Co-funded by the European Union

GUIDE DES BONNES PRATIQUES POUR LES PME

CYBER AGENT 06.2026

Call: ERASMUS-EDU-2022-PI-ALL-INNO
Type of Action: ERASMUS-LS
Project No. 101111732

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Education and Culture Executive Agency (EACEA). Neither the European Union nor EACEA can be held responsible for them.

www.cyberagents.eu

Work Package 6: Dissemination & Exploitation

Deliverable 6.4: Good Practices Guide for SMEs

Leader of WP6 – Women4Cyber Foundation

CONTENT

LISTE DES TABLEAUX

INTRODUCTION

Le projet CyberAgent a été développé pendant trois ans dans huit pays européens : la Roumanie, la Belgique, la Norvège, l'Espagne, la Turquie, la Pologne, la Lituanie et la Finlande. Son objectif était de concevoir, mettre en œuvre et tester un programme de formation modulaire et accessible en cybersécurité destiné aux employés de PME, aux apprenants de l'enseignement et de la formation professionnels (EFP) ainsi qu'aux étudiants de l'enseignement supérieur. Le principal résultat du projet est la création de la fonction d'Agent du changement en cybersécurité : un employé formé, sans nécessairement posséder une expertise technique, qui agit comme personne de référence en matière de sensibilisation à la cybersécurité au sein de son organisation.

Ce guide transforme l'expérience acquise lors de la mise en œuvre du projet en recommandations concrètes à destination des PME. Il explique ce qu'est le rôle d'Agent du changement en cybersécurité, comment identifier et désigner la personne la plus adaptée, comment accompagner sa formation et comment intégrer les principes d'égalité entre les genres et d'inclusion dès le début du processus. Une liste de contrôle, présentée à la fin du document, permet aux PME de vérifier que toutes les conditions nécessaires à une mise en œuvre réussie sont réunies.

.

1. POURQUOI LA CYBERSECURITE EST ESSENTIELLE POUR CHAQUE PME

Selon le rapport ENISA Threat Landscape 2025, les cybercriminels industrialisent leurs attaques, faisant des PME des cibles privilégiées, quel que soit leur secteur d'activité ou leur taille. Les menaces les plus courantes auxquelles les organisations sont aujourd'hui confrontées sont les rançongiciels (ransomware), le phishing (hameçonnage) et les violations de données. Les rançongiciels représentent à eux seuls la majorité des cyberattaques visant les organisations de l'Union européenne, soit plus de 80 % des incidents. L'industrialisation de ces attaques, notamment grâce au modèle « Ransomware-as-a-Service », a réduit les barrières à l'entrée pour les cybercriminels, faisant des plus petites organisations des cibles viables.

Pour les PME en particulier, les conséquences d'une cyberattaque ne se limitent pas à des perturbations temporaires. Selon l'ENISA, les cyberattaques ont encore des effets négatifs sur l'activité de 90 % des PME une semaine après leur survenue. Pourtant, malgré cette exposition, les PME disposent rarement de personnel dédié à l'informatique ou à la cybersécurité, et leurs employés bénéficient rarement d'une formation structurée dans ce domaine. Les PME emploient environ 100 millions de personnes en Europe et représentent plus de la moitié du PIB européen. L'écart en matière de cybersécurité dans le secteur des PME constitue donc un risque économique et sociétal.

La plupart des cyberattaques réussissent en raison de facteurs humains, tels qu'un clic sur un lien de phishing, l'utilisation de mots de passe faibles ou l'ouverture d'e-mails non vérifiés. Cela signifie que la première ligne de défense n'est pas un outil technique, mais un collaborateur informé et sensibilisé, capable d'identifier les risques et de savoir comment réagir lorsqu'un incident survient. C'est précisément le rôle de l'Agent du changement en cybersécurité.

2. L'AGENT DU CHANGEMENT EN CYBERSÉCURITÉ

Le concept d'Agent du changement en cybersécurité est au cœur du projet CyberAgent. Cette section explique en quoi consiste ce rôle, pourquoi il a été créé et comment il peut être mis en œuvre concrètement au sein des petites et moyennes entreprises (PME).

2.1. QU'EST-CE QUE C'EST ET POURQUOI CE RÔLE EST-IL NECESSAIRE ?

Les PME constituent l'épine dorsale de l'économie européenne, mais elles figurent également parmi les organisations les plus exposées aux menaces de cybersécurité. Contrairement aux grandes entreprises, la plupart des PME ne disposent pas de services informatiques ou de cybersécurité dédiés, et leurs collaborateurs bénéficient rarement d'une formation structurée dans ce domaine. Il en résulte un écart persistant entre les cyber risques auxquels les PME sont confrontées et leur capacité à y faire face.

Le projet CyberAgent et la fonction d'Agent du changement en cybersécurité ont été conçus pour répondre à ce défi en développant de nouvelles compétences au sein des équipes existantes. L'Agent du changement en cybersécurité est un collaborateur formé, non spécialisé sur le plan technique, qui agit comme personne de référence en matière de sensibilisation à la cybersécurité. Il encourage l'adoption de comportements plus sûrs, aide à reconnaître les risques les plus courants et favorise la mise en œuvre de meilleures pratiques de cybersécurité au sein de l'organisation. Il oriente également ses collègues vers les ressources ou les personnes compétentes en cas d'incident.

