Financé par l'Union européenne
NextGenerationEU

Renforcement de la cybersécurité dans les établissements sanitaires

Kit ANS Exercices Cybercrise

Réunion ARS Ile-de-France / DCGDR / SESAN

Jeudi 16 juin 2022

Intervenants

Rémi TILLY
Directeur du département SSI
SESAN

Emilie SAINZ
Adjointe au Directeur du département SSI
SESAN

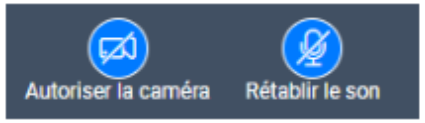
Tania MAC-LUCKIE
RSSI
SESAN

Ordre du jour

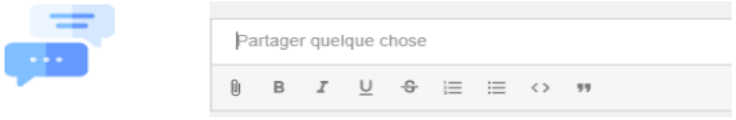
Informations pratiques

Bonnes pratiques de participation au webinaire

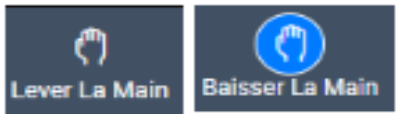
- Je (re)nomme mon nom d'utilisateur : « Etablissement – Nom Prénom »
- Je coupe mon micro et ma caméra quand je ne parle pas



- Les questions doivent être posées par écrit, j'utilise le chat en bas de l'écran pour rebondir, poser mes questions ou commenter. Une réponse concise/synthétique sera effectuée à l'oral. Si besoin un retour dédié sera fait par email ou par une prise de contact.



- Si vous souhaitez compléter oralement, levez la main et la parole vous sera donnée.



Mise en ligne de l'enregistrement vidéo de la session : suivez le lien fourni ultérieurement

Contexte

Contexte

Incidents SI Santé

	2018	2019	2020	2021
Structures ayant déclaré au moins un incident	247	300	369	733
Prises en charge par l'ANSSI	2	11	14	36
Accompagnées par le CERT SANTE	47	70	90	189

	2018	2019	2020	2021
Structures ayant déclaré au moins un incident	-	21%	23%	**99%**
Prises en charge par l'ANSSI	-	450%	27%	**157%**
Accompagnées par le CERT SANTE	-	49%	29%	**110%**

Contexte

SEGUR – Feuille de route Ile-de-France

Objectif IV

- **Contribuer à l'effort de renforcement de la cybersécurité**
  - Promouvoir et suivre les dispositifs et exercices de continuité d'activité
  - Sensibiliser les acteurs de santé aux règles de Cybersécurité

Contexte

SEGUR – Plan Renforcement Cyber

1. Sensibilisation
   - Sensibilisation des décideurs
   - Sensibilisation des acteurs

2. Animation territoriale
   - Partage des pratiques
   - Actions de mutualisation

3. Appui des structures de santé
   - Création d'un centre de ressources régionales

4. Contrôle
   - Veiller à la réalisation d'exercice simple de continuité d'activité avec des procédures de travail en mode numérique dégradé annuellement

Financé par l'Union européenne NextGenerationEU

Contexte

Objectif du KIT débutant de l'ANS

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

Le Kit ANS Débutant

Le Kit ANS Débutant

Vidéo

Le Kit ANS Débutant

Suis-je concerné par le kit "débutant" ?

