Co-funded by the European Union

STRUCUTRE DU PARCROUS D'APPRENTISSAGE DES *CYBER CHANGE AGENTS* POUR LES PME

CYBER AGENT 06.2024

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

Work Package 2: CyberAgent approach and structure design

Deliverable 2.3: SME Cyber Security Change Agents learning pathway's structure

Leader of WP2 – Olemisen Balanssia ry
Leader of deliverable 2.3 – Vilnius University

CONTENT

ABBRÉVIATIONS (ANGLAIS)

CBL – Challenge-Based Learning Model

CL – Cooperative Learning Model

EC – European Commission

ECTS – European Credit Transfer and Accumulation System

EQF – European Qualifications Framework

GICL – Guided Inquiry Collaborative Learning Model

HEI – Higher Education Institutions

PBL – Project-Based Learning Model

POGIL – Process Oriented Guided Inquiry Learning Model

SME – Small and Medium Enterprises

VET – Vocational Education Institutions

LISTE DES FIGURES

LISTE DES TABLEAUX

INTRODUCTION

L'objectif général de ce rapport est de développer et de décrire de nouveaux parcours d'apprentissage professionnel pour améliorer les compétences en cybersécurité des employés des PME (petites et moyennes entreprises) européennes.

Sur la base des résultats de la cartographie des besoins de formation des agents de changement en cybersécurité des PME, une analyse des ressources externes des résultats d'apprentissage en termes de connaissances, d'aptitudes et de compétences a été identifiée. Suite à l'analyse des acquis d'apprentissage identifiés, ce rapport fournit des orientations sur deux types de programmes de formation du CEC (Cadre européen des certifications)niveau 4 à 6 pour couvrir l'éventail des compétences et des connaissances requises pour les groupes cibles du projet, les salariés des PME et les étudiants, et adapter les acquis de la formation aux différents parcours et profils des stagiaires.

- Le niveau 4-5 du CEC sera mis en œuvre pour les employés des PME qui n'ont pas de formation dans un établissement d'enseignement supérieur ni pour les études d'EFP (enseignement et formation professionnels). Ce niveau fournira les compétences et connaissances fondamentales en matière de cybersécurité avec une spécialisation légère dans certains modules.
- Le niveau CEC 5-6 qui sera proposé aux salariés des PME qui disposent également d'une formation adéquate pour le suivre et aux étudiants des HEI (établissements d'enseignement supérieur). À ce niveau, des activités de formation plus avancées et plus complexes seront réalisées.

Il a été décidé de mettre à jour les niveaux du CEC entre 4 et 6, non seulement pour couvrir un large éventail d'acquis d'apprentissage, comme mentionné précédemment, mais également pour permettre une passerelle entre les programmes de formation en tant que parcours de perfectionnement permettant aux étudiants et aux employés de l'EFP de niveau 4 d'atteindre le niveau 4. niveau 6.

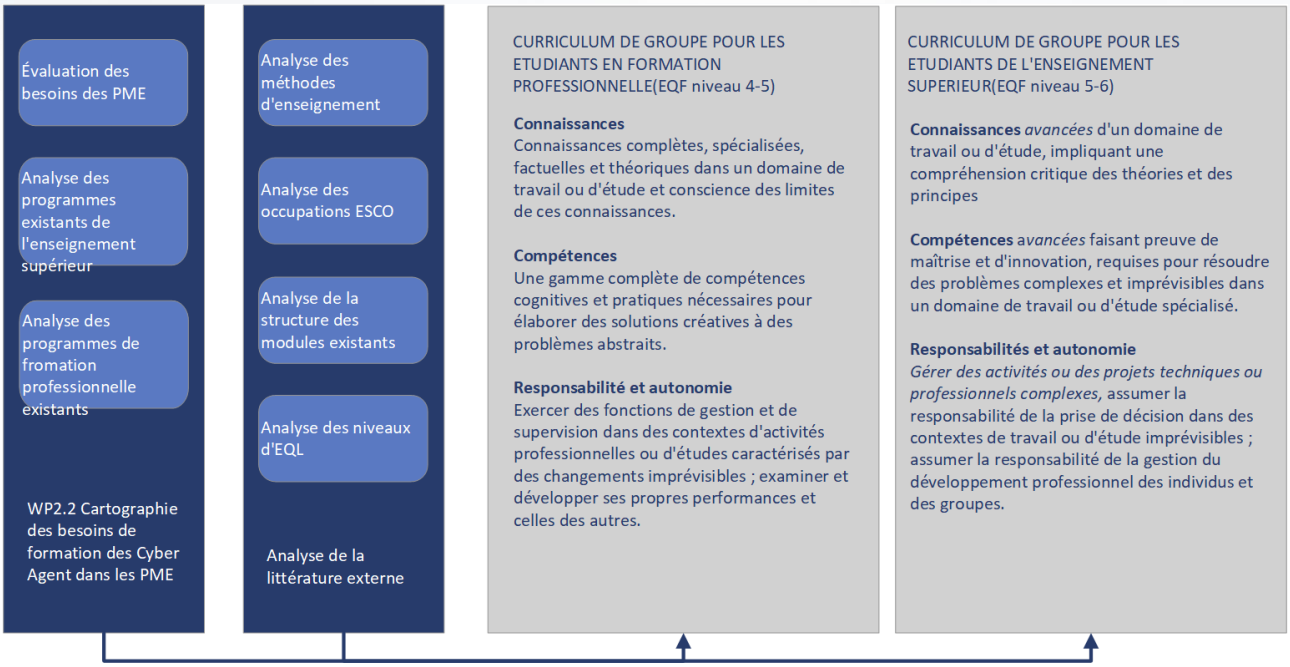

Figure 1. Un diagramme illustratif, conforme aux directives de la CE, représente les huit niveaux du CEC, fournissant une représentation visuelle du cadre éducatif.[1]

Le programme aborde les résultats d'apprentissage et la nécessité de former les employés des PME à se perfectionner pour remplir le rôle d'agents de changement en matière de cybersécurité dans les PME et d'éduquer les étudiants des établissements d'enseignement supérieur et de l'EFP pour qu'ils remplissent ce rôle après leurs études. Chaque programme comprend huit modules couvrant quatre sous-thèmes :

- Compétences techniques - Connaissance actualisée des menaces de cybersécurité et des questions juridiques connexes - Connaissance pratique de la manière de gérer les menaces de cybersécurité.
- Compétences analytiques - Esprit critique - Capacité à analyser et à comprendre les menaces locales, comment elles se produisent, les personnes à risque, etc.
- Gestion des risques - Apprenez à fournir et à décrire les lieux de travail des PME avec des routines de cybersécurité - Créez votre propre manuel PME sur le lieu de travail pour la cybersécurité et comment en assurer le suivi.
- Compétences organisationnelles - Comment mettre en œuvre de nouvelles routines et méthodes de travail en matière de cybersécurité sur les lieux de travail des PME ; Assurer l'accompagnement des leaders en cybersécurité.

En outre, un élément central de la création de parcours d'apprentissage permettant de perfectionner les compétences en matière de cybersécurité parmi les PME européennes est la manière dont les micro-certificats seront mis en œuvre. Ils doivent faire référence aux acquis d'apprentissage (connaissances, aptitudes et compétences), au contenu des cours, à la formation

[1] https://europa.eu/europass/en/description-eight-eqf-levels

(connaissances, aptitudes et compétences), aux éléments de gamification, à la durée et au nombre d'ECTS (Système européen de transfert et d'accumulation de crédits). Pour atteindre cet objectif, ils doivent être mis en œuvre grâce à l'établissement de partenariats entre les établissements d'enseignement supérieur, les prestataires d'EFP et les entreprises privées du secteur de la cybersécurité.

Les micro-sections offrent aux apprenants plus de liberté pour choisir des modules ou des parties de modules et pour décider du niveau de certificat dont ils ont besoin : certificats de participation ou certificat de fin de cours avec test de certification, c'est-à-dire la preuve que le cours a été complété par l'acquisition d'un compétence. Des certificats de fin de cours sont délivrés pour la réussite du test final avec un score d'au moins 75 %, et des certificats de participation sont délivrés pour suivre une formation en face à face, un apprentissage mixte ou une formation en ligne sur des sujets/modules spécifiques. Cette pratique augmente non seulement l'applicabilité et l'efficacité de la formation, mais stimule également la motivation pour l'apprentissage, offrant une perspective de valeur claire pour la carrière et le développement futur des participants.

Dans l'ensemble, ce rapport présente des guides détaillés pour le développement de modules CyberAgent, y compris le contenu des parcours d'études et de carrière, les méthodologies de formation et d'évaluation et la feuille de route pour l'élaboration du programme d'études.

1. PARCOURS D'ÉTUDES

Un parcours d'apprentissage est un parcours complet que le participant suit depuis le moment où il réalise qu'il a besoin d'améliorer ses compétences, de commencer et de terminer une formation, jusqu'au moment où il termine son apprentissage et commence à appliquer les connaissances acquises. Il y a 3 étapes dans un parcours d'apprentissage :

- Pré-apprentissage,
- Apprentissage,
- Post-apprentissage.

La phase de pré-apprentissage est illustrée dans la figure ci-dessous.

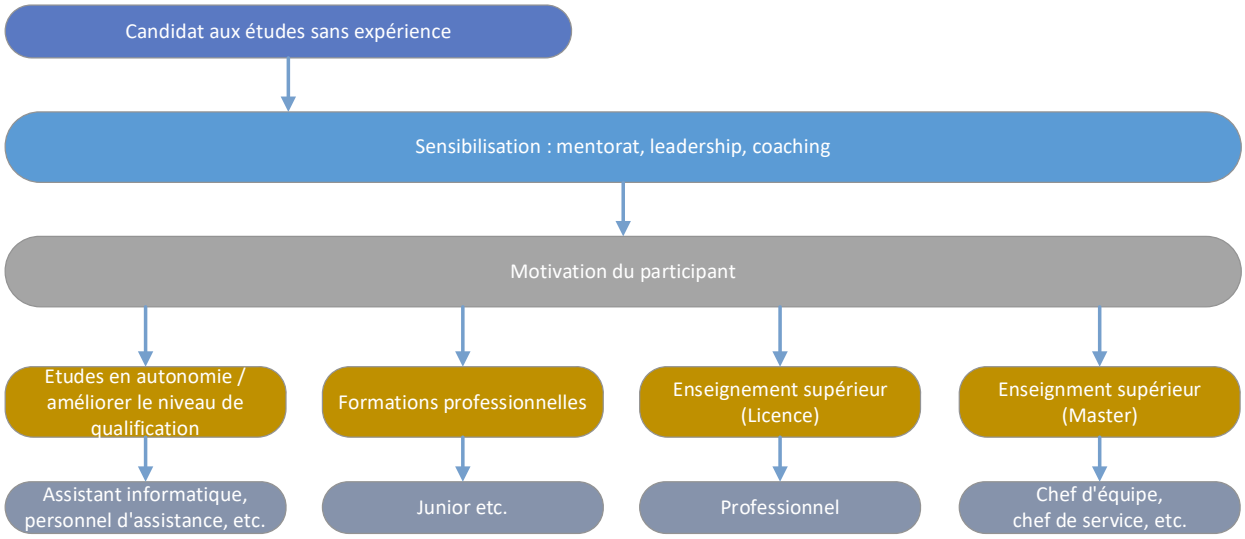

Figure 2. Parcours d'apprentissage avant le début des études

Dans le cadre des PME, ce parcours d'apprentissage/études peut être poursuivi. Dans la figure, soit le participant décide de se former lui-même, soit il est influencé par une campagne de sensibilisation et comprend les avantages de la formation, les opportunités et les carrières qui peuvent être acquises après la formation.

Un parcours d'apprentissage sous forme de module typique via la structure OLE (Online Learning Environment) a également été proposé. Après une analyse de la littérature et plusieurs projets appliquant le principe des micro-certificats[2],[3],[4]chaque module CyberAgent est proposé pour 1 à 5

[2]Nausėdaitė, R., Juška, V., Daunorienė, A. et Ukvalbergienė, K. (2022). Aller de l'avant et au-delà dans l'éducation : concept de parcours d'apprentissage flexibles. Dans les livres électroniques KTU leidykla « Technologie ».https://doi.org/10.5755/e01.9786090218204

[3] https://arqus-alliance.eu/call/arqus-microcredential-development-f2f-workshop/

[4] https://www.youtube.com/watch?v=ECH0VvHIyRI,https://ndma.lt/alta2023/

ECTS (chaque ECTS représente 25 à 30 heures de charge de travail) et commence par une introduction et est ensuite divisé en thèmes, qui sont des sous-thèmes.

