PROJET D'ETUDES
CADRE PEDAGOGIQUE
MODALITES D'EVALUATIONS
MASTÈRE CYBERSECURITE

I. OBJECTIFS DU PROJET

Ce projet a pour finalité de :

- Mettre les étudiants en **situation d'expertise technique et méthodologique** sur un projet complet de leur domaine (Dev, DevOps, Cybersécurité, Chef de Projet, Big Data/IA).
- Favoriser la mobilisation **transversale** des compétences acquises en formation : analyse, conception, développement, déploiement, documentation, communication.
- Développer une **posture professionnelle** : prise d'initiative, travail en équipe, gestion de la relation "client", production de livrables à forte valeur ajoutée.
- Ancrer les apprentissages dans une **démarche d'amélioration continue** : remise en question, qualité, performance, réutilisabilité, documentation.

II. OBJECTIFS PEDAGOGIQUES

À l'issue du projet, les étudiants seront capables de :

- **Évaluer** un besoin complexe en identifiant les enjeux métiers, les contraintes techniques et les attentes implicites du client, afin d'élaborer un diagnostic fonctionnel précis.
- **Formuler** une solution technique argumentée en mobilisant des connaissances expertes et en justifiant les choix technologiques selon des critères de performance, maintenabilité, sécurité et évolutivité.
- **Planifier** et **organiser** de manière autonome l'ensemble des étapes d'un projet informatique, en appliquant des méthodologies agiles ou hybrides et en s'appuyant sur des outils professionnels de gestion.
- **Mettre en œuvre** une solution technique avancée (prototype ou livrable finalisé), en assurant la sécurisation des composants, la traçabilité des actions, la réalisation de tests de sécurité, la production de documentation technique et post-incident, et en garantissant la conformité et la reproductibilité du dispositif.
- **Présenter** et **défendre** leur solution de façon claire, convaincante et adaptée à différents publics (experts, clients, utilisateurs), en valorisant leur posture professionnelle et leur contribution au projet.
- **Critiquer** leur propre travail et celui de l'équipe en identifiant les réussites, les limites et les axes d'amélioration, tout en **formalisant** les compétences techniques et comportementales mobilisées au cours du projet.

III. ORGANISATION DES EQUIPES

L'équipe projet est composée de 2 à 4 maximum.
La constitution des groupes se fait au lancement du projet (kick-off).

IV. LES LIVRABLES - ÉTAPES DU PROJET

Les étapes ci-dessous sont adossées à des évaluations certifiantes en lien avec les blocs de compétences :

	Evaluation certifiante adossée à l'étape
1. **Vidéo & démo du projet -MVP- :** Vidéo 15-20 min présentant le MVP avec prise de parole individuelle. ex : Simulation d'attaque, réponse active, présentation des outils (SIEM, IAM, reverse).	Oui (Rendu)
2. Livrable final : Rapport technique complet : analyse des vulnérabilités potentielles, plan de défense proposé, configuration, architecture, logs, Dossier de sécurisation du SI avec outils, rôles, procédures, REX…	Oui (Rendu)

V. EVALUATIONS DU PROJET

L'évaluation du projet d'étude est découpée en plusieurs livrables certifiants correspondant aux blocs de compétences.

Chaque livrable, écrit ou oral, collectif ou individuel, est évalué via une grille spécifique reprenant les compétences correspondant à chacun des blocs.

VI. LES ETAPES CHRONOLOGIQUES DU PROJET

Toutes les dates sont indicatives et peuvent varier en fonction de la planification des campus et des disponibilités des intervenants

VI.1 – KICK-OFF

Calendrier : *Début d'année*

Objectif : Présentation de l'objectif du projet et du sujet et constitution des groupes

Conseils : Visez la complémentarité des expertises dans vos groupes.

VI.2 - VIDEO & MVP – SAVOIR CONVAINCRE

Calendrier : *Kick off + 6 mois*

Objectifs : Créer une vidéo professionnelle de 15 à 20 min à destination du client, montrant une démonstration du MVP (simulation d'attaque, détection, réponse coordonnée…).

Modalités :

- Screencast de la solution, prise de parole de chaque membre (avec nom affiché), structuration claire (besoin → solution → démo).
- Tous les participants du projet doivent parler et un affichage doit apparaitre avec le nom de la personne au minimum

Livrables attendus : Vidéo .MP4 ou lien vers vidéo youtube en mode non publié.

Forme du livrable :

- Solution 1 : Un fichier Zip contenant la vidéo du groupe.
    - Nomenclature du zip : PE_2526_codepromo(ex : M1DEVA)_nometudiant1_nometudiant2_nom(etc…).zip
    - Nomenclature de la vidéo : PE-2526_codepromo_NomPrenomEtudiant.mp4

OU

- Solution 2 : Un document TXT contenant le lien vers la vidéo du groupe.
    - A héberger sur youtube en mode Non Répertoriée. Toute autre plateforme ne sera pas validée.
    - Nomenclature du document : PE_2526_codepromo(ex : M1DEVA)_nometudiant1_nometudiant2_nom(etc…).txt

Plan :

- Présentation de l'entreprise et de l'équipe projet
- Analyse de la problématique et introduction à la solution proposée
- Organisation et méthodologies appliquées

Présentation de la solution technique

Conseils : répétez, soignez le son et les visuels, mettez en scène la fiabilité de votre système. Appuyez-vous sur les logs, dashboards, et résultats de tests pour convaincre.

