SYNTHÈSE DE LA MISE EN OEUVRE DE LA VEILLE

VEILLE INFORMATIONNELLE

RÉALISÉ PAR

HUGO JACQUEL

Sup Alta
Lyon

2023
BTS SIO 2

Table des matières

1 Présentation du sujet de la veille informationelle & Intérêt de la veille

Sujet de veille : Comment garantir la sécurité des logiciels dans un environnement numérique de plus en plus menaçant ?

Cette veille informationelle est **formel** et **active**. Elle est réaliser dans le but de répertorier un ensemble de **bonnes pratiques / référentiel** et de faire un **partage de connaissance pour notre entreprise** dans le but de former les différents salariés sur les risques en cybersécurité ?

1.1 Mise en oeuvre

1.1.1 Délimitation les besoins

Les informations de cette veille seront délimiter sur une partie des techniques d'attaques les plus communes dans le développement logiciel (progiciel)

1.1.2 Fixer le temps et le budget

La veille est fixé sur **2 semaines** avec un budget de dépense de **0 €**

1.1.3 Cerner les thèmes

Les thèmes de la veilles seront :

- **Explication** des différentes attaques en informatiques
- **Comprendre l'impact** des attaques sur le SI de l'entreprise
- **Appliquer des solutions** pour sécuriser les différents vecteurs d'attaques

1.1.4 Délimitation du type d'information recherché

Il n'y a pas de délimitation sur le type d'information recherché par cette veille, on souhaite se focaliser sur des attaques et risques assez récent (après 2017) **tout en comparant avec les attaques avant 2017 pour dresser un schéma graphique de réflexion pour visualiser le futur des attaques sur le SI des entreprises / anticiper les évolutions**

2 Outils de veille

2.1 1) Phase de collection

La phase de collection des données se déroule sur deux types de méthode de collection :

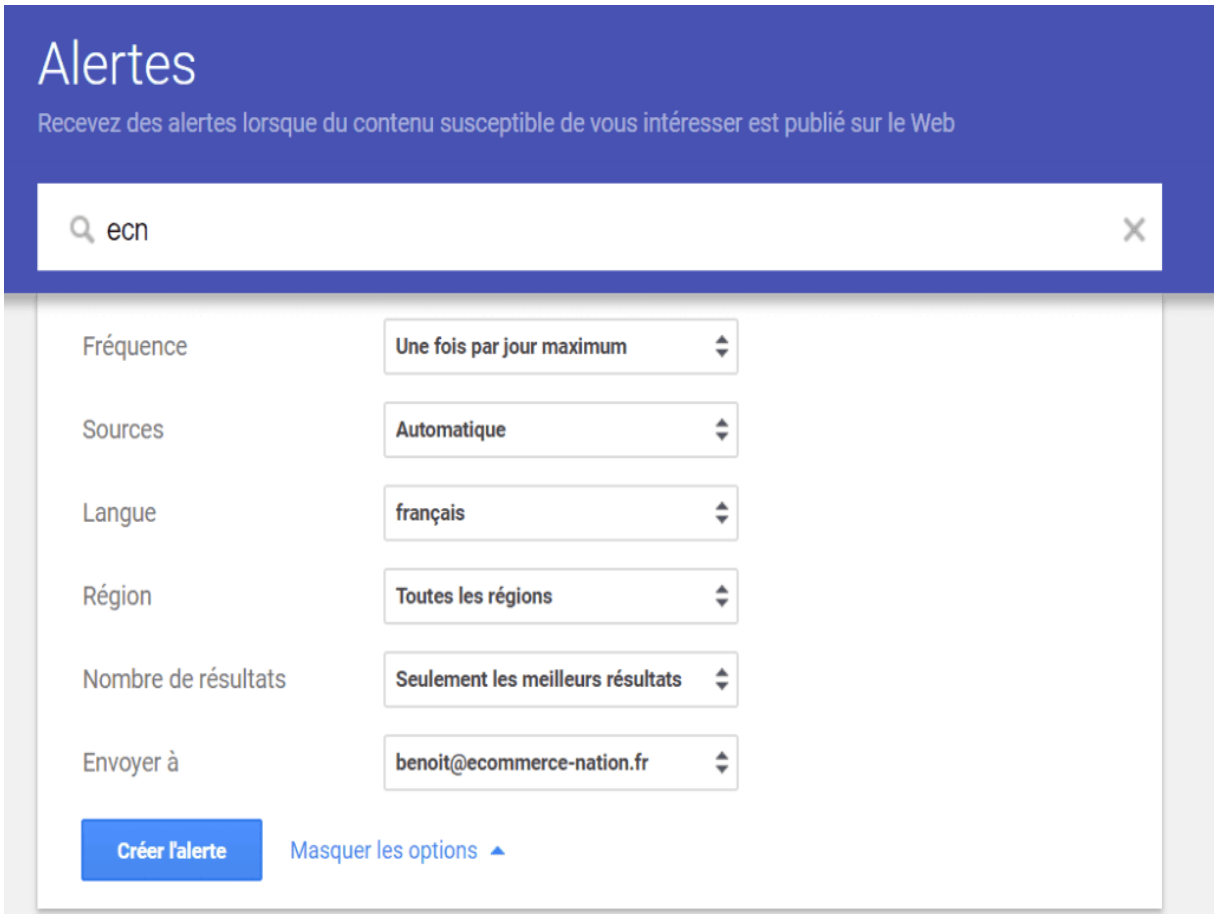
- **Méhtodes PUSH** : Information **poussé de manière automatique** vers le chercheur en fonction de ses préférences et critères préétablis.