A la fin des sujets, un test d'auto-évaluation composé de plusieurs questions est proposé. Le matériel de formation du module doit prendre en charge l'étude de 6 à 8 sujets, dans chacun desquels se trouvent 4 à 6 sous-thèmes. Le cours peut se conclure par un test de connaissances, qui n'est pas obligatoire. Cela donne aux salariés des PME et aux étudiants des établissements de formation la possibilité d'acquérir et de démontrer les compétences acquises dans un module ou une partie spécifique de la formation.

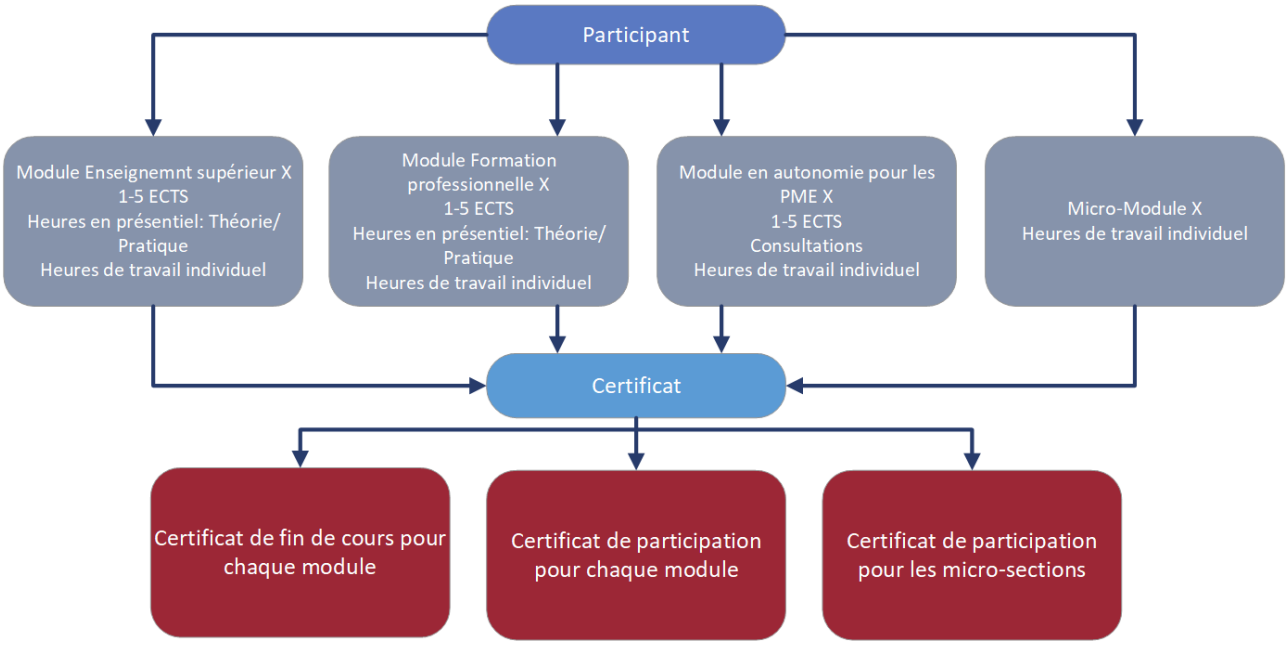

Figure 3. Structure des études

Les micro-certificats sont intégrés au processus d'apprentissage à travers les activités clés suivantes :

- Développement de modules de formation : chaque module doit être soigneusement formulé en tenant compte des connaissances et compétences spécifiques requises dans le secteur des PME, avec des objectifs, des acquis d'apprentissage, des méthodes d'enseignement et d'apprentissage et une durée de cours clairs.
- Tâches et projets pratiques : les apprenants réalisent des tâches pratiques et développent des projets qui sont évalués et témoignent clairement des compétences acquises.
- Stratégie d'évaluation des connaissances et critères d'évaluation clairement décrits : à la fin de chaque module, une évaluation des connaissances est organisée pour déterminer si le participant a atteint les acquis d'apprentissage requis et s'il est éligible à un certificat pour le prouver.

Le groupe cible du projet étant constitué des salariés des PME, des étudiants des HEI et de l'EFP, quatre types d'études sont disponibles, en fonction des possibilités et des besoins des apprenants :

- Études Enseignement supérieur : 8 modules, chacun de 1 à 5 ECTS, comprenant des heures de contact (théorie et pratique) et des heures de travail individuelles ;
- Études d'EFP : 8 modules de 1 à 5 ECTS chacun, comprenant des heures de contact (théorie et pratique) et des heures de travail individuelles ;
- Formation en autonomie (pour les PME) : 8 modules, chacun de 1 à 5 ECTS, comprenant des consultations (si nécessaire) et des heures de travail individuelles ;
- Micro-modules : heure de travail individuelle en fonction du nombre de thèmes choisis.

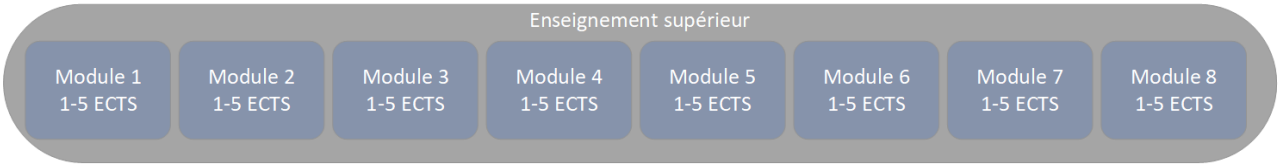

Figure 4. Structure d'études pour l'enseignement supérieur

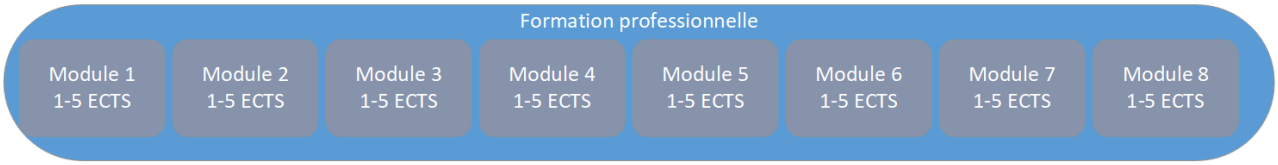

Figure 5. Structure d'études pour l'EFP

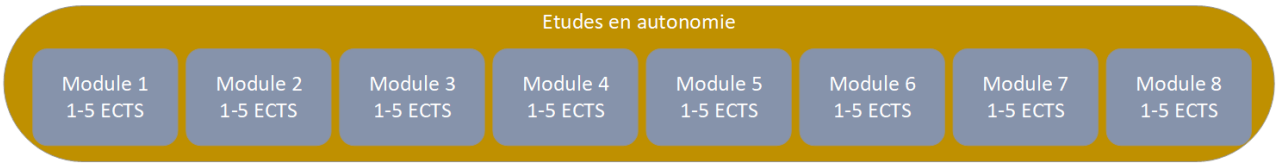

Figure 6. Structure d'études pour les formations en autonomie

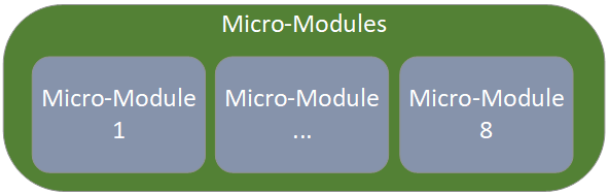

Figure 7. Structure d'études pour les micro-modules

Les étudiants de l'enseignement supérieur et de l'EFP pourront étudier un module de 1 à 5 crédits chacun. Les PME pourront suivre un module à la fois, ou nous pourrons peut-être proposer des micro-modules dans le cadre du cours.

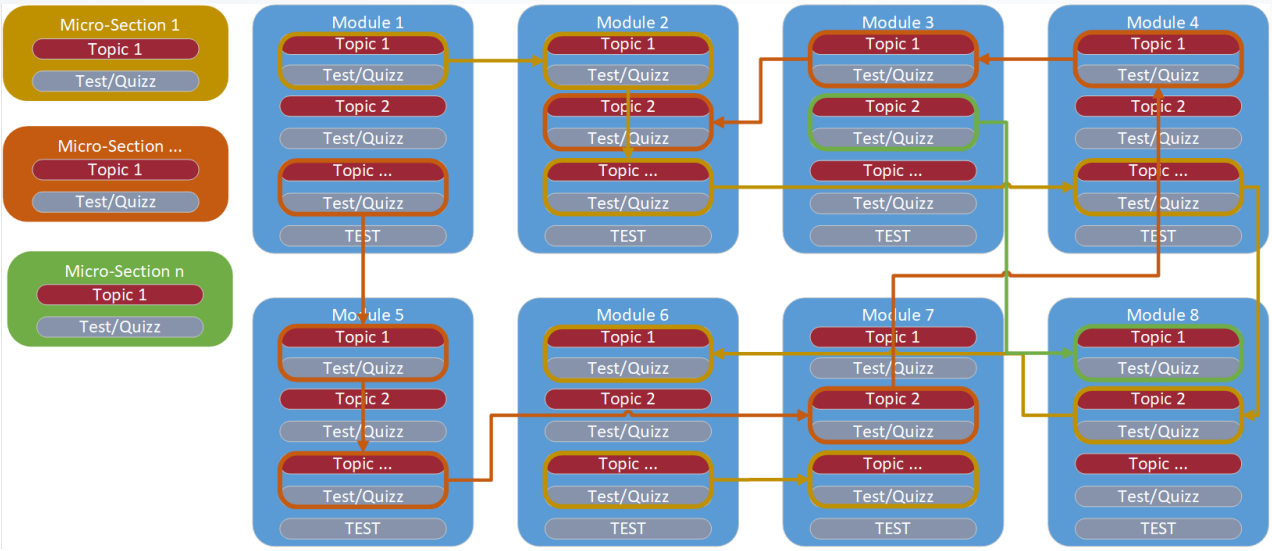

Figure 8. Liens entre les parcours d'apprentissage

Dans les trois types d'apprentissage (EES, EFP, PME), les étudiants étudient 8 modules. Dans le cas des micro-modules, l'étudiant choisit les modules selon son propre choix. Échap

Les micro-modules sont des expériences d'apprentissage courtes ou longues évaluées de manière transparente. Ils sont relevés par le participant avec le défi ou séparément. Chaque micro-module est évalué avec une quantité différente de mesure de la charge de travail d'apprentissage (telle que l'ECTS) et se termine par une évaluation. La réussite de l'évaluation des micro-modules récompense les apprenants avec des micro-certificats.

La proposition est que chaque module du programme HEI puisse être modularisé en un micro-module, chacun comportant des tâches spécialisées et un plan de mise en œuvre détaillé. Les résultats des tests peuvent être évalués au moyen de badges, basés sur des images et universellement lisibles par les ordinateurs. Ces images embarquent des métadonnées détaillant les compétences associées à chaque badge et des informations sur le participant qui le détient.

Le micro-certificat désigne l'enregistrement des résultats d'apprentissage qu'un participant a acquis après un petit volume d'apprentissage. Ces acquis d'apprentissage auront été évalués selon des critères transparents et clairement définis. Les expériences d'apprentissage menant à des micro-certificats sont conçues pour fournir au participant des connaissances, des aptitudes et des compétences spécifiques qui répondent aux besoins sociétaux, personnels, culturels ou du marché du travail.[5],[6].

