

C4T
CYBER 4 TOMORROW

PRÉSENTATION
DE LA

MÉTHODOLOGIE
CYBERSUSTAINABILITY

Soutenu
par



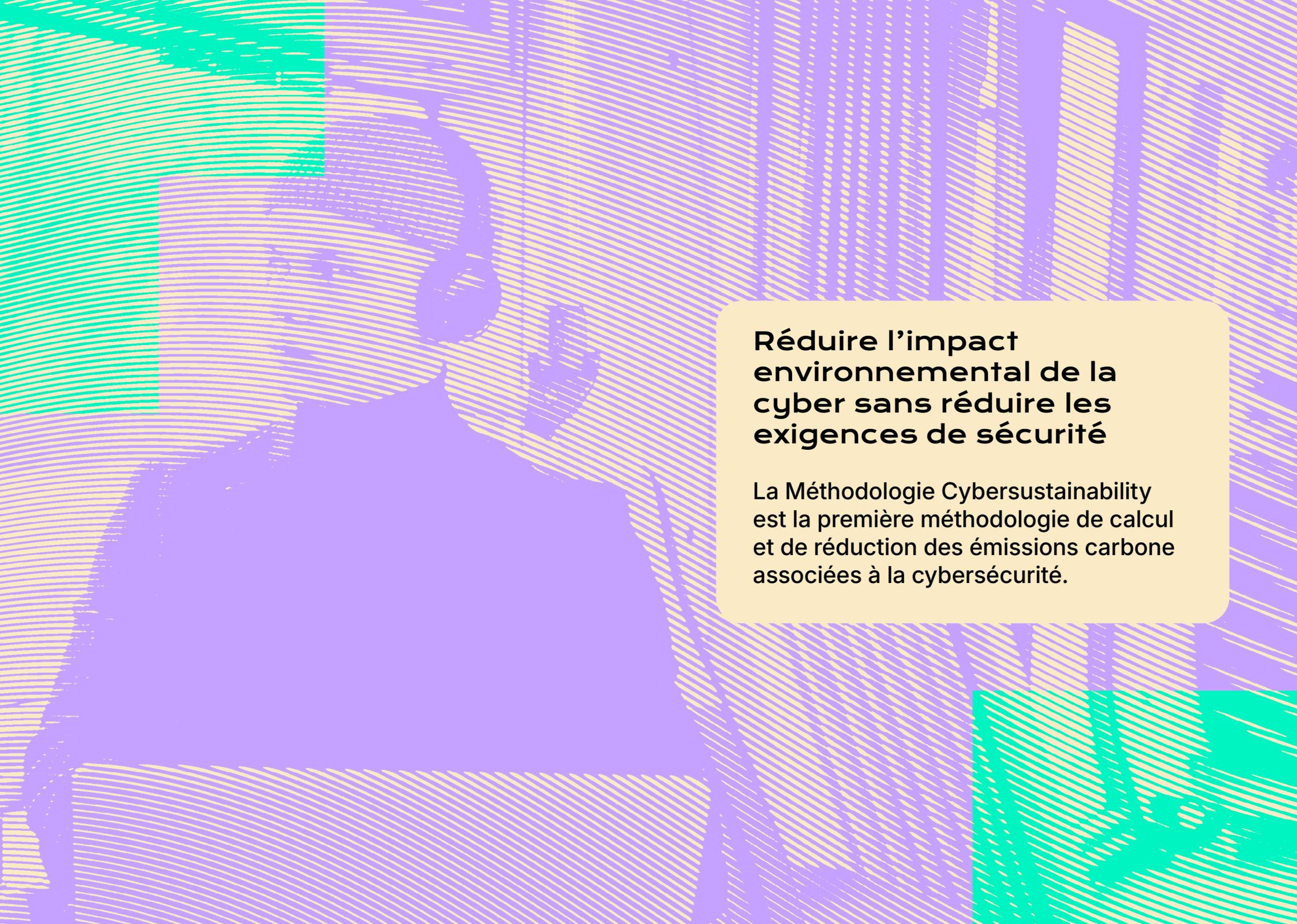
**RÉPUBLIQUE
FRANÇAISE**

*Liberté
Égalité
Fraternité*

ADEME



**AGENCE DE LA
TRANSITION
ÉCOLOGIQUE**

A woman with short dark hair, wearing glasses and a blue blazer, is looking at a laptop screen. The background is a modern office with large windows and a white wall. The image has a light blue tint.