La nécessité de ce rôle est confirmée par les résultats obtenus lors de la phase pilote du projet CyberAgent. Dans les huit pays partenaires, la formation a rassemblé 594 participants inscrits, comprenant des employés de PME, des étudiants de l'enseignement supérieur (HEI) et des apprenants de l'enseignement et de la formation professionnels (EFP/VET). Les employés de PME sont généralement considérés comme le public le plus difficile à mobiliser et à fidéliser dans le cadre d'actions de formation, principalement en raison de contraintes de temps et de leurs responsabilités professionnelles. Malgré cela, le taux élevé d'achèvement de la formation parmi les employés de PME démontre la pertinence réelle de la sensibilisation à la cybersécurité dans leur activité quotidienne.

2.2. RESPONSABILITÉS PRINCIPALES

L'Agent du changement en cybersécurité n'a pas pour mission de résoudre seul les problèmes de cybersécurité. Son rôle repose avant tout sur la sensibilisation, la communication et la coordination. Il est la personne qui veille à maintenir la cybersécurité au cœur des préoccupations de l'organisation et qui aide ses collègues à l'intégrer dans leurs activités quotidiennes. Cette fonction ne requiert pas d'expertise technique. Elle nécessite avant tout une personne de confiance, bien intégrée dans l'organisation et motivée à faire de la cybersécurité une composante naturelle du fonctionnement de l'équipe.

Concrètement, ce rôle se traduit par un ensemble d'activités régulières, simples à mettre en œuvre et peu chronophages, mais ayant un impact significatif sur la culture de cybersécurité de l'organisation :

- **Sensibiliser régulièrement les collaborateurs**. L'Agent du changement partage régulièrement avec ses collègues des messages de sensibilisation concernant les menaces les plus courantes, telles que les e-mails de phishing, les mots de passe faibles, les mauvaises pratiques de gestion des données ou les liens suspects. L'objectif est de maintenir la cybersécurité visible sans qu'elle soit perçue comme une contrainte. Il peut s'agir, par exemple, d'un message mensuel publié sur le canal de discussion de l'équipe, d'un bref rappel avant une période particulièrement chargée ou d'une information concernant une nouvelle escroquerie circulant dans le secteur d'activité. La régularité est plus importante que le format choisi.

- **Inscrire la cybersécurité à l'ordre du jour des réunions.** L'Agent du changement aborde régulièrement des sujets liés à la cybersécurité lors des réunions d'équipe, sous la forme de discussions courtes et concrètes. Il ne s'agit pas d'organiser de longues présentations ou des sessions de formation formelles. Une discussion de cinq minutes sur une tentative récente de phishing ou un rappel concernant la mise à jour des mots de passe suffit à maintenir un niveau élevé de vigilance et à rappeler que la cybersécurité est une responsabilité collective, et non exclusivement celle des équipes techniques.

- **Encourager le signalement des incidents**. L'une des contributions les plus importantes de l'Agent du changement consiste à instaurer une culture dans laquelle les collaborateurs se sentent à l'aise pour signaler toute situation suspecte : un e-mail inhabituel, un comportement anormal d'un système ou encore un clic accidentel sur un lien douteux. De nombreux incidents de cybersécurité prennent de l'ampleur parce que les collaborateurs hésitent à signaler les premiers signes d'alerte, par crainte d'être jugés ou tenus responsables. L'Agent du changement contribue à normaliser ces signalements en étant accessible et en expliquant clairement la procédure à suivre.

- **Accompagner l'intégration des nouveaux collaborateurs.** Les nouveaux employés figurent parmi les personnes les plus vulnérables en matière de cybersécurité, car ils ne connaissent pas encore les procédures internes, sont davantage susceptibles de faire confiance à des demandes inattendues et n'ont souvent pas encore été sensibilisés aux bonnes pratiques de sécurité. L'Agent du changement joue un rôle essentiel en présentant les principes fondamentaux de la cybersécurité lors du processus d'intégration, afin que les bonnes pratiques soient adoptées dès le premier jour, plutôt que mises en place ultérieurement.

- **Agir comme point de contact interne.** L'Agent du changement en cybersécurité est la personne vers laquelle les collaborateurs se tournent lorsqu'ils ont une question relative à la cybersécurité ou lorsqu'ils ne savent pas comment réagir dans une situation donnée. Il sait à qui s'adresser, vers qui escalader un incident et comment orienter ses collègues vers le support approprié. Dans les PME qui ne disposent pas d'un service informatique dédié, ce rôle comble un vide qui laisserait autrement les employés sans interlocuteur clairement identifié.

- **Promouvoir la formation et l'apprentissage continu.** L'Agent du changement encourage ses collègues à utiliser les ressources de formation disponibles, notamment les modules CyberAgent, et se tient informé des évolutions du paysage de la cybersécurité en lien avec le secteur d'activité et les activités de l'organisation.

- **Recueillir les retours d'expérience et les faire remonter.** L'Agent du changement recueille les retours concernant les enjeux de cybersécurité au sein de l'organisation : les points que les collaborateurs jugent peu clairs, les pratiques qui ne sont pas correctement appliquées ou encore les risques qu'ils considèrent comme les plus préoccupants. Il transmet ensuite ces informations à la direction. Cette boucle de retour d'information permet à l'organisation d'améliorer progressivement sa culture de la cybersécurité.

