Dossier de veille 2023

« La maturité cyber des entreprises françaises, et leurs futurs »

Hasnaoui Abdelhadi

M1 Cybersécurité

Année : 2022-2023

Etablissement : Montpellier Ynov Campus

Tuteur d'alternance : M. Sébastien Tombarello

Poste en alternance : Mentor Informatique

Référent : M. Vincent Artz

MONTPELLIER YNOV CAMPUS

Table des matières

MONTPELLIER YNOV CAMPUS

Thématique :

Ah, la technologie ! Elle est partout, n'est-ce pas ? Nos smartphones, ces petits bijoux de technologie qui sont devenus une extension de nous-mêmes, les voitures connectées qui semblent tout droit sorties d'un roman de science-fiction, ou les systèmes informatiques qui font tourner nos entreprises avec une précision digne des plus grands horlogers.

Mais attendez une minute, il y a un "mais". Vous savez, le genre de "mais" qui fait froncer les sourcils et qui nous fait nous interroger sur les implications de tout cela. Avec cette dépendance accrue à la technologie vient une série de défis, et le plus grand de tous est sans doute la cybersécurité. C'est un peu comme si nous avions construit une maison ultra-moderne, mais que nous avions oublié de mettre des serrures sur les portes.

C'est là que la notion de maturité cyber entre en jeu. En gros, c'est notre capacité à gérer ces risques de cybersécurité et à nous protéger contre les menaces potentielles. Un peu comme si nous avions un super-héros de la cybersécurité en interne.

Cependant, malgré l'importance de la cybersécurité, beaucoup d'entreprises ne sont pas encore tout à fait à la hauteur. Que ce soit par manque de ressources, de compétences ou simplement de compréhension, beaucoup d'organisations n'ont pas encore atteint un niveau de maturité cyber qui leur permettrait de gérer efficacement ces risques. Et c'est un problème, parce que cela les rend vulnérables aux cyberattaques, qui peuvent causer des pertes financières, nuire à leur réputation et perturber leurs opérations.

Alors, que faire ? Eh bien, il est crucial de comprendre et d'améliorer la maturité cyber des entreprises. Un peu comme si on faisait un check-up complet pour s'assurer que tout est en ordre. Parce qu'au final, comme le dit le proverbe, mieux vaut prévenir que guérir.

Introduction :

En tant qu'étudiant en cybersécurité, j'ai toujours été fasciné par le monde complexe et en constante évolution de la technologie. Mon parcours m'a permis de comprendre à quel point la cybersécurité est cruciale dans notre société hyperconnectée. C'est un domaine qui me passionne, non seulement pour son aspect technique, mais aussi pour les enjeux sociétaux qu'il soulève. Une question en particulier m'interpelle : l'écosystème des entreprises françaises est-il mature d'un point de vue cyber ?

En effet, on constate que la technologie est devenue omniprésente dans nos vies, et par extension, dans le monde des affaires. Les entreprises, qu'elles soient petites ou grandes, dépendent de plus en plus de la technologie pour fonctionner. Cependant, cette dépendance accrue à la technologie s'accompagne d'un risque accru de cyberattaques. Dans ce contexte, la maturité cyber, c'est-à-dire la capacité d'une entreprise à gérer efficacement les risques liés à la cybersécurité, devient un enjeu majeur. La question qui se pose alors est la suivante : l'écosystème des entreprises françaises est-il suffisamment mature d'un point de vue cyber pour faire face à ces défis ?

Pour répondre à cette question, je vais mener une veille approfondie sur le sujet. Je vais analyser l'état actuel de la maturité cyber des entreprises françaises, en me basant sur des études de cas, des rapports de l'industrie et des recherches académiques. Je vais également examiner comment les nouvelles tendances technologiques, telles que l'intelligence artificielle, le cloud computing, l'Internet des objets et la blockchain, affectent la maturité cyber des entreprises. Enfin, je vais explorer les mesures que les entreprises peuvent prendre pour améliorer leur maturité cyber.

