CaRE Cybersécurité accélération Résilience des Etablissements

Financé par l'Union européenne NextGenerationEU

AGENCE DU NUMÉRIQUE EN SANTÉ

La cybersécurité dans le médico-social : réaliser un exercice de crise

Webinaire – 17/03/2026

Agence du Numérique en Santé

Quelques rappels avant de démarrer ce webinaire

Le micro et la caméra sont automatiquement coupés sauf pour les intervenants.

Je pose mes **questions** dans **l'espace Tchat.**

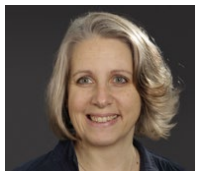
Une FAQ sera publiée sur le site esante à l'issue du webinaire (sur la page **Cybersécurité pour le médico-social)**

Vos intervenants

Equipe médico-sociale

Margaux BUGUET
Référente cybersécurité

Marie-Aude MATHIEU
Directrice générale
AideraVar



Nadège VANNESTE
Chef de projet
CAPSI

Jérémy THOMAS
Directeur de la transition numérique
Fondation Massé - Trévidy

Lionel LECOMTE
Chargé de mission cybersécurité et DPO
ARS Bretagne

De quoi allons-nous parler aujourd'hui ?

1. **La menace cyber dans le secteur médico-social**

2. **Témoignages sur la réalisation d'exercices de crise dans une structure médico-sociale**

3. **Présentation du kit d'exercice de crise de l'ANS**

Ce webinaire s'adresse, en particulier, aux établissements et services médico-sociaux.

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

1. La menace cyber dans le secteur médico-social

Les chiffres clés en 2025 dans le médico-social

Sommes-nous vraiment concernés par les cyberattaques dans le médico-social ?

« La question n'est plus de savoir si mais quand nous allons être touchés »

DSI des PEP CBFC

204
déclarations d'incidents dans des ESSMS

113
incidents d'origine malveillante

Les missions du CERT Santé sont multiples : réponse à incidents (traitement des déclarations d'incidents de sécurité et intervention d'urgence à distance), veille proactive, sensibilisation et partage, audits d'exposition sur internet.

Le Programme CaRE (Cybersécurité accélération et Résilience des Établissements)

[Cybersécurité de la santé | e-santé]

Ce programme ambitieux, **dans lequel le médico-social est pleinement intégré**, se décline, sur la période 2023-2027, autour de **4 axes** :

Délégation de **26 millions €** aux Centres Régionaux de Ressources Cybersécurité (CRRC) dont **18 millions €** pour les objectifs généraux et **8 millions €** pour le **secteur médico-social.** Les CRRC proposent une offre de service variée pour vous accompagner dans votre montée en maturité cyber, et notamment **l'accompagnement à la réalisation d'un exercice de crise cyber.**

Pour prendre contact avec votre CRRC : https://esante.gouv.fr/strategie-nationale/cybersecurite/axe-2

Rappel de la réglementation en vigueur

Obligation de signalement des incidents de sécurité des SI

Issu de l'instruction N° SHFDS/FSSI/2023/78 du 23 mai 2023, qui étend le Décret n°2016-1214 du 12 septembre 2016 aux ESSMS.

Tous les signalements remontent directement à l'ARS compétente territorialement, l'ANS et au CERT Santé via le **portail des signalements des événements sanitaires indésirables (PSIG)**.

Accueil - Portail de signalement des événements sanitaires indésirables (social-sante.gouv.fr)

L'élaboration d'un plan bleu

Équivalent du plan blanc pour le secteur hospitalier, le plan bleu définit, dans le secteur médico-social, les mesures à mettre en œuvre en cas de situation exceptionnelle.

Initialement, ce plan bleu était obligatoire depuis 2005 pour les EHPAD. **L'arrêté du 12 février 2024** prévoit, à compter de 2025, **l'obligation d'élaborer un « plan bleu » pour d'autres ESSMS.**

Guide-Plan-bleu-en-Ehpad-.pdf (solidarites.gouv.fr)

Le nouveau référentiel HAS d'évaluation des ESMS

Dans le cadre de la refonte du dispositif d'évaluation des ESMS, la HAS a publié en 2022 un **nouveau référentiel unique et commun pour l'ensemble des ESMS.**

Ce document comprend plusieurs critères impératifs ayant trait à la **gestion de crise** (dont crise liée à une cyberattaque / panne du SI) et à la **stratégie numérique** (qui doit inclure les éléments de protection et de sécurité du SI).

REFERENTIEL_HAS_ESSMS (has-sante.fr)

… sans oublier **la Politique Générale de Sécurité des Systèmes d'Information de Santé (PGSSI-S), le règlement général de protection des données (RGPD)** (entré en vigueur en 2018), et les réglementations à venir, comme la **directive NIS 2.**

Pourquoi réaliser un exercice de crise ?

L'objectif d'un exercice de crise cyber est de vous aider à **développer** et **renforcer** des savoir-faire concrets **pour mieux anticiper et gérer ces situations**.

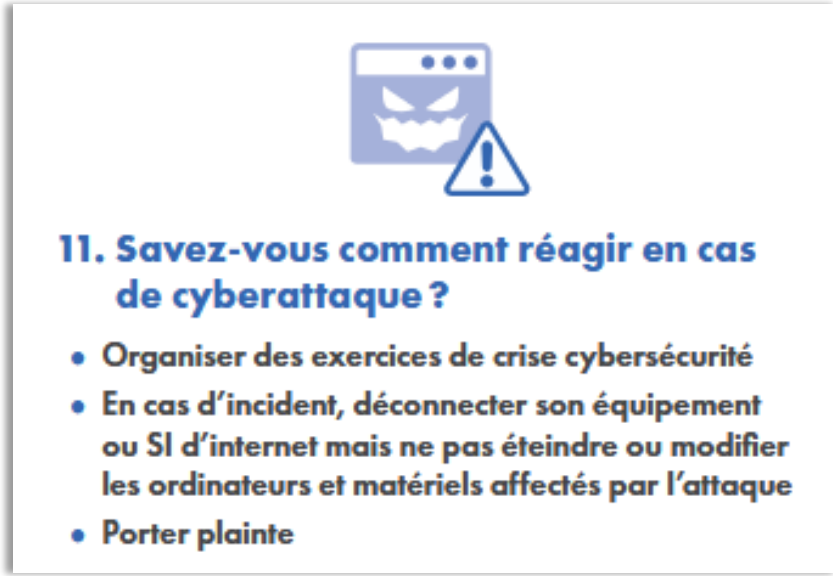
L'exercice de crise cyber doit pouvoir contribuer **à une véritable montée en compétence** pour rendre **les équipes plus autonomes et résilientes**, afin de vous **aider à ancrer des réflexes,** de **structurer une organisation efficace** et **d'améliorer la coordination** pour une gestion de crise optimisée.

« Même si on pense être préparé, on est surpris par les situations rencontrées en exercice »

ADAPEI 16

« C'est important de s'entrainer régulièrement à faire face à une cyberattaque. L'exercice de crise est intéressant sur plusieurs plans en nous permettant de nous préparer, de nous projeter en équipe et d'anticiper les impacts de tels incidents pour l'établissement et nos résidents. »

EHPAD La Pinçonnière – La Forêt



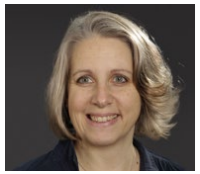
Pour en savoir plus :

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

2. Témoignages et retours d'expérience

La parole à la région Provence-Alpes-Côte d'Azur !

