Direction générale du numérique et des systèmes d'information
Avenue de Longemalle 1, CH-1020 Renens
www.vd.ch – T 41 21 316 26 00

LIVRABLE

ASSURER ET RENFORCER LA SÉCURITÉ DES DONNÉES DANS LES ESPACES DE TRAVAIL COLLABORATIFS DES ADMINISTRATIONS NUMÉRIQUE

- BILAN DE PROJET

PROJET	Code projet	*01004*
	Libellé projet	*Assurer et renforcer la sécurité des données dans les espaces de travail collaboratifs des administrations numérique.*
	Entité Bénéficiaire	*DGNSI*
	Entité DGNSI	*PS-SEC / SEC-SI*
	Chef de projet	*Daniel JAQUET*
	Responsable utilisateur	*Angelo Franco*
	Phases de projet	☐ Initialisation ☐ Conception ☐ Réalisation ☐ Déploiement ☒ Clôture

DOCUMENT	Livrable	BILAN DE PROJET
	Emplacement	**Erreur ! Référence de lien hypertexte non valide.**
	Fichier	bilan de projet dgnsi ans 2025 final (copie de travail).docx
	Classification	☒ Public ☐ Interne ACV ☐ Interne DGNSI ☐ Confidentiel
	Auteur	*Daniel JAQUET*
	Version	*1.0*
	Date	*25.11.2025*
	Statut	☐ En rédaction ☐ En approbation ☒ Validé

HISTORIQUE

RÉVISION

Version	Date	Auteur(s)	Description
0.1	13.10.2025	DJT	Version initiale
0.2	20.10.2025	DJT	Correction après peer review
1.0	10.12.2025	DJT	Version finale

TABLE DES MATIÈRES

1 INTRODUCTION 5
2 FICHE SIGNALÉTIQUE DU PROJET 6
3 CONTEXTE DU PROJET 7
3.1 Environnement actuel 7
3.2 Problématique rencontrée 7
3.3 But à atteindre 7
4 OBJECTIF DU PROJET 9
4.1 Approche proposée 9
4.2 Analyse de risque initiale 9
4.2.1 Risque de divulgation non autorisée de données : 9
4.2.2 Fuite via cyberattaque : 10
4.2.3 Perte de maîtrise sur les traitements : 10
4.2.4 Extraction malveillante par des collaborateurs : 10
4.2.5 Non-respect des obligations légales : 10
5 DÉROULEMENT DU PROJET 11
5.1 Organisation projet 11
5.2 Spécifications 12
5.3 Conception 13
5.3.1 Analyse des solutions et choix technologiques 13
5.3.2 Gouvernance technique 13
5.3.3 Architecture et conception applicative 13
5.4 Industrialisation du PoC 14
5.4.1 Renforcement des composants existants 14
5.4.2 Intégration du moteur IA 14
5.4.3 Génération du rapport d'analyse 14
5.4.4 Préparation du déploiement client 14
5.5 Développement 15
5.5.1 Implémentation des composants logiciels 15
5.5.2 Infrastructure, qualité et open source 15
5.5.3 Améliorations de performances et robustesse 15
5.5.4 Automatisation et fiabilité 15
5.6 Captures d'écran 16
5.7 Documentation utilisateur 21
5.8 Gestion de projet 22
5.8.1 Planification des activités 22
5.8.2 Conduite et suivi du projet 23
6 FINANCEMENT 25
6.1 Estimation des coûts 25
6.1.1 Détail des phases et effort associé 25
7 RÉSULTAT DU PROJET 26
7.1 Evaluation générale du projet 26
7.1.1 Détail des résultats 26
7.2 Satisfaction de la DGNSI 26

8 LIVRAISON ET PARTAGE DU PROGET 27
8.1 Mise à disposition du projet en Open Source 27
9 ANNEXES 28
9.1 Spécifications techniques 28
9.2 Documentation technique et utilisateur 28

1 INTRODUCTION

BUT DU DOCUMENT

Dans le *Bilan de projet*, il s'agit de comparer le prévu et l'effectif au niveau des moyens, des délais et des coûts ; il s'agit également d'analyser les expériences faites et d'apprécier la démarche. Le *Bilan de projet* peut conduire à prendre des mesures complémentaires. Ce modèle de Bilan (format Word) est destiné aux parties prenantes de la DGNSI. La version du Bilan au format PowerPoint pour le COPIL est destinée aussi bien au Métier qu'à la DGNSI.

RÉFÉRENCES

DSI-03.2-1804	03.2 Directive Elaborer et maintenir les solutions.pdf**Erreur ! Référence de lien hypertexte non valide.**
Pitch ANS	DGNSI_Presentation_ANS_V1.pptx
LPrD	**Erreur ! Référence de lien hypertexte non valide.** https://prestations.vd.ch/pub/blv-publication/actes/consolide/172.65?key=1543934892528&id=cf9df545-13f7-4106-a95b-9b3ab8fa8b01

ABRÉVIATIONS, DÉFINITIONS, GLOSSAIRE

IA	L'intelligence artificielle (IA) désigne un ensemble de technologies et d'algorithmes qui permettent aux machines d'imiter des capacités humaines telles que l'apprentissage, le raisonnement, et la prise de décision
DGNSI	Direction générale du numérique et des systèmes d'information. Elle pilote le numérique et les systèmes d'information du canton, en coordonnant la stratégie de transition numérique et la gestion de l'informatique pour l'administration et les services publics.
LLM	Un LLM (Large Language Model) est un modèle d'intelligence artificielle capable de comprendre et de générer du texte de manière cohérente à partir de grandes quantités de données linguistiques
PoC	Un PoC (Proof of Concept) est une réalisation ou un test initial visant à démontrer la faisabilité et la viabilité d'une idée, d'un projet ou d'une technologie avant son développement complet.
PS-ETN	Entité produits et services environnement de travail numérique de la DGNSI
PS-SEC	Entité produits et services sécurité de la DGNSI
ETN-Editique	Entité responsable du produit DGNSI-Wiki

2 FICHE SIGNALÉTIQUE DU PROJET

Titre	Description
Descriptif du projet	Les administrations publiques suisses utilisent des outils collaboratifs afin de mener à bien leurs projets ainsi que pour soutenir leurs activités opérationnelles. Ces outils de type Wiki facilitent et accélèrent les tâches quotidiennes. Mais malgré la formation et la sensibilisation des utilisateurs, il arrive que des données personnelles, des données sensibles et / ou confidentielles se retrouvent dans ces espaces (identifiants de connexions, mots de passe, clés, certificats, etc.) L'Etat de Vaud, au travers d'un PoC, a confirmé la nécessité de surveiller ces espaces et de mettre en place un moyen d'analyser leur contenu à la recherche de ces informations sensibles. Ainsi, ce projet vise à réaliser un outil permettant d'identifier automatiquement à l'aide d'une IA non-publique les données sensibles ou à risque sécuritaire dans des espaces de type documentation Wiki ou encore des outils de gestion de projet. Cet outil permettra également de générer un rapport détaillé d'analyse comprenant des conseils de résolution des risques relevés. L'outil doit être *user friendly* et doit facilement être pris en main par n'importe quel corps de métier, même sans connaissances informatiques avancées.
Complexité métier	2
Complexité technique	3
Nb d'équipes DGNSI impactées	2 : PS-SEC et ETN-Editique
Nb de fournisseurs ext.	1 : Softcom Technologies SA, Prilly VD
Basé sur une plateforme transverse ou pas	Développement spécifique
Produit du marché	Non
Dev spécifique	Oui

