RÉPUBLIQUE FRANÇAISE

Liberté
Égalité
Fraternité

L'IA AU SERVICE DE LA DÉTECTION : ENJEUX ET IMPACTS ?

RETOUR SUR UNE ÉTUDE DU MARCHÉ FRANÇAIS

Étude de marché : objectifs

Objectif ANSSI : mieux **comprendre l'état de l'art technologique en matière d'IA dans les solutions de détection et de réponse** aux incidents.

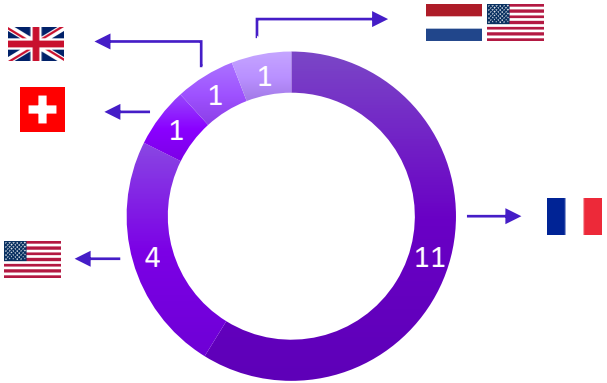
SOUS-OBJECTIFS ANSSI :

- / Confronter les travaux de recherche avec la réalité terrain
- / Enrichir la doctrine de détection
- / Capitaliser pour outiller l'ANSSI
- / Avoir une meilleure connaissance de l'offre (notamment française)

CONSTATS DANS LE SOC :

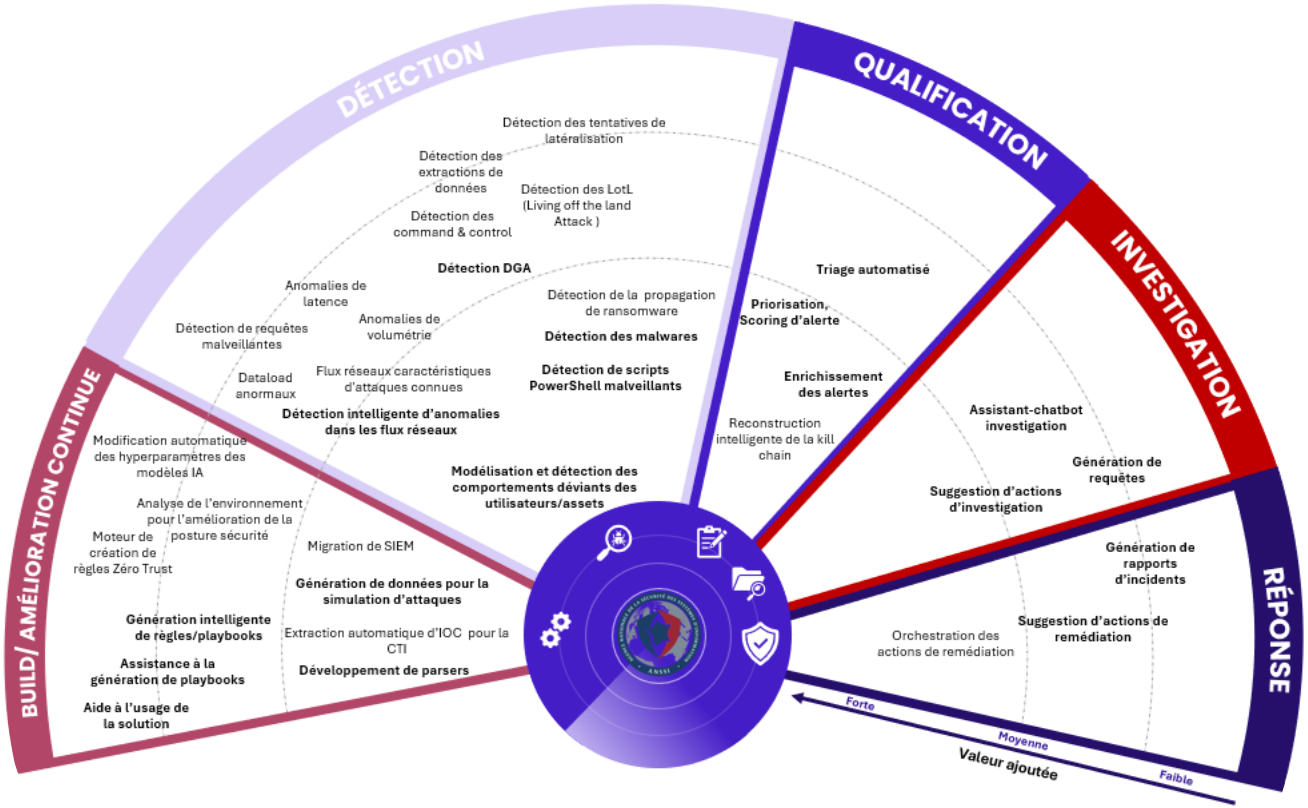
- ↗ Déploiements de l'IA
- ↗ Nombre d'alertes de sécurité
- ↘ Recrutements (pénurie de personnel)
- ↗ Nombre de parties prenantes (sous-traitance)
- ↗ Nombre d'outils déployés

