SWIFT CSCF v2026 · Control 7.3A

Lista di controllo per la preparazione al penetration test SWIFT CSCF v2026 Control 7.3A

1. Definire il perimetro in base alle conseguenze

- [ ] Il patrimonio SWIFT e inventariato: zona sicura, interfaccia di messaggistica, postazioni degli operatori, connessione alla rete e i sistemi di back-office che la alimentano.
- [ ] I percorsi di attacco sono classificati in base alla conseguenza di una compromissione, non in base alla facilita di test.
- [ ] Il perimetro e definito rispetto alla zona sicura e ai suoi confini di fiducia, in modo che il test dimostri che un attaccante non puo spostarsi dal back-office allo strato di messaggistica.
- [ ] Il test e pianificato lungo il ciclo di scenari triennale, coprendo i percorsi applicativi, infrastrutturali e umani.

2. Inquadrare con l'intelligence sulle minacce

- [ ] L'intelligence attuale sugli attori che prendono di mira la messaggistica finanziaria alimenta gli scenari di test.
- [ ] Gli scenari riproducono percorsi di intrusione plausibili e nominati piuttosto che classi generiche di vulnerabilita.
- [ ] La base di intelligence e documentata, in modo che il test si qualifichi come guidato dalle minacce ai sensi di DORA e OSFI B-13.

3. Eseguire secondo lo standard piu rigoroso

- [ ] Il test viene eseguito sia dall'interno sia dall'esterno dei confini dei sistemi, soddisfacendo l'aspettativa di NYDFS Part 500.
- [ ] Il test e svolto da una parte competente e sufficientemente indipendente.
- [ ] Le regole di ingaggio, l'autorizzazione e i controlli di sicurezza per testare i sistemi in produzione sono documentati e approvati.
- [ ] Una cadenza definita e stabilita e registrata, soddisfacendo insieme il minimo annuale NYDFS e il ciclo SWIFT.

4. Misurare le proprie difese

- [ ] L'esercizio misura se il monitoraggio ha rilevato l'intrusione simulata, non solo cosa e stato trovato.
- [ ] Le prestazioni di risposta e contenimento sono registrate rispetto alle funzioni Rilevare e Rispondere.
- [ ] Le lacune di rilevamento sono registrate come risultanze a se stanti.

5. Chiudere il cerchio e mettere a frutto le prove

- [ ] Le risultanze entrano in un ciclo di rimedio tracciato, con responsabili e date.
- [ ] La chiusura del rimedio e provata, non semplicemente affermata.
- [ ] L'intero registro (perimetro, scenari, racconto dell'attacco, risultanze, rimedio, prestazioni di rilevamento) e archiviato una sola volta lungo la struttura portante del NIST Cybersecurity Framework 2.0.
- [ ] Il registro unico e etichettato per ciascun regime: SWIFT 7.3A, DORA, NYDFS Part 500, OSFI B-13.