Co-funded by the European Union

THE SME CYBER SECURITY CHANGE AGENTS TRAINING NEEDS MAPPING REPORT

CYBER AGENT 10.2023

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

Financé par l'Union européenne. Les points de vue et avis exprimés n'engagent toutefois que leur(s) auteur(s) et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive européenne pour l'éducation et la culture (EACEA). Ni l'Union européenne ni l'EACEA ne sauraient en être tenues pour responsables..

Work Package 2: CyberAgent approach and structure design

Deliverable 2.2: The SME Cyber Security Change Agents Training needs mapping report

Leader of WP2 – Olemisen Balanssia ry
Leader of deliverable 2.2 – Olemisen Balanssia ry

CONTENT

INTRODUCTION

Ce rapport de projet vise à analyser et cartographier les besoins de formation afin d'identifier les compétences appropriées requises pour un *Cyber Security Change Agent* dans une PME. Grâce à un examen complet des offres de formation actuelles et à la compréhension des préférences des PME en matière de cybersécurité, ce rapport cherche à combler le fossé entre les compétences actuelles et à définir l'ensemble de compétences idéal requis.

À mesure que les cybermenaces deviennent de plus en plus sophistiquées, les PME doivent impérativement s'assurer qu'elles disposent d'un personnel adéquatement formé pour lutter contre ces menaces. Les *Cyber Security Change Agent* jouent dans ce contexte un rôle crucial. Ce rapport analyse le paysage de la cybersécurité à travers différentes perspectives : l'éducation et la formation, l'inclusion du genre et l'état actuel des PME et des établissements scolaires.

1. MÉTHODOLOGIE

Pour ce processus de cartographie, nous avons utilisé une approche mixte combinant recherche documentaire et recherche sur le terrain.

Dans le cadre de la recherche documentaire, une revue complète de la littérature a été réalisée pour :

- Examiner les dispositions éducatives existantes et émergentes aux niveaux de l'EFP et de l'enseignement supérieur dans le domaine de la cybersécurité dans chaque pays partenaire.
- Rechercher et compiler des articles, des recherches et des rapports liés au contenu et aux besoins de formation en cybersécurité.
- Analyser les cours d'EFP et d'enseignement supérieur, leurs programmes et leur pertinence par rapport aux défis de cybersécurité du monde réel.

Les objectifs étaient les suivants :

- Identifier les composantes actuelles du programme des cours de cybersécurité proposés aux niveaux de l'EFP et de l'enseignement supérieur dans chaque pays.
- Évaluer dans quelle mesure ces programmes s'alignent sur les défis de la cybersécurité.
- Identifiez s'il existe des stratégies ou des programmes spécifiques pour impliquer davantage de femmes dans les études de cybersécurité.

Durant la phase de recherche sur le terrain, nous avons mené 2 enquêtes. Une conçue pour les enseignants et les formateurs des catégories EFP et enseignement supérieur de chaque pays afin de comprendre les nuances des offres de formation actuelles. L'autre adapté aux PME pour avoir une vision et une compréhension de la situation des entreprises dans le domaine de la cybersécurité : comment les salariés sont impliqués et engagés sur ces sujets, les défis et les besoins. L'objectif de cette recherche sur le terrain était également de déterminer les caractéristiques, les besoins de formation et les préférences d'apprentissage, en mettant particulièrement l'accent sur les besoins des femmes en matière de cybersécurité.

Nous avons atteint un nombre significatif de réponses pour les deux questionnaires. 190 enseignants et formateurs de l'EFP et de l'enseignement supérieur et 176 salariés de PME.

Enquête 1 : Cartographie des besoins de formation des *Cyber Security Change Agents* dans les PME - **Enquête EFP et enseignement supérieur.**

Type d'établissement	**Réponses**	**Femme**	**Homme**	**Non renseigné**
Enseignement supérieur	104	28	73	3
EFP (Enseignement et Formation des Professionnels)	86	36	48	2
Total	**190**	**64**	**121**	**5**

Enquête 2: Cartographie des besoins de formation pour les *Cyber Security Change Agents* dans les PME - **Enquête auprès des PME.**

Nombre de réponses	**Nombre**
PME	176
Total	**176**

Les questionnaires et les données complètes se trouvent aux annexes C et D.

2. RECHERCHE (TOUT LES PARTENAIRES)

2.1. DISPOSITIONS ACTUELLES EN MATIÈRE D'ÉDUCATION ET DE FORMATION

Cette section présente la recherche et fournit des informations tirées de la recherche documentaire et des enquêtes, en soulignant les points forts et les lacunes de l'infrastructure actuelle d'éducation et de formation dans les pays partenaires.

2.1.1. APERÇU DES FORMATIONS EN CYBERSÉCURITÉ DE L'EFP ET DE L'ENSEIGNEMENT SUPÉRIEUR

Nous avons procédé à une vaste analyse du paysage de l'éducation à la cybersécurité dans tous les pays partenaires afin d'en décrire l'état actuel et de mettre en évidence les aspects pertinents de l'éducation et des formations en cybersécurité.

En Lituanie, une recherche dans la base de données AIKOS a révélé qu'il existait au total six programmes formels d'enseignement de la cybersécurité proposés par des établissements lituaniens, au niveau de la licence et du master :

Domaine d'étude	Programme	Etablissement	ECTS	Diplôme
Ingénerie de l'informatique	Information and Information Technology Security[1]	Kaunas University of Technology	120	Master of Computer Science
Management	Cybersecurity Management[2]	Mykolas Romeris University	90	Master of Business Management
Ingénerie de l'informatique	Information and information technologies security[3]	Vilnius Gediminas Technical University	120	Master of Computer Science
Ingénerie de l'informatique	Information Systems and Cyber Security[4]	Vilnius University	210	Bachelor of Computer Science
Ingénerie de l'informatique	Technologies of Information Systems and Cyber Security[5]	Marijampole College	180	Professional Bachelor of Computer Science
Ingénerie de l'informatique	Cyber Systems and Security[6]	Kaunas College	180	Professional Bachelor of Computer Science

Les programmes de cybersécurité de niveau master présentent des approches distinctes mais complémentaires. L'université de Kaunas met l'accent sur la méthodologie de la recherche, les

[1] https://www.aikos.smm.lt/studijuoti/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=LO&f=MokGal&key=8618_2023&pt=of&ctx_sr=8Gzz1EUgIeKfy0cWNVrrVdABKo0%3d
[2] https://www.aikos.smm.lt/Registrai/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=PROG&f=Prog&key=2845&pt=of&ctx_sr=za5dHDvp0IGJ2%2fD6Fkt7rIse6a8%3d
[3] https://www.aikos.smm.lt/studijuoti/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=LO&f=MokGal&key=1442_2023&pt=of&ctx_sr=8Gzz1EUgIeKfy0cWNVrrVdABKo0%3d
[4] https://www.aikos.smm.lt/Registrai/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=PROG&f=Prog&key=9664&pt=of&ctx_sr=za5dHDvp0IGJ2%2fD6Fkt7rIse6a8%3d
[5] https://www.aikos.smm.lt/Registrai/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=PROG&f=Prog&key=2775&pt=of&ctx_sr=za5dHDvp0IGJ2%2fD6Fkt7rIse6a8%3d
[6] https://www.aikos.smm.lt/Registrai/_layouts/15/Asw.Aikos.RegisterSearch/ObjectFormResult.aspx?o=PROG&f=Prog&key=3797&pt=of&ctx_sr=za5dHDvp0IGJ2%2fD6Fkt7rIse6a8%3d

méthodes de sécurité de l'information et les aspects juridiques de l'espace électronique, en se concentrant sur le développement de compétences en matière de conception et de mise en œuvre de systèmes informatiques sécurisés. L'université technique de Vilnius Gediminas donne la priorité à la formation de spécialistes ayant une approche systématique des questions de sécurité de l'information, en associant les connaissances scientifiques aux méthodes et technologies permettant d'assurer la sécurité de l'information, tout en encourageant la pensée critique et le leadership. L'université Mykolas Romeris, quant à elle, se distingue par son orientation vers la gestion de la cybersécurité, visant à former des spécialistes capables de superviser les environnements informatiques modernes et les tâches complexes liées à la cybersécurité, en mettant fortement l'accent sur la gestion stratégique dans des contextes technologiques dynamiques.

Les programmes d'études en cybersécurité au niveau de la licence visent tous à former des professionnels qualifiés dans les domaines de l'informatique et de la cybersécurité, mais chacun d'entre eux met l'accent sur des aspects distincts. Le programme de l'université de Vilnius vise à fournir une base complète en ingénierie informatique, en mettant l'accent sur l'analyse, la conception, le développement et la maintenance de systèmes d'information sécurisés. Le Marijampole College, tout en visant également à former des informaticiens compétents, met davantage l'accent sur les aspects pratiques tels que la création, la maintenance et l'administration de réseaux et de systèmes informatiques. Le Kaunas College se différencie en visant à préparer des spécialistes capables non seulement de concevoir et de mettre en œuvre des cyber-systèmes, mais aussi de diriger des équipes, de comprendre les implications éthiques, juridiques et sociales, et de travailler efficacement dans des environnements multiculturels. Si les trois établissements visent à doter les étudiants de compétences techniques en matière de cybersécurité, leurs objectifs varient : compétence technique (université de Vilnius), application pratique et développement de compétences non techniques (collège de Marijampole), et combinaison de considérations techniques, de leadership et d'éthique (collège de Kaunas).

La recherche a également révélé l'existence de quatre programmes de formation non formelle pour adultes en matière de cybersécurité, chacun d'entre eux étant axé sur les compétences essentielles pour reconnaître, enquêter et prévenir les cyberattaques, en particulier à l'aide de la cryptographie. Si tous les programmes partagent cet objectif central, leurs approches et leurs champs d'application diffèrent. Certains se concentrent sur la cybersécurité et les stratégies préventives, tandis que d'autres proposent un programme plus large, couvrant des domaines tels que l'ingénierie sociale, la gestion de l'identité et la gestion des risques. Notamment, plusieurs programmes commencent par la programmation de base et progressent vers des sujets de cybersécurité avancés, adaptés aux débutants. Un programme remarquable, en collaboration avec Cybint, s'adresse aux personnes ayant des connaissances limitées en informatique, en leur offrant des compétences pratiques et concrètes, à temps plein ou à temps partiel. L'ensemble de ces programmes vise à développer diverses compétences en matière de cybersécurité, allant de la programmation de base à un apprentissage approfondi axé sur les applications.

Plusieurs politiques visant à renforcer la sécurité et la défense nationales en Finlande ont influencé les programmes d'enseignement liés à la cybersécurité. Le nombre d'initiatives de recherche et de développement, de programmes d'enseignement et de formation, et de professionnels certifiés dans le domaine de la cybersécurité a augmenté. La *Fininish Cyber Security Strategy* (2019) (**https://turvallisuuskomitea.fi/en/finlands-cyber-security-strategy-2019/**) et le *Cyber Security Development Programme* (2021) soulignent l'importance de renforcer les compétences nationales en matière de cybersécurité par l'éducation et la recherche. Pour le système d'enseignement scolaire, l'objectif est de doter les élèves des compétences et des connaissances nécessaires pour naviguer en toute sécurité dans le monde numérique et de les sensibiliser aux cybermenaces et aux mesures de protection **Lehto-IWS-018.pdf (jyu.fi**)

Dans l'enseignement et la formation professionnelle (EFP) finlandais, la cybersécurité n'est pas explicitement présentée comme un thème distinct ou spécialisé dans la plupart des contenus. Toutefois, cela ne signifie pas nécessairement que la cybersécurité est totalement absente des programmes d'EFP. Compte tenu de l'importance croissante de la culture numérique et de la cybersécurité dans tous les secteurs, ces sujets sont intégrés dans des programmes d'enseignement technique et informatique plus larges. Il est important de noter que les fournisseurs d'EFP en Finlande ont l'autonomie d'organiser leurs offres éducatives en fonction des exigences régionales et spécifiques à chaque domaine. L'enseignement et la formation professionnelle finlandais ont récemment fait l'objet de la plus vaste réforme depuis près de 20 ans. L'objectif de la réforme de 2018 était de créer un système d'EFP plus efficace et plus flexible, basé sur les compétences et orienté vers le client, d'améliorer son efficacité et de mieux faire correspondre les qualifications aux besoins du marché du travail. Pour ce faire, il convient principalement d'alléger la réglementation et d'introduire davantage d'autonomie et de responsabilité pour les prestataires d'EFP. (Source : **https://www.cedefop.europa.eu/files/8133_en.pdf)**) Cela signifie que certains établissements pourraient proposer des modules plus spécialisés dans des domaines tels que la cybersécurité, en fonction des demandes et des partenariats avec l'industrie locale. D'après les recherches de Lehto, la cybersécurité n'est pas une matière distincte, mais elle est intégrée à d'autres matières, en particulier dans le contexte des technologies de l'information et de la communication (TIC). La responsabilité de l'enseignement incombe aux enseignants, qui doivent intégrer l'éducation à la cybersécurité dans leurs matières. Cette approche entraîne des variations dans la manière dont elle est mise en œuvre selon les écoles et les niveaux scolaires et souligne la nécessité d'adopter des approches plus structurées et plus cohérentes pour enseigner la cybersécurité, notamment en en faisant éventuellement une matière distincte ou une partie plus importante de l'enseignement des TIC.

Au niveau de l'enseignement supérieur, les universités finlandaises proposent des programmes complets en cybersécurité. Ces programmes sont conçus pour doter les étudiants de connaissances et de compétences avancées dans divers domaines de la cybersécurité. Nombre d'entre elles proposent un master en sécurité de l'information et en technologies de l'information, qui met l'accent sur les implications et les applications de ces concepts dans le monde réel. Ils sont accessibles sur place et à distance

Le secteur de la cybersécurité en Belgique connaît une demande accrue de professionnels qualifiés, avec environ 4 000 postes vacants dans ce domaine (en novembre 2022). Conscients de l'urgence et de la nécessité de combler cette lacune, plusieurs initiatives et programmes éducatifs ont été mis en place pour développer l'expertise du pays en matière de cybersécurité. De nombreuses institutions belges, telles que la KU Leuven, la Solvay Business School, la Howest University of Applied Sciences et bien d'autres, ont mis au point des programmes spécialisés en anglais, en français et en néerlandais, capables de toucher un large public. Toutefois, des recherches menées par l'organisation belge Agoria ont mis en évidence la nécessité d'une formation continue, y compris pour les professionnels qui ne fréquentent plus l'université, afin de les tenir au courant de l'évolution du domaine de la cybersécurité et des menaces qui pèsent sur lui. La stratégie belge de cybersécurité pour les années 2021-2025 reconnaît le niveau élevé d'intégration de la cybersécurité dans l'environnement universitaire du pays et souligne le rôle essentiel que jouent les universités et les autres établissements d'enseignement pour stimuler les efforts de recherche et de développement dans ce domaine. Selon la base de données du CBB (Centre for Cybersecurity Belgium), il existe en Belgique 33 formations (licence, master et certifications) proposées par les établissements d'enseignement supérieur, qui s'ajoutent à une série de programmes d'enseignement et de formation professionnelle proposés dans les secteurs public et privé. La CBB est l'organisme qui supervise, coordonne et contrôle la mise en œuvre de la stratégie belge en matière de cybersécurité. Elle met actuellement au point une formation gratuite de sensibilisation à la cybersécurité à l'intention des employés belges afin de diffuser encore davantage les connaissances en matière de cybersécurité au sein de la population. Dans l'ensemble, la cyber stratégie belge souligne l'importance de diffuser les connaissances et les compétences par l'éducation et s'engage à développer les cours universitaires, à promouvoir la recherche dans ce domaine, à encourager l'enseignement des STIM et à offrir des possibilités de formation pratique pour répondre à la demande croissante de professionnels dans le paysage belge de la cybersécurité.

En Norvège, la cybersécurité n'est pas une matière principale que l'on peut étudier au niveau de l'EFP. Des éléments du programme sont inclus dans un programme d'EFP intitulé « Informatique et électronique ». Il n'existe pas de cadre du ministère de l'éducation pour la cybersécurité, il est seulement mentionné dans les compétences de base générales en matière de culture numérique pour l'ensemble de l'éducation que les étudiants doivent être capables d'utiliser et de naviguer dans les ressources numériques à l'intérieur et à l'extérieur des réseaux et de préserver la sécurité de l'information et des données.

La **stratégie nationale pour la compétence en matière de cybersécurité** souligne, le 14 novembre 2023, l'importance de l'apprentissage de la cybersécurité par les élèves de l'enseignement professionnel. Pour de nombreuses matières professionnelles, c'est très pertinent et important. Les cours professionnels manquent de matériel pédagogique sur la cybersécurité et les enseignants n'ont pas les compétences nécessaires pour enseigner, en particulier dans des domaines tels que la protection de la vie privée, la technologie des maisons intelligentes et l'IdO. Les programmes existants d'éducation à la cybersécurité, tels que GenCyber et CyberFirst, ne répondent pas spécifiquement aux besoins de ce programme professionnel. (**source 1 - 2**)

Grâce à une collaboration entre l'UiO, la NTNU et les enseignants de certaines écoles de formation professionnelle, il est prévu de développer du matériel d'apprentissage pour la cybersécurité, qui sera ensuite mis à disposition sur la plateforme nationale d'apprentissage **NDLA (National Digital Learning Arena)**.

Dans l'enseignement supérieur, on trouve à la fois un programme d'un an en culture de la sécurité numérique et des programmes de licence en cybersécurité. Le sujet est également abordé dans un certain nombre de programmes de master en sciences des données et en informatique. Il existe une variété d'études spécifiques en matière de cybersécurité, telles que l'informatique appliquée et les technologies de l'information, le bachelor en cybersécurité, le bachelor en criminalistique numérique, l'infrastructure numérique et la cybersécurité, la culture de la sécurité numérique et le master en sécurité de l'information basé sur l'expérience. Il existe également des études dans lesquelles la cybersécurité est incluse, comme la culture et la direction de l'HSE, les coopératives municipales de préparation aux situations d'urgence et le travail du conseil dans la pratique, ainsi que l'étude annuelle sur la gestion des crises.

En Pologne, ces dernières années, les cyber études se sont multipliées. De plus en plus de cours sur la cybersécurité ont ouverts dans les universités et, dans le même temps, le nombre de formations professionnelles disponibles augmente.

La demande de professions dans le domaine de la cybersécurité a augmenté en Pologne ces dernières années et la délégation polonaise est de plus en plus sensibilisée à la cybersécurité, ce qui incite les entreprises à employer des experts en cybersécurité et à protéger les informations. En Pologne, comme dans la plupart des pays européens, un diplôme universitaire est considéré comme obligatoire et, par conséquent, les cours en cybersécurité sont souvent un complément d'étude après le diplôme. En effet, la plupart des études sont plus longues mais théoriques. Il existe des cours de cybersécurité de courte durée, mais la plupart d'entre eux se concentrent sur l'apprentissage pratique qui prépare au travail réel.

Le grand défi pour un étudiant dans le domaine de la cybersécurité est que la plupart des établissements d'EFP ne disposent pas de leur propre financement, de sorte qu'une solution financière est nécessaire, et que cette option ne convient pas toujours aux personnes intéressées.

Même si la cybersécurité devrait être une priorité pour tous les domaines d'activité, le système d'enseignement professionnel en Roumanie n'est pas encore prêt à garantir que les étudiants soient compétents dans ce domaine. L'analyse du programme d'études du lycée - filière technologique - dans tous les domaines de la formation professionnelle montre que le programme scolaire de culture technique ne prévoit pas d'unités d'apprentissage sur la cybersécurité. Certaines compétences spécifiques dans ce domaine peuvent être trouvées dans le programme de connaissances générales, dans la discipline des technologies de l'information et de la communication.

Ces compétences sont les suivantes:

1. Description et application des mesures de sécurité dans l'utilisation de l'Internet

- Utilisation intelligente de l'internet
- L'importance du cryptage de la transmission des données
- Utilisation de la signature numérique
- Moyens de défense contre les virus

2. Utilisation du service de chat :

- Présentation des applications collaboratives pour la vidéoconférence
- Présentation des règles du réseau

En ce qui concerne l'enseignement supérieur, l'université Transilvania de Brasov fait preuve d'un engagement fort en faveur de l'enseignement de la cybersécurité, en proposant un programme complet de maîtrise en cybersécurité entièrement dispensé en anglais. L'engagement de l'université à favoriser l'expertise dans ce domaine critique est évident dans le programme d'études complet proposé dans le cadre du programme.

Le programme de master de l'université de Transylvanie est une excellente opportunité pour les étudiants qui souhaitent acquérir une formation complète en cybersécurité dans un cadre universitaire international. La combinaison d'un programme d'études solide et d'un enseignement en anglais permet aux diplômés de réussir dans le domaine dynamique et stimulant de la cybersécurité.

L'Université Babes-Bolyai de Cluj-Napoca, par l'intermédiaire de la Faculté de mathématiques et d'informatique, a lancé à partir de l'année universitaire 2023-2024 un programme de master en anglais en cybersécurité, visant à préparer de futurs spécialistes dans ce domaine d'une importance vitale dans le contexte de la transition vers la société de l'information. Les cours du nouveau programme débutent en octobre de cette année, en même temps que l'année académique 2023-2024, l'admission amenant une compétition au-delà des attentes. Plus de 40 étudiants, y compris de l'étranger, admis au programme deviendront des spécialistes dans le domaine de la cybersécurité, les candidats admis peuvent même choisir d'étudier une année académique dans d'autres universités renommées en Europe.

À la faculté de mathématiques et d'informatique, le programme de master Technologies de l'Internet (en anglais) propose également, au second semestre de la première année, un cours de cryptographie et de sécurité des systèmes, qui initie les étudiants au domaine de la cybersécurité et aux méthodes spécifiques de cryptage des données.

En outre, le programme de master Technologies modernes en ingénierie des systèmes logiciels propose, au premier semestre de la deuxième année, un cours optionnel intitulé Sécurité des systèmes informatiques, centré sur les principaux défis de la cybersécurité.

Ces deux cours permettent aux étudiants en master de la faculté de mathématiques et d'informatique d'acquérir des connaissances et une expertise dans ce domaine, qui revêt une importance vitale dans le contexte international actuel, et d'être sensibilisés aux défis du cryptage et de la sécurité des systèmes modernes.

