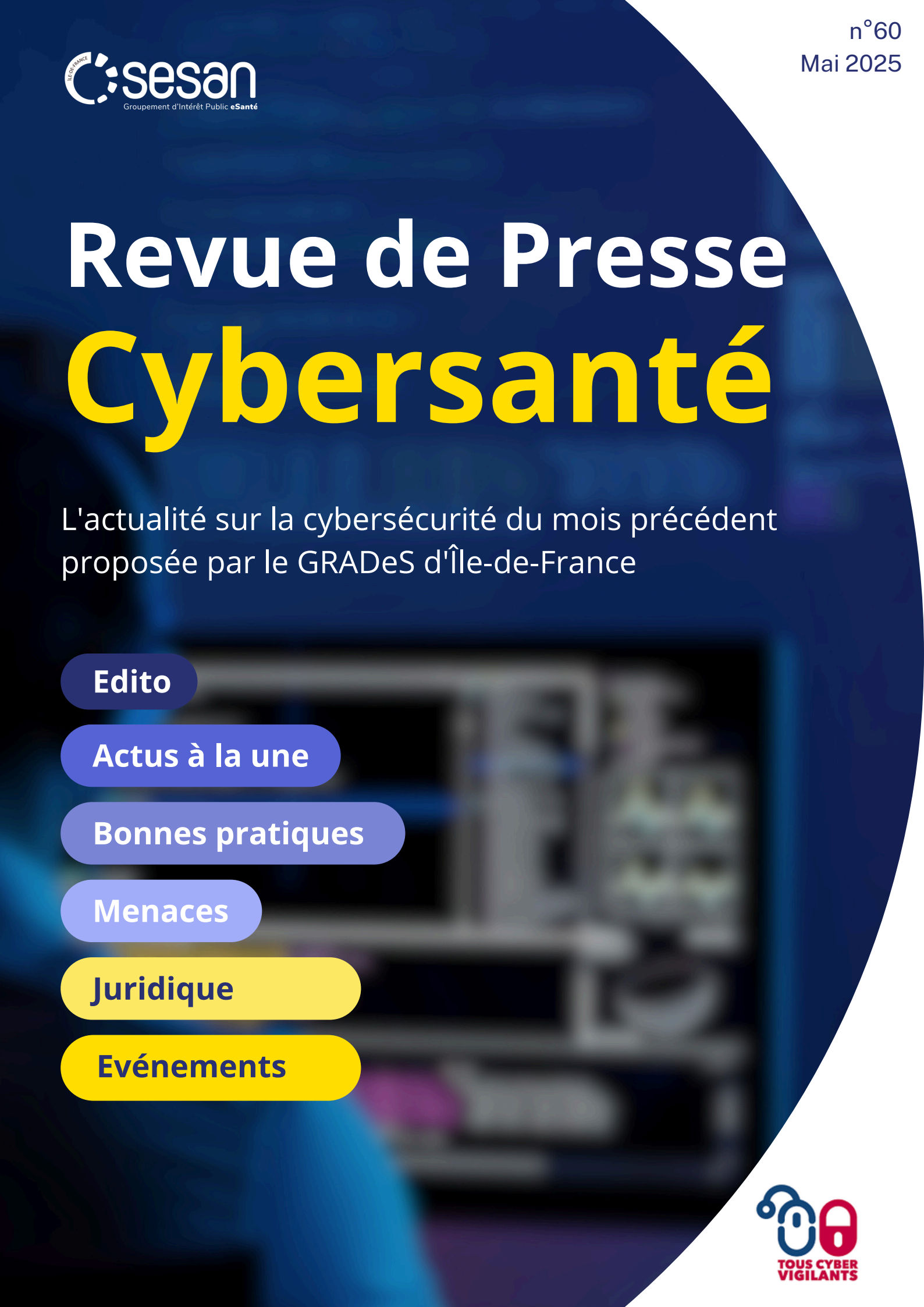
n°60
Mai 2025

sesan
Groupement d'Intérêt Public eSanté

Revue de Presse Cybersanté

L'actualité sur la cybersécurité du mois précédent proposée par le GRADeS d'Île-de-France



Edito
Actus à la une
Bonnes pratiques
Menaces
Juridique
Evénements

TOUS CYBER VIGILANTS

Édito

Chers Adhérents,

Le 10 avril 2025, SESAN a eu l'honneur d'organiser une journée dédiée à la cybersécurité dans le secteur de la santé. Cet événement, qui a réuni plus d'une centaine de participants, a permis de rassembler des acteurs essentiels de notre secteur : des hôpitaux, des structures médico-sociales, ainsi que des structures de coordination. Des témoignages de professionnels ont mis en lumière la complexité des défis auxquels nous faisons face au quotidien. La cybersécurité, constitue un enjeu central pour garantir non seulement la protection des données sensibles, mais aussi la continuité des soins. .