Marie-Aude MATHIEU
Directrice générale
AideraVar



Nadège VANNESTE
Chef de projet
CAPSI

L'association

- Organisation évènements famille
- Recherche de fonds
- Parrain GEM Autisme Var CoéZion
- Présidence du PARIH 83
- Représentation dans divers instances

Aidera.Var
Accompagner l'Autisme

1 association
5 pôles d'activité

Jeunesse

- IME La Frégate 21 places + 1 place accueil temporaire (27 enfants en file active)
- UEMA Canot major 7 places
- SESSAD Le Galion, 6 places et 9 enfants en file active
- Unité Externalisée Collège la Marquisanne L'optimiste
- Section Pré pro partenariat AVENS 83
- Unité Mobile de Soutien à l'Inclusion (UMSI) (180 familles en file active)
- SESSAD L'Oumiak, 12 places et 18 enfants en file active

Adultes

- MAS la Goélette 24 places
- Nausica Dispositif Hors les Murs 15 places en file active
- 2 places d'accueil temporaire
- Accueil de jour 10 places
- Accueil de répit loisirs adultes à Barjols

Santé et recherche

- Handi-consult AVISO partenariat CHITS Toulon (plus de 300 consultations annuelles)
- Equipe mobile de aux soins à Brignoles
- Participation à des travaux de recherche. Partenariats touchant à la santé (Aviso CHITS, la Timone Dr FERRON, IJL…)

Pôle Ressources, loisirs et répit

- Centre de Ressources et Guidance parentale
- Accueil temporaire
- Séjours de répit (Var Autisme Loisirs)

Formation, qualité Innovation et Numérique

- Centre de formation
- Veille numérique
- Suivi des plans de formations et leur adéquation aux projets d'établissements
- Formations au profit d'organismes extérieurs

Objectif de l’exercice de crise

1. Monter en compétences sur la gestion d’une crise d’origine cyber.
2. Éprouver les premiers éléments d’une gestion de crise d’origine cyber ainsi que l’appropriation du dispositif de crise par les acteurs de la cellule pour identifier les points forts et les axes d’amélioration.
3. Illustrer la pluralité des impacts d’une crise d’origine cyber.
4. Tester la stratégie de communication interne et externe de la cellule de crise.
5. Se questionner sur les bonnes pratiques à adopter pour assurer au mieux la continuité d’activité en cas de crise d’origine cyber.

1. Ce que l'exercice a permis de tester

Scénario de travail

Un mail de phishing conduit à la compromission d'un compte. Très vite, la messagerie devient suspecte, un outil métier n'est plus jugé fiable, et la structure doit décider si elle bascule en mode dégradé.

L'exercice a surtout permis de tester 4 choses

- le déclenchement de l'alerte
- la répartition des rôles direction / IT / DPO
- la décision de fonctionnement dégradé
- les signalements externes et la communication

Chronologie synthétique

T0 — **Signal faible** : Mail inhabituel, clic, doute sur un compte ou un poste.

T+15 — **Qualification** : Qui décide ? Qui isole ? Qui trace ?

T+45 — **Arbitrage** : Peut-on continuer ? Faut-il couper ? Passer en papier ?

T+90 — **Escalade** : ARS, CERT Santé, CAPSI, DPO/CNIL selon l'impact.

Pour nous la valeur de l'exercice n'est pas de reproduire une attaque complexe, c'était surtout de vérifier que chacun sait quoi faire dans la première heure.

2. Ce que le RETEX a permis de mettre en évidence

Ce qui a bien fonctionné

Décision rapide

La logique 'protéger l'activité essentielle d'abord' a été comprise.

Réflexe mode dégradé

Le basculement papier / téléphone a été envisagé tôt, avant la panne totale.

Lecture collective

Direction, IT et métiers ont convergé vers une même image de la situation.

Ce qui a dû être renforcé

Annuaire incomplet

Sous stress, on perd du temps si les contacts, rôles et suppléances ne sont pas prêts.

Signalements à clarifier

ARS, CERT Santé, CAPSI, CNIL : le qui / quand / pourquoi doit être connu sans débat.

Traçabilité de crise

La main courante et les décisions prises ne doivent pas dépendre d'une seule personne.

Conseil: Le RETEX doit déboucher sur peu d'actions, mais des actions tenues : annuaire, rôles, mode dégradé, signalements, exercice suivant.

3. Plan d’action concret à la suite de l’exercice

0-30 jours	**Fiabiliser l'annuaire de crise cyber**	Contacts internes, ARS, CERT Santé, CAPSI, DPO, prestataires, assureur, suppléances.
30-90 jours	**Clarifier les rôles**	Qui alerte, qui décide, qui appelle, qui trace, qui communique.
90-120 jours	**Tester le mode dégradé (PCRA)**	Messagerie indisponible, outil métier indisponible, perte d'Internet, papier sécurisé.
120-300 jours	**Refaire un exercice court**	Format 45 minutes, centré sur la première heure de crise et la chaîne d'alerte.

Conclusion : Pour AIDERA Var il était important en priorité de savoir qui décider, alerter, protéger et redémarrer sans perdre l'essentiel.

CAPSI : un portefeuille de services pour une cybersécurité de la santé renforcée

CAPSI offre une panoplie de services pour sécuriser les systèmes d'information des hôpitaux, structures médico-sociales et professionnels de santé en PACA.

ÉVALUER

- Audit de sécurité
- Analyse de vulnérabilités
- Contrôle des accès (Active Directory)

PROTÉGER

- Évaluation des risques
- Conseil en gestion d'incidents
- Assistance sauvegarde
- Conformité RGPD
- Analyse des menaces
- Échange sécurisé (BlueFiles)
- Accès Réseau PEPS

FORMER

- E-learning cybersécurité
- Simulations d'attaques
- Campagnes de phishing
- Ateliers pratiques
- Escape Game Cyber
- Formations techniques

RÉAGIR

- Intervention rapide (PRIS)
- Analyse post-incident
- Reprise d'activité
- Gestion de crise et communication

COLLABORER

- Club DSI
- Journées Cyber
- Partage d'informations
- Réseau d'experts

450+
Structures Aidées
Plus de 450 structures en PACA accompagnées.

72 000+
Professionnels formés
Plus de 72 000 professionnels formés.

12
Incidents Gérés
12 cyberincidents importants gérés.

87%
Satisfaction
87% de satisfaction client.

Formation Cybersécurité : L'humain, notre meilleure défense

Une majorité des incidents sont dus à l'erreur humaine.

La sécurité informatique repose sur les individus. Dans le secteur de la santé, où les données sont cruciales, des formations claires sont indispensables.

Pour les équipes IT : Maîtriser les risques

- **Formation EBIOS (2 jours)** : Évaluer les dangers spécifiques au secteur de la santé.
- Identifier les failles et leurs impacts sur les soins.
- Protéger les systèmes et données patients.

Pour Soignants & Administration : Bons gestes quotidiens

- **E-learning sécurité** : Modules courts (15-30 min) sur les règles clés (phishing, mots de passe, données patients).
- **Escape Game "Crack'n Hack"** : Jeu interactif (1h/équipe) pour s'exercer à la sécurité.

Pour Directions & Utilisateurs : Vigilance & Protection

- **Sensibilisation RGPD** : Comprendre la protection des données et les règles santé.
- **Campagnes de signalement** : Signaler facilement toute activité suspecte.

Pour tous : Exercices de préparation

- **Simulation de Cyberattaque** : Exercices réels avec le personnel.
- **Tester le Plan de Continuité** (PCRA) et renforcer la réactivité.
- Rapport détaillé pour améliorer les procédures.

72 000+

Professionnels formés

en 2024, pour une meilleure sécurité numérique.

342

Exercices d'urgence

organisés pour améliorer les plans en cas de problème.

+- 100

Sessions d'Escape games

animés, pour apprendre la sécurité en s'amusant.

