SWIFT CSCF v2026 · Control 7.3A

SWIFT CSCF v2026 Control 7.3A पेनट्रिेशन-टेस्ट तैयारी जाँच-सूची

1. परिणाम के अनुसार स्कोप करें

- ☐ SWIFT संपदा की सूची तैयार है: सुरक्षति क्षेत्र, मैसेजगि इंटरफ़ेस, ऑपरेटर वर्कस्टेशन, नेटवर्क से कनेक्शन, और वे बैक-ऑफ़सि सिस्टम जो उसे फ़ीड करते हैं.
- ☐ हमले के रास्ते परीक्षण की आसानी के अनुसार नहीं, बल्कि समझौते के परिणाम के अनुसार क्रमबद्ध किए गए हैं.
- ☐ स्कोप को सुरक्षित क्षेत्र और उसकी विश्वास सीमाओं के विरुद्ध परिभाषित किया गया है, ताकि परीक्षण यह सिद्ध करे कि कोई हमलावर बैक ऑफ़िस से मैसेजिंग परत में नहीं घुस सकता.
- ☐ परीक्षण की योजना तीन-वर्षीय परिदृश्य चक्र में बनाई गई है, जिसमें एप्लिकेशन, अवसंरचना और मानवीय रास्ते शामिल हैं.

2. खतरा-आसूचना से रूपरेखा बनाएँ

- ☐ वित्तीय मैसेजिंग को निशाना बनाने वाले अभिकर्ताओं पर मौजूदा आसूचना परीक्षण परिदृश्यों को दिशा देती है.
- ☐ परिदृश्य सामान्य भेद्यता श्रेणियों के बजाय प्रशंसनीय, नामित घुसपैठ रास्तों का पूर्वाभ्यास करते हैं.
- ☐ आसूचना का आधार प्रलेखित है, ताकि परीक्षण DORA और OSFI B-13 के अंतर्गत खतरा-नेतृत्व वाले के रूप में योग्य हो.

3. सबसे सशक्त मानक तक निष्पादित करें

- ☐ परीक्षण सिस्टम की सीमाओं के भीतर और बाहर दोनों से चलाया जाता है, जो NYDFS Part 500 की अपेक्षा को पूरा करता है.
- ☐ परीक्षण किसी सक्षम और पर्याप्त रूप से स्वतंत्र पक्ष द्वारा किया जाता है.
- ☐ लाइव सिस्टम के परीक्षण हेतु संलग्नता के नियम, प्राधिकरण और सुरक्षा नियंत्रण प्रलेखित और अनुमोदित हैं.
- ☐ एक निर्धारित आवृत्ति तय और दर्ज की गई है, जो NYDFS की वार्षिक न्यूनतम सीमा और SWIFT चक्र दोनों को एक साथ संतुष्ट करती है.

4. अपनी स्वयं की रक्षा-व्यवस्था को मापें

- ☐ यह अभ्यास मापता है कि निगरानी ने अनुकरणित घुसपैठ का पता लगाया या नहीं, केवल यह नहीं कि क्या मिला.
- ☐ प्रतिक्रिया और नियंत्रण के प्रदर्शन को Detect और Respond कार्यों के विरुद्ध दर्ज किया जाता है.
- ☐ पता लगाने की खाइयों को अपने आप में निष्कर्षों के रूप में लॉग किया जाता है.

5. लूप बंद करें और साक्ष्य संचित करें

- ☐ निष्कर्ष एक ट्रैक किए गए उपचार चक्र में प्रवेश करते हैं जिसमें स्वामी और तिथियाँ होती हैं.
- ☐ उपचार के समापन को केवल दावे के रूप में नहीं, बल्कि साक्ष्य सहित प्रमाणित किया जाता है.
- ☐ पूरा अभिलेख (स्कोप, परिदृश्य, हमले का विवरण, निष्कर्ष, उपचार, पता लगाने का प्रदर्शन) NIST Cybersecurity Framework 2.0 की रीढ़ के विरुद्ध एक बार दाखिल किया जाता है.
- ☐ एकल अभिलेख को प्रत्येक व्यवस्था के लिए टैग किया जाता है: SWIFT 7.3A, DORA, NYDFS Part 500, OSFI B-13.