**Sécurité des Systèmes d'Information**

**Protection des données**

# Pourquoi et comment
# AGIR DÈS AUJOURD'HUI

TESIS
E-SANTÉ

# LE PITCH !

## pour tout comprendre en une minute

### CYBERSÉCURITÉ RISQUE IMMÉDIAT, CONSÉQUENCES GRAVES

Le secteur santé traverse une crise cyber durable. Des dizaines d'établissements sont touchés chaque année par des attaques informatiques qui peuvent paralyser les infrastructures techniques et stopper l'activité. Les dégâts se chiffrent alors en millions d'euros, mais surtout en vies humaines.
En cause : le manque de préparation et d'anticipation, et les défauts de conformité des structures de santé.

### RÉPONDRE À VOS BESOINS URGENTS

Dans ce contexte, le GCS TESIS lance une offre régionale pour aider vos établissements à assurer la sécurité des SI (SSI) et protéger les données personnelles de vos employés et usagers (PDP).

### UNE OFFRE À LA CARTE

Choisissez votre mode d'accompagnement : intervention ponctuelle **ou** régulière sur 3 ans dans le cadre d'un plan de mise à niveau.

### MUTUALISATION ET MAÎTRISE DES COÛTS

Une démarche régionale pour renforcer la cohérence de vos actions et diminuer l'impact financier pour vos structures :

INTERVENTION DU GCS TESIS :
→ Accompagnement par le GCS TESIS chiffré au temps passé, facturé à prix coûtant.

CATALOGUE DE PRESTATIONS EXTERNALISÉES
→ Prestations ponctuelles externalisées à tarifs négociés grâce aux procédures de marché simplifiées du GCS.

**TARIFS P. 26 - 27**

### APPROCHE GLOBALE DES RISQUES

Nous couvrons l'ensemble des vulnérabilités et des obligations légales : audit, détection des failles, gouvernance, gestion des incidents, plans de continuité mais aussi formation- sensibilisation professionnelle et information usagers.

### LES MEILLEURES INNOVATIONS DU MARCHÉ

Retrouvez sur catalogue des services spécialisés pour maximiser l'engagement et la sensibilisation de vos équipes (campagnes de phishing, e-Learning), mais aussi des prestataires solides pour vous épauler dans la gestion des incidents.

### ACCOMPAGNEMENT PERSONNALISÉ

Nous partons de vos besoins et de votre maturité pour dimensionner toutes nos interventions. **Vous ne payez que le nécessaire.**

### UN PÔLE D'EXPERTISE SSI & PDP

Coordonnée par le RSSI Régional, l'équipe Cybersécurité du GCS TESIS s'appuie sur des profils experts internalisés, formés spécialement aux enjeux des SI santé.

Nos experts peuvent :

→ **intervenir ponctuellement dans vos structures,**

→ **accompagner vos établissements dans la durée,**

→ **exercer les fonctions RSSI et DPD pour votre compte.**

## Quel est le prix de votre sécurité ?

### Prenons rendez-vous !

Mathias Laurent,
Responsable Régional de la Sécurité des Systèmes d'Information en Santé, est à votre disposition pour évaluer vos besoins.

**m.laurent@tesis.re**

**06 93 93 37 35**

# Sommaire



TESIS
E-SANTÉ

La sécurité des systèmes d'information et le respect des règles de confidentialité sont au cœur de nombreux enjeux pour les structures sanitaires et médico-sociales, quelle que soit leur taille.

Garantir la qualité et la sécurité des soins et de l'accompagnement aux usagers

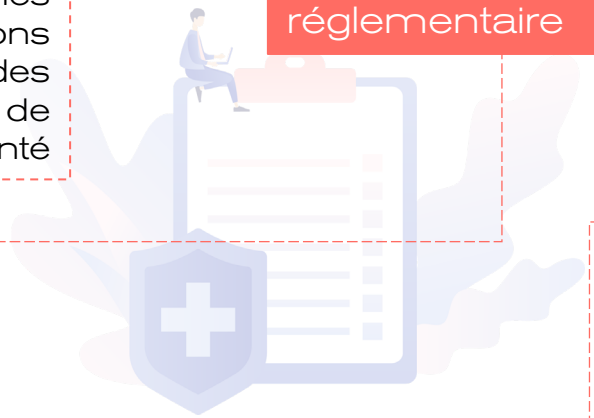
Améliorer les conditions d'exercice des professionnels de santé

Assurer votre conformité légale et réglementaire

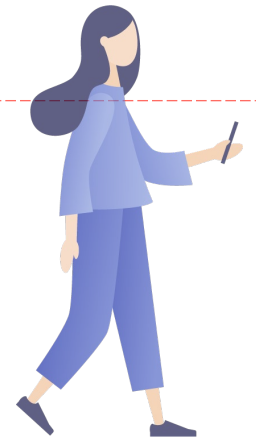
Vous prémunir de potentielles attaques, d'origine interne ou externe

Préserver vos ressources financières

Maintenir l'efficacité et la continuité opérationnelle de vos structures



Protéger la vie privée de vos employés, fournisseurs, partenaires et usagers



Protéger votre image et votre notoriété

Sécurité des Systèmes d'Information

Protection des données

# Pourquoi est-ce le moment d'agir ?

## 1. Le risque cyber est critique dans le secteur santé

Plus de 150 attaques par des rançongiciels ont frappé avec succès des établissements français depuis 2018, et les chiffres augmentent chaque année.

La menace atteint aujourd'hui un seuil critique, et peut être considérée comme immédiate.

Lorsqu'elles frappent des structures mal préparées, ces attaques ont de lourdes conséquences sur la prise en charge des usagers : arrêt de l'activité, indisponibilité des services informatiques, des plateaux techniques, de la climatisation…

Les impacts sont dévastateurs :

- Dégradation des prises en charge
- Pertes financières
- Image dégradée (ces attaques font l'objet d'une plus grande couverture médiatique)
- Etc.