Collaborer

Animation d'une communauté d'acteurs en charge des systèmes d'information dans le secteur médico-social

NOMBRE DE RENCONTRES **15**
Sessions programmées

SESSIONS AVEC VOLET CYBERSÉCURITÉ **10+**
Échanges dédiés

RETEX PARTAGÉS (CYBER ET SI) **12+**
Partage d'expériences

Illustrations générées par une intelligence artificielle

La parole à la région Bretagne !

Jérémy THOMAS
Directeur de la transition numérique
Fondation Massé - Trévidy

Lionel LECOMTE
Chargé de mission cybersécurité et DPO
ARS Bretagne

Médico-social : notre accompagnement cyber régional depuis 2024 en Bretagne

1- Marché régional d'acquisition de prestations de cyber-résilience depuis 2023

➢ Contexte du marché :

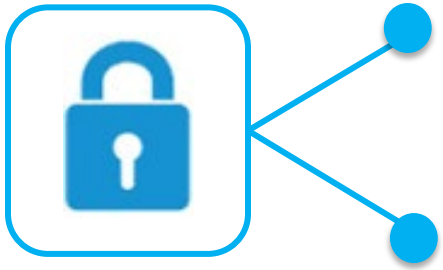
Augmentation des risques de cyberattaques

SÉGUR NUMÉRIQUE

Programme CaRE

Comité Régional SSI & Protection des données

➢ Objectifs du marché :



Se préparer

Entrainement et renforcement des capacités de réaction et de continuité d'activité

Ex. Procédure de gestion de crise, exercices de simulation de cyber-crises, PCA/PRA...

Réagir

Appui à la réponse aux incidents de sécurité

Ex. Prestataire régional de Réponse aux Incidents de Sécurité (PRIS)...

Médico-social : notre accompagnement cyber régional depuis 2024 en Bretagne

2 - POC, Appels à manifestation d'intérêt, Exercices de crise d'origine cyber, Cyber diagnostiques

2024 : 1er POC « exercices de crise d'origine cyber » - 5 mois

➢ Contexte :

26 600 €
3 800€ / exercice

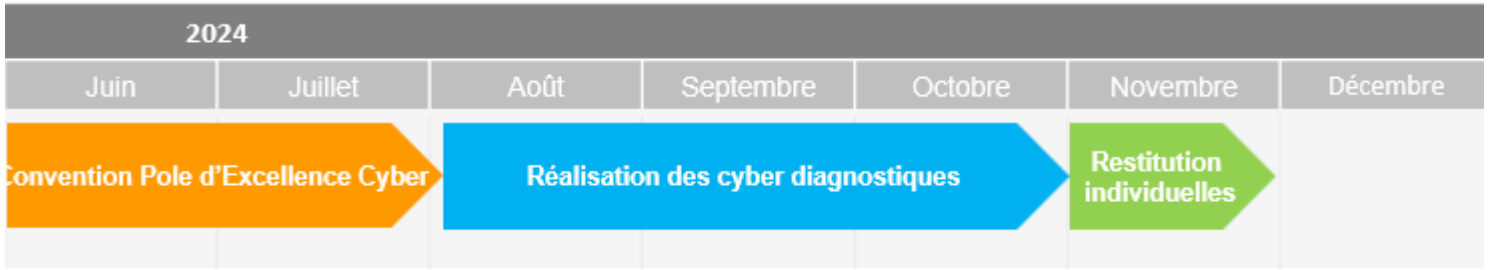
7 ESMS

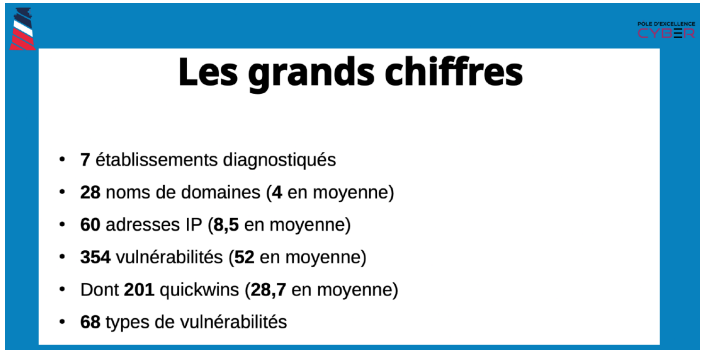
2024 : 2e POC « cyber diagnostiques » - 6 mois

➢ Contexte :

12 600 €
1 800€ / cyberdiag

7 ESMS





Médico-social : notre accompagnement cyber régional depuis 2024 en Bretagne

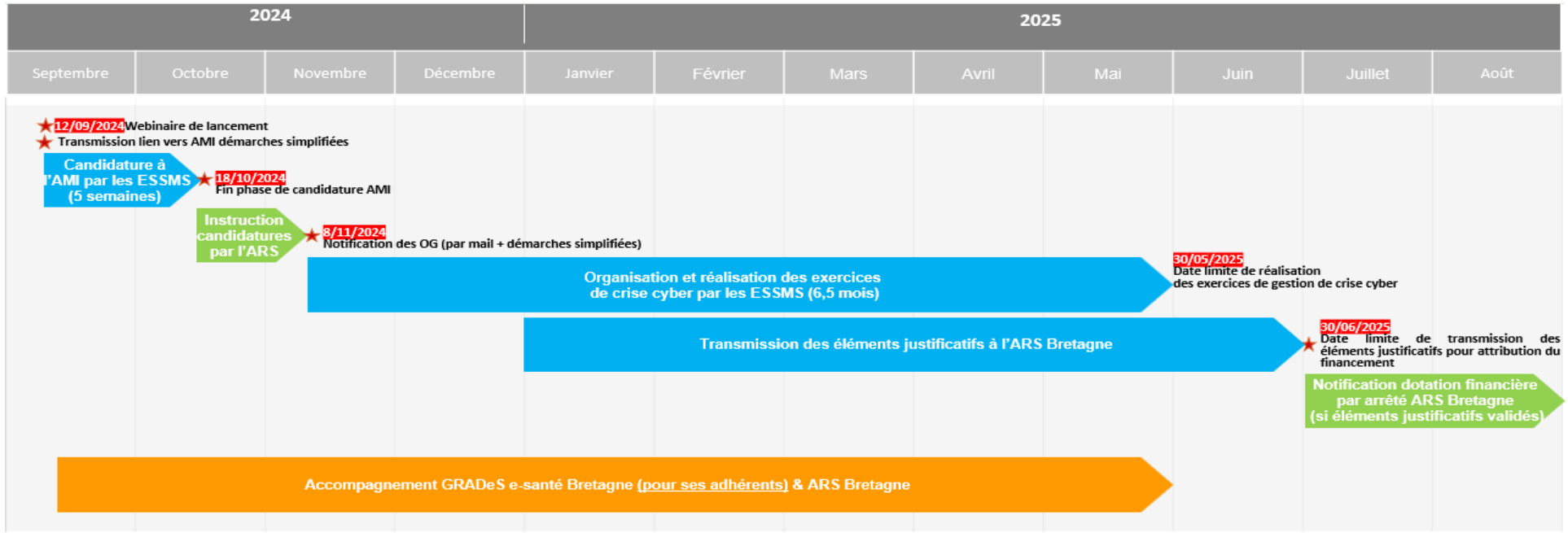
2 - POC, Appels à manifestation d'intérêt, Exercices de crise d'origine cyber, Cyber diagnostiques

➢ Contexte :