L'université de Bucarest, faculté de mathématiques et d'informatique, propose un programme de master en sécurité et logique appliquée (en anglais), qui offre une série de cours consacrés à la cryptographie et à la sécurité des systèmes. Les étudiants peuvent acquérir des connaissances dans les domaines de la sécurité des systèmes d'exploitation, de la cryptographie, de la sécurité des réseaux et de la cybersécurité, et être ainsi préparés à relever les défis de ce domaine.

En Espagne, la plupart des études en cybersécurité se font au niveau de l'enseignement supérieur, en licence ou en master. Selon les données recueillies par l'Institut national de cybersécurité de l'Espagne, il existe :

- Environ 87 masters en cybersécurité proposées par des universités publiques et privées et d'autres établissements d'enseignement supérieur.
- 4 spécialisations, principalement dans le domaine de la criminalistique informatique.
- 3 diplômes universitaires, tous proposés par le secteur privé.

En ce qui concerne la formation au niveau de l'EFP, les instituts de formation professionnelle espagnols proposent une soixantaine de cours. Tous sont régis par le même programme, approuvé par le ministère de l'éducation en mai 2020 par le décret royal 479/2020 du 7 avril, qui établit le cours de spécialisation en cybersécurité dans les environnements de technologie de l'information.

Malgré les programmes existants, la nécessité de poursuivre les efforts est reconnue. L'Espagne a mis en œuvre divers plans, notamment le plan national de compétences numériques, le plan de numérisation des PME 2021-2025 et le plan Espagne numérique 2025, en mettant l'accent sur la création de nouveaux talents pour répondre à la demande croissante de compétences numériques, en particulier dans le domaine de la cybersécurité.

En Turquie, le besoin de cybersécurité a augmenté rapidement et est devenu très important dans le pays, ainsi que dans le monde entier, en particulier au cours des dernières années. Parallèlement aux développements technologiques, les cyber-risques et les cyber-menaces ont également évolué au même rythme et sont devenus complexes. Les cyber-risques et les cyber-menaces ont atteint le potentiel de causer des conséquences négatives beaucoup plus importantes que les attaques physiques. Des secteurs tels que la finance, les communications électroniques, l'énergie, les transports et l'aviation fournissant des services dans un environnement numérique sécurisé, la garantie de la cybersécurité nationale est devenue l'une des principales priorités du pays. Dans ce contexte, des études se poursuivent pour diffuser la formation à la cybersécurité dans la formation professionnelle et l'enseignement supérieur en fonction des besoins du secteur et pour développer et enrichir les contenus de formation.

Dans le cadre de ces études, dans l'enseignement professionnel : Cours sur les fondamentaux de la cybersécurité dans l'exploitation des réseaux dans le domaine des technologies de l'information. Dans le domaine de la cybersécurité, les bases de la programmation, la sécurité des systèmes, les technologies de réseau, le développement de logiciels sécurisés, les tests de pénétration et la réponse aux cyberincidents, la criminalistique informatique, etc. Les résultats des cours sont remis aux étudiants.

Dans l'enseignement supérieur, le programme de diplôme d'associé « Analyste et opérateur en cybersécurité » dans les écoles professionnelles de cybersécurité, le programme de licence en ingénierie informatique légale dans les universités et les programmes de maîtrise pertinents sont proposés dans les universités.

En outre, les centres de formation continue des universités, les centres d'éducation publique des municipalités, les institutions officielles telles que TÜBİTAK, TSE et les établissements d'enseignement privés proposent également des formations sur la cybersécurité.

2.1.2. LES DÉFIS DE LA CYBERSÉCURITÉ ET LES BESOINS DE L'INDUSTRIE

Sur la base d'une analyse documentaire approfondie, nous avons dressé la liste des défis en matière de cybersécurité auxquels sont confrontées les PME dans les pays concernés par le projet. Dans le paysage évolutif de la cybersécurité, les petites et moyennes entreprises (PME) de Lituanie sont confrontées à de multiples défis en matière de cybersécurité. Alors que ces entreprises s'appuient de plus en plus sur les technologies numériques pour leurs opérations, elles deviennent plus vulnérables à un éventail de cybermenaces, ce qui nécessite une compréhension globale et une approche stratégique pour gérer ces risques de manière efficace.

Dans l'étude de 2022, Bukauskas et al. distinguent des types d'organisations en fonction de leur maturité en matière de cybersécurité et de leurs besoins en compétences. Selon l'étude, les petites organisations sont comparables aux individus dans la société, car le principal paramètre de la sécurité de l'espace de travail numérique est le niveau de cyber hygiène, qui est influencé par la compréhension générale des menaces de cybersécurité. À ce niveau, la cybersécurité est coordonnée en interne au sein de l'organisation, ce qui entraîne des failles de sécurité potentielles dans les processus d'entreprise. Dans les entreprises de taille moyenne, la gestion et la réglementation de la cybersécurité sont également faiblement coordonnées. Les réponses aux incidents ou autres activités de cybersécurité ne sont pas non plus mises en avant au sein de l'organisation. Sachant qu'en Lituanie, les petites entreprises représentent 97 % de l'ensemble des sociétés, Bukauskas et al. (2022) ont conclu qu'il existe un besoin important de spécialistes de l'informatique qui fournissent des services informatiques, consultent les utilisateurs et dont les fonctions incluent la garantie des principes fondamentaux de la cybersécurité. Ils ont également mis en évidence un manque notable dans le domaine du renseignement sur les menaces et de la recherche scientifique, ainsi qu'un besoin visible de spécialistes de la cybersécurité dans les domaines de l'ingénierie de la sécurité et du cycle de vie des systèmes.

Quelques années auparavant, le programme « Create for Lithuania », en collaboration avec le ministère de la défense nationale, a organisé une consultation publique sur l'amélioration de la sensibilisation à la cybersécurité dans les petites et moyennes entreprises. L'initiative est également arrivée à la conclusion qu'il est évident que le niveau de sensibilisation à la cybersécurité parmi les PME en Lituanie n'est pas élevé et que les petites entreprises n'ont pas atteint un niveau adéquat de cyber-résilience en raison d'un manque de compréhension des risques numériques. En outre, l'initiative a noté que plus de la moitié (57 %) des chefs d'entreprise ont déclaré qu'ils n'avaient pas les connaissances suffisantes pour choisir des solutions de cybersécurité ou qu'ils n'étaient pas sûrs de les avoir, et plus de trois quarts des employés ont reconnu qu'ils ne disposaient pas d'informations facilement compréhensibles.

Si l'on compare les conclusions de Bukauskas et al. (2022) et de l'initiative antérieure « Create for Lithuania » (2019), il est évident que la situation en matière de cybersécurité dans les PME lituaniennes a peu évolué. Les deux études soulignent le manque persistant de connaissances de base en matière de cybersécurité et de préparation dans ces entreprises. Malgré une dépendance accrue aux technologies numériques, les PME continuent de présenter des vulnérabilités dues à une cyber-résilience inadéquate et à un manque général de compréhension des risques numériques. Ce défi permanent met en évidence le besoin urgent d'améliorer la sensibilisation et la formation à la cybersécurité dans les PME, un secteur critique qui constitue la majorité du paysage commercial de la Lituanie.

En Finlande, une étude de l'ETLA (Elinkeinoelämän tutkimuslaitos), Institut de recherche économique de Fin-land a souligné que le nombre de violations de données dans les entreprises finlandaises, y compris les PME, avait doublé en deux ans. Les entreprises finlandaises ont signalé des violations de données trois fois plus que la moyenne européenne en 2019, la plupart des incidents étant liés à des escroqueries, des attaques par hameçonnage, des violations de données, des logiciels malveillants et des vulnérabilités. Cette étude met également en évidence la pénurie de professionnels qualifiés en cybersécurité comme principal défi pour les PME finlandaises. **https://www.etla.fi/en/publications/kyberuhat-yleistyvat-miten-suomen-yritykset-parjaavat/**

Le Centre national de cybersécurité de Finlande (NCSC-FI) (**https://www.kyberturvallisuuskeskus.fi/en**) est une initiative menée par le gouvernement finlandais. Il fait partie de l'Agence finlandaise des transports et des communications (Traficom), une agence gouvernementale responsable de la réglementation des secteurs des communications et des transports en Finlande. Il fournit des informations sur l'état actuel de la cybersécurité et propose des conseils et des outils aux particuliers et aux organisations pour améliorer leurs pratiques en matière de cybersécurité. Le centre participe également à des initiatives nationales en matière de cybersécurité, telles que des alertes à la vulnérabilité, et encourage la sensibilisation et la préparation aux cybermenaces.

Leurs rapports hebdomadaires donnent un bon aperçu des défis auxquels sont confrontées les PME. Nous apprenons que les PME finlandaises, comme beaucoup d'autres, ont été confrontées aux mêmes problèmes de sécurité décrits par l'institut ETLA en étant la cible de nombreux

messages d'hameçonnage et d'escroquerie. Il s'agit notamment de tentatives d'usurpation de services légitimes tels que Suomi.fi afin d'obtenir des informations d'identification ou d'autres informations sensibles. Les ressources financières des PME peuvent limiter le déploiement de solutions modernes de cybersécurité pour se défendre contre les cybermenaces. Par ailleurs, les PME déjà équipées ont du mal à se tenir au courant des nouvelles menaces en matière de cybersécurité.

Dans notre effort pour comprendre la situation de cybersécurité à laquelle sont confrontées les PME en Belgique, nous avons mené une recherche approfondie. Cependant, nous avons trouvé difficile d'obtenir des données ou des sources complètes traitant de cette question cruciale. Ce manque d'informations rend difficile la création de stratégies et de solutions efficaces pouvant aider les PME à protéger leurs actifs numériques contre les cybermenaces.

Nous avons pu contacter des professionnels activement impliqués dans le domaine de la cybersécurité en Belgique, grâce au vaste réseau de la Fondation Women4Cyber . Ces experts nous ont fourni des informations et des perspectives essentielles qui nous ont aidés à comprendre les différents défis auxquels sont confrontées les PME en matière de cybersécurité. Nous avons reçu l'avis d'Iva Tasheva, membre notable de Women4Cyber Belgium, qui a partagé sa vaste expérience et ses connaissances sur les défis auxquels les PME sont confrontées lorsqu'elles tentent de protéger leur infrastructure numérique contre les cybermenaces.

Les PME sont confrontées à plusieurs défis en matière de cybersécurité, tels que les difficultés d'accès à une assistance ad hoc, le manque de formation en gestion des identités et des accès pour leur personnel et une compréhension limitée des rôles et responsabilités des services cloud. De plus, les PME ont un accès limité à des solutions abordables d'analyse des vulnérabilités et à des outils de surveillance, ce qui les rend plus vulnérables aux cybermenaces. L'hyperconnectivité omniprésente dans les environnements commerciaux expose les PME au vol d'identité et aux activités frauduleuses, tandis que le phishing et les escroqueries présentent des risques permanents. Pour relever ces défis, les PME doivent prendre des mesures proactives, mettre en œuvre des protocoles de sécurité robustes et proposer une formation complète aux employés afin de renforcer leurs compétences et de se protéger contre les violations potentielles et les pertes financières.

La cybersécurité est devenue l'une des principales priorités des entreprises espagnoles, y compris des petites et moyennes entreprises (PME). L'augmentation du télétravail et des cours en ligne a conduit, entre autres, à une utilisation généralisée des fonctions de bureau à distance, du cloud computing et des outils collaboratifs, augmentant ainsi les risques et les attaques informatiques. Le rapport du Centre National de Cryptologie (CCN-CERT) relie l'augmentation du télétravail et de l'utilisation de la technologie à l'augmentation de ces risques. Les attaques les plus fréquentes subies par les entreprises sont les ransomwares et les attaques contre les systèmes d'accès à distance. L'augmentation des cybermenaces a conduit les entreprises à augmenter le nombre de personnes affectées aux équipes de cybersécurité, que ce soit en interne ou en externe. Malgré cela, les entreprises externalisent encore environ 50 % de ces fonctions.

De plus, 21 % des entreprises espagnoles ne disposent toujours pas de centres d'opérations de sécurité (SOC) pour traiter les incidents. En termes d'éducation à la cybersécurité dans l'environnement des entreprises, l'analyse de Deloitte souligne qu'en 2022, les heures de formation en ligne en cybersécurité pour les employés des organisations analysées ont augmenté de près de 30 % par rapport aux données de 2021. Cependant, près de 50 % des entreprises en Espagne ne disposent d'aucune certification en matière de cybersécurité, ce qui constitue un défi évident pour l'avenir.

Néanmoins, le plus grand défi auquel sont confrontées les entreprises espagnoles reste le manque de talents en matière de cybersécurité. Selon le rapport « Analyse et diagnostic des talents en cybersécurité en Espagne » préparé par ObservaCiber, en 2021, l'Espagne avait un déficit de talents estimé à 24 119. En 2024, on estime que l'Espagne aura besoin de plus de 83 000 experts, ce qui portera le déficit de talents à 57,5 %.

Il apparaît que le maillon le plus faible qui amène les PME à faire face aux défis de cybersécurité est le facteur « humain ». Le plus grand défi pour les PME est que le personnel responsable de la cybersécurité ne peut pas consacrer suffisamment de temps au domaine de la cybersécurité car il a des responsabilités dans plusieurs domaines. Dans le même ordre d'idées, l'absence d'une équipe distincte de cybersécurité occupe la troisième place dans la liste des difficultés rencontrées par les PME en matière de gestion de la cybersécurité. Les PME ont des difficultés à recruter et à conserver des employés qualifiés en matière de cybersécurité.

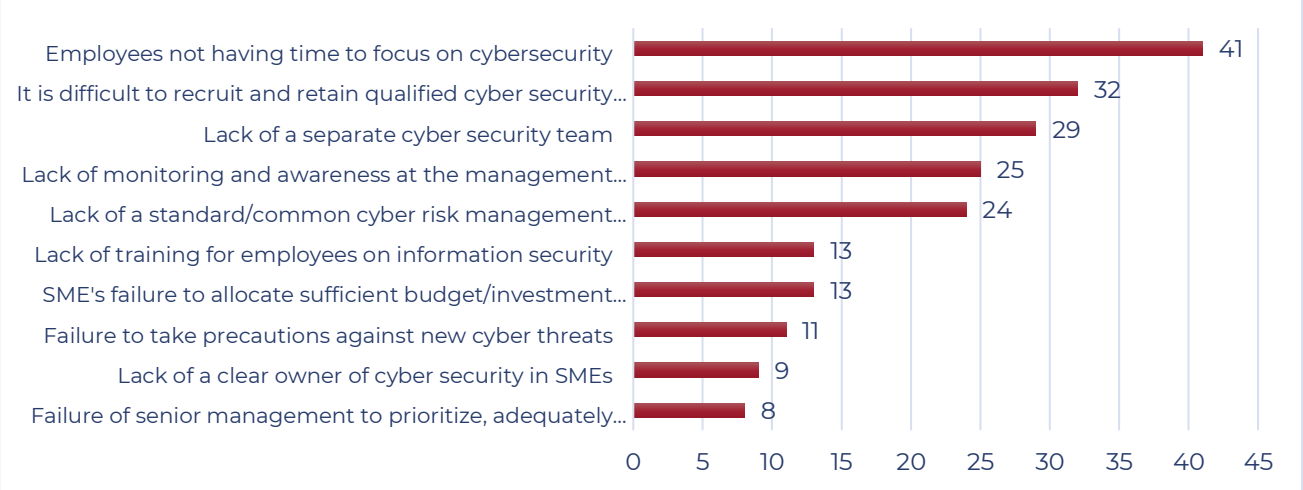


Figure 1 – Défis des PME – Recherche en Turquie.

En Roumanie, l'environnement en ligne offre des opportunités commerciales et des connexions qui peuvent aider les PME à se développer, mais il comporte également de nombreux risques.

La cybersécurité n'est plus une histoire, c'est aussi une réalité en Roumanie, même si jusqu'à présent nous n'avons pas connu de cyberattaque majeure.

La source d'information utilisée est le VERIZON REPORT sur les cybermenaces en 2023 - les principaux points clés pour les PME (DATA BREACH INVESTIGATIONS REPORT - DBIR), basé sur

16 312 incidents de sécurité, dont 5 199 ont été confirmés comme des violations de la sécurité des données.

Points d'intérêt pour les PME :

- Les surfaces d'attaque des PME et des entreprises sont similaires, car elles utilisent des logiciels basés sur le cloud. Les pénétrations non autorisées dans le système, les techniques d'ingénierie sociale et les attaques d'applications Web de base représentent 92 % du total des types d'attaques pour violations enregistrées par les PME (85 % pour les entreprises).
- ransomware 24% des cas (les données sont volées avant d'être chiffrées)
- Pénétration non autorisée dans le système – attaques complexes basées sur des logiciels malveillants et/ou du piratage pour atteindre leurs objectifs.
- Les attaquants externes représentent la plus grande menace, causant 83 % des failles de sécurité actuelles, atteignant 94 % dans le cas des attaques PME. 94 % des acteurs impliqués dans la propagation des menaces sont externes, contre 89 % dans le cas des grandes organisations, et 98 % des violations sont motivées par des raisons financières, contre 97 % dans le cas des entreprises.
- La motivation financière arrive en tête dans 95% des cas, ce pourcentage pouvant atteindre 98% dans le cas d'attaques contre des PME. Seulement 1% sont motivés par l'espionnage.
- Les salariés représentent le maillon faible de la chaîne de sécurité - 74 % de tous les cas (mauvaise sensibilisation aux cybermenaces). La principale méthode d'intrusion peut être due à l'utilisation d'identifiants volés - 49 % et au phishing - 12 % ou à d'autres méthodes, telles qu'une mauvaise configuration ou l'envoi erroné de données sensibles.
- E-mails professionnels compromettants : la victime est amenée à transférer d'importantes sommes d'argent sur les comptes des attaquants.

En Norvège, les petites et moyennes entreprises (PME) sont confrontées à des défis importants en matière de cybersécurité. Beaucoup n'ont pas une compréhension approfondie des risques encourus, ce qui conduit à des vulnérabilités potentielles. Il existe des lacunes notables dans la formation efficace des employés en matière de cybersécurité, ce qui fait de l'erreur humaine un facteur de risque courant. Les PME, en particulier celles qui déclarent disposer de ressources limitées, ont souvent du mal à investir dans des mesures avancées de cybersécurité et dans du personnel qualifié. Ils doivent également se familiariser avec des lois complexes sur la protection des données, ce qui augmente la complexité de garantir la conformité tout en protégeant les informations sensibles. L'augmentation des attaques de phishing et de l'ingénierie sociale montre encore davantage leur vulnérabilité, tout comme le manque de sécurité des réseaux et le risque de menaces internes. La gestion de ces risques est essentielle, mais les PME trouvent souvent difficile une évaluation et une gestion efficaces des risques. De plus, le recours à des fournisseurs tiers introduit un autre niveau de complexité, exposant potentiellement les PME à des menaces de cybersécurité supplémentaires.

2.2. LES FEMMES DANS LA CYBERSÉCURITÉ

Nous avons analysé les besoins de formation et d'accompagnement des femmes, les qualifications et compétences existantes des femmes en cybersécurité et des recommandations pour impliquer davantage de salariées dans les défis de cybersécurité.

Microsoft a réalisé une enquête dans 35 pays européens, selon laquelle moins d'un diplômé en informatique sur cinq était une femme. L'intérêt pour les sciences, la technologie, l'ingénierie et les mathématiques (matières STEM) diminue bien trop tôt. En fait, le Programme international pour le suivi des acquis des élèves (PISA) de l'OCDE révèle que les garçons sont beaucoup plus susceptibles que les filles de s'imaginer comme des professionnels des TIC, des scientifiques ou des ingénieurs. (Microsoft, 2017).

Si l'on examine la part des femmes parmi les spécialistes des TIC ayant un emploi, dans l'UE27, en 2020, seulement 18,5 % de tous les spécialistes des TIC étaient des femmes. Les plus grandes proportions de femmes se trouvaient en Bulgarie – 28,2 %, en Grèce – 26,6 % et en Roumanie – 26,2 % (voir graphique 5 (Women go tech, 2021)). Les pays de la région nordique-baltique se situent également pour la plupart en haut de la liste, à l'exception de la Norvège, qui se situe plutôt au milieu du classement des pays. (Les femmes se lancent dans la technologie, 2021).

Selon le Département des statistiques de la République de Lituanie, le nombre d'employés dans la catégorie de l'information et de la communication au quatrième trimestre 2022 était de 29 400 hommes et 21 500 femmes. Au premier trimestre 2023, il y avait 34,6 mille hommes et 20,7 mille femmes. Pour le deuxième trimestre 2023, il y avait 36,8 mille hommes et 14,8 mille femmes, et au troisième trimestre 2023, les chiffres étaient 34,5 mille hommes et 18,0 mille femmes. Il y a une diminution notable du nombre d'employées féminines entre le premier et le deuxième trimestre 2023, suivie d'une augmentation au troisième trimestre 2023 (Rodiklių Duomenų Bazė - Oficialiosios Statistikos Portalas, s.d.).

Avec jusqu'à 11 % de femmes travaillant dans le domaine de la cybersécurité, une enquête a été réalisée pour connaître l'opinion du public sur les perspectives des femmes dans ce domaine. Dans les conflits, 44,4% des personnes interrogées ont répondu que le nombre de femmes dans le domaine de la cybersécurité devrait se situer entre 30 et 60%. La plus grande partie des personnes interrogées ont répondu que les femmes devraient représenter entre 30 et 60 % des femmes professionnelles (35,2 %). En analysant les réponses par sexe et par tranche d'âge, on constate que les femmes, surtout les plus jeunes (moins de 25 ans et 25-45 ans), pensent le plus souvent que le nombre de femmes devrait être d'environ la moitié. Les jeunes hommes (de moins de 25 ans) pensent que jusqu'à 30 % des femmes devraient être des femmes. On constate que les femmes elles-mêmes ont tendance à voir un nombre beaucoup plus élevé de femmes dans le domaine de la cybersécurité que ce n'est actuellement le cas sur le marché. C'est une bonne nouvelle, car attirer les femmes dans ce domaine contribuerait non seulement à remédier à la pénurie de professionnels, mais augmenterait également la sécurité des organisations elles-mêmes. (Bukauskas et coll., 2022).

