PROJET FIL ROUGE : PROJET D'ETUDES MASTERE CYBERSECURITE

A DESTINATION DES CANDIDATS

SOMMAIRE

I. PRINCIPAUX ELEMENTS DU PROJET

I.1 - OBJECTIFS

Le projet fil rouge se déroule tout au long de la formation.
Le but du projet est d'acquérir et de développer les compétences des 2 blocs obligatoires en fonction des spécialités du titre ainsi que de valider l'acquisition de ces compétences.

Compétences Transverses :

- **Travailler en équipe :** Démontrer une capacité à collaborer de manière efficace au sein d'équipes pluridisciplinaires, en s'appuyant sur les forces de chaque membre et en intégrant divers points de vue. Utiliser des outils de gestion de projet (Jira, Trello, etc.) pour structurer et suivre le travail. Favoriser une communication claire et proactive afin d'améliorer la coordination et de résoudre rapidement les problèmes.
- **Développer sa communication :** Savoir échanger et collaborer avec des clients et des partenaires, qu'ils aient ou non une expertise technique. Renforcer sa capacité à présenter et expliquer des solutions logicielles de façon accessible, en s'adaptant au niveau de compréhension de chaque interlocuteur. Développer des compétences en communication orale et écrite pour des présentations impactantes et adaptées à différents publics.
- **Compétences spécifiques en Cybersécurité :** Maîtriser les techniques de détection et de gestion des vulnérabilités dans les systèmes d'information. Savoir implémenter des stratégies de sécurité proactive, y compris la gestion des accès, la surveillance en temps réel et les audits de sécurité. Réagir rapidement et efficacement en cas d'incidents de sécurité pour minimiser les impacts et assurer la continuité des opérations.

I.2 - ORGANISATION

Le projet est décomposé en 4 étapes dont 3 étapes débouchent sur des rendus.

Les 4 étapes :

	Evaluation certifiante adossée à l'étape
1. Le Kick-off : présentation du projet aux étudiants par l'animateur. (RP / Formateur)	
2. Analyse du sujet – Connaitre la maitrise du sujet par l'étudiant à travers un pdf de question sur le sujet. (RP/Formateur)	Oui (Rendu)
3. Planification : Analyse des spécifications fonctionnelle et techniques – Dossier complet de planification avec contribution individuels (RP/Formateur)	Oui (Rendu)
4. Soutenance & démo du projet -MVP- : par chaque groupe de projet étudiant devant le « client » via une vidéo. L'idée est de convaincre le client final via la démonstration ainsi que de revenir sur le déroulement projet en faisant une rétrospective. – 30 à 40 min de vidéo – (RP/Formateur)	Oui (Rendu)
5. Livrable final : C'est la dernière étape du projet, les étudiants rendent le projet technique et chacun d'entre eux livre un rapport personnel sur ses tâches effectuées via une description de la planification. (Formateur)	Oui (Rendu)

Composition des équipes :
L'équipe projet est composée de 3 étudiants. Les groupes sont composés par les étudiants lors du Kick-off.

I.3 - EVALUATION CERTIFIANTE DU PROJET D'ETUDE / FIL ROUGE

L'évaluation du projet d'étude est découpée en plusieurs épreuves certifiantes correspondant aux blocs de compétences.
Chaque épreuve, écrite ou orale, collective ou individuelle, est évaluée via une grille spécifique reprenant les compétences correspondant à chacun des blocs.

BC1 - Management de projet et d'équipes **(20 % de la note Globale)**	1.1 - **Analyse du sujet**	**50 %** de l'évaluation du bloc
	1.2 – **Backlog & Timeline du projet**	**50 %** de l'évaluation du bloc
BC2 - Management, Supervision et Sécurisation des Systèmes d'Information en Cybersécurité **(80 % de la note Globale)**	2.1 - **Soutenance & démo du projet -MVP-**	**30 %** de l'évaluation du bloc en **M1** et **70 %** de l'évaluation du bloc en **M2**
	2.2 - **Livrable final**	**70 %** de l'évaluation du bloc **en M1** et **30 %** de l'évaluation du bloc en **M2**

II. LES ETAPES CONSEILLES CHRONOLOGIQUES DU PROJET

II.1 – KICK-OFF

Calendrier : N - mois (Date sur César)
Objectif : Présentation de l'objectif du projet et du sujet
Organisation

- Première ½ J :
  - Introduction : présentation de l'ensemble des éléments structurants du projet (objectifs, calendrier, modalités d'évaluation, …) afin de bien préciser les attendus, expliquer les temps forts et fournir des conseils
  - Présentation du sujet / temps de réponse aux questions
- Le reste de la demi-journée vous permettra de commencer à réfléchir au projet.

