doshas consulting

# INTERVIEW CROISÉE

OCTOBRE 2023

**Élodie Chaudron** (Agence du Numérique en Santé)
**et Steven Garnier** (Agence Régionale de Santé Bourgogne Franche-Comté)

# DES KITS D'EXERCICES DE CRISE CYBER, PRÉCIEUX POUR LES ÉTABLISSEMENTS DE SANTÉ

**La réalisation d'exercices de crise cybersécurité dans les établissements de santé étant l'une des actions prioritaires du Plan de renforcement cybersécurité du ministère de la Santé et de la Prévention, un groupe de travail réunissant l'ANS, le FSSI, les ARS et les GRADeS a élaboré des kits prêts à l'emploi et autoporteurs pour faciliter leur organisation.**
**Le point sur la méthodologie et le contenu avec Élodie Chaudron et Steven Garnier.**

## Comment est née l'idée d'élaborer des kits d'exercices de crise cyber et comment s'est-elle concrétisée ?

**Élodie Chaudron :** « En miroir du lancement de la stratégie nationale sur le numérique en santé, les représentants des Agences Régionales de Santé (ARS) et des Groupements Régionaux d'Appui au Développement de la e-Santé (GRADeS) qui siègent désormais au conseil d'administration de l'Agence du Numérique en Santé (ANS) ont remonté le besoin, au printemps 2021, de créer un espace de travail, sans sujet prédéfini au départ. Peu de temps après, la feuille de route du Fonctionnaire Sécurité des Systèmes d'Information (FSSI) sur le renforcement de la cyber-sécurité des ARS listait un certain nombre d'actions. Parmi elles, l'amélioration de la continuité d'activité a fait l'objet de premières réunions collégiales qui ont tout de suite fléché le besoin de mettre, à la disposition des établissements sanitaires, sociaux et médico-sociaux, des kits d'exercices de crise cyber.

Comme il existe plusieurs degrés de maturité dans les établissements, nous avons lancé des ateliers pour produire trois niveaux de kits : débutant, intermédiaire et confirmé. Nous avons ensuite mis en place des pilotes pour les tester et revoir les contenus, en fonction des premiers retours. »

**Steven Garnier :** « Disposer d'une vision régionale était une demande forte de notre part. En tant qu'agence, nous voulions aussi sortir un peu de notre rôle habituel d'organismes de contrôle auprès des établissements de santé. La conception de ces kits d'exercices était l'occasion de les accompagner dans la mise en place de prestations qualitatives. »

## Quel est le contenu de ces kits ?

**S.G. :** « Les membres les plus actifs du groupe de travail territorial ont été sollicités pour apporter leur vue du terrain et leur expertise du fonctionnement des structures, afin de rendre les exercices les plus réalistes possibles. Comme le disait Élodie, il est apparu le besoin de décliner plusieurs niveaux de difficulté, parce les établissements de santé, qui ont la possibilité de s'auto-évaluer via une grille d'éligibilité, n'évoluent pas tous dans le même contexte en matière de cybersécurité et de continuité d'activité. Pour faciliter l'organisation d'exercices au sein des structures, ces kits d'exercices de crise cyber sont prêts à l'emploi et autoporteurs. Ils contiennent un document central qui est le déroulé simulé de l'attaque, composé de stimuli qu'on a essayé de rendre les plus réalistes possibles. Naturellement, on ne demande pas aux établissements de débrancher leur SI ! Il s'agit d'un exercice sur table, dont l'ambition première est de faire prendre conscience des enjeux aux directions des établissements. Il s'accompagne d'un certain nombre de documents à vocation plus pédagogique, pour amener les membres des cellules de crise à comprendre ce qu'est réellement une cyberattaque, les sensibiliser aux bonnes pratiques et faire passer quelques messages sur les aspects, un peu plus techniques, de sécurisation des SI. »

