Red Hat

Renforcer la sécurité grâce à l'automatisation

Recueil de témoignages client Red Hat

Sommaire

Intro-duction

L'automatisation fait évoluer la sécurité

L'intégration des équipes et des solutions informatiques au sein d'un environnement en rapide évolution est un défi que chaque entreprise se doit de relever. Bien que chaque approche de la sécurité soit différente, il existe des stratégies qui peuvent être assimilées et adaptées pour protéger vos données importantes, applications, systèmes informatiques, réseaux et appareils contre toute activité malveillante ou non sollicitée.

Pour mettre en lumière ces stratégies, nous avons réuni dans ce livre numérique cinq témoignages de clients Red Hat® Ansible® Automation Platform qui utilisent l'automatisation pour intégrer leurs solutions de sécurité et les mettre à l'échelle, afin d'analyser les menaces et d'y répondre au sein de leur entreprise de manière coordonnée et unifiée.

Comment l'automatisation peut-elle améliorer la sécurité ?

La plupart des entreprises disposent d'une équipe de sécurité compétente, mais ne peuvent pas consacrer le temps et les ressources nécessaires à une configuration manuelle pour protéger les systèmes et les applications, surtout lorsque ces derniers se comptent par milliers.

L'automatisation permet de combler ce déficit de compétences et de ressources grâce à l'application de normes de sécurité qui peuvent être adaptées pour répondre à des exigences internes et externes en matière de sécurité. Les temps de réponse et la vulnérabilité sont ainsi considérablement réduits.

> ***Les entreprises qui ont entièrement déployé l'IA et l'automatisation ont été en mesure de détecter et contenir les failles de sécurité beaucoup plus rapidement que celles qui n'ont pas réalisé ces déploiements.***
>
> IBM, « Rapport 2022 sur le coût d'une violation de données », juillet 2022.

Avec Ansible Automation Platform, vous pouvez automatiser et intégrer des solutions de sécurité pour examiner les menaces dans l'entreprise et y répondre de manière coordonnée et unifiée, grâce à un ensemble de modules, de rôles et de playbooks.

En quoi consiste une approche de sécurité unifiée ?

Les solutions de sécurité évoluent en permanence pour continuer à devancer les menaces. Il est important de tenir compte des points suivants :

Enrichissement des investigations

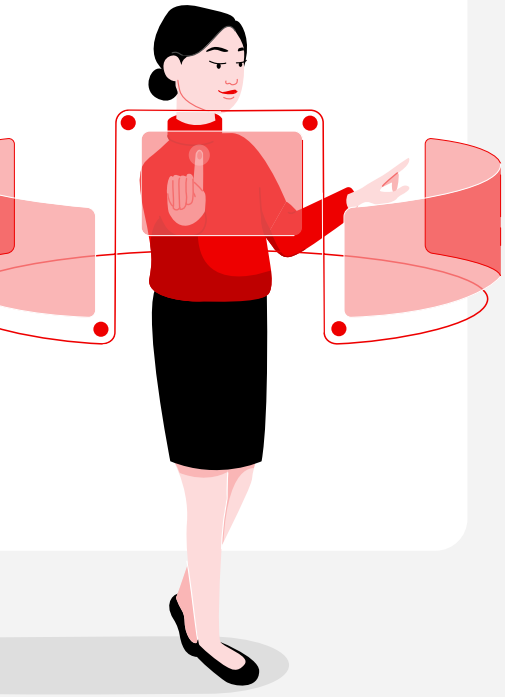
La collecte des journaux des pare-feu, des systèmes de détection d'intrusion et d'autres systèmes de sécurité programmatiques permettent l'enrichissement à la demande des opérations de triage effectuées via des systèmes de gestion des informations et des événements de sécurité.

Traque des menaces

Réglez automatiquement le niveau de journalisation et créez de nouvelles règles de détection d'intrusion et politiques de pare-feu pour détecter les menaces plus rapidement.

Résolution des incidents

Effectuez des actions qui accélèrent l'automatisation, par exemple la mise sur liste noire d'adresses IP ou de domaines, la mise sur liste blanche du trafic non menaçant ou l'isolation des charges de travail suspectes pour un examen futur.



Pourquoi choisir Ansible pour automatiser la sécurité ?