II.2 - Premier rendu : Analyse du sujet

Calendrier : N+1 mois (Date sur César)

Modalités :

- Chaque groupe pourra poser des questions d'éclaircissement au client via un pdf et valider sa compréhension du sujet.

Préparation :
Chaque groupe transmet la liste des questions par PDF (voir date sur César). Le responsable pédagogique transmet les questions au référent du sujet qui peut ainsi s'y préparer en collaboration avec l'animateur pédagogique. 3 questions minimum par étudiant.

Évaluation :
Épreuve notée comptant pour 50 % de la note d'oral du bloc 1 « Management de projet et d'équipes ».
La qualité de des questions est évaluée en évaluant la logique et la qualité des questions.

II.3 - Deuxième rendu : BACKLOG & TIMELINE DU PROJET

Calendrier : N+2 mois (Date sur César)

Modalités :

- **Document de planification à soumettre** : Chaque groupe doit fournir un document de planification du projet sous format PDF. Ce document devra inclure :
    - **Les grandes étapes du projet** : Identification et organisation des actions majeures nécessaires à la réalisation du projet.
    - **Une timeline détaillée** : Échéances claires pour chaque étape ou livrable important, permettant un suivi rigoureux de l'avancement du projet.
    - **Ressources allouées** : Description des ressources humaines, matérielles et financières nécessaires pour chaque étape, en fonction des besoins du projet.
    - **Estimation des risques** : Une analyse des risques potentiels, incluant leur identification, leur impact et la stratégie de mitigation proposée.

Note : L'analyse financière et la gestion des risques doivent être abordées **uniquement par les étudiants de M2**. Les étudiants de M1 sont exemptés de ces sections spécifiques dans le rendu final.

Étapes de préparation :

- **Identification des livrables clés** : Chaque groupe doit définir les principaux livrables, en veillant à leur pertinence par rapport aux objectifs globaux du projet.
- **Définition des ressources nécessaires** : Évaluation des ressources requises, qu'elles soient humaines, matérielles ou financières.
- **Aspect financier (M2 uniquement)** : L'analyse financière se limite aux concepts du cours de budget IT, incluant les coûts estimés pour les services IT, les licences logicielles

et le matériel informatique nécessaire au projet. Cela permet aux étudiants de M2 d'appliquer concrètement les notions budgétaires dans un contexte projet.

Contenu attendu dans le rendu :

- **Backlog et Timeline** : Ces éléments doivent être mis en avant dans le document, avec un backlog structuré et une timeline claire, mettant en évidence les tâches prioritaires et les échéances importantes. Le rendu final doit inclure un **backlog global** (collectif) pour l'ensemble du groupe, ainsi qu'un **backlog individuel** pour chaque membre, détaillant les contributions spécifiques de chacun
- **Aspects financier et gestion des risques (M2 uniquement)** : Ces éléments sont obligatoires dans les rendus des étudiants de M2, mais ne sont pas requis pour les étudiants de M1.

Évaluation :

- **Bloc évalué** : La note comptera pour **50 % du bloc 1 "Management de projet et d'équipes"** et sera attribuée selon les critères suivants :
    - **Cohérence de la planification** : Les étapes et les ressources doivent être en adéquation avec les objectifs fixés pour une organisation optimale.
    - **Clarté du calendrier** : La timeline doit être précise, indiquant clairement les échéances et les responsabilités.
    - **Gestion des risques (M2 uniquement)** : Identification des risques majeurs (retards, difficultés techniques, problèmes de coordination, etc.), avec évaluation de leur impact et probabilité, et des stratégies pour les atténuer. Un suivi régulier des risques est également attendu pour les étudiants de M2.
    - **Qualité de la documentation** : La documentation doit être bien structurée, pertinente et claire, afin de faciliter la compréhension et le suivi du projet.

Outils pour créer un diagramme de planification : Chaque groupe est libre du choix de la solution logiciel.