3 CONTEXTE DU PROJET

3.1 Environnement actuel

La DGNSI met à disposition de ses utilisateurs des outils de collaboration de type wiki permettant de pouvoir facilement partager de l'information en interne, durant l'exécution d'un projet, pour supporter les activités opérationnelles ou pour faciliter la collaboration entre équipes.

Ces espaces sont gérés au travers des règles poussées depuis la solution utilisée (Altassian Confluence). Une personne administre la solution, les créations d'espaces se font au travers de demandes validées par la hiérarchie et un répondant est nommé pour chaque espace pour gérer les accès, le contenu et l'utilisation de l'espace.

Selon les directives de gestion documentaires de la DGNSI ces espaces ne sont pas des référentiels de documents, mais permettent de faciliter le travail de construction et de partage d'information lorsque nous sommes en phase de conception et de réalisation des projets.

En regard de ceci, l'entité Sécurité de l'information de la DGNSI se doit de s'assurer que les exigences en matière de sécurité et de protection des données sont bel et bien respectées au travers de contrôles de conformité.

3.2 Problématique rencontrée

La création de contenu dans ces espaces est relativement libre par les utilisateurs, qui ne sont contraints au niveau de la protection des données et de la sécurité de l'information uniquement par les lois et directives en vigueur dans le Canton de Vaud et à la DGNSI.

Ce qui veut dire que, concrètement, aucune mesure technique n'est présente pour faire appliquer et respecter ces lois et directives. Ce serait exactement la fonctionnalité principale d'une solution DLP, mais nous ne disposons pas de ce type de solutions sur cette plateforme.

L'entité sécurité de l'information et gouvernance de la DGNSI a donc décidé d'auditer en 2024 les données présentes dans ces espaces collaboratifs sous l'angle de la sécurité et de la protection des données. Les résultats obtenus, sans rentrer dans les détails, montrent que des données personnelles, des données personnelles sensibles, ainsi que des informations confidentielles s'y trouvaient.

Cela démontre que l'approche uniquement basée sur les directives de sécurité et la formation des utilisateurs n'est pas suffisante, et qu'il est nécessaire de mettre en place un mécanisme de contrôle de la conformité.

3.3 But à atteindre

La cible de ce projet est d'apporter à la DGNSI un outil pratique, simple d'utilisation, remontant des résultats pertinents sur l'existence de données confidentielles ou personnelles dans nos espaces wiki.

L'outil doit être capable d'effectuer des analyses régulières des contenus indépendamment du volume d'information s'y trouvant

Les résultats doivent être présentés sous une forme lisible et exportable afin que l'on puisse les intégrer dans notre gestion des actions correctives et que l'on puisse facilement les transmettre aux personnes en charge des différents espaces pour correction.

4 OBJECTIF DU PROJET

4.1 Approche proposée

A la suite du PoC réalisé (audit 2024), nous souhaitions pouvoir industrialiser la notion de contrôles de ces informations pour les raisons suivantes :

- **Volumétrie** : Impossible de continuer à vérifier manuellement un volume d'informations aussi conséquent
  - 229 espaces
  - 65'000 pages
- **Conformité** : Nous souhaitons être en conformité avec nos directives de sécurité et la LPrD
  - 1 contrôle par année de la conformité des données contenues dans ces espaces

La DGNSI, dans son organisation de maintien du patrimoine informatique, n'ayant pas les ressources suffisantes en interne pour apporter une solution à cette problématique, bous avons donc pris la décision d'externaliser le développement de cette solution.

Nous avons donc rassemblé nos exigences métiers et avons travaillé avec le prestataire Softcom pour définir le mandat de prestations qui a permis la création de cette solution.

Une économie d'échelle a pu être atteinte, car le contexte, la problématique était déjà connue par ce fournisseur qui nous avait déjà accompagné lors du POC de 2024.

L'utilisation de l'IA basée sur un modèle LLM local proposée par le fournisseur s'est rapidement imposée comme la solution la plus fiable afin de garantir un traitement sécurisé de la problématique. L'IA nous permet aussi de définir un moyen simple et flexible pour la recherche d'information sans devoir définir des filtres complexes (trouver les données sans connaitre leur forme exacte).

Softcom a donc orienté son travail dans le sens de leur proposition.

4.2 Analyse de risque initiale

Une analyse de risque initiale a été effectuée sur le contexte et la plateforme utilisée. Parmi les différents risques identifiés, les risques suivants peuvent être mitigé par la mise en place de ce projet.

4.2.1 Risque de divulgation non autorisée de données :

L'accès élargi et la nature collaborative d'un wiki favorisent la diffusion involontaire de données confidentielles, sensibles ou personnelles, soit par erreur de manipulation, configuration inadaptée des droits ou partage de liens.

- Mitigation apportée par la solution :
  - Identifier les données problématiques présentes dans ces espaces

- Minimiser le volume de données problématiques contenu dans ces espaces
- Limiter les canaux de fuites de données

4.2.2 Fuite via cyberattaque :

Les wikis sont des cibles potentielles pour les cybercriminels qui cherchent à exploiter des failles afin d'exfiltrer des données, d'utiliser des vulnérabilités zero-day, ou de compromettre des comptes utilisateurs (ex : attaque RCE sur XWiki).

- Mitigation apportée par la solution :
  - Identifier les données problématiques présentes dans ces espaces
  - Minimiser le volume de données problématiques contenu dans ces espaces (en cas de cyberattaque, l'impact serait moins grand)
  - Limiter les canaux de fuites de données

4.2.3 Perte de maîtrise sur les traitements :

Une diffusion désorganisée ou la création de pages non contrôlées peut engendrer un inventaire flou des données stockées et d'éventuels traitements illicites ou non conformes.

- Mitigation apportée par la solution :
  - Cartographier l'utilisation et les données sensibles contenues dans les espaces wiki
  - Sensibiliser les utilisateurs aux bonnes pratiques de gestion des données dans les espaces wiki

4.2.4 Extraction malveillante par des collaborateurs :

Des collaborateurs mal intentionnés pourraient copier massivement des informations, une possibilité facilitée par la nature accessible et structurée du wiki.