- **Méthodes PULL** : le veilleur obtient les informations de manière manuelle en faisant des recherches (il n'y a pas d'information qui vient à lui, **il va à la recherche des informations**)

2.1.1 Méthodes PUSH

Alertes Google

Google Alerts permet de créer des alertes personnalisées pour surveiller des mots-clés spécifiques liés à la cybersécurité. On reçoit des notifications par e-mail lorsque de nouvelles informations correspondant à vos critères sont publiées en ligne.



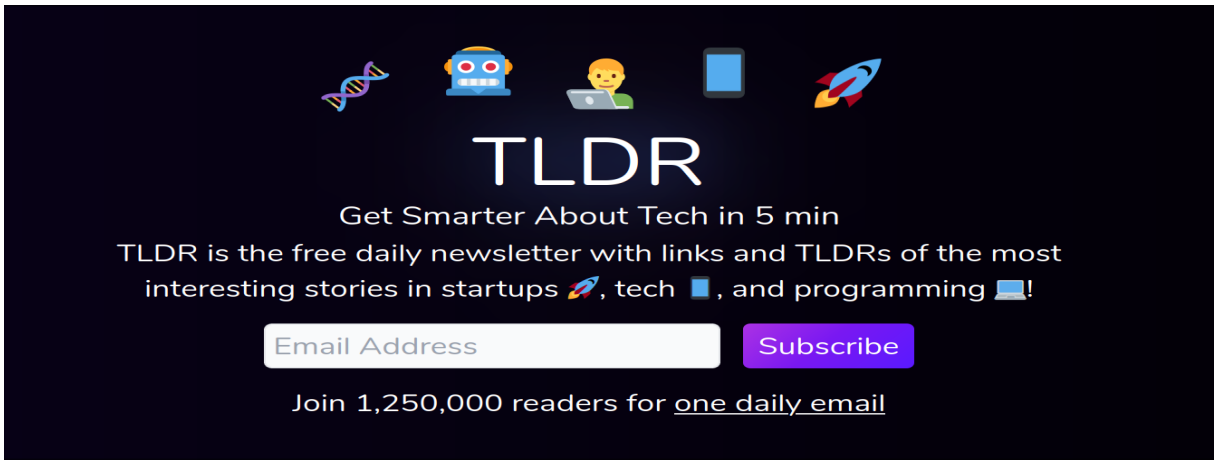
Flux RSS

On peut s'abonner à des **flux RSS** de sites web, de blogs ou de publications de sécurité pour **recevoir automatiquement** les dernières mises à jour via un lecteur RSS. Ils existent des agrégateurs de flux RSS tels que Feedly ou Inoreader peuvent aider à organiser et à suivre des flux particuliers (sous formes de catégories et sous catégories) pour notre veille

Notifications d'organisations / applications de sécurité

De nombreuses organisations et applications de sécurité, comme **CERT (Computer Emergency Response Team)**, publient des **bulletins d'alerte** et **des mises à jour sur les menaces et les vulnérabilités**. On peut s'abonner à leurs newsletters ou leurs alertes pour être informé en temps réel. Ces notifications peuvent être **centralisés** dans un espace de données pour **facilité**. Les plateformes de renseignement sur les menaces comme ThreatConnect, ThreatQuotient, ou Anomali peuvent être configurées pour collecter, agréger et diffuser automatiquement des informations sur les menaces de cybersécurité.

Newsletter spécialisés



Similairement au notifications d'organisations, les newsletter spécialisés comme **TLDR**, permettent de recevoir les informations utile sur de la **veille technologique**. L'intérêt de ces newsletter et de trier les informations et de résumés de manière **synthétique**.

L'avantage des newsletters et que le reçu d'information est **fréquent** permettant ainsi de faire une **veille active** et de pouvoir retrouver **facilement les sources** pour approfondir les recherches manuellement (Méthode **PULL**).

Ici pour **TLDR**, la newsletter envoie un **mail chaque jour** :

TLDR Boîte de réception OpenAI explores AI chips 🤖, Apple discussed ditching Google 🔍, how computers tell time ⏰ - //tldr.tech/signup?utm_source=tl... 6 oct.
