RAPPORT DE STAGE

CAISSE NATIONALE D'ASSURANCE VIEILLESSE

THÉO OGER

12 Mai - 06 Juillet 2025

Maître de stage: Daniel LOPEZ

SOMMAIRE

I) Remerciements

Je tiens à exprimer ma profonde gratitude à toute l'équipe de la sécurité des systèmes d'information de la CNAV (Caisse Nationale d'Assurance Vieillesse), en particulier à Tarik, Jean-Pierre et Rachel, qui m'ont chaleureusement accueilli au sein de leur bureau. Leur accompagnement, leur patience et leur volonté de partager leur expertise ont été essentiels pour me familiariser rapidement avec les métiers de la sécurité informatique. Leur soutien m'a permis de mieux comprendre les enjeux liés à la cybersécurité et d'acquérir des compétences précieuses pour mon parcours professionnel.

Je remercie également Monsieur Lopez, responsable du service de sécurité des systèmes d'information, pour la confiance qu'il a accordée à ma candidature et pour m'avoir intégré à son équipe malgré mon manque initial de connaissances dans ce domaine. Son encadrement bienveillant m'a permis de progresser et de m'impliquer pleinement dans les différentes missions qui m'ont été confiées.

Enfin, je suis particulièrement reconnaissant envers l'établissement qui m'a offert cette opportunité unique d'évoluer dans un environnement exigeant. Travailler dans un secteur aussi sensible requiert rigueur et esprit d'équipe, et j'ai été honoré d'apprendre auprès de professionnels engagés.

Je souhaite également remercier Monsieur Stéphane David, directeur de la DIE, dont le soutien et la recommandation ont grandement facilité mon intégration au sein de cette structure.

II) Introduction

Élève en BTS SIO (Services Informatiques aux Organisations), j'ai effectué un stage de 8 semaines, du 12 mai au 6 juillet 2025.

Dans le cadre de notre formation, il est nécessaire d'accomplir 8 semaines de stage en première année afin de valider le passage en seconde année. Par la suite, 6 semaines supplémentaires sont à réaliser en deuxième année pour l'obtention du diplôme. Ces périodes de stage sont essentielles, car elles viennent compléter les enseignements théoriques par une expérience concrète sur le terrain. La validation des 14 semaines de stage est obligatoire.

J'ai eu l'opportunité d'effectuer mon stage au sein de la CNAV (Caisse Nationale d'Assurance Vieillesse) à Paris, sous la responsabilité de Monsieur Daniel Lopez, au sein de l'équipe de Sécurité des Systèmes d'Information.

III) Présentation de l’établissement

1. La CNAV

La Caisse Nationale d’Assurance Vieillesse (CNAV) est l’organisme chargé de la gestion et du versement des pensions de retraite du régime général en France. Elle joue un rôle essentiel dans le suivi administratif et financier des retraites, tout en accompagnant les assurés dans leurs démarches liées à la vieillesse.

La CNAV est un établissement public national à caractère administratif, représentant le premier régime de retraite français. Elle couvre les salariés du secteur privé, les travailleurs indépendants, les contractuels de droit public ainsi que les artistes-auteurs. Son fonctionnement repose sur le principe de la répartition, où les cotisations des actifs financent les pensions des retraités.

Le siège de la CNAV gérant la région Île-de-France est situé au 110 avenue de France, 75013 Paris. Cet établissement a été créé le 1er mars 1983.

Fondée en 1945, la CNAV a évolué au fil des décennies pour s’adapter aux besoins des assurés et aux réformes du système de retraite. Elle mobilise un effectif estimé entre 2 000 et 4 999 collaborateurs, contribuant à la gestion des retraites de millions de Français. Par ailleurs, 15 Carsat (Caisses d’Assurance Retraite et de la Santé au Travail) sont réparties sur l’ensemble du territoire français.

En complément de sa mission principale de gestion des pensions, la CNAV mène également des actions de prévention et d’accompagnement visant à favoriser le bien-vieillir et la préservation de l’autonomie des retraités.

Bâtiment de la CNAV

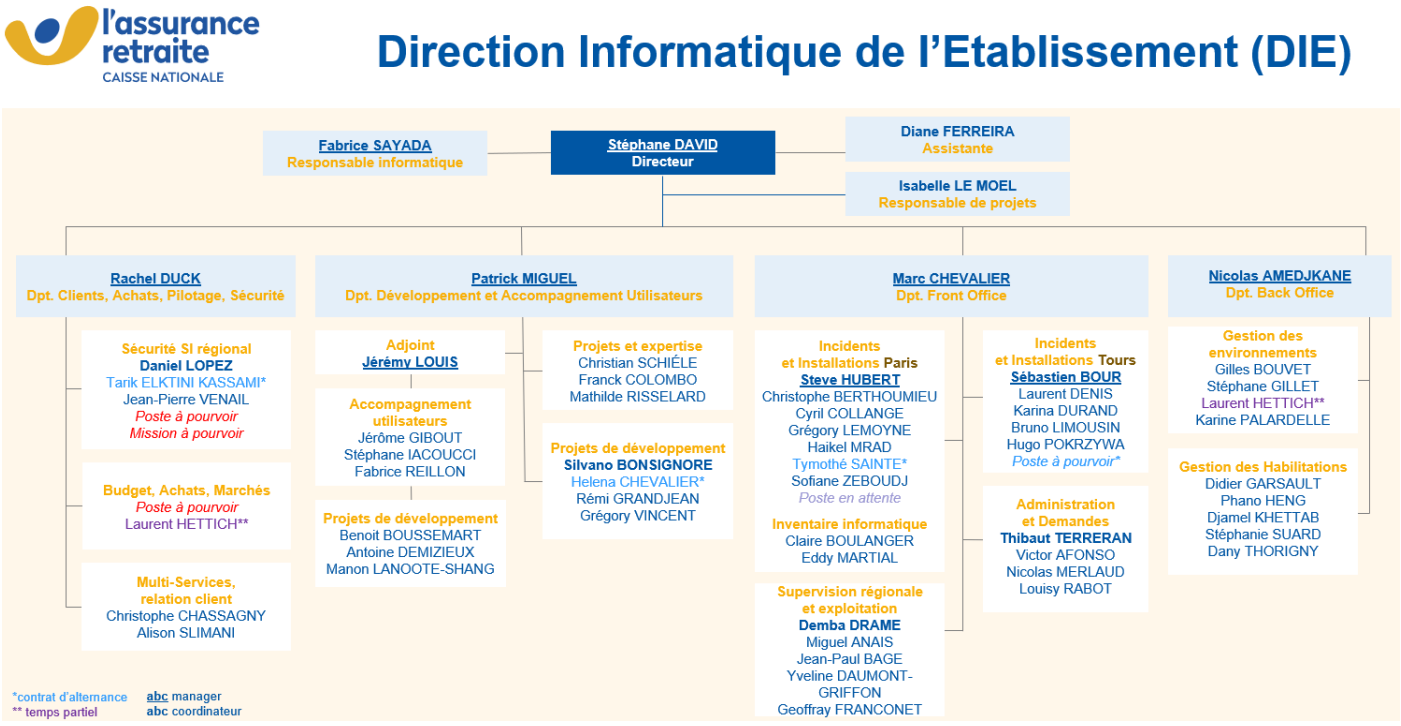
2. Le service sécurité du système d'information

Le Service de Sécurité des Systèmes d'Information (SSI) a pour mission de garantir la protection et l'intégrité du système informatique de la CNAV. Il assure la sécurisation des données et des accès en mettant en œuvre des contrôles rigoureux, notamment via la gestion des habilitations et la validation des services en mode SaaS.

Le SSI joue également un rôle central dans la prévention et la gestion des incidents de sécurité, en surveillant en permanence les menaces potentielles et en intervenant rapidement dès la détection d'anomalies. Par ailleurs, il œuvre à la sensibilisation des utilisateurs aux bonnes pratiques, notamment à travers la charte informatique et des campagnes de formation dédiées.

Au cours de mon stage, j'ai participé activement au bon fonctionnement du SSI en réalisant diverses missions, telles que la vérification des habilitations, le suivi des incidents de sécurité, ainsi que l'accompagnement des utilisateurs dans le respect et l'application des règles de sécurité.

