

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

RETOURS SUR UNE ÉTUDE DU MARCHÉ EUROPÉEN



1. INTRODUCTION



L'objectif de cette étude est de permettre à l'ANSSI et aux Centres Européens de Compétences Cyber d'avoir une vision de l'état de l'art technologique de l'intelligence artificielle et des tendances actuelles et à venir sur le marché de détection et de réponse aux incidents.

Périmètre de l'étude



L'étude se concentre principalement sur les **éditeurs européens**, tout en incluant également des éditeurs internationaux ayant une forte présence sur le **marché de l'Union Européenne**, dans le but de **comparer leurs pratiques et usages en matière d'IA**.



Démarche

1

Etude conceptuelle et identification des acteurs

Réalisation d'un panorama de l'IA dans les outils de cybersécurité sur la base de travaux académiques.

2

Rencontres éditeurs

Atelier de travail d'1h30 à 2h avec **chacun des éditeurs**. Les entretiens ont été menés avec l'appui d'un **questionnaire** élaboré en **collaboration** avec l'équipe de l'**ANSSI**.

3

Synthèse et analyse

Elaboration d'une synthèse reprenant les informations essentielles, obtenues lors des différents entretiens, enrichies de l'expertise et des convictions de Wavestone.



De plus en plus de difficultés pour les SOC à suivre le rythme



→ De plus en plus d'alertes de sécurité

- Augmentation continue du nombre d'attaques.
- Extension des périmètres de détection (cloud, environnement mobile, etc.).
- Complexité des attaques.



→ Pénurie mondiale de personnel

- Pénurie de compétences en cybersécurité et absence de temps pour acquérir les compétences nécessaires.
- Turnover important dans les équipes N1/N2 en raison de la répétitivité de leurs tâches.



→ Les SOC ne se résument plus à un SIEM et une seule équipe

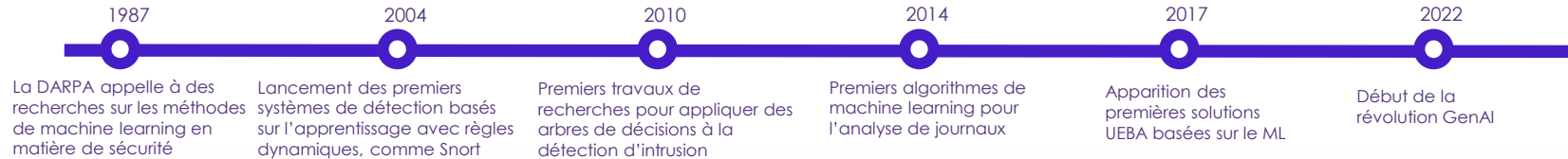
- Diversification des parties prenantes en raison de modèles de SOC complexes (équipes locales et centrales, MSSP et ressources internes, etc.).
- Augmentation du nombre d'outils (Threat Intel, EDR, ITSM, CSPM, etc.) déployés dans les SOC pour gérer l'ensemble du cycle de vie des incidents de cybersécurité.

Cette situation rend difficile le maintien du rythme, la pertinence et l'exhaustivité de la couverture des alertes

Comment l'IA peut contribuer à répondre à ces défis ?



A partir de la décennie 2010, l'IA à travers le Machine Learning va, pas à pas, s'intégrer dans les solutions à disposition du SOC pour améliorer et étendre les capacités de détection



Mais des tâches chronophages et complexes dans la chaîne de détection restaient encore à la charge des analystes à la fin de la décennie 2010 :

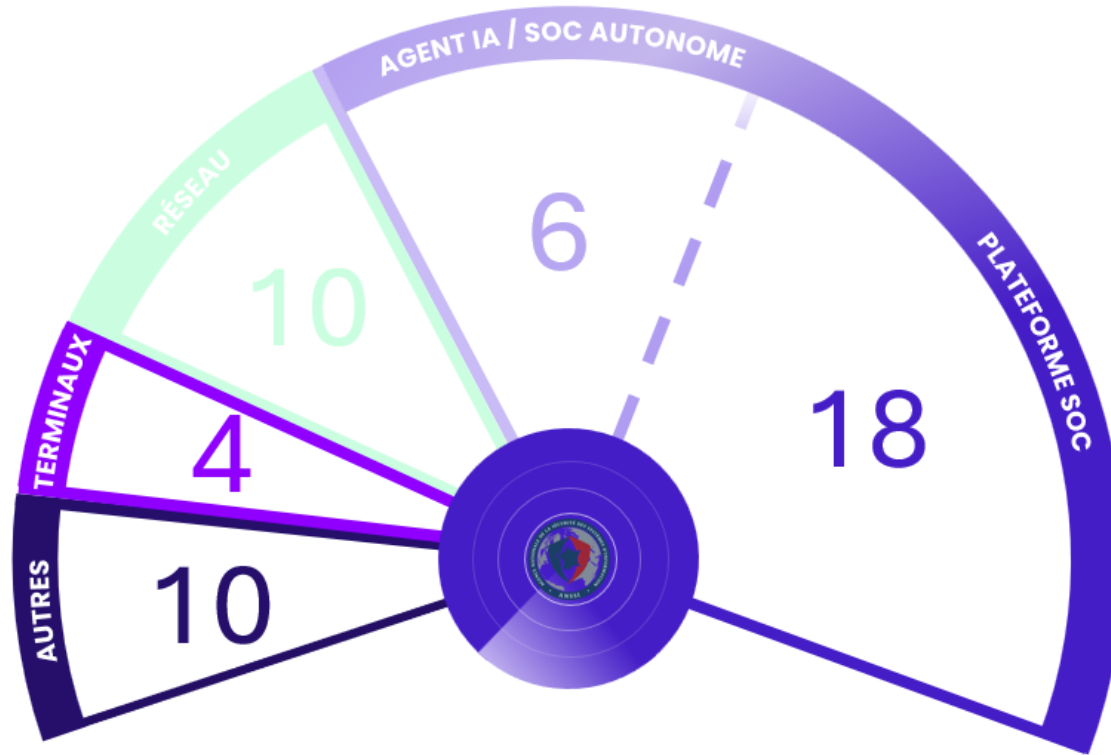
- / Le travail laborieux de **développement des parsers**, pour permettre l'intégration de logs provenant de sources de plus en plus variées
- / **L'enrichissement des alertes**, à la recherche des éléments pertinents dans une montagne d'information
- / **La qualification des alertes**, impossible lorsque le volume d'alertes explose
- / **L'investigation des incidents** une tâche très complexe nécessitant des compétences et une bonne connaissance de l'environnement