Cette veille me permettra non seulement de répondre à ma question, mais aussi de contribuer à la discussion sur la maturité cyber des entreprises françaises. Je suis convaincu que cette recherche sera une étape importante dans mon parcours d'étudiant en cybersécurité et j'ai hâte de partager mes découvertes.

Processus de veille :

La veille est un processus constant qui demande une rigueur, une bonne méthodologie et plein d'outils différents pour être constamment à jour sur les dernières failles de sécurité, l'activité de groupe de cyber attaquant, et aussi les avancées techniques et technologiques afin d'avoir de bonnes pratiques en cyber sécurité.

Je vais donc présenter certains outils que j'utilise pour faire ma veille.

Twitter :

Twitter est un outil surpuissant, en suivant les bons comptes (principalement les CERT [1]et d'autres chercheurs) j'arrive à avoir beaucoup d'informations et surtout des avis constructifs sur des décisions d'entreprise qui sont critiqués ou débattus par certains experts. Pour trouver des comptes de chercheurs qui ont une expertise reconnue, j'ai d'abord suivi les chercheurs qui ont fait des interventions à des conférences, tel que la defcon ou encore black hat et puis je regarde quels comptes eux-mêmes suivent et leurs interactions.

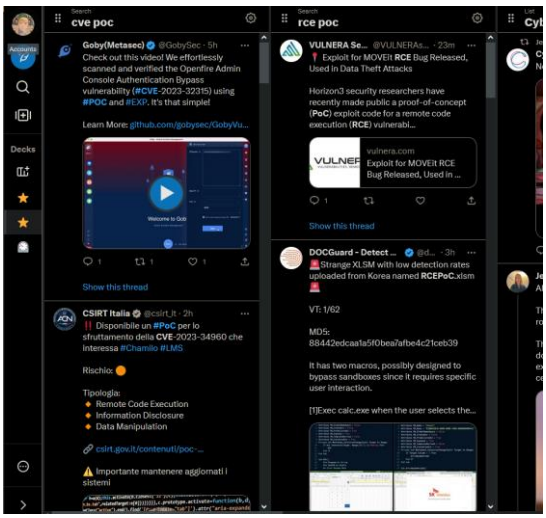


figure 1 : screen de mon interface de tweetdeck

[1] Computer Emergency Response Team, est une organisation ou une équipe qui répond aux incidents de sécurité informatique

Sur twitter je fais attention à vérifier les informations au minimum chaque matin et soir et plusieurs fois dans la journée, tout en sauvegardant les informations que je considère comme étant essentiel.

CERT :

Les flux RSS des CERT (Computer Emergency Response Teams) constituent une ressource inestimable pour la veille en cybersécurité. Ces fils d'information fournissent des mises à jour régulières sur les dernières vulnérabilités et menaces de cybersécurité, directement dans votre lecteur de flux. Personnellement, j'utilise Feedly, un outil de gestion de flux RSS robuste et intuitif. Il me permet de centraliser les flux de plusieurs CERT du monde entier, créant ainsi un hub d'information sur la cybersécurité.

Chaque matin, je commence ma journée en parcourant les dernières alertes et bulletins de sécurité. Cela me permet de rester informé des dernières tendances et menaces en matière de cybersécurité. De plus, Feedly offre la possibilité de personnaliser les alertes, ce qui me permet de filtrer les informations en fonction de leur pertinence pour ma recherche. Par exemple, si je mène une veille sur la maturité cyber des entreprises françaises, je peux configurer mon lecteur de flux pour recevoir des alertes sur les menaces spécifiques qui touchent les entreprises en France et dans le reste du monde, car avec la mondialisation une entreprise bloquée en inde peut entraîner des répercussions sur les supply chains d’entreprises françaises. Ainsi, je peux me concentrer sur les informations les plus pertinentes pour ma veille, optimisant ainsi mon temps et mes efforts.

Alors l’objectif n’est pas de présenter tous mes outils de veilles, mais d’en présenter certains.

