Collectif SI
MÉDICO-SOCIAL
Provence-Alpes-Côte d'Azur

Les midis numériques

La cybersécurité des acteurs du médico-social

Juin 2022

Les midis numériques

Date	07/06/2022 (date de dernière modification)
Version	20220614-0.0 (YYYYMM-VV ou VV est le numéro de la dernière révision du document)
Classification	C0 - Public (voir notes ci-dessous pour les différents niveaux de classification)
Diffusion	partenaires concernés et participants

Cycle de vie du document

Date	Révision	Rédacteur	Note
07/06/2022	0.0	**Philippe PASSIS**	Création du document

Classification

C0 - Public : les documents associés à un niveau de confidentialité C0 peuvent être diffusés librement, il peuvent être mis à disposition selon les termes de la Licence Creative Commons Attribution - Pas d'Utilisation Commerciale - Partage dans les Mêmes Conditions 4.0 International. CC BY-NC-SA https://creativecommons.org/licenses/by-nc-sa/4.0/

C1 - Interne : les documents associés à un niveau de confidentialité C1 ne peuvent être diffusés en dehors du collectif SI MS PACA.

C2 - Restreint : cela veut dire que la donnée sensible qu'il renferme est vouée à une diffusion restreinte. Ces informations ne peuvent pas être communiquées à d'autres personnes que celles disposant d'une autorisation. Les destinataires peuvent tout aussi bien être des personnes internes ou externes au Collectif SI MS PACA. Un encart est présent dans le document pour préciser la liste des destinataires.

C3 - Confidentiel : le libellé C3 est le plus haut degré de confidentialité attribué à un document. La donnée confidentielle qu'il renferme est classifiée secrète. On marque C3 un document dont la perte ou le vol risque de nuire aux intérêts stratégiques, à la sécurité ou à l'existence même du collectif. Il n'y a que le personnel dûment habilité qui puisse attribuer ce degré de confidentialité à un document. Encore une fois, ces informations ne peuvent être consultées que par les personnes disposant d'une autorisation. Un encart est également présent pour préciser la liste des destinataires.

Avant de commencer

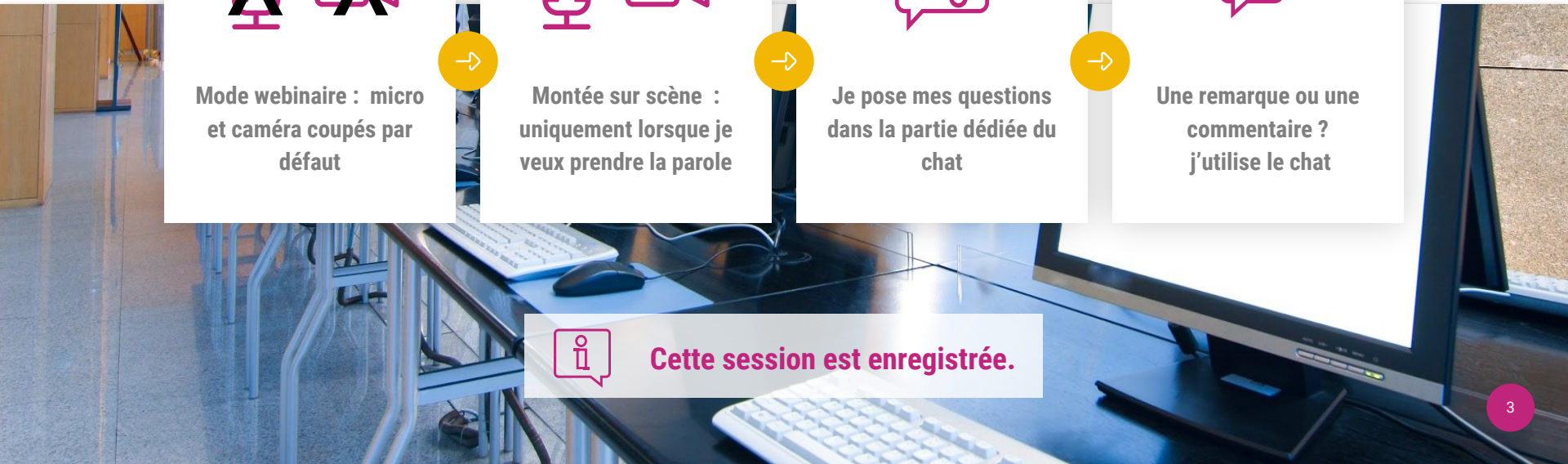
Quelques bonnes pratiques pour notre réunion :

Mode webinaire : micro et caméra coupés par défaut

Montée sur scène : uniquement lorsque je veux prendre la parole

Je pose mes questions dans la partie dédiée du chat

Une remarque ou une commentaire ? j'utilise le chat



Cette session est enregistrée.

