SWIFT CSP assessment services

SWIFT Customer Security Program (CSP) a été établi en 2016, pour sécuriser les environnements des utilisateurs du réseau SWIFT.

Ce programme doit permettre de protéger le réseau et son organisation à travers un framework de contrôle – le SWIFT CSCF.

Les attestations de conformité sont publiées et partagés au sein de la communauté SWIFT et se présentent sous forme d'un reporting sur le niveau de conformité au CSCF.

SWIFT Customer Security Program.

SWIFT CSP a été créé pour aider sa communauté mondiale de clients à se protéger contre les cyber-attaques, ceci a été motivée par :

- Plusieurs compromissions de membres SWIFT entre 2016 et 2018 qui ont défrayé la chronique
- Des attaques via les membres SWIFT
- La menace actuelle des Blockchains sur le modèle SWIFT

Le programme permet l'adoption de bonnes pratiques de sécurité dans la communauté SWIFT et ce en apportant un ensemble de contrôles de sécurité – Customer Security Controls Framework (CSCF) – qui ont pour objectifs de :

- Améliorer la sécurité des membres
- Renforcer la transparence entre partenaires
- Réduire les attaques et la fraude

Ces contrôles sont validés par une attestation annuelle.

CSP Security Controls Framework (CSCF).

Basé sur trois principes clés et huit chapitres, CSCF répond à une variété de risques cyber et définit des contrôles sécurité qui peuvent aussi être étendus aux environnements utilisateurs.

Principe clé 1: Sécuriser votre environnement	Limiter l'accès à internet
	Dissocier les systèmes critiques de l'environnement informatique et bureautique général
	Réduire la surface d'attaque et les vulnérabilités
	Sécuriser physiquement l'environnement
Principe clé 2: Contrôler et limiter l'accès	Se protéger contre les vols d'intifiants
	Gérer les identités et ségréguer les privilèges
Principe clé 3: Détecter et réagir	Détecter les activités anormales dans les systèmes ou les relevés d'opérations
	Établir un plan d'actions en cas d'incident et de partage d'informations

verizon

10 années d'expertise PCI DSS et ISO 27001 au service de SWIFT CSP

Verizon a mis en œuvre une approche pragmatique et souple pour la conformité au standard SWIFT CSPF, basée sur plus de 10 années d'expertise sur PCI DSS.

Notre méthodologie se base sur 6 étapes essentielles à la réussite du programme SWIFT CSP :

Phase 1

Le Client complète le **SWIFT WELCOME PACKAGE (SWP)** afin de bien cadrer le champ d'application et le périmètre de conformité (fonctionnel, technique et organisationnel).

Phase 2

Verizon effectue un **examen préliminaire** de tous les éléments fournis avant de commencer l'évaluation.

Phase 3

Verizon démarre la **revue à distance** en se basant sur la documentation et les preuves demandées.

Phase 4

Verizon **mène les entretiens d'évaluation sur site** en fonction de l'agenda et du calendrier prévus, avec la collecte des preuves sur place.

Phase 5

Verizon effectue une **réévaluation (sur place – à distance)** des écarts de conformité découverts afin d'atteindre la conformité **(priorité aux contrôles obligatoires).**

Phase 6

Verizon finalise le reporting en fournissant les livrables: Outil d'évaluation CSCF, la lettre d'évaluation indépendante, présentation exécutive.

Les éléments clés de l'environnement SWIFT à considérer.

Echange de données	Toutes les applications en relation avec SWIFT et de transfert de données (MT/MX messages; fichiers; etc.).
Infrastructure SWIFT Locale	Dépendamment du mode de connexion (on-premises–cloud–Service Provider).
Architecture	Type A ou B.
PC Opérateurs	Poste de travail des opérateurs.
Opérateurs et personnel	Le personnel SWIFT qui utilise ou interagit avec l'environnement.

Pourquoi Verizon.

Verizon est un acteur global de la cyber-sécurité présent en France depuis de nombreuses années. Nos compétences techniques certifiées, notre expertise en termes de réalisation d'audits, les certifications de nos collaborateurs dans le domaine de la cyber-sécurité, permettront une approche qui saura s'adapter à vos besoins.

Nous suivons l'évolution rapide des cyber-menaces d'aujourd'hui en traitant plus d'un million d'événements de sécurité chaque jour dans nos centres d'exploitation de réseau et nos centres d'exploitation de sécurité mondiaux. Ce n'est là qu'une des nombreuses raisons pour lesquelles nous savons comment vous protéger des attaques non seulement à la périphérie de votre réseau, mais aussi de celles qui le menacent au-delà.

Nous contacter.

Pour plus d'informations, merci de vous rapprocher de votre contact commercial ou de contacter le siège de Verizon France au 01 53 75 82 00.

Verizon, Tour CB21

16, Place de l'Iris

92040 Courbevoie

France

enterprise.verizon.com/fr-fr/

verizon