3. Organigramme

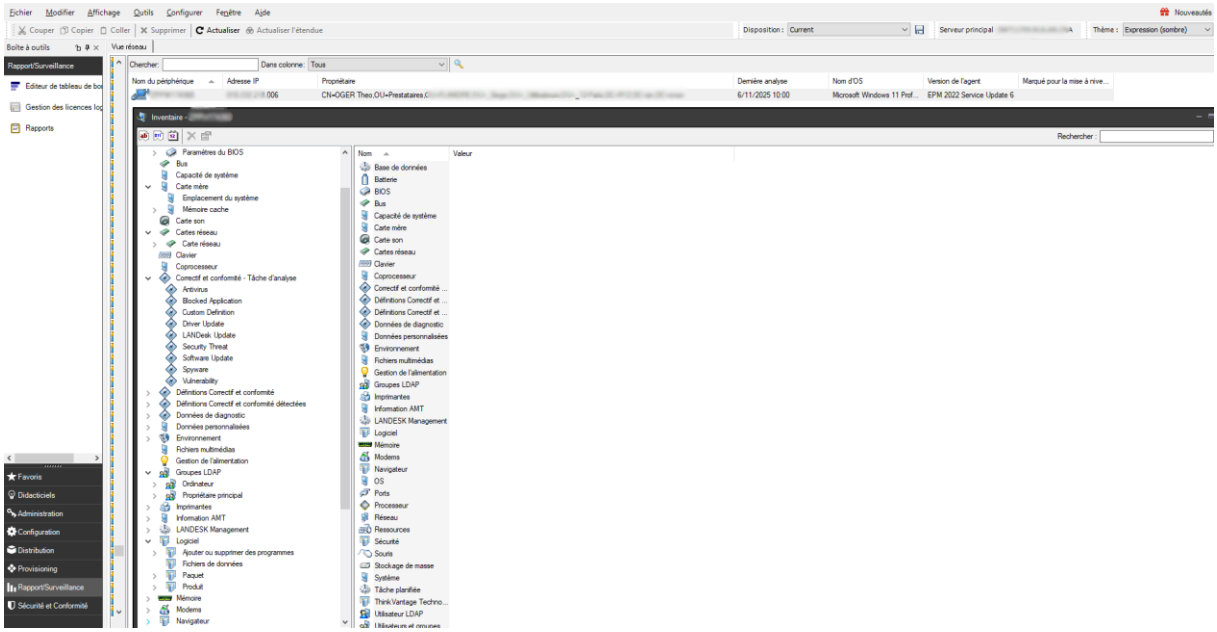


Organigramme de la DIE

IV) Organisation de travail

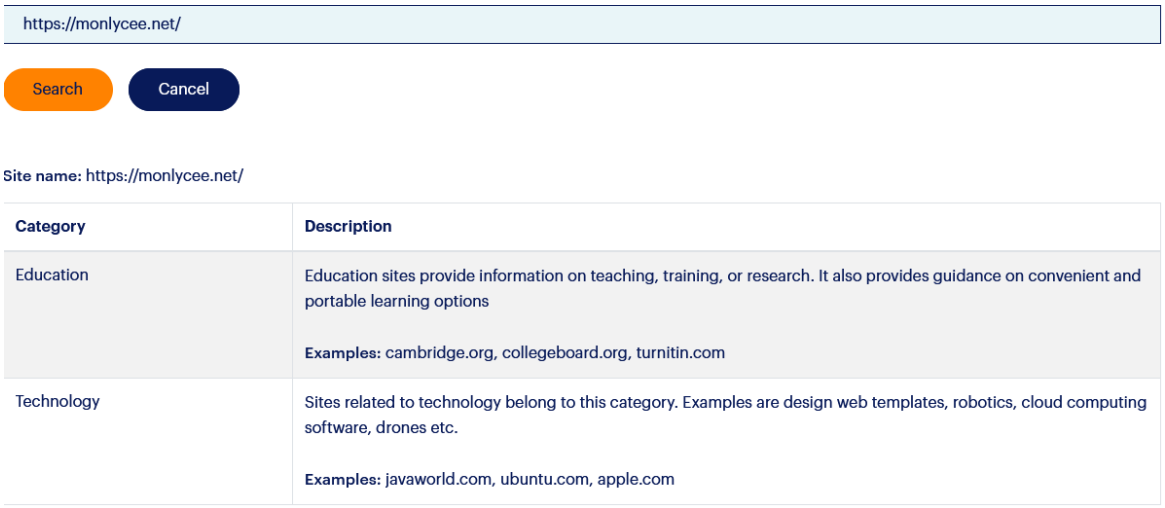
1. Technologique

Citrix est un outil permettant de se connecter à distance à un serveur disposant de droits administrateurs, offrant un accès direct à un compte nominatif. Une fois connecté, il est possible d'accéder à Ivanti, un logiciel de gestion de parc informatique basé sur une base de données. Ivanti fournit toutes les informations relatives à un poste de travail, telles que les logiciels installés, le modèle de l'appareil et les droits d'accès. Il permet également de formuler des requêtes pour identifier l'ensemble des machines répondant à des critères spécifiques.



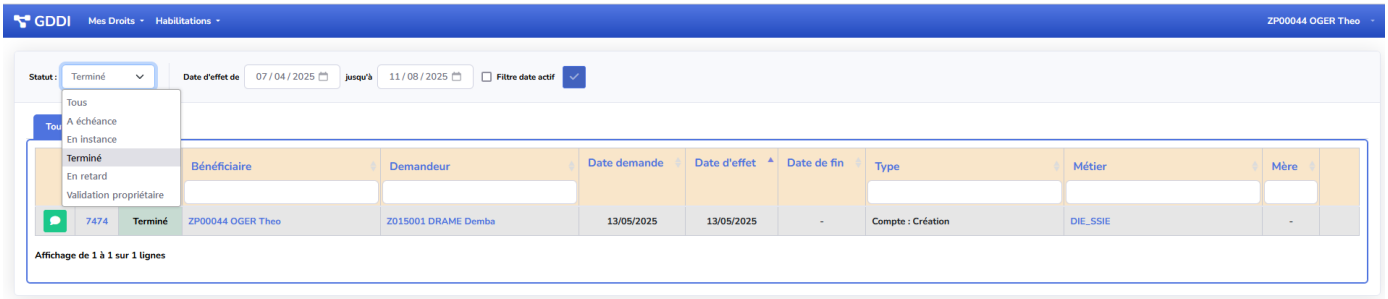
Interface d'Ivanti

URL LOOKUP est un outil permettant de vérifier la catégorisation d'un site web afin de déterminer si le proxy autorisera ou bloquera l'accès aux utilisateurs.



Interface URL LOOKUP

GDDI est un outil dédié aux demandes d'habilitation. Les CLSSI (Correspondants Locaux de Sécurité) sont responsables de formuler ces demandes et de vérifier que les droits sollicités correspondent aux besoins professionnels de l'utilisateur. Ils utilisent GDDI pour accorder des droits discrétionnaires, c'est-à-dire des autorisations spécifiques attribuées individuellement à une personne selon son métier.



Demande de création de compte dans un métiers DIE_SSI

Excel est largement utilisé au sein de la CNAV, notamment pour le PSSI, la revue d'habilitation et d'autres tâches analytiques. Cet outil permet de gérer des données sous forme de tableaux, d'effectuer des calculs, de créer des graphiques et d'automatiser certains processus à l'aide de formules et de macros.

Word, quant à lui, est principalement utilisé pour la création de rapports et la documentation. Il offre des fonctionnalités avancées de mise en page, de rédaction et de structuration de documents, facilitant ainsi la production de contenus professionnels et structurés.

GPM est un outil interne de gestion des profils métiers. Il permet de modifier directement, via Active Directory (AD), les droits associés à chaque métier. Les groupes métiers disposent d'un ensemble de permissions spécifiques, certains ayant des droits que d'autres n'ont pas. Grâce à GPM, il est possible de visualiser, ajouter ou modifier les habilitations d'un groupe métier, ainsi que d'attribuer ou de retirer des droits à chaque groupe.

