CyberAgent

Co-funded by the European Union

D3.1 MODULES DE FORMATION POUR LES ETUDIANTS DES ETABLISSEMENTS D'ENSEIGNEMENT SUPERIEUR

CYBER AGENT 09.2025

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

Financé par l'Union européenne. Les points de vue et opinions exprimés sont toutefois ceux des auteurs uniquement et ne reflètent pas nécessairement ceux de l'Union européenne ou de l'Agence exécutive européenne pour l'éducation et la culture (EACEA). Ni l'Union européenne ni l'EACEA ne peuvent en être tenus responsables.

Lot de travail 3 : CyberAgent Développement de ressources pédagogiques

Livrable 3.1 : Modules de formation pour les étudiants de l'enseignement supérieur

Responsable du WP3 – TIMTAL. Responsable du D3.1 – VU.

CONTENU

INTRODUCTION

Selon le rapport D2.2, les PME sont confrontées à une pénurie importante de spécialistes qualifiés en cybersécurité, et les employés actuels manquent souvent des connaissances systémiques nécessaires pour répondre de manière appropriée à des cybermenaces de plus en plus complexes. Il est donc particulièrement important, dans l'enseignement supérieur, de former des spécialistes capables d'appliquer leurs connaissances dans le contexte des PME, tant dans le domaine technique que dans celui de la gestion. Dans cette optique, un parcours d'apprentissage basé sur les compétences, divisé en différents domaines thématiques et axé sur le développement de compétences pratiques, a été créé dans le document D2.3.

Ce document présente l'un des principaux résultats du projet : les modules de formation destinés aux étudiants de l'enseignement supérieur (D3.1). L'objectif de cette activité est de créer des programmes de formation pour les établissements d'enseignement supérieur (EES) qui couvrent les domaines clés des connaissances, des aptitudes et des compétences en matière de cybersécurité pertinents pour les petites et moyennes entreprises (PME).

Ces modules sont le résultat d'un travail cohérent basé sur une analyse détaillée des besoins (D2.2), au cours de laquelle des représentants des PME, de l'enseignement et de la formation professionnels (EFP) et des établissements d'enseignement supérieur ont été interrogés, ainsi que sur une structure de parcours d'apprentissage clairement définie (D2.3).

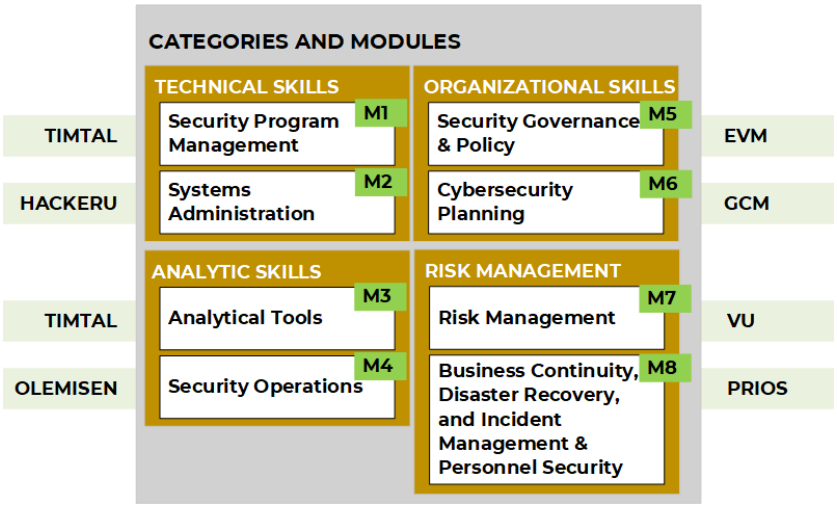
Le programme de formation, qui correspond aux niveaux 5 et 6 du cadre européen des certifications (CEC), est destiné aux étudiants de l'enseignement supérieur et aux employés avancés des PME. Il se compose de huit modules de base et d'un module d'inspiration, couvrant quatre domaines de compétences essentiels :

- **Compétences techniques** (gestion des programmes de sécurité, administration des systèmes).
- **Compétences analytiques** (outils analytiques, opérations de sécurité).
- **Compétences organisationnelles** (gouvernance et politique de sécurité, planification de la cybersécurité).
- **Gestion des risques** (gestion et atténuation des risques, continuité des activités, reprise après sinistre, gestion des incidents et sécurité du personnel).

Chaque module vaut 3 crédits ECTS (correspondant à une charge de travail de 75 heures pour l'étudiant), est conforme aux principes de l'espace européen de l'enseignement supérieur et respecte les recommandations méthodologiques spécifiées dans le document D2.3 : l'enseignement repose sur des méthodes d'apprentissage actif (par exemple, études de cas, apprentissage par projet) et l'apprentissage autonome, les acquis d'apprentissage étant clairement distingués aux niveaux des connaissances, des aptitudes et des compétences.

Chaque module de 3 crédits ECTS a été développé par différents partenaires du consortium, en s'appuyant sur leur domaine spécifique et leur expérience professionnelle.

Les modules développés couvrent les domaines clés suivants, identifiés comme essentiels dans le rapport D2.2 :



1. M1 : GESTION DES PROGRAMMES DE SÉCURITÉ

Titre du module	Code du module
GESTION DU PROGRAMME DE SÉCURITÉ	

Enseignant(s)	Établissement ou département où le module est dispensé

Mode de prestation	Langue
En présentiel, en ligne, hybride	*Anglais, finnois, turc, norvégien, lituanien, roumain, français, polonais, espagnol*

Prérequis
Aucun

Nombre de crédits ECTS attribués	Charge de travail de l'étudiant	Heures de travail en présentiel	Heures de travail individuel
3	75 heures	50 heures	25 heures

Objectif et résultats du module		
À l'issue de ce cours, les étudiants auront acquis les compétences nécessaires pour gérer efficacement les programmes de sécurité en réponse aux menaces de cybersécurité. Ils développeront des stratégies de défense contre les menaces actuelles telles que le phishing, les ransomwares et les attaques DDoS dans le cadre de la gestion de projets et de ressources. En outre, les étudiants apprendront à appliquer des mesures de sécurité et des méthodes d'assurance qualité, acquérant ainsi la capacité d'optimiser les programmes de sécurité, de gérer efficacement les ressources et de renforcer la sécurité organisationnelle en utilisant des outils appropriés contre les menaces en constante évolution. Ce cours leur permettra également de développer leurs compétences en matière d'évaluation des menaces, de reporting et de communication, leur permettant ainsi de mettre en œuvre efficacement des stratégies de cybersécurité au sein de leurs organisations.		
Résultats d'apprentissage du module	**Méthodes d'enseignement et d'apprentissage**	**Méthodes d'évaluation**
Connaissances : les apprenants acquerront des connaissances pratiques sur les dernières menaces en matière de cybersécurité, notamment le phishing, les ransomwares et les attaques DDoS, et apprendront à les gérer grâce à une gestion efficace des projets et des ressources, ainsi qu'à la mise en œuvre de mesures	À sélectionner par le professeur, à partir de la partie 1.3. [Méthodes d'enseignement, par exemple cours théoriques, conférenciers invités, quiz, jeux, travaux pratiques/laboratoires, enseignement et apprentissage entre pairs, apprentissage autoguidé, etc.	Tests d'auto-évaluation Test d'évaluation des connaissances

d'assurance et de contrôle de la qualité.		
Compétences : les apprenants seront capables d'utiliser des outils et des logiciels pour se protéger contre les cybermenaces en constante évolution, et d'appliquer des pratiques de sécurité robustes dans la gestion de projets et de ressources afin d'améliorer les indicateurs de sécurité globaux et le contrôle qualité au sein de leurs organisations.	À sélectionner par le formateur, à partir de la partie 1.3. [Méthodes d'enseignement, par exemple tâches pratiques/laboratoires, activités pratiques, environnements simulés, quiz, jeux, études de cas, etc.] de D2.3 « Structure du parcours d'apprentissage des agents du changement en matière de cybersécurité dans les PME ».	Évaluations pratiques
Compétences : Les apprenants seront capables d'évaluer et d'atténuer les menaces potentielles pour la sécurité, de communiquer efficacement sur les questions de cybersécurité et de signaler avec précision les menaces et les violations par les canaux appropriés au sein de leur organisation.	À sélectionner par le formateur, à partir de la partie 1.3. [Méthodes d'enseignement, par exemple environnements simulés, concours de capture du drapeau, 5E, CBL, CL, POGIL, PBL etc.] de D2.3 « Structure du parcours d'apprentissage des agents du changement en matière de cybersécurité dans les PME »	Simulations Concours

Contenu du module : ventilation des thèmes	**Heures de travail en présentiel**					**Heures de travail individuelles et tâches**	
	Cours	Consultations	Pratique (HEI)	Tests	**Tout travail en**	**Travaux**	**Tâches**
Gestion de projet • Planification de projet • Définition des objectifs du projet • Définition de la portée et des exigences du projet • Préparation du calendrier du projet • Outils de gestion de projet	8	0,5	3	0,5	**12**	**6**	• Planifier un projet de sensibilisation à la cybersécurité pour les employés des PME. • Définir des objectifs clairs pour le projet de sensibilisation à la cy-

