Co-funded by the European Union

NIVEAU CEC 4-5

MODULES DE FORMATION POUR LES ÉTUDIANTS EN FORMATION PROFESSIONNELLE

CYBER AGENT 01.2025

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

Lot de travail 3 : Développement de ressources pédagogiques pour les agents du changement en matière de cybersécurité

Livrable 3.2 : Modules de formation pour les étudiants en EFP
Responsable du 3.2 – TIMTAL (TR)

CONTENU

LISTE DES TABLEAUX 1
INTRODUCTION 2
1. OBJECTIFS DU PROGRAMME CYBERAGENT EQF NIVEAU 4 4
2. LE CADRE EUROPÉEN DES CERTIFICATIONS 5
3. ÉTUDIANTS EN FORMATION PROFESSIONNELLE EN CYBERSÉCURITÉ (NIVEAU 4 DU CEC) 6
3.1. Programme CYBERAGENT LEARNING pour le CEC-4 7
CONCLUSION 24

LISTE DES TABLEAUX

Tableau 1 - Résultats d'apprentissage du niveau 4 du CEC 6
Tableau 2 - Module : 1 7
Tableau 3 - Module : 2 8
Tableau 4 - Module : 3 13
Tableau 5 - Module : 4 15
Tableau 6 - Module : 5 16
Tableau 7 - Module : 6 18
Tableau 8 - Module : 7 20
Tableau 9 - Module : 8 21

INTRODUCTION

Les changements rapides dans les domaines scientifiques et technologiques, l'évolution des besoins des individus et de la société, les innovations et les développements dans les théories et les approches d'apprentissage et d'enseignement ont eu une incidence directe sur les rôles attendus des individus. Ce changement définit un individu qui produit des connaissances, peut les utiliser de manière fonctionnelle dans la vie, peut résoudre des problèmes, penser de manière critique, est entreprenant, déterminé, possède des compétences en communication, peut faire preuve d'empathie, contribue à la société et à la culture, etc.

La vitesse vertigineuse apportée par l'ère de l'information s'accompagne d'une évolution constante des besoins des individus et des sociétés. Les innovations dans les théories d'apprentissage et d'enseignement modifient radicalement les rôles attendus des individus. Aujourd'hui, il ne s'agit plus seulement d'avoir des connaissances, mais aussi de posséder des compétences telles que la capacité à utiliser ces connaissances de manière fonctionnelle dans la vie, à trouver des solutions à des problèmes complexes, à penser de manière critique, à agir avec un esprit entrepreneurial, à communiquer efficacement, à faire preuve d'empathie et à apporter une valeur ajoutée à la société. Cette transformation encourage les individus à apprendre, à s'adapter et à s'améliorer constamment.

Dans ce contexte, la formation professionnelle connaît également une transformation majeure. Les professions traditionnelles sont remplacées par de nouvelles professions axées sur la technologie et en constante évolution. La cybersécurité revêt une importance cruciale dans ce changement. En effet, dans un monde en pleine numérisation, les risques liés à la cybersécurité augmentent dans tous les secteurs et toutes les professions. La cybersécurité joue un rôle essentiel dans de nombreux domaines, des données personnelles à la protection des secrets d'entreprise, en passant par la sécurité des infrastructures critiques et la sécurité des transactions financières.

L'importance de la formation à la cybersécurité dans l'enseignement professionnel ne se limite pas aux compétences techniques. Elle consiste également à former des individus qui ont des valeurs éthiques, un sens élevé des responsabilités, qui connaissent les réglementations légales et qui sont ouverts à l'apprentissage continu. Car la cybersécurité n'est pas seulement un problème technique, mais aussi une responsabilité sociale. Par conséquent, accorder l'importance nécessaire à la formation à la cybersécurité dans l'enseignement professionnel est une étape cruciale pour l'avenir des individus et de la société.

L'enseignement professionnel comprend la planification, la recherche, le développement, l'organisation et la gestion coordonnée, la supervision et les activités d'enseignement de tous les services d'enseignement professionnel et technique, ainsi que les secteurs de l'agriculture, de l'industrie et des services, dans le cadre de l'intégrité du système éducatif. L'objectif de ces activités éducatives est de former des experts qui assureront la continuité de la société et le personnel qualifié nécessaire à chaque étape de la production, et de mettre l'accent sur la formation professionnelle.

Le programme d'enseignement professionnel Cyber Agent (EQF4-5) est conçu pour préparer les individus à la vie dans le domaine de la cybersécurité et est basé sur les besoins du marché du travail et l'analyse des emplois. Le programme Cyber Agent vise à fournir les connaissances, les compétences, les attitudes et les comportements nécessaires pour effectuer le travail et les transactions pertinents à travers des leçons et des réalisations, tandis que, d'autre part, les activités éducatives sont planifiées de manière à préparer les individus à la vie professionnelle conformément à ce cadre.

1. OBJECTIFS DU PROGRAMME CYBERAGENT EQF NIVEAU 4-5

Le besoin de cybersécurité est devenu très important, en particulier dans les pays de l'UE, mais aussi dans le monde entier, et s'est rapidement accru ces dernières années. Parallèlement aux progrès technologiques, les risques et les menaces cybernétiques ont également évolué à la même vitesse et sont devenus complexes. Les cyberrisques et les cybermenaces ont atteint un potentiel qui entraînera des conséquences beaucoup plus importantes et négatives que les attaques physiques. Avec des secteurs tels que la finance, les communications électroniques, l'énergie, les transports et l'aviation qui fournissent des services dans un environnement numérique sécurisé, la garantie de la cybersécurité nationale est devenue l'une des principales priorités de notre pays. Dans ce contexte, l'objectif est de diffuser l'éducation à la cybersécurité dans l'enseignement formel et informel, et de développer et d'enrichir le contenu éducatif.

