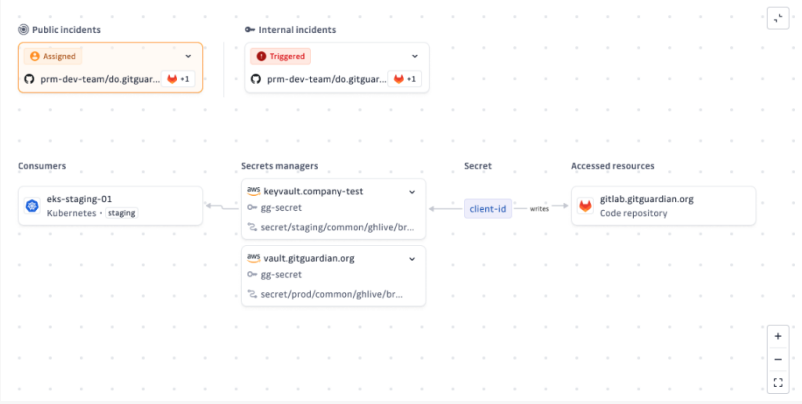
GitGuardian lance NHI Governance pour résoudre le problème de la sécurité des identités machines

NHI Governance offre une visibilité et un contrôle unifiés sur les secrets dans des environnements complexes, adressant ainsi des lacunes critiques de sécurité.



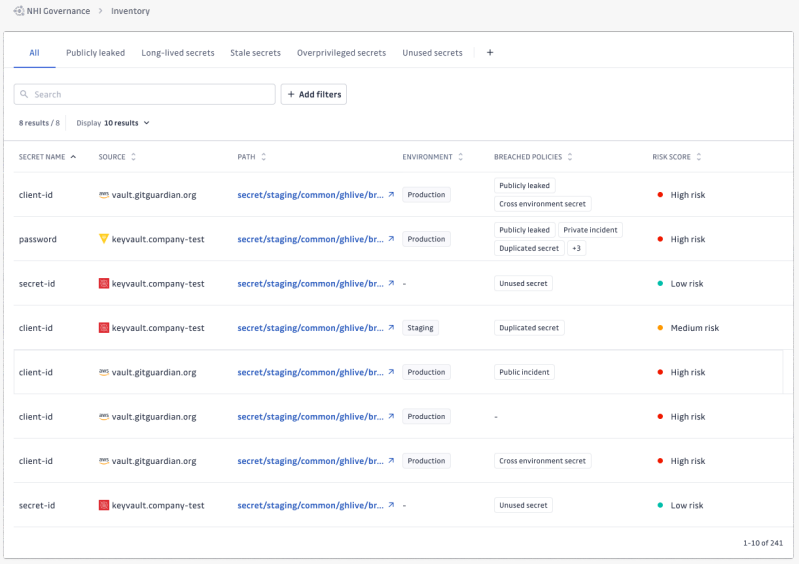
GitGuardian NHI Governance

PARIS, FRANCE, April 15, 2025 /EINPresswire.com/ -- GitGuardian, le leader de la sécurité des secrets, a annoncé aujourd'hui le lancement de NHI Governance. Ce nouveau produit innovant s'attaque à l'un des angles morts les plus critique de la cybersécurité : la sécurité et la gestion des identités machines (NHI) et des secrets qui y sont associés. Dans un paysage où les agents d'IA, l'automatisation no code et les tâches gérées par des machines se développent rapidement, les organisations sont confrontées à une explosion des identités machines - qui sont désormais 100 fois plus nombreuses que celles des utilisateurs humains - créant ainsi une surface d'attaque vaste et de plus en plus ciblée.

> L'essor des identités machine a créé une faille de sécurité ingérable pour les organisations qui est aggravée par l'essor des agents d'IA générant et consommant des secrets à un rythme sans précédent."
>
> *Eric Fourrier, CEO GitGuardian*

"L'essor des identités machines induit par l'automatisation, les API et les architectures cloud-natives redéfinit les priorités des entreprises en matière de sécurité ", déclare Katie Norton, responsable de recherche, DevSecOps et sécurité de la supply chain logicielle chez IDC. " La gestion fragmentée des secrets laisse les organisations vulnérables aux attaques basées sur les informations d'identification qui exploitent les incohérences et les lacunes entre les outils et les environnements ". L'étude d'IDC a révélé que près d'une organisation sur cinq a subi une attaque de supply chain logicielle en 2024, ce qui souligne le besoin urgent d'approches plus unifiées et évolutives pour sécuriser les identités machines."

Avec NHI Governance, GitGuardian étend son expertise en matière de sécurité des secrets pour fournir aux entreprises une solution complète permettant de relever les défis de la gestion des identités et des accès auxquels les équipes de sécurité et d'IAM sont de plus en plus confrontées.



