exaegis.

Blueprint®

Managed SOC for large organizations

2025-2026 Edition

Custom report prepared for:

Advens

Security for the greater good

Summary

The Exaegis Blueprint®

The Blueprint® produced by Exaegis is the reference guide for choosing IT solutions for French leaders, whether they belong to large companies, state organizations, mid-sized companies, SMEs, healthcare establishments or local authorities.

It offers IT buyers a relevant and objective framework for comparisons between digital solution providers.

The Blueprint® is based on a dual expertise, combining know-how: audits and rating of IT providers on the one hand, and analysis of IT markets on the other.

Managed SOC

2025-2026 Edition

This Blueprint®, produced by Exaegis, focuses on managed SOC services provided by managed cybersecurity service providers, enabling public and private organizations to strengthen their security, detect threats, and respond to incidents. It covers the full range of monitoring, investigation, and remediation capabilities, as well as the increasing integration of advanced services such as CTI, VOC, remediation, automation, and artificial intelligence. White-label SOC offerings and providers without teams in France are not included.

The results presented are based on a study conducted during the second half of 2025 with 21 service providers operating in France. The evaluation criteria were defined based on the experience of Exaegis analysts.

Foreword

The managed SOC services market is experiencing sustained growth in France in 2025-2026, despite a tightening market, mirroring the overall trend in the cybersecurity sector. This momentum is driven by technological transformations, the intensification of cyber threats, and the evolving needs of organizations, from large corporations to mid-market players (SMEs, mid-sized companies, and public sector organizations). After an initial phase focused on SIEM platforms and standardized approaches, the sector is reaching a level of maturity where automation, specialization, and orchestration are becoming essential for cybersecurity service providers. Clients are now seeking agile, integrated services tailored to their IT and OT environments, whether multi-site or hybrid cloud.

Managed SOC go beyond simple log monitoring or incident detection. It relies on a combination of complementary components: SIEM for centralizing and correlating events, SOAR for automating response workflows, CTI for enriching analysis, EDR/XDR for enhanced endpoint visibility, VOC scanners for measuring exposure, and threat platforms. hunting to anticipate attacks. These technical building blocks, combined with CERT/CSIRT capabilities, serve the performance of the SOC, by optimizing the detection, remediation of incidents and the operational resilience of organizations.

For large organizations, the hybrid model is essential. It combines industrialized functions (Level 1/Level 2), advanced expertise (Level 3, CTI, forensics), and capabilities adapted to critical environments. MITRE ATT&CK, including its OT matrices, serves as a benchmark for assessing threat coverage and aligning services with international best practices.

The mid-market is growing rapidly. SMEs and mid-sized companies favor turnkey, industrialized, and quickly deployable services, while retaining the option to add more specialized components (XDR, VOC, lightweight CTI, OT monitoring). Pressure from certain players is driving prices down, prompting some providers to revise their pricing while striving to maintain the quality and performance of the services delivered.

Artificial intelligence is becoming a structuring lever. Already integrated into SIEM, behavioral detection or CTI enrichment, it crosses all levels of the SOC to correlate events, reduce false positives, prioritize alerts, accelerate qualification or assist analysts, redefining the value of N1/N2 and N3 roles.

Managed SOC services are moving towards cyber resilience, integrating vulnerability management (VOC), threat hunting, post-incident analysis, and, less frequently, business continuity (DRP, hardening, IT/OT segmentation). This holistic approach anticipates, contains, and rebuilds in the face of growing threats.

Consequently, this 2025-2026 edition of the Blueprint® expands its scope to include all services offered: MDR, CTI, VOC, threat hunting, cyber resilience and automation.

Competition remains intense. Small and medium-sized players are innovating in technological or sectoral niches, while large players are strengthening their catalogs and teams, developing integrated offerings covering IT and OT, and deploying hybrid services combining industrialization, specialized expertise and strategic support to meet the needs of large organizations.

In summary, the managed SOC market in France is rapidly evolving around three dynamics: deep service integration, industrialization and AI, and flexibility for large organizations as well as the mid-market.

This Blueprint® identifies the providers best suited to respond to these transformations, by combining performance, innovation and agility.