État actuel de la maturité cyber des entreprises françaises

La maturité cyber des entreprises françaises est un sujet complexe et en constante évolution. Selon une étude récente intitulée "FORMATION OF BUSINESS ECOSYSTEMS AS A BASIS FOR THE DEVELOPMENT OF THE IT INDUSTRY[2]", la mondialisation moderne déplace l'attention des scientifiques des domaines de production traditionnels vers le domaine des services d'information et de communication. Pour les modèles d'affaires existants dans l'industrie de l'IT, les principales questions sont l'adaptation à la nouvelle main-d'œuvre et la justification des projets qui sont meilleurs d'un point de vue marketing et ceux qui sont meilleurs d'un point de vue d'optimisation du potentiel et de réalisation du retour sur investissement.

Figure 2 : statistique d'enntreprise francaise compilé depuis le rapport d'Hiscox[3]

Statistique	2021	2022	Variation
Entreprises ayant subi au moins une cyber-attaque	49%	52%	+3%
Entreprises ayant subi au moins une attaque par ransomware	14%	19%	+5%
Entreprises ayant souscrit à une cyber-assurance	57%	61%	+4%

[2] Stroiko, T., Voloshyna-Sidei, V., & Druz, Y. (2023). FORMATION OF BUSINESS ECOSYSTEMS AS A BASIS FOR THE DEVELOPMENT OF THE IT INDUSTRY. *Baltic Journal of Economic Studies*, *9*(1), 177-183. https://doi.org/10.30525/2256-0742/2023-9-1-177-183

[3] Hiscox rapport sur la gestion des cyber-risques 2022 https://www.hiscox.fr/courtage/sites/courtage/files/documents/2022%20Rapport%20Hiscox%20sur%20la%20gestion%20des%20cyber-risques_3.pdf

Victimes de ransomware ayant payé la rançon	65%	62%	-3%
Coût financier médian d'une cyber-attaque	16000€	15000€	-1000€
Part du budget informatique alloué à la cybersécurité	20%	22%	+2%

D'après le "Rapport Hiscox 2022 sur la gestion des cyber-risques", il semble que la maturité cyber des entreprises françaises soit un sujet en constante évolution. Les entreprises du secteur de la construction et des loisirs sont à l'autre extrémité du spectre : 53% des deux secteurs disposent d'une forme de couverture contre les cyber-risques. Les entreprises assurées sont plus susceptibles de répondre à une cyber-attaque en renforçant leurs défenses que les autres. Mais cela n'empeche pas la France d'avoir un record d'entreprise touché lors de la compagne de ransomware du groupe ESXIArgs

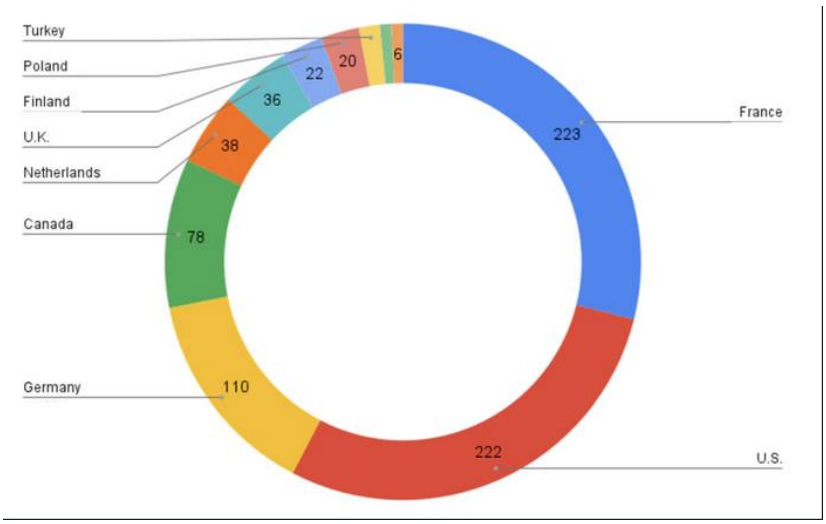


figure 3 : les pays les plus touché par l'attaques ESXIArgs. Données du 6 fevrier 2023, Shodan search engine

