LIVRE BLANC

Piloter le plan d'action de votre feuille de route Sécurité PSSI

Gouvernance, indicateurs, tableaux de bord, outils

JUIN 2022

Les intrusions critiques ont progressé de **37 %** en 2021, d'après l'Agence nationale de la sécurité des systèmes d'information (ANSSI). Jamais le nombre d'entreprises victimes de malveillance informatique n'a été aussi élevé !

Alors que la généralisation des usages numériques et du télétravail continue de représenter un défi de taille, l'ANSSI observe une amélioration constante des capacités des acteurs malveillants. Dans ce contexte, **comment maîtriser les risques liés à la cybersécurité de manière efficace et systématique** ?

Vous recherchez des solutions concrètes pour **transformer votre PSSI en plan d'action** ? Pour **suivre les indicateurs et la réalisation des projets** ?

L'objectif de ce Livre Blanc est de présenter les **enjeux liés au pilotage d'une PSSI**, puis de vous livrer des conseils pratiques pour créer vos **tableaux de bord SSI** et choisir les **bons indicateurs de suivi**.

Sommaire

La création d’un plan d’action SSI

Les objectifs d’une Politique de Sécurité des Systèmes d’Information (PSSI)

> « ***Une Politique de Sécurité des Systèmes d’Information reflète la vision stratégique en matière de Sécurité des Systèmes d’Information (SSI) et de gestion de risques SSI. Elle décrit les éléments stratégiques (enjeux, référentiels, principaux besoins de sécurité et menaces) et les règles de sécurité applicables à la protection du système d’information de l’organisme.*** »
>
> ANSSI

Un défi de taille attend alors le responsable de la PSSI :

- Faire en sorte que les équipes ainsi que la Direction obtiennent le **même niveau d’information**.
- Faciliter la **communication top-down et bottom-down** autour des politiques et règles de sécurité.
- Assurer le **pilotage du plan d’action** associé à la vision stratégique globale.

💡 La Politique de Sécurité des Systèmes d’Information s’élabore sur mesure. Toutefois, on y retrouve en règle générale les éléments suivants :

- le périmètre d’application de la PSSI et les acteurs impliqués,
- les enjeux de sécurité de l’entreprise ou de l’administration,
- le cadre légal et règlementaire à respecter,
- les menaces qui pèsent sur le système d’information et le patrimoine à protéger,
- l’identification et la rédaction des principes et règles de sécurité.

La création d’un plan d’action SSI

L’élaboration d’un plan d’action SSI

Dès lors que la PSSI a été élaborée puis validée par la Direction Générale, il convient de **mettre en application les règles de sécurité définies**.

C’est là qu’intervient le **plan d’action SSI**.

En effet, la mise en œuvre progressive de la Politique de Sécurité des Systèmes d’Information au travers d’un plan opérationnel contribue à contrôler la déclinaison de la stratégie globale.

Elle permet notamment :

- ➔ de décider le **séquencement des mesures à conduire**, car toutes ne seront pas déployées de manière simultanée ;
- ➔ de **mesurer l’avancée des opérations**. À ce titre, le plan d’action constitue un outil de suivi pour le manager ou responsable SSI, mais également de communication vers la Direction.

💡 **L’élaboration d’un plan d’action SSI se réalise en 4 étapes principales :**

- 1. Fixer les responsables des règles de sécurité à mettre en place (Quoi ? et Qui ?).
- 2. Évaluer les ressources requises (Comment ?).
- 3. Prioriser les objectifs de déclinaison opérationnelle des règles, au moyen de jalons prédéterminés.
- 4. Faire valider la méthodologie et sa déclinaison par la direction.

La création d'un plan d'action SSI

[Interview] L'élaboration d'un plan d'action SSI

Interview de Yohann BAUZIL, ex-Chief Information Security Officer d'Airbus OneWeb Satellites

Quelle est la place de la sécurité au sein d'Airbus OneWeb Satellites ?

Le pôle sécurité a une équipe dédiée. Pourtant je dirais que dans le meilleur des mondes, il ne devrait pas y avoir d'équipe sécurité avec simplement une application des process. Mais l'humain reste un point de vigilance. Même si, je dois en convenir, nos collaborateurs ont une vraie sensibilité et une culture sur l'application des principes de sécurité.

Comment l'idée d'un pôle sécurité s'est imposée ?

Le pôle sécurité a émergé assez vite. La SSI (dans l'IT) devient vite un plafond de verre quand on n'a pas de legacy et que l'architecture est mise en place. Un levier de cette évolution a été le RGPD. La DSI avait impulsé les démarches en mai 2017 pour une mise en place effective à partir de mai 2018. Cela m'a amené à devenir correspondant informatique et liberté, puis, logiquement DPO. Cela s'est étoffé avec mon rôle d'adjoint du responsable du site de Toulouse en charge de la sûreté industrielle.