2. LE CADRE EUROPÉEN DES CERTIFICATIONS

L'UE a élaboré le cadre européen des certifications (CEC) comme outil de traduction afin de rendre les certifications nationales plus faciles à comprendre et plus comparables. Le CEC vise à soutenir la mobilité transfrontalière des apprenants et des travailleurs, à promouvoir l'apprentissage tout au long de la vie et le développement professionnel dans toute l'Europe.

Le CEC est un cadre à 8 niveaux, basé sur les acquis de l'apprentissage, qui s'applique à tous les types de qualifications et sert d'outil de traduction entre les différents cadres nationaux de qualifications. Ce cadre contribue à améliorer la transparence, la comparabilité et la portabilité des qualifications des personnes et permet de comparer les qualifications de différents pays et établissements.

Le CEC couvre tous les types et tous les niveaux de qualifications et l'utilisation des acquis d'apprentissage permet de déterminer clairement ce qu'une personne sait, comprend et est capable de faire. Le niveau augmente en fonction du niveau de compétence, le niveau 1 étant le plus bas et le niveau 8 le plus élevé. Plus important encore, le CEC est étroitement lié aux cadres nationaux de certification, ce qui lui permet de fournir une carte complète de tous les types et niveaux de qualifications en Europe, qui sont de plus en plus accessibles grâce aux bases de données sur les certifications.

Le CEC a été créé en 2008, puis révisé en 2017. Sa révision a conservé les objectifs fondamentaux de transparence et de confiance mutuelle dans le paysage des qualifications en Europe. Les États membres se sont engagés à poursuivre le développement du CEC et à le rendre plus efficace pour faciliter la compréhension des qualifications nationales, internationales et des pays tiers par les employeurs, les travailleurs et les apprenants.

Chacun des 8 niveaux du CEC est défini par un ensemble de descripteurs indiquant les acquis d'apprentissage pertinents pour les qualifications de ce niveau dans tout système de qualifications. Les acquis d'apprentissage sont définis en termes de :

- Connaissances : dans le contexte du CEC, les connaissances sont décrites comme théoriques et/ou factuelles.
- Compétences : dans le contexte du CEC, les compétences sont décrites comme cognitives (impliquant l'utilisation d'une pensée logique, intuitive et créative) et pratiques (impliquant la dextérité manuelle et l'utilisation de méthodes, de matériaux, d'outils et d'instruments).
- Responsabilité et autonomie : dans le contexte du CEC, la responsabilité et l'autonomie sont décrites comme la capacité de l'apprenant à appliquer ses connaissances et ses compétences de manière autonome et responsable.

Tableau «1 » - Résultats d'apprentissage du niveau 4 du CEC

Connaissances	**Capacité**	**Responsabilité et autonomie**
Connaissances factuelles et théoriques dans des contextes généraux au sein d'un domaine d'étude ou d'apprentissage	Ensemble de compétences cognitives et pratiques nécessaires pour apporter des solutions à des problèmes spécifiques dans un domaine de travail ou d'éducation	Appliquer l'autogestion dans le cadre de contextes de travail ou d'apprentissage généralement prévisibles mais susceptibles de changer ; superviser le travail quotidien d'autres personnes, assumer une certaine responsabilité dans l'évaluation et l'amélioration des activités de travail ou d'apprentissage

3. ÉTUDIANTS EN FORMATION PROFESSIONNELLE EN CYBERSÉCURITÉ (NIVEAU CEC 4-5)

L'employé en cybersécurité (niveau 4-5) est un professionnel qualifié qui travaille dans le domaine des systèmes d'information sur le lieu de travail, participe à des études sur les activités préventives en matière de cybersécurité dans le cadre des processus de suivi des vulnérabilités et de sensibilisation à la cybersécurité, assure le suivi des actions, surveille le fonctionnement et la durabilité des systèmes utilisés dans les analyses de cybersécurité, détermine les exigences des réseaux simples, met en place des réseaux physiques, effectue des configurations de niveau simple liées au matériel réseau, assure la sécurité, la maintenance et l'amélioration des réseaux, fournit un soutien technique aux utilisateurs et mène des études de développement professionnel afin de protéger les infrastructures informatiques sur le lieu de travail contre les cybermenaces dans le cadre des exigences de qualité en mettant en œuvre des mesures de santé et de sécurité au travail et de protection de l'environnement.

3.1. PROGRAMME CYBERAGENT LEARNING POUR LES NIVEAUX CEC 4-5

Le programme d'enseignement et de formation professionnels (EQF 4-5) a été élaboré en adaptant stratégiquement le programme complet des établissements d'enseignement supérieur (EQF 5-6). Le processus d'adaptation a consisté à concentrer le contenu afin de l'aligner sur le champ d'application de 1 ECTS et à se concentrer sur les résultats d'apprentissage les plus pertinents pour le public de l'EFP et les besoins immédiats des PME. La priorité a été donnée aux thèmes qui mettent l'accent sur l'application pratique et les compétences fondamentales en matière de cybersécurité, tandis que les concepts théoriques plus approfondis ont été rationalisés pour s'adapter au parcours d'apprentissage de l'EFP.

