Renforcer la sécurité du cloud hybride

Protégez votre entreprise en tenant compte de questions essentielles sur la sécurité cloud-native

/Relevez tous les défis

Red Hat

Par Lucy Huh Kerner, directrice, stratégie globale et représentation pour la sécurité, Red Hat

Sommaire

Chapitre 1

Déployer un cloud hybride centré sur la sécurité

L'adoption du cloud est de plus en plus courante et recherchée. À l'heure actuelle, 65 % des entreprises estiment avoir une utilisation intensive du cloud et 72 % disposent d'une stratégie de cloud hybride[1].

Le cloud hybride est une forme d'architecture informatique qui offre un certain degré de portabilité, d'orchestration et de gestion des charges de travail entre au moins deux environnements connectés, mais séparés, y compris des environnements bare metal, des environnements virtualisés, un cloud privé et un cloud public. Avec une architecture de cloud hybride, vous pouvez exécuter les charges de travail dans tout type d'environnement connecté, tout en déplaçant et en utilisant indifféremment les ressources de chacun de ces environnements.

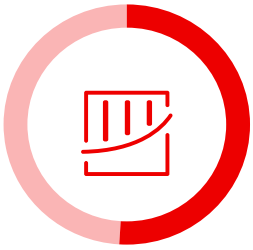
Les entreprises utilisent des environnements de cloud hybride pour :

- Connecter une infrastructure, des plateformes, des applications et des outils de différents fournisseurs.
- Améliorer l'efficacité et l'évolutivité.
- Réduire les coûts.
- Augmenter l'agilité.
- Optimiser le placement des données.

[1] Flexera, « 2023 State of the Cloud Report », mars 2023.

Quel que soit votre état d'avancement en matière de cloud hybride, la sécurité constitue une préoccupation majeure. En effet, 79 % des entreprises déclarent que la sécurité est un problème[1]. Dans un cloud hybride, les vulnérabilités résultent souvent d'une perte de visibilité et de contrôle sur les ressources : utilisation non autorisée du cloud public, manque de visibilité sur les ressources, suivi des modifications inadapté, mauvaise gestion des configurations, contrôle d'accès inefficace, erreur humaine, etc. Des utilisateurs non autorisés peuvent exploiter ces failles pour accéder à des données sensibles et des ressources internes, avec des implications financières potentiellement lourdes.

À l'échelle mondiale, le coût moyen d'une fuite de données a atteint le chiffre record de **4,45 millions de dollars** en 2023, la perte d'activité représentant **29,2 %** de ce coût[2].



51 %

des entreprises prévoient d'investir davantage dans la sécurité après avoir connu une faille[2].

[1] Flexera, « 2023 State of the Cloud Report », mars 2023
[2] IBM Security, « Rapport 2023 sur le coût d'une violation de données », 2023

En 2023, le coût moyen par donnée qui fait l'objet d'une fuite et le temps nécessaire pour stopper les fuites ont tous deux augmenté[2]. Vous pouvez répondre à ces problématiques en déployant un cloud hybride sécurisé, grâce à des méthodes qui tiennent compte des différences entre les architectures cloud et sur site. Ce livre numérique propose de nouvelles approches et réflexions pour la sécurité du cloud hybride.

277 jours

en moyenne pour identifier et stopper une fuite de données en 2023[2]

1,02 million de dollars

économisés si la faille peut être identifiée et corrigée en 200 jours ou moins[2]

[2] IBM Security, « Rapport 2023 sur le coût d'une violation de données », 2023

Chapitre 2

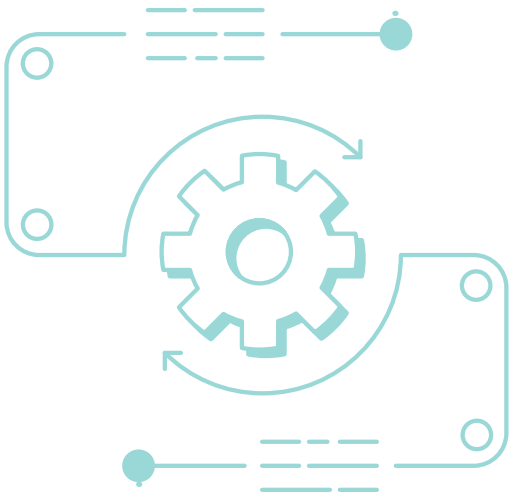
Considérer la sécurité comme un processus plutôt qu'un produit

Un dispositif de sécurité efficace nécessite une démarche globale qui implique à la fois les individus, les processus et les technologies. En effet, il ne suffit pas de déployer des produits centrés sur la sécurité pour protéger votre infrastructure, votre cloud ou votre activité. Il faut également mettre en place des stratégies et des processus de sécurité qui optimisent les fonctionnalités des produits et réduisent les risques.

