BTS SIO - Epreuve E5

Mettre en œuvre des outils et stratégies de veille informationnelle

Rédacteur(s)	Version	Date	Nb pages
robin.reinbold-antenat@ccicampus.fr	1.1	28/04/2025	16

SHADOW IT

SOMMAIRE

1 Introduction

La veille est une activité qui consiste à surveiller en permanence les évolutions dans un domaine particulier (technologique, économique, concurrentiel, juridique, etc…) pour collecter, analyser et exploiter des informations utiles. En gros, c'est rester informé de tout ce qui peut avoir un impact sur un secteur, un métier ou une entreprise.

Les objectifs de la veille sont :

- Anticiper les nouveautés et les évolutions
- Détecter les risques et les opportunités
- S'adapter rapidement aux changements Innover en s'inspirant des tendances
- Innover en s'inspirant des tendances
- Prendre de meilleures décisions basées sur des faits récents

Pour rester compétitive et agile face aux évolutions rapides de son environnement, une organisation doit mettre en place différents types de veille, chacun répondant à un objectif spécifique comme :

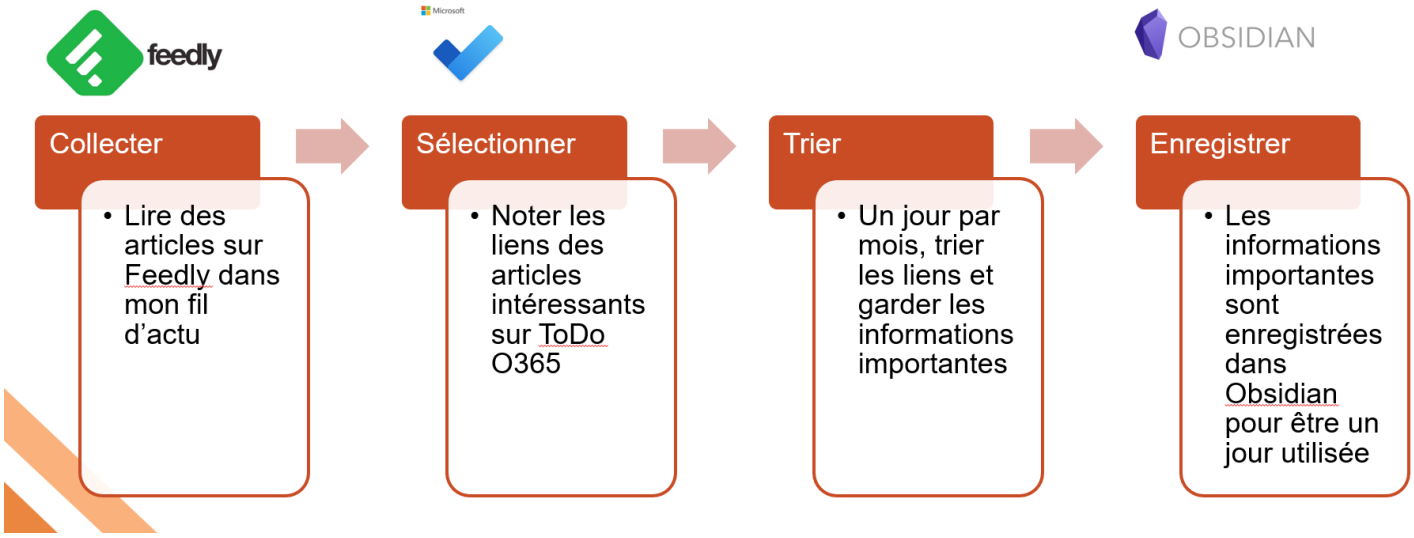
- Veille technologique : surveiller les innovations et avancées techniques
- Veille concurrentielle : observer ce que font ses concurrents
- Veille stratégique : comprendre les grandes tendances de son marché
- Veille réglementaire : suivre les évolutions légales et normatives
- Veille commerciale : repérer de nouveaux marchés ou besoins

Faire de la veille dans son métier permet de se tenir informé des évolutions de son secteur, de développer ses compétences et de s'adapter aux changements. Dans un monde professionnel en constante évolution, la veille est indispensable pour anticiper les risques, repérer les opportunités et innover. Elle offre la capacité de prendre de meilleures décisions et de progresser, tout en apportant de la valeur ajoutée à l'entreprise.

Dans le domaine de l'informatique, la veille technologique est essentielle car les technologies évoluent extrêmement vite : nouvelles architectures, nouveaux langages, nouvelles menaces de cybersécurité, nouvelles réglementations. Sans une veille constante, un professionnel risque de voir ses compétences devenir obsolètes rapidement.
La veille technologique permet donc de rester à jour, de proposer des solutions modernes et performantes, de se protéger contre les nouvelles cybermenaces et d'innover.

2 Ma méthodologie de veille

2.1 Le processus



Etape 1 : Collecter des informations pertinentes. Pour cela, j'utilise deux outils principaux : Feedly, pour suivre facilement l'actualité technologique sur des flux spécialisés, et Google Alerts, où j'ai défini des mots-clés précis comme "Shadow IT", "BYOD risques", ou encore "sécurité des données SaaS". Ces outils permettent de recevoir directement des articles récents et des analyses pertinentes. La consultation se fait de manière régulière, soit quotidiennement soit quelques fois par semaine, afin de ne rien manquer d'important.