Tableau2 -Module : 1

<table>
<tr><th>Unités</th><th>Thèmes</th></tr>
<tr><td>Gestion de projet</td><td>Planification de projet
Définition des objectifs du projet
Menaces actuelles en matière de cybersécurité (DDoS, ransomware, logiciels malveillants, hameçonnage, attaques zero-day, attaques IoT, etc.)
Modélisation des menaces et analyse des vulnérabilités
Signalement des menaces et incidents liés à la cybersécurité</td></tr>
<tr><td colspan="2">Résultats d'apprentissage :
Les apprenants seront capables de définir les phases de gestion de projet et de créer un plan de projet de base. (Application)
Les apprenants seront capables de formuler des objectifs de projet clairs, mesurables et réalisables. (Analyse)
Les apprenants identifieront, classeront et évalueront diverses menaces liées à la cybersécurité. (Analyse)
Les apprenants développeront des modèles de menaces et effectueront des analyses de vulnérabilité pour des scénarios spécifiques. (Application)
Les apprenants prépareront des rapports d'incident conformément aux protocoles établis. (Application)</td></tr>
<tr><td>Gestion des ressources</td><td>Outils et logiciels de sécurité
Utilisation efficace des ressources technologiques</td></tr>
<tr><td colspan="2">Résultats d'apprentissage :
Les apprenants démontreront une utilisation efficace des outils et logiciels de cybersécurité pour la détection et la réponse aux menaces. (Application)
Les apprenants optimiseront les ressources technologiques pour améliorer la sécurité et l'efficacité. (Application)</td></tr>
<tr><td>Indicateurs de sécurité</td><td>Indicateurs de sécurité et techniques de mesure
Collecte de données avec SIEM
Analyse des indicateurs de sécurité
Suivi de projet et évaluation des performances
Rapports sur les indicateurs de sécurité</td></tr>
<tr><td colspan="2">Résultats d'apprentissage :</td></tr>
</table>

• Les apprenants identifieront et appliqueront les mesures de sécurité et les techniques de mesure pertinentes. (Application) • Les apprenants configureront et utiliseront des outils SIEM pour la collecte de données et la surveillance de la sécurité. (Application) • Les apprenants interpréteront et analyseront les indicateurs de sécurité afin d'évaluer le niveau de sécurité. (Analyse) • Les apprenants surveilleront et évalueront les performances du projet à l'aide d'indicateurs de sécurité. (Évaluation) • Les apprenants compileront et présenteront des rapports basés sur l'analyse des indicateurs de sécurité. (Application)	
Assurance qualité et contrôle qualité	Gestion de la qualité Normes de qualité en matière de cybersécurité Techniques de test et de validation
Résultats attendus : • Les apprenants mettront en œuvre des pratiques de gestion de la qualité dans des projets de cybersécurité. (Application) • Les apprenants identifieront et appliqueront les normes de qualité pertinentes en matière de cybersécurité. (Application) • Les apprenants développeront et exécuteront des procédures de test et de validation pour les solutions de cybersécurité. (Application)	

3 du tableau -Module : 2

Unités	**Thèmes**
Administration des systèmes d'exploitation	Systèmes d'exploitation Relation entre le matériel et les logiciels Binaires, comptage hexadécimal Bits et octets Ligne de commande dans le système d'exploitation Commandes Windows et Linux Client et serveur Windows Applications, processus et services sous Windows Extensions et types de fichiers Clés et valeurs du registre Paramètres du Panneau de configuration Utilisateurs et groupes Structure du domaine et gestionnaire de serveur AD et GPO Interfaces Linux et noyau Processus sous Linux

	Conventions de nommage des fichiers et répertoires Shells Linux et syntaxe des commandes Manipulation des fichiers et des dossiers Utilisation des commandes de surveillance des tuyaux et des systèmes Gestion des processus et contrôle des tâches Gestion des services
Résultats d'apprentissage : • Les apprenants compareront et mettront en contraste différents systèmes d'exploitation et leurs architectures. • Les apprenants expliqueront l'interaction entre le matériel et les logiciels dans un environnement OS. • Les apprenants effectueront des conversions binaires et hexadécimales et comprendront la représentation des données. • Les apprenants exécuteront des commandes fondamentales dans des environnements Windows et Linux. • Les apprenants géreront des applications, des services et des processus à l'aide d'outils système. • Les apprenants configureront et géreront Active Directory et les GPO. • Les apprenants interagiront avec les interfaces Linux et effectueront des opérations au niveau du noyau. • Les apprenants géreront les services et les processus système à l'aide de commandes Linux.	
Administration des systèmes de bases de données	Référentiels et listes de sources Gestion d'un serveur Web Journaux système et surveillance des journaux Planification des tâches sous Linux Dépannage du serveur et du réseau Sauvegarde et restauration Sécurisation du GRUB Pare-feu Objets Active Directory et gestion des GPO DNS et DHCP Principes fondamentaux de PowerShell Microsoft BitLocker, AppLocker et pare-feu LDAP et Kerberos NTLM Politiques de mot de passe et de verrouillage Authentification et contrôle d'accès Protocole ICMP (Internet Control Message Protocol) TCP vs UDP NetBIOS et SMB SSL et TLS Certificats Protocoles Telnet et Secure Shell (SSH) HTTP et HTTPS Protocoles des systèmes de messagerie Protocole DNS (Domain Name System)

	FTP et RDP Encapsulation vs décapsulation Sniffeurs de réseau et Wireshark TCP/UDP DHCP, DNS
Résultats d'apprentissage : • Les apprenants configureront des référentiels et géreront des listes de sources. • Les apprenants analyseront et surveilleront les journaux à des fins de dépannage et de sécurité. • Les apprenants effectueront des opérations de sauvegarde et de restauration afin de garantir l'intégrité des données. • Les apprenants mettront en œuvre des mesures de sécurité, notamment des pare-feu, BitLocker et AppLocker.	
Administration réseau	Types de réseaux et réseaux sans fil Réseaux et topologies Identité et accès des appareils Infrastructure et dispositifs de sécurité Périphériques spécialisés et architecture réseau Réseaux virtuels Adresses physiques et logiques Modèles OSI et réseaux Encapsulation et décapsulation des données Protocoles réseau et numéros de port Supports et câbles réseau Technologies sans fil Outils d'administration réseau Cisco Packet Tracer Classes réseau et sous-réseaux Protocole de résolution d'adresse (ARP) Adressage IP statique ou dynamique Traduction d'adresses réseau (NAT) Commutateurs et Cisco IOS Sécurité des ports de commutateur et interfaces de routeur Configuration des VLAN et DTP Routage inter-VLAN Introduction aux ACL Dépannage réseau
Résultats d'apprentissage : • Les apprenants apprendront à concevoir et à gérer des réseaux, en comprenant les protocoles et les topologies. • Les apprenants configureront des VLAN, des ACL et géreront des schémas d'adressage IP. • Les apprenants utiliseront des outils tels que Wireshark et Cisco Packet Tracer pour la surveillance et le dépannage.	
Administration du cloud	Hyperviseurs et machines virtuelles Conteneurs Sécurisation des environnements virtuels Sauvegarde et restauration

