# COMMENT T’AIDER TOI MEME A TROUVER UNE SOCIETE POUR UNE FORMATION EN APPRENTISSAGE DANS LE DOMAINE INFORMATIQUE/CYBERSECURITE

# CHECKLIST PORTFOLIO ÉTUDIANT (IT/Cyber)

**Identité & visibilité**  
- CV **1 page** FR + **photo pro**.  
- **LinkedIn** à jour (accroche orientée résultats, mots‑clés NIS2/Cloud/M365/AD).  
- **GitHub/GitLab/Autres** : Projets / dépôts propres (README, captures, résultats).

**Compétences & preuves**  
- **Matrice de compétences** (auto‑évaluation 1–5) : M365/Entra, AD/GPO, Linux, réseau, DNS/email, vulnérabilités, scripting (PowerShell/Python), SIEM, sauvegardes/PRA, conformité.  
- **Projets avec livrables** (1 dossier ou plus) - *Ex.* « DMARC end‑to‑end » (avant/après, rapports, DMARC Aggregate/Forensic anonymisés).  
- *Ex.* « Durcissement M365 » (Secure Score + plan d’actions).  
- *Ex.* « Test de restauration » (procédure & résultats).  
- **Indicateurs** : % MFA activé, DMARC en “reject”, temps de restauration, nb. vulnérabilités corrigées…

**Conformité & bonnes pratiques**  
- **NIS2 – “premiers pas”** : mini registre des risques, carto des actifs, rôles & responsabilités.  
- **Référentiels** : mapping simple vers **ISO/IEC 27001 Annexe A**/**ANSSI** (SecNumAcadémie validée).  
- **Sécurité personnelle** : 2FA, gestion secrets, hygiène poste (montrez l’exemple).

**Tech & outils**  
- Environnements : Windows Server/AD, Microsoft 365, Linux, virtualisation, cloud (Azure/Amazon/OVH/Scaleway).  
- Outils : **PowerShell**, Wireshark, OpenSSH, OpenVAS/Nessus (si permis), **Wazuh/ELK**, Rclone/restic, Postfix/Exchange Online.  
- **Scripts** utiles (anonymisés) + captures.

**Preuves externes**  
- Certifs/Badges : **ANSSI SecNumAcadémie**, AZ‑900/SC‑900, ITIL, Cisco, TryHackMe/HTB (profils).  
- **Recommandations** (profs, tuteurs de stage), attestations de projet.

**Logistique**  
- **Disponibilités** (rythme, date de début), localisation, travail sur site, **télétravail,** mobilité.  
- Pré‑onboarding : pièces RH prêtes (RIB, carte identité, convention, etc.).

**Pitch**  
- **One‑pager** « ce que je peux livrer en 90 jours » (menu + indicateurs + outils maîtrisés).

# 

# A L’ATTENTION DU RESPONSIBLE INFORMATIQUE/SECURITE DE SOCIETEX SAS

**Apprenti en cybersécurité & IT : Résultats concrets en 90 jours ou moins!**

|  |
| --- |
| **Les entreprises françaises sont attaquées chaque jour par des puissances et des groupes étrangers. Chaque jour, des organisations subissent des pertes d’accès à leurs données et ne peuvent plus opérer, entraînant pertes de chiffre d’affaires, licenciements, perte de confiance des clients et parfois fermeture de la société. De nombreuses réglementations complexes doivent être appliquées par les entreprises françaises (NIS2, RGPD, DORA, Data Act, HDS, etc.).** |

**Pourquoi maintenant ?  
NIS2, ransomware, M365/Active Directory à durcir, sauvegardes à tester… le temps interne manque souvent pour tout couvrir efficacement. Un(e) apprenti(e) encadré(e) peut livrer des « quick wins » — des succès rapides — sans désorganiser les équipes existantes. L’approche consiste à prioriser des mesures simples à fort impact pour améliorer rapidement la posture de sécurité.**

