RÉFÉRENTIEL DE DIPLÔME FEDE

FEDEration for European Education
FÉDÉration Européenne des Ecoles

Bachelor européen

Cybersécurité et gestion des réseaux

www.fede.education
version 04/2026

OING dotée du statut participatif auprès du Conseil de l'Europe - OING dotée du statut consultatif auprès de la Francophonie
OING dotée du statut de partenaire officiel de l'UNESCO et du CESNU
Registre de transparence de l'Union européenne - 313869925841-90
FEDE - La Voie Creuse 16 - 1202 - Genève - SUISSE - RC Genève : CHE-109.997.364

FEDEration for European Education
FÉDÉration Européenne des Ecoles

Fédération Européenne Des Écoles

Federation for European Education

La FEDE est une Organisation Internationale Non Gouvernementale (OING), institution supranationale, créée à Barcelone en 1963. Elle est dotée du statut participatif auprès du Conseil de l'Europe, du statut consultatif auprès de l'Organisation internationale de la Francophonie (OIF), de l'UNESCO et du Conseil économique et social des Nations unies (CESNU). La FEDE est également membre de la Fédération européenne des employeurs de l'éducation (EFEE), de l'Association internationale des Universités (AIU) et de l'Association européenne des établissements de l'enseignement supérieur (EURASHE).

Elle fédère un réseau international de près de 500 établissements d'enseignement supérieur et professionnel, dans 40 pays et sur 4 continents, qui partagent un projet commun d'excellence académique, d'innovation pédagogique, de recherche scientifique et d'ouverture au monde. La FEDE propose plus de 170 référentiels accessibles en français et en anglais, et pour certains en plusieurs langues européennes (espagnol, allemand, italien, roumain, etc.), préparant les apprenants du Foundation Degree, Bachelor européen, Mastère européen, MBA européen, au DBA.

La FEDE rassemble un réseau international de plus de 300 000 personnes.

Cybersécurité et gestion des réseaux

SOMMAIRE

PRESENTATION 6
Contexte 6
Objectifs et compétences 7
Perspectives d'emploi 7
Prérequis d'entrée en formation 8
Correspondances avec les certifications professionnelles 8
Règlements des diplômes 8
Candidat en situation de handicap 9
Formation et Intelligence artificielle (IA) 9
Formation aux compétences linguistiques 9
Formation aux compétences citoyennes 10
ARCHITECTURE DU DIPLOME FEDE 12
UC D31.1 14
Fondamentaux en développement informatique et gestion des systèmes 14
A. Formation 14
B. Évaluation 26
C. Coefficient et ECTS 26
UC D31.2 27
Administration et sécurité des systèmes et réseaux 27
A. Formation 27
B. Évaluation 53
C. Coefficient et ECTS 53
UC D32 54
Epreuve Professionnelle de Soutenance 54
A. Objectifs 54
B. Évaluation 54
C. Règles d'utilisation de l'IA générative dans la rédaction du rapport d'activité 58
D. Coefficient et ECTS 58
UC D33 59
Contrôle continu – Projet de conception et déploiement d'une infrastructure réseau sécurisée 59
A. Objectifs 59
B. Évaluation 59
C. Livrables 61
D. Grilles de notation 62
E. Coefficient et ECTS 62
UC B31 64
Langue Vivante Européenne 1 64
A. Objectif 64
B. Formation 64
C. Ressources pédagogiques mises à la disposition des apprenants par la FEDE 65
D. Évaluation 65
E. Grilles d'évaluation 68
F. Coefficient et ECTS 68

Cybersécurité et gestion des réseaux

UC A2 70
Le projet européen : culture et démocratie pour une citoyenneté en action 70
A. Objectifs 70
B. Formation 70
C. Ressources pédagogiques mises à la disposition des apprenants par la FEDE 73
D. Évaluation 73
E. Coefficient et ECTS 73
UC A3 74
Le management interculturel et les ressources humaines 74
A. Objectifs 74
B. Formation 74
C. Ressources pédagogiques mises à la disposition des apprenants par la FEDE 77
D. Évaluation 77
E. Coefficient et ECTS 77

Cybersécurité et gestion des réseaux

LEXIQUE

UC : Unité Capitalisable

UE : Unité d'Enseignement

ECTS : Le terme ECTS signifie *European Credits Transfer System* en anglais, soit système européen de transfert et d'accumulation de crédits

CECRL : Cadre Européen Commun de Référence pour les Langues

LV : Langue Vivante

PRESENTATION

Contexte

La cybersécurité est devenue une priorité absolue pour les organisations, quels que soient leur taille et secteur d'activité. Les pertes économiques mondiales dues à la cybercriminalité pourraient atteindre 10 500 milliards de dollars par an d'ici 2025[1]. En outre, selon le Fonds monétaire international (FMI), le nombre de cyberattaques a plus que doublé depuis la pandémie de COVID-19. Les pertes directes enregistrées par des sociétés victimes de ces attaques ont également augmenté, certaines entreprises internationales ayant subi des pertes importantes, mettant en évidence l'accélération des menaces et la nécessité de renforcer les dispositifs de protection[2]. Cette réalité impose l'urgence de former des experts compétents, capables de concevoir, d'implémenter et de gérer des systèmes de sécurité fiables.

Le Bachelor européen en cybersécurité et gestion des réseaux vise à répondre à cette demande croissante en offrant une formation adaptée aux exigences du marché et ancrée dans la réalité des menaces actuelles. Le domaine de la sécurité des systèmes et réseaux connaît un essor considérable, avec un taux de croissance annuel composé (CAGR) de 9,7 % prévu jusqu'en 2032. Cette tendance renforce l'importance d'une formation spécialisée pour préparer les nouvelles générations à affronter les défis contemporains et futurs.
En effet, les menaces évoluent constamment, et certaines tendances émergentes modifient la manière dont les organisations abordent la cybersécurité. Deux domaines se démarquent particulièrement :
- La cybersécurité appliquée aux objets connectés (IoT) : avec la multiplication des appareils connectés dans les secteurs de l'industrie, de la santé et des villes intelligentes, leur protection devient impérative face aux attaques ciblant les infrastructures IoT.
- L'intelligence artificielle dans la détection des menaces : l'IA joue un rôle clé dans l'anticipation et la réponse aux cyberattaques, notamment grâce à l'automatisation des SOC (Security Operations Centers) et à l'analyse avancée des anomalies comportementales.

Le programme met également l'accent sur les normes de conformité, telles que le RGPD et ISO 27001, qui imposent des règles strictes en matière de protection des données. Aujourd'hui, les entreprises investissent massivement dans des solutions de cybersécurité pour protéger leurs infrastructures critiques. Si les secteurs de la finance et de la santé restent les cibles majeures, d'autres industries, comme l'énergie et les transports, sont désormais en première ligne. La sécurisation des réseaux électriques, des installations industrielles et des systèmes de transport connectés devient un enjeu stratégique.
Le Bachelor européen en cybersécurité et gestion des réseaux prépare les étudiants à répondre efficacement aux cybermenaces en combinant expertise technique et approche stratégique. Grâce à un apprentissage professionnalisant et axé sur la pratique, ce programme forme des spécialistes capables de concevoir, sécuriser et superviser des infrastructures numériques sûres, résilientes et conformes aux standards internationaux. Il ouvre ainsi l'accès à des postes clés en cybersécurité, avec des perspectives d'évolution de carrière vers des rôles stratégiques.

[1] Source : Cybersecurity Ventures
[2] Source : IMF

Cybersécurité et gestion des réseaux

Objectifs et compétences

- Effectuer une évaluation des risques et recommander des correctifs en utilisant des outils et méthodologies d'audit (OWASP, CVSS, ISO 27005)
- Configurer et déployer des solutions de sécurité (pare-feux, VPN, IAM), en appliquant les bonnes pratiques opérationnelles et les standards du secteur (ISO 27001, NIST)
- Administrer et sécuriser les solutions IAM (Active Directory, AWS IAM, Azure AD), en adoptant des politiques de gestion des accès conformes aux standards de cybersécurité
- Piloter une stratégie de réponse aux incidents, en exploitant les méthodologies reconnues (NIST, ISO/IEC 27035) afin de limiter les impacts des cyberattaques
- Mettre en œuvre des mesures de protection dans un environnement Cloud (chiffrement, IAM, monitoring), en assurant leur conformité aux standards (ISO 27017, SOC 2).
- Mettre en œuvre une veille proactive en cybersécurité, en utilisant des outils spécialisés et des bases de données de vulnérabilités, afin d'anticiper les nouvelles menaces et adapter les stratégies de défense
- Définir et structurer une architecture réseau, en intégrant les mécanismes de segmentation, de chiffrement et de contrôle des accès pour garantir une protection optimale
- Configurer et exploiter un système SIEM pour surveiller les incidents et appliquer des mesures de remédiation en réponse aux cybermenaces identifiées
- Réaliser des tests d'intrusion, en utilisant des méthodologies comme l'OWASP et des outils tels que Metasploit, Nmap et Burp Suite afin d'évaluer la robustesse des infrastructures
- Concevoir et adapter les politiques de cybersécurité en tenant compte des exigences réglementaires (RGPD, ISO 27001, NIS2) et des besoins stratégiques de l'entreprise, afin d'assurer la conformité et une protection efficace face aux évolutions technologiques et aux menaces émergentes
- Former et sensibiliser les collaborateurs aux enjeux de cybersécurité pour instaurer une culture de sécurité proactive

Perspectives d'emploi

Détenir un Bachelor européen de la FEDE, c'est bénéficier de nouvelles opportunités et d'un réseau professionnel international. Le **Bachelor cybersécurité et gestion des réseaux** prépare les futurs professionnels des écoles FEDE aux fonctions de :

Liste des métiers accessibles après l'obtention du Bachelor (0-2 ans d'expérience)

✓ Analyste SOC (Security Operations Center) : surveillance et détection des menaces

✓ Technicien en sécurité réseau : configuration et sécurisation des infrastructures

✓ Administrateur systèmes et réseaux : gestion et sécurisation des systèmes Linux & Windows

✓ Chargé de veille technologique en cybersécurité : identification des nouvelles menaces

✓ Consultant en sécurité junior : conseils en protection des systèmes d'information

✓ Spécialiste IAM junior : gestion des identités et des accès (Active Directory, SSO, MFA)

✓ Spécialiste en sécurité IoT : sécurisation des objets connectés et protocoles embarqués

✓ Spécialiste en sécurité cloud junior : gestion des environnements AWS, Azure, Kubernetes

Liste des métiers accessibles avec 2 à 5 ans d'expérience après la diplomation

✓ Auditeur en sécurité informatique : tests d'intrusion, conformité RGPD, ISO 27001

✓ Ingénieur DevSecOps : sécurisation des pipelines CI/CD et automatisation des contrôles de sécurité

✓ Consultant cybersécurité senior : conseil et implémentation de stratégies de cybersécurité

✓ Spécialiste en réponse aux incidents et forensics : gestion des cyberattaques et investigations numériques

Cybersécurité et gestion des réseaux

✓ Chef de projet cybersécurité : coordination et mise en place de solutions de sécurité
✓ Spécialiste en cybersécurité industrielle (SCADA, OT) : protection des infrastructures critiques
✓ Responsable cybersécurité : supervision de la sécurité des SI et gestion des équipes techniques

Prérequis d'entrée en formation

Le candidat doit être titulaire d'un diplôme ayant validé l'acquisition de 120 ECTS ou être titulaire d'une certification professionnelle de niveau 5 du CEC (Cadre Européen des Certifications) dans la spécialité.

Correspondances avec les certifications professionnelles

Ce référentiel vise à préparer les étudiants aux compétences exigées par les métiers de la cybersécurité. Afin de renforcer leur employabilité, les modules d'enseignement abordés ont été alignés avec des certifications professionnelles reconnues.
Le tableau, ci-dessous, présente les correspondances entre les modules du référentiel et les certifications professionnelles qu'un apprenant pourra envisager de valider en complément de sa formation :

Module	Certifications associées	Compétences professionnelles couvertes
Sécurité des systèmes d'exploitation	*CompTIA Security+*	Gestion des vulnérabilités, durcissement des systèmes, gestion des accès
Sécurité des réseaux	*Cisco CCNA Security, CompTIA Security+*	Firewalls, IDS/IPS, segmentation réseau, VPN
Gestion des identités et des accès (IAM)	*Certified Identity and Access Manager (CIAM)*	Gestion des identités (IAM), MFA, Single Sign-On, gestion des permissions
Cryptographie appliquée	*Certified Encryption Specialist (ECES)*	Chiffrement symétrique et asymétrique, PKI, certificats numériques
Sécurité dans le Cloud et Big Data	*AWS Certified Security - Specialty, Certified Cloud Security Professional (CCSP)*	Sécurisation des environnements Cloud (AWS, Azure), IAM Cloud, chiffrement
Gestion des incidents de sécurité et réponse aux cyberattaques	*GIAC Incident Handler (GCIH), CompTIA CySA+*	Analyse forensic, réponse aux incidents, SOC, SIEM
Pentesting et tests d'intrusion	*Certified Ethical Hacker (CEH), Offensive Security Certified Professional (OSCP)*	Tests d'intrusion, exploitation des vulnérabilités, pentesting avancé
Conformité et gestion des risques en cybersécurité	*Certified Information Systems Auditor (CISA), ISO 27001 Lead Implementer*	Conformité RGPD, audits de sécurité, gestion des risques

Règlements des diplômes

- Règlement général des diplômes FEDE
- Règlement du Bachelor européen de la FEDE

Candidat en situation de handicap

Pour garantir l'égalité des chances entre les candidats, les modalités d'évaluation sont, dans la mesure du possible, inclusives. Des aménagements aux conditions de passation des épreuves orales, écrites et pratiques des examens de CDE FEDE FRANCE, rendus nécessaires en raison d'un handicap ou d'un trouble de la santé invalidant, sont prévus.

En outre, si ces aménagements n'étaient pas suffisants, tout candidat peut saisir le référent handicap du certificateur pour aménager, dans le respect du règlement des examens et des spécifications du référentiel, les modalités d'évaluation.

Formation et Intelligence artificielle (IA)

Consciente des enjeux et des transformations profondes induites par l'IA sur les méthodes pédagogiques, les compétences professionnelles et les métiers de demain, la FEDE encourage ses établissements membres à sensibiliser ses formateurs et apprenants à un usage raisonné et réfléchi de l'IA dans leurs pratiques éducatives et professionnelles.

La FEDE préconise que l'intégration de l'IA dans les parcours de formation s'inscrive dans une approche éthique et soit alignée avec les principes des grandes institutions internationales citées ci-dessous. La FEDE recommande notamment de s'appuyer sur les publications et cadres de référence suivants :

- UNESCO, *Référentiel de compétences en IA pour les apprenants*, 2025
- UNESCO, *Référentiel de compétences en IA pour les enseignants*, 2025
- UNESCO, *Orientations pour l'intelligence artificielle générative dans l'éducation et la recherche*, 2024
- Commission européenne, *Lignes directrices éthiques sur l'utilisation de l'intelligence artificielle (IA) et des données dans l'enseignement et l'apprentissage à l'intention des éducateurs*, 2022
- Council of Europe, *Artificial intelligence and education - A critical view through the lens of human rights, democracy and the rule of law*, November 2022

Les établissements membres sont invités à intégrer ces principes dans leur approche pédagogique et à favoriser une réflexion critique et constructive sur l'impact de l'IA à chaque étape du parcours d'apprentissage.

Formation aux compétences linguistiques

Depuis sa création, en 1963, la FEDE promeut une éducation qui associe développement des compétences professionnelles et citoyennes. Dans un monde caractérisé par la diversité des environnements de travail, la mobilité des parcours et l'intensification des échanges, la maîtrise des langues vivantes constitue un levier important d'insertion professionnelle et d'employabilité. Elle contribue également au développement de compétences interculturelles et à la capacité des diplômés à s'adapter à des contextes variés et à collaborer avec des interlocuteurs d'horizons culturels et linguistiques différents, y compris dans leur propre pays.

Conformément aux principes portés par le Conseil de l'Europe en faveur du multilinguisme et du dialogue interculturel, l'enseignement et l'évaluation d'une langue vivante européenne sont obligatoires dans les diplômes FEDE. Ces enseignements s'appuient sur le Cadre européen commun de référence pour les langues (CECR) et visent à développer des compétences de communication mobilisables dans des situations concrètes d'étude et de travail.

La FEDE inscrit par ailleurs ses dispositifs d'évaluation linguistique dans une démarche de qualité et d'amélioration continue en tant que membre associé de l'Association Language Testers in Europe (ALTE).

Formation aux compétences citoyennes

Les modules de Culture et citoyenneté européennes occupent une place centrale dans les diplômes européens FEDE. Ils traduisent la volonté d'associer l'acquisition de compétences professionnelles au développement de compétences citoyennes, afin de préparer les apprenants à exercer leurs responsabilités dans des sociétés démocratiques, interculturelles et confrontées à des défis économiques, sociaux et environnementaux majeurs.

Cette approche s'inscrit dans les travaux menés au niveau européen en matière de compétences citoyennes, auxquels la FEDE contribue notamment dans le cadre de son statut participatif auprès du Conseil de l'Europe, et s'aligne en particulier sur le Cadre de référence des compétences pour une culture de la démocratie. Elle s'inscrit également dans les initiatives internationales liées à l'éducation au développement durable, en lien avec l'UNESCO, auprès de laquelle la FEDE dispose d'un statut consultatif et participe notamment au Green Education Partnership.

Dans ce cadre, certaines unités d'enseignement sont obligatoires selon le niveau du diplôme : les programmes de Foundation Degree et de Bachelor intègrent des modules consacrés à la compréhension du projet européen, des institutions démocratiques et du dialogue interculturel, tandis que les Mastères incluent un enseignement dédié aux enjeux de la transition écologique et à la responsabilité des organisations face aux défis du développement durable.

Ces enseignements contribuent ainsi à former des apprenants capables d'exercer leurs responsabilités professionnelles avec discernement et d'agir comme citoyens dans des sociétés démocratiques, interculturelles et engagées dans la transition écologique.

UNITES CAPITALISABLES ET HORAIRES INDICATIFS

	Liste des unités capitalisables	Contenu	Horaires indicatifs en face à face pédagogique
Épreuves obligatoires	**UE D** UC D31.1	Fondamentaux en développement informatique et gestion des systèmes	215 à 255 h
	UC D31.2	Administration et sécurité des systèmes et réseaux	270 à 365 h
	UC D32	Mission professionnelle	12 semaines
	UC D33	Contrôle continu	80 h
	UE B UC B31**	Langue vivante européenne 1 *Utilisateur indépendant*	60 à 80 h
	UE A UC A2	Le projet européen : culture et démocratie pour une citoyenneté en action	20 à 25 h
	UC A3	Le management interculturel et les ressources humaines en Europe	20 à 25 h
Épreuves facultatives	UC B32**	Langue vivante 2 *Utilisateur indépendant*	
	UC B33**	Langue vivante 3 *Utilisateur indépendant*	

** Le référentiel d'examens est commun pour toutes les langues vivantes européennes.
Les apprenants ont la possibilité de choisir parmi les langues vivantes suivantes :

- Langue vivante 1 : Allemand, Anglais, Espagnol, Français, Italien, Portugais ;
- Langues vivantes 2 et 3 : Allemand, Anglais, Arabe, Chinois, Espagnol, Français, Italien, Portugais.

NB.1 Attention : les langues vivantes choisies par l'apprenant doivent être différentes de celle dans laquelle il passe les épreuves du domaine européen et du domaine professionnel. Exemple : si les épreuves européennes et professionnelles sont passées en français, les langues vivantes choisies ne peuvent pas comprendre le français.
NB.2 Attention : les horaires ci-dessus représentent les heures de face à face pédagogique préconisées (en présentiel ou en distanciel) et doivent être complétées par les heures de travail personnel de l'apprenant.

ARCHITECTURE DU DIPLOME FEDE

Bachelor européen Cybersécurité et gestion des réseaux				Evaluations	
Épreuves	**U.C.**	**ECTS**	**Coeff.**	**Modalités**	**Durée**
D31 Expertise Professionnelle	**D31.1**	10	3	Épreuve professionnelle écrite + étude de cas	3 h
	D31.2	12	4	Épreuve professionnelle écrite + Étude de cas avancée en cybersécurité	4 h
	D32	12	4	Soutenance professionnelle	0h30
	D33	8	2	Contrôle Continu	-
B31 Langue Vivante Européenne 1	**B31.1**	6	2	Ecrit	1 h
	B31.2	6	2	Oral	40min
A2 Le projet européen : culture et démocratie pour une citoyenneté en action	**A2**	3	1	QCM En ligne	40 min
A3 Le management interculturel et les ressources humaines en Europe	**A3**	3	2	QCM En ligne	40 min
Total		**60**	**20**		
Epreuves facultatives — **B32** Langue Vivante 2	**B32**	6		Écrit + Oral	105 Min
Epreuves facultatives — **B33** Langue Vivante 3	**B33**	6		Écrit + Oral	105 Min

Pour les épreuves facultatives, seuls les points au-dessus de 10/20 sont comptabilisés et comptent double.

UE D | Expertise Professionnelle

UC D31.1

Fondamentaux en développement informatique et gestion des systèmes

A. Formation

Le volume horaire recommandé de formation en face à face pédagogique est de 215 à 255 heures.

