



3 & 4 octobre 2024

Centre Prouvé - 1 Pl. de la République,
54000 Nancy



14^E CNRC

Programme CaRE et illustrations Pays de la Loire et Grand-Est

Stéphane BARCIK – GRADeS Pulsy

Auriane LEMESLE – GRADeS e-santé Pays de la Loire

La genèse du programme CaRE



Des réalisations concrètes et des premiers succès de l'axe 1



Gouvernance et Résilience



CPOM

Intégration d'objectifs cyber dans les CPOM ARS-ES

Certification HAS 2024

Objectif : Intégration de critères numériques et cyber dans le référentiel de certification 2024 et recrutement d'experts visiteurs numériques

- ▶ **La certification v2024** intègre des critères liés au numérique et à la cyber
- ▶ **175 EVN** recrutés et formés
- ▶ **369 établissements visités** à S1 2024

Exercices de crise régionaux

Objectif : Réalisation d'un premier exercice régional (ARS / Préfecture) d'ici S2 2024

- ▶ **Toutes les régions ont réalisé ou planifié leur exercice**

Exercices de crise dans les Etablissements de Santé

Objectif : 80% des ES d'ici S2 2024 réalisent un exercice de crise, démarche qui doit devenir annuelle

- ▶ **Plus de 2220 exercices réalisés ou planifiés soit 78 % des établissements de santé**

Plan de Continuité et de Reprise d'Activité

Objectifs : Mettre en œuvre des Plans de Continuité et de Reprise d'Activité (PCRA) dans les établissements (ES et ESSMS).

- ▶ **Kit PCRA** disponible sur le site de l'ANS

Exercices de crise

93 exercices réalisés ou planifiés (80% des établissements)

Au-delà d'une **très bonne satisfaction globale (84%)**, une véritable **prise de conscience des impacts** d'une crise cyber **sur la continuité des soins** est observée par tous les participants aux exercices de crise cyber



Des réalisations concrètes et des premiers succès de l'axe 2



Ressources et mutualisation



Catalogue des offres cyber

Objectif : Recensement de l'ensemble des offres existantes à destination des ES dans un catalogue dédié disponible sur le site de l'ANS.

- ▶ 467 offres publiques recensées
- ▶ 142 offres d'industriels recensées (catalogue ouvert aux industriels depuis 2024)

Renforcer l'attractivité des ressources en ES

Objectif : Identifier les leviers pour renforcer l'attractivité des ressources en ES

Revalorisation des grilles statutaires des ingénieurs hospitaliers

Financement de la cybersécurité en région (CRRC)

Objectif : Mise en place des centres de ressources cyber (CRRC) qui vont développer une offre de services répondant aux besoins prioritaires des établissements.

Sensibilisation	Prévention	Remédiation
Comité RSSI santé ✓	Retex établissements ✓	Exposition Internet ES ✓
Portail collaboratif ✓	Exercices de crise ES ✓	Stock matériel régional ⚠
Corpus documentaire ✓	Exercices de crise ESMS ✓	Ressources partagées ⚠
Puls'escape ✓	Exercice de crise régional ✓	Entraide ⚠
Campagne de phishing ⚠	Bluefiles régional ✓	
Plateforme sensibilisation ⚠	Accompagnement PCRA ✓	
Nouveaux services pour 2025		
Diagnostic maturité cyber ESMS ⚠	Accompagnement domaines CaRE ⚠	Stock régional de secours ⚠
Formation des DSI / RSSI ⚠	Accompagnement annuaires AD ⚠	Solution VNA/ données ES ⚠
Pulsy Tour Cybersécurité ⚠	Marché négocié exercices de crise ⚠	Réponse à incident ⚠



Des réalisations concrètes et des premiers succès de l'axe 2



Sensibilisation



Campagnes de sensibilisation

Objectif : Réaliser des campagnes de sensibilisation à destination des publics prioritaires, aux niveaux national et régional.

► Lancement de la campagne TousCyberVigilants#2 en T4 2024

Animations

Objectif : Poursuivre l'animation régionale réalisée par les ARS et les GRADeS avec les acteurs SI et SSI dans les territoires.