117 800 €
3 800€ / exercice

31 ESMS

2024-2025 : 1er AMI « exercices de crise d'origine cyber » - 10 mois



Médico-social : notre accompagnement cyber régional depuis 2024 en Bretagne

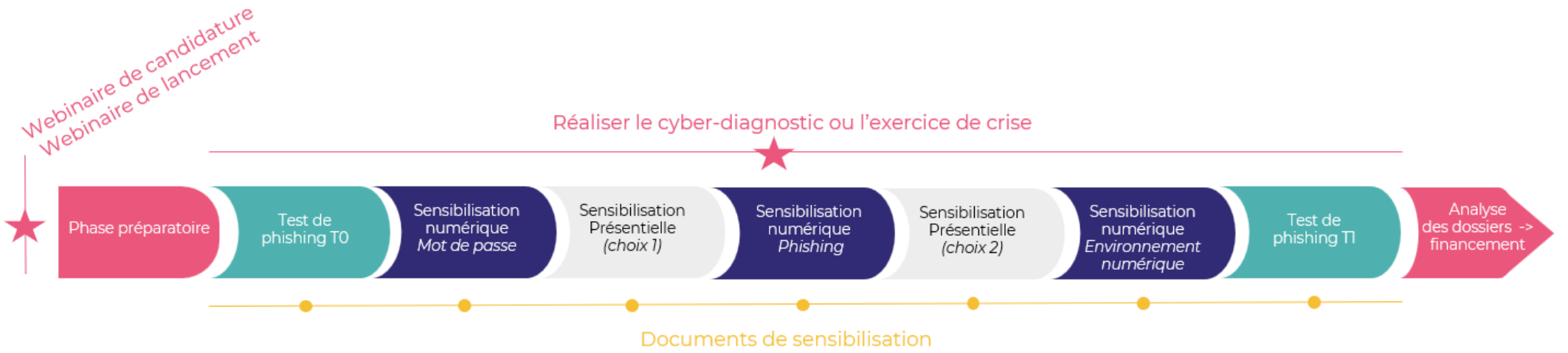
2 - POC, Appels à manifestation d'intérêt, Exercices de crise d'origine cyber, Cyber diagnostiques

2025-2026 : lancement de 3 AMI « parcours cyber » - 9 à 10 mois

Contexte :

240 000 €
5000€ / exercice
3000€ / cyberdiag

60 ESMS



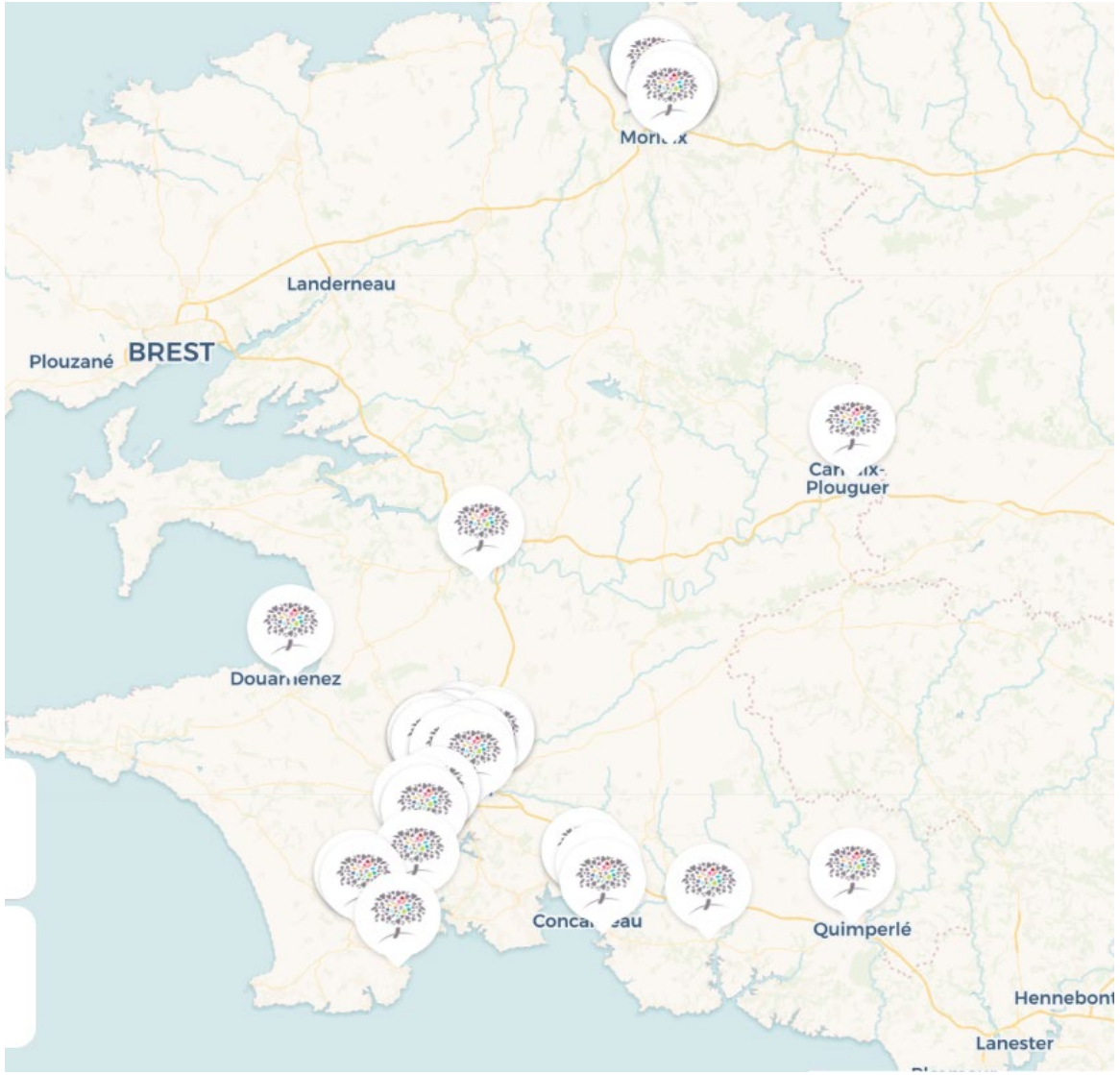
Vague 1	Octobre 2025	Novembre 2025	Décembre 2025	Janvier 2026	Février 2026	Mars 2026	Avril 2026	Mai 2026	Juin 2026
Vague 2	Janvier 2026	Février 2026	Mars 2026	Avril 2026	Mai 2026	Juin 2026	Juillet-Aout 2026	Septembre 2026	Octobre 2026
Vague 3	Mars 2026	Avril 2026	Mai 2026	Juin 2026	Juillet-Aout 2026	Septembre 2026	Octobre 2026	Novembre 2026	Décembre 2026

Budget global depuis 2024 : 400 K€

La parole à la région Bretagne !

FONDATION MASSÉ-TRÉVIDY

- [ ] L'enfance
- [ ] De l'enfance à l'âge adulte
- [ ] Les adultes
- [ ] Les personnes âgées



La parole à la région Bretagne !

Rappel des principaux objectifs

- Découvrir la gestion de crise cyber en condition réelle dans le contexte de votre établissement de santé
- Comprendre l'écosystème cyber de votre structure
- Appréhender les premiers bons réflexes en situation de crise cyber
- Assurer au mieux la continuité des soins

Date

26/05/2025

- 14h00 – 17h00

Participants

- 6 joueurs
- 1 animateur
- 1 observateur

Lieu de réalisation de l'exercice

- 1 salle pour la cellule de crise
- 1 salle pour la cellule animation à distance

AGENCE DU NUMÉRIQUE EN SANTÉ

La parole à la région Bretagne !

Synthèse globale

Organisation et coordination, communication entre les joueurs
Cellule de crise décisionnelle

Coordination avec les autorités : Le contact a été pris rapidement avec la DPO, la CNIL, le CERT Santé, l'ARS, le Conseil Départemental et la direction. Cela montre une maîtrise des procédures réflexes. La collaboration avec l'ARS et le Conseil Départemental a permis l'élaboration d'un communiqué de presse commun.

Structuration de la cellule de crise : L'attribution de référents par secteur a été organisée par le coordinateur pour centraliser les retours. Cette organisation permet de mieux se coordonner et d'améliorer la synthèse des informations.