• Menaces actuelles en matière de cybersécurité (DDoS, ransomware, logiciels malveillants, hameçonnage, attaques zero-day, attaques IoT, etc.) • Modélisation des menaces et analyse des vulnérabilités • Plans d'intervention d'urgence et en cas d'incident • Signalement des menaces et incidents liés à la cybersécurité							bersécurité afin d'améliorer la compréhension des employés des PME concernant les menaces potentielles en matière de sécurité. • Définir la portée et les exigences du projet de sensibilisation à la cybersécurité destiné aux employés des PME, y compris les thèmes de formation et les ressources nécessaires. • Préparez le calendrier du projet de sensibilisation à la cybersécurité destiné aux employés des PME. • Utiliser des outils de gestion de projet pour suivre l'avancement et l'utilisation des ressources du projet de sensibilisation à la cybersécurité destiné aux employés des PME. • Effectuer des recherches sur les menaces actuelles en matière de cybersécurité et compiler les résultats dans un rapport. • Créer un modèle de menace simplifié pour aider les employés des PME à identifier les vulnérabilités potentielles en matière de sécurité dans leurs opérations quotidiennes. • Rechercher et examiner des exemples de plans d'intervention d'urgence et de réponse aux incidents. • Quelles étapes faut-il envisager lors de la préparation d'un rapport sur les menaces et les incidents liés à la cybersécurité ? Effectuez des

							recherches et résumez vos conclusions.
Gestion des ressources • Gestion des ressources humaines (équipes de projet) • Sensibilisation à la sécurité et formation des équipes • Gestion de l'inventaire du matériel et des logiciels • Outils et logiciels de sécurité • Utilisation efficace des ressources technologiques • Budget et allocation des ressources	8	0,5	3	0,5	**12**	**6**	• Élaborez une stratégie de gestion des ressources afin de garantir l'utilisation efficace des ressources d'une PME fictive. • Créer un exemple de plan thématique pour une formation de sensibilisation à la cybersécurité. • Préparez un inventaire du matériel et des logiciels pour une PME fictive. • Rechercher les outils et logiciels de sécurité couramment utilisés. • Créer un exemple de budget et de plan d'allocation des ressources pour une PME hypothétique.
Indicateurs de sécurité • Indicateurs de sécurité et techniques de mesure • Collecte de données avec SIEM • Analyse des indicateurs de sécurité • Suivi du projet et évaluation des performances • Examen des actions et adaptation du projet • Rapports sur les mesures de sécurité	8	0,5	4	0,5	**13**	**6**	• Recherchez les indicateurs de sécurité utilisés pour évaluer la posture de cybersécurité dans les PME. • Recherchez les sources à partir desquelles le logiciel SIEM collecte les journaux. • Configurez et examinez un logiciel SIEM open source. • Analyser les indicateurs de sécurité en collectant des journaux à l'aide d'un logiciel SIEM. • Présentez les résultats de l'analyse des indicateurs de sécurité à l'aide de graphiques et de visuels.
Assurance qualité et contrôle qualité • Gestion de la qualité • Normes de qualité en matière de cybersécurité • Audits de conformité et de qualité	8	0,5	4	0,5	**13**	**7**	• Comment planifier les processus d'assurance qualité et de contrôle qualité afin d'améliorer l'efficacité des applications de cybersécurité

• Techniques de test et de validation • Évaluation et recommandations d'amélioration							dans les PME ? Effectuez des recherches et résumez vos conclusions. • Recherchez les éléments de contrôle de l'annexe A de la norme ISO/IEC 27001:2022. • Faites des recherches et rédigez un rapport sur les techniques de test et de validation. • Quels avantages la révision et l'amélioration continues des processus qualité apportent-elles aux PME ?
Total	**32**	**2**	**14**	**2**	**50**	**25**	

Stratégie d'évaluation	**Pourcentage pondéré comparatif**	**Critères d'évaluation**
Test d'auto-évaluation I	10 %	10 points - 95 à 100 % de réponses correctes. 9 points – 85 à 94 % de réponses correctes. 8 points - 75 à 84 % de réponses correctes. 7 points - 65 à 74 % de réponses correctes. 6 points - 55 à 64 % de réponses correctes. 5 points - 45 à 54 % de réponses correctes. 4 points – 35 à 44 % de réponses correctes. 3 points – 25 à 34 % de réponses correctes. 2 points - 15 à 24 % de réponses correctes. 1 point – 0 à 14 % de réponses correctes.
Test d'auto-évaluation II	10	
Test d'auto-évaluation III	10	
Test d'auto-évaluation IV	10	
Test d'évaluation des connaissances	60	

Matériel d'étude *(Nom, initiale du prénom. (Année, mois, jour). Titre de l'article. Titre du magazine/journal/quotidien, numéro du volume (numéro du numéro), numéros de page de l'article complet, éditeur, URL)*
Lectures obligatoires
Lectures recommandées
https://sansorg.egnyte.com/dl/RFrVIbX2oc https://edwps.com/wp-content/uploads/2018/04/Cyber-PMO-U.S.-Cyber-Magazine.pdf https://healthybyte.net/cybersecurity/what-is-a-security-program-management

2. M2 : ADMINISTRATION DES SYSTÈMES

Titre du module	Code du module
ADMINISTRATION DES SYSTÈMES	

Enseignant(s)	Établissement ou département où le module est dispensé

Mode de prestation	Langue
En présentiel, en ligne, mixte	*Anglais, finnois, turc, norvégien, lituanien, roumain, français, polonais, espagnol*

Prérequis
Aucun

Nombre de crédits ECTS attribués	Charge de travail de l'étudiant	Heures de travail en présentiel	Heures de travail individuel
3	75	50	25

Objectif et résultats du module
À l'issue de ce cours, les étudiants seront capables de gérer en continu (identifier, analyser, évaluer, estimer, atténuer) les risques liés à la cybersécurité des infrastructures, systèmes et services TIC en planifiant, appliquant, rapportant et communiquant l'analyse, l'évaluation et le traitement des risques. Les étudiants connaîtront les principes fondamentaux des réseaux afin de gérer correctement les périphériques réseau, d'utiliser les serveurs Linux et Windows, de les gérer et de les sécuriser. De plus, leurs connaissances sur le cloud et l'IA dans le contexte de la cybersécurité leur seront très utiles pour accélérer correctement les tâches et effectuer des automatisations et des mises à l'échelle. Les étudiants apprendront également à renforcer les systèmes, à rechercher les menaces et à rendre les serveurs disponibles (acronyme de la triade CIA).

Résultats d'apprentissage du module	Méthodes d'enseignement et d'apprentissage	Méthodes d'évaluation

Connaissances : les apprenants acquerront des connaissances en administration réseau, systèmes d'exploitation, principes fondamentaux des réseaux, outils d'administration réseau, sécurité des périphériques réseau, administration de systèmes Linux, administration de systèmes Windows, virtualisation, cloud computing utilisant l'IA pour les procédures de mise en réseau et de cybersécurité, procédures de cybersécurité, détection des menaces, analyse des menaces, réponse aux menaces, remédiation des menaces, principes fondamentaux de la cybersécurité, défense de l'organisation contre les attaques, sécurité des infrastructures et des réseaux, surveillance et analyse des réseaux, gestion des incidents. Ils seront capables d'établir et de décrire des procédures d'administration système efficaces, des routines opérationnelles adaptées aux besoins spécifiques des lieux de travail des PME, conformément aux normes en vigueur.	À choisir par l'enseignant : cours en direct, enregistrements vidéo, présentations, appareils virtuels (le cas échéant), analyse de la littérature, conférenciers invités, enseignement et apprentissage entre pairs, mentorat.	Tests d'auto-évaluation et tests d'évaluation des connaissances.
Compétences : Les apprenants seront capables d'utiliser des méthodologies et des outils pour concevoir et mettre en œuvre des architectures système sécurisées, notamment des systèmes d'exploitation, des bases de données, des réseaux et des infrastructures cloud pour les lieux de travail des PME.	À choisir par le professeur : cours en direct, enregistrements vidéo, présentations, appareils virtuels (le cas échéant), analyse de la littérature, conférenciers invités, enseignement et apprentissage entre pairs, mentorat.	Tests d'auto-évaluation et tests d'évaluation des connaissances
Compétences : Les apprenants seront compétents pour développer et mettre en œuvre des cadres stratégiques de cybersécurité pour l'administration des systèmes, diriger des projets et des équipes afin d'améliorer la sécurité et la disponibilité des systèmes, et prendre des décisions éthiques pour maintenir des pratiques de cybersécurité robustes dans divers domaines administratifs pour les lieux de travail des PME.	À choisir par le professeur : cours en direct, enregistrements vidéo, présentations, appareils virtuels (le cas échéant), analyse de la littérature, conférenciers invités, enseignement et apprentissage entre pairs, mentorat.	Tests d'auto-évaluation et tests d'évaluation des connaissances

Contenu du module : répartition des thèmes	Heures de travail en présentiel					Heures de travail individuelles et tâches	
	Cours	Consultations	Pratique (HEI)	Tests	**Tout travail en**	**Travail individuel**	**Tâches**
Administration du système 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 du système et des pipes • Gestion des processus et contrôle des tâches • Gestion des services	4	0,5	2	0,5	**7**	**3,5**	Comptage hexadécimal Pratique des commandes Windows Pratique des commandes Linux Pratique du Gestionnaire des tâches Création et gestion de fichiers Modification et affichage des clés et valeurs du registre Modification des paramètres du Panneau de configuration Gestion des utilisateurs et des groupes Gestion de la structure du domaine Création et suppression d'objets Active Directory Gestion des processus sous Linux Manipulation des fichiers et des dossiers Utilisation des pipes Commandes de surveillance du système Gestion des services Linux
Administration du système de base de données • Référentiels et listes de sources	4	0,5	2	0,5	**7**	**3,5**	Gestion des référentiels et des 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							Gestion d'un serveur Web Vérification et gestion des journaux système et surveillance des journaux Planification des tâches sous Linux Dépannage du serveur Restauration des sauvegardes Sécurisation du GRUB Gestion des services de base de données Configuration des politiques relatives aux mots de passe Configuration des politiques de verrouillage de compte Configuration de l'authentification et du contrôle d'accès
Administration réseau • Types de réseaux et réseaux sans fil • Réseaux et topologies • Identité des périphériques et périphériques d'accès • Infrastructure et sécurité des périphériques • Périphériques spécialisés et architecture réseau • Réseaux virtuels • Adresses physiques et logiques	4	0,5	2	0,5	**7**	**3,5**	Création de topologies réseau Gestion des périphériques réseau Construire le réseau Sécurisation des périphériques réseau Création de réseaux virtuels Configuration des protocoles réseau et des numéros de port Utilisation de Cisco Packet Tracer

• 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							Utilisation du protocole ARP (Address Resolution Protocol) Planification d'un réseau Configuration d'adresses IP statiques et dynamiques Configuration du DHCP et du NAT Utilisation de Cisco IOS Configuration des VLAN Dépannage du réseau
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)	4	0,5	2	0,5	**7**	**3,5**	Création de machines virtuelles Configuration de conteneurs Sécurisation des environnements virtuels Utilisation des sauvegardes Gestion du réseau cloud Configuration des réseaux virtuels Utilisation des outils de surveillance du cloud Mise en œuvre de l'automatisation et de l'orchestration Détection des menaces et des vulnérabilités de sécurité dans le cloud Configuration de la gestion des identités et des accès (IAM) Mise en œuvre du chiffrement des données dans le cloud Utilisation de Docker et Kubernetes