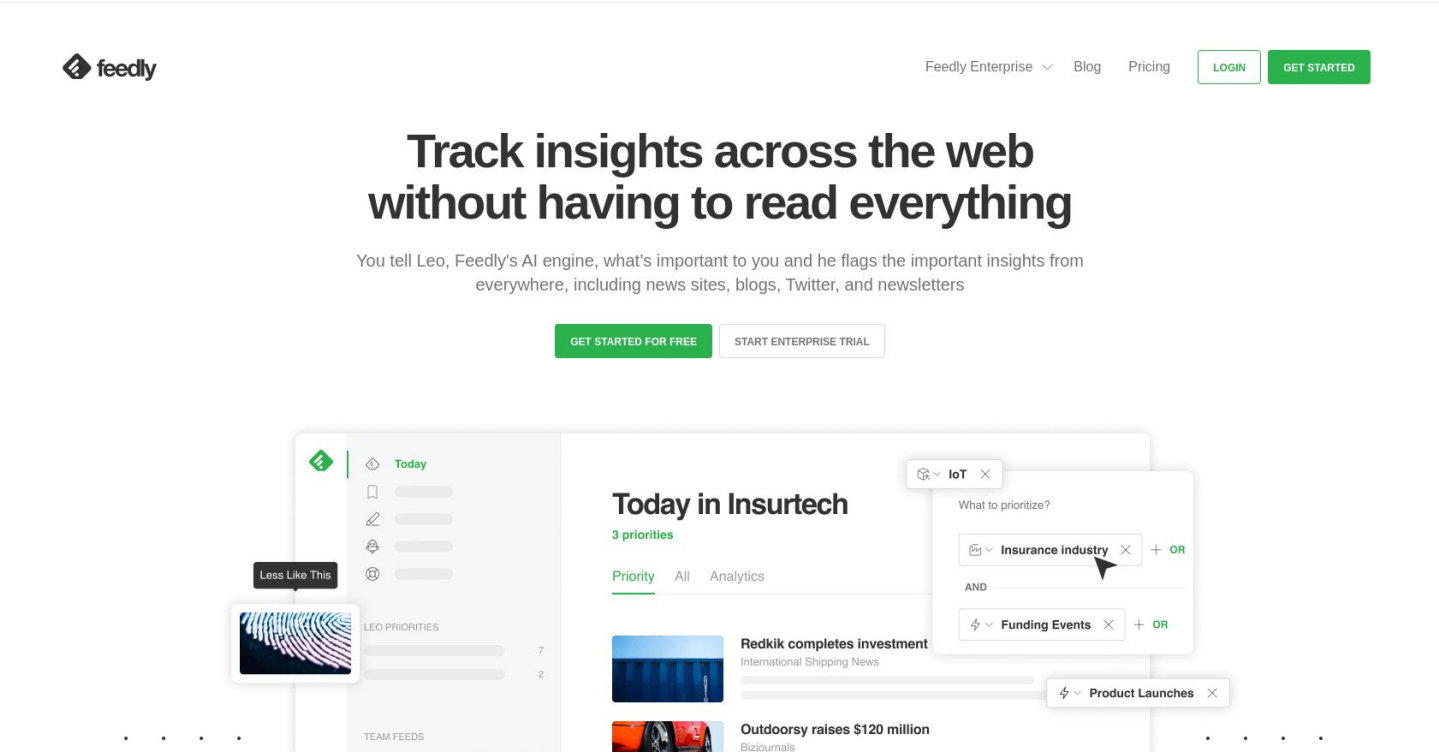
Etape 2 : Après avoir collecté les informations, il est nécessaire de faire une première sélection. Chaque fois qu'un article semble intéressant ou qu'il aborde un aspect nouveau du Shadow IT, je note son lien directement dans Microsoft ToDo. Cet outil me permet d'organiser les articles sous forme de liste et de les retrouver facilement plus tard. À cette étape, je me concentre uniquement sur les ressources qui semblent enrichir ma compréhension ou qui pourraient avoir une utilité future.

Etape 3 : Une fois par mois je prends le temps de revenir sur tous les liens sauvegardés dans Microsoft ToDo. Durant ce tri j'analyse le contenu des articles et je sélectionne uniquement les informations les plus pertinentes : les grandes tendances, les évolutions marquantes, les risques identifiés ou les solutions innovantes. Ce tri est essentiel pour ne conserver que des données de qualité et construire une veille vraiment utile et exploitable.

Etape 4 : Enfin les informations sélectionnées sont enregistrées dans une base de connaissances personnelle comme Obsidian. L'objectif est de constituer une bibliothèque d'informations. Ces ressources pourront être utilisées pour rédiger un rapport, proposer des actions en entreprise, développer des projets ou encore alimenter une réflexion stratégique.