Timothée Veiras

Lead Analyst – Cybersecurity

Exaegis Research

Definition of the segment

Managed SOC				
SOC (Security Operations Center)	**CERT / CSIRT** (Computer Emergency Response Team)	**VOC** (Vulnerability & Orchestration & Correction)	**CTI** (Cyber Threat Intelligence)	**Remediation and reaction**
• Monitoring of security events (logs, endpoints, networks) • Incident detection and real-time alerting • Daily operational management	• Coordination and response to critical incidents • Advanced investigation and analysis of attacks • Support for business continuity and cyber resilience plans	• Vulnerability management • Prioritizing and tracking corrections • Integration with IT/DevOps processes	• Analysis and contextualization of threats • Sharing and using intelligence on attacks • Anticipating the opponent's tactics and techniques	• Corrective actions and incident containment • Orchestration and automation of responses (SOAR / AI) • Post-incident follow-up and continuous improvement

Reporting and monitoring of security indicators

Compliance and audit support

Raising awareness and training internal teams

Integration of advanced automation tools and processes

User profiles

- Business users: CEO, CFO, etc.
- IT users: CIO, CISO, etc.
- Sectors: manufacturing, banking/insurance, public sector, health, utilities, telecoms, distribution/retail, transport/logistics, etc.

Organization profiles

- Large organizations: 10,000 positions or more.
- Mid-market: 250 to 10,000 positions.

exaegis.

Positioning Matrix

Blueprint® Managed SOC for large organizations

2025-2026 Edition

www.exaegis.com

Evaluation criteria

Evaluation criteria	Indicators and information taken into account
Scope of the offer	
	Functional coverage, scope of services
	Sector-specific characteristics
Quality of services	
	Support, skills, functional and technical expertise
	Technologies, architecture and infrastructure
	Security, continuity, stability
	Integration and interoperability
	Product satisfaction and user experience
Offering strategy and innovation	
	Offering roadmap and evolution
	Product culture and R&D
Local adaptation	
	Regulatory compliance, infrastructure location and data
	CSR Commitments

Evaluation criteria	Indicators and information taken into account
Business performance	
	Revenue in the segment
	Growth
	Customer references, number of users
Corporate image	
	Awareness
	Recommendation level
	Overall customer satisfaction
	Thought leadership
	Employer image
Go-to-market and ecosystem	
	Technology Partnerships
	Business Partnerships
	Marketing Development

Market Relevance

Market Impact

Provider classification

Leaders

Leaders are providers who benefit from both a strong market impact *and* an offering that closely matches user needs.
They offer comprehensive and high-performing solutions (*market relevance*), and have a significant number of customer references.
Their solutions and services are recommended for users looking for comprehensive, high-performance solutions with a strong market presence.

Performers

Performers are providers with a strong local market presence and a large customer base. They also have marketing resources, significant partnerships, and a positive brand image (*market impact)*.
They offer products with a strong reputation and installed base within a specific scope (*market relevance*).
Their offerings are recommended for users seeking proven and widely used targeted solutions and services.

