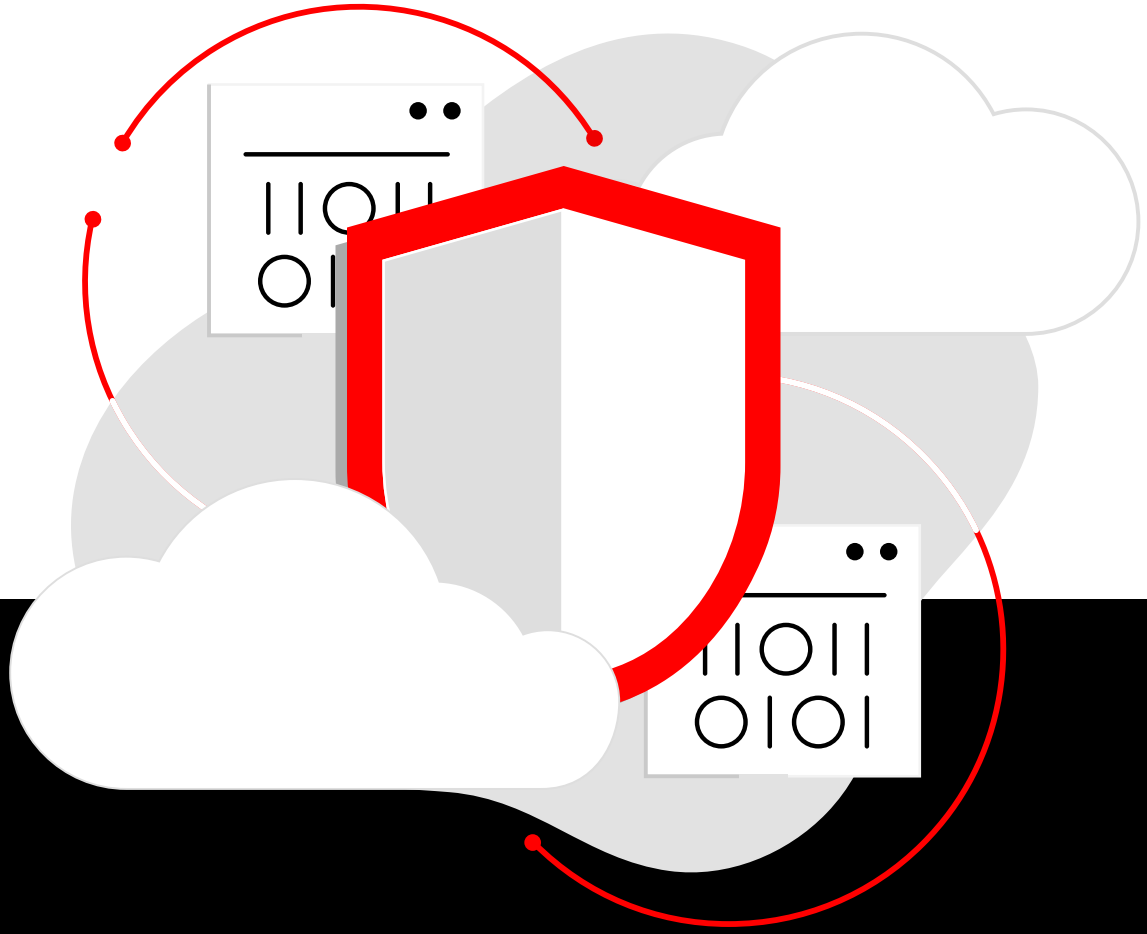
Red Hat



Modernisez et sécurisez le cycle de vie des applications grâce au DevSecOps

Sommaire

Introduction

La sécurité des applications, essentielle à l'ère du numérique

Avec le nombre croissant d'entreprises qui adoptent les technologies de cloud, conteneur et microservices afin de rester compétitives dans un monde numérique, la sécurité demeure une préoccupation majeure. En effet, 50 % des cadres supérieurs de l'informatique citent la cybersécurité comme l'une des trois principales priorités de leurs initiatives technologiques[1]. Dans le même temps, 86 % d'entre eux s'attendent à observer une accélération du rythme de la transformation numérique de leur entreprise en 2021[1].

Ces nouvelles technologies nécessitent une approche différente de la sécurité, car les stratégies classiques basées sur le périmètre sont inefficaces dans les environnements distribués. En outre, avec l'accélération des développements et la flexibilité croissante des déploiements induites par les méthodes DevOps et cloud-native, il est plus important que jamais de tenir compte de la sécurité plus tôt dans le processus. L'application de mesures de sécurité uniquement à la fin du cycle de développement a souvent pour conséquence des retards de distribution et une protection moindre.

L'adoption d'approches et de pratiques **DevSecOps** peut aider à mieux protéger l'environnement d'applications et l'entreprise.