## 2. Vos obligations légales deviennent opposables

La Politique Générale de Sécurité des Systèmes d'Information dans la Santé (PGSSI-S) et la Politique de sécurité des systèmes d'information des Ministères Sociaux (PSSI-MCAS) sont aujourd'hui opposables aux établissements de santé. Ils vous obligent à :

→ Mettre en place une gouvernance SSI

→ Gérer les risques SSI

→ Protéger les données et les systèmes

→ Sensibiliser et former la totalité des personnels

→ Auditer les vulnérabilités du SI

→ Gérer les incidents SSI

→ Sécuriser l'Identification et l' l'Authentification des acteurs

Certains de ces points ont fait l'objet d'un rappel dans le Message d'Alerte Rapide Sanitaire (MARS) du 6 avril 2020, adressé aux structures ultramarines**. D'autres font désormais partie des objectifs inscrits en annexe de vos CPOM avec l'ARS La Réunion.**

## 3. Un levier pour vos financement en matière de numérique

Dans le cadre du Ségur de la Santé et du Plan Ma Santé 2022, vos établissements peuvent financer la mise à niveau et le renouvellement d'équipements informatiques, et les travaux nécessaires pour s'inscrire dans la Doctrine Technique du Numérique en Santé.

Pour être éligible aux programmes suivants, vous devez remplir vos obligations en matière de cybersécurité et de protection des données :

→ HOP'EN

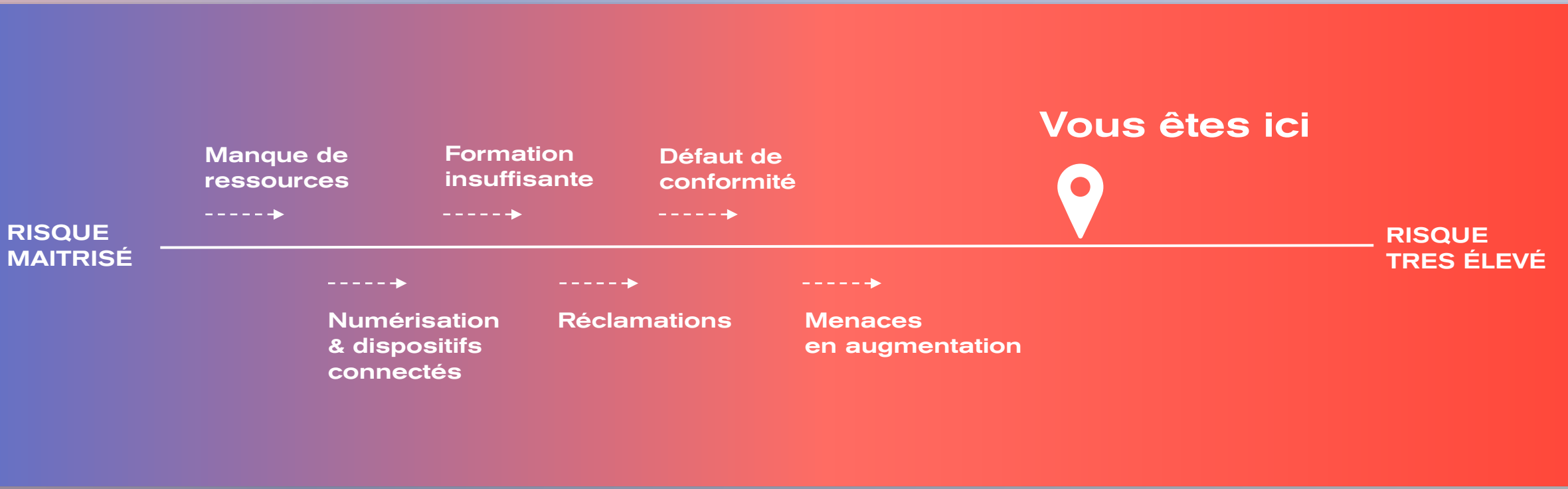
→ SUN-ES

→ ESMS Numériques

Pour y voir clair

Liste complète des obligations et prérequis en annexe, p.25

L’accumulation des failles rend vulnérables les structures de santé. Sans action de votre part, le risque augmente et les conséquences d’un incident deviennent plus graves.



Sécurité des Systèmes d'Information

Protection des données

# Comment TESIS vous accompagne

# NOTRE APPROCHE

Une démarche régionale mutualisée portée par le GCS TESIS, soutenue par un catalogue de prestations externalisées

