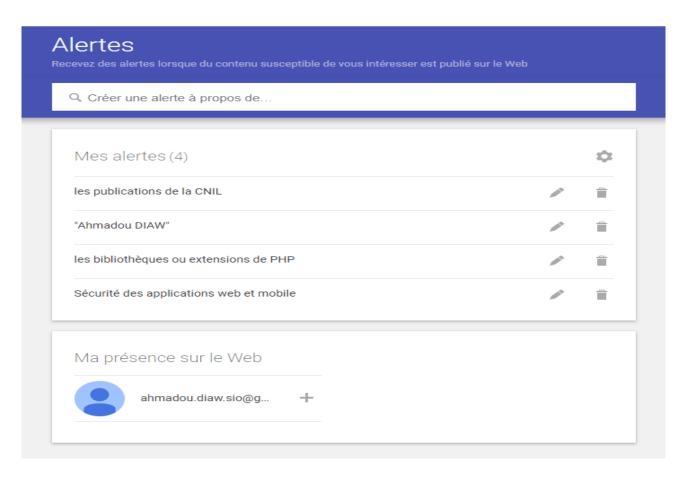
# **Veille Technologique**

Dans un monde de plus en plus numérique, la sécurité des applications web et mobile est devenue une priorité essentielle. Avec la prolifération des cybermenaces et des violations de données, il est crucial de rester à jour sur les meilleures pratiques et les dernières tendances en matière de sécurité informatique. Parallèlement, les publications de la CNIL fournissent un cadre réglementaire important pour garantir la protection des données personnelles et la vie privée des utilisateurs en ligne. En surveillant ces deux sujets, je peux m'assurer de maintenir une approche équilibrée entre les aspects techniques de la sécurité des applications et les exigences légales en matière de protection des données

#### Le fonctionnement :

Lorsque je reçois une alerte sur mon compte mail, je prends rapidement connaissance des articles liés à la sécurité des applications web et mobile ainsi qu'aux publications de la CNIL. Je commence par lire attentivement les contenus des articles pour comprendre les dernières menaces, vulnérabilités ou réglementations en vigueur. Pendant cette lecture, je m'attarde particulièrement sur les aspects pertinents pour mes activités professionnelles et je prends des notes sur les points importants à retenir. Ces notes comprennent des informations sur les nouvelles pratiques de sécurité à adopter, les recommandations de la CNIL, les cas d'utilisation spécifiques, ainsi que les mesures de conformité réglementaire à mettre en œuvre. Une fois ces notes prises, je les intègre dans mes processus de développement ou de gestion de projet, en veillant à tenir compte des meilleures pratiques et des exigences légales pour garantir un niveau optimal de sécurité et de conformité.



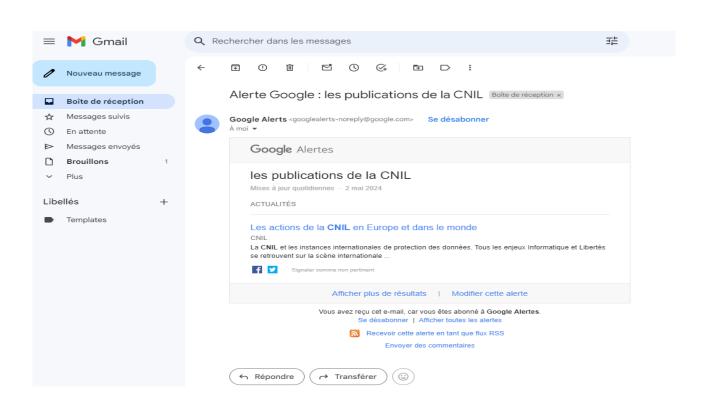
# les alertes

# Alertes

Recevez des alertes lorsque du contenu susceptible de vous intéresser est publié sur le Web

