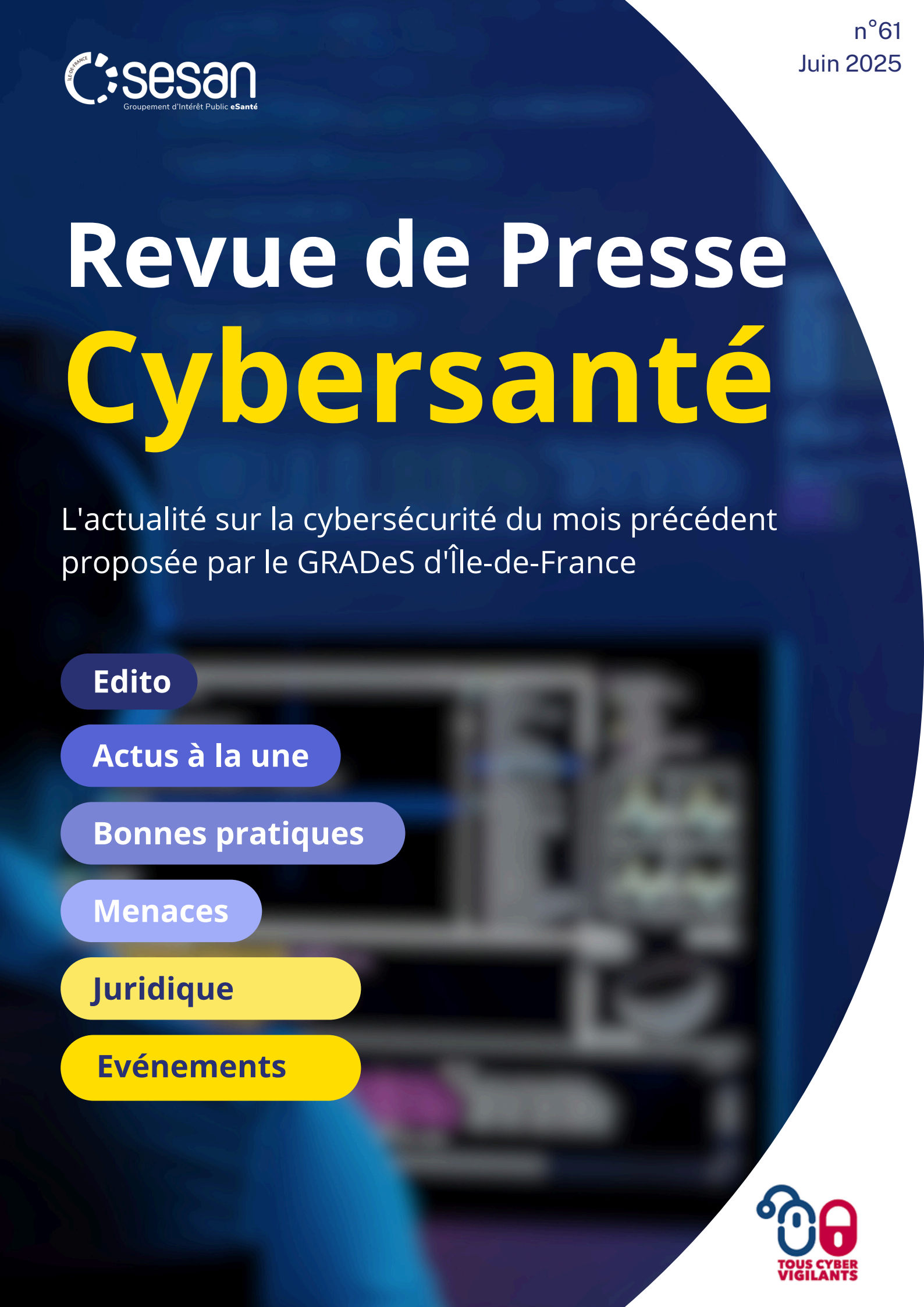
n°61
Juin 2025

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,

Lors du comité de pilotage (COPIL) qui s'est tenu le 23 mai 2025, nous avons présenté les quatre ateliers techniques qui ont été retenus pour accompagner les établissements sur des thématiques clés de la sécurité et de la gestion des systèmes d'information.

Ces ateliers, seront proposés entre octobre 2025 et juin 2026, en présentiel, sous la forme de sessions d'une demi-journée. Le nombre de participants sera limité à 10 personnes par atelier afin de favoriser les échanges et l'apprentissage pratique.

Voici les ateliers sélectionnés :

Atelier "Active Directory" : Cet atelier abordera les bonnes pratiques de sécurisation d'un environnement Active Directory, avec un focus sur les droits, les comptes sensibles, les GPO, et les techniques pour limiter les mouvements latéraux en cas de compromission.

