Projet 1 : Capture The Flag – CTF

Profil : Cyber

Objectif du Projet : L'objectif principal de ce projet est de permettre aux étudiants de développer des compétences en sécurité offensive (attaquante) et en sécurité défensive (défense) en simulant un environnement de Capture The Flag (CTF). Les équipes devront concevoir des défenses robustes tout en explorant et exploitant les vulnérabilités des systèmes adverses.

Étapes du Projet :

1. **Conception de l'Environnement CTF :**
    - Créez un environnement virtuel avec plusieurs machines virtuelles, chacune ayant des vulnérabilités spécifiques.
    - Concevez des défis variés, tels que la recherche de flag, l'exploitation de vulnérabilités, la stéganographie, etc.
    - Assurez-vous que les défenses et les vulnérabilités sont équilibrées pour offrir un défi équitable.

2. **Formation des Équipes :**
    - Les étudiants sont divisés en deux équipes : une équipe attaquante et une équipe de défense.
    - L'équipe attaquante doit comprendre les différentes méthodes d'attaque, tandis que l'équipe de défense doit mettre en place des mécanismes de détection et de prévention.

3. **Déroulement de l'Exercice CTF :**
    - La compétition commence avec l'équipe attaquante recevant des informations minimales sur l'environnement CTF.
    - L'équipe attaquante doit identifier les vulnérabilités, exploiter les systèmes, et récupérer des flags pour marquer des points.
    - L'équipe de défense doit surveiller activement le réseau, détecter les attaques, et corriger les vulnérabilités dès qu'elles sont découvertes.

4. **Temps de Réflexion et d'Amélioration :**
    - Après chaque phase de la compétition, accordez du temps aux équipes pour réfléchir aux tactiques utilisées, aux erreurs commises, et aux améliorations possibles.
    - Encouragez les équipes à partager leurs expériences et à discuter des meilleures pratiques de sécurité.

5. **Attendus et livrables :**
    - À la fin du projet, chaque équipe devra présenter son expérience, les tactiques utilisées, les défis rencontrés, et les leçons apprises.
    - Les équipes de défense doivent expliquer comment elles ont renforcé la sécurité au fil du temps, et les équipes attaquantes doivent partager les vulnérabilités exploitées.

Livrable du Projet : Les étudiants devront préparer un rapport écrit détaillant leurs stratégies, leurs tactiques, les vulnérabilités exploitées, les flags récupérés, ainsi que les améliorations apportées par l'équipe de défense.

Ce projet offre une expérience pratique et immersive dans le domaine de la cybersécurité, permettant aux étudiants de développer des compétences en attaque et en défense tout en renforçant leur compréhension des vulnérabilités et des mécanismes de sécurité.

Projet 2 : Analyse Forensique de Cyberattaque AFC

Profil : Cyber

Objectif du Projet : L'objectif principal de ce projet est de permettre aux étudiants de développer des compétences en analyse forensique en simulant une cyberattaque. Les étudiants auront pour tâche de mener une enquête approfondie pour comprendre la portée de l'attaque, identifier les acteurs impliqués, et proposer des mesures correctives.

Étapes du Projet :

1. **Préparation de l'Environnement :**
    - Créez un environnement virtuel simulant une infrastructure d'entreprise avec des serveurs, des postes de travail, des routeurs, etc.
    - Simulez une attaque en injectant des fichiers malveillants, en modifiant des configurations, ou en utilisant d'autres vecteurs d'attaque.
2. **Détection de l'Incident :**
    - Les étudiants devront mettre en place des outils de surveillance et de détection des incidents.
    - Enregistrez les journaux d'événements, les données réseau, les fichiers système, etc.
    - Les équipes de défense doivent être prêtes à détecter et à signaler l'incident.
3. **Isolation et Préservation des Preuves :**
    - Dès la détection de l'incident, l'équipe doit isoler les systèmes touchés pour éviter une propagation.
    - Utilisez des techniques appropriées pour préserver les preuves numériques, comme la création d'une image disque des machines affectées.
4. **Analyse Forensique :**
    - Les étudiants doivent analyser les images disques, les fichiers journaux, les captures réseau, etc., pour reconstruire la séquence des événements.
    - Identifiez les vecteurs d'attaque, les outils utilisés, et les techniques déployées par les attaquants.
    - Utilisez des outils forensiques tels que EnCase, Autopsy, ou d'autres pour extraire des informations cruciales.
5. **Rapport d'Analyse Forensique :**
    - Préparez un rapport détaillé sur l'analyse forensique, comprenant une chronologie des événements, les conclusions sur la nature de l'attaque, et les recommandations pour la résilience future.
    - Identifiez les failles de sécurité exploitées et proposez des améliorations de sécurité.
6. **Attendus et livrables :**

- Les équipes doivent présenter leurs conclusions devant un panel simulé.
- Partagez les leçons apprises, les défis rencontrés, et discutez des recommandations de sécurité.

  Livrables du Projet : À la fin du projet, les étudiants devraient fournir un rapport écrit complet. Le rapport doit inclure des détails techniques, des captures d'écran, des analyses forensiques, et des recommandations concrètes. La présentation doit résumer ces informations de manière accessible pour un public non technique.

Ce projet permettra aux étudiants d'acquérir des compétences essentielles en analyse forensique tout en développant leur capacité à travailler en équipe et à présenter leurs résultats de manière claire et concise.

Projet 3 : Évaluation de la Sécurité d'une Infrastructure Cloud

Profil : Cyber

Objectif du Projet : L'objectif de ce projet est d'évaluer la sécurité d'une infrastructure cloud en simulant une batterie de tests de sécurité. L'équipe devra identifier les vulnérabilités potentielles, évaluer la configuration de sécurité, et proposer des mesures correctives pour renforcer la posture de sécurité de l'infrastructure.

