解决方案摘要

Recon：Veeam 基础架构的主动威胁检测

概述

Recon 是一款正在申请专利的轻量级软件代理，已集成于 Veeam Data Platform Advanced Edition 和 Veeam Data Platform Premium Edition 中。该解决方案与 Coveware by Veeam 合作开发，是数据保护市场中唯一一款提供基于行为的主动检测根据真实勒索软件事件的解决方案。

工作原理

Recon 持续监控 Veeam 环境，以检测：

- 异常用户行为和暴力登录尝试
- 异常网络连接
- 可疑文件活动和安装
- 数据泄露尝试行为

每个事件都会被分析并映射到已知的对手战术和技术，使 IT 和安全团队能够迅速采取预防措施。

主要优点

- **主动威胁检测：**能够识别可疑行为，防止其升级为严重的网络攻击。
- **MITRE ATT&CK 映射：**自动将检测结果与攻击者的战术、技术和程序（TTP）相关联。
- **快速部署：**可便捷部署于 Veeam Backup & Replication 服务器、代理、网关、Active Directory 服务器及 Veeam 环境中的其他服务器，支持最多 10 台服务器。
- **安全数据处理：**收集的数据经过加密并安全上传到基于云的门户进行分析。检测结果现已可在 Veeam Data Platform Threat Center 查看。
- **检测结果可通过 API 供第三方集成：**Veeam 针对 Microsoft Sentinel 的应用程序包含 Recon 检测结果。

案例研究

一家使用 Veeam Data Platform Premium Edition 的市政当局在其基础架构中部署了 Recon。
它立即检测到来自境外 IP 的暴力破解攻击，并向 IT 团队发出警报。迅速采取措施阻止登录尝试，防止系统被攻破和勒索软件攻击，从而保护敏感的财务和个人数据。

为什么重要

随着勒索软件威胁演变迅速，组织需要的不仅仅是被动防御。Recon 赋能团队在损害发生之前检测和响应威胁，通过提供无与伦比的数据弹性和安心。

补充技术

Recon 属于更广泛的 Veeam Data Platform 安全功能集的一部分，包括：

- **内嵌扫描：**提供内嵌熵分析，并利用 AI 实时检测勒索软件加密和相关文本痕迹，包括暗网链接和勒索说明。
- **来宾索引数据扫描：**在备份期间，通过高级文件系统活动分析检测威胁，如可疑文件出现、大量文件删除、文件重命名或文件扩展名更改。
- **Veeam Threat Hunter：**业界领先的机器学习与启发式分析相结合的基于签名的备份扫描器，旨在检测数百万种恶意软件变种。它包含一个频繁更新的恶意软件签名数据库，以确保防护始终保持最新状态。
- **IoC（入侵指标）工具扫描程序：**识别被攻击者利用的工具，并在造成影响前提前预警。
- **安全与合规分析器：**内置安全评估工具，确保备份环境遵循安全最佳实践。

关于 Veeam Software

Veeam® 是数据弹性领域的 #1 全球市场领导者，其坚信每家企业在中断后都应该能够绝地反弹，并且能够在需要时随时随地自信地控制其所有数据。Veeam 称之为极致弹性，我们致力于通过创新方法来帮助我们的客户实现这一目标。Veeam 解决方案专门通过提供备份数据、数据恢复、数据移植性、数据安全和数据智能功能增强数据弹性。借助 Veeam，IT 和安全领导者可以高枕无忧，因为他们知道其应用程序和数据受到了保护，并且始终在云、虚拟、物理、SaaS 和 Kubernetes 环境中可用。Veeam 总部位于西雅图，在全球 30 多个国家设有办事处，保护着全球超过 550,000 家客户，其中包括 82% 的全球 500 强公司，他们信赖 Veeam 保证其业务正常运行。极致弹性始于 Veeam。请访问 www.veeam.com 了解更多信息或关注 Veeam 的 LinkedIn @veeam-software 和 X @veeam。