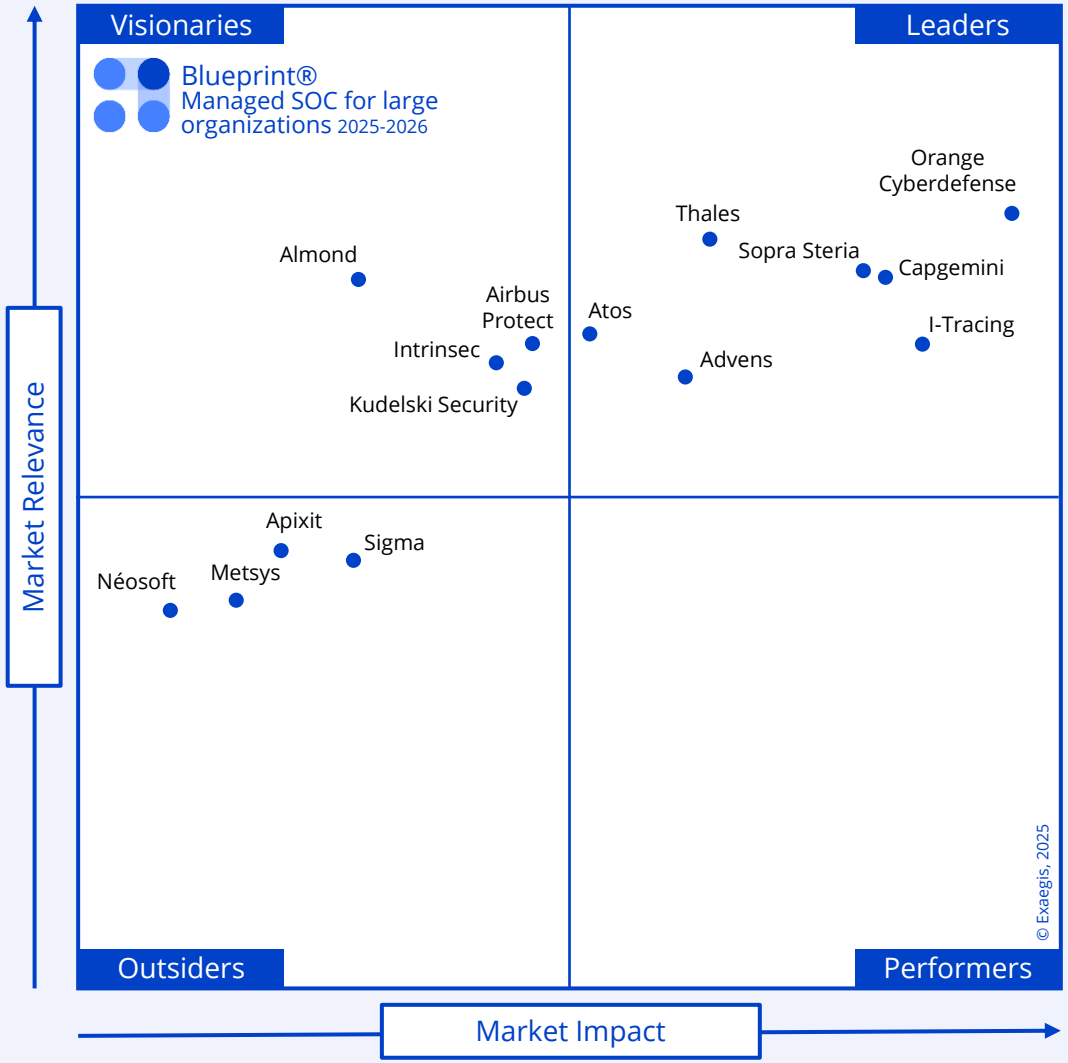
Visionaries

Visionaries are the providers who offer solutions and services particularly suited to users' needs in terms of scope and quality of offering, innovation and adaptation to the local market (*market relevance*).
Their market shares remain limited but may increase in the medium term (*market impact)*.
Their solutions are ideal for users looking for high-performance and innovative solutions.

Outsiders

Outsiders are providers who currently have a limited market presence (*market impact)* and are positioned on a restricted or shallow solution scope (*market relevance*).
Their service offerings are tailored for users wishing to address needs that are limited in scope or complexity, or highly specialized.

Positioning Matrix



Exaegis opinion

To meet the needs of large organizations (10,000 workstations or more), several profiles of managed SOC providers stand out on the French market:

- Cybersecurity-dedicated subsidiaries or divisions of large groups: Airbus Protect (Airbus), Atos, Capgemini, Intrinsec (Neurones), Kudelski Security (Kudelski), Orange Cyberdefense (Orange), Sopra Steria, Thales.
- Independent cybersecurity specialists: Advens, Almond, I-Tracing.
- IT services companies and infrastructure specialists with a Cyber practice: Apixit (Bechtle), Metsys, Néosoft, Sigma.

Large organizations rely on a mix of pure players, subsidiaries of large groups and IT services companies.

These providers are integrating artificial intelligence and automation into their SOCs to accelerate detection, prioritize incidents and improve responsiveness, while deploying on-site teams, supporting the structuring of internal teams and providing advanced N3 expertise.

exaegis.