2. PANORAMA DES ÉDITEURS RENCONTRÉS



Une grande diversité de solutions étudiées



Nombre d'éditeurs rencontrés par catégorie

A retenir

Le panorama des solutions rencontrées est construit autour de **5 grandes catégories** de produits :

- ① Les plateformes SOC
- ② Les agents IA / SOC autonomes
- ③ Les solutions centrées Réseaux
- ④ Les solutions centrées Endpoints
- ⑤ ... et les autres

Ce sont en réalité plus de **18 types** de solutions qui ont été rencontrés :



















- Plateforme d'analyse de malwares
- Plateforme de gestion de risques
- Plateforme d'audit de code
- Plateforme de gestion de vulnérabilités
- Plateforme de lutte contre la fraude cyber
- ASPM (Application security posture management)
- EDR
- NDR
- IDS
- Firewall
- Proxys
- Email security Gateway
- SIEM
- SOAR
- XDR
- AGENTS IA
- EASM
- WAAF
- Etc.....



Une accélération de la consolidation du marché de la cybersécurité

Les acquisitions se multiplient

Le marché de la cybersécurité connaît une forte concentration, avec de nombreuses opérations de rachat visant à renforcer les capacités de détection, de réponse et d'intégration de l'IA (liste non exhaustive) :

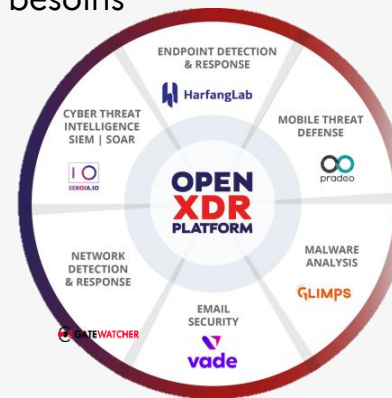
Acquéreur	Cible	Date d'acquisition
Palo Alto Networks 	Talon Cyber Security 	Décembre 2023
SentinelOne 	PingSafe 	Février 2024
CrowdStrike 	Bionic 	Février 2024
Cisco 	Splunk 	Mars 2024
HornetSecurity 	Vade 	Mars 2024
Mimecast 	Aware 	Août 2024
Palo Alto Networks 	IBM Qradar (SaaS) 	Septembre 2024
Logpoint 	Muninn 	Octobre 2024
Proofpoint 	HornetSecurity 	Mai 2025

Une tendance vers la création de plateformes de sécurité couvrant l'ensemble du cycle de détection et de réponse

Des initiatives existent en Europe, même si celles-ci restent minoritaires

2 approches possibles :