Après deux années de pandémie, et plusieurs vulnérabilités de grande ampleur, les entreprises semblent revenir aux fondamentaux. Elles mettent l'accent sur les menaces existantes (en veillant à

ce que les appareils soient dotés des correctifs adéquats et mis à jour), et s'assurent que les polices et procédures sont à jour, notamment en testant leurs plans de réponse aux incidents. Finalement, elles luttent contre les attaques de phishing (le principal mode d'intrusion des attaques par ransomware) en dispensant des formations à la cybersécurité au sein de l'entreprise.

Cependant, il est important de noter que les effets d'une cyberattaque vont bien au-delà des conséquences financières directes. Les entreprises découvrent qu'il y a un impact accru à tous les niveaux, y compris l'augmentation des frais de notification aux clients, l'impact sur l'image de marque et la réputation, la perte de clientèle, les difficultés accrues à attirer les clients, la menace à la solvabilité de l'entreprise, et la possibilité de devoir verser une amende importante.

En somme, la maturité cyber des entreprises françaises a fait des progrès significatifs, mais il reste encore du travail à faire. C'est un peu comme courir un marathon : on a parcouru une bonne distance, mais la ligne d'arrivée est encore loin. Alors, continuons à courir !

Mesure de la maturité cyber des entreprises

Les KPI

Pour bien mesurer l'évolution, il nous faut des indicateurs qui nous permettent d'évaluer cette fameuse, je catégorise ces indicateurs en deux catégories. La première est celle des données internes publiés par l'entreprise aux autorité compétentes (anssi, cnil en cas d'incidents), ou à leurs partenaires économiques. Voici la liste des indicateurs avec une petites description :

- Incident Response Time : Le temps nécessaire pour répondre à un incident de sécurité.
- Patch management Efficiency : Le temps nécessaire pour appliquer les correctifs de sécurité après leur publication.
- User Awareness Training Completion : Le pourcentage d'employés formé et sensibilisé à la sécurité (attention : un employé formé et sensibilisé ne veut pas dire qu'il suit les directives)
- Phishing Test : Le pourcentage d'employé qui signalent les mails de phishing, et ceux qui réponde aux mails de phishing
- Security audit result : Les résultats d'audit de sécurité qu'ils soit interne ou externe
- Number of Unresolved Sercurity Vulnerabilities : Le nombre de vulnérabilité non résolues dans l'infrastrucuture de l'entreprise
- Backup and Recovery Rate : Le pourcentage de succès des opérations de sauvgarde et de récupération.

Pour les KPI Publique voici une liste avec une description la aussi :

- DNS Health Check : Vérification de la santé du DNS, y compris la configuration, la propagation et les erreurs potentielles.
- SSL/TLS Certificate Check : Vérification de la validité du certificat SSL/TLS, y compris la date d'expiration et la force du chiffrement.
- Domain Reputation : Évaluation de la réputation du domaine basée sur diverses sources, y compris les listes noires et les rapports de spam.
- Email Security Check : Vérification de la mise en œuvre de protocoles de sécurité des e-mails tels que SPF, DKIM et DMARC.

- Website Security Check : Vérification de la sécurité du site web, y compris la présence de logiciels malveillants, de vulnérabilités connues et de problèmes de configuration.
- Public Data Breaches : Vérification des violations de données publiques associées à l'entreprise.
- IP Reputation : Évaluation de la réputation des adresses IP associées à l'entreprise

L’analyse active :

Afin de pouvoir donc évaluer les données publiques des enntreprises, je me suis permis de modéliser une base de données qui serait alimenter par des scripts de monitoring et de web scrapping.
En utilisant la base de données et en récoltant le maximum d’information sur l’entreprise je serais ainsi donc dans la capacité de données une note globale à l’entreprises sur sa maturité cyber.

