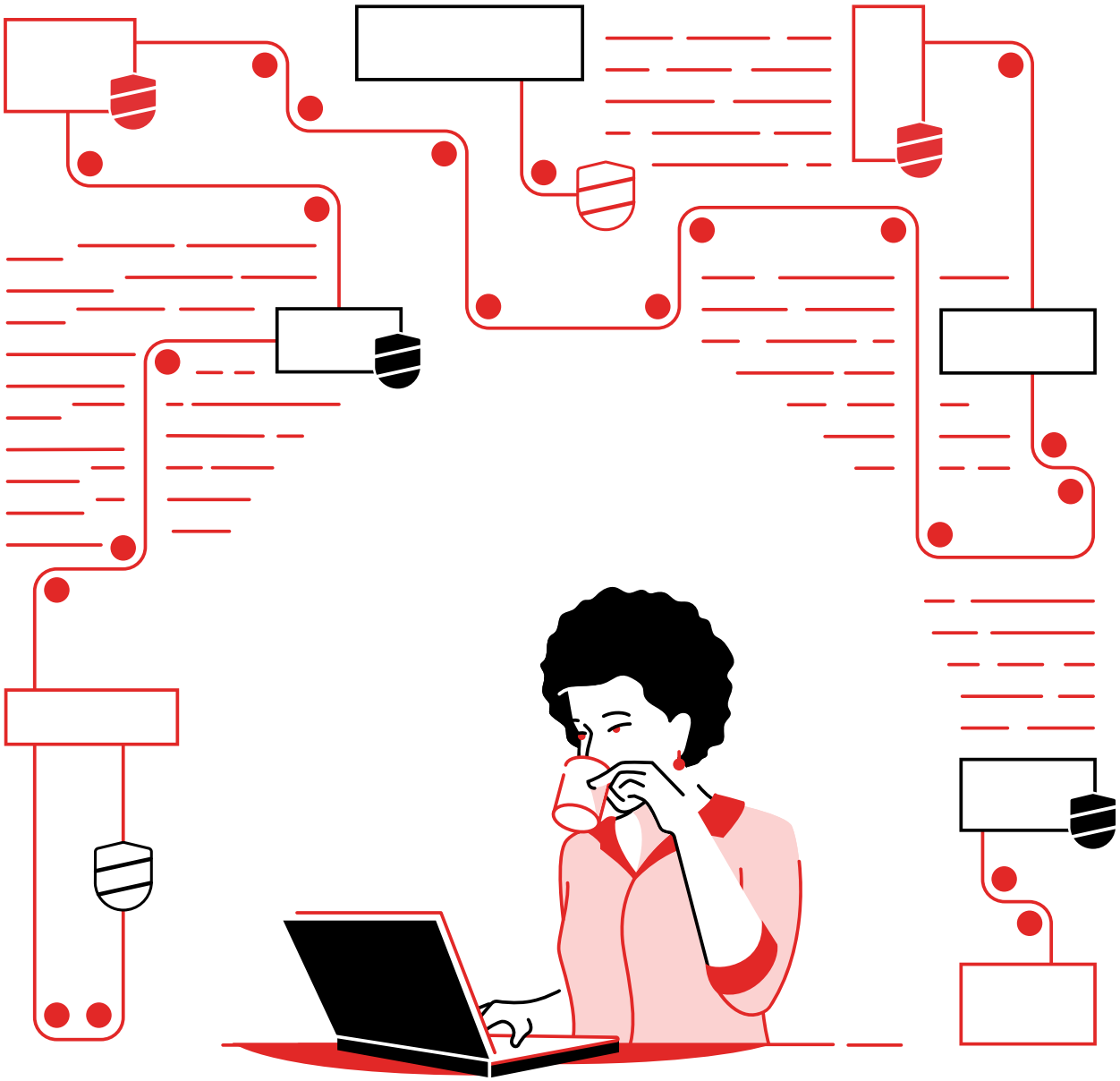
Simplifiez votre centre opérationnel de sécurité

Optimisez votre rapidité, votre temps et votre sécurité à l'aide d'une plateforme d'automatisation unifiée



Red Hat

Sommaire

La sécurité informatique, une préoccupation majeure

La sécurité est une priorité pour de nombreuses entreprises. En effet, 33 % des PDG se disent extrêmement préoccupés par les cybermenaces[1]. Cette appréhension n'est d'ailleurs pas sans fondement, car 32 % des entreprises ont été victimes de cyberattaques majeures au cours des deux dernières années[2].