Réactivité et mobilisation rapide : La cellule de crise a été activée rapidement à la suite de l'analyse des informations. Après l'activation, une communication immédiate a été réalisée auprès des établissements et des parties prenantes (DA, directeurs, DGA, etc.)

Communication externe : Il serait intéressant de prévoir un plan de communication externe en amont de la crise afin d'avoir des éléments dès le début de la cellule de crise.

Répartition des rôles à clarifier : Certains échanges montrent des hésitations sur l'attribution des tâches au sein de la cellule. Un organigramme serait important à afficher au sein de la cellule.

Briefing initial : Il serait pertinent de renforcer le briefing initial en cellule de crise afin qu'il soit plus approfondi et plus synthétique, en s'appuyant notamment sur un modèle structurant le contenu à aborder.

Point de situation : Il pourrait être bénéfique, dès le début de la cellule, de définir une comitologie (régularité des points de situation) et d'avoir une structure synthétique pour animer un point de situation.

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

3. Présentation du kit d’exercice de crise V2

Comment puis-je me préparer à un exercice de crise ?

Etape 1 : Récupérer et télécharger le kit ANS V2. Vous y trouverez **des chronogrammes spécifiques au médico-social**.

Où le trouver ?

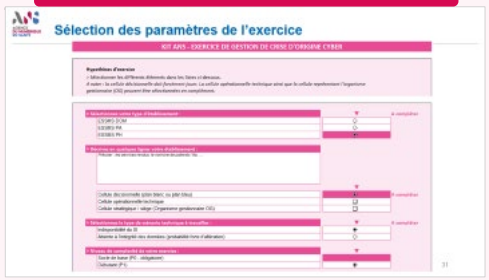
Cybersécurité ANS

Rubrique « **Comment s'approprier les méthodologies CaRE en ESMS ? »**

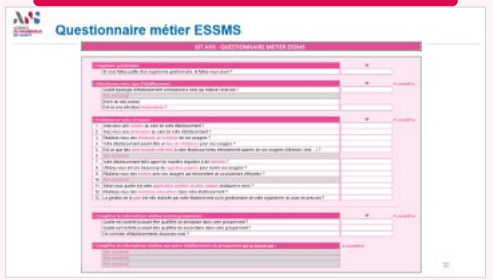
Etape 2 : Lire l'onglet « Lisez-moi» et compléter les différents onglets de préparation.

L'ONGLET « LISEZ –MOI »

PARAMÈTRE EXERCICE



QUESTIONNAIRE MÉTIER



DESCRIPTION DU SI

Etape 3 : Votre chronogramme est généré automatiquement et prêt à être utilisé !

Pour vous faire accompagner dans toutes ces étapes, **prenez contact avec votre CRRC**

L’onglet « Lisez-moi »

MODE D'EMPLOI DU FICHIER

MODE D'EMPLOI DU FICHIER

Important : Ce fichier contient certaines formules permettant la génération d'un chronogramme automatisé et nécessitant l'utilisation d'une version récente de Microsoft Office 365. Si vous disposez d'une version d'Excel non récente, nous vous prions de bien vouloir utiliser le fichier chronogramme non automatisé.

Attention : Il est impératif de ne pas modifier la structure du fichier.

Onglet 1 : Lisez-moi

Vous trouverez dans ce premier onglet le [Lisez-moi] qui vous permettra de comprendre les différents onglets et comment fonctionne le fichier ANS_Chronogramme ESSMS.

Onglet 2 : Sélection paramètres exercice

Dans l’onglet [Sélection paramètres exercice], cochez les cases correspondant à votre type d’établissement, au nombre de cellules que vous souhaitez faire jouer simultanément et au scénario technique que vous voulez travailler.

En fonction de la difficulté que vous sélectionnerez, vous verrez apparaître en dessous des pourcentages. Ces derniers correspondent au pourcentage de savoirs-faire que vous allez travailler sur l’ensemble de la compétence. Cela signifie que si le pourcentage est de 33%, vous allez travailler 33% des savoirs-faire de cette compétence.
Enfin sélectionnez si vous le souhaitez des ateliers de production.

Onglet 3 : Questionnaire métier

Dans l’onglet [Questionnaire métier ESSMS], complétez les informations relatives à votre structure. Cela permet d'adapter le chronogramme à votre environnement et le rendre plus réaliste.

Onglet 4 : Description du Système d’Information (SI)

Décrivez votre Système d’Information dans l’onglet prévu [Description du SI] pour contextualiser le chronogramme technique de votre exercice.

Onglet 5 : Chronogramme généré automatiquement

Votre chronogramme est généré automatiquement et est disponible pour consultation et animation dans l'onglet [CHRONO AUTOMATISE].

Sélection des paramètres de l'exercice

KIT ANS - EXERCICE DE GESTION DE CRISE D'ORIGINE CYBER

Hypothèses d'exercice

> Sélectionner les différents éléments dans les listes ci-dessous.

A noter : la cellule décisionnelle doit forcément jouer. La cellule opérationnelle technique ainsi que la cellule représentant l'organisme gestionnaire (OG) peuvent être sélectionnées en complément.

> Sélectionnez votre type d'établissement :		A compléter
ESSMS DOM	○	
ESSMS PA	○	
ESSMS PH	◉	

> Décrivez en quelques lignes votre établissement :
Préciser : les services rendus, le nombre de patients / lits, …

		A compléter
Cellule décisionnelle (plan blanc ou plan bleu)	◉	
Cellule opérationnelle technique	☐	
Cellule stratégique / siège (Organisme gestionnaire OG)	☐	

> Sélectionnez le type de scénario technique à travailler :		A compléter
Indisponibilité du SI	◉	
Atteinte à l'intégrité des données (probabilité forte d'altération)	○	

> Niveau de complexité de votre exercice :	
Socle de base (P0 - obligatoire)	
Débutant (P1)	◉

Questionnaire métier ESSMS

KIT ANS - QUESTIONNAIRE METIER ESSMS

> Organisme gestionnaire		
	Si vous faites partie d'un organisme gestionnaire, le faites-vous jouer ?	
> Sélectionnez votre type d'établissement :		A compléter
	Quelle typologie d'établissement correspond à celui qui réalise l'exercice ?	
	Non concerné	
	[Nom du site joueur]	
	Est-ce une structure médicalisée ?	
> Précisions sur votre structure		A compléter
1.	Avez-vous une cuisine au sein de votre établissement ?	
2.	Avez-vous une pharmacie au sein de votre établissement ?	
3.	Réalisez-vous des missions au domicile de vos usagers ?	
4.	Votre établissement peut-il être un lieu de résidence pour vos usagers ?	
5.	Est-ce que des intervenants externes à votre établissements interviennent auprès de vos usagers (Médecin, kiné,...) ?	
6.	*Non concerné*	
7.	Votre établissement fait-il appel de manière régulière à de l'intérim ?	
8.	Utilisez-vous encore beaucoup de registres papiers pour suivre vos usagers ?	
9.	Réalisez-vous des sorties avec vos usagers qui nécessitent un ou plusieurs véhicules ?	
10.	*Non concerné*	
11.	Selon vous quelle est votre application (métier) la plus critique (Indiquer le nom) ?	
12.	Réalisez-vous des missions éducatives dans votre établissement ?	
13.	La gestion de la paie est-elle réalisée par votre établisement ou le gestionnaire de votre organisme (si vous en avez un) ?	
> Complétez les informations relatives à votre groupement :		A compléter
	Quelle est l'activité pouvant être qualifiée de principale dans votre groupement ?	
	Quelle est l'activité pouvant être qualifiée de secondaire dans votre groupement ?	
	De combien d'établissements disposez-vous ?	
> Complétez les informations relatives aux autres établissements du groupement qui ne jouent pas :		A compléter
	Non concerné	
	Non concerné	
	Non concerné	

Description du SI

KIT ANS - EXERCICE DE GESTION DE CRISE D'ORIGINE CYBER

Choisir sa situation

> Sélectionner parmi les 5 cas de figure proposés celui qui corresponderait le mieux à votre structure.