2.2 Présentation de mes outils

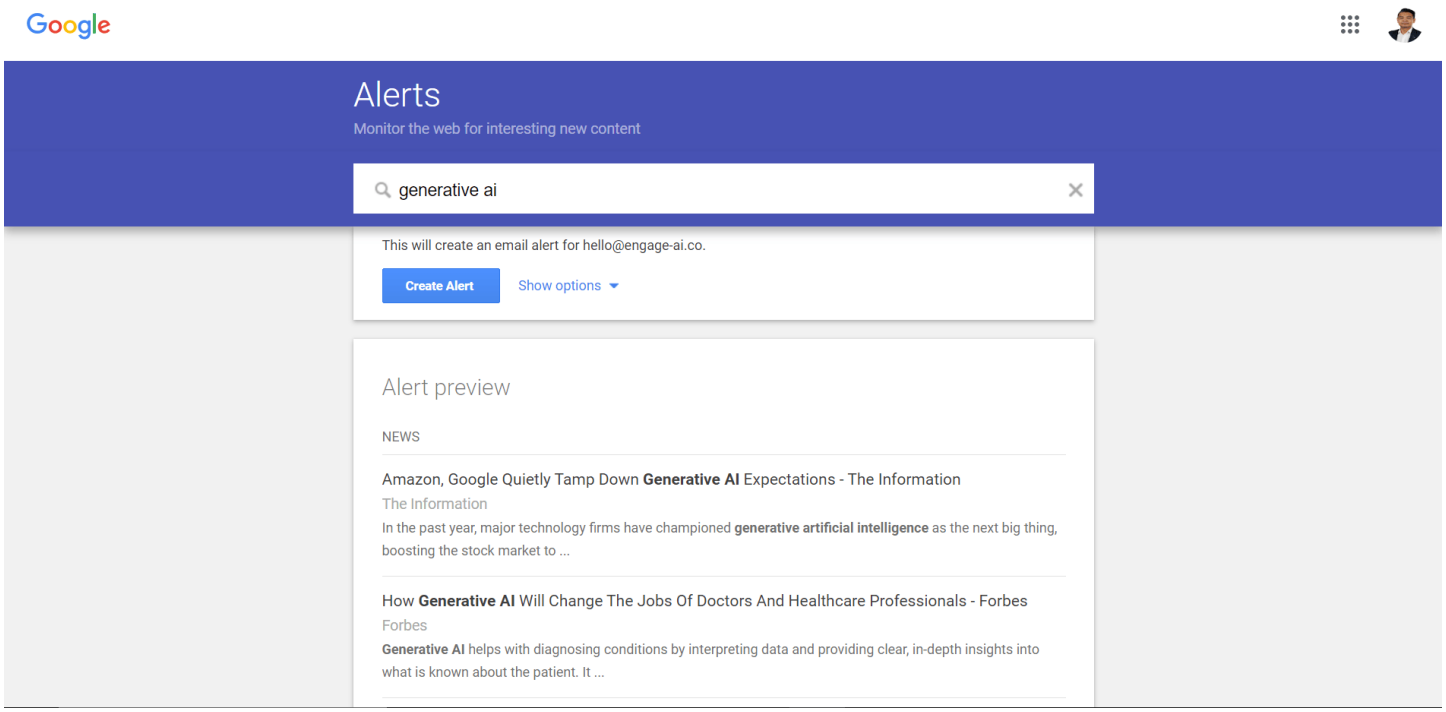
2.2.1 Feedly



Feedly est un outil de veille informationnelle qui permet de centraliser, organiser et consulter en un seul endroit les actualités provenant de différentes sources web. Il fonctionne grâce à la technologie RSS, ce qui permet à l'utilisateur de s'abonner à des flux d'actualités de sites spécialisés, de blogs ou de magazines, sans avoir à les visiter individuellement. Accessible via navigateur ou application mobile, Feedly facilite le suivi des nouveautés en temps réel et offre une interface claire pour classer les contenus par thématique.

Dans le cadre de ma veille technologique, j'utilise Feedly pour centraliser toutes les informations sur le thème du Shadow IT et de la cybersécurité. J'ai configuré des flux d'actualités spécialisés en ajoutant des sites, blogs et magazines reconnus dans le domaine de l'informatique. J'ai également organisé ces sources dans des catégories dédiées, ce qui me permet de suivre facilement les nouveautés selon les sujets qui m'intéressent. Chaque jour ou chaque semaine, je consulte Feedly pour repérer les articles récents et sélectionner ceux qui sont les plus pertinents.