Étapes du Projet :

1. **Préparation Infrastructure Cloud :**
    - Sélectionnez une plateforme cloud populaire soit AWS soit google cloud pour évaluer sa sécurité.
    - Créez un environnement factice sur la plateforme cloud avec divers services configurés.
2. **Analyse des Documents de Configuration :**
    - Analysez les documents de configuration de l'infrastructure cloud fournis (modèles d'infrastructure, politiques de sécurité, etc.).
    - Identifiez les configurations de sécurité recommandées et comparez-les à la configuration réelle de l'environnement.
3. **Tests d'Intrusion et d'Évaluation de la Sécurité :**
    - Menez des tests d'intrusion sur les services cloud (machines virtuelles, stockage, bases de données, etc.).
    - Utilisez des outils de sécurité et des techniques manuelles pour identifier les vulnérabilités possibles et les points faibles.
4. **Analyse des Logs et des Métriques :**
    - Configurez la collecte de logs et de métriques pour surveiller l'activité au sein de l'infrastructure cloud.
    - Analysez ces logs et métriques pour détecter des comportements anormaux ou des activités suspectes.
5. **Évaluation de la Conformité :**
    - Vérifiez la conformité de l'infrastructure aux normes de sécurité spécifiques à l'industrie ou aux réglementations applicables.
    - Identifiez les écarts de conformité et proposez des recommandations pour les corriger.
6. **Attendus et livrables :**

    La livraison du projet comprendra le rapport détaillé, la présentation, les résultats des tests, les recommandations de sécurité, et une évaluation de la conformité par rapport aux normes de sécurité.

L'évaluation sera basée sur la qualité de l'évaluation de la sécurité, l'identification des vulnérabilités, la pertinence des recommandations, la conformité aux normes de sécurité, et la clarté de la présentation. Ce projet permettra aux étudiants de développer des compétences pratiques en

évaluation de la sécurité des systèmes cloud, un domaine crucial dans le contexte actuel de l'informatique moderne.

Projet 4 : Sécurité Wi-Fi et Gestion des Menaces :

Profil :Cyber

Objectif du Projet : L'objectif principal de ce projet est de concevoir, mettre en œuvre et évaluer des mesures de sécurité pour renforcer la protection d'un réseau Wi-Fi. Le projet mettra l'accent sur la détection d'intrusions, la gestion des menaces et la sensibilisation à la sécurité.

Étapes du Projet :

1. **Évaluation de la Configuration Wi-Fi :**
   - Analysez la configuration du réseau Wi-Fi existant, y compris les paramètres de sécurité tels que le type d'authentification, le chiffrement, les contrôles d'accès, etc.
2. **Analyse des Menaces :**
   - Identifiez les menaces potentielles qui peuvent compromettre la sécurité du réseau Wi-Fi, telles que les attaques de force brute, les attaques par déni de service (DoS), les attaques de type Man-in-the-Middle (MitM), etc.
3. **Implémentation de Mécanismes de Détection d'Intrusions :**
   - Mettez en place des systèmes de détection d'intrusions (IDS) pour surveiller le trafic du réseau et détecter toute activité suspecte ou non autorisée.
4. **Configuration des Points d'Accès (AP) :**
   - Configurez les points d'accès Wi-Fi pour renforcer la sécurité, en activant, par exemple, le filtrage MAC, la désactivation du SSID broadcast, et l'utilisation du chiffrement WPA3.
5. **Déploiement de Réseaux Invités Sécurisés :**
   - Mettez en place un réseau Wi-Fi séparé pour les invités avec des restrictions d'accès appropriées. Assurez-vous que le trafic invité est isolé du réseau principal.
6. **Utilisation de Certificats pour l'Authentification :**
   - Implémentez l'authentification basée sur des certificats pour renforcer la sécurité de l'accès au réseau Wi-Fi.
7. **Formation et Sensibilisation à la Sécurité :**
   - Développez des programmes de formation et de sensibilisation à la sécurité pour les utilisateurs du réseau. Sensibilisez-les aux bonnes pratiques en matière de sécurité Wi-Fi et aux risques potentiels.
8. **Monitoring et Rapports de Sécurité :**
   - Configurez des outils de monitoring pour surveiller en temps réel l'activité du réseau Wi-Fi. Générez des rapports de sécurité réguliers pour évaluer l'efficacité des mesures mises en place.

9. **Livrables et attendus:** La livraison du projet comprendra un rapport détaillé sur la configuration du réseau Wi-Fi, les mesures de sécurité mises en œuvre, les résultats des tests de sécurité, des recommandations d'amélioration et une présentation des résultats.

L'évaluation portera sur la qualité des mesures de sécurité mises en place, la détection des menaces, la formation des utilisateurs, la sensibilisation à la sécurité, et la documentation complète du projet.

Ce projet offre une expérience pratique dans la sécurisation d'un réseau Wi-Fi contre les menaces potentielles.

Projet 5 : Génération de Texte avec GPT pour le webmarketing

Profil : IA

Objectif du Projet : L'objectif principal de ce projet est de permettre aux étudiants de développer une compréhension pratique de la génération de texte avec le modèle GPT (Generative Pre-trained Transformer). Les étudiants auront pour tâche de créer un modèle capable de générer du texte de manière cohérente et contextuellement pertinente pour créer du contenu pour un réseau social.

