

RSM Switzerland

Un partenaire à vos côtés

A blue rectangular banner with the text "CYBERSHIELD ACADEMY" in white, bold, sans-serif capital letters.

CYBERSHIELD ACADEMY

CyberShield Academy

1. Qui sommes-nous ?

Nous proposons des solutions complètes de cybersécurité conçues pour aider les organisations à mettre en place des défenses solides contre des menaces qui évoluent constamment. Notre approche met l'accent sur l'éducation, la préparation et la mise en conformité et la standardisation des politiques de sécurité, afin de vous aider à protéger vos actifs numériques tout en sensibilisant votre équipe.

Le saviez-vous ?

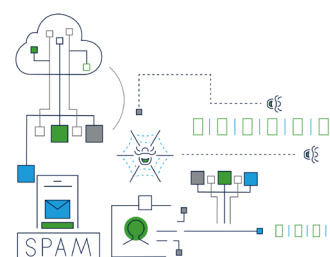
- Selon le rapport "Verizon 2022 Data Breach Investigations Report", 82 % des violations de données mettent en cause un facteur humain, tel que des erreurs, une mauvaise utilisation ou des tactiques d'ingénierie sociale.¹
- Les organisations qui mettent en place des formations régulières de sensibilisation à la cybersécurité peuvent réduire la vulnérabilité au phishing jusqu'à 75 %, comme le montre une étude de KnowBe4.²
- Une étude réalisée en 2024 par Hornet Security a révélé que 78,5 % des organisations estiment que les actions de sensibilisation à la sécurité informatique ont permis d'éviter directement des incidents de cybersécurité.³
- Une étude publiée dans le Journal de l'ISACA indique que les entreprises peuvent obtenir un retour sur investissement (ROI) allant jusqu'à 500 % en mettant en œuvre des programmes de sensibilisation à la cybersécurité, en particulier dans les grandes organisations.⁴

2. Nos services de base

Nous proposons une plateforme centralisée pour sensibiliser l'ensemble de votre organisation à la cybersécurité. Notre système permet de suivre l'engagement et les progrès des employés dans les domaines clés de la sécurité informatique.

Caractéristiques de la plate-forme

- ✓ Formation de sensibilisation à la cybersécurité
- ✓ Simulations d'hameçonnage
- ✓ Surveillance des brèches sur le Dark Web
- ✓ Gestion et suivi des politiques



¹ Keepnet Labs. (2024, 23 janvier). 2025 Security awareness training statistics. <https://keepnetlabs.com/blog/security-awareness-training-statistics>

² KnowBe4. (2011, 11 juillet). New KnowBe4 statistics reveal security awareness training reduces phishing susceptibility by 75%. <https://www.knowbe4.com/press/security-awareness-training-reduces-phishing-susceptibility-by-75>

³ Hornetsecurity. (2024, 3 juin). Security awareness survey: 1 in 4 (25.7%) organizations do not provide I.T. security awareness training. <https://www.hornetsecurity.com/en/blog/security-awareness-survey-2024/>

⁴ Bhaskar, R. (2022, 18 mai). Better cybersecurity awareness through research. ISACA Journal, 2022(3). <https://www.isaca.org/resources/isaca-journal/issues/2022/volume-3/better-cybersecurity-awareness-through-research>

CyberShield Academy

3. Nos offres

Nous proposons ces services sous la forme de trois formules personnalisées, avec des options supplémentaires pour répondre aux besoins spécifiques de votre secteur ou de votre entreprise ([annexe 1](#)).

01

Starter – Prix sur demande

- ✓ Configuration de la plate-forme
- ✓ Campagne d'hameçonnage standard
- ✓ Modules de formation standard
- ✓ Surveillance de base des brèches
- ✓ Stockage et suivi des politiques
- ✓ Rapports mensuels automatisés

Frais de licence annuels
(moins de 2 CHF par utilisateur et par mois)

02

Standard – Prix sur demande

- ✓ Comprend toutes les fonctions de démarrage, plus :
2 simulations d'hameçonnage personnalisées basées sur le secteur de votre entreprise et les rôles des employés

Le droit de licence annuel s'applique

03

Premium – Prix sur demande

- ✓ Comprend toutes les caractéristiques standard, plus :
Surveillance avancée des brèches (Breach Pro)
Débriefing d'une heure sur le rapport trimestriel avec un expert