VI.2 - DOCUMENT TECHNIQUE FINAL

Calendrier : *Kick off + 6 mois*

Objectifs :

- Identifier les surfaces d'attaque potentielles
- Formuler des hypothèses de compromission
- Proposer une stratégie défensive
- Détailler les outils, les configurations et les procédures de défense active
- Créer le plan de supervision et d'alerte
- Consolider l'ensemble du dispositif technique
- Fournir une restitution professionnelle.

Modalités :

- Rapport complet : schéma d'architecture sécurisée (SD-WAN, pare-feu, filtrage), configurations, outils, journaux, tests de charges/sécurité
- REX détaillé avec analyse des incidents simulés
- Planning de déploiement, responsabilité par rôle
- Scripts et documentation des outils (ELK, Splunk, Snort...)
- Documentation complète pour audit

Exemples de livrables attendus en fonction du projet :

- Code de configuration, rapports de forensique
- Tableaux de supervision
- Documentation utilisateur & technique

- Backlog
- Diagrammes
- Rôles dans l'équipe

Forme du livrable :

- Un fichier Zip contenant un rendu groupe (pdf) et un rendu par membre du groupe (voir plan).
- Nomenclature du zip :
  PE_2526_codepromo(ex : M1DEVA)_nometudiant1_nometudiant2_nom(etc…).zip
- Nomenclature du document groupe :
  PE-2526_codepromo_ nometudiant1_nometudiant2_nom(etc…).pdf
- Nomenclature des documents apprenants :
  PE-2526_codepromo_NomPrenomEtudiant.pdf

Plan :

- Rendu groupe :
  - Présentation de l'entreprise et de l'équipe projet
  - Analyse de la problématique et introduction à la solution proposée
  - Gestion des coûts (M2)
  - Organisation de l'équipe, planification détaillée et méthodologies appliquées
  - Présentation de la solution technique

- Rendu individuel :
  - Perspectives d'évolution et réflexion sur l'avenir de l'infrastructure ou de la solution proposée
  - Analyse critique sur les limites techniques rencontrées
  - Annexes :
    - Documentation utilisateur
    - Analyse personnelle
      - Reflexion sur les défis rencontrés
      - Identification des forces et faiblesses personnelles
      - Compétences développées
      - Axes d'améliorations personnels pour de futurs projets

Conseils : Structuration, lisibilité, clarté sont clés. Travaillez comme un prestataire externe.

ANNEXES ET CONSEILS COMPLEMENTAIRES

Cette catégorie sert simplement d'exemple, de tips de ce que vous seriez amenés à produire en fonction du projet.

1.1. Analyse du sujet – Clarification du besoin

Objectif : Identifier les contraintes d'infrastructure, de sécurité, de disponibilité et de scalabilité.

Exemples :

– Quels types de menaces doivent être anticipés (DDoS, phishing, RCE...) ?
– Le SI doit-il être segmenté ou cloisonné ?
– Quels protocoles d'authentification sont en place ?

Cours associés : Cryptologie, IAM, Management de la sécurité, PRA/PCA, SD-WAN.

2.1. Vidéo & démonstration – Posture professionnelle

Vidéo de 15 à 20 minutes destinée au client, structurée (besoin → solution → démo) avec participation de tous les membres.

Montrer la détection, l'analyse, la réponse, et les décisions prises.

L'objectif est de prouver la pertinence de la solution et de convaincre en adoptant une posture professionnelle.

Cours associés *:* *Hacking, SIEM, Firewall, Red Team, Blue Team, Reverse Engineering, SIEM, Reponse à l'incident, Forensique...*

3.1. Livrable technique final – Code, documentation et analyse

À fournir :

- Rapports forensiques
- Scripts de remédiation
- Journaux d'événements
- Documentation post-incident
- Architecture réseau, firewalls, segmentation
- Supervision (SIEM, alerting, corrélation)
- Scripts et politiques de sécurité

Bonnes pratiques :

- Utiliser des logs contextualisés (ELK, Graylog)
- Tester les attaques et valider les réponses.

Cours associés : *SIEM, Firewall, Firewalling applicatif, Cryptologie 1, Red Team,IAM, DevSecOps, Reverse Engineering, Management de la sécurité*

4.1. Tableau de correspondance – Livrables / Cours

Élément clé	Cours associés
Cadrage fonctionnel / Analyse du sujet	Cryptologie, Management de la sécurité, PRA/PCA, SD-WAN
Architecture & planification technique	Blue Team, SIEM, IAM, DevSecOps
Présentation & démonstration	Reponse à l'incident, Forensique, Reverse Engineering
Documentation & livrable technique final	IAM, Management sécurité, DevSecOps