n°35
Février 2023

esesan
Groupement d'Intérêt Public eSanté

Newsletter Cybersanté

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

TOUS CYBER VIGILANTS

Edito

Pour bien débuter l'année, n'oubliez pas de candidater à l'appel à projet de l'ARS Ile-de-France pour réaliser un exercice de cybercrise et évaluer votre capacité de résilience ! Un marché SESAN est disponible pour vous accompagner dans la réalisation des exercices.

Le GIP SESAN propose aussi des solutions et un accompagnement pour :

- Mettre en place une cybersurveillance ;
- Faire des scans de vulnérabilité ;
- Sensibiliser à la cybersécurité ;
- Et bien d'autres services d'intérêt public !

Plus de 100 établissements de la région bénéficient de nos services. Rejoignez-nous !

Un doute ?

Une question ?

Contactez-nous sur

ssi@sesan.fr

Actus à la une

Cybersécurité des hôpitaux : l'exécutif prépare un plan blanc numérique pour mars 2023

L'exécutif prépare un plan blanc numérique pour mars 2023. En France, les cyberattaques contre les hôpitaux se multiplient avec des conséquences graves, allant jusqu'à forcer les établissements à transférer des patients ailleurs.

CARNET DE BORD, 03/01/2023

Lire l'article

Le siège parisien du Groupe Elsan a été impacté par un incident d'origine malveillante

Un incident d'origine malveillante a touché le siège parisien du Groupe Elsan dans la nuit du 17/01 au 18/01. Cet incident est resté circonscrit au SI du siège, sans rebond vers les cliniques du Groupe.

CERT SANTE, 23/01/2023

Lire l'article

L'ANSSI publie un panorama de la cybermenace 2022

Le 24 janvier 2023, l'ANSSI publie un rapport sur les tendances de la menace cyber en France au cours de l'année 2022, abordant les modes opératoires et la victimologie des acteurs malveillants..

CERT SANTE, 27/01/2023

Lire l'article

Trois établissements de santé touchés à Lyon et Bourg-en-Bresse

Une nouvelle cyberattaque a touché le 25 janvier quatre établissements du Groupe Ramsay Santé, dont trois en Auvergne Rhône Alpes. En 2019 déjà, le groupe avait été la cible de hackers.

FRANCE INFO, 30/01/2023

Lire l'article

Bonnes pratiques

Revoir le webinaire : sécurité des systèmes d'IA, enjeux et bonnes pratiques

La CNIL vous propose de décrypter un sujet ou une actualité en lien avec la protection des données à travers une série de webinaires. Retrouvez le troisième épisode consacré à la sécurité des systèmes d'intelligence artificielle.

Lire l'article

CNIL, 10/01/2023

Le CERT Santé publie une fiche concernant la sécurisation des accès à distance des prestataires

Lire l'article

Les accès à distance utilisés par les prestataires pour la maintenance ou la téléassistance sont souvent la cible de tentatives d'intrusion de la part des auteurs de cyber-malveillance. Le CERT santé vient de publier une fiche proposant un ensemble d'exigences de sécurité pour les prestataires et les structures afin de réduire le risque de compromission du SI lié à cet accès..

CERT SANTE, 18/03/2023

Recrutement et données personnelles : cinq questions incontournables à se poser

Quelles informations peuvent être utilisées ? Dans quel cadre les utiliser ? Combien de temps les conserver ? Quelles sont les pratiques interdites ? La CNIL vous répond..

Lire l'article

CNIL, 30/01/2023

Menaces

Une vulnérabilité critique dans Citrix exploitée lors d'attaques contre le secteur de la santé

les utilisateurs de Citrix Application Delivery Controller (ADC) et Citrix Gateway sont encouragés à vérifier que leurs produits sont bien à jour. La vulnérabilité critique CVE-2022-27518, découverte ce mois-ci, est exploitée par le groupe APT (Advanced Persistent Threat) chinois Keyhole Panda, et potentiellement d'autres groupes malveillants.