L'UC D31.1 est composée des 4 modules suivants :

1. Programmation en Python (55 à 60 h)
2. Les bases de données SQL (50 à 55 h)
3. Mathématiques appliquées et optimisation algorithmique (60 à 80 h)
4. Initiation à la conduite de projets informatiques (50 à 60 h)

Contenu	Capacités attendues
Programmation en Python (55 à 60 h)	
Objectifs pédagogiques globaux : - **Assimiler les concepts fondamentaux de la programmation en Python, les structures de contrôle, les fonctions, et les types de données** - **Implémenter des algorithmes de tri, de recherche, et de gestion de données en Python, tout en évaluant leur performance à l'aide de la complexité algorithmique** - **Concevoir des programmes modulaires en Python, en utilisant des fonctions et la POO, et en respectant les principes de réutilisation du code et de documentation** - **Manipuler les structures de données et gérer la lecture/écriture dans des fichiers, en anticipant les erreurs via la gestion des exceptions** - **Développer des solutions logicielles performantes, en utilisant des bibliothèques standards et externes**	
1. Introduction à la programmation et au langage Python • Présentation des principes de base de la programmation ▪ Les variables : *int, float, str, bool.* ▪ Les expressions mathématiques (+, -, *, /, %) pour les opérations ▪ Les instructions séquentielles • La structure d'un programme Python ▪ L'indentation ▪ Les opérateurs de comparaison (==, !=, >, <, >=, <=) dans des conditions ▪ Les fonctions intégrées (ex : *print(), input(), len(), type()* etc.) • Les types de données en Python ▪ Les nombres entiers (*int*) et flottants (*float*) ▪ Les chaines de caractères et les opérateurs + et * ▪ Les booléens (*true, false*) dans des conditions **2. Contrôle de flux et structures conditionnelles** • Les structures conditionnelles : *if, else, elif*	*Déclarer des variables, en utilisant différents types de données, afin de représenter et traiter des informations dans un programme Python* *Réaliser des calculs et des comparaisons, en utilisant des expressions mathématiques et des opérateurs de comparaison, pour manipuler et évaluer des données numériques* *Organiser et structurer un programme, en appliquant les principes d'indentation et d'instructions séquentielles, afin d'assurer la lisibilité et l'exécution correcte du code* *Exploiter les fonctions intégrées et les types de données pour interagir avec l'utilisateur et manipuler efficacement les données* *Contrôler le flux d'exécution, en utilisant des structures conditionnelles et des booléens, pour prendre des décisions et définir le déroulement des opérations dans un programme Python*

▪ Les blocs conditionnels pour exécuter du code en fonction de conditions ▪ L'utilisation des structures *if, else, et elif* pour gérer des alternatives multiples • Les boucles : *for* et *while* ▪ Les boucles *for* pour parcourir des collections de données ▪ Les boucles *while* pour la répétition d'une tâche tant qu'une condition est vraie ▪ La différence entre boucle *for* et *while*, et leurs spécificités • La gestion des interruptions de boucles : *break* et *continue* ▪ La fonction *break* pour sortir d'une boucle. ▪ La fonction *continue* pour ignorer des itérations sans arrêter la boucle	*Évaluer des conditions multiples, via les structures conditionnelles, afin de gérer différentes alternatives dans un programme Python* *Parcourir des collections de données, en employant des boucles for, pour itérer de manière structurée sur des séquences de données* *Répéter des actions sous condition, en utilisant des boucles while, pour exécuter une tâche tant qu'une condition reste vraie* *Différencier les types de boucles, en identifiant les spécificités et l'utilisation appropriée des boucles for et while, dans différents contextes* *Gérer les interruptions de boucles, en se servant des fonctions break et continue, pour contrôler l'exécution des itérations de manière optimale*
3. Fonctions et modularité • Définition et utilisation des fonctions : création, paramètres et retour de valeurs ▪ Le paramétrage d'une fonction et le retournement d'une valeur calculée. ▪ La différence entre une fonction avec et sans valeur de retour • La portée des variables et la modularité ▪ Les notions de portée locale et globale : définition et usage • Les fonctions anonymes et les fonctions intégrées de haut niveau ▪ Les expressions lambda ▪ Les fonctions intégrées comme *map()*, *filter()*, et *reduce(),* pour la manipulation des collections de données • Les bonnes pratiques en programmation modulaire : réutilisation du code, clarté, documentation ▪ Les commentaires pour documenter chaque fonction ▪ Les fonctions réutilisables pour les tâches courantes • Les bibliothèques de fonctions spécifiques	*Concevoir des fonctions, en définissant des paramètres et en retournant des valeurs, afin de structurer et réutiliser le code de manière efficace* *Appliquer la portée des variables, en distinguant la portée locale et globale, afin de gérer l'accès aux données dans différentes parties du programme* *Utiliser des fonctions anonymes, en exploitant les expressions lambda, pour simplifier la manipulation de données dans des situations spécifiques* *Manipuler des collections de données, en utilisant des fonctions intégrées, pour effectuer des transformations et des filtrages* *Adopter les bonnes pratiques de programmation modulaire, en documentant les fonctions et en réutilisant le code, pour assurer la clarté et la maintenabilité du programme*
4. Les structures de données avancées • Les listes et tuples : les opérations de base, les itérations et les méthodes intégrées ▪ La création de listes et de tuples ▪ Les méthodes intégrées de listes (ex : *append()*, *remove()*, *sort()* etc.)	*Créer et manipuler des listes et des tuples, par des opérations de base et des méthodes intégrées, afin de gérer efficacement des séquences de données*

▪ L'itération de listes et tuples avec des boucles pour manipuler les données • Les dictionnaires et les ensembles ▪ La création de dictionnaires pour le stockage des paires clé-valeur ▪ Les ensembles (*set()*) pour créer des collections d'éléments uniques ▪ La recherche dans un dictionnaire ou un ensemble • Les notions avancées de gestion de données : empiler, trier et fusionner des collections ▪ Les piles (stack) pour gérer des tâches en attente ▪ Les fonctions personnalisées pour trier des objets complexes • La gestion de bases de données simples et le tri de données	*Itérer sur des structures de données, en utilisant des boucles pour parcourir et manipuler des listes, tuples, dictionnaires, et ensembles de manière structurée* *Mettre en œuvre des dictionnaires et des ensembles, par la création de paires clé-valeur ou de collections d'éléments uniques, afin de faciliter la recherche et la manipulation des données* *Gérer des piles et trier des collections, par l'utilisation de fonctions personnalisées, pour organiser les données et assurer un traitement optimisé* *Administrer des bases de données simples, via des requêtes de base, afin d'organiser l'information de manière efficace et pertinente*
5. La manipulation des fichiers et la gestion des exceptions • Lecture et écriture dans des fichiers (texte et binaire) ▪ L'ouverture d'un fichier en mode lecture (*r*), écriture (*w*), ou ajout (*a*) ▪ Lecture et affichage dans la console ▪ Ecriture de données dans un fichier et formatage • La gestion des fichiers avec Python : ouverture, fermeture, lecture, écriture ▪ Les commandes *open()*, *read()*, et *write()* pour manipuler des fichiers ▪ La commande *close* pour fermer les fichiers et éviter les fuites de mémoire • La gestion des exceptions ▪ Les blocs *try* et *except* pour la gestion des erreurs courantes ▪ Le bloc *finally* pour vérifier que les actions se produisent	*Lire et écrire dans des fichiers en ouvrant des fichiers en mode lecture, écriture ou ajout, afin de manipuler des fichiers texte et binaires* *Afficher et formater des données, en lisant et en écrivant dans des fichiers, afin de présenter les informations de manière structurée* *Gérer des fichiers, en utilisant les commandes appropriées, pour assurer une manipulation efficace et éviter les fuites de mémoire* *Traiter les exceptions, en employant les blocs « try » et « except », pour gérer les erreurs courantes et assurer la solidité du programme* *Assurer l'exécution finale des actions, en utilisant le bloc finally, afin de garantir la réalisation d'opérations essentielles même en cas d'erreur*
6. Introduction à la Programmation Orientée Objet (POO) • Les principes de la POO : classes, objets, méthodes et attributs ▪ Définition d'une classe avec des attributs et des méthodes ▪ La création d'objets à partir de classes et les méthodes appliquées sur des objets • Héritage, polymorphisme, encapsulation ▪ L'héritage : Les classes-enfants et les classes-parents ▪ Le polymorphisme	*Définir des classes et des objets, via des attributs et des méthodes, afin de structurer des programmes orientés objet* *Mettre en œuvre les concepts d'héritage, de polymorphisme et d'encapsulation, en créant des classes parentes et enfants, pour favoriser la réutilisation du code et protéger les données*

▪ L'encapsulation des données • Les constructeurs, destructeurs et instances ▪ Les constructeurs (__init__()) pour l'initialisation des objets ▪ Les destructeurs (__del__()) pour ma gestion des actions à la suppression d'un objet	*Utiliser des constructeurs et des destructeurs en employant des méthodes init() et del(), afin d'initialiser et de gérer la suppression des objets* *Créer des instances d'objets, en instanciant des classes, afin de représenter des entités réelles dans un programme*
7. Les bibliothèques standard et externes • Introduction aux bibliothèques standards de Python (math, os, sys, datetime, etc.) • Les bibliothèques externes via pip (ex : numpy, matplotlib)	*Adopter les bonnes pratiques de la POO en organisant le code pour assurer la lisibilité, la modularité et la maintenabilité des applications* *Exploiter les bibliothèques standards de Python, en explorant des modules intégrés, afin d'étendre les fonctionnalités des programmes* *Installer des bibliothèques externes, en employant pip pour intégrer des modules, afin de réaliser des calculs avancés et des visualisations*
8. Introduction aux algorithmes • Les concepts et notions de base des algorithmes ▪ Algorithmes de tri classiques : bubble sort, quicksort, insertion sort ▪ Introduction au tri par fusion (merge sort) : « diviser pour mieux régner » ▪ Comparaison des spécificités de chaque algorithme de tri (vitesse, espace mémoire etc.) ▪ Les avantages et inconvénients de chaque méthode de tri, en fonction de la taille des données et de leur état • La complexité algorithmique ▪ Les notions de complexité temporelle et spatiale ▪ Introduction à la complexité en O(n) ▪ La notation Big-O pour estimer la complexité temporelle (O(n), O(n^2), O(log n), O(n log n)) ▪ L'outil *time* en Python • Les algorithmes avancés en Python et l'évaluation des performances ▪ Introduction à l'algorithme de recherche dichotomique (binary search) ▪ Comparaison des algorithmes de tri rapide, insertion et fusion à l'aide de datasets	*Maîtriser les concepts de base des algorithmes, en explorant les algorithmes de tri classiques, afin de connaître leurs spécificités et leur fonctionnement* *Implémenter des algorithmes de tri avancés, en utilisant des techniques telles que le tri par fusion et le principe de « diviser pour mieux régner », afin de résoudre des problèmes complexes de tri* *Comparer les performances des algorithmes, en analysant leur complexité temporelle et spatiale à l'aide de la notation Big-O et en utilisant time en Python, afin de déterminer l'efficacité des algorithmes dans divers contextes* *Mettre en œuvre des algorithmes de recherche, en utilisant des techniques telles que la recherche dichotomique, afin d'optimiser la recherche de données dans des structures appropriées* *Evaluer les avantages et inconvénients des méthodes de tri, en comparant les performances et en fonction de la taille et de l'état des données, afin de choisir l'algorithme le plus adapté à la situation*

Les bases de données SQL (50 à 55 h)	
Objectifs pédagogiques globaux : - **Concevoir des bases de données relationnelles, en respectant les principes de modélisation, avec l'utilisation adéquate des clés primaires et étrangères** - **Rédiger des requêtes SQL efficaces pour insérer, mettre à jour, supprimer et extraire des données à l'aide des filtres, des jointures et des sous-requêtes complexes** - **Optimiser les performances des bases de données grâce à l'indexation, aux procédures stockées et aux techniques de partitionnement** - **Assurer l'intégrité des données et leur cohérence à travers l'utilisation de la normalisation, des transactions et des contraintes** - **Gérer les utilisateurs, les autorisations et la sécurité des bases de données, en protégeant les données sensibles et en auditant les actions des utilisateurs**	
1. Introduction aux bases de données et au modèle relationnel • Définition et rôle d'une base de données • Les différents types de bases de données ▪ Les bases de données relationnelles ▪ Les bases de données non-relationnelles) ▪ Les avantages des bases de données • Le modèle relationnel ▪ Les tables (relations) interconnectées ▪ Les concepts d'entités, d'attributs, et de relations • Les notions de clé primaire, clé étrangère et contraintes d'intégrité ▪ Définition et rôle d'une clé primaire ▪ Définition et rôle d'une clé étrangère dans les relations entre tables ▪ Les contraintes d'intégrité (unicité, non-nullité, etc.)	*Appréhender le concept de base de données, en expliquant son rôle et ses différentes typologies, afin de comprendre leurs spécificités et avantages respectifs* *Comparer les différents types de bases de données, en analysant les avantages et inconvénients des bases de données relationnelles et non-relationnelles, afin de choisir la solution la plus appropriée selon les besoins* *Décrire le modèle relationnel, en expliquant les concepts d'entités, d'attributs et de relations ainsi que la structure des tables, afin de comprendre l'organisation des données* *Expliquer les notions de clé primaire et clé étrangère, en définissant leur rôle dans les relations entre tables et en décrivant les contraintes d'intégrité, afin de garantir la cohérence des données* *Identifier les contraintes d'intégrité en détaillant les notions d'unicité et de non-nullité, afin d'assurer la qualité et la cohérence des données dans le modèle relationnel*
2. Le langage SQL : introduction et opérations de base • Présentation du langage SQL (Structured Query Language) ▪ Définition et utilité du SQL ▪ La syntaxe de base SQL pour créer, insérer, mettre à jour et supprimer des données dans une table • Les requêtes de base SQL ▪ La requête *SELECT* pour extraire des données ▪ La requête *INSERT* pour insérer de nouvelles données dans une table ▪ La mise à jour des données avec *UPDATE* ▪ La suppression des données avec *DELETE*	*Explorer le langage SQL, en définissant son utilité et en analysant sa syntaxe de base, afin de créer, insérer, mettre à jour et supprimer des données dans une table* *Formuler des requêtes SQL de base, en utilisant les commandes adaptées, afin de manipuler les données d'une base de données relationnelle*

• Les filtres et conditions ▪ La requête « *where* » pour filtrer des résultats ▪ Les filtres avancés ○ La recherche de plage « *between* » ○ La correspondance de modèles « *like* » ○ Les valeurs spécifiques « *In* » • L'ordre des résultats ▪ L'organisation des résultats avec la requête « *order by* » ▪ La centralisation des résultats avec « *group by* » (ex : pour la création de statistiques) ▪ Le filtrage des groupes avec la requête « *having* » après un « *group by* »	*Appliquer des filtres et des conditions, en utilisant les clauses « where », « between », « like », et « In », afin de filtrer les résultats des requêtes de manière précise* *Appliquer des filtres et des conditions, en utilisant les clauses « where », « between », « like », et « In », afin de filtrer les résultats des requêtes de manière précise*
3. Les jointures et relations entre tables • La notion de jointure (« *join* ») ▪ L'importance et le rôle des jointures entre les tables • Les différents types de jointures ▪ La jointures interne « *inner join* » ▪ La jointure externe « *left join* », « *right join* » ▪ La jointure complète ▪ Les jointures multiples ▪ Les jointures auto-référentielles • Les sous-requêtes ▪ L'importance des sous-requêtes dans la collecte de résultats complexes ▪ L'utilisation des sous-requêtes dans les clauses *« where » et « from »*	*Examiner la notion de jointure, en expliquant son rôle et son importance, pour relier des tables et permettre une vue intégrée des données* *Mettre en œuvre des jointures internes et externes, à l'aide des fonctions adéquates, afin de relier des tables et obtenir des informations complètes* *Utiliser des jointures multiples et auto-référentielles, en appliquant les techniques appropriées pour relier plusieurs tables ou une même table à elle-même, afin de modéliser des relations complexes entre les données* *Effectuer des sous-requêtes, en les intégrant dans les clauses « where » et « from », afin de collecter des résultats complexes et d'améliorer l'efficacité des requêtes*
4. Normalisation et intégrité des données • Le concept de normalisation ▪ L'importance de la normalisation : la réduction des redondances et le maintien de l'intégrité des données • Les contraintes et la validation des données ▪ Les contraintes *« not null », « unique », « check », « default »* pour la cohérence des données ▪ La validation des données et la réduction des erreurs dans les bases de données • Les transactions et l'atomicité ▪ Le rôle des transactions et l'exécution atomique des opérations ▪ Les commandes « *begin* », « *commit* », et « *rollback* » pour la gestion des	*Assimiler le concept de normalisation, en expliquant son importance, pour réduire les redondances et maintenir l'intégrité des données dans une base de données* *Mettre en œuvre des contraintes de validation des données, en utilisant des contraintes adaptées, afin d'assurer la cohérence et la qualité des données* *Gérer les transactions et l'atomicité, en explorant les commandes « begin », « commit », et « rollback », afin de garantir l'exécution correcte et la récupération des données en cas d'erreur*

transactions et la récupération des données en cas d'erreur	
5. Optimisation des requêtes et indexation • L'indexation et l'optimisation des performances ▪ Le rôle des index dans la vitesse des requêtes ▪ Les index et les colonnes spécifiques pour l'optimisation de la recherche et du tri • Introduction aux procédures stockées : les procédures stockées simples ▪ Les fonctions « *create* », « *procedure* » et « *call* » pour automatiser les tâches récurrentes dans les bases de données • L'analyse des performances des requêtes « *explain* » pour analyser et améliorer les performances des requêtes SQL	*Assimiler le rôle des index, en expliquant leur importance dans la vitesse des requêtes, afin d'améliorer les performances des opérations de recherche et de tri* *Mettre en œuvre l'indexation, en créant des index sur des colonnes spécifiques, pour optimiser la recherche et le tri des données dans les tables* *Créer des procédures stockées simples, à l'aide des commandes idoines, afin d'automatiser des tâches récurrentes dans une base de données* *Analyser et optimiser les performances des requêtes, en utilisant l'instruction « explain », afin de diagnostiquer les requêtes SQL et apporter des améliorations*
6. Triggers et automatisation des bases de données • Introduction, définition et rôle des triggers (déclencheurs) dans l'automatisation de tâches spécifiques • La syntaxe des triggers : « *create trigger* », « *before* », « *after insert* », « *update* », « *delete* »	*Décrire le rôle des triggers dans l'automatisation des bases de données, à l'aide d'exemples concrets, afin d'expliquer leur utilité* *Écrire la syntaxe d'un trigger, en utilisant des commandes spécifiques, afin d'automatiser une tâche à la suite d'une modification des données* *Analyser l'impact d'un trigger sur les performances d'une base de données, en effectuant des tests pratiques, pour mesurer son efficacité et optimiser les performances*
7. La gestion des grandes bases de données et partitionnement • Les techniques de pagination (« *limit* » et « *offset* ») pour collecter des résultats par lots • Introduction au partitionnement des tables ▪ Les types de partitionnement : par plage (« *range* » partitioning), par liste (« *list* » partitioning), par hachage (« *hash* » partitioning) • La gestion des performances avec de grandes bases de données (sharding) ▪ Le concept de sharding ▪ La limitation des bases de données et la notion de scalabilité	*Appliquer les techniques de pagination, via les commandes « limit » et « offset », dans une grande base de données, afin de récupérer efficacement les résultats par lots* *Identifier les différents types de partitionnement, en illustrant leurs utilisations avec des exemples concrets, dans le but d'optimiser la gestion des tables* *Implémenter une solution de partitionnement sur une base de données, en choisissant le type de partitionnement approprié, afin d'améliorer les performances des requêtes* *Décrire le concept de sharding, en détaillant son rôle dans la gestion des grandes bases de données distribuées, pour le maintien de la scalabilité*

8. Les utilisateurs et les permissions • La gestion des utilisateurs ▪ La création et la gestion des utilisateurs dans un système de base de données ▪ La définition des rôles et des permissions spécifiques pour restreindre l'accès aux données sensibles • Les permissions et la sécurité des bases de données ▪ Les niveaux de permission (« *select* », « *insert* », « *update* », « *delete* ») et leurs attributions de manière sécurisée ▪ La protection des données sensibles et la limitation des accès aux seuls utilisateurs autorisés • Audits et gestion des logs ▪ Les audits pour le suivi des actions utilisateurs ▪ La configuration des journaux d'activité pour identifier les accès non autorisés et les erreurs système	*Analyser les performances d'une grande base de données, en comparant l'avant et l'après implémentation du partitionnement et/ou du sharding, afin de mesurer l'impact de ses techniques* *Identifier les limites de scalabilité des bases de données classiques, en expliquant les atouts du sharding et du partitionnement, pour surmonter ces limitations et améliorer les performances à grande échelle* *Créer et gérer des utilisateurs dans un système de base de données, en attribuant les rôles appropriés, afin de garantir une gestion efficace et sécurisée des accès* *Attribuer des permissions de manière sécurisée à différents utilisateurs, en utilisant des commandes SQL spécifiques, afin de restreindre l'accès aux données sensibles* *Examiner les niveaux de permissions et leur rôle dans la gestion sécurisée des bases de données, en montrant des exemples concrets d'attribution de permissions, afin de justifier de l'importance de chaque type de permission* *Mettre en place des politiques de sécurité pour protéger les données sensibles, en limitant l'accès aux seuls utilisateurs autorisés, afin d'assurer la confidentialité des informations* *Auditer les actions des utilisateurs, à l'aide de la configuration des logs, afin de suivre les accès non autorisés et les erreurs système* *Configurer des journaux d'activité, en identifiant et en analysant les erreurs système et les accès non autorisés, afin de renforcer la sécurité des bases de données*
Mathématiques appliquées et optimisation algorithmique (60 à 80 h)	
Objectifs pédagogiques globaux : - **Maîtriser les systèmes de numération et les opérations arithmétiques en base binaire pour les applications informatiques** - **Appliquer la logique mathématique et le calcul des prédicats pour modéliser et résoudre des problèmes informatiques** - **Résoudre des systèmes d'équations linéaires et manipuler des matrices dans des contextes précis liés à l'informatique** - **Assimiler les concepts de dérivée et d'intégrale pour optimiser les algorithmes et analyser les performances des programmes** - **Analyser la complexité algorithmique et optimiser les algorithmes en utilisant des outils mathématiques appropriés**	

Cybersécurité et gestion des réseaux

1. Les systèmes de numération et l'arithmétique informatique • Les systèmes de numération ▪ Les différents systèmes de numération : binaire, octal, hexadécimal, et décimal ▪ La conversion entre les systèmes de numération (binaire vers décimal, hexadécimal vers décimal, etc.) ▪ Les cas d'utilisation des systèmes de numération en informatique (ex : adresses mémoire etc.) • Les opérations arithmétiques en base binaire ▪ Addition, soustraction, multiplication et division en binaire ▪ Complément à deux et représentation des nombres négatifs en binaire • La représentation des nombres flottants ▪ Les normes IEEE pour les nombres à virgule flottante ▪ La précision, les erreurs d'arrondi et la gestion des exceptions (overflow et underflow)	*identifier les différents systèmes de numération, à l'aide d'exemples concrets, afin de comprendre leur rôle en informatique* *Convertir des nombres entre différents systèmes de numération, en utilisant des algorithmes de conversion spécifiques, afin de maîtriser leur manipulation* *Appliquer les systèmes de numération à des cas concrets, en s'appuyant sur des exemples pratiques, afin de comprendre leur utilité en informatique* *Effectuer des opérations arithmétiques en base binaire, en respectant des règles spécifiques, afin de réaliser des calculs en base binaire* *Utiliser le complément à deux, en appliquant des algorithmes spécifiques de conversion et d'opérations, dans le but de manipuler efficacement les données binaires en informatique* *Examiner la représentation des nombres flottants selon les normes IEEE, en analysant les erreurs d'arrondi et les exceptions, afin de comprendre la gestion des nombres à virgule flottante dans les systèmes informatiques*
2. Logique et calcul des prédicats • La logique propositionnelle ▪ Les opérateurs logiques : ET, OU, NON et l'implication ▪ La Table de vérité et l'évaluation de propositions complexes ▪ Les propositions logiques à partir de problèmes réels • Le calcul des prédicats ▪ Introduction aux prédicats et aux quantificateurs (universels, existentiels) ▪ Le calcul des prédicats pour les énoncés et les problèmes complexes ▪ Les règles de déduction et de preuve formelle • L'algèbre booléenne ▪ Introduction aux circuits logiques combinatoires et séquentiels. ▪ L'algèbre de Boole pour la simplification de circuits logiques	*Identifier les opérateurs logiques à partir d'exemples concrets, en utilisant des diagrammes de logique ou des représentations symboliques, afin de formuler et évaluer des propositions logiques* *Construire des tables de vérité, en appliquant les règles des opérateurs logiques, afin d'évaluer des propositions complexes* *Modéliser des propositions logiques tirées de problèmes réels, en les traduisant sous forme d'expressions logiques, afin de formaliser des situations concrètes* *Explorer les prédicats et les quantificateurs, en les appliquant à des énoncés et problèmes complexes, afin de structurer des arguments logiques* *Appliquer les règles de déduction et de preuve formelle dans le calcul des prédicats, en résolvant des exercices de démonstration logique, pour démontrer la validité d'énoncés logiques*

	Simplifier des circuits logiques, en optimisant les expressions booléennes, dans le but de réduire la complexité des circuits combinatoires et séquentiels *Concevoir des circuits logiques simples, en partant des principes de l'algèbre booléenne, afin de lier la logique formelle à la conception des systèmes informatiques*
3. Les matrices et les systèmes d'équations linéaires • Introduction aux matrices ▪ Définition et opérations de base sur les matrices : addition, soustraction, multiplication ▪ La transposée, le déterminant, et la matrice inverse • La résolution des systèmes d'équations linéaires ▪ La résolution d'équations linéaires avec la méthode de substitution, la méthode de Gauss et de Cramer ▪ L'interprétation géométrique des solutions (espaces de solution, plan dans l'espace) • Les applications des matrices en informatique ▪ Utilisation des matrices dans les transformations géométriques (ex : transformations d'images) ▪ Les matrices d'adjacence pour représenter des graphes et pour les applications connectées en réseaux (ex : réseaux informatiques, réseaux sociaux etc.)	*Définir les matrices et effectuer des opérations de base sur des matrices, en appliquant des règles algébriques spécifiques, afin de manipuler des systèmes matriciels* *Calculer la transposée, le déterminant et l'inverse d'une matrice, en utilisant des méthodes algébriques appropriées, dans le but de résoudre des problèmes matriciels* *Résoudre des systèmes d'équations linéaires, en appliquant la méthode de substitution, de Gauss et de Cramer, pour trouver des solutions algébriques* *Interpréter les solutions géométriques des systèmes d'équations linéaires, en représentant graphiquement les espaces de solution, afin de comprendre l'interaction entre les plans et les vecteurs dans l'espace* *Appliquer les matrices aux transformations géométriques, en modifiant des images ou des objets à l'aide de matrices de transformation, pour démontrer leur utilité dans la manipulation d'images* *Utiliser les matrices d'adjacence pour représenter et analyser des graphes, en les construisant à partir de données de réseaux informatiques ou de réseaux sociaux, afin de modéliser des structures connectées*
4. La notion d'intégrale et de calcul différentiel • Introduction au calcul différentiel ▪ Définition et interprétation de la dérivée comme taux de variation ▪ Les règles de dérivation et le calcul des dérivées simples (polynômes, exponentielles, logarithmes) ▪ Les applications des dérivées en optimisation (minimisation, maximisation) • Le calcul intégral ▪ Définition de l'intégrale comme somme d'éléments infinitésimaux ▪ Le calcul des intégrales simples (polynômes, fonctions trigonométriques)	*Examiner la notion de dérivée comme taux de variation, à l'aide d'exemples concrets, afin de comprendre son interprétation en calcul différentiel* *Calculer des dérivées simples, en utilisant les règles de dérivation, afin de résoudre des problèmes mathématiques liés à la variation* *Définir l'intégrale comme somme d'éléments infinitésimaux, en illustrant ce concept par des exemples graphiques, afin de comprendre le principe du calcul intégral*