Des **alliances stratégiques** pour une couverture intégrale des besoins

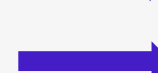


Des **rachats de solutions entre acteurs européens**

LOGPOINT



Muninn



vade



3. FOCUS SUR LA SCÈNE EUROPÉENNE



Iceland



22

Pays étudiés



30-40

Objectif de
rencontres
d'éditeurs



+450

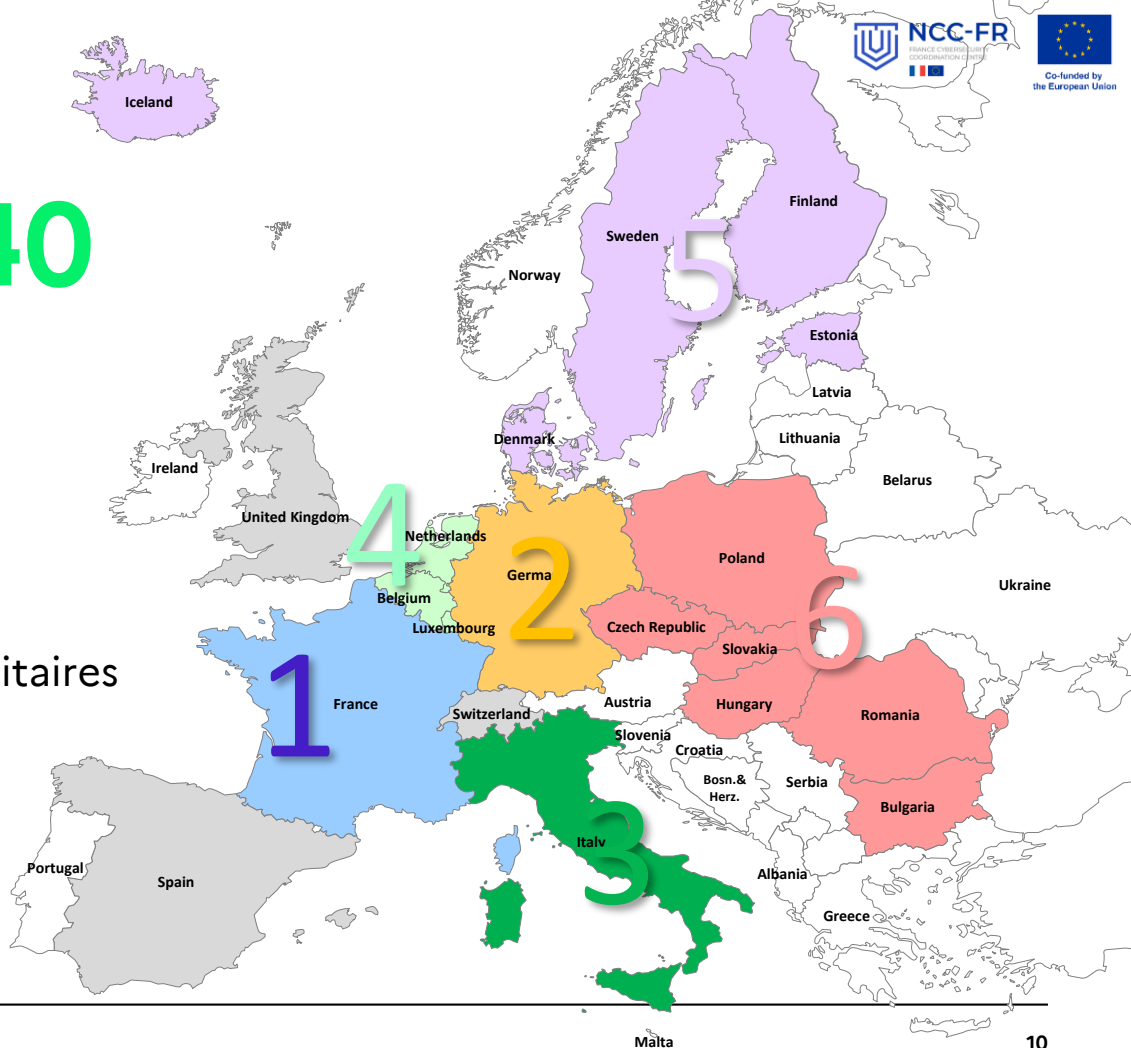
Éditeurs analysés



6

Périmètres géographiques prioritaires

1. France
2. Allemagne
3. Italie
4. Benelux
5. Europe du Nord
6. Europe de l'Est
7. Autres



72

Éditeurs identifiés répondant aux critères de l'étude

- 1 Proposer des solutions de cybersécurité pour la **détection** et/ou la **réponse** à incident.
- 2 Intégrer des fonctionnalités basées sur **l'intelligence artificielle***

*Ensemble de fonctionnalités reposant sur le machine learning/deep learning mettant en œuvre des algorithmes capables d'apprendre à partir de données d'entraînement, et de raisonner ou produire des prédictions sur des situations inédites, non rencontrées lors de la phase d'apprentissage.