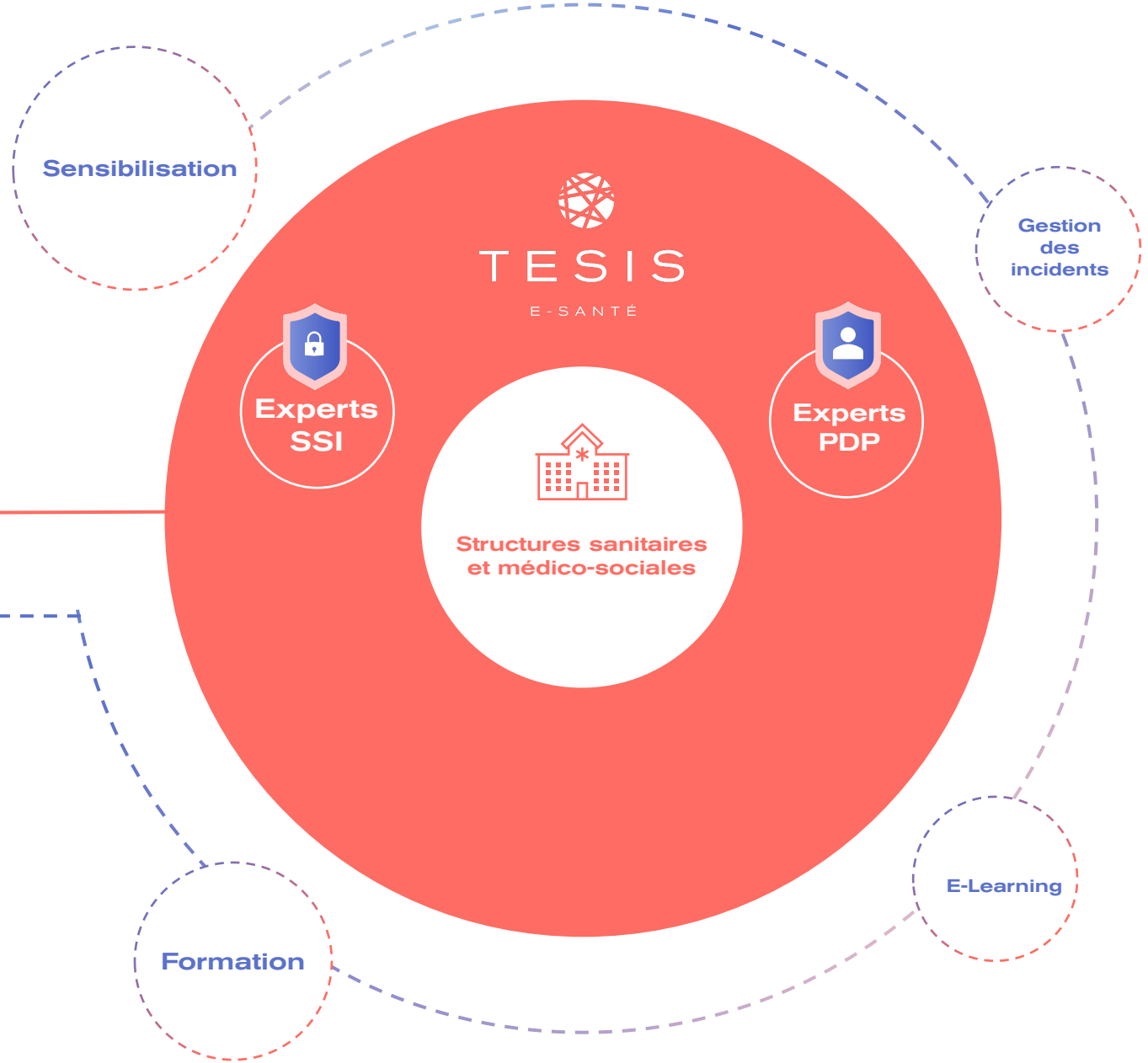
## Intervention du GCS TESIS

Un pool **d'experts** internalisé (RSSI, DPD) peut intervenir dans vos structures, ponctuellement ou dans le cadre d'une mise à disposition, à prix coûtant.

## Externalisé

Délégation des **prestations** spécialisées (sensibilisation, gestion des incidents) grâce aux marchés du GCS TESIS

**Mutualisation des coûts pour les adhérents**



# NOS SERVICES

## Intervention du GCS TESIS

Accompagnement assuré par les équipes du GCS TESIS

### Missions ponctuelles

**Sécurité des Systèmes d'Information**

- Audit de maturité
- Audit et Plan de Contrôle
- Analyse de risques
- Gouvernance
- Documentation
- Cadrage et suivi des projets

**Conformité RGPD & DPD**

- Audit de maturité
- Conformité RGPD et documentation
- Information et droits des usagers
- Gestion des sous-traitants
- Analyse d'impact
- S.O.S DPO !

### Offres packagées

**Plan SSI**

3 ans pour structurer votre sécurité

**Plan RGPD & PDP**

3 ans pour organiser votre gestion des données personnelles

### Ressources dédiées

Votre **RSSI** externalisé

Votre **DPD** externalisé

## Externalisé

Prestations externalisées via les marchés souscrits par le groupement

### Prestations et outils sur catalogue

**Gestion des incidents**

- Prévention et détection
- Gestion de crise
- Réponse aux incidents de sécurité

**Formation & sensibilisation**

- Escape game (Médiscape)
- e-Learning & campagne de phishing
- Evènements de sensibilisation

TESIS E-SANTÉ

# PLAN D'ACCOMPAGNEMENT SSI

## 3 ANS POUR STRUCTURER VOTRE SÉCURITÉ

### Objectifs :

Réduire rapidement votre risque cyber en vous dotant de l'organisation et des moyens pour faire face aux attaques.

Remplir vos obligations réglementaires en matière de SSI, prérequis aux programmes nationaux HOP'EN, SUN-ES et ESMS Numériques.

### Tarifs :

#### Sanitaire

**Petite structure** (activité combinée : 10k-25k) :
→ 8 à 19 JH / an | **3,6 K€ à 9 K€**

**Structure Moyenne** (activité combinée : 25k-50k) :
→ 19 à 46 JH / an | **9 K€ à 23 K€**

**Grande structure** (activité combinée : 50k-550k) :
→ 46 à 530 JH / an | **23 K€ à 256 K€**

#### Médico-social

**Petite structure** (Nb Places : 10 – 250) :
→ 2 à 10 JH / an | **1 K€ à 5 K€**

**Structure Moyenne** (Nb Places : 250 – 800) :
→ 19 à 46 JH / an | **5 K€ à 17 K€**

**Grande structure** (Nb Places : 800 – 2000) :
→ 46 à 530 JH / an | **17 K € à 48 K€**

### Première année

**Vous protéger en cas d'attaques**

- ❑ AUDIT DE MATURITE
- ❑ MISE EN PLACE D'UNE GOUVERNANCE INTERNE
- ❑ PLAN DE TRAITEMENT D'URGENCE :
  - Gestion d'incident
  - Socle de sécurité opérationnelle
  - Sensibilisation
  - Plan de Continuité Informatique (PCI)
  - Plan de Reprise Informatique (PRI)