À mesure que les technologies, menaces et besoins évoluent, vous pourrez adapter ces stratégies et processus. Dans un environnement de cloud hybride au périmètre non défini, vous devez gérer la sécurité différemment, car les approches traditionnelles ne sont pas efficaces.

La gestion centralisée des identités et le contrôle des accès sont des éléments clés des approches de sécurité tournées vers le cloud. Ils appliquent le principe du moindre privilège pour autoriser uniquement les accès dont les utilisateurs ont besoin. Cette démarche suppose un audit des droits d'accès actuels de chaque utilisateur suivi d'une réévaluation afin de déterminer le niveau d'accès approprié pour chacun.

La sécurité du cloud hybride nécessite également une stratégie de défense en profondeur par couche qui utilise les capacités de chaque couche de votre environnement, notamment les systèmes d'exploitation, les plateformes de conteneurs et les outils d'automatisation.



Système d'exploitation

Cherchez des outils intégrés qui vous permettront de répondre aux exigences de conformité en matière de sécurité, de mettre en œuvre des mécanismes de sécurité physiques, de renforcer la sécurité du réseau, de contrôler l'accès des utilisateurs, d'isoler les processus et d'améliorer la sécurité des données. Voici quelques exemples de ces outils : OpenSCAP, USBGuard, Security-Enhanced Linux® (SELinux), la gestion des identités et la technologie NBDE (Network Bound Disk Encryption).

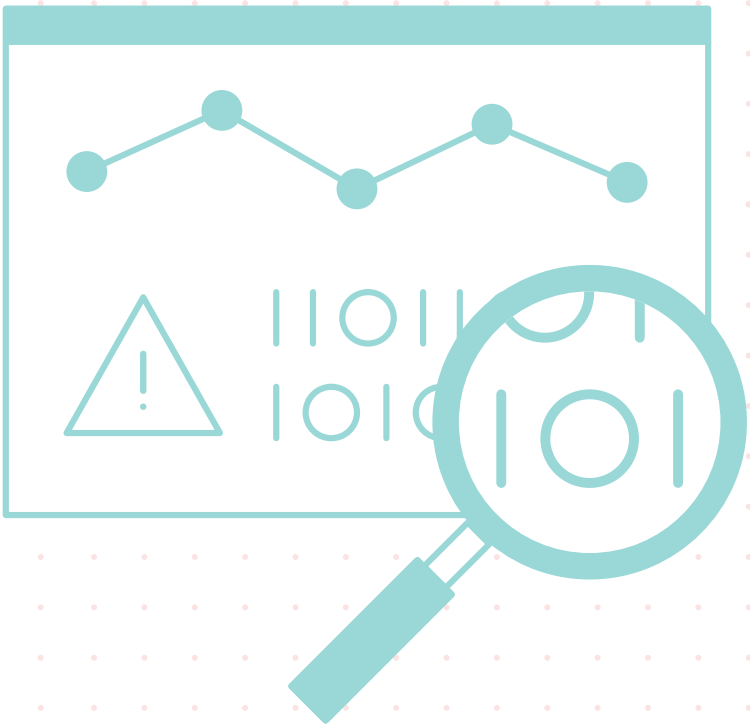
Plateforme de conteneurs

Utilisez les capacités intégrées à votre plateforme et à Kubernetes pour améliorer la sécurité des conteneurs. Voici quelques exemples : politiques de sécurité des pods, contrôles du trafic réseau, contrôles des entrées et sorties des clusters, contrôle d'accès basé sur les rôles, gestion intégrée des certificats et microsegmentation du réseau.

Outils d'automatisation

Choisissez un langage et une plateforme d'automatisation que tous vos salariés peuvent apprendre et utiliser, en particulier les équipes de développement, d'exploitation informatique, de sécurité et de conformité. Recherchez des fonctionnalités de contrôle d'accès, de journalisation et d'audit.

De plus, il est essentiel de revoir vos processus et outils de sécurité existants. Vérifiez que vous utilisez toutes les fonctions disponibles et déterminez si certains paramètres peuvent être modifiés ou reconfigurés afin de fournir une meilleure protection ou si vous devez mettre en place de nouveaux processus et outils.



