



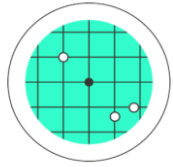
Cyber-way |

Proposition technique et commerciale



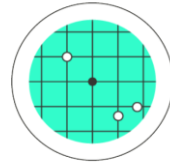
FCE FRANCE
FEMMES CHEFS D'ENTREPRISES

Le 09/02/2023



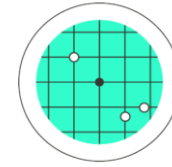
1/2

Des entreprises ont été victimes d'une Cyberattaque en 2022



+600%

Depuis le début de la pandémie en 2020



70%

Visent des TPE/PME



Pannes informatiques



Vol de données



Détournement de fonds



Risques juridiques



Atteinte à la réputation

20% des TPE touchées par une attaque cyber ont subi un préjudice supérieur à 50 000 € et cela peut aller à plus de 100 000 € pour 3% d'entre elles.

Pour les plus modestes des impacts qui vont jusqu'à la cessation d'activité »

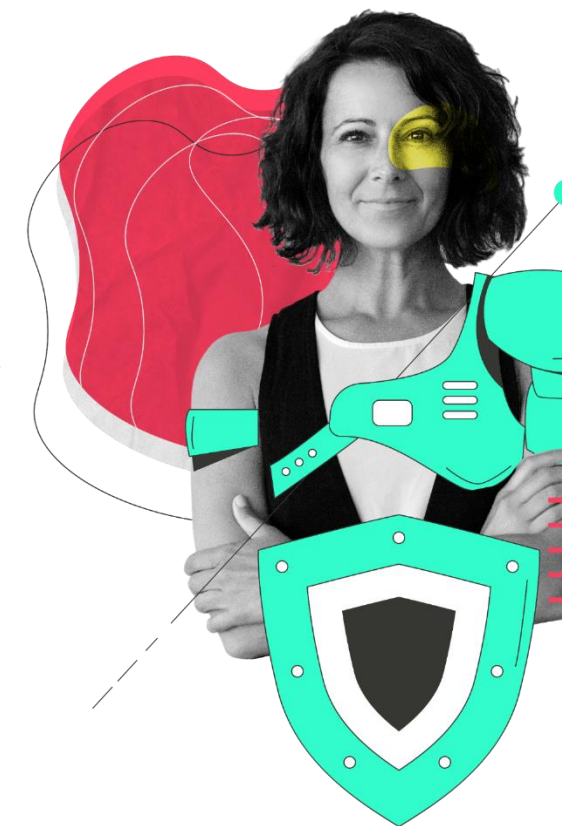
Qui sommes nous ?

CYBER-WAY by crédit Agricole Alpes Provence

Le Crédit Agricole Alpes Provence en tant qu'établissement bancaire a investi depuis des années en Cyber Sécurité et dispose aujourd'hui de moyens de protection robustes et éprouvés ainsi que d'un réseau d'experts dans le domaine.

Avec notre filiale « CYBER-WAY By Crédit Agricole Alpes Provence », notre volonté est désormais de partager notre savoir-faire en matière de Cyber Sécurité et ainsi de vous aider autrement.

Dans un contexte de montée des risques Cyber, notre conviction, c'est pouvoir soutenir nos entreprises, mais aussi les associations et les collectivités publiques du territoire dans leur démarche de Cyber Sécurité .



1



SENSIBILISATION

RDV, Interventions, webinaires auprès des dirigeants/ DAF/ DSI :

- **RDV clients**
- **Évènements** organisés par les chambres de métiers, fédérations et syndicats professionnels, groupement d'entreprises, réseaux d'affaires.

2

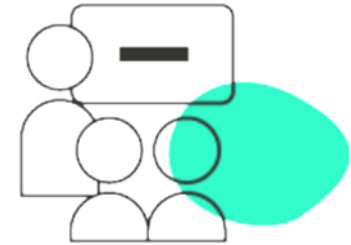


AUDIT

Des niveaux d'audit adaptés à chaque cible :

- **CyberCheckup** : entreprises;
- **CyberDiag** : professionnels
- **Cyberconsultation** : entreprises ou professionnels avec une problématique identifiée et nécessitant pour le dirigeant un conseil externe.