18 éditeurs sollicités

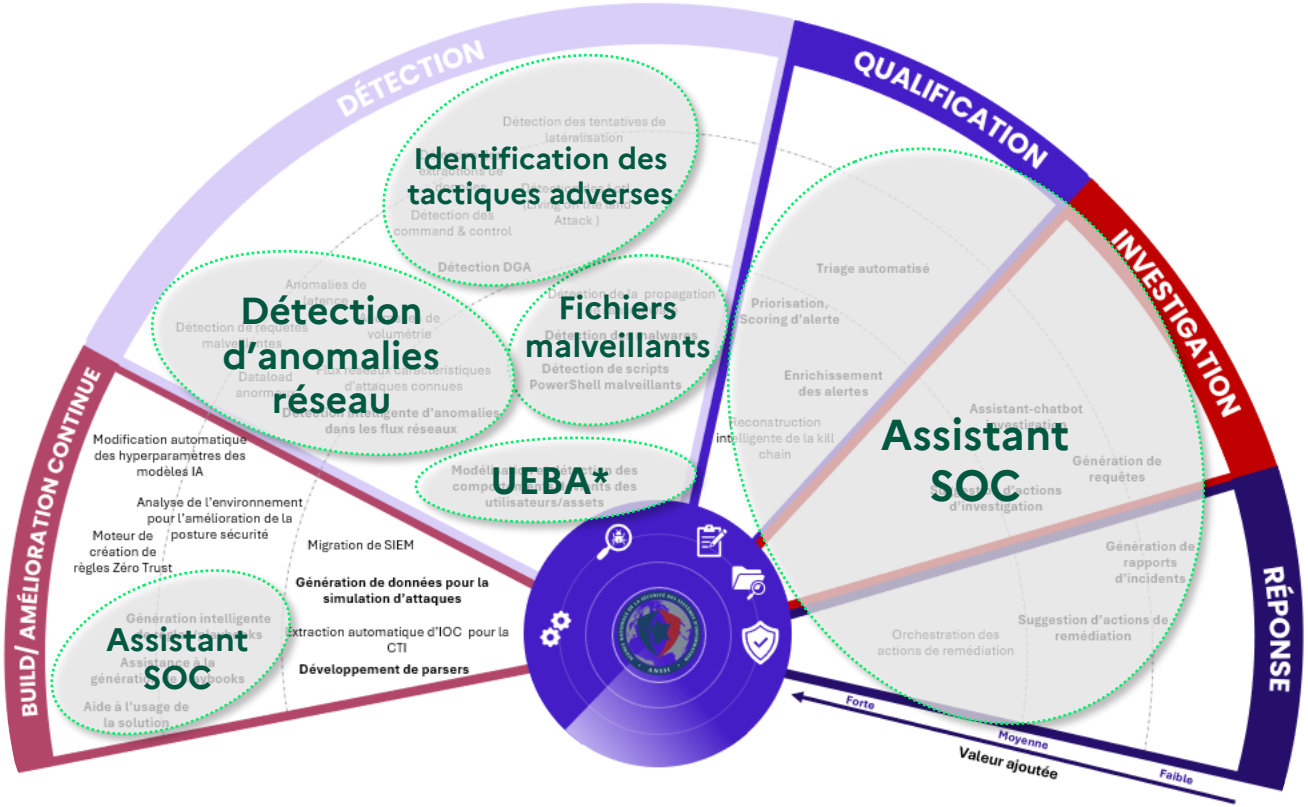


1. PANORAMA DES CAS D'USAGE DE L'IA DANS LA CHAÎNE DE DÉTECTION ET RÉPONSE

Panorama des cas d'usage de l'IA pour le SOC



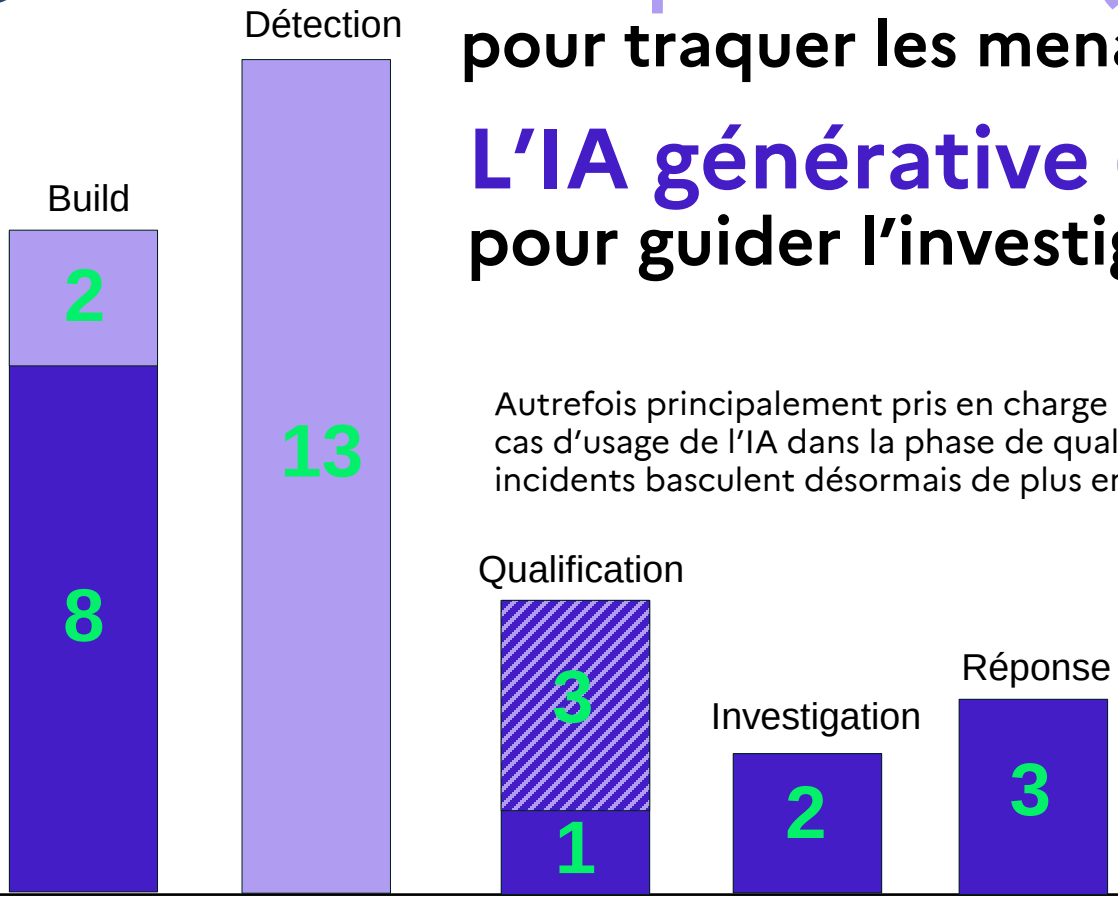
5 catégories de cas d'usage de l'IA pour le SOC



** User & Entity Behavior Analytics*

L'IA prédictive (PredAI)
pour traquer les menaces

L'IA générative (GenAI)
pour guider l'investigation



Autrefois principalement pris en charge par la PredAI, les cas d'usage de l'IA dans la phase de qualification des incidents basculent désormais de plus en plus vers la GenAI.