34

Éditeurs européens rencontrés
lors de la phase d'entretien

 **16 éditeurs français**

 **4 éditeurs allemands**

 **2 éditeurs italiens**

 **2 éditeurs britanniques**

 **2 éditeurs du Benelux**

 **4 éditeurs d'Europe du Nord**

 **3 éditeurs d'Europe de l'Est**

 **1 éditeur suisse**

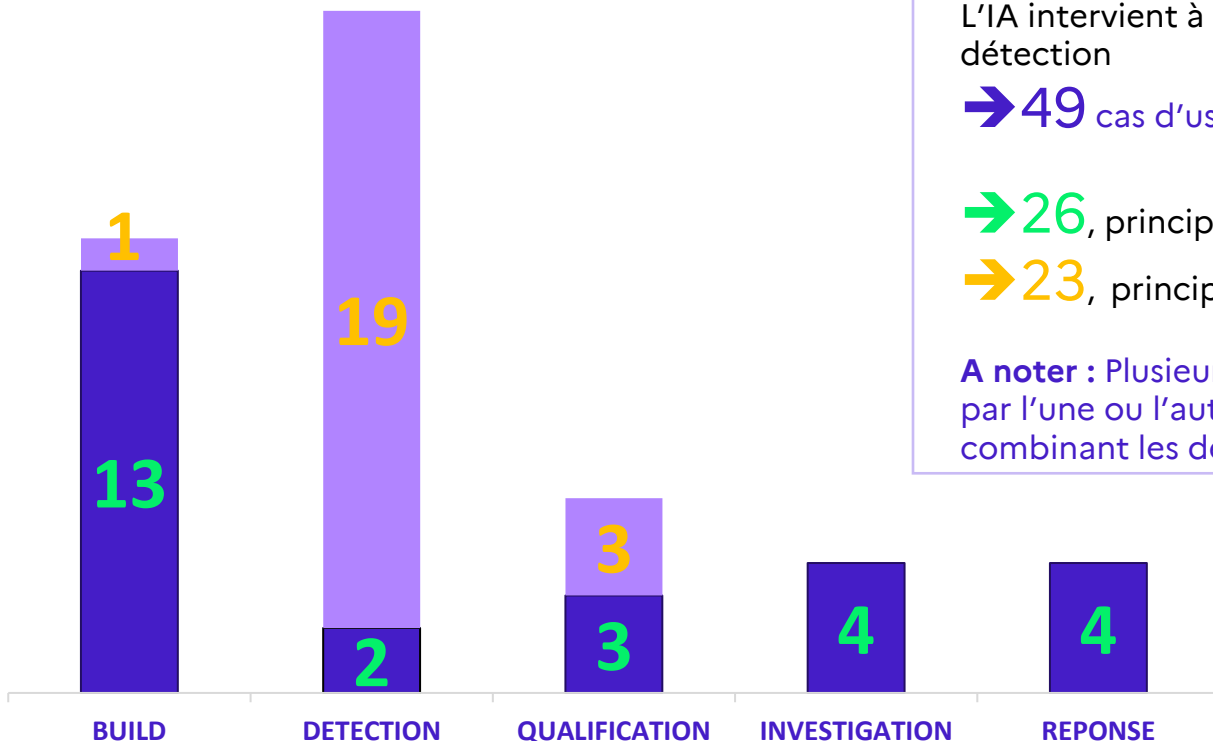




4. PANORAMA DES CAS D'USAGE DE L'IA DANS LA CHAÎNE DE DÉTECTION



basée uniquement sur les cas d'usage discutés lors des entretiens



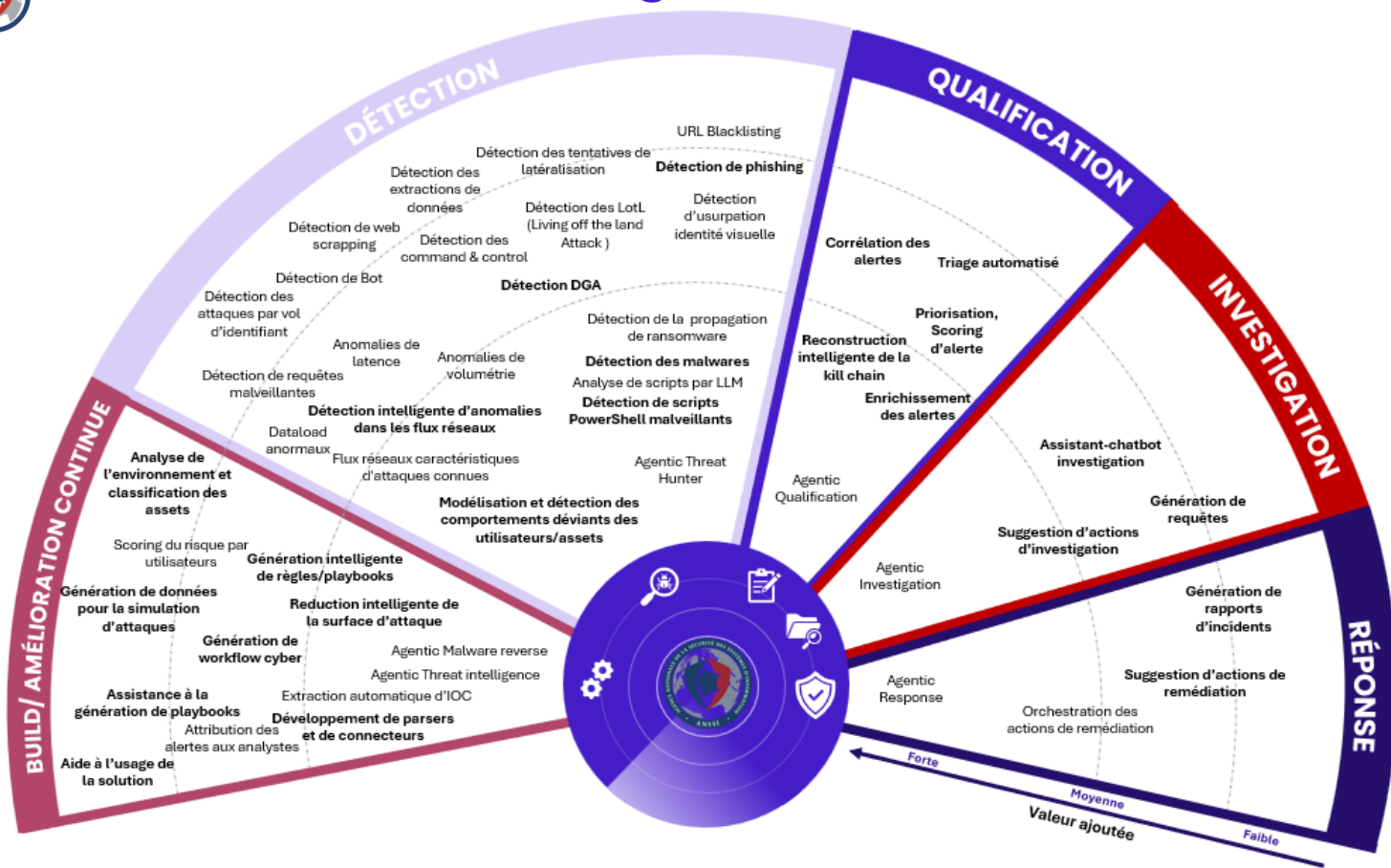
L'IA intervient à tous les niveaux de la chaîne de détection