TLDR Boîte de réception Apple NameDrop 📱, OpenAI's residency program 🤖, how Pixel upgraded cameras 📷 - //tldr.tech/signup?utm_source=tldr]Hire ... 5 oct.
TLDR Boîte de réception Amazon's secret price algo 📈, SpaceX's laser-enabled satellites 🛰️, safe Postgres migrations 👩‍💻 - //tldr.tech/signup?utm_sourc... 4 oct.
TLDR Boîte de réception Chromebook Plus 💻, inside Flexport's CEO ousting 🚢, understanding unicode 👩‍💻 - //tldr.tech/signup?utm_source=tldr]Hire [https://sh... 3 oct.
TLDR Boîte de réception Galaxy S24 leaks 📱, Apple's Formula 1 bid 🏎️, Excel for Python AMA 👩‍💻 - //tldr.tech/signup?utm_source=tldr]Hire [https://share.hs... 2 oct.
TLDR Boîte de réception Jony Ive's iPhone of AI 📱, Microsoft considered selling Bing 🔍, big tech vs startup jobs 👩‍💻 - //tldr.tech/signup?utm_source=tldr]... 29 sept.
TLDR Boîte de réception OpenAI's AI hardware 🤖, Meta's smart glasses 🕶️, Zuckerberg on AI & metaverse 🧑 - //tldr.tech/signup?utm_source=tldr]Hire [h... 28 sept.
TLDR Boîte de réception OpenAI seeks $90B valuation 🏦, Microsoft bets on nuclear ⚡, rise of cloud dev environments 👩‍💻 - //tldr.tech/signup?utm_sourc... 27 sept.
TLDR Boîte de réception ChatGPT vision & audio 🤖, Spotify's AI voice cloning 🗣️, pod living in SF 🚡 - //tldr.tech/signup?utm_source=tldr]Hire [https://sha... 26 sept.
TLDR Boîte de réception Tesla's robot demo 🤖, Pixel 8 camera features 📱, building engineering strategy 👩‍💻 - //tldr.tech/signup?utm_source=tldr]Hire [ht... 25 sept.
TLDR Boîte de réception Apple's sports strategy ⚽, the end of obesity 📉, engineering metrics 👩‍💻 - //tldr.tech/signup?utm_source=tldr]Hire [https://share.... 22 sept.
TLDR Boîte de réception OpenAI's DALL-E 3 🖼️, Apple scraps stock trading plans 🏦, AI UX of the future 🤖 - //tldr.tech/signup?utm_source=tldr]Hire [http... 21 sept.
TLDR Boîte de réception Neuralink human trials 🧠, Google Bard Extensions 🤖, a modern CSS reset 👩‍💻 - //tldr.tech/signup?utm_source=tldr]Hire [https://s... 20 sept.
TLDR Boîte de réception iOS 17 launch 📱, geometric AI art 🖼️, MongoDB's new query engine 👩‍💻 - //tldr.tech/signup?utm_source=tldr]Hire [https://share.hs... 19 sept.
TLDR Boîte de réception iPhone 15 gaming 📱, inside Google's antitrust fight ⚖️, Vercel's AI for React 👩‍💻 - //tldr.tech/signup?utm_source=tldr]Hire [https://... 18 sept.

