RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION
ANSSI

NCC-FR
FRANCE CYBERSECURITY COORDINATION CENTRE

Co-funded by the European Union

AI IN DETECTION SOLUTIONS: CHALLENGES AND UPCOMING IMPACTS

EUROPEAN MARKET INSIGHTS

1. INTRODUCTION

Objective and approach of the study

The purpose of this study is to provide ANSSI and the European Cyber Competence Center with a comprehensive overview of the state of the art in artificial intelligence technologies, as well as an analysis of current and emerging trends in the incident detection and response market.

Scope of the study

The study focuses primarily on **European vendors**, while **including international vendors with a strong presence in the European Union market**, in order to benchmark their practices and uses of AI in their solutions.

Approach

1 Theorical research and vendors' identification

Creation of a panorama of **AI in cybersecurity tools,** based on academic research.

2 Workshop with vendors

Workshops lasting 1.5 to 2 hours were held with each vendor. The interviews were conducted using a questionnaire prepared **in collaboration** with ANSSI's team.

3 Synthesis and analysis

Development of a **synthesis summarizing the key insights** gathered from the various interviews, enriched with **Wavestone's expertise.**

The challenges of the SOC

SOCs are facing increasing challenges

More and more security alerts

- Continuous increase in the number of attacks
- Expansion of detection perimeters (cloud, mobile environments, etc.)
- Growing complexity of attacks

Global staff shortage

- Lack of cybersecurity skills and lack of time to acquire the necessary skills
- High turnover in L1/L2 teams due to the repetitiveness of their tasks

SOC is no longer just a SIEM and a single team

- Diversification of stakeholders due to complex SOC models (local and central teams, MSSPs and internal resources, etc.).
- Growth in the number of tools deployed in SOCs (Threat Intel, EDR, ITSM, CSPM, etc.) to manage the full lifecycle of cybersecurity incidents.

This makes it difficult to maintain the pace, the relevance and the completeness of alert coverage.

How can AI help SOCs to face these challenges?

AI & SOC: a long lasting relationship

Starting in the 2010s AI, through Machine Learning, was **gradually** integrated into SOC solutions **to enhance** and **expand** detection capabilities.

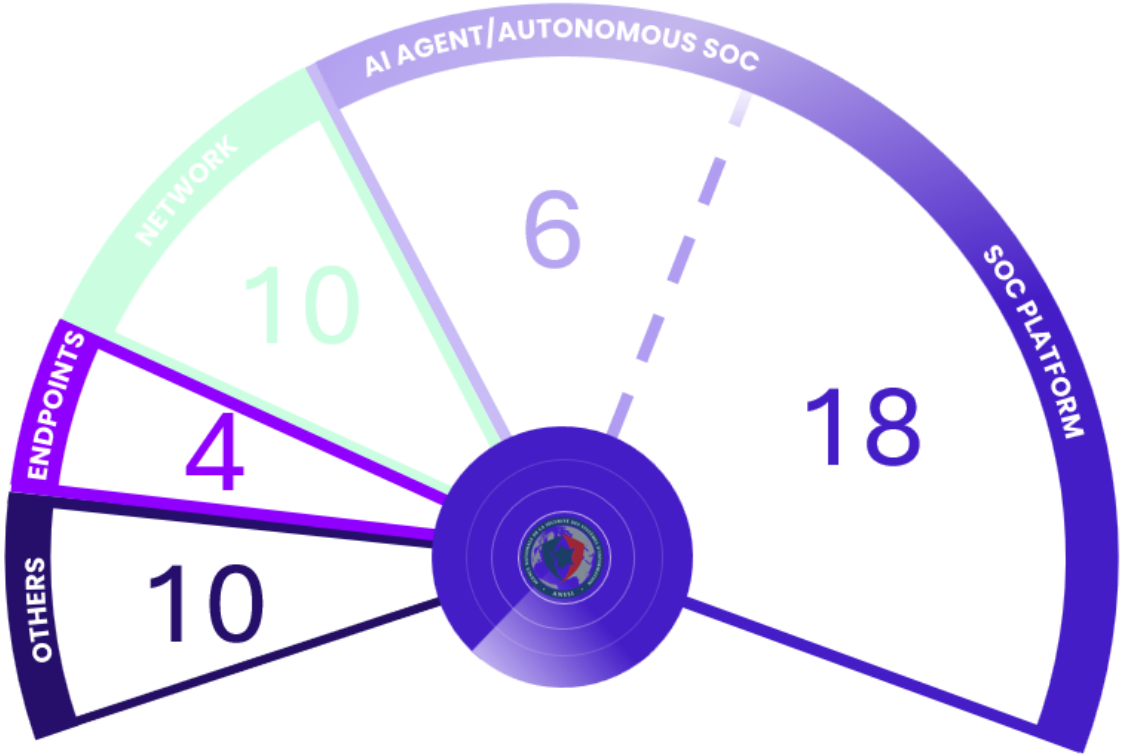
- **1987** — DARPA is calling for research on machine learning methods in the field of security.
- **2004** — Launch of the first detection systems based on rule-based learning with dynamic rules, such as Snort.
- **2010** — Initial research efforts to apply decision trees to intrusion detection.
- **2014** — First machine learning algorithms for log analysis.
- **2017** — Emergence of the first ML-based UEBA solutions.
- **2022** — Beginning of the GenAI revolution.

However by the end of the 2010s, **time-consuming** and **complex tasks** in the detection chain still remained the responsibility of analysts.

- **Strenuous work of developing parsers** to enable the integration of logs from an increasing variety of sources.
- **Alert enrichment**, identifying relevant elements within a massive volume of information.
- **Alert triage**, which becomes impossible when alert volumes surge.
- **Incident investigation**, a highly complex task requiring expertise and thorough knowledge of the environment.