La sécurité est l'affaire de tous. Ansible est un puissant outil sans agent qui rend l'automatisation accessible dans l'entreprise, de l'exploitation informatique au développement en passant par les ingénieurs réseau et les équipes de sécurité, et ce, grâce à un langage lisible par l'utilisateur. Les entreprises peuvent ainsi mettre en place les actions suivantes :

- Augmenter la productivité. Ansible utilise un langage simple et lisible par l'utilisateur, ce qui élimine le besoin de recourir à des compétences spécialisées pour le codage ou la gestion afin que les tâches soient exécutées dans le bon ordre.
- Gérer l'ensemble de l'infrastructure informatique. Vous pouvez collecter et auditer des informations, et gérer efficacement la configuration ainsi que l'orchestration des workflows.
- Améliorer l'efficacité et la sécurité. Une architecture sans agent vous permet de déployer des solutions plus rapidement sans subir la vulnérabilité des agents à exploiter ou à mettre à jour.

Les témoignages client ci-dessous illustrent la puissance et l'évolutivité de l'automatisation pour la sécurité, et présentent la manière dont une plateforme d'automatisation telle qu'Ansible Automation Platform permet aux entreprises d'améliorer leur posture de sécurité.

1

EMORY UNIVERSITY

L'université Emory atténue la menace sudo avec Red Hat Ansible Automation Platform

On pensait ne pas pouvoir appliquer de correctifs à des serveurs Linux tous les 30 jours, mais Red Hat Ansible Automation Platform a rendu cela possible, voire nécessaire.

Steve Siegelman, responsable de l'ingénierie des systèmes, Bureau des technologies de l'information, université Emory

Située à Atlanta, dans l'État de Géorgie, l'université Emory accueille plus de 15 000 étudiants au sein de ses campus. En raison des recherches qu'elle mène en collaboration avec des institutions du monde entier et de son statut d'opérateur du plus grand système de santé de l'État de Géorgie, l'établissement est logiquement la cible de cyberattaques, dont le but est d'accéder à des informations confidentielles et de les exploiter par le biais de leur empreinte numérique.

Une fois la vulnérabilité exploitée, l'intrus est susceptible de naviguer discrètement au sein du réseau, de collecter du contenu propriétaire et de disparaître sans avoir été détecté. Le Bureau des technologies de l'information (Office of Information Technology, OIT) de l'établissement est chargé d'assurer le bon fonctionnement des systèmes pour les étudiants, le personnel, les enseignants, les chercheurs et toutes les parties prenantes afin de protéger les réseaux et les données contre tout accès non autorisé et toute faille de sécurité potentielle. C'est pour cette raison que la situation a été très critique en janvier 2021, lorsque l'équipe Red Hat a informé l'OIT d'une vulnérabilité au sein des systèmes Red Hat Enterprise Linux® de l'université, ce qui a perturbé la commande sudo du système d'exploitation.

L'automatisation avec Ansible accélère la correction des risques pour la sécurité

Des correctifs de mise à jour appliqués en quelques heures plutôt qu'en quelques semaines

Chargé de la gestion de plus de 500 serveurs sous Red Hat Enterprise Linux, l'OIT savait qu'il aurait du mal à installer tous les correctifs manuellement, ce qui exposerait l'infrastructure de l'université à des risques. Pour pallier ce problème, un playbook Ansible a été utilisé afin d'appliquer automatiquement les correctifs à chaque serveur. Une tâche qui aurait pris jusqu'à deux semaines à réaliser sur l'ensemble des serveurs n'a pris que quatre heures grâce à un travail collectif.

Plus de ressources pour des projets à plus forte valeur ajoutée

La solution Ansible Automation Platform a d'abord été utilisée pour les systèmes financiers de l'établissement avant d'être déployée aux systèmes réservés aux étudiants et aux ressources humaines. « Comme de nombreuses entreprises, nous sommes contraints d'assumer une charge de travail plus importante avec le même nombre de personnes. Lorsque vous n'avez plus à réaliser de tâches répétitives gérées par Ansible Automation Platform, vous permettez à votre équipe de travailler sur d'autres projets plus essentiels », explique Steve Siegelman.

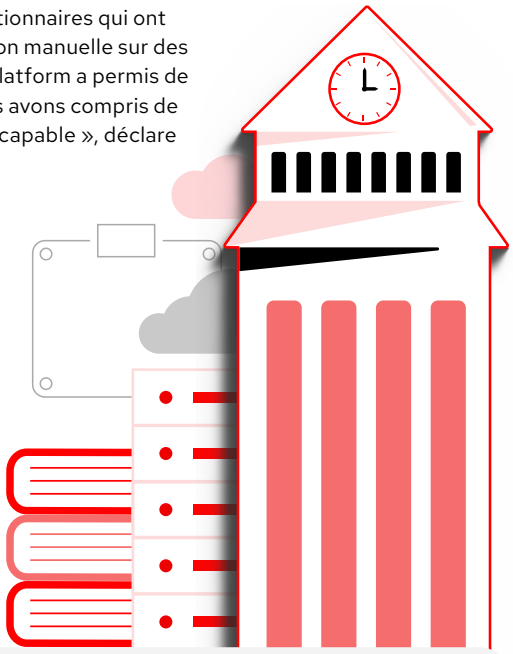
Plus de temps pour permettre aux équipes informatiques de gérer les défis liés à la COVID-19

Un autre exemple pour illustrer la flexibilité d'Ansible Automation Platform est celui de mars 2020, lorsque l'université Emory a été contrainte de fermer ses portes et d'imposer le télétravail à l'ensemble des étudiants et du personnel, comme pratiquement toutes les écoles et entreprises.