[5] Nausėdaitė, R., Juška, V., Daunorienė, A., & Ukvalbergienė, K. (2022). Moving Forward and Beyond in Education: Concept of FLEXIBLE LEARNING PATHWAYS. In KTU leidykla "Technologija" eBooks. https://doi.org/10.5755/e01.9786090218204

[6] Council Recommendation of 16 June 2022 on a European Approach to Micro-Credentials for Lifelong Learning and Employability." Official Journal of the European Union, vol. 2022/C, 16 June 2022, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022H0627(02)&from=EN

2. VOIE PROFESSIONELLE

Le parcours post-apprentissage pourrait être appelé parcours de carrière. Au début du projet, l'analyse de la recherche sur les professions ESCO (décrite dans le rapport : D2.2 - Le rapport de cartographie des besoins en formation des agents de changement en matière de cybersécurité des PME) a été réalisée. L'analyse menée en trois phases visait à enquêter sur différents métiers de la cybersécurité répertoriés dans le cadre ESCO. Dans la première phase, les métiers liés à la cybersécurité ont été identifiés et documentés à partir du **Portail ESCO**, mettant en valeur leurs aptitudes, compétences et connaissances respectives. Ces professions comprenaient des rôles tels que responsable de la sécurité des TIC, expert en criminalistique numérique, ingénieur en sécurité des systèmes embarqués, pirate informatique éthique, responsable de la résilience des TIC, administrateur de la sécurité des TIC, ingénieur en sécurité des TIC, responsable de la sécurité des TIC et ingénieur des connaissances. Chaque profession a été définie par ses responsabilités spécifiques et ses domaines d'intervention dans le domaine de la cybersécurité, allant des fonctions de sécurité d'entreprise à la criminalistique numérique, en passant par le piratage éthique et la planification de la résilience.

Au cours de la deuxième phase, un tableau a été rempli pour chaque profession ESCO examinée, détaillant son titre et ses principales responsabilités. Celles-ci comprenaient des tâches telles que la planification et la mise en œuvre de mesures de sécurité, la réalisation d'évaluations de vulnérabilité, le développement de modèles de résilience et de reprise après sinistre et l'intégration des connaissances dans les systèmes informatiques.

De plus, la troisième phase consistait à cartographier les professions ESCO avec les résultats d'apprentissage associés, en les catégorisant en connaissances, aptitudes et compétences. Ce processus a facilité une compréhension globale des exigences de formation et des compétences attendues pour chaque rôle en matière de cybersécurité, garantissant ainsi l'alignement avec les normes et les meilleures pratiques de l'industrie. À travers ces phases, l'analyse a fourni des informations précieuses pour la poursuite des recherches.

Figure 9. Métiers ESCO définies dans le rapport précédent

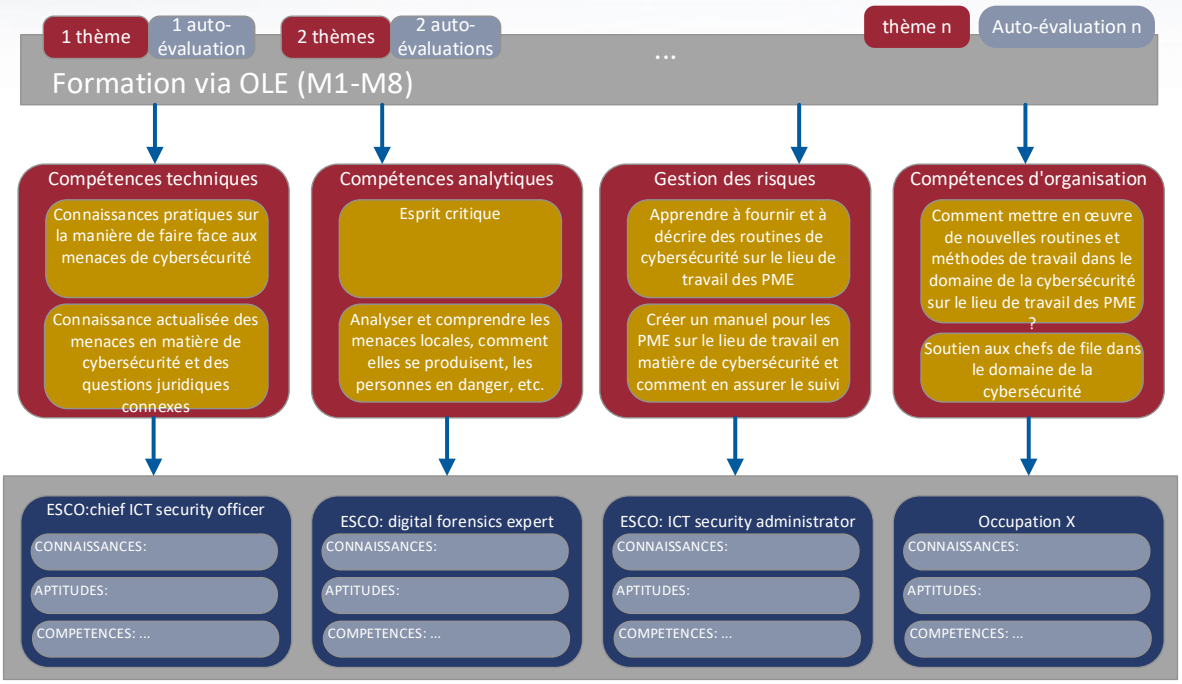

Figure 10. Parcours post-apprentissage possibles

La figure 10 illustre les parcours professionnels potentiels qui peuvent être poursuivis après l'achèvement d'études via OLE (environnement d'apprentissage en ligne) (EES, VET, PME) et l'acquisition de compétences, alignées sur les métiers ESCO.

Grâce à une meilleure compréhension des opportunités de carrière, les étudiants des HEI et de l'EFP qui étudient la cybersécurité comprendront mieux les options de carrière et seront en mesure de choisir un autre domaine d'études ou de travailler dans des entreprises à des postes spécifiques, tandis que les étudiants en informatique et autres pourront choisir les modules CyberAgent comme modules d'étude individuels, améliorant ainsi leurs compétences dans le domaine d'études, telles que les compétences organisationnelles et de gestion des risques, etc.

Le personnel des PME aura la possibilité de perfectionner et de développer ses compétences professionnelles. Sur la base du parcours professionnel développé et des opportunités de carrière claires, d'autres collaborateurs de PME pourront se reconvertir dans le domaine de la cybersécurité.

Une implication accrue des étudiants et du personnel des PME est prévue grâce à l'intégration de programmes de mentorat, à l'organisation d'événements de diffusion, d'ateliers (le projet comprend 6 ateliers conjoints organisés par tous les partenaires, ainsi que des campagnes de diffusion organisées par chaque partenaire), en invitant les entreprises et représentants de la cybersécurité, coopération avec les partenaires sociaux et le réseau CyberAgent, offre de stages aux étudiants, etc. Par ailleurs, nos initiatives en matière de diversité, notamment des programmes de sensibilisation et de soutien ciblés, visent à renforcer la participation des femmes, en favorisant un personnel de cybersécurité inclusif.

En mappant de manière exhaustive les métiers ESCO à nos modules de formation CyberAgent, les participants peuvent passer en toute transparence des environnements d'apprentissage à des rôles importants dans la cybersécurité. Afin de suivre l'évolution de carrière des stagiaires CyberAgent, il est prévu d'organiser des enquêtes pré-formation, post-formation et 3 mois post-formation pour découvrir comment leurs compétences contribuent à la cybersécurité des organisations dans lesquelles ils travaillent. sera intégré à la plateforme de formation et sera proposé automatiquement aux stagiaires avant le début du cours, à la fin du cours pour mesurer les progrès et évaluer le cours et la qualité de la formation. Une troisième enquête permettra de savoir s'il y a eu des changements dans la carrière des participants.

3. MÉTHODES D'ENSEIGNEMENT

L'analyse des méthodes pédagogiques du programme d'études Systèmes d'information et Cybersécurité de l'Université de Vilnius (VU), des programmes d'études Timtal et Moisil Buzau et de la littérature externe nous permet de recommander plusieurs combinaisons innovantes de méthodes d'enseignement. Ces combinaisons pourraient être incluses dans les modules d'étude, en tenant compte de la structure de chaque.[7]

Tableau 1. Méthodes d'enseignement recommandées

Catégorie	Détails
Cours magistral and enseignement direct	- **Cours théoriques :**concepts et théories fondamentaux. - **Conférenciers invités**((spécialistes certifiés en : Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM), CompTIA Security+, Certified Ethical Hacker (CEH), GIAC Security Essentials Certification (GSEC), Systems Praticien certifié en sécurité (SSCP), Praticien en sécurité avancé CompTIA (CASP+), Gestionnaire d'incidents certifié GIAC (GCIH), Professionnel certifié en sécurité offensive (OSCP))).

Apprentissage pratique	- **Tâches pratiques/laboratoires :**expériences pratiques et exercices pratiques.
	- **Des activités pratiques**: applications du monde réel et tâches interactives.
	- **Analyse vidéo technique :**analyse du contenu vidéo pour l'apprentissage de compétences techniques.
	- **Environnements simulés**:
	  o Machines hébergées pour environnement cloud.
	  o Lancez des attaques sur une machine cible.
	  o Machine pour planifier et exécuter des attaques – une boîte d'attaque.

[7] Teaching Cybersecurity: A Project-Based Learning and Guided Inquiry Collaborative Learning Approach https://scholar.utc.edu/cgi/viewcontent.cgi?article=1945&context=theses

Catégorie	Détails
Estimation et évaluation	- **Quiz, jeux, choses à faire et à ne pas faire**: Évaluations engageantes et interactives. - **Tests d'auto-évaluation**: Pour l'auto-évaluation de l'apprenant à la fin des sujets.
Formation en autonomie	- **Apprentissage autoguidé :**cette méthode prend en charge des parcours d'apprentissage personnalisés et peut être enrichie de ressources numériques et de contenus modulaires auxquels les étudiants peuvent accéder selon leurs besoins.
Apprentissage collaboratif et entre pairs	- **Apprentissage collaboratif, travail d'équipe**: projets de groupe et tâches collaboratives. - **Enseignement et apprentissage entre pairs**: les apprenants enseignent et apprennent les uns des autres. - **Mentorat de groupe et/ou mentorat individuel**: encadrement assuré par des personnes plus expérimentées.
Apprentissage soutenu par la technologie	- **Utilisation d'une plateforme d'apprentissage gamifiée en cybersécurité**: engager les apprenants à travers des éléments de type jeu dans les plateformes d'apprentissage. - **Capturez les compétitions de drapeau**: des événements compétitifs pour renforcer les compétences en cybersécurité. - **Compétitions**: les concours testent les compétences et les connaissances des étudiants dans un cadre pratique et appliqué et fournissent une mesure de leurs compétences dans un format compétitif.
Engagement communautaire et public	- **Événements pédagogiques :**des événements spéciaux lors d'initiatives comme le Mois de la cybersécurité. - **Présentations publiques**: séminaires, conférences et webinaires.

Catégorie	Détails
	- **Réseaux sociaux**: utilisation des médias et réseaux sociaux pour l'apprentissage et l'engagement. - **Campus de jour** : implique généralement des événements immersifs sur le campus qui peuvent inclure des ateliers, des conférences et des opportunités de réseautage
Modèles d'apprentissage innovants	- **Modèle pédagogique BSCS 5E (5E)**– les 5E se concentrent sur les phases suivantes qui consistent en : Engagement, Exploration, Explication, Élaboration, Évaluation. - **Modèle d'apprentissage basé sur les défis (CBL)**– une mise en œuvre précoce du CBL fournit un cadre composé de six phases : Décrire le défi, Générer et réfléchir à des idées, Examiner plusieurs perspectives qui remettent en question et soutiennent, Rechercher et réviser pour trouver les meilleures solutions, Tester les hypothèses, Partager les résultats et les conclusions. - **Modèle d'apprentissage coopératif (CL)**– à l'instar des modèles 5E et CBL, l'apprentissage coopératif favorise l'apprentissage actif en petits groupes et les étudiants reçoivent une récompense en fonction de leurs performances qui peut inclure une note, une récompense tangible comme un certificat ou une bourse, ou l'approbation d'un enseignant. - **Modèle d'apprentissage par projet (PBL)**– L'apprentissage par projet et l'apprentissage par problèmes utilisent la même abréviation de PBL et sont tous deux axés sur l'amélioration de la résolution de problèmes, de la pensée critique, du travail d'équipe, de la communication et des compétences créatives ; cependant, ils se composent de différentes phases., Recherche indépendante et en groupe, Développer et présenter, Analyser et évaluer le processus. - **Modèle d'apprentissage par enquête guidée orienté processus (POGIL)**– cette approche guide l'étudiant dans l'exploration d'un concept ;

Catégorie	Détails
	suivi d'une invention de concept où les élèves synthétisent et expliquent le concept ; et clôture le cycle d'apprentissage avec l'application du concept théorique. - **Modèle d'apprentissage collaboratif par enquête guidée (GICL)**– il s'agit d'une nouvelle approche largement basée sur le modèle POGIL.