En effet une chose aussi simple qu’une configuration dns peut rendre indisponible le site ou les applications de l’entreprises donc lui causer des dommages immédiats. Sans parler du faite qu’une mauvaise configuration dns peut elle donnée une mauvaise réputation des serveurs mails de l’entreprises et finir dans les spams de chaque providers mail.

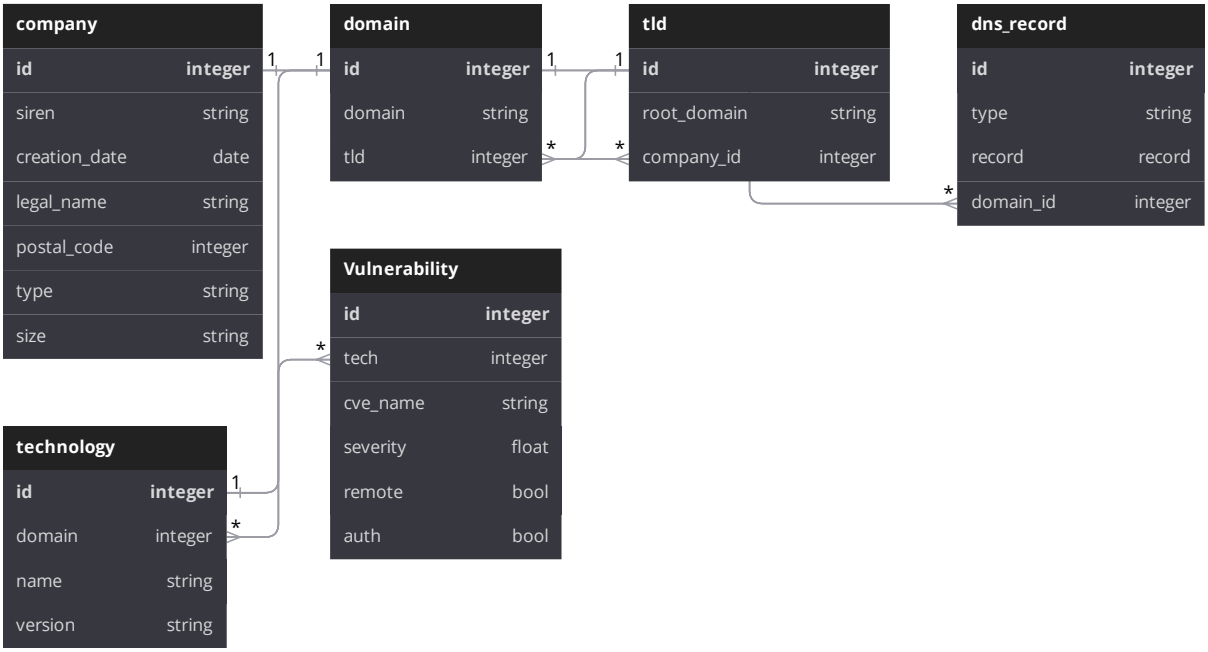


Figure 4 : Modélisation de la base de données utilisé pendant ma veille.