Table 1. Distinction entre les missions des spécialistes informatiques et celles de l'Agent du changement

SPÉCIALISTE INFORMATIQUE (Rôle technique)	AGENT DU CHANGEMENT EN CYBERSÉCURITÉ (Rôle de coordination et de sensibilisation)
Configure les pare-feu et les systèmes de sécurité.	Diffuse des messages de sensibilisation et des alertes de sécurité adaptés aux collaborateurs.
Gère les mises à jour logicielles, les correctifs et les configurations techniques.	Veille à inscrire régulièrement la cybersécurité à l'ordre du jour des réunions d'équipe.
Réagit aux incidents de cybersécurité et aux compromissions techniques.	Encourage les collaborateurs à signaler de manière proactive et transparente toute activité suspecte.
Surveille le trafic réseau, les journaux de sécurité et les paramètres techniques de conformité.	Accompagne les nouveaux collaborateurs lors de leur intégration en leur présentant les règles essentielles d'hygiène numérique.
Met en œuvre les contrôles techniques de sécurité et gère les droits d'accès à l'infrastructure.	Recueille les retours des collaborateurs et fait remonter les problématiques récurrentes à la direction ou au service informatique.

3. SELECTION ET DESIGNATION D'UN AGENT DU CHANGEMENT EN CYBERSECURITE

Identifier la personne la plus adaptée pour assumer le rôle d'Agent du changement en cybersécurité et lui offrir les conditions nécessaires à sa réussite constitue une étape essentielle de la mise en œuvre de cette fonction au sein d'une organisation. Le projet pilote CyberAgent a montré que ce rôle est le plus efficace lorsqu'il est confié à une personne reconnue comme digne de confiance, connaissant bien les procédures internes de l'entreprise et bénéficiant du soutien de la direction. Cette section présente des recommandations pratiques pour définir clairement le rôle, garantir sa pérennité et identifier le candidat le plus approprié.

3.1. COMMENT IDENTIFIER LE BON CANDIDAT

Les résultats du projet pilote CyberAgent montrent que les Agents du changement en cybersécurité les plus efficaces ne sont pas nécessairement ceux disposant d'une expérience ou d'une formation technique. Dans les huit pays partenaires, les participants issus des PME qui se sont le plus investis dans la formation et ont démontré le plus fort potentiel étaient ceux qui combinaient une bonne connaissance du fonctionnement de leur organisation, d'excellentes compétences en communication et une réelle motivation à faire évoluer les pratiques de leur entreprise. Sur la base des enseignements du projet pilote, les caractéristiques suivantes favorisent la réussite dans ce rôle :

- Bonne connaissance des processus internes de l'organisation et des pratiques de gestion des données ;
- Bonnes compétences en communication et en relations interpersonnelles ;
- Soutien de la direction.

Il est important de souligner que cette fonction ne nécessite pas de compétences techniques ni de formation en informatique. Les collaborateurs occupant des fonctions administratives, en ressources humaines, en opérations ou en management peuvent donc exercer efficacement le rôle d'Agent du changement, à condition de bénéficier d'une formation et d'un accompagnement appropriés. La suppression de cette exigence technique constitue un choix délibéré du projet. Elle élargit considérablement le vivier de candidats potentiels et favorise une meilleure diversité, notamment en matière d'égalité entre les femmes et les hommes, comme l'ont démontré les résultats du projet pilote.

Une fois le candidat identifié, il est essentiel de rendre son rôle visible et légitime au sein de l'organisation. La nomination doit être communiquée à l'ensemble des collaborateurs et le périmètre de la fonction clairement défini : les responsabilités de l'Agent du changement, son rattachement hiérarchique ainsi que les missions qui ne relèvent pas de son rôle.

3.2. MISE EN OEUVRE DU RÔLE

L'étape suivante consiste à intégrer concrètement cette fonction au sein de l'organisation. Les recommandations ci-dessous sont directement issues des enseignements tirés du projet pilote CyberAgent dans les différents pays partenaires et ont été conçues pour être adaptées aux PME, quelle que soit leur taille.

3.2.1. SELECTIONNER ET FORMER L'AGENT DU CHANGEMENT EN CYBERSECURITE

Identifiez la personne la plus appropriée au sein de votre organisation et donnez-lui accès au programme de formation CyberAgent. Le programme comprend neuf modules couvrant la gestion des programmes de sécurité (M1), l'administration des systèmes (M2), les outils d'analyse (M3), les opérations de sécurité (M4), la gouvernance et les politiques de cybersécurité (M5), la planification de la cybersécurité (M6), la gestion des risques (M7), la continuité des activités (M8) et le développement des carrières en cybersécurité (M9). Ces neuf modules sont officiellement présentés dans deux livrables du projet : D3.1, consacré au programme d'enseignement supérieur (HEI), et D3.2, consacré au programme d'enseignement et de formation professionnels (EFP/VET). Les modules mentionnés tout au long de ce Guide correspondent donc directement au contenu décrit dans les livrables D3.1 et D3.2 et sont accessibles via la plateforme CyberAgent, quel que soit le profil institutionnel de l'apprenant. En outre, le programme est aligné sur les niveaux 4 à 6 du Cadre européen des certifications (CEC/EQF) pour les employés de PME, offrant des compétences et des connaissances fondamentales en cybersécurité avec une application pratique dans les domaines techniques, analytiques, de la gestion des risques et des compétences organisationnelles.

La formation est proposée en ligne et en autoformation, ce qui permet au collaborateur sélectionné de la suivre de manière flexible, en parallèle de ses responsabilités professionnelles. À l'issue d'un module et après avoir obtenu un score d'au moins 75 % au test d'évaluation des connaissances, l'Agent du changement reçoit un certificat de réussite pour ce module, constituant une preuve officielle des compétences acquises et pouvant être utilisé pour documenter sa formation au sein de l'organisation.