GitGuardian NHI Governance inventory

Résoudre la problématique de la multiplication des secrets managers

Les professionnels de la sécurité sont depuis longtemps confrontés à une gestion fragmentée des secrets, communément appelée "vault sprawl", où les informations d'identification critiques sont dispersées sur plusieurs plates-formes de secrets management, souvent disparates. L'entreprise moyenne disposant de plus de 5 gestionnaires de secrets distincts, cette fragmentation - aggravée par de mauvaises pratiques de développement telles que le provisionnement de secrets surprivilégiés et à longue durée de vie - crée des silos de sécurité et une complexité opérationnelle. Les entreprises ne peuvent pas suivre, sécuriser et appliquer les politiques de manière cohérente, ce qui augmente considérablement le risque d’attaque.

GitGuardian NHI Governance résout ces problèmes grâce à une approche axée sur la découverte qui automatise la visibilité sur l'ensemble de la stack technologique :

-Inventaire unifié des secrets - Fournit une source unique de vérité pour toutes les identités et tous les secrets, éliminant les silos et permettant un suivi en temps réel dans tous les secrets managers intégrés et autres sources.
- Intégration entre secrets managers - Connexion avec les principaux gestionnaires de secrets tels que HashiCorp Vault, CyberArk Conjur, AWS Secrets Manager, Google Cloud Secrets Manager, Azure Key Vault, Akeyless et Delinea, garantissant une visibilité totale dans les environnements de secrets managers fragmentés.
- Application cohérente des politiques - Permet d'appliquer des politiques de sécurité uniformes dans tous les secrets managers, réduisant ainsi les incohérences causées par des équipes différentes qui gèrent des secrets avec des normes de sécurité variables.
- Résolution des incidents entre les secrets managers - Relie les incidents de sécurité directement aux entrées pertinentes dans les secrets managers, éliminant ainsi le besoin d'investigations manuelles sur des systèmes disparates et accélérant la réponse à l'incident.
- Assistance à la migration des secrets managers - Facilite la consolidation sécurisée des secrets en détectant les identifiants en double, orphelins ou périmés, en optimisant leur stockage et en rationalisant les migrations vers des secrets managers moins nombreux et plus sûrs.

- Contexte amélioré pour les secrets protégés - Exploite les métadonnées des secrets managers pour fournir des informations approfondies sur les accès aux secrets, les durées de vie et les autorisations d'accès, ce qui permet de hiérarchiser les risques.

Créer une gouvernance des secrets à l'échelle de l'entreprise

Contrairement aux concurrents qui s'appuient sur des intégrations manuelles et manquent de visibilité sur les secrets, l'approche de GitGuardian fournit une solution plus complète et plus évolutive. NHI Governance va au-delà des solutions traditionnelles qui se contentent de détecter les secrets en offrant une gestion complète du cycle de vie, garantissant que les identités machines et leurs secrets soient :

- Créés en toute sécurité selon les principes du moindre privilège
- Contrôlés en permanence pour détecter des schémas d'accès suspects
- Soumis à rotation en fonction des exigences de conformité
- Révoqués immédiatement lorsqu'ils sont compromis ou qu'ils ne sont plus nécessaires

Cette approche complète aide les organisations à appliquer les principes de confiance zéro, à éliminer les informations d'identification à longue durée de vie et à empêcher les accès surprivilégiés, en s'attaquant aux méthodes exactes utilisées dans les récentes attaques de la supply chain logicielle.

"Sans une gouvernance appropriée des identités machines, les organisations sont aveugles lorsqu'il s'agit de gérer leurs points d'accès les plus privilégiés ", a ajouté Eric Fourrier. "GitGuardian apporte structure et sécurité à cet espace auparavant chaotique, en donnant aux responsables de la sécurité les outils pour mettre en œuvre des politiques cohérentes, automatiser les processus de sécurité critiques et réduire de manière significative leur surface d'attaque. Nous sommes particulièrement bien placés pour nous attaquer au problème de la prolifération des secrets, en offrant une solution qui comble le fossé entre la découverte et la gestion des secrets, et la gouvernance des identités."

Les attaquants ciblant de plus en plus les identités machines comme point d'entrée principal, les organisations ont besoin de plus qu'une simple détection - elles ont besoin d'une sécurité complète et d'une gestion du cycle de vie. GitGuardian est à la pointe de cette évolution, en fournissant une plateforme complète de sécurité des identités machines qui intègre à la fois la sécurité des secrets et la gouvernance des identités machines pour protéger les points d'accès les plus critiques de l'infrastructure moderne.

GitGuardian NHI Governance est désormais disponible. Les responsables de la sécurité et de l'IAM peuvent demander une présentation personnalisée sur : www.gitguardian.com/nhi-governance

Carole Winqwist

GitGuardian
email us here

This press release can be viewed online at: https://www.einpresswire.com/article/801554924

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.
© 1995-2025 Newsmatics Inc. All Right Reserved.