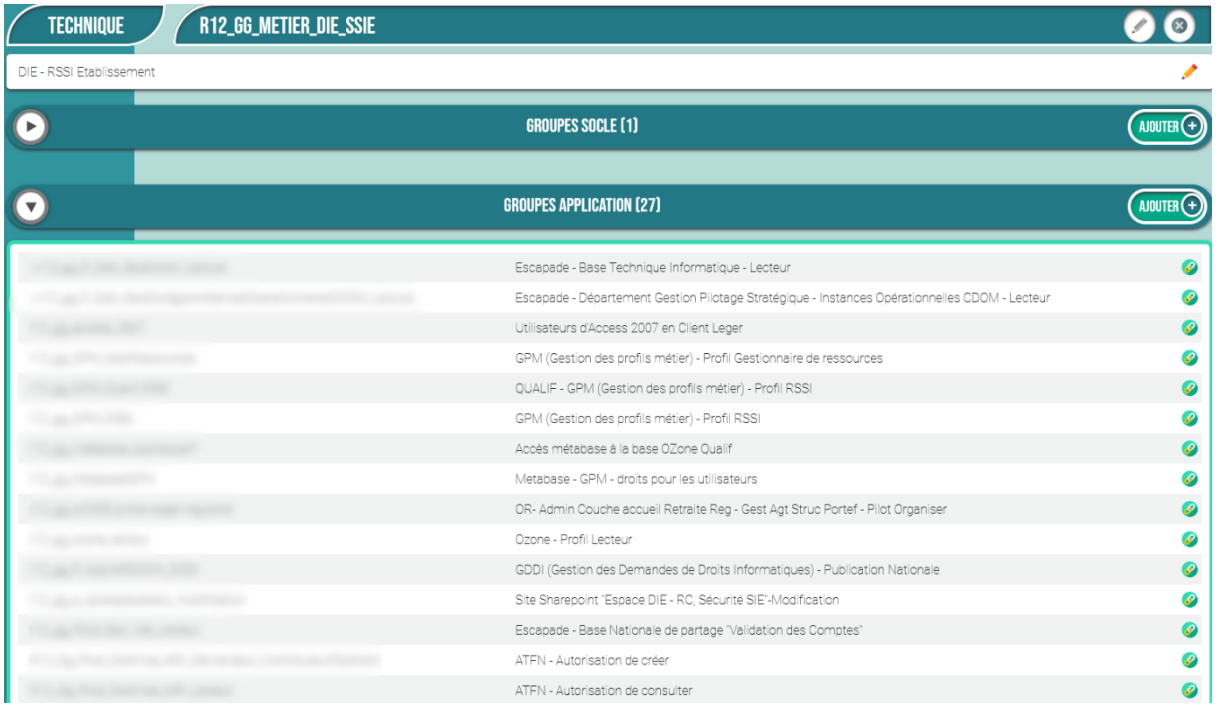


Illustration de GPM, profil métier du service SSI

DOIT est l'outil de ticketing. Il permet de recevoir des tickets envoyés soit par ISI, le groupe chargé de les rediriger vers le service approprié, soit directement par d'autres utilisateurs. Avec DOIT, plusieurs actions sont possibles : demander des informations supplémentaires au créateur du ticket, rediriger le ticket vers un autre service pour solliciter une intervention, ou le clôturer. Lors de la clôture, l'outil exige un suivi détaillé, incluant les actions réalisées ainsi qu'une solution à transmettre à l'utilisateur ayant initié la demande.

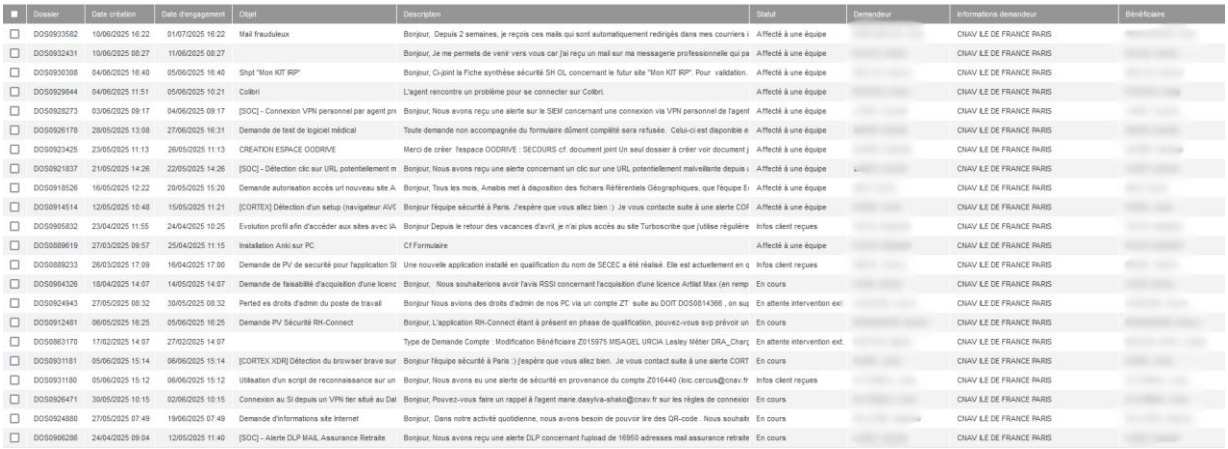


Illustration des tickets dans DOIT

2. Organisationnel

L'organisation au sein d'un pôle SSI est primordiale pour assurer une gestion efficace des tâches. Pour cela, nous utilisons plusieurs outils essentiels, dont Microsoft Outlook, Teams, Planner et les lecteurs réseau.

Tam-Tam est le portail applicatif permettant d'accéder à toute les applications métiers.

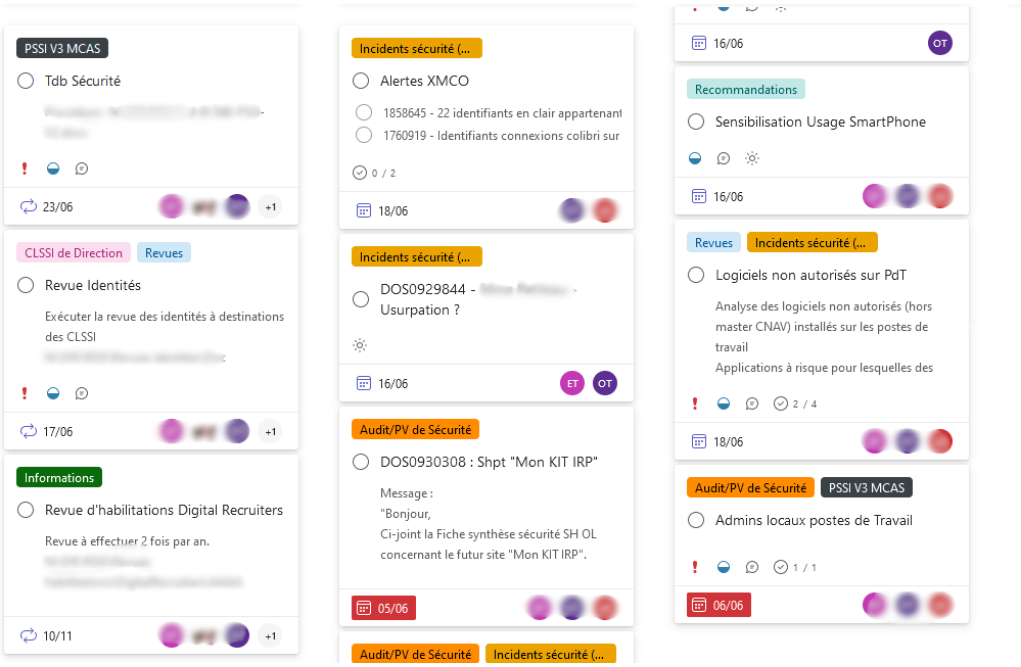
Microsoft Outlook est une plateforme de messagerie électronique qui facilite la communication entre les collaborateurs de la CNAV. Outre l'envoi et la réception de courriels, Outlook permet également la gestion des calendriers, offrant une visibilité sur la disponibilité des collègues. Cette fonctionnalité est particulièrement utile pour la coordination et la planification des réunions et des interventions.

De plus, Outlook propose des groupes dédiés, notamment pour le service SSI. La messagerie partagée entre les membres du SSI permet de conserver une trace des échanges et garantit que tous les collaborateurs disposent des mêmes informations.

