Descriptif de la solution

Recon : détection proactive des menaces sur l'infrastructure Veeam

Aperçu

Recon, agent logiciel léger en instance de brevet, est intégré aux éditions Advanced et Premium de Veeam Data Platform. Développée en collaboration avec Coveware by Veeam, il s'agit de la seule solution sur le marché de la protection des données à proposer une détection proactive basée sur les comportements, fondée sur des incidents réels de ransomware.

Fonctionnement

Recon surveille en continu les environnements Veeam afin de détecter :

- Les comportements utilisateur inhabituels et les tentatives de connexion par « brute force »
- Les connexions réseau inattendues
- Les activités et les installations de fichiers suspectes
- Les tentatives d'exfiltration de données

Chaque événement est analysé et mis en correspondance avec les tactiques et techniques adverses connues, permettant ainsi aux équipes informatiques et de sécurité de réagir rapidement par des mesures préventives.

Principaux avantages

- **Détection proactive des menaces :** Identifie les activités suspectes avant qu'elles ne dégénèrent en cyberattaque à part entière.
- **Mappage MITRE ATT&CK :** Met automatiquement en corrélation les résultats avec les tactiques, techniques et procédures (TTP) de l'adversaire.
- **Déploiement rapide :** S'installe facilement sur les serveurs Veeam Backup & Replication, les proxys, les passerelles, les serveurs Active Directory et les autres serveurs de l'environnement Veeam (jusqu'à 10 serveurs).
- **Gestion sécurisée des données :** Les données collectées sont chiffrées et transférées de manière sécurisée vers un portail basé sur le cloud pour analyse. Les résultats sont également disponibles dans le Centre des menaces de Veeam Data Platform.
- **Résultats disponibles via API pour intégration à des solutions tierces :** L'application Veeam pour Microsoft Sentinel inclut les résultats de Recon.

Étude de cas

Une municipalité utilisant Veeam Data Platform Premium Edition a déployé Recon dans l'ensemble de son infrastructure.
Il a immédiatement détecté des attaques par « brute force » provenant d'adresses IP étrangères et a alerté l'équipe informatique. Des mesures rapides ont été prises pour bloquer les tentatives de connexion, empêchant ainsi toute compromission ou attaque par ransomware, ce qui a permis de protéger les données financières et personnelles sensibles.

Pourquoi c'est important

Avec l'évolution rapide des menaces de ransomware, les organisations ont besoin de plus que de simples défenses réactives. Recon permet aux équipes de détecter et de contrer les menaces avant qu'elles ne causent des dommages, offrant ainsi une résilience des données et une tranquillité d'esprit inégalées.

© 2026 Veeam Software. Informations confidentielles. Tous droits réservés. Toutes les marques déposées sont la propriété de leurs détenteurs respectifs.

Technologies complémentaires

Recon fait partie d'un ensemble plus large de fonctionnalités de sécurité de la Veeam Data Platform, qui comprend :

- **Analyse à la volée :** Fournit une analyse d'entropie à la volée, avec une détection en cours de processus, optimisée par l'IA, du chiffrement de ransomware ainsi que des artefacts textuels, y compris des liens vers le dark web et des notes de rançon.
- **Analyse des données d'index invité :** Détecte les menaces pendant la sauvegarde à l'aide d'une analyse avancée de l'activité du système de fichiers, afin de repérer les fichiers suspects, les suppressions massives, les renommages et les changements d'extension.
- **Veeam Threat Hunter :** Scanner de sauvegarde d'excellence reposant sur l'apprentissage automatique, l'analyse heuristique et la détection par signature conçu pour détecter des millions de variantes de logiciels malveillants. Il inclut une base de données de signatures de logiciels malveillants fréquemment mise à jour pour assurer une protection actualisée.
- **Scanner d'outils IoC (indicateurs de compromission) :** Identifie les outils utilisés par les acteurs de la menace et notifie avant qu'ils n'aient un impact.
- **Security and Compliance Analyzer :** Outil intégré d'évaluation de la sécurité conçu pour aider les environnements de sauvegarde à appliquer les meilleures pratiques de sécurité.

À propos de Veeam Software

Veeam®, le n° 1 mondial de la résilience des données, estime que chaque entreprise doit pouvoir se relever après un incident en conservant la confiance et le contrôle de toutes ses données, au moment et à l'endroit voulus. C'est ce que Veeam appelle la résilience totale. Nous mettons tout en œuvre pour développer des solutions innovantes grâce auxquelles nos clients pourront atteindre cet objectif. Les solutions proposées par Veeam sont conçues pour assurer la résilience des données grâce à des fonctions de sauvegarde des données, de restauration des données, de portabilité des données, de sécurité des données, et de l'intelligence des données. Avec Veeam, les responsables informatiques et de la sécurité ont l'assurance que leurs applications et leurs données sont protégées et disponibles sans interruption dans leurs environnements cloud, virtuels, physiques, SaaS et Kubernetes. Basé à Seattle et possédant des bureaux dans plus de 30 pays, Veeam protège plus de 550 000 clients dans le monde, dont 82 % des entreprises du Fortune 500, qui lui font confiance pour le maintien de leur activité. La résilience totale commence avec Veeam. Pour en savoir plus, rendez-vous sur www.veeam.com ou suivez Veeam sur LinkedIn @veeam-software et X @veeam

© 2026 Veeam Software. Informations confidentielles. Tous droits réservés. Toutes les marques déposées sont la propriété de leurs détenteurs respectifs.