APIs de réseaux sociaux , médias, plateformes

Ils existent aussi des **plateformes de renseignement sur les menaces** comme ThreatConnect, ThreatQuotient ou Anomali offrent des APIs qui permettent de suivre automatiquement des comptes ou des mots-clés liés à la **cybersécurité** par exemple. On peut appliquer l'appels d'APIs également avec les réseaux sociaux.

2.1.2 Méthodes PULL

Similairement aux méthode PUSH , il existe les méthodes PULL en faisant **les recherches soi-même manuellement**

Recherche Internet

Utiliser des moteurs de recherche, des forums spécialisés, des blogs de sécurité et des sites web d'organisations de sécurité pour rechercher des informations pertinentes. On peut utiliser des requêtes spécifiques pour cibler des sujets particuliers (notamment avec **Google Dork**). De manière général, toute forme de **flux d'information digital** permet de faire de la veille via **méthode PULL** : **forums , communautés en ligne, conférences, webinaires, réseaux sociaux**.

Mais aussi :

Abonnements aux newsletters digital et physique

- **Analyse de rapports de sécurité** : Lisez des rapports de sécurité publiés par des entreprises de sécurité, des gouvernements et d'autres organisations pour comprendre les menaces émergentes.

- **Forums de diffusion de vulnérabilités (VDB)** : Consultez des VDB comme CVE (Common Vulnerabilities and Exposures) pour rechercher des détails sur les vulnérabilités récentes.

- **Analyse de codes sources** : Si vous avez des compétences techniques, examinez le code source des logiciels et des systèmes pour identifier des vulnérabilités potentielles.

- **Participation à des groupes de travail et des associations** : Rejoignez des groupes de travail, des associations professionnelles et des comités liés à la cybersécurité pour partager des informations avec d'autres professionnels.

2.1.3 Outils multiple pour automatiser la veille

:

