ZeroPEN

Test d'intrusion Veeam Backup & Recovery

“Zéro compromis.” — Détectez la faille avant que l'attaquant ne détruise vos backups Veeam.

Le problème : Veeam est la référence du backup en entreprise — et la cible numéro un des attaquants. Des failles comme CVE-2024-40711 et CVE-2023-27532 ont été activement exploitées par des groupes de ransomware, dont Akira et Fog, pour prendre le contrôle des serveurs Veeam et supprimer les backups.

Ce que fait ZeroPEN

- Simulation contrôlée de la kill-chain ransomware contre Veeam.
- Cible le serveur VBR, Enterprise Manager, Veeam ONE, la base de configuration et les dépôts.
- Vérifie l'immuabilité, le RBAC et le niveau de correctifs ; produit une fiche de score de durcissement Veeam.
- Démontre la capacité de neutralisation des backups et d'exfiltration — sans causer de dommage réel.

Quatre couches, zéro compromis

ZeroMON Supervision	**ZeroTAM** Conseil	**ZeroPEN** Pentest	**ZeroVault** Stockage cloud

Couverture réglementaire

BDDK Réglementation IT Art.45/51/17	SPK III-35.1 Continuité d'activité
DORA Art.11/12/17 TLPT	KVKK Art.12 sécurité des données
GDPR Art.25/32/33	ISO 27001 / NIST A.12.3 / SP 800-115

Livrables

Synthèse pour la direction · rapport technique mappé CWE/CVE · fiche de score de durcissement Veeam · kill-chain MITRE ATT&CK · matrice de correspondance réglementaire · remédiation priorisée · nouveau test.

Pour commencer : Remplissez le formulaire de périmètre et nous vous fournirons peu après une procédure de test sur mesure.

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