- **Logiciels dédiés à la gestion de projet :**
    - **Microsoft Project :** Un des outils les plus connus, offrant de nombreuses fonctionnalités avancées.
    - **Asana :** Une solution collaborative en ligne, idéale pour les petites et moyennes équipes.
    - **Trello :** Un outil visuel et flexible, parfait pour les projets agiles.
    - **Monday.com :** Une plateforme personnalisable qui s'adapte à différents types de projets.
    - **Logiciels bureautiques :**
        - **Excel :** Vous pouvez créer un diagramme de Gantt simple avec Excel, bien qu'il soit moins adapté pour les projets complexes.
- **Outils en ligne gratuits :**
    - **Lucidchart :** Un outil de création de diagrammes en ligne très complet.
    - **Gantt :** Spécialisé dans les diagrammes de Gantt, il offre une interface intuitive.
    - **Creately :** Un autre outil en ligne polyvalent pour créer différents types de diagrammes.

II.4 - Troisième rendu : VIDEO & MVP – SAVOIR CONVAINCRE

Calendrier :

- N+6 mois (Date sur César)

Modalités :

- Chaque groupe réalisera une soutenance orale accompagnée d'une démonstration du produit minimum viable (MVP) via une vidéo.
- La présentation devra être structurée en plusieurs sections :
    - Contexte et objectifs du projet.
    - Description du MVP et de ses fonctionnalités clés.
    - Démonstration pratique des fonctionnalités.
    - Perspectives de développement et des améliorations futures.

Cours de Prérequis :
Pour les étudiants de **M2**, cette pré-soutenance peut être intégrée dans le cadre du **cours de journée mémoire**, du **Savoir Pitcher** ou de la **préparation à l'oral**. Ils bénéficieront ainsi d'une préparation spécifique pour renforcer leurs compétences oratoires, améliorer leur aisance en public, et structurer un discours convaincant et clair pour la soutenance finale.

Évaluation :

- La vidéo comptera pour **30 % de la note du bloc 2 en M1** et pour **70 % de la note d'oral du bloc 2 en M2**.
- Cette évaluation fait partie du bloc « Management, Supervision et Sécurisation des Systèmes d'Information » et sera réalisée selon les éléments suivants :
    - **Clarté de la présentation** : Structure, fluidité et pertinence des informations présentées.
    - **Qualité de la démonstration** : Fonctionnalités opérationnelles du MVP et capacité à répondre aux attentes du projet.
    - **Vision sur l'avenir** : Pertinence des perspectives d'évolution et de développement du projet.

II.5 - Quatrième rendu : DOCUMENT TECHNIQUE FINAL

Calendrier :

- N+6 mois (Date sur César)

Modalités :

- Chaque groupe devra soumettre un document technique final détaillant tous les aspects de leur projet, incluant la conception, l'implémentation, les tests et la documentation utilisateur.
- Le document doit être structuré pour inclure les sections suivantes :
    - **Introduction** : Objectifs et contexte du projet.

- **Architecture technique** : Schémas, choix techniques, et explications des technologies utilisées.
- **Fonctionnalités** : Description de chaque fonctionnalité, avec un focus sur la manière dont elle répond aux besoins définis initialement.
- **Tests** : Résultats des tests effectués et validation des critères de performance.
- **Documentation utilisateur** : Guide d'utilisation et d'installation et FAQ pour l'utilisateur final.

Préparation :

- **Collaboration** : Les groupes sont encouragés à poser des questions ou à demander des clarifications techniques à l'animateur pédagogique, surtout concernant la conformité aux exigences du projet.

Évaluation :

- La note comptera pour **70 % de la note du bloc technique en M1** et pour **30 % de la note du bloc technique en M2**.
- Elle sera évaluée sur les critères suivants :
  - **Précision technique** : Exactitude des informations et clarté des explications.
  - **Cohérence de l'architecture** : Pertinence des choix techniques et adéquation de l'architecture avec les objectifs du projet.
  - **Documentation** : Qualité de la documentation utilisateur et clarté des instructions fournies.
  - **Rigueur des tests** : Exhaustivité des tests effectués et qualité des résultats présentés.
  - **Professionnalisme du livrable** : Présentation générale, organisation et mise en page du document.