Étapes du Projet :

1. **Compréhension du Modèle GPT :**
    - Les étudiants devront se familiariser avec le modèle GPT, comprendre son fonctionnement, et explorer ses capacités en matière de génération de texte.
2. **Choix de la Tâche de Génération de Texte :**
    - Les étudiants sélectionneront une tâche spécifique de génération de texte, comme la rédaction automatique d'articles, la création de poèmes, ou la production de textes créatifs.
3. **Prétraitement des Données :**
    - Préparez et prétraitez les données d'entraînement adaptées à la tâche choisie. Cela peut inclure le nettoyage des données, le découpage en segments de texte, etc.
4. **Adaptation du Modèle GPT :**
    - Les étudiants adapteront le modèle GPT à leur tâche spécifique en fine-tunant les poids du modèle sur leur ensemble de données d'entraînement.
5. **Entraînement du Modèle :**
    - Entraînez le modèle GPT fine-tuné sur l'ensemble de données préparé, en ajustant les hyperparamètres au besoin.
6. **Ajustement des Paramètres et Optimisation :**
    - Les étudiants ajusteront les paramètres du modèle pour améliorer la qualité de la génération de texte.
    - Ils pourront également expérimenter avec différentes techniques d'optimisation pour renforcer les performances du modèle.
7. **Évaluation Qualitative de la Génération de Texte :**
    - Évaluez qualitativement la génération de texte produite par le modèle. Cela peut se faire en examinant des échantillons générés et en évaluant la cohérence, la pertinence contextuelle, et la fluidité du texte généré.
8. **Optimisation Finale et Livrables :**
    - Effectuez une dernière phase d'optimisation basée sur les retours obtenus lors de l'évaluation.
      La livraison du projet inclura un rapport détaillé comprenant une introduction, la méthodologie, les résultats de l'entraînement, des exemples de texte généré, les ajustements de modèle, et une présentation interactive.

Les évaluations seront basées sur la qualité de la génération de texte, la compréhension démontrée du modèle GPT, l'efficacité de l'adaptation à la tâche spécifique, et la clarté de la présentation des résultats.

Ce projet permettra aux étudiants d'acquérir une expérience pratique dans l'utilisation des modèles d'IA avancés pour la génération de texte, en explorant les aspects techniques de fine-tuning et d'optimisation pour des tâches spécifiques.

Projet 6 : Reconnaissance d'Objets Lego avec un Modèle CNN

Étapes du Projet :

1. **Choix de l'Ensemble de Données Lego :**
    - Les étudiants choisiront ou créeront un ensemble de données d'images contenant différents types de pièces Lego. Ils devront s'assurer que l'ensemble de données est diversifié et représentatif.
2. **Compréhension des Concepts de CNN :**
    - Les étudiants se familiariseront avec les concepts de base des réseaux de neurones convolutionnels (CNN) et leur application dans la reconnaissance d'objets.
3. **Conception de l'Architecture du CNN :**
    - Les étudiants concevront l'architecture du CNN, en tenant compte de la complexité des pièces Lego à reconnaître. Ils peuvent explorer différentes architectures, telles que LeNet, AlexNet, ou créer une architecture personnalisée.
4. **Prétraitement des Images Lego :**
    - Les images de pièces Lego peuvent être prétraitées pour optimiser l'entraînement du modèle. Cela peut inclure le redimensionnement des images, la normalisation des couleurs, ou d'autres techniques de prétraitement.
5. **Entraînement du Modèle CNN :**
    - Les étudiants entraîneront le modèle CNN sur l'ensemble de données Lego. Ils ajusteront les paramètres du modèle et surveilleront les métriques d'entraînement pour garantir une convergence appropriée.
6. **Évaluation des Performances :**
    - Les performances du modèle seront évaluées sur un ensemble de données de test distinct. Les étudiants analyseront les résultats pour mesurer la précision de la classification et identifier les erreurs potentielles.
7. **Optimisation du Modèle :**
    - Si nécessaire, les étudiants pourront optimiser le modèle en ajustant les hyperparamètres, en ajoutant des couches de régularisation, ou en explorant d'autres techniques d'optimisation.
8. **Attendus et livrables :**
    - Les résultats du projet seront présentés sous forme de rapport détaillé, montrant la méthodologie, les performances du modèle, des exemples de classification réussis et des cas d'erreurs, ainsi que les conclusions et les apprentissages tirés.

La livraison du projet comprendra le rapport détaillé, le code source du modèle, l'ensemble de données utilisé (ou des références aux ensembles de données publics), et une présentation interactive.

Ce projet offre une expérience pratique dans le domaine de la reconnaissance d'objets avec des applications concrètes sur des pièces Lego.

Projet 7 : Expertise de Véhicules Accidentés avec un Modèle de Transfer Learning

Profil : IA

Objectif du Projet : L'objectif principal de ce projet est de développer un système d'expertise de véhicules accidentés capable de classer des images de véhicules endommagés en différentes catégories de gravité des dommages. Dans ce projet, un modèle de transfert d'apprentissage, en particulier EfficientNet, sera utilisé.

Étapes du Projet :

1. **Choix de l'Ensemble de Données d'Images de Véhicules Accidentés :**
    - Les étudiants choisiront un ensemble de données d'images de véhicules accidentés, avec des annotations pour la gravité des dommages.

