Développer son projet professionnel

Sommaire :

Partie 2 : Définition des objectifs professionnels (30 min)

1- Identification des points forts et des axes d'amélioration.

J'ai des points forts dans les techniques tel que la Cybersécurité ou bien l'Administration réseau ou même dans les matières générales tel que le Français ou bien les Mathématiques.
Cependant, j'ai des difficultés à m'exprimer à l'oral, ce qui peut être problématique en entreprise.

2- Élaboration d'un projet professionnel en répondant aux questions suivantes :

- **Quelle formation envisagez vous ?**

Après mon BTS, j'ai été accepter à la licence professionnelle MI-ASSR à Sophia-Antipolis (Licence Professionnelle – IUT). Dans cette formation, il y a les matières importantes pour mon futur emploi tel que l'administration réseau et la cybersécurité (pentesting).

- **Quel métier ou domaine me motive ?**

Le domaine qui me motive est la cybersécurité, c'est une métier qui devient de plus en plus important et essentiel pour la vie de tous les jours et en entreprise.
Le métier que j'aimerai faire c'est Pentester car on se mets à la place du hacker afin de pouvoir trouver les vulnérabilités de notre réseau.

- **Quelles compétences dois-je renforcer ou acquérir ?**

Je dois renforcer et acquérir de nombreuses connaissances en cybersécurité, car en BTS on en se spécialise soit dans le développement soit dans le réseau. Mais on a que peu de cours en cybersécurité et se n'est pas forcement du pentesting, avec le BTS je ne pourrai pas demander un emploi dans la cybersécurité (les entreprises cherchent une personne avec un BAC+5 minimum).

- **Quels moyens puis-je mettre en œuvre (formation, stage, veille technologique...) ?**

Il existe tellement de moyens, tel que :
- Formation : à l'aide de certification exemple : Cyber-Ops sur Skills for all
-Stage : entreprise spécialisée dans la cybersécurité et réseau

-Veille technologique : sécurité des mails grâce à l'IA, ce qui a un rapport avec mon projet professionnel

3- Travail sur la formation professionnelle et l'entrepreneuriat :

- Recherche des différentes formations disponibles après un BTS SIO (licence, certification, formation continue).

Lien : Que faire après un BTS SIO ? Les débouchés et poursuites 2025
Que faire après un BTS SIO ? - L'Etudiant

- Licence pro systèmes informatiques et logiciels ;
- Licence pro réseaux et télécommunications ;
- Licence pro automatique et informatique industrielle ;
- Licence informatique ;
- Licence pro métiers de l'informatique : administration et sécurité des systèmes et des réseaux,
- Licence pro métiers de l'informatique : conduite de projets,
- Licence pro métiers de l'informatique : systèmes d'information et gestion de données,
- Licence pro métiers des réseaux informatiques et télécommunications,
- Classe préparatoire ATS ingénierie industrielle (en vue d'intégrer une école d'ingénieurs).

- Étude des dispositifs de financement et d'accompagnement pour la formation professionnelle.

(Les dispositifs de financement de la formation continue | enseignementsup-recherche.gouv.fr)

Les financements de la formation continue sont nombreux (C.P.F., CIF, etc.). Ils dépendent de la situation des candidats (salarié, demandeur d'emploi, etc.), qui peuvent être guidés dans leur recherche par les services universitaires de formation continue.

- Consultation et analyse du site officiel du ministère du Travail : Formation professionnelle - principes généraux.

La formation professionnelle est un outil majeur à la disposition de tous les actifs : salariés, indépendants, chefs d'entreprise ou demandeurs d'emploi. Elle permet de se former tout au long de son parcours professionnel, pour développer ses compétences et accéder à l'emploi, se maintenir dans l'emploi ou encore changer d'emploi.

- Introduction à l’entrepreneuriat dans l’informatique : création d’entreprise, auto-entrepreneuriat, incubateurs.

Auto-entrepreneur en informatique : le guide 2024

Quelles sont les missions d’un auto-entrepreneur en informatique ?

