Renforcer le niveau de sécurité et de conformité

Réduire les risques grâce à une plateforme Linux Open Source et robuste

Red Hat

Sommaire

Linux, une base solide pour l'avenir

Linux® est l'un des systèmes d'exploitation les plus répandus au monde. Il a été largement adopté dans tous les secteurs et avec toutes les technologies émergentes[1]. Couramment utilisé pour les charges de travail essentielles, fiables et à haute disponibilité, dans les datacenters et environnements de cloud computing, il prend en charge divers cas d'utilisation, systèmes cible et appareils. Tous les principaux fournisseurs de cloud public incluent plusieurs distributions Linux dans leur offre.

Cependant, la distribution Linux et les outils de gestion que vous choisissez peuvent avoir des effets considérables sur l'efficacité, la sécurité et l'interopérabilité de votre environnement informatique. Ce livre numérique passe en revue les éléments à prendre en compte et fournit des conseils utiles pour réduire la vulnérabilité des environnements Linux et les risques liés à la conformité.

Sécurité et conformité : deux préoccupations majeures

Les entreprises sont constamment préoccupées par la gestion des risques liés à la sécurité informatique et à la conformité. En effet, 33 % des PDG considèrent les cyberattaques comme une menace majeure contre les perspectives de croissance de leur entreprise[2]. De plus, les vulnérabilités peuvent coûter cher : environ 3,86 millions de dollars en moyenne pour une fuite de données[3].

Les réglementations sectorielles et gouvernementales sont également en pleine évolution. Il est parfois difficile de suivre le rythme de ces changements, et le non-respect des règles de conformité augmente le coût d'une fuite de données de 6 % en moyenne[3].

Les défis courants liés à la sécurité et à la conformité

Différents facteurs compliquent la gestion des vulnérabilités et de la conformité.

Conséquences d'une stratégie de sécurité inefficace

Pour réduire les risques et les effets des vulnérabilités, il est essentiel d'agir rapidement.

3,86 millions de dollars

Coût moyen d'une fuite de données en 2020[3]

280 jours

Temps moyen nécessaire pour identifier et stopper une fuite de données en 2020[3]

1,12 million de dollars

Montant économisé si la faille peut être identifiée et corrigée en 200 jours ou moins[3]

Évolution des exigences en matière de sécurité et de conformité

Les menaces évoluent rapidement, ce qui nécessite une adaptation rapide pour suivre le rythme des nouvelles menaces et réglementations.

Environnements de cloud hybride et multicloud distribués

Les environnements distribués géographiquement et logiquement peuvent empêcher d'avoir une vue complète de l'infrastructure.

Environnements vastes et complexes

Les infrastructures vastes intègrent souvent de multiples outils de sécurité et de conformité, ce qui complique la gestion des risques.

Personnel limité et travail à distance

La plupart des entreprises ne disposent pas du personnel nécessaire pour gérer manuellement les tâches liées à la sécurité et à la conformité.

1 *The Linux Foundation, « Linux is the most successful open source project in history », consulté le 24 septembre 2020*

2 *PWC, « 23rd Annual Global CEO Survey: Navigating the rising tide of uncertainty », 2020*

3 *Rapport IBM Security, « Rapport 2020 sur le coût d'une violation de la confidentialité des données », 2020*

Adoption d'une approche efficace de gestion des risques liés à la sécurité et à la conformité

La gestion des vulnérabilités et de la conformité consiste à surveiller et évaluer les systèmes pour s'assurer qu'ils restent conformes aux politiques de sécurité et de réglementation. Avec une approche adaptée, vous pourrez développer des processus cohérents et reproductibles dans l'ensemble de votre environnement pour effectuer les tâches suivantes :

Évaluer

Identifiez les systèmes non conformes ou vulnérables. Évaluez facilement l'état réel de la sécurité de votre environnement, de l'infrastructure aux charges de travail. Identifiez les avis de sécurité réellement applicables à vos systèmes et à votre environnement.

Établir les priorités

Organisez les mesures de correction en fonction des efforts à fournir, des effets et de la sévérité du problème. Appliquez des techniques de gestion des risques pour déterminer le risque métier réel de chaque problème et planifier les corrections en conséquence. Les risques englobent la probabilité qu'un problème entraîne une fuite, la gravité potentielle d'une fuite et les conséquences de la résolution du problème. Si la correction d'un problème donné peut sembler inutile sur les systèmes de développement et de test, elle peut en revanche être une priorité sur les systèmes de production.