2. **Compréhension du Modèle de Transfer Learning (EfficientNet) :**
    - Les étudiants se familiariseront avec les concepts du transfert d'apprentissage et comprendront comment utiliser un modèle pré-entraîné tel qu'EfficientNet pour leur tâche spécifique.
3. **Prétraitement des Images de Véhicules Accidentés :**
    - Les images de véhicules accidentés seront prétraitées, y compris le redimensionnement, la normalisation des couleurs ou toute autre transformation nécessaire.
4. **Entraînement du Modèle de Transfer Learning :**
    - Les étudiants utiliseront un modèle EfficientNet pré-entraîné sur une tâche similaire (par exemple, ImageNet) en tant que base pour leur modèle d'expertise de véhicules accidentés. Ils ajusteront ensuite le modèle sur leur ensemble de données spécifique.
5. **Évaluation des Performances :**
    - Les performances du modèle seront évaluées sur un ensemble de données de test distinct. Les étudiants analyseront les résultats et mesureront la précision de la classification des dommages.
6. **Optimisation du Modèle de Transfer Learning :**
    - Les étudiants optimiseront le modèle en ajustant les hyperparamètres, en expérimentant avec des techniques d'augmentation de données, ou en explorant d'autres stratégies d'optimisation.
7. **Interprétation des Résultats d'Expertise des Véhicules Accidentés :**
    - Les résultats du projet seront interprétés et présentés de manière détaillée. Les étudiants discuteront de la performance du modèle dans le contexte de l'expertise des véhicules accidentés, identifieront les erreurs potentielles et proposeront des pistes d'amélioration.

    - La livraison du projet comprendra un rapport détaillé, le code source du modèle, l'ensemble de données d'images de véhicules accidentés utilisé, des exemples

d'images correctement classifiées et d'images mal classifiées, ainsi qu'une présentation des résultats.

Ce projet offre une expérience pratique dans l'utilisation du transfert d'apprentissage pour des tâches spécifiques.

Projet 8 : Système de Recommandation Personnalisée pour l'E-commerce :

Profil : IA

Objectif du Projet : L'objectif principal de ce projet est de concevoir un système de recommandation personnalisée pour une plateforme d'e-commerce. Le système utilisera des techniques d'apprentissage automatique pour comprendre les préférences des utilisateurs et recommander des produits pertinents.

Étapes du Projet :

1. **Collecte et Exploration des Données :**
   - Utilisez un ensemble de données d'e-commerce contenant des informations sur les produits, les utilisateurs, et les historiques d'achats. Explorez les données pour comprendre leur structure et leurs caractéristiques.
2. **Choix de l'Algorithme de Recommandation :**
   - Sélectionnez un algorithme de recommandation approprié en fonction des caractéristiques des données. Les approches courantes incluent la recommandation collaborative, la factorisation de matrices, ou les modèles basés sur le contenu.
3. **Prétraitement des Données :**
   - Prétraitez les données en nettoyant les valeurs manquantes, en normalisant les caractéristiques, et en traitant les données catégorielles.
4. **Entraînement du Modèle de Recommandation :**
   - Entraînez le modèle de recommandation en utilisant l'apprentissage supervisé sur les données historiques d'achats. Divisez les données en ensembles d'entraînement et de test pour évaluer la performance du modèle.
5. **Évaluation et Optimisation :**
   - Évaluez la performance du modèle en utilisant des métriques telles que la précision, le rappel, et la F-mesure. Optimisez le modèle en ajustant les hyperparamètres pour améliorer les résultats.
6. **Intégration avec la Plateforme E-commerce :**
   - Intégrez le système de recommandation dans la plateforme d'e-commerce, permettant ainsi aux utilisateurs de recevoir des suggestions personnalisées lorsqu'ils parcourent le site ou l'application.
7. **Interface Utilisateur pour les Recommandations :**
   - Créez une interface utilisateur conviviale pour afficher les recommandations personnalisées aux utilisateurs. Cela peut inclure une section de recommandations sur la page d'accueil ou des e-mails personnalisés.
8. **Gestion des Nouveaux Produits :**
   - Mettez en place un mécanisme pour gérer les nouveaux produits et garantir que le système peut recommander des articles même lorsque les données historiques sont limitées.

9. **Livrables et attendus :**
   - La livraison du projet comprendra un rapport détaillé sur le choix de l'algorithme, le processus d'entraînement, les résultats de recommandation, le code source intégré à la plateforme, et une démo de l'interface utilisateur.

L'évaluation portera sur la précision des recommandations, la pertinence des suggestions pour les utilisateurs, l'efficacité de l'intégration avec la plateforme, et la documentation complète du projet.

Ce projet offre une expérience pratique dans la mise en œuvre de systèmes de recommandation personnalisée pour l'e-commerce.

Projet 9 : Implémentation DevOps pour une Application Web

Étapes du Projet :

1. **Choix de l'Application Web :**
    - Les étudiants choisiront une application web simple, par exemple un blog, une boutique en ligne ou un gestionnaire de tâches.
2. **Mise en Place d'un Système de Gestion de Versions :**
    - Utilisation de Git pour le contrôle de version. Création d'un référentiel Git pour l'application et définition d'une stratégie de gestion de versions.
3. **Automatisation des Tests :**
    - Mise en place de tests automatisés pour l'application. Cela peut inclure des tests unitaires, des tests d'intégration et des tests d'acceptation automatisés.
4. **Mise en Place d'un Serveur d'Intégration Continue (CI) :**
    - Utilisation d'une plateforme CI/CD telle que Jenkins, GitLab CI ou GitHub Actions. Configuration du pipeline CI pour déclencher automatiquement des tests à chaque modification de code.
5. **Gestion de la Configuration avec Infrastructure as Code (IaC) :**
    - Utilisation d'outils comme Ansible, Terraform ou Chef pour déployer et gérer l'infrastructure de l'application de manière automatisée.
6. **Mise en Place de l'Environnement de Staging :**
    - Configuration d'un environnement de staging automatisé pour tester les versions déployées avant la production.
7. **Déploiement Continu (CD) :**
    - Configuration du pipeline CD pour déployer automatiquement l'application sur l'environnement de staging après des tests réussis.
8. **Surveillance et Logging :**
    - Mise en place d'outils de surveillance tels que Prometheus, Grafana ou ELK Stack pour surveiller les performances de l'application. Configuration des journaux (logs) pour faciliter le dépannage.

