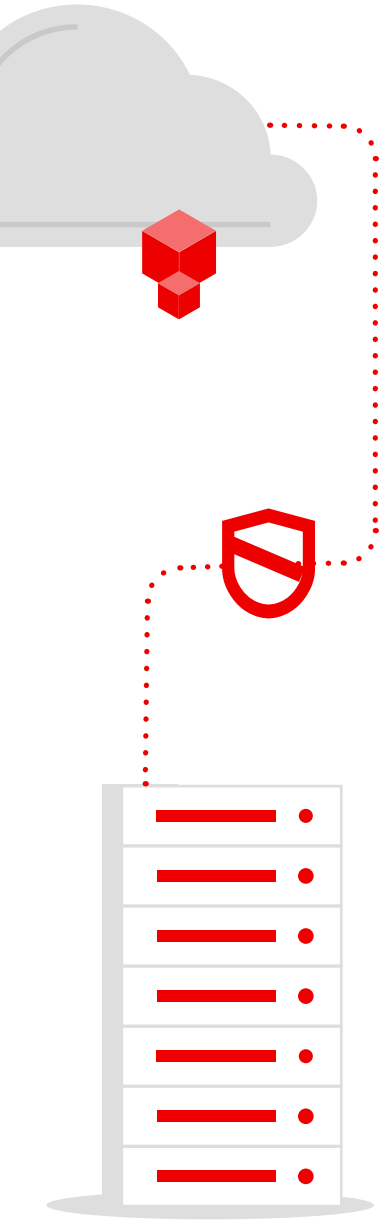
L'approche DevSecOps vise à fournir et à déployer rapidement des applications, des services et des fonctionnalités de haute qualité et axés sur la sécurité, à grande échelle.

Évolutivité

Rapidité

Sécurité

Stabilité



Défis liés à la mise en œuvre de l'approche DevSecOps

Processus manuels

Les tâches de développement, de test et de sécurité peuvent être chronophages, pénibles, sujettes aux erreurs et difficiles à réaliser lorsqu'elles requièrent de fréquentes interventions humaines.

Collaboration limitée entre les équipes

Les équipes de développement, de sécurité et d'exploitation travaillent souvent dans leur propre domaine uniquement. Résultat : les processus sont fragmentés, les transferts d'informations s'effectuent manuellement et chaque groupe ne dispose que d'une connaissance et d'une compréhension limitées des défis et des besoins des autres.

Application tardive des processus de sécurité

Les approches traditionnelles de développement et de lancement d'applications n'appliquent les pratiques et les contrôles de sécurité qu'à la fin du processus, juste avant le déploiement en production.

Complexité de l'environnement d'applications

Il peut être difficile d'appréhender les connexions et implications en matière de sécurité de tous les nouveaux éléments (conteneurs, microservices, services cloud, etc.) qui composent les environnements de développement, de test et de production d'applications d'envergure et complexes.

Dépendances externes

Le développement d'applications cloud-native s'appuie presque toujours sur un certain nombre de dépendances externes, notamment des sections de code Open Source, des bibliothèques et des services, qui doivent également être sécurisées.

Évolution constante de la sécurité

Les menaces et réglementations de sécurité, notamment les exigences métier, techniques et géographiques, changent à un rythme effréné et il s'avère difficile de rester à jour et en conformité.

Les individus, les processus et les technologies sont essentiels

Le DevSecOps ne désigne pas une équipe ni un processus uniques. Il s'agit d'un modèle appliqué à l'échelle de l'entreprise, qui nécessite des changements et des alignements à trois niveaux différents : les individus, les processus et les technologies.

Individus

Le personnel joue un rôle central dans toute initiative à l'échelle de l'entreprise et l'approche DevSecOps n'échappe pas à cette règle. Pour étendre globalement cette approche, toutes les équipes, y compris le développement, la sécurité et l'exploitation, doivent s'impliquer, participer et se faire confiance.

Processus

Les processus font avancer les projets du début à la fin. Afin d'élargir l'adoption du DevSecOps, il est donc essentiel de mettre en place des processus clairs pour la création, le déploiement, la gestion et l'adaptation des applications et de l'infrastructure, ainsi que pour l'intégration de la sécurité tout au long de leur cycle de vie.

Technologies

Votre plateforme d'applications vous permet de créer, de déployer et d'exécuter des applications, ainsi qu'une infrastructure. Une plateforme unifiée qui prend en charge les équipes de développement, de sécurité et d'exploitation fournit une base pour construire et adapter votre modèle DevSecOps.

Préparez votre entreprise à réussir avec le DevSecOps

Aucune entreprise ne peut mettre en place des pratiques DevSecOps complètes du jour au lendemain. L'adoption de l'approche DevSecOps est un parcours progressif. Vous aurez besoin d'une stratégie logique et durable pour progresser et apprendre au fil du temps.

Encouragez la collaboration entre les équipes.

Incitez votre personnel à collaborer au sein de votre entreprise à l'aide de processus adaptés. La coordination permet aux équipes de créer des workflows DevSecOps à plus forte valeur ajoutée. La collaboration aide également à développer un sentiment de propriété et de responsabilité partagées entre les équipes de développement, de sécurité et d'exploitation.

Documentez votre situation initiale.

Documentez en détail vos processus actuels de développement, de gestion des changements et de gouvernance à l'aide de frameworks dynamiques comme **GitOps**. Vous pourrez prendre de meilleures décisions pour l'avenir si vous comprenez où vous en êtes et quels sont les défis à relever. À mesure que vous adapterez vos processus, assurez-vous de documenter tous les nouveaux processus ainsi que les raisons qui ont motivé vos changements.

Évaluez vos processus.

Identifiez et adaptez les processus qui ne sont pas en phase avec vos objectifs DevSecOps. Il peut notamment s'agir de configurations et d'infrastructures d'intégration continue/de déploiement continu (CI/CD) inefficaces ou disparates, de processus trop centralisés ou de processus qui dépendent d'interventions manuelles fréquentes.

Définissez et mesurez la réussite.

Précisez les critères de réussite de votre approche DevSecOps et identifiez les indicateurs de mesure ou de performances clés qui vous aideront à suivre votre progression. Les indicateurs de mesure incluent par exemple : le temps de création et de déploiement des applications, les taux de lancement des changements et de défauts, le délai de résolution des problèmes ou la disponibilité des applications.