Women4Cyber Finlande (W4CFI)

Créée en août 2021, W4CFI est une organisation à but non lucratif visant à augmenter le nombre de femmes employées dans le secteur finlandais de la cybersécurité. Il fait partie de l'initiative plus large Wom-en4Cyber à l'échelle européenne et vise à soutenir une industrie plus diversifiée et plus inclusive en Finlande. W4CFI est impliqué dans diverses activités, notamment en fournissant des conseils, en échangeant des connaissances et en sensibilisant pour accroître et soutenir l'engagement des femmes dans la cybersécurité. Women4Cyber Finlande

Projet du ministère finlandais des transports et des communications et de l'université Aalto

Le ministère finlandais des Transports et des Communications, en collaboration avec l'Université Aalto, développe un programme éducatif visant à faire de la cybersécurité une compétence civique dans l'ensemble de l'Union européenne. Cette initiative met en évidence l'importance croissante de la cybersécurité dans la vie quotidienne et le besoin de sensibilisation et de compétences de tous les citoyens, y compris les femmes. Il souligne le rôle des établissements d'enseignement dans la fourniture d'une éducation et d'une formation accessibles en matière de cybersécurité, ce qui est crucial pour l'autonomisation des femmes dans ce domaine. La Finlande renforce l'enseignement des compétences en cybersécurité dans l'UE. **Digital Skills and Jobs Platform** (europa.eu)

Mouvement « Mimmit koodaa » (Code des femmes)

Cette initiative propose des ateliers, des formations, des opportunités de réseautage, des webinaires et un soutien professionnel. Il se concentre sur la lutte contre les stéréotypes et encourage davantage de femmes à explorer des carrières dans la technologie, y compris la cybersécurité. Cette organisation vise à créer des voies permettant aux femmes d'entrer et d'exceller dans le domaine de la cybersécurité. **Mimmit koodaa**

Dans le paysage belge de la cybersécurité, les femmes représentent 19% des effectifs selon la première étude socio-économique sur le secteur de la cybersécurité en Belgique publiée par Agoria en 2022. Avec la coordination du Ministère belge de l'Économie (SPF Belgique), une politique compétente Les acteurs belges ont élaboré un plan quinquennal en faveur des femmes dans le numérique intitulé « Femmes dans le numérique – Stratégie nationale et intersectionnelle 2021-2026 ». Le plan quinquennal comprend une stratégie commune et intersectorielle basée sur cinq objectifs stratégiques utiles pour lutter contre les préjugés et s'attaquer aux obstacles structurels qui empêchent les femmes de participer à l'économie numérique. Les cinq objectifs sont les suivants :

1. Veiller à ce que davantage de femmes obtiennent un diplôme dans le secteur numérique ; 2. Encourager toutes les femmes à participer au marché du travail numérique et/ou au secteur numérique ; 3. Améliorer la rétention des femmes dans le secteur numérique ; 4. Créer de nouvelles images pour promouvoir le rôle des femmes sur le terrain (à l'écran et hors écran) ; 5. Combler l'écart entre les sexes parmi des groupes cibles spécifiques (**lien vers la stratégie**).

La Fondation Women4Cyber, basée à Bruxelles, organise et soutient un large éventail d'activités destinées aux femmes travaillant ou débutant leur carrière dans la cybersécurité en Belgique et en Europe. En Belgique, la Fondation soutient et coopère avec la section nationale belge (**Women4Cyber Belgium**) dans ces activités. Le Chapitre National Belge compte une vingtaine de membres actifs travaillant sur les initiatives. Les activités, événements et programmes organisés par le Chapitre sont, par exemple : des réunions et événements de networking (virtuels et en personne) tels que le « café virtuel » où le Chapitre Belgique du W4C invite des experts dans divers domaines liés au cyber et parler de la sécurité de l'information ; webinaires et séances d'information ; des programmes de mentorat visant à aider les femmes à améliorer leurs compétences et à faire progresser leur carrière en cybersécurité à tous les niveaux ; des projets et événements en collaboration avec la Coalition belge pour la cybersécurité (comme l'organisation de la **Journée internationale de la femme 2023**) ; promotion de bourses pour des programmes éducatifs liés au cyber, tels que ceux organisés par la Solvay Brussels School of Economics & Management.

En Norvège, il est crucial de remédier à l'écart entre les sexes dans le domaine de la cybersécurité pour constituer une main-d'œuvre résiliente et diversifiée. La proportion de femmes dans l'informatique n'est que de 29 %. Ce faible nombre est étroitement lié au nombre de femmes choisissant des matières mathématiques et techniques au niveau secondaire.

Besoins de formation et de soutien et recommandations pour impliquer les femmes

Il est nécessaire de mettre en place des programmes de cybersécurité sur mesure spécialement conçus pour encourager la participation des femmes. Ces programmes doivent équilibrer les aspects techniques avec les questions de cybersécurité organisationnelles et centrées sur l'humain. Il existe plusieurs formations complémentaires techniques dans le domaine, tandis que les offres de formation continue dans les métiers les plus typiquement féminins (professions pédagogiques et de santé) ne proposent pas de telles offres et le développement d'offres de formation plus courtes en cybersécurité liées à ces métiers permettrait d'atteindre davantage de femmes. Ceci est également soutenu par le secteur lui-même, qui affirme que la diversité peut apporter des perspectives uniques aux défis de cybersécurité. Une sensibilisation accrue des femmes aux carrières internes en cybersécurité pourrait se faire par le biais d'ateliers, de séminaires et de programmes de sensibilisation ciblés dans les écoles et les universités, ce qui pourrait inciter davantage de femmes à se lancer dans ce domaine.

Une autre approche suggérée par bon nombre des 50 meilleures femmes technologiques norvégiennes nominées pour 2022 consiste à établir des programmes de mentorat et des opportunités de réseautage pour les femmes dans le domaine de la cybersécurité afin de leur fournir des conseils et un soutien essentiels, les aidant ainsi à naviguer et à progresser dans ce domaine.

Le secteur de la cybersécurité lui-même suggère que les organisations devraient mettre en œuvre des pratiques et des politiques d'embauche inclusives qui encouragent activement le recrutement et la rétention des femmes dans des postes de cybersécurité. 32 % des femmes

occupant des postes techniques sont souvent « la seule femme présente » au travail, selon le rapport McKinsey « Women in the Workplace 2022 ».

Enfin, la promotion des femmes à des postes de direction dans le domaine de la cybersécurité peut fournir des modèles et inspirer d'autres femmes à suivre des voies similaires, comme par exemple **Mia Landsem.**

En Roumanie, la cybersécurité reste l'un des secteurs technologiques les plus dynamiques et les plus passionnants. Cependant, ce secteur a besoin d'un changement systémique dans la représentation et la rémunération des femmes. Malgré l'intérêt croissant pour le domaine de la cybersécurité, la disparité entre les sexes persiste. Les femmes sont encore largement sous-représentées, alors que la plupart des emplois sont majoritairement masculins. L'avenir de la cybersécurité dépend de la capacité à attirer, retenir et promouvoir davantage de cyberprofessionnels, notamment davantage de femmes.

De nombreuses études ont été réalisées afin de montrer à quel point les femmes sont sous-évaluées partout dans le monde, mais aussi pour faire comprendre à chacun l'importance des femmes dans tous les domaines, et particulièrement dans la cybersécurité. L'extrême différence entre les sexes parmi les employés de la cybersécurité indique que les autres forces en présence ne sont pas du tout égales. Les femmes représentent 39 % de l'effectif global. Ils représentent 38 % des travailleurs occupant des emplois STEM, mais seulement environ 25 % des effectifs en cybersécurité, selon Cybersecurity Ventures.

Divers obstacles empêchent les femmes d'accéder à la cybersécurité. Selon une étude de (ISC)2, une organisation à but non lucratif qui se concentre sur la formation et la certification en cybersécurité, la majorité des femmes qui ont travaillé dans ce domaine signalent une discrimination fondée sur le sexe. Presque toutes les femmes (87 %) ont déclaré avoir subi une discrimination inconsciente, tandis que 19 % ont déclaré avoir été victimes d'une discrimination manifeste. Les femmes ont également cité des retards inexpliqués dans l'avancement de carrière (53 %) et des réponses exagérées aux erreurs (29 %).

La discrimination se manifeste également par un écart de rémunération. (ISC)2 montre que 32 % des hommes travaillant dans le domaine de la cybersécurité gagnent en moyenne entre 50 000 et 100 000 $ par an, tandis que seulement 18 % des femmes dans le domaine de la cybersécurité occupent la même tranche de revenus. Et 25 % des hommes contre 20 % des femmes gagnent entre 100 000 et 500 000 dollars par an.

Il existe de solides arguments en faveur d'une augmentation du nombre de femmes dans la cybersécurité, notamment les avantages de la diversité, de l'innovation, de l'empathie émotionnelle et d'une perspective impartiale, qui sont autant de compétences précieuses pour le lieu de travail en cybersécurité.

Jay Koehler, membre du conseil d'administration de Women in Cybersecurity, a fourni un autre point de vue : « Les femmes abandonnent leurs études parce que c'est un « club de garçons » et il y a un faible sentiment d'appartenance. Ce problème peut être résolu grâce à l'engagement

et à la responsabilisation visant à assurer la sécurité psychologique et un lieu de travail respectueux du genre et en créant des réseaux de femmes.

Il y a de l'espoir que la cybersécurité ne soit plus une « profession à prédominance masculine », mais regorgeant de personnes talentueuses de tous genres et de tous horizons.

La littérature sur la participation des femmes à la cybersécurité en Espagne est rare. La plupart de la littérature existante montre un déséquilibre prononcé entre les sexes dans la communauté scientifique au sens large, y compris dans les disciplines STEM, avec une diminution notable de la progression des femmes vers des niveaux de carrière supérieurs, communément considéré comme un « phénomène de pipeline ». En matière d'enseignement supérieur, l'écart entre les sexes est encore prononcé, puisque seulement 18 % des diplômés dans ces matières sont des femmes. Les femmes employées par les PME pour des postes liés à l'I+D sont encore très faibles, n'atteignant même pas 30% selon les données de l'Institut national de la statistique. En ce qui concerne les femmes chercheuses en cybersécurité dans les EES espagnols, très peu d'entre elles font preuve d'un effectif équilibré en termes de genre. Sur les 31 établissements d'enseignement supérieur examinés par la Fundación Alternativas, 11 d'entre eux ne comptent aucune femme dans leurs équipes de recherche et seuls 5 d'entre eux affichent une main-d'œuvre plus égalitaire. En réponse à ces défis, l'analyse des besoins en formation et en accompagnement identifie les principaux domaines d'amélioration. Des initiatives devraient être développées pour encourager davantage de femmes à poursuivre des études de doctorat et assurer une représentation équilibrée tout au long du parcours éducatif. Il est crucial de lutter contre les préjugés dans les processus d'avancement de carrière, et les programmes de mentorat peuvent jouer un rôle central en guidant les femmes à travers les subtilités du domaine de la cybersécurité. En outre, la collaboration avec des organisations du secteur privé est recommandée pour étudier les trajectoires de carrière et stimuler l'implication des femmes dans des rôles de cybersécurité dans les secteurs privés. L'évaluation des qualifications et des compétences souligne l'importance des programmes de formation personnalisés, mettant l'accent sur les aptitudes et compétences spécifiques en matière de cybersécurité.

2.3. ANALYSE DES OCCUPATIONS DE LA CLASSIFICATION ESCO

Nous interprétons la classification ESCO (Classification multilingue européenne des aptitudes, compétences et professions) existante en ce qui concerne les résultats d'apprentissage identifiés, y compris les connaissances, les aptitudes et les compétences. L'objectif est de

- Analyser les métiers ESCO existants liés à la cybersécurité.
- Cartographier les acquis d'apprentissage identifiés avec les métiers ESCO en termes de connaissances, d'aptitudes, de compétences, etc.

Pour chaque métier, il existe un ensemble de compétences, d'aptitudes et de connaissances. Vous trouverez ci-dessous des définitions et des exemples de compétences, d'aptitudes, de connaissances et de valeurs.

La **compétence** fait référence à la capacité d'un individu à accomplir efficacement une tâche ou un travail spécifique. Il englobe une combinaison de connaissances, de compétences et de comportements appliqués pour améliorer les performances. Exemple : Être compétent en gestion de projet implique une combinaison de compétences organisationnelles, de connaissances des processus de gestion de projet et de capacité à communiquer efficacement avec les membres de l'équipe.

Les **aptitudes** sont des capacités ou des capacités spécifiques acquises par la pratique, la formation ou l'expérience qui permettent à un individu d'effectuer des tâches. Exemple : compétences en matière de tests d'intrusion, capacité à utiliser des outils et des logiciels de cybersécurité, compétences en programmation et capacité à analyser et à répondre aux menaces en temps réel.

La **connaissance** fait référence aux faits, aux informations et à la compréhension acquises grâce à l'éducation ou à l'expérience. Il englobe la compréhension théorique des faits et des principes liés à un domaine particulier. Exemple : Comprendre comment différents types de cyberattaques sont menés (par exemple, phishing, ransomware, attaques DDoS) ou connaissance de diverses méthodes de cryptage et familiarité avec les dernières tendances et développements en matière de cybersécurité

Cette analyse est divisée en 2 phases :

Phase 1 : Examen et sélection des occupations ESCO

Consultation sur le portail ESCO pour filtrer les métiers liés à la cybersécurité et documenter dans la section suivante chaque métier, en accordant une attention particulière aux aptitudes, compétences, connaissances répertoriées.

Titre de l'occupation ESCO	Connaissance	Aptitude	Compétence
3512.3 - Technicien en sécurité TIC	• Réseaux TIC • vecteurs d'attaque matérielle • contre-mesures contre les cyberattaques • Achat de systèmes d'exploitation pour les TIC • équipement réseau • application Web • menaces de sécurité	• aborder les problèmes de manière critique • analyser le système TIC • assurer une bonne gestion des documents • exécuter des tests logiciels et identifier les faiblesses du système TIC	• intégrer les composants du système fournir la documentation technique
2529.1 - responsable de la sécurité des TIC (comprend les personnes exerçant des fonctions de sécurité d'entreprise).	• Risques liés à la sécurité des réseaux TIC • Législation sur la sécurité des TIC • Normes de sécurité des TIC • vecteurs d'attaque • techniques d'audit • contre-mesures contre les cyberattaques • la cyber-sécurité • protection des données • systèmes d'aide à la décision • confidentialité des informations • stratégie de sécurité de l'information • politique interne de gestion des risques • résilience organisationnelle	• sensibiliser à la confidentialité des données • assurer le respect des normes organisationnelles en matière de TIC • assurer le respect des exigences légales • assurer la coopération interdépartementale • garantir la confidentialité des informations • identifier les risques de sécurité des TIC • mettre en œuvre la gestion des risques liés aux TIC • mettre en œuvre des politiques de sécurité des TIC • mettre en œuvre la gouvernance d'entreprise	• diriger des exercices de reprise après sinistre • maintenir le plan de continuité des opérations • gérer les conformités en matière de sécurité informatique • gérer les plans de reprise après sinistre • suivre les évolutions dans le domaine d'expertise • surveiller les tendances technologiques • utiliser le système d'aide à la décision
2529.2 - expert en criminalistique numérique (récupère et analyse les informations provenant	• Risques liés à la sécurité des réseaux TIC • Normes de sécurité des TIC	• appliquer l'ingénierie inverse • développer une stratégie de	• gérer les conformités en matière de sécurité informatique • gérer les données pour les questions

d'ordinateurs et d'autres types de dispositifs de stockage de données ; examine les médias numériques qui peuvent avoir été cachés, cryptés ou endommagés, de manière médico-légale dans le but d'identifier, de préserver, de récupérer, d'analyser et de présenter des faits et des opinions sur les informations numériques.)	• criminalistique informatique • contre-mesures contre les cyberattaques • confidentialité des informations • outil de test d'intrusion • langages de requête • Langage de requête du cadre de description des ressources	sécurité de l'information • sensibiliser à la confidentialité des données • recueillir des données à des fins médico-légales • identifier les risques de sécurité des TIC • identifier les faiblesses du système TIC • mettre en œuvre des outils de diagnostic des réseaux TIC • fournir des conseils en matière de conseil en TIC • sécuriser les informations sensibles des clients • utiliser la programmation de scripts • utiliser un logiciel pour la préservation des données • effectuer des tests de sécurité des TIC	juridiques • effectuer des préservations médico-légales d'appareils numériques
2529.3 - ingénieur en sécurité des systèmes embarqués (les ingénieurs en sécurité des systèmes embarqués se concentrent sur les produits connectés et leurs réseaux de support, et moins sur la sécurité organisationnelle comme pour l'ingénieur en sécurité des TIC.)	• Risques liés à la sécurité des réseaux TIC • Normes de sécurité des TIC • Internet des objets • programmation informatique • contre-mesures contre les cyberattaques • systèmes embarqués • stratégie de sécurité de l'information • anomalies logicielles	• analyser le système TIC • créer un organigramme • définir les politiques de sécurité • développer un pilote de périphérique TIC • développer un prototype de logiciel • exécuter des tests logiciels • identifier les risques de sécurité des TIC	• se tenir au courant des dernières solutions en matière de systèmes d'information • gérer les conformités en matière de sécurité informatique • surveiller les performances du système • effectuer une analyse des risques • rapporter les résultats des tests utiliser des modèles de conception de logiciels • utiliser des

		• identifier les faiblesses du système TIC • interpréter des textes techniques • fournir des conseils en matière de conseil en TIC • effectuer des tests de sécurité des TIC • fournir la documentation technique	bibliothèques de logiciels • utiliser des outils de génie logiciel assistés par ordinateur • définir les exigences techniques
2529.4 - pirate informatique éthique (effectue des évaluations des vulnérabilités de sécurité et des tests d'intrusion conformément aux méthodes et protocoles acceptés par l'industrie ; analyse les systèmes à la recherche de vulnérabilités potentielles pouvant résulter d'une mauvaise configuration du système, de défauts matériels ou logiciels ou de faiblesses opérationnelles)	• vecteurs d'attaque • criminalistique informatique • contre-mesures contre les cyberattaques • éthique • exigences légales des produits TIC • outil de test d'intrusion • anomalies logicielles • outils pour l'automatisation des tests TIC • Menaces de sécurité des applications Web	• effectuer des tests de sécurité des TIC • fournir la documentation technique • développer des exploits de code • exécuter des audits TIC • exécuter des tests logiciels • identifier les risques de sécurité des TIC • identifier les faiblesses du système TIC	• aborder les problèmes de manière critique • analyser le contexte d'une organisation • surveiller les performances du système
2529.5 - Responsable de la résilience des TIC (recherche, planifie et développe des modèles, des politiques, des méthodes, des techniques et des outils qui améliorent la cybersécurité, la résilience et la reprise après sinistre d'une organisation)	• Techniques de récupération des TIC • cybersécurité interne • politique de gestion des risques • résilience organisationnelle • Bonnes pratiques en matière de sauvegarde du système	• élaborer des plans d'urgence pour les situations d'urgence • développer une stratégie de sécurité de l'information • exécuter des audits TIC • identifier les risques de sécurité des TIC • mettre en œuvre un système de récupération des TIC • mettre en œuvre la gestion des risques liés aux TIC	• analyser les processus d'affaires • analyser le contexte d'une organisation • se conformer aux réglementations légales • diriger des exercices de reprise après sinistre • gérer les conformités en matière de sécurité informatique • gérer les plans de reprise après sinistre • gérer la sécurité du système • effectuer des tests de sécurité des TIC
2529.6 - Administrateur de la sécurité des TIC (planifie et	• Risques liés à la sécurité des réseaux TIC	• identifier les faiblesses du système TIC	• appliquer les politiques de l'entreprise

exécute des mesures de sécurité pour protéger les informations et les données contre tout accès non autorisé, attaque délibérée, vol et corruption.)	• Internet des objets • contre-mesures contre les cyberattaques • outils de développement de bases de données • la gouvernance de l'Internet • gestion des appareils mobiles • systèmes d'exploitation • résilience organisationnelle • méthodologies d'assurance qualité • Bonnes pratiques en matière de sauvegarde du système	• interpréter des textes techniques • maintenir la gestion des identités TIC • maintenir la sécurité de la base de données	• veiller à la qualité des systèmes TIC • assurer une bonne gestion des documents • gérer l'architecture des données TIC • gérer les conformités en matière de sécurité informatique • effectuer un dépannage informatique • résoudre les problèmes du système TIC
2529.7 - Ingénieur en sécurité TIC (conseille et met en œuvre des solutions pour contrôler l'accès aux données et aux programmes et assure la protection de la mission et des processus d'affaires de l'organisation.)	• Législation sur la sécurité des TIC • Normes de sécurité des TIC • vecteurs d'attaque • analyse commerciale • contre-mesures contre les cyberattaques • la cyber-sécurité • technologies émergentes • architecture des informations • stratégie de sécurité de l'information • systèmes d'exploitation • résilience organisationnelle • gestion des risques • données non structurées	• développer une stratégie de sécurité de l'information • sensibiliser à la confidentialité des données • assurer la sécurité des informations • exécuter des audits TIC • exécuter des tests logiciels • identifier les risques de sécurité des TIC • identifier les faiblesses du système TIC • mettre en œuvre la gestion des risques liés aux TIC • fournir des conseils en matière de conseil en TIC • analyser le système TIC • définir les politiques de sécurité	• définir des critères de qualité des données • définir les exigences techniques • conserver les enregistrements des tâches • se tenir au courant des dernières solutions en matière de systèmes d'information • gérer les conformités en matière de sécurité informatique • gérer les plans de reprise après sinistre • surveiller les performances du système • effectuer une analyse des données • effectuer une analyse des risques • rapporter les résultats des tests, résoudre les problèmes • vérifier les spécifications formelles des TIC
2529.8 - Responsable de la sécurité des TIC (propose et met en œuvre les mises à jour de sécurité nécessaires ;	• Techniques de gestion des problèmes TIC • Gestion de projet TIC • Politique de qualité des	• définir les politiques de sécurité • développer une stratégie de	• diriger des exercices de reprise après sinistre • maintenir la gestion des identités TIC

conseille, accompagne, informe, forme, sensibilise à la sécurité et agit directement sur tout ou partie d'un réseau ou d'un système.)	TIC • Normes de sécurité des TIC • Exigences des utilisateurs du système TIC • Internet des objets • vecteurs d'attaque • criminalistique informatique • stratégie de sécurité de l'information • politique interne de gestion des risques • la gouvernance de l'Internet • exigences légales des produits TIC	sécurité de l'information • établir un plan de prévention en matière de sécurité des TIC • mettre en œuvre la gestion des risques liés aux TIC	• gérer les conformités en matière de sécurité informatique • gérer les plans de reprise après sinistre • résoudre les problèmes du système TIC
2529.9 - ingénieur des connaissances (intègre des connaissances structurées dans des systèmes informatiques afin de résoudre des problèmes complexes nécessitant normalement un haut niveau d'expertise humaine ou des méthodes d'intelligence artificielle.)	• l'intelligence d'entreprise • modélisation des processus métiers • outils de développement de bases de données • Extraction d'informations • traitement du langage naturel de la structure de l'information • principes de l'intelligence artificielle • Langage de requête du cadre de description des ressources • cycle de vie du développement des systèmes • théorie des systèmes • algorithmisation des tâches • programmation web	• utiliser une interface spécifique à l'application • utiliser des bases de données • utiliser des langages de balisage	• analyser les besoins de l'entreprise • appliquer la théorie des systèmes TIC • évaluer les connaissances en TIC • créer des arbres sémantiques • définir les exigences techniques • gérer l'intégration sémantique des TIC • gérer les connaissances métier • gérer la base de données

Phase 2 : Cartographie des occupations ESCO et des résultats d'apprentissage

Avec le tableau précédent, nous avons analysé les professions documentées et identifié les acquis d'apprentissage associés à chaque rôle. Nous avons utilisé le cadre ESCO pour classer ces résultats en connaissances, aptitudes et compétences.