	Cloud computing et fournisseurs de services cloud Quels sont les modèles de services cloud ? Types de déploiement cloud Réseaux virtuels Services de calcul AWS Amazon Elastic Compute Cloud (EC2) Outils de surveillance du cloud Outils d'automatisation et d'orchestration Menaces et vulnérabilités liées à la sécurité du cloud Gestion des identités et des accès (IAM) Contrôle d'accès basé sur les rôles (RBAC) Authentification multifactorielle (MFA) Chiffrement des données dans le cloud Cloud privé virtuel (VPC) Docker et Kubernetes
Résultats d'apprentissage : • Les apprenants géreront des environnements virtuels à l'aide d'AWS, Docker et Kubernetes. • Les apprenants mettront en œuvre des contrôles de sécurité cloud et la gestion des identités.	
Administration des systèmes cyber-physiques	Sécurité et contrôles d'accès Types d'authentification TACACS+ et RADIUS Configuration AAA Objectifs de gestion des risques Chiffrement et déchiffrement Hachage et tables arc-en-ciel Usurpation MAC et empoisonnement ARP Saut de VLAN et DHCP malveillant Inondation ICMP Inondation TCP et UDP Détournement de session Usurpation DNS Défense en profondeur (DID) et Zero Trust Zones démilitarisées (DMZ) Honeypots et renforcement du réseau Meilleures pratiques pour un réseau sécurisé VPN SSH et VNC Pare-feu avec état et pare-feu sans état Pare-feu basés sur l'hôte ou sur le réseau Pare-feu matériels vs logiciels Pare-feu d'application Web (WAF) IA dans les pare-feu IDS et IPS NIDS et HIDS Snort tcpdump

<table>
<tr><td colspan="2">Résultats d'apprentissage :
• Les apprenants sécuriseront les réseaux à l'aide de pare-feu, d'IDS/IPS et d'outils de détection des menaces.
• Les apprenants appliqueront des techniques de chiffrement et géreront les protocoles de sécurité.</td></tr>
<tr><td>Renforcement du système</td><td>Techniques GenAI
Génération de code
Gestion des comptes utilisateurs et contrôle d'accès
Détection des anomalies et dépannage
Résolution des erreurs du service Apache2
Gestion des correctifs et mises à jour
Sauvegarde et restauration automatisées
Récupération de fichiers supprimés avec GenAI
Procédures de cybersécurité
Détection et analyse des menaces
Réponse aux menaces et remédiation
Exploitation de l'IA pour la détection des menaces en temps réel
Validation et test des modèles GenAI
Configuration et sécurité DNS
Configuration et sécurité DHCP
Principes fondamentaux de PowerShell
Sécurité des ports de commutation
Système d'entrée/sortie de base du réseau (NetBIOS)
Protocole SMB (Server Message Block)
Secure Sockets Layer (SSL) et Transport Layer Security (TLS)
Certificats de sécurité
Protocoles des systèmes de messagerie
Protocole DNS (Domain Name System)
Protocole de transfert de fichiers (FTP)
Protocole RDP (Remote Desktop Protocol)
Planification des tâches sous Linux
Dépannage du serveur
Dépannage réseau
Sauvegarde et restauration
Sécurisation du GRUB
Configuration et sécurisation des pare-feu</td></tr>
<tr><td colspan="2">Résultats d'apprentissage :
• Les apprenants appliqueront des techniques de renforcement pour améliorer la sécurité du système.
• Les apprenants exploiteront l'IA pour la détection des menaces et la surveillance du système.</td></tr>
<tr><td>Renforcement du système</td><td>IR vs SOC
Événements et incidents
Détection et triage des alertes
Documentation et rapports
Que sont les attaques Web ?
DoS et DDoS</td></tr>
</table>

	Injection SQL et XSS Injection de commande et inclusion de fichier local (LFI) Falsification de requêtes intersites (CSRF) Force brute et credential stuffing Pass the Hash et Pass the Ticket Contrôle d'accès défaillant Ransomware Virus informatique et ver Cheval de Troie et logiciel publicitaire Enregistreur de frappe et cryptojacking Malware sans fichier Comprendre la propagation des logiciels malveillants Gérer les IOC et les politiques en matière de mots de passe Politiques d'utilisation acceptable (AUP) Politiques BYOD (Bring Your Own Device) Politiques d'accès à distance
Acquis d'apprentissage : • Distinguer les rôles clés et la collaboration entre R et SOC. • Définir la différence entre les incidents de sécurité et les violations. • Expliquer les sources des alertes de sécurité et les processus de triage. • Fournir une documentation et des rapports efficaces pour les incidents de sécurité. • Décrire les types courants d'attaques Web (DoS/DDoS, injection SQL, XSS, injection de commande, LFI, CSRF). • Expliquer les attaques par force brute et par remplissage de crédenciaux et décrire les contre-mesures. • Comprendre les principes de base des attaques « pass the hash » et « pass the ticket ». • Expliquer comment les vulnérabilités liées au contrôle d'accès peuvent être exploitées. • Expliquer les différents types de logiciels malveillants (ransomware, virus, ver, cheval de Troie, adware, keylogger, cryptojacking, malware sans fichier) et leurs méthodes de propagation. • Expliquer l'importance de la gestion des indicateurs de menace (IOC). • Décrire les éléments clés des politiques de mots de passe forts et des politiques d'utilisation acceptable (AUP). • Évaluer les impacts sur la sécurité des politiques BYOD et d'accès à distance.	

