



La Lettre de veille passée en revue



Présentation de la Lettre de Veille

- Une lettre de veille en sécurité de l'Information née d'une circonstance. Son objectif
- Ses modes de publication et son audience
- Son contenu
- Ses sources, les outils et les "Trucs" utilisés
- L'utilisation de l'IA générative ... ou pas
- Les tendances actuelles dans le domaine
- Éphémère, chronophage, addictive ... alors, pourquoi



Son origine et sa Diffusion

- Une lettre de veille en sécurité de l'Information née sur une circonstance
 - Un produit du hasard et non une démarche préparée, réfléchie, précisément cadrée avec un demandeur et en vue de servir ses besoins d'information
 - A partir de mes connaissances et de mon expérience en tant que MSSSI dans le service public de l'Assurance Maladie
- Ses modes de publication et son audience
 - 3 Lettres/semaine adressées directement à 800 destinataires environ aujourd'hui et une lettre hebdomadaire sur un site dédié pour inscrire dans la durée des lettres éphémères par nature
 - La lettre hebdomadaire est poussée sur Twitter (1 750 abonnés, 200 listes) et sur LinkedIn (1 800 Relations et contacts)
 - Un lectorat très diversifié, étudiants, consultants, métiers de la SI , experts, chercheurs

Suivre l'actualité sur la sécurité de l'Information

- La lettre est adressée à des publics très différents. D'où son approche généraliste de l'information y compris de l'information technique mais aussi mais surtout ...
- Une approche large comme le périmètre de la sécurité de l'Information doit s'entendre, plus que la cybersécurité au sens limité du terme
 - Diverses rubriques pour approcher ce vaste champ ... Informations générales / management de la sécurité de l'Information / Le RGPD, la protection des DCP / les problématiques des (r)évolutions numériques en cours / Des nouvelles du cyberfront (stratégie, attaques, impacts) / des sujets matière à réflexion / Des référentiels, études, enquêtes / Des évènements, journées, conférences le + souvent proposées par des acteurs institutionnels , des Ass. Professionnelles, les Lundi de la cybersécurité évidemment ...
 - Une rubrique dédiée intelligence artificielle sur la demande du Groupe Sécurité du Hub France IA, l'intelligence artificielle et sa bivalence en matière de sécurité de l'Information mais pas seulement

L'information coule de sources ...

Densité et diversité des sources ... Impossible de les citer toutes

- Les grands sites institutionnels
- [ANSSI](#), [Cybermalveillance.gouv.fr](#), [CERT-FR](#), [CNIL](#)
- L'Agence de cybersécurité européenne ([ENISA](#)), l'Agence américaine de cybersécurité et de sécurité des infrastructures ([CISA](#)), l'Institut des normes et standards US ([NIST](#)) ...
- Des Centres de cybersécurité étrangers, NCSC [britannique](#) et [suisse](#), le Centre de cybersécurité [canadien](#)



L'information coule de sources ...

- Des sites d'info dédiés numériques – [ZDNet](#), [GSMag](#), [Numerama](#), NextImpact, [Zataz](#), [Le MagIT](#), [Le Monde Informatique](#) ...
- Des NewsLetters et des lettres de veille – [XMCO](#), [Intrinsec de Sekoia](#), ARCSI (via Francis Bruckmann sur LinkedIn) ...
- [Le CERT-EU](#), composé d'experts informatiques issues des institutions européennes, il collationne et diffuse en permanence des articles, analyses et alertes publiés dans le monde entier
- Toute l'actualité InfoSec [AllInfoSecNews](#) Le site regroupe l'ensemble des actualités, textes, vidéos, podcasts sur les sécurités informatiques, les menaces et les vulnérabilités avec un module interactif d'interrogation
- Des Associations – [CLUSIF](#), [CESIN](#), [ARCSI](#), [ClubEBIOS](#), [l'AFCDP](#)

Les fournisseurs de solutions de sécurité

Quelques adresses ...

- [Malwarebits Labs](#)
- [SecureList Kaspersky](#)
- [Research, News, and Perspectives Trend Micro](#)
- [Symantec](#)
- [Mandiant](#) ...



L'information coule de sources ...

- [Le cyberCercle](#), cercle de réflexion et d'échange avec ses paroles d'experts, ses matinales, ses réunions en régions, son Tour de France
- En parlant d'experts sources d'information, je dois citer Solange Ghernaouti, JJ Quisquater, Gérard Peliks, Gêrôme Billois, Nicolas Arpagian, Cédric Cartau, Philippe Wynckier et d'autres encore ...
- Des médias généralistes, radios, journaux (LeMonde, SudOuest, LeFigaro)
- Des médias étrangers – [BleepingComputer](#), [Dark Reading](#) ...
- Un site juridique – [Village de la justice](#)
- Des vidéos, des podcasts d'événements et une émission hebdomadaire régulière tenue par l'équipe [NoLimitSecu](#) avec notamment Hervé Schauer, Nicolas Ruff, Johanne Ulloa ...

