NEWSLETTER SSI SESAN

Bonjour à toutes et tous,

Pour cette première Newsletter de 2023, le département Sécurité des Systèmes d'Information vous souhaite une excellente année. Bien ou pas, les sujets de cybersécurité seront encore d'actualité. Notre nouveau marché dédié à la gestion de cybercrise a été attribué et permettra de mieux vous préparer et de mieux gérer une cyberattaque. Nous aurons l'occasion de vous le présenter prochainement avec les titulaires.

2023, nouvelle année et nouvelle offre de cybersécurité pour SESAN ! Nous vous en dirons plus dans les prochaines semaines.

Un doute ? Une question ? Contactez-nous sur ssi@sesan.fr !

Indicateur mensuel sur l'origine des incidents déclarés *>>Lire l'article*

Des indicateurs sur l'origine des incidents déclarés en novembre 2022 : type d'incident, impact,...

CYBERVEILLE SANTE, 03/12/2022

REMPAR22, un exercice de simulation de crise inédit le 8 décembre *>>Lire l'article*

Face à la menace cyber croissante et à un nombre d'attaques toujours plus important, l'ANSSI, le Campus Cyber et le Club de la continuité d'activité (CCA) s'unissent pour organiser REMPAR22, un exercice de simulation de crise cyber de grande ampleur, le jeudi 8 décembre 2022, autour d'un scénario unique créé pour l'occasion.

ANSSI, 08/12/2022

Sécurité : les assureurs veulent vous faire payer pour la casse des cyberattaques *>>Lire l'article*

Un dirigeant d'un des plus grands groupes d'assurance au monde déclarait récemment au Financial Times que les coûts induits par les cyberattaques dépassent désormais la compétence d'un assureur. Il appelle à l'intervention des Etats, au travers de partenariats public-privé, financés donc par les impôts des contribuables.

01NET, 27/12/2022

BONNES PRATIQUES

Plan d'action préventif pour réduire le risque d'une compromission massive de domaines Windows et de sauvegardes en cas d'attaques par rançongiciel

>>Lire l'article

Depuis décembre 2020, plusieurs structures de santé ont subi des attaques par rançongiciel qui ont provoqué, pour certaines d'entre elles, un impact majeur sur la continuité de leurs activités. L'ensemble des systèmes Windows a été compromis et les sauvegardes ont été supprimées, entrainant des pertes de données irréversibles.

CYBERVEILLE SANTE, 02/12/2022

Cyberattaques : la Fédération hospitalière et l'AFNOR publient un guide de référence

>>Lire l'article

Pilotés par l'AFOR, une quarantaine d'établissements publics et d'entreprises privées ont mis en commun leurs expériences, au lendemain d'une cyberattaque qu'elles ont subie directement ou indirectement, pour élaborer un guide afin de partager le savoir acquis et leurs meilleures pratiques.

IT SOCIAL, 08/12/2022

Le CERT Santé rappelle les bonnes pratiques en matière de sécurité de l'exposition sur Internet.

>>Lire l'article

Plusieurs établissements ont récemment subi des actes de cybermalveillance. Ces attaques proviennent exclusivement de l'Internet. Il est donc important de veiller à sécuriser son exposition sur Internet et surtout de la maintenir dans le temps.

Le CERT Santé rappelle ci-dessous quelques recommandations d'hygiène et de sécurité à propos des équipements numériques qui sont exposés sur Internet.

CERT SANTE, 09/12/2022

L'ANS publie deux vidéos sur la cartographie des SI *>>Lire l'article*

La première est une présentation synthétique de la démarche de cartographie du SI. Elle est basée sur le guide de l'ANSSI. Elle rappelle dans son introduction l'importance de la cartographie dans la gestion opérationnelle du SI et en particulier dans la réponse à un incident.

La deuxième vidéo est un entretien avec le RSSI du CHU de Brest qui présente comment il a mené ce projet au sein de son établissement et comment la cartographie est maintenue à jour. Il évoque également les avantages de disposer d'une cartographie dans la gestion des risques et des incidents.

ANS, 15/12/2022

MENACES

Pour 2 euros, vous pouvez vous offrir l'accès au compte de messagerie d'une entreprise ! >>Lire l'article

Les cyberattaques sont de plus en plus nombreuses et sur le Darkweb, certaines marketplaces permettent d'acheter un accès à une adresse e-mail professionnelle pour 2 dollars seulement, ce qui fait moins de 2 euros.