Tableau4 -Module : 3

Unités	**Thèmes**
Mesures de performance (indicateurs)	Mesures de performance Surveillance du système et du réseau Surveillance des métriques de performance Cartographie du réseau Analyse des vulnérabilités Analyse du trafic réseau

<table>
<tr><td colspan="2">Résultats d'apprentissage :
Les apprenants définiront les indicateurs de performance et expliqueront leur importance dans l'évaluation des performances du système et du réseau.
Les apprenants démontreront la configuration et l'utilisation d'outils de surveillance pour l'évaluation continue des performances du système et du réseau.
Les apprenants analyseront et interpréteront les indicateurs de performance afin d'évaluer la santé du système et d'identifier les possibilités d'optimisation.
Les apprenants créeront des cartes réseau pour visualiser, surveiller et optimiser les structures réseau.
Les apprenants effectueront des analyses de vulnérabilité, identifieront les risques de sécurité et recommanderont des mesures correctives.
Les apprenants effectueront une analyse du trafic réseau afin de détecter les menaces potentielles et d'y répondre.</td></tr>
<tr><td>Analyse des données</td><td>Collecte de données
Nettoyage et prétraitement des données
Analyse des données
Visualisation des données
Outils analytiques
Applications de l'analyse des données dans le domaine de la cybersécurité</td></tr>
<tr><td colspan="2">Résultats d'apprentissage :
Les apprenants collecteront les données pertinentes à partir des systèmes, des réseaux et des journaux de sécurité à des fins d'analyse.
Les apprenants nettoieront et prétraiteront les données brutes afin d'en garantir l'exactitude et la cohérence.
Les apprenants appliqueront des techniques statistiques et analytiques pour extraire des informations significatives à partir des données.
Les apprenants créeront des visualisations de données afin de communiquer efficacement les résultats de l'analyse.
Les apprenants utiliseront des outils tels que Python, R et Power BI pour une analyse complète des données.
Les apprenants appliqueront des techniques d'analyse de données pour détecter, analyser et atténuer les menaces de cybersécurité.</td></tr>
<tr><td>Renseignements de sécurité</td><td>Comprendre les renseignements de sécurité
Sources de renseignements de sécurité
Méthodes de collecte de renseignements sur les menaces
Études de cas sur les applications du renseignement en matière de sécurité</td></tr>
<tr><td colspan="2">Résultats d'apprentissage :
Les apprenants expliqueront l'importance des renseignements de sécurité dans la gestion proactive des menaces.
Les apprenants évalueront les sources de renseignements de sécurité, notamment les flux d'informations sur les menaces, les rapports et les outils open source.
Les apprenants décriront les méthodes de collecte et d'analyse des renseignements sur les menaces.
Les apprenants examineront des cas réels afin de comprendre l'application du renseignement de sécurité dans la prévention des cybermenaces.</td></tr>
</table>

5 du tableau -Module : 4

Unités	Thèmes
Principes fondamentaux des opérations de sécurité	Comprendre les opérations de sécurité et le SOC (centre des opérations de sécurité) Rôles et responsabilités dans les opérations de sécurité Aperçu des outils et technologies utilisés dans les opérations de sécurité Exemples pratiques et études de cas
Résultats d'apprentissage : • Les apprenants expliqueront l'objectif et la structure d'un centre des opérations de sécurité ainsi que son rôle dans la cybersécurité. • Les apprenants décriront les rôles et responsabilités du personnel chargé des opérations de sécurité, notamment la réponse aux incidents, la recherche des menaces et la surveillance. • Les apprenants identifieront et démontreront l'utilisation des outils et technologies courants utilisés dans le cadre des opérations de sécurité. • Les apprenants analyseront des exemples concrets et des études de cas afin de comprendre les opérations de sécurité dans la pratique.	
Convergence en matière de sécurité	Comprendre la convergence en matière de sécurité Principes fondamentaux de la sécurité physique (principes de sécurité physique, protection des actifs physiques, politiques) Menaces courantes auxquelles sont confrontées les PME Études de cas mettant en évidence les problèmes de convergence
Résultats d'apprentissage : • Les apprenants définiront la convergence en matière de sécurité et expliqueront son importance dans l'intégration des mesures de sécurité physique et cybernétique. • Les apprenants appliqueront les principes de la sécurité physique pour protéger les actifs, les installations et le personnel. • Les apprenants identifieront et évalueront les menaces de sécurité auxquelles sont couramment confrontées les petites et moyennes entreprises (PME). • Les apprenants examineront des études de cas afin de comprendre l'impact des défis liés à la convergence. • Les apprenants passeront en revue les processus de gestion des informations et des événements de sécurité.	
Gestion des informations et des événements liés à la sécurité	Examen des principes de surveillance de la sécurité (basé sur le module d'autres partenaires) Mise en œuvre de solutions SIEM Configuration des journaux et des alertes Révision des méthodologies de renseignement et de détection des menaces (basée sur le module d'autres partenaires)
Résultats d'apprentissage : • Les apprenants expliqueront les principes de surveillance de la sécurité et leur application dans les solutions SIEM.	

• Les apprenants configureront et exploiteront des solutions SIEM pour une détection et une réponse efficaces aux menaces. • Les apprenants configureront des mécanismes de journalisation et d'alerte dans les outils SIEM afin de surveiller les événements de sécurité. • Les apprenants évalueront les méthodologies de renseignements sur les menaces et de détection pour des opérations de sécurité efficaces.	
Pratiques opérationnelles en matière de sécurité	Conformité et réglementation Stratégies d'amélioration continue des opérations de sécurité Automatisation et orchestration Mesures et rapports
Résultats d'apprentissage : • Les apprenants expliqueront l'importance de la conformité et de la réglementation dans les opérations de sécurité. • Les apprenants concevront et mettront en œuvre des stratégies d'amélioration continue pour les opérations de sécurité. • Les apprenants tireront parti de l'automatisation et de l'orchestration pour améliorer l'efficacité des opérations de sécurité. • Les apprenants développeront et utiliseront des mesures de sécurité et des techniques de reporting pour communiquer sur la posture de sécurité.	

