ZeroPEN

Veeam Backup & Recovery ペネトレーションテスト

“妥協ゼロ。” — 攻撃者が Veeam バックアップを破壊する前に発見。

課題： Veeam はエンタープライズバックアップの標準であり — そして攻撃者の第一の標的でもあります。CVE-2024-40711 や CVE-2023-27532 のような脆弱性は、Akira や Fog を含むランサムウェアグループによって、Veeam サーバーを乗っ取りバックアップを削除するために実際に悪用されてきました。

ZeroPEN が行うこと

- Veeam に対するランサムウェアのキルチェーンを、制御された形でシミュレーション。
- VBR サーバー、Enterprise Manager、Veeam ONE、構成 DB、リポジトリを対象とします。
- イミュータビリティ、RBAC、パッチレベルを検証し、Veeam ハードニングスコアカードを作成します。
- バックアップの無力化とデータ持ち出しの可能性を実証します — 実際の被害を発生させることなく。

4つのレイヤー、妥協ゼロ

ZeroMON モニタリング	**ZeroTAM** アドバイザリー	**ZeroPEN** ペンテスト	**ZeroVault** クラウドストレージ

規制対応範囲

BDDK IT 規制 Art.45/51/17	SPK III-35.1 事業継続性
DORA Art.11/12/17 TLPT	KVKK Art.12 データセキュリティ
GDPR Art.25/32/33	ISO 27001 / NIST A.12.3 / SP 800-115

提供物

エグゼクティブサマリー · CWE/CVE にマッピングした技術レポート · Veeam ハードニングスコアカード · MITRE ATT&CK キルチェーン · 規制マッピングマトリクス · 優先順位付けされた是正措置 · 再テスト。

始めるには： スコープフォームにご記入いただければ、その後まもなく、お客様に合わせたテスト手順をご提供します。

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