CYBERSECURA
Cybersécurité & Conformité

La Newsletter CyberSecura

Mai 2024

Profils dirigeants & partenaires | Profils techniques

PRESTATAIRE RÉFÉRENCÉ | OSCP | PECB ISO/IEC 27001 LEAD IMPLEMENTER

Au sommaire de cette newsletter :

1️⃣ L'alerte du mois

✔️ Une vulnérabilité met en danger les serveurs GitHub Enterprise Server.

2️⃣ Les actualités en cybersécurité et conformité RGPD

✔️ Les clés pour bâtir une IA de confiance.

✔️ Vous êtes un acteur de la santé ? La CNIL souhaite faire évoluer ses référentiels, faites part de vos priorités !

3️⃣ Nos contenus et actualités

✔️ Notre témoignage client par Odonatech, concernant prestation de RSSI et DPO externalisés en temps partagé.

✔️ Nos derniers contenus de blog et d'études de cas clients.

✔️ Les actualités de l'équipe CyberSecura.

Alerte du mois

Une vulnérabilité critique met en danger les serveurs GitHub Enterprise Server !

GitHub a déployé des mises à jour de sécurité pour corriger une faille de sécurité critique présente dans sa solution GitHub Enterprise Server et pouvant être utilisée par un attaquant pour contourner l'authentification.

Associée à la référence **CVE-2024-4985** et à un **score CVSS maximal de 10 sur 10**, cette faille de sécurité peut être exploitée par un attaquant pour accéder à l'instance GitHub Enterprise Server, sans être authentifié au préalable. Contrairement à la plateforme GitHub, la solution GitHub Enterprise Server est destinée à être auto-hébergée par les organisations soucieuses de vouloir gérer leur code avec Git sur leur propre serveur.

Au sein de la note de publication de la nouvelle version de GitHub Enterprise Server, voici ce que l'on peut lire : "*Sur les instances qui utilisent l'authentification unique SAML (SSO) avec la fonction optionnelle d'assertions chiffrées, un attaquant pourrait falsifier une réponse SAML pour provisionner*

et/ou obtenir l'accès à un utilisateur avec des privilèges d'administrateur."

L'exploitation de cette vulnérabilité pourrait permettre à un attaquant d'accéder aux différents projets et codes sources présents sur le serveur compromis.

Le 20 mai 2024, GitHub a publié de nouvelles versions pour corriger cette vulnérabilité : 3.12.4, 3.11.10, 3.10.12, et 3.9.15.

Si vous utilisez une version vulnérable de GitHub Enterprise Server, il est recommandé d'effectuer la mise à jour de l'application dès que possible pour vous protéger de cette menace potentielle. Ceci est d'autant plus un important qu'un exploit PoC semble disponible sur GitHub, sur cette page.

En lire plus

Les actualités de cybersécurité & de conformité

Les clés pour bâtir une IA de confiance

La confiance est la clé de l'adoption et de l'appropriation des technologies, en particulier des technologies d'IA. L'IA Act souhaite créer et proposer une IA de confiance, défini comme légale, éthique, robuste et sécurisée.

Mais en quoi consiste une IA de confiance concrètement ? Quelle est la portée de l'IA Act très précisément ? Et où en est la nécessaire collaboration entre spécialistes cyber et IA, pour instaurer cette IA de confiance ? Des experts ont débattu ces questions lors d'une table ronde organisée dans le cadre de la plénière "IA en quête de confiance", du Forum InCyber 2024.

Selon Nozha Boujemaa, vice-présidente "AI innovation & Trust" chez Décathlon, "une IA de confiance se doit d'être robuste, ce qui ne signifie pas nécessairement performante." Selon elle, nous pouvons observer des IA performantes mais non fiables. La robustesse implique notamment "la transparence, l'interprétabilité, la traçabilité et la reproductibilité. [...] Une IA de confiance ce n'est pas juste un "good will", mais repose sur une infrastructure et des outils installés de manière très opérationnelle dans les entreprises et chez les producteurs de services numériques, autant pour les données que pour les modèles. Cela permet l'observabilité et la traçabilité aussi bien des données que des algorithmes, afin d'être capable de détecter toutes les sources de risques et d'y remédier."

Pour permettre de répondre à ces nouveaux enjeux, le Parlement européen a voté la législation harmonisée sur l'intelligence artificielle, dénommée "IA Act" le 13 mars 2024. Ce règlement est tout à fait historique, dans la mesure où il est le premier au monde à disposer d'une telle profondeur de réflexion. Sa construction est cependant complexe car elle tente d'introduire une dialectique entre la sécurité des européens et la compétitivité des entreprises de l'UE.