Afin de garantir que les différentes stratégies de formation proposées ont le meilleur impact possible, chaque approche sera sélectionnée et alignée sur les objectifs d'apprentissage spécifiques des modules de cybersécurité dans le développement d'un programme de module complet et de matériels de formation. Des méthodes supplémentaires peuvent également être choisies par les conférenciers/mentors qui dispenseront la formation CyberAgent. Pendant la phase de développement du matériel de formation, une formation sera dispensée aux instructeurs des formations pilotes pour les informer sur les objectifs, le processus et les responsabilités de la formation, et pour les préparer à enseigner efficacement le programme CyberAgent. Le processus de formation pilote comprend également la collecte de commentaires auprès des apprenants et des formateurs afin de contrôler l'efficacité des méthodes de formation utilisées et de procéder aux ajustements nécessaires.

Les modules se dérouleront sous différents formats d'enseignement :

- au format à distance,
- en apprentissage synchrone (prise en charge totale de l'enseignant),
- et en apprentissage asynchrone (soutien de l'enseignant en cas de besoin), apprentissage mixte et auto-apprentissage.

Étant donné que différentes manières de dispenser la formation sont envisagées, les méthodes de formation sont présentées à ce stade à titre de lignes directrices.

4. STRUCTURE DES MODULES

L'analyse de la structure des modules du programme d'études VU Cyber security, l'analyse de la structure des modules des projets internationaux (**CyberPhish**,**FuseIT**,**dComFra**), et l'analyse de la structure des modules des plateformes commerciales, telles que**Udemy** et **Coursera**, a conduit à la création d'une structure de modules typique qui pourrait être appliquée à la fois aux modules d'enseignement supérieur et d'EFP.

L'objectif principal est de développer 8 modules, dont 8 modules seraient destinés aux étudiants des HEI (niveau CEC 5--6), pour les étudiants de l'EFP et les PME (niveau CEC 4-5) et des micro-modules pour tout type d'étudiants.

Figure 11. Structure des modules

* Il est recommandé que chaque sous-thème soit suivi de questions d'auto-test (auto-réflexion). Cependant, au stade de l'élaboration du module, une méthode ou une option d'évaluation différente peut être choisie en fonction du type d'étude choisi, par exemple les étudiants peuvent se voir proposer des exercices pratiques, des simulations, etc., tandis que des questions d'auto-test sont proposées aux apprenants indépendants.

** Un test d'évaluation des connaissances est facultatif. Si l'apprenant souhaite obtenir une attestation de fin de cours pour vérifier les connaissances acquises, ce test est obligatoire. L'apprenant a toutefois la possibilité d'obtenir une attestation de fin de cours prouvant qu'il a suivi la formation, auquel cas ce test est facultatif.

Pour garantir que chaque module de formation est directement lié à l'applicabilité pratique, la description de chaque module fournira des exemples clairs de la manière dont la théorie est appliquée dans la pratique. Cela comprend non seulement des scénarios détaillés pour l'applicabilité des modules, mais également des tâches spécifiques que les étudiants entreprendront pour consolider les connaissances théoriques dans des situations réelles de cybersécurité.

Chaque module doit fournir des compétences techniques, des compétences analytiques, des compétences en gestion des risques et des compétences organisationnelles dans des proportions différentes. Un test d'auto-évaluation est proposé pour tester les connaissances des apprenants à la fin de n'importe quelle partie du module (sujet). Cela permet non seulement d'évaluer les connaissances acquises, mais également d'enregistrer les progrès de l'apprenant et de collecter des points et des badges, ce qui permet au participant de s'impliquer davantage dans le processus d'apprentissage.

Suite aux formalités ECTS où chaque ECTS représente 25-30 heures de charge de travail. Selon cela, chaque module pourrait être égal à 5 ECTS. Les heures de travail pourraient être réparties de cette façon :

Tableau 2. Heures de charge de travail

	Nombre de modules	**Total d'ECTS**	**Horaires à distance pour les compétences théoriques**	**Horaires à distance pour les compétences pratiques**	**Horaires de travail individuel**	**Nombre d'heures total**
Modules pour les étudiants de l'enseignement supérieur (niveau CEC 5-6)	8	8-40	20%	20%	60%	200-1200
Modules pour les étudiants de l'EFP (niveau CEC 4-5)	8	8-40	15%	25%	60%	200-1200
Formation en autonomie (apprentissage hybride)	8	8-40	10%		90%	200-1080
Formation en autonomie (en ligne)	8	8-40				200-1200
Micro-modules	1-8	1-40				25-1200

Tableau 3. Charge de travail recommandée pour chaque module

Module	ECTS	Nombre d'heures total	Portion de travail	Portion de travail théorique	Portion de travail pratique	Portion de travail individuel
Titre du module pour l'enseignement supérieur	1-5	25-150	40%	20%	20%	60%
Titre du module pour l'EFP	1-5	25-150	40%	15%	25%	60%
Formation en autonomie (apprentissage hybride)	1-5	25-150	10%			90%
Formation en autonomie (en ligne)	1-5	25-150				100%
Micro-sections						10%-100%

Chaque module doit avoir sa propre description. Après analyse du VU, de Timtal et d'autres programmes utilisant des micro-accréditations, une structure de module type est proposée pour chaque module CyberAgent (un exemple de structure de module type est donné en annexe 1).

Tableau 4. Structure standard des modules CyberAgent

Catégorie	Détails
Identification des modules (informations de base sur le module)	- Titre du module - Code des modules - Maître de conférences - Institution ou département où le module est dispensé - Modèle de livraison - Langue - Conditions préalables
Durée du module et charge de travail (clairement engagement de temps et aperçu de la structure)	- Durée totale (nombre d'ECTS) - Charge de travail des étudiants en heures - Horaires de travail - Horaires de travail individuels
Objectifs éducatifs et résultats d'apprentissage (détails sur ce que le module vise à	- Objectif et résultats du module - Résultats d'apprentissage

Catégorie	Détails
réaliser et ce que les étudiants apprendront)	○ Compétences techniques ○ Compétences analytiques ○ Compétences en matière de risque ○ Compétences d'organisation
Méthodes d'enseignement et d'apprentissage	- Méthodes d'enseignement et d'apprentissage
Estimation et évaluation (explication sur la manière dont les étudiants seront évalués)	- Méthodes d'évaluation - Tâches (laboratoires, projets, présentations, rapports, etc.) - Stratégie d'évaluation, critères d'évaluation
Faciliter les ressources	- Équipement, logiciels et technologie
Le contenu des cours	- Sujets et sous-thèmes du module
Ressources	- Liste des sources - Sources supplémentaires

Chaque ECTS est considéré comme 25-30 heures (heures de contact ou en ligne + études individuelles).

Le module doit avoir au moins une hiérarchie à deux niveaux :

- **Le premier niveau de la hiérarchie**- les sujets. À ce niveau, les principaux éléments du module pourraient être l'introduction, le test d'entrée, le test final et l'élément de base – le sujet.
- **Le deuxième niveau de la hiérarchie**– les sous-thèmes, les principaux éléments pédagogiques du module.

Chaque module du premier niveau de la hiérarchie doit comprendre :

- **INTRODUCTION**au module (description textuelle, introduction vidéo) : pertinence et avantages du module, objectifs de base et résultats du module, logiciels et matériels requis, exigences pour les participants.
- **LES SUJETS**– les thèmes principaux du cours, le matériel théorique et les méthodes d'enseignement théorique.
- **SOUS-THÈME**– sous-thème de chaque sujet, analyse et tâches pratiques et analytiques, méthodes d'enseignement pratiques et analytiques. Les sujets et sous-thèmes peuvent inclure des informations textuelles, des vidéos, des clips audio, des présentations, des liens vers des lectures complémentaires.
- **MODULE Test d'introduction**(si besoin). Le test d'introduction aux niveaux intermédiaire et avancé doit confirmer que le candidat maîtrise suffisamment de connaissances et de compétences aux niveaux précédents.
- **MODULE**tests de reconnaissance. Le test de reconnaissance doit fournir une vérification objective des compétences d'un étudiant et démontrer sa compétence par rapport aux exigences du module.
- **DES LIGNES DIRECTRICES**pour les mentors/enseignants. Ce document doit contenir des recommandations méthodologiques destinées aux mentors/enseignants sur l'utilisation des éléments pédagogiques du module.

Chaque SUJET au deuxième niveau de la hiérarchie doit inclure :

- **INTRODUCTION**aux objectifs et aux résultats du sujet, contenu court.
- **SOUS-THÈMES**: tous les éléments pédagogiques nécessaires pour aider l'étudiant à maîtriser les compétences pertinentes.
- **Test de SUJET**: brèves recommandations pour les mentors/enseignants sur la mise en œuvre et l'application du module. Chaque SOUS-THÈME doit être composé d'éléments pédagogiques dont le contenu correspond aux tâches de la description du module. Chaque sous-thème peut (devrait) inclure un TEST de sous-thème, confirmant que l'étudiant maîtrise les compétences pertinentes à un niveau suffisamment élevé.

Le matériel de formation du module doit prendre en charge l'étude de 6 à 8 sujets, dans chacun desquels il y a 4 à 6 sous-thèmes et, au minimum, un test de sujet. Ainsi, le module doit contenir

(environ) 30 à 40 éléments pédagogiques (méthodes décrites dans la section méthodes pédagogiques) et 6 à 8 tests et un test de reconnaissance final du module.

5. CURSUS ET PROGRAMME DE FORMATION CYBERAGENT

Feuille de route pour l'élaboration du programme d'études

Le programme CyberAgent et un programme de formation suivent les lignes directrices du programme d'études pour les programmes d'études postsecondaires en cybersécurité, élaborées par le groupe de travail conjoint de l'ACM, de l'IEEE, de l'AIS SIGSEC et de l'IFIP (2017).[8](ci-après – Lignes directrices). Plus précisément, étant donné que l'objectif général du projet CyberAgent est d'accroître les compétences internes en matière de cybersécurité des PME européennes, le programme suit le cadre du domaine de connaissances sur la sécurité organisationnelle, comme le recommandent ces lignes directrices.

Cela dit, la première étape de l'élaboration d'un programme consiste à mapper les sous-thèmes et modules prédéfinis du projet CyberAgent avec les unités de connaissances et les sujets clés, recommandés et décrits par les lignes directrices (p. 59-70). La cartographie est basée sur la corrélation logique entre ces deux piliers, telle que discutée et convenue par les partenaires du projet.

La deuxième étape consiste à attribuer des résultats d'apprentissage spécifiques, identifiés et décrits à partir du T2.2 « Cartographie des besoins de formation des agents de changement en cybersécurité des PME » avec l'unité de connaissances et les sujets clés cartographiés ci-dessus. Il convient de noter ici que différentes professions liées à la cybersécurité peuvent avoir une variété de connaissances, d'aptitudes et de compétences différentes, comme le montre de manière éloquente le livrable T2.2 mentionné ci-dessus. Cependant, la proposition fournie ci-dessous reflète l'ensemble de connaissances, d'aptitudes et de compétences attendu par CyberAgent, qui peuvent être adaptées aux besoins spécifiques de professions ou de groupes de stagiaires spécifiques.

Cela dit, les résultats de cet exercice d'élaboration du curriculum sont présentés dans le tableau 5 ci-dessous.

