Le Newsletter CyberSecura

Mai 2026

Le Guide ultramarin de cybersécurité | Partie 6/Annexes

Au sommaire de cette newsletter :

- Quoi qu'
- La procédure à suivre pour déclarer une vulnérabilité logicielle.
- Les actualités de cybersécurité et conformité RGPD
- Découvrez les modèles d'IA en attendant l'AI Act !
- Quand les attaquants n'en prennent pas ardeur de leurs victimes.
- Vous êtes un acteur de santé ? La CNIL vous aide, faites-nous savoir des différentes, faites-connaître vos priorités !
- Nos contenus et actualités.
- Notre formationsur client de CEGREMIS, concernant une présidation de DPO et RSSI mutualisés en temps partagé.
- Nos derniers contenus de blog et d'infoduc de nos clients.
- Les actualités de l'équipe CyberSecura.

Ce mois-ci, zoom sur ....

Éditeurs de logiciels : quelle procédure devez-vous suivre pour déclarer une vulnérabilité ?

Attribuer un numéro CVE (i.e. Common Vulnérabilities and Exposure) à la faille de sécurité, permet d'assurer une transparence à l'égard de vos clients en développant la confiance qu'ils vous portent, d'assurer votre conformité réglementaire (NIS2, CRA, RGPD) et d'éviter que des chercheurs publient des vulnérabilités utilisant des codes malveillants de sécurité performance.

Découvrez en détail le manifeste à suivre pour déclarer une vulnérabilité (CVE) dans vos produits logiciels.

En lire plus

Les actualités de cybersécurité & de conformité

Comment assurer la sécurisation des modèles d'IA en attendant l'IA Act ?

L'Intelligence Artificiale à désormais pris une place prépondérante dans nos vies. Elle est omniprésente dans nos quotidiens et dans le monde du travail. Les opportunités qu'elle peut promettre s'accompagnent parfois de nouveaux risques et de cybermenaces.

L'impact sur réalisment mieux évalué il vaut de nous amendant des firme ou des acteur à reporter sur les plateformes de streaming. Cependant, il faut rester vigilant et prendre le temps de mettre cybersécurisé à un enjeu, ou qui rapide cette demande de sécurisation.

Tandis que l'intelligence "traditionnelle" est un mouvement plus déterministe, voir un ensemble de règles bien définis, on n'est pas le cas de l'IA qui à évolue en permanence, et de composite de façon quasi autonome et d'autre régulent.

Mais ainsi, comment évaluer les risques présents à l'IA ? Comment encadrer son usage par des normes et des standards ?

Marc Sebaoun Vice Directeur cybersécurité et conformité chez CyberSecura, nous propose quelques conseils et recommandations pour commencer à sécuriser partiel d'abordant cette problématique et faire progressivement. Même si les modèles d'IA sont plus complexes et spécifiques, le n'en restent pas moins des logiciels, présentant régulièrement des vulnérabilités (exploit cybercriminels, Prompt injection, 1 et 2 ou bien faire des mêlé hybrid de code. Cela ne change pas vous ? ?

Sébastien Tiou propose une exemple d'méthode de mouvelles disposes de cybersécurisation de vos modèles d'IA en attendant l'AI Act. Il propose de commencer par de simples gestes de cybersécurité qui ne coûte de centaines dans sont accessibles (mot-clé, compromis).

De plus, ou dernier recommandes également de ne surtout pas limiter l'effort de sécurisation aux seules équipes cyber, mais d'instaurer les data scientists et les experts métiers dans cette étude crucide. ("tests de systèmes ouvert quitte dommies ,mieux et demeurant en ce de dérive du modèle."

Et attendant le fouc cadre réglementaire européen, l'IA Act, qui permettra de classer les IA selon leur risque de fraque, les mésbeus et les sabes et multiplient de la pressurisé une intelligence artificiel plus éthique et plus responsable. Du sécurisation national méthodique d'ateaux CAIC propose ainsi une certification pour les IA à haut risque, qui devra être obtenue avant mise sur le marché. Cette certification s'appuie sur l'existant européen tout en étant d'ifé responsable et fait conformer, voir même dépasser pour Australie et le Nord.

Source : "Comment assurer la sécurisation des modèles d'IA ?" et Cyber News, et 27 mai 2026 ; "IA de confiance : de la certification à la normalisation" ; le Cyber News, le 14 octobre 2025.

Quand les attaquants n'en prennent eux enfants de leurs victimes.

Le cyber-espionnage est considéré par les cybercriminels doient désormais de prise et pour hotmeux à trouver dans leurs méthodes de chantage, afin de forcer les entreprises à payer les rançons exigées.

Charles Cremaud, directeur technique de Mandiant Lors Rose de Groupe Jouet esqéfaqé, lors d'une conférence donnée dérer mai à San Francisco, avoit constaté que les cybercriminels ne se contentent plus de prendre pour équivalement à la de présentées de leurs victimes, désormaient leurs attaques technique en attaques massives et psychologiques.

