Resumen de la solución

Recon: Detección proactiva de amenazas para infraestructura de Veeam

Descripción general

Recon es un agente de software ligero, pendiente de patente, integrado en las ediciones Advanced y Premium de Veeam Data Platform. Desarrollada en colaboración con Coveware by Veeam, es la única solución en el mercado de protección de datos que ofrece detección proactiva basada en comportamientos y en incidentes de ransomware del mundo real.

Cómo funciona

Recon monitorea continuamente los entornos de Veeam para detectar:

- Comportamiento inusual del usuario e intentos de inicio de sesión por fuerza bruta
- Conexiones de red inesperadas
- Actividad sospechosa de archivos e instalaciones
- Intentos de exfiltración de datos

Cada evento se analiza y se mapea a tácticas y técnicas conocidas de los adversarios, lo que permite a los equipos de TI y seguridad tomar medidas preventivas rápidamente.

Beneficios clave

- **Detección proactiva de amenazas:** identifica la actividad sospechosa antes de que escale a un ciberataque de gran magnitud.
- **Mapeo MITRE ATT&CK:** correlaciona automáticamente los hallazgos con las tácticas, técnicas y procedimientos (TTP) del adversario.
- **Implementación rápida:** se instala fácilmente en servidores Veeam Backup & Replication, proxies, puertas de enlace, servidores de Active Directory (Directorio activo) y otros servidores dentro del entorno de Veeam (hasta 10 servidores).
- **Gestión segura de datos:** los datos recopilados se cifran y se cargan de forma segura en un portal basado en la nube para su análisis. Los hallazgos también están ahora disponibles en el Centro de amenazas de Veeam Data Platform.
- **Hallazgos disponibles a través de API para la integración con terceros:** la aplicación de Veeam para Microsoft Sentinel incluye los hallazgos de Recon.

Estudio de casos:

Un municipio que utiliza Veeam Data Platform Premium Edition desplegó Recon en toda su infraestructura. Inmediatamente detectó ataques de fuerza bruta desde direcciones IP extranjeras y alertó al equipo de TI. Se tomaron medidas inmediatas para bloquear los intentos de inicio de sesión, previniendo una brecha de seguridad y un ataque de ransomware, lo que protegió datos financieros y personales sensibles.

¿Por qué es importante?

Con la rápida evolución de las amenazas de ransomware, las organizaciones necesitan más que defensas reactivas. Recon permite a los equipos detectar y responder a amenazas antes de que se produzcan daños, proporcionando una resiliencia de datos inigualable y tranquilidad.

Tecnologías complementarias

Recon forma parte de un conjunto más amplio de características de seguridad de Veeam Data Platform que incluye:

- **Análisis en línea:** realiza análisis de entropía en línea, con detección en tiempo real impulsada por IA de ransomware cifrado y artefactos de texto, incluidos enlaces a la web oscura y notas de rescate.
- **Análisis de datos del índice de invitados:** detecta amenazas durante el backup utilizando un análisis avanzado de la actividad del sistema de archivos para detectar la aparición de archivos sospechosos, una gran cantidad de eliminaciones de archivos, archivos renombrados o cambios en la extensión de los archivos.
- **Veeam Threat Hunter:** escáner de backup basado en firmas, aprendizaje automático y análisis heurístico de clase mundial, diseñado para detectar millones de variantes de malware. Incluye una base de datos de firmas de malware que se actualiza con frecuencia para garantizar una protección actualizada.
- **Escáner de herramientas IoC (indicadores de compromiso):** identifica herramientas que son utilizadas por actores de amenazas y notifica antes del impacto.
- **Analizador de seguridad y cumplimiento:** herramienta de evaluación de seguridad integrada para garantizar que los entornos de backup sigan las mejores prácticas de seguridad.

Acerca de Veeam Software

Veeam®, el líder n.° 1 del mercado mundial en resiliencia de datos, cree que todas las empresas deberían ser capaces de recuperarse para avanzar después de una interrupción con la confianza y el control de todos sus datos cuando y donde los necesiten. Veeam llama a esto resiliencia radical, y estamos obsesionados en crear formas innovadoras de ayudar a nuestros clientes a conseguirlo. Las soluciones de Veeam están diseñadas específicamente para aumentar la resiliencia de los datos al proporcionar backup de datos, recuperación de datos, portabilidad de datos, seguridad de datos e inteligencia de datos. Con Veeam, los líderes de TI y seguridad descansan tranquilos sabiendo que sus aplicaciones y datos están protegidos y siempre disponibles en sus entornos de nube, virtuales, físicos, SaaS y de Kubernetes. Con sede en Seattle y oficinas en más de 30 países, Veeam protege a más de 550 000 clientes en todo el mundo, incluyendo 82% de las empresas Fortune 500, que confían en Veeam para mantener sus negocios en funcionamiento. La resiliencia radical comienza con Veeam. Más información en www.veeam.com o siga a Veeam en LinkedIn @veeam-software y X @veeam