Définition du DevSecOps

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 par toutes les équipes. Elle n'est plus juste 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.

Avantages de la méthode DevSecOps

Sécurité renforcée et risques réduits

Corrigez les problèmes de sécurité pendant le développement, plutôt qu'en phase de production, pour mieux protéger vos applications et réduire le nombre de déploiements retardés ou interrompus en raison d'échecs aux contrôles de politiques.

Problèmes de sécurité corrigés rapidement

Utilisez des pratiques et outils de sécurité modernes qui encouragent la collaboration et intègrent l'automatisation pour raccourcir les cycles de lancement, accélérer la correction des problèmes de sécurité en production, et économiser du temps et de l'argent.

Conformité et visibilité améliorées

Adoptez des processus et outils automatisés qui réduisent les risques d'erreur humaine et améliorent la prédictibilité et la reproductibilité pour améliorer la conformité et simplifier les processus d'audit.

1 *Flexera, « 2021 Flexera STATE OF TECH SPEND REPORT », janvier 2021*

Les défis de la mise en œuvre de l'approche DevSecOps

Si les approches DevSecOps offrent de nombreux avantages, plusieurs facteurs peuvent rendre difficile leur mise en œuvre.

- **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.
- **Complexité de l'environnement d'applications.** Il peut être difficile d'appréhender les connexions et implications en matière de sécurité de toutes les nouvelles technologies (conteneurs, microservices, services cloud...) qui composent les environnements d'applications d'envergure et complexes.
- **Outils et processus existants inefficaces.** Beaucoup d'équipes commencent par appliquer les outils et processus existants, mais constatent au fil du temps que cette approche dessert leurs objectifs.
- **Multiples outils de sécurité.** Le choix, le test, l'intégration et la maintenance des outils de sécurité adaptés pour l'entreprise nécessitent du temps, des recherches et des efforts permanents.

La réussite du DevSecOps repose sur la culture, les processus et les technologies

La sécurisation du cycle de vie des applications avec la méthode DevSecOps nécessite des changements et alignements dans trois domaines : la culture, les processus et les technologies.

Culture

Encouragez la collaboration et la poursuite d'objectifs communs entre les équipes de développement, d'exploitation et de sécurité. Aidez chaque équipe à comprendre les raisons et les méthodes pour intégrer la sécurité au cycle de vie des applications.

Processus

Standardisez, documentez et automatisez les processus et workflows pour renforcer l'efficacité et la sécurité tout au long du cycle de vie.

Technologies

Intégrez les plateformes, outils et processus de développement, de déploiement et d'exploitation des applications à un système unique et cohérent.

En savoir plus sur les principes de base du DevSecOps

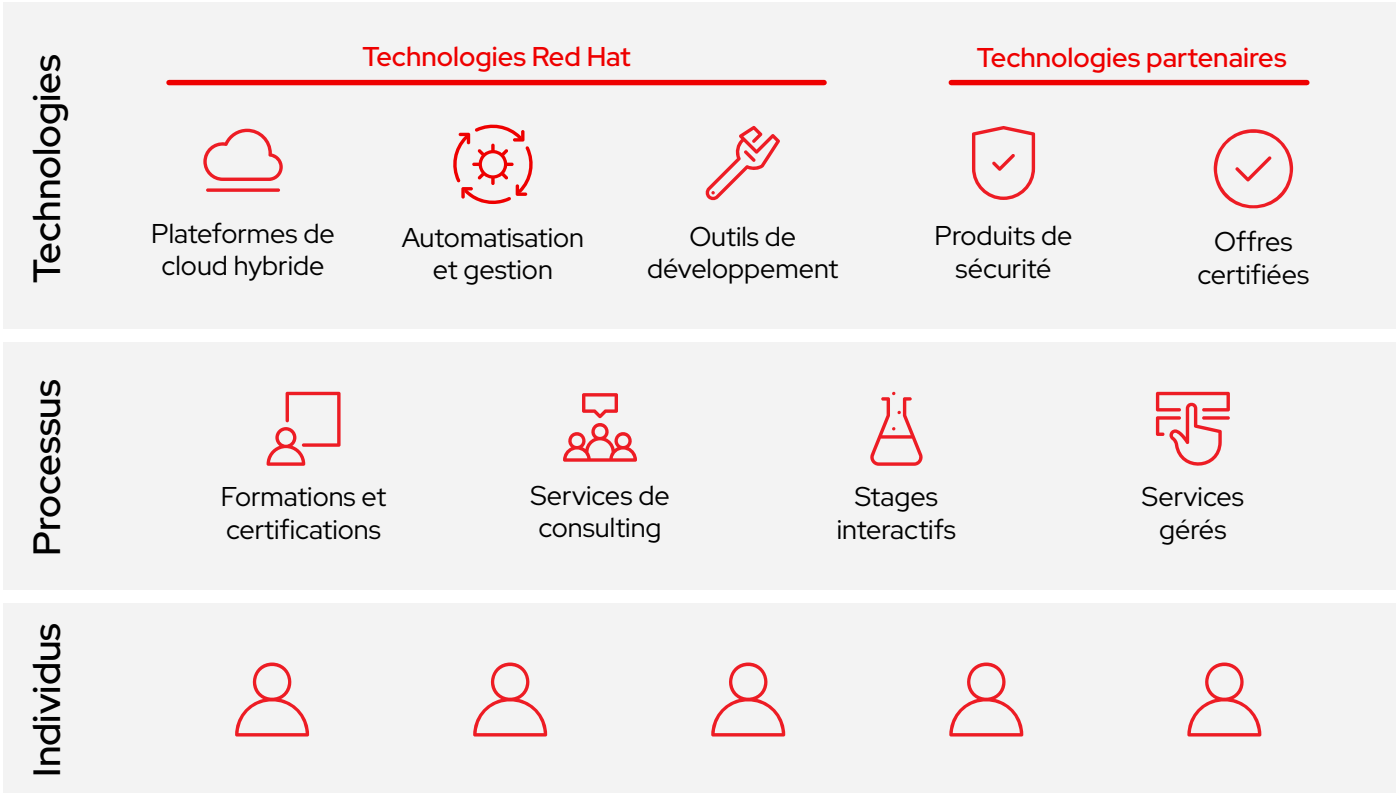
Lisez l'**article de blog Pourquoi vos pratiques ne sont pas toujours à la hauteur** pour découvrir les changements nécessaires à la réussite de la mise en œuvre de l'approche DevSecOps. Lisez le **livre numérique Renforcer la sécurité du cloud hybride** pour savoir comment protéger votre entreprise grâce aux approches de sécurité cloud-native.