Partagez les connaissances et les meilleures pratiques.

Formez une équipe composée de plusieurs parties prenantes (souvent appelée « communauté de pratique » ou « centre d'excellence ») qui partage les bonnes pratiques, les expériences et les réussites en matière de DevSecOps dans toute l'entreprise. Cette équipe a également pour mission d'aider les autres équipes qui sont prêtes à adopter les pratiques DevSecOps et à se lancer.

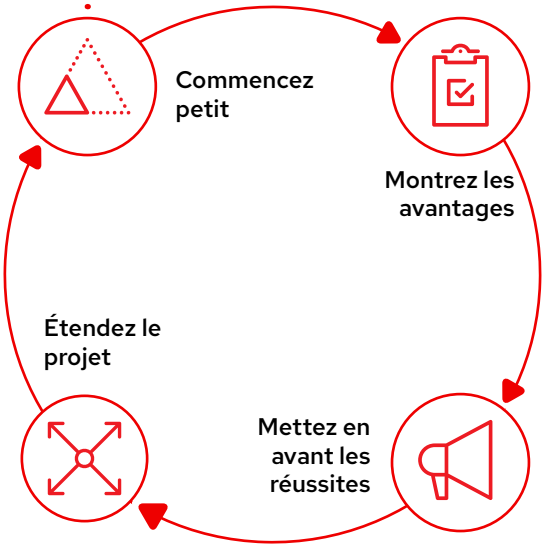
Favorisez l'engagement dans votre entreprise.

Assurez-vous que tous les membres de votre entreprise s'engagent à adopter le DevSecOps. Aidez toutes les équipes à comprendre les raisons derrière chaque changement et soulignez les effets bénéfiques sur leurs rôles. Elles progresseront plus rapidement avec le soutien des dirigeants et des indicateurs de mesure clairs.

Appliquez vos pratiques DevSecOps

Une fois votre stratégie DevSecOps définie, il est temps de vous lancer. Toutes les équipes de développement ne seront pas prêtes à adopter ce nouveau modèle immédiatement. Alors, commencez par les équipes qui ont déjà adopté avec succès de nouveaux processus et de nouvelles plateformes par le passé. Les membres de ces équipes font souvent de bons candidats pour votre équipe de parties prenantes.

Commencez à petite échelle, présentez vos réussites, développez prudemment et réutilisez. Visez des réussites progressives sur des périodes courtes. Suivez les progrès réalisés à l'aide de vos indicateurs de mesure et tirez des leçons des projets ou processus qui ont moins bien réussi. Pour chaque victoire, soulignez les mérites du DevSecOps et partagez l'expérience de l'équipe au sein de l'entreprise. Ainsi, les autres pourront s'appuyer sur l'expérience de chaque équipe pour générer une valeur encore plus importante.



Inspirez-vous des usines pour la distribution des logiciels

La distribution de logiciels modernes repose sur la rapidité, la cohérence et la qualité. Une approche de type « usine logicielle » vous aide à accélérer et appliquer les changements de comportement et les comportements nécessaires pour adopter une culture DevSecOps au sein de votre entreprise. Cette approche vous permet de développer et de déployer rapidement des applications de haute qualité en utilisant une **chaîne d'approvisionnement des logiciels fiable** et un ensemble cohérent de processus agiles tels que le développement par les tests.

Avantages d'une usine logicielle

Une usine logicielle offre des avantages mesurables :

Faible délai de mise en œuvre des changements

Fréquence de déploiement élevée

Rétablissement rapide des services défaillants

Faible taux d'échec des changements

Indicateurs quantifiés des performances en matière de distribution de logiciels[3]

Indicateurs des performances en matière de distribution de logiciels	Avec une usine logicielle	Sans usine logicielle
Délai de mise en œuvre des changements	<1 heure	1 à 6 mois
Fréquence de déploiement	À la demande (>1 par jour)	Une fois tous les 1 à 6 mois
Délai de rétablissement des services	<1 heure	1 jour à 1 semaine
Taux d'échec des changements	Entre 0 % et 15 %	Entre 16 % et 30 %

*3 Google Cloud, « **Accelerate State of DevOps 2021** », septembre 2021.*

À quoi ressemble une usine logicielle ?

Une usine logicielle vous fait passer de processus manuels incohérents à une exploitation cohérente et automatisée.

Sans usine logicielle

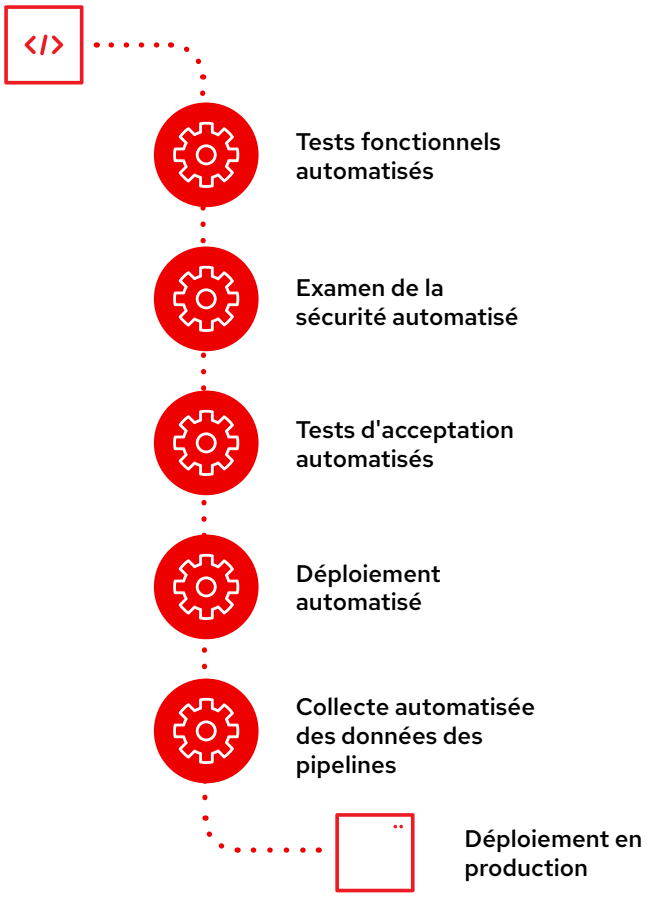
Les processus et approbations manuels ralentissent le développement et le déploiement, les attentes sont peu claires et l'application de la sécurité manque de cohérence. Puisque la mise en œuvre des modifications, même minimes, peut prendre des jours voire des semaines, les équipes essaient souvent d'apporter un grand nombre de changements en un seul déploiement. Cette stratégie augmente le risque d'échec et les problèmes de sécurité.

