



Protéger les entreprises et leurs données avec des solutions de résilience et de transfert de risques.



Nos services de Cyber- résilience

Services de prévention et de transfert de risques

L'accélération de la transition digitale et l'émergence de nouvelles technologies ont rendu les entreprises vulnérables face aux cybercriminels. De la résilience à l'assurance, nous proposons une variété de solutions de cybersécurité pour les entreprises afin de les aider à se protéger contre les risques réputationnels, financiers et de conformité.

Vos défis



Augmentation des cyberattaques

Le paysage des menaces cyber évolue de manière complexe et les attaques deviennent de plus en plus sophistiquées. Les entreprises doivent anticiper ces évolutions et rester proactives en cyber sécurité.



Nécessité de protéger vos données et limiter toute perte financière

Avec l'augmentation de la collecte de données par les entreprises, il est crucial d'identifier les données essentielles pour leurs opérations et protéger celles de leurs clients.



Exigences réglementaires plus complexes

Les entreprises sont confrontées à une demande croissante de démontrer et de rapporter des mesures efficaces, allant de la directive NIS2 à la nouvelle loi sur la protection des données (nLPD), de DORA aux exigences de la FINMA.



Nos solutions



Simplification du monde cyber

Nous vous aidons à naviguer à travers la complexité cyber et à vous conformer aux dernières exigences réglementaires.



Association des services de prévention avec l'assurance

Nos solutions de résilience reposent sur des recherches scientifiques pour des contrôles cyber efficaces et une meilleure assurabilité.



Amélioration de la maturité cyber et la résilience face aux menaces

Avec nos services de cyber-résilience, nous offrons une approche efficace et adaptée à toutes les tailles d'entreprises.



Formations



Formation de sensibilisation Cyber (en ligne)

Cours en ligne présentant les moyens de détecter les potentielles menaces cyber et de réduire les chances de réussite des attaques.



Formation sur site (incluant notre Cyber Escape Game)

Formation personnalisée en présentielle sur les meilleures pratiques en matière de cybersécurité, de protection des données et d'expérience réelle de piratage.



Exercices de phishing

Simulation d'attaques visant à évaluer la capacité des employés à détecter et à réagir aux emails de phishing.



Formation à la gestion de crise cyber

Acquérez les compétences nécessaires pour organiser et gérer les crises cybernétiques afin de les atténuer efficacement et de limiter les dommages.



Cyber Escape Game (jeu d'évasion cyber)

Expérience immersive qui met les participants au défi de résoudre des énigmes de cybersécurité, améliorant ainsi leurs connaissances et leurs compétences de manière ludique et captivante. Cette expérience peut être recréée dans un environnement physique ou à l'aide d'un casque de réalité virtuelle.

Évaluations



Cyber Snapshot

Évaluation automatique réalisée pour déterminer le niveau de sécurité informatique d'une organisation à l'aide d'un score de maturité.



Cyber Healthcheck: Évaluation de maturité cyber

Évaluation basée sur des questionnaires Zurich et le standard NIST, fournissant un rapport détaillé et des recommandations.



Audit sur la protection des données & évaluation de maturité cyber

Audit de conformité aux réglementations locales et internationales en matière de protection des données à caractère personnel et évaluation de la maturité cyber.



Audit ISO 27001

Évaluation de la maturité cyber selon la norme ISO 27001 pour aider les entreprises à se préparer à la certification.



Audit sur la gestion de crise cyber

Évaluation de la préparation, des capacités de réponse et de la résilience d'une organisation face aux menaces et incidents cyber.



Exercice de simulation de crise (table-top exercise)

Exercice basé sur des scénarios pour évaluer et améliorer vos stratégies de préparation et de réponse en cas d'attaque cybernétique.

Services techniques



Scan de vulnérabilités externes et internes.

Processus automatisé permettant d'identifier et de détecter les vulnérabilités de sécurité dans les systèmes informatiques et les réseaux.



Test d'intrusion

Simulation manuelle personnalisée d'attaques réelles (piratage) pour identifier les vulnérabilités et évaluer les risques potentiels.



Service de détection et de réponse à incidents optimisé pour les "PME"

Centre d'opérations de sécurité (SOC) pour les PME, assurant une surveillance en temps réel et une réponse aux menaces cyber.



