

SWIFT CSCF v2026 · Control 7.3A

SWIFT CSCF v2026 Control 7.3A sızma testi hazırlık kontrol listesi

1. Sonuca göre kapsam belirleme

- SWIFT ortamı envantere alınmıştır: güvenli bölge, mesajlaşma arayüzü, operatör iş istasyonları, ağa bağlantı ve onu besleyen back-office sistemleri.
- Saldırı yolları, test edilme kolaylığına göre değil, ele geçirilmenin sonucuna göre sıralanmıştır.
- Kapsam, güvenli bölgeye ve onun güven sınırlarına göre tanımlanmıştır; böylece test, bir saldırganın back-office'ten mesajlaşma katmanına geçemeyeceğini kanıtlar.
- Test, üç yıllık senaryo döngüsü boyunca planlanmış olup uygulama, altyapı ve insan yollarını kapsar.

2. Tehdit istihbaratıyla çerçeveleme

- Finansal mesajlaşmayı hedef alan aktörlere ilişkin güncel istihbarat, test senaryolarını şekillendirir.
- Senaryolar, genel güvenlik açığı sınıfları yerine olası, adlandırılmış izinsiz giriş yollarını canlandırır.
- İstihbarat temeli belgelenmiştir; böylece test, DORA ve OSFI B-13 kapsamında tehdit odaklı (threat-led) olarak nitelendirilir.

3. En güçlü standarda göre yürütme

- Test, sistemlerin sınırlarının hem içinden hem dışından yürütülerek NYDFS Part 500 beklentisini karşılar.
- Test, yetkin ve yeterince bağımsız bir tarafça gerçekleştirilir.
- Çalışma kuralları, yetkilendirme ve canlı sistemlerin test edilmesine yönelik güvenlik kontrolleri belgelenmiş ve onaylanmıştır.
- Tanımlı bir kadans belirlenmiş ve kaydedilmiştir; böylece hem yıllık NYDFS asgarisi hem de SWIFT döngüsü birlikte karşılanır.

4. Kendi savunmalarınızı ölçün

- Çalışma yalnızca neyin bulunduğunu değil, izlemenin simüle edilmiş izinsiz girişi tespit edip etmediğini de ölçer.
- Müdahale ve sınırlama performansı, Detect ve Respond işlevlerine göre kaydedilir.
- Tespit boşlukları kendi başlarına birer bulgu olarak kayıt altına alınır.

5. Döngüyü kapatın ve kanıtı güvenceye alın

- Bulgular, sahipleri ve tarihleri belirlenmiş, izlenen bir düzeltme döngüsüne girer.
- Düzeltmenin kapatılması yalnızca iddia edilmez, kanıtlanır.
- Tam kayıt (kapsam, senaryolar, saldırı anlatısı, bulgular, düzeltme, tespit performansı) NIST Cybersecurity Framework 2.0 omurgasına göre bir kez dosyalanır.
- Tek kayıt her rejime etiketlenir: SWIFT 7.3A, DORA, NYDFS Part 500, OSFI B-13.

Bunun kurumunuz için puanlanmasını ister misiniz? Cambridge Cyber International, SWIFT CSP değerlendirmesini ve 7.3A sızma testini bu standarda göre yürütür ve bulguları kapatılana kadar doğrular. Beyan pencerenizden önce bir kapsam belirleme görüşmesi ayarlayın.

contact@cambridgecyberinternational.com · cambridgecyberinternational.com/tr/contact/