La confiance entre les équipes est souvent ténue en raison du manque de transparence tout au long du processus. Les mesures de sécurité et de conformité sont appliquées manuellement en fin de processus, de sorte que certains problèmes ne sont pas identifiés pendant le développement. Résultat : les développeurs se retrouvent à corriger des problèmes de sécurité et de conformité imprévus dans leurs applications. Ces mauvaises surprises deviennent vite sources de frustration et de méfiance lors d'une phase déjà stressante.

Avec une usine logicielle

Des processus définis et automatisés accélèrent le développement et le déploiement, renforcent la sécurité de manière cohérente et définissent des attentes claires pour toutes les équipes concernées. Puisqu'il est possible de déployer de petits changements en quelques minutes, les équipes peuvent le faire plusieurs fois par jour, ce qui réduit le risque global.

La transparence et la visibilité sont des caractéristiques essentielles des usines logicielles, ce qui facilite l'instauration d'un climat de confiance entre les équipes de développement, d'exploitation et de sécurité. Les mesures de sécurité et de conformité sont automatiquement appliquées pendant le développement, de sorte que les problèmes peuvent être détectés et corrigés plus tôt dans le processus. Des processus et des politiques documentés aident les équipes à comprendre les attentes tout au long du processus et à éviter les surprises au moment de déployer les applications en production.



Créez votre propre usine logicielle

L'**automatisation** est au cœur de l'usine logicielle. Elle est essentielle pour exploiter les environnements cloud-native et adopter des pratiques DevSecOps. L'automatisation vous aide à mettre à l'échelle le développement, la distribution, le déploiement et l'infrastructure de manière contrôlée. Vous pouvez également provisionner et retirer dynamiquement des ressources, des environnements et des applications. Ainsi, votre entreprise peut réagir plus rapidement au changement.

Envisagez d'automatiser tous les aspects de votre workflow DevSecOps, notamment vos processus de développement, de test, de contrôle de la qualité du code, de validation de la conformité, de détection des vulnérabilités et de correction. Utilisez les pipelines CI/CD pour automatiser le développement et l'amélioration des applications ainsi que le déploiement et la gestion des infrastructures. Définissez et documentez les politiques de sécurité et de risque, et automatisez le contrôle de la conformité et la correction par rapport à ces politiques tout au long du cycle de vie de vos logiciels.

L'automatisation déclarative et axée sur l'intention vous aidera à évoluer et à vous adapter plus rapidement et plus facilement.

L'automatisation déclarative vous permet de définir la configuration souhaitée pour une application ou une infrastructure, plutôt qu'un ensemble d'instructions pour la mise en place de ressources. Vous décrivez simplement l'objectif final, plutôt que les moyens d'y parvenir. Votre plateforme d'applications fournit et configure ensuite les ressources nécessaires pour atteindre l'état souhaité. Elle se corrige également seule pour que la configuration des ressources reste correcte au fil du temps. Enfin, cette approche vous prépare à **GitOps**, un ensemble de pratiques de gestion des configurations d'infrastructure et d'application qui utilise le système de contrôle de version Git.

Que faut-il automatiser et quand ?

À l'instar du DevSecOps dans son ensemble, le déploiement de l'automatisation se fait progressivement et nécessite une certaine planification. Suivez ces étapes pour vous lancer dans l'automatisation :

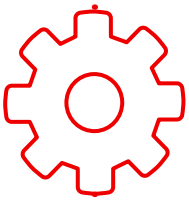
1. Documentez vos processus de manière détaillée.
2. À chaque étape manuelle de votre processus, notez les décisions et décrivez le cheminement : lecture de documents, réflexion sur certains facteurs spécifiques, consultation de divers spécialistes ou autres actions.
3. Identifiez toutes les étapes manuelles faciles à automatiser et déterminez les types de changements à automatiser. Par exemple, vous pouvez automatiser les petits changements, mais exiger une validation par certaines équipes pour les changements plus importants.
4. Concernant les étapes manuelles difficiles à automatiser, évaluez les ressources et efforts nécessaires, puis créez un plan de mise en œuvre de l'automatisation.

Commencez à automatiser immédiatement ; n'attendez pas d'avoir identifié tous les domaines d'automatisation possibles. L'automatisation itérative des processus est, en soi, un processus DevOps. À mesure que vous automatiserez, adapterez et affinerez vos processus, vous acquerrez des compétences et une expérience précieuses pour la mise en place de votre stratégie DevSecOps globale.

Se concentrer sur les tâches intéressantes

L'automatisation n'est pas destinée à remplacer les individus, mais à améliorer la productivité, la cohérence et l'efficacité. C'est le paradoxe de l'automatisation : lorsque vous automatisez, l'intervention humaine devient à la fois plus importante et moins fréquente.

Certains y voient un outil pour remplacer l'homme, mais il faut comprendre qu'il s'agit d'une occasion pour le personnel informatique qualifié de se libérer des tâches quotidiennes et répétitives pour se concentrer sur la résolution des problèmes les plus importants.