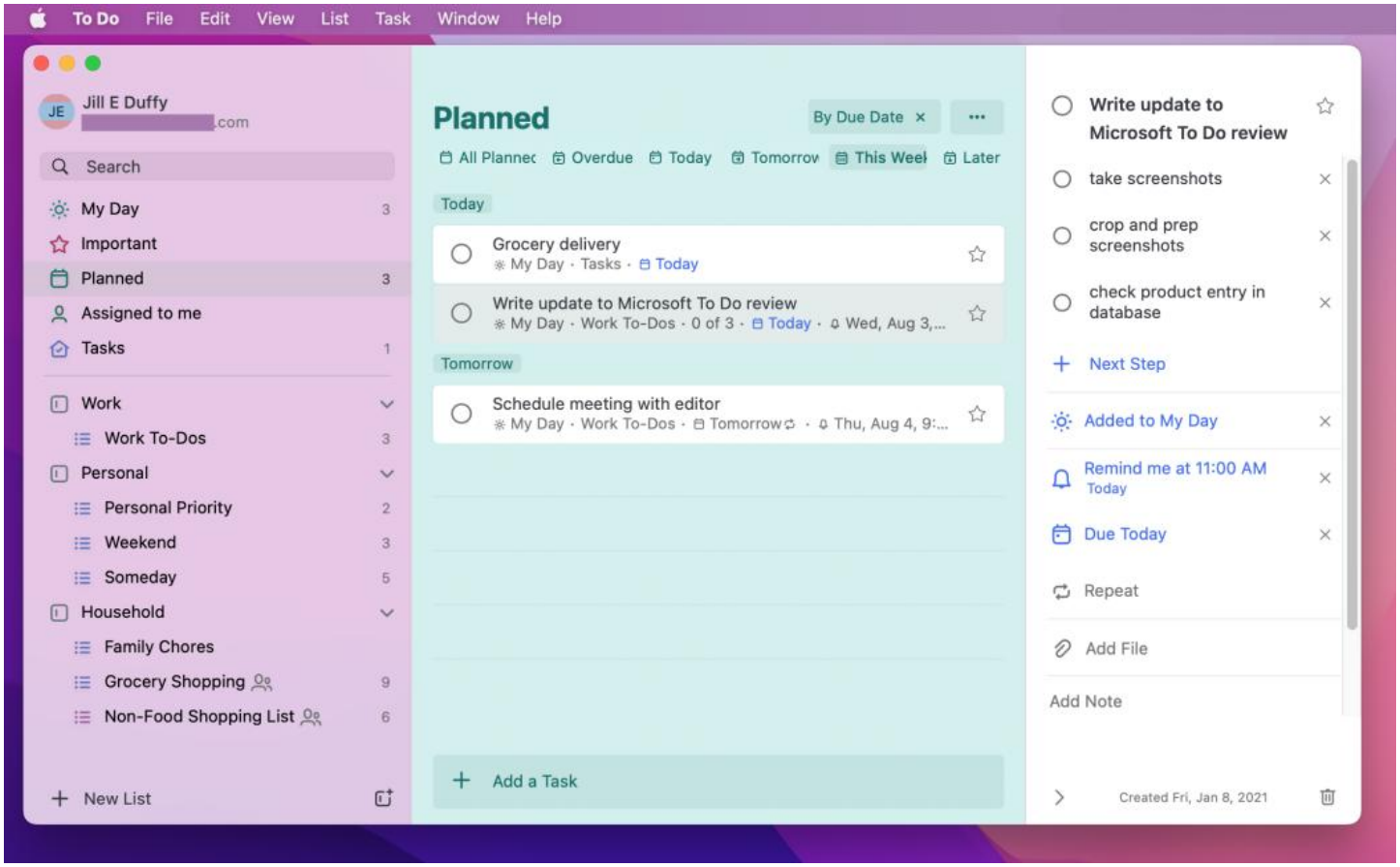
2.2.2
Google alerts



Google Alerts est un service gratuit proposé par Google qui permet de recevoir automatiquement des notifications lorsqu'un nouveau contenu correspondant à des mots-clés définis est publié sur Internet. Le principe est simple : l'utilisateur choisit un ou plusieurs mots-clés (par exemple "Shadow IT", "cybersécurité cloud", "risques BYOD"), et Google envoie des alertes par email à chaque fois qu'un article, une actualité ou une publication en ligne correspond à ces termes.
Google Alerts est très utile pour faire une veille rapide et ciblée, sans avoir besoin de chercher manuellement l'information. Il est possible de paramétrer la fréquence (immédiatement, une fois par jour, une fois par semaine), le type de sources (actualités, blogs, forums…) et la langue ou la région concernées. Cet outil permet ainsi de surveiller efficacement l'actualité d'un sujet spécifique et de gagner du temps dans le processus de veille.

J'utilise Google Alerts pour recevoir automatiquement des articles récents sur le thème du Shadow IT et de la cybersécurité, en configurant des mots-clés précis. Chaque jour ou chaque semaine, je reçois par email une sélection d'actualités correspondant à ces mots-clés, ce qui me permet de ne pas passer à côté des nouveautés importantes sans devoir effectuer de recherche manuelle.