Formation

Objectif : Former l'ensemble des professionnels de santé et/ou administratifs dans les établissements (ES et ESSMS) aux enjeux cyber.
>> Objectif : 100% des formations initiales réformées en 2027.

► Intégration progressive de la cyber dans la totalité des formations initiales médicales, paramédicales, du travail social et dirigeants.

Présence aux évènements nationaux et régionaux, publications

Objectifs : Promouvoir le programme CaRE au sein de l'écosystème et sensibiliser aux enjeux de la Cyber

- Organisation de Webinaires d'information
- Participation/organisation d'évènements régionaux

- Participation/organisation d'évènements nationaux
- Participation à des évènements internationaux

Formation et sensibilisation

Formations régionales



Formations

- Référénts sécurité des SI & Animation d'un COPIL sécurité des SI
- Séminaire secteur médico-social
- Analyse de risques et homologation
- Détection et réaction en cas de cyberattaque par rançongiciel



Guides



- PROTÉGER VOS DONNÉES SENSIBLES
- APPLIQUER DES MESURES D'HYGIÈNE NUMÉRIQUE
- RÉAGIR EN CAS DE CYBERATTAQUE



Organisation et participation à des événements régionaux

- Comité des RSSI de santé GE
- En avant la E-santé
- Club utilisateur Dxcare
- Club des DSI de santé GE
- Journée ETP
- Pulsy tour Cybersécurité (2025)



Autres ?

- HWL – Healthcare Week Luxembourg
- Santexpo
- Congrès de l'APSSIS

Visuels déclinés en différents formats

16 affiches / cartes postales



Stickers à destination des équipes SI :



En fonds d'écran

Tapis de souris

Stickers et badges métalliques



Téléchargeables librement sur le site du GCS e-santé :

<https://www.esante-paysdelaloire.fr/nos-services/securite-numerique-en-sante-99-128.html>



- Mise à disposition d'une plateforme d'e-learning avec des contenus génériques et d'autres contenus contextualisés au domaine de la santé (vidéo, sondage, saynètes, quizz, ...)
- Cette plateforme permet également de tester la vigilance des utilisateurs via des campagnes de faux-phishing (hameçonnage).



- **2 modes sont proposés :**

- Acquisition d'une licence d'administration par les structures pour opérer les campagnes en autonomie
- Délégation de l'administration de la plateforme au GCS e-santé qui opère les campagnes pour le compte des structures

De : GCS esanté PDL <gcs.esante.pdl@pdl.fr>
Date: mar 20 mai 2023 à 13:03
Subject: Vous avez reçu une invitation Teams



Escape game de sensibilisation



Défi à relever en 45 minutes, pas une de plus !

Les participants à l'escape doivent se mettre dans la peau de personnages imaginaires : 5 journalistes peu scrupuleux d'un magazine People qui doivent décrocher un scoop sur l'état de santé d'une célébrité pour sauver leur journal de la faillite.

Les bonnes pratiques de base en matière de sécurité numérique ont-elles été bien suivies dans la structure ou seront-elles la clé d'accès aux informations de santé pour les journalistes ?

Une méthode de sensibilisation innovante, ludique qui implique les apprenants ;

Ne nécessite aucune connaissance technique particulière, s'adresse à tous publics ;

Des participants qui doivent se mettre dans la peau "des méchants" et exploiter les mauvaises pratiques ;

Un scénario contextualisé au secteur santé ;

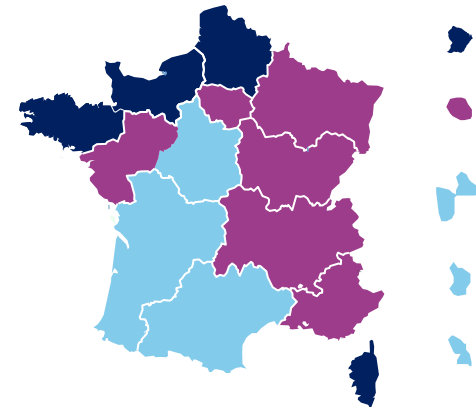
Une durée de jeu de 45 min pour ne pas mobiliser les professionnels plus d'1h (briefing / débriefing inclus) ;

Une formation et un kit de ressources permettant aux structures ligériennes d'être autonomes dans la mise en œuvre.