Corriger

Appliquez les correctifs et reconfigurez les systèmes non conformes rapidement et simplement. Automatisez les processus de configuration et d'application des correctifs pour accélérer la correction, assurer la cohérence entre les systèmes et réduire le risque d'erreur humaine. En appliquant efficacement les outils automatisés, vous pouvez accélérer la correction des problèmes, et ainsi renforcer la sécurité de votre environnement et de votre entreprise.

Générer des rapports

Confirmez la bonne application des changements et automatisez les rapports de correction afin de rationaliser les efforts d'audit. Avec un système de rapport efficace, les dirigeants, auditeurs et équipes techniques obtiennent des informations suffisamment détaillées pour comprendre les risques et vulnérabilités actuels.

Cette approche permet également à l'entreprise de se préparer à l'adoption de techniques de développement et de gestion modernes et rapides telles que le **DevSecOps**. En fait, 38 % des entreprises considèrent qu'une évaluation des vulnérabilités est essentielle aux workflows DevOps[4].

Dans les sections suivantes, nous verrons les principales considérations à prendre en compte et les actions nécessaires pour gérer plus efficacement les risques liés à la sécurité et à la conformité.

4 451 Research, groupe de la S&P Global Market Intelligence : Voice of the Enterprise, DevOps H2 2019

Identification et correction des vulnérabilités dans les environnements Linux

L'identification et la correction des vulnérabilités correspondent au processus d'évaluation des infrastructures qui permet de détecter et réparer les systèmes vulnérables aux attaques. Ces vulnérabilités peuvent être causées par des menaces émergentes, des correctifs obsolètes ou manquants, ou une mauvaise configuration du système. Les mesures de correction comprennent souvent l'application de correctifs ainsi que la mise à jour et la reconfiguration des systèmes.

Pourquoi est-ce important ?

Les vulnérabilités peuvent entraîner des fuites qui coûteront cher à l'entreprise, et qui pourront ébranler la confiance de ses clients, nuire à sa réputation et réduire son chiffre d'affaires. En effet, la perte d'activité représente 39,4 % du coût moyen d'une fuite de données[5].

Les problèmes liés à l'identification et à la correction efficaces des vulnérabilités

La plupart des entreprises n'ont pas de stratégie de sécurité cohérente pour leur exploitation à grande échelle.

- Souvent, les effectifs sont insuffisants et le personnel, déjà débordé, n'est pas qualifié pour élaborer et exécuter une stratégie de sécurité complète.
- Les outils génériques d'analyse de sécurité produisent de longues listes de vulnérabilités potentielles qui ne sont pas toutes applicables à votre environnement. Le personnel est alors obligé de passer beaucoup de temps à enquêter sur ces vulnérabilités et à prendre les mesures de correction qui s'imposent.
- Les processus manuels d'identification, de correction et de suivi ralentissent l'exploitation et souvent, les vulnérabilités connues ne sont pas corrigées.
- Les méthodes de correction ad hoc entraînent une application incohérente des correctifs et une augmentation des risques pour la sécurité.

Les principales fonctionnalités des outils de gestion de la sécurité

Pour une efficacité optimale, vous devez identifier et corriger rapidement les vulnérabilités du système avant qu'elles n'entraînent une fuite. Pour ce faire, optez pour des outils de gestion unifiée de la sécurité qui incluent les fonctionnalités suivantes :

Analyse des systèmes, pour identifier les risques (tant au niveau du système d'exploitation que des charges de travail) dans les systèmes et instances de votre environnement

Automatisation de la correction des risques identifiés, afin d'améliorer la rapidité, la précision et l'efficacité des équipes informatiques et de sécurité

Expertise des fournisseurs et conseils sur les mesures de correction à appliquer aux produits ; il existe peut-être des mesures simples pour réduire les risques

Accès régulier aux données les plus récentes que vos fournisseurs de système d'exploitation et d'applications publient sur les vulnérabilités et risques de sécurité connus

Production de rapports sur les risques potentiels, les mesures de correction et les audits, adaptés à différents profils de lecteurs

5 *Rapport IBM Security, « Rapport 2020 sur le coût d'une violation de la confidentialité des données », 2020*

Gestion de la conformité dans les environnements Linux

La gestion de la conformité consiste à s'assurer que les systèmes restent toujours conformes aux politiques de l'entreprise, aux normes du secteur et aux réglementations applicables. Les infrastructures doivent également être contrôlées afin d'identifier les systèmes non conformes suite aux changements apportés aux réglementations, politiques ou normes, à une erreur de configuration ou pour d'autres raisons.

