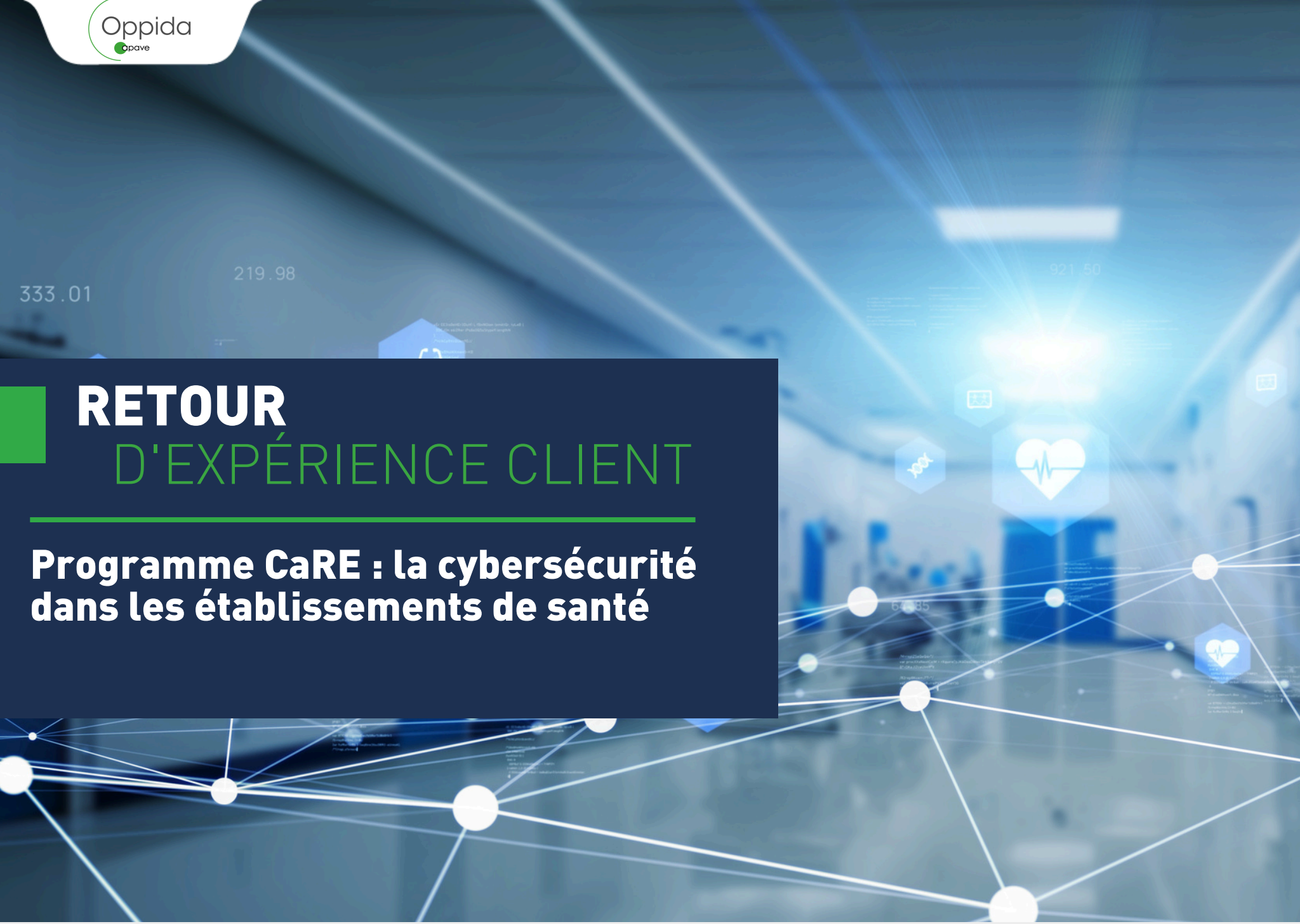
Oppida
apave



RETOUR D'EXPÉRIENCE CLIENT

Programme CaRE : la cybersécurité dans les établissements de santé

CONTEXTE

Etablissement de santé

- Clinique privée spécialisée en ophtalmologie et en ORL
- Localisation : Montauban
- 6 blocs chirurgicaux
- 8 000 interventions de la cataracte par an

ETAT DES LIEUX

Les établissements de santé, qu'ils soient privés ou publics, font aujourd'hui face à de multiples attaques informatiques.
Les rançongiciels notamment bloquent l'accès aux systèmes d'informations et génèrent de nombreux dommages pour les établissements :

- Perturbation des services médicaux et soins aux patients ;
- Perte d'exploitation ;
- Coûts importants de remises en état.