→ 49 cas d'usage uniques ont été recensés

→ 26, principalement construit sur de la GenAI

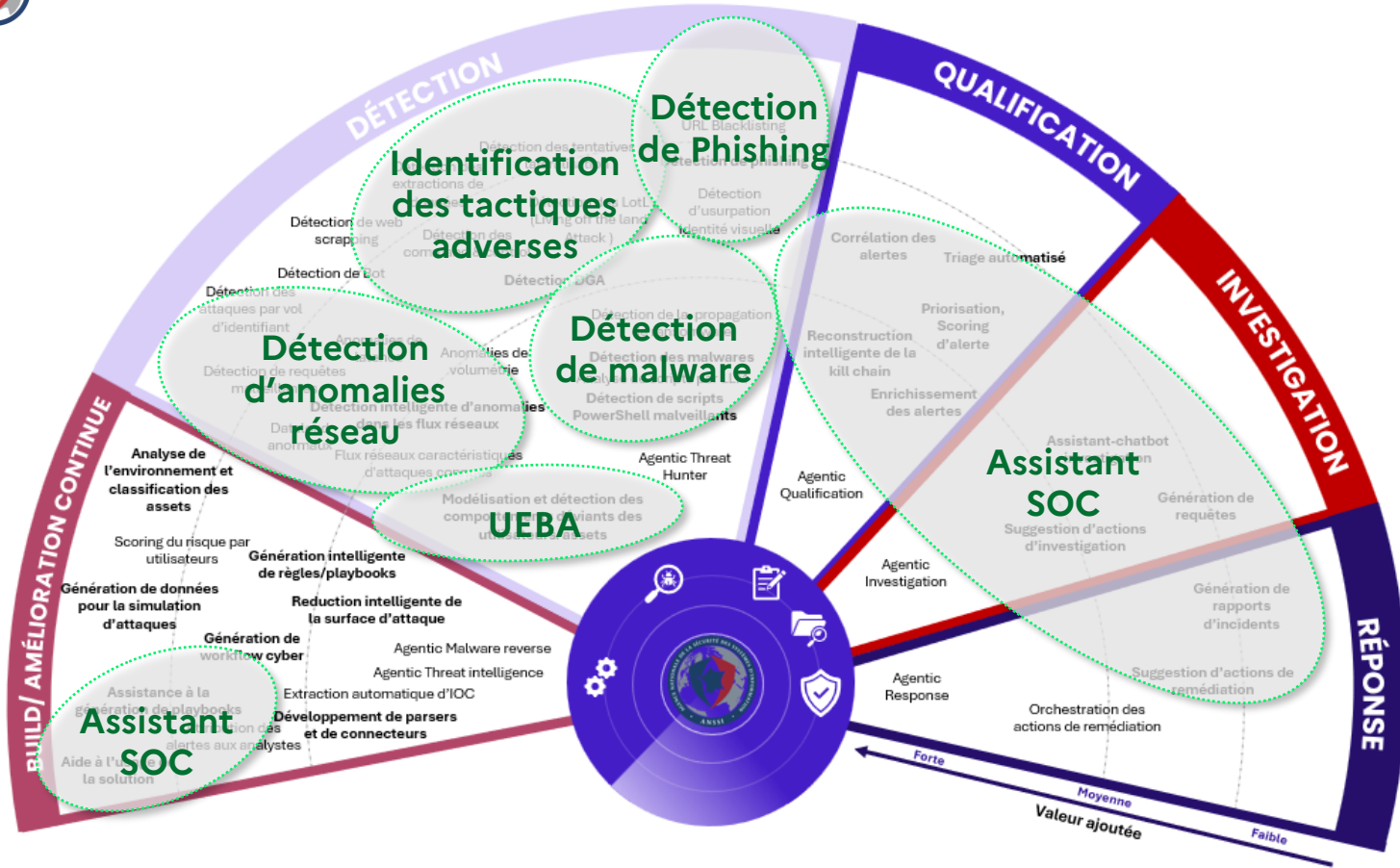
→ 23, principalement construit sur de la PredAI

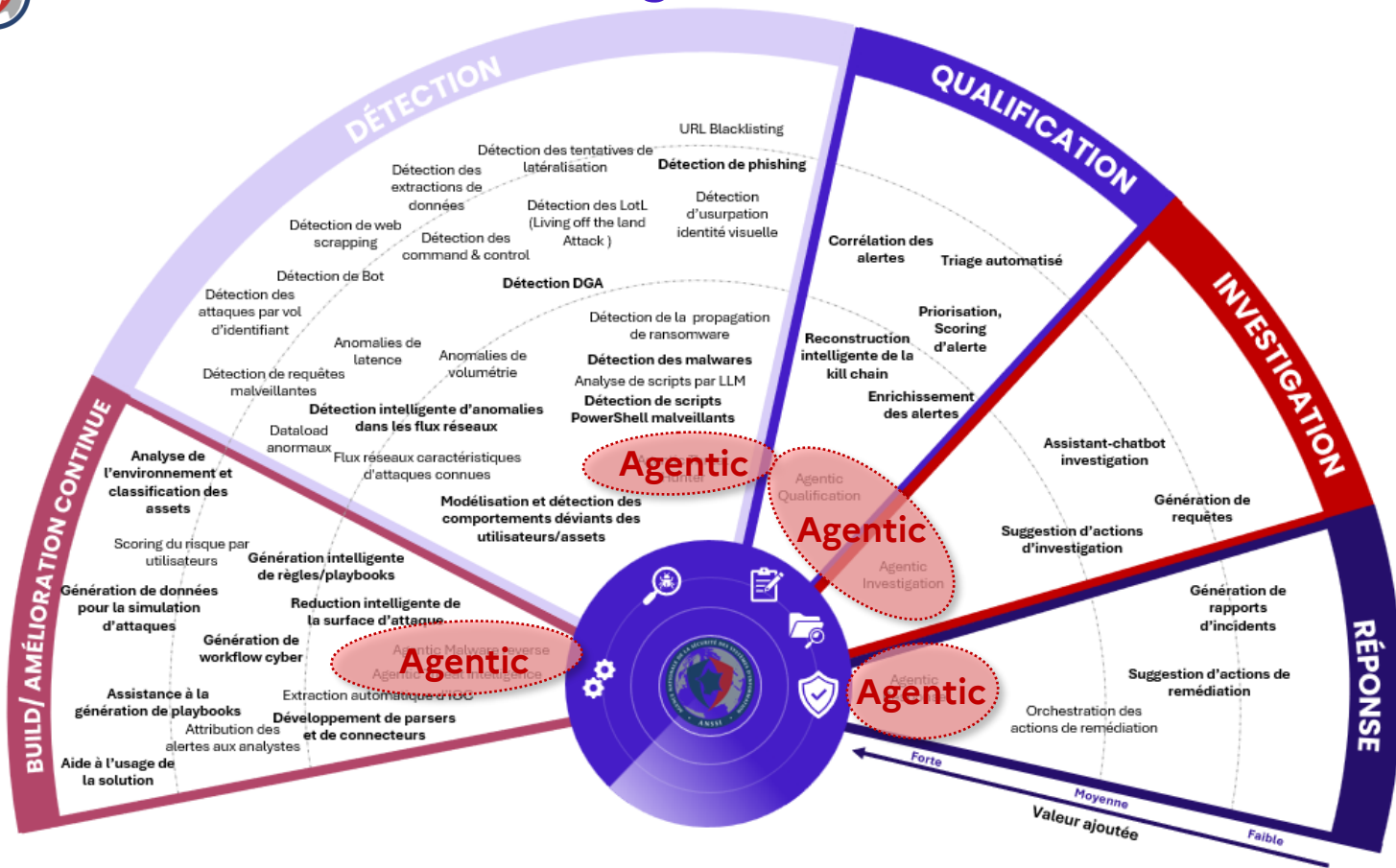
A noter : Plusieurs cas d'usage sont à la fois adressés par l'une ou l'autre des technologies, parfois combinant les deux.