2. VENDORS' OVERVIEW

A wide variety of solutions explored



Number of vendors interviewed by category

Key takeaways

The overview of the solutions analyzed is structured around **five main product categories**:

1. **SOC Platform**
2. **AI agent / Autonomous SOC**
3. **Network-focused solutions**
4. **Endpoints-focused solutions**
5. ... others

In fact, more than **18 different types** of solutions were reviewed:

- Malware analysis platform
- Risk management platform
- Code auditing platform
- Vulnerability management platform
- Cyber fraud prevention platform
- *ASPM (Application security posture management*
- *EDR*
- *NDR*
- *IDS*
- *Firewall*
- *Proxys*
- *Email security Gateway*
- *SIEM*
- *SOAR*
- *XDR*
- *AI Agent*
- *EASM*
- *WAAF*
- *Etc.*

A consolidation of the cybersecurity market

A surge in acquisitions

The cybersecurity market is experiencing strong consolidation, with numerous acquisitions aimed at strengthening detection, response, and AI integration capabilities. *(Below is a NON-EXHAUSTIVE list)*

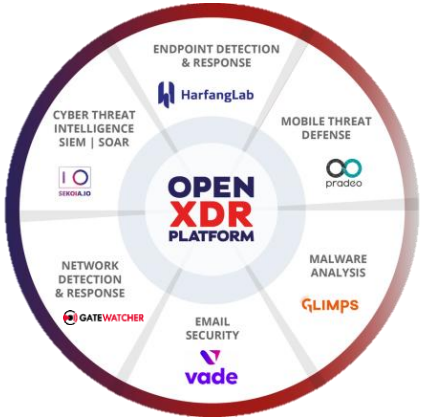
Acquirer	Target	Acquisition Date
Palo Alto Networks	Talon Cyber Security	December 2023
SentinelOne	PingSafe	February 2024
CrowdStrike	Bionic	February 2024
Cisco	Splunk	March 2024
HornetSecurity	Vade	March 2024
Mimecast	Aware	August 2024
Palo Alto Networks	IBM Qradar (SaaS)	September 2024
Logpoint	Muninn	October 2024
Proofpoint	HornetSecurity	May 2025

There is a trend toward creating security platforms that cover the entire detection and response cycle.

A few "platformization" initiatives in Europe

Two approaches:

Strategic alliances to ensure full coverage of needs.



Acquisitions of solutions **among European** vendors.