6 du tableau -Module : 5

Unités	**Thèmes**
Contexte organisationnel	Évolution de la cybersécurité dans les PME Principales menaces et vulnérabilités actuelles Impact de la cybersécurité sur la stratégie commerciale Défis spécifiques de la cybersécurité dans les PME par rapport aux grandes entreprises Comprendre les implications réglementaires des pratiques de cybersécurité et leur adéquation avec les structures de gouvernance. Défis courants en matière de cybersécurité spécifiques aux PME, tels que les budgets limités, le manque de personnel dédié à la sécurité et les méthodes pratiques pour hiérarchiser les investissements en matière de cybersécurité.
Résultats d'apprentissage : • Les apprenants retraceront l'évolution des pratiques de cybersécurité au sein des petites et moyennes entreprises. • Les apprenants identifieront et évalueront les menaces et vulnérabilités actuelles les plus critiques qui affectent les PME. • Les apprenants analyseront l'influence de la cybersécurité sur la stratégie commerciale et la prise de décision opérationnelle. • Les apprenants compareront les défis en matière de cybersécurité auxquels sont confrontées les PME avec ceux rencontrés par les grandes organisations. • Les apprenants interpréteront les exigences réglementaires en matière de cybersécurité et évalueront leur intégration dans la gouvernance organisationnelle.	

• Les apprenants décriront des solutions pratiques aux défis courants des PME en matière de cybersécurité, tels que les contraintes budgétaires et le personnel limité.	
Confidentialité	Principes de confidentialité en matière de cybersécurité Protection des données personnelles et RGPD Impact de la confidentialité sur les opérations des PME Outils et techniques pour la protection de la vie privée
Acquis d'apprentissage : • Les apprenants expliqueront les principes fondamentaux de la confidentialité dans le contexte de la cybersécurité. • Les apprenants appliqueront les exigences du RGPD et évalueront leur impact sur la protection des données personnelles. • Les apprenants évalueront l'impact des réglementations en matière de confidentialité sur les activités quotidiennes et les modèles économiques des PME. • Les apprenants utiliseront des outils et mettront en œuvre des techniques pour préserver la confidentialité et protéger les données sensibles.	
Lois, éthique et conformité	Organisations, politiques et normes en matière de cybersécurité Législation nationale et internationale pertinente Conformité réglementaire dans les PME Éthique en matière de cybersécurité Conséquences juridiques de la non-conformité en matière de cybersécurité Analyse de la manière dont les outils basés sur l'IA peuvent être utilisés pour renforcer la gouvernance en matière de cybersécurité et garantir la conformité grâce à une surveillance continue et à une réponse automatisée aux menaces.
Résultats d'apprentissage : • Les apprenants identifieront les principales organisations de cybersécurité et évalueront les cadres politiques et normatifs pertinents. • Les apprenants résumeront les principales lois ayant une incidence sur la cybersécurité aux niveaux national et international. • Les apprenants concevront des stratégies pour atteindre et maintenir la conformité réglementaire dans le contexte des PME. • Les apprenants examineront les considérations éthiques dans la prise de décision et le comportement en matière de cybersécurité. • Les apprenants évalueront les conséquences juridiques du non-respect des lois sur la cybersécurité. • Les apprenants exploreront comment les outils d'IA peuvent améliorer la gouvernance, automatiser la surveillance et renforcer la conformité.	
Gouvernance de la sécurité	Structure de gouvernance en matière de cybersécurité Rôles et responsabilités dans la gestion de la sécurité Modèles de maturité en matière de cybersécurité Améliorer les capacités à mener des évaluations des risques et à formuler des plans d'intervention stratégiques dans des conditions de crise simulées (ransomware, attaque par hameçonnage, etc.)

	Communication au niveau de la direction et du conseil d'administration Stratégies de communication en matière de cybersécurité Rapports de sécurité à la direction générale Gestion de crise et communication en matière de cybersécurité Maîtriser les compétences en matière de gestion de crise et de prise de décision dans des scénarios très stressants impliquant des attaques basées sur l'IA et des ransomwares.
Résultats d'apprentissage : • Les apprenants concevront et évalueront des structures de gouvernance qui favorisent une gestion efficace de la cybersécurité. • Les apprenants attribueront et clarifieront les responsabilités dans les cadres de sécurité organisationnels. • Les apprenants évalueront la maturité de la cybersécurité à l'aide de modèles établis. • Les apprenants réaliseront des évaluations des risques et élaboreront des stratégies de réponse pour des scénarios tels que les ransomwares ou le phishing. • Les apprenants élaboreront des plans de communication pour transmettre leurs connaissances en matière de cybersécurité aux cadres supérieurs et aux membres du conseil d'administration. • Les apprenants formuleront des stratégies de communication efficaces pour les parties prenantes internes et externes en matière de cybersécurité. • Les apprenants produiront des rapports informant la haute direction des performances et des risques en matière de cybersécurité. • Les apprenants s'exerceront à gérer et à communiquer lors de crises de cybersécurité, y compris celles impliquant des attaques basées sur l'IA.	
Politique de gestion	Mise en œuvre et suivi des politiques
Résultats d'apprentissage : • Les apprenants mettront en œuvre des politiques de cybersécurité et établiront des procédures pour leur suivi et leur application continus.	