Réduire l'impact environnemental de la cyber sans réduire les exigences de sécurité

La Méthodologie Cybersustainability
est la première méthodologie de calcul
et de réduction des émissions carbone
associées à la cybersécurité.

1. Réduire l'impact carbone de la cybersécurité : un enjeu majeur pour les RSSI

La cybersécurité représente une part significative et croissante du budget des entreprises, avec en moyenne 5,3% du budget IT dédié à la sécurité en 2023¹. Ce pourcentage est amené à croître rapidement, poussé par l'utilisation de nouveaux outils comme l'Intelligence Artificielle ou l'hébergement Cloud. Cette multiplication des usages entraîne de facto une augmentation des surfaces d'attaques et donc, des besoins en protection cyber. Si l'on se concentre sur l'impact environnemental du secteur du numérique dont fait partie la cybersécurité, cette croissance va nécessairement entraîner une augmentation de son empreinte carbone.

Malgré ce constat, les acteurs du secteur étaient jusqu'à dans l'incapacité d'évaluer l'impact carbone des mesures spécifiquement liées à la cybersécurité qu'ils déploient au sein de leur organisation, du fait de l'absence d'outils dédiés à ce sujet. Cela fait de la Méthodologie CyberSustainability créée par le Groupe de Travail du Campus Cyber une initiative innovante et pionnière sur le marché, en France comme à l'international.

¹ Chiffre moyen, selon un benchmark Wavestone sur +100 organisations tous secteurs confondus.



2. La Méthodologie CyberSustainability

La Méthodologie CyberSustainability vise à réduire les émissions carbone associées à la cybersécurité au sein d'une organisation. Elle repose sur une calculatrice simple d'utilisation, conçue pour intégrer toutes les données nécessaires à l'évaluation. Elle est adaptée à tout type de structure : grands groupes, PME, collectivités... Les résultats obtenus à la suite du calcul permettent d'établir un plan d'action, en accord avec les capacités et priorités de l'organisation, tout en garantissant le même niveau de protection.

• Construction de la Méthodologie

Les fondements de la Méthodologie CyberSustainability reposent sur l'analyse des principaux référentiels de cybersécurité internationaux, en particulier le NIST² Cybersecurity Framework. L'analyse de l'impact environnemental des 700 contrôles du NIST a permis d'identifier les cinquante recommandations les plus impactantes : la recommandation engendre-t-elle une augmentation du nombre de terminaux, de serveurs ou d'équipements réseau ?