3.2.2. DEFINIR LES RESPONSABILITES ET INTEGRER LE ROLE AUX STRUCTURES EXISTANTES

Une fois la formation entamée ou terminée, l'organisation doit définir officiellement les responsabilités de l'Agent du changement en cybersécurité et intégrer ce rôle aux structures existantes. Cela signifie qu'il convient de déterminer les missions de l'Agent du changement, le temps qu'il consacrera à ce rôle, les personnes avec lesquelles il assurera la coordination, puis de communiquer ces éléments à l'ensemble de l'équipe.

Le projet pilote a montré que le rôle d'Agent du changement en cybersécurité est plus durable lorsqu'il est rattaché à un élément déjà existant dans l'organisation plutôt que lorsqu'il fonctionne de manière isolée. Il peut, par exemple, être intégré à un point récurrent de l'ordre du jour des réunions d'équipe ou être associé à une structure existante en matière de santé et sécurité ou de conformité. L'objectif est de faire de la sensibilisation à la cybersécurité une composante normale du travail quotidien et une responsabilité partagée par l'ensemble de l'organisation, plutôt qu'une activité distincte..

3.2.3. DEVELOPPER LA SENSIBILISATION INTERNE AUTOUR DU ROLE

L'Agent du changement ne peut pas exercer efficacement ses fonctions si ses collègues ne savent pas qui il est ni quel est son rôle. Afin de donner au collaborateur sélectionné la légitimité organisationnelle dont il a besoin pour exercer ses fonctions, il est nécessaire de diffuser une communication interne claire présentant son rôle et ses responsabilités, et d'organiser des réunions régulières permettant aux collaborateurs de poser leurs questions.

Au-delà de cette annonce initiale, l'Agent du changement doit être encouragé à maintenir la cybersécurité visible au sein de l'organisation au travers de réunions régulières. Il ne s'agit pas d'organiser de longues sessions de formation ou des présentations formelles. Dans le contexte des PME, cela peut prendre la forme de courtes activités directement liées à des situations que les collaborateurs rencontrent dans leur travail quotidien.

3.2.4. ASSURER UN SUIVI REGULIER ET LA PERENNITE DU ROLE

Afin que le rôle d'Agent du changement en cybersécurité produise un impact durable, l'organisation doit créer les conditions nécessaires à sa continuité et à son évolution. Cela implique de mettre en place un processus de révision au moins une fois par an, afin d'évaluer ce qui fonctionne, les lacunes qui subsistent et si l'Agent du changement a besoin d'une formation ou d'un soutien supplémentaire.

Les résultats du projet pilote montrent qu'un engagement durable nécessite davantage qu'une formation initiale. Les participants issus des PME ont régulièrement eu besoin d'échéances flexibles, de rappels et d'un soutien ponctuel pour maintenir leur motivation. La mise en place d'un simple bilan annuel et le fait de garantir à l'Agent du changement un accès continu aux ressources constituent les conditions minimales pour assurer l'efficacité du rôle sur le long terme.

4. ÉQUITÉ ET INCLUSION

La cybersécurité demeure l'un des secteurs les plus fortement dominés par les hommes dans l'économie européenne. Les femmes représentent environ 20 % des professionnels de la cybersécurité au sein de l'Union européenne, et leur participation aux formations en cybersécurité reflète le même déséquilibre. Compte tenu de la pénurie actuelle de compétences et de talents, un secteur qui ne mobilise qu'une fraction des talents disponibles aura des difficultés à répondre à l'ampleur des besoins imposés par le paysage actuel des menaces.

Le projet CyberAgent a été conçu en intégrant l'inclusion des genres comme un objectif explicite, et non comme une réflexion secondaire. Dans un domaine où les femmes ne représentent généralement qu'une faible proportion des participants aux formations, le nombre élevé de participantes au projet pilote constitue un résultat significatif, obtenu grâce à des stratégies de sensibilisation ciblées et à une approche inclusive.

4.1. POURQUOI C'EST IMPORTANT POUR LES PME

Pour les PME en particulier, la dimension de genre en matière de cybersécurité constitue à la fois une question liée à la main-d'œuvre et à la culture organisationnelle. La plupart des PME ne disposent pas de personnel dédié à la cybersécurité. Leur cyberrésilience dépend de la sensibilisation et du comportement de l'ensemble des collaborateurs, en particulier ceux occupant des fonctions administratives, en ressources humaines, en finance et en opérations. Par conséquent, exclure les femmes des formations de sensibilisation à la cybersécurité crée une faille de sécurité.

Parallèlement, le rôle d'Agent du changement en cybersécurité offre une opportunité concrète de remédier au déséquilibre entre les femmes et les hommes dans le domaine de la cybersécurité au sein même des PME. Parce que ce rôle est défini par des compétences en communication, une bonne connaissance de l'organisation et une approche orientée vers la gouvernance, plutôt que par une expertise technique, il convient à un large éventail de profils professionnels et offre aux femmes occupant des fonctions non techniques une voie reconnue vers des responsabilités en cybersécurité, sans nécessiter de reconversion professionnelle ni de qualification technique.

4.2. MESURES PRATIQUES POUR TOUCHER LES FEMMES ET LES GROUPES-REPRESENTES

Les mesures pratiques suivantes sont issues de l'expérience du projet pilote CyberAgent et sont conçues pour être mises en œuvre par des PME de toute taille.

Le projet pilote belge a démontré que le fait de s'appuyer sur des réseaux auxquels les femmes font déjà confiance, tels que les associations professionnelles et les réseaux de femmes entrepreneures, permet d'accroître la participation des femmes. En pratique, cela signifie que lorsqu'une PME identifie des candidats au rôle d'Agent du changement en cybersécurité, elle devrait mobiliser activement les réseaux professionnels de femmes pertinents pour son secteur ou sa région, plutôt que de s'appuyer uniquement sur des annonces publiques.

