SWIFT CSCF v2026 · Control 7.3A

قائمة التحقق من الجاهزية لاختبار الاختراق وفق ضابط SWIFT CSCF v2026 Control 7.3A

1. حدد النطاق وفق العواقب

- ☐ جرد ممتلكات SWIFT بالكامل: المنطقة الآمنة، وواجهة المراسلة، ومحطات عمل المشغلين، والاتصال بالشبكة، وأنظمة المكتب الخلفي التي تغذيها.
- ☐ ترتيب مسارات الهجوم بحسب عواقب الاختراق، وليس بحسب سهولة الاختبار.
- ☐ تعريف النطاق مقابل المنطقة الآمنة وحدود الثقة الخاصة بها، بحيث يثبت الاختبار أن المهاجم لا يستطيع التنقل من المكتب الخلفي إلى طبقة المراسلة.
- ☐ التخطيط للاختبار عبر دورة السيناريوهات الممتدة لثلاث سنوات، بما يشمل مسارات التطبيقات والبنية التحتية والمسارات البشرية.

2. أطّر الاختبار بالاستخبارات المتعلقة بالتهديدات

- ☐ الاستخبارات الحالية حول الجهات التي تستهدف المراسلات المالية توجّه سيناريوهات الاختبار.
- ☐ تحاكي السيناريوهات مسارات اختراق معقولة ومحددة الاسم بدلاً من فئات الثغرات العامة.
- ☐ توثيق الأساس الاستخباراتي، بحيث يكون الاختبار مؤهلاً كاختبار موجّه بالتهديدات وفق DORA وOSFI B-13.

3. نفّذ وفق أقوى المعايير

- ☐ يُجرى الاختبار من داخل حدود الأنظمة ومن خارجها معاً، بما يلبي توقعات NYDFS Part 500.
- ☐ يُنفّذ الاختبار بواسطة طرف كفء ومستقل بدرجة كافية.
- ☐ قواعد الاشتباك والتفويض وضوابط السلامة لاختبار الأنظمة الحية موثقة ومعتمدة.
- ☐ تحديد وتيرة معرّفة وتسجيلها، بما يلبي الحد الأدنى السنوي الذي تطلبه NYDFS ودورة SWIFT معاً.

4. قِس دفاعاتك الخاصة

- ☐ يقيس التمرين ما إذا كانت المراقبة قد رصدت الاختراق المُحاكى، وليس فقط ما تم اكتشافه.
- ☐ تسجيل أداء الاستجابة والاحتواء مقابل وظيفتي الكشف والاستجابة.
- ☐ تسجيل ثغرات الكشف بوصفها نتائج قائمة بذاتها.

5. أغلق الدائرة واحفظ الأدلة

- ☐ تدخل النتائج في دورة معالجة متتبَّعة لها أصحاب وتواريخ.
- ☐ إثبات إغلاق المعالجة بالأدلة، وليس مجرد التأكيد عليه.
- ☐ يُحفظ السجل الكامل (النطاق، والسيناريوهات، وسرد الهجوم، والنتائج، والمعالجة، وأداء الكشف) مرة واحدة مقابل العمود الفقري لإطار NIST Cybersecurity Framework 2.0.
- ☐ يُوسم السجل الواحد لكل نظام: SWIFT 7.3A، وDORA، وNYDFS Part 500، وOSFI B-13.