

Intitulé du stage : Intégration des référentiels CIS pour le renforcement de la cybersécurité

Référence de l'offre : DG-STA-2026-01

■ **Présentation de Santé publique France**

Santé publique France est l'Agence nationale de santé publique française. Etablissement public de l'Etat sous tutelle du ministre chargé de la santé créé par l'ordonnance 2016-246 du 15 avril 2016, elle intervient au service de la santé des populations.

Agence scientifique et d'expertise du champ sanitaire, elle a pour missions :

- 1° L'observation épidémiologique et la surveillance de l'état de santé des populations ;
- 2° La veille sur les risques sanitaires menaçant les populations ;
- 3° La promotion de la santé et la réduction des risques pour la santé ;
- 4° Le développement de la prévention et de l'éducation pour la santé ;
- 5° La préparation et la réponse aux menaces, alertes et crises sanitaires ;
- 6° Le lancement de l'alerte sanitaire.

L'Agence est organisée autour de quatre conseils (Conseil d'Administration, Conseil scientifique, Comité d'Ethique et de Déontologie et Comité d'orientation et de dialogue), de directions scientifiques et transversales, et de directions assurant le support et le soutien à l'activité. L'Agence dispose d'implantations régionales (Cellules régionales) auprès des agences régionales de la santé.

Son programme de travail, arrêté par son Conseil d'administration, s'articule autour de 6 enjeux : Anticipation, préparation et réponse aux menaces de santé publique, dont les épidémies ; Numérique en santé publique ; Santé environnementale, changement climatique et environnement de travail ; Fardeau des maladies et de leurs déterminants, efficacité des interventions et retour sur investissement de la prévention ; Stratégie de prévention, marketing social et approche par populations ; Inégalités sociales, vulnérabilités territoriales.

Son siège est situé à Saint-Maurice (94).

Localisation du stage :

- Saint-Maurice
 En région, indiquer la région, le département et la ville concernés :

■ **Le stage**

Contexte :

Santé Publique France, en tant qu'acteur majeur de la santé publique, manipule des données sensibles et doit garantir leur sécurité face aux cybermenaces croissantes. Les référentiels CIS (Center for Internet Security) sont reconnus internationalement pour fournir des bonnes pratiques et des configurations sécurisées pour les systèmes d'information. Leur intégration permet de réduire les risques de cyberattaques et d'améliorer la conformité aux réglementations en vigueur (RGPD, NIS2, etc.).

Ce stage s'inscrit dans une démarche proactive d'amélioration continue de la sécurité des infrastructures informatiques, en alignant les pratiques internes sur les recommandations CIS sur le parc des postes de travail.

Sujet du stage : Intégration des référentiels CIS pour le renforcement de la cybersécurité

Objectifs du stage :

1. **Analyse des référentiels CIS :**
 - Étudier les benchmarks CIS pertinents pour les systèmes Windows 11 utilisés par Santé Publique France (ex : CIS Controls, CIS Benchmarks pour Windows etc.).
 - Identifier les écarts entre les configurations actuelles et les recommandations CIS.
2. **Plan d'intégration dans l'outil d'audit :**
 - Prise en main de l'outil CyberWatch
 - Prioriser les actions en fonction des risques identifiés et des ressources disponibles.
 - Proposer un plan d'action pour l'application des configurations CIS (ex : durcissement des systèmes, gestion des vulnérabilités, surveillance continue).
3. **Mise en œuvre et tests :**
 - Configurer et tester des outils d'automatisation (ex : scripts PowerShell/Bash) pour appliquer les benchmarks CIS à partir de Cyberwatch
 - Documenter les procédures et les résultats des tests (avant/après).
4. **Sensibilisation et formation :**
 - Créer des supports de sensibilisation pour les équipes IT sur l'importance des référentiels CIS.
 - Organiser des ateliers ou des présentations pour partager les bonnes pratiques.
5. **Évaluation et recommandations :**
 - Mesurer l'impact des changements sur la sécurité et la performance des systèmes.
 - Créer les indicateurs de conformité
 - Rédiger un rapport final avec des recommandations pour une intégration pérenne des référentiels CIS.

Missions du stage :

- **Audit initial** : Cartographier les systèmes, et évaluer leur conformité aux benchmarks CIS.
- **Automatisation** : Développer des scripts ou utiliser des outils existants pour évaluer automatiquement les configurations CIS.
- **Collaboration** : Travailler avec les équipes IT pour valider les changements et minimiser les perturbations.
- **Documentation** : Rédiger des guides techniques et des procédures pour les équipes internes.
- **Veille technologique** : Suivre les mises à jour des référentiels CIS et les évolutions des menaces cybersécurité.

Livrables attendus :

- Un rapport d'audit initial avec identification des écarts.
- Un référentiel SPF dans Cyberwatch pour le contrôle de la conformité des postes Windows
- Des scripts ou playbooks pour l'évaluation des benchmarks CIS.
- Un guide de bonnes pratiques pour les équipes IT.
- Un rapport final avec bilan et recommandations.

Bénéfices pour le stagiaire :

- Expérience concrète en cybersécurité dans un environnement critique (santé publique).
- Maîtrise des référentiels CIS, très valorisés dans le domaine.
- Mise en place d'un processus de contrôle de conformité
- Participation à des projets impactant pour la sécurité des données sensibles.
- Possibilité de contribuer à des publications internes ou externes sur le sujet.

Description :

Pour tout renseignement complémentaire, consulter le portail sur le site <http://www.santepubliquefrance.fr>

■ Profil recherché

Étudiant(e) en dernière année d'école d'ingénieur ou master en informatique, spécialisé(e) en cybersécurité. Une première expérience en administration système ou en audit de sécurité serait un plus.

Gratification du stage : selon la réglementation en vigueur dans les établissements publics

■ Date proposée pour le stage et durée :

Sans contrainte de date

A partir de : janvier 2026

Durée minimum : 4 à 6 mois

Extension possible au-delà de la période obligatoire

Oui

Non

■ Prérequis :

Aucun

Compétences spécifiques (préciser) :

- Connaissances en cybersécurité (normes ISO 27001, RGPD, bonnes pratiques).
- Maîtrise des systèmes d'exploitation (Windows, Linux) et langage de scripts Powershell
- Capacité à analyser des logs et à utiliser des outils de scan de vulnérabilités (ex : Nessus, OpenVAS, CyberWatch).
- Rigueur, autonomie et esprit d'équipe.
- Bonnes compétences rédactionnelles pour la documentation technique.

Maîtrise d'un logiciel spécifique (préciser) :

Autre (préciser) :

■ Stage proposé par :

Direction : DG

Unité : CQMR

Maître(s) de stage / personne contact :

Nom : NARDY

Prénom : Stéphane

Fonction : RSSI

Téléphone : 0141795751

Adresse email : stephane.nardy@santepubliquefrance.fr

Co-encadrement

Nom :

Prénom :

Fonction :

Téléphone :

Adresse email :

■ Pour postuler

Adresser les candidatures (lettre de motivation + cv) en indiquant la référence de l'annonce par courriel : recrut@santepubliquefrance.fr