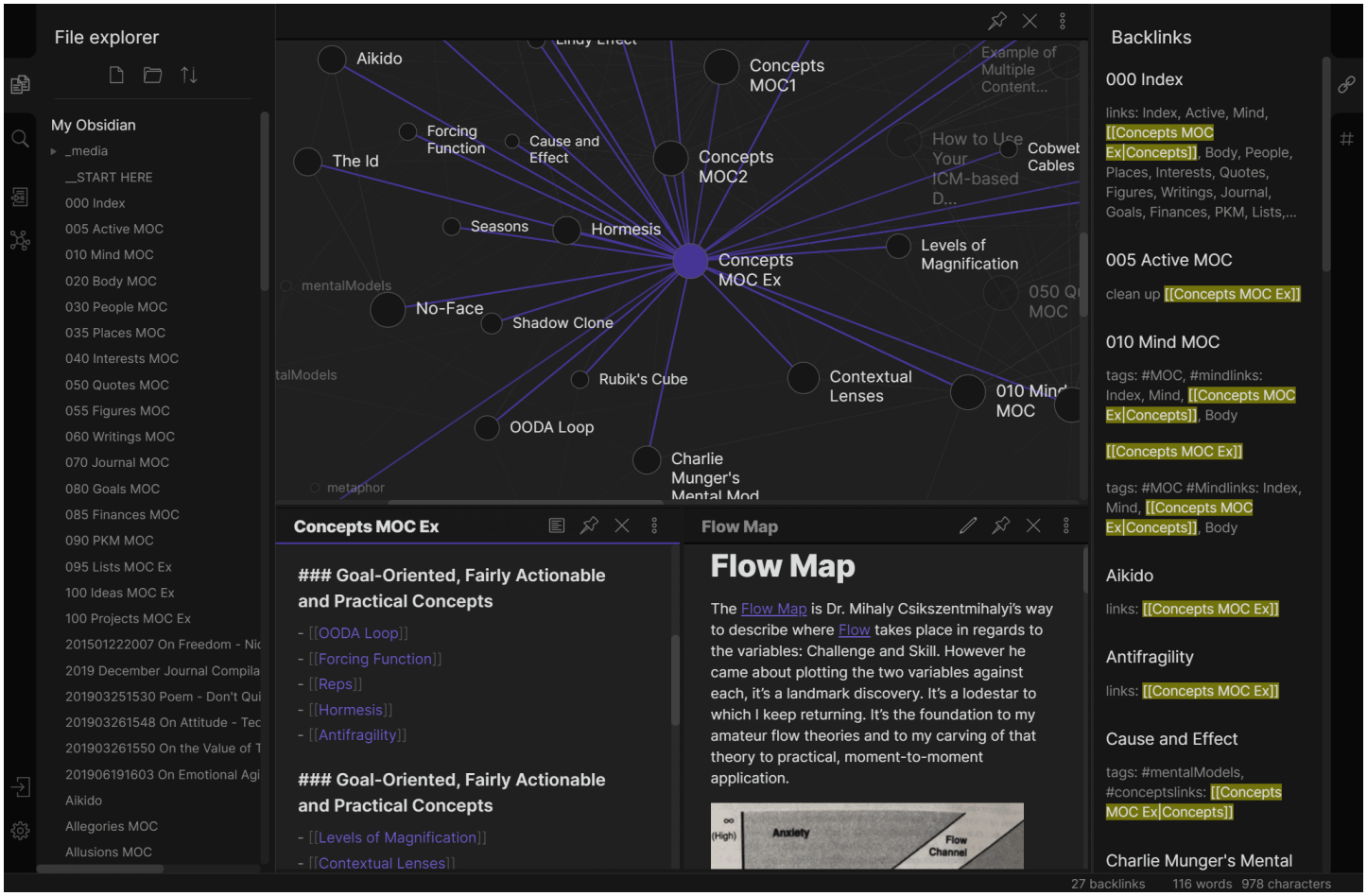
2.2.3
Microsoft To Do



Microsoft To Do est une application de gestion de tâches qui permet d'organiser son travail et ses projets de manière claire et efficace. L'outil propose de créer des listes personnalisées où l'on peut ajouter des tâches, définir des rappels, fixer des échéances et ajouter des notes complémentaires. Grâce à son interface intuitive, Microsoft To Do facilite la planification quotidienne, le suivi des activités importantes et l'organisation d'informations collectées lors d'une veille, comme des liens d'articles ou des idées.

J'utilise Microsoft To Do pour organiser les articles et informations collectées au quotidien. Dès que je repère un contenu intéressant via Feedly ou Google Alerts, je le note dans une liste dédiée sur Microsoft To Do, en y ajoutant parfois un petit commentaire pour préciser l'intérêt de l'article. Cela me permet de ne pas perdre d'informations importantes tout en les classant rapidement sans les traiter immédiatement

2.2.4
Obsidian



Obsidian est un logiciel de prise de notes avancé conçu pour organiser, connecter et structurer des connaissances sous forme de texte. Il fonctionne comme un carnet numérique ultra-puissant, où chaque note est enregistrée localement sous forme de fichier Markdown. Sa principale force réside dans la possibilité de lier facilement les notes entre elles, créant ainsi un véritable réseau d'idées interconnectées (on parle de « deuxième cerveau »).
Obsidian offre une interface très flexible : on peut créer des dossiers, ajouter des balises, visualiser les connexions entre les notes grâce à un graph interactif, et utiliser de nombreux plugins pour personnaliser l'expérience. L'outil est particulièrement apprécié pour gérer des projets complexes, centraliser des recherches, ou conserver durablement des informations issues d'une veille.

Dans le cadre de ma veille technologique, j'utilise Obsidian pour archiver et organiser les informations les plus pertinentes que j'ai sélectionnées. Après avoir trié les articles collectés via Feedly et notés dans Microsoft To Do, je crée dans Obsidian des notes thématiques sur le Shadow IT, la cybersécurité ou d'autres sujets liés. Chaque note contient un résumé des points clés, parfois accompagné d'un lien vers l'article d'origine. Grâce aux liens internes entre les notes, je peux relier différentes informations entre elles, par exemple en associant une menace liée au Shadow IT avec une solution technique adaptée. Cette méthode me permet de constituer une base de connaissances évolutive que je pourrai facilement réutiliser pour un rapport, une présentation ou un projet professionnel futur.

