SWIFT CSCF v2026 · Control 7.3A

SWIFT CSCF v2026 Control 7.3A 모의 침투 테스트 준비 점검표

1. 영향도를 기준으로 범위를 정한다

- ☐ SWIFT 환경의 자산 목록이 작성되어 있다 (보안 구역, 메시징 인터페이스, 운영자 워크스테이션, 네트워크 연결, 그리고 이를 공급하는 백오피스 시스템).
- ☐ 공격 경로가 테스트의 용이성이 아니라 침해 시의 영향도에 따라 순위가 매겨져 있다.
- ☐ 범위가 보안 구역과 그 신뢰 경계를 기준으로 정의되어 있어, 공격자가 백오피스에서 메시징 계층으로 이동할 수 없음을 테스트로 증명한다.
- ☐ 테스트가 3년 시나리오 주기에 걸쳐 계획되어 있으며, 애플리케이션, 인프라, 인적 경로를 포괄한다.

2. 위협 인텔리전스로 구성한다

- ☐ 금융 메시징을 노리는 공격자에 대한 최신 인텔리전스가 테스트 시나리오에 반영되어 있다.
- ☐ 시나리오가 일반적인 취약점 유형이 아니라 그럴듯하고 구체적으로 명명된 침입 경로를 재현한다.
- ☐ 인텔리전스 근거가 문서화되어 있어, DORA 및 OSFI B-13에서 위협 주도형 테스트로 인정된다.

3. 가장 엄격한 기준으로 수행한다

- ☐ 테스트가 시스템 경계의 안쪽과 바깥쪽 양쪽에서 수행되어 NYDFS Part 500의 기대 사항을 충족한다.
- ☐ 테스트가 역량을 갖추고 충분히 독립적인 주체에 의해 수행된다.
- ☐ 가동 중인 시스템을 테스트하기 위한 교전 규칙, 승인, 안전 통제가 문서화되고 승인되어 있다.
- ☐ 정해진 주기가 설정되고 기록되어 있어, NYDFS의 연간 최소 요건과 SWIFT 주기를 함께 충족한다.

4. 자체 방어력을 측정한다

- ☐ 이 훈련은 무엇이 발견되었는지뿐만 아니라, 모의 침입을 모니터링이 탐지했는지 여부를 측정한다.
- ☐ 대응 및 봉쇄 성과가 탐지 기능과 대응 기능에 비추어 기록된다.
- ☐ 탐지 격차는 그 자체로 독립된 발견 사항으로 기록된다.

5. 순환을 마무리하고 증거를 확보한다

- ☐ 발견 사항이 담당자와 기한이 있는 추적 가능한 시정 주기에 등록된다.
- ☐ 시정 완료가 단순한 주장이 아니라 증거로 입증된다.
- ☐ 전체 기록 (범위, 시나리오, 공격 서술, 발견 사항, 시정, 탐지 성과)이 NIST CSF 2.0을 중추로 삼아 한 번만 보관된다.
- ☐ 단일 기록이 각 규제 체계 (SWIFT 7.3A, DORA, NYDFS Part 500, OSFI B-13)에 태그가 지정된다.

귀 기관을 위한 채점을 원하십니까. Cambridge Cyber International는 SWIFT CSP 평가와 이 기준에 따른 7.3A 모의 침투 테스트를 수행하고, 발견 사항을 완료될 때까지 검증합니다. 인증 신청 기간이 시작되기 전에 범위 협의를 예약하십시오.

contact@cambridgecyberinternational.com · cambridgecyberinternational.com/ko/contact/