De trois casquettes : RSSI, Officier de Sécurité et DPO, nous avons fait un chapeau de « CISO » (Chief Information Security Officer) en charge du pôle sécurité.

À noter que cette approche est possible au sein d'une petite structure comme AOS SAS (ndlr : environ 150 personnes). Nous ne sommes pas confrontés à des approches en silo comme on peut le voir dans des structures de tailles plus conséquentes.

En termes d'organisation, le pôle sécurité est-il rattaché à la DSI ?

Au lancement en 2017, oui (ndlr : l'entreprise a été créée en 2016). À partir de 2019, nous avons créé un pôle sécurité dédié pour mieux intégrer la sûreté industrielle et le RGPD. Naturellement, le pôle sécurité s'est rattaché à la Direction Générale. C'est le bon rattachement, notamment pour éviter de potentiel biais de jugement sur le volet IT. Quand un CISO gère la sûreté industrielle, c'est tout sauf un sujet IT. La mission est transverse. Son rattachement logique c'est la Direction Générale.

Vous avez une approche sécurité très matricielle avec de multiples rattachements ?

Oui, car notre rôle est avant tout de fédérer. Le RGPD, par exemple, est avant tout un sujet légal. La sûreté industrielle est très imprégnée de la notion de site. La sécurité des SI doit être structurellement intégrée au métier d'une Direction Informatique. Donc ce triple rattachement est inhérent à la fonction de sécurité et avec pour mission de fédérer.

Comment s'est construite votre Feuille de route sécurité 2017-2020 ?

Je me suis appuyé sur l'analyse des risques pour structurer les principales mesures :

- ➔ **Mesure organisationnelle** avec la mise en place de trois responsabilités (sécurité des systèmes d'information, data protection, sûreté industrielle).
- ➔ **Mesure technique** avec la mise en place de solutions techniques en s'appuyant notamment sur les moyens offerts par le fait d'être une filiale d'Airbus.
- ➔ **Être en veille permanente** : la difficulté n'est pas de faire… mais de savoir ce qu'on veut faire et ce qu'on doit faire. Notre compétence se périme très vite. En deux mois, nous perdons notre expertise. Mettre en place un état d'esprit de « qui-vive » est primordial.

La création d’un plan d’action SSI

[Cas pratique] Feuille de route SSI au sein d’une collectivité

Interview de Marylyne Boubee, Responsable de Sécurité des Systèmes d’Information (RSSI) du Conseil départemental de Haute-Garonne

Quels enjeux pour le Conseil Départemental de la Haute-Garonne ?

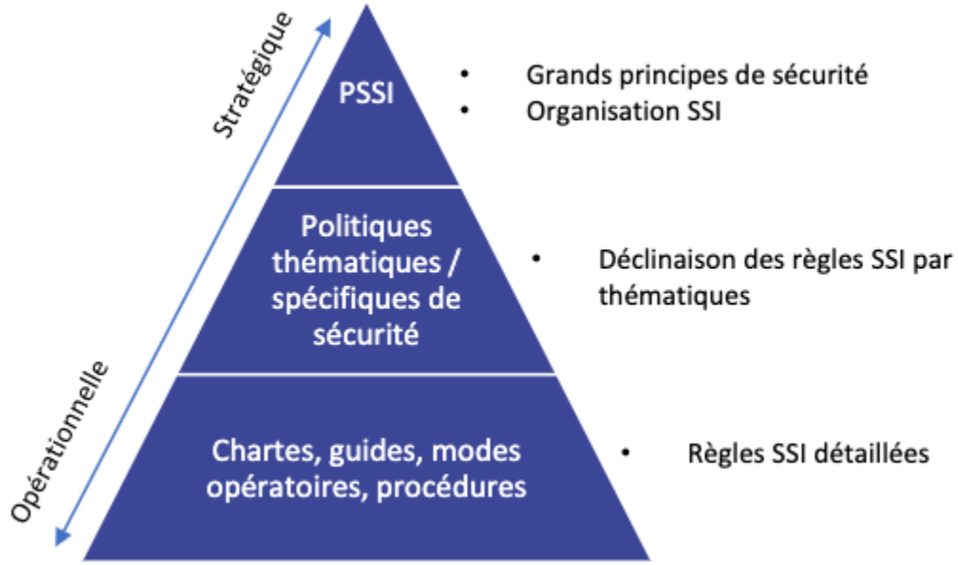
La Direction Générale du département a été interpellée par les chiffres liés à la cybersécurité. En effet, depuis le début de la crise sanitaire, +400 % de cyber menaces ont été recensées !

