



# Leaders in IT/OT Cybersecurity Services in France 2025

SITSI® | Vendor Analysis | PAC INNOVATION RADAR

## Positioning of Atos

Lead analyst: Eric Damage  
December 2025



## TABLE OF CONTENTS

|                                                            |    |
|------------------------------------------------------------|----|
| Introduction.....                                          | 3  |
| PAC RADAR "Leaders in IT/OT Security in France 2025" ..... | 4  |
| Review of Top-Seeded Provider Atos.....                    | 5  |
| Atos.....                                                  | 5  |
| Objective of the PAC RADAR.....                            | 6  |
| Definitions & Segmentation.....                            | 7  |
| PAC RADAR Evaluation Method.....                           | 9  |
| Provider selection & participation .....                   | 9  |
| Considered providers.....                                  | 10 |
| The concept.....                                           | 10 |
| Evaluation criteria.....                                   | 11 |
| PAC RADAR Report License .....                             | 12 |
| About the PAC RADAR.....                                   | 13 |
| About PAC.....                                             | 13 |

## TABLE OF FIGURES

|                                                                    |    |
|--------------------------------------------------------------------|----|
| Fig. 1: PAC RADAR "Leaders in IT/OT Security in France 2025" ..... | 4  |
| Fig. 2: PAC RADAR graph (exemplary presentation) .....             | 6  |
| Fig. 3: PAC INNOVATION RADAR graph (exemplary presentation) .....  | 6  |
| Fig. 4: PAC RADAR – evaluation method.....                         | 10 |

## DOCUMENT INFORMATION

|                      |                                                                                              |
|----------------------|----------------------------------------------------------------------------------------------|
| <b>Author:</b>       | Eric Damage ( <a href="mailto:e.damage-ext@pacanalyst.com">e.damage-ext@pacanalyst.com</a> ) |
| <b>Publication:</b>  | December 2025                                                                                |
| <b>Scope ID:</b>     | Cybersecurity I France I 2025                                                                |
| <b>Portfolio ID:</b> | SITSI I Vendor Analysis I PAC RADAR                                                          |

## INTRODUCTION

This report presents a comprehensive analysis of the cybersecurity services market in France, as assessed by PAC. It comprehensively covers the entire spectrum of services, from consulting to managed services in the cybersecurity space in France.

Our focus encompasses all companies active in the French market, regardless of their headquarters' location.

Our outreach included 42 active companies in the French market, all of which were surveyed with a detailed questionnaire. In the subsequent RADAR, we analyzed 13 specific providers.

To create the final 'data + graph' ranking tool, we followed a questionnaire approach: each player was given the opportunity to provide information via questionnaire, interviews, and public data. The 13

players of the RADAR were given the opportunity to review their position in the RADAR before publication.

Some of the providers surveyed declined to participate. All vendors displayed in the RADAR graph have agreed to be positioned in this research.

To grade and rank the players, we combined financial data (2024) with technical data and additional non-cybersecurity criteria, including contribution to sovereignty & local vendor development, capacity to innovate and produce intellectual property, employer's brand, and talent acquisition capability.

The providers have been categorized according to their expertise in IT and OT security. Some are more focused on OT security, while others are more focused on IT security, and many demonstrate a balanced expertise.