- Grille d'auto-évaluation :
  - ➢ Une fiche d'identité à compléter
  - ➢ Une liste de 23 questions (case à cocher)
  - ➢ Une grille d'appréciation des résultats

Le Kit ANS Débutant

Exemple de question

Score

< 75 : kit débutant

74 < Score < 151 : kit intermédiaire

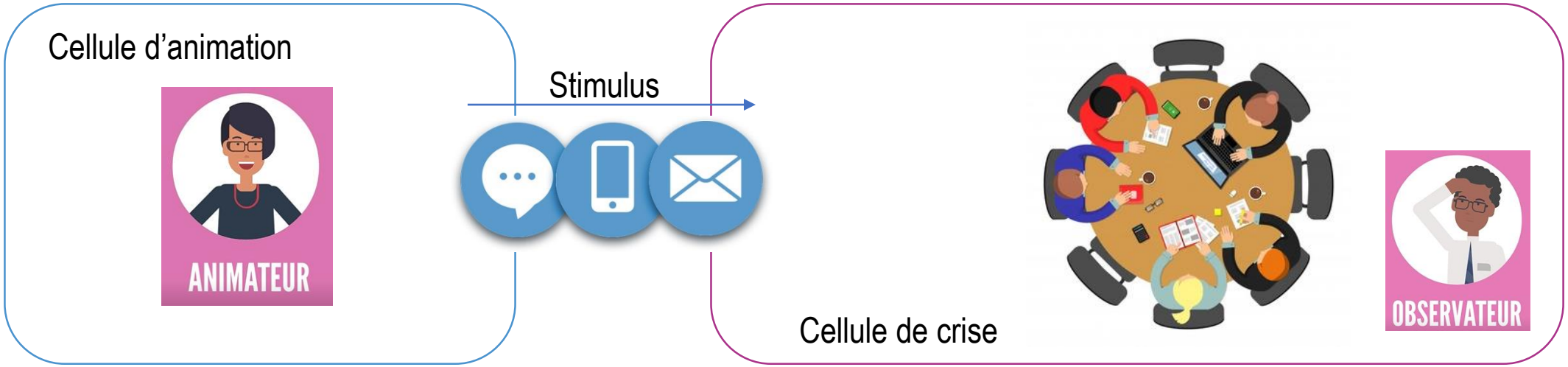
> 150 : kit confirmés

- Grille d'auto-évaluation

Question	Kit débutants		Kit intermédiaires		Kit confirmés	
Comment les utilisateurs à privilèges sont-ils recensés ? Sont-ils informés de leurs rôles et responsabilités en matière de cybersécurité ?	- Les utilisateurs à privilèges sont recensés de manière informelle - Les rôles et responsabilités des utilisateurs à privilèges sont communiqués de manière informelle.		- Un recensement des utilisateurs à privilège est effectué de manière partielle et peu mis à jour - Une charte administrateur est partiellement documentée pour les utilisateurs à privilèges.		- Les utilisateurs à privilège sont tous connu. Un recensement est réalisé régulièrement ainsi qu'une revue d'accès. - Une charte administrateur est partiellement documentée pour les utilisateurs à privilèges. - Les utilisateurs à privilèges sont entraînés régulièrement afin de comprendre leurs rôles et responsabilités et le risque inhérent à leur statut. - La charte est appliquée, les utilisateurs privilégiés signent la charte informatique ou la charte informatique est annexée au contrat / au règlement intérieur	

Le Kit ANS Débutant

Organisation



L'animateur met en action le scénario en envoyant les stimuli à la cellule de crise sous forme de simulations d'appels ou de mails pour susciter une réaction / action des joueurs.

Les joueurs s'adaptent à la situation de crise fictive déroulée par l'animateur en utilisant des moyens de communication et procédures opérationnelles habituellement utilisées dans la structure (si elles existent).

L'observateur apporte un regard extérieur à l'exercice et relève les points positifs et axes d'amélioration selon les objectifs de l'exercice. Il n'intervient pas dans le déroulement de l'exercice.

Le Kit ANS Débutant

Quels profils choisir ?