Un résultat d'apprentissage est une déclaration claire et spécifique qui décrit ce que les élèves sont censés apprendre et être capables de faire à la fin d'une période d'enseignement. L'énoncé comprend des connaissances, des compétences et des attitudes.

Dans la section de classification des professions ESCO, les professionnels des technologies de l'information et des communications sont divisés en deux sous-sections : les développeurs et analyses de logiciels et d'applications et les professionnels des bases de données et des réseaux. Ce dernier est constitué de quatre groupes : Professionnels des bases de données et des réseaux, Administrateurs de systèmes, Professionnels des réseaux informatiques et Professionnels des bases de données et des réseaux non classés ailleurs. Toutes les professions en cybersécurité présentées dans le tableau se retrouvaient dans ce groupe de base. Par exemple, le groupe comprend des spécialistes de la sécurité des technologies de l'information et des communications.

Dans de tels cas, les tâches comprendraient :

(a) élaborer des plans pour protéger les fichiers informatiques contre toute modification, destruction ou divulgation accidentelle ou non autorisée et pour répondre aux besoins urgents de traitement des données.

(b) former les utilisateurs et promouvoir la sensibilisation à la sécurité afin de garantir la sécurité du système et d'améliorer l'efficacité des serveurs et du réseau.

(c) s'entretenir avec les utilisateurs pour discuter de questions telles que les besoins d'accès aux données informatiques, les violations de sécurité et les modifications de programmation.

(d) surveiller les rapports actuels sur les virus informatiques pour déterminer quand mettre à jour les systèmes de protection antivirus.

(e) modifier les fichiers de sécurité informatique pour incorporer de nouveaux logiciels, corriger des erreurs ou modifier le statut d'accès individuel.

(f) surveiller l'utilisation des fichiers de données et réglementer l'accès pour protéger les informations contenues dans les fichiers informatiques.

(g) effectuer des évaluations des risques et exécuter des tests du système de traitement des données pour garantir le fonctionnement des activités de traitement des données et les mesures de sécurité.

(h) chiffrer les transmissions de données et ériger des pare-feu pour dissimuler les informations confidentielles lors de leur transmission et empêcher les transferts numériques corrompus d'entrer.

Description des résultats d'apprentissage pour chaque occupation :

Occupation	Résultats d'apprentissage
Technicien en sécurité TIC (3512.3)	• Démontrer une compréhension globale des réseaux TIC, des vecteurs d'attaque matérielle, des contre-mesures contre les cyberattaques et des systèmes d'exploitation. • Analyser et diagnostiquer de manière critique les vulnérabilités des systèmes TIC afin d'améliorer la sécurité du système. • Mettre en œuvre et gérer des stratégies robustes de gestion de documents qui respectent les protocoles de sécurité des TIC. • Développer et exécuter des plans de tests logiciels détaillés pour identifier et corriger les vulnérabilités logicielles. • Intégrer les composants du système et utiliser un logiciel de contrôle d'accès pour créer des systèmes TIC sécurisés et efficaces.
Responsable de la sécurité des TIC (2529.1)	• Comprendre et analyser les risques, la législation et les normes de sécurité des réseaux TIC pour protéger les informations organisationnelles. • Élaborer et mettre en œuvre des stratégies de sécurité de l'information et des politiques internes de gestion des risques. • Diriger les exercices de reprise après sinistre et maintenir les plans de continuité opérationnelle. • Éduquer le personnel sur la confidentialité des données et assurer la coopération entre les départements pour des pratiques de sécurité améliorées.
Expert en criminalistique numérique (2529.2)	• Analyser et tester la sécurité des systèmes embarqués, notamment dans l'environnement Internet des objets (IoT). • Développer et exécuter des prototypes et des tests de logiciels et utiliser des outils d'ingénierie logicielle assistés par ordinateur. • Gérer les conformités en matière de sécurité informatique et effectuer une analyse des risques et une surveillance des performances du système. • Définir et mettre en œuvre les politiques de sécurité et les exigences techniques pour les systèmes embarqués.

Ingénieur en sécurité des systèmes embarqués (2529.3)	• Analyser et tester la sécurité des systèmes embarqués, notamment dans l'environnement Internet des objets (IoT). • Développer et exécuter des prototypes et des tests de logiciels et utiliser des outils d'ingénierie logicielle assistés par ordinateur. • Gérer les conformités en matière de sécurité informatique et effectuer une analyse des risques et une surveillance des performances du système. • Définir et mettre en œuvre les politiques de sécurité et les exigences techniques pour les systèmes embarqués.
Pirate informatique éthique (2529.4)	• Effectuer des évaluations des vulnérabilités de sécurité et des tests d'intrusion à l'aide de méthodes acceptées par l'industrie. • Identifier et exploiter les vulnérabilités potentielles des systèmes pour améliorer les mesures de sécurité. • Développer des exploits de code et exécuter des audits TIC pour garantir l'intégrité du système. • Analyser le contexte d'une organisation pour adapter efficacement les stratégies de sécurité
ICT Resilience Manager (2529.5)	• Élaborer et mettre en œuvre des plans d'urgence et des stratégies de sécurité de l'information pour les scénarios d'urgence. • Mettre en œuvre et gérer des systèmes de récupération des TIC et des processus de gestion des risques. • Diriger des exercices de reprise après sinistre et gérer la sécurité du système pendant les crises. • Analyser les processus métier pour améliorer la résilience organisationnelle et la conformité aux réglementations légales.
ICT Security Administrator (2529.6)	• Planifier et mettre en œuvre des mesures de sécurité pour protéger les données et gérer les systèmes d'identité TIC. • Maintenir la sécurité des bases de données et garantir l'intégrité et la résilience du système. • Résoudre les problèmes du système TIC et appliquer des méthodologies de dépannage et d'assurance qualité. • Gérer l'architecture des données et respecter les politiques organisationnelles en matière de protection des données.
ICT Security Engineer (2529.7)	• Conseiller et mettre en œuvre des solutions pour contrôler l'accès aux données et protéger les processus métier.

	• Analyser les systèmes TIC et définir des politiques de sécurité et des critères de qualité des données. • Effectuer des analyses de données et des risques, et gérer les conformités en matière de sécurité informatique et les plans de reprise après sinistre. • Se tenir au courant des technologies émergentes et des solutions de systèmes d'information
Responsable de la sécurité des TIC (2529.8)	• Proposer et mettre en œuvre des mises à jour de sécurité et gérer la sécurité des TIC dans divers projets. • Diriger des exercices de reprise après sinistre et établir des plans de prévention de la sécurité des TIC. • Maintenir et gérer les systèmes de gestion des identités TIC et résoudre les problèmes système complexes. • Élaborer et mettre en œuvre des stratégies de sécurité de l'information et gérer les plans de reprise après sinistre.
Ingénieur des connaissances (2529.9)	• Intégrer des connaissances structurées dans les systèmes informatiques à l'aide d'outils avancés tels que le langage de requête RDF et la programmation Web. • Gérer l'intégration sémantique et les systèmes de bases de données pour améliorer la gestion des connaissances commerciales. • Analyser les exigences commerciales et appliquer la théorie des systèmes TIC pour développer des bases de connaissances efficaces. • Créer des arbres sémantiques et évaluer les connaissances en TIC pour résoudre des problèmes complexes à l'aide de méthodes d'IA.

3. ANALYSE ET RÉSULTATS

3.1. ANALYSE DE LA RECHERCHE SUR LE TERRAIN

Analyse de l'enquête de terrain sur l'enseignement supérieur et les EFP

Les données de l'enquête « Cartographie des besoins de formation des agents de changement en matière de cybersécurité des PME » contiennent une série de questions axées sur la formation en cybersécurité dans le contexte de l'enseignement et de la formation professionnels (EFP) et des établissements d'enseignement supérieur (EES). Nous avons collecté des données sur des sujets inclus dans la formation en cybersécurité, les méthodes d'enseignement, l'inclusion du genre et les données démographiques des répondants.

L'objectif de cette étude est d'analyser les réponses pour comprendre l'état actuel de la formation en cybersécurité, les méthodologies utilisées et les perceptions autour de l'inclusivité et de l'efficacité dans ce domaine.

L'analyse des réponses sera basée sur la structure clé suivante :

- Données démographiques
- Programme d'études, besoins de formation et préférences d'apprentissage
- Exigences de compétences et compétences futures
- Informations spécifiques au genre

Données démographiques:

La répartition par sexe parmi les répondants à l'enquête entre les établissements d'enseignement et de formation professionnels (EFP) et les établissements d'enseignement supérieur est la suivante :

Nombre total de réponses par type d'institution :

Type d'institution	Réponses	Femme	Homme	Non renseigné
Enseignement supérieur	104	28	73	3
EFP	86	36	48	2
Total	**190**	**64**	**121**	**5**

Même s'il existe un déséquilibre entre les sexes dans les établissements d'enseignement supérieur et d'EFP, l'écart est plus étroit dans les établissements d'EFP. Afin de fournir une image plus claire de la représentation des sexes par rapport au nombre total de réponses de chaque établissement et d'ajuster les résultats concernant le nombre de biais de réponse, nous avons calculé le pourcentage de chaque sexe au sein des deux types d'établissements.

Répartition des réponses par type d'institution

Type d'institution	Femme %	Homme %	Non renseigné %	Total
Enseignement supérieur	27	70	3	**100%**
EFP	42	56	2	**100%**

Même s'il existe un déséquilibre entre les sexes dans les établissements d'enseignement supérieur et d'EFP, l'écart est plus étroit dans les établissements d'EFP. Afin de fournir une image plus claire de la représentation des sexes par rapport au nombre total de réponses de chaque établissement et d'ajuster les résultats concernant le nombre de biais de réponse, nous avons calculé le pourcentage de chaque sexe au sein des deux types d'établissement. 'établissements.

Programme d'études, besoins de formation et préférences d'apprentissage

Sujet inclus dans les formations existantes en cybersécurité de l'enseignement supérieur et de l'EFP

Sujets	Réponses	Enseignement supérieur	EFP
Fondamentaux de la cybersécurité	151	90	61
Sécurité des réseaux	123	72	51
Analyse et gestion des menaces	99	65	34
Cryptographie	92	57	35
Réponse aux incidents	82	49	33
Gestion des risques	77	43	34
Lois et politiques sur la cybersécurité	73	42	31
Techniques avancées d'atténuation des menaces	54	33	21

Il apparaît que les connaissances et compétences fondamentales ainsi que la sécurité des réseaux sont une priorité. L'analyse et la gestion des menaces, la cryptographie et la réponse aux incidents suggèrent une couverture complète des menaces de cybersécurité dans les formations. Les lois et politiques en matière de gestion des risques et de cybersécurité, même si elles soulignent la nécessité d'une approche holistique incluant la compréhension du contexte juridique et la gestion efficace des risques, ne sont pas toujours retenues. Il est intéressant de noter que les techniques avancées d'atténuation des menaces sont moins incluses dans les formations.

Afin de fournir les résultats sans le biais introduit par le nombre de répondants de chaque type d'établissement (EES et EFP), les données ont été normalisées par le nombre total de réponses pour chaque type d'établissement. Cette approche nous permet de voir la proportion d'institutions qui incluent chaque sujet dans leurs programmes de formation en cybersécurité.

Sujets	Enseignement supérieur	EFP
Fondamentaux de la cybersécurité	15.76%	15.48%
Sécurité des réseaux	12.61%	12.94%
Analyse et gestion des risques	11.38%	8.63%
Cryptographie	9.98%	8.88%
Réponse aux incidents	8.58%	8.38%
Gestion des risques	7.53%	8.63%
Lois et politiques sur la cybersécurité	7.36%	7.87%
Techniques avancées d'atténuation des menaces	5.78%	5.33%

Il est intéressant de noter qu'il existe des priorités similaires avec de légères variations. Les établissements d'enseignement supérieur et d'EFP accordent une importance particulière aux « fondamentaux de la cybersécurité » et à la « sécurité des réseaux ». Cela indique que ces sujets sont reconnus comme des éléments essentiels de l'éducation à la cybersécurité. Les proportions sont très similaires, les « fondamentaux de la cybersécurité » étant légèrement plus mis en avant dans les établissements d'enseignement supérieur que dans les établissements d'enseignement professionnel et la « sécurité des réseaux » présentant une tendance similaire mais avec un écart plus étroit.

Il existe une variation notable dans l'accent mis sur des sujets plus spécialisés tels que « Analyse et gestion des menaces », « Cryptographie » et « Techniques avancées d'atténuation des menaces ». Les EES ont tendance à consacrer une proportion légèrement plus élevée de leurs programmes de formation à ces sujets que les établissements d'EFP. Cela peut s'expliquer par le fait que les établissements d'enseignement supérieur s'efforcent de fournir une compréhension plus complète et plus théorique de la cybersécurité, qui comprend souvent un éventail plus large de sujets spécialisés. En revanche, les établissements d'EFP, tout en couvrant un large éventail de sujets, peuvent donner la priorité aux applications pratiques et à la préparation immédiate à l'emploi.

Méthodes d'enseignment

Méthodes d'enseignment	Enseignment supérieur	EFP
Etudes de cas	60.91%	39.09%
Travaux de groupe	58.95%	41.05%
Cours pratiques	59.02%	40.98%
Cours magistraux	56.97%	43.03%
Classe inversée	34.78%	65.22%
Simulations en ligne	51.35%	48.65%

Les méthodes d'études de cas, de projets de groupe, de cours pratiques et de cours magistraux sont largement utilisées dans les deux types d'établissements, avec une préférence dans les établissements d'enseignement supérieur plutôt que dans l'EFP. En ce qui concerne la méthode de classe inversée, elle est plus répandue dans l'EFP (65,22 %) que dans les établissements d'enseignement supérieur (34,78 %), ce qui indique une tendance vers un modèle d'apprentissage interactif dans l'enseignement professionnel. Les classes inversées

donnent la priorité à l'apprentissage actif et à l'engagement des étudiants, qui correspondent bien à l'approche pratique et basée sur les compétences caractéristique de l'EFP.

Efficacité des méthodes d'enseignment

Méthodes d'enseignement	Nombre
Session pratiques	141
Workshop en présentiel	134
Simulations interractives	104
Cours en ligne	100
Tutoriels vidéos	73
Webinaires	68

Cet aperçu met en évidence une diversité de méthodes d'enseignement privilégiées, mais en mettant clairement l'accent sur des expériences d'apprentissage pratiques, interactives et flexibles. Les séances pratiques et les ateliers en personne sont très appréciés car ils offrent une expérience d'apprentissage interactive et pratique. Les simulations interactives et les cours en ligne ont également reçu des mentions significatives démontrant l'importance des modalités d'apprentissage accessibles.

Les défis auxquels sont confrontés les établissements scolaires

Interrogés sur les principaux défis auxquels sont confrontées les institutions scolaires, voici une synthèse des sujets les plus récurrents :

- **Diversité des compétences et de l'expérience des participants** : les formateurs sont confrontés à des difficultés en raison de la diversité des antécédents et des niveaux d'expertise des participants. Il est difficile d'adapter la formation à l'ensemble du groupe et de garantir que les individus techniques et non techniques puissent bénéficier des sessions.
- **Maintenir le matériel de cours à jour** : L'évolution rapide des menaces de cybersécurité nécessite une mise à jour continue du matériel de formation et des méthodes d'enseignement pour garantir leur pertinence.
- **Contraintes de formation pratique :** Il existe un défi important à fournir une expérience pratique. Les limites incluent des installations de laboratoire insuffisantes, le manque de capacités de simulation dans le monde réel et la difficulté de créer des scénarios réalistes de cyberattaques pour la pratique.
- **Limitations des ressources** : les formateurs doivent souvent faire face à des ressources financières limitées, au manque de personnel qualifié, à du matériel d'étude obsolète et à l'insuffisance des outils matériels et logiciels nécessaires à une formation efficace.
- **Engagement et motivation des étudiants** : il est difficile de maintenir l'attention des étudiants et de les motiver à participer activement à leur apprentissage, en particulier avec la nécessité de couvrir un contenu technique complexe et parfois aride.

- **Programme d'études et structure éducative** : il est nécessaire de disposer de programmes d'études complets et multidisciplinaires couvrant tous les aspects de la cybersécurité. Par ailleurs, l'intégration de la cybersécurité dans les programmes scolaires, notamment au niveau secondaire, reste un défi de taille.
- **Accès aux outils et technologies à jour** : fournir aux étudiants l'accès aux derniers outils et technologies de cybersécurité pour un apprentissage pratique est souvent un défi, ce qui est crucial pour la compréhension pratique.
- **Problèmes de langue et de localisation** : les ressources en matière de cybersécurité peuvent ne pas toujours être disponibles dans la langue maternelle des étudiants, ce qui ajoute une couche de complexité à la formation dans les régions non anglophones.
- **Alignement entre l'industrie et l'éducation :** équilibrer la nécessité d'enseigner les bases théoriques avec les compétences pratiques qui correspondent aux besoins de l'industrie est un défi. Il est également nécessaire de préparer les étudiants au marché du travail avec les compétences pertinentes.
- **Capacité et développement des enseignants** : Il est crucial mais difficile de garantir que les éducateurs disposent de connaissances à jour et sont capables de transmettre efficacement des concepts complexes.

Alignement sur les besoins spécifiques des PME

Option de réponse	Nombre
Neutre	82
Aligné	67
Légèrement non aligné	19
Un peu aligné	17
Non aligné	5

La majorité des réponses indiquent un alignement neutre, suggérant qu'il existe une marge d'amélioration sur ce point. Un nombre important de personnes interrogées ont évalué leurs programmes comme étant alignés, tandis que très peu d'éducateurs estiment que leurs programmes sont fortement alignés ou non sur les besoins de l'industrie. Les réponses à l'extrémité inférieure de l'échelle (Pas aligné et légèrement pas aligné) reflètent les préoccupations ou les défis liés à l'alignement complet du contenu éducatif avec la nature évolutive de la cybersécurité dans le secteur. Cette répartition des réponses montre que le défi consistant à garantir une éducation à la cybersécurité adaptée aux tendances et aux exigences du secteur est toujours d'actualité. Il souligne la pertinence du projet CyberAgent qui vise à fournir des mises à jour continues des programmes, des partenariats industriels et des opportunités de formation pratique pour améliorer l'alignement des programmes de formation en cybersécurité avec les besoins du secteur de la cybersécurité.

Sujets spécifiques aux PME

Sujet/Compétence	Nombre
Cybersécurité de base pour les PME	91
Protection des données et confidentialité pour les PME	75
Aucun sujet ou compétence spécifique aux PME n'est inclus dans le programme	**64**
Réponse aux incidents pour les PME	58
Analyse et gestion des risques dans le contexte des PME	53
Développement d'une politique de cybersécurité pour les PME	46

L'accent est fortement mis sur les principes fondamentaux de la cybersécurité et de la protection des données. Les sujets les plus fréquemment mentionnés, Cybersécurité de base pour les PME et Protection des données et de la vie privée pour les PME, indiquent que les éducateurs donnent la priorité à doter les PME des connaissances nécessaires pour protéger leurs données et comprendre les concepts de base de la cybersécurité. Le chiffre « Aucun sujet ou compétence spécifique aux PME n'est inclus dans le programme » indique une lacune dans certains programmes de formation en cybersécurité en ce qui concerne le contenu adapté aux petites et moyennes entreprises (PME). Il met en évidence un domaine critique à améliorer dans les formations en cybersécurité, en particulier compte tenu des défis et des menaces auxquelles sont confrontées les PME.

Les PME fonctionnent souvent avec des ressources limitées et peuvent ne pas avoir accès à une expertise spécialisée en cybersécurité, ce qui les rend particulièrement vulnérables aux cybermenaces. L'absence de contenu spécifique aux PME dans les programmes de formation en cybersécurité suggère que ces programmes ne répondent peut-être pas pleinement aux besoins distincts des PME, laissant potentiellement une lacune dans leur préparation et leur résilience face aux cyberattaques. Combler cette lacune nécessite l'intégration de sujets et de compétences spécifiquement conçus pour répondre aux besoins des PME en matière de cybersécurité, tels qu'une évaluation des risques adaptée aux opérations des petites entreprises, des pratiques de cybersécurité rentables et des stratégies pour développer une politique de cybersécurité efficace avec des ressources limitées.