Atelier "Sauvegardes" : Il s'agira ici de revoir les fondamentaux d'une stratégie de sauvegarde robuste : typologies de sauvegarde, protection contre le chiffrement malveillant, tests de restauration, et bonnes pratiques de conservation des sauvegardes hors ligne.

Atelier "Bons réflexes en cas d'incident de sécurité" : Cet atelier visera à outiller les participants face à une situation de crise. Il portera sur la détection, les premières mesures à adopter, la coordination avec les équipes internes/externes, et la documentation de l'incident.

Atelier "Durcissement des configurations" : Un tour d'horizon des mesures de durcissement à appliquer aux composants clés du système d'information (postes de travail, serveurs, etc.).

Par ailleurs, deux établissements se sont portés volontaires pour accueillir un atelier technique centré sur leur infrastructure. Dans un esprit de collaboration, ils ont accepté que d'autres établissements puissent assister à ces sessions organisées dans leurs locaux.

La publication officielle de ces ateliers ainsi que les modalités d'inscription seront mises en ligne prochainement sur notre plateforme Jamespot.

L'équipe SSI

Un doute ?

Une question ?

Contactez-nous sur
ssi@sesan.fr

Actus à la une

L'ANS PUBLIE L'OBSERVATOIRE DE CYBERSÉCURITÉ DU SECTEUR MÉDICO-SOCIAL

PARIS (TICsanté) - L'Agence du numérique en santé (ANS) a publié fin avril l'Observatoire permanent de la sécurité des systèmes d'information des établissements et services du secteur médico-social (Opssims).

L'objectif de cet outil est de "fournir une première évaluation du niveau de risque et de maturité 'cyber' au sein de la structure, afin d'identifier des axes d'amélioration".

TIC SANTÉ, 05/05/2025

Lire l'article

CYBERSÉCURITÉ : L'EUROPE SE DOTE DE SA PROPRE BASE DE DONNÉES SUR LES VULNÉRABILITÉS

Lire l'article

L'Agence européenne pour la cybersécurité vient de mettre en ligne la première base de données européenne qui centralise les vulnérabilités informatiques, l'EUVD. Prévue par la directive NIS 2, ce nouvel outil vise à mieux structurer la gestion des risques cyber en agrégeant des données fiables sur les failles affectant les produits et services numériques utilisés en Europe.

L'USINE DIGITALE, 13/05/2025

FORUM DE LA CYBERSÉCURITÉ INCYBER : COMMENT SE PROTÉGER FACE À L'EXPLOSION DES MENACES ?

Dans un contexte de menaces grandissantes, le Forum InCyber dédié à la cybersécurité s'est déroulé à Lille. Capital, partenaire de l'événement, a animé une série de tables rondes en compagnie des «chevaliers blancs» du numérique.

Santé, défense, industrie... Visionnez les tables rondes animées par Capital au Forum InCyber

CAPITAL, 21/05/2025

À visionner

Bonnes pratiques

MFA & CONFORMITÉ CNIL : INTERVIEW CROISÉE ENTRE DROIT ET CYBERSÉCURITÉ

Une interview de Gaëlle TILLOY, Avocate à la Cour, spécialiste des nouvelles technologies et des données personnelles et Marc SCHMITT, Consultant senior cybersécurité chez SASETY.

Lire l'article

GLOBAL SECURITY MAG, 01/05/2025

S'APPUYER SUR UN SOC EXTERNE POUR ÉLEVER SON NIVEAU DE CYBERPROTECTION

Lire l'article

Le sujet de la protection de ses infrastructures IT n'a jamais été aussi important. Avec la multiplication du nombre d'attaques qui affectent les entreprises et structures publiques, ces dernières doivent repenser en profondeur leurs mécanismes de cyberdéfense et se doter de nouvelles approches. Sur ce point, de nombreux paramètres sont à prendre en compte, comme un audit par exemple, mais un sujet est aujourd'hui stratégique : le recours au SOC.

GLOBAL SECURITY MAG, 01/05/2025

RÉINVENTER LA SANTÉ AVEC LES DONNÉES, LE PARI DU CHU DE TOULOUS

L'entrepôt de données de santé du CHU de Toulouse est désormais conforme aux exigences de la Cnil. L'occasion de pleinement utiliser cette plateforme, qui centralise les informations des patients, à des fins de recherche, d'analyses cliniques et de développement d'outils d'IA. Parmi les projets en cours, figure le projet SIMBIOTIC, qui utilise l'IA générative pour créer des profils artificiels de patients afin de prédire les complications postopératoires.

Lire l'article

L'USINE DIGITALE, 16/05/2025

Bonnes pratiques

CYBERSÉCURITÉ : « DANS 99 % DES CAS, ON ARRIVE À ENTRER DANS L'ENTREPRISE »

Lire l'article

Alors que les cyberattaques ne faiblissent pas, de plus en plus d'entreprises soumettent leurs outils de cybersécurité à des tests d'intrusion. Conclusion : les défenses sont rarement imperméables, notamment grâce aux données personnelles publiées sur les réseaux sociaux.