Pourquoi est-ce important ?

Le non-respect des règles de conformité peut nuire à votre entreprise et entraîner des amendes, la perte d'une certification ainsi que des failles du système de sécurité. En moyenne, le coût d'une fuite de données est plus élevé en cas de défaut de conformité[6].

Les problèmes liés à la gestion efficace de la conformité

De nombreuses entreprises gèrent la conformité à l'aide d'opérations manuelles et de scripts personnalisés. Ces processus sont toutefois trop lents et trop limités pour un développement et une exploitation modernes et rapides.

- Il est difficile de comprendre la pertinence et les effets de la gestion sur l'environnement en raison du nombre élevé de normes génériques et de références.
- Les processus manuels ralentissent les opérations de contrôle de la conformité, de correction et d'audit, ce qui entraîne une utilisation inefficace du personnel, une application incohérente des politiques et un risque accru de problèmes de conformité.
- Beaucoup d'entreprises utilisent des outils différents pour la gestion de la sécurité et de la conformité, ce qui réduit l'efficacité opérationnelle et complique la mise en place de politiques cohérentes et personnalisées.

Les principales fonctionnalités des outils de gestion de la conformité

Pour une efficacité optimale, vous devez définir et appliquer des politiques contextuelles, assurer la conformité des systèmes avec ces politiques ainsi que générer et gérer rapidement des rapports de conformité pour les audits. Pour ce faire, optez pour des outils de gestion unifiée de la conformité qui incluent les fonctionnalités suivantes :

Analyses pour identifier de manière cohérente et rapide les risques de non-conformité

Correction automatique des systèmes non conformes

Vue complète du niveau de conformité dans tout l'environnement

Création automatique de rapports de conformité en fonction de vos exigences en matière d'audit et des besoins des lecteurs

Avis de spécialistes et conseils contextuels pour corriger les systèmes non conformes de votre environnement

6 *Rapport IBM Security, « Rapport 2020 sur le coût d'une violation de la confidentialité des données », 2020*

Meilleures pratiques

Analysez régulièrement vos systèmes

Une surveillance quotidienne peut vous aider à identifier les risques de vulnérabilité et de conformité avant qu'un problème n'interrompe l'exploitation ou n'entraîne une fuite. Assurez-vous d'utiliser les données de sécurité les plus récentes publiées par vos fournisseurs de système d'exploitation et d'applications pour améliorer la précision des analyses. Enfin, mettez en place des politiques de sécurité personnalisées et adaptées à votre environnement et à votre exploitation pour optimiser la conformité.

Le coût d'une faille peut être considérablement réduit si elle est identifiée et corrigée en

200 jours

ou moins[7]

Appliquez et testez régulièrement vos correctifs

La mise à jour régulière des systèmes renforce la sécurité, la fiabilité, les performances et la conformité. Appliquez régulièrement les correctifs disponibles pour éliminer immédiatement les problèmes importants. Appliquez dès que possible les correctifs pour traiter les bogues et failles critiques. Testez les systèmes après l'installation des correctifs pour vérifier leur état de fonctionnement avant de les remettre en production.

Avec un outil efficace de gestion des correctifs, vous pouvez corriger les systèmes jusqu'à

88,9 % plus rapidement[8]

Déployez l'automatisation

Plus la taille et la complexité de votre infrastructure augmentent, plus il est difficile de la gérer manuellement. Tirez parti de l'automatisation pour rationaliser la surveillance, accélérer l'application des mesures de correction, améliorer la cohérence et assurer la régularité des rapports.

En automatisant la sécurité, vous pouvez réduire le coût moyen d'une faille de

93 %[7]

Connectez vos outils et harmonisez vos processus

En général, les environnements distribués incluent des outils de gestion différents pour chaque plateforme. Intégrez ces outils via des API et utilisez vos interfaces favorites pour effectuer des tâches dans d'autres outils. Réduisez le nombre d'interfaces pour rationaliser l'exploitation et bénéficier d'une meilleure visibilité sur la sécurité et l'état de conformité de tous les systèmes de votre environnement. Harmonisez aussi les processus de vos différents environnements pour renforcer la cohérence et la fiabilité.