Déficit de compétences chez les salariés des PME

Compétence/Sujet	Nombre
Détection et réponse aux menaces	103
Expertise en sécurité du Cloud	87
Réponse aux incidents et récupération	69
Confidentialité et protection des données	67
Gestion et analyse des risques	63
Technologies émergentes	58
Sécurité des réseaux	41
Connaissances en matière de conformité et de réglementation	36

L'analyse révèle que les employés manquent de compétences dans des domaines clés, la détection et la réponse aux menaces étant les plus fréquemment mentionnées. Cela souligne

l'importance de préparer les étudiants à identifier et à répondre aux menaces de cybersécurité en tant que capacité essentielle dans ce domaine. L'expertise en matière de sécurité du cloud arrive en deuxième position, démontrant la dépendance aux technologies cloud et la nécessité de connaissances spécialisées pour sécuriser les environnements cloud des employés. La réponse aux incidents et la récupération, la confidentialité et la protection des données, ainsi que la gestion et l'analyse des risques sont également valorisées. On considère qu'en ce qui concerne les technologies émergentes, la nécessité de se tenir au courant des dernières avancées dans le domaine n'est pas un domaine déficitaire. Idem pour la sécurité des réseaux qui est un domaine fondamental qui fait partie de la plupart des programmes de formation en cybersécurité. Cela montre l'efficacité des formations sur ce point.

Menaces

Menaces	Nombre
Cyberattaques pilotées par l'IA	117
Attaques de rançongiciels	96
Phishing and ingénérie sociale	87
Failles de sécurité dans le Cloud	82
Vulnérabilités de l'IoT	75
Menaces Deepfake	51
Menaces internes	25

L'analyse révèle que l'accent est mis sur les cyberattaques basées sur l'IA, qui constituent la menace de cybersécurité émergente la plus fréquemment mentionnée, ce qui indique une préoccupation quant à la sophistication et à la complexité des cybermenaces alimentées par l'intelligence artificielle. Les attaques de ransomwares, de phishing et d'ingénierie sociale occupent également une place importante, démontrant la présence de ces vecteurs d'attaque pour les PME. Les failles de sécurité du cloud et les vulnérabilités de l'IoT mettent en lumière les préoccupations liées à la sécurité des services cloud et à l'expansion de l'Internet des objets, reflétant les défis liés à la protection d'écosystèmes technologiques diversifiés et distribués pour les PME. Les menaces Deepfake et les menaces internes ne sont pas considérées comme de grands vecteurs de menace. Des programmes de formation couvrant les 5 principaux sujets peuvent mieux équiper les étudiants et les employés des PME pour faire face aux menaces rencontrées.

Tendances émergentes

Domaine	Nombre
IA et apprentissage automatique en cybersécurité	160
Identité numérique et confidentialité	96
Piratage éthique et compétences défensives	82
Menaces de l'informatique quantique	67
Systèmes de sécurité décentralisés (par exemple, Blockchain)	52
Focus sur les soft skills et la formation interdisciplinaire	47

L'accent est fortement mis sur l'IA et l'apprentissage automatique dans la cybersécurité, domaine le plus fréquemment mentionné, reflétant l'importance de ces technologies dans l'amélioration des mesures de cybersécurité et le besoin de professionnels compétents dans ces domaines. L'identité numérique et la confidentialité constituent un autre objectif important soulignant l'importance de protéger les identités numériques et de garantir la confidentialité. Le score de piratage éthique et de compétences défensives indique une demande de compétences pratiques et pratiques qui permettent aux professionnels d'identifier les vulnérabilités et de se défendre efficacement contre les attaques. Les menaces liées à l'informatique quantique, les systèmes de sécurité décentralisés, tels que la technologie blockchain, ainsi que les compétences générales et la formation interdisciplinaire, n'ont pas été considérés comme des tendances émergentes. La répartition des réponses met en évidence la diversité du domaine de la cybersécurité et l'importance de préparer des professionnels dotés d'un ensemble diversifié de compétences et de connaissances pour relever les défis actuels et futurs. Mais le sujet de l'IA figure en tête de liste.

Egalité des sexes

Pourcentage de femmes	Nombre de réponses
Moins de 10%	57
10% - 25%	79
26% - 50%	43
51% - 75%	8
Plus de 75%	3

Le pourcentage de femmes dans les programmes de formation en cybersécurité révèle une disparité dans la diversité des genres, la majorité des réponses montrant une faible participation féminine. Dans le détail, 79 réponses ont placé la participation des femmes entre 10 % et 25 %, et 57 réponses ont indiqué qu'elle était inférieure à 10 %. Un niveau modéré de diversité des genres est suggéré dans certains programmes, 43 répondants estimant le taux de participation des femmes entre 26 % et 50 %. Cependant, les programmes avec un pourcentage élevé de participantes sont particulièrement rares, comme en témoignent seulement 8 réponses indiquant une fourchette de 51 % à 75 %, et un nombre minimal de 3 réponses estimant plus de 75 %. Ces données soulignent le défi que représente la réalisation de la diversité des genres dans les programmes de formation en cybersécurité, mettant en évidence un écart substantiel dans la participation des femmes dans la plupart des programmes signalés.

Initiatives en faveur de l'égalité des sexes

Réponses	Nombre de réponses
Oui	30
Non	160

Les données indiquent qu'une majorité significative des personnes interrogées, 160 au total, n'utilisent pas d'initiatives ou de stratégies spécifiques pour encourager la participation des femmes à la formation en cybersécurité. Seules 30 personnes interrogées ont confirmé la mise

en œuvre de telles mesures. Cela suggère que même s'il existe une certaine prise de conscience et des efforts visant à accroître la participation des femmes à la formation en cybersécurité par le biais d'initiatives ciblées, la majorité des programmes ne donnent pas encore la priorité ou ne mettent pas en œuvre de stratégies spécifiques pour aborder la diversité des genres. Ce manque d'initiatives ciblées pourrait contribuer aux faibles pourcentages de participation des femmes, comme indiqué dans les réponses à la question précédente.

Gender inclusive training

Réponse	Nombre de réponses
Oui	47
Non	44
Ne sais pas	72
Ne me concerne pas	27

Les résultats suggèrent une opinion partagée parmi les répondants concernant la disponibilité de modules de formation intégrant le genre en matière de cybersécurité. Le groupe le plus important, composé de 72 répondants, a exprimé son incertitude (« Incertain »), indiquant un manque de consensus clair ou de connaissances sur la présence de documents tenant compte du genre. Il existe une répartition presque égale entre ceux qui pensent qu'il existe suffisamment de modules inclusifs sur le genre (47 réponses) et ceux qui ne le pensent pas (44 réponses). De plus, 27 personnes interrogées ont estimé que la question n'était pas pertinente par rapport à leur expérience ou à leur contexte.

Cette division reflète le débat en cours et les perceptions variées sur l'inclusivité du contenu de la formation en cybersécurité. Le nombre élevé de réponses élémentaires met en évidence une lacune potentielle en termes de sensibilisation ou d'accessibilité aux ressources de formation inclusives en matière de genre au sein de l'écosystème d'éducation et de formation en cybersécurité.

Obstacles à l'inclusion des femmes

Barrière	Nombre
Stéréotypes et normes culturelles	107
Manque de sensibilisation aux opportunités dans la cybersécurité	86
Manque de programme de mentorat et de modèles	74
Défis liés à l'équilibre travail-vie personnelle	60
Préjugés perçus dans l'industrie	58

Les obstacles les plus importants à la participation des femmes à la cybersécurité, tels que perçus par les personnes interrogées, sont les stéréotypes ou les normes culturelles (107 mentions) et le manque de sensibilisation aux opportunités en matière de cybersécurité (86 mentions). Ces deux obstacles suggèrent que les perceptions sociétales et le manque d'informations sur les parcours professionnels entravent considérablement l'entrée des femmes dans le domaine de la cybersécurité. Le manque de mentorat ou de modèles de rôle et les problèmes d'équilibre entre travail et vie privée constituent également des obstacles

importants, soulignant l'importance des réseaux de soutien et des environnements de travail flexibles pour encourager la participation des femmes. De plus, les préjugés sexistes perçus dans l'industrie soulignent la nécessité de changements culturels et systémiques dans le domaine pour le rendre plus accueillant et plus équitable pour les femmes.

Programme spécifique pour promouvoir la diversité et l'inclusion

Réponses	Nombre de réponses
Oui	44
Non	85
Ne sais pas	61

Les données révèlent qu'une partie importante des institutions interrogées, avec 85 réponses, n'ont pas mis en place de politiques ou de programmes spécifiques pour promouvoir la diversité et l'inclusion des femmes dans la formation en cybersécurité. Parallèlement, 44 personnes interrogées ont indiqué que leurs institutions mettaient en œuvre de telles initiatives, soulignant une approche visant à aborder la diversité des genres dans ce domaine. Cependant, un nombre notable de personnes interrogées, 61, ne savent pas si leurs institutions disposent de telles politiques ou programmes, ce qui souligne un manque potentiel de communication ou de sensibilisation concernant les efforts existants en matière de diversité et d'inclusion. En outre, cette réponse mitigée suggère que même si certains établissements prennent des mesures pour inclure l'inclusion dans la formation en cybersécurité, un écart important demeure, à la fois dans la mise en œuvre de programmes de diversité et dans la sensibilisation à de telles initiatives parmi les professeurs, le personnel et les étudiants.

Suggestions d'améliorations

Suggestion	Nombre
Visibilité accrue des professionnelles en cybersécurité à succès	95
Davantage de formatrices ou enseignantes en cybersécurité	89
Offrir des bourses	81
Opportunitées de mentorat	49
Contenu de formation évitant les préjugés sexistes	33
Mettre régulièrement à jour les politiques pour soutenir l'inclusivité	31
Etudes de cas et scenarios inclusifs en matière de genre	24
Programmes de formation sur mesure	21
Plus de formations réservées aux femmes	18

L'analyse des réponses concernant les suggestions visant à rendre la formation à la cybersécurité plus inclusive en matière de genre révèle un fort consensus sur l'importance de plusieurs stratégies clés. La suggestion la plus soutenue, avec 95 mentions, est la visibilité accrue des professionnelles de la cybersécurité qui réussissent. Cela souligne le rôle essentiel des modèles et des personnalités ambitieuses pour inciter les femmes à poursuivre une carrière dans la cybersécurité. Juste derrière, avec 89 mentions, se trouve l'appel à davantage de femmes formatrices ou formatrices en cybersécurité, soulignant la nécessité d'une

représentation au sein du personnel éducatif. Offrir des bourses ou des incitations, recevant 81 mentions, est identifié comme crucial pour rendre le domaine plus accessible financièrement et plus attrayant pour les femmes. Les opportunités de mentorat, notées par 49 répondants, soulignent l'importance des conseils et du soutien de professionnels expérimentés dans le domaine. La nécessité d'un contenu de formation qui évite les préjugés sexistes et de politiques régulièrement mises à jour pour soutenir l'inclusivité souligne la nécessité d'ajuster les programmes et les politiques qui reflètent et promeuvent la diversité.

Analyse de l'enquête de terrain sur les PME

Données démographiques :

L'enquête a reçu des réponses des pays partenaires. La Roumanie compte le plus grand nombre de répondants (28), suivie de la Norvège (23), puis de la Lituanie, de l'Espagne et de la Belgique, avec chacune 21 répondants. La Finlande et la Turquie ont également un nombre important de réponses, avec 20 chacune, et la Pologne suit de près avec 19 répondants.

Secteur d'activité

Secteur d'activité	Nombre
IT	18
Education	6
Construction	4
Consultance	4
Cybersecurité	4

Les données indiquent une forte représentation du secteur informatique, avec 18 personnes interrogées identifiant leur entreprise comme opérant dans ce secteur. Les secteurs de l'éducation, de la construction, du conseil et de la cybersécurité ont également des représentations notables, chacun avec des chiffres allant de 4 à 6. Au-delà des cinq premiers, il existe une longue queue de secteurs avec moins de chiffres, illustrant l'approche large de l'enquête dans diverses industries.

Profil des répondants

Poste dans l'entreprise	Nombre
Manager	48
Dirigeant/Propriétaire	35
Technique (Ingénieur/Développeur/Analyste)	27
Autre	25
Coordinateur/Administrateur	8
Vente/Marketing	8
Spécialiste/Expert	8
Employé	8
Consultant	3
Education/Enseignement	2
Finance/Comptabilité	1
Gestion de projet	1
Ressources Humaines	1
Total	**175**

Il existe une grande variété de titres de poste avec un public professionnel diversifié et un large panel de postes tels que « Employé » et « Directeur » qui indique un large éventail de répondants, couvrant différents niveaux au sein des hiérarchies organisationnelles. La cybersécurité est une question transversale qui implique des individus occupant différents rôles et responsabilités au sein des entreprises.

Genre

La répartition par sexe parmi les répondants révèle une représentation plus élevée d'hommes (102) que de femmes (69), une petite partie des répondants (4) préférant ne pas divulguer leur sexe. Cette répartition suggère un écart entre les sexes dans le domaine représenté par l'enquête, qui reflète des tendances plus larges au sein des secteurs de la cybersécurité et de la technologie, où la domination masculine est souvent signalée. Cependant, le nombre important de femmes interrogées indique une participation significative des femmes dans ce domaine, révélant des changements en cours dans la diversité des genres dans le secteur. Si l'écart entre les sexes est évident, la diversité des réponses témoigne également d'une évolution progressive du paysage de la cybersécurité.

Répartition par pays

Pays	Femme	Homme	Non renseigné
Belgique	10	10	1
Finlande	9	11	0
Lituanie	9	12	0
Norvège	8	15	0
Pologne	8	9	2
Roumanie	12	16	0
Espagne	6	14	1
Türkiye	7	13	0

Le tableau montre la répartition par sexe dans différents pays. Les hommes interrogés sont plus nombreux que les femmes dans tous les pays, ce qui est cohérent avec la répartition globale par sexe évoquée précédemment. Cependant, l'écart varie selon les pays, certains pays comme la Belgique affichant un nombre égal d'hommes et de femmes interrogés (10 chacun) et la Pologne ayant une répartition plus étroite entre hommes (9) et femmes (8), un petit nombre de répondants préférant ne dites pas leur sexe (2). Des pays comme la Roumanie et la Norvège comptent globalement un nombre plus élevé de répondants et maintiennent un ratio hommes/femmes plus élevé. Cette répartition par sexe et pays permet une compréhension nuancée de la composition démographique des personnes interrogées, mettant en évidence à la fois les disparités entre les sexes et la diversité géographique dans le domaine de la cybersécurité.

Taille de l'entreprise

Taille de l'entreprise	Nombre
Jusqu'à 10 employés	64
11-50	60
51-250	51

Les réponses à l'enquête indiquent un nombre important de petites et moyennes entreprises parmi les participants. Le groupe le plus important est constitué des entreprises comptant jusqu'à 10 salariés (64 répondants), suivies de près par celles de 11 à 50 salariés (60 répondants), puis par les entreprises de 51 à 250 salariés (51 répondants).

La prédominance des petites entreprises parmi les répondants souligne l'importance de solutions de cybersécurité sur mesure qui répondent aux besoins et contraintes spécifiques des PME.

Niveau de connaissance

Niveau de connaissance en cybersécurité	Nombre
Intermédiaire	85
Débutante	64
Avancé	26

Les réponses à l'enquête indiquent que la majorité des personnes interrogées évaluent le niveau actuel de connaissances de leurs employés en matière de cybersécurité comme étant « intermédiaire » (85), suivi par ceux qui le considèrent comme un niveau « débutant » (64), et une plus petite proportion considère leurs employés comme étant « intermédiaire » (85). Avoir des connaissances « avancées » en cybersécurité (26).

Cette répartition suggère un potentiel important de croissance et de développement des compétences en cybersécurité au sein des organisations représentées. La majorité des niveaux « Intermédiaire » et « Débutant » soulignent la nécessité d'initiatives de formation et d'éducation continues pour élever la base de connaissances en matière de cybersécurité de ces employés. Il met en évidence l'opportunité de programmes de formation ciblés en matière de cybersécurité, adaptés à différents niveaux de connaissances, garantissant ainsi que les principes fondamentaux de la cybersécurité soient bien compris par les débutants.

La présence d'employés possédant des connaissances avancées, bien que moins nombreuses, est encourageante car elle indique l'existence d'un niveau fondamental d'expertise en cybersécurité au sein de certaines organisations.

Niveau de connaissances en function de la taille de l'entreprise

Taille de l'entreprise	Avancé	Débutant	Intermédiaire
Jusqu'à 10 employés	6	25	33
11-50	10	20	30
51-250	10	19	22

Le tableau indique comment les niveaux de connaissances en cybersécurité (Avancé, Débutant, Intermédiaire) sont répartis selon les différentes tailles d'entreprise. Les petites entreprises (jusqu'à 10 salariés) affichent une tendance vers le niveau de connaissances en cybersécurité « Intermédiaire », suivi du niveau « Débutant ». Cela suggère que même si les petites entreprises peuvent avoir une certaine compréhension de la cybersécurité, il y en a encore une part importante au niveau débutant, ce qui indique une marge d'amélioration et la nécessité d'une formation plus fondamentale. Les moyennes entreprises (11 à 50 salariés) ont une répartition équilibrée entre les niveaux de connaissances, avec une légère préférence pour les connaissances « intermédiaires ». Cela pourrait refléter une approche plus structurée de la formation en cybersécurité dans des organisations légèrement plus grandes, mais indique également la présence à la fois de besoins de compréhension avancés et d'apprentissage de base. Les grandes PME (51 à 250 salariés) suivent un modèle similaire à celui des entreprises de taille moyenne, avec un nombre égal de niveaux avancés et débutants et un nombre légèrement inférieur de connaissances intermédiaires.

Dans toutes les tailles d'entreprises, le niveau « Intermédiaire » de connaissances en cybersécurité est le plus courant.

Employés chargés de taches liées à la cybersécurité

Nombre d'employés	Nombre de réponses
1-5	88
0	22
6-10	17
21+	12
11-20	5

Panel d'employés en cybersécurité	Nombre
0-4	113
5-9	17
10-14	13
20-24	4
25-50	6
+100	9

Les tableaux montrent la répartition du nombre d'employés effectuant des travaux liés à la cybersécurité dans différentes organisations. Il offre une vision plus claire de la façon dont les responsabilités en matière de cybersécurité sont réparties entre différentes catégories d'employés. La grande majorité des réponses se situent entre 0 et 4, ce qui indique qu'un grand nombre d'organisations disposent de très petites équipes de cybersécurité, voire aucune, spécifiquement dédiée à la cybersécurité. On constate une baisse significative de la fréquence à mesure que l'on passe à des fourchettes plus élevées, avec une certaine résurgence dans les organisations comptant plus de 100 employés dédiés à la cybersécurité. Cela s'explique par le fait que ces entreprises travaillent dans le domaine de la cybersécurité comme activité principale.

Dans les détails, les données suggèrent une grande diversité dans la taille des équipes de cybersécurité, la taille la plus courante étant un seul employé, suivi par aucun employé dédié à la cybersécurité, ce qui indique que de nombreuses organisations s'appuient peu ou pas du tout sur du personnel dédié à la cybersécurité. La fréquence diminue sensiblement à mesure que la taille de l'équipe augmente.

Cette répartition met en évidence une lacune potentielle dans la répartition des effectifs en matière de cybersécurité, dans la mesure où un nombre important de petites et moyennes entreprises (PME) pourraient ne pas disposer de ressources adéquates dédiées à la cybersécurité, les exposant ainsi à des risques plus importants. La présence d'équipes plus importantes dans certaines organisations suggère une reconnaissance de l'importance de la cybersécurité dans certains secteurs ou grandes entreprises.

Femmes dans la cybersécurité

Panel de femmes dans la cybersécurité	Nombre
0	78
1-5	57
6-10	8
11-15	4
16-20	1

Les résultats de la question « Combien de ces employés sont des femmes ? » mettent en évidence un écart important entre les sexes dans la main-d'œuvre en cybersécurité au sein des PME. Le constat le plus frappant est qu'une majorité d'entreprises, 78 au total, déclarent ne compter aucune femme dans leurs fonctions de cybersécurité. Cela indique un problème répandu de sous-représentation des femmes dans ce domaine critique dans les PME interrogées. Une diminution progressive du nombre est constatée à mesure que le nombre de femmes occupant des postes de cybersécurité augmente, 31 entreprises ayant une femme occupant un tel poste. La présence de quelques entreprises comptant 10 femmes ou plus dans des postes de cybersécurité, bien que positive, reste une exception plutôt que la norme. Ces instances peuvent représenter des organisations disposant d'équipes de cybersécurité plus importantes ou celles qui ont mis un accent particulier sur la diversité des genres au sein de leur personnel de cybersécurité. Cela souligne la nécessité de lancer des initiatives visant à encourager et à soutenir les femmes dans la poursuite de carrières dans le domaine de la cybersécurité. Le nombre important d'entreprises sans aucune femme occupant des postes dans la cybersécurité met en évidence un domaine d'intervention critique pour promouvoir la diversité des genres et l'inclusion au sein du secteur. Combler cet écart entre les sexes pourrait contribuer à des perspectives plus diversifiées pour relever les défis de la cybersécurité.

Utilisation de services externes

Réponse	Nombre
Non	115
Oui	60

Les réponses révèlent un aspect important de la manière dont les PME abordent la cybersécurité. Une majorité des entreprises interrogées, 115 sur 175, indiquent qu'elles ne font pas appel à des services externes pour des travaux de cybersécurité. Cela suggère une préférence ou une nécessité de gérer les efforts de cybersécurité en interne au sein d'un large segment de la population des PME. Divers facteurs pourraient alimenter cette tendance, tels que les contraintes budgétaires, le contrôle perçu sur les pratiques de cybersécurité ou la conviction que leurs ressources internes existantes sont suffisantes pour répondre à leurs besoins en matière de cybersécurité. Cette situation rend le projet CyberAgent très pertinent pour doter l'employé de compétences et de connaissances fondamentales.

60 entreprises ont déclaré avoir recours à des services externes pour des tâches de cybersécurité. Ce groupe reconnaît probablement les avantages de l'externalisation, comme

l'accès à des compétences spécialisées, la mise à jour des dernières menaces et contre-mesures en matière de cybersécurité, ou le renforcement de leurs capacités internes. La décision de faire appel à des services externes peut également refléter une compréhension de la complexité des menaces de cybersécurité, qui peuvent être difficiles à gérer entièrement en interne, en particulier pour les PME aux ressources limitées.

Cette scission met en évidence une divergence de stratégie de cybersécurité parmi les PME, équilibrant entre gestion interne et externalisation externe des fonctions de cybersécurité. Il souligne l'importance d'une approche adaptée à la cybersécurité, reconnaissant que différentes organisations peuvent avoir des besoins, des capacités et des ressources variés qui influencent leurs décisions quant à l'opportunité de rechercher un soutien externe pour les efforts de cybersécurité.