LOGPOINT → Muninn

HORNET SECURITY → vade

3. SPOTLIGHT ON THE EUROPEAN LANDSCAPE

Spotlight on the European landscape

22 countries

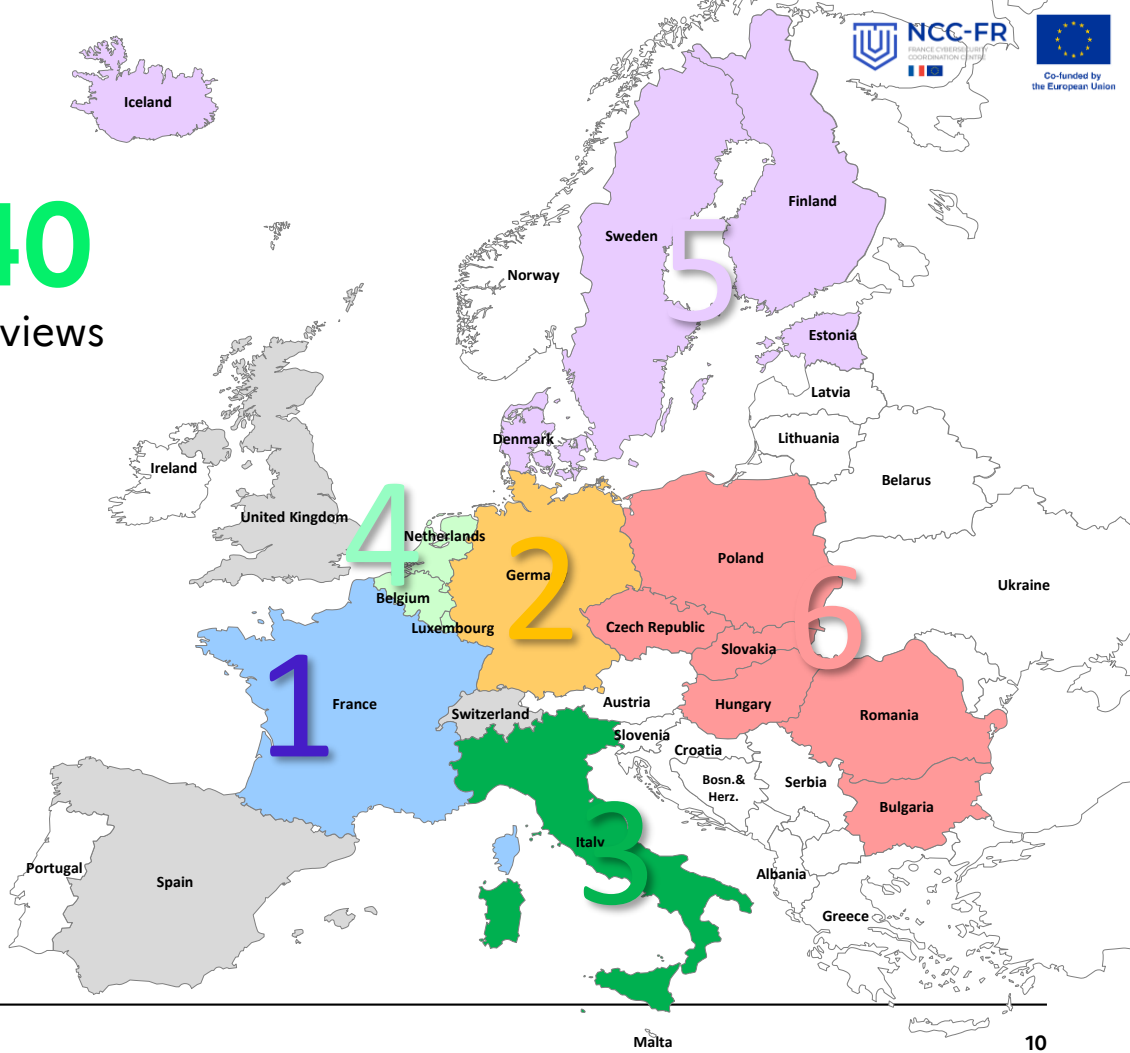
30-40 vendor interviews

+450 Software vendors analyzed

6 Geographic areas prioritized

1. France
2. Germany
3. Italy
4. Benelux
5. Northern Europe
6. Eastern Europe
7. Others

*United Kingdom, Switzerland, and Spain: Non-priority areas



Spotlight on the European landscape

72

Vendors meeting the study criteria

1. Offer cybersecurity solutions for **incident detection and/or response**.

2. Incorporate features based on **artificial intelligence***

*Artificial intelligence–based features: A set of functionalities relying on machine learning/deep learning that implement algorithms capable of learning from training data and reasoning or making predictions on new situations not encountered during the training phase.

Spotlight on the European landscape

34

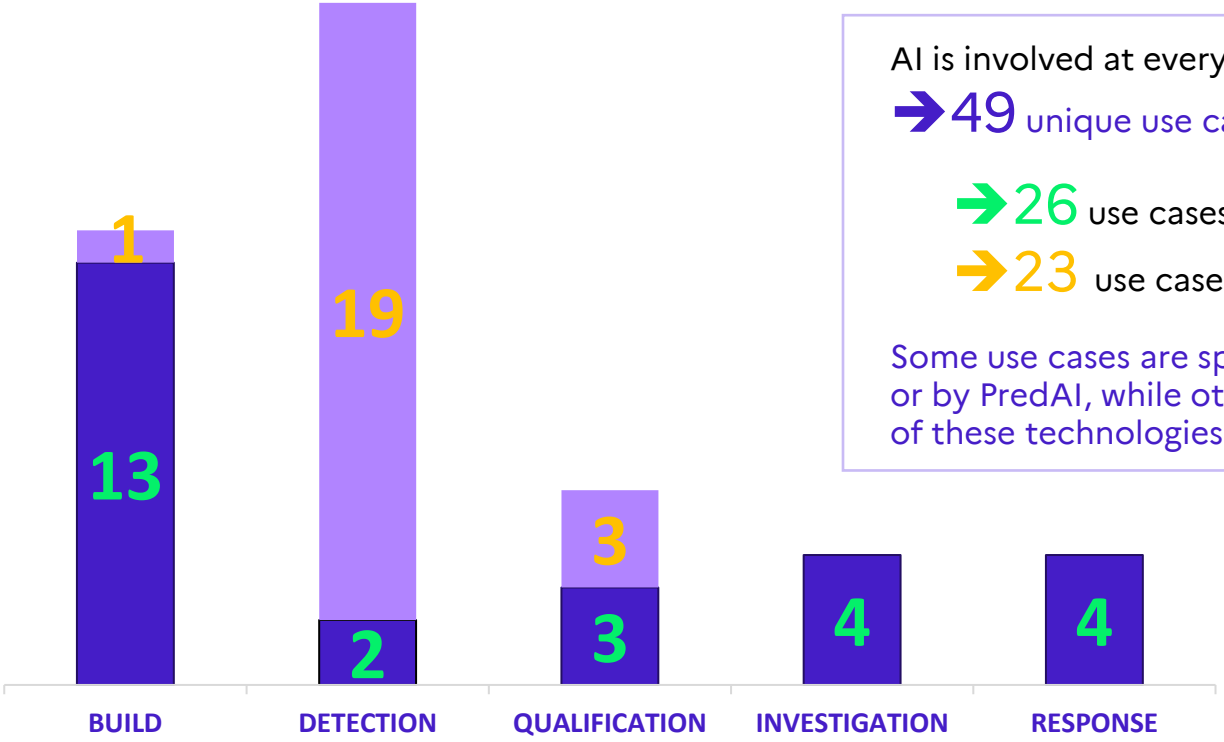
European vendors met during the interview phase

- *16 French vendors*
- *4 German vendors*
- *2 Italian vendors*
- *2 British vendors*
- *2 vendors from Benelux*
- *4 vendors from Northern Europe*
- *3 vendors from Eastern Europe*
- *1 Swiss vendors*