La protection de l'entreprise est essentielle. Cependant, cette tâche peut parfois intimider. Les équipes chargées de la sécurité doivent créer, gérer, adapter des environnements complexes et en assurer le bon fonctionnement à l'aide d'outils et de services divers proposés par un large éventail de fournisseurs souvent concurrents. Chaque année, le nombre d'offres augmente, forçant les équipes à rechercher, évaluer et intégrer sans cesse de nouveaux produits afin de suivre l'évolution du paysage de la sécurité.

En outre, le nombre, la gravité et le coût des failles de sécurité sont de plus en plus importants. Aujourd'hui, une entreprise a 29,6 % de risques de subir une attaque, contre 22,6 % en 2014[3]. Le nombre moyen de dossiers impliqués dans chaque fuite de données a augmenté de 3,9 % entre 2018 et 2019[3], et le coût moyen d'un tel incident a atteint les 3,92 millions de dollars en 2019[3].

La plupart des entreprises réalisent encore leurs opérations de sécurité manuellement. En plus d'être chronophages et pénibles, les tâches liées à la sécurité sont sujettes aux erreurs en cas d'intervention humaine. Résultat : les équipes de sécurité sont submergées. Elles font face à un nombre croissant d'alertes de menaces provenant de nombreux outils. En réalité, 60 % des équipes de sécurité reçoivent plus de 5 000 alertes par jour, et 16 % en reçoivent plus de 100 000[4].

Compte tenu de la croissance et de la complexification des infrastructures, il devient de plus en plus difficile d'identifier les vulnérabilités et de vérifier les failles. En outre, la plupart des outils de sécurité ne s'intègrent pas les uns aux autres, obligeant les équipes spécialisées à intervenir plus souvent. De la même façon, les délais d'investigation et de réponse aux incidents sont de plus en plus longs. En 2019, il fallait en moyenne 279 jours pour identifier et maîtriser une fuite de données, soit 4,9 % de temps de plus qu'en 2018[3]. De plus, il devient difficile de trouver de nouveaux talents pour agrandir les équipes et tenir la cadence : en 2019, 39 % des entreprises ont déclaré manquer de compétences en matière de cybersécurité[2]. Sans compter que les budgets alloués à la cybersécurité sont limités. Seuls 33 % des entreprises affirment avoir des ressources financières suffisantes pour atteindre un haut niveau de résilience[5].

Par conséquent, les équipes de sécurité n'examinent et ne répondent en moyenne qu'à 48 % des alertes reçues et seuls 50 % des menaces légitimes sont maîtrisées[4], ce qui augmente la vulnérabilité de nombreuses entreprises.

77 % des entreprises prévoient d'augmenter l'automatisation pour simplifier et accélérer les délais de réponse dans leurs écosystèmes de sécurité[4].

Conséquences d'une stratégie de sécurité inefficace

Le nombre, la gravité et le coût des failles de sécurité ne cessent d'augmenter.

3,92 millions de dollars
C'est le coût moyen d'une fuite de données en 2019[3]

279 jours
C'est le temps moyen nécessaire pour identifier et stopper une fuite de données en 2019[3]

1,22 million de dollars
C'est le montant économisé si la faille peut être identifiée et corrigée en
200 jours
ou moins[3]

29,6 %
C'est la probabilité d'être confronté à une faille dans les deux prochaines années[3]

50 %
C'est la part de menaces légitimes maîtrisées[4]