Efficacité des programmes de formation

Réponse	Nombre
1 (inefficace)	8
2	38
3	79
4	39
5 (très efficace)	11

Les réponses donnent un aperçu des perceptions concernant l'efficacité des programmes de formation actuels pour préparer les étudiants aux défis réels de cybersécurité dans les PME. La majorité des personnes interrogées, avec 79 points, ont attribué la note « 3 » à l'efficacité des programmes de formation actuels, ce qui indique une perception neutre ou modérée de leur efficacité. Cela suggère que même s'il existe un certain niveau de confiance dans ces programmes, il existe également une marge d'amélioration significative. Les réponses montrent également une tendance vers l'extrémité inférieure de l'échelle, le « 2 » recevant 38 points, ce qui indique un scepticisme quant à l'efficacité de ces programmes de formation. Aux extrêmes, « 1 » (inefficace) a reçu le moins de sélections (8 chefs d'accusation) et « 5 » (très efficace) en a reçu un peu plus (11 chefs d'accusation). Cela indique que très peu de personnes interrogées considèrent les programmes de formation actuels comme totalement inefficaces ou très efficaces pour préparer les étudiants aux défis de cybersécurité dans les PME. Le nombre équilibré de réponses pour « 4 » (39 points) suggère qu'un segment important de participants considère les programmes de formation comme relativement efficaces, bien que non sans limites importantes. Même si les programmes de formation actuels offrent une certaine préparation aux défis réels de cybersécurité dans les PME, il existe un écart entre la formation dispensée et les besoins du secteur. Cet écart peut être dû à plusieurs facteurs, tels que le rythme d'évolution des menaces de cybersécurité, l'application pratique des compétences ou la spécificité des défis auxquels sont confrontées les PME.

Top 3 des domaines de formation en cybersécurité

Catégorie	Nombre
Détection et réponse aux menaces	102
Analyse et gestion des risques	81
Réponse aux incidents et récupération	72
Confidentialité et protection des données	68
Expertise en sécurité du Cloud	51
Sécurité des réseaux	46
Connaissances en matière de cinformité et de réglementation	31
Technologies émergentes	24

L'analyse des réponses révèle que la « Détection et réponse aux menaces » est considérée comme le domaine le plus crucial de la formation en cybersécurité, avec 102 points, ce qui indique une forte conviction en son importance pour relever les défis réels de cybersécurité dans les PME. Ce domaine est suivi de près par « Gestion et analyse des risques » et « Réponse aux incidents et récupération », avec respectivement 81 et 72 points, soulignant l'importance accordée à la compréhension des risques et à la capacité de réagir efficacement aux incidents. La « confidentialité et protection des données » fait également l'objet d'une attention particulière, reflétant l'importance croissante des lois sur la protection des données et la nécessité de protéger les informations personnelles et sensibles à l'ère numérique. « L'expertise en matière de sécurité du cloud » est identifiée comme un domaine clé par 51 personnes interrogées, probablement en raison de l'adoption croissante des services cloud et des défis de sécurité uniques qu'ils présentent. La sécurité des réseaux, avec 46 points, reste une préoccupation fondamentale, soulignant la nécessité de se défendre efficacement contre les menaces réseau. Les « connaissances en matière de conformité et de réglementation » et les « technologies émergentes » sont considérées comme moins importantes.

Compétences et connaissances

Domaine de compétences et de connaissances	Essentiel (%)	Besoin élevé (%)	Besoin modéré (%)	Besoin faible (%)	Pas de besoin (%)
Confidentialité et protection des données	38.29	38.29	13.14	10.29	0.00*
Evaluation et gestion des risques	34.86	36.00	24.00	4.57	0.57
Réponse aux incidents et récupération	33.14	38.86	19.43	8.00	0.57
Compétences en communication	32.57	35.43	22.29	8.00	1.71
Connaissances techniques	30.29	32.00	26.29	8.57	2.86
Intelligence et surveillance des menaces	29.71	37.14	24.00	8.57	0.57
Elaboration et mise en oeuvre des politiques	24.00	37.14	24.00	12.57	2.29

* : Le pourcentage « Non nécessaire » pour « Confidentialité et protection des données » n'est pas disponible (NaN), ce qui pourrait être dû au fait que tous les répondants considèrent ce domaine comme au moins un certain besoin, et peut donc être considéré comme 0 %.

Le tableau présente les scores moyens pour chaque domaine de compétence et de connaissances, dérivés des réponses à l'enquête évaluant leur importance sur une échelle de 1 (non nécessaire) à 5 (essentiel). Ces scores fournissent un aperçu quantitatif de la manière dont les répondants priorisent différents domaines du domaine.

Ce tableau fournit une répartition claire de la façon dont chaque domaine de compétence et de connaissances est valorisé par les répondants. Des domaines tels que « Confidentialité et protection des données » et « Évaluation et gestion des risques » ont le pourcentage le plus élevé de notes « Essentiel », reflétant leur importance cruciale dans le domaine. En revanche, « Élaboration et mise en œuvre de politiques » montre une répartition plus large des réponses, indiquant une perception plus variée de son importance. Les résultats mettent en évidence l'importance accordée aux connaissances techniques, à la sensibilisation aux menaces et à la capacité à répondre aux incidents, ainsi qu'au besoin crucial de pratiques efficaces de communication et de protection des données.

Menaces émergentes dans la cybersécurité

Menaces émergentes dans la cybersécurité	Fréquence
Phishing et ingénérie sociale	105
Cyberattaques pilotés par l'IA	95
Attaques de rançongiciels	90
Failles de sécurité das le Cloud	60
Menaces Deepfake	57
Vulnérabilités IoT	44
Menaces internes	31

Le phishing et l'ingénierie sociale sont considérés comme les menaces les plus urgentes, les cyberattaques pilotés par l'IA et les attaques de ransomware faisant également l'objet d'une attention particulière. Cela suggère une forte prise de conscience parmi les PME de la nécessité de se prémunir contre les cybermenaces traditionnelles et émergentes. Les failles de sécurité du cloud et les menaces Deepfake sont également mises en avant, reflétant les inquiétudes concernant la sécurité des services cloud et l'utilisation abusive potentielle de l'intelligence artificielle. Les vulnérabilités de l'IoT et les menaces internes sont également identifiées, même si elles sont considérées comme moins imminentes que les autres catégories. En particulier, certaines réponses indiquent que certains répondants ne sont pas sûrs de menaces spécifiques ou n'ont pas d'idées au niveau de leur entreprise, ce qui suggère un manque potentiel de sensibilisation ou d'inquiétude concernant des menaces émergentes spécifiques parmi certaines PME.

Ecart dans les connaissances ou compétences en cybersécurité

Ecart dans les connaissances ou compétences en cybersécurité	Fréquence
Faible niveau en Sensibilisation aux menaces	105
Faible niveau en Formations régulières en cybersécurité	88
Faible niveau en Evaluation de la vulnérabilité	80
Faible niveau en Compétences techniques	71
Faible niveau en Compréhension des politiques de réglementations	50
Faible niveau en Compétences interpersonnelles	37

Les lacunes les plus importantes en matière de connaissances ou de compétences en matière de cybersécurité parmi les employés concernent la sensibilisation aux menaces, les formations régulières en matière de cybersécurité, l'évaluation des vulnérabilités, les compétences techniques et la compréhension des politiques et des réglementations. La fréquence de ces réponses met en évidence le besoin crucial d'une éducation et d'une formation complètes en matière de cybersécurité qui abordent ces domaines spécifiques. La sensibilisation aux menaces constitue la lacune la plus importante, indiquant que les employés ne sont peut-être pas pleinement conscients des menaces de cybersécurité qui pourraient avoir un impact sur leur organisation. Cette lacune souligne l'importance d'améliorer les programmes de sensibilisation et la formation pour aider les employés à reconnaître plus efficacement les menaces potentielles. Les formations régulières en matière de cybersécurité sont également considérées comme une lacune, soulignant la nécessité d'une formation continue et de mises à jour sur les dernières pratiques et menaces en matière de cybersécurité, plutôt que de sessions de formation ponctuelles.

Tendances émergentes

Tendances émergentes en matière de formation en cybersécurité	**Fréquence**
IA et apprentissage automatique en cybersécurité	134
Identité digitale et confidentialité	108
Piratage éthique et compétences défensives	86
Focus sur les soft skills et la formation interdisciplinaire	54
Menaces de l'informatique quantique	39
Syst§mes de sécurité décentralisés (par exemple, Blockchain)	28

L'analyse révèle que l'accent est clairement mis sur l'IA et l'apprentissage automatique dans le domaine de la cybersécurité, comme tendance la plus attendue pour les cinq prochaines années. Cela indique une reconnaissance croissante du rôle des technologies avancées dans le renforcement des défenses de cybersécurité et le développement de nouvelles solutions de sécurité. La fréquence élevée des réponses dans cette catégorie suggère que les programmes de formation devront de plus en plus intégrer des composants d'IA et d'apprentissage automatique pour préparer les professionnels de la cybersécurité à l'avenir. L'identité numérique et la confidentialité apparaissent comme la deuxième tendance la plus attendue, soulignant les préoccupations liées à la protection des données personnelles et à la gestion des identités numériques dans un monde de plus en plus en ligne. Cette tendance suggère une

demande de formation couvrant les complexités des lois sur la confidentialité, des techniques de protection des données et des solutions de gestion des identités. Le piratage éthique et les compétences défensives sont identifiés comme la troisième tendance clé, reflétant l'importance des stratégies de défense proactives en matière de cybersécurité. L'accent mis sur le hacking éthique montre une évolution vers des formations permettant aux professionnels de la cybersécurité de penser comme des attaquants afin de mieux défendre leurs organisations.

Adéquation des programmes de formation

Réponse	Fréquence
Oui	81
Ne sais pas	65
Non	29

L'analyse de la question qui explorait les points de vue des répondants sur l'adéquation des programmes actuels de formation en cybersécurité révèle une perspective mitigée parmi les participants. Une partie importante, représentant la majorité des répondants, estime que les programmes de formation actuels en cybersécurité sont adéquats, comme l'indiquent les réponses « Oui ». Cela suggère qu'un certain nombre de personnes estiment que la formation disponible aujourd'hui répond aux besoins de leur organisation ou correspond à leurs attentes quant à ce que devrait comporter la formation en cybersécurité. Cependant, un nombre important de personnes interrogées ne sont « pas sûres » de l'adéquation des programmes de formation actuels, soulignant un degré d'incertitude ou un manque d'informations sur les options de formation disponibles ou sur leur efficacité pour relever les défis actuels en matière de cybersécurité. Cette incertitude pourrait être attribuée à la nature évolutive des cybermenaces et à la difficulté de maintenir les programmes de formation à jour avec les derniers développements dans le domaine. Les réponses « Non », bien qu'elles représentent le groupe le plus restreint, indiquent une préoccupation évidente quant au fait que les programmes de formation existants ne suffisent pas à répondre aux besoins actuels en matière de cybersécurité. Ce groupe peut percevoir des lacunes dans la couverture de la formation sur les menaces, technologies ou méthodologies émergentes.

Inclusivité des programmes de formation

Réponse	Fréquence
Oui	81
Ne sais pas	65
Non	29

L'analyse des réponses indique une perspective diversifiée sur l'inclusivité des programmes actuels de formation en cybersécurité concernant le genre. Une pluralité de répondants estiment que la formation actuelle est inclusive et répond efficacement aux besoins de tous les sexes, comme l'indiquent les réponses « Oui ». Cela suggère qu'une partie importante de la communauté de la cybersécurité estime que les efforts de formation actuels progressent vers l'inclusivité et l'égalité des sexes. Cependant, un grand nombre de personnes interrogées ne

sont « pas sûres » du caractère inclusif de ces programmes, ce qui indique une grande incertitude ou un manque de sensibilisation quant à l'inclusion du genre dans la formation en cybersécurité. Cette réponse pourrait mettre en évidence un déficit de communication entre les prestataires de formation et les participants ou suggérer que les efforts d'inclusion ne sont peut-être pas aussi visibles ou impactants que prévu. Les réponses « Non », qui représentent le plus petit groupe parmi les répondants, soulignent néanmoins une préoccupation majeure : la formation actuelle en matière de cybersécurité ne répond pas suffisamment aux besoins de tous les sexes. Ces commentaires mettent en évidence une lacune dans les efforts d'inclusivité au sein des programmes de formation en cybersécurité, suggérant que des efforts supplémentaires sont nécessaires pour garantir que ces programmes sont accueillants et adaptés aux besoins des individus de toutes identités de genre.

3.2. PRÉFÉRENCES ET BESOINS DE FORMATION

Sur la base des résultats de la recherche sur le terrain, voici une description des caractéristiques identifiées et des besoins de formation, des préférences d'apprentissage, de la formation et de l'accompagnement des femmes impliquées dans la cybersécurité.

Identification des besoins en formation :

Domaine 1 - Connaissances et compétences fondamentales

Une priorité dans l'éducation à la cybersécurité. Surtout des sujets tels que les fondamentaux de la cybersécurité et la sécurité des réseaux. Des lacunes importantes existent dans des domaines tels que la détection et la réponse aux menaces, l'expertise en matière de sécurité du cloud, la réponse et la récupération en cas d'incident, la confidentialité et la protection des données, ainsi que la gestion et l'analyse des risques. Les programmes de formation doivent remédier à ces déficits de compétences. Il existe également un fort besoin de cybersécurité pour les contenus destinés aux PME.

Domaine 2 - Thèmes spécialisés

Il s'agit d'un besoin de formation couvrant un large éventail de menaces et de contre-mesures en matière de cybersécurité. Certains sujets spécialisés tels que l'analyse et la gestion des menaces, la cryptographie et les techniques avancées d'atténuation des menaces ont été mis en avant. La formation doit intégrer du contenu sur les menaces émergentes les plus fréquemment mentionnées, notamment les cyberattaques pilotées par l'IA, les attaques de ransomwares, le phishing et l'ingénierie sociale, les failles de sécurité dans le cloud et les vulnérabilités de l'IoT.

Domaine 3 - Application pratique

La préférence pour les méthodes d'enseignement telles que les cours pratiques, les études de cas et les projets de groupe soulignent l'importance de l'application pratique, interactive et réelle dans la formation en cybersécurité.

Pratiques actuelles :

Concernant la méthode d'enseignement, on peut noter le recours à diverses pratiques telles que des études de cas, des projets de groupe, des laboratoires pratiques et des cours magistraux. Il existe un mélange d'approches théoriques et pratiques dans les programmes de formation actuels.

Les programmes de formation actuels couvrent une gamme de sujets liés à la cybersécurité, les sujets fondamentaux étant prioritaires. Cependant, on constate une absence de contenu spécifique aux PME dans certains programmes.

En ce qui concerne l'inclusivité et l'équilibre entre les sexes, certains programmes ont mis en œuvre des initiatives visant à accroître la participation des femmes et à créer des environnements de formation intégrant le genre, bien que ces efforts semblent être minoritaires.

Défis :

Les principaux défis rencontrés dans l'éducation à la cybersécurité sont :

- - Adapter la formation à différents horizons et niveaux d'expertise est un défi car il existe une diversité de compétences et d'expériences.
- - Maintenir le matériel de cours à jour pour faire face à l'évolution rapide des menaces de cybersécurité. Cela nécessite une mise à jour continue des supports de formation.
- - Contraintes de formation pratique en raison des limitations des installations de laboratoire, des capacités de simulation du monde réel et de la création de scénarios réalistes de cyberattaques pour la pratique
- - Il est difficile de garder les étudiants engagés et motivés, en particulier avec un contenu technique complexe.
- - L'alignement de l'industrie et de l'éducation avec l'équilibre entre les fondements théoriques et les compétences pratiques qui correspondent aux besoins de l'industrie pose un défi.

Suggestion de développement de formation :

- - Adaptation des formations aux besoins des PME : intégrant des thématiques et des compétences spécifiquement conçues pour répondre aux besoins de cybersécurité des PME.
- - Améliorer l'application pratique en élargissant l'utilisation de méthodes d'enseignement pratiques et interactives pour améliorer les compétences pratiques et la préparation au monde réel.
- - Intégrer les tendances émergentes telles que l'IA et l'apprentissage automatique, l'identité numérique et la confidentialité, ainsi que le piratage éthique. Ils sont désormais considérés comme des domaines clés sur lesquels se concentreront à l'avenir dans les programmes de formation.

- - Combler les déficits de compétences en se concentrant sur les domaines dans lesquels les employés font défaut, tels que la détection et la réponse aux menaces, la sécurité du cloud et la réponse aux incidents, afin de mieux les préparer à relever les défis et à devenir un CyberAgent efficace et résilient.
- - Développer des initiatives en faveur de la diversité des genres pour accroître la participation des femmes grâce à des initiatives ciblées, du mentorat et des modèles de rôle.

4. PROFIL DE QUALIFICATION D'UN *CYBERSECURITY CHANGE AGENT* DANS LES PME

Sur la base des résultats d'une recherche documentaire et sur le terrain, voici un exemple de l'ensemble de connaissances, d'aptitudes et de compétences attendues par CyberAgent. Ces résultats articulent les réalisations attendues des participants à la fin de leurs programmes de formation respectifs en cybersécurité, garantissant un développement depuis des connaissances et des compétences fondamentales au niveau 4/5 du CEC jusqu'à des capacités plus avancées et orientées vers le leadership au niveau 6 du CEC.

Profil de qualification CyberAgent	Connaissance	Aptitudes	Compétences
Au niveau 4/5 **du CEC**	**Fondamentaux de la cyber-sécurité** - Concepts de base de la cybersécurité - Types de cybermenaces (phishing, ransom-ware, attaques ddos), vecteurs d'attaque - Importance de la cybersécurité dans la protection des actifs organisationnels. **Cadre juridique et des données en cybersécurité** - Législation, normes et exigences de conformité en matière de cybersécurité - Stratégies et politiques pour la sécurité de l'information - Protection des données - Politiques de gestion des risques	**Sécurité** - Identifier les risques et vulnérabilités potentiels en matière de cybersécurité - Utiliser des outils et des logiciels de cybersécurité pour vous protéger contre les cybermenaces - Promouvoir l'application pratique des pratiques de base en matière de cybersécurité, la création sécurisée de mots de passe, la navigation sécurisée, la sécurité du courrier électronique et la gestion sécurisée des données sensibles.	**Gestion et attenuation des risques** - Évaluer et atténuer les menaces de sécurité potentielles **Communication efficace sur les problèmes de cybersécurité** - Capacité à communiquer efficacement sur les problématiques de cybersécurité, - Signaler les menaces et les violations aux canaux appropriés au sein de l'organisation.

Au niveau 6 du CEC	**Concepts avancés de cybersécurité** - Comprendre les principes avancés de cybersécurité, y compris les cybermenaces sophistiquées et les vecteurs d'attaque, - Sensibilisation aux dernières tendances en matière de menaces de cybersécurité et de mécanismes de défense. **Législation et conformité en matière de cybersécurité** - Connaissance de la législation, des normes et des exigences de conformité nationales et internationales en matière de cybersécurité, ainsi que d'autres pertinentes pour leur secteur spécifique.	**Évaluation et gestion avancées des risques** - Capacité à mener des évaluations complètes des risques - Utiliser des méthodologies et des outils avancés - Concevoir et mettre en œuvre des stratégies efficaces de gestion des risques pour atténuer les risques identifiés. **Expertise en architecture de sécurité et défense des réseaux** - Concevoir, mettre en œuvre et évaluer des architectures de réseau sécurisées, y compris l'utilisation de pare-feu, de systèmes de détection d'intrusion (ids) et de systèmes de prévention des intrusions (ips). **Réponse aux incidents et récupération** - Capacité à se préparer, à réagir et à se remettre des incidents de cybersécurité - Élaborer des plans de reprise et de continuité d'activité.	**Planification et élaboration de politiques** - Capacité à élaborer et à mettre en œuvre des politiques et des cadres stratégiques de cybersécurité alignés sur les objectifs et les obligations de conformité de l'organisation. **Leadership dans les initiatives de cybersécurité** - Diriger et gérer des projets et des équipes de cybersécurité, y compris la capacité d'inspirer et de guider les employés dans la mise en œuvre de stratégies de cybersécurité. **Prise de décision** - Prendre des décisions éthiques concernant les pratiques de cybersécurité

Au niveau 4/5 du CEC, les acquis d'apprentissage possibles pourraient être :

- - Les apprenants apprendront les concepts fondamentaux de la cybersécurité, y compris la terminologie de base, les types de cybermenaces telles que le phishing, les ransomwares et les attaques DDoS, ainsi que leurs vecteurs d'attaque respectifs.
- - Les apprenants seront capables d'identifier les risques et vulnérabilités potentiels en matière de cybersécurité, d'utiliser les outils et logiciels pertinents pour atténuer ces risques et de mettre en œuvre des pratiques de base en matière de cybersécurité telles que la création de mots de passe sécurisés et la navigation sécurisée.
- - Les apprenants acquerront des connaissances sur la législation, les normes et les exigences de conformité en matière de cybersécurité, ainsi que sur les stratégies et politiques de sécurité de l'information et de gestion des risques au sein d'une organisation.
- - Les apprenants développeront les compétences nécessaires pour évaluer et atténuer efficacement les menaces de sécurité potentielles et communiquer clairement et

efficacement les problèmes de cybersécurité au sein de l'organisation, y compris en signalant les menaces et les violations aux canaux appropriés.

Au niveau 6 du CEC, les résultats d'apprentissage possibles pourraient être :

- - Les apprenants développeront une compréhension avancée des principes de cybersécurité, y compris la capacité d'identifier les cybermenaces et les vecteurs d'attaque sophistiqués et de rester informés des dernières tendances en matière de défense de cybersécurité.
- - Les apprenants acquerront une connaissance complète de la législation, des normes et des exigences de conformité nationales et internationales en matière de cybersécurité, en adaptant cette compréhension aux besoins spécifiques de leur secteur.
- - Les apprenants seront capables de mener des évaluations détaillées des risques à l'aide de méthodologies et d'outils avancés, et d'élaborer des stratégies efficaces de gestion des risques pour atténuer ces risques.
- - Les apprenants concevront, mettront en œuvre et évalueront des architectures de réseau sécurisées, notamment en maîtrisant l'utilisation de technologies de sécurité critiques telles que les pare-feu, l'IDS et l'IPS.
- - Les apprenants seront compétents dans la planification et l'exécution de stratégies de réponse aux incidents et de récupération, garantissant ainsi la résilience organisationnelle grâce à des plans de récupération et de continuité des activités efficaces.
- - Les apprenants feront preuve de leadership en matière de cybersécurité en élaborant des politiques stratégiques, en gérant des projets et des équipes de cybersécurité et en prenant des décisions éclairées et éthiques sous pression.