Suggestions d'outils technologiques pour la Cybersécurité :

- **Gestion des informations et des événements de sécurité (SIEM)** : Splunk, IBM QRadar, et Elastic Security pour collecter, analyser et corréler les événements de sécurité à travers divers systèmes afin de détecter les menaces en temps réel.
- **Protection des Endpoints** : Utilisez des solutions comme CrowdStrike Falcon, SentinelOne, ou Microsoft Defender ATP pour protéger les postes de travail et serveurs contre les menaces et les attaques en temps réel.
- **Détection et réponse dans le réseau (NDR)** : Darktrace et Vectra AI pour surveiller le trafic réseau et détecter les anomalies susceptibles d'indiquer une cyberattaque.
- **Gestion des vulnérabilités** : Nessus, Qualys et OpenVAS pour scanner les systèmes et identifier les vulnérabilités avant qu'elles ne soient exploitées par les attaquants.
- **Pare-feu de nouvelle génération (NGFW)** : Palo Alto Networks, Fortinet et Cisco Firepower pour contrôler le trafic réseau avec des fonctionnalités de filtrage avancé, incluant l'inspection des applications et la prévention des intrusions.
- **Analyse des malwares** : Cuckoo Sandbox et Any.Run pour exécuter et analyser des logiciels malveillants en environnement isolé, afin de comprendre leur comportement sans risque pour le réseau.

- **Test d'intrusion (Pentesting)** : Metasploit, Burp Suite, et OWASP ZAP pour tester les systèmes et les applications à la recherche de vulnérabilités exploitables par des attaquants.
- **Gestion des identités et des accès (IAM)** : Okta, CyberArk et Azure Entra pour gérer et sécuriser l'accès aux systèmes et aux applications en utilisant des politiques de contrôle d'accès strictes et des authentifications multiples.
- **Sécurité des API** : 42Crunch et Salt Security pour analyser, tester et protéger les API contre les vulnérabilités et les attaques spécifiques aux API.
- **Chiffrement et gestion des clés** : HashiCorp Vault et AWS Key Management Service (KMS) pour gérer les secrets, les certificats, et les clés de chiffrement, garantissant la confidentialité des données sensibles.
- **Automatisation et orchestration de la sécurité (SOAR)** : Palo Alto Cortex XSOAR, IBM Resilient pour automatiser et orchestrer les réponses aux incidents de sécurité, réduisant ainsi le temps de réaction et la charge sur les équipes de sécurité.
- **Forensic et analyse post-incident** : Autopsy et EnCase pour analyser les systèmes et identifier les traces d'attaques ou les éléments suspects dans le cadre d'une investigation après incident.
- **Sécurité des emails** : Proofpoint et Mimecast pour protéger les emails contre les attaques de phishing, les malwares et les attaques par compromission de la messagerie professionnelle (BEC)

III. ATTENDU DU PROJET

Les étudiants expliquent leurs choix en matière de technologies pour le développement, en fonction des besoins spécifiques du projet et des avantages et inconvénients de chaque technologie.

Contenu attendu pour un projet en Cybersécurité :

- **Comparaison des technologies** : Différentes solutions peuvent être envisagées pour chaque domaine technologique. Une comparaison approfondie entre les solutions utilisées et d'autres alternatives permet d'évaluer leurs avantages et inconvénients respectifs. Cette analyse prend en compte des facteurs tels que la flexibilité, la scalabilité et la capacité à s'intégrer dans un environnement cloud hybride ou multi-cloud.
- **Critères de comparaison** : Les critères retenus pour la comparaison incluent la **performance** des technologies en termes de capacité à gérer des environnements complexes, la **facilité de développement** et de gestion au quotidien, la **maintenabilité** des solutions choisies, le **coût** d'exploitation et d'acquisition, ainsi que la **compatibilité** avec les autres composants du système d'information.
- **Pertinence par rapport aux spécifications fonctionnelles** : Chaque choix technologique doit être justifié par son adéquation avec les spécifications fonctionnelles et les besoins du système. Il est essentiel de s'assurer que les technologies choisies répondent aux exigences de l'architecture globale, en garantissant une infrastructure évolutive, sécurisée et performante.

- **Retour d’expérience ou veille technologique** : Un retour d'expérience sur l'utilisation des technologies choisies ou une veille technologique sur les dernières évolutions dans le domaine du Cybersécurité peut être inclus. Cela permet d'évaluer l’adoption de nouvelles technologies ou de valider la pertinence des solutions actuelles en fonction des tendances du marché.