Dans ce contexte, une PSSI constitue un plan d’action pour maintenir un niveau de sécurité en adéquation avec les enjeux de la collectivité, et reflète sa vision stratégique en matière de Sécurité du Système d’Information.

Quelle démarche a été adoptée ?

La RSSI du département de la Haute-Garonne porte une démarche ambitieuse autour de la cybersécurité, intégrant de nombreux enjeux, en particulier l’**ampleur de son système d’information** :

- 250 logiciels et applications métiers,
- 2 653 postes fixes,
- 3 829 PC portables, etc.



Le Conseil Départemental a donc fait le choix d'une politique alignée avec les spécificités d'une collectivité territoriale : il a d'abord édicté les grands principes de sécurité dans le cadre d'une PSSI très générique, avant de les décliner en politiques thématiques/spécifiques, destinées à être réévaluées plus fréquemment.

Pour coordonner tous les actions et projets découlant de cette PSSI, le département a :

- élaboré une feuille de route dédiée au Système de Management de la Sécurité de l'Information ;
- mis en place un pilotage à 3 étages, impliquant différents comités :
    - au niveau stratégique : le Comité de Sécurité du Système d'Information (COSSI), participant à la vision stratégique et se réunissant au moins une fois par an. Il permet de faire le bilan annuel des actions menées et de valider les points importants.
    - au niveau tactique : le Comité Technique de Sécurité du Système d'Information (CTSSI), qui se tient tous les mois. Son objectif : suivre l'avancement du PSSI, passer en revue les différents indicateurs et prendre certaines orientations.
    - au niveau opérationnel : les comités de pilotage projets IT.
      Ces revues de projet se déroulent toutes les quinzaines environ et servent à observer le déroulement du plan d'action.

La gouvernance de projets autour de la cybersécurité

[Interview] L'élaboration d'un plan d'action SSI

Interview de Yohann BAUZIL, ex-Chief information Security Officer d'Airbus OneWeb Satellites

Comment s'invite le sujet sécurité dans votre gouvernance projets ?

Nous restons dans un état d'esprit start-up avec la nécessité de construire vite. Nous avons une approche tripartie :

- Le business — à qui nous demandons de raisonner en besoin (même si une fois sur deux ils arrivent déjà avec des solutions techniques plutôt qu'une formulation de besoin).
- L'IT propose une solution technique en regard du besoin.
- La sécurité va valider la proposition technique. Cela est facilité par notre proximité originelle avec l'IT. Donc il est rare d'avoir des solutions ne répondant pas à nos exigences.

Comment se passe le dialogue avec les équipes IT ?

Nous venions presque tous du « même monde ». Donc, nous avons des schémas de pensée et de raisonnement de mise en œuvre communs. Nous sommes dans une démarche très vertueuse. Je n'ai pas souvenir d'avoir un jour dit « non » à une de leur proposition.

Comment se passe le dialogue avec le métier, le business ?

Ma seule difficulté, et elle est extrêmement limitée et rare, c'est le shadow it. Le business a les compétences pour avancer sans nous. Donc ils pourraient tout à fait mettre à profit les ouvertures du SI pour mettre en place des solutions sans passer par nous. Mais c'est extrêmement rare.

Le métier de RSSI est tout sauf un métier technique. C'est plus d'aider le business à exprimer un besoin. Un exemple type : le business me demande la mise en place d'un serveur FTP. Ce qui est une solution. Alors que le véritable besoin, c'est d'envoyer des fichiers volumineux en toute sécurité entre un site A et un site B.

Nous sommes une fonction support. Je n'ai pas de légitimité à dire non à un besoin. Je peux simplement demander des ajustements à la solution ou suggérer des solutions pour le besoin.

Comment séquencez-vous votre pilotage, comitologie ?

Nous avons un suivi d'équipe tous les quinze jours avec un suivi opérationnel sur les projets, avec une priorisation des actions. À noter qu'au moins 50 % des projets sécurité sont des projets « IT ».

Cela fait l'objet d'un compte rendu avec production de KPI pour les donneurs d'ordre du pôle sécurité (Président AOS SAS & COO).