Emmanuelle Legrand, magistrate spécialisée détachée à la Direction générale des entreprises (DGE) a participé aux négociations de l'IA Act pour le compte de Bercy.

Ce dernier comporte, selon elle, cinq grandes caractéristiques :

✔ L'IA Act instaure des règles contraignantes (approche plutôt classique de l'Union Européenne) assorties de sanctions en cas de violation, et établit un système de gouvernance définissant les autorités de régulation à désigner les conséquences des infractions aux obligations légales.

✔ L'IA Act n'a pas vocation a régler tous les problèmes ni tous les enjeux liés à l'IA, mais il s'inscrit dans une approche de réglementation des produits, considérant l'IA comme un produit commercialisé dans le marché de l'Union Européenne et ainsi soumis à un certain nombre de conditions.

✔ L'IA Act s'applique à tous les secteurs, publics comme privés, soulevant un défi en termes de précision des règles pour être opérationnel dans des contextes variés.

✔ L'IA Act adopte une approche neutre sur le plan technologique, ciblant les produits incorporant de l'IA et non les technologies elles-mêmes.

✔ Enfin, l'IA Act repose sur une approche fondée sur le risque, en se concentrant non pas sur les risques intrinsèques de la technologie, mais sur ceux associés à certains usages spécifiques de l'IA.

L'objectif serait ensuite de pouvoir étendre ces règles du jeu au-delà de l'Europe : Irakli Khodeli, chef de l'unité "Éthique de l'IA" à l'UNSECO expliquait : "lorsqu'on établit une régulation stricte dans une région du monde, les acteurs ont tendance à se délocaliser dans un autre endroit où la régulation est moins contraignante. Un cadre global s'avère donc nécessaire avec les mêmes règles et standards partout. [...] Les bénéfices de l'IA doivent aussi être accessibles aux pays en développement."

Source : "Quelles briques pour bâtir une IA de confiance ?", In Cyber News, le 16 mai 2024.

Vous êtes un acteur de la santé ? La CNIL souhaite faire évoluer ses référentiels, faites connaitre vos priorités !

Vous êtes un acteur évoluant dans le domaine de la santé, et avez le sentiment que les méthodologies de référence (MR) ne sont pas tout à fait adaptées à vos besoins ? Vous estimez que le référentiel "entrepôt de données de santé" pourrait évoluer ? Vous souhaiteriez pouvoir utiliser plus facilement les nouveaux référentiels proposés par la CNIL ?

La CNIL vous propose de répondre à un questionnaire, afin de l'aider à dresser un bilan des pratiques actuelles dans le secteur de la santé, et afin d'identifier vos priorités.

Tous les référentiels "santé" sont concernés par cet appel à participation : depuis MR-001 jusqu'à MR-008, soit les référentiels relatifs aux entrepôts de données de santé, à la gestion de vigilance sanitaire, aux accès précoces et compassionnels ou encore le référentiel d'accès simplifié aux données de l'échantillon du Système National des données de santé (SNDS).

En effet, de nombreuses évolutions ont contribué à rendre certains éléments de ces référentiels plutôt obsolètes : l'entrée en vigueur de plusieurs règlements européens ("essais cliniques" et dispositifs médicaux), l'essor des traitements de données de santé du SNDS, le développement de l'intelligence artificielle ou encore les répercussions de la crise sanitaire (notamment sur la dématérialisation et/ou la décentralisation des recherches en santé), certains référentiels nécessitent désormais des ajustements.

L'objectif de cette consultation actuellement en place est d'identifier à la fois les modifications à apporter aux référentiels concernés, ainsi que les sujets sur lesquels il pourrait être opportun d'adopter un nouveau cadre de référence ou des recommandations.

Chercheurs, professionnels de santé, entrepreneurs, délégués à la protection des données, juristes ou encore chargés de projet : tous les professionnels évoluant dans le secteur de la santé sont invités à prendre part à cette consultation publique, la CNIL souhaitant permettre au plus grand nombre d'y participer.

Participez à cette concertation en consultant l'article de la CNIL.