1. Dressez un inventaire de vos outils et ressources informatiques.
2. Documentez vos systèmes de sécurité et vos architectures réseau, vos politiques de cybersécurité, vos processus de travail, ainsi que les compétences qui vous manquent.
3. Établissez un modèle de menace et établissez vos stratégies de tolérance et de limitation des risques face aux failles de sécurité informatique.
4. Évaluez vos architectures, politiques et processus pour identifier les possibilités d'amélioration.
5. Évaluez vos outils et ressources actuels pour déterminer s'ils peuvent prendre en charge vos nouveaux processus et stratégies. Planifiez et documentez la manière dont vous allez traiter les failles de sécurité.

Les sections suivantes traitent des éléments clés à prendre en compte pour assurer la sécurité du cloud hybride et propose des conseils pour améliorer votre protection.

Chapitre 3

Question de sécurité 1

Poser des bases solides

Pourquoi est-ce important ?

Si vos charges de travail sont réparties dans plusieurs environnements ou si vous utilisez des technologies Open Source non vérifiées, les vulnérabilités ne seront pas forcément faciles à localiser. Par ailleurs, l'absence d'une base de sécurité solide peut complexifier la mise en place d'un système multi-couche pour réduire les risques. L'utilisation de logiciels Open Source directement téléchargés auprès de communautés en amont peut compromettre la sécurité et vous exposer aux attaques contre la chaîne d'approvisionnement qui exploitent les faiblesses des services et logiciels tiers pour atteindre leur cible finale. Ces attaques prennent des formes multiples, telles que le piratage de mises à jour logicielles pour injecter du code malveillant dans un logiciel approuvé. Ces trois dernières années, les attaques contre la chaîne d'approvisionnement des logiciels ont augmenté de 742 % par an en moyenne[3]. Il est donc essentiel de disposer d'une base stable, unifiée et sécurisée pour protéger votre activité.

Recommandations et meilleures pratiques

Atténuez les risques pour la sécurité de la chaîne d'approvisionnement des logiciels en optant pour les solutions d'un fournisseur Open Source fiable comme Red Hat, qui offre aux entreprises une assistance tout au long du cycle de vie de ses logiciels. Lors du développement, un tel fournisseur suit un processus de sécurité strict pour la chaîne d'approvisionnement des logiciels, qui comprend la sélection de logiciels Open Source pour le compte de ses clients. Ces derniers sont donc sûrs d'utiliser des solutions sécurisées, résilientes et dignes de confiance.

En outre, il est fortement recommandé d'exécuter les applications essentielles sur une plateforme qui intègre des fonctionnalités de sécurité. Les clients disposent ainsi d'un niveau de sécurité de base suffisant pour exécuter ces applications en toute confiance, ajouter des fonctionnalités de sécurité multi-couche pour réduire les risques, et mettre en œuvre des systèmes automatisés pour la sécurité et la conformité.

Choisissez une base sécurisée pour vos applications et processus en optant pour un système d'exploitation fiable et résilient qui offre une stabilité et une sécurité accrues, comme Red Hat® Enterprise Linux®. Grâce à cette base stable, il est possible de faire évoluer des applications essentielles en toute confiance, d'assurer la conformité de la sécurité et de déployer des technologies émergentes de manière cohérente, que ce soit sur des systèmes bare metal, dans des environnements virtuels, dans des conteneurs ou dans tous types de clouds.

[3] Sonatype, « 9th Annual State of the Software Supply Chain », 2023

Une grande partie de la gamme Red Hat repose sur **Red Hat Enterprise Linux**, le système d'exploitation fiable choisi par de nombreuses entreprises pour ses fonctionnalités de sécurité intégrées.

Avec Red Hat Enterprise Linux, vous pouvez :

Éviter d'exposer des données et des systèmes grâce à des fonctionnalités de sécurité intégrées telles que l'application de correctifs sur le noyau. Les correctifs de sécurité sont appliqués sans redémarrage ni interruption de l'exécution. Profitez également d'autres fonctionnalités de sécurité intégrées, comme des listes d'applications autorisées qui spécifient un index d'applications approuvées ou de fichiers autorisés à être exécutés sur un système par un utilisateur particulier, ou SELinux pour contrôler plus précisément les fichiers, les processus, les utilisateurs, les applications et plus encore.

Automatiser la protection des données à grande échelle et assurer leur sécurité au fil du temps avec des fonctionnalités intégrées telles que la technologie NBDE, qui permet d'automatiser le déverrouillage des systèmes chiffrés sans gérer de clés de chiffrement. Appliquées à l'ensemble du système, les politiques de chiffrement offrent de nombreux autres avantages, notamment garantir la sécurité des données et la conformité avec des paramètres de chiffrement cohérents et personnalisables qui répondent aux exigences des politiques spécifiques à votre site.

