Descriptif de la solution

Veeam Recon Scanner : détection proactive des menaces pour renforcer la résilience des données

Aperçu

Recon Scanner, agent logiciel léger en instance de brevet, est intégré à Veeam Data Platform Premium Edition. 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 le comportement fondée sur des incidents réels de ransomware.

Fonctionnement

Recon Scanner 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 cyberattaques 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 accessibles via API pour intégration à des solutions tierces :** notre nouvelle application Veeam pour Microsoft Sentinel intègre désormais également les résultats de Recon Scanner.

 10242025

Descriptif de la solution

Étude de cas

Une municipalité utilisant Veeam Data Platform Premium Edition a déployé Recon Scanner 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.

Technologies complémentaires

Recon Scanner 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 lié aux ransomwares 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.

Pourquoi c'est important

Avec l'évolution rapide des menaces de ransomware, les organisations ont besoin de plus que de simples défenses réactives. Recon Scanner 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.

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. Veeam appelle cela la résilience radicale et s'engage à concevoir des approches innovantes pour permettre à ses clients de l'atteindre. Les solutions Veeam sont conçues pour assurer la résilience des données grâce à des fonctions de sauvegarde, de restauration, de portabilité des données, de sécurité et d'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. Basée à Seattle et présente dans plus de 30 pays, Veeam protège plus de 550 000 clients dans le monde, dont 67 % des Global 2000, qui lui font confiance pour assurer la continuité de leurs activités. La résilience totale commence avec Veeam. En savoir plus sur www.veeam.com ou suivez Veeam sur LinkedIn @veeam-software et X @veeam

→ En savoir plus : veeam.com

→ Cliquez ici pour voir Recon Scanner en action