    Livraison du Projet : La livraison du projet comprendra un rapport détaillé, le code source de l'application, les scripts d'automatisation, la configuration CI/CD, et une présentation des résultats.

L'évaluation portera sur la qualité de l'automatisation, la robustesse du pipeline DevOps, la clarté de la documentation et la présentation des résultats. Ce projet offre une expérience pratique dans la

mise en œuvre de pratiques DevOps pour améliorer l'efficacité du cycle de vie d'une application web.

Projet 10 : Plateforme d'Accessibilité pour les Contenus Web (Web Accessibility Platform) Profil : DevOps

Objectif du Projet : L'objectif de ce projet est de développer une plateforme qui améliore l'accessibilité des contenus web pour les personnes en situation de handicap. La plateforme se concentrera sur l'automatisation des tests d'accessibilité, la création de rapports détaillés, et la fourniture de recommandations pour rendre les sites web plus accessibles.

Étapes du Projet :

1. **Choix des Technologies :**
    - Choisissez les technologies appropriées pour le développement de la plateforme, en tenant compte de l'évolutivité et de l'intégration avec des outils de DevOps.
2. **Développement d'un Robot d'Indexation :**
    - Créez un robot d'indexation qui parcourt les sites web soumis, identifie les pages et extrait les informations nécessaires pour les tests d'accessibilité.
3. **Automatisation des Tests d'Accessibilité :**
    - Intégrez des outils d'automatisation des tests d'accessibilité, tels que Axe, Pa11y, ou WAVE, pour évaluer la conformité aux normes d'accessibilité (par exemple, WCAG).
4. **Création de Rapports Détaillés :**
    - Mettez en place une fonctionnalité qui génère des rapports détaillés sur l'accessibilité des sites web testés, en identifiant les problèmes spécifiques et en fournissant des recommandations.
5. **Intégration avec des Outils DevOps :**
    - Intégrez la plateforme avec des outils de DevOps tels que Jenkins, GitLab CI, ou GitHub Actions pour automatiser le processus de test et de génération de rapports lors des déploiements.
6. **Interface Utilisateur Conviviale :**
    - Créez une interface utilisateur conviviale permettant aux utilisateurs de soumettre des sites web pour les tests, de visualiser les résultats, et d'accéder aux rapports d'accessibilité.
7. **Gestion de Configuration avec Infrastructure as Code (IaC) :**
    - Utilisez des outils d'Infrastructure as Code (IaC) tels que Terraform pour gérer l'infrastructure de la plateforme de manière automatisée.
8. **Déploiement sur le Cloud :**
    - Explorez le déploiement de la plateforme sur une infrastructure cloud telle que AWS, Azure, ou Google Cloud pour assurer la scalabilité et la disponibilité.
9. **Attendus et livrables :**
    - La livraison du projet comprendra un rapport détaillé, le code source de la plateforme, les scripts d'automatisation, des exemples de rapports d'accessibilité générés, et une présentation des résultats.

L'évaluation portera sur la qualité de l'automatisation des tests d'accessibilité, la convivialité de l'interface utilisateur, l'intégration réussie avec des outils DevOps, la gestion de configuration avec IaC, et la documentation complète du projet.

Ce projet offre une opportunité d'appliquer des pratiques DevOps pour créer une solution bénéfique aux personnes en situation de handicap en favorisant une expérience web plus accessible.

Projet 11 : Mise en Place d'une Infrastructure de Microservices avec Orchestration de Conteneurs Profil : DevOps

Objectif du Projet : L'objectif principal de ce projet est de créer une architecture de microservices basée sur des conteneurs Docker et orchestrée avec Kubernetes. Le projet mettra l'accent sur l'automatisation du déploiement, la gestion de la configuration, la surveillance et l'intégration continue.

Étapes du Projet :

1. **Choix des Services Microservices :**
    - Déterminez les services nécessaires à votre application. Par exemple, un service d'authentification, un service de stockage, un service de traitement, etc. Choisissez des services qui illustrent bien les principes des microservices.
2. **Dockerisation des Microservices :**
    - Pour chaque microservice, créez un Dockerfile pour générer une image Docker. Dockerisez les services pour garantir une isolation et une portabilité maximales.
3. **Configuration de Docker Compose :**
    - Utilisez Docker Compose pour définir et gérer l'environnement de développement local. Assurez-vous que les services interagissent correctement lorsqu'ils sont exécutés en tant que conteneurs.
4. **Orchestration avec Kubernetes :**
    - Déployez un cluster Kubernetes et configurez les ressources nécessaires (pods, services, déploiements) pour chaque microservice. Kubernetes permettra l'orchestration, la mise à l'échelle et la gestion des conteneurs.
5. **Automatisation du Déploiement :**
    - Mettez en place un pipeline CI/CD pour automatiser le processus de construction des images Docker, les tests, et le déploiement sur Kubernetes. Utilisez des outils tels que Jenkins, GitLab CI, ou GitHub Actions.
6. **Gestion de Configuration avec Helm :**
    - Utilisez Helm pour gérer la configuration de Kubernetes de manière déclarative. Créez des charts Helm pour chaque microservice, facilitant ainsi le déploiement, la mise à jour et le rollback.
7. **Surveillance avec Prometheus et Grafana :**
    - Intégrez Prometheus pour la collecte de métriques au niveau des microservices et de Kubernetes. Utilisez Grafana pour visualiser ces métriques et configurez des tableaux de bord pertinents.
8. **Tests Automatisés des Microservices :**
    - Intégrez des tests automatisés dans le pipeline CI/CD. Cela inclut des tests d'intégration pour vérifier les interactions entre les microservices et des tests de charge pour évaluer les performances.
9. **Déploiement sur le Cloud :**

- Explorez le déploiement de l'infrastructure de microservices sur une plateforme cloud telle qu'AWS, Azure ou Google Cloud pour tirer parti des avantages de la scalabilité et de la disponibilité.