Teams est également utilisé au sein de la CNAV pour faciliter les échanges en temps réel. Dans mon cas, son utilisation est quotidienne, notamment pour communiquer avec les utilisateurs en cas d'incident de sécurité. Grâce à Teams, il est possible de rechercher un interlocuteur par son nom et d'échanger aussi bien par messages écrits que par appels vocaux ou visioconférences, assurant ainsi un partage des informations.

Planner, disponible sur le portail Microsoft, est utilisé au sein du service SSI comme complément à DOIT. Lorsqu'un ticket est reçu, nous créons une tuile, qui est une copie du ticket initial et permet de suivre précisément l'état d'avancement de la tâche. À chaque action effectuée, un commentaire est ajouté pour indiquer la progression.

Planner permet également de structurer un plan d'action, définissant les tâches à effectuer et leur ordre de priorité, leur date d'échéance. Cet outil est indispensable pour un suivi rigoureux des dossiers en cours et assure une continuité en cas d'absence, permettant à un autre collègue de reprendre la tuile sans difficulté.



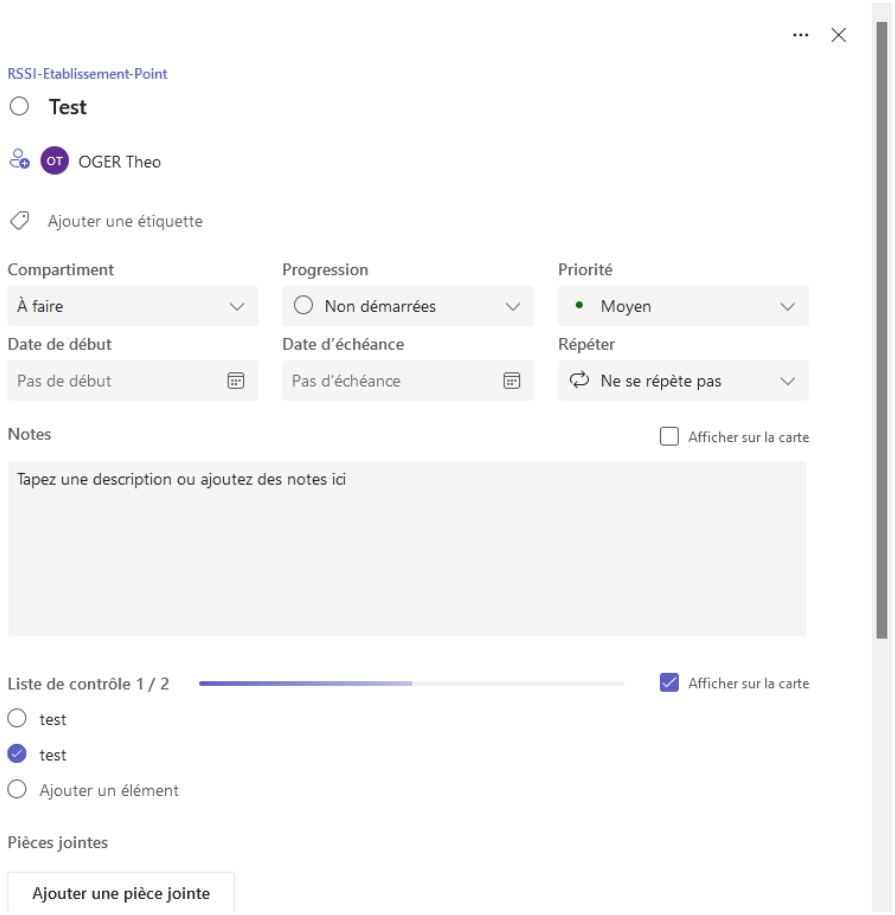


Illustration des tuiles sur le planner

Les lecteurs réseau

Enfin, chaque membre du service SSI dispose d'un lecteur réseau personnel avec un espace de stockage de 2 Go. En complément, un lecteur commun est accessible à l'ensemble du service SSI, regroupant les documentations essentielles telles que les rapports, le PSSI, la charte SSI, ainsi que divers autres travaux et ressources partagées.

V) Activités effectuées

1. Gestion de droit

Durant mon stage, j'ai eu l'opportunité de découvrir le fonctionnement des habilitations au sein de la CNAV.

Les habilitations sont gérées par une équipe dédiée, chargée d'attribuer les droits d'accès en fonction des besoins métier. Cette équipe reçoit les demandes via les CLSSI (Correspondants Locaux Sécurité des Systèmes d'Information), qui analysent la pertinence des droits demandés par rapport aux fonctions exercées par l'agent concerné.

Mon rôle, au sein de cette organisation, consistait à traiter les tickets issus de l'outil GDDI. Une fois la demande prise en charge, il était essentiel de vérifier que l'utilisateur avait bien reçu les droits appropriés, ni plus ni moins. Cette étape est cruciale, car une attribution inadaptée des droits peut représenter un risque significatif pour la sécurité des systèmes d'information.

Notre mission principale était donc de contrôler les droits attribués, de détecter d'éventuelles anomalies et de signaler tout écart. En effet, chaque droit inapproprié accordé à un utilisateur constitue une faille potentielle, augmentant la surface d'attaque et exposant l'entreprise à des risques importants.

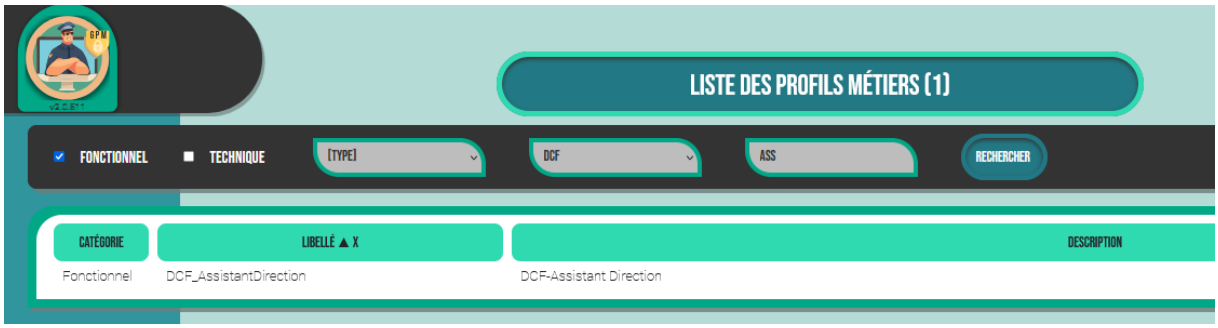
Lorsqu'une demande d'habilitation est reçue, nous intervenons dans l'outil GDDI, qui est directement interconnecté avec Active Directory (AD). Toute modification effectuée dans GDDI ou dans GPM (Gestion des Profils Métiers) est automatiquement répercutée dans l'AD via des scripts Bash. Cependant, ces mises à jour ne sont pas immédiates et nécessitent un temps de traitement.

Concernant GPM, une synchronisation quotidienne est réalisée chaque soir afin d'assurer la cohérence des données avec Active Directory. Un audit est également effectué chaque jour pour garantir cette synchronisation.

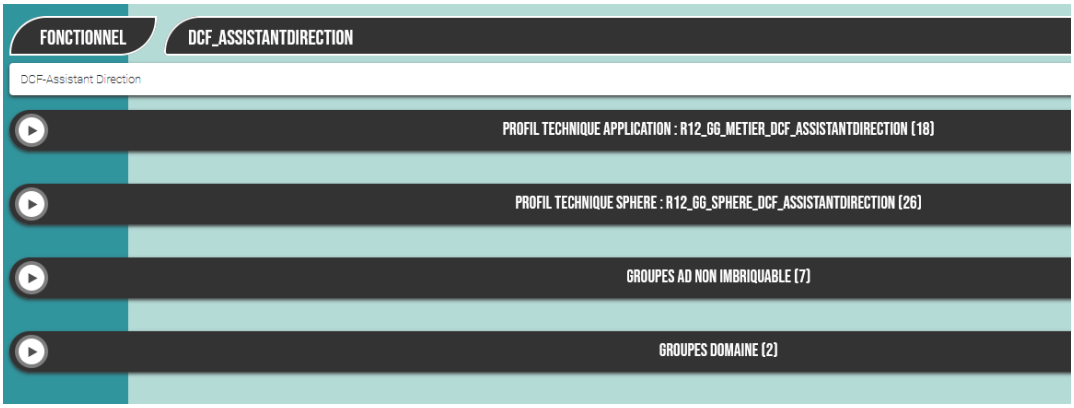
Une fois la demande traitée, il est impératif de vérifier dans GDDI que le droit a bien été attribué ou, en cas de suppression, qu'il a été correctement retiré.