Recherche en santé : comment envoyer une note d'information dématérialisée aux participants ?
Dans le cadre de recherches, études ou évaluations dans le domaine de la santé, certains responsables de traitement souhaitent adresser la note d'information aux participants par voie électronique. La CNIL précise les conditions dans lesquelles elle peut autoriser de tels envois.
CNIL - le 16 mai 2024

Dropbox victime d'une intrusion
Les données dérobées comprennent des e-mails, des noms d'utilisateur, des numéros de téléphone et des hashs de mots de passe, et concernent potentiellement tous les comptes de Dropbox Sign. La fuite touche aussi les personnes non inscrites au service, mais ayant signé électroniquement un document envoyé via Dropbox Sign. Leurs noms et leurs e-mails seraient aussi compromis.
In Cyber News - le 13 mai 2024

Nos contenus

Apprendre & comprendre

LE BLOG
Comment vous assurer que les traitements de données réalisés par votre organisation sont conformes au RGPD ?
Vous traitez des données personnelles dans le cadre de votre activité professionnelle et souhaiteriez vous assurer que vos traitements de données, et notamment l'information des personnes concernées sont réalisés de manière conforme avec la réglementation RGPD ? Découvrez plus en détail quelles sont vos obligations.

Le 22 mai 2024 - 7 minutes de lecture

En lire plus

LES CONTENUS VIDÉO

Chit-Chat with CyberSecura - "La France est-elle en retard dans le domaine de la cybersécurité ?" Découvrez l'avis de notre experte.

Accédez à nos contenus pour en apprendre toujours plus !

Les contenus de blog

La chaine YouTube

Nos témoignages clients

En lire plus

Les études de cas clients à découvrir

Gestion d'une violation de données pour Présantis

Les incidents de sécurité informatique, et notamment les violations de données personnelles sont loin d'être anodines pour la continuité d'une activité, ainsi que pour la réputation d'une entreprise. Pour cette raison, elles doivent être traitées avec beaucoup de réactivité et beaucoup de pragmatisme. Découvrez-en plus sur notre prestation de gestion d'une violation de données à travers l'étude du cas client de Présantis.

Accompagnement à la certification ISO 27001 pour TECHNIDATA

Les certifications de sécurité deviennent désormais incontournables pour de nombreuses entreprises, dont les clients, partenaires et potentiels investisseurs demandent des preuves de sécurité et de gouvernance de la sécurité dans les organisations. Découvrez-en plus sur notre prestation d'accompagnement à la certification ISO 27001 à travers l'étude du cas client de TECHNIDATA.

L'actualité de CyberSecura

CyberSecura devient partenaire de Legal Insight

Legal Insight est un cabinet d'avocats spécialisé dans l'accompagnement des entreprises, des start-ups et des PME innovantes et à forte croissance. Le cabinet dispose d'une expertise pointue dans divers domaines, notamment dans la création de start-ups, les levées de fonds, l'intéressement des équipes, les fusions-acquisitions et la structuration des entreprises et des groupes.

MAILINBLACK

Découvrez l'interview partenaire de Mailinblack !

Dans le cadre du partenariat entre Mailinblack et CyberSecura, Cédric Langlasse, Responsable des partenariats chez Mailinblack a eu l'opportunité de répondre à quelques-unes de nos questions afin de présenter l'entreprise, et plus précisément le nouveau produit Mailinblack : U-Cyber 360°, une plateforme de sécurité exhaustive vous permettant de centraliser tous vos outils de sécurité informatique !

Lire l'interview

Ne manquez aucune de nos offres !

Abonnez-vous à nos offres promotionnelles en cybersécurité et en conformité réglementaire au RGPD !

Si vous vous abonnez à ces communications, vous recevrez chaque mois un nouvel email promotionnel. Vous aurez la possibilité de vous désabonner de ces envois à tout moment via un lien de désabonnement disponible en fin de chaque email.

Je m'abonne

Choisissez quel contenu de newsletter vous souhaitez recevoir !

Vous avez la possibilité de choisir à quelle(s) liste(s) de diffusion vous souhaitez être abonnée en cliquant sur le boutons ci-dessous.

Choisir ma liste de diffusion

Cet email vous a été envoyé par CyberSecura car vous êtes inscrit à notre newsletter ou bien faites partie de notre écosystème en échangeant avec nos collaborateurs. Vous avez la possibilité de vous désabonner à tout moment via le lien en vas de page ou via le bouton "Choisir ma liste de diffusion" ci-dessus.

Retrouvez-nous sur les réseaux sociaux !

Contactez-nous

CyberSecura, 3 Avenue du 8 Mai 1945, Échirolles, FRANCE

Consulter cet email dans un navigateur

Copyright © 2024 CyberSecura, All rights reserved.

Nous contacter :
contact@cybersecura.com

Cliquez ici pour vous désabonner de tous nos envois.

This email was sent to <<Email Address>>
why did I get this? unsubscribe from this list update subscription preferences
CyberSecura · 3 Avenue Du 8 Mai 1945 · Echirolles 38130 · France

INTUIT mailchimp