5. ANNEXES

5.1. ANNEXE A: LISTE DE LA LITTÉRATURE EXAMINÉE

Aperçu de l'éducation à la cybersécurité dans l'EFP et l'enseignement supérieur

1. https://ccb.belgium.be/en/ict-security-education-belgium
2. https://acdn.be/enewsv7/upload/whitepaper/CybersecurityReport.pdf
3. https://ccb.belgium.be/sites/default/files/CCB_Strategie%202.0_UK_WEB.pdf
4. https://www.enisa.europa.eu/topics/education/cyberhead#/programmes?country[]=fin
5. http://www.anc.edu.ro/standarde-pregatire-profesionala/
6. http://217.73.164.21/index.php/articles/curriculum/c556+592/
7. http://217.73.164.21/index.php/articles/c560/
8. https://www.agerpres.ro/english/2023/09/19/first-master-s-program-in-romania-in-cyber-security-accredited-by-eit-digital-at-ubb-cluj-napoca--1171675
9. https://dnsc.ro/invatamant/vezi/5
10. https://www.linkedin.com/posts/eit-digital_ubb-cluj-joins-eit-digital-adding-cybersecurity-activity-7031990099756081152-Sr77/?originalSubdomain=si
11. https://www.unitbv.ro/documente/curriculum-syllabus/Master/Plan%20inv/MI_master_TIN_2017_2018_PI.pdf
12. https://mateinfo.unitbv.ro/images/2023/planuri_inv/Plan_inv_2023_2025_Tehnologii_moderne_in_ingineria_sistemelor_soft.pdf
13. https://drive.google.com/drive/folders/1h9aC1xwobVtGN4qNukWMvDPXICf62FgF
14. Analysis and Diagnosis of Cybersecurity Talent in Spain, March 2022, Observaciber, https://www.observaciber.es/
15. Ciberseguridad. Informe de Situación 2022, Plataforma tecnológica española de tecnologías disruptivas, Ministerio de Ciencia e Innovación https://ptedisruptive.es/wp-content/uploads/2022/12/Informe-situacio%CC%81n-ciberseguridad-2022.pdf
16. Panorama actual de la Ciberseguridad en España, Google https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf
17. Catálogos de formación en ciberseguridad, INCIBE, 2023 https://www.incibe.es/incibe/formacion/catalogos-formacion-ciberseguridad
18. Plan Nacional de competencias digitales https://portal.mineco.gob.es/es-es/digitalizacionIA/Paginas/plan-nacional-competencias-digitales.aspx
19. Plan España Digital 2025 https://avancedigital.mineco.gob.es/programas-avance-digital/paginas/espana-digital-2025.aspx
20. Plan de Digitalización de PYMES 2021-2025 https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/ficheros/210127_plan_digitalizacion_pymes.pdf
21. Real Decreto 479/2020, de 7 de abril, por el que se establece el Curso de especialización en ciberseguridad en entornos de las tecnologías de la información y se fijan los aspectos básicos del currículo https://www.boe.es/diario_boe/txt.php?id=BOE-A-2020-4963

Défis et besoin de l'industrie de la cybersécurité

1. El estado de la ciberseguridad en España, Deloitte, 2022 **https://www2.deloitte.com/es/es/pages/risk/articles/estado-ciberseguridad.html**
2. Ferreirós Orihuel, Inés (coord.). IV Informe sobre la Ciencia y Tecnología en España: Situar a España e el mapa geopolítico de la I+D+i. Fundación Alternativas: 187-206 (2023) **https://digital.csic.es/handle/10261/310469**
3. El reto de la ciberseguridad en España: un país vulnerable, Telefónica **https://www.telefonica.com/es/sala-comunicacion/blog/un-pais-vulnerable-el-reto-de-la-ciberseguridad-en-espana/**
4. Los retos de la ciberseguridad para las empresas españolas, Byte ti, 11 de enero de 2024 **https://revistabyte.es/tema-de-portada-byte-ti/retos-de-la-ciberseguridad/**
5. La falta de profesionales acentúa la amenaza de los ciberataques, el Periódico de España, 7 de Marzo de 2023 **https://www.epe.es/es/tecnologia/20230307/falta-profesionales-acentua-amenaza-ciberataques-84230209**
6. Analysis and Diagnosis of Cybersecurity Talent in Spain, March 2022, Observaciber, **https://www.observaciber.es/**
7. Ciberseguridad. Informe de Situación 2022, Plataforma tecnológica española de tecnologías disruptivas, Ministerio de Ciencia e Innovación **https://ptedisruptive.es/wp-content/uploads/2022/12/Informe-situacio%CC%81n-ciberseguridad-2022.pdf**
8. Panorama actual de la Ciberseguridad en España **https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf**
9. Plan España Digital 2025 **https://avancedigital.mineco.gob.es/programas-avance-digital/paginas/espana-digital-2025.aspx**
10. **Plan de Digitalización de PYMES 2021-2025 https://portal.mineco.gob.es/RecursosArticulo/mineco/ministerio/ficheros/210127_plan_digitalizacion_pymes.pdf**
11. **https://esco.ec.europa.eu/sites/default/files/ethical%20hacker.pdf**
12. **http://data.europa.eu/esco/occupation/276ba420-ef09-4a0e-b215-2c2e2f80ad28**

13. https://nsm.no/fagomrader/digital-sikkerhet/
14. https://www.bdo.no/nb-no/nyheter/2023/na-jakter-hackerne-de-sma-selskapene
15. https://www.evelon.no/artikler/trussellandskapet-i-europa
16. https://norsis.no/sikkerhetskultur2023/sammendrag/
17. https://serit.no/hva-er-god-datasikkerhet-i-bedriften/
18. https://www.duo.uio.no/bitstream/handle/10852/96151/5/Master_thesis_mariwilh.pdf

Femmes dans la cybersécurité

1. Microsoft. (2017, March). Why Europe's girls aren't studying STEM. Microsoft News. Retrieved January 20, 2024, from https://news.microsoft.com/uploads/2017/03/ms_stem_whitepaper.pdf
2. Women go tech. (2021, September). ICT workforce in Europe and its gender challenge after Covid-19. Women Go Tech. Retrieved January 20, 2024, from https://womengotech.com/app/uploads/2021/09/ICT-workforce-in-Europe-and-its-gender-challenge.pdf
3. Rodiklių duomenų bazė - Oficialiosios statistikos portalas. (n.d.) 1. https://osp.stat.gov.lt/statistiniu-rodikliu-analize#/
4. Bukauskas, Brilingaite, Ikamas, Juozapavicius, & Lepaite. (2022, August 5). Ataskaita Lietuvos kibernetinio saugumo kompetenciju¸ žemelapis. Vilnius University. Retrieved January 20, 2024, from https://cs.vu.lt/projects/P-REP-21-2/ataskaita.pdf
5. https://www.digi.no/artikler/debatt-flere-tech-jenter-ma-til-for-a-finne-morgendagens-losninger/535073
6. https://odanettverk.no/2022/03/08/dette-er-norges-50-fremste-tech-kvinner-2022/
7. https://e24.no/naeringsliv/i/k6Goma/etterlyser-flere-kvinner-til-cybersikkerhet
8. https://www.ssb.no/befolkning/artikler-og-publikasjoner/kvinner-velger-fortsatt-kvinneyrker
9. https://live.worldbank.org/en/event/2023/women-business-law-2023
10. https://wbl.worldbank.org/en/data/exploreeconomies/romania/2023
11. https://eige.europa.eu/gender-equality-index/2022/country/RO
12. https://cybernews.com/editorial/cyber-women-grim-statistics-big-opportunities/
13. https://www.weforum.org/agenda/2022/09/cybersecurity-women-stem/
14. https://www.bcg.com/publications/2022/empowering-women-to-work-in-cybersecurity-is-a-win-winFerreirós Orihuel, Inés (coord.). IV Informe sobre la Ciencia y Tecnología en España: Situar a España e el mapa geopolítico de la I+D+i. Fundación Alternativas: 187-206 (2023) https://fundacionalternativas.org/publicaciones/iv-informe-sobre-la-ciencia-y-la-tecnologia-en-espana/
15. Mujeres empleadas en ciencia y tecnología (reparto por sectores). España, UE-27 y UE-28. Serie 2019-2021. https://www.ine.es/jaxi/Tabla.htm?path=/t00/mujeres_hombres/tablas_1/l0/&file=c02002.px&L=0
16. La mujer en la ciencia española, en datos y gráficos, EpData, 7 de marzo de 2023 https://www.epdata.es/datos/mujer-ciencia-espanola-datos-estadisticas/298
17. Analysis and Diagnosis of Cybersecurity Talent in Spain, March 2022, Observaciber, https://www.incibe.es/ed2026/talento-hacker/publicaciones/diagnostico-talento-ciberseguridad
18. Ciberseguridad. Informe de Situación 2022, Plataforma tecnológica española de tecnologías disruptivas, Ministerio de Ciencia e Innovación https://ptedisruptive.es/wp-content/uploads/2022/12/Informe-situacio%CC%81n-ciberseguridad-2022.pdf
19. Panorama actual de la Ciberseguridad en España, Google https://www.ospi.es/export/sites/ospi/documents/documentos/Seguridad-y-privacidad/Google_Panorama-actual-de-la-ciberseguridad-en-Espana.pdf

5.2. ANNEXE B: QUESTIONNAIRE D'ENQUÊTE

Questionnaire EFP & enseignement supérieur

Cette enquête est conçue pour recueillir des informations sur l'état actuel et les besoins futurs en matière de formation en cybersécurité et aider à façonner un programme de formation en cybersécurité efficace et adapté aux défis de cybersécurité des petites et moyennes entreprises (PME).

L'enquête est divisée en 4 sections :

- Démographie
- Programme d'études, besoins de formation et préférences d'apprentissage
- Compétences requises et compétences futures
- Informations spécifiques au genre

L'enquête prendra environ 8 minutes pour être complétée.

DONNÉES DÉMOGRAPHIQUES

Quel est votre pays ?

▫ Lituanie
▫ Belgique
▫ Norvège
▫ Türkiye
▫ Finlande
▫ Roumanie
▫ Espagne
▫ Pologne

Dans quel établissement scolaire enseignez-vous actuellement ?

▫ EFP (Enseignement et Formation Professionelle)
▫ Enseignement supérieur

Quel est votre genre ?

▫ Homme
▫ Femme
▫ Préfère ne pas dire

Depuis combien d'années enseignez-vous une formation en cybersécurité ?

▫ Moins d'1 an
▫ 1-5 ans
▫ 6-10 ans
▫ Plus de 10 ans

CURRICULUM, BESOINS DE FORMATION ET PRÉFÉRENCES D'APPRENTISSAGE

Parmi les sujets suivants, lesquels sont inclus dans votre programme de formation en cybersécurité ? (Sélectionnez tout ce qui s'y rapporte)

▫ Fondamentaux de la cybersécurité

▫ Analyse et gestion des menaces
▫ Techniques avancées d'atténuation des menaces
▫ Cryptographie
▫ Sécurité des réseaux
▫ Lois et politiques sur la cybersécurité
▫ Gestion des risques
▫ Autre: _____

Quelles méthodes pédagogiques utilisez-vous principalement dans votre formation en cybersécurité ? (Sélectionnez tout ce qui s'y rapporte)

▫ Cours magistraux
▫ Cours pratiques
▫ Etudes de cas
▫ Travaux de groupe
▫ Simulations en ligne
▫ Classe inversée
▫ Autre: _____

Quels formats d'apprentissage seraient les plus efficaces pour une formation en cybersécurité ? (Sélectionnez tout ce qui s'y rapporte)

▫ Workshop en présentiel
▫ Cours en ligne
▫ Webinaires
▫ Simulations interactives
▫ Tutoriels vidéo
▫ Sessions pratiques
▫ Autre: _____

Quels sont les plus grands défis auxquels vous êtes confronté pour dispenser une formation efficace en cybersécurité ?

Question ouverte

Sur une échelle de 1 à 5, dans quelle mesure pensez-vous que les programmes de formation actuels préparent efficacement les étudiants aux défis réels de cybersécurité des PME ?

▫ Très efficace
▫ Un peu inefficace
▫ Neutre
▫ Plutôt efficace
▫ Très efficace

Dans quelle mesure pensez-vous que la formation actuelle en cybersécurité correspond aux besoins spécifiques des PME ?

1 (Non aligné)
2 (Légèrement aligné)
3 (aligné)
4 (Bien aligné)
5 (hautement aligné)

Y a-t-il des sujets ou des compétences spécifiques que vous incluez dans votre formation pour répondre aux besoins uniques en matière de cybersécurité des PME ? (Sélectionnez tout ce qui s'y rapporte)

▫ Cybersécurité de base pour les PME
▫ Évaluation et gestion des risques dans le contexte des PME
▫ Réponse aux incidents pour les PME
▫ Protection des données et confidentialité pour les PME
▫ Développement de politiques de cybersécurité pour les PME
▫ Autre: _____

À quelle fréquence personnalisez-vous ou adaptez-vous votre formation en cybersécurité pour mieux répondre aux besoins des PME ?

▫ Toujours
▫ Souvent
▫ Parfois
▫ Rarement
▫ Jamais

Recevez-vous des retours ou êtes-vous en contact avec des représentants de PME ou des professionnels pour vous assurer de la pertinence de vos contenus de formation par rapport à leurs besoins ?

▫ Oui, régulièrement
▫ Occasionnellement
▫ Rarement
▫ Jamais

Sur la base de votre expérience, dans quelle mesure pensez-vous que la formation actuelle en cybersécurité est efficace pour équiper les professionnels des PME à relever les défis de la cybersécurité ?

▫ Très inefficace
▫ Quelque peu inefficace
▫ Neutre
▫ Plutôt efficace
▫ Très efficace

Quelles suggestions avez-vous pour améliorer la pertinence et l'efficacité de la formation en cybersécurité pour les PME ?

Question ouverte

EXIGENCES DE COMPÉTENCES ET COMPÉTENCES FUTURES

Selon vous, quels sont les principaux déficits de compétences parmi la main-d'œuvre actuelle en cybersécurité des PME ?

(Choisissez jusqu'à trois)

▫ Détection des menaces et réponse
▫ Expertise en sécurité cloud
▫ Connaissances en matière de conformité et de réglementation
▫ Réponse aux incidents et récupération

▫ Gestion et analyse des risques
▫ Confidentialité et protection des données
▫ Technologies émergentes
▫ Sécurité du réseau

Veuillez évaluer, sur une échelle de 1 (pas nécessaire) à 5 (extrêmement nécessaire), les compétences et connaissances nécessaires :

	Evaluation				
Évaluation et gestion des risques Comprendre les types de risques et leur impact.					
Connaissances techniques Aspects techniques de la cybersécurité et connaissance des systèmes d'exploitation, des réseaux et de la gestion de bases de données.					
Réponse aux incidents et récupération Identifier, répondre et récupérer des failles et des incidents de sécurité.					
Élaboration et mise en œuvre de politiques Élaborer et mettre en œuvre des politiques et des pratiques de sécurité efficaces					
Intelligence et surveillance des menaces Se tenir au courant des dernières tendances, menaces et méthodologies d'attaque en matière de cybersécurité.					
Compétences en communication Communication efficace avec le personnel, la direction et éventuellement les clients sur les questions de cybersécurité.					
Confidentialité et protection des données Principes de confidentialité des données et comment protéger les informations sensibles .					

Connaissez-vous un ensemble pertinent de compétences et de connaissances non répertoriées dans la question précédente qui pourraient être extrêmement nécessaires pour les PME ?
Question ouverte
Selon vous, à quelles menaces émergentes en matière de cybersécurité les PME doivent-elles se préparer au cours des cinq prochaines années ? (Choisissez jusqu'à trois)
▫ Attaques de ransomwares
▫ Vulnérabilités de l'IoT
▫ Failles de sécurité dans le cloud
▫ Cyberattaques basées sur l'IA
▫ Menaces internes
▫ Autre : _____
Selon vous, quelles seront les trois principales tendances émergentes en matière de formation en cybersécurité pour les 5 prochaines années ? (Choisissez jusqu'à 3 options)
▫ IA et apprentissage automatique en cybersécurité

▫ Focus sur les soft skills et la formation interdisciplinaire
▫ Menaces liées à l'informatique quantique
▫ Piratage éthique et compétences défensives
▫ Identité numérique et confidentialité
▫ Systèmes de sécurité décentralisés (par exemple, Blockchain)
▫ Autre : _____

Existe-t-il des méthodes, des outils ou des plateformes de formation particuliers qui, selon vous, sont exceptionnellement efficaces pour l'éducation à la cybersécurité ?
Question ouverte

Des commentaires ou suggestions supplémentaires pour améliorer la formation en cybersécurité pour les PME ?
Question ouverte

APERÇUS SPÉCIFIQUES AU GENRE

Quel est le pourcentage estimé de femmes parmi les participants à vos programmes de formation en cybersécurité ?
▫ Moins de 10 %
▫ 10 % - 25 %
▫ 26 % - 50 %
▫ 51 % - 75 %
▫ Plus de 75%

Existe-t-il des initiatives ou des stratégies spécifiques que vous employez pour encourager la participation des femmes à la formation en cybersécurité ?
▫ Oui
▫ Non
Si oui, veuillez préciser : _____

Pensez-vous qu'il existe suffisamment de modules de formation intégrant le genre dans le domaine de la cybersécurité ?
▫ Oui
▫ Non
▫ Je ne suis pas sûr
▫ Ne me concerne pas

D'après votre expérience, quels sont les principaux obstacles qui empêchent les femmes de participer ou de progresser dans les formations et les carrières en cybersécurité ?
(Sélectionnez tout ce qui s'y rapporte)
▫ Manque de sensibilisation aux opportunités en matière de cybersécurité
▫ Stéréotypes ou normes culturelles
▫ Manque de mentorat ou de modèles
▫ Défis liés à l'équilibre travail-vie personnelle
▫ Préjugés sexistes perçus dans l'industrie
▫ Autre : _____

Votre institution dispose-t-elle de politiques ou de programmes spécifiques pour promouvoir la diversité et l'inclusion, en particulier pour les femmes, dans la formation en cybersécurité ?
▫ Oui
▫ Non
▫ Je ne suis pas sûr
Qu'est-ce qui pourrait rendre la formation à la cybersécurité plus inclusive ? (Choisissez jusqu'à trois)
▫ Plus de femmes formatrices ou formatrices en cybersécurité
▫ Offrir des bourses ou des incitations
▫ Un contenu de formation qui évite les préjugés sexistes
▫ Visibilité accrue des professionnelles en cybersécurité à succès
▫ Plus de sessions de formation réservées aux femmes
▫ Études de cas et scénarios intégrant le genre
▫ Programmes de formation sur mesure
▫ Possibilités de mentorat
▫ Autres : _____

Questionnaire PME
Cette enquête vise à cartographier les besoins de formation des agents de changement en cybersécurité des PME. Vos réponses aideront à comprendre le paysage actuel des connaissances et des compétences en matière de cybersécurité dans diverses PME, à identifier les lacunes dans la formation en cybersécurité et à améliorer l'efficacité des futurs programmes de formation.

L'enquête est divisée en 3 sections :
- Démographie
- Besoins de formation
- Inclusivité et besoins des femmes en matière de cybersécurité.

L'enquête prendra environ 5 minutes pour être complétée.

DÉMOGRAPHIE
Quel est ton pays?
▫ Lituanie
▫ Belgique
▫ Norvège
▫ Turquie
▫ Finlande
▫ Roumanie
▫ Espagne
▫ Pologne
Quel est votre poste et département actuel dans l'entreprise ?
Position: _____
Département: _____
Quel est votre sexe ?
▫ Homme
▫ Femme
▫ Je préfère ne pas dire
Combien de salariés travaillent dans l'entreprise ?
▫ jusqu'à 10 salariés

▫ 11-50
▫ 51-250

Comment évalueriez-vous le niveau actuel de connaissances et de compétences des employés en matière de cybersécurité ?

▫ Débutant
▫ Intermédiaire
▫ Avancé

Combien d'employés effectuent des tâches liées à la cybersécurité ?

Insérer le nombre : _____

Faites-vous appel à des services externes pour des travaux de cybersécurité ?

▫ Oui
▫ Non

BESOINS DE FORMATION

Sur une échelle de 1 (inefficace) à 5 (très efficace), dans quelle mesure pensez-vous que les programmes de formation actuels préparent efficacement les étudiants aux défis réels de cybersécurité des PME ?

1- Inefficace
5- Très efficace

Selon vous, quels sont les principaux déficits de compétences parmi la main-d'œuvre actuelle en cybersécurité des PME ? (Choisissez jusqu'à trois)

▫ Détection des menaces et réponse
▫ Expertise en sécurité cloud
▫ Connaissances en matière de conformité et de réglementation
▫ Réponse aux incidents et récupération
▫ Gestion et analyse des risques
▫ Confidentialité et protection des données
▫ Technologies émergentes
▫ Sécurité du réseau
▫ Autre : _____

Please rate, from a scale from 1 (not needed) to 5 (essential) the competencies and knowledge needs:

	Evaluation				
Évaluation et gestion des risques Comprendre les types de risques et leur impact.					
Connaissance technique Aspects techniques de la cybersécurité et connaissance des systèmes d'exploitation, des réseaux et de la gestion de bases de données.					
Réponse aux incidents et récupération Identifier, répondre et récupérer des failles et des incidents de sécurité.					
Élaboration et mise en œuvre de politiques Élaborer et mettre en œuvre des politiques et des pratiques de sécurité efficaces.					
Intelligence et surveillance des menaces Se tenir au courant des dernières tendances, menaces et méthodologies d'attaque en matière de cybersécurité.					
Compétences en communication Communication efficace avec le personnel, la direction et éventuellement les clients sur les questions de cybersécurité.					
Confidentialité et protection des données Principes de confidentialité des données et comment protéger les informations sensibles.					

Connaissez-vous un ensemble pertinent de compétences et de connaissances non répertoriées dans la question précédente qui pourraient être extrêmement nécessaires pour les PME ?