Vos **interlocuteurs** et **intervenants**

Patrice THIRIOT
iesS / CAPSI

Philippe PASSIS
iesS / expert ANAP

Marie-Aude MATHIEU
AideraVar / Experte ANAP

Nadège VANNESTE
IRSAM / expert ANAP

Mehdi GASMI
ORPEA / expert ANAP

Les **midis numériques** du collectif SI

Tous les mardis de 12h00 à 12h20

DUI
Je prépare ma réponse à l'appel à projet ESMS Numérique
26/04/2022

DUI
Gestion de l'accompagnement aux changements, sens, appréhension des outils techniques
03/05/2022

RGPD
Faut il nommer un DPO ?
10/05/2022

RGPD
Registre de traitement des données et information usager
17/05/2022

RGPD
Analyse d'impact relative à la protection des données
24/05/2022

Gouvernance SI
Prestataires de services : qui fait quoi et comment gérer mes contrats
31/05/2022

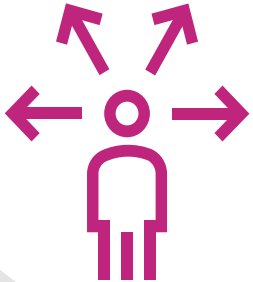
iesS
Le GRADeS et son offre de services
07/06/2022

PEP'S
L'offre de services accès Internet et services de communication
14/06/2022

Cybersécurité
La cybersécurité des acteurs du médico-social
21/06/2022

Télémédecine
28/06/2022

De quoi allons-nous parler ?



1. La cybersécurité dans le secteur du médico-social
2. Les outils et services mis à votre disposition par le GRADeS PACA
3. Focus sur quelques outils CAPSI utilisables
4. Question / Réponses et Conclusion

1. Cybersécurité des ESMS : synthèse des précédentes thématiques

2020-2022 :
Un accroissement des incidents de sécurité dans les secteurs de la santé et du médico-social

MINISTÈRE DES SOLIDARITÉS ET DE LA SANTÉ
Liberté Égalité Fraternité

HFDS
HAUT FONCTIONNAIRE DE DÉFENSE ET DE SÉCURITÉ

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

4 OBSERVATOIRE DES SIGNALEMENTS

4.1 Chiffres clés pour la période 2020-2021

733* / 369*
incidents déclarés sur le portail des signalements

582* / 290*
structures ont déclaré au moins un incident

189* / 90*
Demandes d'accompagnement par le CERT Santé

80* / 32*
interventions techniques d'appui (conseils techniques personnalisés, investigation numérique, remédiation, etc…)1

●● Evènements marquants de la période ●●

Campagnes d'attaque liée à des rançongiciels (Ryuk) via des accès VPN compromis
4 établissements de santé (Clinique de l'Anjou, Dax, Villefranche sur Saône, Oloron) , un acteur important du secteur médico-social (Coallia) et un prestataire d'application hébergée pour services de soins à domicile en ligne fortement impactés.

Attaques liées à des rançongiciels
Un établissement de santé (Saint Gaudens) et un prestataire d'applications pour Ehpad fortement impactés

Attaques liés à des rançongiciels
Un établissement de santé (CH Arles – Groupe Vice Society) et un prestataire d'application pour ESMS fortement impactés (Solware – rançongiciel conti)

Panne de l'hébergeur MIPIH
Plusieurs centaines de structures ont perdu l'accès à leurs applications métier pendant 3 jours.

Fuite d'identifiants concernant un fournisseur de solution VPN
Plusieurs dizaines de structures victimes de connexions illégitimes via les comptes par défaut de la solution dont l'éditeur a les accès. Aucune compromission n'a été constatée suite à une intervention rapide du fournisseur.

Un prestataire est victime d'une fuite de données
500 000 patients de laboratoires de biologie sont impactés

