Protection contre les menaces détectées par l'IA

> Chaque semaine, nous devons effectuer des analyses de sécurité et lister les vulnérabilités dans les paquets présents sur les systèmes d'exploitation. Le cas échéant, nous pouvons immédiatement nous rendre sur le site de Red Hat, afin d'obtenir des explications complètes sur les vulnérabilités et de déterminer si nous sommes affectés. Personne d'autre ne le propose pour les autres distributions Linux. Sans Red Hat, nous aurions tout de suite beaucoup de mal à exécuter un environnement de production d'agence gouvernementale, car nous aurions à effectuer toutes les recherches nous-mêmes chaque mois[2].

Ryan Kimbrell,
ingénieur senior en exploitation cloud chez Zoom

Protection contre les vulnérabilités de l'IA

Les tendances en matière de menaces ont fortement évolué. Désormais, les outils de détection basés sur l'IA identifient des vulnérabilités potentielles à un rythme exponentiellement supérieur à celui des normes traditionnelles. En 2025, les équipes de sécurité d'entreprise devaient déjà repousser leurs limites et gérer en moyenne 132 CVE détectées par jour[2]. Au 1er trimestre 2026, ce nombre avait déjà augmenté de 26 %. Les progrès continus des outils de détection des vulnérabilités basés sur l'IA, tels que Mythos, pourraient rendre les approches traditionnelles de gestion des CVE non viables[1].

En 2020, les équipes disposaient généralement d'un délai de 44 jours pour corriger une vulnérabilité avant toute exploitation[3]. En 2025, elles avaient à la place un retard de 7 jours[4]. À l'heure actuelle, les acteurs malveillants peuvent profiter des nouvelles vulnérabilités une semaine avant la publication d'une nouvelle CVE.

En parallèle, les équipes de sécurité d'entreprise continuent d'exercer à vitesse humaine (tri manuel, réunions de gestion des changements et application des contrats de niveau de service en plusieurs semaines ou mois).

Les approches traditionnelles en matière de sécurité informatique ne permettent pas de suivre le rythme de triage nécessaire pour gérer le volume croissant de CVE. En moyenne, dans les grandes entreprises, 37 % des vulnérabilités détectées en un an restent non corrigées, tandis que le délai moyen de correction dans le secteur des logiciels s'élève à 55 jours[5]. Intenable, cette faille de sécurité met les entreprises en difficulté.

4 grands défis actuels pour les équipes de sécurité d'entreprise

Les entreprises doivent actuellement faire face à quatre difficultés cumulées :

1. **Accélération des machines.** Les modèles d'IA découvrent de nouvelles vulnérabilités à une vitesse que les équipes humaines de sécurité et les processus manuels ne peuvent égaler.
2. **Abondance de volume.** L'afflux massif de versions de correctifs que les fournisseurs publient peut submerger les équipes de sécurité, entraîner une baisse de la vigilance face aux alertes et mettre à rude épreuve les workflows traditionnels de gestion des vulnérabilités.
3. **Stabilité et sécurité.** Les équipes retardent l'application des correctifs pour éviter d'interrompre les applications de production.
4. **Écarts de configuration.** Comparée aux évaluations manuelles classiques, la mise en correspondance par IA est beaucoup plus rapide pour les environnements traditionnels et les comptes surchargés d'autorisations.

La solution ne réside pas dans l'accumulation de logiciels de sécurité. Nos clients ont probablement déjà accès aux capacités intégrées de correction dont ils ont besoin. Il leur suffit de les activer dans leur gamme de solutions.

Création d'une base axée sur la sécurité avec Red Hat Enterprise Linux

La solution Red Hat® Enterprise Linux® permet aux entreprises de limiter l'incidence des CVE pendant qu'elles évaluent, testent et déploient des correctifs. Le mode image pour Red Hat Enterprise Linux offre la plateforme sous forme d'image de conteneur signée et versionnée, accompagnée d'une nomenclature logicielle SBOM (Software Bill of Materials). En outre, les architectures SELinux (Security-Enhanced Linux) et fapolicyd (File Access Policy Daemon) ajoutent des couches d'exécution qui contribuent à bloquer toute exécution non autorisée et à limiter les processus compromis.