A cela s'ajoute l'accès pour les hackers à des données personnelles sensibles : celles des patients.

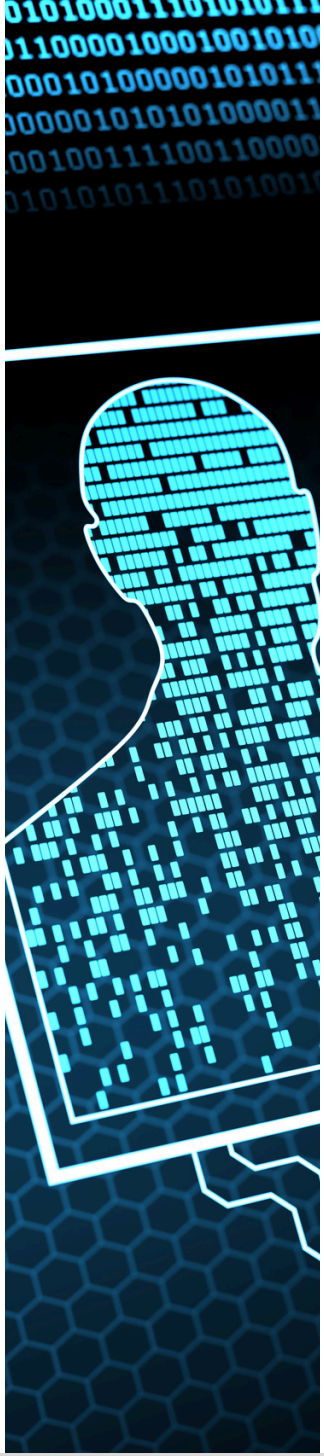
SOLUTION

Renforcer la cybersécurité des établissements de santé en bénéficiant de l'enveloppe dédiée au Domaine 1 du Programme CaRE sur les prestations suivantes :

- **Audit d'exposition Internet**
- **Maîtrise de l'Active Directory**
- **Exercice de crise cyber**

ENJEUX

- **Maîtriser les risques de cyberattaques ;**
- **Engager le personnel dans une démarche de cyber prévention ;**
- **Garantir la bonne prise en charge des patients ;**
- **Assurer la continuité des services auprès des patients.**



PRESTATIONS

1 Audit d'exposition Internet

- Atteindre un niveau de sécurité minimal de son exposition web par une évaluation, l'exposition sur internet étant l'un des principaux vecteurs de cyberattaques.
- L'audit doit être réalisé tous les 2 mois maximum.

2 Maîtrise de l'Active Directory

- Évaluer le niveau de sécurité des Active Directory grâce à l'outil ADS fourni par l'ANSSI
- L'active Directory joue un rôle essentiel dans la propagation des attaques puisqu'il s'agit du maillage informatique de l'établissement.
- L'audit doit être réalisé tous les 2 mois maximum.

3 Gestion de crise cyber

- Plan de gestion de crise
- Exercices de gestion de crise.
- Cet exercice doit être intégré dans le Plan d'Amélioration de la Qualité (PAQ) de l'établissement.

PRISE DE CONSCIENCE POUR L'ÉTABLISSEMENT

- Lorsqu'une crise cyber survient, elle n'impacte pas uniquement les métiers de l'informatique mais bien l'ensemble de la structure.
- L'identification du rôle essentiel de chacun en cas de crise et le processus à suivre pour limiter la propagation de l'attaque.

BÉNÉFICES

- Plus de sérénité pour le personnel de l'établissement et sa Direction.
- La cartographie de l'ensemble des risques potentiels avec identification de mesures nécessaires pour y faire face.
- L'amélioration du processus de gestion en cas de crise.
- Un modèle déployable pour tout autre type de crise.

COÛT POUR LA STRUCTURE

Si les résultats sont positifs et répondent aux objectifs du Programe, les missions seront prises en charge dans le cadre du Programme CaRE.

Focus Programme CaRE

Le programme CaRE est une initiative gouvernementale visant à renforcer la cybersécurité des établissements de santé et médico sociaux face à cette menace.

Ce programme est doté d'un financement de 750 millions d'euros d'ici 2027, dont 250 d'ici 2025. La date de limite de dépôt du dossier de déclaration est fixée au 30 juin 2025 pour bénéficier d'une prise en charge des prestations de cybersécurité.

Découvrir notre accompagnement

Contactez-nous pour vos projets