VERITAS

안정적인 복구 실현

확실한 복구 계획을 구현하십시오.

가동 중단 및 데이터 도용으로 인한 피해를 방지하십시오. 베리타스의 사이버 복구 체크리스트를 통해 지금 대비하고 미래의 레질리언스를 확보하십시오.

1단계

1단계 | 30일

기반 형성

지금 당장 비즈니스 보호를 위해 할 수 있는 일

- 모든 워크로드에 대한 보호 및 보존 정책 생성
- 변조 불가 스토리지 활용
- 3-2-1 백업 전략 구현 — 두 가지 형식의 카피본 3개, 가상 및/또는 물리적 에어 갭(Air Gap)을 포함한 오프사이트 카피본 1개, SaaS 격리 필수
- 보안 제어 적용(예: MFA, MPA, 네트워크 세그먼트화, RBAC, 암호화)
- 전용 하드닝 어플라이언스 사용 고려
- AI 기반 이상 요소 탐지 사용
- 악성 코드 탐지 및 보존 규칙 사용
- 소프트웨어 및 보안 패치 업데이트(진행 중)

2단계

2단계 | 60일

선제적 리스크 관리

사람, 프로세스, 기술에 초점

- '누락된' 중요 자산 파악
- 미확인 데이터 평가 수행
- 중요 데이터 파악 및 분류
- 고위험 엔드유저 행위 식별 및 모니터링
- IRE(Isolated Recovery Environment), 즉 IRE 또는 클린룸(Clean room) 생성
- 복구 런북 개발(작업 우선 순위 지정)
- SecOps와 통합하여 사고 대응 플레이북 설정 (예: SIEM/SOAR/XDR 통합)

3단계

3단계 | 90일

조정. 리허설. 적용

- 데이터 보호 정책을 조정하여 100% 백업 성공률 달성(SLA 기준)
- AI 기반 이상 요소 탐지 세부 조정(오탐지 및 미탐지 문제 해결)
- 무중단 복구 리허설을 비롯한 테이블 테스트 연습 실행
- 복구 리허설 및 결과 검증

전체 사이버 복구 체크리스트 보기 ›

VERITAS

TEL: 02-3468-2100 • www.veritas.com/ko/kr