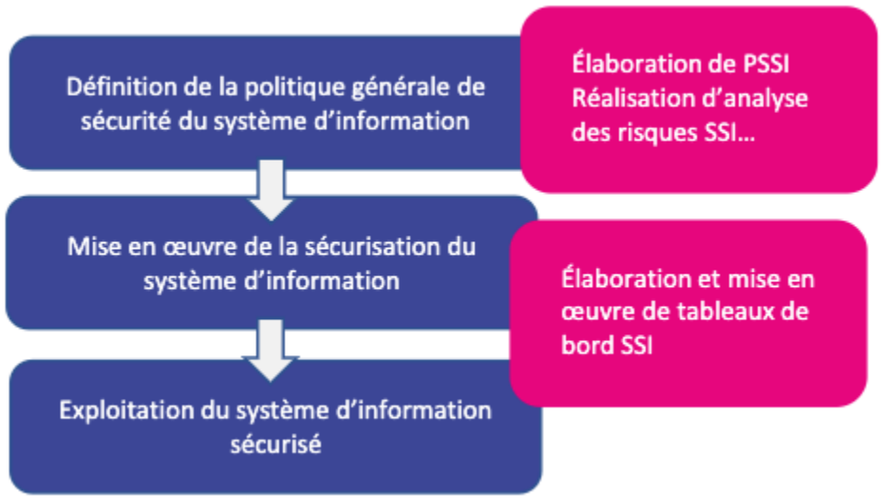
Nous avons en complément un suivi bimensuel avec le COO et un suivi mensuel avec le Président de l'entité Française. Cela s'élargit également à la branche états-unienne. Ces instances sont dédiées à la sécurité.

La gouvernance de projets autour de la cybersécurité

Mettre en place des indicateurs de suivi de la PSSI

Mettre en place des indicateurs de suivi permet :

- ➔ D'apprécier le **niveau de sécurité** et adapter ses priorités d'actions.
- ➔ De mettre en place un **moyen de communication** du RSSI vers les responsables métiers des différents départements de l'entreprise.
- ➔ D'améliorer leur information et leur compréhension du niveau de sécurité, et d'obtenir leur support et leur coopération.
- ➔ De mettre en place un **reporting** du RSSI vers sa Direction.



💡 Construisez les indicateurs selon les niveaux de suivi.

Les tableaux de bord permettent :

➔ **Pour le niveau stratégique :**

- de suivre l'application de la politique de sécurité ;
- d'établir des comparaisons avec d'autres organisations ;
- de préparer les choix de mise en place des ressources (définition de priorités, réévaluation de la menace et du risque).

➔ **Pour le niveau de pilotage et de coordination :**

- de contrôler la réalisation des objectifs par le niveau opérationnel ;
- d'améliorer la qualité de service.

➔ **Pour le niveau opérationnel :**

- de préciser les besoins opérationnels à mettre en œuvre ;
- de mesurer la production et les efforts entrepris pour atteindre les objectifs visés en matière de production ;
- de motiver et dynamiser les équipes.

La gouvernance de projets autour de la cybersécurité

Les étapes pour mettre en place des indicateurs de suivi de la PSSI

1 Établir vos objectifs de sécurité.

2 Identifier les destinataires des tableaux de bord SSI.

3 Comprendre la finalité des tableaux de bord SSI (alerte, prise de décision, information).

4 Lister les points de comitologie et instances de pilotage.

5 Cartographier les sources d'obtention des données.

6 Le calendrier de progression des projets de la PSSI.

La gouvernance de projets autour de la cybersécurité

Fiche pratique pour mettre en place des indicateurs de suivi de la PSSI

	ℹ	Questions à vous poser
Objectifs de sécurité	Ces objectifs découlent de la politique de sécurité établie au préalable, et se déterminent en grande partie par l'analyse des différents risques pesant sur votre organisation.	• Quels sont les objectifs de la politique de sécurité ? • Comment mesurer qu'ils sont atteints ?
Identification des destinataires des tableaux de bord SSI	La composition d'un tableau de bord SSI est intimement liée aux personnes qui auront à s'en servir. Avant d'initier la conception de tableaux de bord SSI, il est impératif d'en connaître le niveau d'utilisation pour choisir des indicateurs adaptés.	• Quels sont les métiers concernés ? • Quels tableau de bord les concernent (opérationnel ; pilotage ; stratégique) ?
Utilisation prévue des tableaux de bord SSI	Pour chaque destinataire identifié, identifier en fonction de ses prérogatives le type de tableau de bord qui le concerne. Interroger les destinataires sur l'usage qu'ils envisagent des tableaux de bord SSI qui leur seront fourni, au travers de leurs prérogatives vis à vis de la sécurité du système étudié.	• Quels types de décisions peuvent-ils être amenés à prendre ? • Quelles actions peuvent-ils mener ? • Sur quels points un tableau de bord SSI peut-il les informer au mieux pour les aider dans leurs tâches ?
Les points de comitologie et instances de pilotage	Les instances de pilotage sont les acteurs fondamentaux du développement et de la pérennité de tous vos projets. Elles jouent un rôle essentiel dans le suivi de vos projets et dans la conduite du changement. En effet, en ces temps de forts changements, le rythme s'est prodigieusement accéléré. Un projet stratégique difficile à mener doit évidemment être mieux contrôlé qu'un projet « annexe » de faible difficulté.	• Quelles sont les différentes instances de gouvernance de pilotage ? • A quelle fréquence se réunissent-elles ? • A quels enjeux majeurs ces instances de gouvernance projet peuvent-elles répondre ? • Sur quels indicateurs peuvent-elles se baser pour suivre les objectifs ?
La connaissance des possibilités d'obtention de données sources	Ce travail consiste à établir, en collaboration avec les interlocuteurs techniques et fonctionnels, les sources de données utilisables dans le système étudié, dans l'objectif de suivre les différents indicateurs et d'élaborer le tableau de bord.	• Quelles sont les sources de données disponibles ? • Comment les données sont-elles gérées ? • Des interfaces sont-elles possibles ?
Le calendrier de progression des projets de la PSSI	On entre dans le phasage de mise en œuvre des mesures de sécurité. Autrement dit, mettez en place un "échéancier" de réalisation, jalonné de niveaux intermédiaires, pour suivre la progression des actions.	• Quels projets sont prioritaires ? • Quelles sont les phases et jalons ? • Il y a-t-il des dépendances entre projets ?