La stratégie DevSecOps de Red Hat

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. Cette association vous permet de mettre en œuvre des solutions DevSecOps complètes afin de mieux protéger vos applications, réduire les risques, améliorer les performances et tirer le meilleur parti de vos investissements.

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. Nos partenaires étendent et améliorent cette base avec des produits novateurs intégrés qui permettent d'appliquer la sécurité et l'automatisation à l'ensemble du cycle de vie des applications. Enfin, pour vous aider à réussir la mise en œuvre du DevSecOps, nous proposons des **formations et certifications**, des **stages interactifs**, des **contrats de consulting** et des **offres gérées**.

Ensemble, nous répondons à vos besoins, peu importe où vous en êtes dans votre parcours vers le DevSecOps. Avec nos solutions modulaires adaptables et nos 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.



Poser des bases DevSecOps ouvertes grâce aux produits Red Hat

Red Hat OpenShift

Red Hat OpenShift® est une plateforme de cloud hybride axée sur la sécurité et adaptée aux entreprises, qui inclut des outils DevOps intégrés et des capacités de sécurité activées par défaut. Cette plateforme fonctionne avec des technologies et outils de sécurité partenaires et tiers pour optimiser la sécurité et mettre en œuvre un modèle DevSecOps robuste. Lisez le **guide de sécurité Red Hat OpenShift** pour découvrir comment nous assurons la sécurité dans toute la pile technologique.

Essayer gratuitement

Fonctions clés de sécurité

- SELinux (Security-Enhanced Linux)
- Contraintes de contexte de sécurité (SCC)
- Gestion des identités et des accès
- Chiffrement des données
- Mode FIPS (Federal Information Processing Standard)

Red Hat Ansible Automation Platform

Red Hat Ansible® Automation Platform est une plateforme flexible et puissante qui automatise et intègre les solutions de sécurité et fournit un langage commun entre vos outils de sécurité. En savoir plus sur les **cas d'utilisation de l'automatisation**.

Red Hat Enterprise Linux CoreOS

Red Hat Enterprise Linux® CoreOS est un système d'exploitation léger, immuable et optimisé pour les conteneurs qui repose sur les capacités de sécurité de Red Hat Enterprise Linux et fait partie intégrante de Red Hat OpenShift.

Red Hat Quay

Red Hat Quay est un registre d'images de conteneurs distribué et hautement disponible qui permet de créer, distribuer et déployer des conteneurs.

Red Hat CodeReady Workspaces

Red Hat CodeReady Workspaces est un outil de développement qui permet de rédiger du code et créer puis tester des applications dans des conteneurs exécutés sur Red Hat OpenShift.

Red Hat Advanced Cluster Security for Kubernetes

Red Hat Advanced Cluster Security for Kubernetes fournit une architecture cloud-native pour la sécurité des conteneurs qui protège les applications, de la création à l'exécution.