Le droit de licence annuel s'applique

4. Compléments optionnels (EXTRAS) – Prix sur demande

Formation en présentiel (session de 4 heures) ([annexe 2](#))

- ✓ Des programmes sur mesure : Adaptés à votre secteur d'activité et aux besoins de votre équipe.
- ✓ Des instructeurs qualifiés : Dirigés par des professionnels de la cybersécurité.
- ✓ Les thèmes abordés sont les suivants
 - ✓ Bonnes pratiques en matière de cyber-hygiène
 - ✓ Sensibilisation à l'ingénierie sociale
 - ✓ Gestion sécurisée des mots de passe
 - ✓ Procédures de réponse aux incidents

CyberShield Academy

Simulations d'hameçonnage personnalisées

- ✓ Conçu en fonction de votre secteur d'activité et des flux de travail de vos employés.
- ✓ Comprend des courriels ciblés, des pages de renvoi, un suivi et une analyse.

Rédaction et déploiement de politiques

- ✓ Identifier les besoins en matière de politique sur la base des meilleures pratiques et des normes (par exemple, ISO 27001).
- ✓ Élaborer et valider les politiques en collaboration avec les dirigeants.
- ✓ Distribuer les politiques et suivre la reconnaissance des employés.

Soutien à l'intégration SSO

- ✓ Coordonnez avec votre équipe IT ou des fournisseurs tiers la mise en œuvre de l'authentification unique (SSO) sur toutes les plateformes.

5. Pourquoi nous choisir ?

- ✓ Plus de 20 ans d'expertise en cybersécurité
- ✓ Une offre complète, de la prévention à l'intervention
- ✓ Des solutions évolutives pour les PME et les grandes entreprises
- ✓ Impact mesurable : Réduction des incidents de phishing, amélioration de la conformité et diminution des primes d'assurance.

Contactez-nous !

Scannez ce code QR et contactez-nous directement sur notre site web.



À propos de RSM

Réseau RSM

Une présence mondiale qui renforce notre offre en Suisse

Depuis la Suisse, RSM exerce ses activités au niveau local tout en tirant parti de la portée et des capacités du réseau international RSM. Cela permet à nos équipes d'appliquer les normes internationales et d'accéder à une expertise spécialisée chaque fois que cela s'avère nécessaire, sans pour autant perdre de vue la proximité ni le leadership local.

- Des cabinets dans **120 pays**, avec une présence dans chacun des **40 principaux centres d'affaires mondiaux**
- **Plus de 56'000 professionnels** à l'échelle mondiale
- **Plus de 500 bureaux** répartis en Amérique, en Europe, dans la région MENA, en Afrique et en Asie-Pacifique



56,000
Employés



500
Bureaux



120
Pays

RSM Switzerland

Une expertise suisse, ancrée dans le tissu économique local

Présent dans toute la Suisse, RSM accompagne les PME, les entreprises de taille intermédiaire suisses ainsi que les grandes entreprises en leur proposant des services d'audit et d'assurance, de fiscalité et de conseil. Nos équipes possèdent une solide connaissance de l'environnement réglementaire, économique et entrepreneurial suisse, ce qui garantit clarté et fiabilité dans chaque mission.

Un interlocuteur unique en Suisse, connecté au monde entier

Nous savons que le temps est précieux. Votre interlocuteur suisse dédié coordonne vos besoins au niveau local et agit comme votre interface centrale, garantissant une collaboration fluide et une prestation efficace, tout en restant proche des réalités de votre entreprise.

Des solutions sur mesure pour les entreprises suisses

Grâce à des relations étroites avec nos clients et à une solide connaissance des secteurs, nous proposons des solutions pratiques et sur mesure.

Notre approche aide les organisations à améliorer leur efficacité, à gérer les risques et à soutenir une croissance durable en Suisse et au-delà.

