ZeroPEN

Veeam Backup & Kurtarma Penetrasyon Testi

“Sıfır taviz.” — Saldırgan Veeam backup'larınızı yok etmeden önce onu bulun.

Sorun: Veeam, kurumsal backup için standarttır — ve saldırganların bir numaralı hedefidir. CVE-2024-40711 ve CVE-2023-27532 gibi açıklar, Akira ve Fog dahil ransomware grupları tarafından Veeam sunucularını ele geçirmek ve backup'ları silmek için aktif olarak kullanılmıştır.

ZeroPEN ne yapar

- Veeam'e karşı ransomware kill-chain'inin kontrollü simülasyonu.
- VBR sunucusunu, Enterprise Manager'ı, Veeam ONE'ı, yapılandırma veritabanını (config DB) ve repository'leri hedefler.
- Değişmezliği, RBAC'yi ve yama seviyesini doğrular; bir Veeam sıkılaştırma karnesi üretir.
- Backup'ı etkisiz hale getirme ve veri sızdırma (exfiltration) yeteneğini — gerçek bir hasara yol açmadan kanıtlar.

Dört katman, sıfır taviz

ZeroMON İzleme	**ZeroTAM** Danışmanlık	**ZeroPEN** Pentest	**ZeroVault** Bulut Depolama

Mevzuat kapsamı

BDDK IT Düzenlemesi Art.45/51/17	SPK III-35.1 İş Sürekliliği
DORA Art.11/12/17 TLPT	KVKK Art.12 veri güvenliği
GDPR Art.25/32/33	ISO 27001 / NIST A.12.3 / SP 800-115

Çıktılar

Yönetici özeti · CWE/CVE eşlemeli teknik rapor · Veeam sıkılaştırma karnesi · MITRE ATT&CK kill-chain · mevzuat eşleme matrisi · önceliklendirilmiş düzeltme · yeniden test.

Başlayın: Kapsam formunu doldurun; kısa süre içinde size özel bir test prosedürü sunalım.

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