• Docker et Kubernetes							
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	4	0,5	2	0,5	**7**	**3,5**	Mise en place de l'infrastructure Principaux composants Mise en œuvre des contrôles de sécurité Utilisation de TACACS+ et RADIUS Configuration AAA Jouer avec le chiffrement et le déchiffrement Analyse des attaques courantes et des techniques de défense Configuration de zones démilitarisées (DMZ) Recherche sur les honeypots Renforcement via les meilleures pratiques pour un réseau sécurisé Installation d'un VPN Utilisation de Secure Shell (SSH) Utilisation de Virtual Network Computing (VNC) Techniques de fonctionnement des pare-feu Mise en œuvre de l'IA dans les pare-feu Utilisation de Snort et tcpdump pour la protection et la détection
Renforcement du système • 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 • Gestion des actifs informatiques et inventaire	4	0,5	2	0,5	**7**	**3,5**	Travailler avec les techniques GenAI Gestion des comptes utilisateurs et contrôle d'accès Détection des anomalies et dépannage Résolution des erreurs du service Apache2 avec GenAI Configuration de la gestion des correctifs et des mises à jour Configuration de la sauvegarde et de la 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 • Cadres de gouvernance et réglementation • Configuration et sécurité DNS • Configuration et sécurité DHCP • Principes fondamentaux de PowerShell • Sécurité des ports de commutateur • 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 de bureau à distance (RDP) • Planification des tâches sous Linux • Dépannage du serveur • Dépannage réseau • Sauvegarde et restauration • Sécurisation du GRUB • Configuration et sécurisation des pare-feu							Gestion des actifs informatiques Récupération des fichiers supprimés avec GenAI Mise en œuvre de la sécurité DNS et DHCP Utilisation de Microsoft BitLocker et Microsoft AppLocker Configuration du pare-feu Microsoft Configuration de la sécurité des ports de commutation Sécurisation du protocole de transfert de fichiers (FTP) Sécurisation du protocole RDP (Remote Desktop Protocol) Planification des tâches de sécurité sous Linux Sécurisation du GRUB Configuration et sécurisation des pare-feu (iptables)
Disponibilité • IR vs SOC • Événements et incidents • Détection et triage des alertes • Documentation et rapports • Que sont les attaques Web ? • DoS et DDoS • Injection SQL et XSS • Injection de commande et inclusion de fichier local (LFI) • Falsification de requêtes intersites (CSRF) • Force brute et credential stuffing	4	0,5	3	0,5	**8**	4	Détection des événements et incidents Effectuer le triage des alertes Documentation et rapports appropriés Mise en œuvre d'activités post-incident Réalisation et protection contre les attaques DoS et DDoS

• Pass the Hash et Pass the Ticket • Reconnaissance LDAP • Contrôle d'accès défaillant • Ransomware • Virus informatique et ver • Cheval de Troie et logiciel publici-taire • Enregistreurs de frappe et cryp-tojacking • Malware sans fichier • Comprendre la propagation des logiciels malveillants • Analyse statique et dynamique des logiciels malveillants • Analyse sécurisée des logiciels malveillants • Analyse hybride Enquête sur les lo-giciels malveillants • Réalisation d'une analyse statique et dynamique des logiciels mal-veillants • Gestion des IOC et des politiques en matière de mots de passe • Politiques d'utilisation acceptable (AUP) • Politiques BYOD (Bring Your Own Device) • Politiques d'accès à distance							Détection des attaques Web et de la propagation des logiciels malveillants Effectuer une analyse statique et dynamique sécurisée des logiciels malveillants Gestion des IOC Mise en place de politiques en matière de mots de passe Mise en place de politiques BYOD (Bring Your Own Device) Mise en place de politiques d'accès à distance
Total	**28**	**3,5**	**15**	**3,5**	**50**	**25**	

Stratégie d'évaluation	**Pourcentage pondéré comparatif**	**Critères d'évaluation**
Test d'auto-évaluation (1)	5 %	10 points - 95 à 100 % de réponses correctes. 9 points - 85 à 94 % de réponses correctes. 8 points - 75 à 84 % de réponses correctes. 7 points - 65 à 74 % de réponses correctes. 6 points – 55 à 64 % de réponses correctes. 5 points - 45 à 54 % de réponses correctes. 4 points – 35 à 44 % de réponses correctes. 3 points – 25 à 34 % de réponses correctes. 2 points - 15 à 24 % de réponses correctes. 1 point – 0 à 14 % de réponses correctes.
Test d'auto-évaluation (2)	5 %	
Test d'auto-évaluation (3)	5 %	
Test d'auto-évaluation (4)	5	
Test d'auto-évaluation (5)	5	
Test d'auto-évaluation (6)	5	
Test d'auto-évaluation (7)	5	
Test d'évaluation des connaissances	65 %	

3. M3 : OUTILS ANALYTIQUES

Titre du module	Code du module
OUTILS ANALYTIQUES	

Enseignant(s)	Établissement ou département où le module est dispensé

Mode de prestation	Langue
En présentiel, en ligne, hybride	*Anglais, finnois, turc, norvégien, lituanien, roumain, français, polonais, espagnol*

Prérequis
Aucun

Nombre de crédits ECTS attribués	Charge de travail de l'étudiant	Heures de travail en présentiel	Heures de travail individuel
3	75	50	25

Objectif et résultats du module		
À l'issue de ce cours, les étudiants auront acquis les compétences nécessaires pour protéger les actifs de l'organisation à l'aide d'indicateurs de performance, d'analyses de données et de renseignements de sécurité. Ils apprendront à utiliser efficacement des outils analytiques pour identifier les risques et vulnérabilités potentiels en matière de cybersécurité, à exploiter les informations issues des données pour renforcer les mesures de sécurité et à utiliser des indicateurs de performance liés aux mots de passe, à l'utilisation des navigateurs, aux e-mails et aux applications de traitement des données. À la fin du module, les participants seront en mesure d'évaluer et d'atténuer les menaces potentielles pour la sécurité à l'aide d'outils appropriés et de signaler toute menace ou perturbation aux instances réglementaires compétentes.		
Résultats d'apprentissage du module	**Méthodes d'enseignement et d'apprentissage**	**Méthodes d'évaluation**
Connaissances : les apprenants acquerront des connaissances pratiques sur la manière d'appliquer les mesures de performance, l'analyse des données et les renseignements en matière de sécurité pour protéger les actifs de l'organisation.	À sélectionner par le professeur, à partir de la partie 1.3. [Méthodes d'enseignement, par exemple cours théoriques, conférenciers invités, quiz, jeux, travaux pratiques/laboratoires, enseignement et apprentissage entre pairs, apprentissage autoguidé, etc.] de D2.3 « Structure du parcours d'apprentissage des agents de changement en matière de cybersécurité dans les PME ».	Tests d'auto-évaluation Test d'évaluation des connaissances

Compétences : les apprenants seront capables d'utiliser des outils analytiques pour identifier les risques et vulnérabilités potentiels en matière de cybersécurité, d'appliquer des connaissances fondées 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, des e-mails et du traitement des données.	À sélectionner par le formateur, à partir de la partie 1.3. [Méthodes d'enseignement, par exemple tâches pratiques/laboratoires, activités pratiques, environnements simulés, quiz, jeux, études de cas, etc.] de D2.3 « Structure du parcours d'apprentissage des agents du changement en matière de cybersécurité dans les PME ».	Évaluations pratiques
Compétences : les apprenants seront capables d'évaluer et d'atténuer les menaces potentielles pour la sécurité à l'aide d'outils analytiques, et de signaler avec précision les menaces et les violations aux canaux appropriés au sein de leur organisation.	À sélectionner par le conférencier, à partir de la partie 1.3. [Méthodes d'enseignement, par exemple environnements simulés, concours de capture du drapeau, 5E, CBL, CL, POGIL, PBL etc.] de D2.3 « Structure du parcours d'apprentissage des agents du changement en matière de cybersécurité dans les PME »	Simulations Concours

Contenu du module : ventilation des thèmes	**Heures de travail en présentiel**					**Heures de travail individuelles et tâches**	
	Cours magistraux	Consultations	Pratique (HEI)	Tests	**Tout travail en contact**	**Travaux individuels**	**Tâches**
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	10	0,5	5	0,5	**16**	**8,5**	• Effectuer des recherches sur les indicateurs de performance et les outils. Comparer les outils de surveillance des performances et identifier leurs différences. • Terminer l'installation de Zabbix et effectuer la configuration de base. • Créer une application pour surveiller les mesures de performance avec Zabbix.

							• Identifier les vulnérabilités du système cible à l'aide d'un logiciel de cartographie réseau (tel que nmap, rustscan, etc.). • Effectuer une analyse des vulnérabilités du système cible à l'aide du logiciel Nessus. Préparer un rapport de test de vulnérabilité. • Effectuer une analyse du trafic réseau à l'aide de Wireshark.
Analyse des données • 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	10	0,5	5	0,5	**16**	**8,5**	• Effectuer les étapes de nettoyage et de prétraitement des données sur un ensemble de données liées aux questions de cybersécurité préparé pour une PME hypothétique. • Analyser l'ensemble de données nettoyé et prétraité provenant de la PME hypothétique et visualiser les résultats. • Quels sont les exemples d'applications de l'analyse de données dans le domaine de la cybersécurité ? Veuillez effectuer des recherches.
Renseignement de sécurité • Comprendre les renseignements de sécurité • Sources de renseignements de sécurité • Méthodes de collecte de renseignements sur les menaces • Cadres de renseignements sur les menaces • Plateformes de renseignements de sécurité basées sur l'IA • Études de cas sur les applications du renseignement en matière de sécurité	10	0,5	7	0,5	**18**	**8**	• Étudiez comment les renseignements de sécurité contribuent aux stratégies de sécurité proactives des PME. • Quelles sont les sources les plus courantes pour obtenir des renseignements sur la sécurité ? Comment évaluer la fiabilité de ces sources ? • Définissez les avantages et les limites de chaque méthode de collecte de renseignements sur les menaces. • Expliquez les principales caractéristiques des cadres de renseignements sur les menaces tels que MITRE

							ATT&CK et Cyber Kill Chain. • Examinez une étude de cas réelle dans laquelle des renseignements de sécurité ont été utilisés. Décrivez les méthodes de collecte de renseignements utilisées dans cette étude de cas.
Total	**30**	**1,5**	**17**	**1,5**	**50**	**25**	

Stratégie d'évaluation	Pourcentage pondéré comparatif	Critères d'évaluation
Test d'auto-évaluation I	15	10 points - 95 à 100 % de réponses correctes. 9 points – 85 à 94 % de réponses correctes. 8 points - 75 à 84 % de réponses correctes. 7 points - 65 à 74 % de réponses correctes. 6 points - 55 à 64 % de réponses correctes. 5 points - 45 à 54 % de réponses correctes. 4 points – 35 à 44 % de réponses correctes. 3 points – 25 à 34 % de réponses correctes. 2 points – 15 à 24 % de réponses correctes. 1 point – 0 à 14 % de réponses correctes.
Test d'auto-évaluation II	15	
Test d'auto-évaluation III	15	
Test d'évaluation des connaissances	55	

