RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

Agence Régionale de Santé Île-de-France

Cybersécurité

Les enjeux en IDF

Enjeux et vision d’ensemble des actions cyber

Contexte cyber 2022-2023

- Une **augmentation globale du niveau de menace** cyber

- **3 cyberattaques en IDF en 2022** :
  - 21 août : CHSF Corbeil Essonne
  - 9 octobre : Maternité des Bluets
  - 4 décembre : CH de Versailles

- **Nouvelles attaques en 2023 :**
  - Hors IDF : CHU de Brest
  - En Ile de France : 1 ESMS, 2 Sites web indisponibles, 1 tentative en avril sur messagerie avec plusieurs comptes corrompus mais sans conséquences

- Ces cyberattaques surviennent **dans un contexte de tensions hospitalières** et font peser un **risque sur les prises en charge**

- **Des incidents cyber**, de nature et de sévérité variées, très régulièrement signalés à l'ARS et au CERT-Santé

- **JO 2024, coupe du monde de rugby** : risque élevé de cyberattaque pour déstabiliser, désorganiser, décrédibiliser

Des impacts majeurs en cas de cyberattaque (1/2)

Les systèmes d'information sont indisponibles partiellement ou totalement, générant des impacts majeurs sur la prise en charge des patients et sur l'ensemble des activités de l'établissement :

- Passage en mode dégradé (en majorité papier/crayon) avec un **fort impact sur les organisations, voire arrêt total d'activité** (transfert des activités, évacuations à envisager…)

- Impact sur le **prise en charge** des patients : plus d'accès aux rendez-vous pour les consultations, aux dossiers patients, aux prescriptions, aux antécédents ou allergies du patient, aux planning de gestion de bloc opératoire, à la gestion des stocks de la pharmacie, des cuisines, au planning du personnel,…

- Si le **SAMU** rattaché à l'établissement est attaqué lui aussi, il ne pourra plus gérer les appels d'urgence, ni concourir à la gestion de crise (non impacté sur le CHSF et CHV)

- **Impossibilité de communiquer en interne/externe** (indisponibilité de téléphonie, accès internet, messagerie)

Des impacts majeurs en cas de cyberattaque (2/2)

- **Arrêt des échanges de données avec l'extérieur (Trésor Public, CPAM, Etablissement Français du Sang, fournisseurs**…) donc plus de possibilité :
  - De facturer et donc arrêt des recettes
  - De passer des commandes, poches de sang
  - De mandater (**paie** du personnel)...
  - D'accéder aux factures dématérialisées

- **Des conséquences financières majeures** :
  - Dépenses : investissements / prestations non prévues pour gérer la crise (achats de matériels, prestations spécialisées cyber…),
  - Recettes : plus de facturation et de codage PMSI ; perte d'activité
  - Problèmes majorés si attaque en période de clôture financière, car impossible à réaliser

- En cas de fuite de données : déclaration CNIL obligatoire et dépôt de plainte et saisie des matériels impactés par l'attaque pour les besoins de l'enquête, qui pénalise aussi la reprise d'activité

→ **Des impacts majeurs et durables sur l'ensemble de l'activité de l'établissement**

Différentes actions portées au niveau national pour améliorer le niveau de résilience du système de santé

- **Acteurs nationaux spécialisés** (ANSSI, CERT Santé, FSSI du Ministère) + DGOS, DNS

- Des **exigences cyber renforcées** :
  - Instruction 309, politique de sécurité informatique de l'Etat, ministérielle, directive NIS2…;
  - Cybersécurité définie comme objectif prioritaire dans le cadre du Ségur numérique pour 2023 avec des **cibles ambitieuses à mai 2023** :
    - 25% des ES ayant réalisé un exercice cyber et 100% des OSE
    - 100% des OSE ayant réalisé un audit « ADS » dans l'année écoulée
    - 100% des OSE ayant réalisé un audit « cybersécurité » dans l'année écoulée
    - 50% des ES ayant renseigné l'OPSSIES concernant la conformité aux mesures prioritaires et budget et 100% des OSE
    - Avoir mis en place un centre de ressources « cyber » au GRADeS

- Des **programmes de financement**, notamment pour la réalisation d'audits et d'exercices cyber (cf. diapo suivante)
- Un **nouvel observatoire national** (OPSSIES) depuis fin 2022, dédié à la sécurité des systèmes d'information, à remplir obligatoirement par les établissements