3

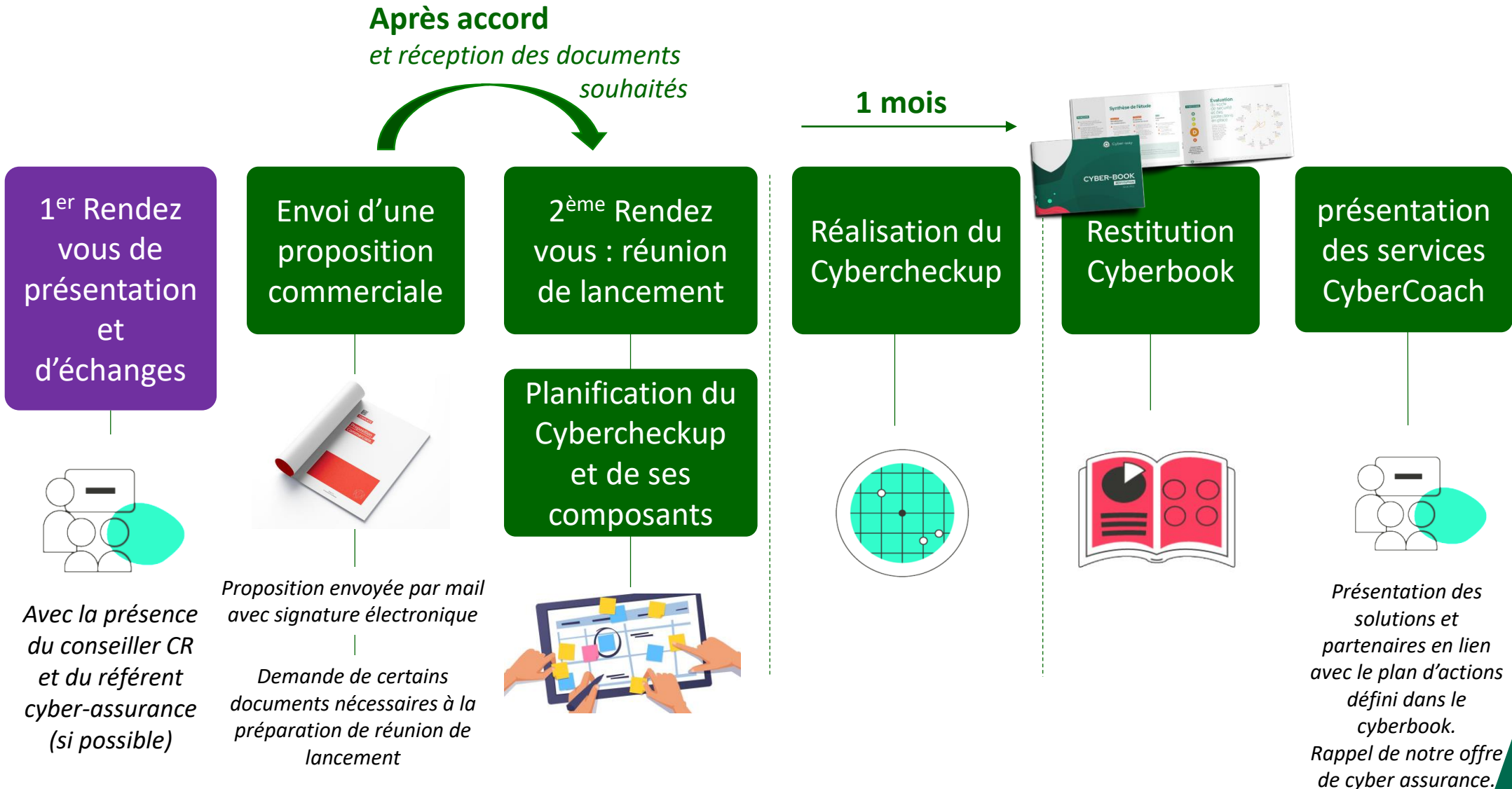


CONSEIL

Un accompagnement dans le temps :

- **Cyber Coaching;**
- **Cyber Surveillance**
- **Cyber Sensibilisation**
- **Soutien à la commercialisation de l' Assurance Cyber .**

Un fonctionnement qui s'appuie sur notre connaissance client



Le « cyber book », un outil stratégique et pédagogique

CYBER SCORE

A
B
C
D
E

L'entreprise dispose d'un socle technique solide.
Le renforcement de la culture cyber sécurité des collaborateurs, associée à l'intégration de la sécurité dans les développements logiciels, et au durcissement des terminaux mobiles, permettront de faire encore progresser la maturité cyber.