- Bon communiquant
- Capacité de synthèse
- A participé à un exercice de crise (exemple plan blanc)
- Peut être un binôme
- Profil possible : élève directeur, rssi

- Capacité de synthèse
- Capacité d'analyse
- A participé à un exercice de crise (exemple plan blanc)
- Profil possible : gestionnaire de risque, rssi

Préparer l’exercice

Le Kit ANS Débutant

Avant l'exercice

1 L'animateur s'approprie et adapte à l'ES l'ensemble des documents du kit d'animation avant l'exercice

- 21 documents :
  - 12 pour l'animateur (dont 6 à destination également de l'observateur)
  - 8 pour chaque participant
  - 1 support de communication
- Prévoir 3 jours pour cette étape de préparation, sur 3 semaines environ

S'entrainer à présenter le PPT de Briefing et de Debriefing

Le Kit ANS Débutant

Avant l'exercice

2 Il s'assure que la structure de santé a transmis les invitations aux joueurs grâce au kit de communication

3 Il récupère la liste des joueurs en faisant compléter l'annuaire des participants à la structure de santé

- L'exercice est destiné à faire prendre conscience du risque cyber. La sélection des participants doit être faite en fonction de cet objectif : Qui veut-on sensibiliser ?

- Qui sont les joueurs?
  - La direction
  - Toute personne qui peut avoir un rôle à jouer en cas de cyber-attaque
    - Communication
    - Chef de service
    - DSI/RSSI
    - …

- Compléter l'annuaire

- Fixer la date de l'exercice **au plus tôt** et envoyer l'invitation

3 bis. Personnaliser le chronogramme

- Le chronogramme est un document listant les différents stimuli
  - Exemple :

N °	FREQUENCE	PHASE	Contenu STIMULI (contenu du mail ou de l'appel téléphonique)	ÉMETTEUR	DESTINATAIRE	MODALITÉ DE TRANSMISSION	INPUT STIMULIS	RÉACTIONS ATTENDUES	Commentaires à l'attention de l'animateur
1	**13h55**	Remontée d'alerte 1	Bonjour, Je vous appelle car je n'arrive plus à accéder à mes dossiers de travail depuis mon poste. Je clique dessus mais il ne se passe rien. J'ai l'impression que mes applications et notamment le logiciel GAM (Gestionnaire Administratif du Malade) ne sont plus accessibles non plus. J'ai demandé de l'aide à mes collègues mais ils ne comprennent pas non plus d'où peut venir le problème.	Accueil de la structure de santé	Support IT	Simulation d'appel téléphonique			**Ce premier stimuli est partagé à la fin du briefing. Il déclenche la mobilisation de la cellule de crise.**

- Mettre à jour sur le chronogramme les destinataires des stimuli en fonction de la liste des participants identifiés par l'établissement.

- Personnaliser les émetteurs par les noms et prénoms de personnes existantes au sein de l'établissement.

Le Kit ANS Débutant

Avant l'exercice

4 Il envoie le kit participant aux joueurs (ou via la structure de santé) une semaine avant l'exercice

- Composition du Kit Participant :
  1. Livret participant relatif à la préparation à l'exercice de crise cybersécurité
  2. Fiche mémo compréhension des spécificités d'une crise cybersécurité
  3. Bonnes pratiques de gestion de crise cybersécurité
  4. Bonnes pratiques de communication en cas de crise cybersécurité
  5. Bonnes pratiques de déclaration d'incident (CERT Santé et CNIL) à l'attention des participants techniques (SSI/IT)
  6. Fiche mémo compréhension du rôle du CERT Santé dans la réponse à incident à l'attention des participants techniques (SSI/IT)
  7. Relevé de l'ensemble des actions/décisions prises pendant l'exercice de crise cybersécurité
  8. Liste du vocabulaire de l'exercice de crise cybersécurité

Financé par l'Union européenne NextGenerationEU

5. Prévoir la logistique

- Réserver 2 salles proches l'une de l'autre
  - Une pour l'animation
  - Une pour la cellule de crise (avec un vidéoprojecteur pour le briefing et le debriefing)
- Prévoir et tester la liaison téléphonique entre les 2 salles
- S'assurer que les participants aient accès à leur ordinateur
- Créer une adresse mail dédiée à l'exercice pour l'envoi des stimuli
  - Préparer en mode "brouillon" les mails de stimuli
- Imprimer :
  - Le chronogramme (en A3)
  - Les questionnaires de satisfaction (pour chacun des joueurs)
  - Le kit participant