- Mitigation apportée par la solution :
  - Identifier et quantifier les données sensibles présentes dans les espaces Confluence
  - Limiter la capacité de partager des données sensibles au travers des espaces wiki
  - Sensibiliser les utilisateurs aux bonnes pratiques de gestion des données dans les espaces wiki

4.2.5 Non-respect des obligations légales :

Une absence de mesures techniques ou organisationnelles adéquates, d'analyses d'impact, ou défaut de notification après une violation expose l'administration à des sanctions administratives et pénales (LPD)

- Mitigation apportée par la solution :
  - Assurer l'adéquation des espaces wiki avec la LPD
  - Assurer le respect des directives de sécurité DGNSI

5 DÉROULEMENT DU PROJET

5.1 Organisation projet

L'équipe projet est constituées des personnes mentionnées dans le tableau ci-dessous :

Rôle	Nom	Enterprise / Organisation	Email
Mandant	Daniel Jaquet	DGNSI	daniel.jaquet2@vd.ch
Responsable projet DGNSI	Daniel Jaquet	DGNSI	daniel.jaquet2@vd.ch
Responsable projet Softcom	Alexandre Luy Loan Rey	Softcom	Supprimé avant publication externe
Responsable applicatif DGNSI	Lionel Conforto	DGNSI	Supprimé avant publication externe
Expert sécurité	Angelo Franco	DGNSI	Supprimé avant publication externe
Développeur, Technical lead	Thibaut Vuillaume	Softcom	Supprimé avant publication externe
Développeur	Guillaume Prunier	Softcom	Supprimé avant publication externe

5.2 Spécifications

Voir annexes §9.2

5.3 Conception

La phase de conception a permis de transformer les besoins métiers identifiés en une architecture technique robuste, sécurisée et pérenne.

Les travaux se sont articulés autour des axes suivants :

5.3.1 Analyse des solutions et choix technologiques

Plusieurs approches ont été explorées pour répondre à la problématique de détection de données sensibles dans les espaces collaboratifs. L'analyse a confirmé la pertinence d'une architecture hybride combinant :

- Une application d'analyse statique pour la préparation et la structuration des contenus,
- Un moteur IA spécialisé pour la détection des PII,
- Un stockage local chiffré pour garantir la confidentialité des résultats,
- Une interface moderne permettant l'exploitation simple et intuitive des analyses.

Ces éléments ont permis d'aligner les choix techniques avec les priorités DGNSI : sécurité, performance, évolutivité, et capacité d'industrialisation.

5.3.2 Gouvernance technique

Une gouvernance technique du projet a été définie, incluant :

- Des normes de développement (qualité, tests, sécurité),
- Des conventions de gestion des dépendances et des repositories open source,
- Un cadre d'optimisation et de maintien du moteur IA,
- Une structuration des modules selon une architecture hexagonale.

Cette gouvernance visait à assurer la maintenabilité de la solution et à réduire les risques liés à l'évolution future des modèles IA.

5.3.3 Architecture et conception applicative

La conception a abouti à une architecture modulaire comprenant :

- Un micro-service IA en Python, exposant ses capacités via gRPC,
- Une application Node.js dédiée au scraping, au pilotage des scans et à la gestion des données métier,
- Une base de données locale avec chiffrement systématique des informations sensibles,
- Une interface utilisateur Angular offrant visualisation, navigation, tri, gestion des scans et export des rapports,
- Un pipeline CI/CD assurant la reproductibilité des déploiements.

Cette architecture permet d'intégrer aisément de nouveaux modèles IA ou de nouvelles sources documentaires (ex. Jira), conformément aux besoins d'évolution identifiés.

5.4 Industrialisation du PoC

La phase d'industrialisation a consisté à transformer le PoC initial, orienté démonstration, en une plateforme opérationnelle stable, automatisée et conforme aux exigences de production de la DGNSI.

5.4.1 Renforcement des composants existants

Les services hérités du PoC ont été consolidés afin d'assurer un fonctionnement fiable :

- Durcissement du scraping Confluence et introduction d'un mécanisme de reprise en cas d'erreur (retry, backoff exponentiel),
- Mise en place de stratégies de contournement du rate limiting et des protections anti-bot,
- Optimisation de la gestion des flux pour garantir une extraction complète des espaces, y compris des pièces jointes.

5.4.2 Intégration du moteur IA

Le composant initial basé sur regex et mots-clés a été entièrement remplacé par un moteur IA plus performant.

Cette intégration a nécessité :

- La définition de formats d'échange standardisés et agnostiques,
- La mise en place d'un service de communication vers le microservice IA,
- Des tests intensifs sur jeu de données réel et synthétique pour valider la pertinence des détections.

5.4.3 Génération du rapport d'analyse

Le service de production du rapport a été industrialisé pour offrir :

- Un rapport global consolidé,
- Un rapport détaillé par espace,
- Un regroupement des PII par criticité, famille et occurrence,
- Une prévisualisation immédiate dans l'UI.

5.4.4 Préparation du déploiement client

L'ensemble de la solution a été packagé afin de permettre une installation simple chez la DGNSI :

- Création des images Docker,
- Documentation de la procédure d'installation,
- Paramétrage externalisé et sécurisé (credentials, configuration IA, connexion Confluence).

Cette phase a permis de stabiliser la solution avant d'entamer le développement complet.

5.5 Développement

La phase de développement a constitué le cœur de la réalisation de la solution. Elle a porté sur la mise en œuvre de l'ensemble des fonctionnalités prévues, dans une logique agile et itérative.

5.5.1 Implémentation des composants logiciels

Les travaux ont abouti à :

- La création du micro service IA en Python, exposant les fonctions d'analyse via gRPC,
- La modernisation de l'application d'analyse statique en Node.js, désormais autonome et capable de gérer l'intégralité du cycle de scan,
- L'implémentation de l'UI Angular, fournissant dashboard, navigation, tri, pagination, gestion des scans, visualisation du contexte des PII et export,
- L'intégration d'un module d'export Excel, permettant d'exploiter les résultats de manière externe.

5.5.2 Infrastructure, qualité et open source

Le développement a inclus :

- La mise en conformité du code pour publication en open source (licence MIT, gestion des secrets, audit de sécurité),
- La mise en place des pipelines CI/CD,
- La configuration des mécanismes de protection (linting, scans de vulnérabilités, git leaks, dependabot).

5.5.3 Améliorations de performances et robustesse

Un travail spécifique a été mené pour optimiser :

- La vitesse d'analyse des espaces,
- L'utilisation des modèles IA,
- La gestion mémoire des scans,
- La fluidité de l'interface pour les volumes importants (229 espaces, 65'000 pages).