Présentez le rôle en mettant l'accent sur son impact organisationnel plutôt que sur l'expertise technique. Les femmes occupant des fonctions non techniques sont davantage susceptibles de s'engager dans une formation en cybersécurité et d'assumer le rôle d'Agent du changement lorsque celui-ci est présenté en termes de valeur ajoutée pour l'organisation plutôt qu'en termes de compétences techniques. Le rôle peut être présenté comme une fonction qui protège l'entreprise, soutient les collègues et contribue à la gouvernance. Le langage utilisé dans les communications internes, les descriptions de poste et les supports de recrutement est important.

5. BONNES PRATIQUES

La désignation d'un Agent du changement en cybersécurité constitue une première étape importante, mais ce rôle ne peut produire un impact durable que s'il s'inscrit dans une culture organisationnelle qui le soutient activement. Les bonnes pratiques suivantes ont été élaborées pour aider les PME à créer les conditions propices à la réussite de l'Agent du changement et à faire de la sensibilisation à la cybersécurité une composante normale du fonctionnement de l'organisation.

- **Encourager une communication ouverte.** Les collaborateurs doivent se sentir à l'aise pour signaler leurs erreurs, des situations suspectes ou des préoccupations en matière de sécurité, sans crainte d'être blâmés ou embarrassés. Dans de nombreuses organisations, les incidents de cybersécurité s'aggravent précisément parce que les collaborateurs hésitent à signaler une situation dont ils ne sont pas certains ou dont ils se sentent responsables.

- **Privilégier la simplicité et l'intégration dans les routines quotidiennes.** La sensibilisation à la cybersécurité ne doit pas nécessairement prendre la forme de formations formelles ou d'ateliers de longue durée. De brefs rappels pratiques intégrés aux routines existantes sont souvent plus efficaces que des formations intensives organisées ponctuellement. L'objectif est de faire de la cybersécurité une habitude quotidienne plutôt qu'un événement occasionnel.
- **Documenter chaque étape.** L'une des mesures les plus utiles qu'une PME puisse adopter consiste à consigner par écrit ses principales pratiques de cybersécurité : la gestion des mots de passe, le stockage et le partage des données sensibles, la procédure à suivre en cas de réception d'un e-mail suspect et les personnes à contacter en cas d'incident. Il n'est pas nécessaire qu'il s'agisse de documents de politique formels. Une fiche de référence d'une page, accessible à tous les collaborateurs, est suffisante.

- **Donner l'exemple au plus haut niveau.** Les comportements attendus des collaborateurs doivent être clairement adoptés par les responsables et la direction. Si la direction ne respecte pas les règles de sécurité de base, cela envoie le message que ces pratiques sont facultatives. La crédibilité de l'Agent du changement au sein de l'organisation dépend en partie de la culture qui soutient les actions qu'il cherche à promouvoir.

- **Faire de la sensibilisation un processus continu.** Les menaces de cybersécurité évoluent constamment et une formation unique devient rapidement obsolète. La sensibilisation doit être considérée comme un processus permanent plutôt que comme une activité ponctuelle. Cela implique des rappels réguliers, des mises à jour périodiques et un Agent du changement en cybersécurité qui reste informé et partage les informations pertinentes avec l'ensemble de l'organisation.

5.1. RETOURS QUALITATIFS ISSUS DES PROJETS PILOTES NATIONAUX

Les retours qualitatifs montrent que les participants ont généralement porté une appréciation positive sur la formation, nombre d'entre eux indiquant qu'aucune amélioration majeure n'était nécessaire. Les thèmes les plus fréquemment mentionnés dans les réponses libres (D5.3 - *CyberAgent Upskilling Training Program Evaluation*) étaient : l'ergonomie de la plateforme, la navigation ou le déroulement des évaluations ; les problèmes d'accès technique ou de fiabilité ; les appréciations positives concernant l'accessibilité, la flexibilité et l'étendue des connaissances acquises ; les demandes portant sur davantage de cas pratiques, de laboratoires pratiques ou d'exemples concrets issus des PME ; ainsi que la densité du contenu, sa structure ou la différenciation des parcours d'apprentissage. Il convient de noter que le troisième thème le plus fréquemment cité (les appréciations positives concernant l'accessibilité, la flexibilité et l'étendue des connaissances) reflète la satisfaction des participants qui ont indiqué qu'aucune amélioration n'était nécessaire et qui ont spontanément mis en avant les points forts du programme. Il s'agit d'un résultat significatif : dans un champ de réponse libre destiné à recueillir des critiques, près d'un quart des réponses qualitatives exprimaient une satisfaction quant à l'accessibilité et à l'étendue de la formation.

5.2. POINTS D'ACTION POUR LA MISE EN ŒUVRE ET LA GESTION DE LA FORMATION AU SEIN DES PME

Le projet pilote à grande échelle de la plateforme CyberAgent dans huit pays européens a fourni des informations essentielles sur la manière dont les petites et moyennes entreprises adoptent et maintiennent la montée en compétences en cybersécurité. Sur la base des résultats issus de la méthodologie mixte et des obstacles rencontrés par les apprenants, tels que documentés dans le rapport final d'évaluation de la formation (D5.3), il est recommandé aux responsables d'entreprise de mettre en œuvre les actions de gestion, techniques et stratégiques suivantes afin d'optimiser l'impact organisationnel de la formation.