Pour les demandes liées à GPM, celles-ci nous parviennent via l'outil DOIT. Ces requêtes sont particulièrement sensibles, car une erreur pourrait entraîner l'attribution de droits inappropriés à un métier. Il est donc essentiel de s'assurer que le métier concerné reçoit bien les droits correspondant à ses fonctions.

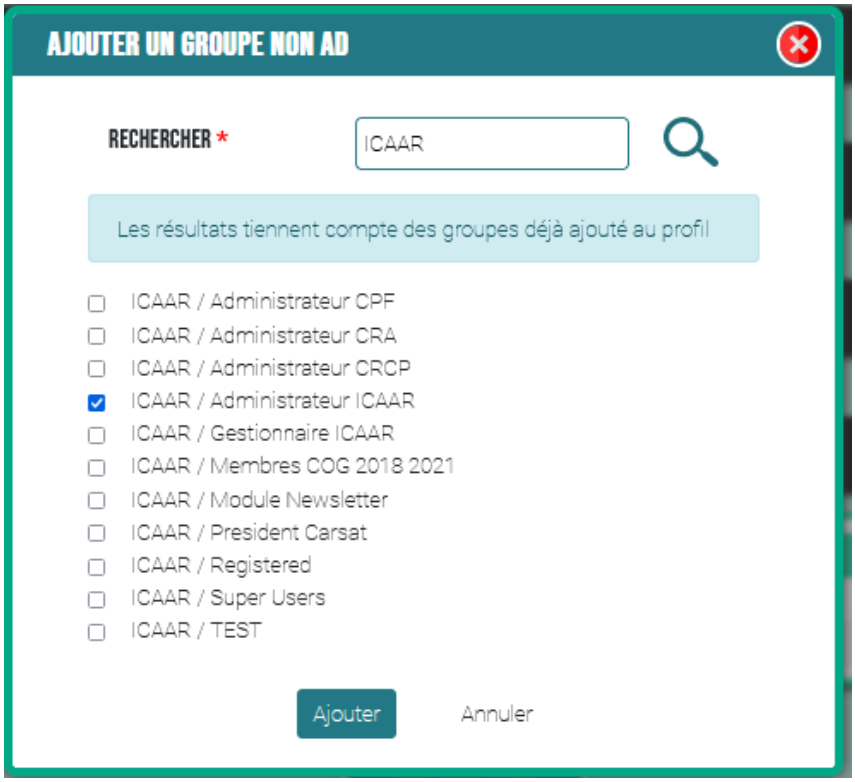
Dans GPM nous cherchons le Profil fonctionnel à mettre à jour



On consulte le profil métier pour le mettra à jour



S'agissant d'un groupe Domaine on développe le 4 élément et on ajoute l'habilitation
On sélectionne l'habilitation puis on l'ajoute et on vérifie sa présence dans la liste des groupes Domaine



2. Résolution de ticket DoIT

La mission la plus courante que j'ai réalisée durant mon stage a été la résolution d'incidents de sécurité. Cette tâche est particulièrement vaste, car elle couvre un large éventail de problématiques liées à la sécurité informatique.

Les demandes reçues via DOIT sont très variées : elles peuvent concerner des problèmes de droits d'accès, des alertes liées à des courriels de phishing, des notifications issues des outils de prévention des pertes de données (DLP), ou des remontées provenant de la surveillance externe effectuée par notre prestataire, qui scrute Internet à la recherche de fuites de données relatives à la CNAV. Ces demandes peuvent également porter sur l'attribution de logiciels, l'analyse de logiciels suspects, ou encore des alertes concernant des vulnérabilités ou attaques potentielles, etc.

La majorité des incidents de sécurité proviennent d'alertes émises par l'équipe SOC, responsable de la gestion centralisée des outils de sécurité. Lorsqu'une alerte est déclenchée, cette équipe nous sollicite pour enquêter et traiter la demande. Ce travail inclut une analyse approfondie, souvent accompagnée d'explications détaillées et d'éléments tels que des logs, des alertes antivirus, ou des rapports de diagnostic.

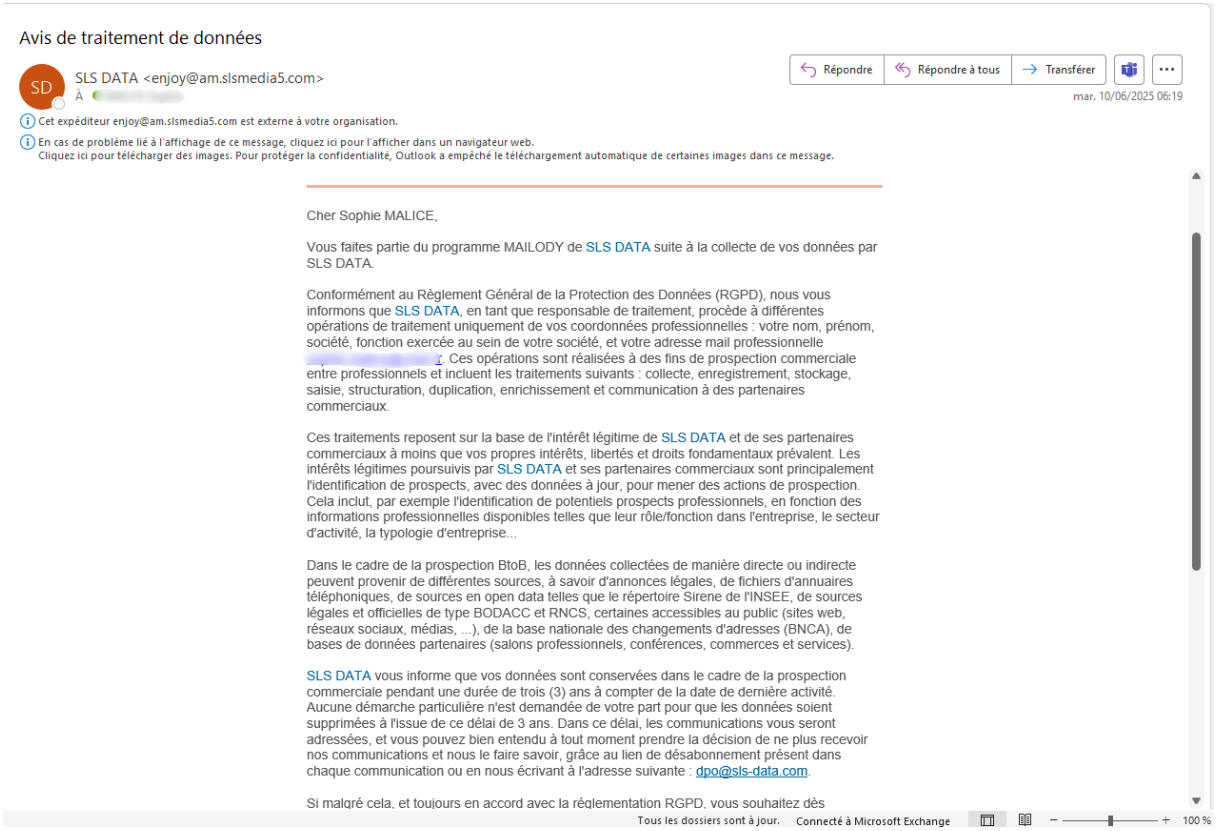
Nous devons alors analyser ces alertes, identifier la source du problème et mettre en œuvre les actions correctives nécessaires afin de résoudre l'incident. Un rapport de sécurité est systématiquement rédigé pour garantir une traçabilité complète de l'événement.

Étant donné la diversité des cas rencontrés, j'ai choisi de présenter trois situations représentatives, car il m'était impossible de détailler l'ensemble des incidents traités.

Cas 1

Contexte : Tous les utilisateurs disposent d'une boîte mail et sont donc exposés à des risques de phishing. Les signalements de mails suspects sont fréquents.

