Comment déployer une solution DevSecOps complète

La sécurisation du modèle DevOps est un exercice complexe

La sécurisation des processus DevOps est une tâche difficile en raison de l'évolution rapide des outils. De plus, les conteneurs et Kubernetes peuvent vite complexifier les environnements et les rendre vulnérables à de nouveaux vecteurs d'attaque et risques. Aussi, les équipes de développement et d'exploitation doivent intégrer la sécurité tout au long du cycle de vie des applications, afin de protéger l'infrastructure informatique essentielle et les données confidentielles tout en s'adaptant aux changements.

Notre structure DevSecOps constitue une base solide pour une solution DevSecOps complète et hautement évolutive.

Red Hat a collaboré avec ses partenaires spécialisés dans les écosystèmes de sécurité afin de créer une structure qui fournit un modèle et des bases solides pour distribuer des solutions DevSecOps qui se déploient et évoluent plus efficacement. La structure Red Hat® DevSecOps répond aux principales exigences de sécurité tout au long du cycle de vie DevOps grâce à une stratégie de défense détaillée complète. Red Hat collabore avec ses partenaires pour la sécurité afin de vous aider à réduire les risques en sécurisant les processus DevOps et en accélérant l'adoption de l'approche DevSecOps.

Les services de nos partenaires pour la sécurité (comme Anchore, Aqua, CyberArk, Lacework, NeuVector, Palo Alto Networks, Portshift, Snyk, StackRox, Synopsys, Sysdig, Thales, Tigera, Trend Micro et Tufin) s'ajoutent aux fonctionnalités de sécurité natives de Red Hat pour vous offrir des solutions DevSecOps complètes qui vous permettent d'améliorer vos niveaux de sécurité et de tirer le meilleur parti des technologies Red Hat.

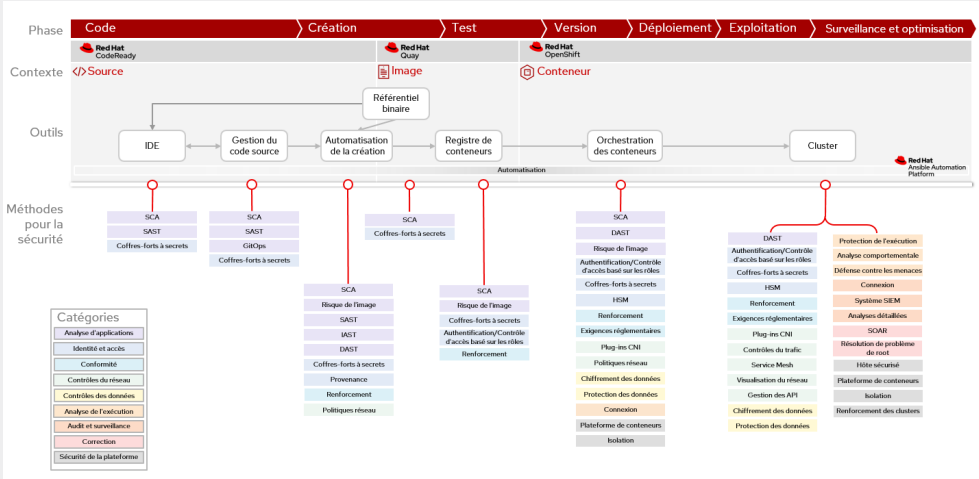

Figure 1. Structure DevSecOps

facebook.com/redhatinc
@RedHat_France
linkedin.com/company/red-hat

Notre structure complète est destinée à diverses méthodes de sécurité

La structure Red Hat DevSecOps distingue neuf catégories de sécurité et 32 méthodes et technologies qui couvrent l'intégralité du cycle de vie d'une application. Dans cette structure, nos capacités intégrées, les chaînes d'outils DevOps et les solutions de sécurité de nos partenaires représentent les points d'intégration clés du pipeline. Vous pouvez décider de mettre en œuvre toutes les méthodes et technologies d'une catégorie ou seulement une partie, en fonction de la portée de votre environnement DevOps et de vos besoins.

Sécurité de la plateforme

Il est essentiel de sécuriser votre plateforme Kubernetes. La préparation d'un tel environnement, capable de prendre en charge les applications essentielles de manière sûre, fiable et évolutive, peut représenter un véritable défi. À ce jour, le déploiement et la gestion de Kubernetes représentent toujours les deux plus grands défis des entreprises[1]. Red Hat OpenShift® est une plateforme de conteneurs Kubernetes pour les entreprises qui élimine la complexité, réduit les obstacles à l'adoption et inclut diverses fonctions de sécurité intégrées.

La structure Red Hat DevSecOps fournit des fonctions de base qui permettent de sécuriser l'hôte de conteneurs sous-jacent (Red Hat Enterprise Linux® et Red Hat CoreOS) ainsi que la plateforme de conteneurs. La plupart de nos fonctions de sécurité sont activées par défaut afin de simplifier le déploiement et de minimiser les risques. Ces fonctions vous aident à sécuriser les conteneurs aux frontières et à protéger l'hôte contre les fuites de conteneurs.