> Ce sont des paramètres généraux orientant le scénario technique.

> Il est obligatoire de choisir l'un d'entre-eux, toutefois nous vous invitons à vous rapprocher de vos interlocuteurs pour des cas très particuliers.

Note : ces éléments visent à contextualiser au mieux les aspects techniques du scénario. Cependant, des incohérences peuvent subsister, ce qui est inhérent à l'exercice de crise en kit.

	Votre réseau est-il cloisonné (avec filtrage) ou est-il à plat (e.g. LAN spécifique mais sans filtrage) ?	*Votre SI est-il infogéré ou interne ?*	*Votre serveur de gestion des sauvegardes est-il isolé ou non-isolé ?*	*Votre infrastructure est elle interne (on-prem) ou hébergé par un tiers ?*
Cas n°1	Cloisoné	Infogéré	Isolé	Infra on-prem
Cas n°2	Cloisoné	Infogéré	Isolé	Hébergement Tiers
Cas n°3	Non-cloisoné	Infogéré	Non-isolé	infra on-prem
Cas n°4	Cloisoné	Interne	Isolé	infra on-prem
Cas n°5	Non-cloisoné	Interne	Non-isolé	Infra on-prem

Choix du cas	**Cas n°3**

Description du SI

Votre SI est-il centralisé au niveau siège ?	Oui

		Hébergement & connexion	Nom de l'asset	Si externalisé, nom du partenaire / prestataire / fournisseur	Commentaire
		A compléter			
Transverse					
	Votre équipe DSI est-elle …				Pour un établissement dont l'informatique est géré au niveau du siège, merci de le préciser en commentaire
	Votre support informatique pour les utilisateurs du SI de l'établissement est-il …		[Nom du support informatique ou d'un membre de l'équipe]		Idem que ci-dessus
	Avez-vous une cyber assurance ?		[Nom de l'assurance]		
	Avez-vous un CERT (autre que CERT-Santé) ? (préciser si PRIS en commentaire)		[Nom du CERT]		
		A compléter			
Infrastructure & réseau (SI IT)					
	Votre infrastructure (les ADs, DHCP, DNS...) est-elle hébergée …		[Nom]		Si plusieurs AD avec hébergement en hybridre, préciser ici svp
	Avez-vous un VPN ?		[Nom]		
	Utilisez vous des outils d'administration spécifiques ?		[Nom]		Préciser si oui : quels outils utilisez vous ?
	Avez-vous un EDR ?		[Nom de l'EDR]		Préciser le nom de l'EDR; et les autres outils utilisés le cas échéant

Les éléments que vous renseignez dans les différents onglets du fichier permettront de générer un chronogramme qui sera le plus adapté possible à votre contexte.

Réalisation de l'exercice de crise

Qui doit participer à l'exercice de crise ?

Cela dépend de votre organisation mais nous préconisons que soient présents :

- Des membres de la direction,
- Des membres du métier (cadre, infirmier, chef de service,…)
- Des membres de la technique (responsable du système d'information,….)

Peuvent également participer des membres des RH, de la qualité,….

Combien de temps devons-nous prévoir ?

Entre le rappel de la démarche, l'exercice en lui-même et le debrief « à chaud », il faut compter environ 3H.

Une fois l'exercice réalisé, utilisez la grille d'évaluation

Pourquoi ?

Vous trouverez dans le kit une **grille** permettant de générer automatiquement des **diagrammes** illustrant le niveau d'acquisition des compétences.

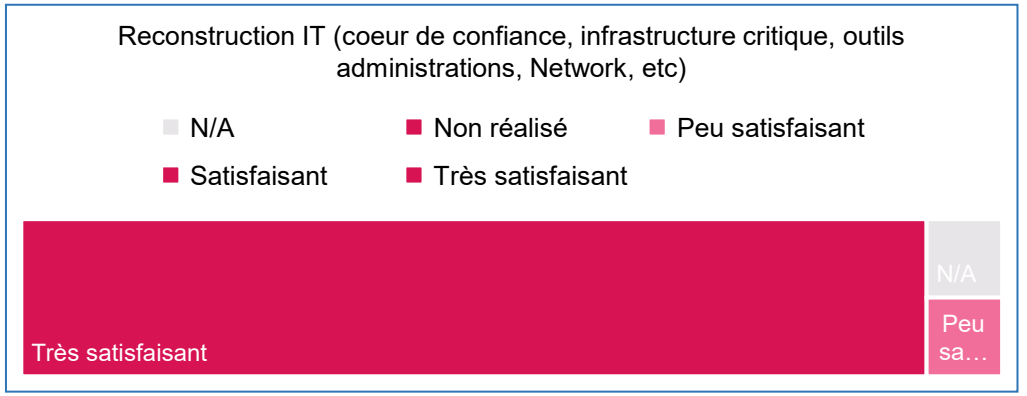
Comment ?

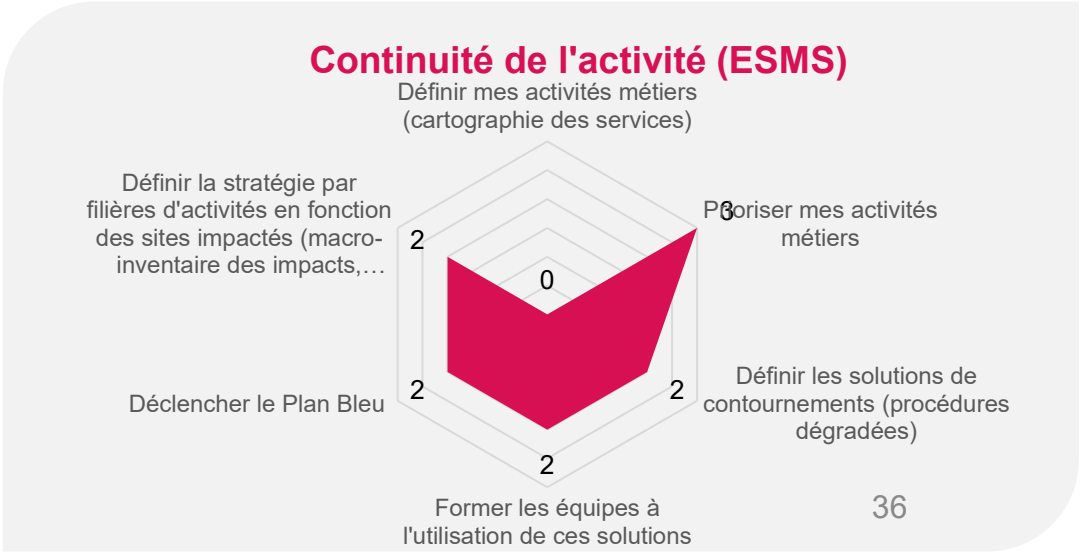
En complétant simplement l'onglet ***« d'évaluation par compétences »*** !