Matériel d'étude *(Nom, initiale du prénom. (Année, mois, jour). Titre de l'article. Titre du magazine/journal/quotidien, numéro du volume (numéro du numéro), numéros de page de l'article complet, éditeur, URL)*
Lectures obligatoires
…
Lectures recommandées
https://brainstation.io/career-guides/what-tools-do-cybersecurity-analysts-use **https://www.comptia.org/content/articles/what-is-wireshark-and-how-to-use-it** **https://medium.com/@jcm3/wireshark-traffic-analysis-part-1-tryhackme-walkthrough-a9bec11d94d9** **https://www.kali.org/tools/nmap/** **https://www.freecodecamp.org/news/what-is-nmap-and-how-to-use-it-a-tutorial-for-the-greatest-scanning-tool-of-all-time/** **https://www.varonis.com/blog/cyber-kill-chain** **https://www.youtube.com/watch?v=kVnvIBNiC58**

4. M4 : OPÉRATIONS DE SÉCURITÉ

Titre du module	Code du module
OPÉRATIONS DE SÉCURITÉ	

Enseignant(s)	Établissement ou département où le module est dispensé

Mode de prestation	Langue
En présentiel, en ligne, mixte, consultations	*Anglais, finnois, turc, norvégien, lituanien, roumain, français, polonais, espagnol*

Conditions préalables
Aucun

Nombre de crédits ECTS attribués	Charge de travail de l'étudiant	Heures de travail en présentiel	Heures de travail individuel
3	75	50	25

Objectif et résultats du module		
À l'issue de ce cours, les étudiants seront capables de gérer efficacement les opérations de sécurité au sein des infrastructures, des systèmes et des services TIC. Ils acquerront les compétences nécessaires pour surveiller, détecter, réagir et remédier aux incidents de cybersécurité en appliquant les meilleures pratiques, les outils et les cadres pertinents pour les opérations de sécurité.		
Résultats d'apprentissage du module	**Méthodes d'enseignement et d'apprentissage**	**Méthodes d'évaluation**
Connaissances : les apprenants acquerront des connaissances avancées en matière d'opérations de sécurité, notamment la surveillance, la détection, la réponse aux incidents et la récupération. Ils seront capables d'établir et de décrire des routines opérationnelles efficaces en matière de cybersécurité, adaptées aux besoins spécifiques des PME, conformément aux normes de cybersécurité.	À sélectionner par l'enseignant, à partir de la partie 1.3. [Méthodes d'enseignement, par exemple cours théoriques, analyse de la littérature, conférenciers invités, enseignement et apprentissage entre pairs, mentorat, etc.] de D2.3 « Structure du parcours d'apprentissage des agents du changement en matière de cybersécurité dans les PME ».	Tests d'auto-évaluation Test d'évaluation des connaissances

Compétences : les apprenants seront capables d'appliquer des méthodologies et des outils avancés pour effectuer des tâches liées à la sécurité, concevoir et mettre en œuvre des stratégies de surveillance efficaces, gérer les incidents et développer des routines opérationnelles robustes spécialement adaptées aux lieux de travail des PME.	À sélectionner par le conférencier, à partir de la partie 1.3. [*Méthodes d'enseignement, par exemple cours théoriques, analyse de la littérature, conférenciers invités, enseignement et apprentissage entre pairs, mentorat, etc.]* de D2.3 « *Structure du parcours d'apprentissage des agents du changement en matière de cybersécurité dans les PME* »	Tests d'auto-évaluation Test d'évaluation des connaissances
Compétences : les apprenants seront compétents pour élaborer et mettre en œuvre des politiques et des procédures stratégiques en matière de sécurité pour les lieux de travail des PME.	À sélectionner par le conférencier, à partir de la partie 1.3. [*Méthodes d'enseignement, par exemple cours théoriques, analyse de la littérature, conférenciers invités, enseignement et apprentissage entre pairs, mentorat, etc.]* de D2.3 « *Structure du parcours d'apprentissage des agents du changement en matière de cybersécurité dans les PME* ».	Tests d'auto-évaluation Test d'évaluation des connaissances

Contenu du module : répartition des thèmes	**Heures de travail en présentiel**					**Heures de travail individuelles et tâches**	
	Cours	Consultations	Pratique (HEI)	Tests	Tout le travail	Travail individuel	Tâches

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 liés aux opérations de sécurité	6	0,5	2	0,5	**9**	6	Identifier et comprendre la structure et le fonctionnement d'un SOC, analyser les différents rôles au sein des opérations de sécurité, rechercher les outils utilisés dans les opérations de sécurité et analyser une étude de cas.
Convergence de la sécurité - Comprendre la convergence de la sécurité - Principes fondamentaux de la sécurité physique (principes de sécurité physique, protection des actifs physiques, politiques) - Étude de cas mettant en évidence les principes de la convergence de la sécurité	8	0,5	4	0,5	**13**	6	Passer en revue la définition et les principes de la convergence de la sécurité, reconnaître l'importance d'intégrer les opérations de sécurité physique et numérique, identifier et évaluer les risques dans les domaines cybernétique et physique.

Gestion des informations et des événements de sécurité - Révision des principes de surveillance de la sécurité - Mise en œuvre de solutions SIEM	8	0,5	4	0,5	**13**	6	Introduction à la surveillance de la sécurité et à la mise en œuvre d'un SIEM. Principes fondamentaux tels que les types de journaux, les méthodes de détection et le cycle de vie de la surveillance. Aspects pratiques du déploiement d'un SIEM, notamment l'architecture, la collecte de données, la création de règles et la gestion des alertes.
Pratiques en matière d'opérations de sécurité - Identifier les sources de données et optimiser la collecte des journaux - Centraliser les alertes avec le SIEM - Tester votre SIEM	4	0,5	10	0,5	**15**	7	Programme de formation complet et axé sur la pratique, couvrant les connaissances essentielles et les compétences pratiques en matière de gestion des journaux, de configuration SIEM et de détection des menaces dans divers environnements informatiques.
Total	**26**	**2**	**20**	**2**	**50**	**25**	

Stratégie d'évaluation	**Pourcentage pondéral comparatif**	**Critères d'évaluation**

Test d'auto-évaluation (1)	10 %	10 points - 95 à 100 % de réponses correctes. 9 points - 85 à 94 % de réponses correctes. 8 points - 75 à 84 % de réponses correctes. 7 points - 65 à 74 % de réponses correctes. 6 points - 55 à 64 % de réponses correctes. 5 points - 45 à 54 % de réponses correctes. 4 points – 35 à 44 % de réponses correctes. 3 points – 25 à 34 % de réponses correctes. 2 points - 15 à 24 % de réponses correctes. 1 point – 0 à 14 % de réponses correctes.
Test d'auto-évaluation (2)	10 %	
Test d'auto-évaluation (3)	10 %	
Test d'auto-évaluation (4)	10	
Test d'évaluation des connaissances	60 %	

Matériel d'étude *(Nom, initiale du prénom. (Année, mois, jour). Titre de l'article. Titre du magazine/journal/quotidien, numéro du volume (numéro du numéro), numéros de page de l'article complet, éditeur, URL)*
Lectures obligatoires
Cybellium (2024). *Guide d'étude sur les centres d'opérations de sécurité (SOC) : guide complet pour apprendre les centres d'opérations de sécurité (SOC)* Muniz, J. (2021). *Le centre d'opérations de sécurité moderne*. Pearson Education. ENISA (2017). *Stratégies de réponse aux incidents et de coopération en cas de cybercrise*. **Stratégies de réponse aux incidents et de coopération en cas de cybercrise — ENISA (europa.eu)**
Lectures recommandées
Basta, A., Basta, N., Anwar, W., Essar, M. I. (2024). Centre d'opérations de sécurité open source (SOC) : guide complet pour la création, la gestion et la maintenance d'un SOC moderne. Cybellium (2023). Gestion d'un centre d'opérations de sécurité (SOC).

5. M5 : GOUVERNANCE ET POLITIQUE DE SÉCURITÉ

Titre du module	Code du module
GOUVERNANCE ET POLITIQUE DE SÉCURITÉ	

Enseignant(s)	Établissement ou département où le module est dispensé

Mode de prestation	Langue
En présentiel / En ligne / Hybride	*Anglais, finnois, turc, norvégien, lituanien, roumain, français, polonais, espagnol*

Prérequis
Aucun

Nombre de crédits ECTS attribués	Charge de travail de l'étudiant	Heures de travail en présentiel	Heures de travail individuel
3	75	50	25

Objectif et résultats du module
Le cours « Gouvernance et politique de sécurité » vise à préparer les étudiants à relever les défis de la cybersécurité dans les PME, en intégrant la gouvernance de la sécurité dans la stratégie commerciale et en garantissant le respect des réglementations légales, telles que le RGPD. Le module couvre des aspects tels que l'identification des menaces et des vulnérabilités, la conception de politiques de sécurité robustes et adaptatives, et la gestion efficace des incidents. En outre, il se concentre sur le développement de structures de gouvernance qui attribuent des rôles clairs au sein de l'organisation, en alignant la cybersécurité sur les objectifs stratégiques. Les étudiants acquerront des compétences techniques en matière d'évaluation et d'atténuation des risques cybernétiques, et développeront des compétences d'analyse afin de proposer des améliorations en matière de maturité de la sécurité. Ils apprendront également à communiquer efficacement les besoins en matière de cybersécurité aux dirigeants, à soutenir la prise de décisions éclairées et à garantir la conformité réglementaire et l'éthique dans le domaine de la cybersécurité. Le module « Gouvernance et politique de sécurité » comprend également un examen approfondi de la prévention du phishing, des cyberattaques basées sur l'IA et de la gestion des ransomwares, en analysant comment ces menaces spécifiques nécessitent une approche intégrée de la gouvernance et de la conformité. L'efficacité des politiques de sécurité sera mesurée non seulement par leur capacité à prévenir les incidents, mais aussi par leur adaptabilité aux menaces émergentes et leur conformité avec les réglementations légales en vigueur.