▪ Les différentes applications de l'intégrale en informatique : les calculs d'aires et l'analyse de courbes • Les applications des dérivées et des intégrales ▪ L'analyse de la complexité des algorithmes ▪ Les méthodes d'optimisation mathématique pour les performances des programmes	*Calculer des intégrales simples, en employant les méthodes d'intégration appropriées, afin de résoudre des problèmes mathématiques* *Utiliser les intégrales pour calculer des aires et analyser des courbes, en appliquant ces concepts à des exemples en informatique, pour illustrer leur utilité dans le traitement des données* *Analyser la complexité des algorithmes, à l'aide du calcul différentiel et intégral, pour optimiser les performances des programmes informatiques*
5. Introduction aux algorithmes et à l'analyse mathématique • Les algorithmes simples et la structure des données ▪ Les algorithmes classiques : tri (tri à bulles, tri rapide), recherche (recherche linéaire, recherche binaire) ▪ Les notions de complexité temporelle et spatiale ▪ Introduction à la notation Big-O pour l'évaluation des performances des algorithmes • L'optimisation des algorithmes ▪ Les techniques d'optimisation des algorithmes pour améliorer leur efficacité (la réduction de la complexité, la parallélisation) ▪ La théorie des graphes et des matrices dans la conception des algorithmes (ex : algorithmes avec le chemin le plus court)	*Décrire les algorithmes classiques de tri et de recherche, en illustrant leur fonctionnement avec des exemples pratiques, afin de comprendre leur logique et leur utilité* *Évaluer la complexité temporelle et spatiale d'un algorithme, en appliquant des méthodes d'analyse, pour déterminer l'efficacité en termes de ressources* *Expliquer la notation Big-O, en s'appuyant sur des exemples concrets d'algorithmes, afin de mesurer les performances en fonction de la taille des données* *Optimiser des algorithmes, en utilisant des techniques adaptées, afin d'améliorer leur efficacité sur des ensembles de données complexes* *Exploiter la théorie des graphes et des matrices pour concevoir des algorithmes, en appliquant des concepts tels que le chemin le plus court, pour résoudre des problèmes d'optimisation dans divers contextes*
Initiation à la conduite de projets informatiques (40 à 50 h)	
Objectifs pédagogiques globaux : - **Identifier les différentes phases d'un projet informatique et la contribution des membres de l'équipe à chaque étape** - **Collaborer efficacement au sein d'une équipe projet, en utilisant des outils de gestion adaptés et en communiquant régulièrement sur ses avancements** - **Utiliser des outils de suivi de tâches, comme les diagrammes de Gantt ou les tableaux Kanban, pour suivre l'avancement de ses propres livrables** - **Organiser son temps pour accomplir ses missions et anticiper les imprévus dans la réalisation des livrables.** - **Participer activement aux réunions de projet, aux revues de sprint, et aux rétrospectives pour contribuer à l'amélioration continue du projet**	

Cybersécurité et gestion des réseaux

1. Introduction à la gestion de projets informatiques • Définition d'un projet informatique : spécificités et caractéristiques (objectifs, délais, ressources, contraintes etc.) • Les différentes phases d'un projet informatique ▪ Les étapes d'un projet informatique : initiation, planification, exécution, suivi, clôture ▪ Les objectifs SMART dans la gestion de projets informatiques ▪ Les contributions des membres de l'équipe à chaque phase	*Définir les caractéristiques précises d'un projet informatique, en analysant des exemples concrets, afin de comprendre la spécificité des projets informatiques* *Déterminer les différentes phases d'un projet informatique, en les illustrant par des études de cas, pour maîtriser le cycle de vie d'un projet* *Formuler des objectifs SMART dans le cadre d'un projet informatique, en utilisant un cas fictif, afin de garantir une planification efficace* *Identifier les contributions individuelles des membres de l'équipe à chaque étape d'un projet, à travers des simulations, afin de favoriser la collaboration interdisciplinaire*
2. La collaboration et l'organisation de l'équipe au sein d'un projet • La planification : le diagramme de Gantt • Les outils d'organisation de travail (ex : Trello ou Jira) pour suivre l'avancement de ses tâches et les partager à l'équipe	*Elaborer un diagramme de Gantt pour planifier les différentes tâches d'un projet, en élaborant des calendriers détaillés, afin de structurer le déroulement du projet* *Utiliser des outils d'organisation de travail et de suivi d'avancement des tâches, en réalisant des simulations de gestion de projet, afin de coordonner efficacement une équipe*
3. Les rôles et la collaboration en équipe • Les différents rôles dans un projet informatique : contributeur, développeur, testeur, UX designer, etc. et leurs méthodes de collaboration • Présentation des méthodes Agile (ex : Scrum) : les sprints, les revues de sprints etc. • La communication avec l'équipe, le chef de projet et les parties prenantes	*Décrire les rôles de chaque membre d'un projet informatique, via des mises en situation professionnelle, afin de comprendre les responsabilités de chacun* *Assimiler les principes des méthodes Agile (ex : Scrum), en participant à des exercices de sprints et de revues de sprints, afin d'optimiser la collaboration en équipe* *Communiquer efficacement avec l'équipe et les parties prenantes, en simulant des réunions de projet, afin de garantir la bonne coordination des activités*
4. Travail en équipe et collaboration interservices en cybersécurité • Travail interservices en cybersécurité ▪ La relation entre les équipes SOC, DevSecOps, DSI, RSSI ▪ La gestion des conflits et priorisation des tâches en cybersécurité • La gestion des parties prenantes et reporting cybersécurité ▪ Les méthodes d'explication d'un risque cyber à une direction non technique ▪ La présentation et la justification des choix techniques devant un comité	*Coordonner les interactions entre les équipes SOC, DevSecOps, DSI et RSSI, en appliquant des méthodes de gestion des conflits et de priorisation des tâches, afin d'optimiser la réponse aux incidents et garantir une collaboration efficace en cybersécurité* *Présenter un risque cyber à une direction non technique, en structurant un discours adapté et en justifiant les choix techniques devant un comité, afin de faciliter la prise de décision et promouvoir une culture de la cybersécurité dans l'entreprise*

5. Le suivi de ses tâches et la gestion des imprévus • Le respect du rétroplanning, des délais de livrables et le maintien des objectifs fixés pour le projet • L'anticipation et la gestion des imprévus et des obstacles dans la réalisation de ses tâches **6. La clôture du projet et les retours d'expériences** • La validation des livrables et la documentation des résultats • Les revues post-projet et les retours d'expériences	*Respecter un rétroplanning et des délais de livrables, en suivant des scénarios de projets, afin de maintenir les objectifs fixés* *Anticiper les imprévus dans la réalisation de ses tâches, en analysant des situations problématiques, afin de proposer des solutions pertinentes face aux obstacles rencontrés* *Valider les livrables d'un projet et documenter les résultats, en complétant un dossier de projet final, afin de garantir la qualité des objectifs atteints* *Réaliser des revues post-projet et collecter des retours d'expériences, afin d'identifier les réussites et les points de vigilance à améliorer pour les projets futurs*

B. Évaluation

Forme de l'épreuve : Épreuve professionnelle écrite (1 h) + étude de cas (2 h)
Durée totale : 3 h
Barème : notation sur 120 points

- Questions théoriques sur les fondamentaux (30 points)
- Mise en situation technique – Étude de cas (90 points)

Matériel autorisé : Calculatrice non programmable et supports fournis en annexe (extrait de documentation technique)

C. Coefficient et ECTS

Ce module vaut coefficient **3** et permet de capitaliser **10 ECTS**.

UC D31.2

Administration et sécurité des systèmes et réseaux

A. Formation

Le volume horaire recommandé de formation en face à face pédagogique est de 270 à 365 heures.

L'UCD31.2 est compose des 10 modules suivants :

1. Introduction à l'administration des systèmes et réseaux (30 à 40 h)
2. Durcissement et sécurité des systèmes d'exploitation (35 à 40 h)
3. Sécurité des réseaux : segmentation, pare-feu et surveillance (30 à 40 h)
4. Sécurité des identités et des accès (IAM) (30 à 40 h)
5. Cryptographie et protection des données (40 à 50 h)
6. Sécurité des applications et services numériques (20 à 30 h)
7. Réponse aux incidents et gestion des crises cyber (20 à 30 h)
8. Sécurisation des environnements cloud et Big Data (30 à 40 h)
9. Normes, conformité et gestion des risques en cybersécurité (25 à 35 h)
10. Veille et prospective en cybersécurité (15 à 20 h)

Contenu	Capacités attendues
Introduction à l'administration des systèmes et réseaux (30 à 40 h)	
Objectifs pédagogiques globaux : - **Administrer des systèmes d'exploitation courants (Linux et Windows) en configurant et en gérant les services, les utilisateurs et les permissions** - **Configurer et gérer un réseau local (LAN) avec des services critiques tels que DNS et DHCP** - **Mettre en place une surveillance efficace des systèmes et des réseaux à l'aide d'outils adaptés** - **Appliquer des techniques de sécurisation de base pour les systèmes d'exploitation et les réseaux**	
1. Administration des systèmes d'exploitation (Linux et Windows) • Introduction aux systèmes d'exploitation ▪ Les rôles et fonctions d'un système d'exploitation ▪ Les principaux systèmes d'exploitation : les systèmes Linux (distributions principales) et Windows ▪ Installation et configuration initiale d'un système d'exploitation ▪ Démarrage, arrêt et gestion des services système (ex : processus, gestion des services etc.) • La gestion des utilisateurs et des groupes ▪ Création, modification et suppression des utilisateurs et des groupes ▪ Les commandes Linux (ex : useradd, groupadd, etc.) et les outils de gestion de comptes sous Windows (Active Directory) ▪ Les permissions et les rôles d'accès (ex : ACL, politiques de sécurité etc.) ▪ La configuration des permissions avancées sous Linux et Windows	*Analyser, en comparant précisément les rôles et fonctions des systèmes d'exploitation Linux et Windows, pour choisir celui qui répond le mieux aux besoins spécifiques d'une infrastructure* *Installer, en suivant méthodiquement les étapes, un système d'exploitation pour répondre aux besoins de configuration initiale et d'optimisation du système* *Configurer en ajustant les paramètres systèmes, les services et processus pour assurer une gestion performante des systèmes d'exploitation* *Gérer les comptes utilisateurs et les groupes, en utilisant les outils adaptés, pour garantir une administration sécurisée et efficace* *Appliquer les permissions d'accès, en respectant les stratégies de sécurité, pour renforcer la sécurité des comptes utilisateurs sur Linux et Windows*

▪ Les stratégies de sécurité pour les comptes utilisateurs (ex : MFA, authentification forte etc.) • La gestion des services système ▪ La surveillance des services système : le démarrage automatique, la gestion des services critiques ▪ Les outils de gestion des services sous Linux (systemctl, service, etc.) et sous Windows (Services.msc) ▪ La surveillance et le redémarrage automatique des services critiques	*Mettre en œuvre des mécanismes comme le MFA, en appliquant rigoureusement des politiques d'authentification forte, pour sécuriser l'accès aux systèmes d'exploitation* *Superviser les services critiques, en exploitant les outils de surveillance, pour maintenir leur disponibilité et anticiper les défaillances*
2. Administration des réseaux • Les concepts de base des réseaux (LAN, VLAN, WAN) ▪ Introduction à l'adressage IP : IP statique, IP dynamique, sous-réseaux (ex : calcul de masque, CIDR etc.) ▪ La configuration des VLANs pour la segmentation du réseau ▪ La configuration des routeurs et des commutateurs pour un réseau local sécurisé ▪ Le routage basique (routeurs Cisco, switches VLANs) • Les services réseau (DNS, DHCP) ▪ La configuration des serveurs DHCP pour l'attribution dynamique d'adresses IP ▪ La mise en place d'un serveur DNS : les concepts de base : zones, transferts de zone et enregistrements ▪ La sécurisation des services réseau (ex : le filtrage des IP, la restrictions d'accès etc.)	*Configurer un réseau local, en ajustant précisément les adresses IP, VLANs et routeurs, afin d'assurer une segmentation et une sécurité optimales* *Segmenter un réseau, en utilisant efficacement les VLANs, pour isoler les différentes sections du réseau et améliorer sa performance* *Superviser le routage basique, en surveillant régulièrement les routeurs et switches, pour maintenir un flux de données stable et sécurisé* *Mettre en place des serveurs DNS et DHCP, en configurant correctement les services réseau, pour garantir une attribution dynamique et une résolution des noms efficace* *Sécuriser les services réseau, en définissant minutieusement des règles de filtrage, pour prévenir les accès non autorisés et renforcer la protection des données*
3. Surveillance et diagnostic des systèmes et réseaux • La surveillance des systèmes et des services ▪ Introduction aux outils de surveillance des systèmes : top, htop, Task Manager etc. ▪ Les suivi des performances des services critiques et l'identification des goulets d'étranglement ▪ Introduction aux journaux système et à leur gestion : Syslog sous Linux, Event Viewer sous Windows • Les outils de surveillance et de diagnostic réseau	*Utiliser les outils de surveillance des systèmes, en analysant régulièrement les performances des services critiques, pour identifier les goulets d'étranglement et prévenir les pannes* *Superviser les journaux système, en exploitant efficacement Syslog sous Linux et Event Viewer sous Windows, afin de détecter les erreurs et comportements anormaux* *Diagnostiquer les problèmes de connectivité, en appliquant minutieusement les outils de diagnostic réseau, pour rétablir la communication réseau*

▪ Introduction à la surveillance des réseaux avec Wireshark et NetFlow ▪ Utilisation de ping, traceroute, netstat, et les autres outils de diagnostic réseau pour identifier les problèmes de connectivité : Wireshark, NetFlow, Nagios etc. ▪ La détection et le diagnostic des anomalies réseau : analyse du trafic, la capture de paquets, les logs réseau etc.	*Mettre en place des solutions de surveillance réseau, en configurant correctement les outils dédiés, pour assurer une visibilité optimale des activités réseau* *Analyser le trafic réseau, en capturant précisément les paquets avec Wireshark, pour identifier les anomalies et potentiels problèmes de sécurité* *Détecter les anomalies réseau, en surveillant attentivement les logs et le trafic, pour anticiper et résoudre les dysfonctionnements*
Durcissement et sécurité des systèmes d'exploitation (35 à 40 h)	
Objectifs pédagogiques globaux : - **Mettre en œuvre des stratégies de sécurisation pour les systèmes d'exploitation Linux et Windows** - **Configurer les pare-feux système et les stratégies de gestion des accès et des permissions** - **Appliquer des techniques de renforcement de la sécurité (hardening) des systèmes d'exploitation** - **Utiliser des outils de détection et de gestion des vulnérabilités pour sécuriser un système**	
1. Sécurisation des systèmes d'exploitation (Linux et Windows) • Introduction à la sécurité des systèmes d'exploitation ▪ Les principales menaces pour les systèmes d'exploitation : malwares, spywares, virus, trojan, ransomware, phishing, rootkits, vulnérabilités systèmes etc. ▪ Les stratégies globales de sécurisation pour les systèmes Linux et Windows (ex : sécurisation des comptes utilisateurs, contrôle d'accès basé sur les permissions, renforcement de la sécurité des services réseaux, hardening du système, sauvegardes, gestion des journaux, gestion des correctifs de sécurité etc.) ▪ Les différences entre la sécurisation sous Linux et Windows (ex : permissions, systèmes de fichiers, politiques de sécurité etc.) • Gestion des permissions et des accès ▪ Les permissions sous Linux (chmod, chown) et Windows (ACL, GPO) ▪ La gestion des comptes utilisateurs et des groupes avec des politiques de sécurité strict ▪ Les stratégies de sécurité renforcées pour les utilisateurs (MFA, restrictions d'accès etc.) ▪ Les stratégies de gestion des accès à distance (SSH, RDP) et la sécurisation des connexions	*Identifier les principales menaces pour les systèmes d'exploitation, en surveillant attentivement les vulnérabilités, pour prévenir les attaques de type malwares, trojans et ransomwares* *Mettre en œuvre des stratégies globales de sécurisation, en appliquant efficacement des méthodes de renforcement de la sécurité, pour protéger les systèmes Linux et Windows contre les intrusions* *Configurer les permissions des utilisateurs et des groupes, en suivant rigoureusement les politiques de sécurité sous Linux et Windows, pour garantir un accès sécurisé aux ressources* *Sécuriser les accès à distance, en configurant précisément les connexions SSH et RDP, afin de limiter les risques d'intrusion externe*

Cybersécurité et gestion des réseaux

• Pare-feux système et sécurité réseau de base ▪ La configuration des pare-feux locaux sous Linux (iptables, UFW) et Windows (Windows Defender Firewall) ▪ Les politiques de filtrage de paquets et de contrôle des connexions ▪ La sécurisation des services exposés (serveur web, FTP, etc.) à l'aide des pare-feux	*Mettre en place des pare-feux locaux, en définissant minutieusement des politiques de filtrage sous Linux et Windows, pour contrôler le trafic réseau et protéger les services exposés* *Renforcer la sécurité des services exposés, en configurant strictement les pare-feux, pour limiter les accès non autorisés et sécuriser les serveurs critiques*
2. Hardening des systèmes d'exploitation • Techniques de durcissement des systèmes d'exploitation : hardening ▪ Hardening de base sous Linux : désactivation des services inutiles, modification des permissions des fichiers sensibles ▪ Renforcement de la sécurité des systèmes Windows : GPO, audit de sécurité, désactivation des services critiques non utilisé ▪ Les outils de hardening ○ Linux : Lynis (Linux), Bastille Linux, AppArmor, SELinux ○ Windows : Security Baseline ▪ Les journaux d'audit et de surveillance pour détecter les comportements anormaux (Auditd sous Linux, Windows Event Logs)	*Appliquer les techniques de durcissement des systèmes d'exploitation, en désactivant précisément les services inutiles, pour réduire la surface d'attaque sous Linux et Windows* *Renforcer la sécurité des fichiers sensibles, en ajustant minutieusement les permissions, pour protéger les données critiques contre les accès non autorisés* *Configurer des politiques de sécurité renforcées sous Windows, en utilisant efficacement les GPO et l'audit de sécurité, pour durcir les systèmes contre les attaques* *Mettre en place des outils de hardening, en installant rigoureusement des solutions adaptées, pour améliorer la protection des systèmes* *Surveiller les journaux d'audit, en suivant régulièrement les événements, afin de détecter rapidement les comportements anormaux et les menaces potentielles*
3. Détection et gestion des vulnérabilités • Détection des vulnérabilités et patch management ▪ Introduction aux outils de détection de vulnérabilités (OpenVAS, Nessus) ▪ Les failles de sécurité des systèmes d'exploitation ▪ Les correctifs de sécurité et les mises à jour régulières pour Linux (apt, yum) et Windows (Windows Update, WSUS) ▪ La gestion proactive des correctifs et des mises à jour automatiques • La surveillance des systèmes et l'analyse des logs ▪ Les journaux système pour détecter les comportements suspects ○ Syslog, journalctl pour Linux ○ Event Viewer pour Windows	*Identifier les vulnérabilités des systèmes, en utilisant efficacement des outils de détection, pour prévenir les failles de sécurité* *Appliquer des correctifs de sécurité, en installant régulièrement les mises à jour sous Linux et Windows, pour réduire les risques d'exploitation des vulnérabilités* *Gérer les correctifs de manière proactive, en configurant précisément les mises à jour automatiques, afin de maintenir la sécurité des systèmes d'exploitation* *Analyser les journaux système, en utilisant Syslog et Event Viewer, pour détecter les comportements suspects* *Mettre en place des outils de surveillance, en configurant efficacement des solutions comme Nagios et Zabbix, pour anticiper les incidents et renforcer la protection des systèmes*

▪ Les outils de surveillance pour une gestion proactive (ex : Nagios, Zabbix etc.) ▪ Les logs de sécurité et la prévention des incidents grâce aux logs	*Prévenir les incidents de sécurité en analysant régulièrement les logs de sécurité pour détecter rapidement les anomalies et réagir avant l'apparition de menaces*
Sécurité des réseaux : segmentation, pare-feux et surveillance (30 à 40 h)	
Objectifs pédagogiques globaux : - **Configurer et sécuriser un réseau local et un réseau étendu, en utilisant des techniques de segmentation et de filtrage** - **Mettre en œuvre des solutions de sécurité réseau, y compris les pare-feux, les VPN, et les systèmes de détection et de prévention d'intrusions** - **Appliquer des protocoles de sécurité pour protéger les communications réseau** - **Surveiller le trafic réseau pour détecter et répondre aux menaces**	
1. Les concepts fondamentaux de la sécurité des réseaux • Introduction à la sécurité des réseaux ▪ Panorama des principales menaces pesant sur les réseaux : les attaques DDoS, man-in-the-middle, spoofing, etc. ▪ Les modèles de sécurité réseau : la défense en profondeur, le principe du moindre privilège ▪ Les normes et les bonnes pratiques en matière de sécurité réseau (ISO 27001, NIST) • Segmentation et isolation des réseaux ▪ La configuration et la gestion des VLANs pour segmenter les réseaux et isoler les différents segments ▪ Les DMZ (zones démilitarisées) pour isoler les services exposés à Internet ▪ Les réseaux privés virtuels (VPN) pour des communications sécurisées • Sécurisation des objets connectés (IoT) ▪ Identification des risques spécifiques liés aux IoT (vulnérabilités matérielles et logicielles) ▪ Présentation des attaques connues (Mirai Botnet, Stuxnet) ▪ Les techniques de sécurisation adaptées aux environnements IoT • Protocoles IoT sécurisés (MQTT, CoAP, Zigbee, BLE) ▪ Les protocoles et leurs faiblesses potentielles ▪ Les bonnes pratiques pour chiffrer et authentifier les flux de données IoT • Les tests d'intrusion IoT et surveillance des flux IoT	*Identifier les principales menaces sur les réseaux, en surveillant attentivement les attaques potentielles, pour anticiper et prévenir les vulnérabilités* *Appliquer les modèles de sécurité réseau, en respectant les principes de défense en profondeur et du moindre privilège, pour renforcer la protection des infrastructures* *Mettre en œuvre des bonnes pratiques de sécurité, en suivant strictement les normes ISO 27001 et NIST, pour garantir une sécurisation conforme des réseaux* *Configurer la segmentation des réseaux, en organisant précisément les VLANs, pour isoler les différents segments et protéger les données sensibles* *Sécuriser les services exposés, en configurant des DMZ, pour protéger les systèmes ouverts à Internet* *Identifier les risques spécifiques aux objets connectés, en analysant leurs vulnérabilités matérielles et logicielles, afin d'anticiper les menaces et renforcer la sécurité des infrastructures IoT* *Mettre en œuvre des protocoles IoT sécurisés, en appliquant des techniques de chiffrement et d'authentification adaptées, afin de garantir la confidentialité et l'intégrité des communications IoT* *Réaliser des tests d'intrusion sur des infrastructures IoT, en exploitant des outils spécialisés, afin d'évaluer la résilience des dispositifs et recommander des correctifs adaptés*