Cette journée a également été l'occasion de rappeler que SESAN joue désormais un rôle de structure aidante dans le cadre du dispositif "MonAideCyber". Un établissement accompagné dans cette démarche a d'ailleurs témoigné de l'impact positif de notre soutien. Grâce à des diagnostics gratuits de cybersécurité, nous offrons aux structures les moins matures sur ces sujets, l'opportunité de débuter leur démarche de sécurisation de manière simple et structurée, avec un plan d'action clair et un suivi assuré par nos équipes. À ce jour, 15 diagnostics sont déjà programmés.
Si vous n'avez pas encore sollicité ce service, n'hésitez pas à nous contacter pour obtenir le vôtre !

L'équipe SSI

Un doute ?

Une question ?

Contactez-nous sur
ssi@sesan.fr

Actus à la une

MONAIDECYBER, LA START-UP D'ÉTAT QUI AIDE LES ORGANISATIONS PEU MATURES À SÉCURISER LEURS SYSTÈMES

Incubée au sein de l'Anssi, la start-up publique MonAideCyber s'adresse aux organisations peu expérimentées dans la sécurisation de leurs systèmes pour dresser un diagnostic et aider à mettre en place des mesures. Elle s'appuie pour l'heure sur une communauté de près de 1500 bénévoles issus d'entreprises ou d'administrations.

Lire l'article

L'USINE DIGITALE, 11/04/2025

PODCAST - UN CERT POUR PROTÉGER NOTRE SANTÉ

A écouter

Une attaque, une faille, un hôpital paralysé... et ce sont des urgences vitales et des soins qui ne peuvent plus être pris en charge.Derrière les écrans, une équipe veille 24h/24 pour protéger les établissements de santé français : le CERT-Santé.

SMART LINK, 17/04/2025

PUBLICATION DE L'OPSSIMS : OBSERVATOIRE PERMANENT DE LA SÉCURITÉ DES SI SPÉCIFIQUE AU SECTEUR MÉDICO-SOCIAL

L'OPSSIMS (Observatoire Permanent de la Sécurité des Systèmes d'Informations des établissements et services du secteur Médico-Social) est l'observatoire de la sécurité des SI, spécifique au secteur médico-social, basé sur un standard commun avec le référentiel du secteur sanitaire, l'OPSSIES.

Lire l'article

ANS, 18/04/2025

VERS UNE MONTÉE EN COMPÉTENCE DES ÉTABLISSEMENTS DE SANTÉ GRÂCE AUX EXERCICES DE CRISE

Lire l'article

Dans le cadre du programme "CaRE", le gouvernement veut que les établissements de santé montent en compétence en matière de gestion de crise cyber. L'Agence du numérique en santé vient de publier de nouveaux kits d'exercices.

L'USINE DIGITALE, 24/04/2025

Bonnes pratiques

AUTHENTIFICATION MULTIFACTEUR : LES RECOMMANDATIONS DE LA CNIL POUR MIEUX PROTÉGER LES DONNÉES

La CNIL souhaite promouvoir des solutions de cybersécurité conformes au RGPD, tant dans leur usage que dès leur conception. Dans ce but, elle publie une recommandation destinée à accompagner les utilisateurs et les fournisseurs de solutions d'authentification multifacteur.

Lire l'article

CNIL, 01/04/2025

GUIDE - L'HOMOLOGATION DE SÉCURITÉ DES SYSTÈMES D'INFORMATION

Lire l'article

A travers le guide d'homologation de sécurité, il semblait important de comprendre et de détailler la démarche permettant aux organisations d'homologuer leurs systèmes d'information.