les publications de la C	1 mai 2024  ❖ >
les publications de la o	7 202 .
il y a 1 jour	
ACTUALITÉS	
Les actions de la <b>CNIL</b> en Europe et dans le monde	
La CNIL et les instances internationales de protection des données. Tous les enjeux Inforretrouvent sur la scène internationale	matique et Libertés se
il y a 7 jours	
ACTUALITÉS	
La CNIL a enregistré un nombre record de plaintes en 2023 - Mac4Ever	
Marquée notamment par l'augmentation des piratages (les cyberattaques de France Trav l'organisation des Jeux olympiques de Paris,	ail par exemple) et
il y a 8 jours	
ACTUALITÉS	
CNIL : record de plaintes pour atteintes à la vie privée en 2023 - Journal de l'économie	économie
Le rapport annuel de la Commission nationale de l'informatique et des libertés (CNIL) révalarmant : une augmentation	rèle un phénomène
La CNIL publie son rapport annuel 2023	
La <b>publication</b> de son rapport d'activité permet à la <b>CNIL</b> de rendre compte de ses actions quatre grandes missions : informer et	s au regard de ses





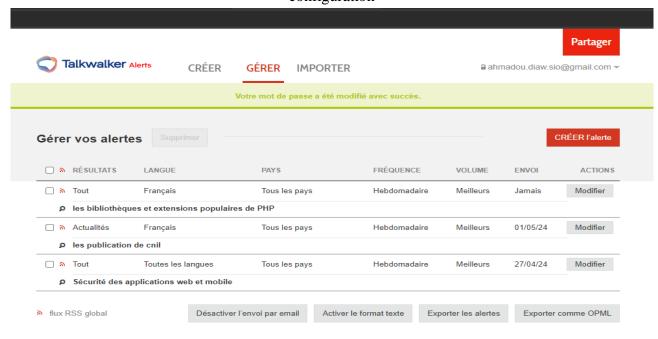




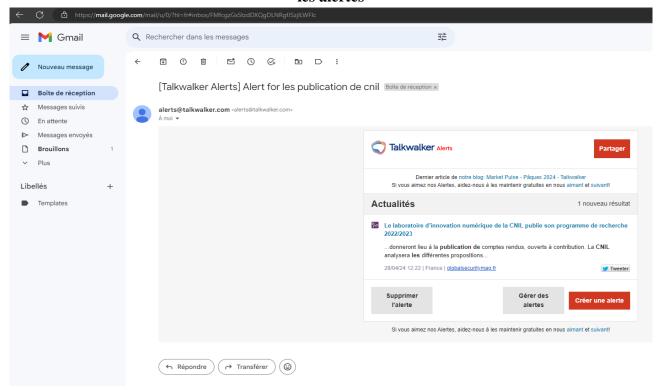
### Pour talkwalker

La CNIL au sein du Comité européen de la protection des données

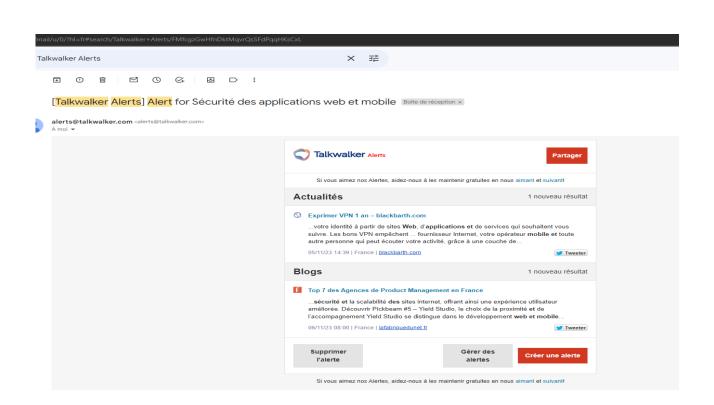
# configuration

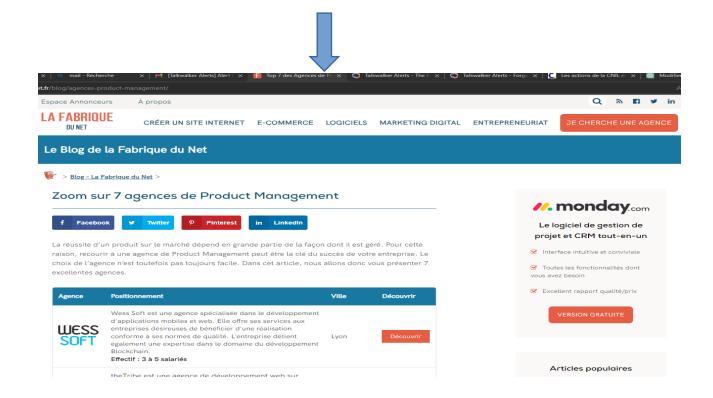


# les alertes









# Quelques articles collectés

Comment les développeurs d'applications protègent-ils les utilisateurs contre les cyberattaques ?