[8]Le Groupe de travail conjoint sur l'éducation à la cybersécurité. (2017). Lignes directrices du programme d'études pour les programmes d'études postsecondaires en cybersécurité : un rapport de la série de programmes d'études en informatique. Association for Computing Machinery, 31 décembre 2017. Disponible sur :**https://cybered.hosting.acm.org/wp-content/uploads/2018/02/newcover_csec2017.pdf**[Consulté le 3 mars 2024]

Tableau 5. Feuille de route pour l'élaboration du programme d'études

Sous-thèmes et modules	Unité de connaissances et sujets clés	Acquis d'apprentissage des EES	Résultats d'apprentissage de l'EFP
Compétences techniques			
- Connaissance actualisée des menaces de cybersécurité et des questions juridiques associées	**Gestion du programme de sécurité** - Gestion de projet - La gestion des ressources - Mesures de sécurité - Assurance qualité et contrôle qualité	**Connaissance**: Les apprenants acquerront des connaissances avancées sur les principes avancés de cybersécurité, y compris les cybermenaces et vecteurs d'attaque sophistiqués, la législation nationale et internationale en matière de cybersécurité, les normes et les exigences de conformité pertinentes pour leur secteur. **Aptitudes**: Les apprenants seront compétents pour concevoir et mettre en œuvre des stratégies avancées d'évaluation et de gestion des risques afin d'atténuer les risques identifiés, à l'aide de méthodologies et d'outils avancés. **Compétences**: Les apprenants seront compétents pour diriger et gérer des projets et des équipes de cybersécurité mettant en œuvre des politiques et des cadres stratégiques de cybersécurité alignés sur les objectifs et les	**Connaissance**: Les apprenants acquerront des connaissances pratiques sur les dernières menaces de cybersécurité, notamment les attaques de phishing, de ransomware et de DDoS, et sur la manière de les gérer grâce à une gestion efficace des projets et des ressources, ainsi qu'à la mise en œuvre de mesures d'assurance qualité et de contrôle. **Aptitudes**: Les apprenants seront capables d'utiliser des outils et des logiciels de protection contre l'évolution des cybermenaces et d'appliquer des pratiques de sécurité robustes dans la gestion de projets et de ressources afin d'améliorer les mesures de sécurité globales et le contrôle qualité au sein de leurs organisations. **Compétences**: Les apprenants seront compétents pour évaluer et atténuer les menaces de sécurité potentielles, communiquer efficacement les problèmes de cybersécurité et signaler

		obligations de conformité de l'organisation.	avec précision les menaces et les violations via les canaux appropriés au sein de leur organisation.
- Connaissances pratiques sur la façon de faire face aux menaces de cybersécurité	**Administration des systèmes** - Administration du système d'exploitation - Administration du système de base de données - L'administration du réseau - Administration cloud - Administration de systèmes cyber-physiques - Durcissement du système - Disponibilité	**Connaissance**: Les apprenants acquerront des connaissances avancées dans l'administration des systèmes d'exploitation, de bases de données, de réseaux, de cloud et de systèmes cyber-physiques, ainsi que dans d'autres domaines, leur permettant de renforcer efficacement les systèmes et d'en garantir la disponibilité tout en appliquant les derniers mécanismes de défense en matière de cybersécurité. **Aptitudes**: Les apprenants seront capables d'utiliser des méthodologies et des outils avancés pour concevoir et mettre en œuvre des architectures de systèmes sécurisées, y compris des systèmes d'exploitation, des bases de données, des réseaux et des infrastructures cloud. **Compétences**: Les apprenants seront compétents pour développer et mettre en œuvre des cadres stratégiques de cybersécurité pour l'administration du système, diriger des projets et des équipes pour améliorer le	**Connaissance**: Les apprenants acquerront des connaissances pratiques sur la façon d'administrer et de sécuriser les systèmes d'exploitation, les bases de données, les réseaux, les cloud et les systèmes cyber-physiques contre les cybermenaces courantes telles que le phishing, les ransomwares et les attaques DDoS, tout en mettant en œuvre des politiques efficaces de gestion des risques. **Aptitudes**: Les apprenants seront capables d'identifier les risques et vulnérabilités potentiels de cybersécurité sur diverses plates-formes système, d'utiliser des outils et des logiciels spécialisés pour améliorer le renforcement et la disponibilité du système, et de mettre en œuvre des pratiques de cybersécurité de base telles que la création de mots de passe sécurisés, la navigation sécurisée et la gestion sécurisée des données sensibles. . **Compétences**: Les apprenants seront compétents pour évaluer et atténuer les menaces de sécurité au sein de l'administration du système,

		renforcement et la disponibilité du système, et prendre des décisions éthiques pour maintenir des pratiques de cybersécurité robustes dans divers domaines administratifs.	communiquer efficacement les problèmes de cybersécurité et signaler rapidement toute menace et violation aux canaux organisationnels appropriés.
Compétences analytiques			
- Esprit critique	**Outils analytiques** - Mesures de performances (métriques) - Analyse des données - Renseignement de sécurité	**Connaissance**: Les apprenants acquerront des connaissances avancées sur la législation, les normes et les exigences de conformité nationales et internationales en matière de cybersécurité, ainsi que sur d'autres pertinentes à leur secteur spécifique. **Aptitudes**: Les apprenants seront capables d'utiliser les mesures de performance, l'analyse des données et les renseignements de sécurité pour concevoir et mettre en œuvre des stratégies efficaces de gestion des risques. **Compétences**: Les apprenants seront compétents dans l'utilisation d'outils analytiques pour élaborer des politiques stratégiques de cybersécurité avec un esprit critique et	**Connaissance**: Les apprenants acquerront des connaissances pratiques sur la manière d'appliquer les mesures de performance, l'analyse des données et les renseignements de sécurité pour protéger les actifs de l'organisation. **Aptitudes**: Les apprenants seront capables d'utiliser des outils analytiques pour identifier les risques et vulnérabilités potentiels de cybersécurité, d'appliquer des informations basées sur les données pour renforcer les pratiques de cybersécurité et d'utiliser des mesures de performance pour évaluer et améliorer la sécurité des mots de passe, de la navigation, du courrier électronique et de la gestion des données. **Compétences**: Les apprenants seront compétents pour évaluer et atténuer les

		prendre des décisions en matière de pratiques de cybersécurité alignées sur les objectifs organisationnels et les obligations de conformité.	menaces de sécurité potentielles à l'aide d'outils analytiques, en signalant avec précision les menaces et les violations aux canaux appropriés au sein de leur organisation.
- Analyser et comprendre les menaces locales, comment elles se produisent, les personnes à risque, etc.	**Opérations de sécurité** - Convergence de la sécurité - Centres d'opérations de sécurité mondiale (GSOC)	**Connaissance**: Les apprenants acquerront des connaissances avancées sur les cybermenaces locales, en utilisant les informations des centres d'opérations de sécurité mondiaux et les tendances actuelles en matière de stratégies de défense en matière de cybersécurité. **Aptitudes**: Les apprenants seront capables d'utiliser des méthodologies et des outils avancés au sein des centres d'opérations de sécurité mondiaux pour concevoir des stratégies efficaces de gestion des risques et élaborer des plans pour atténuer efficacement les menaces locales de cybersécurité. **Compétences**: Les apprenants seront compétents dans l'élaboration et la mise en œuvre de politiques stratégiques de cybersécurité qui répondent aux menaces locales grâce à l'utilisation de centres d'opérations de sécurité mondiaux.	**Connaissance**: Les apprenants acquerront des connaissances pratiques sur les cybermenaces locales et leurs origines, évalueront l'impact de ces menaces sur les actifs de l'organisation. **Aptitudes**: Les apprenants seront capables d'identifier les risques et les vulnérabilités locales en matière de cybersécurité, en utilisant des outils et des logiciels tels que la création de mots de passe sécurisés, la navigation sécurisée et la gestion sécurisée des données adaptées à leurs environnements spécifiques. **Compétences**: Les apprenants seront compétents pour évaluer et atténuer les menaces de sécurité locales en utilisant les informations des centres d'opérations de sécurité mondiaux, en communiquant efficacement les problèmes de cybersécurité et en signalant avec précision les menaces et les violations aux canaux appropriés au sein de leur organisation.

Gestion des risques			
- Apprenez à fournir et à décrire le lieu de travail des PME avec des routines de cybersécurité	**Gestion des risques** - Identification des risques - Évaluation et analyse des risques - Menaces internes - Modèles et méthodologies de mesure et d'évaluation des risques - Contrôle des risques	**Connaissance**: Les apprenants acquerront des connaissances avancées sur les processus de gestion des risques, y compris l'identification, l'évaluation et le contrôle des risques, leur permettant d'établir et de décrire des routines de cybersécurité efficaces adaptées aux besoins spécifiques des lieux de travail des PME, conformément aux normes nationales et internationales. **Aptitudes**: Les apprenants seront capables d'appliquer des méthodologies et des outils avancés pour mener des évaluations complètes des risques, concevoir et mettre en œuvre des stratégies efficaces de gestion des risques et développer des routines de cybersécurité robustes spécifiquement adaptées aux lieux de travail des PME. **Compétences**: Les apprenants seront compétents dans l'élaboration et la mise en œuvre de politiques stratégiques de cybersécurité pour les lieux de travail des PME.	**Connaissance**: Les apprenants acquerront des connaissances pratiques sur les processus d'identification, d'évaluation et de contrôle des risques, ainsi que sur les stratégies de gestion des risques pour protéger efficacement les lieux de travail des PME. **Aptitudes**: Les apprenants seront capables d'identifier et d'analyser les risques potentiels de cybersécurité dans les environnements des PME, d'utiliser des outils et des logiciels appropriés pour atténuer les menaces, ainsi que de promouvoir et de mettre en œuvre des pratiques essentielles de cybersécurité, notamment la création de mots de passe sécurisés, la navigation sécurisée et la manipulation sécurisée des données sensibles. **Compétences**: Les apprenants seront compétents pour évaluer et atténuer les menaces de sécurité sur les lieux de travail des PME, communiquer efficacement les problèmes et les procédures de cybersécurité et signaler avec précision les menaces et les violations pertinentes aux canaux organisationnels appropriés.

- Créer son propre manuel pour les PME sur le lieu de travail sur la cybersécurité et comment en assurer le suivi	**Continuité des activités, reprise après sinistre, gestion des incidents et sécurité du personnel** - Réponse aux incidents - Reprise après sinistre - Continuité de l'activité - Sensibilisation, formation et éducation à la sécurité - Pratiques d'embauche en matière de sécurité - Pratiques de résiliation de sécurité - Sécurité tierce - Sécurité dans les processus d'examen - Numéro spécial sur la confidentialité des informations personnelles des salariés	**Connaissance**: Les apprenants acquerront des connaissances avancées sur la façon de créer et de mettre en œuvre un manuel complet de cybersécurité sur le lieu de travail des PME, intégrant des principes avancés de cybersécurité, les derniers mécanismes de défense et le respect des législations et normes nationales et internationales en matière de gestion des incidents, de continuité des activités et de sécurité du personnel. **Aptitudes**: Les apprenants seront compétents pour créer et maintenir un manuel de cybersécurité sur le lieu de travail des PME, en utilisant des méthodologies avancées pour évaluer les risques, concevoir des stratégies efficaces de gestion des risques et de réponse aux incidents, et développer des plans complets de continuité des activités adaptés aux besoins de leur organisation. **Compétences**: Les apprenants seront compétents pour élaborer et mettre en œuvre un manuel de cybersécurité pour les PME, diriger efficacement des projets et des équipes de sécurité, en garantissant l'alignement avec les	**Connaissance**: Les apprenants acquerront des connaissances pratiques sur la façon de créer un manuel complet de cybersécurité sur le lieu de travail des PME qui intègre des stratégies de réponse aux incidents, de reprise après sinistre, de continuité des activités et de sécurité du personnel, en protégeant les actifs de l'organisation et les données sensibles. **Aptitudes**: Les apprenants seront capables d'identifier les risques potentiels de cybersécurité, d'utiliser des outils et des logiciels pour se protéger contre les menaces et d'appliquer les meilleures pratiques en matière de cybersécurité pour développer et maintenir un manuel PME qui aborde la création de mots de passe sécurisés, la navigation, la sécurité du courrier électronique et la protection des données. **Compétences**: Les apprenants seront compétents pour évaluer et atténuer les menaces de sécurité, communiquer efficacement les politiques et pratiques de cybersécurité et signaler systématiquement les incidents de sécurité au sein de leur PME, comme indiqué dans leur manuel de cybersécurité personnalisé.