ANSSI, 01/04/2025

ACTIVE DIRECTORY : 4 OUTILS GRATUITS ET EFFICACES POUR AUDITER LES MOTS DE PASSE

En environnement Active Directory, la gestion des mots de passe est essentielle, car des mots de passe faibles ou compromis peuvent entraîner des compromissions de comptes. Les comptes concernés, difficilement identifiable sans un audit, ouvrent la porte à différentes attaques, dont celles par dictionnaire (brute force, credential stuffing).

Lire l'article

IT-CONNECT, 03/04/2025

Bonnes pratiques

CYBERSÉCURITÉ : LES CINQ GESTES QUI SAUVENT

Lors d’une cyberattaque, les salariés sont souvent considérés comme les maillons faibles de la sécurité informatique. Ils peuvent au contraire être une force s’ils sont formés aux bons comportements.

Lire l'article

LE FIGARO, 01/05/2025

Menaces

PLUS DE LA MOITIÉ DES CYBERATTAQUES « COMMENCENT DANS VOTRE BOÎTE DE RÉCEPTION

Lire l'article

Les cybercriminels prennent d'assaut votre boite mail. près de 7 cyberattaques sur 10 débutent par l'envoi d'un mail malveillant. Bien souvent, ce mail comporte un PDF taillé pour piéger les internautes.

01NET, 04/04/2025

DES MALWARES SQUATTENT LES NOMS DE PAQUETS HALLUCINÉS PAR LES MODÈLES DE LANGAGE

Les IA génératives spécialisées dans le code peuvent parfois halluciner, allant jusqu'à créer des noms de paquets. Des chercheurs montrent que les hallucinations des grands modèles de langage ont tendance à générer les mêmes faux noms de paquets. Une occasion en or pour des acteurs malintentionnés qui pourraient squatter ces noms et créer des paquets infestés.

Lire l'article

NEXT, 14/04/2025

LE VIRUS RESOLVERRAT PREND D'ASSAUT LE SECTEUR DE LA SANTÉ ET DE LA PHARMACIE

Lire l'article

Un nouveau virus du nom de ResolverRAT se propage dans le monde entier. Le malware piège les entreprises du secteur de la santé et de la pharmacie avec des mails de phishing calibrés. Au terme de l'attaque, il orchestre le vol de toutes les données de l'ordinateur infecté.

01NET, 18/04/2025

Menaces

LA SURFACE D'ATTAQUE AUGMENTE À CAUSE DE LA SÉCURITÉ DES API QUI REPOSENT SUR DES MÉCANISMES D'AUTHENTIFICATION INSUFFISANTS

Lire l'article

L'IA transforme la sécurité des sites Web et des API ; bien qu'elle améliore la détection des menaces, elle crée aussi de nouveaux défis. L'essor des applications et API basées sur l'IA élargit considérablement la surface d'attaque et expose les entreprises à des menaces toujours plus complexes.

IT SOCIAL, 25/04/2025

Juridique

EEDS : JUSQU'À 20 MILLIONS D'EUROS D'AMENDE POUR VIOLATION DES DONNÉES DE SANTÉ

Lire l'article

A quoi servirait un cadre de protection sans son régime de sanctions ? Pour garantir l'effectivité du cadre de l'accès et de l'utilisation des données de santé au sein de l'Union européenne, le Règlement (UE) 2025/327 sur l'Espace Européen des Données de Santé (EEDS) prévoit un dispositif répressif sur le modèle du RGPD.

HAAS AVOCATS, 02/04/2025

DEMANDES D'AUTORISATION EN SANTÉ : BILAN POUR L'ANNÉE 2024 DE L'ACTION DE LA CNIL

En 2024, la CNIL a reçu 619 demandes d'autorisation pour des traitements de données de santé, en hausse de 20 % par rapport à 2023. La qualité des dossiers s'améliore, entraînant une réduction des délais d'instruction. La CNIL poursuit son accompagnement et prévoit de nouveaux outils pour faciliter les démarches.

Lire l'article

CNIL, 07/04/2025

COMPROMISSION DE DONNÉES CHEZ UN SOUS-TRAITANT : QUELS SONT LES RISQUES DES ACCÈS NON SÉCURISÉS ?