**Ce que nous livrons (menu de missions clés, au choix)**

* **Sécurisation e‑mail/DNS : SPF, DKIM, DMARC, MTA‑STS, TLS‑RPT, BIMI, avec rapport de configuration et de conformité.**
* **Durcissement Microsoft 365 / Entra ID : MFA / accès conditionnel, amélioration du Secure Score, exploitation des journaux d’audit et de connexion.**
* **Active Directory & postes : baseline de durcissement, LAPS, revues d’accès, rapport de sécurité GPO ; analyse passive de la sécurité d’Active Directory et production de rapports.**
* **Sauvegardes & PRA : vérification 3‑2‑1, tests de restauration, documentation pas à pas et consignes de reprise.**
* **Journalisation & détection : collecte de base (ex. Wazuh/ELK), tableaux de bord, alertes et procédures d’escalade.**
* **Conformité « premiers pas » NIS2 : inventaire des actifs, registre des risques, plan de réponse aux incidents et responsabilités.**
* **Sensibilisation des utilisateurs : kit phishing, mini‑charte mots de passe & mobile, atelier de 45 minutes ; création de supports de formation et/ou de vidéos.**
* **Création de rapports de sécurité : mise en place de rapports quotidiens ou hebdomadaires consolidant les systèmes sondés (indicateurs, tendances, écarts).**

IDEE DE FLYER PARTIE 1 PAR LA POSTE

UTILISER LE SITE PAPPERS.IN POUR TROUVER DES SOCIETES DANS VOTRE REGION

**Rythme & encadrement**  
- Rythme école/entreprise (ex. **3 semaines** en entreprise / **1 semaine** à l’école).  
- **Tuteur école** identifié : point hebdomadaire (30 min) + **revue mensuelle** des livrables.  
- **Confidentialité** : NDA + bonnes pratiques d’accès en environnements sensibles.

**Coûts & aides (indicatif)**  
- **Aide 1re année** (contrats signés en 2025) : **5 000 €** (<250 salariés) ou **2 000 €** (≥250), **6 000 €** si apprenti reconnu handicap.  
- **Participation employeur** formations **Bac+3 et + (niveaux 6–7)** : **750 €** par contrat (à verser au CFA).  
- **Exemple** (21–25 ans, 1re année) : rémunération env. **~53 % du SMIC (~955 € brut/mois)**. Charges employeur + tutorat à prévoir

**Démarrage en 2 semaines**  
1) Échange **30-60 min** pour cibler vos besoins.  
2) Sélection d’un **mini‑projet** (3 mois).  
3) Montage **OPCO/ASP** : on s’occupe de l’administratif.  
4) **Onboarding** + plan de livrables.

**Contact**  
[Nom & rôle] — [École/Promo] — [Téléphone] — [Email] — [Ville/Région]  
Options : visio Teams/Meet, déplacement sur site.

*Mentions* : Aides et participations selon textes en vigueur (2025), 1re année uniquement, conditions d’éligibilité et proratisation possibles. Vérification au cas par cas.

IDEE DE FLYER PARTIE 2 PAR LA POSTE

UTILISER LE SITE PAPPERS.IN POUR TROUVER DES SOCIETES DANS VOTRE REGION

# TEMPLATE D’EMAIL À FROIDS

Objet : Obtenez 5 quick wins cyber en 90 jours — sans alourdir vos équipes

Ou encore

Objet : Mini‑projet cyber (M365/AD/DMARC) avec apprenti encadré — éligible aux aides 2025

Bonjour [Nom],

« Dans ce contexte de **risques cyber croissants** et de **surcharge réglementaire** (NIS2, RGPD, DORA…), les societes peinent à dégager du temps pour durcir **leur infrastructure, Active Directory, Office 365, Azure, Amazon**, les emails, les services DNS et les **sauvegardes entre autres..**. »