Animer l’exercice

Le Kit ANS Débutant

Pendant l'exercice

1. L'animateur prépare les joueurs à l'exercice en présentant le support de briefing qu'il diffuse dans la salle
2. Il débute l'exercice en lançant par téléphone le premier stimuli présent sur le chronogramme qu'il a imprimé en amont

- Briefing :
  - Organisation et déroulement de l'exercice
  - Principales règles à retenir
  - Outils à votre disposition

Le Kit ANS Débutant

Pendant l'exercice

3 Au cours de l'exercice, il varie le type de stimuli transmis aux joueurs grâce à son livret de stimuli : il pourra en envoyer certains par mail via la boite aux lettres créée pour l'exercice

- Suivre le chronogramme en veillant à respecter au maximum la cadence prédéfinie
- Rayer au fur et à mesure les stimuli qui ont été réalisé

ÉMETTEUR	DESTINATAIRE	MODALITÉ DE TRANSMISSION	INPUT STIMULIS	RÉACTIONS ATTENDUES
Animateur ou personne en charge de la communication sur l'exercice				Prise de connaissance des particulière attendue.
Animateur	Tous les joueurs	A l'oral + support de présentation		

Le Kit ANS Débutant

Pendant l'exercice

L'observateur assiste à l'exercice auprès de la cellule de crise et rempli la grille d'évaluation

- Il n'est pas conseillé de remplir la grille en temps réel mais plutôt de prendre des notes et de la compléter par la suite
- Elle a pour but d'évaluer de manière objective le déroulé de l'exercice ainsi que la réponse apportée par l'ensemble des joueurs.

- 6 thématiques :
  - Méthodologie de gestion de crise
  - Organisation de la cellule de crise
  - Prise de décision
  - Réponse technique
  - Réponse métier
  - Compétences de gestion de crise de la cellule

		Non applicable	Non réalisé	Peu satisfaisant	Satisfaisant, des points à améliorer	Très satisfaisant
		N/A	0	1	2	3
Méthodologie de gestion de crise						
1	Le déroulé classique de gestion de crise (briefing initial/alerte, qualification, gestion de la crise, clôture) a-t-il été bien suivi ?					
2	Le scénario de l'exercice a-t-il été bien compris ?					

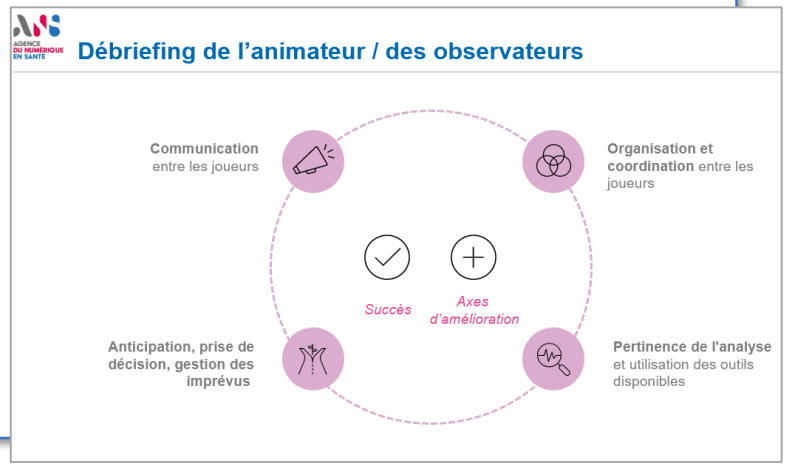
Financé par l'Union européenne NextGenerationEU

Préparer le Debriefing

Pendant la phase de debriefing, l'observateur participe à la définition des points forts de la cellule de crise et met en avant les axes d'amélioration

- 15 min d'échanges entre l'observateur et l'animateur

- Identifier les succès et les axes d'amélioration sur les thématiques suivantes:
  - Communication entre les joueurs
  - Organisation et coordination entre les joueurs
  - Pertinence de l'analyse et utilisation des outils disponibles
  - Anticipation, prise de décision et gestion des imprévus