## PAC RADAR "LEADERS IN IT/OT CYBERSECURITY IN FRANCE 2025"

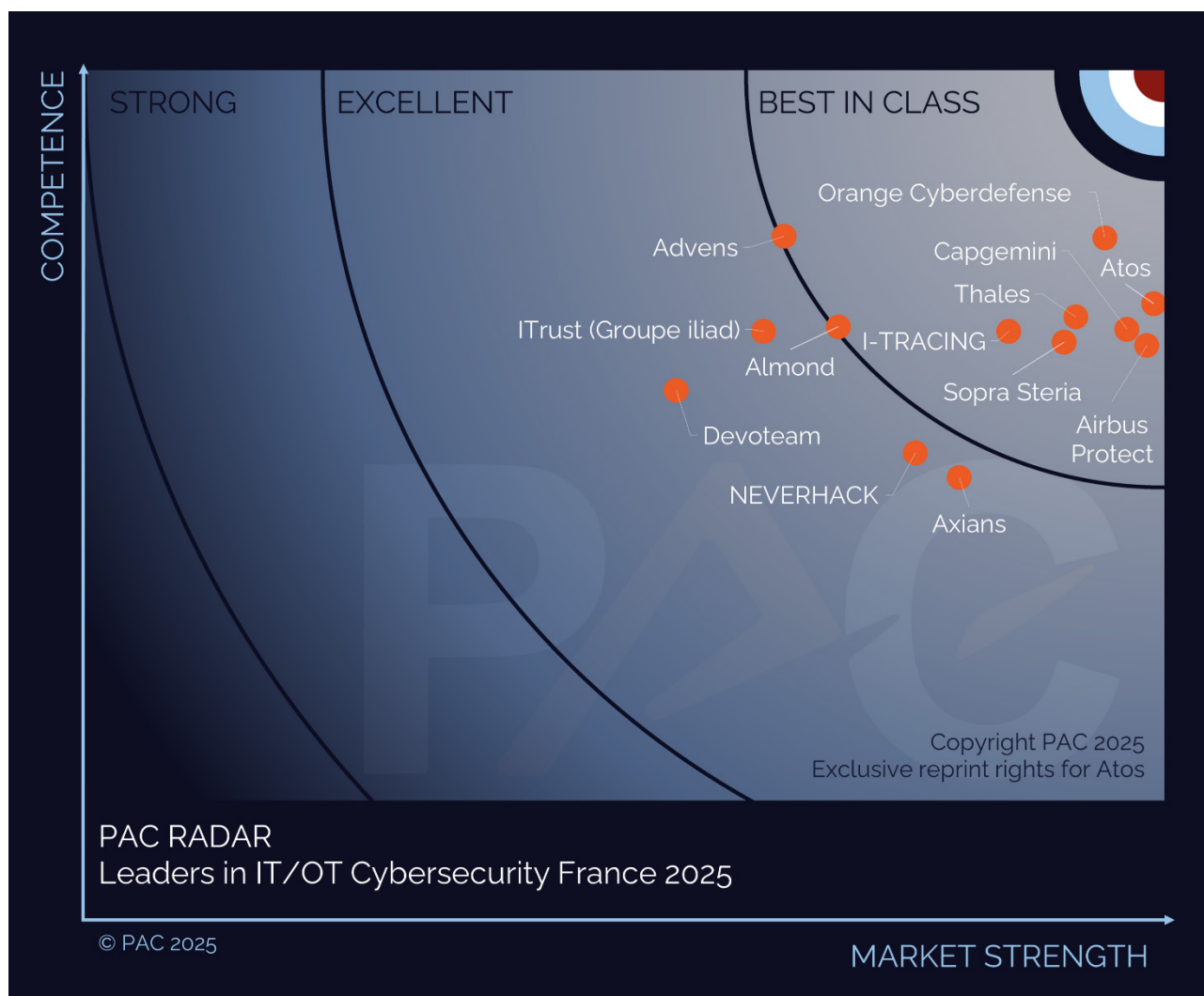


Fig. 1: PAC RADAR "Leaders in IT/OT Cybersecurity in France 2025"

Based on the scores in competence and market strength, the overall score is calculated. From the resulting overall score, each provider receives their characteristic positioning within the PAC RADAR.

Here, the following applies: The closer a company is to the top right corner, the closer they are to meeting customers' requirements.