Résultats d'apprentissage du module « »	Méthodes d'enseignement et d'apprentissage	Méthodes d'évaluation
Connaissances : les apprenants acquerront des connaissances avancées sur la manière de mettre en œuvre de nouvelles routines et de nouveaux flux de travail en matière de cybersécurité dans les PME, en intégrant les principes et les tendances actuels en matière de cybersécurité, ainsi que la conformité avec la législation nationale et internationale applicable à leur secteur d'activité. Acquérir des connaissances avancées sur la manière d'intégrer la prévention du phishing, de gérer les menaces liées à l'IA et de répondre aux ransomwares dans les environnements des PME.	**Cours magistraux (lectures dirigées) :** les cours magistraux fourniront une base conceptuelle solide en matière de cybersécurité, de gouvernance, de confidentialité et de conformité, en encourageant la participation active des étudiants. Elles comprennent des cours interactifs qui intègrent régulièrement des sessions de questions-réponses, des sondages et des exercices de résolution de problèmes en direct. À l'aide d'outils tels que Mentimeter et Poll Everywhere, **Participation à des discussions et à des forums :** la participation à des discussions et à des forums permettra aux étudiants de débattre et d'analyser de manière critique les questions de cybersécurité, ce qui favorisera leurs compétences en matière d'argumentation. Cela s'appliquera aux questions liées à l'éthique, aux politiques et à la prise de décision en matière de cybersécurité. **Études de cas :** les études de cas permettront aux étudiants d'analyser des situations de cybersécurité dans des PME, en appliquant leurs connaissances théoriques à la résolution de problèmes réels. Elles porteront sur des sujets tels que la gestion des violations de données, les ransomwares, le phishing, les attaques basées sur l'IA, la mise en œuvre des politiques de sécurité et la gouvernance.	**Tests d'auto-évaluation :** les auto-tests permettent aux étudiants d'évaluer leur compréhension de chaque sous-thème à travers une série de questions, leur fournissant ainsi un retour d'information continu afin d'identifier les domaines à améliorer. Ils n'ont pas d'incidence sur la note finale, mais sont essentiels à l'apprentissage autonome. **Examen final (facultatif) :** l'examen final est facultatif et permet aux étudiants d'obtenir un certificat de réussite en évaluant leur compréhension globale du cours à travers des questions de développement, des analyses de cas et des questions à choix multiples. Il est nécessaire de le réussir pour obtenir le certificat de réussite, tandis que ceux qui ne le passent pas recevront un certificat de participation.
Compétences : Les apprenants seront capables d'utiliser des	**Ateliers pratiques :** Les ateliers pratiques permettront aux étudiants d'appliquer les concepts de	**Évaluations pratiques :** les évaluations pratiques tout

méthodologies avancées pour mener des évaluations des risques, concevoir et mettre en œuvre de nouvelles routines de cybersécurité et préparer des stratégies de réponse, garantissant ainsi une gouvernance et une conformité efficaces au sein des PME. Développer des compétences dans la conception et la mise en œuvre de routines complètes de cybersécurité qui répondent aux menaces avancées et garantissent la conformité de l'organisation à l' .	cybersécurité à travers des exercices tels que l'élaboration de politiques et des simulations d'incidents, avec des commentaires en temps réel de la part du formateur. Ils sont conçus pour renforcer les compétences pratiques et préparer les étudiants à appliquer ce qu'ils ont appris dans des situations réelles. **Travaux pratiques et projets individuels :** les travaux pratiques et les projets individuels permettront aux étudiants d'appliquer les concepts de cybersécurité à travers des tâches telles que la rédaction de politiques et l'analyse des risques, le développement de compétences de travail autonomes et l'application pratique des connaissances théoriques. **Projets collaboratifs :** les projets collaboratifs permettront aux étudiants de travailler en équipe pour développer des solutions de cybersécurité pour les PME, notamment des politiques de sécurité et des modèles de gouvernance. Ils encourageront le travail d'équipe, la gestion de projet et l'application pratique des connaissances acquises, avec les commentaires des enseignants et des pairs.	au long du cours permettront aux étudiants d'appliquer leurs connaissances théoriques à des situations simulées, telles que l'élaboration de politiques de cybersécurité et des simulations d'incidents, dans le but d'évaluer leur capacité à résoudre des problèmes réels dans le contexte des PME. **Projets de groupe :** les projets de groupe permettront aux étudiants d' r à développer un projet complet de cybersécurité, de l'identification des risques à la proposition de modèles de gouvernance et de plans d'intervention en cas d'incident, en évaluant à la fois la qualité du contenu et la capacité à collaborer. Ce projet est essentiel à l'évaluation finale et intègre tout l'apprentissage du cours.
Compétences : Les apprenants seront compétents pour élaborer et mettre en œuvre des politiques stratégiques de cybersécurité, mener des initiatives visant à établir de nouvelles routines et de nouveaux flux de travail sur les lieux de travail des PME, et prendre des décisions éthiques conformes aux objectifs organisationnels et aux exigences de conformité.	**Simulations de scénarios :** Les simulations de scénarios permettront aux étudiants de gérer des incidents de cybersécurité dans des environnements virtuels qui reproduisent des attaques réelles, en prenant des décisions stratégiques sous pression. Cette méthode améliore les compétences en matière de gestion de crise et de réponse aux incidents, et est essentielle pour enseigner l'évaluation des politiques de sécurité et la prise de décision dans des situations critiques.	**Simulations et gestion des incidents :** les étudiants seront évalués sur leur capacité à gérer des incidents de cybersécurité dans des simulations reproduisant des crises réelles dans une PME. L'objectif est de mesurer leur capacité à gérer la pression, à prendre des décisions stratégiques et à exécuter des plans d'intervention en temps

Devenir compétent dans la formulation et l'exécution de politiques de cybersécurité qui préviennent les cybermenaces sophistiquées et garantissent la conformité aux réglementations internationales en matière de cybersécurité.	Les étudiants devront démontrer comment ils appliqueraient les politiques de gouvernance pour prévenir ou répondre à des incidents spécifiques tels que les attaques de phishing, les ransomwares et les attaques basées sur l'IA, en évaluant leur compréhension du cadre réglementaire pertinent.	réel, en évaluant leur application pratique dans des situations dynamiques.

Contenu du module : répartition des thèmes	Heures de travail en présentiel					Heures de travail individuelles et tâches	
	Cours	Consultations	Pratique (HEI)	Tests	**Tout travail en**	**Travaux**	**Tâches**
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.	5	0,5	3	0,5	**9**	**4**	Lecture, recherche, préparation d'études de cas
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	4	0,5	3	0,5	**8**	**4**	Analyse des politiques, travail individuel
Lois, éthique et conformité -Cybersécurité Organisations, politiques et normes -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	5	0,5	3	0,5	**9**	**5**	Étude de cas, analyse législative

continue et à une réponse automatisée aux menaces.							
Gouvernance en matière de sécurité -Structure de gouvernance de la cybersécurité -Rôles et responsabilités dans la gestion de la sécurité -Modèles de maturité en matière de cybersécurité -Intégration de la cybersécurité dans la gouvernance d'entreprise - 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.)	4	0,5	3	0,5	**8**	**4**	Analyse de scénarios de gestion des risques
Communication au niveau de la direction et du conseil d'administration -Stratégies de communication en matière de cybersécurité -Rapports sur la sécurité à la direction générale -Prise de décision basée sur les données de sécurité -Gestion de crise et communication en matière de cybersécurité - Maîtrise des 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.	4	0,5	3	0,5	**8**	**4**	Préparation de présentations, communication avec les parties prenantes
Politique managériale -Élaboration de la politique de sécurité -Mise en œuvre et suivi des politiques -Évaluation et amélioration continue des politiques - Adaptation des politiques de sécurité aux changements technologiques et réglementaires - Exploration de la manière dont des politiques efficaces de formation et de sensibilisation peuvent constituer un élément essentiel de la conformité réglementaire et de l'atténuation des risques.	4	0,5	3	0,5	**8**	**4**	Rédaction et révision d'un document stratégique
Total	**26**	**3**	**18**	**3**	**50**	**25**	

Stratégie d'évaluation	**Pourcentage pondéré comparatif**	**Critères d'évaluation**

Auto-évaluation I	10 %	Évaluation des concepts fondamentaux relatifs au contexte organisationnel.
Auto-évaluation II	10	Évaluation des concepts fondamentaux relatifs à la vie privée.
Auto-évaluation III	10	Évaluation des lois, de l'éthique et des politiques de conformité.
Auto-évaluation IV	10	Évaluation des politiques en matière de cybersécurité.
Auto-évaluation V	10	Évaluation de la communication au niveau de la direction.
Auto-évaluation VI	10	Évaluation des politiques managériales et de la création de politiques en matière de sécurité.
Test d'évaluation des connaissances	40	Examen final couvrant des questions intégratives sur tous les thèmes du cours.

10 points - 95 à 100 % de réponses correctes.
9 points - 85 à 94 % de réponses correctes.
8 points - 75 à 84 % de réponses correctes.
7 points - 65 à 74 % de réponses correctes.
6 points - 55 à 64 % de réponses correctes.
5 points - 45 à 54 % de réponses correctes.
4 points – 35 à 44 % de réponses correctes.
3 points – 25 à 34 % de réponses correctes.
2 points - 15 à 24 % de réponses correctes.
1 point – 0 à 14 % de réponses correctes.

Matériel d'étude *(Nom, initiale du prénom. (Année, mois, jour). Titre de l'article. Titre du magazine/journal/quotidien, numéro du volume (numéro du numéro), numéros de page de l'article complet, éditeur, URL)*

Lectures obligatoires

...

« EU Cybersecurity Law: Governing Resilience and Coherence in the Digital Age » (Loi européenne sur la cybersécurité : régir la résilience et la cohérence à l'ère numérique) par Luisa Marin

- Cet ouvrage propose une analyse approfondie des lois et politiques de l'UE en matière de cybersécurité, essentielle pour comprendre comment la gouvernance de la cybersécurité est structurée et mise en œuvre dans le contexte européen.

« Cybersecurity in the European Union: Resilience and Adaptability in Governance Policy » (La cybersécurité dans l'Union européenne : résilience et adaptabilité dans la politique de gouvernance) par George Christou

- Cet ouvrage explore les cadres de gouvernance et les processus décisionnels en matière de cybersécurité au sein de l'UE, aidant les étudiants à comprendre l'interaction dynamique entre les différents niveaux de gouvernance.

« **Hameçonnage et contre-mesures : comprendre le problème croissant du vol d'identité électronique »** par Markus Jakobsson et Steven Myers

- Bien qu'il ne soit pas spécifique à l'UE, cet ouvrage explore en détail les techniques de phishing et les contre-mesures, qui peuvent être contextualisées au sein de l'UE en mettant l'accent sur la conformité au RGPD et les principes de protection des données.