Dans notre cas, une utilisatrice a reçu un mail provenant apparemment d'une société à laquelle elle serait inscrite



Mail frauduleux reçu par l'utilisatrice

Ce mail, bien que faussement bienveillant, présente clairement les caractéristiques d'une fraude. L'utilisatrice, faisant preuve de vigilance, a signalé le message via un ticket DoIT.

Notre rôle est d'expliquer la procédure à suivre en cas de doute, afin qu'elle puisse signaler tout message suspect, mais également de vérifier qu'il s'agit bien d'un mail frauduleux, d'identifier son origine et d'en comprendre les intentions.

Après analyse de l'adresse électronique expéditrice, il s'est avéré qu'il s'agissait d'un spam déguisé émanant de la société SLS-DATA. Celle-ci propose un lien de désabonnement qui, en réalité, sert à confirmer la validité de l'adresse électronique en cas de clic. La société revend ensuite ces adresses électroniques à des entreprises pour du démarchage publicitaire.

Cas 2

Demande d'analyse de logiciel en mode non SaaS

Les utilisateurs ont des besoins spécifiques, chacun pouvant avoir certaines préférences ou des usages temporaires particuliers.

Dans notre cas, une utilisatrice a formulé une demande pour utiliser le logiciel Anki afin de préparer un examen en lien avec la CNAV. Une analyse de sécurité a donc été nécessaire pour évaluer si ce logiciel pouvait être installé sans risque. Un rapport a été établi afin de justifier que l'utilisation de ce logiciel ne représentait pas une menace pour l'environnement de la CNAV.

J'ai été chargé de réaliser cette analyse pour déterminer si Anki pouvait être accepté au sein de la CNAV. Dans ce cadre, j'ai présenté le logiciel en expliquant ses fonctionnalités et son utilité.

Une collecte d'informations a été réalisée, car plus celle-ci est complète, plus l'analyse est précise. Après quelques recherches, nous avons identifié plusieurs modes d'utilisation :

- Une utilisation en ligne, en mode SaaS. Ce mode nécessite une analyse approfondie et la mise en place d'un contrat spécifique.
- Une installation locale, via un agent, qui constitue une version non SaaS et représente une alternative possible.

L'utilisation d'Anki via Anki Web permet de stocker et synchroniser les cartes sur un serveur distant. Toutefois, cette solution comporte certains risques.

Nous avons néanmoins évalué une certaine fiabilité du mode SaaS, sous réserve de l'application de précautions spécifiques.

Cependant, nous avons constaté que, même dans ce mode, les mesures de sécurité liées à Anki ne sont pas suffisamment robustes.

Risques :

- Absence de chiffrement avancé pour le stockage des données.
- Fréquence limitée des mises à jour de sécurité du logiciel, étant open source.
- Possibilité d'installation d'adons créés par la communauté, qui peuvent contenir des logiciels malveillants.

Impacts :

- Exposition des données personnelles (vol des cartes, mots de passe et adresse courriel en cas de compromission du serveur).
- Installation de malwares via des extensions ou des cartes créées par la communauté.

Cependant nous allons donc collecter des informations sur l'utilisation en local d'Anki

L'installation d'Anki en local permet d'utiliser l'application sans connexion Internet, en stockant toutes les données directement sur l'ordinateur de l'utilisateur.

Risques :

- Une synchronisation involontaire avec Anki Web peut exposer les données aux mêmes risques que l'utilisation en ligne.
- L'installation de paquets de cartes téléchargés depuis Internet peut contenir des fichiers malveillants.

Impacts :

- Perte ou vol de données si la synchronisation est activée accidentellement.
- Infection par des malwares via des fichiers importés

Nous remarquons donc un réel problème dans le cas d'Anki, nous allons donc devoirs décider de si nous allons pouvoirs accepté le logiciel car cela passera en réunion d'arbitrage.

J'ai quand même procédé à une petite conclusion sur si le logiciel est accepté les mesures de sécurité qu'on doit prendre.

Anki propose deux modes d'utilisation : en ligne avec Anki Web et en local. La version en ligne présente des risques liés à la confidentialité et à la sécurité des données, notamment en cas de synchronisation ou d'installation d'adons non vérifiés.

La version locale, en revanche, ne nécessite pas la création de compte ni d'enregistrement d'informations personnelles, réduisant ainsi les risques de fuite de données. Toutefois, une sensibilisation des utilisateurs est essentielle :

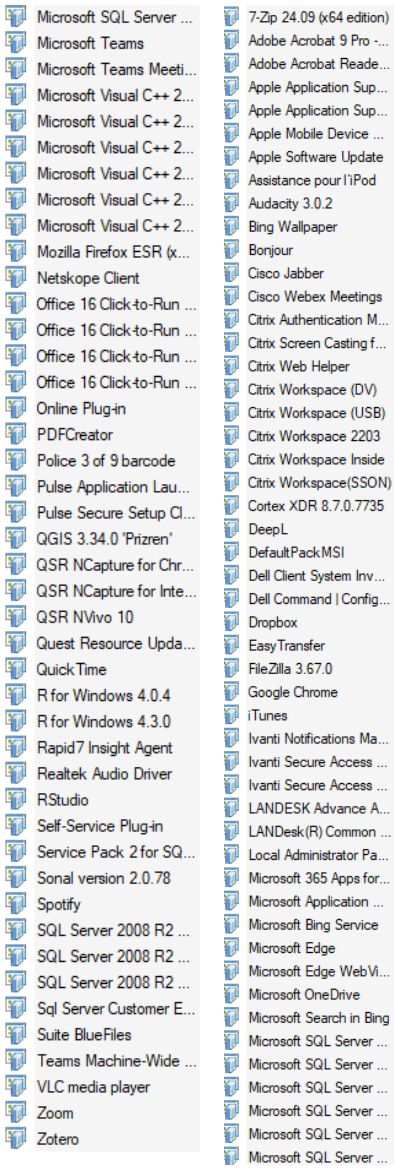
- Éviter toute synchronisation avec Anki Web pour préserver la confidentialité.
- Ne pas téléchargés de carte depuis internet.
- Maintenir le logiciel à jour pour éviter tout problème de corruption de donnée.

Cas 3

Contexte : L'utilisateur nous a contactés via DoIT en réponse à un mail envoyé par le RSSI, indiquant que toute personne ne répondant pas à nos sollicitations concernant la suppression de logiciels interdits sur leur poste verrait sa session verrouillée.

Dans sa demande DoIT, l'utilisateur sollicite une prolongation d'utilisation du logiciel Dropbox. Étant donné que ce logiciel n'est pas autorisé au sein de la CNAV, une étude approfondie a été nécessaire.

Dans un premier temps, par mesure de sécurité et pour prévenir tout incident, nous avons vérifié que l'utilisateur ne disposait pas d'autres logiciels interdits installés sur son poste. Nous avons donc procédé à une recherche des logiciels installés via Ivanti.



Résultat de la recherche de logiciel via Ivanti

Certains logiciels font partie du socle commun, c'est-à-dire qu'ils sont préinstallés lors de la mise en service d'un poste au sein de la CNAV.

Sur ce poste, nous avons constaté qu'un nombre important d'applications installées ne figurent pas parmi celles autorisées par la CNAV. Cela représente un risque majeur en matière de sécurité, car ces logiciels ne bénéficient pas de mises à jour automatiques ou centralisées, n'étant pas gérés par la CNAV. De plus, plus le nombre d'applications non maîtrisées est élevé, plus la surface d'attaque potentielle augmente.

- Spotify (fournisseur suédois de services multimédias et de streaming audio)
- Zoom (Logiciel de visiophonie)
- DeepL (DeepL est un service de traduction automatique utilisant IA)
- DropBox (Application/site d'hébergement de fichiers proposant comme service le stockage, le partage de fichiers en ligne ainsi que la signature électronique)
- easyTranfert (application qui rend possible les transferts d'argent entre les différents opérateurs de monnaie électronique.)
- Zotero (Zotero est un logiciel de gestion de références bibliographiques multiplateforme)
- QGIS (logiciel destiné au traitement des données géographiques.)
- QSR (extension de navigateur Web qui permet de collecter du contenu Web à importer dans NVivo(logiciel d'analyse capable d'enrichir vos données non-structurées))
- R for windows (Créer des visualisations à partir de vos ensembles de données)
- R Studio (environnement de développement gratuit)
- Sonal (logiciel gratuit d'enquête qualitative)
- Audacity (logiciel d'enregistrement de son numérique et d'édition de sources audionumériques)
- Google Chrome (un navigateur web)
- Quicktime (Lecteur vidéo)

Liste des logiciels interdits sur le poste de l'utilisateur

Nous avons identifié 15 applications non réglementaires au sein de la CNAV. Il a donc été nécessaire de faire appel à l'équipe du P2I afin de demander la suppression de ces logiciels, ainsi qu'une analyse antivirale pour s'assurer que l'utilisateur n'était pas contaminé par un quelconque malware.