La gouvernance de projets autour de la cybersécurité

Exemples d'indicateurs

Le choix des indicateurs, et leur représentation lors de l'élaboration d'un tableau de bord SSI, repose sur 3 types d'indicateurs :

- ➔ **Les indicateurs stratégiques**, pour suivre le management de la sécurité et l'organisation du SMSI (Système de Management de la Sécurité des Informations, au sens de la norme ISO 27001).
- ➔ **Les indicateurs relatifs au pilotage et à la coordination**, afin d'apporter un éclairage sur la connaissance des risques et sur leur maîtrise par toutes les directions métier de l'organisation.
- ➔ **Les indicateurs opérationnels**, destinés à suivre le niveau de sécurité réel obtenu dans les divers domaines (sécurité des personnes, des locaux, des documents, des systèmes d'information, des incidents, de la conformité, etc.).

Les indicateurs stratégiques

- Taux de projets menés selon les règles de la PSSI,
- Nombre d'incidents de sécurité SI significatifs,
- Nombre de violations de données à caractère personnel, ▪ Nombre de collaborateurs formés,
- Nombre d'analyses de risques nouvelles ou mises à jour, ▪ Nombre de risques critiques couverts et non couverts,
- Nombre de risques critiques réduits, etc.

Les indicateurs de pilotage

- Nombre d'incidents avérés,
- Nombre d'alertes,
- Nombre d'applications configurées de manière sécurisée,
- Évaluation de la pratique du shadow IT,

- Taux de postes de travail et serveurs disposant des derniers correctifs,
- Taux de postes de travail et serveurs disposant d'un logiciel antiviral à jour,
- Nombre d'audits réalisés,
- Nombre d'analyses de risques effectuées, etc.

Les indicateurs opérationnels

- Nombre de dispenses au référentiel,
- Nombre d'applications ayant fait l'objet d'un audit,
- Nombre d'applications ayant fait l'objet d'un test d'intrusion,
- Taux d'accès standard recertifiés,
- Taux d'accès privilégiés recertifiés,
- Taux d'installation des correctifs de sécurité par application,
- Taux de serveurs (par environnement) avec les derniers correctifs de sécurité,
- Taux de postes de travail (par environnement) avec un logiciel antiviral à jour,
- Taux de serveurs (par environnement) avec un logiciel antiviral à jour,
- Taux de règles pare-feux revues selon une fréquence donnée, etc.

La mise en œuvre efficace de votre PSSI grâce aux outils de pilotage

[Cas pratique] De la feuille de route aux outils pour accompagner la PSSI

Interview de Marylyne Boubee, Responsable de Sécurité des Systèmes d'Information (RSSI) du Conseil départemental de Haute-Garonne

Pour mener à bien ses projets sécurité, le Conseil Départemental compose avec un certain nombre d'outils, tels que :

- **des logiciels de bureautique** : réalisation des templates d'analyse, des audits, etc.,
- **Cyberwatch** : scan des vulnérabilités,
- **EGERIE** : analyse des risques à intégrer dans le cycle projet, aide à la décision et identification des mesures à mettre en œuvre,
- **Project Monitor** : animation des revues de projets et des différentes instances, suivi de l'avancement des projets, du plan de charge et des budgets.

Au regard de la charge que représente le déploiement de sa PSSI, le Conseil Départemental de Haute-Garonne a choisi de se tourner vers un outil permettant :

- d'**industrialiser au maximum le pilotage et le suivi des indicateurs** (éviter l'usage généralisé d'Excel, les nombreux échanges de mails, etc.) ;
- d'**obtenir une vision d'ensemble** et de la partager top-down ou bottom-up ;
- de **maîtriser les coûts** du projet de sécurité et du suivi des plans d'action.

