SWIFT CSCF v2026 · Control 7.3A

Lista kontrolna gotowości do testu penetracyjnego SWIFT CSCF v2026 Control 7.3A

1. Zakres według konsekwencji

- [ ] Środowisko SWIFT jest zinwentaryzowane: strefa bezpieczna, interfejs komunikacyjny, stacje robocze operatorów, połączenie z siecią oraz systemy back-office, które je zasilają.
- [ ] Ścieżki ataku są uszeregowane według konsekwencji kompromitacji, a nie według łatwości testowania.
- [ ] Zakres jest zdefiniowany względem strefy bezpiecznej i jej granic zaufania, tak aby test dowiódł, że atakujący nie może przejść z back-office do warstwy komunikacyjnej.
- [ ] Testowanie jest zaplanowane w ramach trzyletniego cyklu scenariuszy, obejmując ścieżki aplikacyjne, infrastrukturalne i ludzkie.

2. Ramy oparte na analizie zagrożeń

- [ ] Aktualna analiza dotycząca aktorów atakujących komunikację finansową stanowi podstawę scenariuszy testowych.
- [ ] Scenariusze odtwarzają prawdopodobne, nazwane ścieżki włamania, a nie ogólne klasy podatności.
- [ ] Podstawa analityczna jest udokumentowana, dzięki czemu test kwalifikuje się jako prowadzony w oparciu o zagrożenia (threat-led) zgodnie z DORA i OSFI B-13.

3. Realizacja według najwyższego standardu

- [ ] Test jest przeprowadzany zarówno wewnątrz, jak i na zewnątrz granic systemów, spełniając oczekiwanie NYDFS Part 500.
- [ ] Test jest wykonywany przez kompetentną i wystarczająco niezależną stronę.
- [ ] Zasady zaangażowania, autoryzacja oraz mechanizmy bezpieczeństwa testowania systemów produkcyjnych są udokumentowane i zatwierdzone.
- [ ] Określona kadencja jest ustalona i zapisana, spełniając jednocześnie roczne minimum NYDFS i cykl SWIFT.

4. Zmierz własne mechanizmy obronne

- [ ] Ćwiczenie mierzy, czy monitoring wykrył symulowane włamanie, a nie tylko to, co zostało znalezione.
- [ ] Skuteczność reakcji i powstrzymania jest rejestrowana względem funkcji Detect i Respond.
- [ ] Luki w wykrywaniu są odnotowywane jako ustalenia same w sobie.

5. Zamknij pętlę i zabezpiecz dowody

- [ ] Ustalenia trafiają do śledzonego cyklu działań naprawczych z przypisanymi właścicielami i terminami.
- [ ] Zamknięcie działań naprawczych jest udowodnione, a nie jedynie deklarowane.
- [ ] Pełny zapis (zakres, scenariusze, narracja ataku, ustalenia, działania naprawcze, skuteczność wykrywania) jest składany raz względem szkieletu NIST Cybersecurity Framework 2.0.
- [ ] Pojedynczy zapis jest oznaczony dla każdego reżimu: SWIFT 7.3A, DORA, NYDFS Part 500, OSFI B-13.