Les outils utilisés

- Les outils ...
 - Quelques alertes Google quotidiennes ... cybersécurité, confidentialité, sécurité de l'Information, données de santé, données médicales, cyberdéfense, vie privée ...
 - Un agrégateur de flux RSS, Feedly pour être informé temps réel des modifications intervenues sur un site
 - Twitter, ses listes et son moteur de recherche avancée
 - LinkedIn et son classement par pertinence
 - Un agrégateur d'articles, FlipBoard et son particulièrement son dossier "Technologie"
 - Un fichier au format rtf sous Writer d'Office pour la réalisation des lettre(s)



Twitter et son mode de recherche avancée

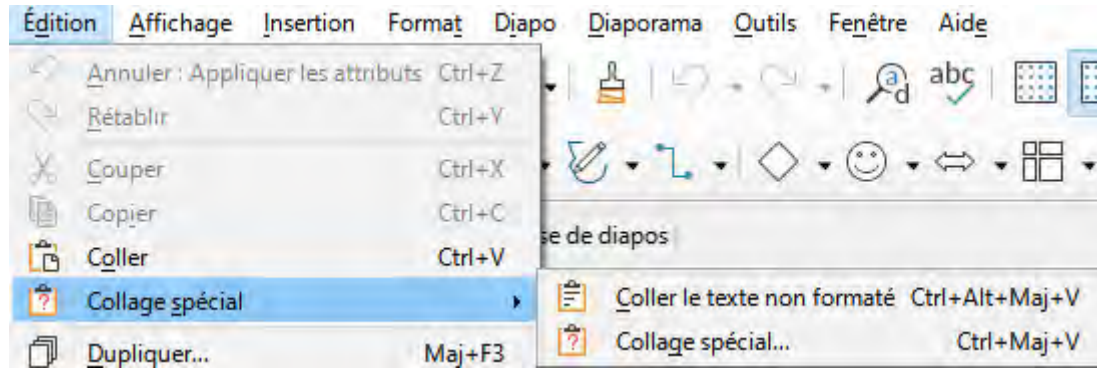
- La sélection de comptes, la gestion de listes, le choix de sujets et de centres d'intérêt dans les paramètres / confidentialité & sécurité / contenu ...
- Pas seulement les #
- D'abord, une recherche simple
- Affichage de premiers résultats, de filtres de personnes et de localisation mais surtout de la fonction "Recherche avancée"
- Accès à un formulaire d'aide pour choix des mots, groupe de mots, inclus, exclus, langue, hashtags, comptes, une recherche sur une période avec possibilité d'affiner encore la recherche ...
- Très commode pour interroger un réseau social en mode de publication continu comme twitter

Google et ses commandes de recherche avancée

- Les commandes ... "" NOT ou OR ou AND et d'autres
- Sur LinkedIn recherche booléenne et accès aux posts par pertinence plutôt que par ordre chrono ...
- Sur https://www.google.com/advanced_search et les puissantes commandes Google dorks à utiliser pour la bonne cause
- Voir sur le web, de nombreux guides ...
- Évidemment des commandes très utiles lors d'une recherche ciblée

Des macros pour faciliter la mise en forme

- Notamment pour pratiquer le copier-coller de texte non formaté



... appelé par CTRL+9 pour exécuter la macro

```
458 sub collage
459 rem -----
460 rem define variables
461 dim document as object
462 dim dispatcher as object
463 rem -----
464 rem get access to the document
465 document = ThisComponent.CurrentController.Frame
466 dispatcher = createUnoService("com.sun.star.frame.DispatchHelper")
467
468 rem -----
469 dim args1(0) as new com.sun.star.beans.PropertyValue
470 args1(0).Name = "SelectedFormat"
471 args1(0).Value = 1
472
473 dispatcher.executeDispatch(document, ".uno:ClipboardFormatItems", "", 0, args1())
474
475
476 end sub
```

Une base de formules d'auto-corrections ...

- Une fonction très pratique qui donne quelques chances d'écrire sans commettre trop de fautes mais qui permet aussi d'automatiser des formules utilisées régulièrement. Quelques exemples ...
- Epv = Et puis, dans la vie personnelle comme dans la vie professionnelle
- Ccisa = Agence américaine de cybersécurité et de sécurité des infrastructures (CISA)
- Lcp = le communiqué de presse
- Cans = Agence Nationale de la Sécurité des Systèmes d'Information
- Cenis = Agence de l'Union Européenne pour la cybersécurité (ENISA)
- Csi = sécurité de l'Information
- Vaiv = (voir aussi la lettre de veille du

L'intelligence artificielle, utile ou pas ...

- Nouvelle outil de veille à suivre
- Pour l'instant, pas d'efficacité en veille directe ou continue.
- Par contre, fort potentiel d'aide au veilleur dans l'identification des sources et dans toutes les séquences d'une lettre de veille (identification des besoins, recherche, analyse et diffusion) sous réserve de quelques précautions à connaître
- notamment montrer de la pugnacité et du savoir-faire dans l'art de poser les bonnes questions
- Une bonne adresse, le site de Christophe DESCHAMPS notamment sa série d'articles "ce que ChatGPT fait à la veille" ... <https://www.outilsfroids.net/author/christophe/>



Les tendances actuels en sécurité de l'Information

Quelles sont les tendances de ces dernières semaines ...

- Le foisonnement législatif de l'UE, les dispositions adoptées, en particulier la directive NIS2 mais aussi DORA et d'autres (DMA, DSA ...) et les dispositions en cours d'examen (CRA, CSA ...)
- "L'intelligence artificielle", son actualité désormais fournie et les questions qu'elle pose, notamment, mais pas seulement, en cybersécurité
- Une tendance saisonnière en cette fin d'année, les prévisions/prédictions des fournisseurs de solutions
- La manipulation de l'information, la cybersécurité des PME et des collectivités locales, la pénurie de compétences "Demain spécialiste cyber", la gestion de crise ...

Pour terminer ...

- du temps et ... la pratique aboutie des raccourcis-clavier notamment
- éphémère sauf si ... <https://veillecyberland.wordpress.com/>
- chronophage, addictive ... alors, pourquoi
- des remerciements à toutes ces sources qui me donnent la possibilité de vous proposer la lettre, la revue de presse, que je tiens

Comment la recevoir ...

Guillet.lionel@gmail.com

À l'écoute de vos questions