1 *PWC, « 23rd Annual Global CEO Survey: Navigating the rising tide of uncertainty », 2020.* pwc.com/ceosurvey.
2 *Harvey Nash et KPMG, « CIO Survey 2019: A Changing Perspective », 2019.* home.kpmg/xx/en/home/insights/2019/06/harvey-nash-kpmg-cio-survey-2019.html.
3 *IBM Security, 2019 « Cost of a Data Breach Report », 2019.* ibm.com/security/data-breach.
4 *Cisco, « Cisco Benchmark Study: Securing What's Now and What's Next », février 2020.* cisco.com/c/en/us/products/security/ciso-benchmark-report-2020.html.
5 *Ponemon Institute, commissionné par IBM Security, « The Cyber Resilient Organization », avril 2019.* ibm.com/account/reg/us-en/signup?formid=urx-37792.

L'automatisation de la sécurité, qu'est-ce que c'est ?

L'automatisation de la sécurité consiste à automatiser les tâches manuelles qui permettent d'assurer la sécurité de votre entreprise. Elle englobe diverses pratiques, que nous avons classées en quatre grandes catégories :

Gestion et résolution
Activités orientées événements qui impliquent la participation et/ou les conseils d'un analyste de la sécurité

Opérations de sécurité
Activités quotidiennes orientées processus et politiques réalisées par les équipes technologiques dans votre infrastructure de sécurité

Conformité de la sécurité
Activités veillant à ce que l'infrastructure soit conforme aux politiques et réglementations en matière de sécurité

Renforcement
Application des politiques de sécurité personnalisées à l'infrastructure dans une démarche et avec des objectifs ciblés

Ce livre numérique aborde l'automatisation des activités de gestion, des mesures de correction ainsi que des opérations de sécurité.

En savoir plus sur la conformité et le renforcement de la sécurité

Découvrez comment l'automatisation contribue à la conformité et au renforcement de la sécurité en consultant les ressources suivantes :

- **Livre numérique « Renforcer la sécurité du cloud hybride »**
- **Présentation « L'automatisation de la sécurité et de la conformité »**
- **Fiche technique « Services Red Hat : automatisez la sécurité et les workflows de fiabilité »**

Avantages de l'automatisation des activités de gestion, de correction et des opérations de sécurité

Rapidité et efficacité améliorées

Avec l'automatisation, plus besoin d'intervention manuelle. Les tâches sont rationalisées, ce qui accélère les opérations de sécurité et permet aux équipes de se concentrer sur les initiatives à forte valeur ajoutée. Cela permet également de simplifier l'infrastructure informatique : 40 % des entreprises dotées de systèmes d'automatisation élaborés déclarent posséder le nombre adéquat de solutions et de technologies de sécurité[6].

Augmentation de la sécurité à l'échelle de l'entreprise

L'automatisation de l'ensemble d'une infrastructure de sécurité permet d'assurer la cohérence et d'adopter une approche plus globale. Tous les membres de votre personnel peuvent ainsi gérer davantage d'outils, d'appareils et de systèmes afin que vous puissiez mener vos opérations à grande échelle. L'automatisation réduit également le risque d'erreurs humaines, améliorant ainsi la précision.

Réduction du risque et du coût des failles

Les entreprises qui ont pleinement adopté l'automatisation sont davantage capables de prévenir les incidents de sécurité et les interruptions d'activités[6]. L'automatisation totale des tâches de sécurité permet de réduire le coût moyen d'une faille de 95 %[7]. Ainsi, 52 % des entreprises l'ont déployée dans une certaine mesure et 36 % prévoient de le faire dans les deux prochaines années[7].

6 Ponemon Institute, commissionné par IBM Security, « The Cyber Resilient Organization », avril 2019. ibm.com/account/reg/us-en/signup?formid=urx-37792.