2.3 Mes sources

Catégorie	Site Web
Cyber-sécurité	https://www.leblogduhacker.fr
Cyber-sécurité	http://www.leblogduhacker.fr
Cyber-sécurité	https://pcsecurise.fr
Cyber-sécurité	http://itsocial.fr
Cyber-sécurité	https://www.seeyar.fr
Cyber-sécurité	http://www.brankovucinec.com
Systèmes	http://www.tecmint.com
Systèmes	https://www.astuces-aide-informatique.info
Systèmes	http://www.windows8facile.fr
Systèmes	https://rdr-it.com
Systèmes	https://technet365.fr
Systèmes	https://techexpert.tips
Systèmes	http://www.tutos-informatique.com
Systèmes	http://pbarth.fr
Systèmes	http://www.adminpasbete.fr
Réseaux	https://special-it.fr
Réseaux	https://networkcorp.fr
Réseaux	http://www.dsfc.net
Réseaux	https://websetnet.com
Réseaux	https://all-it-network.com
Réseaux	http://www.geek-directeur-technique.com
Généraliste	https://www.infonovice.fr
Généraliste	https://www.it-channels.com
Généraliste	http://lewebpedagogique.com

Catégorie	Site Web
Généraliste	http://feeds2.feedburner.com
Généraliste	http://feeds.feedburner.com
Généraliste	http://www.winsupersite.com
Généraliste	http://theitbros.com
Généraliste	http://www.papergeek.fr
Généraliste	https://www.barzek.com
Généraliste	https://labo-tech.fr
Généraliste	https://www.pcastuces.com

3 Mon sujet de veille

3.1 Introduction

Afin d'éprouver ma méthodologie de veille, j'ai choisi d'étudier et de résumer le sujet suivant :

« SHADOW IT // Quels sont les enjeux de sécurité liés au Shadow IT et comment y répondre efficacement sans freiner l'innovation des équipes ?»

J'ai choisi de travailler sur le Shadow IT car c'est un phénomène de plus en plus présent dans les entreprises avec l'évolution rapide des outils numériques et du télétravail. Le Shadow IT représente un risque majeur pour la sécurité des données et la conformité réglementaire, mais il est aussi révélateur d'un besoin d'agilité et d'innovation de la part des utilisateurs. Ce sujet est donc au cœur des enjeux actuels des services informatiques, qui doivent trouver un équilibre entre contrôle, flexibilité et sécurité. En réalisant une veille technologique sur le Shadow IT, je peux mieux comprendre ses impacts, ses risques, et les solutions qui existent pour le maîtriser, ce qui est essentiel dans un contexte professionnel où la sécurité informatique est devenue une priorité stratégique.

3.2 Synthèse de ma veille sur le sujet

3.2.1 Historique

Années 1990 — Apparition du phénomène
Le terme "Shadow IT" commence à émerger dans les années 1990 avec l'arrivée des premiers ordinateurs personnels et logiciels bureautiques accessibles aux salariés. Les employés installent parfois des outils informatiques non validés par leur service IT pour gagner en productivité.

Années 2000 — Explosion avec Internet et les premiers services cloud
Avec la généralisation d'Internet dans les entreprises et la naissance des premiers services cloud (Google Docs, Dropbox, Salesforce) le phénomène s'accélère. Les utilisateurs peuvent désormais accéder à des services en ligne sans passer par l'IT souvent pour contourner des outils internes jugés trop rigides.

Années 2010 — Démocratisation du BYOD (Bring Your Own Device)
Le développement du BYOD (utilisation d'appareils personnels au travail) renforce encore le Shadow IT. Les smartphones, tablettes et applications mobiles pénètrent les entreprises sans contrôle total ce qui augmente les risques de sécurité (fuite de données, non-conformité RGPD).

À partir de 2015 — Prise de conscience par les entreprises
Face à la montée des cyberattaques et aux fuites de données, les entreprises commencent à prendre conscience de l'ampleur du problème. Les stratégies de sécurité évoluent : mise en place de politiques "Zero Trust", développement de solutions de CASB (Cloud Access Security Broker) pour surveiller les usages non validés.

2020 et après — Accélération avec la pandémie de COVID-19
Le télétravail massif imposé par la pandémie a provoqué une explosion du Shadow IT. De nombreux utilisateur isolés

utilisent des outils non approuvés pour travailler efficacement (Zoom, Slack, outils collaboratifs cloud), ce qui multiplie les risques de cybersécurité.

3.2.2 Problématique

- **Manque de contrôle et de visibilité**
  Dès l'apparition du Shadow IT, la principale difficulté a été pour les services informatiques de ne pas avoir de visibilité sur les outils et applications utilisés par les employés. Cela empêchait de contrôler les accès, de sécuriser les données et d'appliquer les politiques internes.

- **Failles de sécurité**
  Le Shadow IT a très vite introduit de nouvelles vulnérabilités dans les systèmes d'information. Les applications non validées n'étaient pas nécessairement sécurisées, et les transferts de données sensibles vers des plateformes non conformes ont multiplié les risques de cyberattaques et de fuites de données.

