제로데이 대응 모의훈련 결과 보고

훈련의 목적은 못 하는 것을 찾는 것

요 약

외부 공개 웹서비스에 미공개 취약점을 통한 웹셸 업로드가 발생한 상황을 가정해 모의훈련을 실시했다. 훈련 결과 기술적 탐지 역량보다 의사결정 체계와 커뮤니케이션에서 더 큰 공백이 확인됐다.

1. 훈련 시나리오

새벽 시간대 외부 웹서비스에 웹셸이 업로드되고, 30분 뒤 내부 자산으로 측면 이동이 시도되는 시나리오로 구성했다.

2. 확인된 문제

새벽 시간대 담당자 연결에 40분이 소요됐다. 서비스 차단 결정 권한이 명확하지 않아 대응이 지연됐으며, 로그 보존 기간이 짧아 초기 침투 시점 추정에 실패했다.

3. 개선 과제

비상 연락망을 분기별로 실제 호출해 검증하고, 서비스 중단 권한 위임 규정을 문서화한다. 로그 보존 기간을 확대하고 중앙 수집 체계를 갖춘다.

4. 다음 훈련

고객 공지 템플릿을 사전 준비하고, 다음 훈련에서는 대외 커뮤니케이션까지 평가 범위에 포함한다.