Resumo da solução

Recon: Detecção proativa de ameaças para infraestrutura da Veeam

Visão geral

Recon é um agente de software leve e com patente pendente, integrado às edições Veeam Data Platform Advanced Edition e Veeam Data Platform Premium Edition. Desenvolvida pela Veeam em colaboração com a Coveware by Veeam, é a única solução no mercado de proteção de dados que oferece detecção proativa baseada em comportamento detecção baseada em incidentes reais de ransomware.

Como funciona

Recon monitora continuamente ambientes Veeam em busca de:

- Comportamento incomum do usuário e tentativas de login com força bruta
- Conexões de rede inesperadas
- Atividade suspeita de arquivos e instalações
- Tentativas de exfiltração de dados

Cada evento é analisado e mapeado paratáticas e técnicas adversárias conhecidas,permitindo que as equipes de TI e segurança tomem medidas preventivas rapidamente.

Estudo de caso

Um município que utiliza a Veeam Data Platform Premium Edition implantou o Recon em toda a sua infraestrutura.
Ele imediatamente detectou ataques de força bruta de IPs estrangeiros e alertou a equipe de TI. Ações imediatas foram tomadas para bloquear as tentativas de login, evitando o comprometimento e um ataque de ransomware, protegendo assim os dados financeiros e pessoais confidenciais.

Benefícios essenciais

- **Detecção proativa de ameaças:** Identifica atividades suspeitas antes que evoluam para um ataque cibernético de grande escala.
- **Mapeamento MITRE ATT&CK:** Correlaciona automaticamente as detecções com as Táticas, Técnicas e Procedimentos (TTPs) do adversário.
- **Implantação rápida:** Instalação simplificada em servidores Veeam Backup & Replication, proxies, gateways, servidores Active Directory e demais servidores dentro do ambiente Veeam (até 10 servidores).
- **Tratamento seguro de dados:** Os dados coletados são criptografados e transferidos de forma segura para um portal baseado na nuvem para análise. As detecções também já estão disponíveis no Centro de Ameaças da Veeam Data Platform.
- **Detecções disponíveis via API para integração de terceiros:** O aplicativo Veeam para Microsoft Sentinel inclui as detecções do Recon.

Por que é importante

Com as ameaças de ransomware evoluindo rapidamente, as organizações precisam de mais do que defesas reativas. Recon permite que as equipes detectem e respondam a ameaças antes que ocorram danos, proporcionando resiliência de dados sem igual e tranquilidade.

Tecnologias complementares

O Recon faz parte de um conjunto mais amplo de recursos de segurança da Veeam Data Platform, incluindo:

- **Varredura em linha:** Fornece análise de entropia em linha, com detecção em tempo real impulsionada por IA de criptografia de ransomware e artefatos de texto, incluindo links da dark web e notas de resgate.
- **Varredura de índice de convidado:** Detecta ameaças durante o backup usando análise avançada de atividade do sistema de arquivos para detectar o aparecimento de arquivos suspeitos, grande quantidade de exclusões de arquivos, arquivos renomeados ou alterações na extensão de arquivos.
- **Veeam Threat Hunter:** Scanner de backup de classe mundial baseado em assinaturas, aprendizado de máquina e análise heurística projetado para detectar milhões de variantes de malware. Inclui um banco de dados de assinaturas de malware frequentemente atualizado para garantir proteção sempre atualizada.
- **Scanner de Ferramentas IoC (Indicadores de Comprometimento):** Identifica ferramentas utilizadas por agentes de ameaça e notifica antes do impacto.
- **Analisador de Segurança e Conformidade:** Ferramenta integrada de avaliação de segurança para garantir que os ambientes de backup sigam as melhores práticas de segurança.

Sobre a Veeam Software

A Veeam®, a líder nº 1 do mercado global em resiliência de dados, acredita que toda empresa deve ser capaz de retornar à frente após uma interrupção com a confiança e o controle de todos os seus dados, quando e onde forem necessários. A Veeam chama isso de resiliência radical, e estamos determinados a criar formas inovadoras de ajudar nossos clientes a alcançá-lo. As soluções da Veeam são desenvolvidas especificamente para impulsionar a resiliência de dados, fornecendo backup de dados, recuperação de dados, portabilidade de dados, segurança de dados e inteligência de dados. Com a Veeam, os líderes de TI e segurança ficam tranquilos sabendo que seus aplicativos e dados estão protegidos e sempre disponíveis em seus ambientes físicos, virtuais, na nuvem, SaaS e Kubernetes. Com sede em Seattle e escritórios em mais de 30 países, a Veeam protege mais de 550.000 clientes no mundo inteiro, incluindo 82% das empresas da Fortune 500, que confiam na Veeam para manter seus negócios em operação. Resiliência radical começa com a Veeam. Saiba mais em www.veeam.com ou siga a Veeam no LinkedIn @veeam-software e X @veeam