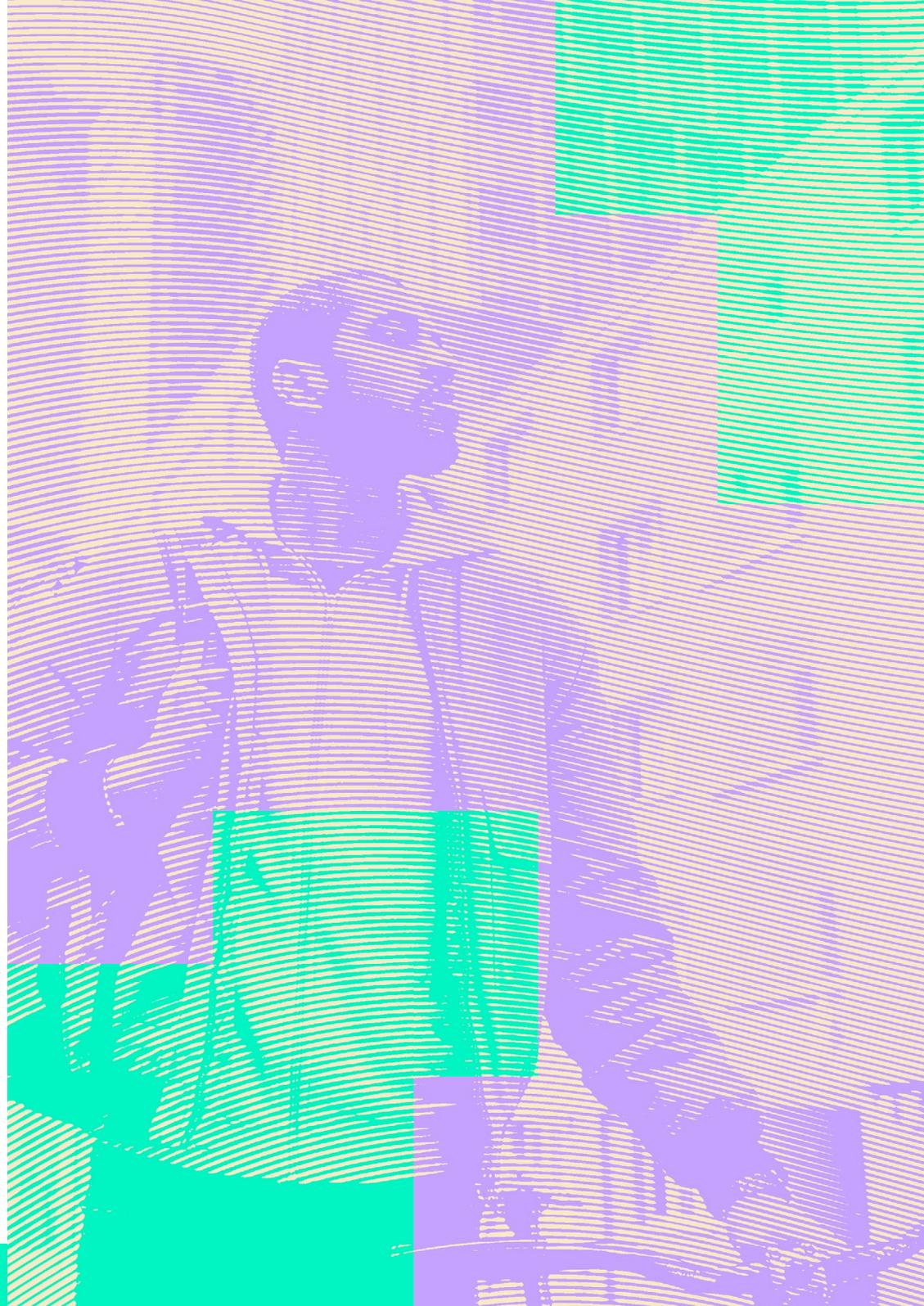
² National Institute of Standards and Technology.

Si oui, son impact est avéré et doit donc être mesuré pour être compris et contrôlé. Les émissions de gaz à effet de serre de ces cinquante recommandations ont ensuite été évaluées lors d'une expérimentation, sur des périmètres réels et de tailles variées. Cinq grandes entreprises et deux collectivités territoriales ont ainsi participé à un pilote, en déployant la première version de la méthodologie et en fournissant leurs retours d'expérience.

Ces structures ont été accompagnées par les cinq cabinets de conseil (Wavestone, Advens, Capgemini, Qorum Secur'Num, CS GROUP - France en qualité de société affiliée de Sopra Steria) membres du Groupe de Travail associé à l'expérimentation, orchestré par le Campus Cyber et avec le soutien de l'ADEME. Cette expérimentation a permis de classer les recommandations selon leur impact à partir des résultats calculés et d'identifier les pistes d'amélioration concrètes.

Parmi les mesures identifiées comme les plus émettrices, on retrouve celles liées à la résilience des systèmes d'information (serveurs dupliqués, serveurs de sauvegarde et PC de secours), suivies de celles associées aux périphériques utilisateurs spécifiques (comme ceux exigés pour les prestataires et les administrateurs, en plus de leurs terminaux du quotidien). À elles seules, ces deux catégories représentent près de 50% des émissions de la cybersécurité.

L'ambition de la Méthodologie est de proposer des pistes d'actions concrètes, directement activables, sans dégrader le niveau de sécurité des systèmes d'information. Par exemple : optimiser la collecte de logs, les redondances et les sauvegardes, le nombre de solutions d'IAM utilisées...