7 IBM Security, « 2019 Cost of a Data Breach Report », 2019. ibm.com/security/data-breach.

Intégrez vos outils, systèmes et processus de sécurité grâce à l'automatisation

Vos équipes, processus et outils enfin réunis sur une seule plateforme flexible et cohérente

Une plateforme d'automatisation peut faire office de couche d'intégration entre vos équipes, outils et processus de sécurité. Une plateforme interopérable flexible permet de :

- connecter vos systèmes, outils et équipes de sécurité ;
- collecter des informations à partir des systèmes, puis les diriger vers des systèmes et emplacements prédéfinis, rapidement et sans intervention manuelle ;
- modifier et propager des configurations rapidement à partir d'interfaces centralisées ;
- créer des contenus automatisés et personnalisés relatifs à vos outils et processus de sécurité, les conserver et y accéder ;
- automatiser des actions déclenchées par de multiples outils de sécurité lorsqu'une menace est détectée.

L'utilisation d'un langage et d'une plateforme d'automatisation cohérents dans l'ensemble de votre entreprise permet également de favoriser la communication et la collaboration. Lorsque toutes les solutions de sécurité d'une gamme sont automatisées dans le même langage, les analystes comme les opérateurs sont en mesure de réaliser une série d'actions sur divers produits en un temps record, maximisant ainsi l'efficacité globale de l'équipe de sécurité. De plus, avec un framework et un langage communs, les équipes informatiques et de sécurité peuvent partager leurs conceptions, processus et idées plus facilement, au sein de leur service comme dans l'ensemble de l'entreprise.

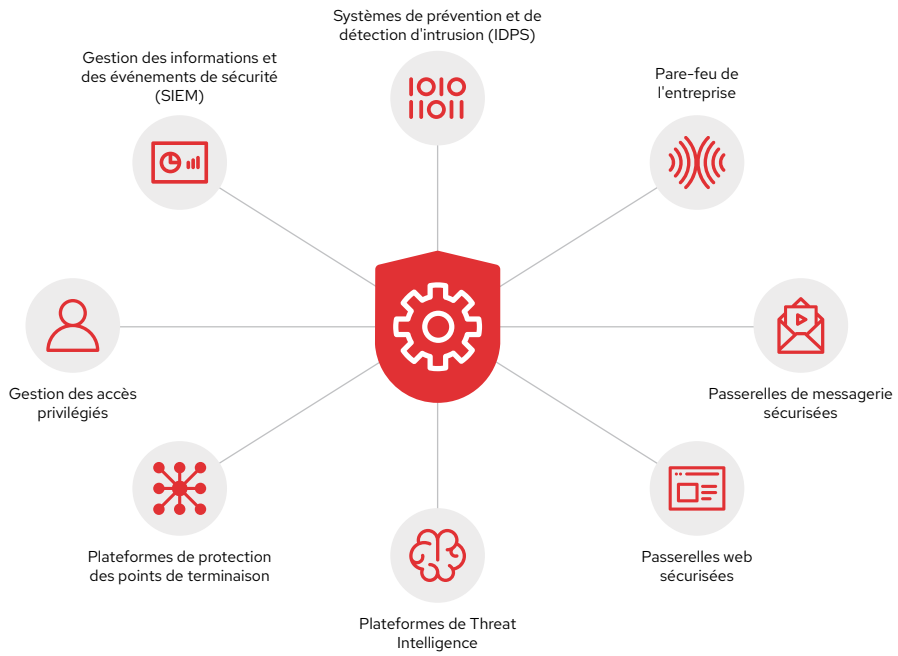


Figure 1. Une plateforme d'automatisation permet de réunir vos systèmes, outils et équipes de sécurité.

Automatisation réussie = équipes + processus + plateforme

Pour optimiser la valeur de l'automatisation, votre entreprise ne peut pas compter que sur ses outils. Elle doit aussi s'appuyer sur ses équipes, processus et plateformes.

- **Les équipes** sont au cœur de toute initiative métier. La participation au sein d'une équipe ou entre plusieurs équipes permet un échange des idées et une collaboration plus efficaces.
- **Les processus** font évoluer les projets de bout en bout au sein de l'entreprise. Il est indispensable de mettre en place des processus clairs et détaillés pour assurer l'efficacité de l'automatisation.
- **Une plateforme** d'automatisation permet de construire, d'exécuter et de gérer vos processus d'automatisation. Contrairement aux outils d'automatisation simples, une plateforme d'automatisation fournit à votre entreprise une base cohérente et unifiée pour créer, déployer et partager des contenus et des connaissances à l'échelle de l'entreprise.