Le Kit ANS Débutant

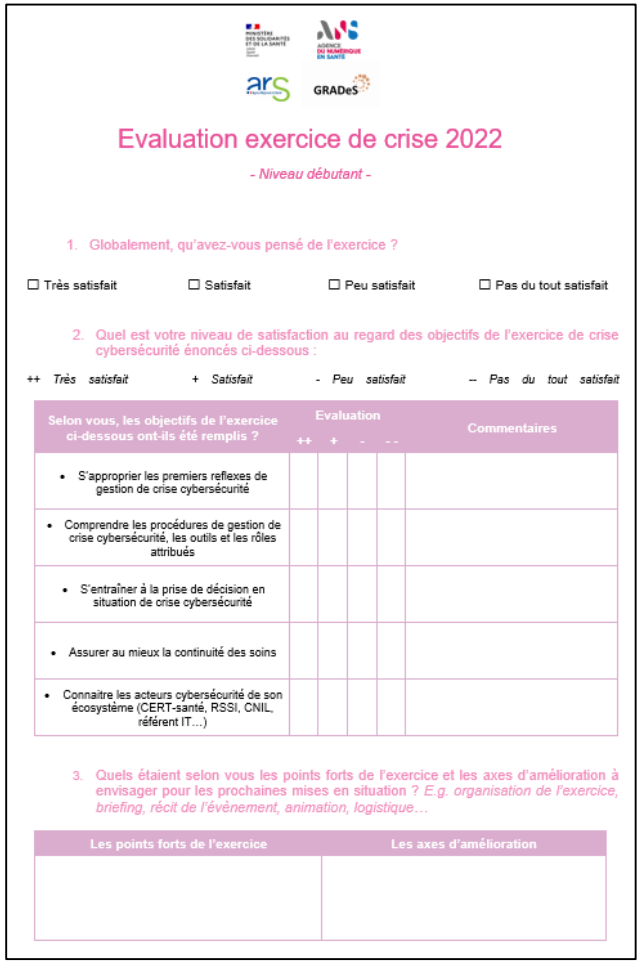
Pendant l'exercice

4 Une fois l'exercice clos, l'animateur présente le support de debriefing qu'il diffuse dans la salle et distribue le questionnaire de satisfaction pour récupérer les retours des participants

- Contenu:
  - Rappel du contexte de l'exercice
  - Que s'est-il passé ?
  - Debriefing à chaud de l'exercice
    - Veiller à ce que tous les participants s'expriment
  - Souvenez-vous de ces quelques bonnes pratiques !

- Compter 30 minutes de débriefing à chaud (penser à prendre connaissance du support en amont)

- Distribuer les enquêtes de satisfaction aux participants



Evaluation exercice de crise 2022

- Niveau débutant -

1. Globalement, qu'avez-vous pensé de l'exercice ?

☐ Très satisfait ☐ Satisfait ☐ Peu satisfait ☐ Pas du tout satisfait

2. Quel est votre niveau de satisfaction au regard des objectifs de l'exercice de crise cybersécurité énoncés ci-dessous :

++ *Très satisfait* + *Satisfait* - *Peu satisfait* -- *Pas du tout satisfait*

Selon vous, les objectifs de l'exercice ci-dessous ont-ils été remplis ?	Evaluation ++	+	-	--	Commentaires
• S'approprier les premiers reflexes de gestion de crise cybersécurité					
• Comprendre les procédures de gestion de crise cybersécurité, les outils et les rôles attribués					
• S'entraîner à la prise de décision en situation de crise cybersécurité					
• Assurer au mieux la continuité des soins					
• Connaitre les acteurs cybersécurité de son écosystème (CERT-santé, RSSI, CNIL, référent IT…)					

3. Quels étaient selon vous les points forts de l'exercice et les axes d'amélioration à envisager pour les prochaines mises en situation ? *E.g. organisation de l'exercice, briefing, récit de l'évènement, animation, logistique…*