4. OVERVIEW OF AI USE CASES IN THE DETECTION CHAIN

Distribution of use cases across the detection chain

based solely on the use cases discussed during the interviews



AI is involved at every level of the detection chain

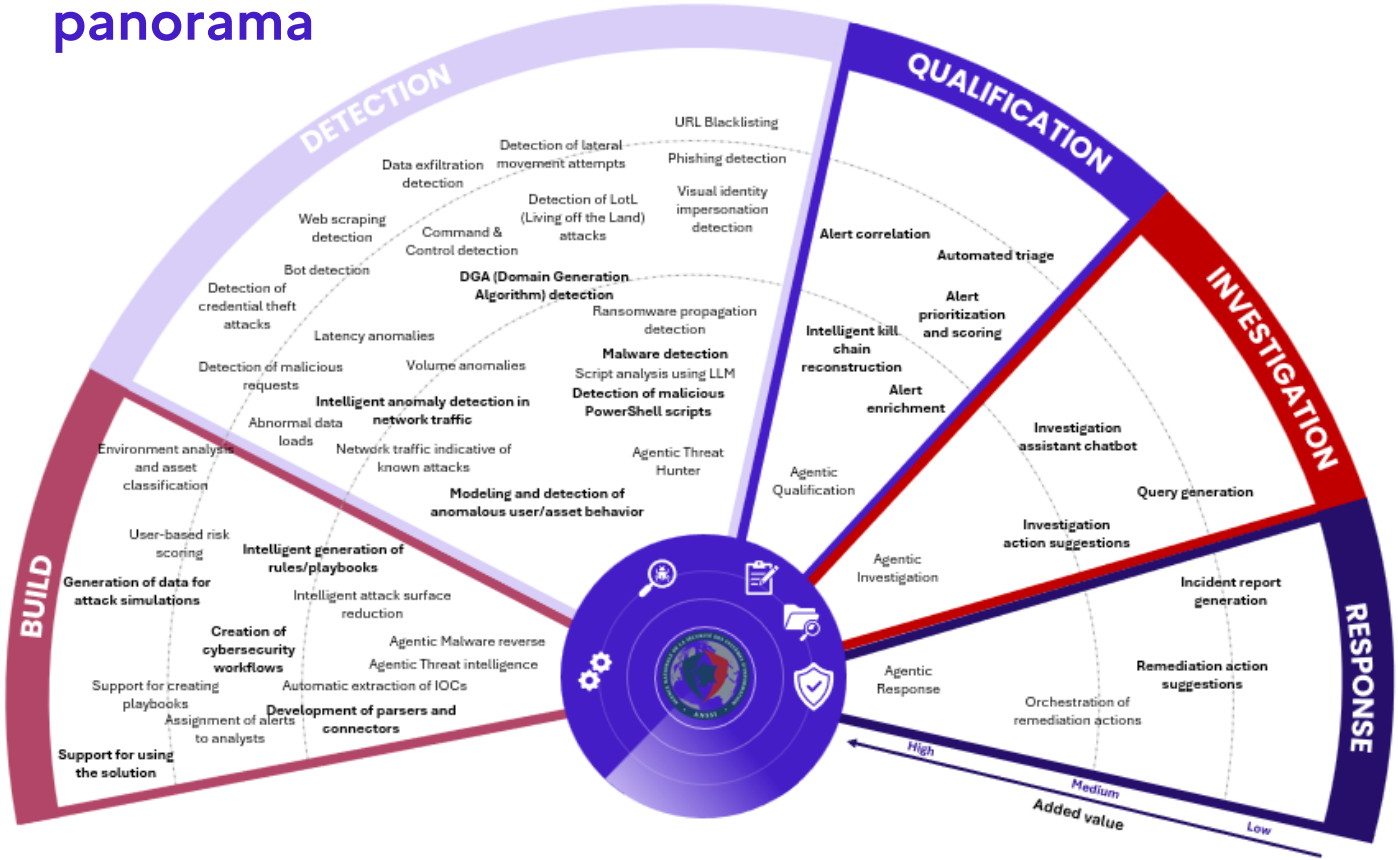
→ 49 unique use cases have been identified

→ 26 use cases are mainly based on GenAI

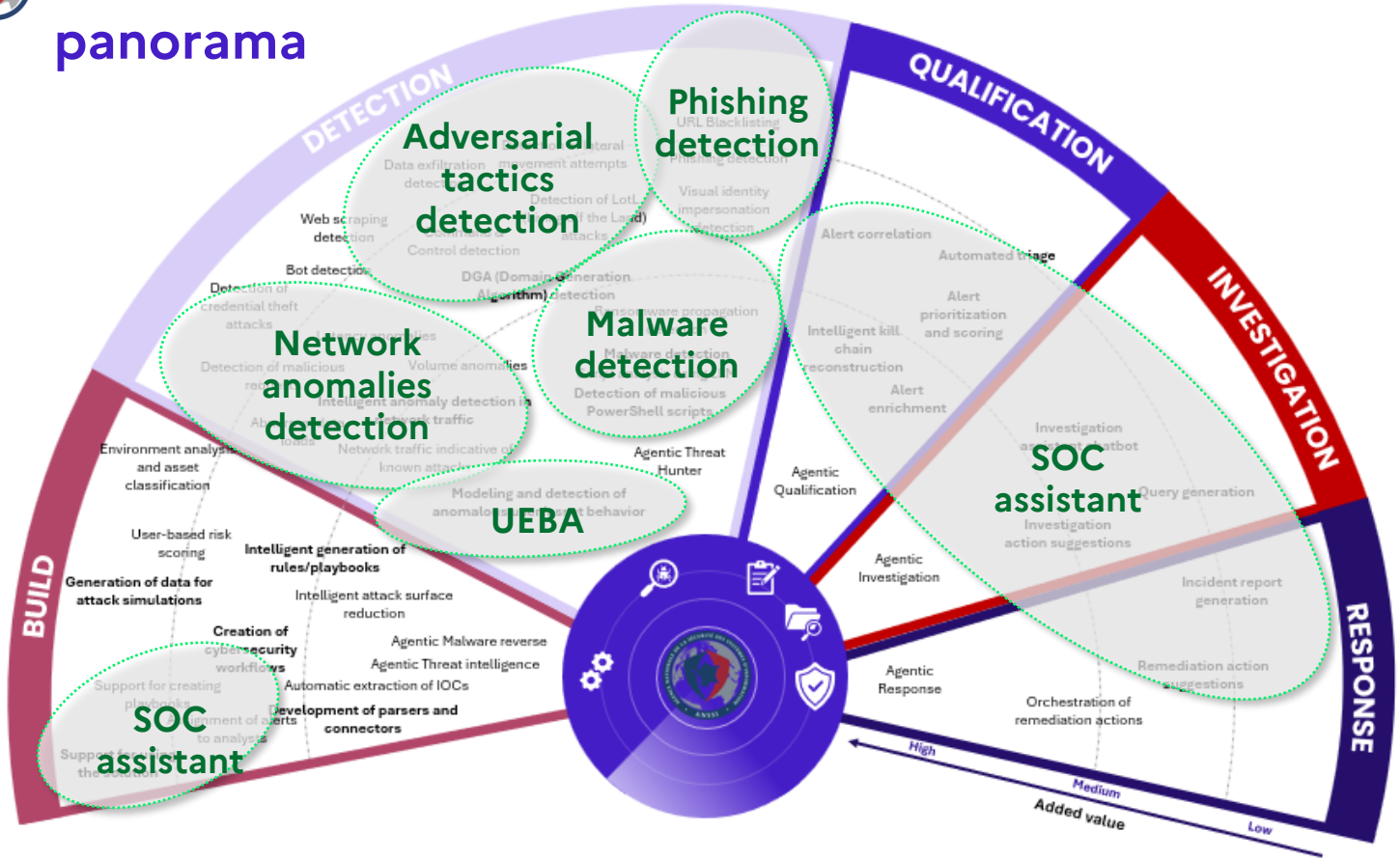
→ 23 use cases are mainly based on PredAI