Apprenez à automatiser à l'échelle de l'entreprise

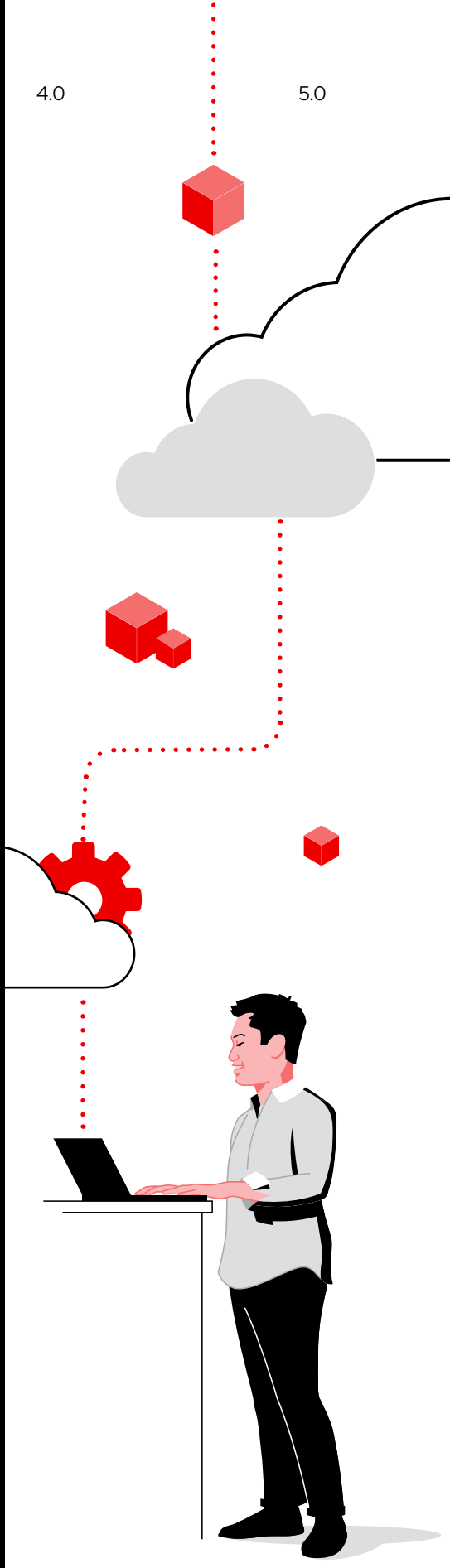
L'automatisation peut réunir vos équipes, processus et technologies pour augmenter la flexibilité, l'innovation et la valeur de votre entreprise.

Pour en savoir plus sur l'adoption de l'automatisation dans l'ensemble de votre entreprise, lisez le livre numérique « **L'entreprise automatisée** ».

Des outils pour votre usine logicielle

Les outils sont une partie importante de votre usine logicielle. Nous vous recommandons d'utiliser et d'automatiser les catégories d'outils suivantes. Nous avons indiqué des exemples pour chaque type d'outil, mais vous pouvez en choisir d'autres.

Catégorie d'outils	Exemples
Gestion de projets	▸ Confluence avec Jira ▸ Trello
Gestion du code source	▸ GitHub ▸ Gitlab
Environnements de développement intégrés	▸ VS.code ▸ **Red Hat OpenShift Dev Spaces**
Référentiels d'artéfacts	▸ Nexus ▸ Artifactory
CI/CD	▸ **Red Hat OpenShift Pipelines** ▸ **Jenkins**
Environnements d'exécution	▸ **Red Hat Runtimes** ▸ Golang
Création	▸ Maven ▸ Commande dotnet build
Test unitaire	▸ JUnit ▸ NUnit
Analyse du code source	▸ Sonarqube ▸ Fortify
Tests statiques de la sécurité des applications	▸ CheckMarx ▸ **Red Hat Advanced Cluster Security for Kubernetes**
Tests d'acceptation par l'utilisateur	▸ Cucumber ▸ Cyprus
Tests dynamiques de la sécurité des applications	▸ Veracode ▸ Synopsys
Télémétrie, indicateurs de mesure et journalisation	▸ **Prometheus** ▸ **Grafana** ▸ **Elasticsearch, Fluentd et Kibana (EFK)** ▸ Splunk
Service Mesh	▸ Linkerd ▸ **Red Hat OpenShift Service Mesh**



Créez, déployez, exécutez

Les architectes de plateforme ou les ingénieurs DevOps configurent souvent des usines logicielles pour le compte des développeurs. Lorsque vous construisez votre usine logicielle, tenez compte des meilleures pratiques de sécurité dans ces trois domaines : création, déploiement et exécution.

Création

Contrôlez la sécurité et la conformité des applications.

Pour le déploiement des applications cloud-native, il est essentiel que la sécurité soit intégrée.

- Utilisez des sources fiables pour le contenu externe des conteneurs et des applications, y compris les environnements d'exécution.
- Choisissez un registre de conteneurs privé et fiable pour gérer les images.
- Automatisez vos pipelines de développement et de déploiement.
- Mettez en œuvre les exigences non fonctionnelles dans le code en utilisant des pratiques agiles comme le développement par les tests.
- Améliorez la sécurité dans vos pipelines d'applications avec l'analyse de la qualité du code, de la vulnérabilité des images et du déploiement Kubernetes.
- Automatisez le déploiement et le placement des applications.

Déploiement

Protégez votre plateforme.

Une sécurité efficace nécessite de protéger votre plateforme Kubernetes et d'automatiser les politiques de déploiement.

- Réduisez la surface d'attaque en utilisant un système d'exploitation optimisé pour les conteneurs.
- Automatisez la gestion de la configuration et l'application des politiques sur les clusters.
- Mettez en œuvre le principe de moindre privilège pour les accès avec des contrôles d'accès basés sur les rôles très précis.
- Chiffrez les données de la plateforme et des applications en transit et au repos.
- Utilisez des solutions automatisées de conformité, d'évaluation des risques et de correction.
- Réduisez les risques lors du déploiement grâce aux politiques de contrôle d'admission des pods Kubernetes.

Exécution

Sécurisez les environnements d'exécution de vos conteneurs.

Assurez la sécurité des applications au moment de l'exécution.

- Isolez les applications en cours d'exécution avec SELinux (Security-Enhanced Linux®), les contraintes de contexte de sécurité (SCC), les espaces de noms Kubernetes, les contrôles d'accès basés sur les rôles et les politiques de réseau.
- Utilisez des quotas pour éviter les conflits de ressources et les problèmes de performance associés.
- Gérez l'accès aux applications et protégez les données des applications grâce à la gestion des utilisateurs avec l'authentification unique et unifiée, à la gestion de la sécurité à l'entrée et à la sortie, au trafic chiffré de pod à pod et à la gestion des interfaces de programmation d'applications (API).
- Auditez et surveillez l'activité des plateformes et des applications.
- Automatisez la détection des menaces et les corrections sur les pods qui présentent un comportement anormal, en cas de réattribution des privilèges et sur les processus à risque comme le cryptominage.
- Utilisez des contrôleurs d'admission pour empêcher le déploiement des conteneurs non conformes aux politiques de sécurité.
- Créez des réseaux Zero Trust à l'aide de Service Mesh et de politiques réseau.