Lire le livre numérique

La grande aventure de l'automatisation de la sécurité

La mise en œuvre de l'automatisation à tous les niveaux d'une entreprise n'est pas un processus immédiat et vous n'êtes pas obligé de tout automatiser d'un seul coup. Vous pouvez envisager l'automatisation de la sécurité comme un voyage. Chaque entreprise commence et s'arrête à des étapes différentes en fonction de ses besoins, et ce sont ces mêmes besoins qui détermineront son parcours. Toutefois, quelle que soit votre avancée dans ce parcours, même les plus petits efforts d'automatisation vous offriront des avantages.

Évaluez le niveau de maturité de l'automatisation de vos systèmes de sécurité

La plupart des entreprises se situent à l'une des trois étapes principales qui décrivent la maturité de l'automatisation de la sécurité. En identifiant la situation de votre entreprise, vous pourrez adopter les outils et processus appropriés en temps opportun pour réussir au mieux votre transition vers l'automatisation.

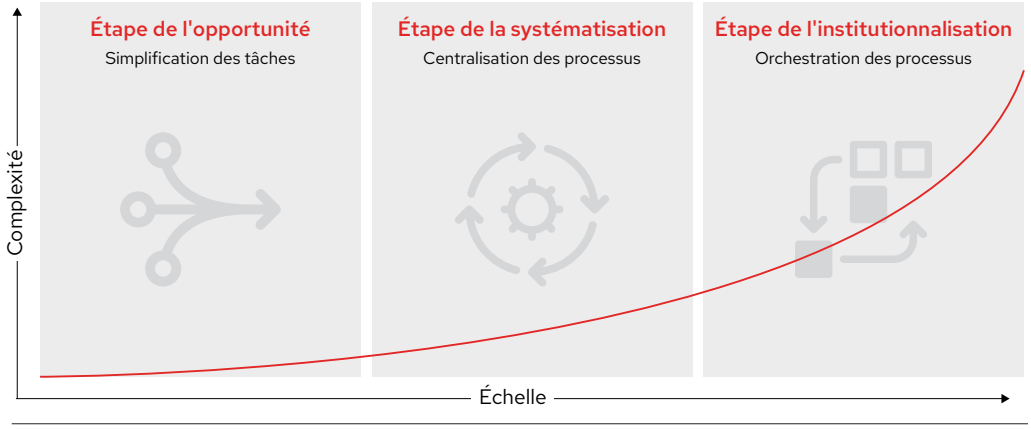


Figure 2. *Étapes de la maturité de l'automatisation de la sécurité*

Étape 1 : l'opportunité

Cette étape consiste à gagner du temps en automatisant les opérations de sécurité. Parmi les objectifs communs figurent la standardisation des tâches de sécurité sur les appareils et technologies similaires, ainsi que la rationalisation des tâches manuelles réalisées sur divers produits de fournisseurs différents.

Étape 2 : la systématisation

Cette étape vise à améliorer les processus et l'efficacité en adoptant un ensemble cohérent d'outils et de services dédiés aux opérations de sécurité. Parmi les objectifs communs figurent la création de processus de sécurité dans des workflows de plus haut niveau et la centralisation des processus de résolution des problèmes de sécurité.

Étape 3 : l'institutionnalisation

Cette étape favorise la collaboration et intègre la sécurité à tous les niveaux de votre entreprise. Parmi les objectifs communs figurent la création de workflows automatisés et programmés qui couvrent tous les aspects de la sécurité, ainsi que l'intégration de vos technologies informatiques et de sécurité.

Lire l'article de blog

Cas d'utilisation et intégrations

Organisez votre transition vers l'automatisation de la sécurité

Cas d'utilisation fréquents de haut niveau pour l'automatisation de la sécurité

Vous pouvez vous baser sur l'un des cas d'utilisation suivants pour entamer votre transition vers l'automatisation de la sécurité. La meilleure approche consiste à commencer par de petites tâches, puis à évoluer à votre rythme.