		objectifs organisationnels et les obligations de conformité.	
Compétences organisationnelles			
- Comment mettre en œuvre de nouvelles routines et méthodes de travail dans le domaine de la cybersécurité sur les lieux de travail des PME	**Gouvernance et politique de sécurité** - Contexte organisationnel - Confidentialité - Lois, éthique et conformité - Gouvernance de la sécurité - Communication au niveau de la direction et du conseil d'administration - Politique managériale	**Connaissance**: Les apprenants acquerront des connaissances avancées sur la façon de mettre en œuvre de nouvelles routines et flux de travail de cybersécurité sur les lieux de travail des PME, en intégrant les principes et tendances actuels en matière de cybersécurité et le respect de la législation nationale et internationale pertinente pour leur secteur. **Aptitudes**: Les apprenants seront capables d'utiliser des méthodologies avancées pour effectuer des évaluations des risques, concevoir et mettre en œuvre de nouvelles routines de cybersécurité et préparer des stratégies de réponse, garantissant une gouvernance et une conformité efficaces sur les lieux de travail des PME. **Compétences**: Les apprenants seront compétents pour élaborer et mettre en œuvre des politiques stratégiques de	**Connaissance**: Les apprenants acquerront des connaissances pratiques sur la manière d'intégrer de nouvelles routines et pratiques de cybersécurité sur les lieux de travail des PME, conformément à la législation, aux normes, aux stratégies et aux politiques de cybersécurité en matière de sécurité de l'information, de gestion des risques et de protection des données. **Aptitudes**: Les apprenants seront compétents dans l'application d'outils et de logiciels de cybersécurité pour mettre en œuvre de nouvelles routines de sécurité, identifier et atténuer les risques et promouvoir des pratiques essentielles de cybersécurité telles que la création de mots de passe sécurisés, la navigation et la gestion des données dans le cadre de gouvernance des lieux de travail des PME. **Compétences**: Les apprenants seront compétents pour évaluer et atténuer les menaces de sécurité potentielles, communiquer efficacement les changements et les politiques de

		cybersécurité, diriger des initiatives visant à établir de nouvelles routines et flux de travail sur les lieux de travail des PME et prendre des décisions éthiques qui s'alignent sur les objectifs organisationnels et les exigences de conformité.	cybersécurité et signaler avec précision les incidents de sécurité au sein des PME conformément aux exigences de gouvernance et de conformité.
- Assurer l'accompagnement des leaders dans le domaine de la cybersécurité.	**Planification de la cybersécurité** - Planification stratégique - Gestion opérationnelle et tactique	**Connaissance**: Les apprenants acquerront des connaissances avancées sur la manière d'intégrer les principes avancés de cybersécurité et les tendances actuelles dans la planification stratégique et la gestion opérationnelle. **Aptitudes**: Les apprenants seront compétents en planification stratégique et en gestion opérationnelle, ce qui leur permettra de concevoir et de mettre en œuvre efficacement des stratégies de cybersécurité qui répondent aux risques émergents et garantissent des réponses tactiques robustes. **Compétences**: Les apprenants seront compétents dans l'élaboration et la mise en œuvre de cadres stratégiques de cybersécurité, ainsi que dans la direction et la gestion d'initiatives de cybersécurité.	**Connaissance**: Les apprenants acquerront des connaissances pratiques sur la manière d'intégrer la planification stratégique et la gestion opérationnelle dans la cybersécurité pour protéger les actifs de l'organisation, se conformer à la législation et aux normes pertinentes et mettre en œuvre des stratégies efficaces de sécurité de l'information et des politiques de gestion des risques. **Aptitudes**: Les apprenants seront compétents pour identifier les risques de cybersécurité, utiliser des outils de planification stratégique et de gestion opérationnelle pour se prémunir contre les menaces et promouvoir la mise en œuvre de pratiques fondamentales de cybersécurité dans leurs rôles de soutien au leadership. **Compétences**: Les apprenants seront compétents pour évaluer et atténuer les menaces de sécurité, communiquer

			efficacement les stratégies et les problèmes de cybersécurité et signaler de manière fiable les incidents et les vulnérabilités aux canaux appropriés au sein de leur organisation.

6. STRATÉGIE D'ÉVALUATION DES COURS

L'évaluation des connaissances fait partie intégrante du processus d'apprentissage et favorise un apprentissage plus approfondi. Ce chapitre décrit l'approche d'évaluation des cours qui est nécessaire pour garantir que tous les participants aux cours CyberAgent atteignent les résultats d'apprentissage et les compétences requis. Le processus d'évaluation du cours est divisé en deux parties principales : des tests d'auto-évaluation et d'évaluation des connaissances, qui sont adaptés aux étudiants de l'enseignement supérieur (HEI) et de l'enseignement et de la formation professionnels (EFP), en tenant compte de leurs différents besoins et objectifs d'apprentissage. .

Étant donné que les sujets des modules peuvent être les mêmes pour les EES et l'EFP, certaines questions peuvent convenir à la fois aux cours des EES et de l'EFP. Ainsi, lors de la conception des questions, il sera possible de préciser si la question est destinée uniquement à l'EFP ou aux établissements d'enseignement supérieur ou aux deux. Cette façon de noter ne sera utilisée que lors de la conception des questions car elle facilitera la conception des questions. Une fois les questions importées dans la plateforme, les bases de données seront différentes pour l'EFP et les HEI.

Figure 12. Bases de données d'auto-évaluation t d'évaluation des connaissances

1. Tests d'auto-évaluation: Après avoir terminé chaque sujet du cours, les étudiants passeront des tests d'auto-évaluation. Ces évaluations sont conçues pour fournir une rétroaction immédiate, aidant les étudiants à évaluer leur compréhension de la matière récemment abordée. Cette étape encourage l'autoréflexion et aide à renforcer les objectifs d'apprentissage de chaque sujet. De plus, il permet aux apprenants d'identifier les domaines dans lesquels ils pourraient avoir besoin d'études plus approfondies ou de clarifications, favorisant ainsi une approche proactive de leur parcours d'apprentissage.

En utilisant des tests d'auto-évaluation, les participants au cours ont pu identifier leur niveau initial de connaissances et vérifier leurs progrès après chaque sujet de formation.

Un quiz d'auto-évaluation de 3 à 5 questions, avec un mélange de questions vrai/faux, de correspondance et/ou à choix multiples, est recommandé. Un autre sujet ne devrait être déverrouillé qu'une fois que toutes les questions auront reçu une réponse correcte. Il ne devrait y avoir aucune limite de temps ni aucune restriction sur les tentatives. La tentative doit sélectionner au hasard des questions dans la base de données correspondante.

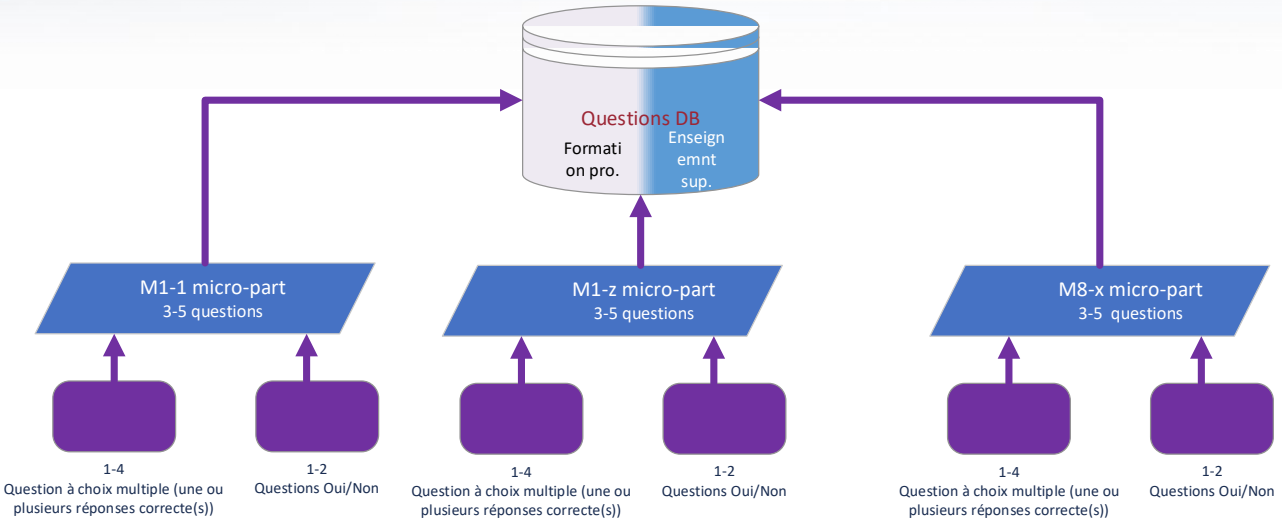

Figure 13. Structure de la base de données d'auto-évaluation

2. Test d'évaluation des connaissances*: Après avoir terminé tous les sujets du cours, les étudiants devront passer un test final afin d'obtenir un certificat de fin de cours. Cette évaluation complète évalue leur compréhension globale et leur maîtrise du contenu du cours. Le test final évalue la rétention de la matière par les étudiants et identifie dans quelle mesure ils peuvent appliquer leurs connaissances dans un contexte plus large.

* Lors de l'élaboration du programme et du matériel, d'autres méthodologies d'évaluation de l'achèvement du cours et des connaissances seront prises en compte, telles que des études de cas, des exercices pratiques et des rapports de réflexion, qui permettront une évaluation plus complète des participants. compétences analytiques et de pensée critique. Cette approche sera également disponible pour les enseignants des étudiants des HEI et de l'EFP dans le cadre de la dispensation des cours.

En utilisant le test d'évaluation des connaissances, les participants au cours pouvaient identifier leur niveau final de connaissances et, s'ils le réussissaient, recevoir un badge d'achèvement du cours (certificat).

Un test d'évaluation des connaissances de 36 questions, avec un mélange de questions vrai/faux, d'appariement et à choix multiples, est recommandé. Il devrait y avoir un délai de 45 minutes et une seule tentative autorisée. Le test doit être administré en sélectionnant au hasard des questions dans une base de données.

En outre, l'évaluation devrait également prendre en compte la prévention de la tricherie et, par conséquent, environ quatre séries de questions devraient être développées. Certaines des questions des tests de connaissances pour l'EFP et les HEI peuvent se chevaucher, nous aurons donc trois attributs au moment du développement : VET, HEI ou VET et HEI.

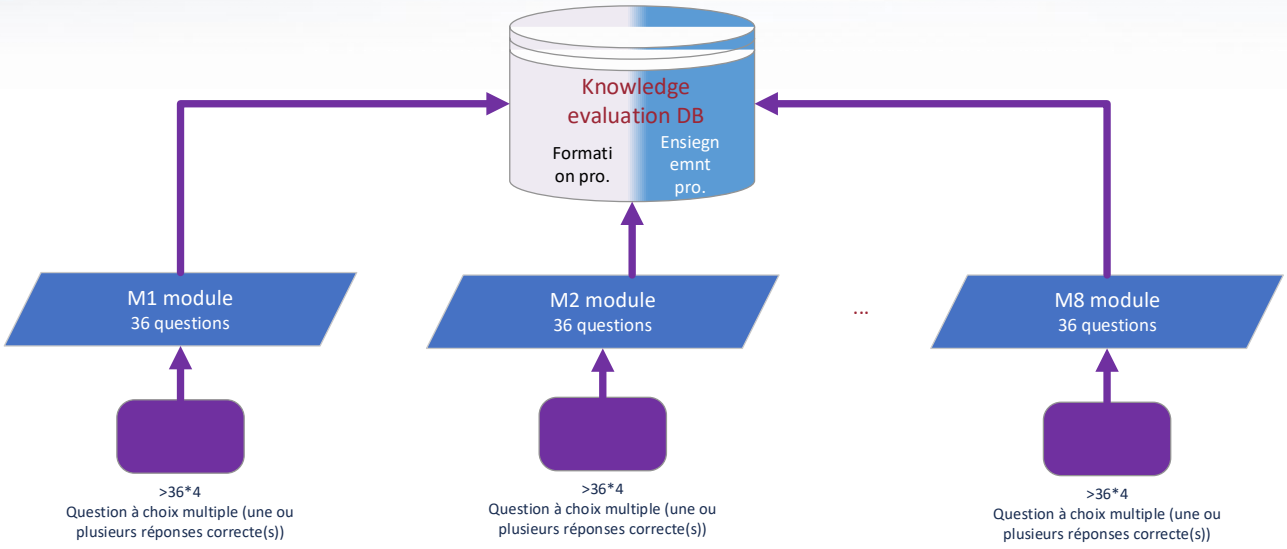

Figure 14. Structure de la base de données d'évaluation des connaissances

Cette stratégie d'évaluation en deux étapes soutient non seulement un apprentissage efficace en fournissant de multiples boucles de rétroaction, mais permet également aux apprenants de jouer un rôle actif dans leur formation.

Des tests d'auto-évaluation et des tests d'évaluation des connaissances seront développés selon le programme des cours et sur la base des résultats et des recommandations développés dans ce projet.

COMPOSITION DE LA BASE DE DONNÉES DES QUESTIONS

Afin de garantir une base de questions suffisamment large et équilibrée, au moins 5 questions vrai/faux ou correspondantes et 5 questions à choix multiples seront créées pour chaque sujet du cours de l'EFP ou des HEI.

En supposant qu'il y aura au moins 10 sujets dans chaque cours, la base globale de chaque cours d'EFP ou d'enseignement supérieur doit contenir au moins 10 à 20 % de vrai/faux ou de correspondance, et 90 à 80 % de questions à choix multiples. Il s'agit d'une ligne directrice générale, mais l'enseignant aura la possibilité de choisir la structure des questions en fonction de la matière du cours.