Red Hat Advanced Cluster Management for Kubernetes

Red Hat Advanced Cluster Management for Kubernetes fournit une console unique pour le contrôle des clusters et des applications, avec des politiques de sécurité intégrées.

Gagner en flexibilité et fiabilité avec un écosystème de partenaires certifiés pour la sécurité

Aucun prestataire n'est en mesure d'offrir seul toutes les capacités nécessaires à la mise en œuvre complète d'une méthode DevSecOps efficace. En outre, chaque entreprise est différente et nécessite une combinaison unique de produits et technologies pour répondre à ses besoins.

Red Hat collabore avec des **partenaires novateurs et experts de la sécurité** afin de proposer des solutions complètes basées sur des intégrations, images de conteneurs et **opérateurs Red Hat OpenShift** certifiés. Vous pouvez choisir en toute confiance et à tout moment les partenaires, produits et technologies les mieux adaptés à vos besoins, avec la certitude que ces solutions fonctionneront ensemble de manière fiable et cohérente. Nos services, notre assistance et nos formations assurés par des experts soutiennent ces solutions et vous aident dans la mise en œuvre de la culture, des processus et des outils DevSecOps.

Avantages de l'écosystème des partenaires pour la sécurité de Red Hat

Choix

Choisissez les produits et prestataires qui répondent le mieux aux besoins de votre entreprise à tout moment.

Certification

Créez votre solution en toute confiance, avec la certitude que tous les composants sont certifiés et fonctionnent ensemble de manière fiable.

Expertise

Bénéficiez de l'expertise et de l'expérience DevSecOps combinées de Red Hat et de ses partenaires.

Services

Recevez de l'aide pour la mise en œuvre de la culture, des processus et des outils DevSecOps dans votre entreprise.

Formation

Développez les meilleures pratiques et les compétences nécessaires pour adopter les approches DevSecOps.

Red Hat Vulnerability Scanner Certification

Le service Red Hat Vulnerability Scanner Certification réduit les différences entre les résultats d'analyse des vulnérabilités. Red Hat travaille avec des partenaires certifiés pour la sécurité afin de proposer des résultats d'analyse des vulnérabilités de conteneurs plus précis et fiables pour les images et les paquets publiés par Red Hat.

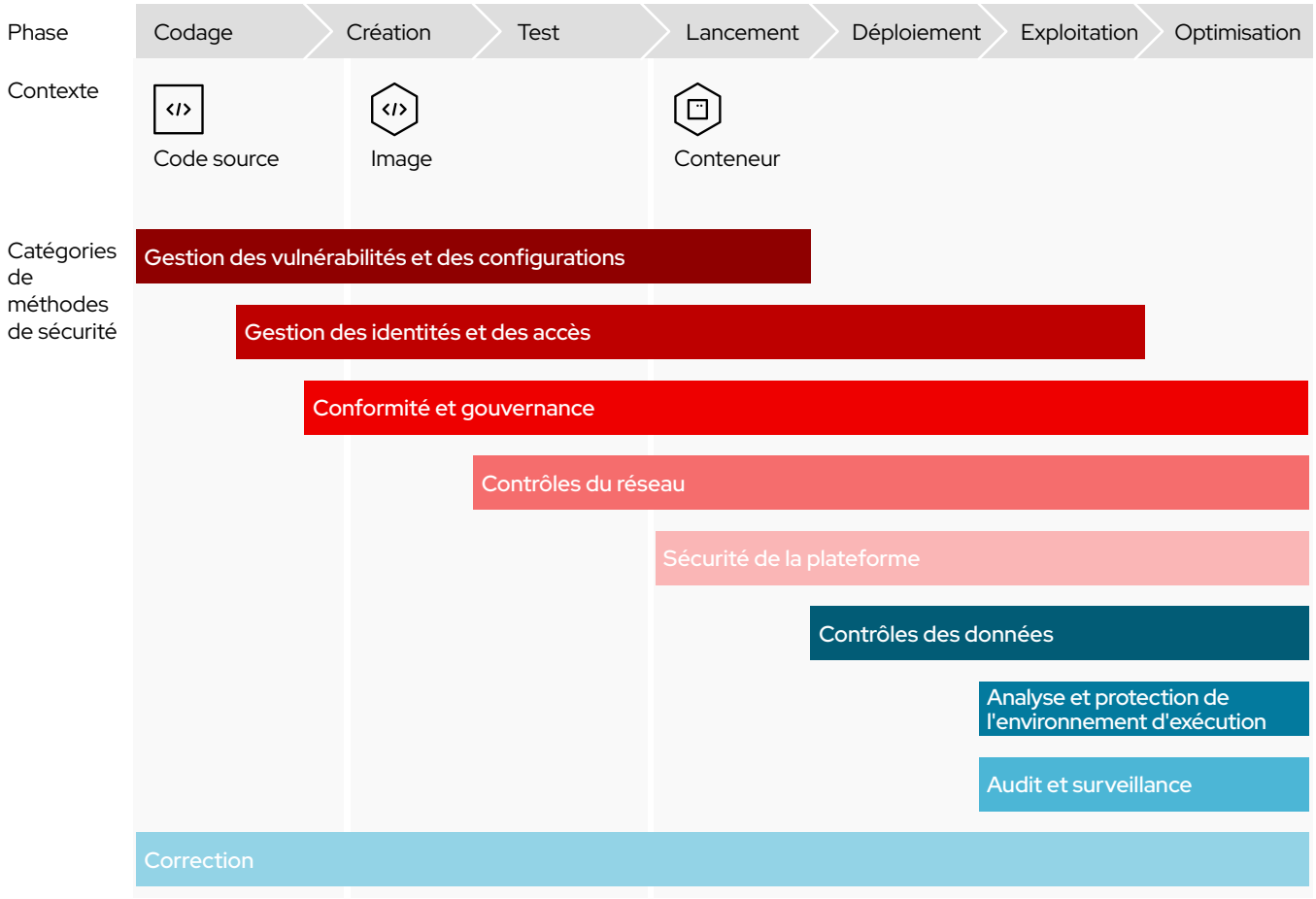
- Réduisez les faux positifs et autres différences.
- Libérez du temps et du budget pour les projets et initiatives stratégiques.
- Améliorez votre niveau d'assurance.
- Améliorez la précision avec des données centralisées pour les images publiées par Red Hat.
- Simplifiez la gestion des vulnérabilités.