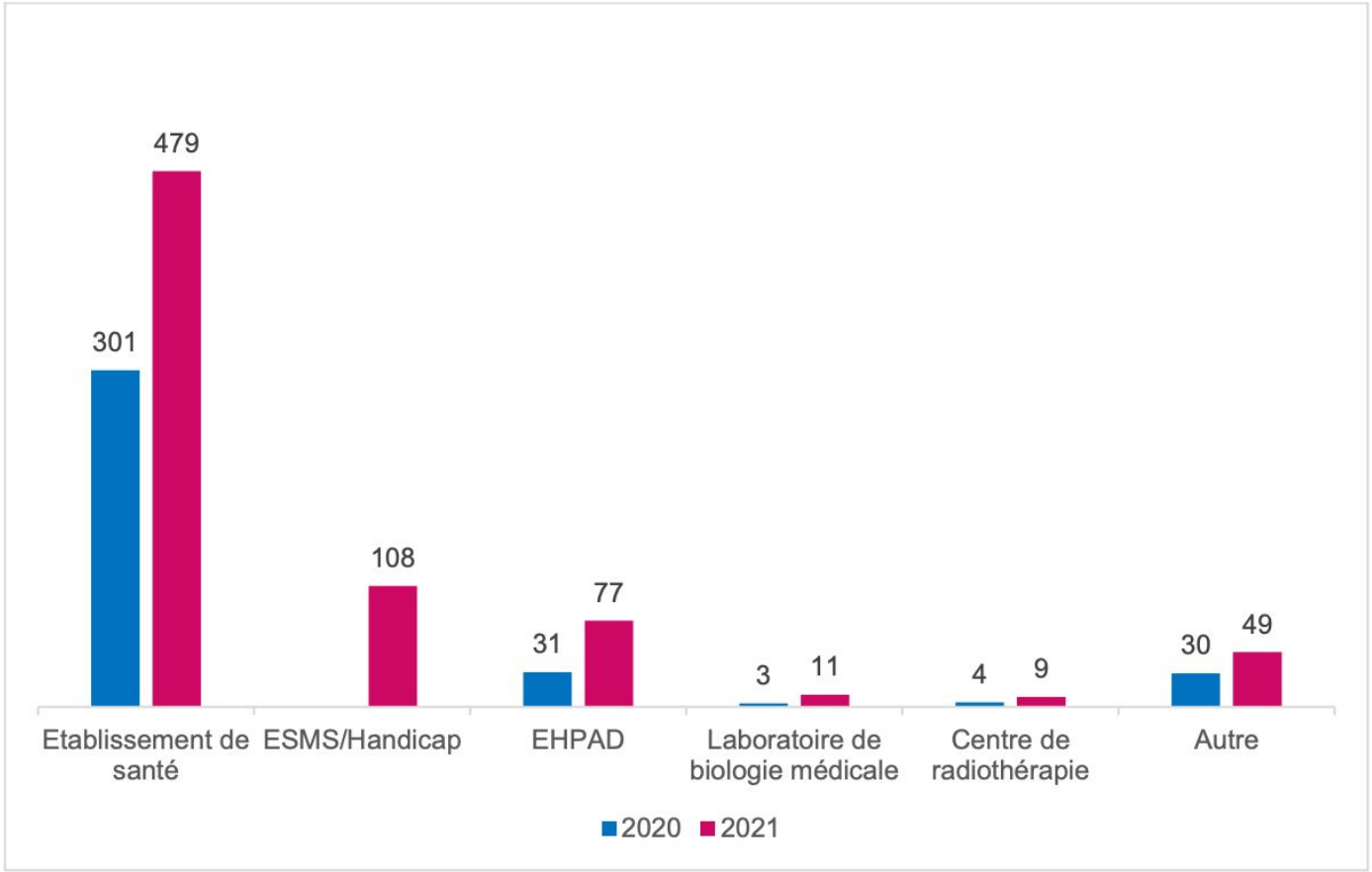
Incendie du datacenter OVH de Strasbourg
Des dizaines de ES – HAD ont perdu l'accès à leur application métier pendant plusieurs jours.

Un laboratoire (CERBA) expose par erreur sur Internet 40Go de données à caractère personnel

L'APHP est victime d'une exfiltration de données suite à l'exploitation d'une faille de sa solution de partage de fichiers sécurisé
Des données de santé à caractère personnel liées au SI DEP et concernant 1,4 million de personnes ont été volées.

Tentative d'escroquerie fausse facture Office
Plusieurs dizaines d'établissements ont reçu par voie postale une fausse facture Office demandant le règlement d'une somme importante. L'hébergeur du site web référencé sur cette fausse facture a désactivé celui-ci à la demande du CERT Santé.