52 %

des entreprises optimisent l'infrastructure et les processus informatiques pour renforcer la sécurité[9]

Adoptez une stratégie de sécurité cohérente et continue

Un dispositif de sécurité efficace nécessite une démarche globale qui implique à la fois les individus, les processus et les technologies. Pour assurer la sécurité en continu, il faut s'appuyer sur les retours d'expérience et sans cesse adapter les systèmes afin de prendre en compte les techniques de développement modernes, les pratiques DevSecOps et les besoins des entreprises numériques. Adoptez une approche de défense en profondeur qui utilise les capacités de chaque couche de votre environnement, y compris les systèmes d'exploitation, les plateformes de conteneurs, les outils d'automatisation, les ressources SaaS et les services cloud.

En adoptant une approche DevSecOps, vous pouvez réduire le coût moyen d'une fuite de données de

5 %[7]

7 *Rapport IBM Security, « Rapport 2020 sur le coût d'une violation de la confidentialité des données », 2020*

8 *Principled Technologies, article d'analyste commissionné par Red Hat, « Save administrator time and effort by activating Red Hat Insights to automate monitoring », septembre 2020*

9 *Qualtrics et Red Hat, étude sur l'optimisation informatique, février 2020*

Outils recommandés

Les outils de sécurité et de conformité à privilégier incluent plusieurs fonctions et capacités essentielles.

Analyses proactives

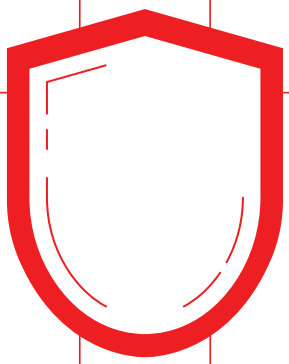
Pour améliorer vos niveaux de sécurité et de conformité, commencez par mieux les comprendre. Optez pour des outils qui fournissent des analyses automatisées, assurent une surveillance régulière des systèmes et vous alertent en cas de problème, sans trop mobiliser le temps et l'énergie de vos équipes.

Corrections hiérarchisées

Les outils qui offrent des instructions de correction normatives vous évitent d'avoir à chercher vous-même les mesures à appliquer, ce qui représente un gain de temps et réduit le risque d'erreurs. Les créneaux pour l'application des correctifs sont limités, et la hiérarchisation des mesures en fonction des potentielles conséquences et des systèmes affectés permet d'optimiser leur utilisation.

Résultats personnalisables

Des contrôles de vulnérabilité et de conformité peuvent ne pas s'appliquer à certains systèmes en raison de leur configuration, utilisation ou charge de travail spécifiques. Optez pour des outils qui vous permettent de définir un contexte métier afin de réduire le nombre de faux positifs, de gérer les risques métier et de fournir une vue plus réaliste de l'état de conformité et du statut d'intégrité.



Rapports lisibles

Les outils qui génèrent des rapports clairs et lisibles sur les systèmes à jour, ceux qui nécessitent un correctif et ceux qui ne sont pas conformes aux politiques de sécurité augmentent l'auditabilité et vous permettent de mieux comprendre l'état de votre environnement.

Interface unifiée

Les outils qui vont au-delà de la gestion d'un seul composant ou d'une seule couche de votre environnement simplifient les opérations de sécurité et permettent de mieux comprendre le niveau de sécurité et de conformité dans l'entreprise. Les outils unifiés peuvent également fournir un contexte amélioré pour les analyses et conseils de correction.

Données exploitables

Les outils qui fournissent des informations adaptées à votre environnement vous aident à identifier plus rapidement les problèmes de conformité et les vulnérabilités, les systèmes affectés et les conséquences potentielles sur votre activité. Ils peuvent également vous aider à hiérarchiser et planifier les mesures de correction.

Davantage de sécurité et de conformité avec les solutions Red Hat

Red Hat suit une approche globale en matière de gestion des risques liés à la sécurité et à la conformité, qui augmente la rapidité, l'évolutivité et la stabilité dans l'ensemble de l'environnement informatique, des serveurs bare metal et virtuels aux infrastructures de cloud public, privé ou hybride. Les solutions Red Hat® impliquent à la fois les individus, les processus et les technologies pour optimiser l'efficacité opérationnelle, stimuler l'innovation et améliorer la satisfaction des salariés.