▪ Utilisation de Wireshark et Tshark pour analyser le trafic IoT ▪ Les outils de pentesting pour objets connectés (Shodan, Metasploit, binwalk) ▪ La segmentation et l'isolation des réseaux IoT (VLAN, SDN, Firewalls spécifiques)	*Analyser le trafic des objets connectés, en utilisant Wireshark et Tshark, afin de détecter les anomalies et identifier les potentielles cyberattaques ciblant les environnements IoT*
• Routage et filtrage des paquets ▪ La configuration et la gestion des routeurs et des commutateurs sécurisés (ex : Cisco, Juniper etc.) ▪ Les listes de contrôle d'accès (ACL) pour filtrer les paquets entrants et sortants ▪ Le routage sécurisé : VRF, VSS, et les autres techniques avancées pour améliorer la sécurité du réseau	*Implémenter des réseaux privés virtuels (VPN), en configurant des tunnels sécurisés, pour garantir la confidentialité des communications* *Filtrer les paquets entrants et sortants, en utilisant efficacement des listes de contrôle d'accès, pour prévenir les accès non autorisés* *Gérer le routage sécurisé, en configurant avec précision des routeurs et commutateurs, pour contrôler les flux de données et améliorer la sécurité des réseaux*
2. Les différentes solutions de sécurité réseau • Les pare-feux (firewalls) ▪ Introduction aux divers types de pare-feux : les pare-feux matériels et logiciels ▪ La configuration des pare-feux sous Linux (iptables, firewalld) et sous Windows (Windows Defender Firewall) ▪ Les règles de filtrage des paquets pour limiter les connexions non autorisées	*Configurer des pare-feux, en paramétrant des solutions matérielles et logicielles, pour filtrer efficacement les connexions non autorisées* *Appliquer des règles de filtrage des paquets, en définissant les règles sous Linux et Windows, afin de limiter les accès non sécurisés*
• L'implémentation des systèmes IDS/IPS ▪ Présentation et introduction aux systèmes de détection d'intrusion (IDS) et de prévention d'intrusion (IPS) ▪ Snort et Suricata pour détecter des comportements anormaux ▪ Les journaux IDS/IPS et la réponse aux alertes de sécurité	*Mettre en place des systèmes IDS/IPS, en installant précisément des outils adaptés, pour détecter et prévenir les comportements anormaux sur les réseaux* *Répondre aux alertes de sécurité, en analysant attentivement les journaux IDS/IPS, pour réagir rapidement aux menaces identifiées*
• La sécurisation des communications avec SSL/TLS et IPsec ▪ Les protocoles SSL/TLS pour sécuriser les échanges entre les serveurs et les clients ▪ La configuration de VPN avec IPsec pour garantir la confidentialité et l'intégrité des communications réseau ▪ Les certificats numériques pour sécuriser les connexions SSL/TLS (PKI)	*Sécuriser les communications réseau, en utilisant les protocoles SSL/TLS, pour protéger les échanges entre les serveurs et les clients* *Configurer des VPN, en appliquant rigoureusement les protocoles, pour garantir la confidentialité et l'intégrité des communications* *Utiliser des certificats numériques, en intégrant des solutions PKI, pour sécuriser les connexions SSL/TLS et assurer l'authentification*
3. Surveillance et diagnostic des réseaux • La surveillance et l'analyse du trafic réseau ▪ Les outils Wireshark et NetFlow pour la surveillance du trafic réseau en temps réel	*Exploiter des outils comme Wireshark et NetFlow, en capturant les paquets, pour surveiller le trafic réseau et détecter les anomalies ou tentatives d'intrusion*

Cybersécurité et gestion des réseaux

▪ La capture et l'analyse de paquets pour détecter des anomalies ou des tentatives d'intrusion ▪ Les solutions de monitoring réseau (ex : Nagios, Zabbix etc.) pour surveiller les performances et les failles • La gestion des journaux réseau et la réponse aux incidents ▪ La configuration et la gestion des journaux réseau pour détecter des activités suspectes ▪ Les solutions de surveillance de la sécurité (ex : Splunk ou ELK Stack) pour centraliser et analyser les journaux • Les outils de sécurisation des réseaux ▪ Environnements virtualisés pour la configuration des réseaux (Cisco Packet Tracer, GNS3). ▪ Outils de surveillance et de diagnostic réseau : Wireshark, NetFlow, Nagios, Zabbix. ▪ Systèmes IDS/IPS : Snort, Suricata. ▪ Logiciels de gestion des pare-feux : iptables, firewalld, Windows Defender Firewall	*Mettre en place des solutions de monitoring réseau, en employant des outils comme Nagios et Zabbix, pour surveiller les performances et anticiper les failles* *Gérer les journaux réseau, en configurant des systèmes de surveillance, pour centraliser et analyser les logs et détecter les activités suspectes* *Réagir aux incidents réseau, en analysant les journaux, pour répondre rapidement aux menaces et éviter toute compromission du réseau* *Configurer des environnements virtualisés, en utilisant Cisco Packet Tracer ou GNS3, pour simuler et sécuriser les réseaux* *Surveiller les réseaux, en utilisant des outils de diagnostic et des pare-feux, pour prévenir les intrusions et garantir une protection optimale*
4. Cybersécurité des objets connectés (IoT) • Introduction à l'IoT et enjeux de cybersécurité ▪ Définition de l'IoT et panorama des objets connectés ▪ La différence entre IT (Information Technology) et OT (Operational Technology) ▪ Contexte des attaques sur l'IoT : Mirai Botnet, Stuxnet, BrickerBot ▪ Présentation des risques spécifiques (piratage, accès non sécurisé, faiblesse des protocoles etc.) • Protocoles et architectures IoT sécurisées ▪ Les protocoles IoT : MQTT, CoAP, Zigbee, Bluetooth Low Energy (BLE), LoRaWAN ▪ La sécurisation des flux de données : chiffrement et authentification des communications ▪ Les bonnes pratiques de conception : Zero Trust pour l'IoT • Sécurisation des infrastructures IoT ▪ La sécurisation des firmwares et les mises à jour OTA (Over The Air)	*Analyser les enjeux de la cybersécurité IoT, en identifiant les menaces et vulnérabilités spécifiques, afin de prévenir les risques liés aux objets connectés* *Distinguer les architectures IT et OT, en comparant leurs caractéristiques et contraintes de sécurité, afin de comprendre les défis liés à la protection des infrastructures industrielles et IoT* *Évaluer la sécurité des protocoles IoT, en analysant leur fonctionnement et mécanismes de chiffrement, afin d'identifier leurs faiblesses et appliquer des mesures de protection adaptées* *Implémenter des stratégies de sécurisation IoT, en configurant le chiffrement, l'authentification et les bonnes pratiques de Zero Trust, afin de garantir l'intégrité et la confidentialité des communications IoT* *Configurer la sécurité des firmwares et des mises à jour OTA, en appliquant des principes de durcissement et de contrôle d'intégrité, afin de réduire les risques d'exploitation des vulnérabilités logicielles*

▪ La segmentation des réseaux IoT (isolation des objets connectés via VLAN, SDN) ▪ L'utilisation de TLS/SSL pour les connexions IoT ▪ Les outils de détection d'intrusion dans les systèmes IoT (Snort, Suricata) • Les tests d'intrusion IoT ▪ Capture et analyse de trafic IoT avec Wireshark et Tshark ▪ L'analyse d'un firmware IoT avec binwalk ▪ Pentesting des objets connectés avec Shodan et nmap ▪ L'exploitation de vulnérabilités IoT avec Metasploit	*Sécuriser les infrastructures IoT, en mettant en place des mécanismes de segmentation réseau, de filtrage et de surveillance des flux afin d'isoler et protéger les objets connectés des cyberattaques* *Détecter des menaces sur les objets connectés, en utilisant des outils IDS/IPS, afin de réagir rapidement aux tentatives d'intrusion et limiter les dommages* *Effectuer des tests d'intrusion IoT, en capturant et analysant le trafic réseau avec Wireshark et Tshark, afin d'identifier les vulnérabilités exploitables sur les objets connectés* *Analyser la sécurité des firmwares IoT, en utilisant binwalk pour extraire et examiner les composants logiciels, afin de détecter des failles pouvant être exploitées par un attaquant* *Exploiter des vulnérabilités IoT, en réalisant des audits avec Shodan, nmap et Metasploit, afin d'évaluer la solidité des dispositifs connectés et recommander des mesures correctives*
Sécurité des identités et des accès (IAM) (30 à 40 h)	
Objectifs pédagogiques globaux : - **Implémenter des systèmes de gestion des identités et des accès IAM, pour sécuriser les accès aux systèmes et aux données.** - **Configurer et gérer des systèmes d'authentification centralisés comme Active Directory et OpenLDAP** - **Mettre en œuvre des solutions d'authentification forte pour renforcer la sécurité des accès** - **Gérer et surveiller les permissions et les rôles d'accès au sein d'une organisation**	
1. La gestion des identités et des accès IAM • Identity and Access Management ▪ Les concepts fondamentaux de l'IAM : authentification, autorisation et gestion des identités numériques ▪ L'importance de la gestion des accès pour la sécurité des systèmes ▪ Les principes de sécurité associés à l'IAM ○ Le moindre privilège ○ La séparation des responsabilités ▪ Les normes standards et les bonnes pratiques en matière d'IAM (NIST, ISO 27001) • La gestion centralisée des identités ▪ Introduction à Active Directory (AD) : structure, fonctionnement et gestion des objets (utilisateurs, groupes, unités organisationnelles etc.)	*Maîtriser les concepts fondamentaux de l'IAM, en identifiant les principes d'authentification, d'autorisation et de gestion des identités, pour renforcer la sécurité des systèmes* *Appliquer les principes de moindre privilège et de séparation des responsabilités, en définissant des politiques d'accès, pour limiter les risques d'abus de privilèges* *Mettre en œuvre les bonnes pratiques IAM, en suivant strictement les normes NIST et ISO 27001, pour garantir une gestion sécurisée des identités* *Configurer Active Directory, en gérant efficacement les utilisateurs, le groupes et les unités organisationnelles, pour centraliser la gestion des identités dans un environnement Windows*

▪ Présentation d'OpenLDAP pour la gestion des identités dans un environnement Linux ▪ Comparaison entre AD et OpenLDAP ▪ La création des comptes utilisateurs, des groupes et des politiques d'accès ▪ La sécurisation de l'accès aux services via des solutions IAM centralisées	*Administrer OpenLDAP, en ajustant les paramètres, pour gérer les identités dans un environnement Linux et sécuriser les accès aux services* *Comparer les fonctionnalités d'Active Directory et d'OpenLDAP, en analysant leurs différences, pour choisir la solution IAM la mieux adaptée pour l'entreprise*
2. Authentification et gestion des accès : Multi-Factor Authentication ▪ L'authentification forte : MFA, 2FA (authentification à deux facteurs) ▪ Le système MFA : les tokens matériels (ex : Yubikey), MFA pour applications mobiles (ex : Google Authenticator) ▪ L'authentification biométrique : ses applications pratiques et ses contraintes ▪ Les solutions cloud pour la gestion des identités et l'authentification forte (ex : Azure Active Directory, AWS IAM etc.) • La gestion des autorisations et des rôles d'accès : Role-Based Access Control (RBAC) ▪ Les rôles et les permissions dans Active Directory et OpenLDAP ▪ Les fonctions du modèle Role-Based Access Control (RBAC) : création de rôles, assignation des permissions en fonction des rôles ▪ Les principes du moindre privilège dans les systèmes d'accès ▪ La révision régulière des accès et des permissions (ex : audit des permissions, rapports d'accès etc.)	*Mettre en place des solutions d'authentification forte, en configurant des systèmes MFA, pour renforcer la sécurité des accès aux systèmes critiques* *Configurer des tokens matériels et applications mobiles, en utilisant des solutions adaptées, pour garantir une authentification à deux facteurs (2FA)* *Appliquer l'authentification biométrique, en exploitant les dispositifs compatibles, pour améliorer la sécurité en respectant les contraintes légales et techniques* *Gérer les identités dans le cloud, en configurant des solutions idoines, pour garantir une authentification sécurisée dans les environnements cloud* *Administrer les autorisations et les rôles d'accès, en suivant le modèle Role-Based Access Control (RBAC), pour assigner les permissions en fonction des rôles* *Réviser les accès et permissions, en auditant régulièrement les rôles et les autorisations, pour garantir l'application du principe du moindre privilège*
3. Sécurisation et surveillance des accès • Single Sign-On (SSO) ▪ Les concepts de Single Sign-On (SSO) : avantages et inconvénients ▪ L'intégration du SSO dans les environnements d'entreprise : les protocoles SAML, OAuth, OpenID Connect etc. ▪ Les cas d'utilisation du SSO pour simplifier et sécuriser l'accès aux ressources multiples ▪ Configuration de SSO avec Active Directory Federation Services (ADFS) ou un fournisseur de services cloud ▪ Surveillance des accès via SSO pour identifier les comportements anormaux	*Configurer des solutions Single Sign-On (SSO), en intégrant des protocoles spécifiquement dédiés, pour simplifier et sécuriser l'accès aux ressources multiples* *Mettre en œuvre le SSO dans un environnement d'entreprise, en utilisant Active Directory Federation Services (ADFS) ou des services cloud, pour centraliser et sécuriser l'authentification* *Surveiller les accès via SSO, en analysant régulièrement les journaux d'accès, pour détecter les comportements anormaux et les tentatives d'accès non autorisées*

• Audit et surveillance des accès IAM ▪ La mise en place de journaux d'audit pour suivre les activités des utilisateurs et des administrateurs ▪ La surveillance des accès et des tentatives d'accès non autorisés ▪ Les outils de surveillance des permissions : SolarWinds Access Rights Manager, Microsoft Identity Manager etc. ▪ Les politiques de révision périodique des droits d'accès pour détecter les abus de privilèges	*Mettre en place des journaux d'audit, en configurant des outils de suivi, pour surveiller les activités des utilisateurs et des administrateurs* *Surveiller les tentatives d'accès, en utilisant des outils comme SolarWinds Access Rights Manager, pour identifier les tentatives non autorisées et prévenir les abus de privilèges* *Réviser périodiquement les droits d'accès, en suivant les politiques de révision des permissions, pour garantir le respect des principes de sécurité IAM*
Cryptographie et protection des données (40 à 50 h)	
Objectifs pédagogiques globaux : - **Appliquer les principes fondamentaux de la cryptographie pour sécuriser les données et les communications** - **Mettre en œuvre des algorithmes de chiffrement symétrique et asymétrique pour protéger les informations sensibles** - **Utiliser les fonctions de hachage et les signatures numériques pour garantir l'intégrité et l'authenticité des données** - **Implémenter des infrastructures à clé publique (PKI) et gérer les certificats numériques pour sécuriser les communications réseau**	
1. Les principes fondamentaux de la cryptographie • Les concepts clés de la cryptographie ▪ Historique et évolution de la cryptographie ▪ La différence entre le chiffrement symétrique et asymétrique ▪ Les notions de confidentialité, d'intégrité, d'authenticité et de non-répudiation ▪ Les principes de base du chiffrement : les clés, les algorithmes et les protocoles ▪ Les divers cas pratiques d'utilisation de la cryptographie pour sécuriser les systèmes et les réseaux • Le chiffrement symétrique ▪ Le fonctionnement des algorithmes symétriques : AES, DES, 3DES ▪ Les techniques de gestion des clés : la génération, la distribution et le stockage sécurisé ▪ Les exemples d'application pratique du chiffrement symétrique dans des scénarios courants (ex : chiffrement de fichiers, VPN, mise en œuvre de l'AES dans des systèmes de chiffrement de données locales etc.)	*Identifier les concepts clés de la cryptographie, en retraçant son évolution historique, pour comprendre les différences entre chiffrement symétrique et asymétrique* *Appliquer les notions de confidentialité, d'intégrité, d'authenticité et de non-répudiation, en utilisant des algorithmes cryptographiques, pour sécuriser les systèmes d'information* *Mettre en œuvre des techniques de chiffrement, en configurant des clés, des algorithmes et des protocoles, pour protéger les données sensibles dans divers contextes* *Configurer des algorithmes de chiffrement symétrique, en utilisant des solutions comme AES et 3DES, pour sécuriser les communications et les fichiers* *Gérer les clés de chiffrement, en appliquant des techniques de génération, de distribution et de stockage, pour garantir leur sécurité dans des systèmes cryptographiques* *Illustrer l'usage du chiffrement symétrique, en mettant en place des scénarios pratiques, pour protéger les données locales et réseau*

2. Le chiffrement asymétrique et les signatures numériques • Le chiffrement asymétrique : RSA et ECC ▪ Présentation du chiffrement asymétrique : RSA, les courbes elliptiques (ECC) ▪ Les cas d'utilisation du chiffrement asymétrique pour sécuriser les échanges de clés ▪ Les différences entre RSA et ECC quant à leur efficacité et applications ▪ L'utilisation de RSA dans les communications HTTPS et pour les clés SSH • Les signatures numériques et l'intégrité des données ▪ Les cas d'utilisation des signatures numériques pour l'authenticité et l'intégrité des messages ▪ Le fonctionnement des signatures numériques avec RSA et ECC ▪ L'intégrité des données avec les fonctions de hachage : MD5, SHA-2, SHA-3 ▪ La création, la vérification de signatures numériques et le hachage de fichiers	*Explorer le chiffrement asymétrique, en décrivant les principes de RSA et des courbes elliptiques (ECC), pour identifier leurs rôles dans la sécurisation des échanges de clés* *Comparer RSA et ECC, en analysant leurs différences d'efficacité, pour choisir la meilleure solution en fonction de la spécificité de la situation* *Mettre en œuvre des solutions RSA, en les configurant précisément, pour sécuriser les communications HTTPS et les clés SSH dans des environnements réseau* *Utiliser des signatures numériques, en appliquant les techniques de RSA et ECC, pour garantir l'authenticité et l'intégrité des messages échangés* *Assurer l'intégrité des données, en utilisant des fonctions de hachage, pour vérifier l'intégrité des fichiers et des messages* *Créer et vérifier des signatures numériques, en manipulant les algorithmes de hachage et de chiffrement, pour garantir la protection et l'authenticité des données*
3. Infrastructures à clé publique (PKI) et les certificats numériques • Les fonctions de hachage et d'intégrité des données ▪ Les principes et les cas d'utilisation des fonctions de hachage : MD5, SHA-256, SHA-3 ▪ Les calcul du condensat d'un fichier ou d'un message pour en vérifier l'intégrité ▪ La vérification d'intégrité dans les protocoles réseau (ex : certificats SSL/TLS, HTTPS) • PKI (Public Key Infrastructure) et gestion des certificats ▪ Les infrastructures à clé publique (PKI) et à la gestion des certificats numériques ▪ L'importance de l'utilisation des certificats pour sécuriser les échanges de données dans les protocoles SSL/TLS ▪ La création, la gestion et la révocation des certificats numériques (CA, certificats auto-signés, CRL etc.) ▪ La gestion des certificats pour un réseau d'entreprise • Les outils cryptographiques et les environnements de développement	*Appliquer les fonctions de hachage, en utilisant des algorithmes comme MD5, SHA-256 et SHA-3, pour vérifier l'intégrité des fichiers et des messages dans divers environnements* *Calculer le condensat d'un fichier, en employant des fonctions de hachage, pour assurer l'intégrité des données dans les protocoles réseau* *Mettre en œuvre des infrastructures à clé publique (PKI), en gérant les certificats numériques, pour sécuriser les échanges de données dans les protocoles SSL/TLS* *Révoquer des certificats numériques, en suivant les procédures de gestion, pour garantir la validité et la sécurité des échanges dans un réseau d'entreprise*

▪ Le langage Python et OpenSSL pour implémenter des algorithmes de cryptographie (ex : AES, RSA, SHA-2) ▪ Les outils PKI : les certificats SSL/TLS avec OpenSSL, les certificats numériques pour des serveurs Web ▪ SSL/TLS pour la sécurisation des communications dans des environnements cloud et/ou locaux	*Utiliser des outils cryptographiques comme OpenSSL et Python, en implémentant des algorithmes de chiffrement, pour sécuriser les communications et les données* *Configurer des certificats SSL/TLS, en les déployant sur des serveurs Web, pour protéger les communications dans des environnements cloud et locaux*
Sécurité des applications et services numériques (20 à 30 h)	
Objectifs pédagogiques globaux : - **Identifier et corriger les vulnérabilités des applications web et des services réseau** - **Sécuriser les API et les services en utilisant des standards de sécurité modernes comme OAuth, JWT et SSL/TLS** - **Appliquer des méthodes de tests de sécurité pour protéger les applications et les services contre les attaques courantes** - **Gérer et sécuriser les mises à jour et les correctifs des applications pour garantir une protection continue contre les failles de sécurité**	
1. Vulnérabilités des applications et des services • Les vulnérabilités des applications web ▪ Les principales vulnérabilités des applications web (injections SQL, cross-site scripting (XSS), cross-site request forgery (CSRF), etc.) ▪ Exemples et principes de fonctionnement des attaques sur le Web ▪ Les rapports OWASP (Open Web Application Security Project) pour identifier les risques et les vulnérabilités les plus courants • La prévention et la correction : les injections SQL et XSS ▪ Le fonctionnement des injections SQL et XSS : analyse de ces attaques dans les failles des entrées utilisateurs non validés ▪ Les techniques de prévention : la validation et le nettoyage des entrées utilisateur, les requêtes paramétrées (PDO, Prepared Statements etc.) ▪ La correction de scripts vulnérables aux injections SQL et aux attaques XSS	*Identifier les principales vulnérabilités des applications web, en analysant les failles comme les injections SQL, XSS et CSRF, pour anticiper les risques d'attaques* *Maîtriser les principes de fonctionnement des attaques web, en étudiant les exemples d'attaques courantes, afin de mieux comprendre les mécanismes de compromission* *Utiliser les rapports OWASP, en appliquant leurs recommandations, pour identifier et corriger les vulnérabilités les plus fréquentes dans les applications web* *Analyser le fonctionnement des injections SQL et XSS, en examinant les failles dans les entrées utilisateurs non validés, pour comprendre les points faibles des applications* *Mettre en œuvre des techniques de prévention, en validant et nettoyant les entrées utilisateur et en utilisant des requêtes paramétrées pour éviter les attaques* *Corriger les scripts vulnérables, en adaptant le code, pour empêcher les injections SQL et les attaques XSS dans les applications web*

Cybersécurité et gestion des réseaux

2. La sécurisation des services et des API • La sécurisation des APIs avec OAuth et JWT ▪ Les principes de sécurité des API (REST, SOAP etc.) ▪ OAuth 2.0 pour la gestion des permissions et des autorisations dans les services web ▪ Les JSON Web Tokens (JWT) pour authentifier et sécuriser les échanges entre un client et une API ▪ La création d'une API sécurisée avec OAuth 2.0 et JWT • La sécurisation des communications entre services : SSL/TLS ▪ Les protocoles SSL/TLS pour sécuriser les échanges de données sur le réseau ▪ La création et la gestion des certificats SSL/TLS pour chiffrer les communications ▪ La configuration de certificats SSL/TLS sur un serveur Web et API pour protéger les échanges de données	*Analyser les principes de sécurité des APIs, en détaillant les protocoles comme REST et SOAP, pour comprendre les enjeux de sécurisation des échanges entre services* *Configurer OAuth 2.0, en l'utilisant pour gérer les permissions et les autorisations dans les services web, afin de protéger les accès aux ressources* *Mettre en œuvre des JSON Web Tokens (JWT), en les exploitant efficacement, pour authentifier et sécuriser les échanges entre un client et une API* *Créer une API sécurisée, en intégrant OAuth 2.0 et JWT, pour protéger les interactions entre les services et les utilisateurs* *Sécuriser les communications entre services, en appliquant les protocoles SSL/TLS, pour chiffrer les échanges de données sur le réseau* *Gérer des certificats SSL/TLS, en les configurant sur un serveur Web et API, pour garantir la confidentialité des échanges de données*
3. Les tests de sécurité et les mises à jour • Les tests de sécurité des applications ▪ Les tests d'intrusion (pentests) pour identifier les vulnérabilités dans les applications ▪ Les outils de test de vulnérabilité : OWASP ZAP, Burp Suite, et Nessus ▪ Les tests de sécurité sur des applications web et l'analyse des résultats pour corriger les failles • La gestion des correctifs et des mises à jour ▪ L'importance de la gestion proactive des correctifs et des mises à jour des applications pour corriger les vulnérabilités ▪ Les outils de gestion des correctifs : WSUS, Ansible, Puppet ▪ Les différentes stratégies de gestion des correctifs dans un environnement multiserveurs (ex : staging, automatisation des correctifs avec des outils Cloud-natifs, l'approche « Rolling Update », le déploiement des correctifs avec Azure Arc ou AWS Outposts etc.)	*Effectuer des tests d'intrusion, en utilisant des outils comme OWASP ZAP et Burp Suite, pour identifier et analyser les vulnérabilités des applications* *Corriger les failles de sécurité, en analysant les résultats des tests d'intrusion, pour renforcer la sécurité des applications* *Gérer les correctifs et mises à jour, en appliquant proactivement des stratégies adaptées, pour corriger les vulnérabilités dans les applications et les services* *Mettre en place des outils de gestion des correctifs comme WSUS, Ansible et Puppet, en les configurant efficacement, pour automatiser la correction des failles dans des environnements multiserveurs* *Déployer des correctifs avec des outils Cloud-natifs, en suivant des stratégies comme « Rolling Update », pour assurer une mise à jour continue et sécurisée des applications*

