| SAE Architecture système réseau et sécurité | Semestre 6 | **Responsable :** Jérôme RIDET |
|---|---|---|

**Objectifs de la SAE en termes de compétences et d'acquis d'apprentissage visés**

**A l'issue de cette SAE, l'apprenant aura progressé sur les compétences suivantes du référentiel de la formation :**

- BC1.1 : Manager une équipe de collaborateurs et contribuer au développement des diverses compétences collectives et individuelles (Notion - non essentielle)
- BC1.3 : Identifier les éléments de contexte d'un projet et les formaliser : besoins exprimés par un client, politique de l'entreprise, aspects réglementaires (Maîtrise)
- BC1.4 : Adopter un comportement éthique et transparent au regard de la responsabilité sociétale et environnementale (Notion - non essentielle)
- BC1.5. Appliquer des stratégies de pilotage de projets en mettant en œuvre des démarches d'innovation et de créativité. (Application - non essentielle)
- BC1.6. Structurer un discours et/ou un support en faisant preuve de clarté, de pédagogie et de concision. (Maîtrise)
- BC1.8 : Effectuer une recherche documentaire (Application)
- BC2.1 : Modéliser un problème ou un besoin fonctionnel exprimé par un client et spécifier une solution informatique (Application)
- BC2.2 : Étudier, comparer et sélectionner les outils et méthodes nécessaires à la conception, au développement et au test d'une solution informatique (Notion)
- BC2.4 : Documenter une étude et une solution informatique (Notion)
- BC2.5 : Analyser et identifier les aspects réglementaires et techniques (Notion)
- BC3.3 : Proposer, planifier et développer des évolutions (Notion)
- BC3.5 : Fiabiliser et sécuriser (Application)
- BC4.1 : Mettre en œuvre des outils d'analyse de la solution informatique et des solutions de communication avec le client pour suivre les évolutions (Notion)
- BC4.2 : Anticiper et prévoir les évènements impactant la solution informatique (Notion)
- BC4.4 : Administrer une solution informatique (Notion)
- BC4.5 : Former l'utilisateur à l'usage de la solution informatique (Application)

**Plus précisément, il sera capable de :**

- Chiffrer des données sensibles au repos et en transit, utilisation de certificats numériques pour authentifier les serveurs et les clients, implémentation de solutions de signature numérique pour garantir l'intégrité des données
- Mettre en place le protocole HTTPS pour chiffrer les communications web, utilisation de HSTS pour forcer le navigateur à utiliser HTTPS, implémentation de CSP (Content Security Policy) pour limiter les scripts et les contenus malveillants
- Segmenter le réseau en zones de sécurité distinctes, mettre en place des firewalls et des règles de filtrage, contrôle d'accès aux ressources réseau
- Mettre en place une authentification forte et multi-facteurs et utilisation de solutions SSO (Single Sign-On) pour simplifier la gestion des accès
- Mettre en place des solutions de surveillance et de détection d'intrusions et utilisation de checksums et de signatures numériques pour garantir l'intégrité des fichiers et des données

## Description de la SAE

Les étudiants sont mis en situation professionnelle en tant que salariés de l'entreprise sur laquelle s'appuie la situation soit en tant que pirate informatique visant l'organisation. La situation est découpée en missions menant à des recherches documentaires, de la création de procédures à destination des salariés de l'entreprise, des tests de sécurité visant à améliorer la sécurité périmétrique. Un rapport est également à fournir au chef d'entreprise qui n'est pas spécialiste du domaine afin de lui présenter les diverses activités réalisées durant la situation proposée.

La situation d'évaluation est réalisée de façon individuelle mais des échanges avec le groupe sont indispensables.

Contexte de la situation :

Le système d'information de l'entreprise est actuellement exposé à plusieurs risques de sécurité, tels que :

- Fuites de données sensibles

- Attaques par injection SQL

- Détournement de session

- Malware et ransomwares

- Attaques par déni de service

La solution proposée consiste à mettre en place une série de mesures de sécurité pour contrer les risques identifiés.

Le projet sera réalisé en plusieurs phases :

- Phase 1 : Analyse des besoins et des risques

- Phase 2 : Conception de la solution

- Phase 3 : Déploiement de la solution

- Phase 4 : Formation des utilisateurs

- Phase 5 : Prévision de la maintenance et suivi de la sécurité

**Prérequis**

Fondements de la sécurité, Développement web, Réseaux TCP/IP

**Références**