Conseil de sécurité

Lisez le livre blanc « **Une approche multicouche de la sécurité des conteneurs et de Kubernetes** » pour en savoir plus sur la protection des applications conteneurisées gérées avec Kubernetes.

Création	Déploiement	Exécution
Cycle de vie des applications	**Gestion des configurations de l'environnement**	**Observabilité de l'environnement et alertes**
Analyse des vulnérabilités	Contrôleur d'admission de politique	Analyse comportementale de l'exécution
Analyse de la configuration des applications	Évaluation de la conformité	Recommandations sur la politique réseau
API pour l'intégration CI/CD	Profil de risques	Détection des menaces et réponse
Contenu fiable	Cycle de vie de la plateforme Kubernetes	Isolation des conteneurs
Registre de conteneurs	Gestion des identités et des accès	Isolation du réseau
Gestion de versions	Données de plateforme	Accès aux applications et données
Pipelines CI/CD	Politiques de déploiement	Observabilité

DevSecOps

Mettez en œuvre le DevSecOps avec les experts

Red Hat rassemble un écosystème de partenaires certifiés, une vaste expertise et des plateformes novatrices pour créer, sécuriser et déployer des applications dans tous les environnements de cloud hybride. Red Hat compte plusieurs années d'expérience en matière de soutien aux entreprises et les aide à surmonter leurs défis technologiques et métier en utilisant les meilleures pratiques du secteur et les technologies Open Source.

Avec une chaîne logistique des contenus fiable, l'assistance d'une équipe de sécurité spécialisée et des rétroportages de fonctions clés de sécurité, les plateformes Red Hat créent une base idéale pour les solutions DevSecOps. Enfin, pour vous aider à réussir rapidement la mise en œuvre du DevSecOps, Red Hat propose des **formations et certifications**, des **stages interactifs**, des **contrats de consulting** et des **offres gérées**.

Red Hat répond à vos besoins, peu importe où vous en êtes dans votre parcours vers le DevSecOps.

Avec ses plateformes Open Source éprouvées et ses services d'expert, vous pouvez déployer ce dont vous avez besoin aujourd'hui, vous adapter aux changements à venir et apprendre les méthodes et approches nécessaires pour une adoption efficace et rentable du DevSecOps.

En savoir plus sur les avantages de Red Hat pour le DevSecOps.

Tirez le meilleur parti de votre investissement dans le DevSecOps

Les services Red Hat peuvent vous fournir les ressources dont vous avez besoin pour lancer, accélérer et étendre votre approche DevSecOps.

- **Red Hat Open Innovation Labs**
  Stages durant lesquels les clients collaborent avec les équipes Red Hat pour apprendre de nouvelles méthodes de travail, telles que le DevSecOps, et obtenir des résultats
- **Red Hat Services Solution: DevSecOps**
  Contrat de service qui vous aide à mettre en œuvre une usine logicielle en utilisant une approche modulaire
- **Red Hat Services Journey: Container Adoption**
  Service de consulting pour l'adoption des conteneurs dans des domaines clés
- **Red Hat Services Journey: Automation Adoption**
  Service de consulting qui fournit une structure pour gérer votre parcours d'adoption de l'automatisation à l'échelle de l'entreprise

Déployez une plateforme pour le DevSecOps

La plateforme **Red Hat OpenShift Platform Plus** fournit une base technologique et un framework orienté (« opinionated ») pour le DevSecOps. Il s'agit d'une plateforme d'application novatrice qui fonctionne et évolue de manière cohérente dans une infrastructure sur site et cloud. Red Hat OpenShift Platform Plus propose une plateforme Kubernetes d'entreprise de premier plan pour créer, déployer, exécuter, protéger et gérer des applications de manière cohérente dans tout votre environnement. Les outils de gestion de plusieurs clusters offrent une visibilité et un contrôle complets sur vos clusters Kubernetes. Les fonctionnalités DevSecOps et de sécurité natives pour Kubernetes protègent la chaîne logistique des logiciels, l'infrastructure et les charges de travail. Un registre évolutif, distribué à l'échelle mondiale, et un système de gestion des données de cluster protègent votre environnement et vos informations.

Les interfaces d'intégration ouvertes et l'**écosystème de partenaires certifiés** de Red Hat vous permettent d'utiliser des outils de développement, de test, d'exploitation et de sécurité anciens et nouveaux avec la plateforme Red Hat OpenShift Platform Plus. De nombreux fournisseurs proposent des **opérateurs Red Hat OpenShift certifiés** ou des **conteneurs logiciels certifiés** afin de simplifier l'installation et la gestion de leurs logiciels sur les plateformes Red Hat. Vous pouvez également acheter et déployer de nombreux produits logiciels directement à partir de **Red Hat Marketplace**. Enfin, Red Hat collabore avec d'importants partenaires fournisseurs de cloud afin de proposer des **services cloud Red Hat OpenShift** gérés qui rationalisent le déploiement et l'exploitation et qui coûtent moins cher qu'une solution développée par les équipes internes.

Composants de Red Hat OpenShift Platform Plus

Red Hat OpenShift

Red Hat OpenShift est une plateforme d'applications Kubernetes pour les entreprises qui automatise l'exploitation de toute la pile pour la gestion des déploiements de clouds hybrides et d'edge computing. Elle comprend des fonctionnalités qui stimulent la productivité et la rapidité des développeurs.

Red Hat Advanced Cluster Management for Kubernetes

Red Hat Advanced Cluster Management for Kubernetes est une console qui permet de visualiser l'ensemble de votre domaine Kubernetes avec des fonctionnalités intégrées de gouvernance et de gestion du cycle de vie des applications..

Red Hat Advanced Cluster Security for Kubernetes

Red Hat Advanced Cluster Security for Kubernetes est une solution qui fournit des fonctions de sécurité natives pour Kubernetes afin d'améliorer la protection et la visibilité sur l'infrastructure et les charges de travail tout au long du cycle de vie de vos applications.

Red Hat Quay

Red Hat Quay est un registre d'images de conteneurs Open Source qui fournit un stockage et vous permet de concevoir, distribuer et déployer des conteneurs dans des datacenters et des environnements cloud.

