ZeroPEN

Veeam Backup & Recovery 침투 테스트

"타협은 없다." — 공격자가 Veeam 백업을 파괴하기 전에 찾아내십시오.

문제: Veeam은 엔터프라이즈 백업의 표준이며 — 동시에 공격자의 최우선 표적입니다. CVE-2024-40711 및 CVE-2023-27532과 같은 취약점은 Akira 및 Fog를 포함한 랜섬웨어 그룹이 Veeam 서버를 장악하고 백업을 삭제하는 데 적극적으로 악용해 왔습니다.

ZeroPEN이 하는 일

- Veeam을 대상으로 한 랜섬웨어 킬 체인의 통제된 시뮬레이션.
- VBR 서버, Enterprise Manager, Veeam ONE, 구성 DB 및 리포지토리를 표적으로 합니다.
- 불변성, RBAC 및 패치 수준을 검증하고 Veeam 하드닝 스코어카드를 생성합니다.
- 실제 피해를 입히지 않으면서 — 백업 무력화 및 유출 가능성을 입증합니다.

4개 계층, 타협 없음

ZeroMON	ZeroTAM	ZeroPEN	ZeroVault
모니터링	자문	침투 테스트	클라우드 스토리지

규제 적용 범위

BDDK IT 규정 Art.45/51/17	SPK III-35.1 비즈니스 연속성
DORA Art.11/12/17 TLPT	KVKK Art.12 데이터 보안
GDPR Art.25/32/33	ISO 27001 / NIST A.12.3 / SP 800-115

산출물

경영진 요약 · CWE/CVE 매핑 기술 보고서 · Veeam 하드닝 스코어카드 · MITRE ATT&CK 킬 체인 · 규제 매핑 매트릭스 · 우선순위화된 개선 조치 · 재테스트.

시작하기: 범위 산정 양식을 작성해 주시면 곧이어 맞춤형 테스트 절차를 제공해 드립니다.

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