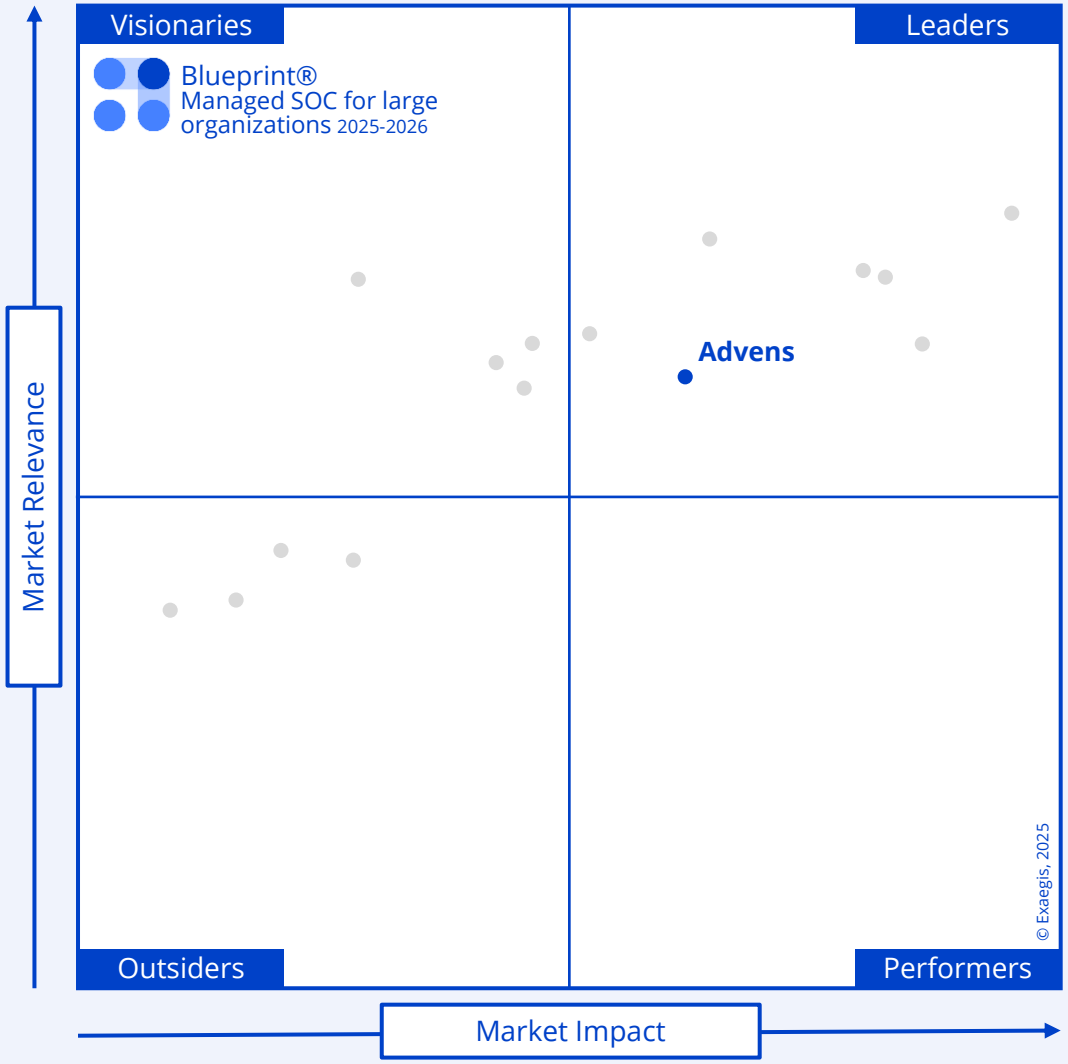
Focus on Advens

Blueprint® Managed SOC for large organizations

2025-2026 Edition

www.exaegis.com

Focus on Advens



Advens named a Leader in the 2025-2026 Blueprint® for Managed SOC for large organizations

exægis.

Exaegis opinion

For large organizations, Advens delivers comprehensive functional coverage, integrating SOC, CERT, CTI, VOC/EASM, remediation and monitoring to meet the requirements of distributed, complex or multi-country environments.

The system offers excellent detection and response capabilities, relying on experienced SOC and CERT teams, advanced multi-technology correlation, and powerful in-house tools. The integration of AI/ML capabilities and a purple team approach supports the continuous improvement of detection scenarios, the automation of alerts, and the enhancement of security maturity levels.

The model is also distinguished by strong operational responsiveness: 24/7 availability, strict SLAs, fluid coordination and regular exchanges adapted to the internal teams of large groups.

Advens sustained growth, combined with an increasingly strong presence in the large accounts market, confirms its ability to effectively address multi-site and multi-sector organizations.

Its high-level certifications, PDIS, PASSI RGS, PRIS, ISO 27001, finally strengthen its credibility with critical sectors such as defense, energy or finance.

Focus on Advens

Presentation

Advens named a leader in this Blueprint® for Managed SOC for large organizations.