« European Cybersecurity Law and Regulation » (Législation et réglementation européennes en matière de cybersécurité), sous la direction de Nadya Purtova et Bert-Jaap Koops

- Cet ouvrage collectif couvre les mesures juridiques et réglementaires spécifiques à la cybersécurité dans l'Union européenne, y compris les défis en matière de conformité et les cadres tels que la directive NIS et le RGPD.

« Ransomware : Comprendre l'extorsion numérique et la menace qu'elle représente pour votre organisation » par Allan Liska et Timothy Gallo

- Ce texte, complété par des études de cas et des exemples spécifiques à l'UE, aidera les étudiants à comprendre les implications des attaques par ransomware dans le cadre de la réglementation européenne.

Lectures recommandées

« Le règlement général sur la protection des données (RGPD) de l'UE : un commentaire » par Lukas Feiler et Nikolaus Forgó

- Ce commentaire fournit des informations détaillées sur le RGPD, essentielles pour comprendre le paysage réglementaire de l'UE et son impact sur les pratiques en matière de cybersécurité.

« Protection des données et cybersécurité en Europe : cadres juridiques et considérations pratiques » par Paul Lambert

- Cet ouvrage offre des informations pratiques sur l'alignement des stratégies de protection des données et de cybersécurité dans l'UE, y compris la conformité aux réglementations et les meilleures pratiques en matière de mesures de sécurité.

« Sécurité des réseaux et de l'information : perspectives européennes et internationales » édité par Jeanne Pia Mifsud Bonnici et Joe Cannataci

- Cet ouvrage examine le paysage de la sécurité des réseaux et de l'information d'un point de vue européen et international, offrant ainsi un contexte plus large aux efforts de l'UE en matière de cybersécurité.

« L'intelligence artificielle dans la cybersécurité : pratiques, défis et éthique » par Elena Fersman et Martin Fredriksson

- Une vue d'ensemble complète de l'intégration des technologies d'IA dans la cybersécurité, abordant les défis éthiques, opérationnels et réglementaires, particulièrement pertinents dans le contexte de l'UE.

« Cybersécurité à l'ère numérique : outils, techniques et applications » par Gregory B. White, Eric A. Fisher et James L. Antonakos

- Bien qu'il ne se concentre pas exclusivement sur l'UE, cet ouvrage couvre également un large éventail de thèmes liés à la cybersécurité moderne.

Matériel d'étude *(documents originaux de HackerU et Cybint)*

Lectures obligatoires

- TCP/IP Network Administration: Help for Unix System Administrators 3rd Edition, par Craig Hunt (O'Reilly)

• Essential System Administration Pocket Reference : Commands and File Formats (Pocket Administrator) par Eleen Frisch (O'Reilly) • Computer Networking: The Beginner's guide for Mastering Computer Networking, the Internet and the OSI Model, par Ramon Nastase
Lectures recommandées
• CompTIA A+ Certification All-in-One For Dummies (Informatique/Technologie) 5e édition par Glen E. Clarke, Edward Tetz, Timothy L. Warner • Coding All-in-One For Dummies 1ère édition par Nikhil Abraham • Les bases des technologies de l'information, volume 1 : Introduction aux systèmes d'information, par Eric Frick • IT Architecture For Dummies 1ère édition par Kalani Kirk Hausman, Susan L. Cook • Cybersecurity For Dummies (Informatique/Technologie) 1re édition par Steinberg • Linux pour les nuls, 10e édition, par Richard Blum • Windows 10 pour les nuls, 3e édition (Informatique/Technologie) 3e édition par Rathbone • Networking For Dummies, 12e édition, par Doug Lowe

6. M6 : PLANIFICATION DE LA CYBERSÉCURITÉ

Titre du module	Code du module
PLANIFICATION DE LA CYBERSÉCURITÉ	

Enseignant(s)	Établissement ou département où le module est dispensé

Mode de prestation	Langue
En présentiel, en ligne, mixte, consultations	*Anglais, finnois, turc, norvégien, lituanien, roumain, français, polonais, espagnol*

Prérequis
-

Nombre de crédits ECTS attribués	Charge de travail de l'étudiant	Heures de travail en présentiel	Heures de travail individuel
3	75	50	25

Objectif et résultats du module		
À l'issue de ce cours, les étudiants seront capables de comprendre et d'appliquer les principes fondamentaux de la planification et de la gestion de la cybersécurité. Ils acquerront la capacité de mettre en œuvre des normes et des cadres internationaux, d'élaborer des stratégies de sécurité à long terme, de gérer des mesures opérationnelles et tactiques de cybersécurité et de planifier des architectures réseau sécurisées telles que le cloud et le zero trust. En outre, les étudiants seront en mesure de concevoir des plans d'intervention efficaces en cas d'incident et de mettre en œuvre des stratégies de continuité des activités, garantissant ainsi la résilience organisationnelle et l'efficacité des mesures de cybersécurité face à l'évolution des menaces.		
Résultats d'apprentissage du module	**Méthodes d'enseignement et d'apprentissage**	**Méthodes d'évaluation**
Connaissances : 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.	Cours magistraux, études de cas, discussions de groupe, apprentissage autonome	Tests d'auto-évaluation, tests d'évaluation des connaissances

Compétences : les apprenants acquerront des compétences en matière de planification stratégique et de 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 solides.	Exercices pratiques, ateliers, études de cas	Évaluations basées sur des projets, évaluations pratiques.
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 en matière de cybersécurité	Ateliers, séminaires, exercices de jeux de rôle	Évaluation continue, tests basés sur des scénarios

Contenu du module : répartition des thèmes	**Heures de travail en présentiel**					**Heures de travail individuelles et tâches**	
	Cours magistraux	Consultations	Pratique (HEI)	Tests	**Tout travail en contact**	**Travaux individuels**	**Tâches**
1. 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)	8	0,5	6	0,5	**15**	**8**	Définir les aspects juridiques de la sécurité des données, des personnes et de la société, ainsi que les lois et politiques qui régissent les données dans les PME. Classer les types de cyberattaques pertinentes pour les PME. Identifier les outils utiles pour prévenir les cyberattaques.

2. Planification stratégique -Définition des buts et objectifs en matière de cybersécurité -Analyse SWOT (forces, faiblesses, opportunités, menaces) -Élaboration de stratégies de sécurité à long terme -Définition d'indicateurs clés de performance (KPI) -Révision et mise à jour de la stratégie de sécurité	8	2	6	2	**18**	**8**	Définir des objectifs de cybersécurité pertinents pour les PME à l'aide d'une analyse SWOT, élaborer des stratégies à long terme pour faire face aux risques, allouer les ressources et le budget en conséquence, fixer des indicateurs clés de performance pour mesurer les progrès et mettre régulièrement à jour la stratégie en fonction des nouvelles menaces.
3. Gestion opérationnelle et tactique -Mise en œuvre de contrôles d'accès -Gestion des correctifs et mises à jour logicielles - Surveillance continue du système - Formation des employés à la sécurité	8	1	6	2	**17**	**9**	Mettre en œuvre des mesures de contrôle d'accès pour restreindre les accès non autorisés, assurer la maintenance des systèmes grâce à la gestion des correctifs, mettre en place une surveillance des activités inhabituelles et dispenser aux employés une formation de sensibilisation à la cybersécurité.
Total	**24**	**3,5**	**18**	**4,5**	**50**	**25**	

Stratégie d'évaluation	**Pourcentage de pondération comparative**	**Critères d'évaluation**
Test d'auto-évaluation (1)	10	10 points - 96 à 100 % de réponses correctes. 9 points - 91 à 95 % de réponses correctes. 8 points – 86 à 90 % de réponses correctes. 7 points – 80 à 85 % de réponses correctes. 6 points – 70 à 79 % de réponses correctes. 5 points – 60 à 69 % de réponses correctes. 4 points – 50 à 59 % de réponses correctes. 3 points – 40 à 49 % de réponses correctes. 2 points – 30 à 39 % de réponses correctes. 1 point – 0 à 29 % de réponses correctes.
Test d'auto-évaluation (2)	10	
Test d'auto-évaluation (3)	10	
Test d'évaluation des connaissances	70	

Matériel d'étude *(Nom, initiale du prénom. (Année, mois, jour). Titre de l'article. Titre du magazine/journal/quotidien, numéro du volume (numéro du numéro), numéros de page de l'article complet, éditeur, URL)*
Lectures obligatoires
1. Nair, A., & Greeshma, M. R. (2023). Mastering Information Security Compliance Management: A Comprehensive Handbook on ISO/IEC 27001:2022 Compliance. Packt Publishing Limited. 2. Falco, G. J., & Rosenbach, E. (2021). Confronting Cyber Risk: An Embedded Endurance Strategy for Cybersecurity. Oxford University Press. 3. The NIST Cybersecurity Framework (CSF) 2.0, National Institute of Standards and Technology, 26 février 2024
Lectures recommandées
1. Mehta, S. (2023). *Guide d'examen ISACA Certified in Risk and Information Systems Control (CRISC®)*. Packt Publishing Limited. 2. Gregory, P. H. (2021). *Guide d'examen tout-en-un pour la certification CISM Certified Information Security Manager*. McGraw-Hill. 3. ISACA. (2021). *Manuel de révision CRISC, 7e édition*. ISACA. 4. Parlement européen et Conseil. (14 décembre 2022). *Règlement (UE) 2022/2554 sur la résilience opérationnelle numérique du secteur financier*. 5. Guide sur le règlement général sur la protection des données (RGPD), Bureau du commissaire à l'information

7. M7 : GESTION ET ATTÉNUATION DES RISQUES

Titre du module	Code du module
GESTION ET ATTÉNUATION DES RISQUES	

Enseignant(s)	Établissement ou département où le module est dispensé

Mode de prestation	Langue
En présentiel, en ligne, mixte, consultations	*Anglais, finnois, turc, norvégien, lituanien, roumain, français, polonais, espagnol*

Prérequis			
Aucun			
Nombre de crédits ECTS attribués	**Charge de travail de l'étudiant**	**Heures de travail en présentiel**	**Heures de travail individuel**
3	75	50	25

Objectif et résultats du module
À l'issue de ce cours, les étudiants seront capables de gérer en continu (identifier, analyser, évaluer, estimer, atténuer) les risques liés à la cybersécurité des infrastructures, systèmes et services TIC en planifiant, appliquant, rapportant et communiquant l'analyse, l'évaluation et le traitement des risques.