ÉVALUATION DES COMPÉTENCES

RÉSULTATS

TABLEAU DE BORD





Evaluation des compétences

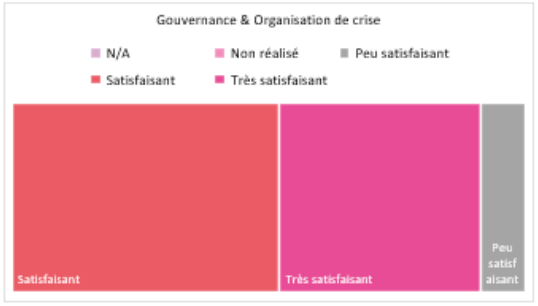
		Non applicable	Non réalisé	Peu satisfaisant	Satisfaisant, des points à améliorer	Très satisfaisant	
		N/A	D	C	B	A	
Gouvernance & Organisation de crise							**Commentaires**
C01-SF1	Définir et connaître le dispositif de gestion de crise				x		
C01-SF2	S'assurer que les rôles fondamentaux de gestion de crise sont bien attribués (pilote, coordinateur, secrétaire de crise)				x		
C01-SF3	Qualifier la situation et donner l'alerte					x	
C01-SF4	Activer le dispositif de gestion crise adaptée au niveau d'alerte					x	
C01-SF5	Connaître le Plan Blanc ou Bleu et savoir le déclencher				x		
C01-SF6	Présenter les différents membres de la cellule (si nécessaire)				x		
C01-SF7	Répartir les rôles au sein de la cellule de crise et expliquer les missions de chacun			x			
C01-SF8	Réorganiser la cellule de crise initiale en sous-cellule pour plus d'agilité et de précision au moment opportun (si nécessaire)			x			
C01-SF9	Savoir s'inscrire dans son écosystème				x		
C01-SF10	Gérer la remontée d'information vers l'organisme gestionnaire (GHT, Organisme gestionnaire ESMS)					x	
C01-SF11	Gérer la remontée d'informations vers l'ARS, CERT-Santé (ANS), GRADeS, Ministère de tutelle				x		
Pilotage & Coordination							**Commentaires**
C02-SF1	Définir les modes de communications au sein de la cellule de crise et s'assurer que tout le monde y a accès				x		
C02-SF2	Définir le rythme de "bataille" pour assurer la coordination au sein de la cellule (rythme des points de situation au sein de la cellule)				x		
C02-SF3	Définir les modes de communications entre les différentes cellules de crise et s'assurer que tout le monde y a accès				x		
C02-SF4	Définir le rythme de "bataille" pour assurer la coordination entre les différentes cellules (rythme des points de situation entre les cellules)				x		
C02-SF5	S'assurer du respect des règles de savoir-être et savoir vivre au sein des cellules (respecter le temps de parole de chacun, ...)				x		
C02-SF6	Assurer la traçabilité des événements, des décisions prises et des actions à réaliser (main courante, tableau de suivi des actions,...)				x		
C02-SF7	Piloter une crise impactant plusieurs établissements				x		
C02-SF8	Définir les modes de communications entre les différents établissements impactés et s'assurer que tout le monde y a accès				x		
C02-SF9	Définir le rythme de "bataille" pour assurer la coordination entre les différents établissements impactés (rythme des points de situation entre les cellules)					x	

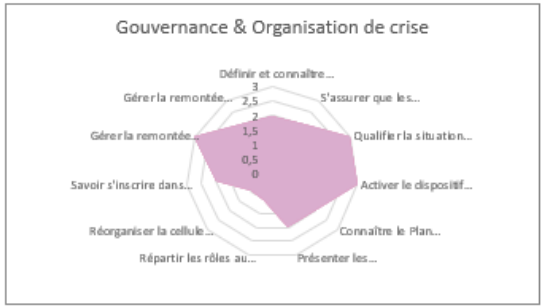
Résultats

	N/A	Non réalisé	Peu satisfaisant	Satisfaisant		Très satisfaisant		Qualité	Sous-total Qualité	Sous-total
Gouvernance & Organisation de crise	0	0	2	6	12	3	9			2,090909
Pilotage & Coordination	0	0	0	8	16	1	3			2,111111
Continuité des soins (ES MCO - ES hors MCO)	1	1	1	1	2	7	21			2,4
Continuité administrative	1	0	0	1	2	6	18			2,857143
Continuité de l'activité (ESMS)	0	1	1	5	10	0	0			1,833333
Continuité informatique & Résilience	0	1	1	0	0	4	12			2,166667
Détection, Investigation, Supervision	0	0	6	0	0	0	0			1
Remédiation (Endiguement, Eviction, Eradication)	0	0	0	10	20	0	0			2
Reconstruction IT (coeur de confiance, infrastructure critique, outils administrations, Network, etc)	1	0	1	0	0	8	24			2,777778
Ressources Humaines	0	0	5	0	0	2	6			1,571429
Communication	0	0	10	0	0	0	0			1
Anticipation des évolutions	0	0	0	5	10	0	0			2
Reconstruction applicative (appli métier, etc)	0	0	2	0	0	1	3			1,666667
Gestion des obligations légales	0	0	3	0	0	2	6			1,8
Gestion logistique	0	0	0	5	10	1	3			2,166667
Gestion Technique du Bâtiment et Sécurité Physique	0	0	8	0	0	0	0			1
				MOYENNE TOTALE						1,72954

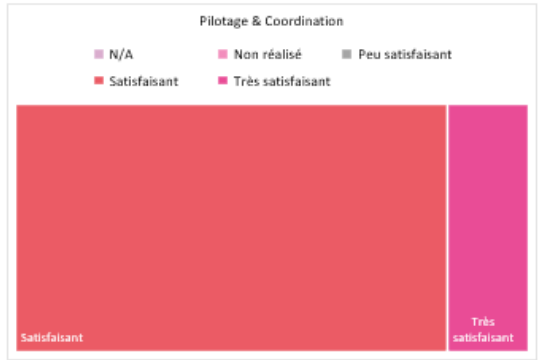
Tableau de bord

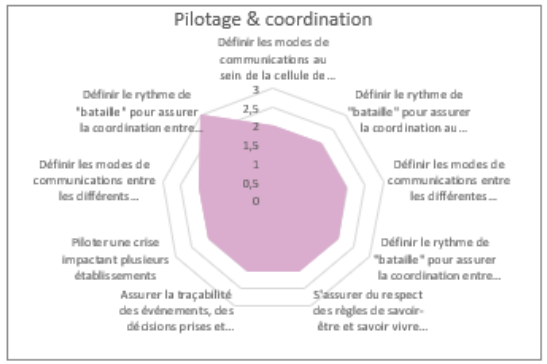
			N/A	Non réalisé	Peu satisfaisant	Satisfaisant	Très satisfaisant	Sous-total
C01	Gouvernance & Organisation de crise		0	0	2	12	8	2,090909091
C01	C01-SF1	Définir et connaître le dispositif de gestion de crise	0	0	0	2	0	2
C01	C01-SF2	S'assurer que les rôles fondamentaux de gestion de crise sont bien attribués (pilote, coordinateur, se	0	0	0	2	0	2
C01	C01-SF3	Qualifier la situation et donner l'alerte	0	0	0	0	3	3
C01	C01-SF4	Activer le dispositif de gestion crise adaptée au niveau d'alerte	0	0	0	0	3	3
C01	C01-SF5	Connaître le Plan Blanc ou Bleu et savoir le déclencher	0	0	0	2	0	2
C01	C01-SF6	Présenter les différents membres de la cellule (si nécessaire)	0	0	0	2	0	2
C01	C01-SF7	Répartir les rôles au sein de la cellule de crise et expliquer les missions de chacun	0	0	1	0	0	1
C01	C01-SF8	Réorganiser la cellule de crise initiale en sous-cellule pour plus d'agilité et de précision au moment	0	0	1	0	0	1
C01	C01-SF9	Savoir s'inscrire dans son écosystème	0	0	0	2	0	2
C01	C01-SF10	Gérer la remontée d'information vers l'organisme gestionnaire (GHT, Organisme gestionnaire ESM	0	0	0	0	3	3
C01	C01-SF11	Gérer la remontée d'informations vers l'ARS, CERT-Santé (ANS), GRADeS, Ministère de tutelle	0	0	0	2	0	2