Réponse aux incidents et gestion des crises cyber (20 à 30 h)	
Objectifs pédagogiques globaux : - **Détecter et diagnostiquer des incidents de sécurité en analysant les journaux et les indicateurs de compromission** - **Répondre efficacement aux cyberattaques à travers des plans de réponse adaptés et la mise en place de contre-mesures rapides et immédiates** - **Mettre en œuvre des stratégies de confinement, d'éradication et de récupération des systèmes affectés par un incident** - **Utiliser des outils de gestion des incidents de sécurité (SIEM) pour surveiller, analyser et réagir face aux incidents de manière proactive**	
1. Détection des incidents de sécurité • La gestion des incidents de sécurité ▪ Définition et classification des incidents de sécurité (intrusions, attaques DDoS, ransomwares, phishing, etc.) ▪ Les différents processus de gestion des incidents : identification, réponse, récupération, plan de rétention ▪ Les notions de RTO (Recovery Time Objective) et RPO (Recovery Point Objective) dans le cadre des incidents	*Classer les incidents de sécurité, en définissant les différentes catégories, pour mieux comprendre leurs impacts et priorités de réponse* *Appliquer les processus de gestion des incidents, en suivant les étapes d'identification, de réponse et de récupération, pour limiter les impacts sur les systèmes*
• La détection des incidents de sécurité ▪ Les indicateurs de compromission (IoC) pour la détection des incidents (ex : fichiers suspects, adresses IP malveillantes, comportement réseau anormal etc.) ▪ Les journaux d'événements pour identifier les attaques : logs de système, réseau et applications ▪ Les outils de surveillance des incidents : Splunk, Graylog, ELK Stack (Elasticsearch, Logstash, Kibana etc.) ▪ Les systèmes de détection et de prévention des intrusions (IDS/IPS) pour détecter les activités suspectes	*Analyser les indicateurs de compromission (IoC), en les surveillant attentivement, pour détecter les comportements réseau ou fichiers suspects et réagir rapidement* *Exploiter les journaux d'événements, en les analysant, pour identifier les tentatives d'attaques à travers les logs de système, réseau et applications* *Mettre en œuvre des outils de surveillance des incidents, en configurant des solutions comme Splunk, Graylog, ou ELK Stack, pour centraliser et détecter les anomalies* *Utiliser des systèmes IDS/IPS, en les configurant de manière précise, pour prévenir et détecter les activités suspectes dans les environnements réseau*
2. Les réponses aux cyberattaques • Les processus de réponse aux cyberattaques ▪ Les étapes clés de la réponse à un incident : identification, confinement, éradication, récupération ▪ Les plans de réponse aux incidents : la création et la gestion d'un IRP (Incident Response Plan) ▪ La priorisation des réponses selon la gravité de l'incident (ex : escalade, isolement des systèmes affectés)	*Appliquer les étapes de réponse aux cyberattaques, en suivant les processus d'identification, de confinement, d'éradication et de récupération, pour limiter les impacts des incidents* *Mettre en place un Incident Response Plan (IRP), en le créant méthodiquement, pour organiser la gestion des incidents et structurer les réponses appropriées* *Prioriser les réponses aux incidents, en évaluant la gravité des cyberattaques, pour isoler rapidement les systèmes affectés et éviter leur propagation*

▪ Gestion d'une attaque réseau (DDoS) et réponse avec confinement et récupération • Les outils de réponse aux incidents ▪ Les systèmes SIEM (Security Information and Event Management) pour centraliser et analyser les alertes de sécurité ▪ Les outils de gestion d'incidents : Splunk, IBM QRadar, ArcSight ▪ La configuration des outils de surveillance pour répondre à un incident en temps réel ▪ Les méthodes d'analyse post-incident : la collecte des preuves, la documentation sur les événements, et l'identification des vecteurs d'attaque	*Gérer une attaque DDoS, en appliquant précisément les étapes de confinement et de récupération, pour rétablir le fonctionnement du réseau* *Utiliser des systèmes SIEM, en les configurant efficacement, pour centraliser et analyser les alertes de sécurité en temps réel* *Analyser les incidents post-cyberattaque, en collectant les preuves et en documentant les événements, pour identifier les vecteurs d'attaque et améliorer la sécurité future*
3. Confinement, éradication et récupération • Confinement et éradication des cybermenaces ▪ Les stratégies de confinement : isolation des systèmes infectés pour limiter la propagation des attaques ▪ Les techniques d'éradication ○ Identification et suppression des fichiers malveillants ○ Désactivation des comptes compromis ○ Fermeture des vulnérabilités exploitées ▪ Les outils pour neutraliser les menaces : les antivirus, l'EDR (Endpoint Detection and Response) et les systèmes de sauvegarde • La récupération des données post-incidents ▪ La récupération des systèmes et des données après un incident de sécurité ▪ La reprise après sinistre : restauration des systèmes à partir de sauvegardes cloud et on-premise ▪ La planification des tests de restauration pour vérifier l'efficacité des processus de récupération ▪ La mise en œuvre d'un plan de restauration après une attaque virale	*Mettre en œuvre des stratégies de confinement, en isolant les systèmes infectés, pour limiter la propagation des cyberattaques* *Éradiquer les cybermenaces, en identifiant et supprimant les fichiers malveillants, en désactivant les comptes compromis et en fermant les vulnérabilités exploitées, pour neutraliser l'attaque et restaurer la sécurité des systèmes* *Utiliser des outils de neutralisation des menaces, en appliquant des solutions comme les antivirus et l'EDR, pour stopper et supprimer les cybermenaces* *Récupérer les systèmes et données après un incident, en suivant les procédures de restauration à partir de sauvegardes cloud et on-premise, pour minimiser les pertes* *Planifier des tests de restauration, en les exécutant périodiquement, pour vérifier l'efficacité des processus de récupération après une attaque* *Mettre en place un plan de restauration post-attaque virale, en appliquant les meilleures pratiques, pour assurer une reprise sécurisée des activités*
4. Analyse post-incident et processus d'amélioration continue • L'analyse post-incident et le retour d'expérience	*Rédiger des documentations post-incident, en analysant les incidents de sécurité, pour en tirer des leçons et améliorer la gestion des futures attaques*

▪ Rédaction de documentations et de retours d'analyse des incidents de sécurité pour en tirer des leçons (post-mortem ▪ Mise à jour des politiques de sécurité et révision des stratégies en fonction des résultats post-incident ▪ L'application des correctifs et la mise en place de mesures préventives pour éviter un retour d'incidents. ▪ Les attaques majeures (ex : WannaCry, SolarWinds) et les réponses spécifiques à appliquer	*Mettre à jour les politiques de sécurité, en ajustant les stratégies en fonction des résultats post-incident, pour renforcer la prévention contre les attaques similaires* *Appliquer des correctifs et des mesures préventives, en les implémentant dans la stratégie, pour éviter la récurrence des incidents de sécurité* *Analyser des cas d'attaques majeures comme WannaCry ou SolarWinds, en identifiant les failles exploitées, pour appliquer des réponses adaptées à ces types de cybermenaces*
5. Les outils de détection et de réponse aux incidents • Les outils SIEM (ex : Splunk, Graylog, ELK Stack, IBM QRadar, ArcSight etc.) • Les systèmes de détection et de réponse : IDS/IPS (Snort, Suricata), les outils de surveillance (ex : Nagios, Zabbix etc.) • Les outils d'analyse des journaux (ex : Wireshark, tcpdump, Kibana etc.) • Les environnements virtualisés : les serveurs simulés pour tester les réponses aux incidents et les techniques de récupération	*Utiliser des outils SIEM, en configurant des solutions comme Splunk, Graylog et ELK Stack, pour centraliser et analyser les alertes de sécurité* *Surveiller les systèmes critiques, en utilisant des outils de surveillance comme Nagios et Zabbix, pour anticiper les incidents et optimiser la protection* *Mettre en œuvre des systèmes IDS/IPS, en exploitant leurs fonctionnalités, pour détecter et répondre aux incidents de sécurité dans des environnements réseau* *Analyser les journaux réseau, en utilisant des outils comme Wireshark et tcpdump, pour identifier les tentatives d'intrusion et comportements anormaux* *Tester les réponses aux incidents, en configurant des environnements virtualisés, pour simuler des attaques et améliorer les processus de récupération*
6. Les SOC (Security Operations Center) • Les concepts opérationnels des SOC ▪ Rôle et fonctionnement d'un SOC (Niveaux 1, 2 et 3) ▪ Les missions des analystes SOC : détection, investigation, remédiation ▪ Les environnements et outils utilisés dans un SOC • La détection avancée des menaces avec SIEM ▪ Présentation des outils SIEM (Splunk, QRadar, ELK Stack) ▪ L'analyse des logs et identification des anomalies ▪ Threat Intelligence et utilisation des bases de menaces (MISP, MITRE ATT&CK).	*Définir le rôle et le fonctionnement d'un SOC en différenciant les niveaux d'intervention et les missions des analystes, afin de comprendre l'organisation et les responsabilités des équipes de cybersécurité opérationnelles* *Détecter des cybermenaces, en exploitant les outils SIEM et les bases de Threat Intelligence, afin d'identifier les activités suspectes et renforcer la surveillance des systèmes d'information*

Cybersécurité et gestion des réseaux

• Analyse des logs et gestion des alertes de sécurité ▪ Le différents types de logs (firewall, endpoint, application, cloud) ▪ La corrélation des événements et l'analyse comportementale ▪ L'automatisation des réponses avec SOAR (Security Orchestration, Automation and Response)	*Analyser les logs de sécurité, en appliquant des techniques de corrélation d'événements et d'analyse comportementale, afin d'identifier les anomalies et anticiper les attaques avancées* *Automatiser les réponses aux incidents, en configurant des solutions SOAR pour orchestrer la remédiation des alertes, afin de réduire le temps de réaction et limiter l'impact des cyberattaques sur l'organisation*
7. Gestion de crise et communication en cybersécurité	
• Processus de gestion de crise en cybersécurité ▪ Les différentes phases d'un incident cyber (détection, confinement, éradication, récupération) ▪ L'élaboration d'un Cyber Incident Response Plan (CIRP) ▪ La coordination entre équipes techniques, RSSI, direction et autorités	*Coordonner la gestion d'un incident cyber, en appliquant les phases du Cyber Incident Response Plan, afin d'assurer une réponse efficace et limiter l'impact sur l'organisation*
• Communication en situation de crise cyber ▪ La gestion de la communication interne et externe ▪ L'élaboration de messages pour limiter l'impact médiatique ▪ La rédaction d'un rapport post-incident ▪ Le débriefing et l'amélioration continue des procédures	*Élaborer une stratégie de communication de crise, en structurant les messages internes et externes adaptés aux parties prenantes, afin de minimiser les impacts médiatiques et organisationnels d'un incident cyber*
8. Éthique et hacking éthique en cybersécurité	
• Introduction aux principes de l'éthique en cybersécurité ▪ Distinguer hacking éthique et cybercriminalité ▪ Les notions de responsabilité individuelle et collective en cybersécurité ▪ Les risques liés aux tests d'intrusion non autorisés	*Différencier le hacking éthique de la cybercriminalité, en analysant les principes éthiques et les responsabilités légales, afin d'adopter des pratiques de cybersécurité conformes aux réglementations en vigueur*
• Cadre légal et réglementaire du hacking éthique ▪ Les lois encadrant les tests de sécurité (LOPSSI, RGPD, NIS2, CFAA USA) ▪ Les autorisations et les obligations des professionnels de la cybersécurité ▪ Les sanctions et les conséquences en cas de non-respect des lois	*Appliquer les cadres légaux et réglementaires, en respectant les obligations en matière de tests de sécurité, afin d'effectuer des audits et des analyses en toute légalité*
• Les principes du hacking éthique et les bonnes pratiques ▪ Les certificats et normes (CEH, OSCP, GPEN)	*Rédiger une charte d'engagement éthique pour les interventions en cybersécurité, en intégrant les bonnes pratiques et les normes professionnelles, afin de garantir la transparence et l'intégrité des actions menées*

▪ Les dilemmes éthiques et les limites du hacking défensif ▪ La rédaction d'une charte d'engagement éthique pour les tests de sécurité ▪ La gestion de la découverte d'une faille critique dans une infrastructure sensible	*Évaluer les implications éthiques d'un test de sécurité ou d'une divulgation de vulnérabilité, en identifiant les dilemmes moraux afin d'adopter une posture responsable et conforme aux attentes des entreprises*
Sécurisation des environnements cloud et Big Data (30 à 40 h)	
Objectifs pédagogiques globaux : - **Assimiler les principes fondamentaux de la sécurité dans le cloud et leur application aux environnements Big Data** - **Mettre en œuvre des stratégies de protection des données dans le cloud et sécuriser les infrastructures Big Data** - **Appliquer des méthodes de chiffrement, de gestion des accès, et de surveillance des activités pour garantir la sécurité dans les environnements cloud** - **Utiliser des solutions de sécurité cloud (AWS, Azure, Google Cloud) pour protéger les données et les services critiques dans les environnements Big Data**	
1. Les concepts fondamentaux de la sécurité dans le cloud • Introduction à la sécurité dans le cloud ▪ Définition et présentation des principaux modèles de services Cloud : IaaS, PaaS, SaaS ▪ Les concepts de sécurité spécifiques au cloud : la responsabilité partagée, la sécurité des infrastructures cloud et les menaces spécifiques (ex : attaques DDoS, vol de données etc.) ▪ Les principaux risques liés au cloud : la perte de contrôle des données, la non-conformité, l'exposition des API etc. ▪ Les exemples d'incidents de sécurité inhérents aux environnements Cloud • Les principes de gestion des accès et des identités dans le Cloud ▪ Les politiques de gestion des accès dans le cloud : IAM (Identity and Access Management), les rôles, les groupes et les permissions ▪ La sécurisation des API cloud : OAuth et les tokens JWT pour les accès sécurisés ▪ La surveillance des accès et la détection des anomalies à l'aide d'outils de gestion des identités (ex : AWS IAM, Azure Active Directory etc.) **2. Sécurisation des données dans les environnements Cloud et Big Data** • La sécurité des données dans le Cloud	*Décrire les principaux modèles de services cloud, en identifiant leurs caractéristiques, pour comprendre les enjeux de sécurité dans le cloud* *Analyser les concepts de sécurité spécifiques au cloud, en distinguant les responsabilités partagées et les menaces spécifiques, pour anticiper les risques comme les attaques DDoS et le vol de données* *Repérer les principaux risques liés au cloud, en étudiant les menaces comme la perte de contrôle des données et l'exposition des API pour prévenir les incidents de sécurité* *Illustrer les exemples d'incidents de sécurité dans le cloud, en examinant des cas réels, pour comprendre les vulnérabilités inhérentes aux environnements cloud* *Mettre en œuvre des politiques de gestion des accès dans le cloud, en configurant des solutions IAM, pour garantir un contrôle sécurisé des identités et des permissions* *Sécuriser les API cloud, en utilisant efficacement OAuth et les tokens JWT, pour garantir des accès protégés et surveiller les anomalies d'accès* *Superviser les accès au cloud, en exploitant des outils de gestion des identités comme AWS IAM et Azure Active Directory, pour détecter et réagir aux comportements anormaux*

▪ Les techniques de chiffrement des données au repos et en transit : SSL/TLS, le chiffrement symétrique et asymétrique ▪ La gestion des clés de chiffrement dans les plateformes Cloud (AWS KMS, Azure Key Vault, Google Cloud KMS etc.) ▪ La sécurisation des bases de données et des données sensibles stockées dans le Cloud ▪ Les solutions de chiffrement dans un environnement AWS pour protéger les données sensibles • La sécurisation des infrastructures Big Data ▪ Les risques spécifiques liés aux infrastructures Big Data (ex : vol de données, attaques sur les clusters Hadoop/Spark, les fuites de données dans les environnements NoSQL) ▪ Les stratégies de protection des données Big Data dans le cloud : le chiffrement, la segmentation des réseaux, la gestion des permissions ▪ La gestion des accès dans les infrastructures Big Data	*Appliquer les techniques de chiffrement, en configurant des solutions comme SSL/TLS et le chiffrement symétrique, pour protéger les données au repos et en transit dans le cloud* *Gérer les clés de chiffrement, en utilisant des outils comme AWS KMS, Azure Key Vault et Google Cloud KMS, pour assurer la sécurité des données sensibles* *Sécuriser les bases de données dans le cloud en implémentant des solutions de chiffrement, pour protéger les informations critiques stockées dans les environnements cloud* *Mettre en œuvre des solutions de chiffrement AWS, en suivant les procédures, pour protéger les données sensibles dans les environnements AWS* *Analyser les risques spécifiques liés aux infrastructures Big Data, en identifiant les menaces comme le vol de données ou les attaques sur les clusters Hadoop/Spark, pour prévenir les incidents* *Mettre en place des stratégies de protection des données Big Data, en utilisant des techniques adaptées pour sécuriser les infrastructures Big Data* *Gérer les accès dans les infrastructures Big Data, en configurant des permissions, pour contrôler les droits d'accès aux données et prévenir les fuites*
3. Sécurité Cloud et virtualisation • Les principes fondamentaux de la sécurité Cloud ▪ Définition des modèles IaaS, PaaS, SaaS et leurs implications en cybersécurité ▪ Les principaux fournisseurs : AWS, Azure, Google Cloud ▪ La responsabilité partagée en cybersécurité cloud • Sécurisation des infrastructures cloud ▪ La gestion des accès et IAM cloud (AWS IAM, Azure AD) ▪ Les stratégies de chiffrement des données (KMS, secrets management) ▪ La sécurisation des API et endpoints cloud ▪ La protection contre les attaques DDoS et injections cloud • Kubernetes et la sécurité des containers	*Différencier les modèles IaaS, PaaS et SaaS, en identifiant leurs implications en cybersécurité, afin d'adapter les stratégies de protection aux environnements cloud spécifiques* *Mettre en œuvre des stratégies de gestion des accès et des identités, en configurant IAM sur AWS, Azure AD et Google Cloud, afin de contrôler et sécuriser les autorisations et privilèges d'accès* *Sécuriser les infrastructures cloud, en appliquant des politiques de chiffrement, de protection des API et de mitigation des attaques DDoS, afin de garantir l'intégrité et la confidentialité des données et services cloud*

Cybersécurité et gestion des réseaux

▪ Les concepts de conteneurisation avec Docker et Kubernetes ▪ La gestion des politiques de sécurité avec Kubernetes RBAC et Network Policies ▪ L'analyse des vulnérabilités avec Trivy, Falco, Sysdig ▪ La protection des CICD pipelines avec DevSecOps	*Renforcer la sécurité des conteneurs et des clusters Kubernetes, en utilisant RBAC, Network Policies et des outils d'analyse des vulnérabilités, afin de prévenir les attaques et garantir l'isolation des workloads*
• Sécurité avancée des environnements AWS, Azure, Kubernetes ▪ La gestion des permissions et des accès cloud (IAM avancé, RBAC, Security Groups) ▪ La sécurisation des API Cloud et la gestion des clés de chiffrement ▪ La protection des environnements multi-cloud et hybrid-cloud	*Sécuriser les environnements cloud, en appliquant les bonnes pratiques de gestion des accès et de protection des API, afin de prévenir les vulnérabilités liées aux infrastructures AWS, Azure et Kubernetes*
• Automatisation de la sécurité avec Terraform et Ansible ▪ Infrastructure as Code (IaC) et gestion sécurisée des configurations cloud ▪ Le déploiement sécurisé des environnements cloud via Terraform ▪ L'analyse des erreurs de configuration cloud et corrections automatisées	*Automatiser la gestion de la sécurité cloud en utilisant des outils d'Infrastructure as Code, afin de déployer des environnements conformes aux standards de cybersécurité et limiter les erreurs de configuration*
• Sécurité CI/CD et principes de DevSecOps ▪ Introduction au DevSecOps : intégration de la sécurité dans le développement cloud ▪ L'analyse des vulnérabilités dans la chaîne CI/CD (SAST, DAST, IAST) ▪ Les tests de conformité et scans de conteneurs (Trivy, Aqua Security, Snyk)	*Intégrer des mesures de sécurité dans les pipelines CI/CD en appliquant les principes du DevSecOps et en utilisant des outils de scan de vulnérabilités (Trivy, Aqua Security, Snyk) afin de identifier et corriger les failles dès les premières étapes du développement.*
• Automatisation et conformité cloud ▪ Automatisation de la sécurité avec Terraform et Ansible ▪ L'intégration de Cloud Security Posture Management (CSPM) ▪ Frameworks et normes : CIS AWS Benchmark, ISO 27017, SOC 2	*Automatiser les contrôles de sécurité et la conformité cloud, en déployant des solutions Terraform, Ansible et CSPM, afin d'assurer un monitoring en continu et répondre aux exigences des standards CIS AWS Benchmark, ISO 27017 et SOC 2*
• Les tests d'intrusion cloud ▪ Audit de sécurité AWS avec ScoutSuite et Prowler ▪ L'exploitation des erreurs de configuration cloud avec Pacu ▪ La simulation d'attaques sur Kubernetes avec kube-hunter	*Analyser la conformité des infrastructures cloud, en exploitant des outils d'audit et de surveillance des configurations, afin de s'assurer du respect des standards ISO 27017 et CIS AWS Benchmark*

4. Conformité et gestion des risques dans le cloud et Big Data • Les normes et les audits de sécurité dans le Cloud ▪ Les principales normes de conformité pour le cloud et les environnements Big Data : RGPD, ISO 27001, SOC 2 ▪ Les stratégies de sécurité conformes aux exigences réglementaires ▪ Les audits de sécurité dans le Cloud ▪ Les outils et bonnes pratiques pour assurer la conformité des environnements Cloud ▪ La réalisation d'un audit de conformité RGPD pour une infrastructure de données dans le Cloud • La surveillance et les réponses aux incidents dans le cloud et les infrastructures Big Data ▪ Les solutions de surveillance pour détecter les anomalies dans les environnements Cloud (ex : CloudWatch, Azure Monitor etc.) ▪ La gestion des incidents de sécurité dans le cloud : les stratégies de réponse aux incidents, l'isolation des systèmes et la restauration des données ▪ Les systèmes SIEM (Security Information and Event Management) pour surveiller les environnements Big Data et répondre aux incidents	*Appliquer les normes de conformité, en suivant strictement les exigences du RGPD, ISO 27001 et SOC 2, pour assurer la sécurité des environnements cloud et Big Data* *Mettre en œuvre des stratégies de sécurité conformes, en ajustant les pratiques de gestion des risques, pour respecter les exigences réglementaires des environnements cloud* *Effectuer des audits de sécurité, en suivant les processus de vérification, pour garantir la conformité des infrastructures cloud avec les normes en vigueur* *Utiliser des outils de conformité, en appliquant les bonnes pratiques, pour maintenir la sécurité et la conformité des environnements Cloud* *Réaliser un audit de conformité RGPD, en vérifiant les infrastructures de données dans le cloud, pour garantir la protection des données personnelles* *Surveiller les environnements cloud et Big Data, en configurant des outils comme CloudWatch et Azure Monitor, pour détecter rapidement les anomalies* *Gérer les incidents de sécurité dans le cloud, en suivant des stratégies de réponse comme l'isolation des systèmes et la restauration des données, pour minimiser l'impact des cyberattaques* *Exploiter les systèmes SIEM en les configurant avec précision, pour surveiller les environnements Big Data et réagir efficacement aux incidents de sécurité*
Normes, conformité et gestion des risques en cybersécurité (25 à 35 h)	
Objectifs pédagogiques globaux : - **Identifier et évaluer les risques liés à la sécurité des systèmes d'information en fonction des menaces et vulnérabilités spécifiques** - **Mettre en place des stratégies de gestion des risques et des plans de réduction des risques pour protéger les données et les systèmes** - **Examiner les exigences légales et les normes de conformité (GDPR, ISO 27001, NIST) et leur mise en application au sein d'une organisation** - **Élaborer et suivre des politiques de sécurité pour assurer la conformité et minimiser les risques organisationnels**	
1. Introduction à la gestion des risques en cybersécurité	