Notre présence en Suisse



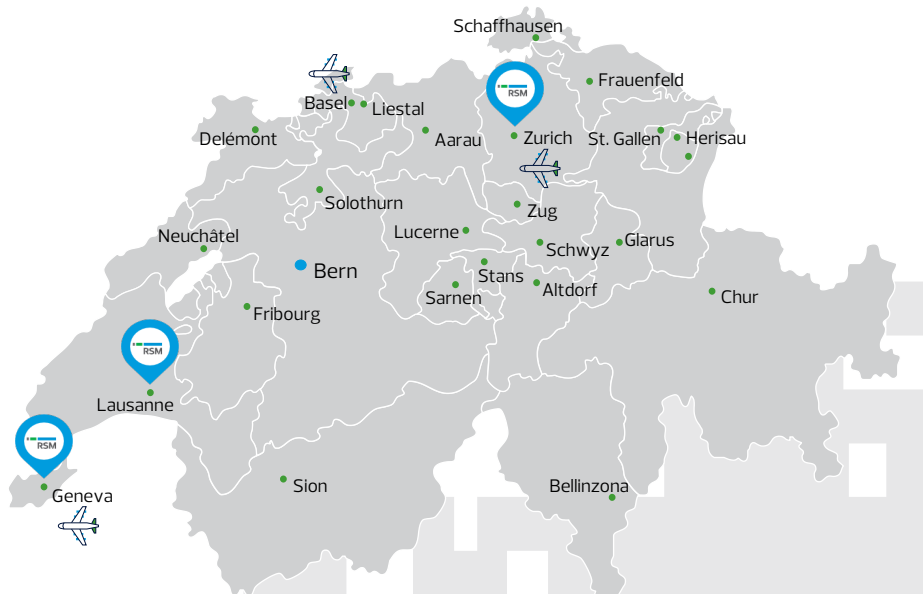
3
Bureaux



13
Partners



140+
Employés



LISTE DES FORFAITS ET TARIFS DISPONIBLES (ANNEXE 1)

	Offre			
	Démarrage	Standard	Prime	Extra
Mise en place	x	x	x	–
Hameçonnage	x	x	x	–
Formation	x	x	x	–
Contrôle des infractions	x	x	x	–
Stockage des politiques	x	x	x	–
Rapport mensuel automatisé	x	x	x	–
Suivi des licences annuelles	x	x	x	
2 Phishing personnalisé lié aux activités des employés/au secteur de l'entreprise	–	x	x	–
Breach Pro Insight	–	–	x	–
1h de compte-rendu par trimestre	–	–	x	–
Formation en personne Demi-journée	–	–	–	Sur demande
Phising personnalisé lié aux activités des employés/au secteur de l'entreprise	–	–	–	Sur demande
Rédaction de la politique	–	–	–	Sur demande
Connexion SSO	–	–	–	Sur demande
TOTAL	Sur demande	Sur demande	Sur demande	

PLAN DE FORMATION À LA CYBERCONSCIENCE (ANNEXE 2)

	Heure de début	L'heure de la fin	Période
Accueil	8:30	9:00	0:30
Introduction - Présentation du formateur et brise-glace - Objectifs et attentes en matière de formation - Présentation de l'ordre du jour	9:00	9:15	0:15
Paysage des cybermenaces - Pourquoi la cybersécurité est importante (impact sur le monde réel) - Les cybermenaces courantes : - Hameçonnage - Logiciels malveillants et rançongiciels - Ingénierie sociale - Menaces d'initiés - Tendances des menaces et évolution des risques	9:15	9:45	0:30
Phishing et ingénierie sociale - Comment fonctionne l'hameçonnage (courriel, SMS, voix) - Tactiques et exemples d'ingénierie sociale - Comment détecter et signaler un hameçonnage ?	9:45	10:15	0:30
Pause 1	10:15	10:30	0:15
Mots de passe, MFA et sécurité des comptes - Pratiques de sécurisation des mots de passe - Gestionnaires de mots de passe : comment et pourquoi - L'importance de l'AMF et son fonctionnement - Pièges liés à la récupération des comptes	10:30	11:00	0:30
Protection des données - Qu'est-ce qu'une donnée sensible ? - Classification et étiquetage des données - Aperçu juridique (GDPR, lois locales) - Comment protéger les données au travail et en déplacement ?	11:00	11:30	0:30
Pause 2	11:30	11:45	0:15
Travail à distance sécurisé et sécurité des appareils - Travailler à domicile en toute sécurité - Utiliser le Wi-Fi public en toute sécurité - Cryptage des appareils, USB, téléphones portables - Politiques BYOD	11:45	12:15	0:30
Rapport d'incident, Q&R, Synthèse - Comment signaler une activité suspecte - Aperçu de la réponse aux incidents	12:15	12:30	0:15
Récapitulation des points à retenir	12:30	12:40	0:10
Quiz final	12:40	13:00	0:20
Q&R + Conclusion	13:00	13:15	0:15
TOTAL			4:45