Répartition des cas d'usage PredAI vs **GenAI**

2. PREDAI, DES USAGES CENTRÉS SUR LA DÉTECTION

Les principaux cas d'usage de la PredAI pour le SOC

1

User & Entity Behavior Analytics (UEBA)

Analyse des comportements des utilisateurs et des équipements afin de détecter des écarts ou des activités suspectes.

2

Détection d'anomalies réseau

Analyse du trafic réseau pour la détection d'anomalies (volumétrie, latence, protocoles, scans etc.)

3

Priorisation d'incident

Attribution de scores de criticité et de priorité à une alerte

4

Détection de malware

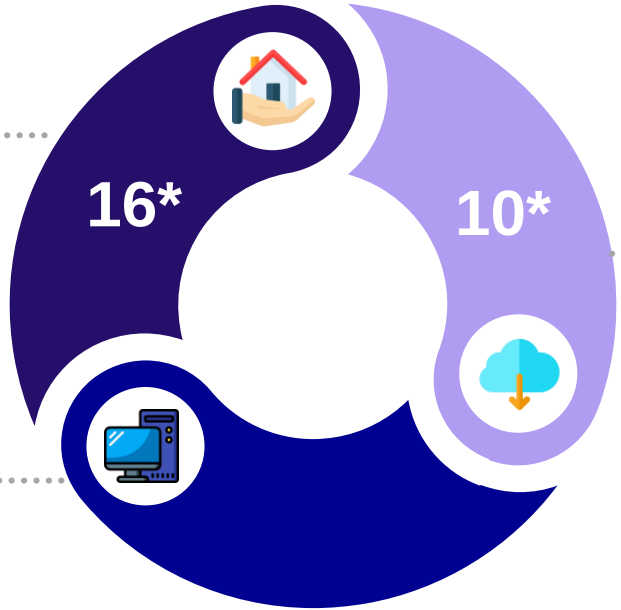
Analyse des fichiers pour la détection de logiciels malveillants

Leur performance continue de progresser !

Les modalités de développement et d'hébergement de la PredAI

1 **Des modèles développés en interne…**

Des modèles développés quasi exclusivement en interne par les éditeurs, notamment grâce aux librairies OpenSource



2 **…et souvent hébergés dans le Cloud…**

Pour utiliser des modèles puissants (et lourds) et traiter de grandes quantités données, l'hébergement des modèles dans le cloud s'impose.