Cybersécurité et gestion des réseaux

• Les concepts de base de la gestion des risques en cybersécurité ▪ Définition des risques, des menaces et des vulnérabilités en cybersécurité ▪ Les différents modèles de gestion des risques : l'identification, l'évaluation, le traitement, la surveillance ▪ Les processus d'évaluation des risques : les analyses quantitatives et qualitatives ▪ La gestion des risques en fonction de la taille de l'entreprise • Analyse des menaces et des vulnérabilités ▪ Les menaces courantes pour les systèmes d'information ○ Les attaques externes (DDoS, phishing, ransomwares etc.) ○ Les menaces internes (insiders) ○ Les vulnérabilités techniques (ex : logiciels non mis à jour etc.) ▪ Les méthodologies d'analyse des vulnérabilités : CVSS (Common Vulnerability Scoring System) et les scans de vulnérabilités avec des outils comme Nessus ou Qualys	*Explorer les concepts de risques, menaces et vulnérabilités en cybersécurité, en analysant leurs implications, pour mieux anticiper les incidents potentiels* *Appliquer les modèles de gestion des risques, en suivant les étapes d'identification, d'évaluation, de traitement et de surveillance, pour sécuriser les systèmes d'information* *Évaluer les risques, en utilisant des analyses quantitatives et qualitatives, pour mesurer les impacts potentiels et prioriser les actions de sécurisation* *Adapter la gestion des risques, en ajustant les stratégies en fonction de la taille de l'entreprise, pour garantir une cybersécurité efficace et conforme aux besoins* *Analyser les menaces courantes, en identifiant les attaques externes et internes, pour protéger les systèmes d'information* *Utiliser le système CVSS, en l'appliquant convenablement, pour mesurer la gravité des vulnérabilités et prioriser les actions correctives* *Évaluer les vulnérabilités techniques, en utilisant des outils comme Nessus ou Qualys, pour identifier les failles et renforcer la sécurité des systèmes*
2. La cybersécurité industrielle • La sécurisation des infrastructures critiques (énergie, transport, industrie) ▪ Les menaces et les attaques spécifiques aux infrastructures industrielles ▪ Les cyberattaques notables (Stuxnet, Triton, BlackEnergy) ▪ Les enjeux de cybersécurité pour les systèmes de contrôle industriels (ICS) • La protection des systèmes SCADA et ICS ▪ Le fonctionnement des systèmes de supervision industrielle (SCADA, DCS, PLC) ▪ La sécurisation des communications industrielles (Modbus, OPC-UA, DNP3) ▪ La segmentation réseau et isolation des environnements OT • Les normes spécifiques aux environnements industriels (ISO 62443, NERC CIP) ▪ Présentation des référentiels de cybersécurité industrielle	*Analyser les menaces et cyberattaques spécifiques aux infrastructures critiques, en étudiant les incidents notables, afin de comprendre les vulnérabilités des systèmes industriels et anticiper les attaques ciblées* *Sécuriser les systèmes SCADA et ICS, en mettant en œuvre des protocoles de protection adaptés et des techniques de segmentation réseau, afin de préserver l'intégrité et la disponibilité des infrastructures industrielles* *Appliquer les normes de cybersécurité industrielle, en intégrant les référentiels ISO 62443, NERC CIP et IEC 61850 dans les stratégies de protection, afin de garantir la conformité réglementaire et renforcer la résilience des infrastructures critiques* *Auditer la sécurité des environnements industriels, en utilisant des méthodologies d'évaluation des risques et des outils d'analyse spécifiques aux infrastructures OT, afin d'identifier les vulnérabilités et proposer des mesures correctives adaptées*

Cybersécurité et gestion des réseaux

▪ Les bonnes pratiques pour protéger les infrastructures critiques ▪ Audits et conformité des systèmes OT	
3. La gestion des risques et les stratégies de mitigation • L'évaluation et la gestion des risques ▪ Les techniques de hiérarchisation des risques ○ La matrice des risques ○ La cartographie des risques. ▪ Les approches fondées sur l'impact et la probabilité des menaces ▪ Les stratégies de mitigation des risques : éviter, transférer, accepter ou atténuer les risques ▪ L'élaboration du plan de gestion des risques : la mise en place de stratégies de réduction pour différents types de menaces (ex : cyberattaques, pannes systèmes, erreurs humaines etc.)	*Hiérarchiser les risques, en utilisant des techniques comme la matrice des risques et la cartographie, pour identifier les menaces les plus critiques* *Appliquer des approches d'évaluation des risques, en les basant sur l'impact et la probabilité des menaces, pour prioriser les actions de mitigation* *Mettre en œuvre des stratégies de mitigation des risques, en choisissant soit d'éviter, de transférer, d'accepter ou d'atténuer les menaces identifiées, pour minimiser leur impact* *Élaborer un plan de gestion des risques, en définissant les stratégies de réduction adaptées à différents types de menaces, pour assurer une gestion proactive des risques*
4. Conformité et réglementation en cybersécurité • Les contraintes légales et les différentes réglementations en matière de cybersécurité ▪ Les lois et les réglementations en matière de cybersécurité : RGPD (GDPR), ISO 27001, NIST (National Institute of Standards and Technology) ▪ Les obligations légales relatives à la protection des données personnelles et la sécurité des systèmes ▪ Réalisation d'un audit de conformité RGPD dans un environnement simulé	*Analyser les lois et réglementations en matière de cybersécurité, en évaluant les obligations imposées par le RGPD, ISO 27001, et NIST pour garantir la conformité légale des organisations* *Mettre en œuvre des politiques de protection des données personnelles, en appliquant les exigences légales, pour sécuriser les systèmes et protéger la vie privée des utilisateurs* *Réaliser un audit de conformité RGPD, en suivant les procédures dans un environnement simulé, pour vérifier le respect des normes de protection des données*
5. Cadres réglementaires internationaux et cybersécurité multiculturelle • Les réglementations en dehors de l'Europe ▪ CCPA (California Consumer Privacy Act) ▪ HIPAA (Health Insurance Portability and Accountability Act) ▪ PDPA (Personal Data Protection Act) ▪ Cyber Security Law of China • Comparaison des réglementations et implications en cybersécurité ▪ Les différences entre RGPD, CCPA, HIPAA, PDPA	*Comparer les cadres réglementaires internationaux en analysant leurs exigences spécifiques, afin d'adapter les stratégies de cybersécurité aux obligations légales en fonction des zones géographiques* *Évaluer l'impact des réglementations internationales sur la cybersécurité, en identifiant les différences en matière de protection des données et de conformité, afin d'anticiper les contraintes liées aux transferts de données transfrontaliers et aux audits de conformité*

▪ Les impacts sur les entreprises internationales et sur la protection des données ▪ Les exigences en matière de stockage et transfert de données transfrontaliers • Les défis multiculturels en cybersécurité ▪ La gestion des cyberattaques dans un environnement globalisé (réglementations locales et coopérations internationales) ▪ La sensibilité culturelle et la protection des données (ex : perception différente de la vie privée selon les pays) ▪ La gestion des équipes de cybersécurité à l'international (barrières linguistiques, différences juridiques et éthiques) • L'élaboration d'une politique de conformité pour une entreprise opérant en Europe, aux États-Unis et en Asie • La mise en œuvre de politiques de conformité ▪ Élaboration et gestion des politiques de sécurité pour assurer la conformité aux normes et lois en vigueur ▪ Les processus d'audit interne et externe pour vérifier la conformité aux régulations ▪ Exemple de création d'une politique de conformité pour une organisation, intégrant les exigences réglementaires pertinentes (ex : RGPD, ISO 27001)	*Adapter les politiques de cybersécurité d'une entreprise en tenant compte des défis multiculturels, afin de garantir une gestion efficace des risques dans un contexte international* *Concevoir une politique de conformité globale, en intégrant les normes et réglementations internationales applicables aux entreprises opérant dans plusieurs pays, afin d'assurer une sécurité homogène tout en respectant les exigences locales* *Élaborer des politiques de sécurité, en ajustant les règles, pour garantir la conformité aux normes et lois en vigueur dans les systèmes d'information* *Effectuer des audits internes et externes, en vérifiant la conformité aux régulations, pour garantir que les organisations respectent les exigences légales* *Créer une politique de conformité pour une organisation, en intégrant les exigences du RGPD et ISO 27001, pour assurer une protection optimale des données et des systèmes*
6. Audits de sécurité et surveillance des risques • L'importance des audits réguliers pour assurer la conformité et la gestion continue des risques • Les différents processus de surveillance des politiques de sécurité : monitoring des incidents, la revue des accès et permissions, les tests d'intrusion • Présentation et utilisation des outils d'audit de sécurité (Qualys, OpenVAS) pour vérifier la conformité des systèmes	*Réaliser des audits de sécurité réguliers, en suivant rigoureusement les procédures, pour garantir la conformité et une gestion continue des risques* *Surveiller les politiques de sécurité, en monitorant les incidents, les accès, et les permissions pour identifier les vulnérabilités et prévenir les risques* *Utiliser des outils d'audit comme Qualys et OpenVAS, en les configurant pour vérifier la conformité des systèmes et identifier les failles de sécurité*
Veille et prospective en cybersécurité (15 à 20 h)	
Objectifs pédagogiques globaux : - **Effectuer une veille technologique régulière pour suivre l'évolution des menaces et des solutions en matière de cybersécurité** - **Identifier et analyser les nouveaux enjeux et tendances de la cybersécurité, tels que l'IA, la blockchain, l'IoT, la 5G et la sécurité des environnements Cloud**	

Cybersécurité et gestion des réseaux

- **Appliquer des méthodes de veille stratégique afin d'anticiper les évolutions technologiques et réglementaires dans le domaine de la cybersécurité**
- **Intégrer la veille technologique dans des stratégies de cybersécurité pour améliorer la résilience des systèmes d'information**

1. Veille technologique et méthodes de recherche	
• La veille technologique : méthodologies ▪ Définitions et objectifs d'une veille technologique : motifs et méthodes pour effectuer une veille dans le domaine de la cybersécurité	*Effectuer une veille technologique, en identifiant les motifs et méthodes appropriées, pour anticiper les évolutions dans le domaine de la cybersécurité*
▪ Les outils et les méthodologies pour la veille technologique : les outils de veille (ex : Google Alerts, RSS, plateformes spécialisées etc.), les bases de données (ex : CVE - Common Vulnerabilities and Exposures, MITRE ATT&CK etc.)	*Utiliser des outils de veille technologique, en appliquant des solutions comme Google Alerts, RSS et CVE, pour rester informé des dernières vulnérabilités et menaces*
▪ Les processus de veille sur les vulnérabilités : analyse des failles zero-day, les outils de surveillance des vulnérabilités, et le suivi des correctifs (patch management)	*Surveiller les failles zero-day, en analysant les vulnérabilités identifiées et en suivant les correctifs, pour renforcer la sécurité des systèmes*
• La mise en place d'une veille stratégique ▪ Les méthodologies de recherche et de sélection des sources fiables (ex : blogs, forums, bases de données, conférences etc.)	*Mettre en place une veille stratégique, en sélectionnant des sources fiables, pour garantir une information de qualité et à jour*
▪ Les outils de gestion de l'information et les procédures d'automatisation de la veille technologique (ex : Feedly, Twitter, GitHub etc.)	*Automatiser le flux d'information, en configurant des outils comme Feedly et Twitter, pour obtenir un flux de veille personnalisé sur les sujets actuels en cybersécurité*
▪ La mise en place d'un flux de veille personnalisé sur des sujets actuels en cybersécurité	
2. Les nouveaux enjeux technologiques en cybersécurité	
• Les nouvelles technologies et leurs impacts en termes de sécurité ▪ L'Internet des objets (IoT) : la sécurité des objets connectés avec des exemples d'attaques récentes (ex : Mirai Botnet) et les solutions et réponses émergentes pour sécuriser les réseaux IoT	*Analyser les enjeux de sécurité des objets connectés, en étudiant les attaques récentes, pour développer des solutions adaptées aux réseaux IoT*
▪ La norme 5G : les enjeux de sécurité dans les réseaux de nouvelle génération, les vulnérabilités potentielles et leur impact sur les infrastructures critiques	*Identifier les vulnérabilités de la norme 5G, en examinant les impacts potentiels sur les infrastructures critiques, pour anticiper les menaces liées à cette nouvelle technologie*
▪ La blockchain : les différentes applications de la blockchain dans la cybersécurité (ex : authentification,	*Évaluer les applications de la blockchain, en analysant leurs avantages et limitations, pour l'authentification et la protection des données*

protection des données etc.) et ses limitations • Cybersécurité et environnements Cloud ▪ L'évolution des menaces dans le cloud (ex : fuites de données, attaques DDoS, compromission des API Cloud etc.) ▪ Veille et suivi des évolutions des services de sécurité dans les plateformes cloud (ex : AWS, Azure, Google Cloud etc.), de la gestion des identités, du chiffrement et des solutions de détection et réponse	*Surveiller les évolutions des menaces dans le cloud, en effectuant une veille continue sur les risques comme les fuites de données et les compromissions d'API, pour adapter les stratégies de cybersécurité aux nouvelles vulnérabilités* *Suivre les mises à jour des services de sécurité sur les plateformes cloud, en restant informé des nouveautés sur AWS, Azure et Google Cloud, pour renforcer la gestion des identités et le chiffrement*
3. IA et cybersécurité • Introduction à l'IA et son application en cybersécurité ▪ Définition et typologie : Machine Learning (ML), Deep Learning (DL), IA Générative ▪ Enjeux et opportunités : détection des attaques, automatisation des défenses, prédiction des menaces ▪ Présentation des principaux outils : IBM Watson for Cybersecurity, Splunk AI, Google Chronicle • Détection des menaces grâce au Machine Learning ▪ Supervised vs Unsupervised Learning appliqués à la cybersécurité ▪ La modélisation et la classification des cyberattaques avec ML • Automatisation des réponses aux incidents via l'IA ▪ SIEM et SOAR basés sur l'IA (ex : Splunk, Microsoft Sentinel) ▪ Threat Intelligence augmentée (analyse automatique des menaces et pattern d'attaque) ▪ Détection comportementale via l'IA (ex : UEBA - User and Entity Behavior Analytics) • Deepfakes et menaces liées à l'IA ▪ Attaques par Deepfake et IA Générative ▪ Poisoning Attacks (exploitation des modèles IA pour biaiser les résultats) ▪ Détection et contre-mesures	*Analyser les concepts fondamentaux de l'IA, en différenciant leur typologie, afin de comprendre leurs implications en cybersécurité* *Examiner les opportunités et risques de l'IA en cybersécurité, en identifiant les cas d'usage dans la détection des menaces, l'automatisation et la prédiction des attaques, afin d'évaluer leur pertinence* *Utiliser des outils d'IA pour la cybersécurité, en explorant IBM Watson for Cybersecurity, Splunk AI et Google Chronicle, afin d'expérimenter l'automatisation de l'analyse des menaces* *Différencier les approches supervisées et non supervisées du Machine Learning, en appliquant ces techniques à la détection des cyberattaques, afin d'identifier des menaces inconnues et des anomalies comportementales* *Modéliser des cyberattaques, en utilisant des algorithmes de classification Machine Learning, afin de développer des scénarios de détection avancée* *Implémenter des stratégies d'automatisation de la réponse aux incidents, en utilisant des outils SIEM et SOAR basés sur l'IA, afin de réduire le temps de réaction face aux cybermenaces* *Évaluer les risques des Deepfakes et des attaques par IA Générative, en étudiant leurs impacts sur la cybersécurité, afin de mettre en place des stratégies de protection adaptées* *Tester les attaques par Poisoning Attacks, en explorant les techniques de manipulation des modèles IA, afin de comprendre la manière dont les cybercriminels exploitent les biais des algorithmes*

4. Adaptation des stratégies de sécurité aux évolutions technologiques • Veille technologique et stratégies de cybersécurité ▪ Les méthodologies d'intégration des résultats de veille technologique dans des stratégies de sécurité d'entreprise ▪ Élaboration d'une stratégie de sécurité proactive et flexible, en fonction des tendances technologiques émergentes ▪ La mise à jour du plan de sécurité en fonction des résultats de la veille technologique et des nouveaux risques identifiés dans le cloud et les infrastructures IoT • Les outils de veille technologique ▪ Feedly, Google Alerts, RSS et les plateformes de vulnérabilités (CVE, MITRE ATT&CK) etc. ▪ Les bases de données : CVE, NVD (National Vulnerability Database), les rapports de cybersécurité (ENISA, OWASP etc.)	*Intégrer les résultats de veille technologique, en appliquant des méthodologies spécifiques, pour adapter les stratégies de sécurité d'entreprise face aux évolutions technologiques* *Élaborer une stratégie de sécurité proactive, en l'ajustant en fonction des tendances technologiques émergentes, pour renforcer la résilience des systèmes* *Mettre à jour le plan de sécurité, en l'adaptant aux résultats de la veille technologique et aux nouveaux risques identifiés dans le cloud et les infrastructures IoT, pour assurer une protection continue et efficace* *Utiliser des outils de veille technologique comme Feedly et Google Alerts, en les configurant efficacement, pour rester informé des menaces et vulnérabilités actuelles* *Consulter les bases de données de vulnérabilités, en analysant régulièrement les rapports de cybersécurité, pour anticiper et répondre aux nouvelles menaces*

B. Évaluation

Forme de l'épreuve : Épreuve professionnelle écrite (1h30) + étude de cas avancée en cybersécurité (2h30)
Durée : 4 h
Barème : notation sur 120

- Épreuve écrite - Théorie (20 points)
- Analyse d'un incident de cybersécurité (50 points)
- Mise en œuvre d'une stratégie de sécurité (50 points)

Matériel autorisé : calculatrice non programmable et documentation technique fournie (extraits de standards ISO/NIST)

C. Coefficient et ECTS

Ce module vaut coefficient **4** et permet de capitaliser **12 ECTS**

UC D32

Epreuve Professionnelle de Soutenance

A. Objectifs

La pédagogie doit faire une large place à l'initiative de l'apprenant et à son travail personnel pour mettre en œuvre les connaissances et les compétences acquises. À cette fin, les missions professionnelles effectuées en entreprise impliquent l'élaboration d'un rapport d'activité qui donne lieu à une soutenance orale.

Le Bachelor européen réalise une mise en contact réelle de l'apprenant avec le monde du travail de manière à lui permettre d'approfondir sa formation et son projet professionnel et de faciliter son insertion dans l'emploi.

Une partie de la formation peut être accomplie à l'étranger dans le cadre d'une convention.

B. Évaluation

L'épreuve professionnelle de soutenance permet de valider les capacités de l'apprenant à mener un projet professionnel, à développer une problématique dans un rapport d'activité et à expliquer et défendre sa démarche devant un jury.

En raison de l'intérêt qu'elle représente dans la formation de l'apprenant, cette épreuve est obligatoire.

1. Modalités de préparation

Quel que soit le pays d'exercice, l'élaboration du rapport d'activité peut s'appuyer sur différentes modalités d'expériences formatives :

- Soit un stage en entreprise ;
- Soit un emploi salarié ou un contrat d'alternance ;
- Soit des travaux plus théoriques par le biais d'un projet tutoré.

1.1. Le stage en entreprise

Durée : 12 semaines minimum.
Contenu : Réalisation d'une ou plusieurs actions liées à la cybersécurité et gestion des réseaux, donnant lieu à un rapport d'activité.

- Déploiement d'une infrastructure réseau sécurisée
- Mise en place et administration de serveurs sécurisés
- Gestion des incidents et réponse aux cyberattaques
- Audit de sécurité et conformité
- Maintenance et amélioration des systèmes
- Sensibilisation des utilisateurs à la cybersécurité
- Création et gestion de base de données sécurisées
- Supervision et monitoring des systèmes
- Développement et sécurisation d'applications Web

Capacités attendues : Appréhender les réalités d'une activité liée à la cybersécurité et gestion des réseaux.

- Autonomie dans le travail
- Aptitude à tenir à jours ses connaissances et à maîtriser les évolutions technologiques
- Capacité d'adaptation
- Capacité d'initiative
- Curiosité intellectuelle

Le stage doit se dérouler pendant la formation.

La date et la planification de ce stage sont laissées à la libre appréciation de l'établissement de formation, en accord avec sa propre organisation pédagogique.

Par exemple, le stage peut être scindé en 2 parties ou organisé selon un rythme hebdomadaire propre à l'alternance (n jours en école, n jours en entreprise).
Toutefois, il semble préférable, pour des motifs pédagogiques, que le stage ainsi scindé se déroule dans la même entreprise ou organisation.

Le terrain de stage doit être choisi en fonction des possibilités d'actions professionnelles de l'apprenant, et soumis à l'équipe pédagogique de l'école, qui en valide le bien-fondé et l'adéquation avec le diplôme préparé ainsi que le niveau exigé. Il peut s'agir d'une entreprise publique ou privée ou d'une organisation au sens large.

Ce stage donne l'occasion à l'apprenant de déterminer, en relation avec son tuteur en entreprise et, éventuellement, son tuteur-enseignant, les études, les actions ou les missions qui lui seront confiées et qui constitueront la matière de son rapport d'activité.

La production d'un certificat de fin de stage mentionnant la durée, les dates et les missions confiées par l'entreprise, sera exigé au moment de l'épreuve de soutenance.

1.2. L'alternance ou l'emploi salarié

La préparation du rapport d'activité peut également s'appuyer sur l'expérience professionnelle de l'apprenant, qu'il soit salarié à temps plein, à temps partiel ou en contrat d'alternance, pourvu que la nature de ses activités professionnelles et le niveau de ses responsabilités soient conformes aux spécificités et aux exigences du présent référentiel et des examens FEDE qui y sont rattachés.

Dans ce cas, ce sont les missions qui sont confiées au salarié qui deviennent la matière de son rapport d'activité.
La production d'un certificat de travail mentionnant la durée, les dates et, éventuellement les études ou missions confiées par l'entreprise, sera exigé au moment de l'épreuve de soutenance.

1.3. Le projet tutoré

En cas de difficulté majeure pour trouver un stage ou un contrat d'alternance en entreprise, l'apprenant a la possibilité de réaliser un projet tutoré en accord avec son centre de formation et la FEDE.

Dans ce cas, le projet de rapport d'activité est négocié et déterminé en début d'année en concertation avec l'équipe pédagogique et plus spécialement un tuteur-enseignant, qui aura pour rôle de superviser le projet et guider l'apprenant.

Toutefois, l'obtention d'un stage ou d'un contrat d'alternance en entreprise doit constituer la priorité.

Durée : ¼ du volume de la formation, hors stage
Contenu : Dans le cadre d'un travail individuel ou collectif, réalisation d'un rapport d'activité retraçant l'ensemble des actions menées pour la réalisation d'une opération liée à la cybersécurité et gestion des réseaux, définie en début d'année et validée par le tuteur enseignant.

- La mise en place d'une infrastructure sécurisée
- L'installation et l'administration de serveurs
- Le développement et sécurisation de sites Web
- La sensibilisation des utilisateurs à la cybersécurité
- La création et l'administration de bases de données
- La supervision et surveillance des réseaux
- La gestion proactive des incidents
- La réalisation d'un audit de sécurité et conformité

Capacités attendues : Mettre en œuvre une stratégie permettant la réalisation effective d'une action liée à la cybersécurité et gestion des réseaux

1.3.1. Contenu du projet

Dans la mesure du possible, ce projet aura une dimension européenne et sera élaboré en liaison avec une entreprise ou une organisation professionnelle où il pourrait trouver une application.

1.3.2. Rôle du tuteur

Le tuteur est un des enseignants de l'apprenant. En tant que tuteur, son rôle consiste à :

- Suggérer des idées de projet ou d'étude ;
- Valider le projet et négocier avec l'apprenant l'évolution du projet ;
- Orienter ses recherches bibliographiques et documentaires ;
- Fournir des pistes pour mettre en place des relations avec des entreprises ou des organisations professionnelles ;
- Surveiller la qualité d'ensemble du travail fourni ;
- Participer, le cas échéant au jury d'examen.

2. Le rapport d'activité

Ce rapport d'activité constitue une partie du travail évalué par le jury. En tant que tel, il est donc un objet d'évaluation et représente **30%** de la note finale.

2.1. Le contenu du rapport d'activité

Le rapport d'activité ne doit pas se résumer à un simple descriptif de l'activité de l'apprenant ou à un simple compte rendu de lecture.

Il doit représenter un effort de recherche, d'analyse et d'application concernant un aspect réel et bien délimité de l'activité d'une entreprise (entendue au sens large), dans un contexte économique européen si possible.

L'observation des pratiques de l'entreprise ou de l'organisation et/ou la lecture des ouvrages théoriques en relation avec le sujet doit permettre à l'apprenant de cerner une problématique relative à un contexte précis, et lui donner l'occasion de développer une analyse et des propositions concrètes qu'il doit être capable de justifier.

L'organisation du rapport d'activité est importante, il doit respecter une ordonnance classique, en abordant dans un ordre logique les différentes étapes de l'élaboration du projet, dont voici quelques exemples :

- Introduction ;
- La demande ou la commande ;
- La problématique ;
- L'idée de départ, le projet initial ;
- Les hypothèses de recherche ;
- Les résultats attendus ;
- La méthodologie utilisée ;
- Les arguments du projet, les propositions ;
- L'évaluation, la comparaison avec d'autres projets ;
- La confrontation avec la réalité, le terrain, les entreprises ;
- Les résultats éventuellement obtenus ;
- Les outils de contrôle éventuellement mis en place ;
- Les avantages apportés par le projet ou l'étude.

2.2. *Présentation du rapport d'activité*

Le rapport d'activité sera saisi au traitement de texte et présentera les caractéristiques suivantes :

- Format A4 ;
- Nombre de pages : environ 30 à 35 pages (hors annexes) ;
- Impression recto seul ;
- Marges 2,5 cm de chaque côté ;
- Interligne 1,5 ;

- Relié.

Le rapport peut contenir quelques annexes essentielles qui ne doivent pas dépasser un volume maximum de 10 feuilles A4.

La provenance de ces annexes doit être clairement indiquée (document élaboré par l'apprenant, tiré de telle publication, fourni par l'entreprise…).