Recommandations en matière de gestion de la qualité

Les supports de formation CyberAgent présentent un volume conséquent de connaissances opérationnelles et stratégiques. Les responsables devraient éviter d'assigner l'ensemble du programme en une seule fois ; au contraire, l'établissement d'un calendrier modulaire permet de limiter la surcharge cognitive et de faciliter l'intégration progressive des compétences dans les activités quotidiennes de l'entreprise.

Recommandations concernant l'intégration technique

Les premières données issues du projet pilote ont montré que certaines difficultés techniques lors de l'inscription, telles que le retard ou le filtrage des e-mails de confirmation d'inscription à la plateforme, peuvent freiner l'adoption initiale. Avant de déployer les inscriptions des utilisateurs, les responsables devraient coordonner avec les administrateurs réseau afin de s'assurer que les domaines externes de la plateforme d'apprentissage en ligne sont autorisés et inviter les collaborateurs à vérifier également leurs dossiers de courrier indésirable.

Recommandations pour le déploiement stratégique

Les données issues des projets pilotes nationaux ont montré que les modules stratégiques de niveau avancé – en particulier le M6 (Planification de la cybersécurité) et le M8 (Continuité des activités) – nécessitent une solide expérience préalable pour être pleinement exploités. Afin de maximiser la valeur ajoutée immédiate pour l'entreprise, ces modules devraient être prioritairement destinés aux collaborateurs exerçant des responsabilités de management, d'exploitation ou de gouvernance de l'entreprise.

5.2.1. LE POINT DE VUE DE L'AGENT DU CHANGEMENT

La phase pilote, qui a regroupé 272 réponses complètes à l'enquête dans huit pays européens, a mis en évidence trois effets transversaux sur les groupes cibles.

Grande flexibilité de mise en œuvre et conciliation entre travail et apprentissage

Une proportion significative de 86,0 % des répondants s'est déclarée d'accord ou tout à fait d'accord avec le fait que le format asynchrone et en autoformation était suffisamment flexible pour s'intégrer facilement à leurs contraintes professionnelles et académiques, permettant ainsi aux employés des PME de développer leurs compétences tout en poursuivant leurs activités quotidiennes.

Pertinence méthodologique pour les profils non techniques

Les résultats du projet pilote confirment le principe pédagogique fondamental du programme CyberAgent, démontrant qu'une cyberrésilience organisationnelle efficace ne nécessite pas de compétences avancées en informatique ou en programmation. Selon les données de l'évaluation d'impact présentées dans le livrable D5.3, 77,2 % des participants ont indiqué que la formation leur avait permis de comprendre clairement comment leur propre rôle professionnel influence et contribue à la protection des pratiques quotidiennes de sécurité au sein de leur organisation.

Progression mesurable des connaissances chez les débutants

Les données analytiques de la plateforme montrent que 89,3 % des participants ont enregistré une amélioration vérifiée de leurs connaissances en cybersécurité. Plus important encore, cette progression a été particulièrement marquée chez les débutants : 90,9 % des apprenants qui avaient évalué leur niveau initial comme « Très faible » avant le programme ont déclaré avoir considérablement renforcé leurs connaissances et leur confiance dans leur capacité à identifier les cyberrisques en entreprise.

5.2.2. << A FAIRE ET A EVITER>>

Sur la base des retours des pays pilotes concernant la différenciation des parcours d'apprentissage, nous présentons les recommandations suivantes à destination des entreprises :

Table 2 « À faire et à éviter »

À NE PAS FAIRE (Écueils pour les PME)	**RECOMMANDÉ (Bonne pratique)**
S'attendre à ce qu'un employé suive les 8 modules dans un délai irréaliste et très court (par exemple, une semaine ou un mois). Les études pilotes (D5.3) ont révélé que le manque de temps dû aux responsabilités professionnelles quotidiennes constituait le principal obstacle pour les employés de PME, entraînant un taux de réussite plus faible aux tests.	Créer un calendrier d'apprentissage flexible et individuel, adapté aux besoins et aux disponibilités de l'employé, en appliquant les principes du micro-apprentissage. Permettre aux apprenants de se concentrer sur les modules qui renforcent directement leur domaine d'impact professionnel.
S'attendre à ce que l'Agent du changement en cybersécurité formé remplace les spécialistes en ingénierie informatique ou résolve de manière autonome des incidents cyber complexes. Transférer des responsabilités techniques essentielles d'infrastructure à du personnel non technique crée une forte ambiguïté de rôle.	Encourager l'Agent du changement à agir comme coordinateur interne de la sécurité et catalyseur de sensibilisation. Il est plus efficace lorsqu'il contribue à renforcer la culture de sécurité, rappelle les formations internes et anime de brèves mises à jour lors des réunions d'équipe.
Laisser le processus d'apprentissage en ligne fonctionner entièrement en pilote automatique, sans visibilité au niveau de l'entreprise. Un simple lien d'inscription ne garantit pas une valeur organisationnelle à long terme.	Utiliser un cadre de suivi structuré (tel que le Tableau 3) pour suivre les étapes clés et désigner un mentor interne. Les indications issues de l'évaluation pilote (D5.3) confirment que la présence d'un responsable ou mentor désigné est explicitement corrélée à la finalisation vérifiée des tests.
Laisser l'étude autonome se dérouler dans un isolement total, au risque que les blocages d'apprentissage individuels ou les difficultés techniques cachées ne soient pas détectés. Sans interaction, les débutants complets se retrouvent souvent bloqués et abandonnent silencieusement le programme.	Associer l'étude autonome à des points de contact opérationnels proactifs, tels que de courts points de suivi ou des rappels numériques. L'alignement actif avec la direction permet de lever directement les obstacles à l'apprentissage, en renforçant la motivation des employés et les taux d'achèvement des cours.