Répondre aux exigences de conformité et rationaliser les audits. Red Hat Enterprise Linux intègre des capacités de vérification et de correction de la conformité avec OpenSCAP, afin d'analyser la configuration et les vulnérabilités d'un système local pour valider sa conformité avec dde nombreuses normes de sécurité du secteur.

Les produits tels que **Red Hat OpenShift** exploitent l'approche de sécurité offerte par la base Red Hat Enterprise Linux sur laquelle ils sont exécutés pour protéger autant que possible les conteneurs et Kubernetes. Les fonctionnalités de sécurité Red Hat s'étendent sur toute la pile, jusqu'aux composants Kubernetes. **Red Hat Ansible Automation Platform** fonctionne sur le même principe, avec des capacités intégrées grâce auxquelles les entreprises automatisent la sécurité et la conformité à grande échelle.

Étapes stratégiques

Suivez ces étapes pour sécuriser votre cloud hybride :

Passez aux versions commerciales

Remplacez vos logiciels Open Source obtenus directement à partir des projets communautaires par des versions commerciales fiables. Ces versions sont testées et validées pour réduire le risque de bogues et de vulnérabilités. Elles incluent parfois un service d'assistance aux entreprises qui distribue rapidement les correctifs de sécurité requis et vous aide à configurer votre logiciel de manière sécurisée. En adoptant les logiciels d'un fournisseur de solutions Open Source d'entreprise fiable, vous savez qu'ils sont développés selon un processus strict de sécurisation de la chaîne d'approvisionnement des logiciels, et qu'une assistance aux entreprises est offerte tout au long de leur cycle de vie. Les entreprises peuvent ainsi utiliser des logiciels Open Source tout en minimisant les risques pour la sécurité.

Choisissez une plateforme qui intègre des fonctions de sécurité

Il est essentiel d'opter pour une plateforme (un système d'exploitation, une plateforme d'applications conteneurisées ou une plateforme d'automatisation) qui intègre des fonctionnalités de sécurité. Les clients disposent ainsi d'un niveau de sécurité de base suffisant pour exécuter ces applications en toute confiance, ajouter des fonctionnalités de sécurité multi-couche pour réduire les risques, et mettre en œuvre des systèmes automatisés axés sur la sécurité et la conformité à grande échelle.

Mettez en œuvre la sécurité sur l'ensemble de la pile technologique

Après avoir posé les bases de la sécurité, assurez-vous que les couches de technologies qui s'y ajoutent bénéficient du même niveau de sécurité et qu'elles s'associent pour former une sécurité multi-couche.

Chapitre 4

Question de sécurité 2

Mettre en œuvre une chaîne d'approvisionnement des logiciels fiable avec l'approche DevSecOps

Pourquoi est-ce important ?

En 2023, 12 % des fuites de données résultaient d'une attaque contre la chaîne d'approvisionnement des logiciels[2]. L'utilisation de logiciels Open Source non vérifiés et directement téléchargés auprès de communautés en amont peut causer des vulnérabilités et vous exposer aux attaques contre la chaîne d'approvisionnement qui exploitent les faiblesses des services et logiciels tiers pour atteindre leur cible finale. Ces attaques prennent des formes multiples, telles que le piratage de mises à jour logicielles pour injecter du code malveillant dans un logiciel approuvé.

Les approches de sécurité compartimentées génèrent souvent des failles de sécurité ainsi qu'une redondance des tâches parce que la sécurité n'est pas intégrée dès le départ aux processus de développement des applications et de déploiement des infrastructures. Avec l'accélération des développements et l'augmentation de la flexibilité des déploiements, il est plus important que jamais de tenir compte de la sécurité tout au long du processus.

Recommandations et meilleures pratiques

Pour adopter une approche axée sur la sécurité de la chaîne d'approvisionnement des logiciels, vous devez cultiver un état d'esprit DevSecOps. C'est ainsi que les équipes de développement d'applications, d'exploitation informatique et de sécurité peuvent collaborer pour sécuriser la chaîne d'approvisionnement tout au long du cycle de développement logiciel et du cycle de vie de l'infrastructure, en s'appuyant sur une base Open Source renforcée pour les entreprises dans le cloud hybride.

[2] IBM Security, « Rapport 2023 sur le coût d'une violation de données », 2023

L'approche DevSecOps automatise l'intégration de la sécurité à chaque étape du cycle de développement logiciel, de la conception initiale, à l'intégration, aux tests, au déploiement et jusqu'à la distribution.

En adoptant un processus DevSecOps, vous pouvez :

- Aider les équipes informatiques et de sécurité à relever les défis liés au personnel, aux processus et aux technologies.
- Améliorer l'efficacité, la cohérence, la reproductibilité et la collaboration.
- Réduire les risques, notamment en évitant les erreurs humaines.