Specializing in Security-as-a-Service, the company has more than 600 employees and relies on a strong presence in France in particular, Spain, Italy, Germany and Canada.

Advens offers a wide range of services, including CISO Office, SOC, CERT, and expertise in offensive security strategy, integration, compliance and technology management.

Strengths

Comprehensive functional coverage: SOC, CERT, CTI, VOC, remediation and monitoring services tailored to complex and multi-country environments.

Excellent detection and response quality: experienced SOC and CERT teams, high-performance tools, advanced multi-technology correlation.

R&D and innovation: Flexible internal SOC, integrating AI and purple team to strengthen detection and customer maturity, while pooling analysis.

AI/ML investments: continuous improvement of detection and alert automation capabilities for complex IT environments.

Enhanced responsiveness and support: 24/7 SOC availability, strict SLAs, regular exchanges tailored to mature clients.

Sustained growth and consolidated position: brand awareness and commercial traction in the key accounts segment, ability to address multi-site environments.

High-level certifications: PDIS, PASSI RGS, PRIS and ISO 27001 certifications, guarantees of credibility for critical sectors (e.g., defense, energy, finance).

Target

Advens addresses SMEs, mid-sized companies and large organizations.

The company offers expertise in health, the public sector and manufacturing 4.0.

Points for attention

Limited technological flexibility: smaller portfolio of software partners, which may limit integration in very heterogeneous environments.

CERT and CTI still have some room for improvement: their depth and volume are lower than those of players with more massive structures.

Remediation in progress: less robust and mature than some major players.

Limited influence on software vendors' roadmaps: development of some SOC tools in-house, which may reduce the direct impact on technological developments.

3 questions for Advens

What challenges are you currently seeing among your clients and prospects?

Our clients face three major challenges. First, the need for effective co -management: they want to maintain control of their environments while relying on a partner capable of operating and enhancing detection and response on a daily basis. Second, the acceleration of detection and remediation time has become strategic in the face of faster and more sophisticated attacks; organizations are seeking significantly greater investigation and automation capabilities. Finally, protecting OT environments, often new or poorly understood, is a growing challenge: limited visibility, heterogeneous technologies, and operational constraints require an integrated IT/OT approach to effectively secure these critical perimeters.

How do your solutions address these needs?

Our mySOC offering addresses these needs through several key advancements. First, a unified interaction portal, unique on the market, centralizes collaboration, management, and security insights to streamline co -management with internal teams. Second, the acceleration of our SOC services around Microsoft Sentinel strengthens our ability to detect and investigate more quickly in Microsoft environments. We are also rolling out our "augmented analyst" AI model, which increases the speed of analysis and the depth of decision-making for our teams. Finally, the growing maturity of our OT SOC/VOC offerings based on more than 15 operational services enables us to secure often heterogeneous and still poorly understood industrial environments.

What next developments do you plan to propose?

We are preparing several major developments. First, we are ramping up our operations in Europe, with a strengthened network to offer greater proximity and expanded response capabilities. We will also launch a new VOC offering integrating external surface analysis and offensive capabilities to provide a more comprehensive and proactive view of organizations' exposure. Finally, we are developing a new generation of specialized AI agents, dedicated to specific areas of operation (identity, cloud, OT, investigation), to further increase the relevance, speed, and automation of operational decisions within mySOC.

Guillaume Djourabtchi
Director of Offers and Strategy

Advens

exaegis.

Methodology

Blueprint® Managed SOC

2025-2026 Edition

www.exaegis.com

Methodology

The Blueprint ® produced by Exaegis is based on a proven methodology and a rigorous process to promote a reliable and objective reading:

- Selection of a typology of solutions or services,
- Selection by Exaegis of the relevant offers and providers,
- For all providers, provision of private and secure online folders for collecting information and documentation including a provider questionnaire, a confidentiality agreement, and an online folder dedicated to the deposit of documentation (brochures, customer case studies, offer catalogues, etc.),
- Technical demonstration of solutions and opening of access to test spaces,
- Analysis of the collected information and comparison to Exaegis' internal databases, from the perspective of the analysts,
- Aggregation of results and presentation of preliminary results to the selected providers,
- Publication and distribution to users.

Analysts and authors

Timothée Veiras
Lead Analyst - Cybersecurity

Nicolas Beyer
Director of Research

Ronan Mevel
Associate Director, Head of Infrastructure and Cloud practice