Trouver des produits certifiés

Créer des solutions DevSecOps complètes

Red Hat propose un framework pour la création de solutions DevSecOps complètes, évolutives et conformes aux exigences de sécurité, dans l'ensemble du cycle de vie des applications. Conçu avec nos partenaires pour la sécurité, ce framework peut vous aider à mettre en œuvre le DevSecOps dans votre entreprise en tenant compte de vos besoins actuels et à venir.

Le framework DevSecOps de Red Hat met en correspondance un ensemble complet d'outils de sécurité et de méthodes (catégorisées par fonction) avec le cycle de vie du développement d'applications.



Lire la présentation

Choisir les méthodes et produits de sécurité adaptés à vos besoins

Le framework DevSecOps de Red Hat classe 34 méthodes de sécurité primaires en 9 catégories. Red Hat et les technologies partenaires certifiées s'alignent sur une ou plusieurs de ces méthodes pour vous aider à créer une solution DevSecOps complète qui répond aux besoins de votre entreprise et s'adapte aux changements à venir.

Gestion des vulnérabilités et des configurations

- Tests statiques de la sécurité des applications (SAST)
- Analyse statique du code (SCA)
- Tests interactifs de la sécurité des applications (IAST)
- Tests dynamiques de la sécurité des applications (SAST)
- Gestion des configurations
- Risque de l'image

Gestion des identités et des accès

- Authentification
- Autorisation
- Coffres-forts à secrets
- Boîtes noires transactionnelles (HSM)
- Provenance

Conformité et gouvernance

- Audits de la conformité réglementaire
- Contrôles de conformité et correction

Contrôles du réseau

- Plug-ins Container Network Interface (CNI)
- Politiques réseau
- Contrôle du trafic
- Service Mesh
- Visualisation
- Analyse des paquets
- Gestion des API (Application Programming Interface)

Sécurité de la plateforme

- Hôte sécurisé
- Plateforme de conteneurs
- Espace de noms
- Isolation
- Renforcement de Kubernetes et des conteneurs

Contrôles des données

- Protection et chiffrement des données

Analyse et protection de l'environnement d'exécution

- Contrôleur d'admission
- Analyse comportementale des applications
- Défense contre les menaces

Audit et surveillance

- Surveillance du cluster
- Gestion des informations et des événements de sécurité (SIEM)
- Analyses détaillées

Correction

- Plateformes d'orchestration, d'automatisation et de réponse aux incidents de sécurité informatique (SOAR)
- Résolution automatique

Trouver des partenaires certifiés

Présentation de notre partenaire

Sysdig

Sysdig aide les entreprises à exécuter en toute confiance des charges de travail dans le cloud avec des technologies DevOps axées sur la sécurité. Les produits Sysdig pour la surveillance et la sécurité des applications, des charges de travail et des conteneurs permettent à des centaines d'entreprises d'accélérer la mise sur le marché de leurs applications cloud-native.