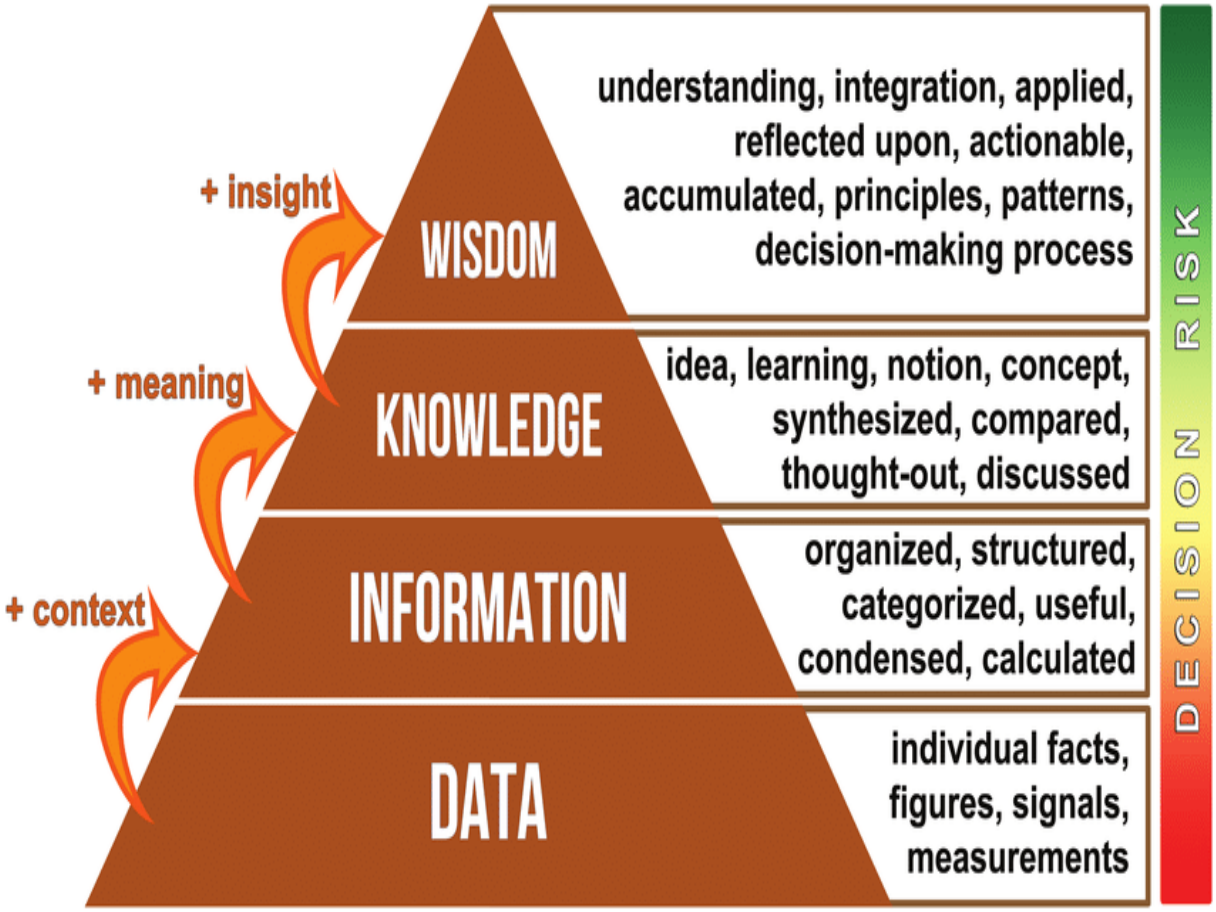
IFTTT

IFTTT vous permet d'automatiser une partie de votre veille. Cet outil repose sur la programmation de microapplications qui vont effectuer une action de manière automatique. Dit comme cela, ça semble compliqué, mais rassurez, c'est très simple !

L'acronyme IFTTT signifie : IF This Then That. Autrement dit : s'il se passe telle chose, il faut réaliser telle action.

2.2 2) Phase de qualification du contenu

La phase de **qualification du contenu** est essentiel car elle permet de transformer **la donnée** en **information** grâce à des systèmes de **contextuelisation** notamment avec des **tags/catégories** mais aussi grâce à des **situations**.



Transformation de la **donnée brute** en **information** grâce à la contextualisation.

