Panoramica della soluzione

Recon: rilevamento proattivo delle minacce per l'infrastruttura Veeam

Panoramica

Recon è un agente software leggero e in attesa di brevetto, integrato nelle edizioni Advanced e Premium di Veeam Data Platform. Sviluppata in collaborazione con Coveware by Veeam, è l'unica soluzione sul mercato della protezione dei dati che offre un rilevamento proattivo basato sul comportamento e su incidenti ransomware reali.

Come funziona

Recon monitora costantemente gli ambienti Veeam per:

- Comportamenti insoliti degli utenti e tentativi di accesso con forza bruta
- Connessioni di rete impreviste
- Attività sui file sospette e installazioni sospette
- Tentativi di esfiltrazione dei dati

Ogni evento viene analizzato e mappato rispetto alle tattiche e alle tecniche note dell'avversario, consentendo ai team IT e di sicurezza di adottare rapidamente misure preventive.

Principali vantaggi

- **Rilevamento proattivo delle minacce:** identifica le attività sospette prima che si trasformino in un attacco informatico vero e proprio.
- **MITRE ATT&CK Mapping:** correla automaticamente i risultati alle tattiche, tecniche e procedure (TTP) dell'avversario.
- **Implementazione rapida:** facilmente installabile sui Server Veeam Backup & Replication, proxy, gateway, Server Active Directory e altri Server all'interno dell'ambiente Veeam (fino a 10 Server).
- **Gestione sicura dei dati:** i dati raccolti vengono crittografati e caricati in modo sicuro su un portale basato sul cloud per l'analisi. I risultati sono ora disponibili anche nel Veeam Data Platform Threat Center.
- **Risultati disponibili tramite API per l'integrazione con terze parti:** l'app Veeam per Microsoft Sentinel comprende i risultati di Recon.

Caso di studio

Un comune che utilizza Veeam Data Platform Premium Edition ha distribuito Recon nella propria infrastruttura. Ha rilevato immediatamente attacchi di forza bruta da IP esteri e ha avvisato il team IT. Sono stati adottati provvedimenti tempestivi per bloccare i tentativi di accesso, prevenendo la compromissione e un attacco ransomware, salvaguardando così dati finanziari e personali sensibili.

Perché è importante

Con le minacce ransomware in rapida evoluzione, le organizzazioni hanno bisogno di qualcosa di più di semplici difese reattive. Recon consente ai team di rilevare e rispondere alle minacce prima che si verifichino danni offrendo resilienza dei dati e tranquillità senza pari.

Tecnologie complementari

Recon fa parte di un set più ampio di funzionalità di sicurezza di Veeam Data Platform, tra cui:

- **Scansione inline:** offre un'analisi dell'entropia inline con rilevamento in-process basato sull'intelligenza artificiale di crittografia ransomware e artefatti testuali, inclusi i link al dark web e le note di riscatto.
- **Scansione dei dati dell'indice guest:** rileva le minacce durante il backup tramite un'analisi avanzata dell'attività del file system per individuare la presenza di file sospetti, un numero elevato di eliminazioni di file, file rinominati o cambiamenti di estensione dei file.
- **Veeam Threat Hunter:** scanner di backup all'avanguardia basato su apprendimento automatico, analisi euristica e scanner basato su firme, progettato per individuare milioni di varianti di malware. Dispone di un database frequentemente aggiornato di firme di malware per garantire una protezione sempre aggiornata.
- **Scanner di strumenti IoC (indicatori di compromissione):** identifica gli strumenti utilizzati dagli autori delle minacce e avvisa prima dell'impatto.
- **Analizzatore di sicurezza e conformità:** strumento di valutazione della sicurezza integrato per garantire che gli ambienti di backup seguano le best practice di sicurezza.

Informazioni su Veeam Software

Veeam®, leader di mercato n. 1 al mondo nella resilienza dei dati, ritiene che ogni azienda dovrebbe essere in grado di fare un salto in avanti dopo un'interruzione, con la sicurezza e il controllo di tutti i dati ovunque e in qualsiasi momento ne abbia bisogno. Veeam la chiama resilienza radicale e si impegna al massimo per creare modi innovativi per aiutare i propri clienti a raggiungerla. Le soluzioni Veeam sono progettate appositamente per migliorare la resilienza dei dati garantendo backup, ripristino, portabilità, sicurezza e intelligence dei dati. Con Veeam, i responsabili IT e della sicurezza hanno la tranquillità di sapere che le loro applicazioni e i loro dati sono protetti e sempre disponibili negli ambienti cloud, virtuali, fisici, SaaS e Kubernetes. Con sede a Seattle e uffici in oltre 30 Paesi, Veeam protegge più di 550.000 clienti in tutto il mondo, incluso l'82% delle aziende Fortune 500, che si affidano a Veeam per mantenere operative le proprie attività. La resilienza radicale inizia con Veeam. Per maggiori informazioni, visita il sito www.veeam.com o segui Veeam su LinkedIn @veeam-software e su X @veeam