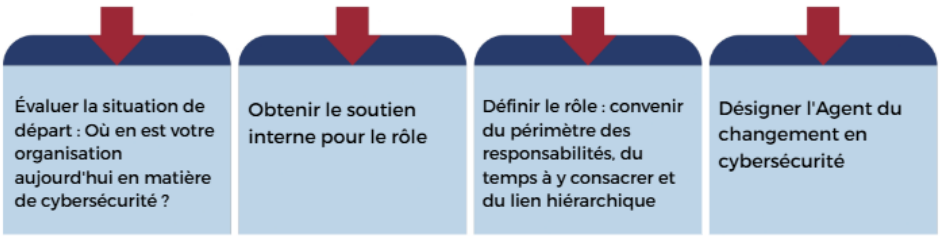
6. FEUILLE DE ROUTE POUR LA MISE EN ŒUVRE DE L'AGENT DU CHANGEMENT EN CYBERSECURITE

La mise en œuvre du rôle d'Agent du changement en cybersécurité commence bien avant sa désignation. Prendre le temps d'évaluer la situation actuelle de l'organisation, de susciter l'adhésion en interne et de définir clairement le rôle dès le départ augmente considérablement les chances de réussite à long terme. Les étapes suivantes sont conçues pour guider les PME de manière pratique tout au long de cette phase de préparation.

1. La première étape consiste à évaluer la situation actuelle de l'organisation. Cela implique d'examiner honnêtement les pratiques de cybersécurité déjà en place, ou leur absence. Les collaborateurs sont-ils sensibilisés aux menaces de base telles que le phishing ? Existe-t-il une procédure pour signaler les incidents suspects ? Les données sensibles sont-elles traitées de manière cohérente au sein de l'équipe ?
2. La deuxième étape consiste à obtenir le soutien de l'organisation pour ce rôle. L'Agent du changement ne peut pas exercer efficacement ses fonctions sans le soutien de la direction. Avant de sélectionner un candidat, la décision d'introduire ce rôle doit être discutée et approuvée au niveau de la direction, avec un engagement clair à consacrer du temps à cette fonction, à la reconnaître officiellement et à soutenir activement la personne qui l'assumera.
3. La troisième étape consiste à définir le rôle avant de le pourvoir. Cela signifie qu'il faut s'accorder sur le périmètre des responsabilités, le temps à consacrer à cette fonction et la manière dont elle s'intégrera dans la structure organisationnelle existante. Un mandat clair, même sous la forme d'une simple description d'un paragraphe, permet d'éviter toute ambiguïté et confère au futur Agent du changement en cybersécurité la légitimité nécessaire pour agir.

Ce n'est qu'une fois ces trois étapes mises en place que l'organisation est prête à identifier et à désigner le candidat le plus approprié. La section suivante présente la liste de contrôle qui guidera la mise en œuvre réussie du rôle.

Figure 1 - Feuille de route visuelle pour la mise en œuvre de l'Agent du changement en cybersécurité



7. CHECKLIST

La liste de contrôle suivante est destinée à vérifier si les principales conditions nécessaires à une mise en œuvre réussie de l'Agent du changement en cybersécurité sont réunies. Elle est fondée sur les enseignements tirés du projet pilote CyberAgent.

7.1. DIRECTION

[ ] Le rôle d'Agent du changement a été officiellement approuvé et un budget lui a été alloué.

[ ] Un mandat clair a été défini : périmètre des responsabilités, temps à consacrer au rôle et rattachement hiérarchique.

[ ] La désignation a été communiquée à l'ensemble de l'organisation.

[ ] Une évaluation du rôle a été programmée au cours des 12 prochains mois.

[ ] L'Agent du changement dispose d'un temps dédié dans son planning pour exercer ce rôle.

7.2. RESSOURCES HUMAINES

[ ] Le processus de sélection était ouvert à tous, indépendamment du genre ou du parcours.

[ ] Le rôle est présenté sous l'angle de son impact organisationnel, et non de l'expertise technique.

[ ] Les responsabilités de l'Agent du changement figurent dans sa fiche de poste ou ses objectifs.

[ ] Les nouveaux collaborateurs sont présentés à l'Agent du changement en cybersécurité lors de leur intégration.

[ ] Un registre des formations et des certifications de l'Agent du changement est conservé.

7.3. AGENT DU CHANGEMENT EN CYBERSÉCURITÉ

[ ] Inscrit sur la plateforme CyberAgent et parcours d'apprentissage défini.

[ ] A terminé au moins un module et obtenu un certificat.

[ ] Les collaborateurs savent comment contacter l'Agent du changement.

[ ] Les pratiques essentielles en matière de cybersécurité sont documentées et accessibles à l'ensemble du personnel.

[ ] Des actions régulières de sensibilisation sont mises en place (réunions, messages ou rappels).

[ ] Une procédure claire permet aux collaborateurs de signaler les situations suspectes.

[ ] Les retours concernant les problématiques de cybersécurité sont recueillis régulièrement et transmis à la direction.

8. COMMENT MESURER LA REUSSITE DE LA MISE EN OEUVRE

La mise en œuvre du rôle d'Agent du changement en cybersécurité constitue un engagement continu. Les indicateurs suivants peuvent aider les PME à évaluer si ce rôle produit un réel impact au fil du temps.

[ ] Le nombre de collaborateurs participant aux activités de sensibilisation à la cybersécurité a augmenté depuis la désignation de l'Agent du changement.