Some use cases are specifically addressed by GenAI or by PredAI, while others can be addresses by both of these technologies.

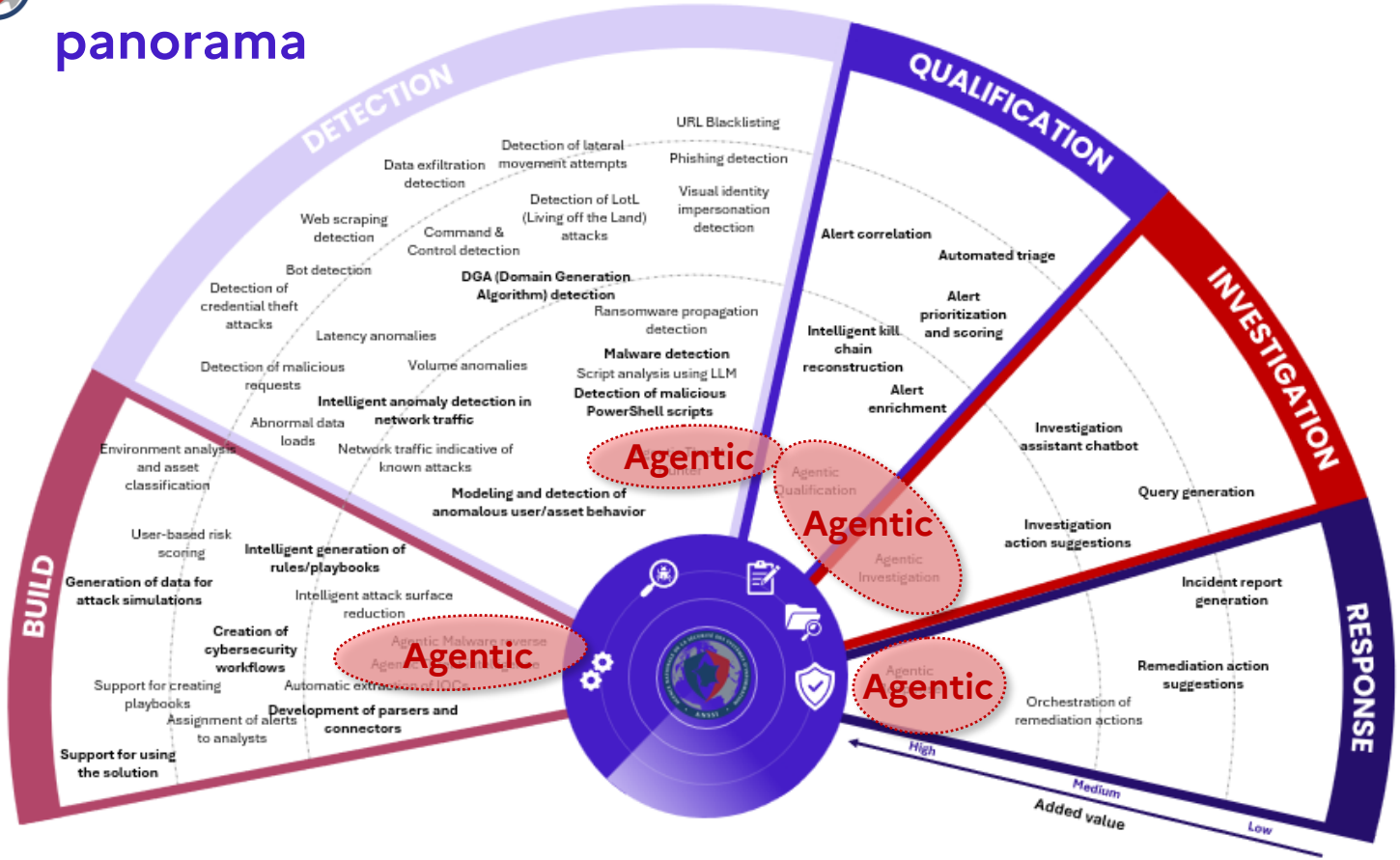
AI use cases panorama



AI use cases panorama



AI use cases panorama



RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

Co-funded by the European Union

Consistent observations across the European scope

Emergence of GenAI through chatbots, with functionality still limited and varying across countries

A variety of PredAI use cases, with some European vendors implementing it for over 15 years, demonstrating **advanced expertise**

Early initiatives around agentic AI, mainly expected to ease qualification and investigation tasks

Results should be interpreted **with caution**, given the non-exhaustive sample of vendors consulted

5. PREDAI, DETECTION-FOCUSED USE CASES

Top 5 PredAI use cases

1. **User & Entity Behavior Analytics**
   Analysis of user and asset behavior to detect anomalies or suspicious activities.