Son choix s'est alors porté sur la solution proposée par Virage Group, déjà en place au sein de la DSI :

Project Monitor, le logiciel de Gestion de portefeuille projets. Un outil tout-en-un : tableaux de bord multi projets, plan de charge, planning, tâches, suivi des demandes informatiques, suivi budgétaire.

Le département se sert donc de cet outil comme d'un véritable **cockpit de pilotage** de la cybersécurité, doté d'une **vue à 360°** :

- des vues globales, intégrables dans un reporting destiné au top management,
- des vues opérationnelles utiles à la prise de décisions rapides sur les actions à prioriser.

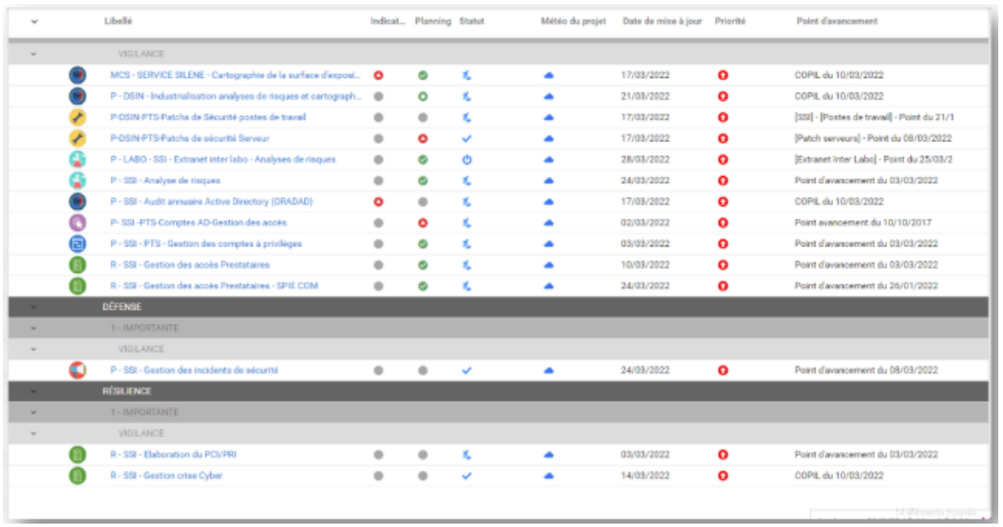
La mise en œuvre efficace de votre PSSI grâce aux outils de pilotage

Les tableaux de bord de la sécurité

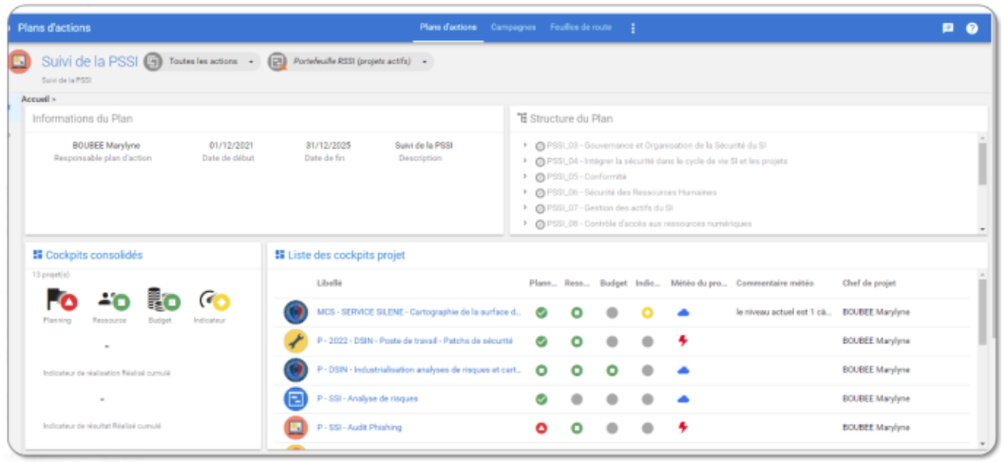
Éléments clés du dialogue RSSI/Direction, les tableaux de bord de Project Monitor permettent de piloter les projets liés à la cybersécurité.

Le Conseil Départemental de la Haute-Garonne utilise le logiciel Project Monitor pour **rentrer dans le détail des projets** (élaboration, planification, etc.) rattachés aux 11 axes de son PSSI. Il a repris dans cet outil tous les chapitres de son PSSI pour suivre l'avancée de chaque projet rattaché à un ou plusieurs axes de la politique de sécurité.