La plateforme **Red Hat Enterprise Linux** se trouve au cœur de cette stratégie. Base d'exploitation stable et intelligente pour l'informatique moderne et les déploiements de cloud hybride d'entreprise, elle offre un avantage optimal à votre entreprise. D'une efficacité constante sur toutes les infrastructures, elle vous permet de déployer des applications, des charges de travail et des services en utilisant les mêmes outils, quel que soit votre environnement.

La sécurité est un élément clé de l'architecture et du cycle de vie de la plateforme Red Hat Enterprise Linux. Les systèmes multicouches de défense contre les fuites utilisent des contrôles de sécurité automatisés et reproductibles pour réduire le risque d'exposition aux vulnérabilités. Les mises à niveau de sécurité critiques et les correctifs en direct sont inclus dans votre souscription Red Hat Enterprise Linux et vous aident à maintenir votre environnement à jour et sécurisé.

Les outils de gestion de Red Hat s'intègrent à Red Hat Enterprise Linux afin de vous fournir les fonctionnalités dont vous avez besoin pour gérer efficacement les risques de vulnérabilités et la conformité.

- Les outils et références configurables réduisent le nombre de faux positifs et vous donnent une vue précise de l'état de vos infrastructures.
- Les fonctionnalités d'automatisation améliorent la précision de la configuration et des correctifs tout en réduisant les erreurs humaines.
- Les vues personnalisables fournissent rapidement des informations pertinentes.
- Les mesures de correction automatisées et proactives vous aident à résoudre les problèmes plus rapidement, sans contacter le service d'assistance.
- Une vaste bibliothèque de ressources fournit des informations détaillées et ciblées 24 heures sur 24, 7 jours sur 7.
- Les options sur site et SaaS vous permettent de déployer les outils selon vos préférences.

« La création de serveurs configurés, prêts à l'emploi et plus sûrs dès le premier jour est une nécessité pour notre service informatique. Avec la plateforme Red Hat Enterprise Linux et la solution Red Hat Insights, c'est possible. Nous pouvons ainsi déployer des serveurs utilisables immédiatement qui répondent à nos besoins spécifiques dès leur mise en service. »[10]

Steve Short
Responsable des plateformes, Unix, Kingfisher PLC

10 *Communiqué de presse Red Hat, « Red Hat Delivers Force Multiplier for Enterprise IT with Enhanced Intelligent Monitoring, Unveils Latest Version of Red Hat Enterprise Linux 8 », 21 avril 2020*

Outils de gestion intégrés

Les outils de gestion Red Hat reposent sur des années d'expérience en matière de développement Linux et d'assistance. Ils fonctionnent ensemble pour rationaliser l'administration informatique, ce qui permet à votre équipe d'éviter les pertes de temps et les dépenses d'énergie inutiles, et améliore la sécurité, l'efficacité et la fiabilité de votre environnement.

Red Hat Insights

Analyse prédictive des risques informatiques

Incluse dans toutes les souscriptions Red Hat Enterprise Linux actives, la solution **Red Hat Insights** aide les équipes informatiques à identifier et corriger de manière proactive diverses menaces afin d'éviter les pannes, les temps d'arrêt non planifiés et les risques pour la sécurité et la conformité.

- Analyse des systèmes en profondeur pour détecter de manière proactive les vulnérabilités, les problèmes de conformité et les violations des politiques
- Suggestion et hiérarchisation des mesures de correction, et génération de playbooks Red Hat Ansible® Automation Platform pour simplifier leur mise en œuvre
- Comparaison des systèmes aux références, aux historiques et à d'autres systèmes
- Déploiement facile dans l'ensemble des environnements sur site et cloud

96 % d'accélération pour la détection des problèmes propres aux applications[11]

91 % d'accélération pour l'identification des vulnérabilités de sécurité[11]

89 % d'accélération pour la détection des écarts de configuration[11]

En savoir plus

Red Hat Smart Management

Facilité de gestion et de correction

La solution **Red Hat Smart Management** associe les puissantes capacités d'infrastructure de la solution Red Hat Satellite à la simplicité de gestion du cloud pour renforcer et compléter les fonctionnalités de l'offre Red Hat Insights.