Ensemble, Red Hat et Sysdig aident les entreprises à adopter rapidement des approches cloud-native. Les solutions **Sysdig Secure DevOps Platform**, **Sysdig Secure** et **Sysdig Monitor** fonctionnent avec Red Hat OpenShift et **Red Hat Advanced Cluster Management for Kubernetes** afin d'unifier la sécurité, la conformité et la surveillance pour les environnements de cloud privé, hybride et multicloud. Grâce à ces solutions, vous pouvez créer des pipelines sécurisés, détecter et traiter les menaces, valider en continu l'intégrité du cloud, assurer la conformité et surveiller les performances. Basées sur une pile Open Source, les capacités de surveillance, de sécurité et d'analyses détaillées cloud-native de Sysdig vous donnent le contrôle et les informations nécessaires pour migrer vers le cloud à moindre risque.

2020

Partenaire étoile montante Red Hat de l'année pour le secteur public[2]

Avec les solutions Red Hat et Sysdig, vous pouvez :

- analyser des images directement dans vos pipelines d'intégration et de déploiement continus (CI/CD) ;
- surveiller les performances et la disponibilité à l'échelle du cloud ;
- mettre en œuvre la conformité continue et la sécurité de l'environnement d'exécution ;
- valider les configurations d'infrastructure Red Hat OpenShift ;
- résoudre et traiter plus facilement les problèmes.

Gestion des risques pour la sécurité

Identifiez et corrigez les vulnérabilités dans l'ensemble des pipelines. Détectez et bloquez les menaces lors de l'exécution avec des politiques et contrôles automatisés. Traitez et analysez les incidents, même après la suppression des conteneurs.

Amélioration des performances et de la disponibilité

Interrogez et conservez des millions d'indicateurs de mesure. Surveillez l'intégrité et les performances de l'environnement pour détecter et corriger les problèmes de manière proactive. Résolvez plus facilement les problèmes dans les clusters, pods et conteneurs.

Validation de la conformité du cloud

Validez la conformité de l'environnement Red Hat OpenShift avec les normes courantes. Auditez les clusters, nœuds et conteneurs grâce à des rapports d'activité détaillés. Surveillez l'intégrité des fichiers dans l'ensemble du cycle de vie des conteneurs.

Accéder aux intégrations

2 Blog Red Hat, « **Red Hat awards North American partners for commitment to open source innovation** », 23 avril 2020

Présentation de notre partenaire

Synopsys

Synopsys fournit des solutions d'analyse de la composition logicielle statique et dynamique pour la création rapide de logiciels sécurisés. En associant des outils, services et une expertise de pointe, Synopsys permet d'optimiser la sécurité et la qualité dans l'ensemble du cycle de vie du développement de logiciels grâce à l'approche DevSecOps.

Red Hat et Synopsys vous aident à créer plus rapidement du code de qualité axé sur la sécurité, tout en réduisant les risques et en augmentant la productivité. La solution **d'analyse de la composition logicielle (SCA) Synopsys Black Duck** s'intègre à Red Hat OpenShift pour augmenter la visibilité et le contrôle sur les vulnérabilités de sécurité et les violations de politiques dans le code Open Source de vos conteneurs. **Black Duck for OpenShift** détecte, analyse, surveille et inspecte automatiquement toutes les images de conteneurs dans vos clusters Red Hat OpenShift pour identifier les risques liés à la sécurité et à la conformité du code Open Source à toutes les étapes de la création des conteneurs. Ce logiciel vous permet également de vous assurer que des conteneurs vulnérables ne passent pas en production et de réagir rapidement aux nouvelles vulnérabilités qui affectent les conteneurs en exécution.

La solution Black Duck for OpenShift :

- fournit une liste complète de tous les codes Open Source tiers dans chaque image de conteneur et annote vos pods avec des métadonnées concernant les politiques et vulnérabilités ;
- signale immédiatement les nouvelles vulnérabilités qui affectent les conteneurs, et identifie les images et conteneurs touchés ;
- comprend les ramifications et rétroportages du code Open Source et identifie les vulnérabilités corrigées le cas échéant, pour réduire le nombre de vulnérabilités exigeant une analyse ;
- **s'intègre** à Red Hat Advanced Cluster Management for Kubernetes pour garantir le déploiement cohérent des conteneurs sur l'ensemble des clusters.

Analyse automatique des images de conteneurs

Surveillance continue du code Open Source

Identification des vulnérabilités de sécurité

« Synopsys et Red Hat partagent une vision semblable de l'avenir du développement et du déploiement sécurisés des applications. Ensemble, notre objectif est d'aider les entreprises à créer de la confiance dans leurs applications conteneurisées. »

Vatsal Sonecha
Vice-président Développement commercial, Synopsys

Accéder aux intégrations

Présentation de notre partenaire

Palo Alto Networks

Palo Alto Networks conçoit des solutions novatrices pour soutenir la transformation numérique, même lorsque le rythme des changements s'accélère. L'entreprise propose une gamme de solutions qui sécurisent plus de 60 000 clients dans le monde.

