Communiqué de presse
Lyon, le 2 juin 2025

Cybersécurité : l'ARS et le GCS Sara font évoluer leur offre de services pour accompagner et former les acteurs de santé

La santé est le 3e secteur le plus touché en France par le risque cyber avec 10% des attaques recensées au sein des établissements publics de santé.[1] En 2024, 53 signalements d'incidents de sécurité liés aux systèmes d'information ont été enregistrés en Auvergne-Rhône-Alpes.

Pour faire face aux enjeux croissants liés à la protection des systèmes d'information et répondre aux nouveaux défis qu'ils impliquent, l'ARS Auvergne-Rhône-Alpes et le GCS Sara font évoluer leur offre de services à destination des établissements sanitaires et médico-sociaux. L'objectif : renforcer la résilience des acteurs de la santé et continuer à les préparer aux risques de cybermenaces.

A travers son Centre Régional de Ressources Cybersécurité (CRRC) créé en mai 2024, **l'ARS et le GCS Sara proposent ainsi de nouveaux services adaptés selon les structures, tels que :**

- un accompagnement à la mise en place du plan de continuité et de reprise d'activité (PCRA),
- une assistance en cas d'incident de sécurité,
- des campagnes de sensibilisation, notamment à destination des libéraux,
- des formations techniques sur la sécurité IT et cyber.

« Le secteur de la santé est en première ligne face aux risques cyber. Il est vital de protéger les données sensibles tout en assurant la continuité des soins. Notre ambition est claire : donner aux établissements les moyens d'anticiper, de se protéger et de réagir efficacement, à travers des services concrets, mutualisés et évolutifs », explique **Bertrand Pellet, directeur du GCS Sara**.

« Pour répondre à ces enjeux, l'ARS dédie un budget de 3,2 millions d'euros[2] (2,1 millions pour le sanitaire et 1,1 million pour le médico-social) afin de mettre en œuvre les services proposés par le Centre de Ressources » précise **Pierre Leroux, responsable des systèmes d'information sanitaires et de la cybersécurité à l'ARS**.

Un programme ambitieux pour renforcer la résilience des établissements de santé

Face aux menaces toujours plus importantes (sinistres, cyberattaques, etc.), ce programme régional d'**accompagnement méthodologique et pratique** aide les établissements de santé dans l'élaboration ou la consolidation de leur **plan de continuité et de reprise d'activité.** L'objectif : garantir la continuité des soins et la sécurité des patients, en toutes circonstances.

Initié en avril 2025, ce dispositif compte déjà plus d'une centaine d'établissements, très investis dans la démarche. Il se distingue par une approche concrète, s'appuyant sur des **ateliers** impliquant les services clés (pharmacie, biologie, imagerie…) et les directions des soins.
Les sessions sont proposées sur plusieurs sites de la région, pour en favoriser l'accessibilité et encourager échanges, partage d'expériences et de bonnes pratiques entre professionnels.

L'objectif est de former les personnels de 150 établissements d'ici fin 2025.

---

[1] D'après l'Agence nationale de la sécurité des systèmes d'information
[2] Fonds européen

De nouvelles formations pour les professionnels des services numériques

Jusqu'à la fin du mois de juin, 13 sessions de formation sont organisées à destination des équipes en charge du déploiement des mesures de sécurité informatique au sein des établissements sanitaires et médico-sociaux.

Elles traiteront deux thématiques majeures :

- la **sécurisation de l'*Active Directory***[3] : **240 structures sanitaires de la région s'y sont inscrites** (cadre du programme CaRE – Domaine 1)[4]
- la sécurisation **des sauvegardes** (perspective du lancement du domaine 2 de CaRE).

D'autres outils de sensibilisation (e-learning, Escape Game, etc.) sont proposés par le Centre Régional de Ressources Cybersécurité.

Une hotline pour toute question ou incident

En cas de suspicion ou d'incident avéré de sécurité au sein d'un établissement, une assistance opérationnelle est proposée par des prestataires experts en la matière (sélectionnés dans le cadre d'un marché public). Accessible toute l'année, 24h/24 et 7j/7 par téléphone, ce service est déjà opérationnel et disponible pour les plus de 150 structures publiques et privées adhérentes au programme. Elle permet d'améliorer la réponse en cas d'incident et ainsi mieux assurer la continuité d'activité.

Des campagnes de sensibilisation pour les professionnels de santé libéraux

Entre 2024 et 2025, la plateforme régionale de sensibilisation en e-learning a permis de former 77 000 professionnels issus de 120 établissements de santé et ESMS. Elle s'ouvre désormais aux professionnels de santé libéraux (accès gratuit).

Déployé en partenariat avec l'Union régionale des professionnels de santé (URPS) Médecins, les communautés professionnelles territoriales de santé (CPTS), et plus récemment avec l'URPS Infirmiers, ce programme de sensibilisation compte déjà une centaine de professionnels libéraux inscrits. L'objectif est d'élargir cette offre aux fédérations professionnelles.

Quelques chiffres clés des actions cyber en Auvergne-Rhône-Alpes :

- Réalisation d'exercices de crise : 1,2 million d'euros pour 230 établissements sanitaires (ES)
- Programme CaRE - Domaine 1 : 230 établissements de santé engagés dont les 13 GHT, pour un budget de 6 millions d'euros environ
- Mise en œuvre du CRRC : 3,2 millions d'euros

Contacts presse :
GCS Sara – Sylviane Piedallu
Tél : 04 73 31 87 34 - communication@sante-ara.fr

ARS Auvergne-Rhône-Alpes
Tél. 04 27 86 55 55 - ars-ara-presse@ars.sante.fr

[3] *L'Active Directory* regroupe tout ce qui compose un réseau administré : serveurs, postes de travail, comptes utilisateurs, dossiers partagés, etc.
[4] Programme CaRE : Cybersécurité accélération et résilience des établissements