CERT SANTE, 05/01/2023

Lire l'article

IcedID : Compromission d'un Active Directory en moins de 24h

Lire l'article

Apparu en 2017 comme cheval de Troie pour voler des informations bancaires, IcedID (ou BokBot) est désormais utilisé comme dropper (outil déployant d'autres maliciels). .

CERT SANTE, 20/01/2023

Une carte des cyberattaques recensées contre les collectivités et établissements publics

Le réseau national de mutualisation informatique et numérique du secteur public, Déclic, a cartographié toutes les cyberattaques ayant touché des collectivités et établissements publics depuis 2019. Élaborée à partir des informations publiées par la presse locale, la carte doit sensibiliser ces acteurs à investir dans leur cybersécurité.

USINE DIGITALE, 27/01/2023

Lire l'article

Juridique

La certification HDS : une condition de validité des contrats informatiques

Le défaut de certification HDS peut coûter cher aux éditeurs de logiciel qui sont dans l'incapacité de démontrer la certification HDS de leur hébergeur, dès lors que la prestation offerte aux clients prévoit ou implique l'hébergement de données de santé. Une récente décision de la Cour d'appel de Nîmes (arrêt du 15 décembre 2022, n°21-01214) illustre cette situation.

DSIH, 17/01/2023

Lire l'article

Comment traiter une violation de données au plan juridique et technique ?

Lire l'article

À l'occasion de la journée de la protection des données qui a eu lieu en janvier dernier, la Cnil relève que la moitié des sanctions prononcées en 2021 comportait un manquement en lien avec la sécurité des données personnelles.

LEXING, 28/01/2023

La CNIL publie un guide pour les recruteurs

Un processus de recrutement implique nécessairement le traitement d'un nombre important de données personnelles sur les candidats. La CNIL propose un guide ainsi qu'un ensemble de fiches pratiques pour accompagner les acteurs du recrutement dans leur mise en conformité..

CNIL, 30/01/2023

Lire l'article

Communauté

Question du mois

"L'EDR est-il un équipement de sécurité indispensable contre les attaques par ransomware ?"

L'EDR – *Endpoint Detection and Response* est une solution de sécurité des terminaux (serveurs, postes de travail, smartphone,...) qui intègre une détection proactive des menaces et une réponse automatique à ces dernières. Equipé d'une intelligence artificielle, l'EDR peut détecter les actions anormales effectuées sur le système d'information (chiffrement en masse par exemple) et être en mesure de les contenir. Les menaces identifiées par l'EDR peuvent être connues (virus par exemple) mais également complexes ou inconnues comme l'exploitation de des failles zero day et l'utilisation de menaces avancées type ransomware.

Si la définition de cette solution est elle-même un premier élément de réponse, nous pouvons ajouter à cela quelques chiffres :

- Seulement **47% des attaques sont détectées** (Rapport CESIN- baromètre cyber sécurité des entreprise) par les antivirus classiques. Les antivirus classiques vont se contenter d'identifier et bloquer les menaces dont la signature est connue.
- Le risque d'attaque par ransomware augmente constamment dans le secteur sanitaire. On constate que les **attaques ayant ciblé les établissements publics de santé ont augmenté de 30%** entre 2020 et 2021 (Panorama de la cybercriminalité par l'ANSSI).

Pour conclure, nous pouvons donc dire que l'EDR est un équipement de sécurité indispensable notamment pour le secteur hospitalier. Nous vous recommandons une gestion managée de votre EDR pour la supervision des évènements, le traitement des alertes et des faux positifs, ce que l'on appelle un SOC (Security Operation Center).

L'équipe SSI

Une question?

Le sondage du mois

Répondre

Selon vous, quelles sont les deux mesures de sécurité prioritaires?


sesan
Groupement d'Intérêt Public eSanté