Red Hat et Palo Alto Networks vous aident à protéger votre environnement avec une sécurité et une conformité cloud-native dans l'ensemble du cycle de vie du développement. **Prisma Cloud par Palo Alto Networks** fonctionne avec Red Hat OpenShift pour offrir une gestion complète du niveau de sécurité du cloud (CSPM) et une protection des charges de travail dans le cloud (CWP) pour vos déploiements. Cette solution fournit une sécurité complète du cycle de vie pour les hôtes, conteneurs et systèmes serverless, ainsi qu'une visibilité et une gouvernance sur votre niveau de sécurité.

Partenaire de Red Hat depuis

2017

Fonctions et avantages principaux

Gestion des vulnérabilités

Intégrez la sécurité du développement à la production avec la détection, la compréhension et la prévention des vulnérabilités à chaque étape du cycle de vie des applications.

Conformité

Facilitez l'application et le respect des critères CIS (Center for Internet Security), régimes de conformité externes et exigences personnalisées.

Sécurité CI/CD

Ajoutez la sécurité à vos processus d'intégration continue (CI) pour détecter et corriger les problèmes avant le déploiement en production.

Défense de l'exécution

Appliquez la sécurité à grande échelle avec l'apprentissage automatique qui crée des modèles d'exécution sur le principe du moindre privilège et d'une liste d'autorisations pour chaque version d'une application.

Sécurité des interfaces et applications web

Protégez-vous contre les menaces de la couche 7 et les **dix risques les plus critiques pour la sécurité des applications web (projet OWASP)**, sur tous vos clouds privés et publics.

Contrôle des accès

Contrôlez et surveillez les accès aux charges de travail et applications, tout en intégrant les outils existants de gestion des identités, accès et secrets.

Accéder aux intégrations

Présentation de notre partenaire

CyberArk

CyberArk applique une approche unique orientée sécurité au contrôle des accès privilégiés basé sur les identités. Ce partenaire propose des solutions complètes pour protéger les secrets et les identifiants utilisés par les individus, applications, scripts et machines dans les environnements d'entreprise, cloud et DevOps.

Ensemble, Red Hat et CyberArk vous aident à améliorer la sécurité de vos environnements de conteneurs et de vos scripts d'automatisation. Les politiques de sécurité des accès privilégiés limitent les risques en vous offrant plus de visibilité, des capacités d'audit et d'application des mesures de sécurité, et la gestion des secrets. Les produits DevSecOps de CyberArk, notamment Conjur Secrets Manager et Credential Providers, s'intègrent à Red Hat OpenShift et Red Hat Ansible Automation Platform pour protéger, assurer la rotation, surveiller et gérer les identifiants privilégiés des individus, applications, scripts et autres identités non humaines, le tout via une plateforme centralisée. Avec un point de contrôle unique pour l'ensemble de l'entreprise, vous pouvez unifier la gestion de la sécurité, réduire les vulnérabilités, limiter les surfaces d'attaque et rationaliser l'exploitation.

L'architecture modulaire vous permet de déployer chaque composant indépendamment et ainsi de protéger l'ensemble de vos environnements de cloud hybride, multicloud, conteneurs et DevOps selon vos besoins. L'authentification robuste de l'exécution et les contrôles d'accès basés sur les rôles vous apportent l'assurance que seuls les pods et conteneurs autorisés reçoivent les secrets. Avec l'intégration à Red Hat Ansible Automation Platform, il est possible d'accéder aux secrets gérés via les playbooks, ce qui élimine le besoin de saisie et rotation manuelles des secrets. L'intégration vous permet également d'automatiser la résolution des incidents de sécurité détectés.

Unification de la sécurité

Centralisez la gestion et la sécurisation des secrets et des identifiants d'accès privilégiés dans l'ensemble de l'infrastructure, en fonction des politiques.

Simplification de l'exploitation

Donnez aux développeurs et ingénieurs en automatisation les moyens nécessaires pour sécuriser, gérer et assurer la rotation des secrets et des identifiants en fonction des politiques de l'entreprise.

Amélioration de la cohérence

Protégez de manière cohérente les secrets et identifiants utilisés par les applications, scripts et individus qui accèdent aux consoles de gestion.

Regarder le webinar

Présentation de notre partenaire

Tigera

Tigera transforme la manière dont les entreprises sécurisent, observent et dépannent les déploiements de microservices et réseaux Kubernetes.