- **Task force nationale cyber** depuis début 2023

Des programmes nationaux, déclinés et mis en œuvre régionalement, visant notamment la réalisation d'audits et d'exercices cyber

L'Etat finance via les ARS la réalisation **d'audits cyber** (obligatoires pour les OSE), ainsi que des **exercices de simulation de cyberattaque** dans le cadre du Ségur pour aider les établissements à identifier leurs vulnérabilités et se préparer au mieux à une cyberattaque :

- **Des financements spécifiques accordés aux OSE** dans le cadre de « France Relance » (3 x 8M€ sur 2021, 2022 et 2023 France entière, dont **3 x 1,3M€ en IDF**) pour réaliser des **audits cyber**

- **Des financements pour la réalisation d'exercices cyber** (simulation de cyberattaque) : un appel à projet de l'ARS IDF est en cours. 10M€ alloués en 2023 France entière, dont **1,4M€ en IDF**, pour aider les ES à réaliser des **exercices de crise** (simulation de cyberattaque).

- Dans le cadre du **Ségur numérique**, le programme SUN-ES contient des exigences sur la réalisation d'audits cyber par les ES et alloue des **financements** aux établissements (32M€ sur 2 ans en IDF) qui permettent aux ES de financer différentes actions dont des actions de renforcement de la cyber. A date, **296 ES franciliens dans le programme SUN-ES**, représentant 76% des ES de la région et 89% de l'activité combinée.

Pour améliorer le niveau de sécurisation des SI et prévenir les cyberattaques, des actions régionales de formation et de sensibilisation

- Des **objectifs « cyber » ont été fixés dès 2022 par la DG ARS à tous les directeurs d'établissement** de santé franciliens (renforcement des mesures SI dans leur ES, réalisation d'un exercice cyber)

- L'ARS a significativement **augmenté les fonds alloués au GIP SESAN** au cours des derniers mois pour renforcer les actions cyber pour diverses actions de sensibilisation et d'accompagnement des établissements. Le SESAN et l'ARS organisent régulièrement des **webinaires techniques ou de sensibilisation** et intègrent aux journées de la e-sante une thématique cyber.

- Le SESAN anime conjointement avec l'ARS, un **collège sécurité** du SI, avec des **comités** et un **forum** sécurité du SI.

- Le plan d'actions cyber a vocation à être **enrichi encore en 2023**, notamment pour :
  - Mener un **audit cyber des SI SAMU** (en cours)
  - Inclure des actions à destination du **médico-social et de la ville**
  - Elaborer un plan **ORSAN cyber**
  - Poursuivre et de renforcer l'**accompagnement** fourni par l'ARS et SESAN auprès des ES victimes de cyberattaque, dans la phase aigüe de la crise mais aussi dans la phase de « reconstruction »

Quelques chiffres pour l'IDF

OPSSIES (Observatoire des la Sécurité des SI) au 14/04/2023

- **51 %** des établissements ont des données actualisées dans l'**OPSSIES** (soit 201 établissements sur 394), dont **89%** des OSE, mais seulement 10,4% seulement ont actualisé l'OPSSIES sur la partie exercice de crise (41 sur 394)
- **Un enjeu à poursuivre le remplissage d'OPSSIES pour disposer d'une vision du niveau de préparation des établissements vis-à-vis du risque cyber**

Les OSE (Opérateurs de Services Essentiels)

Suite enquête téléphonique et courriel (déclaratif) :

- 85 % déclarent avoir réalisé/planifié au audit de l'active directory via l'ANSSI entre 2022-2023
- 90 % déclarent avoir réalisé/planifié au audit d'intrusion via l'ANS entre 2022-2023
- 90 % déclarent avoir réalisé/envisagé un exercice cyber entre 2022-2023
- 7 OSE ont réalisé des exercices via le SESAN
- **Seuls 2 OSE et l'AP-HP ont répondu à l'appel à projet d'exercices cyber**

Focus sur l'AAP pour la réalisation d'exercices cyber

Un appel à projet pour financer les exercices de continuité d'activité au sein des ES sur l'année 2023