Enrichissement des investigations

Pour analyser les incidents et alertes de sécurité, il est nécessaire de recueillir les données d'une multitude de systèmes de sécurité afin de déterminer si un événement légitime s'est produit. Les informations sont généralement collectées via une série d'interfaces utilisateur, d'e-mails et d'appels téléphoniques. L'inefficacité de ce processus est susceptible de retarder l'application des mesures contre les menaces, ce qui rend votre entreprise plus vulnérable et augmente les coûts liés à une éventuelle faille. L'automatisation permet de programmer la collecte des informations dans vos systèmes de sécurité, tout en favorisant l'enrichissement à la demande des activités de tri menées par le biais de systèmes de gestion des informations et des événements de sécurité (SIEM). Résultat : vous évaluez et traitez les alertes et incidents plus rapidement.

Traque des menaces

Traquer une menace consiste à identifier les menaces potentielles pour la sécurité et à enquêter de façon proactive. Comme pour les analyses liées aux incidents, les équipes collectent et envoient manuellement les informations à travers de nombreux systèmes. Grâce à l'automatisation, vous pouvez personnaliser et rationaliser les alertes, les recherches de corrélation et les manipulations de signatures afin d'examiner les menaces potentielles plus rapidement. Cela permet également de créer et de mettre à jour automatiquement des requêtes de corrélation SIEM ainsi que les règles des systèmes de détection d'intrusion (IDS) afin d'en augmenter l'efficacité. De cette manière, les défenses de votre entreprise peuvent être mises à jour plus souvent et plus efficacement pour mieux vous protéger.

Résolution des incidents

La résolution d'un incident implique de prendre les mesures nécessaires pour interrompre la progression d'une faille. Une fois la faille découverte, les équipes de sécurité doivent réagir rapidement et dans l'ensemble de l'entreprise pour la maîtriser. Toutefois, les mesures de résolution comprennent souvent de nombreuses tâches manuelles, ce qui ralentit la correction et laisse votre entreprise plus longtemps vulnérable aux attaques. L'automatisation permet de réagir plus vite en codifiant les actions sous la forme de playbooks préapprouvés et reproductibles. Vous pouvez accélérer certaines tâches, telles que le blocage des attaques contre les adresses IP ou domaines, favoriser le trafic non menaçant, geler les identifiants compromis et isoler les charges de travail suspectes afin d'approfondir les investigations et de minimiser les dommages causés par l'incident.

L'intégration est essentielle

Pour adopter l'automatisation de façon unifiée, vous devrez intégrer votre plateforme d'automatisation à vos technologies de sécurité. Parmi les intégrations essentielles :

- **Les pare-feu** contrôlent le flux du trafic entre les réseaux et protègent les applications exposées à Internet. L'automatisation permet d'accélérer les changements de configuration des journaux et politiques.
- **Les systèmes de prévention et de détection d'intrusion (IDPS)** surveillent le trafic du réseau en quête d'activités suspectes, émettent des alertes en cas de menace et bloquent les attaques. L'automatisation peut simplifier la gestion des règles et des journaux.
- **Les systèmes de gestion des informations et des événements de sécurité** collectent des données sur les événements relatifs à la sécurité et les analysent afin de déceler et de maîtriser les menaces. L'automatisation fournit un accès programmé aux sources de données.
- **Les outils de gestion des accès privilégiés (PAM)** surveillent et gèrent les comptes et accès privilégiés. L'automatisation rationalise la gestion des identifiants.
- **Les systèmes de protection des points de terminaison** surveillent et gèrent les appareils afin de renforcer leur sécurité. L'automatisation permet de simplifier les tâches fréquentes de gestion des points de terminaison.