3. Un impact positif sur les organisations et sur l'écosystème cyber français

Plusieurs bénéfices directs ont été observés par les organisations ayant déployé la Méthodologie CyberSustainability :

• Bénéfices environnementaux :

Le potentiel de réduction des émissions CO2 liées à la cybersécurité est estimé à 5% et 10% selon les organisations. La connaissance et la prise en compte des enjeux environnementaux permettent de considérer et de limiter l'impact des futurs projets cyber.

• Bénéfices organisationnels :

Une meilleure compréhension du SI et une meilleure maîtrise du parc cyber, ce qui permet d'agir sur l'efficacité opérationnelle.

• Bénéfices sociaux et RH :

L'intégration de la cybersécurité dans les efforts de réduction de l'impact carbone de l'organisation renforce son attractivité auprès des salariés et des candidats, en donnant du sens à leur travail.

• Bénéfices financiers :

Il est possible d'optimiser et réduire les coûts liés à la maintenance et à la mise à jour du SI.

• Bénéfices réglementaires :

Le déploiement de la Méthodologie permet de préparer et d'anticiper des grandes réglementations environnementales, telles que la CSRD.

Au-delà des bénéfices directs pour l'organisation, la mise en place de la Méthodologie CyberSustainability s'inscrit dans un mouvement européen en faveur de l'éco-conception de la cybersécurité. Elle favorise notamment :

• **Une meilleure transparence tout au long de la chaîne de valeur**, en encourageant les fournisseurs de solutions et les hébergeurs Cloud à communiquer sur l'impact de leurs solutions et en favorisant l'intégration de critères environnementaux dans les cahiers des charges ou les réponses à appels à projet.

• **Une meilleure compétitivité des solutions françaises et européennes**, en faisant du respect des exigences environnementales un critère différenciant sur le marché international.



4. Le déploiement via l'initiative Cyber4Tomorrow

Le développement de la Méthodologie CyberSustainability s'opère dans le cadre de l'initiative Cyber4Tomorrow.

Le développement de la Méthodologie CyberSustainability s'opère dans le cadre de l'initiative Cyber4Tomorrow.

Portée par le Campus Cyber et Numeum, l'initiative Cyber4Tomorrow vise à promouvoir un grand mouvement «cybercitoyen» en embarquant une large communauté d'acteurs: professionnels de la cybersécurité (ESN, startups, clients finaux, etc.), institutionnels, acteurs de la recherche ou encore étudiants pour répondre aux défis sociaux et environnementaux liés à la sécurité numérique.

Cette plateforme unique s'adresse à tous les professionnels de la filière et propose un catalogue d'actions concrètes, conçues et testées afin qu'elles soient directement activables, en fonction du profil du volontaire et du public visé. Ces actions sont référencées autour de 3 piliers fondateurs :

- **Le pilier CyberSustainability**, qui vise à promouvoir des pratiques de cybersécurité respectueuses de l'environnement et durables, afin de minimiser l'empreinte écologique du secteur tout en maintenant un bon niveau de sécurité.

- **Le pilier CyberCitizenship**, qui vise à sensibiliser les individus et les organisations à l'importance des bonnes pratiques d'hygiène numérique, en fournissant des ressources éducatives et en encourageant l'adoption de comportements responsables en ligne.

- **Le pilier CyberSpecialists**, qui vise à rendre les métiers de la cybersécurité accessibles à toutes et tous, en encourageant la diversité et en offrant des opportunités de formation et de développement professionnel pour les aspirants et les professionnels de la sécurité.