L'OIT avait besoin de déployer rapidement des serveurs de base de données pour gérer le suivi des principales équipes et libérer le campus. Les personnes sélectionnées ont rempli des questionnaires qui ont servi à alimenter le système. Une telle configuration manuelle sur des serveurs aurait pris plusieurs jours, mais Ansible Platform a permis de la réaliser en quelques minutes seulement. « Nous avons compris de quoi l'automatisation au niveau du back-end était capable », déclare Steve Siegelman.

L'innovation en matière de sécurité au-delà du campus grâce à l'automatisation

Le besoin d'automatisation est essentiel pour garantir les projets futurs de l'université, notamment dans le cadre de sa transition vers le cloud. « Nos systèmes existants sont plus ou moins récents, et nous mettons tout en œuvre pour déployer notre plateforme AWS », poursuit Steve Siegelman. « Ansible Automation Platform garantit la reproductibilité et la rationalisation des processus entre ces différents systèmes. Qu'il s'agisse d'une plateforme dans le cloud ou sur site, chaque chose est à sa place. »



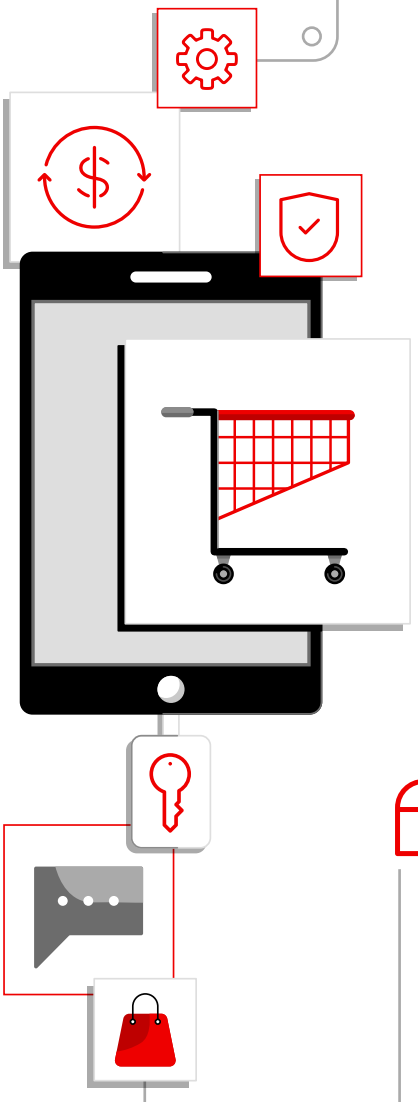
Télécharger
le témoignage de
l'université Emory

2

Le distributeur Schwarz automatise son infrastructure avec Red Hat Ansible Automation Platform

Le groupe allemand Schwarz est le quatrième plus grand distributeur au monde et détient plus de 12 500 magasins dans 33 pays. Le groupe, qui renforce rapidement sa présence à l'international, doit gérer les magasins de façon cohérente et faire preuve d'agilité pour en ouvrir d'autres rapidement, en particulier sur les nouveaux marchés, tout en veillant à s'adapter à la demande locale et à atténuer les risques.

Pour y parvenir, le groupe est passé du système de gestion Puppet à Red Hat Ansible Automation Platform. Grâce à une base d'exploitation cohérente, il est en mesure d'utiliser des capacités de libre-service pour déployer rapidement des services numériques novateurs et préserver sa compétitivité tout en garantissant une posture de sécurité forte.



La cohérence comme garantie de sécurité au sein de milliers de magasins dans le monde

Schwarz IT compte plus de 3 500 ingénieurs pour assurer le bon fonctionnement de plus de 1 000 systèmes SAP et de 28 Po de stockage en datacenter. Chaque magasin Schwarz dispose d'un Storeserver, un système d'exploitation central installé par l'équipe informatique locale de l'entreprise et qui contrôle un ensemble de fonctions du magasin, parmi lesquelles les systèmes de caisse, les caméras de surveillance, le recyclage et les programmes de fidélité.