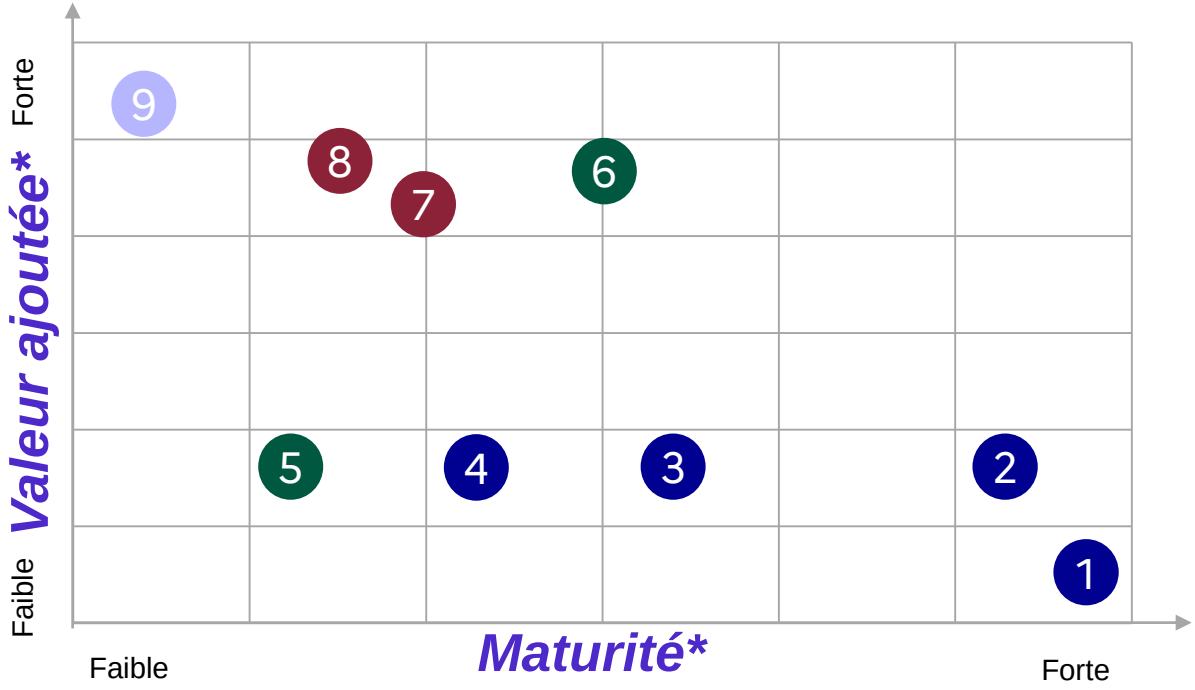
3 **…à l'exception des modèles conçus pour les EDRs**

Pour les solutions EDRs, les modèles sont hébergés au plus près des données, c'est-à-dire sur les terminaux, à condition d'être légers et peu gourmands en ressources.

* Parmi les 18 éditeurs rencontrés, 16 développent leurs propres modèles de PredAI en interne et 10 utilisent au moins partiellement le cloud pour l'hébergement.

3. GENAI, POUR GUIDER ET ACCÉLÉRER LES TÂCHES DE L'ANALYSTE

Matrice des cas d'usage GenAI



*Valeur ajoutée : Estimation **théorique** de l'apport de la fonctionnalité perçue par l'utilisateur (gain de temps/efficacité)
*Maturité : Estimation basée sur : date moyenne de mise en place, nombre d'éditeurs proposant le cas d'usage, complexité et retour terrain.

Assister

1. Assistance à l'utilisation de la solution
2. Assistance à la génération de requête
3. Assistance à la construction de playbooks et de règles de détection
4. Assistance à l'identification d'actions d'investigation et de réponse

Enrichir

5. Génération de rapports d'incidents
6. Enrichissement des alertes

Interpréter

7. Génération autonome de playbooks et de règles
8. Qualification des alertes

Agir

9. Orchestration autonome des outils de réponse à incident

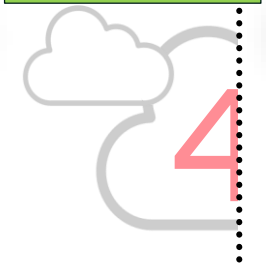
L'hébergement des LLM, un sujet sensible pour les données

LLM propriétaire

Hébergé chez le fournisseur du modèle

Le modèle est géré et hébergé par le fournisseur de modèle et la connexion se fait par un lien API (ex. OpenAI GPT-4, Google Gemini).
Maitrise de la donnée: **FAIBLE**
Constat : Modèle privilégié à date

LLM OpenSource



Hébergé chez un cloud provider

Le modèle est géré et hébergé par le cloud provider et la connexion se fait via API (AWS Bedrock, Azure AI).
Maitrise de la donnée: **FAIBLE**

LLM OpenSource

Hébergé chez l'éditeur de solution de sécurité

Le modèle est géré et hébergé par l'éditeur de la solution qui est en charge de l'infrastructure et du modèle.
Maitrise de la donnée: **MOYENNE**

LLM OpenSource

Hébergé en interne (Bring Your Own Model)

Le modèle est géré et hébergé par le client.