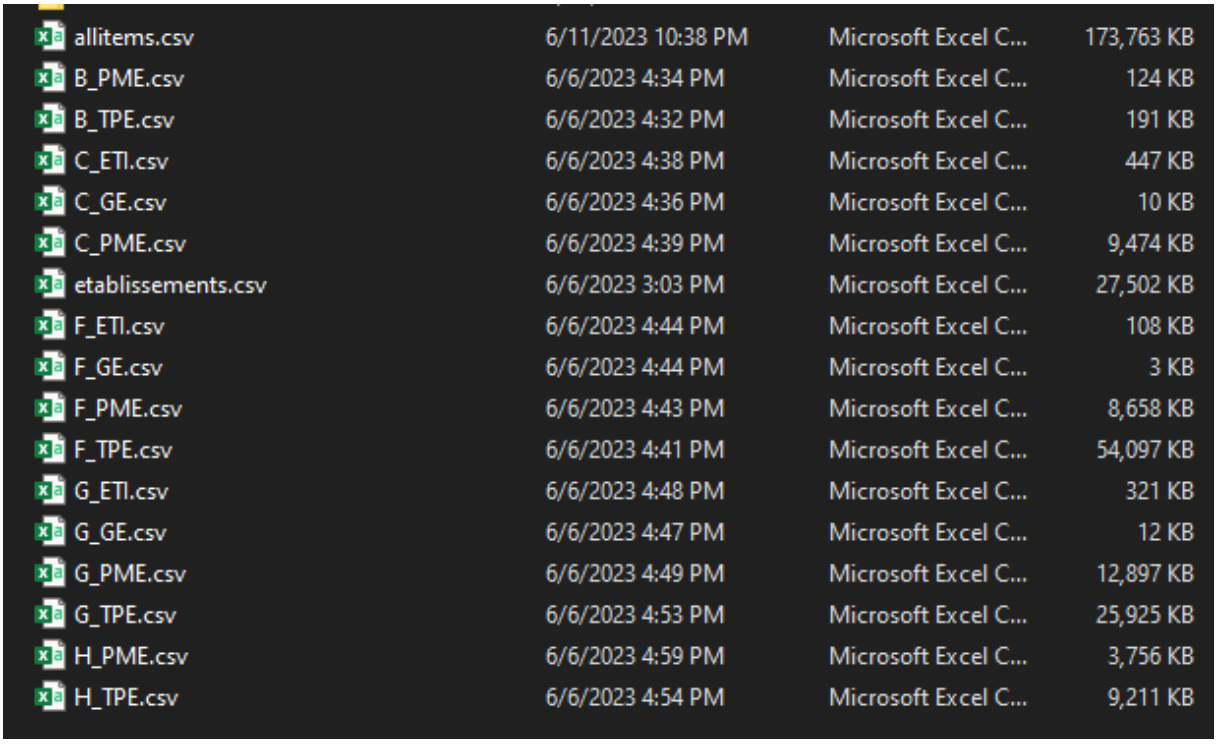
Pour les outils j'utilise pour l'instant deux langage différents, javascript et python. Le javascript est un langage qui me permet de facilement faire du web scrapping avec l'utilisation de la librairie Wappalyzer nous permet d'avoir les librairies et les technologies utilisé ainsi que leurs versions. Pour la partie vulnérabilité, c'est une fois que le scan de Wappalyzer fait, que l'on va chercher sur le site cve.org qui ressence toutes les vulnérabilités qui existe.
Après cela mon script python lui vas regarder pour chaque cve qui se trouve dans la base de données, si un poc existe pour celle-ci sur un repo github [4]. Le github recessent tout les poc pour chaque cve publique qui se trouve sur internet, celui-ci est maintenue et alimenté principalement par la communauté et aussi par l'entreprise qui le produit trickest[5].

Pour la finalité, j'ai un autre script python qui vas me faire des statistiques selon les paramètres que j'aurais prédéfinis, grâce aux librairies numpy, et pandas.

[4] https://github.com/trickest/cve
[5] https://trickest.com c'est une entreprise spécialisé dans le threat hunting

Source de données :

Il est bien beau de vouloir scanner des entreprise mais il faudrait déjà avoir la liste des entreprise et leurs catégorie afin de pouvoir les scanner et surtout leurs donné un score. Si vous avez eu le temps de lire la modélisation de la base de donnée, la table **company** possède une entré siren car pour trouver les entreprise je fais un extracte du site sirene.fr qui est un site gouvernementale qui ressence tout les entreprises par différents paramatre tel que la taille, l'industrie, ect …



