ZeroPEN

Veeam Backup & Recovery 渗透测试

“零妥协。”— 抢在攻击者摧毁您的 Veeam 备份之前发现问题。

问题所在： Veeam 是企业备份的标准 — 同时也是攻击者的头号目标。CVE-2024-40711 和 CVE-2023-27532 等漏洞已被包括 Akira 和 Fog 在内的勒索软件团伙积极利用，以接管 Veeam 服务器并删除备份。

ZeroPEN 的作用

- 针对 Veeam 对勒索软件杀伤链进行受控模拟。
- 以 VBR 服务器、Enterprise Manager、Veeam ONE、配置数据库和存储库为目标。
- 验证不可变性、RBAC 和补丁级别；生成 Veeam 加固评分卡。
- 证明备份失效和数据外泄的可能性 — 且不会造成实际损害。

四层防护，零妥协

ZeroMON 监控	**ZeroTAM** 咨询	**ZeroPEN** 渗透测试	**ZeroVault** 云存储

法规覆盖

BDDK IT 法规 Art.45/51/17	SPK III-35.1 业务连续性
DORA Art.11/12/17 TLPT	KVKK Art.12 数据安全
GDPR Art.25/32/33	ISO 27001 / NIST A.12.3 / SP 800-115

交付物

执行摘要 · 映射到 CWE/CVE 的技术报告 · Veeam 加固评分卡 · MITRE ATT&CK 杀伤链 · 法规映射矩阵 · 按优先级排序的修复建议 · 复测。

如何开始： 填写范围表单，随后我们将很快交付量身定制的测试流程。

www.backupsec.com · info@backupsec.com · BackupSec