Identification de l'exposition réelle aux risques avec Red Hat Lightspeed

vant de pouvoir appliquer des mesures de correction à grande échelle, les équipes doivent identifier clairement les zones d'exposition. Au lieu de s'appuyer sur une base de données générique des vulnérabilités, elles doivent s'adapter à leur environnement spécifique, à leurs configurations réelles et à leurs charges de travail actives.

Red Hat Lightspeed aide les entreprises à établir un ordre de priorité pour les CVE dans les systèmes Red Hat Enterprise Linux en combinant les données consultatives et celles des paquets avec des règles de sécurité définies par Red Hat, le regroupement des charges de travail et une évaluation tenant compte de la configuration, notamment des contrôles tels que SELinux et l'exposition des services. Contrairement à l'analyse basée sur les versions, cette solution distingue les systèmes qui présentent des vulnérabilités exploitables de ceux qui sont vulnérables, mais non affectés. Ainsi, les équipes peuvent concentrer leur attention sur les risques sur lesquels elles peuvent agir. Lors de tests réalisés sur 90 hôtes, les processus automatisés de détection et de correction utilisant Red Hat Lightspeed ont permis de réduire le temps d'intervention manuelle des équipes d'administration de 79 % pour les CVE et de 86 % pour les problèmes d'exploitation connus, par rapport à l'utilisation de scripts manuels[6].

Cette précision contextuelle compte aujourd'hui plus que jamais. Le grand nombre de vulnérabilités récemment détectées a donné naissance à une nouvelle forme de paralysie opérationnelle : les alertes intempestives. Lorsque des centaines de CVE sont divulguées en très peu de temps, aucune équipe n'est capable de les évaluer manuellement. Red Hat Lightspeed élimine le superflu et permet au personnel de concentrer ses efforts de correction sur les dangers les plus importants pour son environnement spécifique.

Vérification et contrôle des correctifs avec Red Hat Satellite

Le défi ne se limite pas à l'identification des vulnérabilités à corriger. Pour tester, vérifier, approuver et mettre en production les correctifs adaptés sans créer d'instabilité, il convient de suivre un processus contrôlé et reproductible.

La solution Red Hat Satellite permet la gestion des errata sur site et l'indexation des contenus à grande échelle dans les infrastructures locales, hybrides et entièrement air gap. Satellite crée des vues de contenus, c'est-à-dire des instantanés logiciels vérifiés à un moment précis, et les diffuse dans des environnements de cycle de vie restreints (du développement à la mise en production, en passant par les tests). Les correctifs doivent passer par des passerelles d'approbation définies avant d'atteindre la phase de mise en production, afin de subir une vérification complète en amont du déploiement.

Satellite contribue également à la protection de la chaîne d'approvisionnement des logiciels : les paquets qui intègrent l'environnement sont signés de manière cryptographique et proviennent de nos référentiels vérifiés. Ces capacités restent inchangées même sans accès direct à Internet. Les entreprises qui opèrent dans des environnements hautement réglementés ou déconnectés peuvent ainsi contrôler les logiciels autorisés dans l'ensemble des systèmes. La génération des rapports de conformité est automatisée à l'aide de l'environnement d'analyse OpenSCAP (Open Security Content Automation Protocol). Celui-ci produit des rapports vérifiables conformément aux pratiques de l'intégration continue, aux directives STIG de la DISA (Defense Information Systems Agency's Security Technical Implementation Guides) et aux références de sandbox de développement propres au secteur des cartes de paiement.

Correction à grande échelle avec Red Hat Ansible Automation Platform

Une fois les correctifs vérifiés et préparés, il reste un défi : les appliquer de manière cohérente à un ensemble complexe de systèmes hybrides comprenant des milliers de serveurs, plusieurs environnements cloud, des datacenters sur site et des environnements air gap, le tout sans créer de backlog manuel qui instaurerait un nouvel écart de vitesse.