Évaluation du socle de sécurité et des protections en place

À l'appui de points de vérification adaptés au contexte de l'entreprise, inspirés des bonnes pratiques de l'ANSSI, des constats sont établis autour de 13 thèmes de cyber sécurité.

- 00. Gouverner
- 01. Sensibiliser et former
- 02. Connaître le système d'information
- 03. Authentifier et contrôler les accès
- 04. Sécuriser les postes
- 05. Sécuriser le réseau
- 06. Sécuriser l'administration du SI
- 07. Gérer le nomadisme
- 08. Maintenir à jour le système d'information
- 09. Superviser, auditer, réagir
- 10. Sécuriser la conception des services
- 11. Assurer la reprise d'activité après un sinistre
- 12. Prévenir et traiter la fraude

Principaux événements redoutés

CONFIDENTIEL

Évaluation des risques liés à l'indisponibilité de services

Principaux scénarios

Scénario	Vraisemblance	Impact	Niveau de protection	Capacité à réagir	Année Écoulée	Commentaires et mesures prioritaires
11. Piratage de SI malin	3 - Scénario probable	3 - Impact important : Arrêt d'un site de réservation en ligne	1 - Peu satisfaisante	2 - Satisfaisante	2 - Moyen	Risque : Indisponibilité d'un site Internet Mesure : vérifier auprès de l'Éditeur l'application de bonnes pratiques de développement sécurisé (au-delà des mises à jour du Framework de développement et au-delà des traitements des vulnérabilités du top 10 OWASP, revue de code, tests d'intrusion...)
12. Piratage de SI banal	3 - Scénario probable	3 - Impact important : Arrêt d'un site de réservation en ligne	1 - Peu satisfaisante	2 - Satisfaisante	2 - Moyen	Risque : Indisponibilité d'un site Internet Mesure : vérifier auprès de l'Éditeur l'application de bonnes pratiques de développement sécurisé (au-delà des mises à jour du Framework de développement et au-delà des traitements des vulnérabilités du top 10 OWASP, revue de code, tests d'intrusion...)
13. Abus de privilèges	2 - Peu	2 - Impact important : Arrêt d'un site de réservation en ligne	1 - Peu satisfaisante	2 - Satisfaisante	2 - Moyen	Risque : Indisponibilité d'un site Internet Mesure : vérifier auprès de l'Éditeur l'application de bonnes pratiques de développement sécurisé (au-delà des mises à jour du Framework de développement et au-delà des traitements des vulnérabilités du top 10 OWASP, revue de code, tests d'intrusion...)
14. Piratage de SI espion	2 - Peu	2 - Impact important : Arrêt d'un site de réservation en ligne	1 - Peu satisfaisante	2 - Satisfaisante	2 - Moyen	Risque : Indisponibilité d'un site Internet Mesure : vérifier auprès de l'Éditeur l'application de bonnes pratiques de développement sécurisé (au-delà des mises à jour du Framework de développement et au-delà des traitements des vulnérabilités du top 10 OWASP, revue de code, tests d'intrusion...)
15. Piratage de services fournis par des tiers	3 - Scénario probable	3 - Impact important : Arrêt d'un site de réservation en ligne	1 - Peu satisfaisante	2 - Satisfaisante	2 - Moyen	Risque : Indisponibilité d'un site Internet Mesure : vérifier auprès de l'Éditeur l'application de bonnes pratiques de développement sécurisé (au-delà des mises à jour du Framework de développement et au-delà des traitements des vulnérabilités du top 10 OWASP, revue de code, tests d'intrusion...)

EN RÉSUMÉ

Les principales mesures à mettre en œuvre à très court terme sont :

- Bloquer la connexion au réseau interne de l'entreprise pour les appareils non référencés par l'INFOGERANT
- Renforcer les mots de passe des utilisateurs
- Sécuriser le cycle de développement de la solution Métier

ÉVALUATION DU RISQUE

- Faible** : La vulnérabilité doit être traitée soit dans les 6 mois, soit en cours de cycle de développement, soit faire l'objet d'une acceptation formelle du risque résiduel par le métier
- Moyen** : La vulnérabilité doit être traitée dans les 3 mois



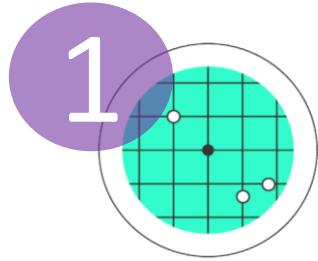
Mesures à mettre en œuvre en urgence

Coût : € faible / €€ moyen / €€€ haut
Complexité : 🟢 simple / 🟡 moyen / 🔴 complexe

