SWIFT CSCF v2026 · Control 7.3A

Контрольный список готовности к тесту на проникновение SWIFT CSCF v2026 Control 7.3A

1. Определение объёма по последствиям

- ☐ Среда SWIFT инвентаризирована: защищённая зона, интерфейс обмена сообщениями, рабочие станции операторов, подключение к сети и системы бэк-офиса, которые его питают.
- ☐ Пути атаки ранжированы по последствиям компрометации, а не по простоте тестирования.
- ☐ Объём определён относительно защищённой зоны и её границ доверия, чтобы тест доказал, что злоумышленник не может перейти из бэк-офиса в уровень обмена сообщениями.
- ☐ Тестирование спланировано в рамках трёхлетнего цикла сценариев и охватывает прикладные, инфраструктурные и человеческие пути.

2. Опора на анализ угроз

- ☐ Актуальные сведения об акторах, нацеленных на финансовый обмен сообщениями, лежат в основе тестовых сценариев.
- ☐ Сценарии воспроизводят вероятные, поименованные пути вторжения, а не общие классы уязвимостей.
- ☐ Основа в виде анализа угроз задокументирована, благодаря чему тест квалифицируется как ориентированный на угрозы (threat-led) согласно DORA и OSFI B-13.

3. Выполнение по самому строгому стандарту

- ☐ Тест проводится как изнутри, так и снаружи границ систем, отвечая ожиданию NYDFS Part 500.
- ☐ Тест выполняется компетентной и достаточно независимой стороной.
- ☐ Правила взаимодействия, авторизация и меры безопасности для тестирования действующих систем задокументированы и утверждены.
- ☐ Установлена и зафиксирована определённая периодичность, удовлетворяющая одновременно ежегодному минимуму NYDFS и циклу SWIFT.

4. Измерьте собственную защиту

- ☐ Мероприятие измеряет, обнаружил ли мониторинг смоделированное вторжение, а не только то, что было найдено.
- ☐ Эффективность реагирования и сдерживания фиксируется относительно функций Detect и Respond.
- ☐ Пробелы в обнаружении регистрируются как самостоятельные находки.

5. Замкните цикл и зафиксируйте доказательства

- ☐ Находки попадают в отслеживаемый цикл устранения с назначенными ответственными и сроками.
- ☐ Закрытие устранения подтверждается доказательствами, а не просто утверждается.
- ☐ Полная запись (объём, сценарии, описание атаки, находки, устранение, эффективность обнаружения) подшивается один раз относительно опоры NIST Cybersecurity Framework 2.0.
- ☐ Единая запись помечается для каждого режима: SWIFT 7.3A, DORA, NYDFS Part 500, OSFI B-13.