**E.C. :** « Même s'ils ont été conçus pour être les plus autoporteurs possibles, il a été jugé indispensable que, pour la première

réalisation de chaque exercice, les établissements soient accompagnés par des professionnels. L'ambition du FSSI étant qu'ils réalisent un exercice par an. »

### Cette ambition passe-t-elle par une obligation légale ?

**E.C. :** « Le sujet est aujourd'hui pris au sérieux par les directions d'établissements qui sont souvent confrontés à des problématiques de ressources dédiées. J'espère que l'obligation de réaliser ces exercices de crise aidera à faire bouger les consciences et peut-être à mobiliser un peu plus de budget sur la cybersécurité dans les établissements.

Les premiers retours d'expérience montrent que les exercices sont très appréciés, notamment par leur dimension métier et la mise en place rapide de solutions et procédures en faveur de l'hygiène informatique, mobilisant l'ensemble des Comités de Direction (CoDir). Ils apparaissent comme un bon outil de sensibilisation pour parvenir à une acculturation assez naturelle. »

**S.G. :** « C'était une demande en parallèle de notre part. Au niveau régional, on voulait bien se faire les porte-paroles pour inciter les directions, mais il fallait que l'on s'appuie sur quelque chose qui les oblige légalement à le faire, comme la publication d'une instruction, composée d'un ensemble de mesures dites prioritaires, dont celle de la réalisation annuelle d'un exercice de crise cyber. D'autant plus qu'un établissement de santé n'est jamais à l'abri de se faire cyberattaquer plusieurs fois ! »

### Est-ce que vous constatez un changement au sein des établissements de santé vis-à-vis de la cybersécurité ?

**S.G. :** « Ce qui change, c'est une avancée dans la prise de conscience qui doit être collective et malheureusement chaque cyberattaque concourt à cette prise de conscience. Plus elles sont médiatisées, plus cela nous aide en termes de mobilisation et de sensibilisation des utilisateurs sur les risques encourus. C'est fondamental. »

**E.C. :** « La médiatisation est à double tranchant. Elle est à la fois positive et contraignante pour les projets de e-santé par la peur qu'elle peut susciter dans l'opinion publique. D'où la nécessité de rassurer les patients sur le cadre régalien et très sécuritaire du partage de leurs données de santé. Il existe encore beaucoup de craintes qui démobilisent l'ensemble des citoyens et ont un impact sur leur propre santé, surtout en matière de prévention. »

### Si vous aviez un message à faire passer ?

**S.G. :** « L'écosystème de la santé a besoin de travailler avec les industriels du secteur pour continuer à faire bouger les lignes et à lutter contre la menace cyber. Il me parait aussi nécessaire d'échanger sur le sujet avec d'autres secteurs pour partager nos pratiques. »

**E.C. :** « Faites vos exercices de crise et, si possible, pas tous en même temps… »


**Doshas Consulting**
**153 boulevard Haussmann 75008 PARIS**
**+33 (0)1 84 20 27 83**
**contact@doshas-consulting.com**
**www.doshas-consulting.com**




BIO EXPRESS

**ÉLODIE CHAUDRON**
Responsable du développement territorial pour l'Agence du Numérique en Santé (ANS), elle anime le groupe de travail territorial cybersécurité qui rassemble toutes les Agences Régionales de Santé (ARS) et tous les correspondants cyber des Groupements Régionaux d'Appui au Déploiement de la e-Santé.

**STEVEN GARNIER**
Référent technique du département e-santé à l'Agence Régionale de Santé (ARS) Bourgogne Franche Comté, il s'occupe notamment de la problématique de la cybersécurité, en agissant comme sponsor du groupe de travail territorial sur la cybersécurité animé par l'ANS et représentant des ARS dans la *task force* cyber du ministère.


*Conception : Doshas Consulting*
*Responsable de la publication : Didier Ambroise*
*Rédaction : Cécile Jouanel*
*Conception, réalisation : Studio Bleu Canari / Agence Biskot.Bergamote*