allitems.csv	6/11/2023 10:38 PM	Microsoft Excel C...	173,763 KB
B_PME.csv	6/6/2023 4:34 PM	Microsoft Excel C...	124 KB
B_TPE.csv	6/6/2023 4:32 PM	Microsoft Excel C...	191 KB
C_ETI.csv	6/6/2023 4:38 PM	Microsoft Excel C...	447 KB
C_GE.csv	6/6/2023 4:36 PM	Microsoft Excel C...	10 KB
C_PME.csv	6/6/2023 4:39 PM	Microsoft Excel C...	9,474 KB
etablissements.csv	6/6/2023 3:03 PM	Microsoft Excel C...	27,502 KB
F_ETI.csv	6/6/2023 4:44 PM	Microsoft Excel C...	108 KB
F_GE.csv	6/6/2023 4:44 PM	Microsoft Excel C...	3 KB
F_PME.csv	6/6/2023 4:43 PM	Microsoft Excel C...	8,658 KB
F_TPE.csv	6/6/2023 4:41 PM	Microsoft Excel C...	54,097 KB
G_ETI.csv	6/6/2023 4:48 PM	Microsoft Excel C...	321 KB
G_GE.csv	6/6/2023 4:47 PM	Microsoft Excel C...	12 KB
G_PME.csv	6/6/2023 4:49 PM	Microsoft Excel C...	12,897 KB
G_TPE.csv	6/6/2023 4:53 PM	Microsoft Excel C...	25,925 KB
H_PME.csv	6/6/2023 4:59 PM	Microsoft Excel C...	3,756 KB
H_TPE.csv	6/6/2023 4:54 PM	Microsoft Excel C...	9,211 KB

Figure 5 : dossier data qui répertorie une partie des extraits au format csv

La première lettre représente l'industrie, et les lettres qui suivent le tiret du bas, elle représente la taille de l'entreprise (TPE, PME, ect …)

Après avoir analyser au moins 300 entreprises pour chaque type et catégories avec des limites sur les grands groupes car il n'y en as pas tant que ça en France. Le choix du nombres 300 est arbitraire et il

me faudrait plus de recherche pour avoir un nombre parfait qui me permettrait d'avoir un échantillon statistique viable.

Problématique :

L'utilisation de Wappalyzer à grande échelle est entravée par des problèmes de bande passante et par des solutions de protection web comme Cloudflare.

La bande passante peut devenir un goulot d'étranglement lors de l'analyse d'un grand nombre de sites web. Cela peut ralentir le processus et rendre difficile l'obtention de résultats en temps réel. De plus, des solutions comme Cloudflare peuvent bloquer les tentatives d'analyse automatisée, considérant ces activités comme potentiellement malveillantes.

Face à ces défis, plusieurs solutions peuvent être envisagées :

1. **Utilisation d'un service proxy** : Les services proxy peuvent aider à contourner les restrictions de bande passante et à éviter le blocage par des solutions comme Cloudflare. Cependant, ils peuvent être coûteux et leur utilisation doit être conforme aux lois et réglementations en vigueur.
2. **Rate Limiting** : Il s'agit de limiter le nombre de requêtes envoyées par unité de temps. Cela peut aider à éviter d'être bloqué par des solutions comme Cloudflare, mais cela peut également ralentir le processus de collecte de données.
3. **Utilisation d'APIs publiques** : Certaines informations peuvent être obtenues via des APIs publiques, qui sont souvent plus tolérantes à l'égard des requêtes automatisées. Cependant, toutes les informations nécessaires peuvent ne pas être disponibles via des APIs.
4. **Collaboration avec les entreprises** : Dans certains cas, il peut être possible de travailler directement avec les entreprises pour obtenir les informations nécessaires. Cela peut nécessiter des accords de confidentialité et d'autres arrangements formels.

Il est important de noter que la collecte de données publiques doit toujours être effectuée de manière éthique et en conformité avec toutes les lois et réglementations applicables.

Quel futur :

Risques :

D'après le document "Identifying Emerging Cyber Security Threats and Challenges for 2030" publié par l'ENISA en mars 2023, il est clair que les menaces et défis en matière de cybersécurité évoluent constamment. Les menaces identifiées dans ce rapport couvrent un large éventail de sujets, dont beaucoup sont déjà pertinents aujourd'hui. Cependant, ces menaces ne resteront pas statiques, mais évolueront et se complexifieront en raison de l'augmentation des dépendances et du développement de nouvelles technologies.