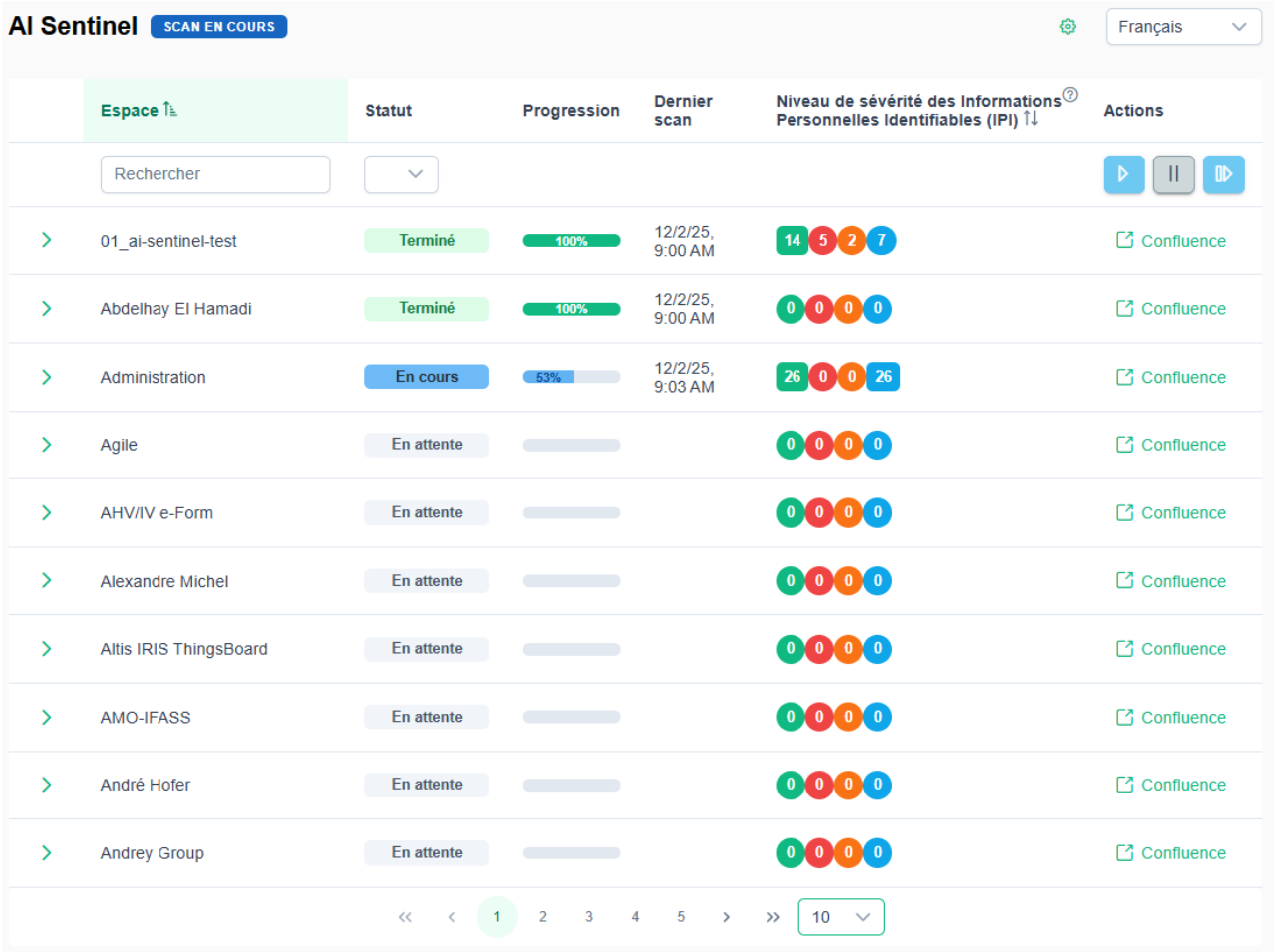
5.5.4 Automatisation et fiabilité

Plusieurs services ont été créés pour garantir une exploitation fluide :

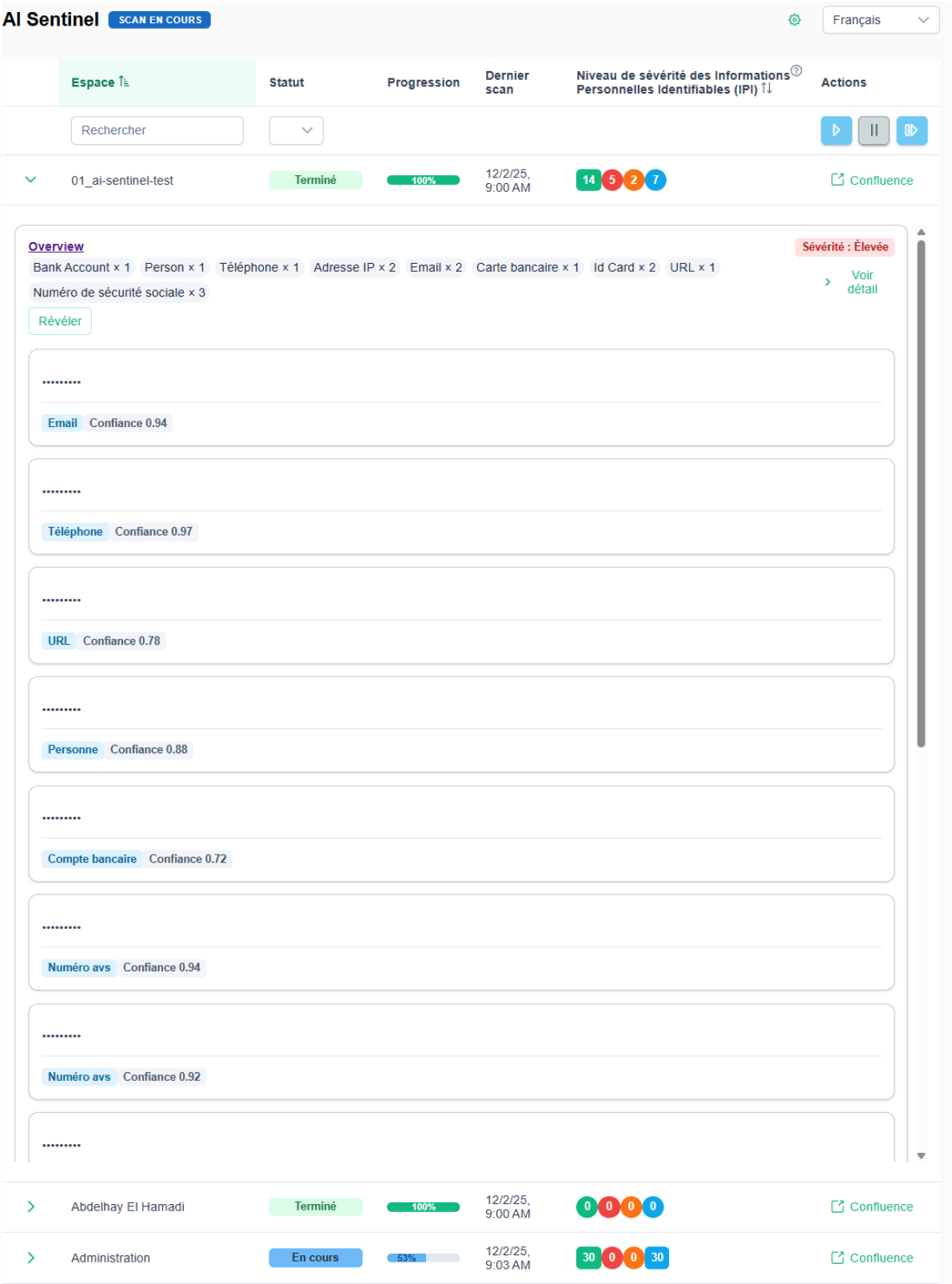
- Détection dynamique des nouveaux espaces,
- Préchargement local pour affichage instantané,
- Interruption et reprise de scans,
- Stockage chiffré du contexte de détection.