En savoir plus

Simplifiez votre centre opérationnel de sécurité grâce à la solution Red Hat Ansible Automation Platform

Il existe de nombreuses solutions d'automatisation, mais toutes n'offrent pas les capacités nécessaires pour assurer une automatisation de la sécurité efficace. Une bonne plateforme d'automatisation offre les avantages suivants :

- **Un langage d'automatisation universel et accessible.** En utilisant un langage facile à comprendre et à écrire, vous pourrez recueillir des informations et les partager avec les membres des équipes de sécurité aux domaines d'expertise variés.
- **Une approche ouverte et neutre.** Pour être efficace, votre plateforme d'automatisation doit interagir avec l'ensemble de votre infrastructure de sécurité et de votre écosystème de fournisseurs.
- **Une conception modulaire et extensible.** Une plateforme modulaire vous permettra de déployer l'automatisation par étapes. Grâce à son extensibilité, vous pourrez si nécessaire intégrer des outils de sécurité supplémentaires provenant d'autres fournisseurs.

Faites avancer la sécurité dans votre entreprise grâce à Red Hat

La solution **Red Hat® Ansible® Automation Platform** est une base qui permet de créer et d'exploiter des services d'automatisation à grande échelle. Elle fournit tous les outils et toutes les fonctions dont vous avez besoin pour mettre en œuvre l'automatisation de la sécurité. Elle associe un langage d'automatisation simple et facile à lire à un environnement d'exécution modulable et éprouvé ainsi qu'à des capacités de partage et de collaboration sécurisées. Avec sa base ouverte, vous pouvez réunir et automatiser presque toutes les tâches que vous souhaitez dans votre infrastructure informatique et de sécurité, créant ainsi une plateforme commune qui favorisera la collaboration et le partage dans l'ensemble de votre entreprise. La solution Red Hat Ansible Automation Platform a également généré des résultats probants dans d'autres domaines, tels que l'exploitation informatique et réseau ou encore le DevOps.

La plateforme inclut une série de **collections Ansible axées sur la sécurité**, telles que des modules, des rôles et des playbooks. Ces ressources coordonnent l'activité des différentes catégories de solutions de sécurité pour une réponse plus unifiée aux cybermenaces et aux opérations de sécurité :

- Enchaînement des workflows et playbooks pour une réutilisation modulaire
- Consolidation et centralisation des journaux
- Prise en charge des contrôles d'accès et services d'annuaire local
- Intégration des applications externes à l'aide des interfaces de programmation d'application (API) RESTful

La solution Red Hat Ansible Automation Platform inclut également des outils et capacités qui permettent d'optimiser vos efforts d'automatisation. **Automation Analytics** fournit des informations sur la façon dont votre entreprise utilise l'automatisation. **Automation Hub** permet aux membres des équipes d'accéder à des contenus certifiés relatifs à l'automatisation via un référentiel centralisé. Enfin, **Content Collections** simplifie la gestion, la distribution et l'utilisation des ressources dédiées à l'automatisation.

Sollicitez l'aide d'experts

Red Hat peut vous aider à déployer l'automatisation plus rapidement et efficacement.

- **Le programme Red Hat Services Journey: Automation Adoption** fournit un cadre pour gérer un parcours d'adoption de l'automatisation à l'échelle de l'entreprise.
- **Les services de formation et de certification Red Hat** proposent des formations et certifications pratiques pour vous aider à utiliser l'automatisation efficacement.
- **Les services d'assistance Red Hat** vous accompagnent pour assurer la réussite de votre transition. Les services d'assistance web primés[8] mettent à votre disposition des meilleures pratiques, des documents, des mises à jour, des alertes de sécurité et des correctifs. Vous pouvez également contacter un ingénieur de l'assistance ou un responsable de compte technique pour résoudre certains problèmes et bénéficier de conseils spécialisés.
- Grâce aux **collections de contenus partenaires certifiés**, vous pourrez facilement automatiser le matériel et les logiciels d'un large éventail de fournisseurs. Ce contenu d'automatisation fiable et préconçu est disponible dans l'Automation Hub et est pris en charge par le partenaire et par Red Hat.