### Deuxième année

**Identifier vos failles et renforcer votre sécurité**

- ❑ ANALYSE DES RISQUES CRITIQUES
- ❑ CONSTRUIRE VOTRE SECURITE A LONG TERME
  - Gestion des identités et des accès
  - Gestion des actions d'administration
  - Sécurité des réseaux
  - Gestion des sous-traitants – Homologation des projets
  - PCI / PRI de niveau 2

### Troisième année

**Améliorer votre performance globale**

- ❑ REVUE ET EXTENSION DE L'ANALYSE DE RISQUES
- ❑ CONSOLIDATION ET SUIVI DES MESURES MISES EN ŒUVRES AUX NIVEAUX 1 ET 2

**+ AU BESOIN**

commande de prestations externalisées

# PLAN D'ACCOMPAGNEMENT RGPD & PDP

## 3 ANS POUR ORGANISER LA PROTECTION DES DONNÉES PERSONNELLES

### Objectifs :

Réduire rapidement votre risque face à un défaut de conformité RGPD.

Remplir vos obligations réglementaires en matière de PDP, prérequis aux programmes nationaux HOP'EN, SUN-ES et ESMS Numériques.

### Tarifs :

#### Sanitaire

**Petite structure** (activité combinée : 10k-25k) :
→ 4 à 10 JH / an | **2 K€ à 5 K€**

**Structure Moyenne** (activité combinée : 25k-50k) :
→ 10 à 21 JH / an | **5 K€ à 10 K€**

**Grande structure** (activité combinée : 50k-550k) :
→ 21 à 220 JH / an | **10 K€ à 105 K€**

#### Médico-social

**Petite structure** (Nb Places : 10 – 250) :
→ 1 à 6 JH / an | **0,5 K€ €** à **3 K€**

**Structure Moyenne** (Nb Places : 250 – 800) :
→ 6 à 17 JH / an | **3 K€** à **8 K€**

**Grande structure** (Nb Places : 800 – 2000) :
→ 17 à 43 JH / an | **8 K €** à **21 K€**

### Première année

**Vous doter d'un socle minimal de conformité au RGPD**

- ❑ AUDIT DE MATURITE
- ❑ MISE EN PLACE D'UNE GOUVERNANCE INTERNE
- ❑ MISE EN PLACE DU REGISTRE
- ❑ PLAN DE TRAITEMENT D'URGENCE : **(sur les traitements les plus sensibles)**
  - Gestion de l'information et droits des personnes concernées
  - Analyse d'impact
  - Sensibilisation
  - Gestion de la contractualisation avec les sous-traitants

### Deuxième année

**Mettre en œuvre vos actions de conformité**

- ❑ SENSIBILISATION
- ❑ INFORMATION ET GESTION DU CONSENTEMENT DES TRAITEMENTS
- ❑ 2e NIVEAU DE MESURES EN PRIORITE SUR LES TRAITEMENTS LES PLUS SENSIBLES
  - Gestion des droits des personnes concernées
  - Analyse d'impact
  - Gestion des sous-traitants
  - Notification des incidents

### Troisième année

**Améliorer votre gestion de la conformité RGPD**

- ❑ AUDIT DES MESURES MISES EN PLACE
- ❑ CONSOLIDATION DES MESURES MISES EN PLACE AUX NIVEAUX 1 ET 2
- ❑ EXTENSION AUX AUTRES TRAITEMENTS

**+ AU BESOIN**

commande de prestations externalisées

# EXTERNALISATION DES FONCTIONS RSSI & DPD – Sanitaire

## DES EXPERTS À PRIX COÛTANT

**Optez pour la mutualisation**

**pour la gouvernance**

**de la cybersécurité,**

**la conformité RGPD**

**et piloter votre plan d'action**

→ Recrutement et formation continue assurés au sein du Pôle Cybersécurité du GCS TESIS.

→ Financement des ressources au prorata de leur utilisation pour les besoins de votre structure.

### Coût annuel sur la base d'un tarif journalier de 480€

| | Petite structure 10 à 25k AC** | Structure moyenne 25 à 50k AC** | Grande structure 50 à 550k AC** |
|---|---|---|---|
| RSSI | 15 - 38JH* | 38 - 80 JH * | 80 - 800 JH |
| | 7–18K€ | 18-38K€ | 38-384K€ |
| DPD | 8 - 20 JH * | 20 - 33 JH * | 33 - 367 JH * |
| | 4- 10K€ | 10-16K€ | 16-176K€ |
| RSSI + DPD | 23 - 58JH* | 58 - 113JH* | 113- 1167JH* |
| | 11-28K€ | 28-54K€ | 54-560K€ |

* Estimation du temps mis à disposition en Jours Hommes annuels

** Activité combinée (Hop'en)

### AVANTAGES

- Maîtrise des coûts
- Transversalité des actions
- Une réelle expertise SSI & RGPD

TESIS E-SANTÉ

# EXTERNALISATION DES FONCTIONS RSSI & DPD – Médico-Social

## DES EXPERTS À PRIX COÛTANT

**Optez pour la mutualisation**

**pour la gouvernance**

**de la cybersécurité,**

**la conformité RGPD**

**et piloter votre plan d'action**

→ Recrutement et formation continue assurés au sein du Pôle Cybersécurité du GCS TESIS.

→ Financement des ressources au prorata de leur utilisation pour les besoins de votre structure.