Maitrise de la donnée: **FORTE**

* Observations parmi les 18 éditeurs rencontrés

La provenance du modèle de fondation jouera un rôle de plus en plus déterminant pour les éditeurs de solution

Critères de choix des modèles

Performance

- Rapidité d'exécution
- Qualité des réponses fournies

+

Accessibilité des modèles

- *Propriétaire* / *OpenSource*
- *Semi-ouvert*

+

Coût de calcul

- Ressources informatiques nécessaires

+

Provenance modèle

Dans un contexte où ces modèles joueront un rôle ***stratégique dans la prise de décision et l'automatisation des processus critiques, leur origine et leur chaîne d'approvisionnement devront être évalués avec attention.***

Les éditeurs ont une approche similaire dans l'utilisation des LLM

Science du Prompt

La qualité et la précision des réponses est liée à la capacité à construire des prompts de qualité. Ainsi, les éditeurs investissent sur l'optimisation de ces derniers.

Pas de réentrainement

- L'amélioration continue des performances des LLM rend rapidement les modèles ré-entrainés obsolètes.
- La faible valeur ajoutée sur les performances par rapport aux coûts financiers d'un ré-entraînement.

RAG

La personnalisation des modèles s'effectue systématiquement via l'approche « Retrieval-Augmented Generation. »

Confiance et sécurité de la donnée : des enjeux critiques

	Risques	Approches des éditeurs
Confiance	Hallucination	Améliorer la qualité des prompts
	Variabilité des réponses	Assurer un contrôle des résultats
	Corruption des modèles	
Données	Fuite des données	Hébergement des modèles
		Contrôle des informations transmises aux modèles

4. QUE CONCLURE ?

Que conclure ?

MESSAGES CLÉS

- **Investissements** : ↘ PredAI ↗ GenAI
- **PredAI** : développement *from scratch* avec l'OpenSource.
- **GenAI** : s'appuie sur les LLM des grands éditeurs.
- **Enjeux éditeurs** : qualité des jeux de données pour l'entrainement, supervision de la performance des modèles dans le temps.
- La **protection des données des clients** devient un enjeu crucial.

PISTES DE RÉFLEXION

- **Besoin de financer des projets innovants sur l'IA et la détection ?** → *Appels à projets (France 2030, NCC-FR…).*
- **Une offre de marché en phase avec la demande de nos bénéficiaires ?**
- **Anticiper l'apport de l'IA sur d'autres segments de la cybersécurité.**
- **Identifier les bons leviers d'action pour accompagner l'offre.**

Travaux de l'ANSSI sur l'IA

ANSSI : autorité nationale sur les enjeux cyber liés à l'IA

IA : technologie à forts enjeux de cybersécurité dans le plan stratégique de l'ANSSI 2025-2027 (lien)

PLUSIEURS GRANDS AXES DE TRAVAIL DONT :

- Connaissance et accompagnement de l'offre
- Certification de produits cyber intégrant de l'IA
- Accompagnement des administrations et opérateurs régulés dans la sécurisation de leurs SIA

PUBLICATIONS :

- Recommandations de sécurité pour un système d'IA générative (avril 2024 - lien)
- Recommandations de sécurité concernant les assistants de programmation basés sur l'IA (ANSSI-BSI, octobre 2024 - lien)
- Développer la confiance dans l'IA par une approche par les risques cyber (février 2025 – lien)

Détails et remerciements

L'ANSSI a été **accompagnée par Wavestone** dans la réalisation de cette étude de marché et remercie l'ensemble des consultants impliqués.

L'ANSSI et Wavestone remercient les **18 éditeurs rencontrés** lors de cette étude pour leur disponibilité et le partage de leurs travaux : Sekoia, Nucleon Security, OGO Security, Parcoor, Mindflow, Tehtris, Custocy, Sesame IT, HarfangLab, Gatewatcher, Qevlar AI, Microsoft, Trellix, Elastic, Extrahop, Exabeam, Nozomi Networks et Darktrace.

Pour toute question portant sur cette étude, n'hésitez pas à contacter la Division Industrie et Technologies à l'adresse suivante : industries@ssi.gouv.fr