Avec le modèle DevSecOps, la sécurité devient une responsabilité partagée, intégrée du début à la fin. En lieu et place d'une équipe déconnectée qui serait seule responsable de la définition des politiques de sécurité, les équipes de sécurité, de développement et d'exploitation travaillent main dans la main et partagent la visibilité, les commentaires, les leçons à retenir et les informations importantes dont elles bénéficient. Pour plus de protection, le modèle DevSecOps permet d'intégrer les processus de sécurité dès le début du développement de l'application et du déploiement de l'infrastructure.

Les équipes de développement d'applications qui créent des fonctionnalités logicielles pour leur entreprise doivent à la fois renforcer leur posture de sécurité et réduire leur charge cognitive. Elles doivent mettre en œuvre la sécurité tout au long du cycle de développement logiciel : à l'étape de codage, en intégrant des vérifications de sécurité pour repérer les problèmes dès le départ et limiter les temps d'arrêt prolongés, à l'étape de création, en protégeant les systèmes grâce à des workflows d'intégration et de distribution continues (CI/CD) sécurisés, et aux étapes de déploiement et d'exécution, en utilisant des modèles de référence, des analyses de vulnérabilité, des signatures d'artéfact, des attestations, des analyses de provenance, des mécanismes de contrôle de l'application des politiques et des nomenclatures logicielles.

Votre stratégie doit également comprendre des mesures pour garantir que les technologies Open Source utilisées par vos équipes sont issues de sources fiables, mises à jour en continu de façon automatisée et configurées pour favoriser la sécurité. D'autre part, vous devez encourager l'utilisation des offres Open Source professionnelles qui comprennent une assistance aux entreprises tout au long de leur cycle de vie.

En optant pour des offres Open Source adaptées aux entreprises comme celles de Red Hat, vous bénéficiez du fruit de plus de 30 ans d'expérience dans la sécurisation de la chaîne d'approvisionnement de logiciels Open Source. Par ailleurs, les entreprises ont besoin de solutions qui facilitent le déploiement, la gestion et la sécurisation de leurs clusters Kubernetes, ainsi que d'une méthode unifiée pour créer, moderniser et déployer des applications à grande échelle en toute sécurité.

Red Hat OpenShift Platform Plus est une plateforme unifiée qui inclut Red Hat OpenShift, Red Hat Advanced Cluster Security for Kubernetes, Red Hat Advanced Cluster Management for Kubernetes, Red Hat Quay et Red Hat OpenShift Data Foundation. Elle aide les entreprises à créer, moderniser et déployer de manière sûre des applications Kubernetes conteneurisées à grande échelle. La sécurité, la conformité et la gestion des données et des applications sur plusieurs clusters sont assurées pour garantir la cohérence de la chaîne d'approvisionnement des logiciels.

Étapes stratégiques

Essayez de suivre ces étapes pour mettre en œuvre des pratiques DevSecOps et renforcer la sécurité de la chaîne d'approvisionnement des logiciels :

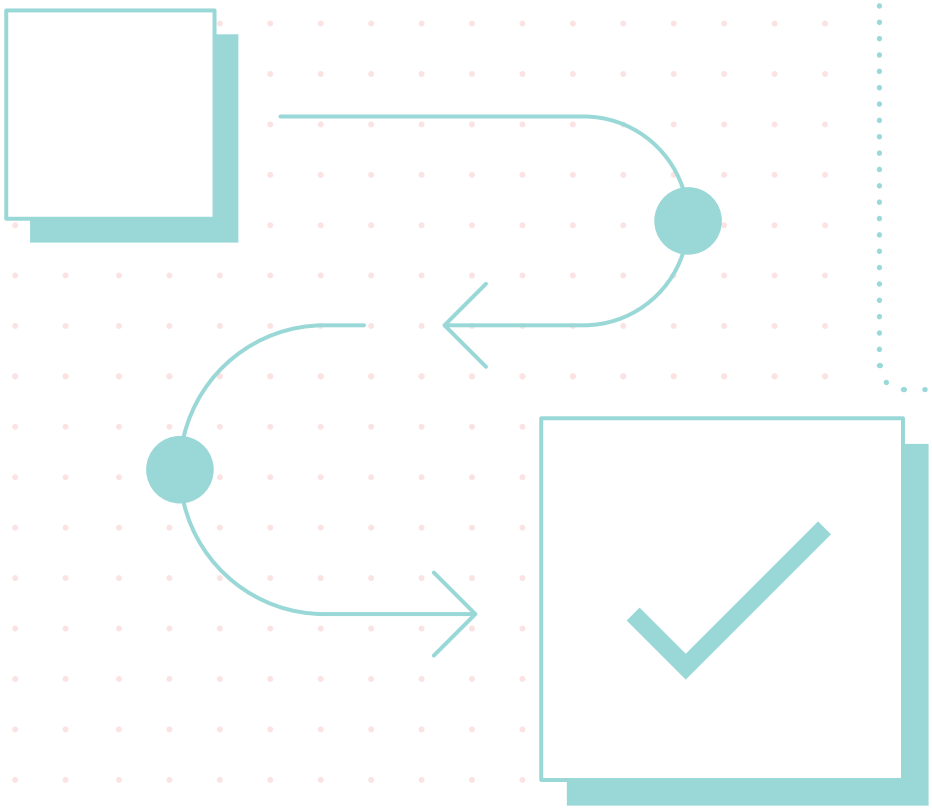
Commencez à petite échelle et évoluez. Pour commencer, choisissez un seul projet. Encouragez l'expérimentation et l'amélioration continue par itération pour ajuster précisément et optimiser vos processus. Valorisez les réussites et mettez en lumière les bénéfices démontrés au sein de votre entreprise.