Compte tenu des différences entre les objectifs et les résultats d'apprentissage de l'EFP et des EES, la composition globale de la base de données de questions pour un seul cours devrait contenir ce qui est indiqué dans le tableau ci-dessous.

Tableau 6. Types de questions

	Questions vrai/faux ou correspondantes	Questions à choix multiple
Partie commune du cours	20%	80%
Partie spécifique du cours pour l'EFP	20%	80%
Partie spécifique du cours pour l'enseignement supérieur	20%	80%
Total pour l'EFP et l'enseignement supérieur	20%	80%

DIRECTIVES POUR LA CONSTRUCTION DES QUESTIONS

Les questions des tests d'auto-évaluation et d'évaluation des connaissances doivent être préparées en anglais, puis localisées dans les langues partenaires.

Lors de l'élaboration de questions de test pour l'auto-évaluation et l'évaluation des connaissances dans le cadre du cours, il est essentiel de garantir que les questions sont claires, concises et accessibles à tous les candidats, quel que soit leur parcours. Cette approche garantit que les évaluations reflètent avec précision la compréhension des apprenants du contenu du cours et leur capacité à atteindre les compétences et les objectifs énoncés dans le programme de cours.

Lignes directrices générales pour la construction des questions :

Des lignes directrices claires seront appliquées lors de l'élaboration des questions du test : les questions doivent être compréhensibles et directement liées aux objectifs d'apprentissage du cours, sans utiliser de terminologie complexe ou de formulation prêtant à confusion. Les questions culturellement spécifiques ou déroutantes seront également évitées afin de garantir l'équité et l'accessibilité pour tous les participants au cours. Des conseils supplémentaires sur la conception des questions sont fournis ci-dessous.

Clarté et simplicité :les questions doivent être simples, en évitant l'utilisation d'un langage ou d'un jargon complexe qui pourrait confondre ou induire les candidats en erreur. L'objectif est d'évaluer les connaissances et la compréhension des candidats du sujet, et non leur capacité à déchiffrer des questions complexes.

Franchise et pertinence: chaque question doit être directement liée aux compétences clés et aux objectifs du programme de cours. Les contenus non pertinents ou tangentiels doivent être évités afin de maintenir l'accent sur l'évaluation des résultats d'apprentissage escomptés.

Sensibilité culturelle et contextuelle: veillez à ce que les questions ne présupposent pas de connaissances ou d'expériences culturelles spécifiques, les rendant accessibles et équitables aux candidats d'horizons divers.

Pas de questions délicates :l'intention de chaque question doit être claire, sans tentative d'induire en erreur ou de tromper les candidats. Les questions conçues pour surprendre les candidats ou pour tester leur capacité à détecter les supercheries n'évaluent pas efficacement leur compréhension du sujet.

Présentation sans ambiguïté et concise: les questions doivent être formulées de manière à ne laisser aucune place à l'interprétation, afin de garantir que tous les candidats comprennent la question de la même manière. Gardez les questions concises, en évitant toute longueur inutile qui pourrait obscurcir le point principal.

Phrase positive: évitez d'utiliser des formulations négatives dans les questions (par exemple, "Lequel des énoncés suivants n'est PAS..."). Les formulations négatives peuvent prêter à confusion et à des interprétations erronées, en particulier dans les conditions d'un examen. Au lieu de cela, formulez toutes les questions de manière positive pour favoriser la clarté.

Directives spécifiques pour la construction des questions :

Questions à choix multiple: assurez-vous que toutes les options sont plausibles et pertinentes par rapport à la question. La bonne réponse doit être incontestablement correcte, tandis que les éléments de distraction doivent être clairement incorrects pour quelqu'un qui comprend le contenu.

Questions vrai/faux: présentez des déclarations claires et factuelles directement liées au contenu du cours, en garantissant qu'il n'y a aucune ambiguïté quant à leur valeur de vérité.

Questions correspondantes: assurez-vous que les deux listes (par exemple, les termes d'un côté et les définitions de l'autre) sont clairement liées et qu'il existe une base simple pour faire chaque correspondance. Évitez les listes inégales dans lesquelles le nombre d'éléments ne correspond pas, sauf s'il est explicitement indiqué que certains éléments ne seront pas utilisés ou pourront être utilisés plusieurs fois.

La formation pilote analysera les informations sur les méthodologies d'évaluation des connaissances et le processus d'évaluation en recueillant les commentaires des apprenants et des formateurs. Cela permettra d'évaluer la pertinence des méthodes d'évaluation des connaissances et, si nécessaire, de compléter ou d'améliorer la démarche d'évaluation.

GAMIFICATION

Cette section introduit la description des éléments de gamification implémentés dans les cours CyberAgent. La gamification est le processus d'intégration des principes de gamification dans les activités d'apprentissage traditionnelles afin d'augmenter la motivation et l'engagement des participants. Ces éléments ont été sélectionnés sur la base des dernières recherches en matière de technologie éducative, qui montrent que la gamification peut améliorer considérablement les performances d'apprentissage, augmenter la motivation des étudiants à apprendre et renforcer leur engagement dans le processus d'apprentissage.

Les éléments de gamification qui seront intégrés aux cours comprennent des badges, des points, des classements et des surnoms à code couleur qui reflètent l'expérience et les réalisations du participant.

- Des badges seront attribués pour :

- **Achèvement du module**.
- **Pour réussir un test basé sur le pourcentage de réussite**. Par exemple, un participant recevra un badge de bronze pour une note de passage minimale au test final, un badge d'argent pour une note de passage minimale de 75 %, un badge d'or pour une note de passage minimale de 76 % à 90 % et un badge de platine. pour une note de passage de 90 % à 100 %. Dans ce cas, un participant peut disposer de 8 badges de ce type.
- **Terminer le sujet**.
- **Connexion au système tous les jours pendant dix jours**.
- **Un badge d'activité spécial**pour chaque sujet sera également décerné par le mentor/instructeur du cours.

- Points et scores calculés sur la base des résultats des tests d'auto-évaluation + des résultats des tests finaux avec multiplicateur.

Les participants au cours CyberAgent ne pourront pas voir leurs progrès individuellement, mais pourront rivaliser avec d'autres participants en groupes ou en équipes (en fonction du plus grand nombre de points marqués, mais également en fonction du plus grand nombre de badges). Cela encourage non seulement la compétition et la coopération individuelles mais aussi en équipe, ce qui est important pour développer les compétences de coopération.

Chaque participant verra son pseudo lors de sa connexion au cours, qui sera codé par couleur en fonction de l'avancement du cours et de l'expérience acquise (cours terminés/enregistrés).

Cela aidera les participants au cours à mieux s'impliquer dans le processus de formation. Les participants au cours peuvent répéter plusieurs fois le même test pour améliorer leur score (des points sont attribués pour le plus grand nombre de tests d'auto-évaluation correctement passés).

Un algorithme spécial calculera le score de chaque participant en tenant compte du temps mis pour répondre, du nombre de fois que le test est répété et d'autres paramètres, minimisant ainsi les risques de triche.

Toutes les règles de gamification seront clairement décrites et communiquées aux participants afin que chacun puisse facilement comprendre comment les différents niveaux de gamification peuvent être atteints et comment ils sont calculés.

7. PROCESSUS D'APPRENTISSAGE/D'ENSEIGNEMENT CYBERAGENT

Cette section résume les informations de tous les chapitres de ce document et décrit en détail le processus d'apprentissage/d'enseignement, commençant par l'inscription à un cours CyberAgent sur la plateforme d'apprentissage et se terminant par la fin du cours ou la délivrance d'un certificat.

Les cours CyberAgent sont conçus pour s'adresser à un large éventail d'apprenants, notamment des étudiants d'établissements d'enseignement supérieur (EES), des étudiants d'enseignement et de formation professionnels (EFP), ainsi que des employés de PME. Notre objectif est de donner à chaque participant la possibilité de choisir la méthode d'apprentissage qui lui convient le mieux, en tenant compte de sa situation personnelle et des politiques organisationnelles de l'établissement de formation.

Malgré la méthode d'apprentissage/formation choisie, les participants s'inscrivent sur la plateforme CyberAgent et utilisent la plateforme pendant la formation.

Inscription

Les participants potentiels intéressés à s'inscrire au cours CyberAgent doivent remplir un formulaire d'inscription, en sélectionnant les modules souhaités et la méthode d'apprentissage préférée. Un diagramme conceptuel est fourni pour guider les participants tout au long du parcours d'apprentissage du premier au huitième module CyberAgent.

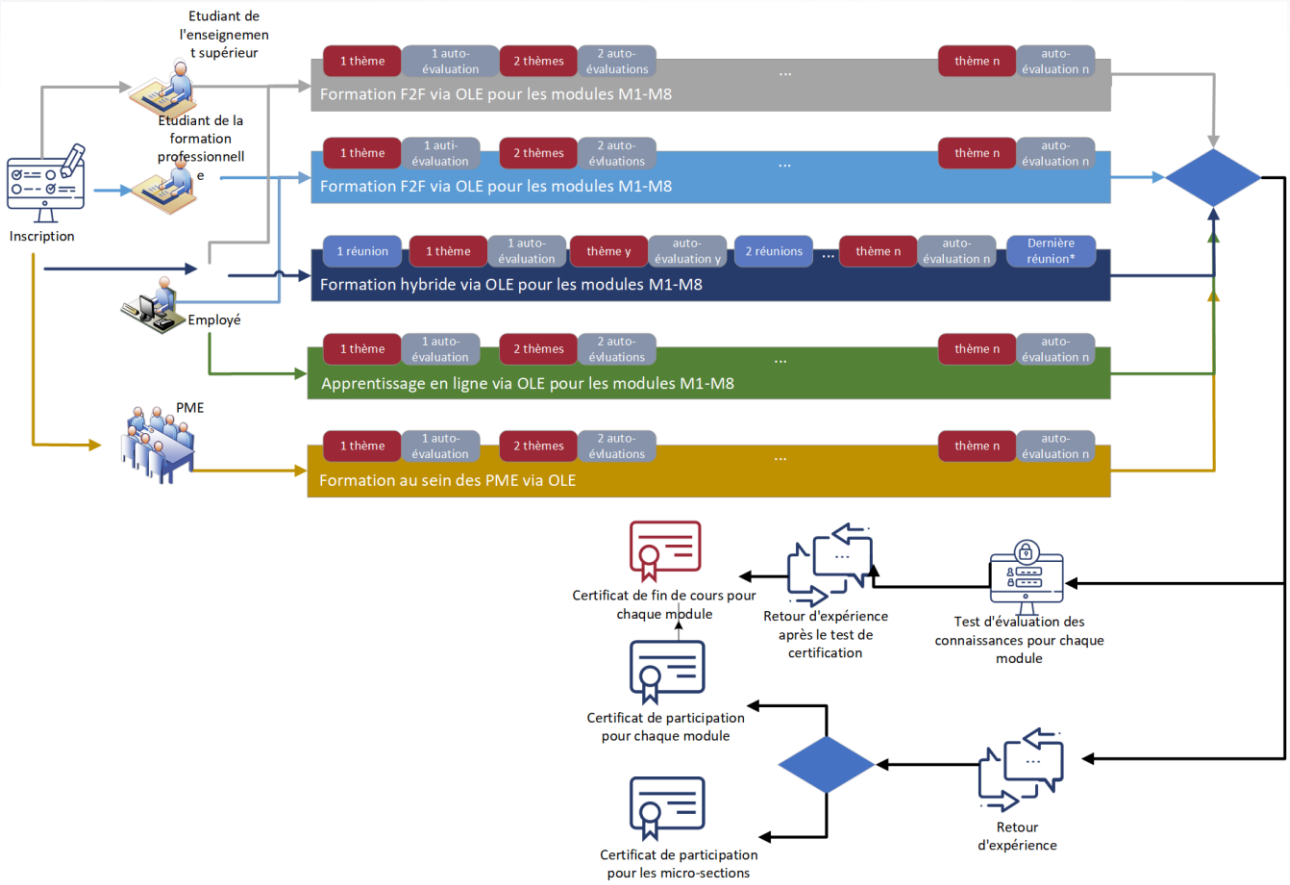

Figure 15. Parcours d'apprentissage/enseignement CyberAgent

La confidentialité des informations des participants sera assurée lors du processus d'inscription, notamment au regard des exigences du RGPD. Lors de l'inscription, les participants auront la possibilité de se familiariser avec le règlement de la plateforme de formation, les règles de confidentialité et de protection des données.

