SWIFT CSCF v2026 · Control 7.3A

Liste de controle de preparation au test d'intrusion SWIFT CSCF v2026 Control 7.3A

1. Cadrer par consequence

- [ ] Le perimetre SWIFT est inventorie : zone securisee, interface de messagerie, postes de travail des operateurs, connexion au reseau et systemes de back-office qui l'alimentent.
- [ ] Les chemins d'attaque sont classes selon la consequence d'une compromission, et non selon la facilite de test.
- [ ] Le perimetre est defini par rapport a la zone securisee et a ses frontieres de confiance, de sorte que le test prouve qu'un attaquant ne peut pas pivoter du back-office vers la couche de messagerie.
- [ ] Le test est planifie sur le cycle de scenarios de trois ans, couvrant les chemins applicatifs, d'infrastructure et humains.

2. Cadrer avec le renseignement sur les menaces

- [ ] Le renseignement actuel sur les acteurs ciblant la messagerie financiere alimente les scenarios de test.
- [ ] Les scenarios reproduisent des chemins d'intrusion plausibles et nommes plutot que des categories generiques de vulnerabilites.
- [ ] La base de renseignement est documentee, de sorte que le test se qualifie comme pilote par la menace au titre de DORA et OSFI B-13.

3. Executer selon la norme la plus exigeante

- [ ] Le test s'execute depuis l'interieur et l'exterieur des frontieres des systemes, repondant a l'attente de NYDFS Part 500.
- [ ] Le test est realise par une partie competente et suffisamment independante.
- [ ] Les regles d'engagement, l'autorisation et les controles de securite pour tester des systemes en production sont documentes et approuves.
- [ ] Une cadence definie est etablie et consignee, satisfaisant a la fois le minimum annuel NYDFS et le cycle SWIFT.

4. Mesurer vos propres defenses

- [ ] L'exercice mesure si la surveillance a detecte l'intrusion simulee, et pas seulement ce qui a ete trouve.
- [ ] La performance de reponse et de confinement est consignee au regard des fonctions Detecter et Repondre.
- [ ] Les lacunes de detection sont enregistrees comme constatations a part entiere.

5. Boucler la boucle et capitaliser les preuves

- [ ] Les constatations entrent dans un cycle de remediation suivi, avec responsables et dates.
- [ ] La cloture de la remediation est prouvee, et non simplement affirmee.
- [ ] Le dossier complet (perimetre, scenarios, recit d'attaque, constatations, remediation, performance de detection) est classe une seule fois selon la colonne vertebrale du NIST Cybersecurity Framework 2.0.
- [ ] Le dossier unique est etiquete pour chaque regime : SWIFT 7.3A, DORA, NYDFS Part 500, OSFI B-13.