7 du tableau -Module : 6

Unités	**Thèmes**
Introduction à la planification de la cybersécurité : sécurité des données, des personnes et de la société	Sécurité des données - Sécurité du stockage des informations, processus d'enquête Sécurité des données - Techniques d'attaque par mot de passe Sécurité humaine - Sensibilisation et compréhension Sécurité sociétale - Qu'est-ce que la cybercriminalité, la cyberéthique Sécurité sociétale - Cyberdroit - Preuves numériques, contrats numériques, conventions multinationales (accords)
Résultats d'apprentissage : • Les apprenants mettront en œuvre des stratégies pour sécuriser les informations stockées et soutenir les processus d'enquête.	

<table>
<tr><td colspan="2">

Les apprenants identifieront et analyseront les techniques courantes d'attaque par mot de passe et élaboreront des contre-mesures appropriées.
Les apprenants sensibiliseront à la cybersécurité et favoriseront la compréhension parmi les employés et les parties prenantes.
Les apprenants expliqueront les implications sociétales de la cybercriminalité et évalueront les considérations éthiques dans les environnements numériques.
Les apprenants interpréteront les concepts clés du droit numérique, notamment les preuves numériques, les contrats et les accords internationaux.

</td></tr>
<tr><td>Gestion opérationnelle et tactique</td><td>Mise en œuvre des contrôles d'accès
Gestion des correctifs et mises à jour logicielles
Surveillance continue du système
Formation des employés à la sensibilisation à la sécurité</td></tr>
<tr><td colspan="2">Résultats d'apprentissage :

Les apprenants concevront et mettront en œuvre des mécanismes de contrôle d'accès efficaces pour protéger les systèmes et les données.
Les apprenants établiront des procédures pour la gestion des correctifs et les mises à jour logicielles en temps opportun afin de réduire les vulnérabilités.
Les apprenants effectueront une surveillance continue des systèmes afin de détecter les incidents de sécurité et d'y répondre.
Les apprenants élaboreront et dispenseront des programmes de formation à la sensibilisation à la sécurité afin de renforcer l'engagement des employés et de réduire les risques humains.

</td></tr>
</table>

8 du tableau -Module : 7

Unités	**Thèmes**
Évaluation des risques	Cadre et processus généraux de gestion des risques Principes de gestion des risques Normes de gestion des risques Exemples pratiques et études de cas
Acquis d'apprentissage : • Les apprenants seront capables de décrire et d'appliquer le cadre général et le processus de gestion des risques en matière de cybersécurité. • Les apprenants expliqueront les principes fondamentaux qui guident une gestion efficace des risques liés à la cybersécurité. • Les apprenants identifieront et interpréteront les normes de gestion des risques largement acceptées. • Les apprenants évalueront des scénarios de risque à l'aide d'exemples concrets et d'études de cas.	
Identification des risques	Sources tangibles et intangibles de risque Causes et événements Menaces et opportunités Vulnérabilités et capacités Changements dans le contexte externe et interne Indicateurs de risques émergents Nature et valeur des actifs et des ressources Conséquences et leur impact sur les objectifs Limites des connaissances et fiabilité des informations Biais, hypothèses et croyances des personnes impliquées. Exemples pratiques et études de cas.
Résultats d'apprentissage : • Les apprenants sauront distinguer les sources de risque tangibles et intangibles dans les environnements de cybersécurité. • Les apprenants identifieront les causes des risques et les événements déclencheurs. • Les apprenants analyseront les menaces liées à la cybersécurité et évalueront les possibilités d'amélioration. • Les apprenants évalueront les vulnérabilités et les capacités organisationnelles en matière de gestion des risques. • Les apprenants évalueront l'influence des changements contextuels sur les risques liés à la cybersécurité. • Les apprenants identifieront les indicateurs signalant l'émergence de nouvelles menaces de cybersécurité. • Les apprenants évalueront la valeur des actifs et la criticité des ressources par rapport au risque. • Les apprenants estimeront les conséquences potentielles et leur impact sur les objectifs stratégiques. • Les apprenants reconnaîtront les limites des informations et des connaissances dans le processus d'identification des risques.	

• Les apprenants réfléchiront à la manière dont les facteurs humains affectent la perception et l'identification des risques. • Les apprenants appliqueront des techniques d'identification à travers des scénarios réels.	
Menaces internes	Définition et types de menaces internes Détection et identification des menaces internes Exemples pratiques et études de cas
Résultats d'apprentissage : • Les apprenants définiront les menaces internes et classeront les différents types. • Les apprenants développeront des compétences pour détecter et réagir aux indicateurs de menaces internes. • Les apprenants analyseront des études de cas d'incidents réels liés à des menaces internes.	
Modèles et méthodologies de mesure et d'évaluation des risques	Modèles et méthodologies d'évaluation quantitative et qualitative des risques Probabilité des événements et conséquences Nature et ampleur des conséquences Niveaux de sensibilité et de confiance. Exemples pratiques et études de cas
Résultats d'apprentissage : • Les apprenants compareront et appliqueront des modèles quantitatifs et qualitatifs dans le cadre d'évaluations des risques liés à la cybersécurité. • Les apprenants évalueront la probabilité et les conséquences potentielles des risques identifiés. • Les apprenants évalueront la gravité et l'ampleur des conséquences associées aux risques liés à la cybersécurité. • Les apprenants détermineront les niveaux d'incertitude et de confiance dans les évaluations des risques. • Les apprenants mettront en œuvre des modèles d'évaluation des risques dans des scénarios pratiques.	
Contrôle des risques	Surveillance et révision Enregistrement et rapports Exemples pratiques et études de cas
Résultats d'apprentissage : • Les apprenants mettront en place des processus réguliers de surveillance et d'examen des risques. • Les apprenants documenteront et rendront compte efficacement des mesures de contrôle des risques. • Les apprenants examineront des exemples concrets afin de comprendre la mise en œuvre efficace du contrôle des risques.	