La page de titre doit comporter les mentions suivantes :
- Nom et prénom de l'apprenant ;
- Numéro de candidat attribué par la FEDE ;
- Titre éventuel du rapport ;
- « Examens de la FEDE » ;
- « Rapport d'activité présenté à l'épreuve professionnelle de soutenance du diplôme visé de [année] ».

Il devra contenir un sommaire au début, une bibliographie à la fin et éventuellement une table des annexes.
Il sera exigé la même rigueur que pour les travaux universitaires en ce qui concerne la présentation des références, des citations, etc.
Il faut prévoir une édition en au moins deux exemplaires, un pour le jury, un pour l'apprenant.

2.3. Délai de fourniture du rapport d'activité

Les rapports d'activités doivent être envoyés en deux exemplaires au centre d'examen (pour transmission au jury) au moins 3 semaines avant le début de la période annoncée pour ce type d'épreuve.

3. Déroulement de la soutenance

Le jury est composé d'un enseignant de la spécialité auquel il est adjoint un professionnel. L'épreuve dure 30 minutes. Pas de temps de préparation.
La soutenance orale représente **70%** de la note finale.

3.1. Exposé théorique (de 10 à 15 min)

Dans un premier temps, le jury invitera l'apprenant à justifier le choix de son projet ou de son étude et à livrer les conclusions auxquelles il est parvenu.

Ce travail de soutenance ne doit pas conduire l'apprenant à « lire » son rapport devant le jury. Cette partie de l'épreuve est une évaluation des compétences de communication orale dans un contexte professionnel et technique.

L'apprenant s'efforcera donc de retracer, d'une manière construite et raisonnée, son cheminement dans le choix d'un sujet ou d'un projet, les difficultés qu'il a connues et comment il les a surmontées, la place que ce projet a prise par rapport à son projet professionnel global, l'intérêt qu'il a trouvé, le bénéfice qu'il a tiré d'un travail personnel d'élaboration et de recherche, les contacts qu'il a pu nouer à cette occasion avec des professionnels, des organisations, les suites qui seront éventuellement données…

Il devra savoir introduire et conclure son exposé, et maîtriser son temps de parole.

L'apprenant peut utiliser à sa guise des documents complémentaires qui ne sont pas dans le rapport d'activité remis au jury et qu'il aura apporté avec lui.

L'apprenant a aussi la possibilité d'utiliser les techniques de présentation qu'il juge utiles (par exemple : présentation assistée sur ordinateur…) pourvu qu'il soit autonome dans l'utilisation de ces outils et qu'il reste dans le temps imparti.

Pendant cet exposé de 10 à 15 minutes, l'apprenant ne sera pas interrompu.

3.2. Discussion avec le jury (15 à 20 min)

Dans un deuxième temps, le jury reviendra sur des aspects plus techniques ou professionnels, notamment sur le contenu du rapport d'activité, et posera les questions suscitées par la lecture de celui-ci.

Toutefois, s'agissant de la partie « soutenance orale » de l'épreuve, le jury évaluera moins la précision et la justesse des éléments de réponse technique fournis que la capacité de l'apprenant, à maîtriser la situation de communication, à comprendre et à traiter une objection, à organiser un discours, à convaincre…

4. Objectifs et critères d'évaluation

- Grille de notation
- Eléments observables

C. Règles d'utilisation de l'IA générative dans la rédaction du rapport d'activité

L'utilisation de l'IA générative (et des technologies assistées par l'IA) dans le processus de rédaction des rapports est autorisée, sous certaines conditions détaillées ci-dessous.

1. Les règles d'utilisation de l'IA dans la rédaction des travaux rédactionnels

En cas d'utilisation de l'IA dans le processus de rédaction par les candidats, trois règles prévalent et correspondent à trois principes, afin de garantir la possibilité d'une évaluation pertinente de la production personnelle du candidat : le respect des sources, la transparence et la responsabilité.

- Respecter les règles relatives au plagiat, à la copie et à la nécessité de citer les sources utilisées.
- Déclarer dans le manuscrit avoir utiliser l'IA dans le processus rédactionnel et indiquer quelles IA ont été utilisées et pour quel usage.
- Le candidat est ultimement responsable du contenu de son travail et des textes soumis pour évaluation. L'IA ne doit pas être citée comme auteur ou co-auteur.

2. L'IA et le risque de plagiat

Utiliser l'IA pour générer le texte du rapport d'activité est assimilé à du plagiat et peut être sanctionné par une disqualification.

Rappel des règles de base relatives au plagiat :

- L'auteur d'un texte doit citer ses sources sous peine de faire du plagiat et d'être disqualifié.
- La paraphrase sans citation de source est une autre forme de plagiat.
- Si le jury estime qu'il y a plagiat, paraphrase, copie d'un modèle sans apport original ou encore qu'il y a recours à un tiers de substitution, et que cela constitue un obstacle à l'évaluation objective des compétences, savoirs et savoir-faire d'un candidat, le jury est fondé à disqualifier le travail de l'étudiant.

3. L'IA et la transparence

Afin de permettre aux membres du jury d'évaluer de la façon la plus pertinente possible la production personnelle du candidat, celui-ci est tenu de déclarer, si c'est le cas, qu'il a eu recours à l'utilisation de l'intelligence artificielle dans la rédaction de son travail rédactionnel, en précisant : quel(s) outil(s), quel(s) usage(s), quelle(s) finalité(s).

4. L'IA et la responsabilité

L'IA ne doit pas être citée comme auteur ou co-auteur, la qualité d'auteur renvoyant à une personne physique. Le candidat est in fine l'auteur du rapport d'activité. Les candidats sont ainsi ultimement responsables du contenu de leur travail et des textes soumis pour évaluation.

D. Coefficient et ECTS

Ce module vaut coefficient **4** et permet de capitaliser **12 ECTS**.

UC D33

Contrôle continu – Projet de conception et déploiement d'une infrastructure réseau sécurisée

A. Objectifs

Les évaluations sous la forme du contrôle continu certificatif doivent être réalisées en cours de formation à la fin d'une séquence d'apprentissage et permettre l'évaluation de l'acquisition d'un groupe de compétences.
Ces évaluations nécessitent de s'appuyer sur des modalités provoquant des situations observables faisant appel à la mobilisation de diverses connaissances théoriques, de stratégies, de savoir-être et de savoir-faire. Elles doivent s'approcher de l'action et des situations de travail et traduire une mise en œuvre opérationnelle de plusieurs compétences liées à une activité et un métier en cohérence avec le niveau attendu. L'objectif est de valider au fur et à mesure l'acquisition des compétences avant les évaluations finales de la session d'examens FEDE.
De façon générale, l'UC D33 permet également de prendre en compte l'implication et l'assiduité de chaque apprenant dans la formation.

Le temps de travail requis pour mener à bien le contrôle continu est estimé à 80 heures. Cette activité évaluée doit être encadrée par un formateur, afin d'accompagner les groupes et orienter les apprenants dans leurs réflexions.

B. Évaluation

L'évaluation, réalisée sous forme d'un projet pratique en groupe de 3 ou 4, place les apprenants en situation professionnelle réaliste. Le sujet proposé les invite à concevoir, déployer et sécuriser une infrastructure réseau et système pour une PME fictive, en appliquant des stratégies de gestion des risques et des techniques de réponse aux incidents. Ce projet mobilise l'ensemble des connaissances théoriques, pratiques et techniques abordées dans la formation, notamment en administration des systèmes, sécurité des infrastructures, conformité réglementaire et gestion des crises cyber.
L'évaluation est progressive, avec plusieurs livrables intermédiaires (analyse des risques, implémentation technique, audit de conformité), et se clôture par une soutenance orale et une simulation de gestion d'incident cyber.

Phases/contenus	Livrables attendus	Compétences évaluées
Phase 1 : Analyse des risque et conception (8 à 10 h)		
• Identification des ressources critiques et du périmètre de sécurité • Analyse des menaces et des vulnérabilités avec CVSS et scans de vulnérabilités (Nessus, OpenVAS) • Cartographie des risques selon ISO 27005 (matrice des risques) • Définition des exigences de sécurité en fonction des réglementations applicables (RGPD, ISO 27001, NIS2)	**Rapport d'analyse des vulnérabilités**	*Identifier des menaces et vulnérabilités* *Analyser des risques et définir des stratégies de sécurité* *Respecter des cadres réglementaires*
Phase 2 : Mise en œuvre technique (10 à 12 h)		
• Configuration des équipements réseau (pare-feu, segmentation VLAN, IDS/IPS)	**Preuve de concept (PoC) de**	*Configurer des éléments de sécurité*

• Mise en place d'un système d'authentification et de gestion des accès (IAM, MFA, SSO) • Sécurisation des flux et données (VPN, TLS, chiffrement des bases de données) • Implémentation d'un SIEM (Splunk, ELK) pour la surveillance en temps réel	**sécurisation d'un SI**	*Gérer des accès et protection des données* *Mettre en place un monitoring efficace*
Phase 3 : Mise en œuvre technique (8 à 10 h)		
• Vérification de la conformité aux réglementations et standards (ISO 27001, SOC 2, RGPD) • Audit des configurations de sécurité (IAM, segmentation réseau, logs) • Tests de pénétration internes et correction des vulnérabilités • Rédaction du rapport d'audit avec recommandations et plan d'amélioration	**Audit de conformité et rapport de synthèse**	*Analyser la conformité et auditer des configurations* *Identifier des failles et procéder à leur remédiation* *Rédiger la documentation et réaliser un reporting*
Phase 4 : Soutenance et gestion de crise (6 à 8 h)		
• Présentation des choix techniques et justifications des décisions de sécurisation • Mise en situation d'une cyberattaque simulée et réaction des équipes • Élaboration d'un Cyber Incident Response Plan (CIRP) en temps réel • Débriefing et retour d'expérience post-incident	**Présentation du projet devant un jury et simulation de gestion de crise cyber**	*Justifier des décisions techniques* *Gérer efficacement un incident de cybersécurité* *Communiquer clairement avec des parties prenantes*

GLOSSAIRE TECHNIQUE

Termes	Définitions
IAM (Identity and Access Management)	*Système de gestion des accès basé sur les rôles pour protéger les ressources de l'organisation*
VPN (Virtual Private Network)	*Connexion sécurisée via Internet pour protéger les échanges de données*
DS/IPS (Intrusion Detection/Prevention System)	*Outils de détection et prévention d'intrusions dans le réseau*
CAGR (Compound Annual Growth Rate)	*Taux de croissance moyen annuel sur plusieurs années*
MFA (Multi-Factor Authentication)	*Authentification nécessitant plusieurs preuves d'identité (ex. : mot de passe, code)*
RBAC (Role-Based Access Control)	*Contrôle des accès basé sur les rôles pour limiter les permissions*
SIEM (Security Information and Event Management)	*Centralise les alertes et incidents pour les analyser*
PKI (Public Key Infrastructure)	*Infrastructure de gestion de certificats numériques pour sécuriser les échanges*
	Protocoles de cryptage des communications réseau

SSL/TLS (Secure Sockets Layer / Transport Layer Security)	*Sauvegardes de données permettant la récupération en cas d'incident*
Backups	*Méthode de cryptage avec clés publique et privée*
Cryptographie asymétrique	*Logiciel malveillant chiffrant les données pour exiger une rançon*
Ransomware	*Norme pour le système de gestion de la sécurité des informations*
ISO 27001	*Guide des vulnérabilités courantes en applications web*
OWASP (Open Web Application Security Project)	*Fichiers de journalisation pour suivre les activités des systèmes*
Logs	*Centre d'opérations pour la surveillance en temps réel des incidents*
SOC (Security Operations Center)	*Conversion de données en condensé fixe pour vérifier leur intégrité*
Hashing	*Sous-réseau virtuel pour segmenter le réseau*
VLAN (Virtual Local Area Network)	*Filtre le trafic pour protéger les systèmes des accès non autorisés*
Firewall (Pare-feu)	*Système simulé pour attirer et analyser les cyberattaques*
Honeypot	

C. Livrables

1. **Rapport d'analyse des vulnérabilités (Note de groupe : 20 points)**
   1.1. Fond
   - Identification des ressources critiques (systèmes, réseaux, applications)
   - Cartographie des risques selon ISO 27005 (menaces, vulnérabilités, impact)
   - Scans de vulnérabilités et analyse CVSS (exploitation des résultats de Nessus, OpenVAS)
   - Définition des exigences de sécurité (en lien avec RGPD, ISO 27001, NIS2)
   - Recommandations initiales pour la sécurisation

   1.2. Forme
   - Rapport écrit structuré au format PDF
   - Taille : 15 pages maximum (hors annexes)
   - Structure professionnelle avec :
     - Une introduction et périmètre de l'analyse
     - Une cartographie des risques
     - Les résultats des scans de vulnérabilités
     - L'évaluation des impacts et recommandations
     - Une conclusion et des annexes (rapports de scan, CVSS scoring)
   - Schémas et graphiques obligatoires pour la cartographie des risques et le scoring CVSS

2. **Preuve de concept (PoC) de sécurisation d'un SI (Note de groupe : 20 points)**
   2.1. Fond
   - Configuration des équipements réseau (pare-feu, VLAN, segmentation, ACL)
   - Sécurisation des accès (IAM, MFA, SSO, gestion des rôles)
   - Implémentation d'un SIEM (Splunk, ELK Stack) et configuration des logs
   - Tests de fonctionnement et validation des mesures de sécurité

   2.2. Forme
   - Format : Code source et configurations réseau + rapport technique au format PDF
   - Taille du rapport : 10 pages maximum
   - Contenu du rapport :

- Présentation des solutions mises en place
- Captures d'écran des configurations et logs
- Explications des choix techniques
- Résultats des tests de validation (ex : logs de connexion, trafic bloqué par firewall etc.)

➢ Dépôt Git recommandé pour le scripts d'automatisation et les fichiers de configuration

3. Audit de conformité et rapport final (Note de groupe : 20 points)

3.1. Fond

➢ Audit de conformité aux standards ISO 27001, NIS2, SOC 2
➢ Évaluation de la sécurité IAM, segmentation réseau, logs SIEM
➢ Tests de pénétration internes et correction des vulnérabilités
➢ Plan d'amélioration et recommandations finales

3.2. Forme

➢ Rapport écrit au format PDF avec les annexes techniques
➢ Taille : 12 pages maximum
➢ Structure recommandée :
- Résumé des points conformes et non conformes
- Analyse des failles et mesures correctives
- Comparaison avec les standards ISO/NIS2
- Plan d'amélioration recommandé
- Annexes : Résultats des audits techniques

4. **Dossier de présentation orale et gestion de crise (Note individuelle : 20 points)**

4.1. Fond

➢ Présentation du projet et justification des choix techniques
➢ Scénario de cyberattaque simulée et réaction des équipes
➢ Élaboration d'un plan de réponse aux incidents (CIRP)
➢ Retour d'expérience et axes d'amélioration

4.2. Forme

➢ Durée : 20 minutes de présentation orale + 10 minutes de questions et d'échange avec le jury
➢ Contenu du support :
- Contexte du projet et objectifs
- Démonstration des solutions mises en place
- Analyse du scénario de cyberattaque et réaction
- Plan de réponse aux incidents et lessons learned

➢ Mise en situation réelle avec présentation d'une simulation de crise et réponse du groupe

D. Grilles de notation

Dans le cadre de ces évaluations en contrôle continu, et pour chaque candidat, voici le dossier candidat et les grilles de notations à utiliser obligatoirement : Dossier candidat / D33 / Contrôle continu / Cybersécurité et gestion des réseaux

E. Coefficient et ECTS

Ce module vaut coefficient **2** et permet de capitaliser **8 ECTS**.

UE B | Langue Vivante Européenne

UC B31

Langue Vivante Européenne 1
Utilisateur indépendant – Niveau B1 du CECR

Le référentiel de cette unité d'enseignement est commun pour toutes les langues vivantes, qu'il s'agisse d'une langue vivante 1 (UC B31), langue vivante 2 (UC B32) ou langue vivante 3 (UC B33).

Les apprenants ont la possibilité de choisir parmi les langues vivantes suivantes :
- **Langue vivante 1** : Allemand, Anglais, Espagnol, Français, Italien, Portugais ;
- **Langues vivantes 2 et 3 (facultatives)** : Allemand, Anglais, Arabe, Chinois, Espagnol, Français, Italien, Portugais

La langue vivante choisie par l'apprenant doit être différente de celle dans laquelle il passe les épreuves de la Culture et citoyenneté européennes et du domaine professionnel.

A. Objectif

Atteindre le niveau B1 du Cadre européen commun de référence pour les langues (CECR) en compréhension écrite et orale, production écrite et orale, interaction et médiation.

B. Formation

Le volume horaire recommandé de formation en face à face pédagogique est de 60 à 80 heures.

Utilisateur Indépendant, Niveau B1 du Cadre Européen Commun de Référence du Conseil de l'Europe

Écouter	Je peux comprendre les points essentiels quand un langage clair et standard est utilisé et s'il s'agit de sujets familiers concernant le travail, l'école, les loisirs… Je peux comprendre l'essentiel de nombreuses émissions de radio ou de télévision sur l'actualité ou sur des sujets qui m'intéressent à titre personnel ou professionnel si l'on parle d'une façon relativement lente et distincte.
Lire	Je peux comprendre des textes rédigés essentiellement dans une langue courante ou relative à mon travail. Je peux comprendre la description d'événements, l'expression de sentiments et de souhaits dans des lettres personnelles.
Prendre part à une conversation	Je peux faire face à la majorité des situations que l'on peut rencontrer au cours d'un voyage dans une région où la langue est parlée. Je peux prendre part sans préparation à une conversation sur des sujets familiers ou d'intérêt personnel ou qui concernent la vie quotidienne (par exemple famille, loisirs, travail, voyage et actualité).
S'exprimer oralement en continu	Je peux m'exprimer de manière simple afin de raconter des expériences et des événements, mes rêves, mes espoirs ou mes buts. Je peux brièvement donner les raisons et explications de mes opinions ou projets. Je peux raconter une histoire ou l'intrigue d'un livre ou d'un film et exprimer mes réactions.
Écrire	Je peux écrire un texte simple et cohérent sur des sujets familiers ou qui m'intéressent personnellement. Je peux écrire des lettres personnelles pour décrire expériences et impressions.

Médiation	Je peux transmettre les points essentiels de contenus clairs sur des sujets familiers ou d'intérêt personnel. Je peux relayer, dans une langue simple, les informations principales d'un document ou d'une discussion.

C. Ressources pédagogiques mises à la disposition des apprenants par la FEDE

Afin de permettre aux apprenants de s'entraîner sur ce module, la FEDE met à la disposition des écoles et des apprenants des annales d'évaluation (sujets et corrigés).

D. Évaluation

UC B31.1 – Langue Vivante Européenne 1 (Epreuve écrite)

Nota : Aucun document, support de cours ni outil complémentaire (outil d'intelligence artificielle, calculatrice, dictionnaire, etc.) n'est autorisé durant cette évaluation.

Durée : 1 heure

1. Compréhension écrite

Étude de deux textes de 250 à 300 mots chacun, portant sur des thèmes listés par la FEDE. Pour chaque texte, quatre questions sont posées à l'apprenant sous la forme d'un questionnaire à choix multiple.

Parmi les quatre réponses proposées pour chaque question, une seule est correcte.

Objectifs : évaluer la compréhension générale et la capacité à repérer des informations spécifiques ainsi qu'à saisir la logique d'ensemble d'un texte écrit.
Barème : 3 points pour une bonne réponse, 0 pour non-réponse ou réponse erronée.

2. Compétences lexicales et grammaticales en contexte

Questionnaire à choix multiple portant sur l'usage du lexique et de la grammaire en contexte, à partir des textes de compréhension et/ou des thèmes du programme.
L'apprenant répond à seize questions ; parmi les quatre réponses proposées pour chaque question, une seule est correcte.
Objectifs : évaluer la connaissance d'un vocabulaire varié et des structures grammaticales de base, ainsi que la capacité à comprendre le sens d'un énoncé et à sélectionner l'élément linguistique approprié en fonction du contexte.
Barème : 3 points pour une bonne réponse, 0 pour non-réponse ou réponse erronée.

3. Production écrite

Rédaction d'un courrier (lettre, fax, mail ou mémo) dans la langue vivante choisie par l'apprenant à partir d'un canevas fourni dans cette même langue étrangère, éventuellement en réaction à un document fourni dans l'énoncé (publicité, offre d'emploi, courrier).

Nombre de mots : 150 à 200.

Objectifs : évaluer la capacité à rédiger un texte simple et cohérent en fonction d'un contexte donné, à demander ou fournir des informations, à décrire des expériences, à exprimer des sentiments ou impressions et à présenter brièvement une opinion ou une explication.

La présentation ne fera pas l'objet d'une notation spécifique, mais peut être prise en compte pour affiner l'évaluation.

La production écrite est évaluée à partir des critères FEDE correspondant au niveau B1 du Cadre européen commun de référence pour les langues (CECR).

Barème :

Compréhension écrite (8 questions x 3) : 24 points
Compétences lexicales et grammaticales en contexte (16 questions × 3) : 48 points
Production écrite : 28 points
Total : **100 points**

UC B31.2 – Langue Vivante Européenne 1 (Epreuve orale)

L'épreuve orale vise à évaluer la capacité de l'apprenant à comprendre, produire, interagir et assurer une médiation simple dans des situations de communication relevant du niveau B1 du CECR.

Nota : Aucun document, support de cours ni outil complémentaire (outil d'intelligence artificielle, calculatrice, dictionnaire, etc.) n'est autorisé durant cette évaluation.

Durée totale de l'épreuve orale : 40 minutes (préparation comprise).

1. **Présentation et commentaire à partir d'un document iconographique (préparation : 10 min ; passation : environ 10 min)**

Objectif : évaluer la capacité de l'apprenant à présenter et commenter un document visuel de manière organisée, à en dégager les informations essentielles, à exprimer un point de vue simple et à interagir avec l'examinateur.

- **Préparation (10 min)**

L'apprenant tire au sort un document iconographique parmi un choix de 6 à 12 documents et prépare une présentation et un commentaire en réaction à ce document.
Le document iconographique est une photographie, un dessin, un graphique ou un montage de plusieurs de ces éléments portant sur les thèmes du référentiel et des sujets d'actualité s'y rapportant.
L'apprenant peut prendre des notes, mais uniquement comme support d'oral ; toute lecture mot à mot sera pénalisée.
L'apprenant est amené à identifier le message principal du document et à en proposer une interprétation simple.

- **Présentation et commentaire par l'apprenant du document iconographique (4-5 min)**

L'examinateur laisse à l'apprenant le temps de s'exprimer afin d'évaluer la structuration du discours et la clarté de l'expression.
Présentation et commentaire par l'apprenant du document iconographique.
L'examinateur doit laisser à l'apprenant le temps de s'exprimer seul afin de juger de la logique du discours.

- **Discussion sur le document (4-5 min)**

Entretien entre l'examinateur et l'apprenant sur le document, permettant à ce dernier d'expliquer ses idées, de justifier brièvement son point de vue et d'illustrer ses propos.

2. **Compréhension et médiation orales (durée indicative : environ 12 minutes)**

L'examinateur lit à l'apprenant un texte clair et structuré d'environ 250 à 300 mots, portant sur les thèmes du référentiel et des sujets d'actualité s'y rapportant. L'apprenant répond à huit questions de compréhension orale.
Le texte est lu une première fois intégralement afin que l'apprenant en saisisse le sens général. Il est ensuite relu par segments ; après chaque segment, l'examinateur pose la question correspondante. Si nécessaire, le passage concerné peut être relu une fois.
La prise de notes est autorisée ; elle sert de soutien à la compréhension et à la formulation des réponses, et non à la mémorisation stricte.
Cet exercice permet d'évaluer la capacité à comprendre les informations principales et secondaires d'un message oral et à en restituer le sens de manière simple.

3. Entretien

Entretien portant sur le parcours de formation, la spécialité professionnelle de l'apprenant (expérience acquise ou en cours, projet tutoré, spécialisation présente et future), ainsi que sur des aspects de sa vie quotidienne ou de ses centres d'intérêt.
L'examinateur pose des questions et propose des relances permettant à l'apprenant de donner des informations, de décrire des expériences, d'exprimer et de justifier brièvement ses opinions.

Liste des thèmes de l'épreuve de Langue Vivante

Pour le niveau B1, les supports proposés sont adaptés aux capacités des apprenants et mobilisent un lexique courant et spécifique simple, en lien avec des situations de la vie quotidienne, académique ou professionnelle. Ils peuvent faire appel à des contenus comportant une dimension descriptive ou explicative et inviter à exprimer un point de vue ou à justifier brièvement une opinion, sans nécessiter de traitement conceptuel complexe.

- L'Europe et la citoyenneté
  - La citoyenneté européenne et mondiale ;
  - Les droits humains et les valeurs démocratiques ;
  - Les enjeux et débats politiques, sociaux et économiques actuels en Europe ;
  - La participation civique et l'engagement citoyen.