Panorama des cas d'usages







Des constats homogènes sur le périmètre européen



Émergence de la **GenAI** à travers des chatbots, aux fonctionnalités encore limitées et disparates en fonction des pays



Application pour des cas d'usage variés de la **PredAI** chez certains éditeurs européens depuis plus de 15 ans, **preuve d'une maîtrise avancée**



De **premières initiatives** autour de l'IA agentique, attendue surtout pour soulager les tâches de qualification et d'investigation



Des résultats **à interpréter avec prudence**, compte tenu de l'échantillon non-exhaustif d'éditeurs consultés



5. PREDAI, DES USAGES CENTRÉS SUR LA DÉTECTION



Top 5 des cas d'usage de la PredAI

1 User & Entity Behavior Analytics

Analyse des comportements des utilisateurs et des assets 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

5 Détection de phishing

Analyse des emails pour détection de tentative de phishing

Et ils continuent de progresser



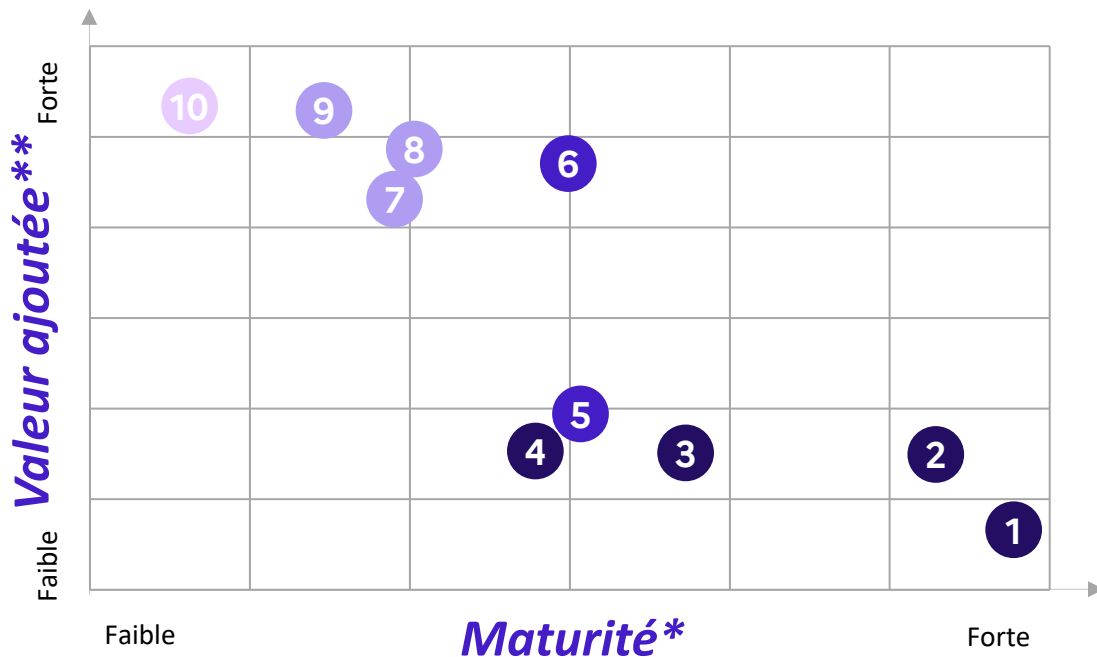
6. GENAI, UN USAGE MAJORITAIREMENT POUR GUIDER LES ANALYSTES ET ACCÉLÉRER LES ACTIONS



La GenAI est utilisée au travers « d'assistants » plus ou moins « intelligents »

Matrice des cas d'usage de la GenAI

*basée sur les éditeurs investis dans le développement d'un assistant SOC



Assister

- 1 Assistance à l'utilisation de la solution
- 2 Assistance à la génération de requêtes
- 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

