Lösungsübersicht

Recon: Proaktive Bedrohungserkennung für Veeam Infrastructure

Überblick

Recon ist ein zum Patent angemeldeter, leichtgewichtiger Software-Agent, der in die Veeam Data Platform Advanced- und Premium-Editionen integriert ist. Das Produkt wurde in Zusammenarbeit mit Coveware by Veeam entwickelt und ist die einzige Lösung auf dem Markt für Datenschutz, die eine proaktive, ereignisgesteuerte Erkennung auf der Grundlage echter Ransomware-Vorfälle bietet.

So geht's

Recon überwacht Veeam-Umgebungen kontinuierlich im Hinblick auf:

- Ungewöhnliches Benutzerverhalten und Brute-Force-Anmeldeversuche
- Unerwartete Netzwerkverbindungen
- Verdächtige Dateiaktivitäten und Installationen
- Versuchte Datenexfiltration

Jedes Event wird analysiert und bekannten Taktiken und Techniken von Angreifern zugeordnet, sodass IT- und Sicherheitsteams schnell vorbeugende Maßnahmen ergreifen können.

Wesentliche Vorteile

- **Proaktive Erkennung von Bedrohungen:** Identifiziert verdächtige Aktivitäten, bevor sie zu einem schwerwiegenden Cyberangriff eskalieren.
- **MITRE ATT&CK Mapping:** Korreliert automatisch die Ergebnisse mit den Taktiken, Techniken und Verfahren (TTPs) von Angreifern.
- **Schnelle Bereitstellung:** Unkomplizierte Installation auf Veeam Backup & Replication-Servern, Proxies, Gateways, Active Directory-Servern und anderen Servern innerhalb der Veeam-Umgebung (bis zu 10 Server).
- **Sichere Datenhandhabung:** Erfasste Daten werden verschlüsselt und sicher in ein cloudbasiertes Portal zur Analyse übertragen. Die Ergebnisse sind jetzt auch im Veeam Data Platform Threat Center verfügbar.
- **Ergebnisse per API für die Integration von Drittanbietern verfügbar:** Die Veeam-App für Microsoft Sentinel umfasst Recon-Ergebnisse.

Fallstudie

Eine Gemeinde, die Veeam Data Platform Premium Edition verwendet, hat Recon in ihrer gesamten Infrastruktur eingesetzt.
Die Lösung erkannte sofort Brute Force-Angriffe von ausländischen IP-Adressen und alarmierte das IT-Team. Es wurden umgehend Maßnahmen ergriffen, um Login-Versuche zu blockieren, eine Kompromittierung und einen Ransomware-Angriff zu verhindern und so sensible Finanz- und persönliche Daten zu schützen.

Warum das wichtig ist

Angesichts der rasanten Entwicklung von Ransomware-Bedrohungen benötigen Unternehmen mehr als reaktive Schutzmaßnahmen. Recon ermöglicht Teams, Bedrohungen zu erkennen und darauf zu reagieren, bevor Schaden entsteht, indem es unübertroffene Datenresilienz und Sicherheit sowie beruhigende Gewissheit bietet.

Komplementäre Technologien

Recon ist Teil eines umfassenden Sicherheits-Feature-Sets der Veeam Data Platform, das Folgendes umfasst:

- **Inline-Scanning:** Bietet Inline-Entropie-Analyse mit KI-gestützter Erkennung von Ransomware, Verschlüsselung und Textartefakten während des Prozesses, einschließlich Dark-Web-Links und Lösegeldforderungen.
- **Gastindex-Datenscan:** Erkennt Bedrohungen während des Backups mit fortschrittlicher Dateisystemaktivitätsanalyse, einschließlich verdächtiger Dateien, einer großen Anzahl von Dateilöschungen, umbenannter Dateien oder Änderungen von Dateierweiterungen.
- **Veeam Threat Hunter:** Führender, signaturbasierter Backup-Scanner der Spitzenklasse, der auf maschinellem Lernen und heuristischer Analyse basiert und zur Erkennung von Millionen von Malware-Varianten entwickelt wurde. Es enthält eine häufig aktualisierte Datenbank mit Malware-Signaturen, um einen aktuellen Schutz zu gewährleisten.
- **IoC (Indicators of Compromise) Tools Scanner:** Identifiziert Tools, die von Bedrohungsakteuren verwendet werden, und warnt frühzeitig vor Auswirkungen.
- **Security and Compliance Analyzer:** Integriertes Tool zur Sicherheitsbewertung, um zu gewährleisten, dass Backup-Umgebungen Best Practices befolgen.

Über Veeam Software

Veeam®, der Weltmarktführer im Bereich Datenresilienz, ist der Überzeugung, dass jedes Unternehmen nach einer Unterbrechung des Business in der Lage sein sollte, den Betrieb zuversichtlich und mit Kontrolle über alle Daten wieder aufzunehmen, wann und wo immer diese Daten benötigt werden. Veeam bezeichnet dies als maximale Ausfallsicherheit, und wir arbeiten kontinuierlich daran, innovative Lösungen zu entwickeln, mit denen unsere Kunden diese Zielvorgabe erreichen. Veeam-Lösungen sind speziell auf Datenresilienz ausgelegt und bieten umfassende Funktionen für Backup, Wiederherstellung, Portabilität, Sicherheit und Intelligenz Ihrer Daten. Mit Veeam können Verantwortliche im IT- und Sicherheitsbereich darauf vertrauen, dass ihre Anwendungen und Daten in allen Umgebungen, ob in der Cloud, virtuell, physisch, SaaS oder Kubernetes, sicher und jederzeit verfügbar sind. Veeam hat seinen Hauptsitz in Seattle und ist mit Niederlassungen in mehr als 30 Ländern vertreten. Weltweit schützt Veeam mehr als 550.000 Kunden, darunter 82% der Fortune 500-Unternehmen, die auf Veeam vertrauen, um einen zuverlässigen Geschäftsbetrieb zu gewährleisten. Maximale Ausfallsicherheit beginnt mit Veeam. Erfahren Sie mehr unter www.veeam.com oder folgen Sie Veeam auf LinkedIn @veeam-software und X @veeam