- Le monde du travail
  - Relations humaines au travail ;
  - Organisation du travail : temps, formation, mobilité, conflits, équilibre vie privée/vie professionnelle ;
  - Évolutions sociales et professionnelles en Europe ;
  - Orientation, éducation et apprentissage tout au long de la vie.

- Économie et société
  - Les enjeux économiques du quotidien (consommation, emploi, innovation) ;
  - La mondialisation et ses impacts sociaux, culturels et environnementaux ;
  - Développement durable et responsabilité sociétale.

- Vie professionnelle
  - Communication professionnelle écrite (lettres, courriels, messages) ;
  - Offres d'emploi et candidatures ;
  - Communication pratique : téléphone, visioconférence, outils numériques etc.

- Communication
  - Publicité, médias et communication publique ;
  - Nouveaux outils technologiques et réseaux sociaux ;
  - Médias et information : esprit critique, fake news, influence des médias ;
  - Citoyenneté numérique et responsabilité en ligne.

- Arts, culture et patrimoine
  - Histoire, civilisations et sociétés ;
  - Diversité culturelle et dialogue interculturel ;
  - Expressions culturelles et artistiques.

- Sujets d'actualité
  - Enjeux européens et internationaux ;
  - Société et citoyenneté : environnement, santé, inclusion, égalité ;
  - Coopération et gestion des conflits dans la société.

L'évaluation est réalisée à partir d'une grille critériée conforme aux descripteurs du niveau B2 du Cadre Européen Commun de Référence pour les Langues (CECR).

Elle porte sur les capacités suivantes :

- compréhension de messages clairs portant sur des sujets familiers ou liés au domaine d'études ou professionnel ;
- capacité à s'exprimer et à interagir à l'oral de manière simple mais organisée, en développant des réponses et en exprimant un point de vue ;
- médiation orale simple (reformulation ou transmission des informations principales d'un message ou d'un document) ;
- correction linguistique globale permettant une communication efficace malgré certaines erreurs
- prononciation, aisance et intelligibilité du discours ;
- organisation et cohérence du discours.

E. Grilles d'évaluation

Le détail des critères et des niveaux de maîtrise figure dans les grilles officielles d'évaluation :
UC B3.1- Grille de notation - Niveau B1 du CECR
UC B3.2- Grille de notation - Niveau B1 du CECR

F. Coefficient et ECTS

L'épreuve écrite UC B31.1 vaut coefficient 2 et permet de capitaliser 6 ECTS.

L'épreuve orale UC B31.2 vaut coefficient 2 et permet de capitaliser 6 ECTS.

UE A | Culture et Citoyenneté Européennes

UC A2

Le projet européen : culture et démocratie pour une citoyenneté en action

A. Objectifs

- Analyser l'étude de l'histoire et sa relation avec la culture, la démocratie et la citoyenneté ;
- Comprendre le modèle européen et ses particularités, aux plans historique et culturel ;
- Développer une compréhension critique de la politique, du droit et des droits humains ;
- Développer une connaissance et une compréhension critique de la culture, des cultures, et des religions ;
- Acquérir des connaissances précises sur les institutions européennes et leur fonctionnement ;
- Comprendre le modèle européen d'un point de vue réglementaire et juridique ;
- Mobiliser des outils de compréhension de l'espace européen et des actualités européennes ;
- Acquérir des compétences liées à la culture de la démocratie et au dialogue multiculturel.

B. Formation

Le volume horaire recommandé de formation en face à face pédagogique est de 20 à 25 heures.

Contenu	Capacités attendues
Module d'introduction : Importance de l'histoire	OBSERVATOIRE DE L'ENSEIGNEMENT DE L'HISTOIRE EN EUROPE — **OHTE Conseil de l'Europe**
• La discipline de l'histoire et les concepts de la pensée historique : o Causes et conséquences o Continuité et changement o Pertinence historique o Perspective historique o Sources o La dimension éthique • La relation entre l'étude de l'histoire et la démocratie contemporaine • La pertinence de la pensée et de la compréhension historiques dans le présent et l'avenir	*Souligner les aspects clés, les objectifs et les défis de la discipline de l'histoire* *Décrire les six concepts de la pensée historique* *Utiliser les concepts de la pensée historique pour analyser des événements historiques, des périodes et/ou des individus* *Décrire les liens entre l'étude de l'histoire et la démocratie contemporaine* *Reconnaitre la pertinence de la pensée historique et de la compréhension de l'histoire pour le présent et l'avenir*
Chapitre 1 : L'Europe Actuelle	
• La naissance de l'unité européenne et les prémices de la construction européenne • Les organisations (Conseil de l'Europe, UE, OSCE, AELE, EEE, OECD) • Une Europe multiple (espaces européens, adhésion/appartenance) • Le Conseil de l'Europe	*Analyser le processus de la construction européenne et le processus d'intégration* *Décrire le processus d'adhésion* *Reconnaitre la multiplicité des organisations sur le continent européen et leur géographie variable* *Expliquer le rôle des valeurs communes de la démocratie, de la primauté du droit et du respect des droits de*

○ L'origine et les valeurs du Conseil de l'Europe ○ La structure et les membres ○ L'histoire : faits marquants ○ Champs d'intervention ○ OING	*l'homme au sein du Conseil de l'Europe en tant qu'organisation* *Décrire la structure, le fonctionnement et les champs d'action du Conseil de l'Europe*
Chapitre 2 : L'Europe et le monde	
• Élimination des frontières intérieures • Gestion des frontières extérieures • Espaces transfrontaliers • Frontières et crises • La politique étrangère commune et la politique de sécurité et défense de l'Union européenne ○ Le rôle de l'OTAN • L'Union européenne et ses frontières ○ La Politique Etrangère et de Sécurité Commune ○ La Politique Européenne de Voisinage • L'Union européenne et le monde : ○ Focus sur l'Afrique • Enjeux de la politique commerciale • Les organisations internationales : ○ L'ONU et ses institutions (OMS, Unesco, OIT, FAO) ○ Organisations à caractère économique (OMC, FMI, Banque mondiale) ○ Cours internationales (CIJ, Cour Pénale internationale) ○ Alliances de défense (OTAN)	*Identifier les différents types de frontières définissant l'espace européen* *Décrire la coopération transfrontalière et ses espaces* *Expliquer le contexte géopolitique européen* *Mener une réflexion critique sur les évènements actuels concernant la politique étrangère de l'Union européenne* *Analyser les relations entre l'Union européenne et le monde* *Décrire l'ordre international et le multilatéralisme* *Décrire la multiplicité des organisations internationales* *Identifier des exemples des champs d'intervention des organisations internationales*
Chapitre 3 : Cultures et diversité en Europe	
• La diversité des religions en Europe • La liberté de pensée, de conscience et de religion en Europe : limites et enjeux • Minorités et lutte contre les discriminations en Europe • Les mouvements de migration récents et les principaux instruments d'accueil des migrants	*Définir les critères de discrimination et reconnaître les faits de discrimination* *Décrire les réglementations introduites par les institutions européennes en ce qui concerne les minorités et la discrimination et expliquer comment elles sont appliquées* *Mettre à profit le dialogue interculturel pour faciliter la reconnaissance de différentes identités et appartenances culturelles*

Chapitre 4 : La citoyenneté européenne	
• La Charte des droits fondamentaux de l'Union européenne • La libre circulation et les droits liés à la citoyenneté européenne • Démocratie et participation citoyenne dans l'UE • Conférence sur l'avenir de l'Europe et suites institutionnelles	*Identifier les concepts politiques et juridiques de base de la citoyenneté* *Mener une réflexion critique sur les droits humains en tant que cadre de valeurs européennes* *Expliquer les différentes façons dont les citoyens peuvent influencer les politiques*
Chapitre 5 : Le fonctionnement de l'Union européenne	
• L'Union européenne, ses institutions et leur fonctionnement ○ L'origine de l'UE ○ L'histoire : faits marquants ○ La structure institutionnelle ○ La procédure législative ordinaire ○ Les compétences et les actes de l'UE ○ Gouvernance multiniveau ○ Le contrôle par les juges (UE et juges nationaux) • Les actions de l'Union européenne ○ Les compétences exclusives (douanes, Euro) ○ Les compétences partagées (PAC, Politiques régionales, énergie, climat, transports) ○ Les compétences d'appui (éducation, santé, protection civile)	*Identifier les grands principes de fonctionnement des institutions européennes* *Décrire les modalités de la prise de décision dans l'UE* *Identifier la participation des institutions et organes de l'UE dans la vie des citoyens européens* *Analyser le champ d'action de l'Union Européenne* *Montrer la répartition des compétences entre l'UE et ses États membres* *Appréhender les règles fondamentales de mise œuvre des politiques européennes et leur impact sur la vie des citoyens européens*
Chapitre 6 : Enjeux, défis et avenir de la construction européenne	
• La souveraineté européenne • La transition écologique • La Boussole stratégique • Les débats sur l'Europe (euroscepticisme, genre, inclusion, participation) • L'avenir de l'UE dans le monde (Ukraine, Russie, Chine, US)	*Mener une réflexion critique sur l'actualité européenne depuis différentes perspectives en prenant en compte les facteurs historiques qui ont façonné le monde contemporain* *Mesurer les enjeux et défis européens et mondiaux (immigration, populisme, pandémie, guerres...) pour mieux cerner les desseins à venir de la construction européenne* *Réfléchir de manière critique aux différentes possibilités pour l'avenir de l'Europe*

Chapitre 7 : Focus sur la corruption	GRECO Groupe d'Etats contre la corruption Conseil de l'Europe
• Définir la corruption • Les différentes formes de corruption • Cartographier et mesurer la corruption • Les causes de la corruption • Endiguer la corruption • Les standards internationaux de lutte contre la corruption	*Appréhender les conséquences de la corruption* *Définir les termes spécifiques du vocabulaire de la lutte contre la corruption* *Distinguer les moyens de lutte contre la corruption, en aval et en amont* *Appréhender les enjeux de la dimension internationale de la lutte contre la corruption*

C. Ressources pédagogiques mises à la disposition des apprenants par la FEDE

La FEDE met à la disposition des écoles et des apprenants :
- Des fiches thématiques comportant des outils d'auto-évaluation pour se préparer à l'épreuve
- Des annales d'évaluation (sujets et corrigés).

D. Évaluation

Forme de l'épreuve : Questionnaire à Choix Multiples (QCM) en ligne
Durée : 40 minutes
Nombre de questions : 40 questions
Nombre de propositions : 2 à 4 propositions de réponses par question. Une seule proposition est exacte.
Total de points : 120

Le barème de notation est le suivant :
- **+ 3 points par bonne réponse**
- **0 point par réponse erronée**
- **0 point par non-réponse**

Aucun document, support de cours ou outil complémentaire (outil d'intelligence artificielle, calculatrice, dictionnaire, etc.) n'est autorisé durant cette évaluation.

NB : Formation en présentiel : heures d'enseignement réparties selon l'organisation propre à chaque établissement, à la spécialité du diplôme préparé et à la zone géographique du lieu de formation.

E. Coefficient et ECTS

Ce module vaut coefficient 1 et permet de capitaliser 3 ECTS.

UC A3

Le management interculturel et les ressources humaines

A. Objectifs

- Valoriser la diversité culturelle et s'appuyer sur le dialogue interculturel afin de développer une culture du « vivre ensemble » ;
- Développer l'altérité culturelle et la capacité d'interagir et travailler avec des personnes ayant des valeurs, des habitudes, des comportements et des références culturelles différents des siens ;
- S'approprier certains codes culturels afin de comprendre leurs impacts dans les relations interpersonnelles ;
- Mener une réflexion critique sur les différentes conventions de communication appliquées dans un autre groupe social ou une autre culture ;
- Mesurer l'impact de la culture dans la gestion des ressources humaines et participer à l'adaptation et mise en œuvre des pratiques de management interculturel et gestion des ressources humaines ;
- Accompagner et favoriser la mobilité des professionnels afin de leur permettre d'évoluer dans un contexte international.

B. Formation

Le volume horaire recommandé de formation en face à face pédagogique est de 20 à 25 heures.

Contenu	Capacités attendues
Partie 1 : Le management interculturel en Europe	
Chapitre 1 : Culture et diversité culturelle	
• Compréhensions de la culture ○ Bases ethnique, linguistique et religieuse ○ Fondements économiques, technologiques et politiques ○ Culture et style de vie ○ Éducation et culture • Langue et culture ○ La diversité linguistique ○ Plurilinguisme et multiculturalisme • Le multiperspectivisme ○ Définition et enjeux du multiperspectivisime ○ Approches pour reconnaître et prendre en compte les différentes perspectives, expériences et valeurs des individus dans une organisation	*Comprendre que la diversité culturelle au sein d'une société doit être perçue positivement et valorisée* *Analyser l'origine des cultures pour comprendre leur impact sur les valeurs fondamentales de l'individu et leur relation avec le comportement au travail* *Comprendre que le dialogue interculturel doit être mis à profit pour faciliter la reconnaissance de nos différentes identités et appartenances culturelles* *Distinguer l'approche multiperspectiviste dans le contexte de la gestion interculturelle au sein d'une organisation*
Chapitre 2 : La communication interculturelle dans une organisation	
• Valeurs et dimensions culturelles • La culture organisationnelle ○ La construction des valeurs de l'entreprise ○ La communication interculturelle	*Reconnaitre les enjeux liés à la construction des valeurs de l'entreprise et leur impact sur les individus et l'organisation*

• Ethnorelativisme • Conseils et outils pour une communication interculturelle efficace	*Définir différents styles de communication et faciliter la communication entre des personnes d'origines culturelles différentes* *Mener une réflexion critique sur les effets des différents styles d'utilisation de la langue dans des situations sociales et professionnelles*
Chapitre 3 : Gérer l'interculturel et résoudre des conflits culturels	
• Comment gérer et travailler dans une équipe multiculturelle ○ Diversité ethnique ○ Diversité linguistique ○ Les discriminations • Culture générationnelle ○ Les différences générationnelles ○ Création et gestion d'équipes transgénérationnelles • Culture européenne ○ L'identité européenne : identité historique collective et identités locales • La résolution des conflits culturels ○ Méthodes et cas particuliers	*Distinguer les modes de pensée et la langue des générations pour réunir des équipes multigénérationnelles autour d'un projet commun* *Reconnaître la diversité des influences au sein d'une équipe et percevoir les effets de la diversité culturelle* *Analyser les filtres culturels et les intégrer dans la gestion des équipes* *Communiquer et appréhender les différences culturelles en Europe pour construire dans la diversité une pensée convergente* *Instaurer régulièrement la communication pour contribuer à résoudre des conflits interpersonnels* *Acquérir des outils pour prévenir et gérer les conflits interculturels de manière efficace*
Partie II : Les ressources humaines en Europe	
Chapitre 4 : Travailler en Europe	
• L'Union européenne et la stratégie européenne pour l'emploi ○ La Stratégie décennale de l'UE en faveur des droits des personnes en situation de handicap • L'Union européenne et le droit du travail ○ La durée du travail en Europe ○ Les contrats de travail ○ Les salaires en Europe ○ Disparités salariales ○ Charges sociales et coût du travail ○ Santé et sécurité au travail ○ Protection contre les discriminations • L'immigration professionnelle et les espaces européens ○ L'Espace économique européen ○ L'Union européenne ○ L'espace Schengen	*Identifier les institutions européennes impliquées dans l'élaboration du droit européen du travail* *Connaître les sources principales du droit européen du travail* *Distinguer les relations en droit national et droit européen du travail* *Reconnaitre les principaux objectifs et orientations de l'Union européenne en matière de droit du travail* *Distinguer les textes du Conseil de l'Europe et de l'Union européenne en matière de droit du travail* *Mener une veille réglementaire* *Définir la libre circulation des travailleurs et des citoyens de l'UE et expliquer ses implications*

○ Intégration des migrants originaires de pays non-membres de l'UE •Mobilité professionnelle vers et en Europe : les différents statuts ○ Types de contrats de travail ○ Les principaux éléments d'un contrat de travail • Recrutement en Europe ○ Types de recrutement et contraintes juridiques	*Distinguer les conditions d'immigration d'un citoyen européen de celles d'un ressortissant non européen* *Différencier les différents statuts de la mobilité professionnelle* *Expliquer l'action de l'UE en faveur de la mobilité professionnelle* *Choisir et utiliser les outils et les plateformes européennes de recrutement*
Chapitre 5 : Les systèmes de protection sociale en Europe	
Introduction : L'influence des conventions internationales à portée universelle sur la protection sociale en Europe • Le Conseil de l'Europe et la mobilité des travailleurs ○ Charte sociale européenne (1961) ○ Code européen de sécurité sociale (1964) ○ Les conventions bilatérales et multilatérales de sécurité sociale entre États • La sécurité sociale en Europe : ○ Carte européenne d'assurance maladie ○ Les tendances actuelles en matière de sécurité sociale en Europe ○ Nouveaux défis ○ Variables d'ajustement	*Illustrer les enjeux culturels de la protection sociale en Europe* *Distinguer et respecter les règles de la protection sociale applicables au sein des différents pays d'Europe pour faciliter la mobilité professionnelle et protéger les salariés* *Identifier les possibilités de liaison entre régimes des différents pays de l'UE pour renforcer l'ouverture à l'internationale de l'entreprise* *Comprendre le fonctionnement général des différentes branches de protection sociale dans les pays de l'UE* *Mettre en place un système de veille des évolutions en matière de règles de la protection sociale en Europe*
Chapitre 6 : La responsabilité sociétale des entreprises (RSE)	
• LA RSE : définition et enjeux ○ Des origines au concept : entre volontarisme et obligation ○ Définition de la RSE : entre enjeux sociaux et sociétaux • Le périmètre de la RSE ○ Lignes directrices ○ La notion de parties prenantes et de sphère d'influence ○ Le principe de transparence et son corollaire ○ La RSE et les institutions européennes • La question sociale au cœur de l'entreprise : les textes de références de la RSE ○ RSE et RH, prise en compte des risques psychosociaux et de la Qualité de vie au travail (QVT-QVCT) ○ Respect des Droits humains et lutte contre les discriminations : Devoir de vigilance et	*Expliquer les bases conceptuelles et courants de pensée à l'origine de la RSE et appréhender l'écosystème de la RSE* *Distinguer les opportunités et les risques d'une démarche RSE* *Décrire les enjeux liés à la RSE en Europe et les envisager comme des leviers d'action pour renforcer l'entreprise* *Illustrer de quelle manière la RSE impacte la gestion des ressources humaines dans un contexte européen* *Participer au développement d'une politique RH et RSE en entreprise*

prise en compte de la chaîne d'approvisionnement • Politiques d'inclusion ○ Enjeux des politiques de gestion de la diversité ○ Enjeux et des défis liés à l'égalité hommes-femmes (diversité et performance) ○ Le harcèlement en entreprise ○ Les politiques LGBTQIA+ • Politiques d'inclusion des personnes en situation de handicap	*Analyser des enjeux liés à la diversité et à l'inclusion en milieu professionnel et les enjeux des politiques de gestion de la diversité* *Participer au développement des solutions pour favoriser l'inclusion des personnes en situation de handicap*

C. Ressources pédagogiques mises à la disposition des apprenants par la FEDE

La FEDE met à la disposition des écoles et des apprenants :
- Des fiches thématiques comportant des outils d'auto-évaluation pour se préparer à l'épreuve
- Des annales d'évaluation (sujets et corrigés).

D. Évaluation

Forme de l'épreuve : Questionnaire à Choix Multiples (QCM) en ligne
Durée : 40 minutes
Nombre de questions : 40 questions
Nombre de propositions : 2 à 4 propositions de réponses par question. Une seule proposition est exacte.
Total de points : 120

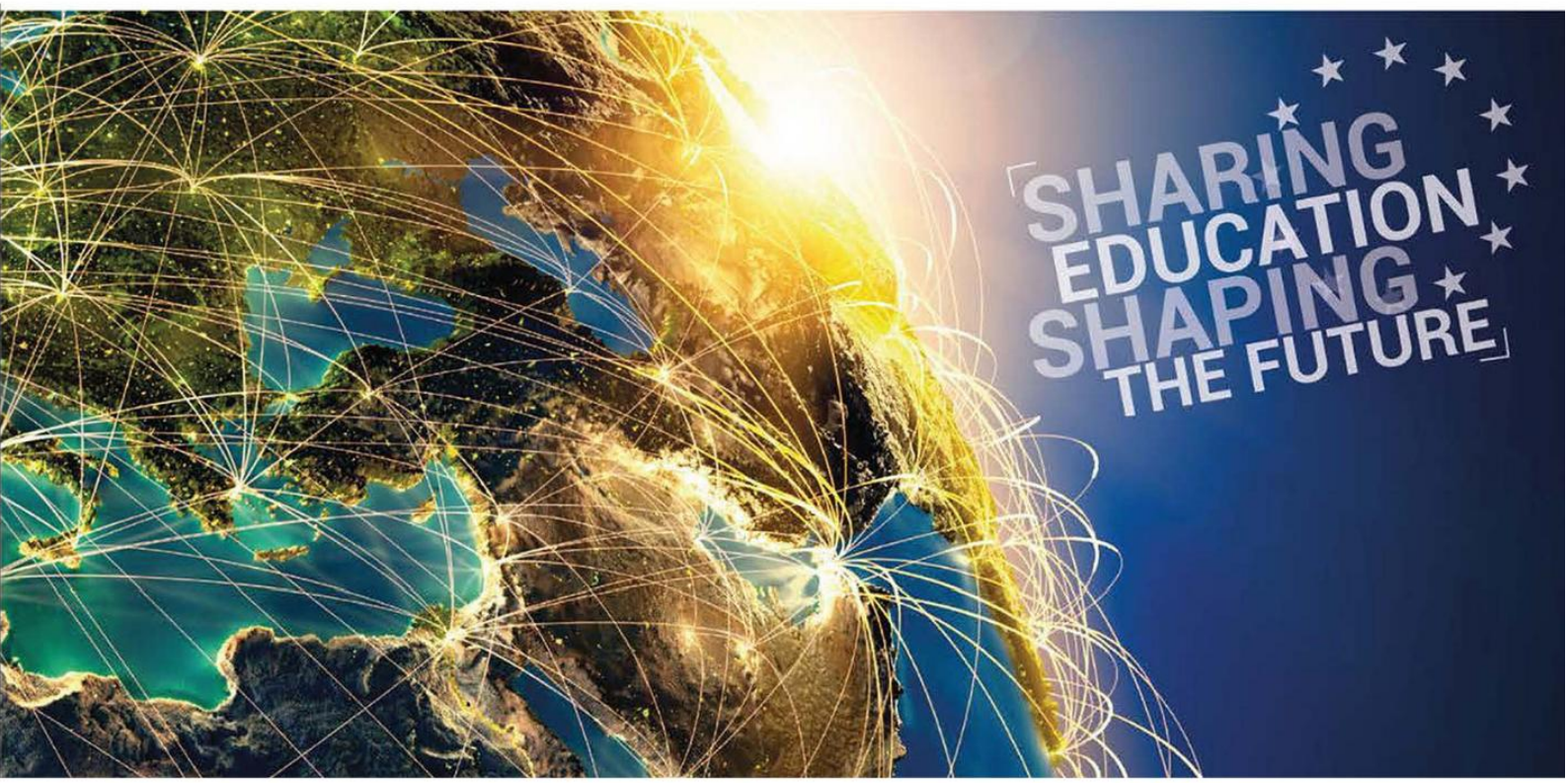
Le barème de notation est le suivant :
- **+ 3 points par bonne réponse**
- **0 point par réponse erronée**
- **0 point par non-réponse**

Aucun document, support de cours ou outil complémentaire (outil d'intelligence artificielle, calculatrice, dictionnaire, etc.) n'est autorisé durant cette évaluation.

NB : Formation en présentiel : heures d'enseignement réparties selon l'organisation propre à chaque établissement, à la spécialité du diplôme préparé et à la zone géographique du lieu de formation.

E. Coefficient et ECTS

Ce module vaut coefficient 2 et permet de capitaliser 3 ECTS.



FEDEration for European Education
FÉDÉration Européenne des Ecoles

INGO holding participatory status with the Council of Europe
OING dotée du statut participatif du Conseil de l'Europe
INGO holding consultative status with la Francophonie
OING dotée du statut consultatif auprès de la Francophonie
INGO holding the status of official partner of UNESCO and of ECOSOC
OING dotée du statut de partenaire officiel de l'UNESCO et du CESNU

FEDE - La Voie Creuse 16 - 1202 - Genève - SUISSE
www.fede.education - mailbox@fede.org

Copyright @2024 FEDE | Photo Credit Shutterstock.com
Do not litter on the public area Ne pas jeter sur la voie publique