Red Hat et Tigera aident les entreprises à intégrer la sécurité aux environnements Kubernetes grâce à la gestion, l'analyse et la surveillance du trafic réseau. Certifiée pour Red Hat OpenShift, la solution **Tigera Calico Enterprise** facilite l'exploitation, l'optimisation et la protection des applications conteneurisées critiques dans l'ensemble de vos environnements cloud. L'architecture native pour Kubernetes permet de l'intégrer à l'environnement d'applications pour fournir des contrôles de sécurité détaillés et une meilleure visibilité entre les couches réseau et microservices. Cette solution s'intègre également aux outils, environnements et centres opérationnels de sécurité (SOC) existants, et offre ainsi des contrôles et capacités supplémentaires pour les charges de travail modernes. Améliorez la sécurité des applications dans vos environnements de développement, test et production grâce à un réseau à vérification systématique, des contrôles du trafic sortant, une visibilité du trafic, une défense et protection contre les menaces et des rapports automatisés d'audit de conformité.

Capacités de sécurité étendues

Protégez les applications avec les pare-feux existants, une sécurité basée sur le moindre privilège et le chiffrement du trafic inter-pods.

Visibilité réseau

Accédez aux flux de réseau pour déboguer la connectivité, chasser les menaces et automatiser les rapports de conformité.

Conformité

Surveillez la conformité des applications et envoyez des alertes en temps réel pour les charges de travail non conformes.

Accéder à l'opérateur

Présentation de notre partenaire

Aqua Security

Aqua Security aide les clients à innover et assurer la bonne marche de l'activité, en évitant les difficultés. L'entreprise fournit une automatisation de la prévention, détection et remédiation des menaces dans l'ensemble du cycle de vie des applications afin d'améliorer la sécurité sur tous les aspects de votre environnement.

Red Hat et Aqua Security vous aident à gérer et mettre à l'échelle les charges de travail cloud-native de manière plus sécurisée dans les environnements sur site, hybrides et cloud. La solution Aqua Cloud Native Security Platform s'intègre à Red Hat OpenShift pour fournir une gestion des vulnérabilités axée sur les risques, une protection de l'exécution détaillée et une assurance et conformité complètes de l'infrastructure. Elle permet aux équipes de développement, de sécurité et d'exploitation de distribuer les applications de manière plus sécurisée, de se prémunir contre les menaces lors de l'exécution, ainsi que d'évaluer et de corriger les configurations d'infrastructure d'après des contrôles de politiques.

Fonctions et avantages principaux

Prise en charge des approches DevSecOps

- Analysez le code, les configurations et les autorisations pour les images de registres Red Hat OpenShift à grande échelle.
- Hiérarchisez les vulnérabilités en fonction du risque.
- Automatisez les processus de création avec l'intégration aux pipelines CI/CD.

Protection des applications en cours d'exécution

- Détectez et limitez automatiquement les activités de conteneurs non autorisées sans perturber les applications.
- Appliquez l'immuabilité des conteneurs en identifiant et empêchant les modifications non autorisées des images standard.

Amélioration de la sécurité pour la chaîne logistique des logiciels

- Exécutez et validez les images dans des environnements de test en préproduction protégés.
- Identifiez les logiciels malveillants avancés indétectables par les outils d'analyse statiques avant le déploiement.

Préservation de la conformité de l'infrastructure

- Analysez et validez des centaines de configurations et politiques de contrôle d'après les meilleures pratiques et les critères CIS.
- Appliquez le contrôle d'accès basés sur les rôles au moyen de politiques d'assurance déclaratives basées sur Open Policy Agent (OPA).

Accéder aux intégrations

Prêt à commencer votre parcours vers le DevSecOps ?

La sécurité des applications est une nécessité pour les entreprises numériques. L'adoption d'approches DevSecOps peut aider à mieux protéger l'environnement d'applications et l'entreprise.

Red Hat propose une base technologique novatrice associée à un écosystème DevSecOps complet et une large expertise pour vous aider à réussir la mise en œuvre du DevSecOps dans l'ensemble de votre entreprise.

- Choisissez parmi un éventail d'outils et de technologies de qualité et certifiés pour répondre à vos besoins actuels et à venir.
- Apprenez les meilleures pratiques et développez vos compétences DevSecOps à l'aide de nos ressources de formation.
- Accélérez le déploiement avec nos services spécialisés et nos contrats de consulting.

En savoir plus sur la mise en œuvre du modèle DevSecOps avec Red Hat :

redhat.com/fr/partners/devsecops

© 2021 Red Hat, Inc. Red Hat, le logo Red Hat, Red Hat Enterprise Linux, Ansible et OpenShift sont des marques commerciales ou des marques déposées de Red Hat, Inc. ou de ses filiales aux États-Unis et dans d'autres pays. Linux® est la marque déposée de Linus Torvalds aux États-Unis et dans d'autres pays.

F29623_0721_KVM

Red Hat