Pour améliorer la gestion des utilisateurs et les autorisations, Schwarz IT a souhaité pouvoir bénéficier de capacités de libre-service contrôlées et efficaces afin d'accélérer les processus de déploiement. Le groupe a donc décidé de mettre en œuvre Ansible Automation Platform.

> *Nous n'étions pas satisfaits de la version communautaire à cause de la complexité et de la lenteur des processus. L'automatisation est essentielle à notre activité. Nous avons choisi la solution de Red Hat pour l'assistance aux entreprises qu'elle inclut.*
>
> Felix Kuehner, responsable des Storeservers, Services d'infrastructure de base, Schwarz IT

Au cours d'un atelier de deux jours, les équipes de Schwarz IT ont collaboré avec les experts techniques de Red Hat afin d'examiner l'architecture et de définir des meilleures pratiques pour la nouvelle solution d'automatisation.

Le groupe exécute aujourd'hui plus de 5 000 tâches par jour avec Ansible Automation Platform pour gérer ses Storeservers.

Mieux gérer les risques avec l'accès basé sur les rôles

Avec les fonctionnalités en libre-service d'Ansible Automation Platform, Schwarz IT peut contrôler plus efficacement les accès aux systèmes par les applications et équipes de développement. Le contrôle d'accès basé sur les rôles permet aux équipes chargées des applications d'automatiser les déploiements depuis un compte classique, sans demander un accès root aux systèmes centraux. « Cette fonction offre un niveau élevé de cohérence et favorise la gestion proactive de tous les projets, y compris les nouveaux », explique M. Kuehner.

Ravie de la nouvelle solution Ansible Automation Platform, la division Schwarz IT reste engagée dans une démarche d'amélioration de la cohérence et de la réactivité des magasins du groupe.

> ***Nous avons apprécié notre collaboration avec Red Hat et nous espérons continuer à utiliser Ansible pour moderniser notre entreprise et gagner en efficacité.***
>
> Felix Kuehner, responsable des Storeservers, Services d'infrastructure de base, Schwarz IT

Télécharger
le témoignage de Schwarz

Agile Defense améliore la conformité en matière de sécurité avec Red Hat Ansible Automation Platform

3

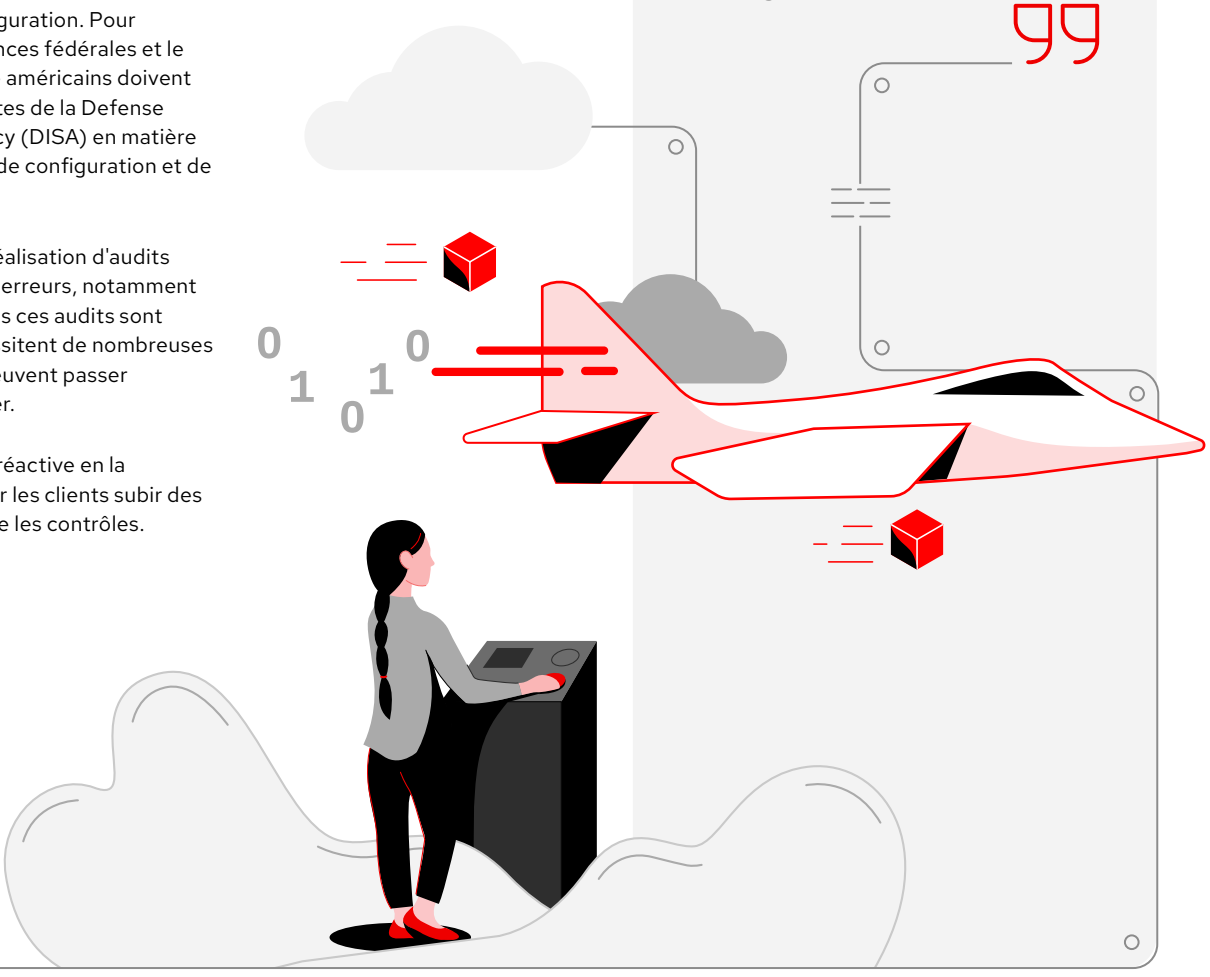
Agile Defense est une entreprise leader dans le domaine des services liés aux technologies de l'information. Elle est basée à Reston, en Virginie, et possède de nombreux clients au sein du gouvernement américain, parmi lesquels plusieurs agences civiles et diverses branches du département de la Défense des États-Unis. La sécurité informatique est donc une priorité essentielle.