Les points forts de l'exercice	Les axes d'amélioration

Après l'exercice

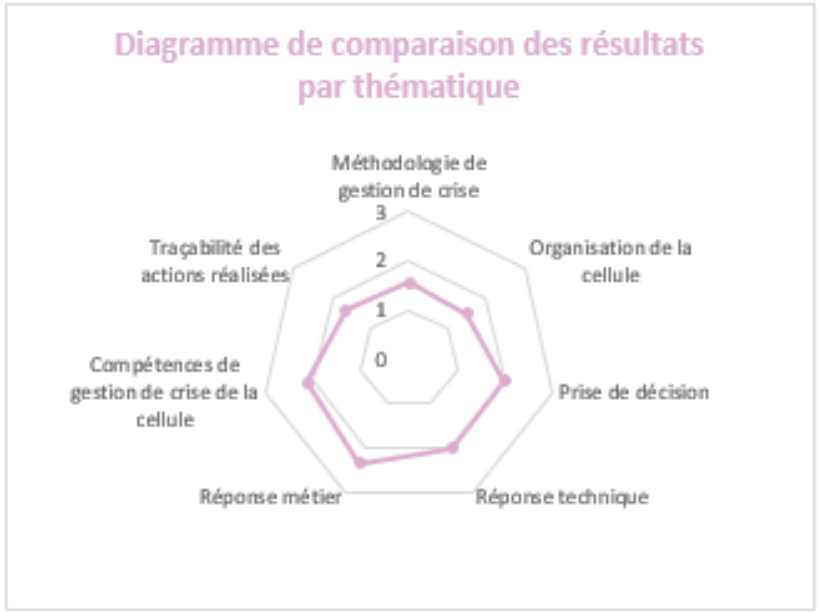
Le Kit ANS Débutant

Après l'exercice

1 L'animateur prend connaissance de la grille d'évaluation remplie par l'observateur ainsi que des retours des joueurs sur le questionnaire

- 40 critères, répartis sur 7 thématiques, évalués de 0 à 3 (non réalisé à très satisfaisant)

		Non applicable	Non réalisé	Peu satisfaisant	Satisfaisant, des points à améliorer	Très satisfaisant
		N/A	0	1	2	3
13	Des points de situation réguliers ont-ils été organisés tout au long de l'exercice ?					