The classification of providers is based on the overall score:

|                 |            |
|-----------------|------------|
| "Best in Class" | 1.0 – 1.99 |
| "Excellent"     | 2.0 – 2.99 |
| "Strong"        | 3.0 – 3.99 |

## REVIEW OF TOP-SEEDED PROVIDER ATOS

### Atos

| Leaders in IT/OT Cybersecurity in France 2025 |            | Positioning:<br>Best in Class |
|-----------------------------------------------|------------|-------------------------------|
| Cluster                                       | Average    | Atos                          |
| Market Strength                               | 1.67       | 1.03                          |
| Competence                                    | 1.92       | 1.81                          |
| Total Score                                   | <b>178</b> | <b>139</b>                    |

| Criteria rated significantly ABOVE AVERAGE<br>(more than 0.75)                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          | Criteria rated significantly BELOW AVERAGE<br>(more than 0.75)                                       |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"> <li>- Comprehensiveness of company's OT security services (auditing, consulting, field operations, managed services)</li> <li>- OT - international capacity</li> <li>- Experience in OT - background &amp; history in OT</li> <li>- Expert OT SOC</li> <li>- OT sec - vulnerability operations center</li> <li>- OT sec - field operations for OT</li> <li>- OT - qualifications (ISO, etc.)</li> <li>- IT sec - proprietary cybersecurity threat intelligence (CTI) feeds</li> <li>- Total number of cybersecurity professionals employed by the company</li> </ul> | <ul style="list-style-type: none"> <li>- PRIS certification</li> <li>- PDIS certification</li> </ul> |

## OBJECTIVE OF THE PAC RADAR

### What is the PAC RADAR?

The PAC RADAR is an effective tool for the holistic evaluation and visual positioning of software and ICT service providers on local markets. Numerous ICT and business decision-makers in user companies of all industries and company sizes rely on the PAC RADAR when selecting their partners and developing their sourcing strategies. With the help of predefined criteria, PAC evaluates and compares providers' strategies, development, and market position, as well as their performance and competencies within specific market segments.

Each PAC RADAR focuses on a specific IT market segment. Up to 30 leading providers are evaluated per segment. Participation in the PAC RADAR is free of charge. All providers are evaluated using PAC's proven methodology, which is based on personal face-to-face interviews and a detailed self-disclosure from each provider.

PAC reserves to also evaluate and position relevant providers in the PAC RADAR that do not participate in the self-disclosure process. After evaluating the predefined criteria, each supplier's position is plotted on the PAC RADAR. The criteria are classified by clusters and can all be attributed to the "Competence" and "Market Strength" clusters. The provider evaluation, including a market description, is published as a report.

### PAC RADAR graph

The PAC RADAR graph is a visual representation of the results of the provider evaluation, specifically regarding their market strength (horizontal axis) and competence (vertical axis) within the respective analyzed market segment.

The closer a company is to the center, the closer they are to meeting customers' requirements.

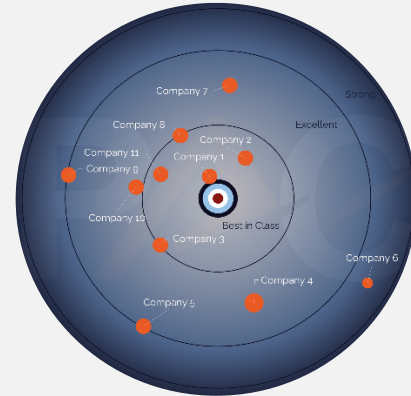


Fig. 2: PAC RADAR graph (exemplary presentation)

### What is the PAC INNOVATION RADAR?

Concept and methodology of the PAC INNOVATION RADAR are similar to those of the traditional PAC RADAR.

While the traditional PAC RADAR focuses on mature market segments, the PAC INNOVATION RADAR, on the other hand, positions providers in new and innovative market segments or in specific niche markets.

Thus, the focus of the evaluation is on the portfolio, vision, strategy, and early client engagements rather than on existing revenue numbers and resources

### PAC INNOVATION RADAR graph

The PAC INNOVATION RADAR graph is a visual presentation of the results of the provider evaluation.

The closer a company is to the top right corner, the closer they are to meeting customers' requirements.