Service de détection et de réponse à incidents (SOC)

Centre d'opérations de sécurité complet pour la surveillance en temps réel et la réponse aux menaces de cybersécurité.

Support en stratégie



Gouvernance cyber

Assistance dans la rédaction de votre documentation de gouvernance en matière de cybersécurité (contrôle d'accès, mot de passe, classification des données, chiffrement, etc.).



Plan de gestion d'incidents

Procédure documentée détaillant la réponse et la gestion des incidents de cybersécurité.



Exposition financière (quantification du risque cyber)

Évaluation continue de l'impact financier pour orienter la priorisation et la justification des investissements et de la stratégie en matière de cybersécurité.



Gestion des sous-traitants

Plateforme Zurich permettant de surveiller la maturité cyber de l'ensemble de la chaîne d'approvisionnement, basé sur différents niveaux d'évaluation.



Services de continuité d'activité.

Définition de la stratégie de continuité d'activité, y compris l'évaluation de l'impact sur l'activité (BIA), l'élaboration de politiques et autres.



Expert Cyber à la demande

Assistance ponctuelle fournissant une expertise spécialisée pour développer, mettre en œuvre et gérer une stratégie de cybersécurité.



Contacts



Sylvain Luiset

Cyber Team Leader
Switzerland

sylvain.luiset@zurich.ch
+41 79 377 26 44



Jenany Sivathasan

Cyber Risk Consultant

jenany.sivathasan@zurich.ch
+41 76 536 91 52



Suvathihan
Uthayakumaran

Cyber Risk Consultant

suvi.uthayan@zurich.ch
+41 76 456 75 84

Pourquoi Zurich Cyber Resilience Solutions?



Nous vous aidons à devenir assurable



Nous disposons de données sinistres (connaissance des attaques) ainsi que de benchmark clients par secteur d'activité



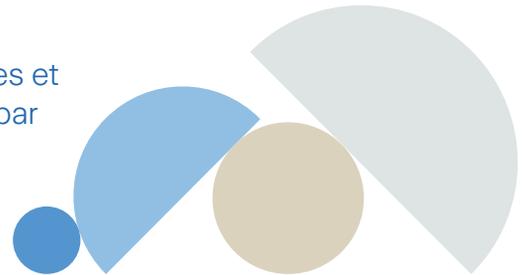
Nous proposons des services sur mesure selon la taille de l'entreprise



En plus de l'expertise, nous disposons de méthodes et solutions validées par des études scientifiques et par notre équipe interne de R&D.



Nous sommes présents sur tous les continents



This is a general description of (insurance) services such as risk engineering or risk management services by Zurich Resilience Solutions which is part of the Commercial Insurance business of Zurich Insurance Group, and does not represent or alter any insurance policy or service agreement. Such (insurance) services are provided to qualified customers by affiliated companies of Zurich Insurance Company Ltd (Zurich Insurance Group). The prices stated are exclusive of VAT and are subject to change at any time.

The opinions expressed herein are those of Zurich Resilience Solutions as of the date of the release and are subject to change without notice. This document has been produced solely for informational purposes. All information contained in this document has been compiled and obtained from sources believed to be reliable and credible but no representation or warranty, express or implied, is made by Zurich Insurance Company Ltd or any members of Zurich Insurance Group as to their accuracy or completeness. This document is not intended to be legal, underwriting, financial, investment or any other type of professional advice. Zurich Insurance Group disclaims any and all liability whatsoever resulting from the use of or reliance upon this document. Nothing express or implied in this document is intended to create legal relations between the reader and any member of Zurich Insurance Group.

Certain statements in this document are forward-looking statements, including, but not limited to, statements that are predictions of or indicate future events, trends, plans, developments or objectives. Undue reliance should not be placed on such statements because, by their nature, they are subject to known and unknown risks and uncertainties and can be affected by numerous unforeseeable factors. The subject matter of this document is also not tied to any specific service offering or an insurance product nor will it ensure coverage under any insurance policy.

This document may not be distributed or reproduced either in whole, or in part, without prior written permission of Zurich Insurance Company Ltd, Mythenquai 2, 8002 Zurich, Switzerland. No member of Zurich Insurance Group accepts any liability for any loss arising from the use or distribution of this document. This document does not constitute an offer or an invitation for the sale or purchase of securities in any jurisdiction.