Il faut **organiser et qualifier** les **informations de sa veille** en fonction de la rationalisation de la veille. Elle peut être pour but :

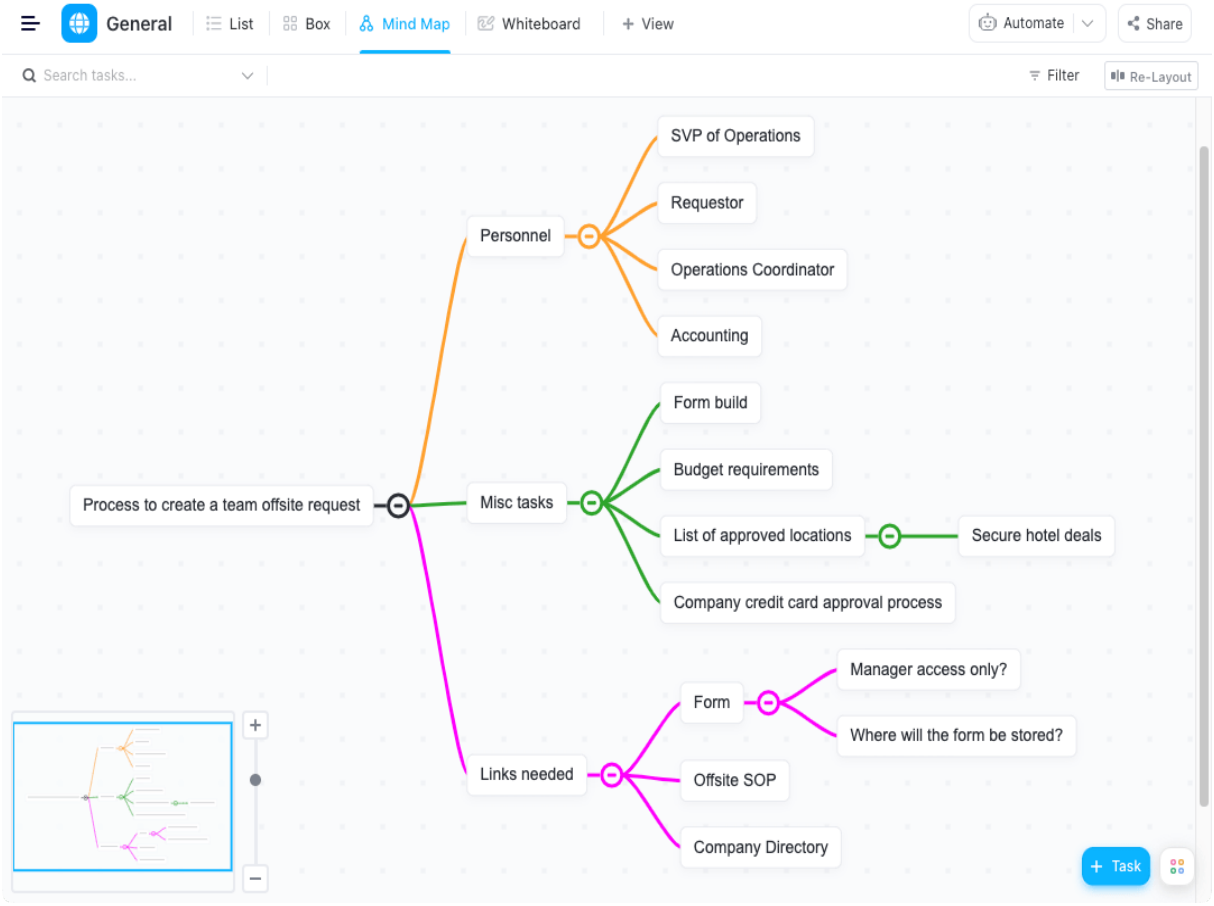
- **économique**
- de **production**
- de **management**
- **légales**
- **organisationnel**
- **préventives**

L'objectif final de la qualification des informations est d'organisation **un processus de manière à accroître l'éfficacité et l'intéret de la veille**.