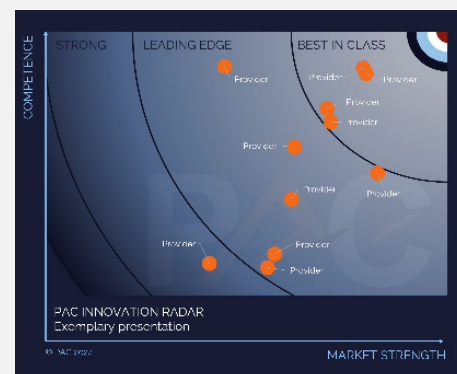


Fig. 3: PAC INNOVATION RADAR graph (exemplary presentation)

## DEFINITIONS & SEGMENTATION

### IT Cybersecurity Services (Consulting + Managed)

This value proposition offers a comprehensive suite of managed and consulting services designed to address the evolving cybersecurity landscape and the multifaceted obligations faced by modern IT environments. This portfolio is structured to provide end-to-end support, from strategic planning and risk assessment to continuous monitoring and incident remediation.

1. **Managed cybersecurity services:** 24/7 managed services designed to continuously monitor, detect, and respond to cyber threats, ensuring the ongoing security and resilience of your IT infrastructure. This includes: managed detection and response (MDR), vulnerability management as a service, managed firewall and intrusion prevention/detection systems, security information and event management (SIEM)/ security orchestration, automation and response (SOAR), endpoint security management, cloud security management, system integration .
2. **Cybersecurity consulting technical:** technical security testing and assessment with: penetration testing (ethical hacking), vulnerability assessments, security audits, incident response and recovery services: incident response planning and preparation, incident response and handling; CSIRT (cybersecurity incident response team), digital forensics and analysis, business continuity and disaster recovery planning; cybersecurity awareness and training, security awareness training programs.
3. **Cybersecurity consulting governance:** This chapter provides expert guidance to establish a strong cybersecurity foundation aligned with business objectives and regulatory requirements. This may include: **cybersecurity strategy and policy development, risk assessment and management, compliance and regulatory advisory; cybersecurity governance framework design, supply chain security consulting.**

### OT Cybersecurity Services (Consulting + Managed)

OT cybersecurity services are designed to address the unique challenges and requirements of securing industrial control systems (ICS) and operational technology (OT) environments. It is typically offered as a layered approach that encompasses assessment, protection, detection, response, and maintenance to ensure the security, availability, integrity, and confidentiality of critical OT assets. A mix of consulting and managed services covers the following:

1. **OT security assessment and risk analysis services:** in-depth assessments to understand the OT environment, identify vulnerabilities, and analyze potential risks.
2. **OT security maintenance and patch management services:** **integration and deployment** help maintain the security state of your OT environment over time by managing updates, patches, and the overall lifecycle of security controls.
3. **OT network security and segmentation services:** design and implement secure network architectures for OT environments, focusing on preventing threats from accessing sensitive OT systems.
4. **OT endpoint security and hardening services:** protect individual devices within the OT environment, minimizing their attack surface and preventing malicious code execution.
5. **OT security monitoring and threat detection services:** provide continuous monitoring of OT environment to detect anomalies, suspicious activities, and potential security incidents in near-real time.
6. **OT incident response and recovery services:** In the event of a security incident, provide a structured approach to contain the threat, eradicate it, and recover your OT systems with minimal impact on production and safety.

## PAC Cybersecurity Market Taxonomy (Consulting + Managed Services) for IT

| RAAR                               | Segments                                               | Sub-segments                                                                                      |
|------------------------------------|--------------------------------------------------------|---------------------------------------------------------------------------------------------------|
| Consulting/<br>Project<br>Services | Audit, consulting<br>planning<br>and advisory services | Risk/threat assessments                                                                           |
|                                    |                                                        | Attack simulations                                                                                |
|                                    |                                                        | Security audits / certifications and compliance assessments                                       |
|                                    |                                                        | Vulnerability testing                                                                             |
|                                    |                                                        | Penetration testing                                                                               |
|                                    |                                                        | Security strategy, planning and management advice                                                 |
|                                    |                                                        | Digital forensics: post-event (incident/intrusion) analysis, investigation and proof preservation |
|                                    | System integration<br>and implementation               | Security engineering, design and architecture development                                         |
|                                    |                                                        | Implementation and integration, interoperability testing                                          |
|                                    |                                                        | Implementation support (technical assistance/expert support services)                             |
|                                    | Security training                                      | Employee security awareness training                                                              |
|                                    |                                                        | Management security awareness training                                                            |
|                                    |                                                        | Security solution training                                                                        |
|                                    |                                                        | Personal training / certifications                                                                |
| Managed/<br>Outsourced<br>Services | Management and<br>operations services                  | Operational support (technical assistance/expert support services)                                |
|                                    |                                                        | SOC / SIEM / mitigation services                                                                  |
|                                    |                                                        | Compliance management                                                                             |
|                                    |                                                        | Managed security services, security system management and operations                              |
|                                    |                                                        | Security outsourcing                                                                              |
|                                    |                                                        | Continuity and recovery management                                                                |
|                                    |                                                        | Trusted third party, e-content and e-reputation services                                          |