-Un auto-entrepreneur en informatique désigne un prestataire qui peut proposer les services suivants:
-le dépannage informatique, l’assistance, la réparation et le remplacement de matériel ou d’outils informatiques ;

-la formation et le conseil pour expliquer le fonctionnement des matériels et des logiciels professionnels ou non professionnels, dans le cadre des services à la personne ;

-la vente de matériel informatique, tels que des processeurs ou des écrans ;

des activités de support technique comme l’installation de logiciels et les mises à jour.

- Étude de cas : parcours d’un entrepreneur en informatique.

Auto-entrepreneur en informatique : le guide 2024

Quelles sont les qualités requises pour créer son auto-entreprise d’informatique ?

Il est recommandé de rassembler les compétences et qualités suivantes :

- Être à l’aise avec l’outil informatique : cela implique de maîtriser les techniques de base de dépannage informatique, ainsi qu’être capable d’utiliser, monter et démonter un ordinateur ou divers périphériques ;

- Avoir des connaissances de base en matière de logiciels et l’utilisation d’Internet ;

- Rester constamment informé des dernières avancées technologiques, car ce domaine évolue rapidement et requiert une expertise technique.

Cependant, ces compétences techniques ne suffisent pas à garantir le succès :

- Il faut faire preuve de réactivité et de disponibilité : certains de vos clients seront novices en informatique, il sera donc nécessaire de prendre le temps de comprendre précisément la source de leurs problèmes.

-Et faire preuve de pédagogie : vous serez souvent amené à conseiller vos clients sur le choix du matériel adapté ou à leur proposer des alternatives aux outils qu'ils utilisent déjà. Or tous ne s'y connaissent pas forcément dans le domaine.

4- Étude du choix du métier sur le site France Travail :

Fiche métier Administrateur / Administratrice réseau informatique | MétierScope par France Travail

J'ai choisi pentester :

- Recherche et analyse des perspectives d'emploi selon les métiers du numérique.

Pentester : Rôles, Compétences et Perspectives de Carrière

Les perspectives de carrière pour un Pentester

Le pentesting est un domaine en pleine croissance, riche en **opportunités de pentesting**. Les entreprises de différents secteurs cherchent des testeurs d'intrusion. Ils jouent un rôle clé pour protéger les systèmes informatiques contre les cyberattaques.

Les opportunités d'emploi dans différents secteurs

Les pentesters trouvent des postes intéressants dans le numérique, les banques, le gouvernement, et la défense. Ces postes apprécient leur capacité à être rapides et précis. Ceci est crucial pour un *consultant en sécurité* ou un *chef de projet en sécurité*.

L'évolution de carrière possible

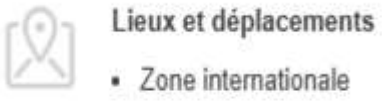
Le pentesting peut conduire à des postes à haute responsabilité, comme **chef de projet en sécurité**. Il est aussi possible de devenir **consultant en sécurité**, aidant à créer des stratégies de sécurité pour les entreprises. En outre, devenir un **expert en cybersécurité** est envisageable après avoir acquis des compétences avancées. Ils travaillent avec les équipes bleues pour renforcer les défenses.