- **Non-conformité réglementaire**
  Avec l'apparition de normes comme le RGPD (en Europe) ou d'autres législations sur la protection des données, le Shadow IT a posé un problème majeur de conformité. En utilisant des outils non approuvés, les entreprises prenaient le risque de violations de données sans en être conscientes, exposant l'organisation à des sanctions financières et juridiques.

- **Surcharge d'outils et fragmentation**
  Le développement incontrôlé du Shadow IT a aussi conduit à une multiplication des plateformes et des outils utilisés dans les entreprises, créant une fragmentation des données et des workflows. Cela rendait la collaboration plus difficile et entraînait une perte d'efficacité dans certains processus métier.

- **Résistance au changement**
  Lorsque les DSI ont commencé à vouloir contrôler et limiter le Shadow IT, elles ont souvent rencontré une résistance des utilisateurs qui percevaient ces outils alternatifs comme plus pratiques et modernes que les solutions internes officielles. Cela a rendu la gestion du changement complexe.

- **Difficulté d'intégration et d'interopérabilité**
  Beaucoup d'applications de Shadow IT ne s'intégraient pas facilement aux systèmes existants de l'entreprise (ERP, CRM, etc.). Cela compliquait l'interopérabilité des données et augmentait les risques d'erreurs ou de pertes d'informations.

3.2.3
Avantages / inconvénients <> points forts / points faibles

Mettre en place une approche structurée du Shadow IT présente plusieurs avantages stratégiques pour une entreprise.

Tout d'abord, cela permet de favoriser l'agilité des employés qui ont souvent besoin de solutions rapides pour répondre à des besoins métiers spécifiques. En autorisant et encadrant certains outils issus du Shadow IT l'entreprise pourrait gagner en réactivité et accélérer l'innovation interne. Cela améliore aussi la satisfaction et l'implication des équipes, car les collaborateurs se sentent écoutés dans leurs besoins opérationnels.

Ensuite, encadrer le Shadow IT permet de transformer une menace en opportunité. Plutôt que d'interdire systématiquement, l'entreprise peut analyser les outils utilisés spontanément et intégrer les plus performants dans son système d'information, après validation de leur sécurité. Cela permet de moderniser l'infrastructure informatique sans imposer des solutions mal adaptées.

De plus, une gestion proactive du Shadow IT renforce la cybersécurité : en identifiant les applications utilisées, les services informatiques peuvent mettre en place des règles de sécurité adaptées (par exemple avec des CASB, de l'authentification forte ou du chiffrement). Cela réduit les risques tout en maintenant la souplesse nécessaire à l'activité.

3.2.4
Dimension juridique

Le Shadow IT soulève plusieurs problèmes juridiques majeurs pour les entreprises, principalement autour de la protection des données, de la responsabilité et de la conformité réglementaire.

- **Protections des données personnelles (RGPD)**
  Le principal risque juridique lié au Shadow IT est la violation des règles de protection des données personnelles, notamment sous le Règlement Général sur la Protection des Données (RGPD) en Europe.
  Si un collaborateur utilise une application non validée pour traiter ou stocker des données personnelles (clients, salariés, fournisseurs) l'entreprise reste légalement responsable de la sécurité de ces données et risque en cas de fuite de données des sanctions financières

- **Non-conformité aux politiques internes**
  Le Shadow IT viole souvent les politiques internes d'utilisation des ressources numériques (chartes informatiques, règlements internes) ce qui peut entrainer des sanctions disciplinaires pour l'utilisateur comme un licenciement dans le pire des cas.

- **Confidentialité et propriété intellectuelle**
  L'utilisation d'applications non sécurisées peut entraîner la divulgation involontaire d'informations stratégiques (projets confidentiels, secrets industriels) et des risques de violation de contrats

3.2.5
L’avis des experts

Le Shadow IT est aujourd'hui au cœur des préoccupations des spécialistes de la cybersécurité, du cloud et du management informatique. De nombreux experts s'accordent à dire que le phénomène est inévitable, mais qu’il peut devenir une opportunité pour l'entreprise s'il est correctement encadré.

- **Le Shadow IT est massif et en croissance**
  Selon le Cloud and Threat Report 2023 publié par Netskope (https://www.netskope.com/netskope-threat-labs/cloud-threat-report) plus de 70 % des applications cloud utilisées dans les entreprises ne sont pas approuvées par les services informatiques officiels. Cela montre que le phénomène du Shadow IT est profondément enraciné et incontrôlable par des méthodes traditionnelles.

- **Le Shadow IT est inévitable**
  D’après Satya Nadella, PDG de Microsoft, lors de son discours au Microsoft Ignite 2020 (https://www.youtube.com/watch?v=OS0nUXssgfY), le Shadow IT est un symptôme du besoin d'agilité et de modernisation des outils métiers. Selon lui, il ne faut pas chercher à l’éliminer totalement, mais plutôt à l'encadrer intelligemment en offrant aux utilisateurs des solutions modernes et sécurisées.

- **Une source d'innovation cachée**
  Les experts d'IDC ("*Shadow IT: Embrace It and Manage It*", 2021) insistent sur un point clé : le Shadow IT peut être un puissant levier d'innovation. Il traduit souvent l'incapacité du système d'information officiel à répondre rapidement aux besoins métiers, et pousse donc l’organisation à évoluer vers des outils plus efficaces.