Lire l'article

Régulièrement, la CNIL communique sur des violations de données typiques inspirées d'incidents réels qui lui sont notifiés. Cette publication a pour objectif de permettre à tous les professionnels de comprendre et de prévenir les risques d'accès à des données détenues par les sous-traitants.

CNIL, 23/04/2025

Juridique

CYBERSÉCURITÉ : FACE AUX FUITES DE DONNÉES MASSIVES, LA CNIL VA HAUSSER LE TON

Lire l'article

Après une année 2024 marquée par des fuites massives de données, la Commission nationale de l'informatique et des libertés (Cnil) exigera un système de double authentification pour les bases contenant plus de deux millions de personnes, selon son rapport annuel publié mardi 29 avril 2025.

LA CROIX, 29/04/2025

Evénements

Journées

SANTEXPO

Collectif des GRADeS

Date: Du 20 au 22 mai 2025
Lieu: Paris, Porte de Versailles - Hall 1, Stand E12

Au programme :

- Égalité d'accès aux techniques innovantes
- Solidarité envers les populations les plus fragiles
- Accessibilité géographique et financière...
- Acceptabilité par les acteurs (usagers, professionnels, financiers, industriels, ...)

inscrivez vous vite : Inscriptions

JOURNÉE RGPD

CNIL et le Centre de Recherche sur les Relations entre les Risques et le Droit de l'Université catholique de Lille

Date: 14 mai 2025
Lieu: Faculté de droit de l'Université Catholique de Lille

Au programme :
Actualités, retours d'expérience, bonnes pratiques : une Journée RGPD dédiée aux données de santé

inscrivez vous vite : Inscriptions

Evénements

Formation

FORMATION RPCRA

- **Profil :** Responsable PCRA désigné de l'établissement
- **Prérequis :** connaissance globale du fonctionnement de l'établissement
- **Nombre de participants :** 12 participants (maximum 1 participant par structure)

Temps 1 : Webinaire le 21 avril matin

- Rappel du contexte : enjeux de continuité notamment face aux cyberattaques, enjeux du programme CaRE, certification HAS ...
- Enjeux de continuité et reprise d'activité : études de cas, présentation de la «règle de 3», mise en perspective des apports du PCRA
- Cadrage et pilotage du PCRA : qui, quoi, quel périmètre, combien de temps, quelles ressources?
- Travail préparation de la session présentielle

Atelier 2 : Atelier en présentiel le 28 mai après-midi dans nos locaux (Porte de Versailles)

- Tour de table : question/réponse par rapport au webinaire, état actuel des travaux et réflexions pour chaque établissement
- Etude de cas : le formateur mène un entretien «enlive»
- Debriefing et questions/réponse
- Atelier en trinôme : conduite d'entretiens et utilisation des outils
- Debriefing global, questions/réponse

Si votre Responsable PCRA est intéressé(e), nous l'invitons à nous contacter, ssi@sesan.fr

Evénements

Formation

RSSI SANTÉ - DE PAIRS À PAIRS

Dates:

- Jeudi 18 et vendredi 19 septembre
- Jeudi 20 et vendredi 21 novembre

Prérequis :

- Avoir assisté à la formation de 3 jours dispensée par l'APSSIS "Cybersécurité et Santé : Technicité et savoir-faire pour piloter la politique de sécurité"
- Occuper une fonction de RSSI Santé dans un établissement de Santé depuis au moins 3 ans.

Organisation séquentielle de la formation :

- 1 séquence de coaching de 2 jours pour appréhender le PROCESS COM, se comprendre, se challenger et progresser.
- 1 période de 2 mois comprenant des exercices et 2 séances de coaching individuel (1 avec Patrice METAIS, 1 avec Vincent TRELY), ainsi qu'une hotline par mail ou par téléphone avec le coordinateur et le coach.
- 1 séquence de formation de 2 jours, délivrée par des experts, représentant les parties prenantes du RSSI Santé
- 1 session de virtual learning sur le PCM intégrée

Pour candidater à cette formation : envoyer les éléments justifiant les prérequis à ssi@sesan.fr. Toutes les candidatures recevront une réponse avant le 31 mai.

L'équipe "formation PtoP" - SESAN/APSSIS


ILE-DE-FRANCE
sesan
Groupement d'Intérêt Public eSanté