LATRIBUNE, 20/05/2025

L'INDISPENSABLE CADRE DE GOUVERNANCE ET DE GESTION DES RISQUES SPÉCIFIQUE À L'IA

Pour tirer le meilleur parti de l'intelligence artificielle sans être la proie des risques qui lui sont propres, les entreprises doivent mettre en place un cadre de gouvernance, de risque et de conformité (GRC) spécifique à l'IA.

Lire l'article

CIO ONLINE, 21/05/2025

Menaces

DÉTECTION VS RECHERCHE DE COMPROMISSIONS : LA DISCUSSION CONTINUE

La détection de compromissions consiste à identifier automatiquement des activités malveillantes en temps réel via des outils comme les SIEM ou les EDR. La recherche de compromissions (ou threat hunting) est une démarche proactive où les analystes explorent les systèmes pour découvrir des signes subtils d'intrusions passées ou en cours. Tandis que la détection réagit à des alertes, la recherche anticipe les menaces silencieuses.
Reste à se demander : dans un contexte de menaces de plus en plus furtives, la chasse ne devient-elle pas indispensable ?

À écouter

NO LIMIT SECU, 11/05/2025

BULLETIN D'ACTUALITÉ DU CERT-FR

Lire l'article

Ce bulletin d'actualité du CERT-FR revient sur les vulnérabilités significatives de la semaine passée pour souligner leurs criticités. Il ne remplace pas l'analyse de l'ensemble des avis et alertes publiés par le CERT-FR dans le cadre d'une analyse de risques pour prioriser l'application des correctifs. Toutes les vulnérabilités évoquées dans les avis du CERT-FR doivent être prises en compte et faire l'objet d'un plan d'action lorsqu'elles génèrent des risques sur le système d'information.

CERT FR, 19/05/2025

FORTINET - CVE-2025-32756

Un défaut de contrôle de la mémoire dans plusieurs produits Fortinet permet à un attaquant non authentifié, en envoyant des requêtes HTTP spécifiquement forgées, d'exécuter du code arbitraire.

Lire l'article

CYBERVEILLE ESANTE, 28/05/2025

Menaces

UN BUG DE SÉCURITÉ DANS ONEDRIVE OUVRE UN ACCÈS COMPLET AUX FICHIERS

Lire l'article

Une mauvaise implémentation d'OAuth dans la fonction File Picker de OneDrive donne un accès complet à l'ensemble des fichiers d'un ordinateur.

LE MONDE INFORMATIQUE, 30/05/2025

Juridique

TRAVAIL ET DONNÉES PERSONNELLES : LE MOOC DE LA CNIL S'ENRICHIT D'UN NOUVEAU MODULE

L'atelier RGPD, le MOOC de la CNIL, propose désormais un nouveau module dédié aux traitements des données RH. Avec près de vingt heures d'auto-formation, il est accessible à tous ceux qui souhaitent approfondir leurs connaissances sur la protection des données personnelles;

Lire l'article

CNIL, 13/05/2025

ESPACE EUROPÉEN DES DONNÉES DE SANTÉ : ENJEUX ET CONSÉQUENCES DU NOUVEAU RÈGLEMENT.

Lire l'article

Le Règlement relatif à l'espace européen des données de santé (EEDS) officialise une nouvelle approche européenne de la santé numérique. Ce Règlement institue une libre circulation des données de santé électroniques, incluant les données issues des applications de bien-être. Il renforce les droits des patients sur leurs données de santé électroniques et crée des infrastructures européennes pour favoriser l'utilisation secondaire des données à des fins de recherche, d'évaluation des technologies de la santé et d'adoption de politiques de santé.

VILLAGE JUSTICE, 14/05/2025

Evénements

Webinaire

LA CYBERSÉCURITÉ DANS LE MÉDICO-SOCIAL : QUELLES PREMIÈRES ACTIONS METTRE EN PLACE ?

ANS

Date: 03 juin 2025
Lieu: Distanciel

Au programme :

- Rappel des enjeux autour de la cybersécurité pour le médico-social
- Les premières actions à mettre en place
- REX de structures et de régions

inscrivez vous vite : Inscriptions

ACCOMPAGNEMENT CYBER POUR LES ESMS D'ILE-DE-FRANCE

L'ARS Ile-de-France et le GIP SESAN vous invitent à participer à ce webinaire de présentation du guichet d'accompagnement cyber ouvert aux ESMS de la région IDF.

Date: 24 juin 2025
Lieu: Distanciel

inscrivez vous vite : Inscriptions

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