10. **Livrables et attendus :** La livraison du projet comprendra un rapport détaillé comprenant l'architecture globale, les scripts d'automatisation, les fichiers de configuration Kubernetes et Helm, des exemples de métriques surveillées, le code source des microservices, et une présentation des résultats.

L'évaluation portera sur la mise en œuvre réussie de l'infrastructure de microservices, l'efficacité du pipeline CI/CD, la gestion de configuration avec Helm, la surveillance des performances, la scalabilité sur le cloud, et la documentation complète du projet. Ce projet offre une expérience pratique dans la mise en œuvre de pratiques DevOps pour une architecture de microservices moderne.

Projet 12 : Portail Client Hubspot pour Voyelle

Profil : DevOps

Objectif du Projet : L'objectif principal de ce projet DevOps est de concevoir, développer, déployer et maintenir un portail client personnalisé exploitant les API d'Hubspot. Le portail doit étendre les fonctionnalités existantes en intégrant la gestion des temps, en fournissant un CRUD complet pour les tickets, et en permettant le suivi des factures provenant de Pennylane si nécessaire.

Étapes du Projet :

1. **Configuration du Repository :**
   - Utilisez Git pour créer un repository pour le code source du portail client. Adoptez une structure de branches Git pour le développement, les tests, et la production.
2. **Infrastructure en tant que Code (IaC) :**
   - Utilisez Terraform pour définir l'infrastructure en tant que code. Automatisez la création des ressources nécessaires pour le portail client, y compris les serveurs, bases de données, et services associés.
3. **Choix de l'Outil de CI/CD :**
   - Sélectionnez un outil CI/CD tel que Jenkins, GitLab CI, ou GitHub Actions pour automatiser les étapes de construction, de test, et de déploiement.
4. **Développement des Pipelines CI/CD :**
   - Créez des pipelines CI/CD qui automatisent le processus de construction, de test, et de déploiement du portail client. Intégrez également des tests automatisés pour garantir la qualité du code.
5. **Intégration avec les API Hubspot :**
   - Développez des modules pour intégrer les API Hubspot dans le portail client. Assurez-vous que les fonctionnalités existantes de gestion de compte utilisateur et de CRUD Ticket sont correctement intégrées.
6. **Ajout de la Gestion des Temps :**
   - Développez des fonctionnalités pour la gestion des temps, avec chaque ticket décomptant du temps d'un contrat. Intégrez ces fonctionnalités dans le portail client tout en exploitant les API d'Hubspot.
7. **Suivi des Factures (en option) :**
   - Si nécessaire, développez des fonctionnalités pour le suivi des factures provenant de Pennylane. Intégrez ces fonctionnalités dans le portail client pour une gestion centralisée.
8. **Tests Automatisés et Manuels :**
   - Intégrez des tests automatisés pour chaque fonctionnalité ajoutée. Réalisez également des tests manuels pour valider l'expérience utilisateur et la conformité avec les besoins opérationnels.
9. **Déploiement Graduel :**
   - Utilisez des déploiements progressifs pour minimiser les risques lors de la mise à jour du portail client en production.
10. **Surveillance et Journalisation :**
    - Intégrez des outils de surveillance et de journalisation pour suivre les performances du portail client en production. Configurez des alertes pour détecter rapidement tout problème.

11. **Livraison du Projet :** La livraison du projet comprendra un rapport détaillé sur la configuration des pipelines CI/CD, les intégrations avec les API Hubspot, les fonctionnalités ajoutées, des exemples de déploiements réussis, et un démonstrateur complet du portail client.

L'évaluation portera sur la robustesse des pipelines CI/CD, l'intégration réussie avec les API Hubspot, l'ajout de fonctionnalités (gestion des temps, suivi des factures), la stabilité en production, et la documentation complète du processus de développement et de déploiement. Ce projet offre une expérience pratique dans l'application des pratiques DevOps à un portail client complexe.

Projet 13 : **Détection d'Anomalies dans les Flux Réseau avec l'IA**

Profil : Cyber/IA

Objectif du Projet : L'objectif principal de ce projet est de développer un système de détection d'anomalies dans les flux réseau en utilisant des techniques d'intelligence artificielle. Le projet vise à identifier les comportements anormaux et potentiellement malveillants dans un réseau, renforçant ainsi la sécurité.

Étapes du Projet :