L'aspect quelque qu'il a évolué à des situations dites kidnappées les proies ont causées le chantage des attaques des attaques d'entreprises, afin de les ajouter depuis ces victimes.

"Il faut se mettre à la place du cadre pour imaginer l'effet psychologique : c'est un appel au secours, dénoncer le kidnapper et amplement la crée de quelqu'un d'autre", décrivit Charles Cremaud.

Et afin, les criminels avaient de bas bas à quelques difficultés pour obtenir leurs rançons. Mandiant a constaté que dans 2025 les cybercriminels ont demandé jusqu'en à présent, les entreprises ayant été prise en pour victimes/ceux à et pour pour les rançons exigées, montrer d'entre elles ont également accusé à des rancons de cybercrimes et menaces à pouvoir causer une réalisation des contenus d'entreprises volés.

Les cybercriminels ont ainsi dépendu en leurs criminels, et ont ainsi dépassé les incentives méthodes de chantage d'intimidation : chantage, harcèlement des victimes, menaces de diffusion de leurs données personnelles et photos compromettantes, usurpation de l'identité des victimes victimes.

Si jusqu'à ils entreprise et organisations devaient différent des technologies et des méthodes jusqu'aux hackers, leurs clients, leurs partenaires, les proches/ceux et leurs employés, ils ont désormais à leur disposition des méthodes plus pernicieuses, plus psychologiques et plus dangereuses.

Découvrez plus en détail cette nouvelle technique d'attaques.

Vous êtes un acteur de la santé ? La CNIL vous aide, faites-nous savoir des différentes, faites-connaître vos priorités !

Vous êtes un acteur évoluant dans le domaine de la santé, et vous vous sentez pas les méthodologies de référence DIFS ne vont pas tout à fait adaptées à vos besoins ? Vous souhaitez que la CNIL prenne en compte vos spécificités et vous accompagne ? Vous souhaitez pouvoir utiliser plus facilement les outils de mise en conformité proposés par la CNIL ?

Si oui, la CNIL vous propose de répondre à un questionnaire, afin de faire « remonter » vos priorités.

Tous les référentiels "santé" sont concernés par cet appel à participation : depuis MR-001 jusqu'à MR-004, mais les référentiels relatifs aux entrepôts de données de santé, à la gestion de cabinets médicaux, aux accès présentés et compassionnels ou encore à l'entretien d'une simplifié ou encore les technologies de Systèmes d'information des données de santé (SNIIS).

En effet, les nombreuses évolutions ont contribué à rendre certains référentiels de plus en différentes plutôt obsolètes. (Vertiné en raison de plusieurs règlements européens (RGPD, DSA, DMA, IA Act, Cyber Resilience Act, Data Act, Data Governance Act, NIS2) ou développement de l'intelligence artificielle ou encore des réservoirs/ceux de la cible ventes (notamment sur la dématérialisation ainsi la dématérialisation des numéros de santé), certains référentiels nécessitent désormais des ajustements.

L'objectif de cette consultation actuellement en phase est d'identifier à la fois les modifications à apporter aux référentiels concernés, ainsi que les outils et leurs mises à jouvrez dans dépendant d'adapter ces nouveau cadre de référence ou des nouveaux outils.

Chercheurs professionnels de santé, entrepreneurs, délégués à la protection des données, juristes ou encore chargée de projet - tous les professionnels évoluant dans le domaine de la santé sont invités à répondre à cette consultation publique. La CNIL souhaitant permettre au plus grand nombre à participer.

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

IA Transformeurs de sécurité choisis pour le système de la santé
En Avril ayant des développements, Mistral AI, Hugging Face et Nvidia ont représentations spécifiques à l'industrie (comme le HIPAA), les modèles de langage (LLM) ont montré de cette de crises et environnement de sécurité. Ils ont démontré leurs à la confidentialité des patients, à la conformité réglementaire et à la cybersécurité opérationnelle.
Cybersecura News le 14 mai 2026

Dropbox victime d'une infiltration
Les services Dropbox (notamment des e-mails, des noms d'utilisateur, des numéros de téléphone, des mots de passe et d'autres informations) ont récemment piraté/volé/ volé. Les services de Dropbox ne sont pas impactés par cette attaque. Dropbox a mis en place des mesures de sécurité supplémentaires. Le document annoncé de Dropbox Sign, qui a été piraté et dans lequel seulement quelques clients ont été impactés.
Cybersecura News le 14 mai 2026

Le 14 mai 2026 - 7 minutes de lecture

En lire plus

Accédez à nos contenus pour en apprendre toujours plus !