- **La nécessité du Zero Trust**
  Face à la généralisation du travail hybride et du cloud, Palo Alto Networks recommande l’adoption d’une approche "Zero Trust" ("*Implementing Zero Trust to Address Shadow IT Risks*", 2022). Cette stratégie repose sur le principe de "ne jamais faire confiance, toujours vérifier", et permet de réduire efficacement les risques liés aux applications et services non validés par l'IT.

- **L'ampleur du phénomène aujourd'hui**
  Enfin, d'après le Netskope Cloud and Threat Report 2023, près de 70 % des applications SaaS utilisées dans les entreprises ne sont pas approuvées par les services informatiques. Ce chiffre montre que le Shadow IT est désormais massif et structurant, et qu’ignorer le problème est devenu impossible.

3.2.6
Etat actuel

Le Shadow IT est en phase de démocratisation avancée : omniprésent dans les entreprises, il est devenu une réalité que les organisations doivent apprendre à encadrer plutôt qu'à combattre.

Aujourd'hui, le Shadow IT est largement répandu dans toutes les entreprises, quel que soit leur secteur d'activité ou leur taille. Ce phénomène n'est plus en phase de simple apparition ou d'expérimentation : il est complètement entré dans la pratique courante, porté par la généralisation du cloud, des applications SaaS, du télétravail et de l'utilisation massive des outils personnels dans l'environnement professionnel (BYOD).

Selon plusieurs rapports récents (notamment Netskope Cloud and Threat Report 2023), plus de 70 % des applications cloud utilisées en entreprise ne sont pas validées par les services informatiques. Ce chiffre montre que le Shadow IT n'est plus un comportement isolé mais un phénomène structurel.

La technologie n'est donc plus en phase de développement : le Shadow IT est en pleine phase de démocratisation et de maturité. Il est omniprésent, même dans les organisations ayant mis en place des politiques de sécurité strictes.

Face à cette situation, les entreprises n'essaient plus d'éradiquer totalement le Shadow IT — ce qui serait illusoire — mais cherchent plutôt à l'encadrer

3.2.7
Evolution

À mon avis, le Shadow IT va continuer à se développer dans les années à venir, porté par plusieurs grandes tendances du numérique : la multiplication des applications SaaS, l'essor du télétravail et l'agilité croissante des équipes métiers. Les utilisateurs chercheront toujours à utiliser les outils qu'ils estiment les plus efficaces pour accomplir leurs tâches, même en dehors du cadre officiel fixé par l'IT.

Cependant, l'approche des entreprises face au Shadow IT va changer profondément. Elles chercheront moins à l'interdire et davantage à l'encadrer grâce à des stratégies de surveillance intelligente (CASB, SIEM, analyse réseau), des politiques Zero Trust et des programmes de sensibilisation.

Un autre facteur déterminant dans l'évolution du Shadow IT sera l'intelligence artificielle (IA).
L'IA aura un double impact :

- D'une part, elle alimentera encore davantage le Shadow IT, car les utilisateurs adoptent spontanément de nouveaux outils d'IA (ChatGPT, assistants) souvent sans validation IT.

- D'autre part, l'IA sera utilisée pour mieux encadrer et contrôler ces usages : des systèmes intelligents permettront de détecter automatiquement les comportements à risque, de cartographier les flux d'applications et de bloquer les menaces en temps réel.

Enfin, la pression des réglementations comme le RGPD obligera les entreprises à tracer et sécuriser de manière plus stricte les outils utilisés pour manipuler des données sensibles.

En résumé, je considère que le Shadow IT restera une constante, mais qu'il sera encadré plus intelligemment grâce à l'usage de l'IA, à l'amélioration des services IT internes et à une prise en compte réelle des besoins métiers.

4 Bilan de ma veille

Grâce à cette veille technologique sur le Shadow IT, j'ai développé une compréhension approfondie des enjeux liés à l'usage non contrôlé des technologies dans l'entreprise.
J'ai appris que le Shadow IT n'est pas simplement un problème technique, mais un phénomène complexe, mêlant besoins métiers, innovation spontanée et risques de cybersécurité.
J'ai également découvert que les approches modernes ne consistent plus à essayer de l'éliminer, mais plutôt à l'encadrer intelligemment

Dans mon futur métier, où je serai amené à travailler dans le domaine de l'informatique, de la cybersécurité ou de la gestion de projet numérique, les compétences développées grâce à cette veille seront précieuses.
Je saurai :

- Mettre en place une veille technologique efficace pour rester informé des nouveautés et anticiper les risques.
- Identifier les risques de Shadow IT au sein d'une organisation et proposer des solutions réalistes pour les encadrer
- Sensibiliser les équipes aux bonnes pratiques de sécurité numérique en expliquant les dangers mais aussi les opportunités du Shadow IT.

Enfin, cette expérience me donne une meilleure posture professionnelle : plutôt que de voir le Shadow IT uniquement comme un problème, je saurai l'aborder comme un levier d'amélioration continue, en aidant les entreprises à adapter leurs outils aux besoins réels tout en renforçant leur sécurité.