1. **Collecte des Données Réseau :**
   - Mettez en place une infrastructure pour collecter des données sur le trafic réseau. Utilisez des sondes ou des dispositifs de surveillance pour capturer des informations sur les flux réseau.
2. **Prétraitement des Données :**
   - Prétraitez les données pour les rendre adaptées à l'entraînement des modèles d'IA. Cela peut inclure la normalisation, la suppression des valeurs aberrantes, et la transformation des données en séquences temporelles.
3. **Choix du Modèle d'IA :**
   - Sélectionnez un modèle d'apprentissage automatique adapté à la détection d'anomalies dans les séquences temporelles. Les réseaux de neurones récurrents (RNN) ou les autoencodeurs peuvent être des choix pertinents.
4. **Entraînement du Modèle :**
   - Entraînez le modèle avec les données prétraitées. Utilisez un ensemble de données comprenant des exemples normaux et des exemples d'anomalies pour permettre au modèle d'apprendre à distinguer les comportements suspects.
5. **Validation et Ajustement :**
   - Validez la performance du modèle en utilisant des données de validation. Ajustez les hyperparamètres du modèle pour optimiser la précision de la détection d'anomalies.
6. **Intégration dans l'Infrastructure de Sécurité :**
   - Intégrez le modèle d'IA dans l'infrastructure de sécurité du réseau. Configurez le système pour déclencher des alertes en cas de détection d'anomalies.
7. **Adaptation Dynamique :**
   - Si possible, développez une capacité d'adaptation dynamique du modèle aux changements dans le trafic réseau et aux nouvelles menaces. Assurez-vous que le modèle reste efficace dans un environnement en évolution constante.
8. **Gestion des Faux Positifs :**
   - Mettez en place des mécanismes pour gérer les faux positifs générés par le modèle. Ceci peut inclure des filtres supplémentaires, des règles de corrélation, ou des analyses manuelles.
9. **Surveillance des Modèles d'IA :**
   - Implémentez des mécanismes de surveillance continue pour les modèles d'IA afin de détecter toute dégradation de la performance ou toute tentative de contournement.
10. **Livrables et attendus :** La livraison du projet comprendra un rapport détaillé sur la configuration du modèle d'IA, l'intégration dans l'infrastructure de sécurité, les résultats de détection d'anomalies, des exemples d'adaptation dynamique, et un démonstrateur du système en action.

L'évaluation portera sur l'efficacité de la détection d'anomalies, la capacité d'adaptation aux nouveaux comportements malveillants, la gestion des faux positifs, la stabilité en production, et la documentation complète du projet. Ce projet offre une expérience pratique dans l'intersection de la cybersécurité et de l'intelligence artificielle.

Projet 14 : **Détection d'Attacks de Phishing avec des Modèles d'IA**

Profil : Cyber/IA

Objectif du Projet : L'objectif principal de ce projet est de développer un système de détection avancée des attaques de phishing en utilisant des techniques d'intelligence artificielle. Le projet vise à renforcer la sécurité des utilisateurs en identifiant et en bloquant les tentatives de phishing de manière proactive.

Étapes du Projet :

1. **Collecte de Données de Phishing :**
   - Rassemblez un ensemble de données représentatif d'emails de phishing. Vous pouvez utiliser des sources publiques ou créer un ensemble de données synthétiques pour couvrir divers scénarios de phishing.
2. **Prétraitement des Données :**
   - Prétraitez les emails pour extraire les caractéristiques pertinentes. Cela peut inclure l'extraction de liens, l'analyse de la syntaxe, et la détection de pièces jointes malveillantes.
3. **Choix du Modèle d'IA :**
   - Sélectionnez un modèle d'apprentissage automatique, tel qu'un modèle de classification (comme les réseaux de neurones, les arbres de décision, ou les machines à vecteurs de support), pour entraîner le système à distinguer les emails de phishing des emails légitimes.
4. **Entraînement du Modèle :**
   - Entraînez le modèle en utilisant l'ensemble de données de phishing. Divisez les données en ensembles d'entraînement et de test, et assurez-vous que le modèle apprend efficacement à différencier les emails malveillants.
5. **Intégration dans la Passerelle Email :**
   - Intégrez le modèle d'IA dans la passerelle email de l'organisation. Configurez le système pour analyser chaque email entrant et déclencher des alertes en cas de détection de phishing.
6. **Évaluation de la Performance :**
   - Évaluez la performance du modèle en utilisant des métriques telles que la précision, le rappel, et la F-mesure. Optimisez le modèle en ajustant les hyperparamètres pour améliorer les résultats.
7. **Adaptation Dynamique :**
   - Implémentez des mécanismes d'adaptation dynamique pour le modèle afin de s'ajuster aux nouvelles tactiques utilisées par les attaquants. Assurez-vous que le système reste efficace face aux campagnes de phishing en constante évolution.
8. **Analyse des Faux Positifs :**
   - Mettez en place des procédures pour analyser les faux positifs générés par le modèle. Ceci peut inclure des mécanismes de retour d'information pour améliorer la précision du modèle au fil du temps.
9. **Livrables et attendus:** La livraison du projet comprendra un rapport détaillé sur le modèle d'IA, son intégration dans la passerelle email, les résultats de détection de phishing, des exemples d'adaptation dynamique, et un démonstrateur du système en action.

L'évaluation portera sur l'efficacité de la détection de phishing, la capacité d'adaptation aux nouvelles tactiques d'attaque, la gestion des faux positifs, la stabilité en production, et la documentation complète du projet. Ce projet offre une expérience pratique dans l'application de l'IA à la cybersécurité pour la protection contre les attaques de phishing.

Projet 15 : Développement d'une Plateforme de Commerce Électronique Évolutive

Profil : Dev

Objectif du Projet : L'objectif principal de ce projet est de concevoir et de développer une plateforme de commerce électronique évolutive qui peut gérer de manière efficace et sécurisée une grande variété de produits. La plateforme doit offrir une expérience utilisateur exceptionnelle, des fonctionnalités de gestion robustes et être capable de s'adapter à une augmentation significative du volume de transactions.