8 Récompenses et prix octroyés au portail client Red Hat, **access.redhat.com/recognition**.

La solution Red Hat Ansible Automation Platform offre une véritable valeur métier

La solution Red Hat Ansible Automation Platform permet d'automatiser votre centre opérationnel de sécurité de façon simple et efficace. Les études menées par les analystes auprès d'entreprises qui utilisent la solution Red Hat Ansible Automation Platform mettent en évidence une valeur métier significative. En effet, IDC a interrogé plusieurs décideurs à propos de leur expérience avec la solution Red Hat Ansible Automation Platform. Il en ressort que chaque entreprise a amélioré de manière significative la productivité, l'agilité et l'exploitation grâce à l'automatisation.

de hausse d'efficacité et de productivité des équipes chargées de la sécurité informatique[9]

de hausse d'efficacité dans l'atténuation de l'impact des incidents[9]

de hausse d'efficacité des correctifs de sécurité[9]

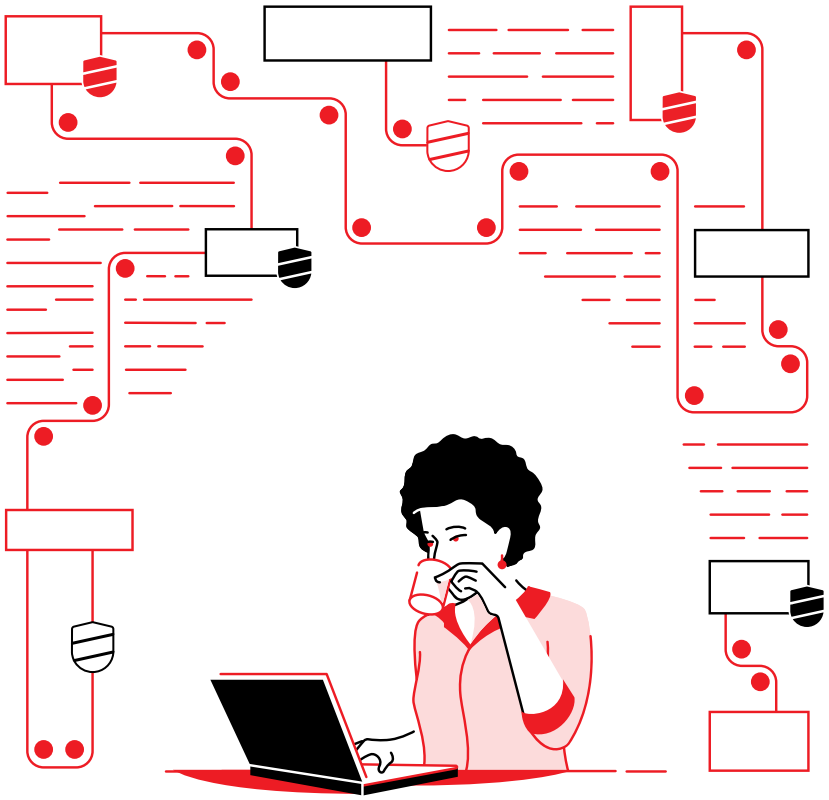
« La solution Red Hat Ansible Automation Platform est formidable pour rassembler les équipes informatiques. Les équipes chargées des serveurs, de la sécurité, des réseaux et des bases de données peuvent toutes travailler de leur côté, puis utiliser Red Hat Ansible Automation pour créer leurs propres playbooks. »[9]

Lire le rapport d'analyste

9 *Livre blanc IDC, commissionné par Red Hat. « Red Hat Ansible Automation améliore l'agilité informatique et réduit les délais de commercialisation », juin 2019.* redhat.com/fr/resources/business-value-red-hat-ansible-automation-analyst-paper.

Prêt à simplifier votre centre opérationnel de sécurité ?

L'automatisation peut vous aider à identifier et à traiter plus vite et à grande échelle le nombre croissant de menaces pour la sécurité. Red Hat vous aide à protéger votre entreprise en réunissant vos équipes, outils et processus de sécurité au sein d'une seule plateforme d'automatisation collaborative et cohérente.



Découvrez comment automatiser la sécurité avec la solution Red Hat Ansible Automation Platform : **red.ht/automate-security**

F24343_0720_KVM

Red Hat