

FAQ

Webinaire régional d'Île-de-France Ségur Numérique

« Renforcement de la cyber sécurité dans les établissements sanitaires »

À destination des établissements sanitaires d'Île-de-France, dont tous les établissements opérateurs de services essentiels (OSE)

- 09.01.2023 -

Question 1 : Est-ce que le prestataire informatique actuel peut réaliser l'accompagnement de cyber crise de l'établissement de santé ?

Oui, vous pouvez passer par le SESAN si vous êtes adhérent ou par la CAIH, mais vous pouvez utiliser la modalité qui vous paraît la plus pertinente comme passer par votre prestataire informatique actuel à partir du moment où vous respectez les conditions dans le formulaire comme joindre le bon de commande.

Question 2 : Quel est le coût "moyen" d'un accompagnement à l'exercice de cyber crise Niveau 2 ou 3 ?

Au niveau de SESAN, nous avons une cotation de l'exercice au niveau 1 (débutant), niveau 2 et 3 sont en cours de cotation puisque les référentiels ont été publiés assez tard par l'ANS. Nous aurons l'information d'ici 2 semaines concernant ces types d'accompagnement. Le coût de l'accompagnement pour le Kit niveau 1 est de 2000 euros.

Question 3 : Notre exercice de cyber crise est prévu pour le 13 janvier. Peut-on candidater quand même ?

Oui, il faudra nous joindre le bon de commande ainsi que la preuve que vous recourez à un prestataire et du moment que vous répondez aux prérequis à savoir : la grille d'auto-évaluation, la mise à jour de l'OPSSIES, il n'y a pas de contre-indication.

Question 4 : Deux établissements en direction commune peuvent-ils s'associer pour faire un exercice commun ?

Oui, l'audit peut être commun, mais il faudra réaliser deux commandes (transmission de deux bons de commande) dans le cadre de la candidature.

Question 5 : C'est 4 k€ par ES du GHT ?

Oui, tout à fait. Au sein d'une structure, plusieurs établissements peuvent candidater et obtenir 4 000 euros maximum à hauteur du bon de commande par établissement.

Question 6 : Quel est l'outil de cartographie utilisé par le SESAN ?

L'outil utilisé est "SOLU-QIQ". Il est disponible au travers du marché de la CAIH. Si vous prenez une licence, SESAN sera en mesure de vous aider à mettre à jour votre cartographie avec un accompagnement annuel. Cet outil permet de générer un intranet et de partager à l'ensemble de l'équipe les informations facilement.

Question 7 : Est-ce que le dépôt de candidature se fait également sur la plateforme OSIS ?

Non, le dépôt des candidatures se fait via démarches simplifiées, le lien est le suivant : <https://www.iledefrance.ars.sante.fr/media/104116/download?inline>

En revanche, un des pré requis pour bénéficier du financement est d'avoir mis à jour l'OPSSIES via sur la plateforme OSIS.

Question 8 : Et pour un GHT Fusionné (4 sites ex ES) comment est-ce que cela fonctionne ? Quelle est la hauteur du financement dans ce cadre-là?

L'exercice est très organisationnel donc ce serait un financement au niveau de l'établissement (x4 le cas échéant), l'idée étant de garantir que chacune des directions soit impliquée dans la gestion de la crise. Toutefois, ce sera limité au montant du bon de commande.

Question 9 : Est-ce que l'outil de cartographie s'intègre avec CENTREON pour ne pas avoir à ressaisir les données ?

Non, il ne s'intègre pas avec CENTREON, c'est une cartographie statique, mais des imports/exports peuvent être possibles sur Excel.

Question 10 : L'exercice de crise intégrera un SAMU. Faut-il le considérer comme un établissement ?

Non, dans ce cas, il ne s'agit pas de l'échelle de l'établissement. Bien qu'il soit intéressant d'intégrer le SAMU dans l'exercice de cyber crise, vous ne pourrez pas candidater au titre du SAMU. La candidature se fait au niveau de l'établissement.

Question 11 : Suite aux attaques du CHSF et de Versailles, existe-t-il un lieu d'échanges "techniques" permettant à chacun d'améliorer ses pratiques et de partager ses axes d'amélioration ?

Plusieurs supports ont été partagés lors de ce webinaire que vous pourrez retrouver. De plus, suite à ces attaques, des groupes de travail réunissant quelques acteurs, dont Versailles et le CHSF ont été initiés afin de mieux se préparer à d'autres cyberattaques. Afin de pouvoir échanger sur ces sujets techniques, nous vous invitons à adhérer au service SSI de SESAN qui comporte notamment une plateforme permettant l'échange direct entre RSSI.