Ces développements ont produit une solution complète, opérationnelle, extensible et répondant pleinement aux objectifs définis.

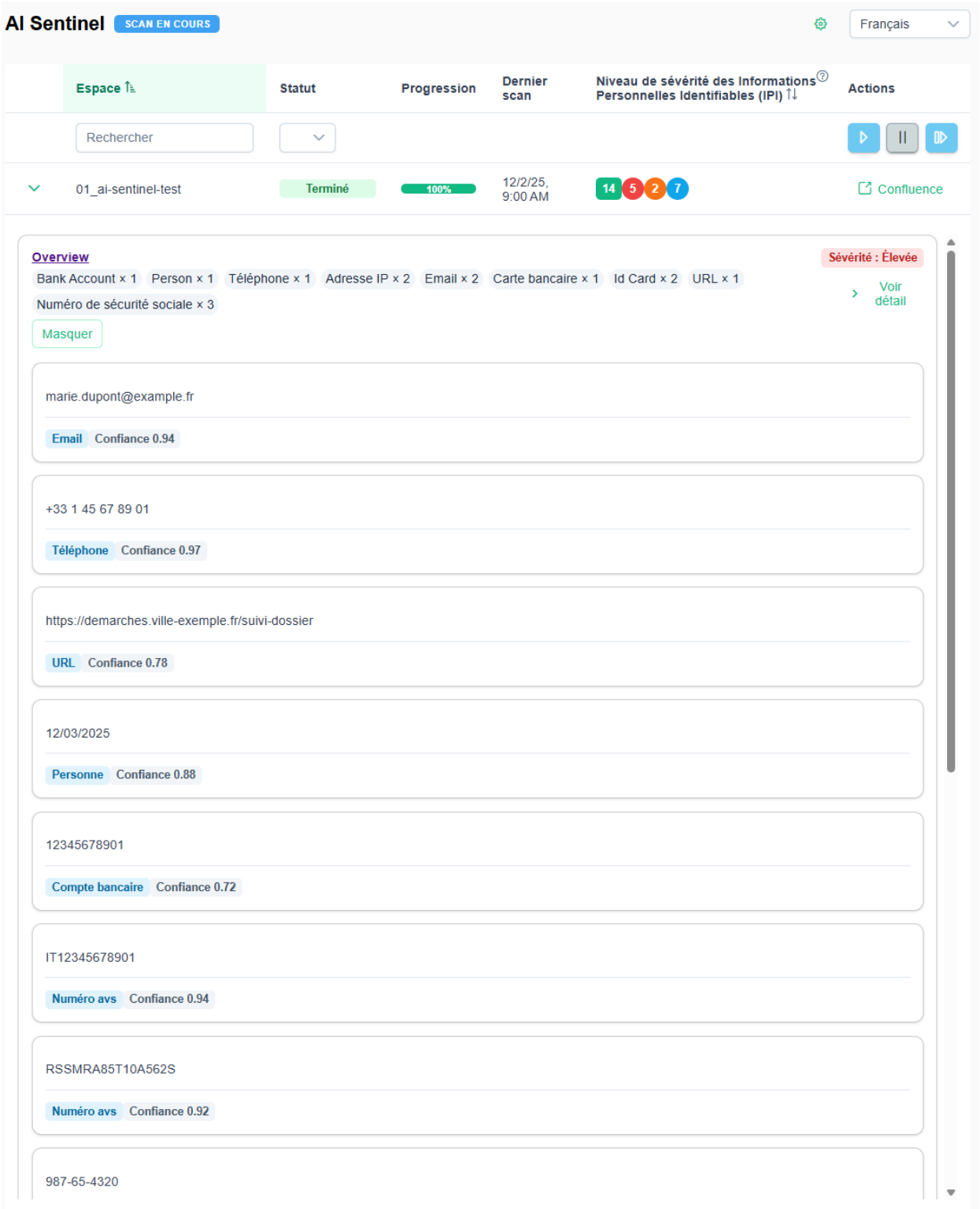
5.6 Captures d'écran



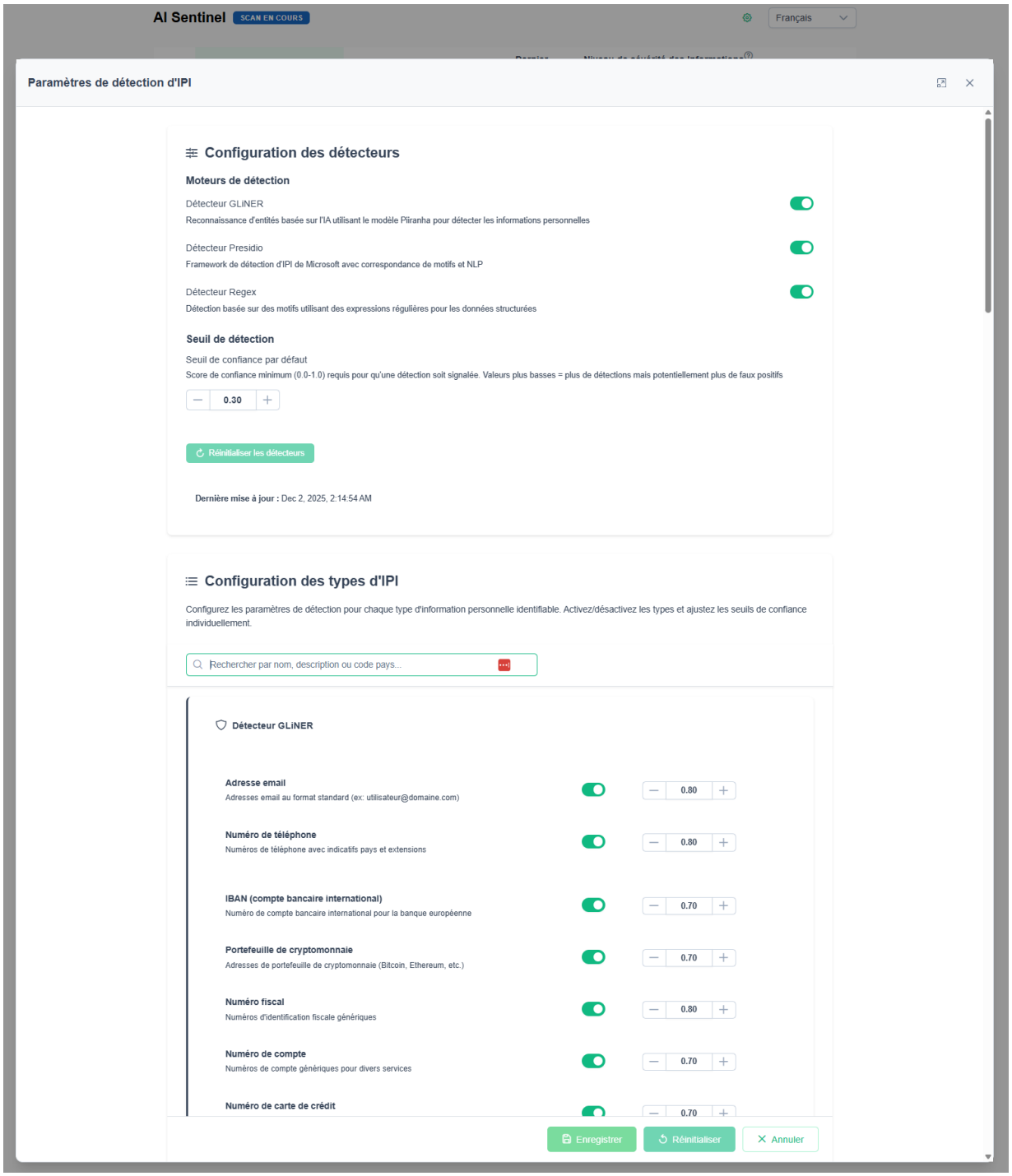
L'interface rend compte de l'analyse en cours des espaces Confluence.