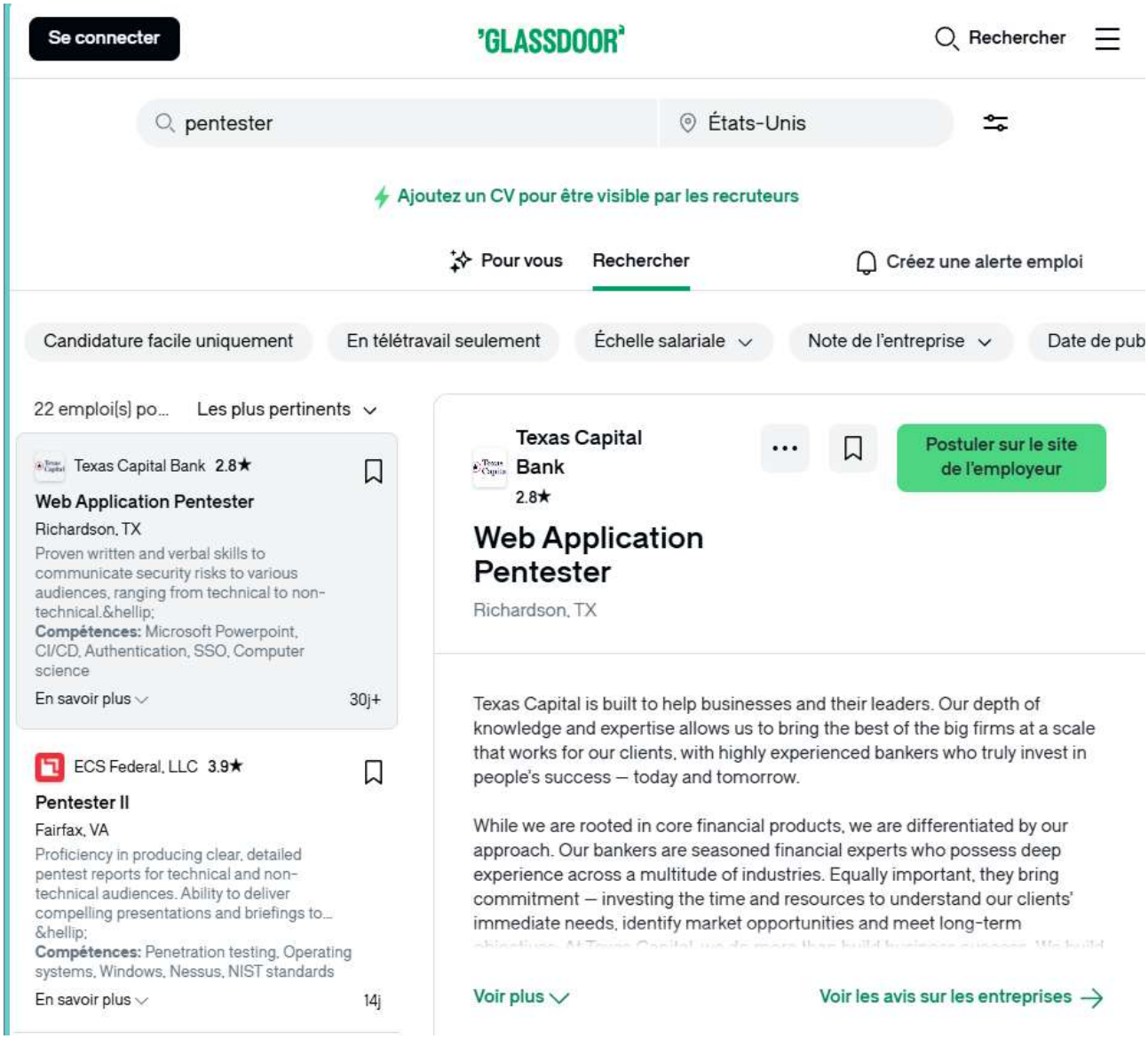
- Identification des compétences attendues.

- Conditions de travail et salaires moyens.

Le salaire d'un débutant peut fluctuer entre **3 000 € et 3 500 € par mois**. Par an, un pentester junior peut donc gagner entre 36 000 € et 42 000 €. Les pentesters expérimentés peuvent toucher entre 4 000 € et 4 500 € par mois, soit une rémunération comprise entre 48 000 € et 54 000 € par an.

- Mobilité géographique et opportunités à l’international.





- Consultation du site [France Travail] pour une analyse approfondie.

Autres emplois décrits

- Analyste en vulnérabilité de code logiciel
- Auditeur / Auditrice en sécurité des systèmes d'information
- Auditeur / Auditrice en système d'information
- Auditeur / Auditrice Sécurité des systèmes d'information (SSI)
- Auditeur informaticien / Auditrice informaticienne
- Expert / Experte en tests d'intrusion - sécurité des systèmes d'information
- Pentesteur
- Post auditeur / Post auditrice en sécurité des systèmes d'information

Définition

L'Évaluateur / Évaluatrice sécurité des systèmes et produits informatiques joue un rôle crucial dans la protection des infrastructures numériques.