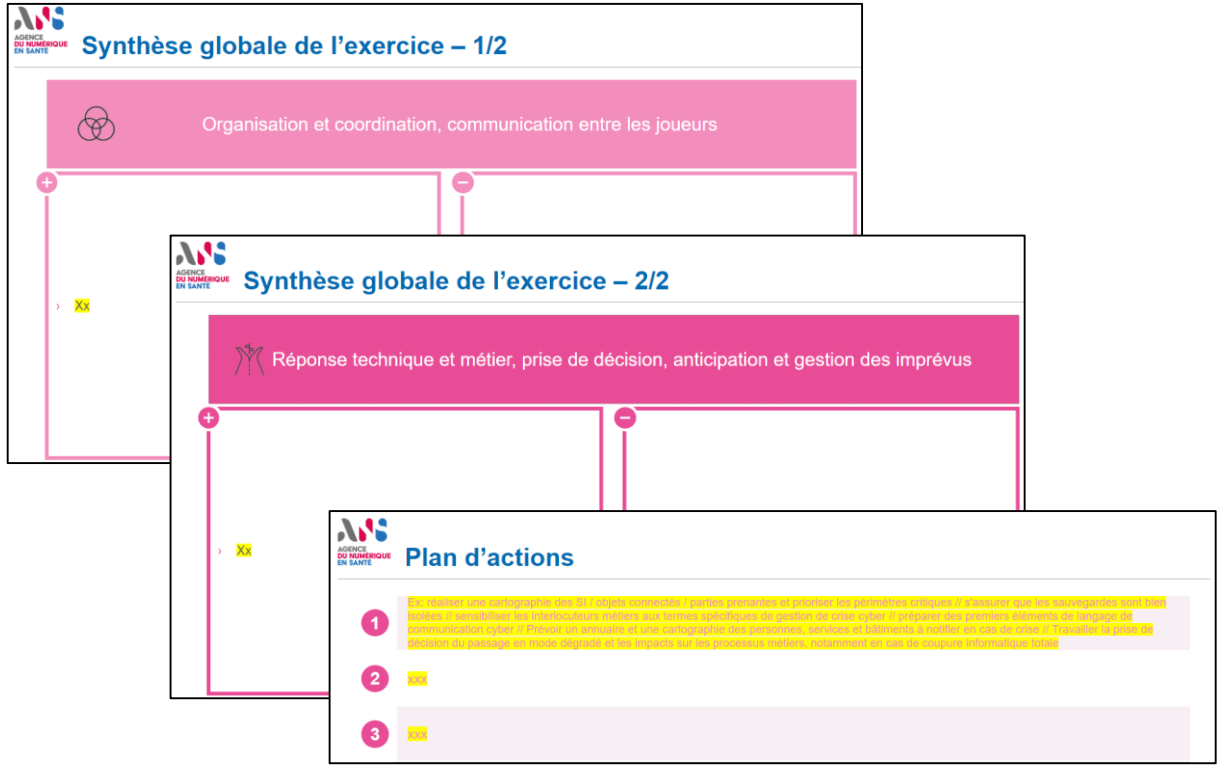


Le Kit ANS Débutant

Après l'exercice

2 Il organise une réunion de restitution d'une heure avec les participants en formalisant un support de présentation à partir des éléments recueillis

- Restitution après une durée raisonnable (max 3 semaines)
- Restitution aux participants et a minima un représentant de la direction :
  - Rappel de l'organisation
  - Analyse de la mise en place et organisation de la cellule
  - Analyse des décisions
  - Analyse du plan de communication
  - Recommandation d'amélioration



Le Kit ANS Débutant

Après l'exercice

3 Selon le mode de fonctionnement choisi, l'animateur pourra transmettre un retour d'expérience anonymisé à l'ARS/GRADeS

- Reporting en fonction des directives nationales et régionales
- Dans tous les cas :
  - garder une trace (élément de preuve) de la réalisation de l'exercice
  - prévoir suivi dans le temps

Et après ?

Le Kit ANS Débutant

Et après?

- Exemples du Plan d'actions :
  - Réaliser une cartographie des SI / objets connectés / parties prenantes et prioriser les périmètres critiques
  - S'assurer que les sauvegardes sont bien isolées
  - Sensibiliser les interlocuteurs métiers aux termes spécifiques de gestion de crise cyber
  - Préparer des premiers éléments de langage de communication cyber
  - Prévoir un annuaire et une cartographie des personnes, services et bâtiments à notifier en cas de crise
  - Travailler la prise de décision du passage en mode dégradé et les impacts sur les processus métiers, notamment en cas de coupure informatique totale

Créer une instance de suivi du plan d'action
Pour chaque action, définir un responsable et une échéance

Le Kit ANS Débutant

Et après?

- Organiser un exercice de Cyber-crise l'année suivante
  - Utilisation du kit débutant en modifiant le scenario
  - Utilisation du kit intermédiaire
  - Utilisation du guide de l'ANSSI
    https://www.ssi.gouv.fr/guide/organiser-un-exercice-de-gestion-de-crise-cyber/

Que peut faire SESAN pour vous ?

SESAN

Obtenir le kit ANS

Contacter votre GRADeS pour obtenir la version finale du Kit ANS Débutant.

Pour l'Ile-de-France contacter : ssi@sesan.fr

SESAN

Offres d'accompagnement

Missions du Département SSI:

- Renforcement de la cybersécurité des ES et ESMS franciliens
- Animation de la communauté RSSI Santé régionale
- Mutualisation de solutions régionales

Offres Cybercrise à destination des adhérents:

- Accompagnement d'un membre de l'équipe au déploiement des Kits de l'ANS
- Accompagnement via un marché régional par des experts en gestion de crise (animation des kits ANS, assistance à chaud, gestion de crise avec cellules opérationnelles et stratégiques, accompagnement post exercice)

SESAN

Contact

Des questions ?

Contactez : ssi@sesan.fr