Étapes du Projet :

1. **Analyse des Besoins et Conception :**
   - Effectuez une analyse approfondie des besoins du commerce électronique, y compris les fonctionnalités nécessaires pour les utilisateurs (clients, administrateurs) et les exigences de sécurité. Concevez l'architecture de la plateforme en utilisant des pratiques de conception évolutives.
2. **Choix de la Technologie :**
   - Sélectionnez les technologies appropriées pour le développement de la plateforme, y compris le choix du langage de programmation, de la base de données, du framework web, et d'autres composants nécessaires.
3. **Développement du Frontend :**
   - Développez une interface utilisateur conviviale en utilisant des technologies modernes telles que React, Angular ou Vue.js. Assurez-vous que l'interface est réactive, intuitive et compatible avec différents appareils.
4. **Développement du Backend :**
   - Implémentez la logique métier et les fonctionnalités côté serveur en utilisant des frameworks tels que Django, Ruby on Rails, ou Spring Boot. Intégrez des fonctionnalités telles que la gestion des utilisateurs, le traitement des paiements, et la gestion des commandes.
5. **Intégration de la Gestion des Produits :**
   - Mettez en œuvre un système robuste de gestion des produits qui prend en charge divers types de produits, des variantes, des promotions, et des informations détaillées sur les produits. Assurez-vous que la plateforme est extensible pour ajouter de nouveaux types de produits.
6. **Intégration des Services de Paiement :**
   - Intégrez des services de paiement sécurisés tels que Stripe, PayPal, ou d'autres solutions de paiement en ligne. Assurez-vous de respecter les normes de sécurité et de conformité.
7. **Mise en Place de la Sécurité :**
   - Mettez en œuvre des mesures de sécurité telles que le chiffrement des données, la gestion des sessions sécurisée, la protection contre les attaques CSRF, et la validation rigoureuse des entrées utilisateur.
8. **Optimisation des Performances :**
   - Optimisez les performances de la plateforme en utilisant des techniques telles que la mise en cache, la compression des ressources, et l'optimisation des requêtes de base de données. Assurez-vous que la plateforme peut évoluer pour gérer un trafic accru.
9. **Tests et Assurance Qualité :**
   - Réalisez des tests approfondis, y compris des tests d'unité, des tests d'intégration, des tests de système, et des tests de charge pour garantir la fiabilité et la stabilité de la plateforme.

10. **Livrables et attendus :** La livraison du projet comprendra la plateforme de commerce électronique entièrement fonctionnelle, la documentation complète du code source, les résultats des tests, et un guide d'utilisation pour les administrateurs et les utilisateurs.

L'évaluation portera sur la qualité de l'interface utilisateur, la robustesse de la plateforme, la sécurité, les performances, la gestion des produits, et la documentation du projet. Ce projet offre une expérience pratique dans le développement d'une application web complexe et évolutive.

Projet 16 : Construction d'une Plateforme d'Apprentissage en Ligne (E-Learning)

Profil : Dev

Objectif du Projet : L'objectif principal de ce projet est de concevoir et de développer une plateforme d'apprentissage en ligne innovante qui offre une expérience éducative interactive et personnalisée. La plateforme devrait prendre en charge plusieurs types de contenus éducatifs, des fonctionnalités de suivi des progrès des étudiants et des outils d'interaction en temps réel.

Étapes du Projet :

1. **Analyse des Besoins et Conception :**
   - Menez une analyse approfondie des besoins éducatifs, des caractéristiques spécifiques à la plateforme, et des exigences en matière d'interaction. Concevez l'architecture de la plateforme en utilisant des pratiques adaptées aux environnements d'apprentissage en ligne.
2. **Choix de la Technologie :**
   - Sélectionnez les technologies appropriées pour le développement de la plateforme, en tenant compte des exigences de contenu multimédia, d'interactivité et de gestion des utilisateurs. Considérez l'utilisation de frameworks comme Django, Ruby on Rails, ou Laravel.
3. **Gestion des Cours et Contenus :**
   - Mettez en œuvre un système de gestion des cours qui prend en charge la création, la publication et la gestion de divers types de contenus éducatifs, y compris des vidéos, des documents, et des quiz interactifs.
4. **Personnalisation de l'Expérience Éducative :**
   - Intégrez des mécanismes de personnalisation pour adapter l'expérience éducative en fonction des préférences des étudiants, de leur niveau de compétence et de leurs performances antérieures.
5. **Suivi des Progrès et Évaluation :**
   - Implémentez des fonctionnalités de suivi des progrès des étudiants, des évaluations automatisées, et des retours personnalisés pour améliorer l'engagement et faciliter l'évaluation.
6. **Interaction en Temps Réel :**
   - Intégrez des outils d'interaction en temps réel tels que des salles de classe virtuelles, des forums de discussion, et des sessions de questions-réponses en direct pour favoriser la collaboration et la participation.
7. **Système de Gestion des Utilisateurs :**
   - Mettez en place un système de gestion des utilisateurs robuste, avec des rôles définis (enseignant, étudiant, administrateur), une authentification sécurisée et une gestion des droits d'accès.
8. **Intégration des Technologies Éducatives :**
   - Intégrez des technologies éducatives innovantes, telles que la réalité virtuelle (VR), la réalité augmentée (AR), ou des algorithmes d'adaptation intelligente pour enrichir l'expérience d'apprentissage.
9. **Tests et Assurance Qualité :**
   - Réalisez des tests approfondis, y compris des tests d'acceptation utilisateur, des tests de performance et des tests de sécurité pour garantir la fiabilité et la qualité de la plateforme.
10. **Livrables et attendus :** La livraison du projet comprendra la plateforme d'apprentissage en ligne entièrement fonctionnelle, la documentation complète du code source, les résultats des tests, et des guides d'utilisation pour les enseignants et les étudiants.

L'évaluation portera sur la qualité de l'expérience éducative, la facilité d'utilisation, l'efficacité des fonctionnalités personnalisées, la sécurité, les performances, et la documentation du projet. Ce projet offre une expérience pratique dans le développement d'une plateforme d'apprentissage en ligne moderne et interactive.