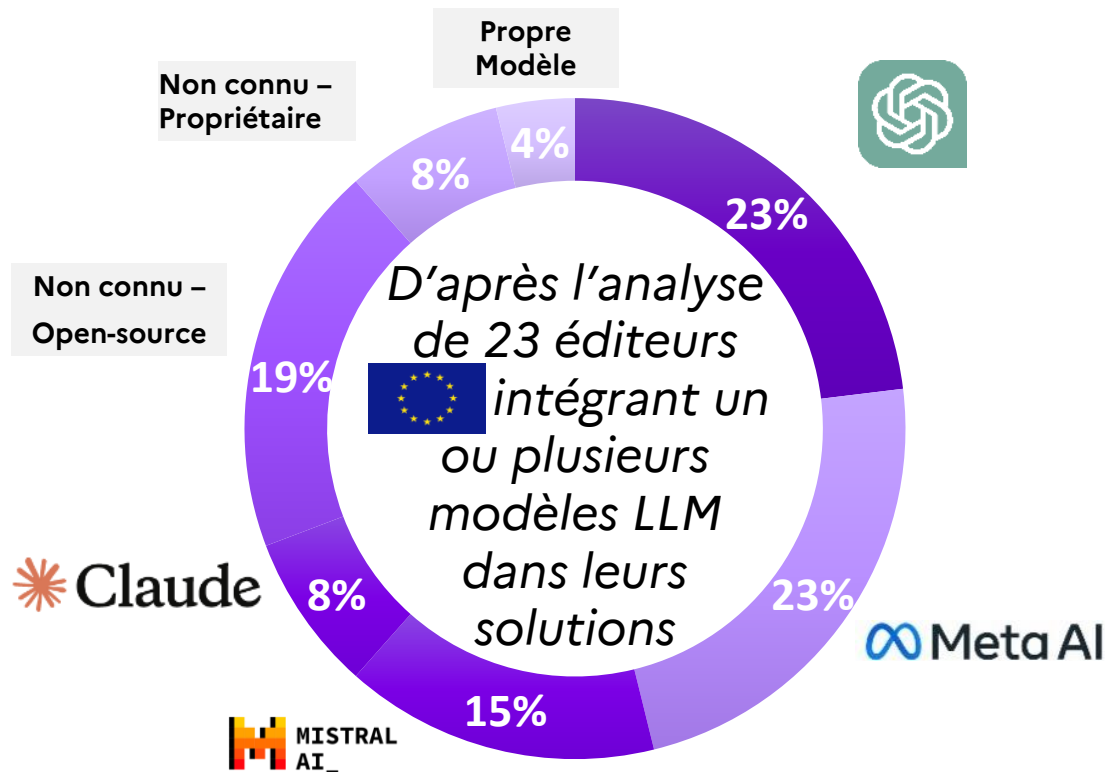
- 7 Génération autonome de playbooks et de règles
- 8 Qualification / Triage autonome des alertes
- 9 Investigation autonome

Agir

- 10 Réponse autonome



Les éditeurs interrogés s'appuient majoritairement sur 4 fournisseurs de modèles d'IA

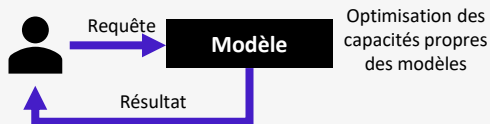


Les éditeurs européens privilégient généralement les modèles open-source tels que les solutions Llama et Mistral AI.

Ceux qui utilisent des solutions propriétaires envisagent de migrer vers des solutions open-source.

3 approches utilisées par les éditeurs pour optimiser les performances des modèles de fondations

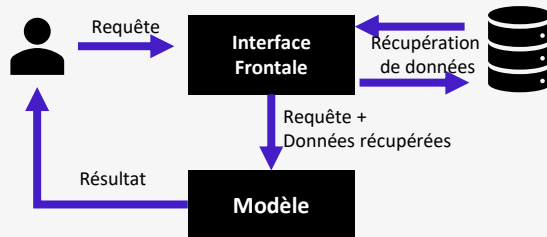
Prompt Engineering



- + Rapide à mettre en œuvre
- + Pas d'infrastructure supplémentaire
- Performance variable (*dépendant de la qualité du prompt*)
- Connaissance limitée aux données d'entraînement du modèle

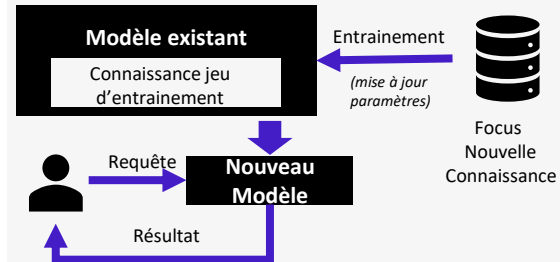
RAG

Retrieval-Augmented Generation



- + Utilisation de données spécifiques et à jour (*client/éditeur/contexte cyber*)
- + Facilité de mise à jour des données
- + Réduction des hallucinations
- Performance réduite (*latence*)
- Infrastructure supplémentaire (*coût/complexité/sécurité*)
- Qualité dépendante des documents sources

Fine-Tuning



- + Réponse rapide sur des cas spécifiques
- + Spécialisation métier / domaine (*cyber*)
- + Amélioration de la pertinence et de la précision
- Phase d'entraînement complexe (*volume et qualité du dataset*)
- Coût élevé de la phase d'entraînement
- Maintien des données à jour (*réentraînement nécessaire*)
- Perte de compétences générales

La majorité des éditeurs privilégient une approche pragmatique basée sur le RAG, exploitant des données spécifiques à leurs produits, des éléments liés à la cybersécurité et des données clients pour personnaliser les réponses. Cette stratégie est renforcée par le prompt engineering, qui optimise les capacités des modèles existants. À l'inverse, le fine-tuning, plus complexe et coûteux, reste limité à quelques acteurs, illustrant une différenciation nette dans les choix technologiques.



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

LLM propriétaire

38%

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, Mistral AI, Anthropic).

Maitrise de la donnée: **FAIBLE**

Constat : *Modèle privilégié par les éditeurs utilisant notamment le modèle d'OpenAI*

LLM partenaire

LLM open source

15%

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: **MOYENNE**

Constat : *Modèle privilégié par les éditeurs voulant un accès à plusieurs modèles dont des modèles historiquement accessibles uniquement depuis les environnements du fournisseur du modèle.*

Hébergé chez l'éditeur de solution de sécurité

32%

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: **FORTE**

Constat : *Modèle privilégié par les éditeurs cherchant à garantir un niveau de confidentialité élevé.*

15%

Hébergé dans l'environnement client

Le modèle est géré par l'éditeur et hébergé dans l'environnement client.