2. **Network anomaly detection**
   Network traffic analysis for anomaly detection (volume, latency, protocols, scans, etc.).

3. **Incident prioritization**
   Assignment of severity and priority scores to an alert.

4. **Malware detection**
   File analysis for malware detection.

5. **Phishing detection**
   Email and link analysis for phishing attempts detection.

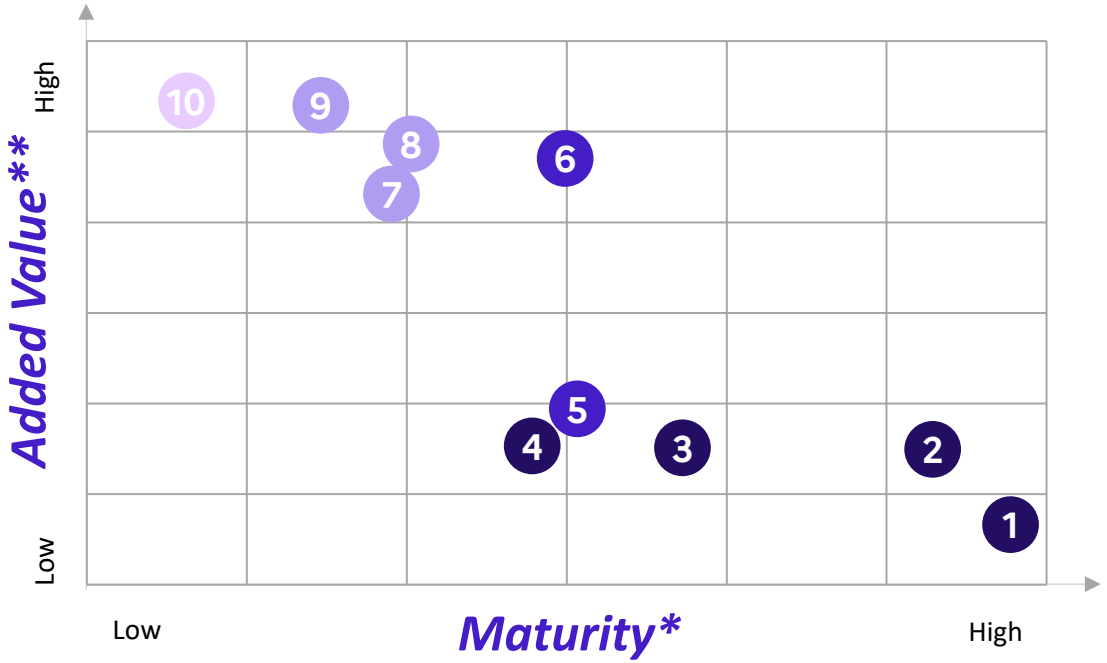
And they keep making progress

6. GENAI, MAINLY USED TO GUIDE ANALYSTS AND ACCELERATE TASKS

GenAI used through more or less intelligent “assistants"

GenAI use case matrix

*"based on vendors involved in the development of a SOC assistant"



Assist

1. Assistance in using the solution
2. Query generation assistance
3. Assistance in building playbooks and detection rules
4. Assistance in identifying investigative and response actions

Enrich

5. Generating incident reports
6. Alert enrichment

Analyze

7. Autonomous generation of playbooks and rules
8. Qualification / Autonomous Alert Triage
9. Autonomous Investigation

Act

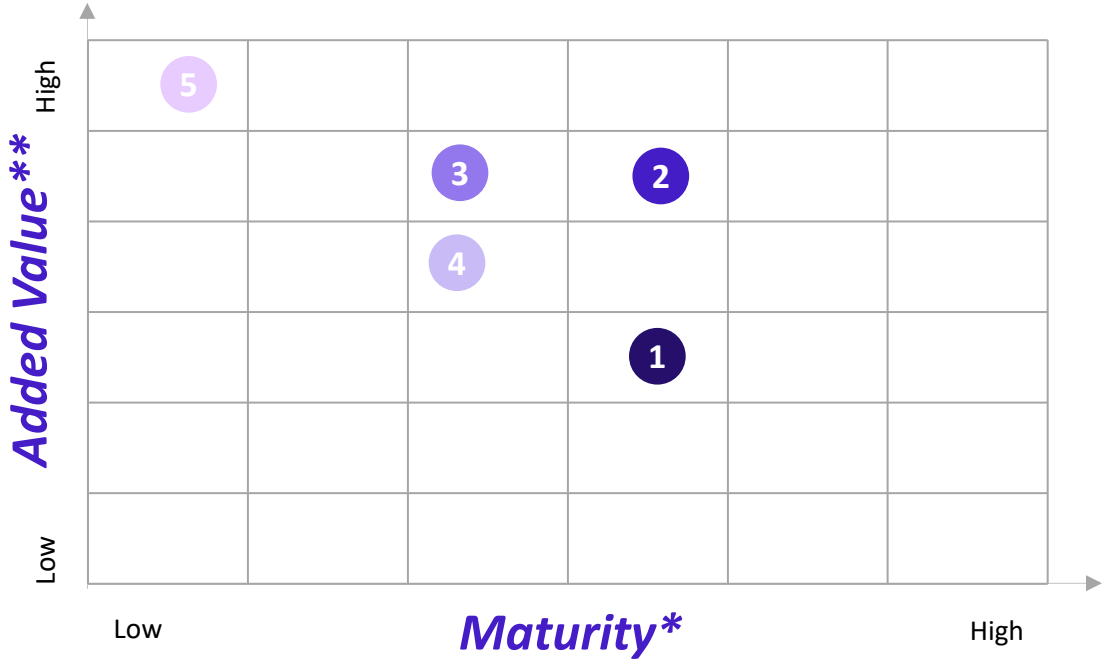
10. Autonomous response

Added value: Theoretical estimation of the benefit provided by the feature as perceived by the user (e.g., time savings).
***Maturity** : Estimation based on factors: average implementation date, number of vendors offering the use case, its complexity, and feedback from the field.