Red Hat OpenShift Data Foundation

Red Hat OpenShift Data Foundation est une couche de services de données et de stockage évolutive qui assure l'efficacité, la résilience et la sécurité des données pour les environnements Red Hat OpenShift.

Red Hat OpenShift Platform Plus vous accompagne à toutes les étapes de votre projet DevSecOps, quelle que soit votre situation de départ, et vous donne une base pour avancer à votre propre rythme.

Fonctionnalités de sécurité intégrées

Surveillez les charges de travail en cours d'exécution pour identifier les problèmes et menaces grâce à la collecte et à l'analyse de données au niveau du système et à plus de 60 politiques de sécurité intégrées applicables durant tout le cycle de vie de vos applications.

Exploitation cohérente

Appliquez aux clusters Red Hat OpenShift des politiques d'exécution cohérentes en matière de sécurité, configuration, conformité et gouvernance, dans le cloud et dans le datacenter sur site.

Outils de développement

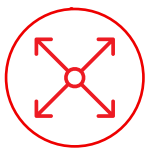
Créez, exécutez et déployez des applications plus rapidement grâce à une bibliothèque intégrée d'outils de création, de langages, de pipelines et de frameworks pris en charge. Operator Framework fournit des intégrations pour les outils de développement les plus récents, dont la compatibilité avec Red Hat OpenShift a été testée et vérifiée.

Gestion de bout en bout

Gérez votre environnement Red Hat OpenShift de manière cohérente avec une interface uniforme pour les administrateurs et les développeurs qui fonctionne dans les environnements sur site, dans le cloud et en périphérie, y compris ceux basés sur différentes distributions Kubernetes.

Prise en charge du modèle DevSecOps

Intégrez des politiques de sécurité déclaratives dans les outils et workflows de développement. Utilisez des contrôles natifs pour Kubernetes pour limiter les menaces et appliquer des politiques de sécurité qui protègent contre les risques liés à l'exploitation.



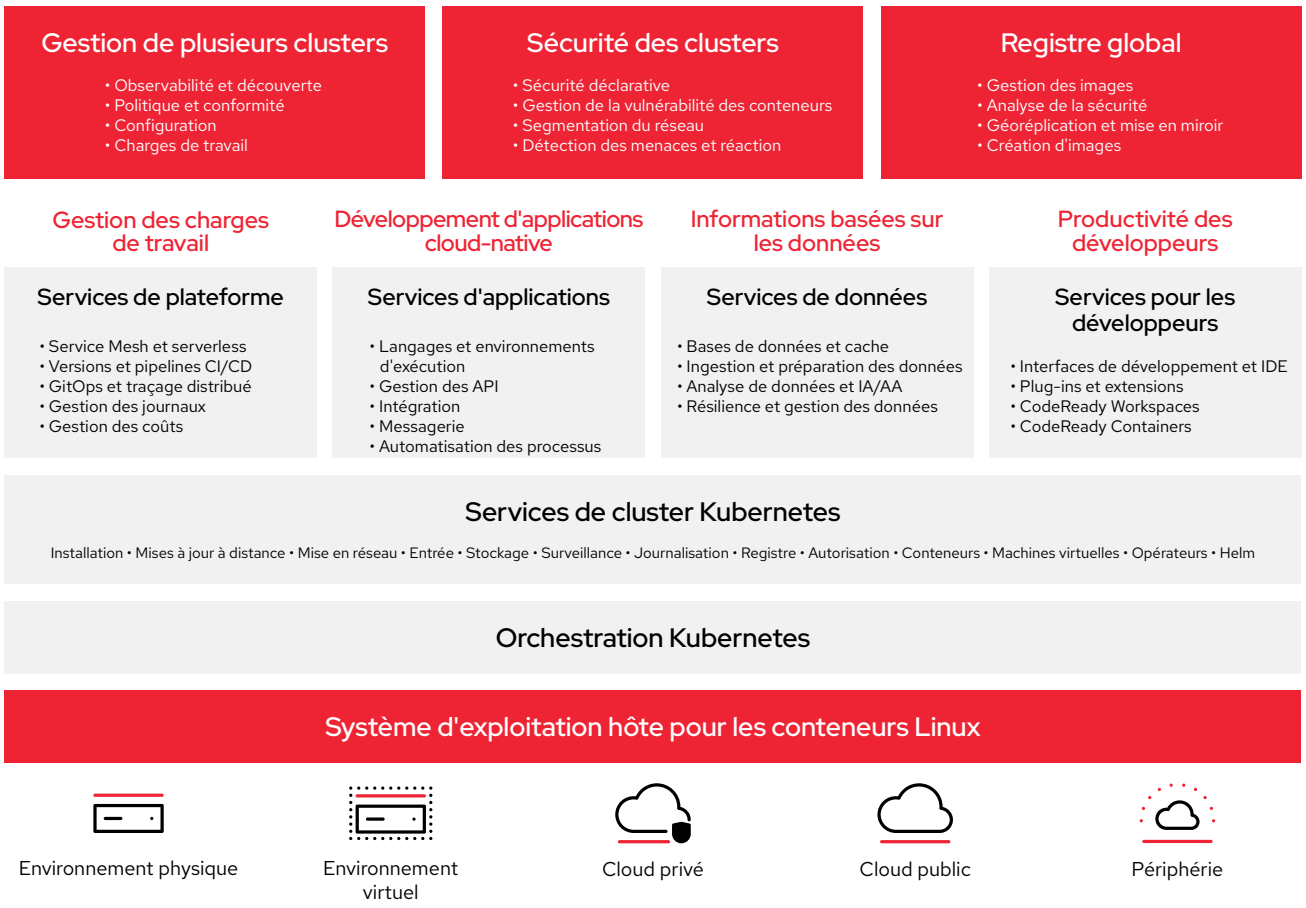
Services de données évolutifs

Rationalisez la gestion des données sur vos clusters. Grâce à la prise en charge des protocoles de données en mode fichier, bloc et objet, la solution Red Hat OpenShift Data Foundation offre un stockage persistant résilient pour les applications stateful et les services de cluster.

Capacités de mise en réseau Zero Trust

Mettez en œuvre des **réseaux Zero Trust** pour assurer des communications résilientes, sûres et observables entre les applications et les services. **Red Hat OpenShift Service Mesh** est inclus et intégré à Red Hat OpenShift pour vous aider à protéger vos communications plus facilement.