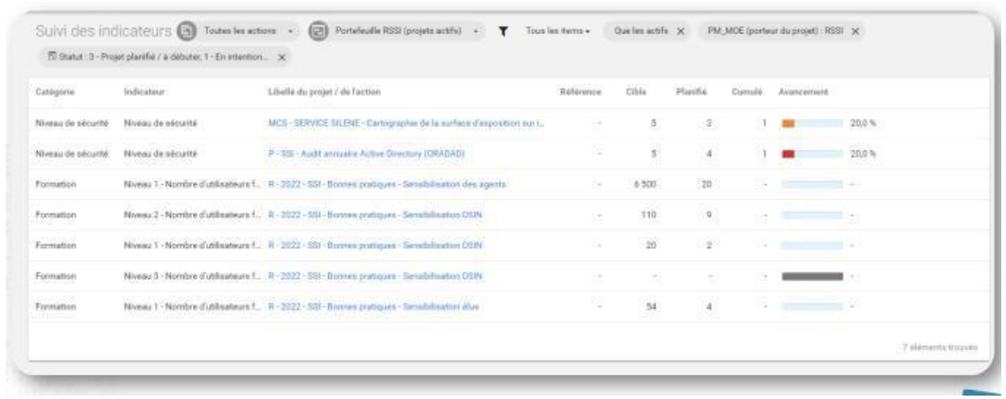
Le département utilise également la partie portefeuille pour **animer les réunions de travail** (notamment le CTSSI), au moyen d'un support bien plus dynamique qu'un simple PowerPoint. Les parties prenantes sélectionnent les projets qu'ils souhaitent voir abordés, puis ils déroulent les différents points associés avant d'acter leurs décisions.



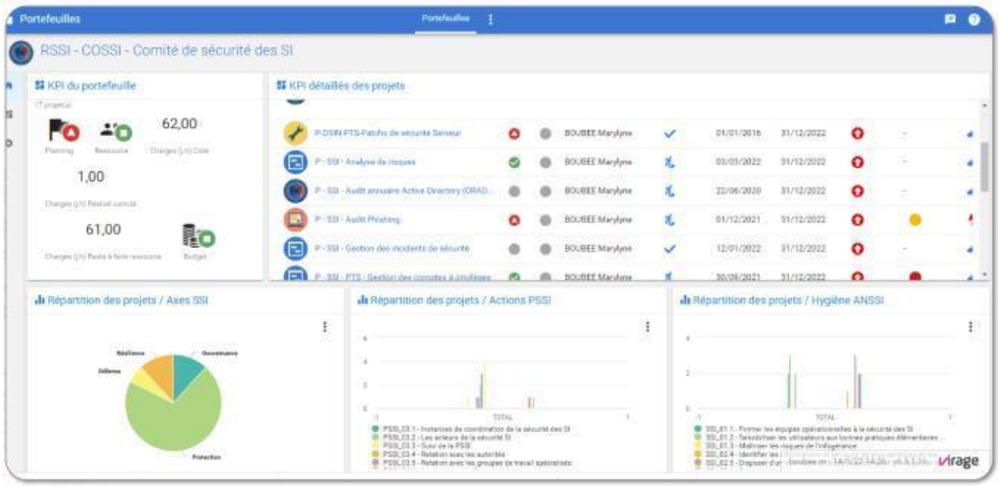
Suivi du CTSSI et des projets prioritaires



Vue pour le suivi de la PSSI et du plan d'action au global



Suivi des indicateurs



Vue des portefeuilles pour la comitologie

La mise en œuvre efficace de votre PSSI grâce aux outils de pilotage

Découvrez Project Monitor, la solution au service du RSSI pour le pilotage de la cybersécurité