- Analyse et évalue les risques de sécurité des systèmes et produits informatiques
- Réalise des audits de sécurité pour identifier les vulnérabilités et les failles
- Propose des solutions pour renforcer la sécurité et prévenir les attaques informatiques
- Effectue des tests d'intrusion pour évaluer la robustesse des systèmes face aux tentatives d'effraction
- Documente les procédures de sécurité et forme les utilisateurs aux bonnes pratiques de sécurité
- Collabore avec les équipes de développement pour intégrer la sécurité dès la conception des produits

Accès à l'emploi

Cet emploi est accessible avec une Licence Professionnelle en Sécurité des systèmes d'information, un Master en Sécurité informatique ou un Diplôme d'Ingénieur en Informatique spécialité sécurité.

Certifications et diplômes :

- Licence pro mention métiers de l'informatique : administration et sécurité des systèmes et des réseaux
- Licence pro mention métiers de l'informatique : systèmes d'information et gestion de données
- Licence pro mention métiers des réseaux informatiques et télécommunications
- Certificat de compétence analyste en cybersécurité
- Mastère spécialisé cybersécurité
- Mastère spécialisé cybersécurité et cyberdéfense
- Mastère spécialisé sécurité informatique
- Expert en cybersécurité
- Expert en cybersécurité des systèmes d'information
- Expert en sécurité des systèmes d'information
- Ingénieur diplômé de l'institut national des sciences appliquées Centre Val de Loire spécialité sécurité informatique
- Ingénieur diplômé de l'institut national des sciences appliquées Hauts-de-France spécialité informatique et cybersécurité (Université polytechnique Hauts-de-France)
- Spécialiste en cybersécurité

Compétences

Savoir-faire

Prévention des risques	**Évaluer, prévenir, et gérer les risques et la sécurité** **Analyser les risques de sécurité pour les systèmes informatiques** Mener un processus de test en cybersécurité Développer des stratégies de mitigation des risques
Data et Nouvelles technologies	**Analyser les logs pour identifier les tentatives d'intrusion** Utiliser des outils de cryptographie pour sécuriser les données **Tester un logiciel, un système d'informations, une application** Faciliter l'intégration de solutions d'intelligence artificielle dans les projets existants Émergent
Droit, contentieux et négociation	**Veiller au respect de la loi Informatique et Libertés et du RGPD dans l'entreprise, gérer la liste des traitements de données à caractère personnel, faire l'interface avec la Commission Nationale de l'informatique et des Libertés - CNIL**
Qualité	**Réaliser des audits de sécurité pour identifier les vulnérabilités** Contrôler la qualité et la conformité des process
Recherche, Innovation	**Participer à des conférences sur la sécurité pour rester informé des dernières menaces** Réaliser une veille technique ou technologique pour anticiper les évolutions Tester la résilience des systèmes face aux attaques simulées
Conseil, Transmission	**Sensibiliser et former les personnels aux consignes de sécurité et de prévention**
Stratégie de développement	Superviser les équipes de sécurité lors des audits externes
Organisation	Documenter les procédures de sécurité pour le personnel technique Documenter les interventions et les anomalies rencontrées Documenter les procédures techniques et configurations Documenter les procédures de sécurité pour les utilisateurs

Savoir-être professionnels

	Faire preuve d'autonomie Faire preuve de réactivité Faire preuve de rigueur et de précision Prendre des initiatives et être force de proposition

Savoirs

Domaines d'expertise	Gestion des accès et identités Gestion des vulnérabilités Systèmes de gestion de base de données Protection contre les malwares Sécurité des applications mobiles Sécurité des communications unifiées Sécurité des infrastructures critiques Sécurité des paiements en ligne Sécurité des serveurs web Sécurité des systèmes embarqués Sécurité des transactions électroniques Systèmes d'exploitation informatique Technologie de l'internet Réseaux informatiques et télécoms Audit des systèmes d'information Sécurité des réseaux sans fil
Normes et procédés	Cryptographie appliquée Détection des intrusions réseau Gestion des risques (Risk Management) Normes de sécurité Procédures de tests Procédures qualité et sécurité des systèmes d'information et de télécoms Protection des données personnelles Règles de sécurité Informatique et Télécoms Sécurité physique des systèmes informatiques

Contextes de travail

	Conditions de travail et risques professionnels	Travail en mode projet
	Horaires et durée du travail	Travail en journée
	Lieux et déplacements	Zone internationale
	Statut d'emploi	Salarié secteur privé (CDI, CDD)