Le fait de pouvoir empêcher les cybercriminels d'obtenir un accès non autorisé à ses systèmes et son infrastructure constitue également une priorité. De nombreuses failles surviennent suite à des erreurs de configuration. Pour éviter les menaces, les agences fédérales et le département de la Défense américains doivent respecter des normes strictes de la Defense Information Systems Agency (DISA) en matière d'information, de sécurité, de configuration et de conformité.

Ces normes impliquent la réalisation d'audits réguliers pour contrôler les erreurs, notamment celles de configuration, mais ces audits sont répétitifs, coûteux et nécessitent de nombreuses ressources. Les agences peuvent passer plusieurs mois à les préparer.

Une approche manuelle et réactive en la matière impliquait de laisser les clients subir des vulnérabilités connues entre les contrôles.

> ***Les tâches de production de nos clients étaient interrompues en prévision d'une inspection pendant la mise en conformité de leur documentation.***
>
> Shawn Draper, ingénieur en solutions chez Agile Defense



L'automatisation pour atténuer les effets néfastes des audits

Les erreurs de configuration et les audits représentent un défi de taille pour de nombreux clients gouvernementaux d'Agile Defense. Spécialisée dans l'innovation par les technologies de l'information, l'entreprise de services informatiques s'est associée à Red Hat pour créer STIG (Security Technical Implementation Guide), un outil de configuration, de correction et de création de rapports. Cette solution d'automatisation effectue des audits de systèmes ad hoc, corrige éventuellement les erreurs de configuration et génère des rapports sur l'état des appareils. Aussi connue comme la solution CPaaS (Compliance as a Service) d'Agile Defense, STIG utilise Red Hat Ansible Automation Platform en raison de ses capacités d'automatisation flexibles et évolutives.

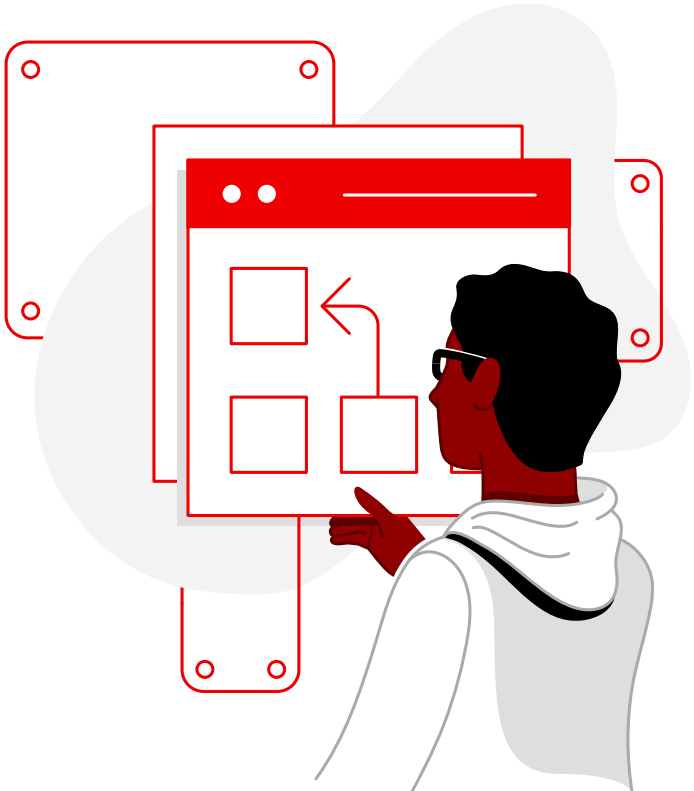
De plus, Red Hat a travaillé avec la DISA sur une solution STIG pour Red Hat Enterprise Linux et connaît l'importance de créer des normes pour chaque appareil, système d'exploitation et version logicielle.