Méthodes de sécurisation de la plateforme

- Sécurité de l'hôte : cette méthode fournit des contrôles d'accès obligatoires avec SELinux, des fonctions de noyaux permettant de contrôler les appels système avec la fonctionnalité de sécurité seccomp, et des fonctions de noyaux permettant d'isoler l'utilisation du processeur, de la mémoire et d'autres ressources avec les groupes de contrôle cGroups.
- Sécurité de la plateforme de conteneurs : cette méthode fournit un environnement d'exécution de conteneurs léger avec CRI-O et un registre d'images de conteneurs sécurisé avec Quay.
- Espaces de noms Linux : cette méthode permet d'isoler les applications entre les équipes, les groupes et les services.
- Renforcement de Kubernetes et des conteneurs : cette méthode applique des normes telles que NIST 800-190 et les critères CIS (Center for Internet Security).

Analyse d'applications

Les fonctions d'analyse d'applications vous aident à identifier les vulnérabilités de votre application ainsi que d'autres problèmes de sécurité au début du cycle de vie. En déplaçant la sécurité au début du cycle de vie DevOps, vous pouvez identifier et traiter au plus tôt les vulnérabilités, et ainsi éviter les tâches répétitives par la suite.

Méthodes d'analyse d'applications

- Tests statiques de la sécurité des applications (SAST) : permettent d'analyser le code en cours de développement pour identifier les vulnérabilités et les problèmes de qualité.
- Analyse de la composition logicielle (SCA) : permet d'examiner les paquets dépendants inclus dans les applications pour identifier les vulnérabilités connues et les problèmes de licence.
- Tests interactifs (IAST) et dynamiques (DAST) de la sécurité des applications : permettent d'analyser les applications en cours d'exécution pour identifier les vulnérabilités.

---

1 *Mike Vizard : « Survey Sees Kubernetes Enterprise Adoption Gains », Container Journal (mars 2020)*

L'analyse d'applications inclut également des méthodes de sécurité telles que la gestion de la configuration GitOps ainsi que des fonctionnalités de gestion des risques liés aux images de conteneurs (comme la détection de logiciels malveillants, de secrets intégrés et de défauts de configuration).

Gestion des identités et des accès

Les méthodes de gestion des identités et des accès (IAM) s'appuient sur l'identité de l'utilisateur ou de l'application ainsi que sur les politiques définies par les administrateurs pour contrôler l'accès aux ressources, applications et données sur site et dans le cloud. Elles sont disponibles à chaque étape du cycle de vie DevOps et peuvent vous aider à vous protéger contre les accès au système non autorisés et les déplacements latéraux.

Méthodes de gestion des identités et des accès

- Contrôles liés à l'authentification et l'autorisation : vérifiez l'identité des utilisateurs et des applications, et autorisez-les à accéder à des ressources et fonctions spécifiques.
- Contrôles d'accès basés sur les rôles (RBAC) : autorisez un ensemble d'utilisateurs à accéder à des ressources ou fonctions selon leurs responsabilités, simplifiez les tâches d'administration et d'inscription, et réduisez l'accumulation de privilèges inutiles.
- Fournisseurs d'identité, coffres-forts à secrets et boîtes noires transactionnelles (HSM) : gérez et protégez vos identifiants de sécurité, clés, certificats et secrets au repos et en transit.

D'autres méthodes de gestion des identités et des accès incluent des fonctions qui permettent d'identifier la provenance et la signature des images. Vous pouvez ainsi confirmer l'authenticité des images de conteneurs et instaurer la confiance.

Conformité

Les méthodes et technologies de mise en conformité vous aident à respecter les réglementations du secteur et gouvernementales ainsi que les politiques de votre entreprise. Elles automatisent les processus de validation et de signalement tout au long du pipeline DevOps, ce qui simplifie les audits et permet d'éviter d'éventuelles amendes et poursuites judiciaires coûteuses.

Elles améliorent également votre mise en conformité grâce à divers impératifs relatifs à la confidentialité des données et la sécurité des informations, tels que :

- la norme PCI-DSS (Payment Card Industry Data Security Standard) ;
- la norme ISO 27001 (gestion de la sécurité de l'information) ;
- la loi HIPAA (Health Insurance Portability and Accountability Act) ;
- le Règlement général sur la protection des données (RGPD) de l'UE.

Contrôles et segmentation du réseau

Les méthodes de contrôle et de segmentation du réseau vous permettent de contrôler, séparer et visualiser le trafic Kubernetes. Elles vous aident à isoler les clients et à sécuriser les flux de communication entre les applications conteneurisées et les microservices.