Question ouverte

Selon vous, à quelles menaces émergentes en matière de cybersécurité les PME doivent-elles se préparer au cours des cinq prochaines années ? (Choisissez jusqu'à trois)

▫ Attaques de rançongiciels

▫ Vulnérabilités de l'IoT

▫ Failles de sécurité dans le cloud

▫ Cyberattaques basées sur l'IA

▫ Menaces internes

▫ Autre : _____

Selon vous, quelles sont les lacunes spécifiques, le cas échéant, dans les connaissances ou compétences actuelles des employés en matière de cybersécurité ?

▫ Faible niveau de compétences techniques

▫ Faible niveau de soft skills

▫ Faible niveau d'évaluation de la vulnérabilité

▫ Faible niveau de compréhension des politiques et des réglementations

▫ Faible niveau de sensibilisation aux menaces

▫ Faible niveau de formations régulières en cybersécurité

▫ Autre : _____

Selon vous, quelles seront les trois principales tendances émergentes en matière de formation en cybersécurité pour les 5 prochaines années ? (Choisissez jusqu'à 3 options)

▫ IA et apprentissage automatique en cybersécurité

▫ Focus sur les soft skills et la formation interdisciplinaire

▫ Menaces liées à l'informatique quantique

▫ Piratage éthique et compétences défensives

▫ Identité numérique et confidentialité

▫ Systèmes de sécurité décentralisés (par exemple, Blockchain)

▫ Autre : _____

INCLUSIVITÉ ET BESOINS DES FEMMES EN CYBERSÉCURITÉ

Pensez-vous que la formation actuelle en cybersécurité est inclusive et répond efficacement aux besoins de tous les genres ?

▫ Oui

▫ Non

▫ Je ne suis pas sûr

Si vous vous identifiez comme une femme, avez-vous rencontré des obstacles ou des difficultés pour accéder ou participer à des formations/études en cybersécurité ?

▫ Oui

▫ Non

▫ Je préfère ne pas dire

▫ Si oui, veuillez préciser : _____

Connaissez-vous des initiatives ou des programmes au sein de votre organisation qui soutiennent ou promeuvent spécifiquement la participation des femmes à la cybersécurité ?

▫ Oui

▫ Non

▫ Je ne suis pas sûr

Quels types de soutien ou de ressources encourageraient davantage de femmes dans votre organisation à participer à une formation en cybersécurité ? (ouvert)

Question ouverte

Quelles améliorations ou innovations suggéreriez-vous pour renforcer l'efficacité de la formation en cybersécurité ?

Question ouverte

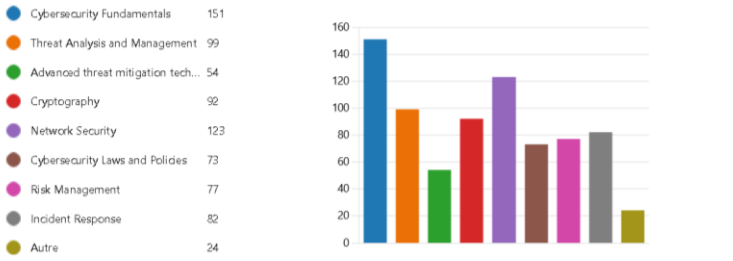
5.3. ANNEXE C: RÉSULATS DE L'ENQUÊTE

VET & HEI

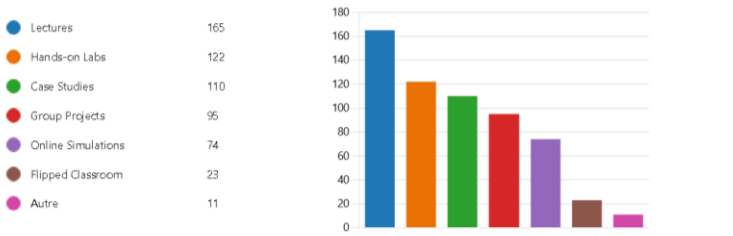
Mapping the training needs for SME Cyber Security Change Agents - VET and HEI survey

190 Responses

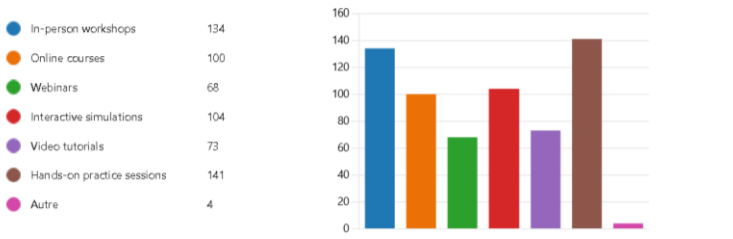
1. **Which of the following topics are included in your cybersecurity training program? (Select all that apply)**



2. **What teaching methods do you primarily use in your cybersecurity training? (Select all that apply)**



3. **What teaching method would be the most effective for cybersecurity training? (Select all that apply)**



4. **What are the biggest challenges you face in delivering effective cybersecurity training?**

190
Réponses

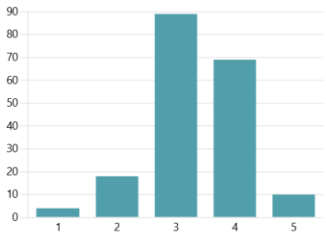
Dernières réponses
"-"
"-"
"keeping up with Technology Changes, Basic knowledge of the students, Soft...

Mettre à jour

34 répondants (**19**%) répondu **students** pour cette question.

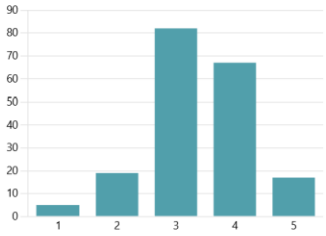
5. **On a scale of 1 (Very Ineffective) to 5 (Very Effective), how effectively do you think the current training programs prepare students for real-world SMEs cybersecurity challenges?**

3.33
Évaluation moyenne



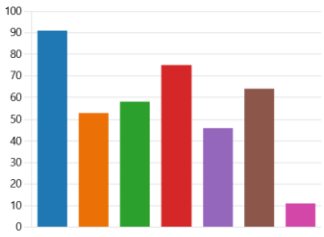
6. **On a scale of 1 (Not aligned) to 5 (Highly aligned), how well do you believe the current cybersecurity training aligns with the specific needs of SMEs?**

3.38
Évaluation moyenne



7. **Are there specific topics or skills that you include in your training to address the unique cybersecurity needs of SMEs? (Select all that apply)**

Basic Cybersecurity for SMEs	91
Risk Assessment and Managem...	53
Incident Response for SMEs	58
Data Protection and Privacy for ...	75
Cybersecurity Policy Developme...	46
No SME's specific topic or skills ...	64
Autre	11



8. **How often do you customize or adapt your cybersecurity training to better cater to SMEs?**

Always	14
Often	60
Sometimes	55
Rarely	47
Never	14

9. **Do you receive feedback or are you in contact with SME representatives or professionals to ensure the relevancy of your training content to their needs?**

Yes, regularly	43
Occasionally	64
Rarely	54
Never	29

10. **Based on your experience, how effective do you believe the current cybersecurity training is in equipping SME professionals to handle cybersecurity challenges?**

Very Ineffective	7
Somewhat Ineffective	21
Neutral	65
Somewhat Effective	88
Very Effective	9

11. **What suggestions do you have for improving the relevance and effectiveness of cybersecurity training for SMEs?**

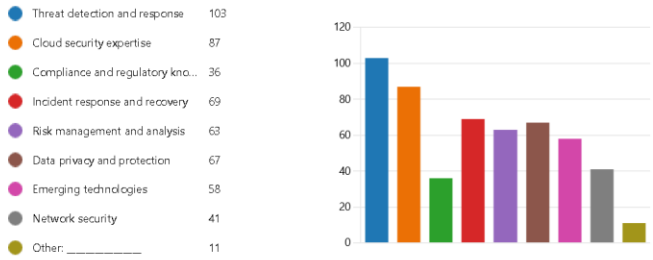
117
Réponses

Dernières réponses
"leverage external expertise, practical hands-on exercises, interactive training...

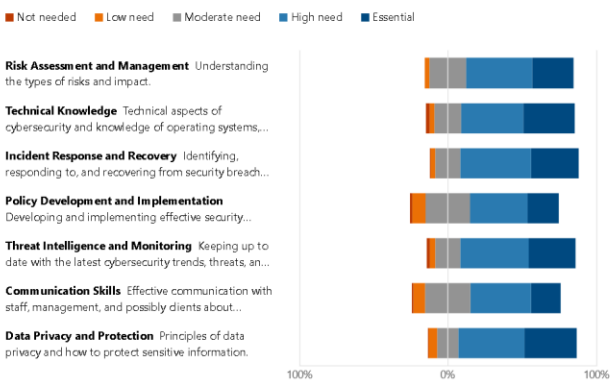
Mettre à jour

36 répondants (**31**%) répondu **trainings** pour cette question.

12. **In your opinion, what are the top skills deficits in the current SME cybersecurity workforce? (Choose up to three)**



13. **Please rate, from a scale from 1 (not needed) to 5 (essential) the competencies and knowledge needs:**



14. **Do you see any relevant set of skills and knowledge not listed in the previous question that might be highly needed for SMEs?**

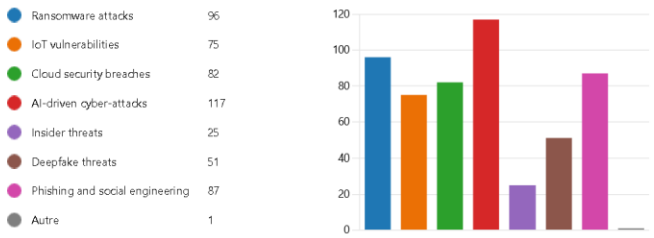
190
Réponses

Dernières réponses
"-"
"-"
"Cloud Security, AI"

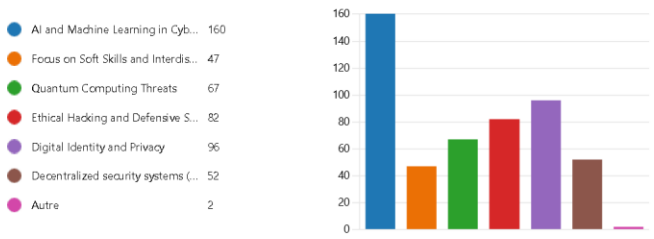
Mettre à jour

10 répondants (**5**%) répondu **skills** pour cette question.

15. **Which emerging cybersecurity threats do you believe SMEs need to be prepared for in the next 5 years? (Choose up to three)**



16. **What do you foresee as the top 3 emerging trends in cybersecurity training for the next 5 years? (Choose up to 3 options)**



17. **Are there any particular training methods, tools, or platforms that you believe are exceptionally effective for cybersecurity education?**

115
Réponses

Dernières réponses
"TryHackMe, HackTheBox"

Mettre à jour

12 répondants (**11**%) répondu **platform** pour cette question.

18. **Any additional comments or suggestions for improving cybersecurity training for SMEs?**

80
Réponses

Dernières réponses
"Uniform Course material"

Mettre à jour

9 répondants (**11**%) répondu **SMEs** pour cette question.

19. **What is the estimated percentage of women among the participants in your cybersecurity training programs?**

Less than 10%	57
10% - 25%	79
26% - 50%	43
51% - 75%	8
More than 75%	3

20. **Are there any specific initiatives or strategies you employ to encourage women's participation in cybersecurity training?**

Yes	30
No	160

21. **If you replied "Yes" to the previous question, please specify**

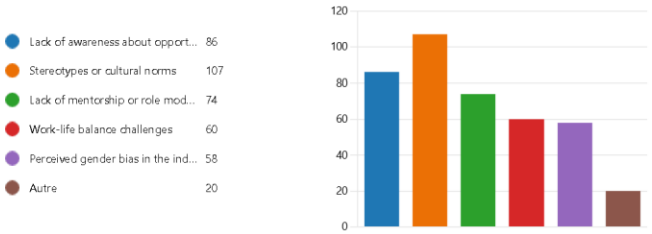
35
Réponses

Dernières réponses

13 répondants (**37**%) répondu **women** pour cette question.

22. **Do you believe there are enough gender-inclusive training modules available in cybersecurity?**

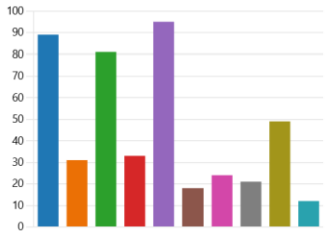
23. **In your experience, what are the primary barriers that prevent women from participating or advancing in cybersecurity training and careers? (Select all that apply)**



24. **Does your institution have specific policies or programs to promote diversity and inclusion, particularly for women, in cybersecurity training?**

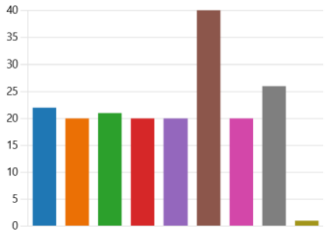
25. **What could make cybersecurity training more gender-inclusive? (Choose up to three)**

More female cybersecurity instr...	89
Regularly update policies to sup...	31
Offer scholarships or incentives	81
Training content that avoids gen...	33
Increased visibility of successful ...	95
More women-only training sessi...	18
Gender-inclusive case studies a...	24
Tailored training programs	21
Mentorship opportunities	49
Autre	12



26. **What is your country?**

Lithuania	22
Belgium	20
Norway	21
Türkiye	20
Finland	20
Romania	40
Spain	20
Poland	26
Azerbaijan	1



27. **In which school institution are you currently teaching?**

VET (Vocational Education and T...	86
HEI (Higher Education (HE) Instit...	104

28. **What is your gender?**

Male	121
Female	64
Prefer not to say	5

29. **How many years have you been involved in cybersecurity training? (Either general, specific, short and long trainings)**

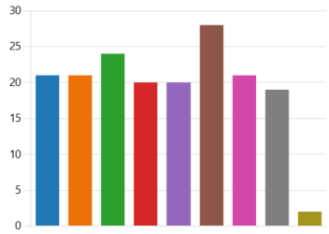
Less than 1 year	21
1-5 years	85
6-10 years	53
More than 10 years	31

Mapping the training needs for SME Cyber Security Change Agents - SMEs survey

176 Responses

1. **What is your country?**

Lithuania	21
Belgium	21
Norway	24
Türkiye	20
Finland	20
Romania	28
Spain	21
Poland	19
Azerbaijan	2



2. **What is your company sector?**

176
Réponses

Dernières réponses
"Consultancy"
"Cyber Security - Management Consultancy"
"Education, VET"

Mettre à jour

13 répondants (**7**%) répondu **education** pour cette question.

3. **What is your current position in the company?**

176
Réponses

Dernières réponses
"Team lead"
"Owner & Director"
"Teacher"

Mettre à jour

43 répondants (**25**%) répondu **Manager** pour cette question.

4. **What is your gender?**

5. **How many employees are working in the company?**

6. **How would you rate employees' current level of cybersecurity knowledge and skills?**

7. **How many employees perform work related to cybersecurity?**

176
Réponses

Dernières réponses
"3"
"2"
"3"

Mettre à jour

36 répondants (**21**%) répondu **1** pour cette question.

8. **How many of these employees are women?**

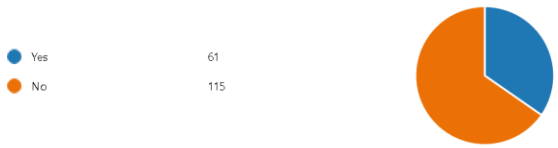
176
Réponses

Dernières réponses
"1"
"1"
"0"

Mettre à jour

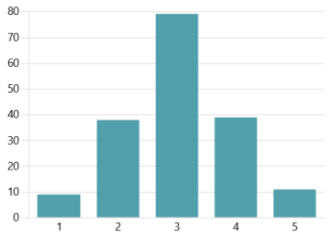
31 répondants (**18**%) répondu **1** pour cette question.

9. **Do you hire external services for cybersecurity work?**



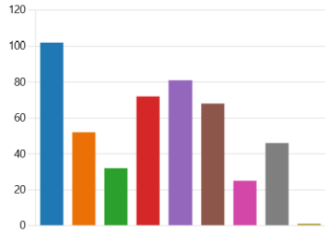
10. **On a scale of 1 (ineffective) to 5 (very effective), how effectively do you think the current training programs prepare students for real-world SMEs cybersecurity challenges?**

3.03
Évaluation moyenne

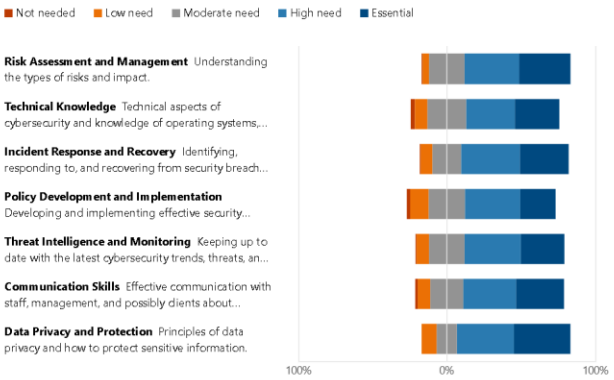


11. **In your opinion, what are the top skills deficits in the current SME cybersecurity workforce? (Choose up to three)**

Threat detection and response	102
Cloud security expertise	52
Compliance and regulatory kno...	32
Incident response and recovery	72
Risk management and analysis	81
Data privacy and protection	68
Emerging technologies	25
Network security	46
Other: _____	1



12. **Please rate, from a scale from 1 (not needed) to 5 (essential) the competencies and knowledge needs:**



13. **Do you see any relevant set of skills and knowledge not listed in the previous question that might be highly needed for SMEs?**

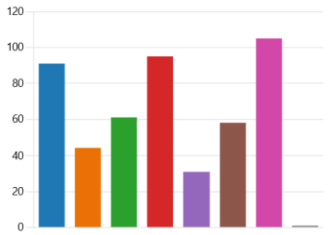
175
Réponses

Dernières réponses
"My assumption is that Subject matter experts (SME's) in a big company are ...
"Cyber Security on all these topics arround Generative AI - which is complete...
"Not sure"

4 répondants (**2**%) répondu **skills** pour cette question.

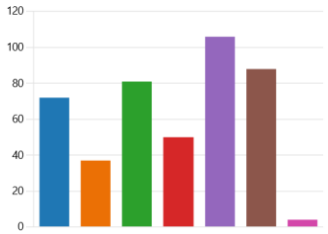
14. **Which emerging cybersecurity threats do you believe SMEs need to be prepared for in the next 5 years? (Choose up to three)**

Ransomware attacks	91
IoT vulnerabilities	44
Cloud security breaches	61
AI-driven cyber-attacks	95
Insider threats	31
Deepfake threats	58
Phishing and social engineering	105
Autre	1



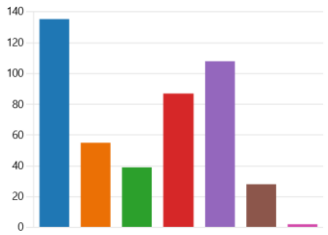
15. **What specific gaps, if any, do you feel exist in employee's current cybersecurity knowledge or skills status? (Choose up to three)**

Low level of Technical skills	72
Low level of Soft skills	37
Low level of Vulnerability assess...	81
Low level of Policy and regulatio...	50
Low level of Threat awareness	106
Low level of Cybersecurity regul...	88
Autre	4



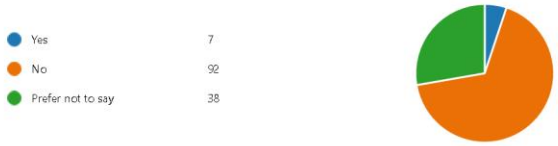
16. **What do you foresee as the top 3 emerging trends in cybersecurity training for the next 5 years? (Choose up to 3 options)**

AI and Machine Learning in Cyb...	135
Focus on Soft Skills and Interdis...	55
Quantum Computing Threats	39
Ethical Hacking and Defensive S...	87
Digital Identity and Privacy	108
Decentralized security systems (...	28
Autre	2



17. **Do you feel that current cybersecurity training is inclusive and addresses the needs of all genders effectively?**

18. **If you identify as female, have you faced any barriers or challenges in accessing or participating in cybersecurity training/studies?**



19. **If you replied "Yes" to the previous question, please specify**

11
Réponses

Dernières réponses
"I feel that previous question is missing one more answer such as "I'm a male...
"I have to actively look for help and support for us females who work in the C...

Mettre à jour

3 répondants (**30**%) répondu **male** pour cette question.

20. **Are you aware of any initiatives or programs within your organization that specifically support or promote the participation of women in cybersecurity?**

21. **If you replied "Yes" to the previous question, please specify**

17
Réponses

Dernières réponses
"I am a strong female advocate for Cyber Security, Women Supporting Wom..."

8 répondants (**47**%) répondu **Women** pour cette question.

5.4. ANNEXE D: LISTE DES OCCUPATIONS ESCO EXAMINÉES

References:

2529.1 https://esco.ec.europa.eu/sites/default/files/chief%20ICT%20security%20officer.pdf
2529.2 https://esco.ec.europa.eu/sites/default/files/digital%20forensics%20expert.pdf
2529.3 https://esco.ec.europa.eu/en/classification/occupation?uri=http%3A%2F%2Fdata.europa.eu%2Fesco%2Foccupation%2F1c5a896a-e010-4217-a29a-c44db26e25da
2529.4 https://esco.ec.europa.eu/sites/default/files/ethical%20hacker.pdf
2529.5 https://esco.ec.europa.eu/sites/default/files/ICT%20resilience%20manager.pdf
2529.6 https://esco.ec.europa.eu/sites/default/files/ICT%20security%20administrator.pdf
2529.7 https://esco.ec.europa.eu/sites/default/files/ICT%20security%20consultant.pdf
2529.8 https://esco.ec.europa.eu/sites/default/files/ICT%20security%20manager.pdf
2529.9 https://esco.ec.europa.eu/sites/default/files/knowledge%20engineer.pdf

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

TEKNOPARK ISTANBUL Mesleki ve Teknik ANADOLU LİSESİ

HackerU by ThriveDX

Olemisen Balanssia ry

WOMEN 4CYBER European Cyber Security Organisation

Liceul Tehnologic Grigore C. Moisil Buzau