> ***Nous avons choisi la solution Red Hat Ansible Automation Platform pour résoudre ce problème, car elle peut communiquer avec tout.***
>
> Shawn Draper, ingénieur en solutions chez Agile Defense

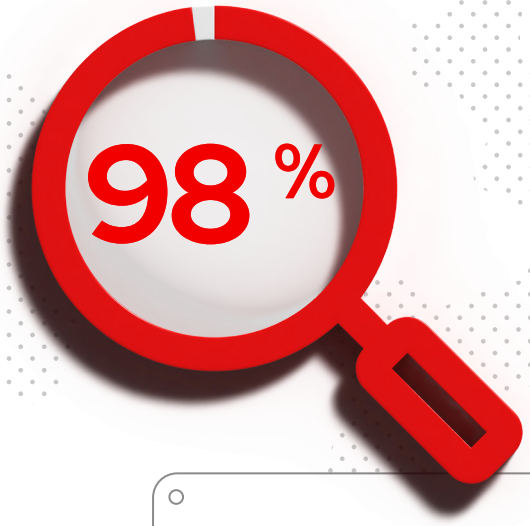
L'avantage des playbooks Ansible en matière de sécurité

La solution CPaaS utilise les capacités d'automatisation de la gestion des configurations de Red Hat Ansible Automation Platform pour auditer les vulnérabilités. « Red Hat Ansible Automation Platform se connecte aux appareils et exécute les commandes spécifiées dans un playbook Ansible », explique M. Draper.

L'identification automatique des erreurs par la solution CPaaS lui permet également de les corriger en suivant les commandes d'un playbook Ansible créé sur mesure. Agile Defense a conçu de nombreux playbooks dont le but est de tester un type d'appareil différent, par exemple pour les plateformes Red Hat, les appareils Windows, les hyperviseurs VMware, les routeurs et commutateurs Cisco ainsi que les pare-feu.



Réduction du temps passé par les clients sur les audits de



La solution CPaaS simplifie également la partie administrative et produit automatiquement tous les documents nécessaires. Plus précisément, elle utilise Ansible Automation Platform afin de créer un fichier de vérification XML (consultable dans STIG Viewer de DISA) pour chaque appareil sur le réseau et chaque vulnérabilité identifiée, de manière à les présenter à l'auditeur. Ces fonctionnalités permettent d'afficher des informations actualisées et de démontrer la mise en œuvre de configurations de sécurité particulières. Ansible Automation Platform permet également aux clients d'étendre les capacités de la solution CPaaS pour gérer les workflows et l'inventaire, planifier des audits et mettre en place le contrôle d'accès basé sur les rôles. La cohérence entre les appareils est également garantie par la solution CPaaS.

> ***L'une des forces de l'automatisation et qu'elle réalise la même tâche en permanence.***
>
> Shawn Draper

La surveillance proactive de la posture de sécurité d'une agence par la solution CPaaS est essentielle pour continuer à se protéger des cybermenaces. Cette surveillance impliquait jusqu'ici l'utilisation de nombreuses ressources et de logiciels supplémentaires au niveau des points de terminaison. Grâce à l'analyse des vulnérabilités réalisée par Ansible Automation Platform, la solution CPaaS d'Agile Defense permet à ses clients gouvernementaux de réduire de 98 % le temps passé sur les audits.

Télécharger
le témoignage d'Agile Defense

4

Cepsa améliore son efficacité avec Red Hat Ansible Automation Platform

Cepsa, une multinationale du secteur de l'énergie et de la chimie, s'est donné pour mission de réduire son empreinte carbone à l'échelle mondiale. En 2022, l'entreprise a présenté sa stratégie pour devenir leader de la mobilité durable, des biocarburants et de l'hydrogène vert. Elle souhaite se concentrer sur l'Espagne et le Portugal, et ainsi devenir un acteur majeur de la transition énergétique.