Résultats d'apprentissage du module	Méthodes d'enseignement et d'apprentissage	Méthodes d'évaluation
Connaissances : les apprenants acquerront des connaissances avancées sur les processus de gestion des risques, notamment l'identification, l'évaluation et le contrôle des risques, ce qui leur permettra d'établir et de décrire des routines efficaces en matière de cybersécurité, adaptées aux besoins spécifiques des PME, conformément aux normes nationales et internationales.	À sélectionner par l'enseignant, à partir de la partie 1.3. [*Méthodes d'enseignement, par exemple cours théoriques, analyse de la littérature, conférenciers invités, enseignement et apprentissage entre pairs, mentorat, etc.]* de D2.3 « *Structure du parcours d'apprentissage des agents du changement en matière de cybersécurité dans les PME* ».	Tests d'auto-évaluation Test d'évaluation des connaissances
Compétences : 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 spécialement adaptées aux lieux de travail des PME.	À sélectionner par le conférencier, à partir de la partie 1.3. [*Méthodes d'enseignement, par exemple tâches pratiques/laboratoires, quiz, jeux, analyse de vidéos techniques, études de cas, activités pratiques, etc.]* de D2.3 « *Structure du parcours d'apprentissage des agents du changement en matière de cybersécurité dans les PME* »	Tests d'auto-évaluation Test d'évaluation des connaissances
Compétences : les apprenants seront compétents pour élaborer et mettre en œuvre des politiques stratégiques de cybersécurité pour les lieux de travail des PME	À sélectionner par l'enseignant, à partir de la partie 1.3. [*Méthodes d'enseignement, par exemple concours, CTF, environnements simulés, 5E, CBL, CL, PBL, etc.]* de D2.3 « *Structure du parcours d'apprentissage des agents du changement en matière de cybersécurité dans les PME* ».	Tests d'auto-évaluation Test d'évaluation des connaissances

Contenu du module : ventilation des thèmes	Heures de travail en présentiel					Heures de travail individuelles et tâches	
	Cours magistraux (HEI)	Consultations	Pratique (HEI)	Tests	Tout le travail en contact	Travail individuel	Tâches
Évaluation des risques Processus général de gestion des risques Cadre général de gestion des risques Principes de gestion des risques Normes de gestion des risques Exemples pratiques	2	0	2	0	**4**	5	Décrivez brièvement les étapes clés du processus de gestion des risques, notamment l'identification, l'évaluation et le contrôle des risques. Définissez les contextes interne et externe de la gestion des risques pour une PME. Précisez la portée de l'évaluation des risques et identifiez les principaux facteurs de risque. Élaborez des critères de risque spécifiques à la PME choisie.
Identification des risques Leadership et engagement dans la gestion des risques Définition de la portée des activités de gestion des risques Contexte externe et interne de la gestion 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	4	0	4	0	**8**	5	Identifier les sources de risque tangibles et intangibles pour les PME. Classer les risques en fonction des causes, des événements, des menaces et des opportunités. Analyser les vulnérabilités et les capacités internes de la PME, et évaluer comment les changements dans les contextes externes et internes pourraient affecter l'entreprise. Identifier les risques émergents potentiels pour la PME et proposer des indicateurs pour les surveiller. Examiner

Limites des connaissances et fiabilité des informations Biais, hypothèses et croyances de l' des personnes impliquées Exemples pratiques et études de cas							comment la nature et la valeur des actifs et des ressources influencent cette analyse.
Menaces internes Définition et types de menaces internes Coûts des menaces internes Mise en place d'un programme d'atténuation des menaces internes Détecter et identifier les menaces internes Évaluation des menaces internes Gestion des menaces internes Exemples pratiques et études de cas	6	0	6	0	**12**	5	Définir et classer les différents types de menaces internes pertinentes pour les PME. Discuter des coûts potentiels que ces menaces pourraient imposer à l'entreprise. Élaborer un programme de base visant à atténuer les menaces internes pour une PME. Mettre en évidence les éléments clés tels que les stratégies de détection, d'identification et de gestion. Proposer une méthode d'évaluation des menaces internes et décrire les mesures à prendre pour gérer efficacement ces menaces dans le contexte d'une PME.
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 Complexité et connectivité Facteurs liés au temps et volatilité Évaluation de l'efficacité des contrôles existants	6	0	6	0	**12**	5	Comparez et opposez un modèle d'évaluation des risques quantitatif et un modèle qualitatif. Évaluez la probabilité d'un événement à risque ainsi que la nature et l'ampleur de ses conséquences pour une PME. Tenez compte de l'influence de la complexité, des facteurs liés au temps et de la volatilité sur cette évaluation. Évaluez l'efficacité des contrôles actuels dans

Niveaux de sensibilité et de confiance Exemples pratiques et études de cas							la gestion des risques identifiés. Incluez une analyse des niveaux de sensibilité et de confiance dans les mesures de contrôle.
Contrôle des risques Formulation et sélection des options de traitement des risques Planification et mise en œuvre du traitement de l' des risques Évaluation de l'efficacité de ce traitement Décider si le risque résiduel est acceptable Suivi et révision Enregistrement et rapports Exemples pratiques et études de cas	6	0	6	0	**12**	5	Identifiez et sélectionnez les options appropriées de traitement des risques pour les PME. Justifiez votre sélection en vous basant sur l' ez la nature des risques impliqués. Élaborez un bref plan de traitement des risques, décrivant comment les options de traitement sélectionnées seront mises en œuvre dans un environnement de PME. Proposer une méthode pour évaluer l'efficacité du traitement des risques et déterminer si le risque résiduel est acceptable.
Total	**24**	**2**	**24**	**0**	**50**	**25**	

Stratégie d'évaluation	**Pourcentage pondéral comparatif**	**Critères d'évaluation**
Test d'auto-évaluation (1)	5	10 points - 95 à 100 % de réponses correctes. 9 points – 85 à 94 % de réponses correctes. 8 points - 75 à 84 % de réponses correctes. 7 points - 65 à 74 % de réponses correctes. 6 points - 55 à 64 % de réponses correctes. 5 points - 45 à 54 % de réponses correctes. 4 points – 35 à 44 % de réponses correctes. 3 points – 25 à 34 % de réponses correctes. 2 points - 15 à 24 % de réponses correctes. 1 point – 0 à 14 % de réponses correctes.
Test d'auto-évaluation (2)	5	
Test d'auto-évaluation (3)	5	
Test d'auto-évaluation (4)	5	
Test d'auto-évaluation (5)	5	
Test d'évaluation des connaissances	75	

	Matériel d'étude *(Nom, initiale du prénom. (Année, mois, jour). Titre de l'article. Titre du magazine/journal/quotidien, numéro du volume (numéro du numéro), numéros de page de l'article complet, éditeur, URL)*
	Lectures obligatoires
1.	Adarsh Nair et Greeshma M. R. (2023) Mastering Information Security Compliance Management : A Comprehensive Handbook on ISO/IEC 27001:2022 Compliance. Packt Publishing, Limited **https://ebookcentral.proquest.com/lib/viluniv-ebooks/detail.action?docID=30652023&**query=risk%20management
2.	Gregory J. Falco, Eric Rosenbach (2021) Confronting Cyber Risk: An Embedded Endurance Strategy for Cybersecurity. Oxford University Press, eBook
3.	Kristina Narvaez, Betty Simkins, John Fraser (2014) Mise en œuvre de la gestion des risques d'entreprise : études de cas et meilleures pratiques. John Wiley & Sons
-	ENISA (2022) Normes de gestion des risques
4.	Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures visant à assurer un niveau élevé commun de cybersécurité dans l'Union, modifiant le règlement (UE) n° 910/2014 et la directive (UE) 2018/1972, et abrogeant la directive (UE) 2016/1148 (directive NIS 2)
5.	ISO 31000 Gestion des risques — Lignes directrices
	Lectures recommandées
-	Shobhit Mehta (2023) Guide d'examen ISACA Certified in Risk and Information Systems Control (CRISC®). Packt Publishing, Limited **https://ebookcentral.proquest.com/lib/viluniv-ebooks/detail.action?docID=30806680&query=risk%20management**
-	Peter H. Gregory (2021) Guide d'examen tout-en-un pour la certification CISM Certified Information Security Manager. McGraw-Hill
-	ISACA (2021) Manuel de révision CRISC, 7e édition. ISACA
-	Règlement (UE) 2022/2554 du Parlement européen et du Conseil du 14 décembre 2022 sur la résilience opérationnelle numérique du secteur financier et modifiant les règlements (CE) n° 1060/2009, (UE) n° 648/2012, (UE) n° 600/2014, (UE) n° 909/2014 et (UE) 2016/1011

8. M8 : CONTINUITÉ DES ACTIVITÉS, REPRISE APRÈS SINISTRE, GESTION DES INCIDENTS ET SÉCURITÉ DU PERSONNEL

Titre du module	Code du module
CONTINUITÉ DES ACTIVITÉS, REPRISE APRÈS SINISTRE, GESTION DES INCIDENTS ET SÉCURITÉ DU PERSONNEL	

Enseignant(s)	Établissement ou département où le module est dispensé

Mode de prestation	Langue
En présentiel, en ligne, mixte, consultations	*Anglais, finnois, turc, norvégien, lituanien, roumain, français, polonais, espagnol*

Prérequis
Aucun

Nombre de crédits ECTS attribués	Charge de travail de l'étudiant	Heures de travail en présentiel	Heures de travail individuel
3	75	50	25

Objectif et résultats du module		
À l'issue de ce cours, les étudiants seront capables de formuler et d'administrer des plans complets de continuité des activités et de reprise après sinistre (BC/DR), d'élaborer un programme fonctionnel de gestion des incidents et d'établir une politique de sécurité du personnel solide et efficace. Les étudiants apprendront comment protéger les actifs, éviter les pertes excessives, prévenir les temps d'arrêt, éviter ou limiter les situations de crise et les environnements de gestion de crise. À l'issue de ce cours, les étudiants seront capables de rédiger et de contrôler la mise en œuvre durable d'un manuel complet sur la cybersécurité destiné aux PME, en utilisant des principes et des technologies avancés en matière de cybersécurité, intégrés conformément à toutes les lois nationales et internationales. Les étudiants assureront également le suivi de l'application de ces mesures.		
Résultats d'apprentissage du module	**Méthodes d'enseignement et d'apprentissage**	**Méthodes d'évaluation**