- Application des correctifs, approvisionnement et contrôle des hôtes Red Hat Enterprise Linux, et rapports généraux détaillés avec Red Hat Satellite
- Identification et correction des problèmes via le site cloud.redhat.com, avec la solution Red Hat Insights
- Correction des problèmes identifiés par la solution Red Hat Insights en un clic via Cloud Connector

56 % d'efficacité en plus pour l'application des correctifs système[12]

14 % d'efficacité en plus pour les équipes de sécurité informatique[12]

23 % de productivité en plus pour les équipes de conformité[12]

En savoir plus

11 *Principled Technologies, article d'analyste commissionné par Red Hat, « **Save administrator time and effort by activating Red Hat Insights to automate monitoring** », septembre 2020*

12 *Livre blanc d'IDC commissionné par Red Hat, « **Red Hat Satellite Helps Enterprise Organizations Optimize Infrastructure with Automation Tools** », mars 2020, document #US46109220*

Témoignage client

Metalloinvest

Garantir les performances des systèmes essentiels grâce aux données et à l'analyse prédictive des risques

Défi

Le groupe Metalloinvest est l'un des principaux producteurs et fournisseurs mondiaux de fer briqueté à chaud et de produits de minerai de fer, également producteur régional d'acier de haute qualité. Après plus de vingt ans d'activité, Metalloinvest a dû relever un nouveau défi : le passage à la quatrième révolution industrielle, ou « industrie 4.0 », c'est-à-dire la transition vers une exploitation automatisée et centrée sur les données. En automatisant et en numérisant la production, l'entreprise souhaite optimiser son fonctionnement et l'utilisation des ressources. Son objectif : devenir la société minière la plus importante et la plus productive au monde. Afin de créer une base solide pour son passage à l'industrie 4.0, l'entreprise a cherché à intégrer et optimiser son environnement SAP® complexe.

Solution

Avec l'aide de son prestataire de services gérés JSA-Group, Metalloinvest a adopté la plateforme Red Hat Enterprise Linux for SAP Solutions afin de créer une base d'entreprise solide pour son environnement SAP S/4HANA®. Développée conjointement par **Red Hat et SAP**, cette plateforme comprend la solution Red Hat Insights pour l'analyse prédictive des données, et la solution Red Hat Smart Management pour une gestion simplifiée des environnements Red Hat Enterprise Linux grâce aux services de gestion de cloud et à Red Hat Satellite. Cette souscription unique associe la fiabilité, l'évolutivité et les capacités hautes performances de Linux à des technologies qui répondent aux exigences spécifiques des applications SAP.

Metalloinvest exécute désormais l'ensemble de son environnement de production SAP S/4HANA sur la plateforme Red Hat Enterprise Linux for SAP Solutions. L'entreprise peut profiter d'informations complètes sur ses données et d'analyses prédictives des risques pour garantir la fiabilité et la stabilité des performances de ses systèmes essentiels, tandis qu'elle se prépare à numériser son environnement de production.

« Les solutions Red Hat nous fournissent des outils qui améliorent la productivité de notre personnel et de l'exploitation. »

Konstantin Zelenkov
Directeur technique, JSA Group

Amélioration de la fiabilité et des performances des systèmes essentiels

Informations complètes sur les données grâce à une meilleure intégration de SAP

Réduction des risques grâce à la gestion de la sécurité et à une assistance complète

Lire le témoignage client

Prêt à renforcer la sécurité et la conformité ?

Votre entreprise dépend de votre infrastructure informatique et de vos applications. En adoptant des approches et outils efficaces de gestion des vulnérabilités et des risques liés à la conformité, vous protégez votre entreprise. Nous proposons une plateforme Linux qui intègre les outils de gestion nécessaires pour assurer la sécurité de l'exploitation et des innovations.

Commencez dès maintenant à utiliser la solution Red Hat Insights :

redhat.com/insights

Découvrez comment accélérer vos workflows informatiques avec Red Hat Insights :

red.ht/insights_savetime

Lisez le résumé sur la gestion des risques liés à la sécurité avec Red Hat Insights :

red.ht/insights-security-brief

Regardez la vidéo de démonstration sur la gestion des risques avec Red Hat Insights :

red.ht/insights-security-demo

F26049_1120_KVM

Red Hat