Pour y parvenir, il lui était impératif d'augmenter l'efficacité et d'assurer la conformité avec les exigences réglementaires, tout en réduisant les coûts, les risques et les temps d'arrêt. L'entreprise a donc commencé à automatiser ses processus pour réduire le nombre d'heures de travail, améliorer les temps de réponse du service et renforcer la sécurité informatique. En collaboration avec les services de consulting Red Hat, Cepsa a utilisé Red Hat Ansible Automation Platform pour faire de l'automatisation le moteur de sa stratégie d'innovation, sous la supervision d'un responsable spécialisé. L'entreprise a ainsi augmenté sa productivité de 35 % et accéléré ses temps de réponse de 10 à 15 %.

Améliorer la sécurité informatique grâce à un contrôle des accès renforcé

Forte du succès des premiers projets d'automatisation et de son long partenariat avec Red Hat, Cepsa a décidé d'étendre l'utilisation d'Ansible à toute l'entreprise. La solution Ansible Automation Platform offre aux entreprises une base qui permet de créer et d'exploiter des services d'automatisation à grande échelle, ainsi qu'un environnement modulable, collaboratif et éprouvé. L'efficacité est ainsi améliorée et les environnements informatiques complexes au sein desquels la sécurité est primordiale sont rationalisés.

La syntaxe simple du playbook Ansible a permis à Cepsa de définir des paramètres de sécurité pour chaque partie de son système, qu'il s'agisse des règles de pare-feu, du verrouillage de comptes utilisateur et de groupes ou de politiques de sécurité personnalisées. Grâce à la rationalisation des processus, Cepsa a été en mesure de réduire le nombre d'autorisations supplémentaires accordées par les administrateurs des systèmes, et ainsi d'atténuer les risques. Aujourd'hui, les utilisateurs sont regroupés par rôle et par service. Ils reçoivent donc uniquement le niveau d'autorisation dont ils ont besoin.

L'entreprise a ainsi augmenté sa productivité de 35 % et accéléré ses temps de réponse de 10 à 15 %.

L'équipe technique peut désormais accéder à Ansible Automation Platform et redémarrer le service sans informations d'identification, ce qui garantit l'exécution du processus conformément au code prédéterminé.

Productivité
en hausse de **35 %**

Temps de réponse
réduits de **10 à 15 %**

L'automatisation a contribué à un changement de culture positif, et ainsi renforcé la collaboration entre les équipes. Nous collaborons avec Red Hat pour mettre en œuvre les meilleures pratiques et bénéficier de leur expertise dans toute l'entreprise.

Francisco José Martín, responsable de l'automatisation, service Exploitation et opérations, Cepsa

Favoriser une culture axée sur la sécurité grâce à des conseils d'experts en automatisation

Les services de consulting Red Hat ont aidé l'équipe de Cepsa à mettre en place les changements nécessaires pour tirer le meilleur parti de sa nouvelle stratégie d'automatisation et des technologies associées. Au contact des spécialistes Red Hat, elle a aussi pris conscience de l'intérêt de travailler de façon agile et d'améliorer en permanence la qualité via une approche CI/CD (intégration et distribution continues).

Télécharger
le témoignage de Cepsa

5

SIEMENS

Siemens optimise la sécurité des communications avec Red Hat Ansible Automation Platform

Basée à Munich, en Allemagne, Siemens est la plus grande entreprise d'ingénierie en Europe. Ce groupe technologique international concentre ses activités principalement sur l'électrification : génération, transmission et distribution de l'énergie, solutions de réseaux électriques intelligents, et optimisation de l'utilisation de l'énergie électrique.

En raison de la nature sensible de son activité, Siemens s'engage à rester à la pointe de la technologie en matière de sécurité. Pour protéger efficacement l'accès aux informations confidentielles, les 295 000 personnes employées par l'entreprise ainsi que les 100 000 collaborateurs de ses partenaires utilisent des infrastructures à clé publique (PKI) afin de vérifier les certificats et l'identité des clés publiques. L'utilisation croissante de cette technologie a pour but de sécuriser les communications de type IoT (Internet des objets) et assure désormais le bon fonctionnement de deux environnements PKI pour différents cas d'utilisation d'applications.