Établissez des objectifs et un calendrier clairs et consensuels. La transparence joue un rôle central. Assurez-vous que toutes les personnes concernées comprennent et approuvent les objectifs et le calendrier du projet.

Diversifiez les compétences de vos équipes.
Établissez des parcours de formation sur la sécurité, l'infrastructure et le développement qui seront régulièrement mis à jour et mis à disposition de tous les membres de l'équipe.

Créez un groupe de travail sur la sécurité.
Rassemblez une équipe interdisciplinaire intégrée pour définir des cas d'utilisation et des stratégies de sécurité. Apprenez de vos pairs. Exploitez les découvertes d'autres entreprises.

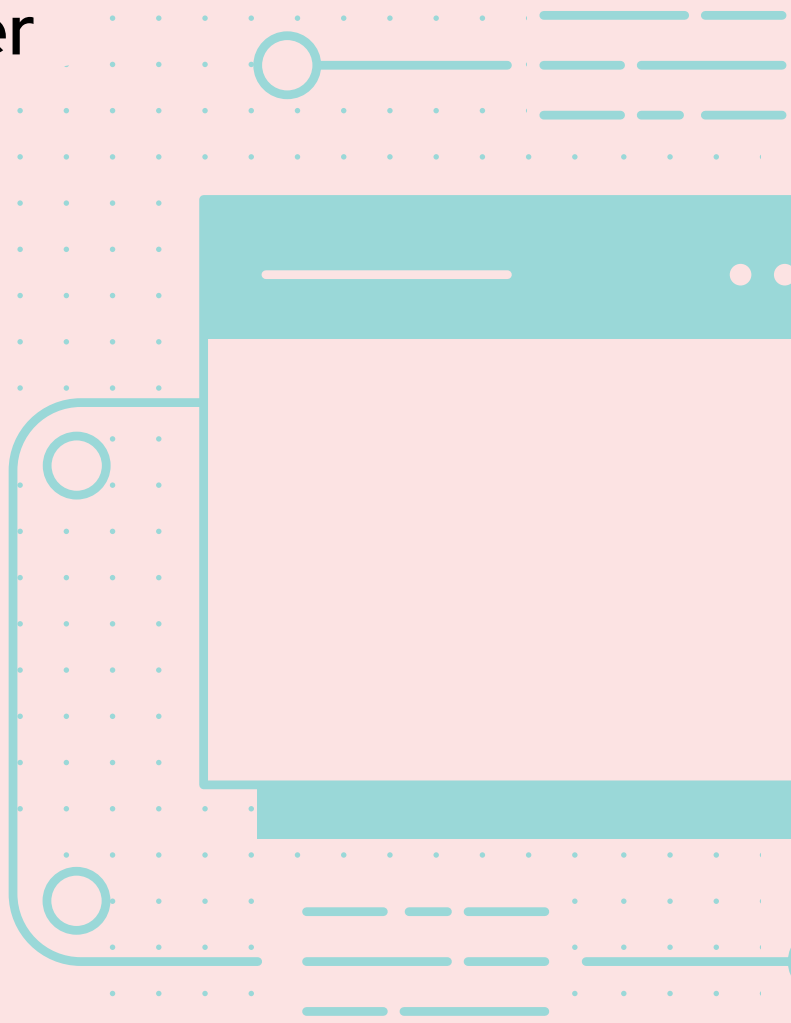
Mettez en œuvre la sécurité tout au long du cycle de développement logiciel sur une plateforme d'applications unifiée.
Il faut mettre en œuvre la sécurité tout au long du cycle de développement logiciel : à l'étape de codage, en intégrant des vérifications de sécurité pour repérer les problèmes dès le départ et limiter les temps d'arrêt prolongés, à l'étape de création, en protégeant les systèmes grâce à des workflows CI/CD sécurisés, et aux étapes de déploiement et d'exécution, en utilisant des modèles de référence, des analyses de vulnérabilité, des signatures d'artéfact, des attestations, des analyses de provenance, des mécanismes de contrôle de l'application des politiques et des nomenclatures logicielles.