1652 participants en PDL

227 participants en GE

Escape game basé sur
Sant'escape sécurité numérique
déploqué



Déploiement à l'étude

Formation à la détection et réaction face à une attaque par rançongiciel

Un apport théorique ...



- Panorama de la menace (zoom sur le secteur de la santé)
- Focus sur la menace de type rançongiciel (exemples du secteur)
- Conséquences d'une cyberattaque pour un établissement de santé
- Descriptif des différentes phases de l'attaque
- Cas concrets permettant d'identifier des signaux faibles en amont



Une demi-journée (3h)

Des supports variés :

Quiz



Présentation



Vidéos



... et pratique

- Pour alerter et protéger via la fiche de qualification et d'alerte



À destination des membres
des équipes SI

286 personnes formées

(Satisfaction moyenne : **9,02 / 10**)



Des réalisations concrètes et des premiers succès de l'axe 4



Sécurité opérationnelle



Domaine Annuaires techniques et exposition sur internet

Objectif : Maîtriser les risques d'exposition sur internet et la sécurisation de leurs annuaires.

HospiConnect

Objectif : Simplifier et sécuriser l'accès des professionnels aux services numériques sensibles.

Domaine Stratégie de continuité et de reprise d'activité

Objectif : Reconstituer rapidement les services critiques en cas d'incident et assurer la continuité et reprise d'activité.

Domaine Sécurisation des accès distants

Objectif : Sécuriser l'ensemble des accès distants, couvrant à la fois les fournisseurs et les accès du personnel des établissements.

Webinaires régionaux

17 sessions réalisées

207 participations

Satisfaction globale

9,61 / 10

Base documentaire

Marché PCRA

Marché public de prestation permettant d'accompagner les GHT dans leur Plan de Continuité et de Reprise d'activités

EWS

Outil régional de scan d'exposition internet permettant de Sécuriser l'ensemble des accès distants





3 & 4 octobre 2024

Centre Prouvé - 1 Pl. de la République,
54000 Nancy



14^E CNRC

Place au quiz cyber !

Sécuriser ses mots de passe

- Le penseur de Login -



Qu'est-ce qu'un bon mot de passe ?

- A. Un mot de passe complexe que je peux retenir facilement (ex : Louis2004#)
- B. Un mot de passe complexe qui n'est pas basé sur des mots existants et différent pour chaque compte
- C. Un mot de passe complexe et unique pour tous mes comptes
- D. Le même mot de passe que j'utilise depuis 20 ans, et je n'ai jamais eu de problèmes

Sécuriser ses mots de passe

- Le penseur de Login -



Qu'est-ce qu'un bon mot de passe ?

- A. Un mot de passe complexe que je peux retenir facilement (ex : Louis2004#)
- B. Un mot de passe complexe qui n'est pas basé sur des mots existants et différent pour chaque compte
- C. Un mot de passe complexe et unique pour tous mes comptes
- D. Le même mot de passe que j'utilise depuis 20 ans, et je n'ai jamais eu de problèmes

Sécuriser ses mots de passe

- Le penseur de Login -

SAPERLÉPOPETTE...
C'EST QUOI MON
MOT DE PASSE, DÉJÀ ?



LES BONS RÉFLEXES

- Utiliser un mot de passe suffisamment long, complexe et impossible à deviner
- Changer ses mots de passe régulièrement ou au moindre soupçon de compromission
- Utiliser un coffre-fort de mot de passe
- Utiliser un mot de passe différent pour chaque service
- Activer l'authentification multi-facteur lorsque c'est possible
- Changer les mots de passe par défaut



NE PAS FAIRE

- Enregistrer ses mots de passe dans les navigateurs Internet (Firefox, Chrome...)
- Renseigner ses mots de passe sur un ordinateur partagé
- Écrire ses mots de passe sur papier
- Communiquer son mot de passe à un tiers

Phishing (hameçonnage)

Qu'est-ce que le Phishing?



- A. Un nouveau type de virus informatique
- B. Une tentative d'obtenir des informations confidentielles en se faisant passer pour une personne de confiance
- C. Une technique de pêche sportive

Phishing (hameçonnage)

Qu'est-ce que le Phishing?