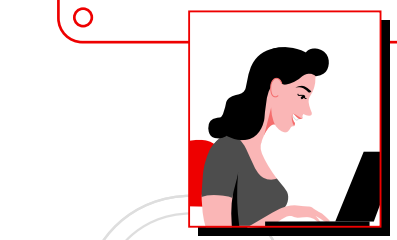
> *Cet aspect est particulièrement important, car l'infrastructure en tant que code avec Red Hat Ansible Automation Platform est plus qu'un simple outil à mettre en œuvre : elle nécessite un changement d'état d'esprit radical de la part des administrateurs système.*
>
> Rufus Buschart, responsable de l'infrastructure à clé publique (PKI), Siemens

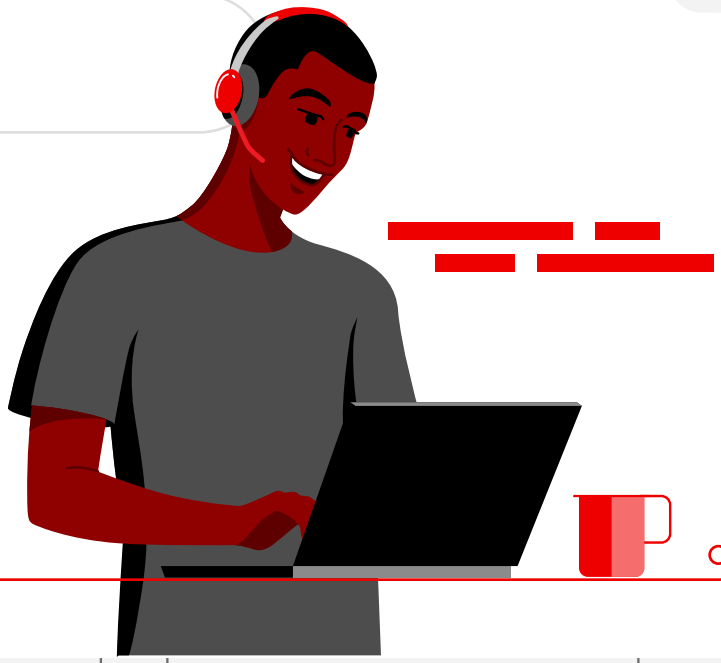
L'équipe Red Hat est disponible dès que nous la sollicitons, et nous cherchons à travailler avec elle pour développer un ensemble de meilleures pratiques qui permettront à l'automatisation d'optimiser l'efficacité et l'innovation de notre entreprise.

Rufus Buschart

À mesure que les communications entre les équipes de service augmentent au sein de l'entreprise, la configuration se complexifie pour l'équipe PKI de Siemens. Pour répondre à ce besoin, l'entreprise a remplacé sa solution d'automatisation existante par Ansible Automation Platform.

Cette transition lui a permis d'automatiser les tâches administratives, d'augmenter la qualité des configurations et de renforcer la sécurité des communications dans toute l'entreprise. De plus, Siemens a pu bénéficier de notre expertise et prévoit une collaboration future afin d'automatiser les processus de test dans le but d'établir un modèle commun pour le déploiement continu.





Télécharger le témoignage de Siemens

Con-clusion

Ansible Automation Platform permet aux entreprises de gérer les systèmes de sécurité automatisés afin de toujours devancer les attaques malveillantes. Grâce à l'accès à des centaines de modules qui aident les équipes de sécurité à automatiser tous les aspects de leur environnement et leurs processus informatiques, Ansible peut s'intégrer à de nombreuses équipes pour protéger les périmètres de sécurité complexes, unifier votre approche de sécurité et renforcer votre posture de sécurité.

Avec la solution Ansible Automation Platform, les équipes de sécurité bénéficient des avantages suivants :

Enchaînement des workflows et playbooks pour une réutilisation modulaire

Les équipes de sécurité peuvent configurer une séquence de tâches qui partagent un inventaire, des playbooks ou des autorisations pour automatiser totalement les tâches de recherche ou de correction.

Consolidation et centralisation des journaux

L'intégration à des services externes de compilation de journaux tiers aide les équipes de sécurité à identifier les tendances, analyser les événements liés à l'infrastructure, surveiller les anomalies et mettre en corrélation des événements disparates.

Prise en charge des contrôles d'accès et services d'annuaire local

L'association de services d'annuaire utilisateur et de l'infrastructure permet aux équipes de sécurité de centraliser l'accès aux tâches ainsi que leur exécution, d'attribuer des sous-ensembles d'exploitation à des rôles spécifiques et de partager des tâches avec d'autres groupes.

Intégration d'applications externes à l'aide d'API RESTful

Les équipes de sécurité peuvent utiliser cette solution pour gérer d'autres applications d'entreprise, comme les solutions d'orchestration, d'automatisation et de réponse aux incidents de sécurité informatique (SOAR).

Renforcez votre posture de sécurité avec l'automatisation.

En savoir plus sur Red Hat Ansible Automation Platform

EUROPE, MOYEN-ORIENT ET AFRIqUE (EMEA)

00800 7334 2835
europe@redhat.com

France

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