Nous proposons une approche très pragmatique : **un apprenti IT/Cyber encadré** par notre école, qui livre en 3 mois un **mini‑projet** choisi parmi :  
• **SPF/DKIM/DMARC + MTA‑STS/TLS‑RPT** (avec rapport avant/après)  
• **Durcissement Microsoft 365 / Entra ID** (MFA, CA, journaux, Secure Score)  
• **Sauvegardes & test de restauration** (procédure, preuves)  
• **“Premiers pas” NIS2** (inventaire, risques, plan incident)

**Ce que ça change pour vous**  
- **Livrables mesurables**, validés chaque mois avec notre **tuteur école**.  
- **Paperasse prise en charge** (OPCO/ASP).  
- **Aide 1re année 2025** jusqu’à **5 000 € (<250)** ou **2 000 € (≥250)** (**6 000 €** si handicap).  
- Pour les diplômes **Bac+3 et +**, **participation 750 €** au CFA à prévoir (règle 2025).

Si vous êtes partant(e), je vous offre un **échange de 20 minutes** pour identifier 3 priorités et voir si un mini‑projet s’y prête.

**Créneaux proposés** : [mar 10:00–10:20] ou [jeu 14:00–14:20] (ou votre préférence).

Bien à vous,  
[Prénom NOM] — [Rôle, École]  
[Téléphone] · [Email] · [Ville]  
[LinkedIn]

P.-S. : Je joins un **one‑pager** (missions, coûts/ aides 2025) et 1 exemple de **rapport livré**.

« Pas d’engagement après l’échange ; nous pouvons commencer par **une immersion PMSMP de 1 à 4 semaines** (non productive, via convention), ou **un stage conventionné de 2 à 8 semaines** (gratification obligatoire au-delà de 2 mois), **ou** démarrer directement en **contrat d’apprentissage** avec **période probatoire de 45 jours (rémunérée)**. »

**EXEMPLE DE CV/ FAIT SIMPLE MAIS DROIT AU BUT**

**Marc CLÉMENT (21 ans)**  
Étudiant / futur ingénieur en cybersécurité  
Basé à Marseille.  
Français et anglais parlés couramment (n’indiquez pas les langues non maîtrisées)  
06 01 02 03 04 / <linkedin.com/in/marclementpro> / [marc.clement.pro@gmail.com](mailto:marc.clement.pro@gmail.com)

**SOMMAIRE**  
Actuellement en Bachelor de cybersécurité à l’école XYZ de Marseille, pleinement investi et sensibilisé aux enjeux de sécurisation des infrastructures, de protection des ressources et des employés au sein des entreprises. Spécialisé en sécurité des environnements et en administration des systèmes, avec un focus sur la gestion des identités, la sécurisation des flux de messagerie et le durcissement des systèmes.

**COMPÉTENCES TECHNIQUES**

* Administration Microsoft Azure, Microsoft 365 et Linux
* Active Directory, DNS, GPO
* Supervision: Nagios, Centreon
* SIEM: …
* Scripting / automatisation: PowerShell…

**EXPÉRIENCES PROFESSIONNELLES**

**Société XYZ – Marseille – Stagiaire administrateur systèmes (janvier 2025 – avril 2025)**

* Participation à l’administration quotidienne d’Active Directory et de Microsoft Exchange au sein d’une équipe de 7 personnes.
* Création de scripts d’automatisation réduisant les incidents grâce à des alertes proactives permettant d’anticiper les pannes avant leur survenue.

**Société ABC – Aix-en-Provence – Technicien réparation PC (juin 2024 – août 2024)**

* Contribution aux activités de réparation et de reconditionnement de PC de seconde main destinés aux étudiants, PME et personnes âgées.
* En me concentrant sur une même marque et des modèles identiques, amélioration de la performance et du nombre d’unités reconditionnées par jour de 30%.

**AUTRES EXPÉRIENCES**  
GitHub – Développement régulier et maintenance d’un lab virtuel comprenant des contrôleurs de domaine Active Directory (lien: unlien.com…