### Coût annuel sur la base d'un tarif journalier de 480€

| | Petite structure 10 – 250 places | Structure moyenne 250-800 places | Grande structure 800-2000 places |
|---|---|---|---|
| RSSI | 4 - 20 JH * | 20 - 60 JH * | 60 - 150 JH |
| | 2 -10K€ | 10-29K€ | 29 - 72K€ |
| DPD | 3 - 12 JH * | 12 - 27 JH * | 27 - 72 JH * |
| | 1,5- 6K€ | 6 - 13K€ | 13 - 35K€ |
| RSSI + DPD | 6 - 32 JH * | 32 - 87 JH * | 87– 222 JH * |
| | 3,5-16K€ | 16-42K€ | 42-107K€ |

* Estimation du temps mis à disposition en Jours Hommes annuels

**AVANTAGES**

- Maîtrise des coûts
- Transversalité des actions
- Une réelle expertise SSI & RGPD

TESIS E-SANTÉ

# Démarche de mise en œuvre

Prise de rdv

## Rencontre TESIS / établissement

Recueillir les besoins de la structure, et définir le périmètre d'intervention du GCS TESIS.

Prévisionnel

TESIS produit un plan d'action prévisionnel et une approche budgétaire personnalisés

## Engagement dans la démarche

La structure valide le périmètre de l'audit de maturité, définition du reporting et de la comitologie

Audit de maturité

TESIS procède à un des lieux précis des besoins, ajuste le plan opérationnel détaillé et les charges associées

## Validation du plan d'action détaillé

La structure valide le plan d'action, les charges et les prestations préconisées suite à l'audit de maturité.

Réunion de lancement

Avec la direction de l'établissement, validation du calendrier opérationnel de mise en œuvre.

GO !

Mise en œuvre des prestations

## Suivi de la prestation

Rapports et Comités de pilotage réguliers

TESIS E-SANTÉ

# ACCOMPAGNEMENT SSI
## MISSIONS PONCTUELLES

### AUDIT DE MATURITÉ

Prérequis à toute intervention ponctuelle du GCS TESIS, l'audit de maturité permet de définir les besoins de votre structure, et de dimensionner les missions réalisées par la suite (jours homme, prestations, tarifs, etc.) au plus près la réalité.

Objectifs :

- Déterminer le niveau de maturité SSI de votre établissement
- Affiner les actions à entreprendre en cohérence avec les besoins de l'établissement

Méthodologie :

- Entretien avec la direction et les représentants du SI sur les grands thèmes de la SSI

### Audit et Plan de Contrôle

Objectifs :

- Identifier les différentes vulnérabilités du SI
- Contrôler l'application des différentes mesures de sécurité déployés ainsi que leur efficacité

Méthodologie :

- Auditer les différents éléments composant le SI (organisation, documentation, technique, etc.)

En pratique :

- Tarifs : selon périmètre

### Analyse de risques

Objectifs :

- Identifier les principales menaces et risques inhérents au SI
- Renforcer le SI avec des mesures adaptées au risques identifiés

Méthodologie :

- Définir le périmètre
- Identifier les risques
- Définir le plan de traitement des risques
- Présenter des risques résiduels

En pratique :

- Tarifs : selon audit de maturité et périmètre

### Gouvernance

Objectifs :

- Structurer et engager l'établissement
- Piloter la SSI au sein de l'organisation

Méthodologie :

- Définir un référent SSI au sein de l'établissement
- Cadrer l'organisation de la sécurité au sein de l'établissement

En pratique :

- Tarifs : selon audit de maturité et périmètre

### Documentation

Objectifs :

- Structurer le fonctionnement de l'établissement
- Tracer les actions

Méthodologie :

- Elaborer des politiques, procédures et processus
- Créer des bases documentaires

En pratique :

- Tarifs : selon audit de maturité et périmètre

### Cadrage et suivi des projets

Objectifs :

- S'assurer de la bonne compréhension des objectifs
- Suivre l'avancée des différentes actions à entreprendre
- Veiller au bon déroulement des différents projets

Méthodologie :

- Désigner un pilote chargé du suivi des projets
- Prioriser les différentes actions à entreprendre
- Contrôler et ajuster

En pratique :

- Tarifs : selon audit de maturité et périmètre

# ACCOMPAGNEMENT RGPD & PDP

## MISSIONS PONCTUELLES

**S.O.S DPO !**

Vous avez un doute sur la réglementation, vous souhaitez vérifier que vous êtes dans les clous sur un projet ou dans vos démarches ?

Les équipes du GCS TESIS sont à votre disposition, même hors du cadre des prestations listées ici !

Contactez-nous, nous répondrons à vos demandes.


m.laurent@tesis.re

0693 93 37 35


### AUDIT DE MATURITÉ

Prérequis à toute intervention ponctuelle du GCS TESIS, l'audit de maturité permet de définir les besoins de votre structure, et de dimensionner les missions réalisées par la suite (jours homme, prestations, tarifs, etc.) au plus près la réalité.

**Objectifs** :

- Déterminer le niveau de maturité sur la conformité RGPD de votre établissement
- Affiner les actions à entreprendre en cohérence avec les besoins de l'établissement

Méthodologie :

- Entretien avec la direction et les représentants du SI sur les grands thèmes de la protection des données

### Information & Droit des usagers

Objectifs :

- Rendre aisément accessible l'information aux personnes concernées
- Faciliter l'exercice des droits des personnes concernées

Méthodologie :

- Définir les supports et contenus d'information
- Définir l'organisation pour l'exercice des droits

En pratique :

- Tarifs : selon audit de maturité et périmètre

### Gestion des sous-traitants

Objectifs :

- Documenter l'activité de la sous-traitance
- Veiller que la sous-traitance respecte le RGPD

Méthodologie :

- Définir les clauses types
- Analyser les écarts et négocier avec les sous-traitants
- Contrôler le respect des clauses

En pratique :

- Tarifs : selon audit de maturité et périmètre

### Analyse d'impact

Objectifs :

- Protéger la vie privée des usagers
- Mise en conformité

Méthodologie :

- Identifier les risques sur la vie privée
- Définir les mesures de traitement de ces risques

En pratique :

- Tarifs : selon audit de maturité et périmètre

### Registre de traitement

Objectifs :

- Disposer d'une vue d'ensemble sur le traitement des données personnelles
- Mise en conformité

Méthodologie :

- Analyse de la documentation existante et entretiens
- Cartographier et catégoriser vos traitements

En pratique :

- Tarifs : selon audit de maturité et périmètre

# Catalogue des prestations externalisées

GESTION DES INCIDENTS

# PREVENTION ET DETECTION

## Objectifs :

- Bénéficier d'un suivi régulier des alertes et failles de sécurité de votre SI
- Outiller les structures pour la détection des vulnérabilités
- Outiller les structures pour la détection des évènements de sécurité
- Analyser et remédier aux cyber-incidents

## En pratique :

- Tarifs : sur catalogue du prestataire retenu

Prestation à souscrire

Participez au choix des prestataires via nos procédures de marché !