Chapitre 5

Question de sécurité 3

Utiliser des solutions d'automatisation et de gestion pour protéger le cloud hybride



Pourquoi est-ce important ?

Les erreurs de configuration ou un suivi des modifications inadapté constituent une menace majeure pour la sécurité[4]. Les erreurs de configuration accroissent la vulnérabilité des systèmes aux attaques. Le suivi des modifications est capital pour savoir qui a modifié les configurations et à quel moment, et pour identifier les éléments modifiés tout au long du cycle de vie des systèmes.

L'automatisation, la gestion et l'intelligence artificielle (IA) vous aident à rationaliser les tâches quotidiennes, ainsi qu'à intégrer la sécurité aux processus, aux applications et à l'infrastructure dès le départ. Avec une stratégie d'automatisation et de gestion à l'échelle de l'entreprise, vous pouvez réduire le risque d'erreur humaine, accélérer les processus, améliorer la cohérence et la reproductibilité, vérifier et auditer les systèmes. De plus, une stratégie d'automatisation et de gestion centralisée permet de renforcer la sécurité et la conformité, car la sécurité est intégrée au développement d'applications et à l'exploitation informatique dès le départ et tout au long du cycle de vie. Les entreprises peuvent ainsi mettre en œuvre le modèle DevSecOps. Il s'avère qu'une forte intégration de l'automatisation, de la gestion et de l'IA dans les processus de sécurité peut réduire le coût moyen d'une faille de 39,3 % en moyenne. Pourtant, seulement 28 % des entreprises ont recours à cette méthode[2].

[2] IBM Security, « Rapport 2023 sur le coût d'une violation de données », 2023

[4] Cloud Security Alliance, « Top Threats to Cloud Computing: Pandemic 11 Deep Dive », octobre 2023

Recommandations et meilleures pratiques

Mettez en œuvre une stratégie d'automatisation et de gestion à l'échelle de l'entreprise pour suivre l'évolution des exigences en matière de sécurité, de conformité et de prévention des risques. Avec une stratégie cohérente dans votre cloud hybride, vous pouvez améliorer l'agilité, la reproductibilité et la cohérence, tout en simplifiant les audits.

Une stratégie d'automatisation et de gestion unifiée réduit le risque d'erreurs de configuration ou d'erreurs manuelles dans l'ensemble de votre entreprise. L'automatisation et la gestion rationalisent et améliorent la cohérence de la gestion de l'infrastructure, du développement d'applications et des tâches de sécurité pour renforcer la protection, augmenter la conformité et améliorer le suivi des modifications. Vous pouvez ainsi :

Configurer vos ressources de façon cohérente selon des politiques préalablement validées et assurer leur maintenance de façon proactive et reproductible tout au long de leur cycle de vie.

Identifier rapidement les systèmes qui nécessitent des correctifs ou qui doivent être reconfigurés.

Rationaliser l'application des correctifs ou modifier les paramètres du système selon les références définies et de façon cohérente, sur un grand nombre de systèmes.

Faciliter l'audit et la résolution des problèmes grâce aux journaux d'action enregistrés automatiquement.

La gestion des identités et le contrôle des accès pour votre plateforme d'automatisation et vos processus vous permettent de garantir que seul le personnel autorisé est en mesure d'exécuter les tâches d'automatisation. Choisissez une plateforme d'automatisation que tous les salariés de votre entreprise peuvent utiliser. Une plateforme qui met en œuvre un langage d'automatisation commun et facile à apprendre améliore les points suivants :

La visibilité. Chaque intervenant peut comprendre les actions de chaque tâche d'automatisation.

La reproductibilité. Une plateforme et un langage accessibles permettent à toute personne habilitée d'utiliser l'automatisation de manière efficace.

La collaboration. Les tâches d'automatisation peuvent être partagées entre les différents services, ce qui permet à d'autres équipes de tirer parti du travail déjà effectué et d'éviter les efforts inutiles.

Les audits. Plusieurs personnes peuvent vérifier les tâches d'automatisation et consulter les journaux en vue d'un audit.