Maitrise de la donnée: **FORTE**

Constat : *Modèle privilégié par les éditeurs voulant maintenir les données dans l'environnement client*

À l'échelle des éditeurs européens, la répartition dans l'utilisation des types d'hébergement est similaire. Cependant, on observe une augmentation de la proportion d'éditeurs qui hébergent leurs modèles dans leur propre infrastructure, contrairement à ceux qui utilisent des solutions SaaS d'hébergeurs Cloud.



La provenance du modèle de fondation jouera un rôle de plus en plus déterminant dans le choix de celui-ci par les éditeurs de solution

Critères de choix des modèles

Performance

- / Rapidité d'exécution
- / Qualité des réponses fournies



Accessibilité des modèles

- / Propriétaire
- / Semi-ouvert
- / Open source



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 de conception devront être évaluées avec attention.***



Confiance et sécurité de la donnée : des enjeux critiques pour l'adoption de la GenAI

Risques

Hallucination

Variabilité des réponses

Empoisonnement des modèles

Fuite de données

Approche des éditeurs

Améliorer la qualité des prompts

Assurer un contrôle des résultats

Hébergement des modèles

Contrôle des informations transmises
aux modèles

Confiance

Données



7. AGENTIC AI



De nouvelles solutions, appelées « Agent IA SOC », ont émergé ces dernières années. Ces agents « intelligents » ont pour objectif d'automatiser la qualification et l'investigation des alertes de sécurité, en reproduisant les raisonnements d'un analyste SOC. Certaines veulent aller plus loin et visent à automatiser la phase de réponse, tout en maintenant des mécanismes de contrôle humain.

Points-clés à retenir

- 1 Une approche combinant ML/DL et LLMs, mais se distinguant entre elles par la technologie de l'orchestrateur : **déterministe** via ML/DL, ou **non-déterministe** via LLMs
- 2 Des LLMs utilisés bien au-delà de la simple synthèse de documents
- 3 Décompose le traitement des alertes en tâches spécialisées
Exemples : classification, génération de requêtes, ...
- 4 Traite la chaîne complète de détection et de réponse, de la qualification à la remédiation
- 5 Un enjeu majeur, **l'explicabilité et la reproductibilité des résultats**

L'Agentic AI ne se limite pas aux nouvelles solutions — elle est également intégrée aux plateformes SOC existantes



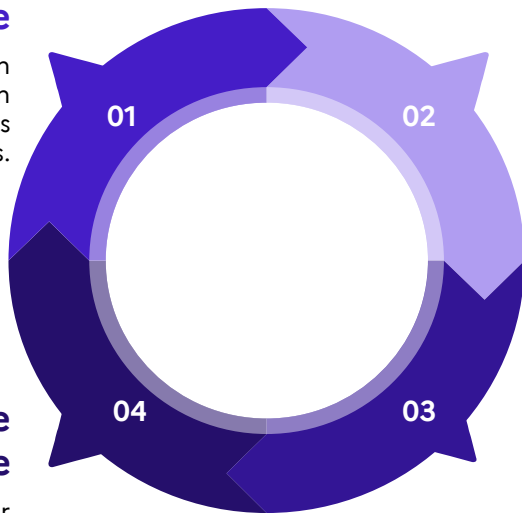
7. ET DEMAIN...



La PredAI est solidement installée et fonctionnelle. Les futures innovations s'appuieront sur la GenAI et l'Agentic AI

Choix du modèle

Le choix du modèle fait par un éditeur aura un impact sur son utilisation dans certains environnements clients.



Une autonomie grandissante

L'IA va permettre, à terme, d'aller vers des fonctionnalités de plus en plus autonomes.

Construire la confiance

Les éditeurs vont devoir mettre en place des mécanismes pour s'assurer de la qualité et de la pertinence des actions produites par la GenAI.

Vers une utilisation systématique de ressources cloud

Aujourd'hui, les modèles LLM requièrent une grande capacité de calcul pour fonctionner.

L'Agentic AI, particulièrement utilisée lors de la phase de qualification des alertes, progresse rapidement. Certains éditeurs l'intègrent déjà dans leurs solutions. Demain, cela pourrait être suivi par la remédiation autonome.

L'intégration de l'IA, en particulier de l'Agentic AI, impose de définir des mécanismes permettant d'évaluer le niveau de confiance et d'en assurer la pérennité dans le temps.



Merci à tous les fournisseurs ayant participé à l'étude « L'IA au service de la détection : enjeux et impacts ». Votre contribution a été essentielle pour enrichir l'analyse et faire progresser l'utilisation de l'IA au sein des opérations SOC.

Simbian Sesame it mindflow DARKTRACE exabeam™ VECTRA™

GATEWATCHER RadiantSecurity pradeo splunk > a CISCO company <TEHRIS> FACE THE UNPREDICTABLE elastic OGO

paloalto® NETWORKS Resistine Google Cloud Security CUSTOCY™ Microsoft Secaire AT Powered Security

ENGINSIGHT Bitdefender CYBEROO sekoia FORTINET™ ExtraHop

LOGPOINT Filigran Qevlar AI hound bytes CLAVISTER ScanDog

imperum Outpost24 NOZOMI NETWORKS Trellix GLIMPS HarfangLab

CROWDSTRIKE NANO CORP. Nucleon Protect data that matters REDCARBON DataDome PARCOOR CYBERSEQ mimecast™ NN5S varist zscaler™

L'ANSSI A ÉTÉ ACCOMPAGNÉE PAR WAVESTONE DANS LA RÉALISATION DE CETTE ÉTUDE DE MARCHÉ ET REMERCIE L'ENSEMBLE DES CONSULTANTS IMPLIQUÉS.

**POUR TOUTE QUESTION PORTANT SUR CETTE ÉTUDE, N'HÉSITÉS PAS À CONTACTER LA DIVISION INDUSTRIE ET TECHNOLOGIES À L'ADRESSE SUIVANTE :
INDUSTRIES@SSI.GOUV.FR**