Une fois ces actions réalisées, j'ai contacté l'utilisateur via Teams afin de recueillir des informations en posant plusieurs questions : pourquoi avait-il besoin d'utiliser cet outil ? Quelle en était son utilisation précise ? La collecte du maximum d'informations était cruciale.

Après ce premier échange et une prise en main à distance avec l'utilisateur, nous avons découvert plusieurs fichiers très sensibles, enregistrés dans Dropbox, utilisés pour partager des documents avec des personnes extérieures à l'organisation. Ce logiciel était installé depuis plus de 10 ans. Les données synchronisées sur les serveurs comprenaient des informations médicales, professionnelles, des anecdotes familiales, des lieux de naissance, etc. Pour donner suite à cette découverte, une enquête approfondie a dû être menée.

Nous avons ensuite dû vérifier la conformité du logiciel. Après recherches, nous avons constaté que Dropbox stocke les données aux États-Unis. La CNIL met en garde les entreprises contre la transmission de données à des prestataires américains, en raison de règles de protection des données différentes. Certaines entreprises sont référencées comme fiables sur un site dédié, mais Dropbox n'en fait pas partie. Dropbox ne respecte pas le RGPD.

Nous avons recensé plus d’une dizaine de fuites de données critiques impliquant Dropbox au cours des 12 dernières années.

Nous avons donc alerté notre service interne en charge de la gestion des données ainsi que les directeurs, qui ont décidé de prendre des mesures, incluant la possibilité de sanctions.

De nombreuses vérifications ont été réalisées, notamment pour déterminer si l’adresse électronique utilisée lors de la création du compte Dropbox était professionnelle ou personnelle, ainsi que pour comprendre comment le pare-feu avait pu autoriser le partage de fichiers vers l’extérieur.

3. Mise a jours de documentation

PSSI

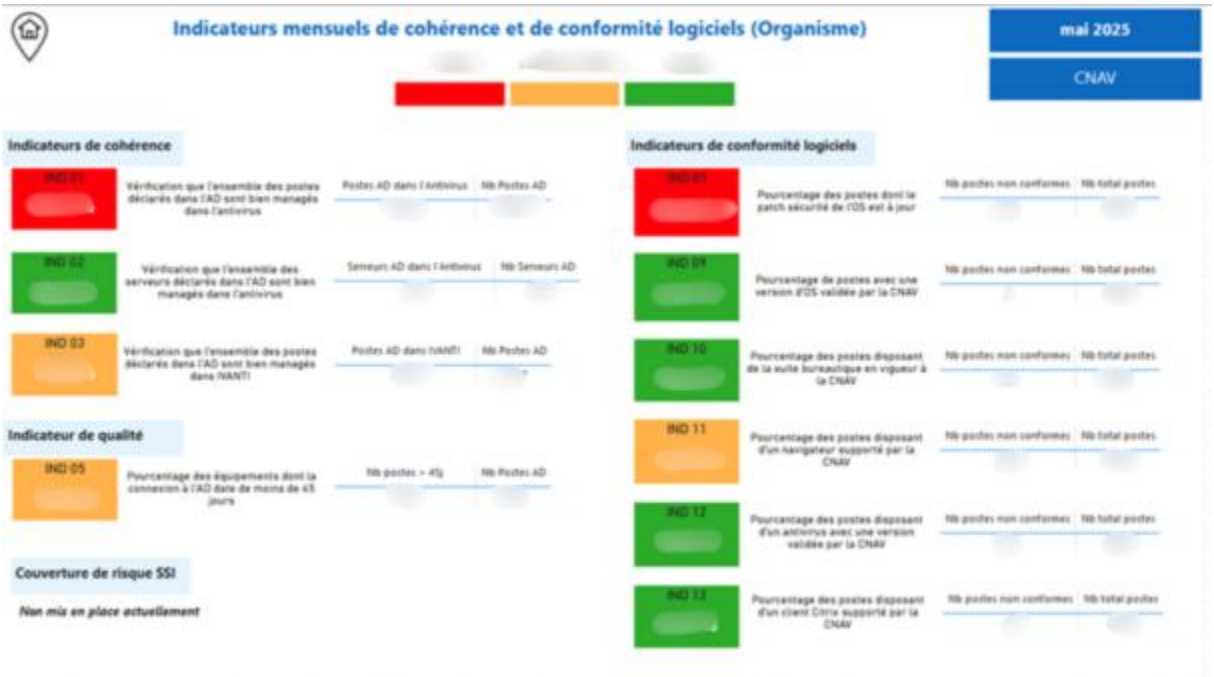
La PSSI, ou Politique de Sécurité des Systèmes d'Information, est un document stratégique qui permet à une organisation/entreprise, administration ou association de structurer sa démarche de cybersécurité. Il ne s'agit pas simplement d'un ensemble de règles techniques, mais plutôt d'une vision globale qui définit comment protéger efficacement le patrimoine numérique de l'organisation.

Concrètement, il sert à établir un cadre cohérent pour identifier les menaces, évaluer les risques, définir les responsabilités de chacun, et mettre en œuvre des mesures adaptées pour protéger les données et les systèmes. Cela inclut la protection contre les cyberattaques, les pertes de données, les erreurs humaines ou encore les défaillances techniques. Le PSSI détermine qui peut accéder à quoi, dans quelles conditions, et avec quels niveaux de contrôle.

C'est aussi un outil de communication interne. Il aide à sensibiliser les collaborateurs à la sécurité informatique, à créer une culture de vigilance, et à garantir que tout le monde adopte des comportements responsables.

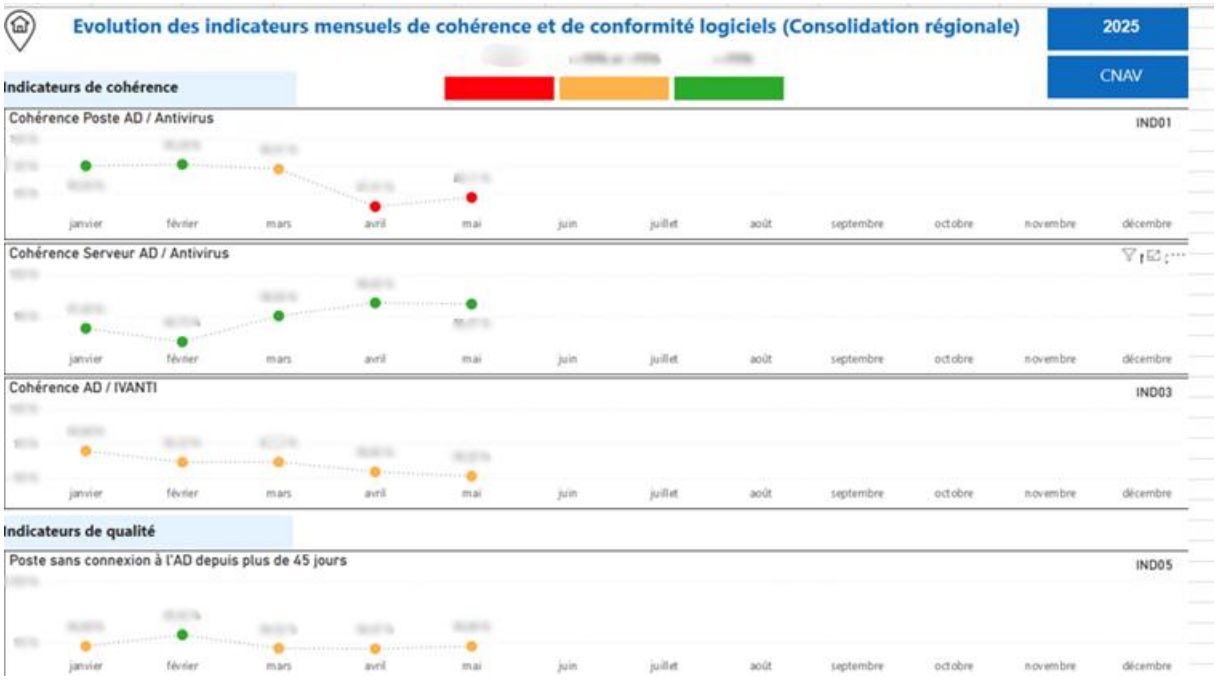
Enfin, sur le plan légal, un PSSI bien construit permet de démontrer sa conformité avec des textes comme le RGPD ou la loi de programmation militaire, et d'être prêt en cas de contrôle ou d'audit.