Les données d'inscription des participants ne sont accessibles qu'aux personnes désignées au sein de l'organisation partenaire, conformément aux politiques internes de l'organisation. Pendant les sessions de formation pilotes, les données des participants des partenaires du projet peuvent être accessibles au coordinateur CyberAgent, et les autres partenaires ne sont pas autorisés à voir les données des participants des autres. Une fois le projet terminé, le coordinateur ne peut accéder qu'aux données anonymisées d'autres partenaires pour suivre les résultats du projet, comme spécifié dans la candidature du projet, pendant une période pouvant aller jusqu'à 5 ans après la conclusion du projet.

Nous proposons des options de formation sur mesure pour répondre aux besoins de nos divers groupes cibles. Les étudiants des HEI et de l'EFP peuvent participer à la formation via des séances de contact universitaires. Les employés des PME peuvent choisir la méthode d'apprentissage qui correspond le mieux à leurs besoins : apprentissage mixte, apprentissage en ligne uniquement ou, plus rarement, participation à des cours d'un établissement d'enseignement supérieur ou d'EFP.

Des formations peuvent également être proposées aux grandes entreprises comptant plusieurs employés. Dans de tels cas, la méthode de formation sera personnalisée pour répondre à des besoins spécifiques tout en intégrant les cours du module CyberAgent.

Lors de leur inscription sur la plateforme, les participants sélectionnent leur méthode d'apprentissage et commencent leurs études. Après avoir terminé un module ou une partie de module, ils peuvent se qualifier pour un certificat de participation ou un certificat d'achèvement de cours, ce dernier étant délivré si un participant réussit le test du module avec un score d'au moins 75 %.

Enfin, les participants doivent remplir un formulaire de commentaires avant de recevoir un certificat. Ces retours sont cruciaux pour l'amélioration continue de nos offres de formation et garantir la satisfaction des participants.

Moyens d'apprentissage/formation

Employésdisposez de plusieurs options pour interagir avec le contenu du cours :

- Si les EES ou les établissements d'EFP autorisent les employés à participer en tant qu'invités, l'employé peut participer aux cours aux côtés des étudiants inscrits. De telles sessions avec des participants externes peuvent être organisées 1 à 2 fois par an, sur la base du programme de conférences publié.
- Les employés peuvent opter pour une approche de formation mixte, où les sessions de formation sont dispensées à des dates spécifiques avec une durée recommandée de 2 à 4 mois. Des groupes d'au moins 10 participants sont conseillés, avec un maximum de 30 participants par groupe. La formation mixte comprend des consultations en face à face et en ligne au début, pendant et à la fin du cours pour faciliter le retour d'information direct et la préparation à l'évaluation finale.
- Les employés peuvent choisir la méthode d'apprentissage en ligne pour un apprentissage à leur rythme, sans durée définie pour l'achèvement du cours.
- De plus amples détails sur les modules CyberAgent sont fournis dans la section 1. Parcours d'étude.

Implication des étudiants

Les étudiants inscrits au programme d'études en cybersécurité peuvent rencontrer différents parcours en fonction de la réglementation de leur établissement universitaire. Ils peuvent soit être tenus de suivre tout ou partie des modules CyberAgent, soit, en fonction des politiques internes de l'université, les étudiants qui répondent aux critères peuvent choisir d'étudier un ou plusieurs modules CyberAgent. Les étudiants des établissements d'enseignement supérieur ou de l'EFP s'engagent généralement dans les matières dans le cadre d'un enseignement traditionnel en classe proposé par leur établissement ou peuvent opter pour des méthodes d'auto-apprentissage pour se préparer au test final d'évaluation des connaissances.

Implication des PME

Dans les organisations où une formation en cybersécurité est jugée nécessaire, un représentant de l'entreprise peut inscrire l'organisation à des sessions de formation internes. Dans de tels cas, après accord séparé avec l'université et/ou les instructeurs, la méthode de formation, le calendrier et la délivrance des certificats peuvent être adaptés aux besoins spécifiques de l'organisation en fonction des modules existants.

Collecte de commentaires

À la fin du module, les participants doivent remplir un formulaire de commentaires anonyme accessible en ligne. Les données de feedback ne sont accessibles qu'au personnel autorisé au sein de l'organisation du partenaire, avec des mesures de confidentialité similaires appliquées lors des sessions de formation pilotes et de l'utilisation des données post-projet.

Les commentaires seront principalement recueillis auprès des participants au cours, mais les commentaires des mentors/formateurs seront également recueillis. Les commentaires recueillis évalueront le niveau organisationnel de satisfaction des participants, les aspects de l'organisation du cours, le processus d'apprentissage, l'utilisation pratique des compétences acquises, le contenu du cours, les stratégies d'évaluation, l'inclusion d'éléments de gamification, les domaines de amélioration, etc

Les résultats des retours d'expérience seront régulièrement examinés et présentés à l'équipe de gestion du projet afin de réagir rapidement et d'améliorer les stratégies de formation en fonction des besoins réels et des évolutions du marché.

Ce n'est qu'en remplissant ce formulaire que les participants peuvent obtenir un certificat de participation ou un certificat de fin de cours ou un certificat de participation.

Certificat d'achèvement de cours

La réussite du test d'évaluation donne lieu à la génération d'un certificat de fin de cours pour le participant. Il y a un test final par module.

Certificat de participation

Les participants qui choisissent de ne pas passer le test d'évaluation des connaissances peuvent recevoir un certificat de participation. Cet accusé de réception peut être délivré à l'issue d'un seul module ou de plusieurs micro-parties du cours.

CONCLUSIONS ET RÉSUMÉ

Ce rapport a développé avec succès des parcours d'apprentissage structurés pour les agents de changement en matière de cybersécurité des PME, adaptés pour répondre aux besoins spécifiques à différents niveaux éducatifs et professionnels, de l'enseignement supérieur à l'EFP et à la formation directe des employés des PME. Le programme conçu, comprenant huit modules complets, intègre des compétences techniques, analytiques, organisationnelles et de gestion des risques qui sont cruciales pour l'autonomisation efficace des futurs professionnels de la cybersécurité.

L'approche structurée des parcours d'apprentissage garantit un parcours éducatif complet aux salariés des PME. À travers les étapes de pré-apprentissage, d'apprentissage et de post-apprentissage, il soutient la rétention des connaissances et l'application pratique. Les micro-modules offrent flexibilité et adaptabilité aux besoins individuels, améliorant l'apprentissage avec des micro-certificats qui fournissent des qualifications reconnues. Cet alignement sur les normes de l'industrie contribue de manière significative à renforcer les capacités de cybersécurité des PME, préparant ainsi les employés à relever les défis actuels et les avancées futures. L'analyse suivante du Carrier Pathway a cartographié la progression des rôles de cybersécurité tels que définis par le cadre ESCO, facilitant une approche éducative ciblée qui prépare les individus à une intégration efficace dans la main-d'œuvre de la cybersécurité, améliorant ainsi leurs perspectives de carrière et leur développement professionnel.

La diversité explorée des approches pédagogiques au sein du programme de cybersécurité devrait permettre un environnement d'apprentissage dynamique et flexible qui s'adapte à différents styles et besoins d'apprentissage. L'intégration de diverses méthodes d'enseignement, notamment des cours théoriques, des laboratoires pratiques, la gamification et des projets collaboratifs, garantit que les étudiants ne sont pas seulement des destinataires de connaissances, mais aussi des participants actifs dans leur parcours d'apprentissage. Cette stratégie globale devrait renforcer l'engagement, la compréhension et mieux préparer les étudiants aux défis réels de la cybersécurité. L'adaptabilité des méthodes d'enseignement aux exigences spécifiques aux modules devrait permettre de personnaliser davantage l'expérience d'apprentissage, en garantissant que les résultats pédagogiques sont maximisés pour chaque étudiant.

En mappant systématiquement les sous-thèmes et modules du projet CyberAgent à des unités de connaissances reconnues au niveau international, le programme non seulement répond mais anticipe les exigences dynamiques du domaine de la cybersécurité. Cette approche méthodique garantit que chaque résultat d'apprentissage est stratégiquement lié à des compétences du monde réel qui sont cruciales pour la gestion efficace des menaces de cybersécurité. L'adaptabilité du programme lui permet de remplir divers rôles professionnels au sein de l'industrie, préparant les apprenants non seulement aux défis immédiats, mais aussi au développement de carrière à long terme dans le domaine de la cybersécurité.

La stratégie d'évaluation des cours décrite offre un cadre pour évaluer les compétences et les progrès des étudiants dans les programmes de cybersécurité. L'approche en deux étapes, combinant des tests d'auto-évaluation et des tests complets d'évaluation des connaissances, permet aux étudiants de s'engager activement dans le matériel, d'évaluer en permanence leur compréhension et d'ajuster leurs stratégies d'apprentissage en conséquence. En concevant l'évaluation pour répondre aux questions personnalisées des étudiants des établissements d'enseignement supérieur et de l'EFP, la stratégie garantit la pertinence et l'adéquation pour chaque niveau d'enseignement, améliorant ainsi l'expérience d'apprentissage. Cette méthode permet de mesurer clairement la maîtrise et la préparation des étudiants à appliquer leurs connaissances de manière pratique. De plus, l'introduction d'éléments de gamification tels que des badges et des systèmes de notation motive non seulement les étudiants, mais favorise également un environnement d'apprentissage compétitif mais collaboratif.

Enfin, le processus d'apprentissage et d'enseignement de CyberAgent fournit un cadre éducatif complet et adaptable adapté à un large éventail d'apprenants des établissements d'enseignement supérieur, d'EFP et de PME. Ce système permet diverses méthodes participatives, notamment l'apprentissage en face à face, mixte et en ligne, garantissant une flexibilité dans la manière dont la formation en cybersécurité est dispensée et accessible. L'inscription sur la plateforme CyberAgent initie un parcours dans lequel les participants sélectionnent les modules et les méthodes d'apprentissage préférés, aboutissant à la délivrance de certificats en cas de réussite et d'évaluation. Cette structure prend non seulement en charge des parcours d'apprentissage personnalisés, mais s'aligne également sur les normes rigoureuses de confidentialité essentielles au maintien de la confidentialité des participants tout au long du processus de formation.

Les recommandations et les conseils fournis dans ce document seront utilisés dans la phase suivante pour développer les programmes de formation complets de CyberAgent, les supports de formation, les tests et évaluations de connaissances, les exercices pratiques et autres contenus de formation, qui seront intégrés dans la plateforme de formation CyberAgent.

ANNEXE 1. DESCRIPTION DU MODULE

DESCRIPTION DU MODULE

Titre du module	Code des modules
...	

Conférencier(s)	Institution ou département où le module est dispensé
...	...

Mode d'enseignement	Langue
Présentiel, en ligne, hybride	*Anglais, ...*

Conditions préalables
...

Nombre de crédits ECTS alloués	Charge de travail de l'étudiant	Horaires de travail	Horaires de travail individuel
5	...	...	...

Objectif et résultats du module		
...		
Acquis d'apprentissage du module	**Méthodes d'enseignement et d'apprentissage**	**Méthodes d'évaluation**
Compétences techniques		
Compétences analytiques		
Compétences en matière de gestion des risques		
Compétences d'organisation		

Faciliter l'accès aux ressources (équipements, logiciels, technologie)
...

Contenu du module: répartition des sujets	Heures de travail					Heures de travail individual et tâches	
	Cours magistraux (HEI/EFP)	Consultations (PME)	Pratique (HEI/EFP)	Essais	**Tout les travaux**	**Travail individuel**	**Tâches**
1							
…							
n							
Total							

Stratégie d'évaluation	Pourcentage comparatif	Critères d'évaluation
Auto test I		…
…		…
Auto test m		…
Test d'évaluation des connaissances		…
Certification HEI/EFP -> Autotest I + …+ Autotest n + Test d'évaluation des connaissances		
Certification PME/Autoformation -> Autotest I + …+ Autotest n + Test d'évaluation des connaissances		
Micro-modules, micro-section -> Autotest I (en option), Autotest n (en option)		

Matériel d'études*(Nom de famille, première initiale. (Année, mois jour). Titre de l'article. Titre du magazine/journal/journal, numéro de volume (numéro de parution), numéros de page de l'article entier, éditeur, URL)*
Lecture obligatoire
…
Lecture recomandée
…

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