Pour anticiper ces menaces futures, il est crucial de ne pas retarder les actions qui aident à éviter et à atténuer les risques futurs. Cela signifie qu'il faut constamment anticiper les menaces à venir. Cependant, ces mesures supplémentaires ne doivent pas se faire au détriment des contrôles de cybersécurité nécessaires et de grande portée, tels que l'éducation, la sensibilisation, le patching, etc.

En ce qui concerne les recommandations pour prévenir ces risques, il est essentiel de reconnaître les changements dans le paysage des menaces et de commencer dès maintenant à préparer des mesures pour assurer la sécurité et la résilience face à ces menaces en évolution. Cela peut impliquer des investissements dans la formation en cybersécurité, l'élaboration de politiques de sécurité claires, et le développement de capacités pour répondre rapidement et efficacement aux incidents de sécurité.

Il est également important de noter que les menaces futures ne seront pas isolées, mais interconnectées. Par conséquent, une approche holistique de la cybersécurité sera nécessaire, qui tient compte de l'ensemble du paysage des menaces et des défis. Cela peut impliquer une

collaboration plus étroite entre les différents acteurs de la cybersécurité, y compris les entreprises, les gouvernements, et les organisations de recherche.

Maturité cyber :

En regardant vers l'avenir, on peut s'attendre à ce que la maturité cyber des entreprises françaises continue de s'améliorer. Les entreprises sont de plus en plus conscientes de l'importance de la cybersécurité et investissent davantage dans des mesures de protection. Cela est dû en partie à une augmentation des cyberattaques, qui ont souligné la nécessité d'une sécurité robuste.

Cependant, il est important de noter que la maturité cyber ne se limite pas à la mise en place de mesures de sécurité. Elle englobe également la formation des employés, la mise en place de politiques de sécurité claires, et la capacité à répondre rapidement et efficacement aux incidents de sécurité. À cet égard, il y a encore beaucoup de travail à faire. De nombreuses entreprises manquent encore de personnel formé en cybersécurité, et les politiques de sécurité sont souvent mal comprises ou mal appliquées.

En outre, le paysage des cybermenaces continue d'évoluer, avec l'apparition de nouvelles formes d'attaques. Cela signifie que les entreprises doivent constamment mettre à jour leurs stratégies de sécurité pour rester à jour. Les entreprises qui ne le font pas risquent de se retrouver en retard, même si elles étaient auparavant considérées comme ayant une maturité cyber élevée.

En conclusion, bien que la maturité cyber des entreprises françaises soit en voie d'amélioration, il reste encore beaucoup à faire. Les entreprises doivent s'engager dans une amélioration continue de leur maturité cyber, en veillant à ce que tous les aspects de la cybersécurité soient pris en compte.

Etapes suivante :

Mon étape suivante sera de trouver une façon de scanner avec wappalyzer sans me faire bloquer par les protections tel que cloudflare. Aussi il me faut avancer et perfectionner la partie statistique de ma veille, sans parler du fait de faire une révision des critères utilisé pour noter la maturité cyber de l'entreprise.

Conclusion

En conclusion, la maturité cyber des entreprises françaises est un sujet complexe et en constante évolution. Les entreprises ont fait des progrès significatifs dans ce domaine, mais il reste encore énormément de points à améliorer. Les menaces futures en matière de cybersécurité seront de plus en plus complexes et interconnectées, nécessitant une approche holistique de la cybersécurité. Les entreprises doivent donc rester vigilantes, investir dans la formation et les technologies de sécurité, et adopter une approche proactive pour anticiper et atténuer les menaces futures. En fin de compte, la maturité cyber n'est pas une destination, mais un voyage continu d'amélioration et d'adaptation aux nouvelles réalités de notre monde numérique.