●● Répartition des signalements selon le type de structure ●●



Quelques motivations et modes opératoires des attaquants

Profils :

- Malveillances extérieures
- Malveillances internes

Outils :

- Rancongiciel
- Phishing
- déni de services

Modes :

- exploitation de vulnérabilités sur vos outils ou équipements
- “Force brute” : tentative de casse des mots de passe

Finalités :

- extorsion de rançons
- Exfiltration des données
- Revente de données

2. Les outils et services de sécurité numérique mis à votre disposition par le GRADeS PACA

CAPSI : périmètres de services aux communautés

Communautés PACA

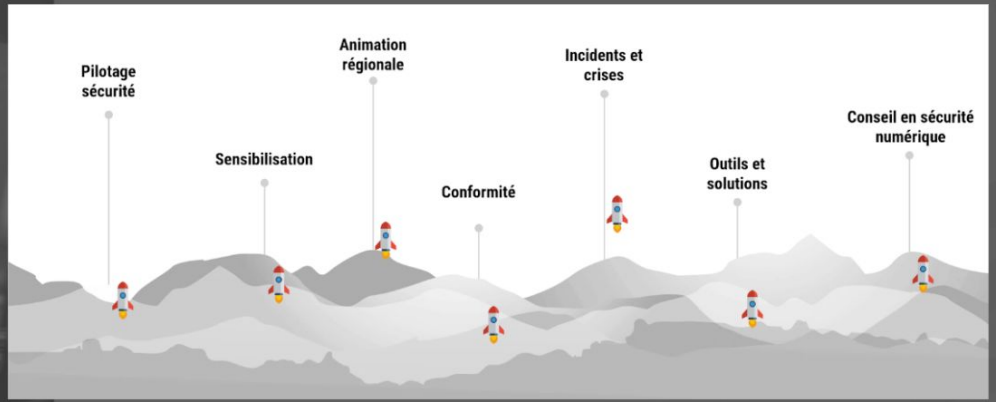
- Pilotage et gouvernance
- Animation régionale
- Incidents et crises
- Outils et solutions
- Conseils de proximité
- Conformité
- Sensibilisation

CAPSI : Focus sur quelques outils et services

- Les kits d'**exercices de gestion de crise** pour permettre aux établissements d'organiser des exercices de gestion de crises numériques au même titre que les exercices d'incendie ou d'évacuation des locaux ;
- La **plateforme régionale de sensibilisation à la sécurité numérique** accessible en ligne par tous les établissements et leurs collaborateurs ;
- Les **sessions ludiques CRACKN'HACK** pour sensibiliser à la sécurité numérique ;
- Les a**ffiches et supports** destinés à porter les discours sur la sécurité numérique dans les structures ;
- Le **livret d'hygiène numérique** spécifiquement écrit pour les ESMS en cours de préparation et qui va être envoyé par l'ANS à toutes les directions ESMS avant l'été ;
- (...)

Capsi

Domaines d'intervention



Gardons le contact :

Suivez-nous !

Nous contacter : Innovation e-Santé Sud

capsi@ies-sud.fr

https://capsi.tech

Page LinkedIn : https://www.linkedin.com/showcase/capsi-paca

Cybersécurité ESMS

Prenons le temps d’échanger...

Pour aller **plus loin...**

Préparer une réponse ESMS Numérique ou SONS ?

Le formulaire de contact du Collectif :
https://cutt.ly/ESMSNum-PACA-2022

Le mail de contact de l'ARS PACA :
ARS-PACA-ESMSNUMERIQUE@ars.sante.fr

Le mail de contact du GRADeS iesS :
esms-numerique@ies-sud.fr

YouTube https://www.youtube.com/channel/UC4J_cUKXF-7fQIfMxt2r0TQ

https://www.linkedin.com/showcase/collectif-si-médico-social-provence-alpes-côte-d'azur/

Save the Date matinée ESMS du GRADeS

ieSS
Innovation e-Santé Sud

LE PARTENAIRE NUMÉRIQUE DES ACTEURS DE SANTÉ

PASQUAL
PACA CORSE Sécurité Qualité
ieSS

GRIVES
Groupe Régional d'IdentitoVigilance En Santé

Matinée ESMS en **présentiel** avec 4 ateliers répétés tout au long de la matinée :

- identitovigilance
- nouveaux référentiel d'évaluation
- serious game Cybersécurité
- virage Numérique

Je m'inscris

- ❏ 15 Juin à Gap
- ❏ 27 Juin à Brignoles
- ❏ 29 juin à Marseille

CAPSI
Cellule d'Appui à la Protection des Systèmes d'Information

Rejoindre le collectif

Un réseau de compétences

Un outil pour accompagner la transformation numérique du secteur

Un espace de mutualisation et de partage

Une feuille de route faite pour les établissements et services, avec les acteurs impliqués dans le collectif

Rester informé de l'actualité du collectif SI MS PACA ?
Inscrivez-vous ici : **https://cutt.ly/collectifSIMS-PACA**

Collectif SI
MÉDICO-SOCIAL
Provence-Alpes-Côte d'Azur

MERCI

A bientôt pour une prochaine présentation