[ ] La cybersécurité est régulièrement abordée lors des réunions d'équipe et n'est plus considérée comme un sujet exceptionnel.

[ ] Les collaborateurs savent qui est l'Agent du changement et se sentent à l'aise pour le solliciter lorsqu'ils ont des questions ou des préoccupations.

[ ] Le nombre d'e-mails suspects, d'incidents ou de préoccupations signalés a augmenté.

[ ] L'Agent du changement a suivi des modules de formation supplémentaires depuis sa désignation.

[ ] Les retours des collaborateurs concernant la cybersécurité au sein de l'organisation sont recueillis périodiquement et pris en compte.

8.1. RECOMMANDATIONS POUR L'ADAPTATION DU MODELE

Afin de garantir que la montée en compétences de votre Agent du changement en cybersécurité se traduise par une cyberrésilience durable de l'entreprise, un suivi structurel continu est indispensable. Le Tableau 3 propose un modèle pratique de suivi destiné aux responsables de PME afin d'évaluer la situation de référence de l'organisation avant la formation et de mesurer les progrès concrets de la culture de cybersécurité 6 et 12 mois après la désignation.

Les responsables devraient considérer ce modèle comme un cadre évolutif. En fonction de la taille de votre entreprise, de son secteur d'activité et de son infrastructure existante, il est recommandé d'adapter et de compléter cette matrice :

- **Personnalisation des échelles**
  Les très petites entreprises (moins de 10 employés) peuvent remplacer les indicateurs exprimés en pourcentage par un nombre de collaborateurs afin de faciliter le suivi.
- **Ajout d'indicateurs**
  Les entreprises opérant dans des environnements fortement numérisés ou à haut risque sont encouragées à ajouter des indicateurs spécifiques, tels que « % du personnel utilisant l'authentification multifacteur (MFA) » ou « Temps moyen de réponse à une menace simulée ».

- **Adaptation locale**
  Adaptez la colonne « Source de données recommandée » à vos propres canaux de communication internes (par exemple : Slack, sondages MS Teams ou registres papier utilisés lors des réunions d'équipe).

Table 3. Modèle de suivi après la désignation de l'Agent du changement à destination des responsables de PME

Indicateur de réussite	Unité / Échelle de mesure	Situation initiale (Avant)	Progression (6 mois)	Objectif (12 mois)	Source de données recommandée
Préparation des collaborateurs face au phishing	% de collaborateurs se déclarant capables de gérer des e-mails suspects	%	%	%	Enquête interne rapide (pulse survey) ou données de la plateforme CyberAgent
Fréquence d'intégration dans les réunions	Nombre de réunions d'équipe au cours desquelles la cybersécurité a été abordée	Nombre	Nombre	Nombre	Comptes rendus ou ordres du jour des réunions d'équipe
Taux de signalement des incidents	Nombre d'incidents suspects documentés et signalés	Nombre / mois	Nombre / mois	Nombre / mois	Registre interne des incidents de sécurité ou boucle de retour du service informatique
Visibilité de l'Agent du changement	% de collaborateurs identifiant correctement l'Agent du changement	%	%	%	Court questionnaire interne
Engagement sur la plateforme	Nombre de collaborateurs participant activement au micro-apprentissage	Nombre	Nombre	Nombre	Tableau de bord analytique de gestion de la plateforme CyberAgent

CONCLUSION

La cybersécurité n'est plus une préoccupation réservée aux grandes organisations disposant de services informatiques dédiés. À mesure que le paysage des menaces évolue et que les exigences réglementaires applicables aux PME se renforcent, la question n'est plus de savoir si elles doivent se protéger, mais comment elles peuvent le faire avec les ressources dont elles disposent réellement.

Le rôle d'Agent du changement en cybersécurité apporte une réponse concrète et proportionnée à cette question. Il ne nécessite ni le recrutement d'un spécialiste, ni des investissements dans des outils coûteux, ni une refonte complète des processus existants. Il consiste à identifier la bonne personne au sein de l'organisation, à lui fournir la formation et le mandat nécessaires pour agir, et à créer les conditions permettant à la sensibilisation à la cybersécurité de faire partie du quotidien professionnel.

Le projet CyberAgent a démontré que cette approche est réalisable. Dans huit pays européens, des employés de PME sans formation technique ont suivi la formation, assumé le rôle d'Agent du changement et commencé à faire évoluer la manière dont leur organisation aborde la cybersécurité. Les résultats sont sans équivoque : lorsque les barrières à l'entrée sont réduites, que le rôle est présenté sous l'angle de la culture organisationnelle plutôt que de l'expertise technique, et que l'inclusion est considérée comme un principe de conception plutôt que comme une réflexion secondaire, les résultats sont au rendez-vous.

Ce Guide est une invitation à franchir cette première étape. La feuille de route est disponible. Les outils existent. Le rôle est à la portée de toute PME prête à investir dans ses collaborateurs.

CyberAgent

Co-funded by the European Union

Get social with the project!

www.cyberagents.eu

contact@cyberagents.eu

@Cyber-Agent-EU

@CyberAgent.EU

@CyberAgentEU

@Cyber.Agent.EU

@CyberAgentEU

Project Partners

Vilniaus Universitetas 1579 Universitas Vilnensis

Kaunas Faculty

Prios

EVM Grupo

Teknopark İstanbul Mesleki ve Teknik Anadolu Lisesi

IT Akademija

ProxyLab

Women4Cyber European Cyber Security Organisation

Liceul Tehnologic Grigore C. Moisil Buzau