GESTION DES INCIDENTS

# RÉPONSE AUX INCIDENTS DE SÉCURITÉ

## Objectifs :

- Appuyer les établissements en temps réel en cas de crise cyber :
  - ✓ Qualification
  - ✓ Pilotage
  - ✓ Remédiation
- Identifier la portée des incidents SSI

## En pratique :

- Tarifs : sur catalogue du prestataire retenu

Prestation à souscrire

Participez au choix des prestataires via nos procédures de marché !

FORMATION & SENSIBILISATION

# GESTION DE CRISE

## Objectifs :

- Sensibiliser les personnels
- Se préparer à la survenue d'incident :
  - ✓ Réduction de la durée d'impact
  - ✓ Diminution de la gravité
- Améliorer les procédures existantes

## En pratique :

- Tarifs : sur catalogue du prestataire retenu

Prestation à souscrire

Participez au choix des prestataires via nos procédures de marché !

## FORMATION & SENSIBILISATION

# ESCAPE GAME : MÉDISCAPE

Sensibiliser aux bonnes pratiques de sécurité dans les structures de santé grâce au jeu d'évasion, un concept collaboratif éprouvé pour maximiser l'engagement.


### Scénario

Six participants se glissent dans la peau de reporters people infiltrés dans une clinique pour dérober le dossier médical d'une célébrité. Ils ont 45 minutes pour pirater le système informatique à l'aide des ordinateurs et des indices laissés dans la pièce.

### Démarche

- Implication des apprenants grâce à l'aspect ludique et pragmatique
- Renforcement de l'esprit d'équipe
- Debriefing et sensibilisation :
  - Expliquer les conséquences des mauvaises pratiques
  - Illustrer l'importance des actions individuelles au service d'une démarche collective
  - Documents de sensibilisation remis à chaque participant

### En pratique

- **Combien de personnes :** 6 participants max par session
- **Durée :** 1h
- **Où :** Les sessions peuvent avoir lieu dans les locaux du GCS TESIS, ou dans la structure demandeuse
- **Tarif : 1/2 journée à 240€**

Devenez autonomes sur la sensibilisation !

Nous pouvons former vos équipes au déploiement de Médiscape dans vos structures

FORMATION & SENSIBILISATION

# CAMPAGNE DE PHISHING et E-LEARNING

## Objectifs :

- Diagnostiquer la maturité de votre personnel
- Cibler les campagnes de sensibilisation

## En pratique :

- Tarifs : sur catalogue du prestataire retenu

Prestation à souscrire

Participez au choix des prestataires via nos procédures de marché !

FORMATION & SENSIBILISATION

# ÉVÈNEMENTS DE SENSIBILISATION

## Objectifs :

- Améliorer la maturité des personnels
- Eviter les comportements à risque pour votre sécurité

## En pratique :

- Tarifs : sur catalogue du prestataire retenu

Prestation à souscrire

Participez au choix des prestataires via nos procédures de marché !