## PAC Cybersecurity Market Taxonomy (Consulting + Managed Services) for OT

| MSS/SOC/<br>CyberSOC               | Asset<br>Inventory &<br>Management | Identity &<br>Access<br>Management   | Network<br>Security                    | Data Security                                     | Vulnerability<br>Management                              | Incident<br>Response              |
|------------------------------------|------------------------------------|--------------------------------------|----------------------------------------|---------------------------------------------------|----------------------------------------------------------|-----------------------------------|
| Managed<br>SIEM/SOAR               | Managed OT<br>asset<br>discovery   | Managed<br>IAM for users             | Firewall<br>management<br>services     | Managed<br>encryption<br>services                 | Managed<br>vulnerability<br>automated<br>detection       | Managed<br>detection<br>& alert   |
| Threat<br>intelligence<br>services | Managed<br>OT asset<br>lifecycle   | Managed<br>IAM machines              | Expert OT<br>network<br>tools services | Managed data<br>leakage<br>prevention<br>services | Managed non-<br>automated<br>vulnerabilities<br>scanning | Managed<br>resilience<br>services |
| Incident<br>response<br>services   |                                    | Managed<br>advanced<br>PAM expert AM | In-house<br>managed<br>technologies    |                                                   | Internal home-<br>grown VM<br>database mgmt.             |                                   |

Vulnerability management: includes home-grown vulnerability database.

Network security expert OT solutions: may include network segregation, diode (one-way firewall) management + all specific OT techs.

PAM: Privileged Access Management

VAPT: vulnerability assessment & penetration testing, consulting base

## PAC RADAR EVALUATION METHOD

### Provider selection & participation

#### What providers are positioned in the PAC RADAR?

Providers are selected and invited according to the following criteria:

Size of revenues in the segment to be analyzed in the specified region;

"Relevance": Even providers that do not belong to the top-selling providers in the segment to be analyzed are considered if PAC classifies them as relevant for potential customers, for instance due to an innovative offering, strong growth, or a focus on a specific customer group (e.g., SMBs).

There is no differentiation as to whether the providers are customers of PAC – neither in the selection of the providers to be positioned, nor in the actual evaluation.

#### What do providers have to do in order to be considered in a PAC RADAR analysis?

The decision as to which providers are considered in the PAC RADAR analysis is entirely up to PAC. Providers do not have any direct influence on this decision.

However, in the run-up to a PAC RADAR analysis, providers can make sure in an indirect way that PAC can adequately evaluate their offerings and positioning – and thus their relevance – e.g., by means of regular analyst briefings, etc.

#### Why should providers accept the invitation to participate actively?

Whether or not a provider participates in the RADAR process does not actually affect their inclusion and positioning in the PAC RADAR, nor their assessment. However, there are a whole host of benefits associated with active participation:

- Participation ensures that PAC has access to the largest possible range of specific and up-to-date data as a basis for the assessment.
- Participating providers can set out their specific competencies, strengths, and weaknesses as well as their strategies and visions.
- The review process guarantees the accuracy of the assessed factors.
- The provider gets a neutral, comprehensive, and detailed view of their strengths and weaknesses as compared to the direct competition – related to a specific service in a local market.
- A positioning in the PAC RADAR gives the provider prominence amongst a broad readership as one of the leading players in the segment under consideration