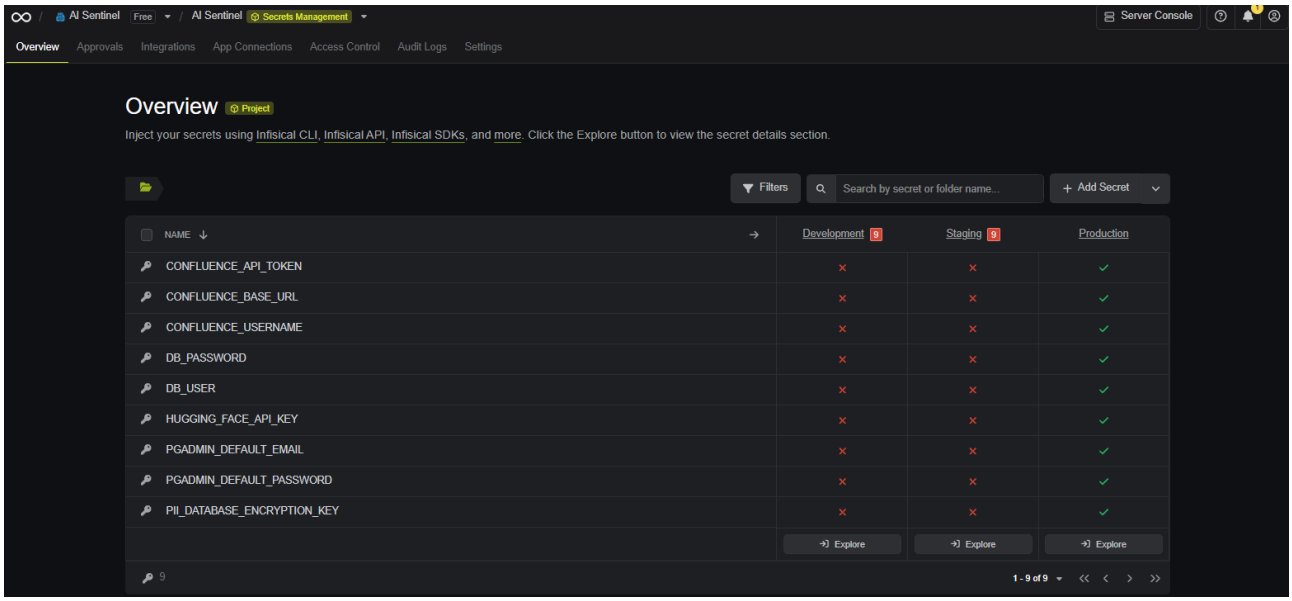
Le détail des PII trouvés est affiché lorsqu'on déroule la ligne décrivant un espace Confluence.



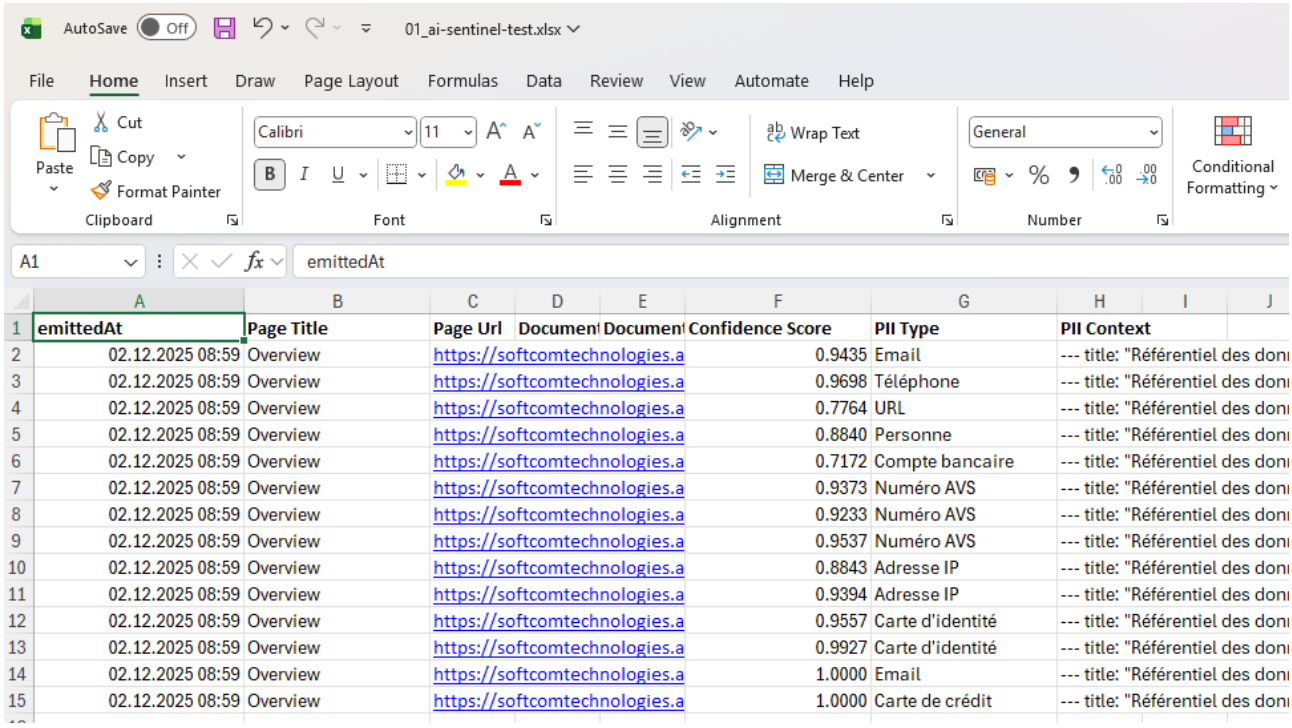
L'outil permet de révéler les valeurs des PII (fonctionnalité configurable).