Red Hat OpenShift Platform Plus offre les technologies et les capacités nécessaires à une adoption efficace du modèle DevSecOps. Lisez le **guide de sécurité Red Hat OpenShift** pour découvrir comment Red Hat assure la sécurité dans toute la pile technologique.



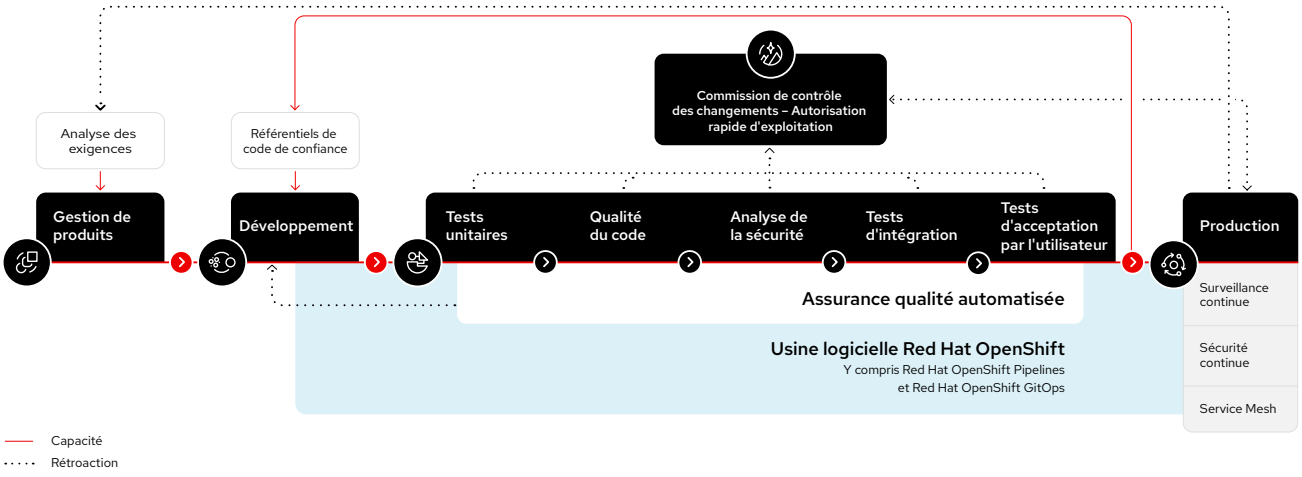
Faites vos premiers pas plus rapidement avec les services cloud Red Hat OpenShift

Les services cloud Red Hat OpenShift sont disponibles sur **AWS**, **Google Cloud**, **IBM Cloud** et **Microsoft Azure**. Vous pouvez donc choisir l'option qui correspond le mieux aux besoins de votre entreprise. Chaque service fournit des environnements complets avec tous les services nécessaires, des options en libre-service simples et l'assistance de spécialistes 24 h/24 et 7 j/7 dans le cadre de contrats de niveau de service (SLA) stricts.

Pour en savoir plus, lisez le document **En faire plus avec les services cloud Red Hat OpenShift**.

Construisez une base pour votre usine logicielle avec Red Hat OpenShift Platform Plus

La plateforme Red Hat OpenShift Platform Plus constitue une base fiable, adaptable et modulable pour votre usine logicielle. Elle vous permet d'intégrer des contrôles de sécurité dans vos pipelines CI/CD. Elle permet aussi d'automatiser la sécurité des workflows existants, de protéger les charges de travail et l'infrastructure Kubernetes contre les erreurs de configuration et la non-conformité, ainsi que de mettre en œuvre la détection et la réponse aux menaces au moment de l'exécution



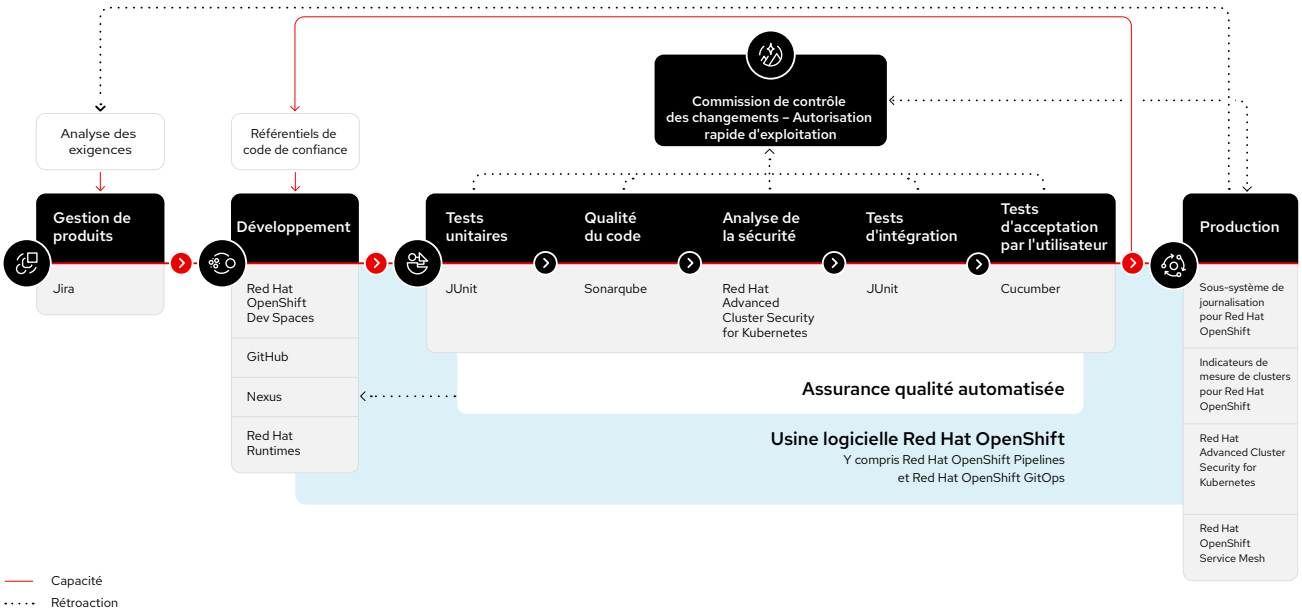
Composez des usines logicielles complètes avec un écosystème d'outils tiers