# Annexes & grille des tarifs

# Annexe 1 | Vos obligations en matière de SSI et de PDP

| Vos obligations | Comment y répondre ? | Domaine | Textes et Programmes associés | Les offres qui vous permettent d'y répondre |
|---|---|---|---|---|
| Auditer les vulnérabilités du SI | Commanditer des audits SSI par un tiers (audit technique, organisationnel, physique, tests d'intrusion, etc.) | SSI | PGSSI-S / MCAS; MARS 28; HOP'EN, SUN-ES, ESMS Numériques; Inst. 309 | Audit de maturité, Plan SSI Année 1 |
| Conformité RGPD | Désigner un pilote et suivre un plan d'action priorisant les actions permettant une mise en conformité de la structure | PDP | CPOM ARS; HOP'EN, SUN-ES, ESMS Numériques | Plan PDP 1ère année, Conformité RGPD et documentation* |
| Force probante des documents de santé | Remplir les conditions permettant de donner une valeur de preuve aux documents numériques de santé produits et conservés par votre structure durant la période légale de conservation des données. | SSI | PGSSI-S / MCAS | Plan SSI, Documentation* |
| Gérer les incidents et violations de données | Définir des procédures afin d'encadrer la gestion des incidents ainsi que leurs notifications. Elles intègreront des processus qui vont permettre de bien identifier les incidents, les qualifier et les traiter afin de minimiser la durée d'impact. | SSI PDP | PGSSI-S / MCAS | Plan SSI 1ère année, Prestation externalisée : Gestion des incidents *, Plan PDP |
| Gérer les risques SSI | Identifier par le biais d'analyses de risques les différentes menaces et leur vraisemblance afin d'appliquer les mesures adaptées afin de traiter les différents risques en lien avec votre structure. | SSI | PGSSI-S / MCAS; CPOM ARS | Missions ponctuelles SSI, Plan SSI 1ère année |
| Gestion des sauvegardes | Mettre en place des modalités de sauvegarde des données assurant leur intégrité et leur confidentialité en cas d'incident. | SSI | PGSSI-S / MCAS; MARS 28; Inst. 309 | Plan SSI 1ère année * |
| Gouvernance SSI | Désigner au sein de votre structure un RSSI rattaché à la Direction Générale, et désigner un Délégué à la Protection des Données. | SSI | PGSSI-S / MCAS; CPOM ARS; HOP'EN, SUN-ES, ESMS Numériques; Inst. 309 | Plan SSI 1ère année, Missions ponctuelles : Gouvernance * |
| Identification et Authentification des acteurs | Utiliser des méthodes d'identification et d'authentification permettant de garantir les accès aux bonnes personnes de votre structure. Gérer les identités et le choix de mécanismes d'authentification au regard de la criticité des ressources concernées. | SSI PDP | PGSSI-S / MCAS; CPOM ARS; Inst. 309 | Plan SSI 2ème année |
| Imputabilité des actions | Mettre en place d'un dispositif d'imputabilité capable d'établir des traces des actions réalisées dans votre système d'information, de les conserver et de les rendre accessibles à des personnes autorisées. | SSI | PGSSI-S / MCAS | Plan SSI 1ère et 2ème année |
| Plan de Continuité d'Activité (PCA) / Plan de Reprise d'Activité (PRA) | Définir un plan d'action décrivant les moyens techniques, organisationnels et humains permettant d'assurer la continuité et la reprise de l'activité du système d'information en cas d'indisponibilité totale ou partielle. | SSI PDP | CPOM ARS; HOP'EN, SUN-ES, ESMS Numériques | Plan SSI 1ère année |
| Protéger les données et les systèmes | Durcir les différents éléments de votre structure afin le limiter leur surface d'exposition aux risques ciblant l'intégrité et la sécurité des données. (infrastructure, postes de travail, réseaux, etc.) | SSI | PGSSI-S / MCAS; CPOM ARS | Plan SSI |
| Schéma Directeur de la Sécurité des Systèmes d'Information | Cadrer les différents projets et objectifs en matière de sécurité des systèmes d'information en différents thèmes sur la durée afin d'en extraire une trajectoire par périodes et identifier les ressources nécessaires à sa réalisation. | SSI | CPOM ARS | Plan SSI |
| Sensibiliser et former la totalité des personnels | Définir une stratégie de sensibilisation et de formation adaptée aux différents membres de votre structure afin de les accompagner dans la compréhension des différents risques liées à leurs activités quotidiennes et leur permettre d'y faire face. | SSI | PGSSI-S / MCAS | Prestation d'externalisation : Formation et sensibilisation, Mediscape<br>Plan SSI 1ère année, Plan PDP |

# Annexe 2.1 | L'offre d'accompagnement du GCS TESIS - Sanitaire

**Sécurité des Systèmes d'Information**

| | | | Petite Structure 10 à 25k * | Structure moyenne 25 à 50k* | Grande Structure 50 à 550k* |
|---|---|---|---|---|---|
| **Plan : Sécurité des Systèmes d'Information** | Première année | Mise en place d'une gouvernance interne et d'un plan de traitement d'urgence : Gestion d'incidents, Socle de sécurité opérationnelle, Sensibilisation, PCI / PRI de niveau 1 | 8 à 19 JH / an **3,6 K€ à 9 K€** | 19 à 46 JH / an **9 K€ à 23 K€** | 46 à 530 JH / an **23 K€ à 256 K€** |
| | Deuxième année | Analyse des risques critiques, Gestion des Identités et des Accès, Gestion des actions d'administration, Sécurité des Réseaux, gestion des sous-traitants, PCI / PRI de niveau 2 | | | |
| | Troisième année | Audit et extension de l'analyse de risques, Consolidation des mesures prévues aux niveaux 1 et 2 | | | |
| **RSSI Externalisé** | Mise à disposition d'un Responsable de la Sécurité des Systèmes d'Information par le GCS TESIS | | 15 à 38JH / an **7 à 18K€** | 38 à 80 JH / an **18 à 38K€** | 80 à 800 JH / an **38 à 384K€** |
| **Accompagnement personnalisé** | Accompagnement pour une prestation ponctuelle ou sur-mesure suivant votre besoin | | **480 € la journée** | | |

* Activité combinée (Hop'en)

**Conformité RGPD & D.P.D.**

| | | | Petite Structure 10 à 25k * | Structure moyenne 25 à 50k* | Grande Structure 50 à 550k* |
|---|---|---|---|---|---|
| **Plan : Protection des Données Personnelles** | Première année | Mise en place d'une gouvernance interne, du registre de traitement et d'un plan de traitement d'urgence sur les traitements les plus sensibles : Gestion de l'information et droits des personnes concernées, Analyse d'impact, Sensibilisation, Gestion de la contractualisation avec les sous-traitants | 4 à 10 JH / an **2 K€ à 5 K€** | 10 à 21 JH / an **5 K€ à 10 K€** | 21 à 220 JH / an **10 K€ à 105 K€** |
| | Deuxième année | Sensibilisation, information et gestion des consentements, consolidation des mesures sur les traitements (par ordre de priorité sur les traitements les plus sensibles) : : Gestion des droits des personnes concernées, Analyse d'impact, Gestion des sous-traitants | | | |
| | Troisième année | Audit des mesures en place, consolidation des mesures mises en œuvre, extension aux autres traitements | | | |
| **DPD Externalisé** | Mise à disposition d'un Responsable de la Sécurité des Systèmes d'Information par le GCS TESIS | | 8 à 20 JH /an **4 à 10K€** | 20 à 33 JH / an **10 à 16K€** | 33 à 367 JH/ an **16 à 176K€** |
| **Accompagnement personnalisé** | Accompagnement pour une prestation ponctuelle ou sur-mesure suivant votre besoin | | **480 € la journée** | | |