2.3 3) Phase d'organisation du contenu et de réalisation de veille

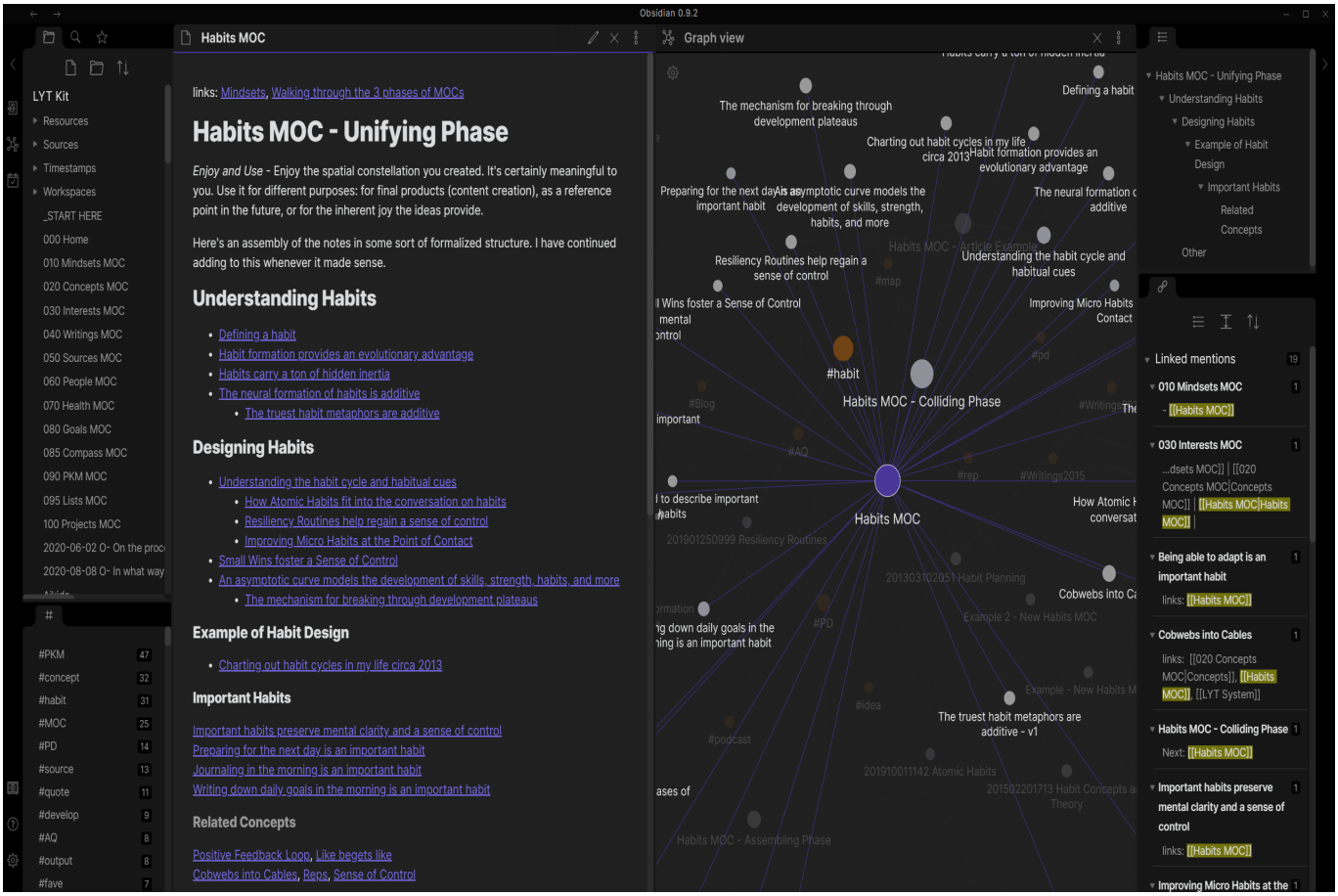
Après la phase de qualification des données , il faut les **organiser** en **idées** et en les **contextualiser**.