Chaque cas d'utilisation nécessite d'ajouter des outils différents à votre usine logicielle. Avec Red Hat OpenShift Platform Plus, vous pouvez composer chaque étape de votre usine logicielle en utilisant vos produits et technologies tiers préférés :

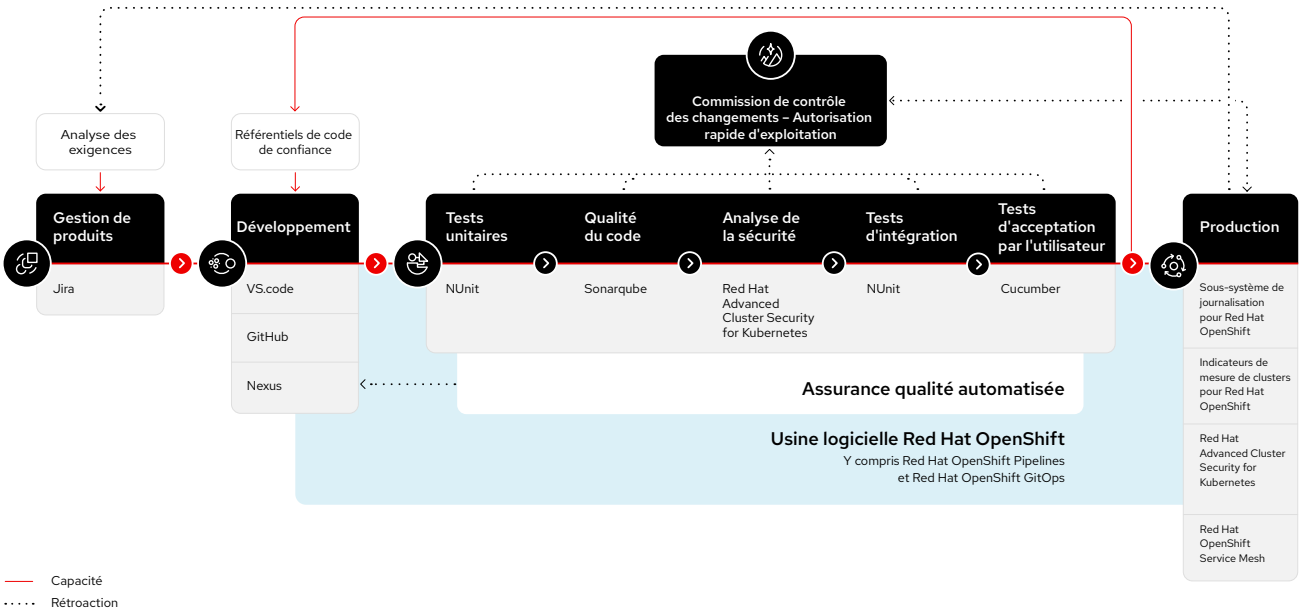
- Outils de gestion des accès privilégiés
- Autorités de certification externes
- Coffres-forts externes et solutions de gestion de clés
- Outils d'analyse du contenu des conteneurs et outils de gestion des vulnérabilités
- Outils d'analyse de l'exécution des conteneurs
- Systèmes de gestion des informations et des événements de sécurité
- Outils de gestion du contrôle de source
- Référentiels d'artéfacts
- Outils de tests logiciels

Par exemple, une usine logicielle pour le développement cloud-native d'applications Spring Boot utilisera des outils d'exécution, de création et de test différents de ceux d'une usine logicielle destinée à des applications .Net Core. Vous trouverez ci-dessous un exemple de composition pour chacune de ces deux usines logicielles qui illustre bien la flexibilité de la plateforme Red Hat.

Usine logicielle pour le développement cloud-native d'applications Spring Boot basées sur des microservices



Usine logicielle pour le développement cloud-native d'applications .Net Core basées sur des microservices



Témoignages de réussite

Snam, l'un des plus grands réseaux de gaz naturel au monde, a adopté les technologies et services Red Hat, notamment Red Hat OpenShift, Red Hat Quay et **Microsoft Azure Red Hat OpenShift**, pour favoriser la transformation numérique de l'entreprise. Snam déploie désormais des applications de manière automatisée en 30 minutes seulement, divisant ainsi par plus de 10 le délai de distribution des nouveaux logiciels. L'entreprise peut également faire évoluer les charges de travail et les applications sur n'importe quel cloud public ou privé afin de répondre aux besoins métier futurs, ce qui réduit les risques de dépendance à un cloud.

> Red Hat OpenShift est la pierre angulaire de notre projet de transformation. Cette solution nous a permis de créer une plateforme informatique efficace, performante et fiable qui simplifie la gestion des systèmes et applications complexes.

Roberto Calandrini
Directeur de l'architecture, Services numériques et IA, Snam

En savoir plus

VodafoneZiggo, l'un des principaux fournisseurs de services de communication et de divertissement pour les particuliers et les entreprises aux Pays-Bas, a déployé une plateforme de cloud hybride basée sur Red Hat OpenShift pour unifier son infrastructure d'applications. L'entreprise a également fait appel aux services de consulting Red Hat pour l'aider à adopter la méthode DevSecOps et à passer à une culture plus ouverte et collaborative. VodafoneZiggo est désormais en mesure de s'adapter plus rapidement et efficacement à l'évolution des besoins métier et de la demande du marché, dans plusieurs clouds et en périphérie du réseau.

> Nous considérons Red Hat OpenShift comme une couche cohérente pour les applications et les services cloud-native qui nous permettra d'augmenter la productivité et de proposer une innovation continue.

André Beijen
Directeur, Réseau mobile, VodafoneZiggo

En savoir plus

Adoptez le modèle DevSecOps

La vitesse, l'évolutivité et la sécurité sont essentielles dans un monde cloud-native.

Une usine logicielle basée sur Red Hat OpenShift Platform Plus vous aide à mettre en place une approche DevSecOps efficace qui accélère le développement, rationalise l'exploitation et protège votre entreprise.

Essayer gratuitement Red Hat OpenShift : cloud.redhat.com/try

En savoir plus sur Red Hat OpenShift Platform Plus : red.ht/openshift-platform-plus

F31657_0522_KVM

Red Hat