- A. Un nouveau type de virus informatique
- B. Une tentative d'obtenir des informations confidentielles en se faisant passer pour une personne de confiance
- C. Une technique de pêche sportive

Le phishing, ou hameçonnage en français, est une technique frauduleuse utilisée par les cybercriminels pour voler vos informations personnelles (mots de passe, numéros de carte de crédit, etc.). Ils se font passer pour une entreprise de confiance (banque, service des impôts, etc.) en vous envoyant un e-mail ou un sms. L'objectif est de vous inciter à cliquer sur un lien ou à ouvrir une pièce jointe qui vous mènera vers un faux site où vous serez invité à saisir vos informations.

Se protéger contre le phishing



LES BONS RÉFLEXES

- S'assurer de l'authenticité des émetteurs et des destinataires en cas de mails suspects
- Examiner les liens contenus dans le mail en les survolant avec la souris (sans cliquer)
- Vérifier l'orthographe et la grammaire du mail
- Alerter le service informatique en cas de mails frauduleux
- Supprimer les mails douteux et vider la corbeille



NE PAS FAIRE

- Ouvrir des pièces jointes ou des liens suspects contenus dans les mails
- Communiquer des informations confidentielles par mail
- Naviguer sur des sites non sûrs et illicites

En situation de mobilité

En déplacement, je me connecte à internet en utilisant :

- A. Le Wifi de la gare ou du TGV
- B. Le Wifi de l'hôtel
- C. Le Wifi du Centre Prouvé
- D. Le partage de connexion de mon téléphone



En déplacement, je me connecte à internet en utilisant :

- A. Le Wifi de la gare ou du TGV
- B. Le Wifi de l'hôtel
- C. Le Wifi du centre Prouvé
- D. Le partage de connexion de mon téléphone

Les réseaux Wi-Fi publics (cafés, aéroports, TGV, hôtels, etc...) sont considérés peu fiables. N'importe qui peut potentiellement intercepter les données qui transitent sur ce réseau, y compris vos mots de passe, numéros de carte bancaire, données personnelles et de santé.

Le partage de connexion à partir du téléphone professionnel doit être utilisé lors des déplacements professionnels.

Se protéger en situation de mobilité

✓ LES BONS RÉFLEXES

- Respecter les mêmes consignes de sécurité qu'au bureau
- Sauvegarder ses documents avant et après déplacement
- Utiliser un VPN pour accéder aux ressources de l'entreprise
- Attacher son ordinateur avec un antivol adapté
- En cas de perte ou de vol d'un équipement mis à sa disposition le signaler le plus rapidement possible au service informatique
- Utiliser un filtre de confidentialité sur l'écran
- Saisir son mot de passe à l'abri des regards
- Rester vigilant lors des conversations, notamment dans les lieux publics (transports en commun, restaurants...)

✗ NE PAS FAIRE

- Se connecter à des réseaux Wifi publics ou inconnus
- Laisser sa session ouverte sans surveillance
- Connecter des médias amovibles non maîtrisés
- Partager ses équipements avec des personnes extérieures à l'entreprise



Partager les données de santé



Je partage les données de santé en utilisant :

- A. Mon vieux fax fonctionne toujours
- B. Gmail, c'est pratique, rapide et déjà sur mon téléphone
- C. Les outils nationaux et régionaux disponibles
- D. WhatsApp, c'est pratique rapide et déjà sur mon téléphone

Partager les données de santé



Je partage les données de santé en utilisant :

- A. Mon vieux fax fonctionne toujours
- B. Gmail, c'est pratique, rapide et déjà sur mon téléphone
- C. Les outils nationaux et régionaux disponibles
- D. WhatsApp, c'est pratique rapide et déjà sur mon téléphone

Partage de données – Les outils



Parceo
e-Parcours

Des solutions de E-parcours existent dans chaque région. Rapprochez-vous des acteurs concernés (Grades? ARS?)



Solution nationale de messagerie sécurisée de santé et messagerie citoyenne



BlueFiles

Editeur Français, certifié Hébergeur de données de santé (HDS). Initiative locale selon région. Possibilité d'utiliser un compte gratuit