La solution Red Hat Ansible® Automation Platform permet d'appliquer des corrections à grande échelle dans l'ensemble des systèmes hybrides à l'aide d'une approche PaC (Policy-as-Code), à des fins de cohérence, d'auditabilité et de reproductibilité. Le composant Event-Driven Ansible met fin à la boucle en automatisant le workflow de correction : lorsque Satellite termine une synchronisation de référentiel qui contient un nouveau correctif de sécurité, un webhook indique automatiquement à Ansible Automation Platform d'identifier les systèmes vulnérables et de déclencher le playbook de correction. Les systèmes à haut risque peuvent être automatiquement mis en quarantaine avant même le déploiement d'un correctif, ce qui limite l'exposition pendant la période d'intervention décisive. Chaque action est exécutée à l'aide des collections de contenus certifiés Red Hat Ansible Certified Content Collection. Il est ainsi possible de maintenir un journal d'audit PaC clair, qui contribue à répondre aux exigences de conformité sans outil supplémentaire.

Notre solution de correction en boucle fermée n'est pas un simple regroupement de produits distincts. Il s'agit d'une seule gamme intégrée, accessible via une souscription unique et prise en charge par une même équipe. Les entreprises qui utilisent nos solutions ont probablement déjà mis en place les outils nécessaires pour se protéger contre les menaces basées sur l'IA. La connexion de ces outils réduit le délai moyen de correction, qui passe de plusieurs semaines d'interventions manuelles à quelques heures de tâches automatisées, grâce à un journal d'audit complet et vérifiable pour chaque système de l'environnement.

Informations supplémentaires sur Red Hat Lightspeed

Vous souhaitez accélérer la correction des CVE ? Apprenez-en plus sur Red Hat Lightspeed.

Informations supplémentaires sur Red Hat Satellite

Pour en savoir plus sur la manière dont Red Hat Satellite rationalise la gestion de l'infrastructure à grande échelle, consultez la page du produit.

Stratégie d'automatisation optimisée

Pour découvrir comment Red Hat Ansible Automation Platform contribue à réduire les erreurs humaines dans les processus répétitifs, consultez la page du produit.

1. Programme CVE, « Metrics », CVE : Common Vulnerabilities and Exposures, consulté en juin 2026
2. Étude de cas Red Hat, « Sécurité renforcée pour Zoom for Government grâce à une plateforme Red Hat », 10 mars 2023
3. Article de blog Google Cloud, « How Low Can You Go? An Analysis of 2023 Time-to-Exploit Trends », 15 octobre 2024
4. Article de blog Google Cloud, « M-Trends 2026: Data, Insights, and Strategies From the Frontlines », 23 mars 2026
5. Edgescan, « 2026 Vulnerability Statistics Report », 2026
6. Rapport Principled Technologies, commissionné par Red Hat, « Save administrator time with the automated remediation capabilities of Red Hat Lightspeed », novembre 2025 (version révisée)

À propos de Red Hat

Chez Red Hat, premier éditeur mondial de solutions logicielles Open Source d'entreprise, nous nous appuyons sur une approche communautaire afin de fournir des technologies fiables et performantes pour le cloud, le développement, l'IA, Linux, l'automatisation et les plateformes d'applications. Nous aidons nos clients à développer des applications cloud-native, à intégrer des applications nouvelles et existantes ainsi qu'à gérer et automatiser des environnements complexes. Conseillers de confiance auprès des entreprises du Fortune 500, nous proposons des services primés d'assistance, de formation et de consulting qui apportent à tous les secteurs les avantages de l'innovation ouverte. Situés au cœur d'un réseau mondial d'entreprises, de partenaires et de communautés, nous participons à la croissance et à la transformation des entreprises et nous les aidons à se préparer à un avenir toujours plus numérique.

Amérique du Nord	1 888 REDHAT1	www.redhat.com	@red-hat
Asie-Pacifique	+65 6490 4200	apac@redhat.com	@redhat
Amérique latine	+54 11 4329 7300	info-latam@redhat.com	@redhat
Europe, Moyen-Orient et Afrique	00800 7334 2835	europe@redhat.com	@red_hat