# Annexe 2.1 | L'offre d'accompagnement du GCS TESIS – Médico-Social

## Sécurité des Systèmes d'Information

| | | | Petite Structure<br>Nb Places : 10 à 250 | Structure moyenne<br>Nb Places : 250 à 800 | Grande Structure<br>Nb Places : 800 à 2 000 |
|---|---|---|---|---|---|
| **Plan : Sécurité des Systèmes d'Information** | Première année | Mise en place d'une gouvernance interne et d'un plan de traitement d'urgence : Gestion d'incidents, Socle de sécurité opérationnelle, Sensibilisation, PCI / PRI de niveau 1 | 2 à 10 JH / an<br>**1 K€ à 5 K€** | 19 à 46 JH / an **5 K€ à 17 K€** | 46 à 530 JH / an<br>**17 K € à 48 K€** |
| | Deuxième année | Analyse des risques critiques, Gestion des Identités et des Accès, Gestion des actions d'administration, Sécurité des Réseaux, gestion des sous-traitants, PCI / PRI de niveau 2 | | | |
| | Troisième année | Audit et extension de l'analyse de risques, Consolidation des mesures prévues aux niveaux 1 et 2 | | | |
| **RSSI Externalisé** | Mise à disposition d'un Responsable de la Sécurité des Systèmes d'Information par le GCS TESIS | | 4 à 20 JH / an<br>**2 à 10K€** | 20 à 60 JH / an<br>**10 à 29K€** | 60 à 150 JH / an<br>**29 à 72K€** |
| **Accompagnement personnalisé** | Accompagnement pour une prestation ponctuelle ou sur-mesure suivant votre besoin | | **480 € la journée** | | |

## Conformité RGPD & D.P.D.

| | | | Petite Structure<br>Nb Places : 10 à 250 | Structure moyenne<br>Nb Places : 250 à 800 | Grande Structure<br>Nb Places : 800 à 2 000 |
|---|---|---|---|---|---|
| **Plan : Protection des Données Personnelles** | Première année | Mise en place d'une gouvernance interne, du registre de traitement et d'un plan de traitement d'urgence sur les traitements les plus sensibles : Gestion de l'information et droits des personnes concernées, Analyse d'impact, Sensibilisation, Gestion de la contractualisation avec les sous-traitants | 1 à 6 JH / an **0,5 K€ €** à **3 K€** | 6 à 17 JH / an<br>**3 K€** à **8 K€** | 17 à 43 JH / an<br>**8 K €** à **21 K€** |
| | Deuxième année | Sensibilisation, information et gestion des consentements, consolidation des mesures sur les traitements (par ordre de priorité sur les traitements les plus sensibles) : : Gestion des droits des personnes concernées, Analyse d'impact, Gestion des sous-traitants, Notification des incidents | | | |
| | Troisième année | Audit des mesures en place, consolidation des mesures mises en œuvre, extension aux autres traitements | | | |
| **DPD Externalisé** | Mise à disposition d'un Responsable de la Sécurité des Systèmes d'Information par le GCS TESIS | | 3 à 12 JH / an<br>**1,5 à 6K€** | 12 à 27 JH / an<br>**6 à 13K€** | 27 à 72 JH / an<br>**13 à 35K€** |
| **Accompagnement personnalisé** | Accompagnement pour une prestation ponctuelle ou sur-mesure suivant votre besoin | | **480 € la journée** | | |

# Annexe 2.2 | Le catalogue de prestations à la carte

## Gestion des incidents

| | | Petite structure | Structure moyenne | Grande structure |
|---|---|---|---|---|
| **PREVENTION ET DETECTION** | Bénéficier d'un suivi régulier des failles de sécurité de votre SI : Détecter, analyser et remédier aux cyber-incidents | Sur catalogue du prestataire retenu | | |
| **GESTION DE CRISE** | Se préparer à la survenue d'incident cyber afin de réduire leur durée d'impact, leur gravité et améliorer les procédures existantes. | Sur catalogue (offre nationale) | | |
| **REPONSE AUX INCIDENTS DE SECURITE** | Appuyer les établissements en temps réel en cas de crise cyber pour la qualification, le pilotage en gestion de crise et la remédiation de l'incident | Sur catalogue du prestataire retenu | | |

## Formation & sensibilisation

| | | Petite structure | Structure moyenne | Grande structure |
|---|---|---|---|---|
| **ESCAPE GAME : MEDISCAPE** | Sensibiliser aux bonnes pratiques de sécurité dans les structures de santé grâce au jeu d'évasion, un concept collaboratif éprouvé pour maximiser l'engagement. | ½ journée : 240 € | | |
| **CAMPAGNE DE PHISHING E-LEARNING** | Diagnostiquer la maturité de votre personnel et cibler les campagnes de sensibilisation | Sur catalogue du prestataire retenu | | |
| **EVENEMENTS DE SENSIBILISATION** | Améliorer la maturité des personnels pour éviter les comportements à risque pour votre sécurité | Sur catalogue du prestataire retenu<br>-<br>Evènements organisés par TESIS pour l'ensemble des adhérents | | |

# L'EQUIPE CYBERSÉCURITÉ DU GCS TESIS

## Pilotage et expertise

**Mathias Laurent**

RSSI / DPD du GCS TESIS

8 ans d'expérience SSI et PDP secteur santé

Certifications :
- ISO 27001
- ISO 22301

**Stéphane Duchesne**

RSSI / DPD du GHT Réunion

15 ans d'expérience SSI et PDP secteur santé

Certifications :
- ISO 27001

## Expertise et appui opérationnel

**Cédric**

1 an d'expérience SSI et DPD secteur santé

**Dorian**

Jeune diplômé filière Cybersécurité

**Antoine**

Jeune diplômé filière Cybersécurité

## Renforts à recruter en fonction des besoins des membres

**Ingénieur**

SSI / PDP

**Ingénieur**

SSI / PDP

**Ingénieur**

SSI / PDP