9 du tableau -Module : 8

Unités	Thèmes
Réponse aux incidents	Définition et importance de la réponse aux incidents Éléments clés d'un plan de reprise après sinistre efficace

	Menaces courantes en matière de cybersécurité
Objectifs pédagogiques • Les apprenants définiront la réponse aux incidents et expliqueront son importance dans la gestion de la cybersécurité. • Les apprenants identifieront et mettront en œuvre les éléments clés d'un plan de reprise après sinistre structuré. • Les apprenants reconnaîtront les menaces courantes en matière de cybersécurité rencontrées lors du traitement des incidents et y répondront.	
Reprise après sinistre	Comprendre la reprise après sinistre Rôles et responsabilités dans la reprise après sinistre Étapes de reprise après sinistre
Résultats d'apprentissage • Les apprenants expliqueront les principes et les objectifs de la reprise après sinistre dans le contexte de la cybersécurité. • Les apprenants décriront les rôles et responsabilités des membres de l'équipe impliqués dans la reprise après sinistre. • Les apprenants élaboreront un plan étape par étape pour restaurer les systèmes et les opérations après une cybercatastrophe.	
Continuité des activités	Comprendre la continuité des activités Rôles et responsabilités dans la continuité des activités Analyse d'impact sur l'activité
Résultats d'apprentissage : • Les apprenants expliqueront le concept et l'importance de la planification de la continuité des activités. • Les apprenants identifieront les rôles et responsabilités liés à la continuité des activités. • Les apprenants réaliseront une analyse d'impact sur l'activité afin d'évaluer les fonctions critiques et les dépendances.	
Sensibilisation, formation et éducation à la sécurité	Comprendre la sensibilisation à la sécurité Responsabilités des employés en matière de cybersécurité
Résultats d'apprentissage : • Les apprenants expliqueront le rôle de la sensibilisation à la sécurité dans la réduction des risques liés à la cybersécurité liés à l'humain. • Les apprenants reconnaîtront les responsabilités des employés dans le respect des protocoles et des meilleures pratiques en matière de cybersécurité.	
Pratiques d'embauche en matière de sécurité	Définition des exigences relatives aux postes liés à la sécurité Réalisation de vérifications approfondies des antécédents
Résultats d'apprentissage : • Les apprenants définiront les rôles liés à la cybersécurité et formuleront les exigences appropriées. • Les apprenants appliqueront les meilleures pratiques en matière de vérification des antécédents pour les rôles sensibles en matière de sécurité.	
Pratiques de résiliation pour des raisons de sécurité	Révocation immédiate de l'accès Notification des équipes concernées Considérations juridiques et de conformité

<table>
<tr><td colspan="2">Résultats d'apprentissage :
Les apprenants mettront en œuvre des procédures permettant de révoquer rapidement l'accès d'un employé lors de son départ.
Les apprenants coordonneront la communication avec les services concernés pendant le processus de départ.
Les apprenants examineront les exigences légales et de conformité liées à la cessation d'emploi dans le domaine de la cybersécurité.</td></tr>
<tr><td>Sécurité des tiers</td><td>Évaluation des risques liés aux tiers
Mise en œuvre des contrôles et des exigences de sécurité
Surveillance et audit continus
Réponse aux incidents et communication</td></tr>
<tr><td colspan="2">Résultats d'apprentissage :
Les apprenants évalueront les risques de sécurité associés aux fournisseurs et partenaires tiers.
Les apprenants concevront et appliqueront des clauses contractuelles afin de garantir la conformité des tiers en matière de sécurité.
Les apprenants mettront en place des pratiques de surveillance et d'audit continus pour la sécurité des tiers.
Les apprenants coordonneront leurs actions avec les tiers lors des activités de réponse aux incidents.</td></tr>
<tr><td>Sécurité dans les processus d'examen</td><td>Intégration de la sécurité dans les révisions
Évaluation de la vulnérabilité et tests de pénétration
Examens post-incident</td></tr>
<tr><td colspan="2">Résultats d'apprentissage :
Les apprenants intégreront les considérations de sécurité dans les processus d'examen organisationnels.
Les apprenants réaliseront des évaluations de vulnérabilité et des tests de pénétration dans le cadre des activités d'examen.
Les apprenants effectueront des examens post-incident afin d'évaluer l'efficacité et d'améliorer les réponses futures.</td></tr>
<tr><td>Problématique particulière relative à la confidentialité des informations personnelles des employés</td><td>Limites de la collecte de données
Stockage et contrôle d'accès
Respect des réglementations en matière de confidentialité
Partage des données et tiers
Consentement et droits des employés</td></tr>
<tr><td colspan="2">Résultats d'apprentissage :
Les apprenants identifieront les limites appropriées pour la collecte des données personnelles des employés.
Les apprenants appliqueront des mesures de stockage sécurisé et de contrôle d'accès pour les données sensibles des employés.
Les apprenants veilleront au respect des réglementations applicables en matière de confidentialité, telles que le RGPD.
Les apprenants évalueront les risques et les règles entourant le partage des données des employés avec des tiers.
Les apprenants comprendront les droits des employés et l'importance d'obtenir leur consentement éclairé.</td></tr>
</table>

CONCLUSION

Ce rapport présente le programme d'études adapté au niveau de l'enseignement professionnel qui doit être pris en compte pour la mise en œuvre réussie de la formation CyberAgent. À la suite des recherches menées depuis le début du projet afin d'identifier les besoins en matière de formation, ce document décrit les besoins des étudiants de l'enseignement professionnel pour leur participation.

Le programme préparé pour le projet CyberAgent de niveau 5-6 du CEC a été pris comme référence lors de la préparation du programme. À partir de ce programme de niveau, des thèmes adaptés au niveau 4-5 du CEC ont été sélectionnés.

Enfin, afin de garantir que la formation soit de la plus haute qualité en termes de contenu, d'organisation et de développement des compétences, des questions liées à des thèmes non transférés du niveau CEC 5-6 ont été posées.

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