Complexité	Coût	Mesure
COMPLEX.	COÛT	02. Connaître le système d'information
🟢	€	Restreindre l'usage du réseau d'entreprise aux seuls matériels autorisés par l'entreprise par des moyens techniques à définir avec l'INFOGERANT (Adresse MAC, certificats ...)
COMPLEX.	COÛT	10. Sécuriser la conception des services
🟢	€	Demander à l'ÉDITEUR de renforcer ses pratiques de développement sécurisé ; mettre en œuvre une recette sécurité (communiquer à l'ENTREPRISE les résultats), faire réaliser une revue de code, renforcer la protection des données des utilisateurs (conservation et complexité des mots de passe) ...
COMPLEX.	COÛT	05. Sécuriser le réseau
🟢	€	Sensibiliser les collaborateurs à l'usage de mots de passe complexes : <ul style="list-style-type: none"> Stockage sécurisé des mots de passe (éviter l'enregistrement des mots de passe dans les navigateurs, utiliser un coffre-fort numérique ...) Sécurisation des mots de passe sur des services externes à l'entreprise (Smartphones, messagerie en ligne ...)
🟢	€	Voir avec l'INFOGERANT comment activer la double authentification pour l'accès aux ressources sensibles de l'entreprise : VPN pour les collaborateurs, NAS pour l'INFOGERANT ...

- ⇒ L'évaluation de ses mesures de protections permet d'attribuer un **cyber score** au Client,
- ⇒ Une analyse de risque de ses **événements redoutés** permet d'identifier les **mesures à mettre en place en urgence**

Une démarche d'accompagnement en 3 temps



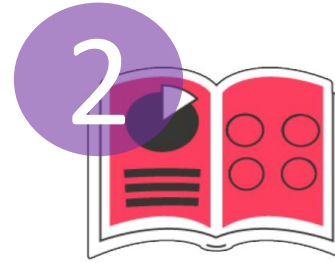
Réalisation d'un **CYBERCHECKUP/ CYBERDIAG**

SOCLE DES PRESTATIONS ESSENTIELLES

- **Audit de maturité Cyber 360°** selon 2 méthodologie (Cybercheckup/ Cyberdiag).
- **Revue de configuration sécurité** du poste de travail
- **Recherche** de « Data Leak »

PRESTATIONS OPTIONNELLES

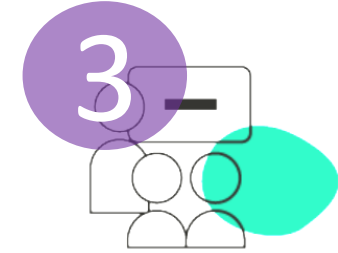
- **Test de faux phishing**
- **Autres tests techniques** selon spécificités client (test d'intrusion..)



Présentation et échanges autour de votre **CYBERBOOK**

BILAN DU CYBERCHECKUP

- **Une évaluation de votre socle de sécurité** avec les mesures de sécurité en place ou manquantes.   
- **Un Cyber score** en référence au guide d'hygiène de l'ANSSI.     
- **Des Fiches pratiques**
- **Votre analyse de risques** : revue des scénarios de menaces cyber possibles.
- **Votre Plan d'Assurance Sécurité** qui répertorie les mesures de sécurité permettant à l'entreprise d'assurer la sécurité des services qu'elle propose.



Mise en œuvre de solutions **CYBERACTIVES**

PARTAGE DE NOS SOLUTIONS

- **Cyber coaching** vous accompagne dans le suivi du pilotage de votre feuille de route.
- **Cyber Surveillance** afin de détecter une présence illégitime d'informations liées à un nom de domaine de l'entreprise sur internet.
- **Cyber Sensibilisation** auprès de vos collaborateurs (webinaires/ faux phishing/ passeport package)
- **Soutien à la commercialisation de l' Assurance Cyber .**

« Je n'ai pas grand-chose à vous remonter comme amélioration, j'en suis désolé, **nous avons été totalement satisfait de votre prestation.** »

« **Heureusement que vous êtes le Crédit Agricole, parce qu'avec tout ce que je vous ai raconté ...** »

« **Vous avez un prix intelligent !** »

" **Bravo, merci j'ai tout compris. Je sais exactement là où j'en suis et ce qu'il me reste à faire.** »

« **Merci, votre restitution est très pédagogique.** »