Le lien de l'article est : https://waza-tech.com/comment-les-developpeurs-dapplications-protegent-ils-les-utilisateurs-contre-les-cyberattaques/

L'article "Comment les développeurs d'applications protègent-ils les utilisateurs contre les cyberattaques?" publié sur le site waza-tech.com aborde un sujet crucial dans le domaine de la sécurité des applications. L'article explore les différentes stratégies et techniques utilisées par les développeurs pour protéger les utilisateurs contre les cyberattaques. Il examine notamment les mesures de sécurité telles que le chiffrement des données, l'authentification à deux facteurs, les mises à jour régulières des logiciels, et la gestion des vulnérabilités. En outre, l'article met en évidence l'importance de la sensibilisation à la sécurité pour les utilisateurs, ainsi que les bonnes pratiques de développement sécurisé. Cette ressource fournit des informations précieuses pour les développeurs d'applications cherchant à renforcer la sécurité de leurs produits et à protéger les utilisateurs contre les menaces en ligne.

Quels sont les 5 principaux défis émergents en matière de cybersécurité ? Le lien de l'article est : https://metatrone.fr/66382-quels-sont-les-5-principaux-defis-emergents-en-matiere-de-cybersecurite/

L'article "Quels sont les 5 principaux défis émergents en matière de cybersécurité ?" explore les nouveaux défis auxquels sont confrontées les organisations en matière de sécurité informatique. Voici un résumé des points principaux de l'article :

- Attaques de sécurité mobile : Les appareils mobiles sont de plus en plus ciblés par des attaques de phishing, des logiciels malveillants et d'autres menaces. Les entreprises doivent renforcer la sécurité des appareils mobiles utilisés par leurs employés pour accéder aux données sensibles et aux réseaux d'entreprise.
- Rançongiciel (Ransomware): Les attaques de ransomware continuent de constituer une menace majeure pour les entreprises. Les cybercriminels utilisent des logiciels malveillants pour chiffrer les données des victimes et demander une rançon en échange de leur déchiffrement. La prévention, la détection précoce et la réponse rapide sont essentielles pour atténuer les dommages causés par les attaques de ransomware.
- Risques liés au travail à distance : Avec l'essor du travail à distance, les entreprises sont confrontées à de nouveaux défis en matière de sécurité. Les employés travaillant à distance peuvent être plus vulnérables aux attaques de phishing, aux accès non autorisés aux réseaux d'entreprise et à d'autres menaces. Il est essentiel de mettre en place des politiques de sécurité robustes pour protéger les données et les systèmes des entreprises dans un environnement de travail à distance.
- Attaques internes: Les menaces internes, telles que les employés malveillants ou négligents, représentent également un risque important pour la sécurité des entreprises. Les entreprises doivent surveiller de près les activités des utilisateurs autorisés et mettre en place des mesures de sécurité pour prévenir, détecter et répondre aux incidents impliquant des menaces internes.
- Ancien matériel: L'utilisation de matériel obsolète ou non pris en charge expose les entreprises à des risques de sécurité accrus. Les appareils et les systèmes anciens peuvent comporter des failles de sécurité connues et ne pas recevoir de correctifs de sécurité réguliers. Il est important pour les entreprises de mettre à jour leur matériel et leurs logiciels pour réduire les risques de sécurité associés à l'utilisation d'équipements obsolètes.

Ces cinq défis soulignent l'importance pour les entreprises de rester proactives et de prendre des mesures pour renforcer leur posture de sécurité et protéger leurs données et leurs systèmes contre les menaces émergentes en matière de cybersécurité.

Sécurité contre les cybermenaces : La sécurité des applications web et mobile est essentielle pour protéger les utilisateurs contre les cyberattaques. En se tenant au courant des dernières avancées et des meilleures pratiques en matière de sécurité, on peut mettre en place des mesures préventives efficaces pour prévenir les violations de données et les cybermenaces, assurant ainsi l'intégrité et la fiabilité des applications.