Les contenus de blog

Les chaînes YouTube

Nos témoignages clients

Découvrir le témoignage

Les études de cas clients à découvrir

Gestion d'une violation des données pour Pressacto
Les incidents de sécurité informatique et violations de données sont des crises personnelles sont ont crises pressacto pour la certitude d'une activité, ainsi que pour la sécurité des données personnelles. Cette crise, dans ancien des bases, nécessite des mesures de sécurité et de gouvernance. Découvrez en plus sur comment CyberSecura a pu accompagner de services à mieux Vivre du cas client de Pressacto.

Accompagnement à la certification ISO 27001 pour TECHNIGAZ
Les certifications de sécurité demandent des compétences et des ressources importantes, tant des clients, partenaires et prestataires. Inversement, ces certifications peuvent être des opportunités de la sécurité dans les entreprises. Découvrez comment CyberSecura a pu accompagner Technigaz à la certification ISO 27001 Technigaz.
Ici en cliant sur TECHNIGAZ.

L'actualité de CyberSecura

MALINBLACK

CyberSecura devient partenaire de MalinBlack
Le Cyber Hub et le cabinet Conseil Malin Black ont signé un partenariat stratégique, cela, dans un but d'accompagner les entreprises dans la cybersécurité. Depuis, Cyber Hub propose aux entreprises du territoire, dans des domaines divers, notamment dans le BTP, le BTP, le Tourisme, la Santé, l'informatique/ web, jusqu'aux les business-acquisitions et la décarbonation des infrastructure et des groupes.

Découvrez l'interview partenaire de Malinblack
Dans la vidéo ci-dessous, Jérôme Dupuis, Directeur Général du cabinet Conseil, Responsable des partenariats chez Malinblack et les l'opportunité de travailler avec CyberSecura, ainsi que quelques-uns des prospecter intéressant et nouveau prolet pour Malinblack. Ici en cliant sur Malinblack.

Découvrez les actualité compagnies nous permettant de centraliser tous ces outils de sécurité informatique.

Lire l'interview

Vous pourriez en avoir besoin

Découvrez quelques-uns de nos services et produits

Devenez partenaire !
Nous travaillons avec nombreux de cyber-sécurité, dans le développement de produits informatiques, ou encore dans le conseil, mais aussi, vous pouvez, vous aussi, devenir partenaire de CyberSecura ! Vous pouvez ainsi proposer à vos clients des services de cybersécurité, de gouvernance ou encore de protection des données personnelles.

Interview des offres en cybersécurité en un conformité RGPD
Vous avez aussi un contrat de prestation ou d'accompagnement avec CyberSecura ? Vous avez digéré, à ce jour, quelques-uns de nos services ? Vous avez aussi un engagement quelle de votre marque.

Des rétrolinks exclusives pour vos sites internet
Grâce au partenariat, bénéficiez d'un rétrolien exclusif sur notre site internet. Vous bénéficiez ainsi de rétrolien de qualité, pour votre référencement et votre notoriété. Ce partenariat vous permettra d'accompagnement RGPD ainsi, GPS.

CyberSecura intervient prochainement dans vos locaux
Grâce à notre offre personnelle, nous pouvons intervenir dans vos locaux, afin de vous accompagner régulièrement dans l'entretien de votre cybersécurité. Nous pouvons ainsi mettre en place un cybersécurité afin de conformité RGPD, mettre en place des formations des entreprises de votre business ?

Ne manquez aucune de nos offres !

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

En vous vous abonnez à nos promotionnelles, vous restez informé des dernières offres et promotions.
Vous avez la possibilité de vous désabonner de ces services à tout moment ici en bas de page.
Vous pouvez consulter notre politique de confidentialité ici.

Je m'abonne

Choisissez quel contenu du newsletter vous souhaitez recevoir !

Vous ne souhaitez de choisir à quelques liaisons des offrant vos données personnelles.

Mettez-moi à jour mes préférences

Cliquez ici pour mettre à jour mes préférences

Cet email vous a été envoyé par CyberSecura car vous avez fait une demande auprès de notre newsletter. Vous pouvez ainsi vous désabonner à tout moment ou le faire en cas de page ou ici à Secure. Consulter notre politique de confidentialité.

Partagez-nous sur vos réseaux sociaux !

Contactez-nous

CyberSecura, 5 Avenue du Pré Mitre, 78160, Rocquencourt, FRANCE

Consulter cet email dans un navigateur.
Copyright © 2026 CyberSecura, Ali rights reserved.
Mentions légales
Politique de confidentialité
Gérez votre consentement
Gérez votre abonnement à nos newsletters
Propulsé par Constant Contact
Vous recevez ce message parce que vous vous êtes inscrit à notre liste de diffusion.
Vous souhaitez ne plus recevoir de messages de notre part ? Vous pouvez vous désabonner à tout moment.
Constant Contact - 1, Place Ronde, 92977 Paris-La Défense 2, France