Dans notre cas nous travaillons sur un fichier Excel appelé tableau de bord, l'objectif est de fournir au nationale l'information sur la CNAV demandé. Nous avons donc la mission de mettre à jours le fichier Excel afin de le retransmettre au national. Le fichier se présente sous cette forme :



Indicateurs mensuels de cohérence et de conformité logiciels

Le PSSI permet de suivre l'évolution des mesures de sécurité mises en place, notamment à travers des indicateurs visuels tels que des graphiques et des courbes de progression.



Evolution des indicateurs mensuels de cohérence et de conformité logiciels

Ce tableau de bord permet d'assurer un suivi des mesures de sécurité mises en œuvre, notamment en ce qui concerne la mise à jour des postes informatiques. Il offre une vision claire de l'avancement global et de la conformité du parc informatique.

Ma mission a consisté à actualiser le fichier Excel avec les données extraites de Power BI, en y intégrant les évolutions observées mois après mois.

Ces informations sont ensuite transmises à l'équipe nationale, qui consolide l'ensemble des PSSI des différentes structures afin d'évaluer l'état global de la sécurité au sein de la CNAV, en identifiant les zones à risque ou les écarts de conformité

Modèle rapport d’incident de sécurité

Les rapports de sécurité sont des éléments essentiels dans la gestion des incidents. Ils permettent de conserver une trace structurée des événements, des actions menées, des dates clés, ainsi que des éléments de contexte, afin d’assurer une traçabilité complète.

Ces rapports peuvent être consultés par divers interlocuteurs, tels que des directeurs, des membres du service SSI ou encore de nouveaux collaborateurs. Il est donc crucial qu’ils soient clairs, complets et compréhensibles par tous, quel que soit le niveau technique du lecteur.

Dans le cadre de mon stage, j’ai décidé de revoir et d’améliorer le modèle de rapport d’incident utilisé au sein de la CNAV. Certains outils mentionnés dans l’ancien modèle n’étant plus utilisés (par exemple, Lansweeper remplacé par Ivanti, ou Symantec par Cortex), une mise à jour s’imposait pour garantir la cohérence avec les outils actuellement en place (voir annexe 1).

Lors de cette révision, plusieurs lacunes importantes ont été identifiées :

- Absence de date d’ouverture du ticket DoIT
- Absence de mention de la direction concernée (utile car chaque direction utilise des outils différents)
- Manque d’explication sur les outils utilisés dans l’analyse
- Rubrique “prise de contact” trop vague, sans informations sur le ressenti de l’utilisateur ni sur les échanges réalisés
- Actions menées listées de façon trop générale, sans distinction entre les actions réalisées et celles en cours ou à déléguer
- Absence de conclusion ou de résultat clair permettant de clôturer le rapport

J’ai donc proposé une nouvelle version de ce modèle de rapport, plus détaillée et adaptée aux besoins opérationnels du service. Ce modèle vise à assurer un suivi rigoureux de chaque incident et à faciliter la compréhension du dossier par toute personne amenée à le consulter (voir annexe 2).

VI) Conclusion

J’ai effectué un stage de 8 semaines au sein de la CNAV dans le service SSI.

Ce stage a été une expérience plus que bénéfique pour moi. Les personnes qui m’ont pris en charge ont fait preuve d’une grande confiance et m’ont laissé en totale autonomie, ce qui m’a permis d’apprendre et de me forger une idée concrète du monde de la sécurité informatique. J’ai pu constater l’importance de la rigueur, de l’analyse et de la traçabilité dans un environnement aussi critique, et mieux comprendre la réalité du métier.

L’environnement dans lequel j’ai évolué était particulièrement stimulant. J’ai eu l’opportunité d’être pleinement acteur, d’émettre des propositions, et de voir que mon avis comptait réellement au sein de l’équipe. Cette reconnaissance m’a encouragé à m’impliquer davantage et à développer mon sens de l’initiative. J’ai été totalement autonome dans la gestion de certaines missions, ce qui m’a permis de gagner en assurance et en maturité professionnelle.

En revanche, le stage s’est rapidement montré très technique, avec un niveau d’exigence élevé et un volume de travail conséquent. Certaines tâches comportaient une réelle responsabilité, notamment en lien avec les incidents de sécurité et la sécurité des systèmes, ce qui a pu être stressant par moments. De plus, le travail réalisé était très orienté vers l’analyse, la gestion des risques la conformité, la sensibilisation et non vers la configuration ou l’intervention technique directe.

Ce stage a renforcé ma passion pour la cybersécurité et a confirmé ma décision de poursuivre mes études avec une licence informatique, une étape importante dans ma quête d'une carrière dans ce domaine. Il m’a permis de comprendre la réalité du terrain, de faire le lien avec les connaissances acquises en cours, et d’apporter une réelle contribution au service malgré mon statut de stagiaire.

ANNEXE

Annexe 1

Cnav Retraite & Action sociale — Sécurité sociale	Rapport-NomOrdinateur-User Confidentiel – Diffusion restreinte aux destinataires	DIE

1. Contexte

Incident DOS0XXXX ouvert par XXXX XXXXX :

[Copié-collé du résumé de la demande DOIT + capture d'écran des graphiques]

2. Analyse

2.1 Liste logiciels installés

[Via Lansweeper faire une vérification de tous les softwares installés, pour potentiellement identifier des programmes suspects.]

2.2 Antivirus

[Exporter le rapport de la plateforme Symantec en mettant en avant les Attack Signature

https://www.broadcom.com/support/security-center/attacksignatures?

SOURCE : Console SYMANTEC : https://sepmconsole.infra.n18.an.cnav:8443/console/apps/sepm

2.3 Prise de contact

[Lister les modalités de prise de contact avec l'utilisateurs, teams à distance et le déroulé du scénario]

3. Action.

[Lister toutes les actions effectuées, étape par étape]

4. Résultat

[Lister tous les résultats des précédentes actions accomplies, si présence de virus tenter de l'identifier et d'effectuer des recherches dessus.]

Annexe 2

l'assurance retraite CAISSE NATIONALE	Rapport-NomOrdinateur-Login-NomPrénom-Direction	

1. Contexte de l'incident

Incident DOS0XXXX :

Date de l'incident :

Nom du service de l'utilisateur :

[Copié-collé du résumé de la demande DOIT + capture d'écran des graphiques]

2. Recueil d'informations et analyse

2.1. Logiciels installés

[Via Ivanti, effectuer une vérification de tous les logiciels installés afin d'identifier potentiellement des programmes suspects. Les lister et fournir une brève présentation du/des logiciel(s) en question]

2.2. Prise de contact

- Date de prise de contact
- Explication du contexte fourni par l'utilisateur ou recueil de toutes explications possibles fournies par celui-ci

3. Actions

3.1. Actions mises en œuvre

[Liste des actions entreprises sur le poste de l'utilisateur : Lister toutes les actions effectuées, étape par étape]

3.2. Actions restant à mettre en œuvre

- Demander aux P2I d'effectuer une recherche antivirale sur le(s) poste(s) de(s) l'utilisateur(s) et de nous transmettre les résultats
- Décrire les autres actions entreprises et/ou demandées
  Exemple : suppression d'un exe avec n° de DoIT associer

3.3. Résultats des actions à mettre en œuvre

[Lister tous les résultats des actions précédemment accomplies ainsi que toute information annexe]

4. Synthèse

[Explication de la menace, fonctionnement, origines, mode de diffusion…]