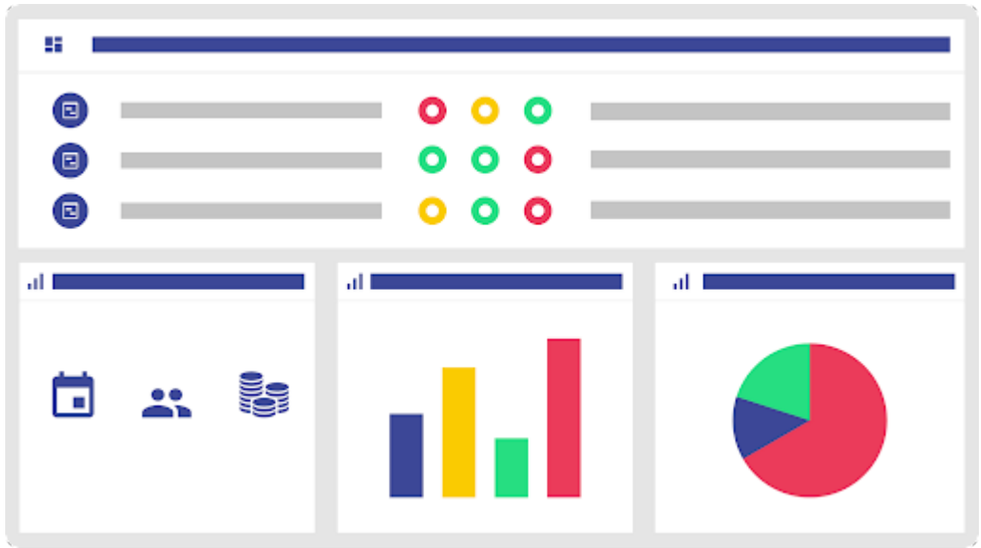
Centralisez les indicateurs de pilotage

Identifiez et diffusez les indicateurs de pilotage auprès des différentes parties prenantes.

Vos décisions sont alors nourries des informations clés pour un pilotage efficace de vos projets.

Visualisez l'avancement : charges, budget, météo projet.

Pilotez le budget de vos projets



Définissez et planifiez les prévisions de dépenses et recettes par mois/trimestre/année ou exercice.

Régulez vos charges et investissements dans un tableau de bord pour optimiser vos dépenses et ainsi améliorer la performance de vos projets.

Vous pouvez ainsi suivre vos engagements et calculer le retour sur vos investissements (ROI).

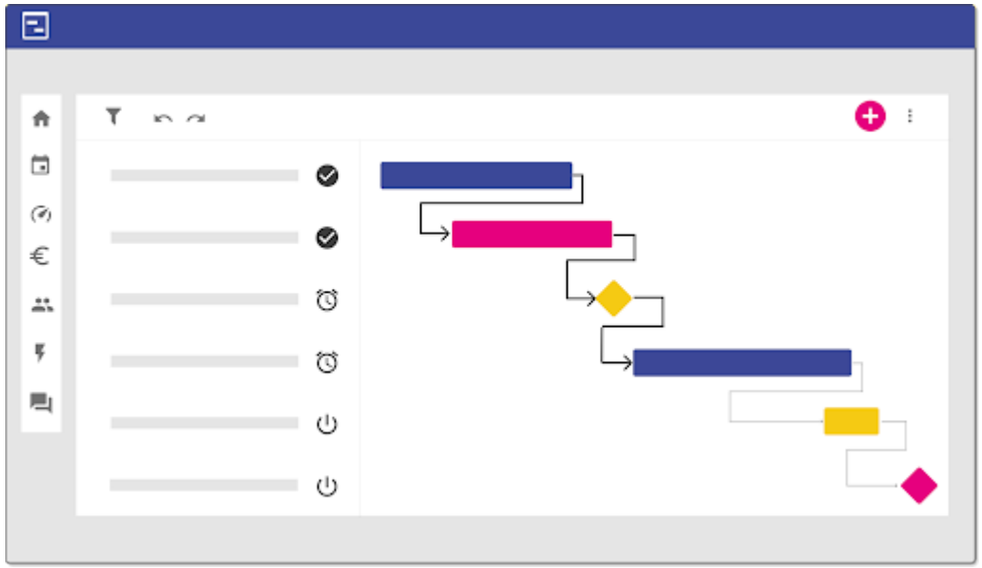
Obtenez une meilleure qualification de la charge de travail

Suivez les activités des collaborateurs via la feuille de saisie des temps.

Project Monitor calcule, en temps réel, la disponibilité de chaque ressource.

À partir de la charge planifiée sur les projets, le manager peut alors consulter les ressources en sous-charge et surcharge. Ajustez le staffing et les plannings.

Planifiez les projets de votre portefeuille



Déclinez les Schémas directeurs en projets.

Grâce aux Gantt et Multi Gantt, vous optimisez la planification et identifiez les dépendances.

Ce rapport permet de suivre le planning de plusieurs projets. Des mécanismes de filtres permettent de cibler les données souhaitées.

Sources et documents

- Panorama des menaces informatiques
- Le tableau de bord de la sécurité, élément clé du dialogue RSSI/Directions
- Élaboration de tableaux de bord SSI
- Fiche produit du logiciel Project Monitor

appvizer

Appvizer est le premier média en Europe dédié aux logiciels professionnels.

Sa mission est de permettre aux professionnels de trouver facilement les bons logiciels pour être plus compétitifs et travailler plus agréablement au quotidien.

Virage Group est éditeur - intégrateur de logiciels, dédiés à la coopération autour des projets.

Sa solution Project Monitor permet de couvrir tous les enjeux du pilotage de portefeuille projets (planning, suivi d'activité, finance, risque, collaboratif, aide à la décision).