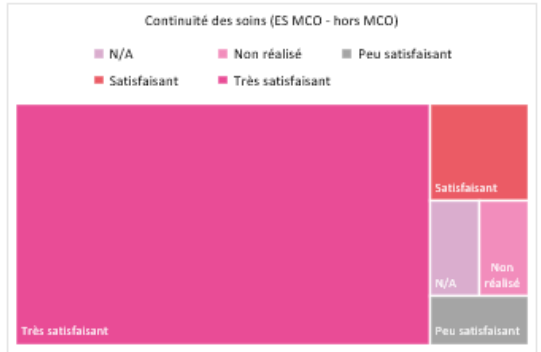


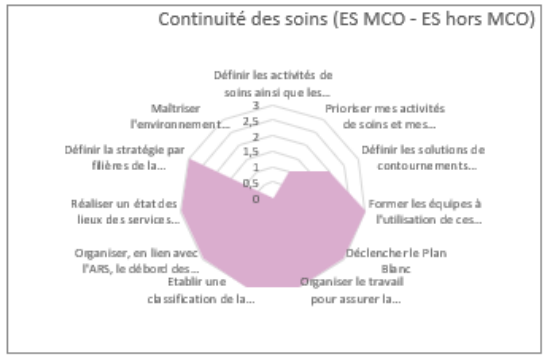
			N/A	Non réalisé	Peu satisfaisant	Satisfaisant	Très satisfaisant	Sous-total
C02	Pilotage & Coordination		0	0	0	16	3	2,111111111
C02	C02-SF1	Définir les modes de communications au sein de la cellule de crise et s'assurer que tout le monde y a accès	0	0	0	2	0	2
C02	C02-SF2	Définir le rythme de "bataille" pour assurer la coordination au sein de la cellule (rythme des points de situation au sein de la cellule)	0	0	0	2	0	2
C02	C02-SF3	Définir les modes de communications entre les différentes cellules de crise et s'assurer que tout le monde y a accès	0	0	0	2	0	2
C02	C02-SF4	Définir le rythme de "bataille" pour assurer la coordination entre les différentes cellules (rythme des points de situation entre les cellules)	0	0	0	2	0	2
C02	C02-SF5	S'assurer du respect des règles de savoir-être et savoir vivre au sein des cellules (respecter le temps de parole de chacun, ...)	0	0	0	2	0	2
C02	C02-SF6	Assurer la traçabilité des événements, des décisions prises et des actions à réaliser (main courante, tableau de suivi des actions,...)	0	0	0	2	0	2
C02	C02-SF7	Piloter une crise impactant plusieurs établissements	0	0	0	2	0	2
C02	C02-SF8	Définir les modes de communications entre les différents établissements impactés et s'assurer que tout le monde y a accès	0	0	0	2	0	2
C02	C02-SF9	Définir le rythme de "bataille" pour assurer la coordination entre les différents établissements impactés (rythme des points de situation entre les cellules)	0	0	0	0	3	3



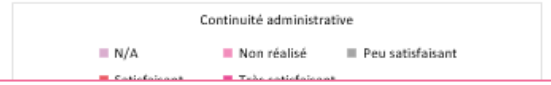


			N/A	Non réalisé	Peu satisfaisant	Satisfaisant	Très satisfaisant	Sous-total
C03	Continuité des soins (ES MCO - ES hors MCO)		1	1	1	2	21	2,4
C03	C03-SF1	Définir les activités de soins ainsi que les activités transverses aux soins (cartographie des services)	0	1	0	0	0	0
C03	C03-SF2	Prioriser mes activités de soins et mes activités transverses aux soins	0	0	1	0	0	1
C03	C03-SF3	Définir les solutions de contournements (procédures dégradées)	0	0	0	2	0	2
C03	C03-SF4	Former les équipes à l'utilisation de ces solutions de contournements	0	0	0	0	3	3
C03	C03-SF5	Déclencher le Plan Blanc	0	0	0	0	3	3
C03	C03-SF6	Organiser le travail pour assurer la continuité des soins (e.g. réorganiser les effectifs de l'établissements pour aider les services les plus en difficulté,...)	0	0	0	0	3	3
C03	C03-SF7	Etablir une classification de la criticité de prise en charge des patients	0	0	0	0	3	3
C03	C03-SF8	Organiser, en lien avec l'ARS, le débord des patients	0	0	0	0	3	3
C03	C03-SF9	Réaliser un état des lieux des services pour connaître leur niveau de fonctionnement	0	0	0	0	3	3
C03	C03-SF10	Définir la stratégie par filières de la continuité des soins en fonction de la territorialité (macro-inventaire des impacts, plan de réponse coordonnée par filières de soins)	0	0	0	0	3	3
C03	C03-SF11	Maîtriser l'environnement biomed en cas de crise cyber (cartographie, dépendances)	1	0	0	0	0	N/A





			N/A	Non réalisé	Peu satisfaisant	Satisfaisant	Très satisfaisant	Sous-total
C04	Continuité administrative		1	0	0	2	18	2,857142857
C04	C04-SF1	Définir mes activités administratives (cartographie des activités)	1	0	0	0	0	N/A



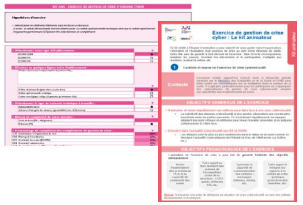
Les supports à disposition

Page Cybersécurité pour le médico-social

Webinaire « Les premières actions cyber à mettre en place »

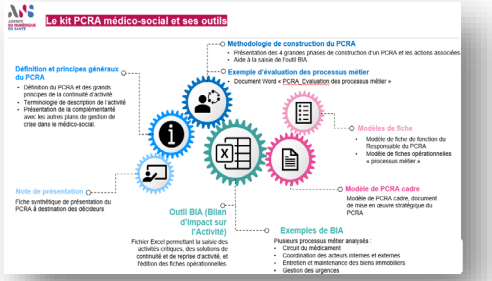
Guide cybersécurité en 13 questions

Kits Exercices de crise



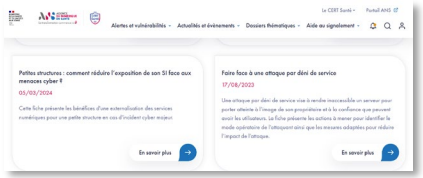
Pourquoi réaliser un exercice de crise ? RETEX de la Ligue Havraise

Le kit PCRA pour le médico-social



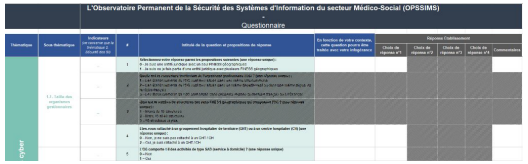
Modules sur la thématique cyber

Fiches thématiques – portail cyberveille



Offre de service des CRRC

L'OPSSIMS – Observatoire Permanent de la Sécurité des Systèmes d'Information dans le Médico-Social



Un grand merci pour votre écoute !

Des retours à nous faire sur le webinaire ? Des thématiques cybersécurité pour le médico-social à traiter lors d'un prochain webinaire ? ….

Nous vous invitons à renseigner un rapide sondage pour nous faire part de votre satisfaction concernant ce webinaire et de vos besoins futurs

Et maintenant ?

« *Nous invitons les ESMS à se faire accompagner par leur CRRC (centre régional de ressources cyber) car une cyberattaque, ça peut arriver à tout le monde. C'est important de pouvoir se projeter et de connaitre les points où nous sommes en fragilité.* »

Directeurs, L'Olivier Bleu

Pour prendre contact avec votre CRRC : https://esante.gouv.fr/strategie-nationale/cybersecurite/axe-2

AGENCE
DU NUMÉRIQUE
EN SANTÉ

esante.gouv.fr

Le portail pour accéder à l'ensemble des services et produits de l'agence du numérique en santé et s'informer sur l'actualité de la e-santé.

@esante_gouv_fr

linkedin.com/company/agence-du-numerique-en-sante