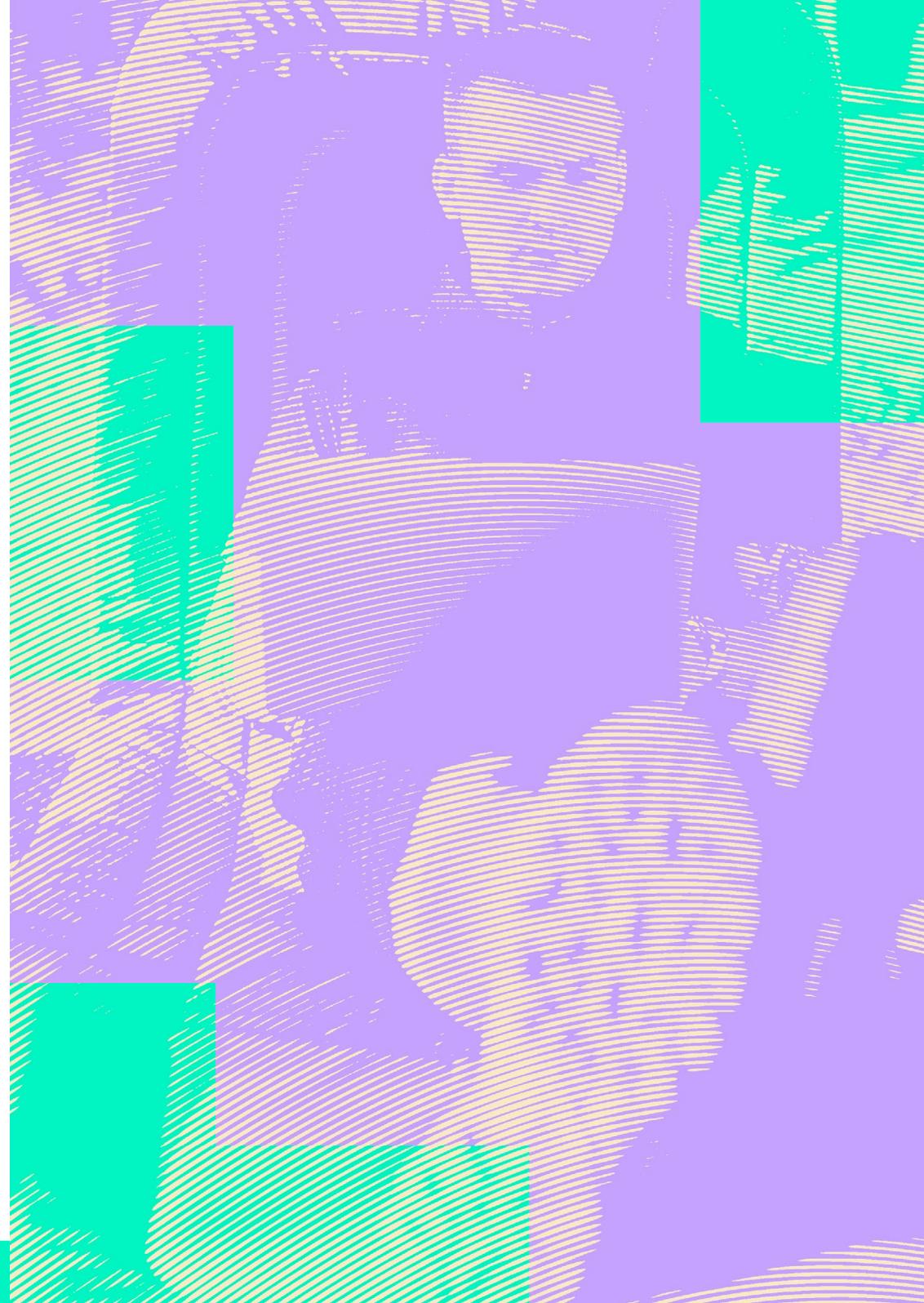
Chaque fiche action est accessible en ligne, avec les ressources nécessaires pour permettre aux professionnels de s'engager immédiatement en faveur de la sécurité numérique.

5. Contacts utiles

Pour plus d'informations sur la Méthodologie CyberSustainability et/ou sur Cyber4Tomorrow :

- Consultez la plateforme <https://cyber4tomorrow.fr>
- Ecrivez-nous à contact@cyber4tomorrow.fr

Basée sur la Méthodologie V1 créée et mise à disposition par Wavestone, la méthodologie a été produite par le Groupe de Travail du Campus Cyber conduit par Wavestone en coopération avec Advens, Capgemini, Qorum Secur'Num, CS GROUP - France en qualité de société affiliée de Sopra Steria, et avec le soutien de l'ADEME.





C4T

CYBER 4 TOMORROW

POUR PLUS D'INFORMATIONS



cyber4tomorrow.fr



Soutenu
par