GenAI also increases vendors' agility

Use case matrix for vendors

*"based on vendors involved in the development of a SOC assistant"



1 Synthetic data generation

- *Generation of data to illustrate attacks and enable testing of detection models (network data traffic, phishing campaigns, etc.).*

2 IOC extraction

- Extracts IOC and its context directly from reports.

3 Parser development

- *By providing an example dataset, the AI is able to develop the associated parser.*
- Used for both market solutions and custom client applications.

4 Connector development

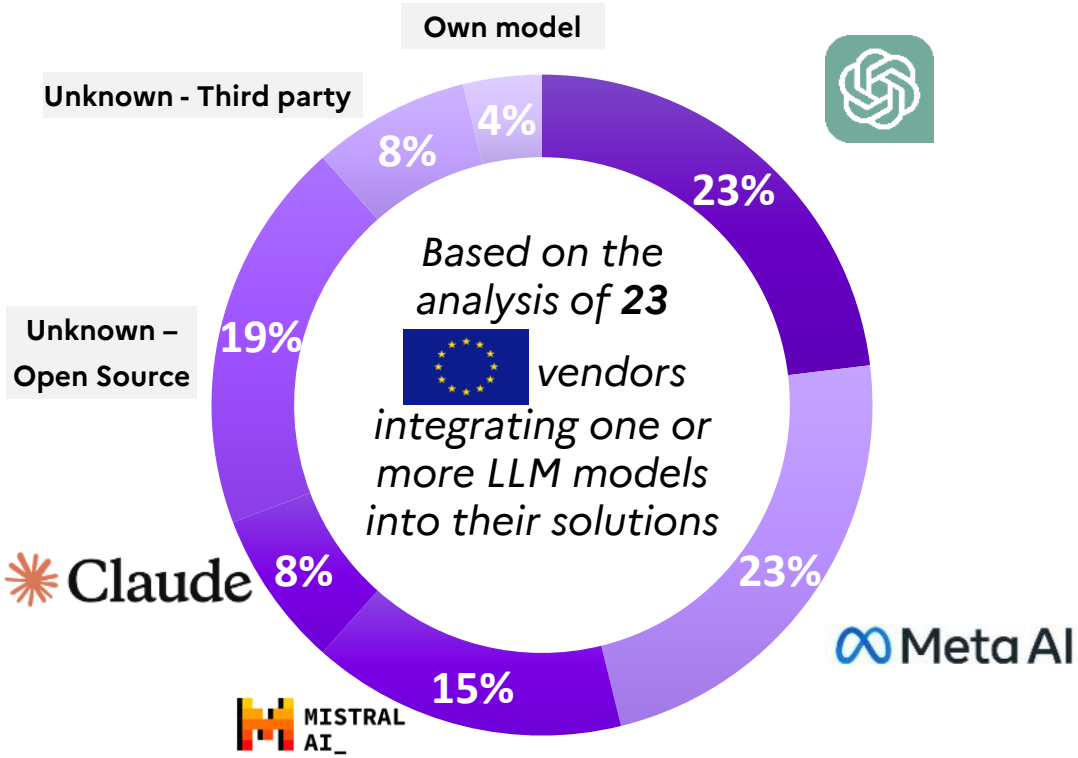
- Generation of API connectors from OpenAPI specifications or technical documentation.

5 SIEM migration

- Transposition of detection rules from one technology to another.

Added value: **Theoretical estimation of the benefit provided by the feature as perceived by the user (e.g., time savings).
*Maturity : Estimation based on factors: average implementation date, number of vendors offering the use case, its complexity, and feedback from the field.

Four LLM providers stand out among the the solution providers interviewed

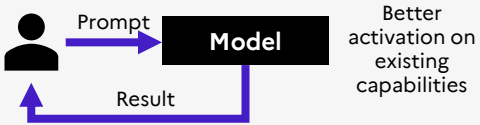


EU vendors usually favor open source AI models such as Llama and Mistral AI.

Vendors using proprietary solutions are considering migrating to open source alternatives.

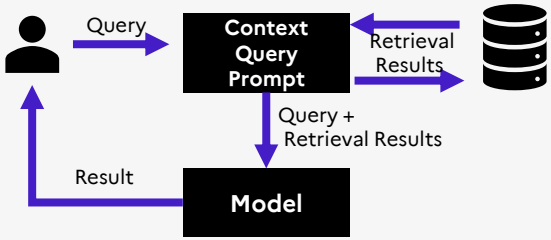
3 approaches used by vendors to optimize the performance of foundation models

Prompt Engineering



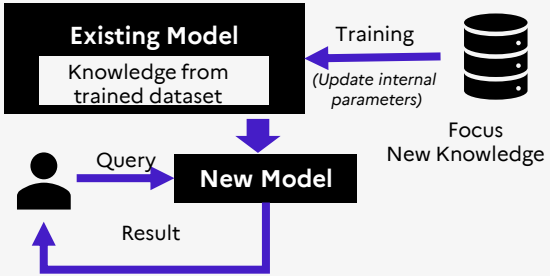
+ Quick to implement
+ No additional infrastructure
- Variable performance (depends on the quality of the prompt)
- Limited knowledge to the model's training data

RAG
Retrieval-Augmented Generation



+ Use of specific and up-to-date data (relevant to the product or customer)
+ Easy to update data sources
+ Reduction of hallucinations
- Reduced performance *(latency)*
- Additional infrastructure *(cost/complexity/security)*
- Quality depends on source documents

Fine-Tuning



+ Fast response on specific cases
+ Domain/industry specialization *(Cyber)*
+ Improved relevance and accuracy
- Training phase is complex and costly *(Data volume and quality)*
- Keeping data up to data *(retraining required)*
- Loss of general skills

Most vendors favor a pragmatic approach based on RAG, leveraging data specific to their products, cybersecurity elements, and customer data to customize responses. This strategy is reinforced by prompt engineering, which optimizes the capabilities of existing models. Conversely, fine-tuning, which is more complex and costly, remains limited to a few players, illustrating a clear differentiation in technology choices.