Une fenêtre regroupe différents paramètres permettant une configuration assez fine de l'outil d'analyse.



Les tokens d'accès à Confluence, notamment, sont sécurisés via un vault Infisical.



	A	B	C	D	E	F	G	H	I	J
1	emittedAt	Page Title	Page Url	Document	Document	Confidence Score	PII Type	PII Context		
2	02.12.2025 08:59	Overview	https://softcomtechnologies.a			0.9435	Email	--- title: "Référentiel des don		
3	02.12.2025 08:59	Overview	https://softcomtechnologies.a			0.9698	Téléphone	--- title: "Référentiel des don		
4	02.12.2025 08:59	Overview	https://softcomtechnologies.a			0.7764	URL	--- title: "Référentiel des don		
5	02.12.2025 08:59	Overview	https://softcomtechnologies.a			0.8840	Personne	--- title: "Référentiel des don		
6	02.12.2025 08:59	Overview	https://softcomtechnologies.a			0.7172	Compte bancaire	--- title: "Référentiel des don		
7	02.12.2025 08:59	Overview	https://softcomtechnologies.a			0.9373	Numéro AVS	--- title: "Référentiel des don		
8	02.12.2025 08:59	Overview	https://softcomtechnologies.a			0.9233	Numéro AVS	--- title: "Référentiel des don		
9	02.12.2025 08:59	Overview	https://softcomtechnologies.a			0.9537	Numéro AVS	--- title: "Référentiel des don		
10	02.12.2025 08:59	Overview	https://softcomtechnologies.a			0.8843	Adresse IP	--- title: "Référentiel des don		
11	02.12.2025 08:59	Overview	https://softcomtechnologies.a			0.9394	Adresse IP	--- title: "Référentiel des don		
12	02.12.2025 08:59	Overview	https://softcomtechnologies.a			0.9557	Carte d'identité	--- title: "Référentiel des don		
13	02.12.2025 08:59	Overview	https://softcomtechnologies.a			0.9927	Carte d'identité	--- title: "Référentiel des don		
14	02.12.2025 08:59	Overview	https://softcomtechnologies.a			1.0000	Email	--- title: "Référentiel des don		
15	02.12.2025 08:59	Overview	https://softcomtechnologies.a			1.0000	Carte de crédit	--- title: "Référentiel des don		

Le rapport exporté au format Excel décrit les PII trouvés, facilitant la collaboration avec les responsables des différents espaces Confluence.

5.7 Documentation utilisateur

La documentation utilisateur fournie dans le cadre de ce projet prend la forme d'un README.md complet, structuré et conforme aux standards des projets open source modernes. Ce choix découle de la nature même de la solution développée : un outil autonome, intuitif, et conçu pour être directement utilisable par les équipes opérationnelles sans nécessiter de manuel exhaustif ou de formation spécifique.

L'interface utilisateur d'AI Sentinel a été pensée pour être self-explicative, guidant naturellement l'administrateur ou l'utilisateur dans les différentes étapes d'analyse des espaces Confluence : lancement de scans, visualisation des résultats, exploration des PII, configuration des paramètres, export des rapports, etc. Ainsi, le besoin d'une documentation volumineuse ou narrative ne s'imposait pas.

Le README.md fait office de documentation unique car il rassemble, dans un format structuré et maintenable, toutes les informations nécessaires à l'installation, à la configuration, à l'exploitation et au support de la solution. Ce document constitue un point d'entrée centralisé, facilement accessible dans le repository open source et adapté aux contributions futures. Il couvre notamment :

- La présentation générale de l'outil et de ses fonctionnalités principales,
- L'architecture technique (microservices, modèles IA, flux d'analyse),
- Les prérequis techniques,
- La procédure d'installation et de configuration (notamment via Infisical),
- Les commandes utiles et les points d'intégration (API, gRPC),
- Le dépannage (troubleshooting),
- Les guides de contribution et les normes de développement.

Les pages qui suivent dans ce chapitre reprennent intégralement le contenu de ce README, afin d'intégrer la documentation utilisateur directement au livrable DGNSI et d'assurer la cohérence entre la version projet et la version open source.

Ce format garantit :

- Une documentation exhaustive mais concise,
- Une lisibilité optimale pour les équipes DGNSI,
- Une facilité de maintenance par Softcom ou par les futurs contributeurs,
- Une évolutivité naturelle en cas d'amélioration ou d'extension fonctionnelle.

Cette approche est en adéquation avec les bonnes pratiques de développement d'outils IA et de solutions open source, et elle répond aux exigences du mandat : mettre à disposition une documentation claire, opérationnelle, et directement exploitable par la DGNSI.

Le document README.md est disponible en annexe de ce document

5.8 Gestion de projet

5.8.1 Planification des activités

La planification du projet a été structurée en six grandes phases successives, intégrant néanmoins des itérations agiles et des points d'alignement réguliers avec la DGNSI. Les activités se sont déroulées entre mai 2025 et décembre 2025, selon la séquence suivante :

5.8.1.1 Phase 1 : Lancement & cadrage (mai 2025)

- Kick-off avec la DGNSI, validation des objectifs, périmètre et livrables.
- Constitution de l'équipe projet (DGNSI + Softcom).
- Revue du PoC réalisé précédemment pour identifier les éléments à industrialiser.

5.8.1.2 Phase 2 : Spécification & conception (mai – juin 2025)

- Ateliers fonctionnels et techniques.
- Rédaction des exigences métiers et techniques.
- Définition de l'architecture cible (microservice IA + application Node.js + base de données locale sécurisée).
- Finalisation des user stories et priorisation du backlog.