Pour faciliter l'organisation des idées, on peut utiliser un **logiciel de MindMapping** et de **prise de note** comme **Obsidian ou Notion** par exemple.



Carte mental : Méthode de visualisation d'idée et de notions par système de catégorie codifées par des couleurs.

2.3.1 Obsidian : Logiciel de prise de note



Obsidian : Logiciel de prise de note en **Markdown** pour faciliter **l'organisation** et le **lien** entre les notes permettant de réaliser une veille **éfficacement**

Obsidian permet de créer des notes en Markdown est permet de faire de la mise en page et du lien d'idée facilement grâce à son **système de noeuds** et de **catégories**.

A l'aide de nombreux **plugins** disponible sur la plateforme, il est possible de transformer Obsidian en **véritable logiciel d'organisation** grâce notamment :

- **Calendar** : Un calendrier connecté au **vault Obsidian** qui permet d'assigner des tâches à des jours dans le calendrier et de le **synchroniser** à un **agenda client** (Google Agenda, Outlook, etc)

- **Kanban** : Création d'un Kanban permettant **l'organisation des tâches lié à la veille** pour s'y retrouver plus facilement et de manière organiser et **rigoureuse**

- **Excalidraw** : Permet de créer des **dessins** et des **diagrammes** pour **organiser** ou **schématiser** une idée / un concept.

- **Mindmap et autre** : Permet de transformer les notes en autres type de structure de données : **carte mental, pictoleçons, fichier PDF résumé, etc**

Pour résumé Obsidian permet de :

- **Organisation des informations** : Permet de créer une base de données de notes **interconnectées**. Organisations des informations sur la cybersécurité en créant des notes pour chaque **concept, technologie, tendance ou événement pertinent**.

- **Liens entre les idées** : L'une des caractéristiques clés d'Obsidian est la possibilité d'établir des liens entre vos notes. Création de liens pour montrer les relations entre différents concepts de cybersécurité, ce qui peut aider à mieux comprendre les **implications** et les **connexions**.

- **Mindmapping dynamique** : Création des **cartes mentales dynamiques** en reliant des notes et des idées à l'aide de liens. Cela permet la visualisation et de navigation facilement dans notre corpus de connaissances sur la cybersécurité.

- **Recherche et exploration** : Obsidian dispose d'une fonction de recherche puissante qui vous permet de retrouver rapidement des informations pertinentes. Vous pouvez rechercher des mots-clés, des tags ou des relations entre les notes pour accéder aux données dont vous avez besoin.

- **Gestion des tâches** : Vous pouvez utiliser Obsidian pour créer des listes de tâches liées à votre veille technologique en cybersécurité. Les tâches peuvent être associées à des notes spécifiques pour un suivi facile.

- **Annotation et résumé** : Anotation et résumé des articles, des rapports ou d'autres ressources pertinentes directement dans Obsidian. Cela vous permet de capturer les informations essentielles et de les relier à vos notes existantes.

- **Intégration de flux RSS** : Obsidian peut être configuré pour importer automatiquement des articles et des informations de ces sources. Vous pouvez ensuite organiser et analyser ces informations dans Obsidian.

2.4 4) Phase de partage ou d'utilisation

Pour finir, la phase de **partage et d'utilisation** détermine comment la **veille** et ses **informations catégorisés** sont utilisé.

Dans notre cas on souhaite **informer** le plus de personnes sur les différents risques lié aux **attaques logiciel**. Pour le partage, on peut privilégier des **présentation powerpoint**, **diffusion de webinar** et formation des **salariés**.

Cette veille peut aussi servir à n'importe qu'elle personne **qui s'intéresse au sujet** et **souhaite voir les perspectives d'avenir sur les attaques en cybersécurité** tout en comprenant celles d'actualité.