Connaissances : les apprenants acquerront des connaissances avancées sur la manière de créer et de mettre en œuvre un manuel complet sur la 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.	À sélectionner par l'enseignant, à partir de la partie 1.3. [Méthodes d'enseignement] du D2.3 « Structure du parcours d'apprentissage des agents du changement en matière de cybersécurité pour les PME ».	Tests d'auto-évaluation, test d'évaluation des connaissances
Compétences : les apprenants seront capables de créer et de tenir à jour un manuel sur la cybersécurité au travail dans les PME, en utilisant des méthodologies avancées pour évaluer les risques, concevoir des stratégies efficaces de gestion des risques et de réponse aux incidents, et élaborer des plans complets de continuité des activités adaptés aux besoins de leur organisation.	À sélectionner par le formateur, à partir de la partie 1.3. [Méthodes d'enseignement] du document D2.3 « Structure du parcours d'apprentissage des agents du changement en matière de cybersécurité dans les PME ».	Tests d'auto-évaluation, test d'évaluation des connaissances
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, et garantir l'alignement avec les objectifs organisationnels et les obligations de conformité.	À sélectionner par le formateur, à partir de la partie 1.3. [Méthodes d'enseignement] du document D2.3 « Structure du parcours d'apprentissage des agents du changement en matière de cybersécurité dans les PME ».	Tests d'auto-évaluation, test d'évaluation des connaissances

Contenu du module : ventilation des thèmes	**Heures de travail en présentiel**					**Heures de travail individuel et tâches**	
	Cours magistraux	Consultations	Pratique (HEI)	Tests	**Tout le travail encadré**	**Travail individuel**	**Tâches**

Réponse aux incidents - Définition et importance de la réponse aux incidents dans le domaine de la cybersécurité - Éléments clés d'une réponse efficace aux incidents - Aperçu des menaces courantes en matière de cybersécurité (hameçonnage, menaces internes, etc.) - Élaboration d'un plan de réponse aux incidents (IRP) - Rôles et responsabilités au sein de l'équipe de réponse aux incidents - Simulation de l'incident : mise en œuvre d'un plan fictif.	5	0,5	3	0,5	**9**	**5**	Élaborez un plan d'intervention détaillé pour votre PME, incluant les rôles, les responsabilités et les mesures à prendre en cas d'incident de cybersécurité. Simulez un incident et organisez un exercice pour tester l'efficacité de votre plan.
Reprise après sinistre - Comprendre la reprise après sinistre - Élaboration d'un plan de reprise après sinistre - Rôles et responsabilités dans la reprise après sinistre - Étapes de reprise après sinistre	5	0,5	3	0,5	**9**	**5**	Élaborez un plan de reprise après sinistre qui décrit les procédures de restauration de l'infrastructure informatique et des données après un événement catastrophique. Prévoyez un calendrier de reprise et attribuez des responsabilités aux membres de l'équipe pour chaque phase du processus.
Continuité des activités - Comprendre la continuité des activités - Élaboration d'un plan de continuité des activités (PCA) - Rôles et responsabilités dans la continuité des activités - Analyse d'impact sur l'activité - Tester et améliorer le PCA	5	0,5	3	0,5	**9**	**5**	Élaborer un plan de continuité des activités qui garantit le maintien des fonctions opérationnelles essentielles pendant et après une perturbation. Identifier les services et ressources essentiels et définir des stratégies d'urgence pour les maintenir dans divers scénarios.

Sensibilisation, formation et éducation à la sécurité - Comprendre la sensibilisation à la sécurité - Élaboration d'un programme de formation à la sécurité - Responsabilités des employés en matière de cybersécurité - Mesure de l'efficacité de la sensibilisation à la sécurité -	1	0,5	2	0,5	**4**	**1**	Élaborez un programme de formation à la sensibilisation à la sécurité pour votre PME, en mettant l'accent sur les politiques clés en matière de cybersécurité et les meilleures pratiques. Organisez une session de formation pour les employés et évaluez leur compréhension à l'aide de quiz ou d'activités interactives.
Pratiques d'embauche en matière de sécurité - Définition des exigences relatives aux rôles en matière de sécurité - Réalisation de vérifications approfondies des antécédents - Réalisation d'entretiens pour les composantes liées à la sécurité - Évaluation et développement continus	1	0,5	2	0,5	**4**	**1**	Mettre en place des pratiques d'embauche axées sur la sécurité, notamment des vérifications des antécédents et des questions d'entretien destinées à évaluer la sensibilisation des candidats à la cybersécurité. Créer une liste de contrôle des qualifications et des caractéristiques essentielles en matière de sécurité pour les futurs employés.
Pratiques de licenciement pour raisons de sécurité - Révocation immédiate de l'accès - Récupération des données et des appareils - Entretien de départ pour obtenir des informations sur la sécurité - Notification des équipes concernées - Considérations juridiques et de conformité	1	0,5	2	0,5	**4**	**2**	Rédigez une procédure de licenciement sécurisée qui comprend les étapes suivantes : révocation de l'accès, récupération des actifs de l'entreprise et entretiens de départ. Mettez en place un scénario de licenciement fictif afin d'évaluer l'efficacité de votre procédure.

Sécurité des tiers - Évaluation des risques liés aux tiers - Diligence raisonnable dans la sélection des fournisseurs - Mise en œuvre de contrôles et d'exigences de sécurité - Surveillance et audit continus - Réponse aux incidents et communication	2	0,5	2	0,5	**5**	**2**	Identifiez les risques potentiels associés aux fournisseurs tiers et créez une liste de contrôle pour évaluer leur conformité aux normes de cybersécurité de votre PME. Rédigez un modèle de contrat qui inclut les exigences en matière de sécurité et les sanctions en cas de non-conformité.
Sécurité dans les processus d'examen - Intégrer la sécurité dans les révisions - Réalisation d'audits de sécurité réguliers - Évaluation de la vulnérabilité et tests de pénétration - Examens post-incident	1	0,5	1,5	0,5	**3,5**	**2**	Élaborez un processus pour examiner et mettre à jour régulièrement les politiques et procédures de cybersécurité de votre PME. Planifiez et réalisez un audit simulé pour vous assurer que toutes les mesures de sécurité sont à jour et conformes aux normes applicables.
Problématique particulière relative à la confidentialité des informations personnelles des employés - Limites de la collecte de données - Stockage et contrôle d'accès - Conformité aux réglementations en matière de confidentialité - Partage des données et tiers - Consentement et droits des employés	2	0,5	2	0,5	**5**	**2**	Rédiger une politique de confidentialité pour le traitement des informations personnelles des employés, en veillant au respect des lois sur la protection des données et des meilleures pratiques. Réaliser une évaluation des risques afin d'identifier les vulnérabilités potentielles dans la manière dont les données des employés sont stockées et traitées.
Total	**23**	**2**	**20,5**	**4,5**	**50**	**25**	

Stratégie d'évaluation	**Pourcentage pondéral comparatif**	**Critères d'évaluation**
Test d'auto-évaluation (1)	5	10 points - 95 à 100 % de réponses correctes. 9 points – 85 à 94 % de réponses correctes.

Test d'auto-évaluation (2)	5	8 points - 75 à 84 % de réponses correctes. 7 points - 65 à 74 % de réponses correctes. 6 points - 55 à 64 % de réponses correctes. 5 points - 45 à 54 % de réponses correctes. 4 points – 35 à 44 % de réponses correctes. 3 points – 25 à 34 % de réponses correctes. 2 points – 15 à 24 % de réponses correctes. 1 point – 0 à 14 % de réponses correctes.
Test d'auto-évaluation (3)	5	
Test d'auto-évaluation (4)	5	
Test d'auto-évaluation (5)	5	
Test d'évaluation des connaissances	75	

Matériel d'étude *(Nom, initiale du prénom. (Année, mois, jour). Titre de l'article. Titre du magazine/journal/quotidien, numéro du volume (numéro du numéro), numéros de page de l'article complet, éditeur, URL)*

Lectures obligatoires

- Gregory J. Falco, Eric Rosenbach (2021). *Confronting Cyber Risk: An Embedded Endurance Strategy for Cybersecurity*. Oxford University Press, eBook.
- Michael Wallace, Lawrence Webber (2017). *The Disaster Recovery Handbook: A Step-by-Step Plan to Ensure Business Continuity and Protect Vital Operations, Facilities, and Assets.* AMACOM.
- Institut national des normes et technologies (NIST). *Guide de planification d'urgence pour les systèmes informatiques*. NIST SP 800-34 Rev. 1.
- Cochran, K.A. (2024). Réponse aux incidents, continuité des activités et reprise après sinistre. Dans : Cybersecurity Essentials. Apress, Berkeley, Californie. **https://doi.org/10.1007/979-8-8688-0432-8_14**

Lectures recommandées

- ISACA (2023). *Manuel de révision CISM, 15e édition*. ISACA.
- Peter H. Gregory (2021). *Guide d'examen tout-en-un pour la certification CISM Certified Information Security Manager*. McGraw-Hill.
- IT Governance (2022). *ISO 22301:2019 – Systèmes de gestion de la continuité des activités. Exigences.*
- M. Souppaya, L. Feldman, G. Witte [2024], Guide for Cybersecurity Incident Recovery, Division de la sécurité informatique, Laboratoire des technologies de l'information, Institut national des normes et technologies, Département du commerce des États-Unis
- Ihab Hanna Sawalha [2021]. Points de vue sur la continuité des activités et la reprise après sinistre. International Journal of Emergency Services

ANNEXES

MODÈLE DE PROGRAMME

DESCRIPTION DU MODULE

Titre du module	Code du module
...	

Enseignant(s)	Établissement ou département où le module est dispensé
...	...

Mode de prestation	Langue
En présentiel, en ligne, mixte, consultations	*Anglais, ...*

Prérequis
...

Nombre de crédits ECTS attribués	Charge de travail de l'étudiant	Heures de travail	Heures de travail individuelles
3	...	...	...

Objectif et résultats du module		
...		
Résultats d'apprentissage du module	**Méthodes d'enseignement et d'apprentissage**	**Méthodes d'évaluation**

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

Contenu du module : répartition des thèmes	Heures de travail en présentiel					Heures de travail individuelles et tâches	
	Cours magistraux	Consultations	Pratique (HEI)	Tests	**Tout le travail en contact**	**Travail individuel**	**Tâches**
1							
...							
n							
Total							

Stratégie d'évaluation	Pourcentage pondéré comparatif	Critères d'évaluation
Auto-évaluation I		...
...		...
Auto-test n		...
Test d'évaluation des connaissances		...

Matériel d'étude *(Nom, initiale du prénom. (Année, mois, jour). Titre de l'article. Titre du magazine/journal/quotidien, numéro du volume (numéro du numéro), numéros de page de l'article complet, éditeur, URL)*
Lectures obligatoires
...
Lectures recommandées
...

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