Hosting of LLM models, a sensitive topic for data

Proprietary LLM

38%

Hosted by the model provider

The model is managed and hosted by the model provider, and the connection is made via an API link (e.g., OpenAI GPT-4, Google Gemini, Mistral AI, Anthropie).
Data control: LOW
Observation: *Model favored by vendors notably using OpenAI's model.*

Proprietary LLM
Open source LLM

15%

Hosted by a cloud provider

The model is managed and hosted by the cloud provider, and the connection is made via API (AWS Bedrock, Azure AI).
Data control: MEDIUM
Observation: *Model favored by vendors seeking access to multiple models, including those historically available only within the provider's environments.*

32%

Open source LLM

Hosted by the security solution vendor

The model is managed and hosted by the solution vendor, who is responsible for both the infrastructure and the model.
Data control: HIGH
Observation: *Preferred by vendors aiming for strong data confidentiality.*

15%

Open source LLM

Hosted in the client environment

The model is managed by the vendor and hosted in the client environment.

Data control: HIGH
Observation: *Preferred by vendors aiming to keep data in the client environment.*

The origin of the foundation model will play an increasingly decisive role for detection vendors

Model selection criteria

Performance

- Execution speed
- Quality of responses provided

Model Accessibility

- Proprietary
- Open source
- Semi-open

Computational Cost

- Necessary IT resources

Model Provenance

In a context where these models will play a **strategic role in decision-making** and the automation of critical processes, **their origin and the entire design chain must be carefully evaluated.**

Trust and Data Security: Critical Issues for GenAI Adoption

	Risks	Vendors approaches
Trust	Hallucination Variability of responses Corruption of models	Improve prompt quality Ensure monitoring of results
Data	Data leakage	Models hosting strategy Control of information sent to models

7. AGENTIC AI

Towards autonomous cybersecurity with agentic AI?

New solutions, called "SOC AI Agents," have emerged in recent years. These "intelligent" agents aim to automate the qualification and investigation of security alerts by replicating the reasoning of a SOC analyst. Some go even further by automating the response phase, while maintaining human control mechanisms.

Keys takeaway

1. An approach systematically combining ML/DL and LLMs, but differing in the orchestrator technology: **deterministic** via ML/DL, or **non-deterministic** via LLMs.
2. LLMs go far beyond simple synthesis
3. Breaking down alert processing into specialized tasks.
   - *Ex : classification, query generation, result analysis*
4. Manage full detection and response cycle, from qualification to remediation
5. A major challenge: **explainability and reproducibility**.

Agentic AI isn't limited to these new solutions — it's also being directly embedded into SOC platforms themselves.

7. AND TOMORROW…

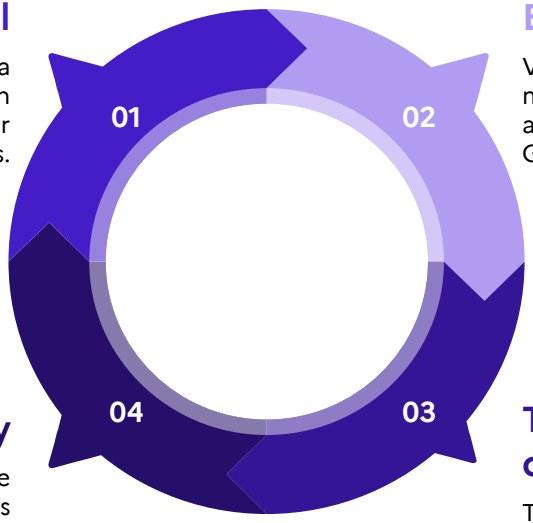
PredAI is a mature technology. Future innovations will come from GenAI and Agentic AI

Choice of model

The choice of model made by a provider will have an impact on its use in certain customer environments.

Building trust

Vendors will need to implement mechanisms to ensure the quality and veracity of actions produced by GenAI.



Growing autonomy

AI will eventually enable increasingly autonomous functionalities.

Towards systematic use of cloud resources

Today, LLM models require significant computational capacity to operate.

Agentic AI, particularly used during the alert qualification phase, is quickly evolving. Some vendors are already integrating it into their solutions. Tomorrow, this could be followed by autonomous remediation.

The integration of AI, particularly Agentic AI, requires mechanisms to assess the trust level and ensure its sustainability over time.

With our thanks

Thank you to all the vendors who took part in the AI4SOC study. Your contribution was essential in enriching the analysis and advancing the use of AI within SOC operations.

Simbian
Sesame it
mindflow
DARKTRACE
exabeam
VECTRA
GATEWATCHER
RadiantSecurity
pradeo
splunk> a CISCO company
<TEHTRIS> FACE THE UNPREDICTABLE
elastic
OGO
paloalto NETWORKS
Resistine
Google Cloud Security
CUSTOCY
Microsoft
Secaiure AI 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
N5S
DataDome
varist
PARCOOR
zscaler
CYBERSEQ
mimecast

ANSSI WAS SUPPORTED BY WAVESTONE IN CARRYING OUT THIS MARKET STUDY AND THANKS ALL THE CONSULTANTS INVOLVED.

FOR ANY QUESTIONS REGARDING THIS STUDY, PLEASE CONTACT THE INDUSTRY AND TECHNOLOGIES DIVISION AT THE FOLLOWING ADDRESS:
INDUSTRIES@SSI.GOUV.FR