5.8.1.3 Phase 3 : Industrialisation du PoC (juin – juillet 2025)

- Transformation du PoC en solution robuste et reproductible.
- Développement du scraping Confluence, gestion du rate limiting, mécanismes de retry et reprise automatique.
- Premières intégrations du moteur IA dans la chaîne d'analyse.

5.8.1.4 Phase 4 : Développement complet de la solution (août – octobre 2025)

- Implémentation du microservice IA (gRPC).
- Refonte de l'application d'analyse statique.
- Création de l'UI, tableaux de bord, gestion des scans, navigation, tri, pagination.
- Génération du rapport d'analyse.
- Mise en place de la CI/CD, packaging et préparation du déploiement client.
- Mise à disposition des repositories en Open Source.

5.8.1.5 Phase 5 : Tests, stabilisation & documentation (octobre – novembre 2025)

- Tests unitaires, intégration, tests end-to-end, tests de performance.
- Audit de sécurité (absence de données sensibles dans le code / dépendances).
- Rédaction de la documentation utilisateur et technique.

- Prémices du support pour les équipes DGNSI.

5.8.1.6 Phase 6 : Recette, transfert & clôture (novembre – décembre 2025)

- Sessions de démonstration et validation des critères d'acceptation.
- Correction des dernières anomalies.
- Transfert opérationnel à la DGNSI (installation, paramétrage, accompagnement).
- Finalisation du bilan et fermeture administrative du projet.

5.8.2 Conduite et suivi du projet

Le projet a été conduit en mode agile, avec un pilotage rapproché entre Softcom et la DGNSI. La gouvernance adoptée a permis une grande transparence, une prise de décision rapide et une adaptation continue aux retours utilisateurs.

5.8.2.1 Rythme de pilotage

- Synchronisations toutes les deux semaines entre Softcom et DGNSI :
  - Présentation des résultats de sprint,
  - Démonstrations (démos fonctionnelles),
  - Revue des développements effectués,
  - Mise à jour du backlog et ajustement des priorités.
- Comité projet mensuel avec revue d'avancement, budget, risques et décisions.
- Canal de communication continu via Teams pour assurer les échanges opérationnels.

5.8.2.2 Mode de travail

- Découpage du travail en user stories priorisées selon la valeur métier.
- Démonstrations fréquentes permettant à la DGNSI de valider rapidement les orientations.
- Tests continus et itératifs pour réduire les risques techniques.
- Collaboration étroite entre Softcom (développement, IA, architecture) et DGNSI (sécurité, gouvernance, métier).

5.8.2.3 Gestion des risques et décisions clés

- Mise en place précoce d'une stratégie de contournement des limitations Confluence (rate limiting, bot detection).
- Sécurisation du stockage local via chiffrement conforme aux standards.
- Contrôle strict de l'absence de données sensibles dans les repositories Open Source.
- Ajustements réguliers du périmètre en fonction des retours utilisateurs, sans impact sur la qualité des livrables.

5.8.2.4 Qualité et satisfaction

Les démonstrations bimensuelles ont permis à la DGNSI de suivre l'évolution de la solution en quasi-temps réel et d'exprimer rapidement ses besoins. Ce mode de conduite a favorisé :

- Une adoption rapide de la solution,
- Une compréhension partagée des enjeux,
- La validation progressive de toutes les fonctionnalités avant la recette finale.

L'ensemble du déroulement du projet a permis de livrer une solution conforme aux attentes, sécurisée, ouverte, et industrialisable à long terme.

Le code de l'application a été vérifié au travers de l'outil SonarCube

Le SCA de l'application a été vérifié au travers de l'outil Dependency Track

6 FINANCEMENT

6.1 Estimation des coûts

En 2024, la DGNSI avait déjà mandaté la société Softcom pour faire une évaluation des données sensibles présentes dans nos espaces wiki. Cette activité avait été effectuée en mode audit de sécurité « one shot » car les ressources allouées n'avaient pas permis d'industrialiser l'activité.

Mais cette activité préalable a permis de supporter la création des spécifications pour le développement de la solution finale.

6.1.1 Détail des phases et effort associé

Le tableau ci-dessous décrit les différents lots de travail définis, ainsi que les efforts associés

Titre	Somme (HT)
Spécification et conception	CHF 3'600
Industrialisation du PoC	CHF 4'500
Développement	CHF27'900
Tests et documentation	CHF 6'300
Gestion de projet (fournisseur)	CHF 2'700
TOTAL	**CHF 45'000**

7 RÉSULTAT DU PROJET

7.1 Evaluation générale du projet

	Métrique	Valeur	Commentaires
Mesure du succès	Satisfaction des parties prenantes (1)	4 (2)	La DGNSI est la seule partie prenante
	Satisfaction de la DGNSI (3)	4 (2)	
	Acceptation de la solution (4)	Oui	Pas de réserve à l'acceptation de la solution
	Atteinte des objectifs (5)	100%	

(1) Les parties prenantes sont principalement les entités bénéficiaires concernées de l'ACV mais aussi éventuellement les communes ou d'autres organisations partenaires, à l'exception de la DGNSI dont la satisfaction est évaluée de manière spécifique.

(2) Barème pour l'évaluation de la satisfaction :
1 : Très Insatisfait
2 : Insatisfait
3 : Satisfait
4 : Très Satisfait
5 : Satisfait Au-delà des attentes

(3) La métrique *Satisfaction de la DGNSI* correspond à l'évaluation de la satisfaction de la DGNSI en tant qu'organisation permanente.

(4) La métrique *Acceptation de la solution* par les parties prenantes se base sur le livrable « Protocole de recette d'une solution »

7.1.1 Détail des résultats

Le projet a permis le développement d'un outil qui apporte à la DGNSI la capacité d'analyser, à intervalles réguliers, le contenu des espaces wiki. Cette possibilité permet d'améliorer le niveau de sécurité global.

7.2 Satisfaction de la DGNSI

Date de l'évaluation : 15.12.2026

Satisfaction totale. Quelques différences de fonctionnalités observées entre les spécification initiale et l'implémentation, mais les capacités de l'outil à couvrir le scope initial est complet.

8 LIVRAISON ET PARTAGE DU PROGET

8.1 Mise à disposition du projet en Open Source

Etant donné que ce projet est financé au travers de l'initiative **Erreur ! Référence de lien hypertexte non valide.**, nous avons décidé de mettre le projet à disposition au travers du repository github suivant, accessible publiquement sous licence Open Source MIT : https://github.com/Softcom-Technologies-Organization/ai-sentinel.

Le projet est aussi disponible sur le github de l'Etat de Vaud https://github.com/DSI-VD/ai-sentinel

9 ANNEXES

9.1 Spécifications techniques

AISentinel_tech_specs.pdf

9.2 Documentation technique et utilisateur

README.md

=== FIN DU DOCUMENT ===