Les entreprises automatisent leurs processus informatiques pour gérer la sécurité des systèmes d'exploitation, applications, opérations de sécurité et environnements de cloud hybride de plus en plus complexes. **Red Hat Ansible Automation Platform** est une plateforme d'automatisation de bout en bout qui offre un environnement cohérent pour développer et gérer l'automatisation à grande échelle dans l'entreprise, tout en renforçant la sécurité à chaque étape. Elle donne les clés pour améliorer l'efficacité, la productivité et le contrôle des risques et des dépenses, tout en aidant les équipes à mettre en place des systèmes de sécurité et de conformité automatisés et cohérents dans toute l'entreprise, de manière reproductible. La solution met également à disposition des contenus d'automatisation certifiés afin de coordonner la réponse aux menaces avec l'assistance d'entreprise Red Hat, disponible à tout moment.

Avec Red Hat Ansible Automation Platform, les entreprises ont accès à des capacités automatisées telles que la gestion des configurations ou l'application de correctifs et la correction pour gérer des processus de sécurité automatisés qui préviennent les attaques. La solution Red Hat Ansible Automation Platform peut aussi constituer un point d'intégration des solutions de sécurité, par le biais des contenus de partenaires certifiés tels que CyberArk, IBM et Palo Alto Networks. Les utilisateurs peuvent ainsi gérer et intégrer diverses technologies de sécurité tierces de façon automatisée.

Étapes stratégiques

Voici quelques propositions de mesures pour commencer à automatiser la sécurité.

Commencez par un seul projet.
N'essayez pas de tout automatiser d'un seul coup. Choisissez un nombre limité de tâches pour démarrer.

Choisissez des tâches répétitives.
Automatisez les tâches répétitives comme la gestion des configurations, la gestion des correctifs et des paquets logiciels, l'identification et la correction des vulnérabilités et l'application des politiques.

Mesurez, adaptez et répétez.
Travaillez de façon itérative pour déployer l'automatisation, mesurer les résultats et adapter la procédure en conséquence.

Préparez votre évolution en vous appuyant sur une plateforme d'automatisation de bout en bout pour les entreprises.
Assurez-vous que tous vos processus d'automatisation peuvent être vérifiés, audités et partagés afin que d'autres services puissent tirer profit de vos réussites et mettre à l'échelle via une plateforme d'automatisation de bout en bout pour entreprise.

Chapitre 6

Premiers pas

La sécurité du cloud hybride constitue une responsabilité partagée dans toutes les entreprises. Quelle que soit votre situation actuelle, Red Hat peut vous aider à déployer un cloud hybride centré sur la sécurité.

Avec ses capacités de sécurité intégrées, la gamme de logiciels Open Source adaptés à la production de Red Hat vous offre les outils et les plateformes nécessaires pour relever les défis actuels et futurs en matière de sécurité et de conformité. Red Hat propose également un service d'assistance aux entreprises, des formations pratiques, ainsi que les services de ses spécialistes qui vous aident à déployer et utiliser votre environnement de cloud hybride de manière plus efficace et plus sûre.

Découvrir l'approche de Red Hat en matière de sécurité du cloud hybride

Consultez les ressources suivantes pour en savoir plus sur l'approche de Red Hat en matière de sécurité et de conformité dans un cloud hybride.

- Aperçu de la sécurité du cloud hybride
- Évaluation de sécurité du cloud hybride
- Approches de sécurité pour les environnements de cloud hybride
- Renforcer la sécurité du cloud hybride

À propos de Lucy Huh Kerner, directrice, stratégie globale et représentation pour la sécurité, Red Hat
Lucy Huh Kerner est responsable de l'encadrement éclairé de la sécurité et dirige les stratégies techniques et de mise sur le marché des produits de sécurité pour l'ensemble des systèmes et de la gamme Red Hat à l'échelle mondiale. De plus, elle participe au développement et à la distribution de contenus techniques liés à la sécurité sur le terrain ainsi qu'auprès des clients, des partenaires, des analystes et de la presse. Elle s'est également exprimée lors de nombreux événements, notamment des conférences au sujet de la sécurité. Lucy Huh Kerner dispose de plus de 20 ans d'expérience professionnelle en tant qu'ingénieure en développement logiciel et matériel, architecte de solutions et spécialiste de la stratégie de sécurité mondiale. Au cours de ces mandats, elle a travaillé sur divers aspects de la sécurité.

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

FRANCE
00 33 1 41 91 23 23
fr.redhat.com

facebook.com/redhatinc
@RedHatFrance
linkedin.com/company/red-hat
fr.redhat.com