IT-CONNECT, 09/12/2022

« Les hôpitaux mieux ciblés demain ? » intensification des attaques hybrides et d'attaques IoT en 2023 >>Lire l'article

Une intensification des méthodes d'attaques hybrides qui associent l'automatisation à l'action humaine devrait contribuer à éviter les attaques « inadaptées » du type de celle de l'hôpital de Corbeille Essonne le mois dernier, et à les rendre plus rentables par extorsion double, triple quadruple.

GLOBAL SECURITY MAG, 14/12/2022

Santé : attaques de type Social Engineering >>Lire l'article

Le CERT Santé a été informé qu'un acteur de la santé a été touché par des attaques de type Social Engineering ciblant des PC d'automates interne. Ces cyberattaques ont un schéma assez similaire, en deux temps : ingénierie sociale et accès frauduleux par TeamViewer.

CYBERVEILLE SANTE, 22/12/2022

Vulnérabilités critiques du 26/12/22 au 31/12/22 *>>Lire l'article*

Ce bulletin d'actualité du CERT-FR revient sur les vulnérabilités significatives de la semaine 52 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.

Veuillez-vous référer aux avis des éditeurs pour obtenir les correctifs.

CERT FR, 02/01/2023

RGPD/ JURIDIQUE

Hébergement de données de santé : quoi de neuf ? >>Lire l'article

À la date d'écriture du présent article, la phase de concertation d'un nouveau référentiel HDS est terminée depuis quelques jours ? Pour mémoire, ce référentiel définit les exigences de la certification s'imposant aux termes de l'article L1111-8 du Code de la santé publique à « *toute personne qui héberge des données de santé à caractère personnel recueillies à l'occasion d'activités de prévention, de diagnostic, de soins ou de suivi social et médico-social, pour le compte de personnes physiques ou morales à l'origine de la production ou du recueil de ces données [...]* ».

DSIH, 06/12/2022

Quelques conseils pratiques dans votre démarche de conformité au RGPD >>Lire l'article

La majorité des plaintes s'articule autour des droits d'accès le plus souvent sur les dispositifs innovants tels que les caméras de vidéos surveillance/protection ou sur la problématique de la durée de conservation des données personnelles et celle de la non-conformité lors des traitements des données à caractère personnel des personnes concernées. Voyons quelques points problématiques et les conseils qui en découlent.

VILLAGE JUSTICE, 12/12/2022

Transfert des données UE-US : La Commission européenne avance >>Lire l'article

Un pas supplémentaire a été franchi par la Commission européenne sur l'accord-cadre sur les transferts de données transatlantiques. L'exécutif bruxellois a entamé le processus d'approbation du successeur du Privacy Shield.

LMI, 14/12/2022

Médico-social: création du traitement de données personnelles "Tableau de bord de la performance"

>>Lire l'article

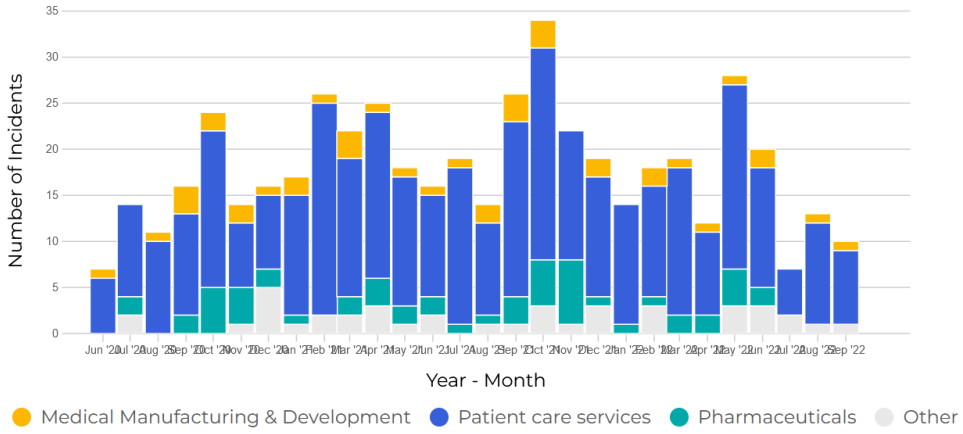
Un décret publié début décembre au Journal officiel a créé un traitement de données à caractère personnel dénommé "Tableau de bord de la performance dans le secteur médico-social" et détaille les finalités et données contenues dans ce tableau.

TIC SANTE, 26/12/2022

TRUCS ET ASTUCES

Traceur d'incident cyber dans le secteur de la santé [>>Visualiser]

CIT #HEALTH contient des données sur 501 cyberattaques contre le secteur de la santé dans 43 pays.



CYBERPEACE INSTITUTE, 31/12/2022