# Renforcer le niveau de cyberconformité en automatisant l'infrastructure

Surveillez les événements de plusieurs organismes et automatisez les réponses avec leur playbook individuel

**Solutions Red Hat**

Red Hat Integration connecte les données des périphériques réseau, des serveurs et des appareils en périphérie du réseau de plusieurs organismes.

Open Data Hub exécuté sur Red Hat OpenShift permet d'entraîner des modèles d'apprentissage automatique à reconnaître les comportements malveillants.

Red Hat Decision Manager fait correspondre les événements de sécurité et les réponses en fonction des règles de chaque organisme.

Red Hat Ansible Automation Platform appelle automatiquement l'action indiquée dans le playbook de l'organisme lors de la détection d'une menace.

## La séparation des services ne suffit pas à contrer les logiciels malveillants

Les organismes fédéraux chargés de faire respecter la loi doivent protéger des données telles que les casiers judiciaires, les enquêtes criminelles, les données biométriques, les déclarations d'impôts, les images de vidéosurveillance et les dossiers du personnel. La divulgation de données sensibles peut perturber l'activité, mettre les équipes en danger et décrédibiliser le gouvernement. Souvent, les attaques consistent en des exfiltrations de données et des saturations de service.

Au sein des forces de l'ordre, la cyberconformité est souvent altérée par ce qui suit :

- **Personnel limité.** Les équipes de sécurité ne disposent pas des ressources nécessaires pour surveiller le volume de trafic croissant, notamment les flux d'appareils en périphérie du réseau. Les caméras IP, par exemple, peuvent transporter des logiciels malveillants. La détection et la correction des menaces prennent plus de temps, ce qui prolonge la vulnérabilité.
- **Surveillance insuffisamment centralisée entre les organismes.** Lorsqu'elles ciblent plusieurs organismes, les attaques sont souvent plus sophistiquées et risquent davantage de conduire à une interruption importante de l'activité ainsi qu'à une fuite de données. Pour ne pas sous-estimer le danger, il faut avoir conscience qu'un événement de sécurité fait partie d'une attaque à plus grande échelle.
- **Impossibilité d'interrompre l'activité lors de la correction.** Souvent, un appareil compromis ne peut être coupé sans interrompre la continuité de l'activité. Les forces de l'ordre ont besoin d'une correction qui s'adapte à la sévérité de la menace.

## La solution : une vue globale des événements réseau et une réponse automatisée

Pour protéger les données publiques, les organismes fédéraux chargés de faire respecter la loi ont besoin de deux capacités qui leur font aujourd'hui défaut : une vue globale de l'ensemble des réseaux et de l'activité des serveurs dans les entreprises, et une correction automatisée basée sur la nature de la menace ainsi que sur le playbook de l'organisme. Il peut s'agir d'utiliser la même liste noire d'adresses réseau dans tous les organismes, d'envoyer des alertes si ces adresses sont détectées, de mettre en quarantaine une charge de travail suspecte jusqu'à la fin de l'enquête ou encore de supprimer un serveur virtuel en cas de comportement anormal pour le remplacer par un nouveau serveur issu d'une source fiable.

Au sein des forces de l'ordre, l'automatisation de la cyberconformité apporte les avantages suivants :

- Les incidents sont détectés plus rapidement.
- Les corrections vont plus vite, ce qui réduit la fenêtre de vulnérabilité.
- Moins de ressources sont nécessaires pour corriger la menace.
- La satisfaction des équipes de cybersécurité augmente, car elles peuvent mettre de côté les tâches de surveillance courantes pour se concentrer sur un aspect plus important de leur travail. Cela favorise en outre le recrutement et la fidélisation.

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

## Pourquoi choisir Red Hat ?

**Sécurité renforcée.** Nos solutions respectent les exigences de sécurité fédérales les plus strictes.

**Écosystème de partenaires.** Grâce à nos partenaires, accédez à des solutions pour l'interrogation des données et la correction automatisée.

**Service approuvé par le gouvernement fédéral.** Le Département de la Sécurité intérieure et le Département de la Défense ainsi que d'autres organismes civils aux États-Unis utilisent Red Hat OpenShift.

**API ouvertes pour plus de flexibilité.** Surveillez vos appareils nouveaux et existants avec des API ouvertes.

**Réduction des coûts.** Nos souscriptions peuvent être plus abordables que des licences de logiciels propriétaires et des contrats d'assistance.

## L'approche de Red Hat en matière d'automatisation de la cyberconformité

Nous offrons une solution complète pour renforcer la cyberconformité en automatisant l'infrastructure.

**Entraînez un modèle d'apprentissage automatique à déterminer quelles activités sont normales et lesquelles ne le sont pas.** Utilisez la plateforme d'intelligence artificielle (IA) Open Data Hub sur Red Hat® OpenShift®. Testez le modèle en simulant des menaces. Ajustez-le en permanence en y ajoutant des données sur de nouvelles menaces et sur les réponses efficaces pour les contrer.

**Faites correspondre différents types de menaces et leur correction.** Avec Red Hat Decision Manager, spécifiez des réponses telles que le blocage de l'adresse IP d'une personne malintentionnée, la mise sur liste blanche du trafic non menaçant, la mise en quarantaine d'une charge de travail suspecte ou le remplacement d'un serveur virtuel infecté par un nouveau serveur.

**Automatisez la surveillance et les réponses des organismes.** Utilisez Red Hat Ansible® Automation Platform pour récupérer les journaux d'activité des pare-feux, systèmes de détection d'intrusion (IDS), appareils en périphérie du réseau et produits d'écosystème, comme Sensu pour la compilation des journaux ou ServiceNow pour la gestion de cas d'exploitation, auprès de plusieurs organismes. Ansible Automation Platform appelle automatiquement l'action indiquée dans le playbook. Si celle-ci ne résout pas le problème, la solution envoie une alerte et crée un ticket dans ServiceNow.

**Aidez les organismes à contrôler leurs playbooks.** Les organismes individuels savent mieux que quiconque le niveau de risque qu'ils peuvent tolérer avant de fermer un service précis. Grâce à Ansible Automation Platform, les équipes de cybersécurité peuvent utiliser une interface web afin d'adapter les seuils, les noms d'hôtes et les playbooks aux exigences de la mission.

**En savoir plus** Pour en savoir plus sur la manière dont nous pouvons aider les équipes informatiques gouvernementales à innover, rendez-vous sur redhat.com/government.

### À propos de Red Hat

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

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

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

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

fr.redhat.com
#F26748_0121