- **La cible** : tous les ES franciliens (en priorité les OSE, ES à forte activité combinée, et ceux qui font de la MCO).
- **Les pré-requis pour bénéficier du financement** : avoir rempli la grille d'autoévaluation (niveau de maturité 1, 2 ou 3), avoir mis à jour l'OPSSIES dans les 3 mois qui précédent la candidature, avoir transmis un bon de commande et avoir renseigné le formulaire de candidature (*démarches simplifiées*).
- **Les modalités de financement** : **une allocation forfaitaire (4000 euros maximum).**
- **Le calendrier** : lancement de l'AAP le 12/01/23 sur le site de l'agence, **ouvert jusqu'à juin 2023**
- **A date : 15 établissements ont déposé leur candidature** (9 établissements sur le Kit maturité 1, 6 sur le kit maturité 2) → **dynamique à poursuivre et à amplifier**

Focus sur l'offre SESAN / exercices cyber

- 30 exercices à réaliser (29 pour des OSE / AP-HP + 1 ESMS)
- Au total sur 1 année glissante : **7 OSE/19 ont fait un exercice via SESAN** ; 29 ES ont fait un exercice (soit 7,4%)

Organisation de la réponse à une cyberattaque : les travaux en cours au niveau régional

Un « plan de réaction régional » en cas de cyberattaque

Les constats :

- Une mobilisation supra-départementale pour la continuité des prise en charge en soins critique, la réorganisation du SNP
- Un besoin de communiquer pour réorganiser la prise en charge des files actives
- Un besoin de renfort RH, d'expertise, de moyens techniques immédiat (<24h) mais aussi dans la durée (jusqu'à 6 mois)
- Une articulation nécessaire entre l'expertise médicale et l'expertise SI

Travailler la réponse collective à un incident, qu'il soit d'origine malveillante ou non.

ORSAN CYBER : Choix francilien d'une planification dédiée au risque cyber

L'objectif est d'établir, sur la base des connaissances disponibles, un **référentiel de gestion des incidents cyber majeurs (doctrine, manœuvres), de définir et d'acquérir les équipements nécessaires à la réponse, de définir les besoins de formation et l'identification d'une offre idoine, de prescrire les attendus (en matière de résilience et de réaction) pour chaque opérateur santé** en fonction de ses caractéristiques.

<u>Cette planification s'articulera autour de 2 thèmes majeurs :</u>

- Garantir l'offre et la sécurité de soins ;
- Construire les moyens de réponse, définir les moyens nécessaires à la remédiation technique des premiers instants pour stabiliser les modes dégradés mis en place et permettre d'initier la reconstruction.

Des travaux déjà initiés

Groupe de Travail SESAN/Crisalyde/PWC

- Réalisation d'un état des lieux de la documentation existante concernant le risque cyber pour en extraire les bonnes pratiques en cas de cyberattaque.
- Réalisation d'un diagnostic des impacts d'une cyberattaque sur les activités métiers pour les secteurs sanitaire, médico-sociaux et ville.
- Recommandations des mesures/manœuvres à mettre en œuvre.