Méthodes de contrôle et de segmentation du réseau

- Politiques de sécurité du réseau Kubernetes : permettent de contrôler les flux de trafic au niveau de l'adresse IP ou du port et peuvent être renforcées avec des fonctions de contrôle du trafic entrant et sortant des clusters ainsi que des fonctionnalités de journalisation et de visualisation du réseau.
- Mise en réseau logicielle (SDN) : fournit une infrastructure de réseau programmable et adaptable qui est approvisionnée en temps réel afin de répondre aux exigences de sécurité dynamiques et à l'évolution des besoins des entreprises.
- Service Mesh : fournit des fonctionnalités de segmentation, de visualisation du réseau, d'authentification et d'autorisation pour les applications conteneurisées et les microservices.

Contrôles des données

Les méthodes et technologies de contrôle des données aident à préserver l'intégrité des données et empêchent la divulgation de données non autorisée. Elles s'appliquent aux données au repos et en transit afin de vous aider à protéger la propriété intellectuelle ainsi que les informations confidentielles de vos clients.

Méthodes de contrôle des données

- Chiffrement des données : empêche la divulgation non autorisée de données dans les bases de données, les fichiers et les conteneurs grâce à un service de jetons et des fonctionnalités de cryptographie, de masquage de données et de gestion des clés.
- Protection des données : détecte, classe les données et effectue le suivi et l'audit des activités afin de protéger les données sensibles et d'améliorer la mise en conformité.

Analyse et protection de l'environnement d'exécution

Ces méthodes de protection de l'environnement d'exécution en production permettent de maintenir le bon fonctionnement de vos clusters en identifiant et en limitant les activités suspectes et malveillantes en temps réel.

Méthodes d'analyse et de protection de l'environnement d'exécution

- Contrôleur d'admission : agit comme un outil de surveillance Kubernetes qui régit et applique ce qui est autorisé à s'exécuter sur le cluster.
- Analyse comportementale des applications en cours d'exécution : examine l'activité du système et détecte de manière intelligente les actions suspectes ou malveillantes en temps réel.
- Autoprotection des applications en cours d'exécution (RASP) : détecte et bloque les cyberattaques en temps réel.
- Gestion des API : contrôle l'accès aux API et sécurise leur trafic.

Audit et surveillance

Les méthodes d'audit et de surveillance fournissent des informations sur les incidents de sécurité qui surviennent dans votre environnement de production. Elles indiquent le moment auquel l'événement s'est produit et décrivent sa cause probable ainsi que son impact. Cela vous permet d'améliorer votre niveau de visibilité et d'accélérer la résolution des incidents.

Ces méthodes incluent ce qui suit :

- Gestion des informations et des événements de sécurité (SIEM) : cette méthode centralise les rapports sur les événements en consolidant les données des journaux et des flux réseau à partir des appareils distribués, des points de terminaison et des applications.
- Analyses détaillées : cette méthode présente des informations sur les failles de sécurité, fournit des preuves dans le cadre des audits de conformité et accélère les efforts de récupération.

Correction

Ces méthodes permettent de prendre automatiquement des mesures correctives lorsque des incidents de sécurité surviennent en production. Elles vous permettent d'améliorer votre taux de disponibilité et d'éviter d'éventuelles pertes de données.

Méthodes de correction

- Plateformes d'orchestration, d'automatisation et de réponse aux incidents de sécurité informatique (SOAR) : automatisent les actions et s'intègrent à d'autres outils de sécurité pour résoudre les incidents.
- Résolution de problème de root : permet de résoudre automatiquement les problèmes liés à des erreurs de configuration et au non-respect des politiques de Kubernetes.

Conclusion

La structure Red Hat DevSecOps constitue une base fiable et évolutive qui vous aide à étendre la sécurité DevOps et à réduire les risques. Avec l'aide de nos partenaires de sécurité, nous vous offrons les technologies dont vous avez besoin pour simplifier et accélérer votre mise en œuvre de DevSecOps. Contactez-nous pour en savoir plus.

À PROPOS DE RED HAT

Premier éditeur mondial de solutions logicielles Open Source pour les entreprises, Red Hat s'appuie sur une approche communautaire pour proposer des technologies Linux, de cloud hybride, de conteneur et Kubernetes fiables et performantes. Red Hat aide ses clients à intégrer des applications nouvelles et existantes, à développer des applications natives pour le cloud, à standardiser leur environnement sur son système d'exploitation leader sur le marché ainsi qu'à automatiser, sécuriser et gérer des environnements complexes. Red Hat propose également des services d'assistance, de formation et de certification primés qui lui ont valu le titre de conseiller de confiance auprès des entreprises du Fortune 500. Partenaire stratégique des prestataires de cloud, intégrateurs système, fournisseurs d'applications, clients et communautés Open Source, Red Hat aide les entreprises à se préparer à un avenir toujours plus numérique.

facebook.com/redhatinc
@RedHat_France
linkedin.com/company/red-hat

EUROPE, MOYEN-ORIENT ET AFRIQUE (EMEA)
00800 7334 2835
europe@redhat.com

FRANCE
00 33 1 4191 2323
fr.redhat.com

fr.redhat.com
#F26043_1220