ZeroPEN

Teste de Penetração de Veeam Backup & Recovery

“Zero concessões.” — Encontre antes que o atacante destrua os seus backups Veeam.

O problema: O Veeam é o padrão para backup corporativo — e o alvo número um dos atacantes. Falhas como CVE-2024-40711 e CVE-2023-27532 têm sido ativamente exploradas por grupos de ransomware, incluindo Akira e Fog, para assumir o controle de servidores Veeam e excluir backups.

O que o ZeroPEN faz

- Simulação controlada da kill-chain de ransomware contra o Veeam.
- Tem como alvo o servidor VBR, o Enterprise Manager, o Veeam ONE, o banco de dados de configuração (config DB) e os repositórios.
- Verifica imutabilidade, RBAC e nível de patch; produz um scorecard de hardening do Veeam.
- Comprova a capacidade de neutralização de backups e de exfiltração — sem causar danos reais.

Quatro camadas, zero concessões

ZeroMON Monitoramento	**ZeroTAM** Consultoria	**ZeroPEN** Pentest	**ZeroVault** Cloud Storage

Cobertura regulatória

BDDK Regulamentação de IT Art.45/51/17	SPK III-35.1 Continuidade de Negócios
DORA Art.11/12/17 TLPT	KVKK Art.12 segurança de dados
GDPR Art.25/32/33	ISO 27001 / NIST A.12.3 / SP 800-115

Entregáveis

Resumo executivo · relatório técnico mapeado por CWE/CVE · scorecard de hardening do Veeam · kill-chain MITRE ATT&CK · matriz de mapeamento regulatório · remediação priorizada · reteste.

Comece agora: Preencha o formulário de escopo e, logo em seguida, entregaremos um procedimento de teste personalizado.

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