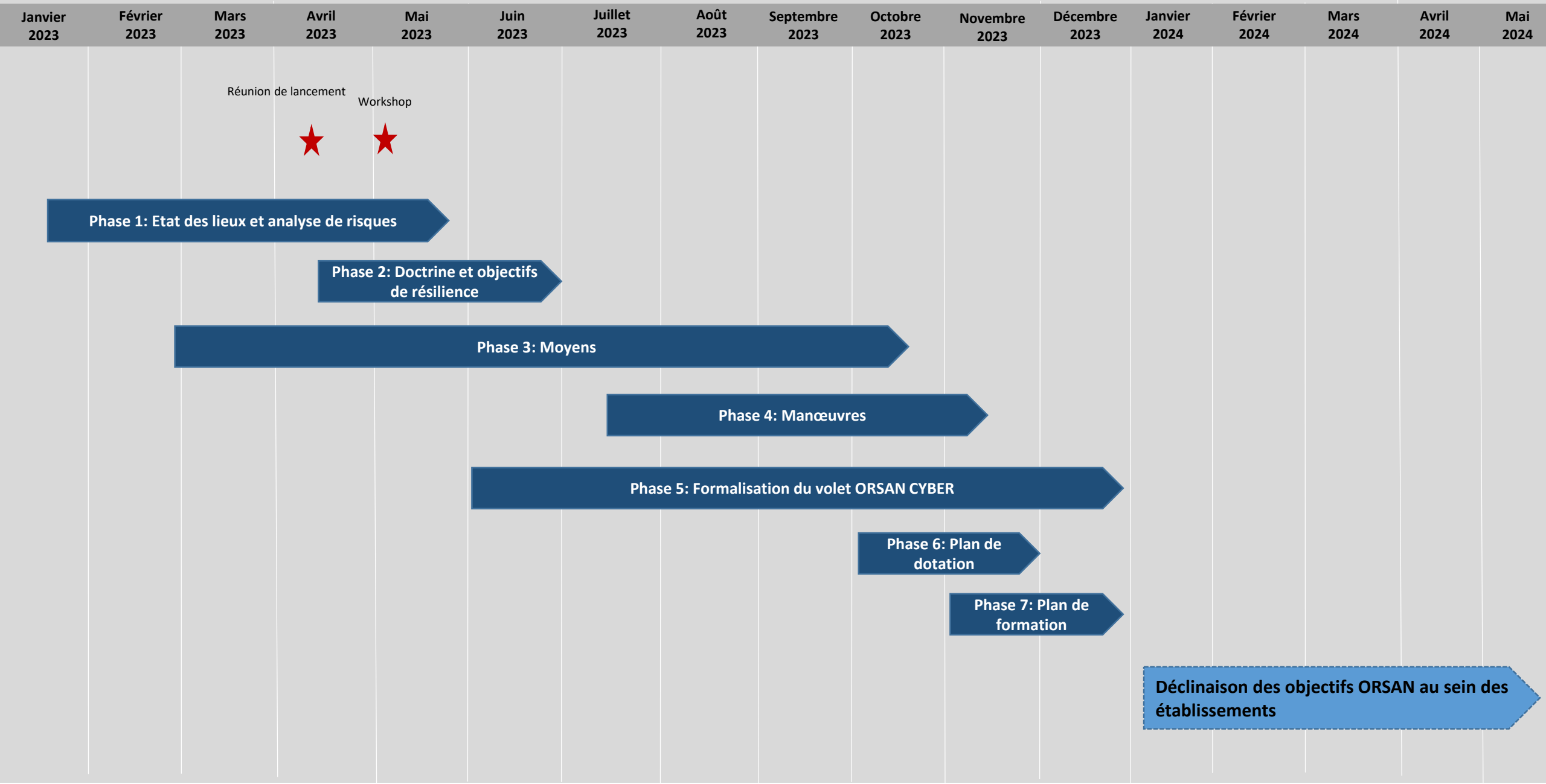
APHP et ses travaux sur la gestion d'une crise CYBER

- Organisation de la réponse à une crise d'origine CYBER
- Réalisation de 4 exercices de gestion de crise CYBER en 2021/2022
- Mise en place d'une force d'intervention rapide au niveau régionale (ex: Assistance aux CHSF, CH Versailles et CHU Brest)
- Elaboration d'un PCA du soin en cas de cyber-attaque par les métiers et la DSN/DSI

Des travaux complémentaires

- Etude des matériels informatiques nécessaires dans le mois suivant la cyberattaque et analyse des moyens de mise à disposition (ex: stocks tournants, centrales d'achats, accords industriels…)
- Etude sur la projection d'équipements biomédicaux des stocks tactiques et stratégiques.

MACRO PLANNING ORSAN CYBER



Mise à disposition de matériels – Quelle réflexion est actuellement menée ?

Définition des besoins « bruts »

Actions envisagées

- Disposer des moyens RH experts
- Disposer de postes de travail
- Disposer de serveurs
- Disposer de moyens d'hébergements
- Disposer de matériels réseau
- Disposer de connexions internet sécurisée de secours
- Disposer de moyens de téléphonie (PABX, postes…)
- …

Définition des capacités et modalités d'emploi

Dimensionnement

- Cinétique de déploiement en cas de crise ?
- Combien ?
- Paramètres techniques à appliquer pour chaque matériel ?
- Quels services associés ?

- *Ex pour le poste de travail :*
  - *cinétique de mise à disposition 10% sous 48h, 40% sous 2 semaines, 50% sous 1 mois*
  - *faut-il un portable ou fixe?*
  - *Quels OS, quels logiciels?*

Définition de l'organisation opérationnelle

Modes de mise à disposition

- Pour chacun des matériels et chacune des cinétique de mise a disposition:
  - Quelle voie d'acquisition?
    - Stocks dormants spécifique
    - Stocks tournants des ES
    - Location
    - Pré-réservation industriels
    - Accord centrale d'achat…
  - Quel opérateur pour la mise en œuvre?
  - Quel financement?