## Considered providers

### Leaders in IT/OT Cybersecurity in France 2025

|                |           |                       |        |
|----------------|-----------|-----------------------|--------|
| Advens         | Axians    | ITrust (Groupe iliad) | Thales |
| Airbus Protect | Capgemini | NEVERHACK             |        |
| Almond         | Devoteam  | Orange Cyberdefense   |        |
| Atos           | I-TRACING | Sopra Steria          |        |

## The concept

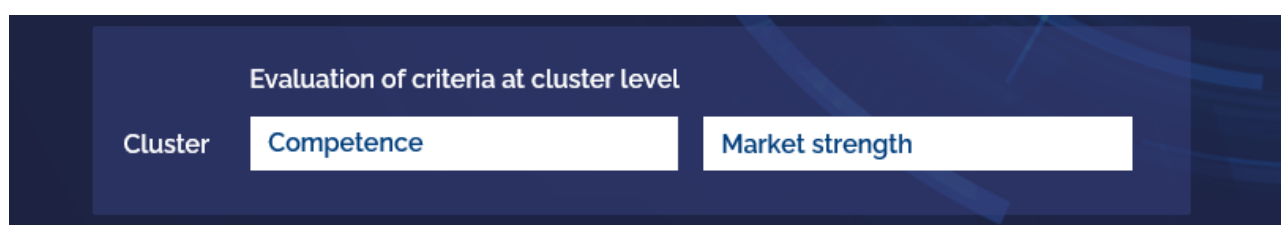


Fig. 4: PAC RADAR – evaluation method

PAC uses **predefined criteria** to assess and compare the providers within given service segments. The assessment is based on the report-card score within the peer group of the positioned providers.

This is based on:

- The provider's detailed self-disclosure about resources, distribution, delivery, portfolio, contract design, pricing, customer structure, customer references, investments, partnerships, certifications, etc.;
- The analysis of existing PAC databases;
- Secondary research;
- Dedicated face-to-face interviews as relevant.

The provider data is verified by PAC and any omissions are rectified based on estimates.

**If the provider does not participate**, the assessment is performed using the proven PAC methodology, mainly based on:

- Information obtained from face-to-face interviews with the provider's representatives, analyst briefings, etc.;
- An assessment of company presentations, company reports, etc.;

- An assessment of PAC databases;
- An assessment of earlier PAC RADARs in which the provider participated;

### Reissue of published RADARs

The scores in the PAC RADAR represent an assessment of the providers within the given peer group in the year in which the respective PAC RADAR is published.

The evaluation may not be directly comparable with that of any previous version due to subsequent content modifications. In particular, it does not depict a development of individual providers over time.

Methodological and/or organizational modifications may be made due to changing market conditions and trends, and may include:

- A different peer group in the focus of the analysis;
- Modification of individual criteria within clusters;
- Increased or altered expectations by user companies;
- Adjustment of the weighting of individual criteria.

## Evaluation criteria

**General criteria (considered at a European level to varying extents for several RADARs) Criteria's in Red are overrated with their index (x)**

### Competence

- Total number of cybersecurity professionals employed by the company
- Mix of expert consultants per silo - architect, threat/pentester, detection/remediation
- Number of SOC level 1, 2, 3 experts and 24/7 availability
- Mix of internal (employees) vs. external consultants (subcontractors, freelancers, etc.)
- Consultant location - France or Europe
- OT certification
- PASSI certification
- PRIS certification
- PACS certification
- PDIS certification
- PAMS certification
- Other certification (CISSP, CISM)
- HR - attractiveness/retention/training policy and employer's branding (x4)
- Ecosystem & contribution - capacity to contribute to alliances or syndicates
- Innovation & product development capacity - ownership of IP solution, R&D (x4)

### Market strength

- Company's financial stability and ability to expand operations in recent years
- Total years of experience providing both IT & OT security services
- Stability of the company ownership, who funds it, and how is the track record
- Comprehensiveness of company's IT security services (auditing, consulting, integration, managed services)
- Comprehensiveness of company's OT security services (auditing, consulting, field operations, managed services)
- OT - international capacity
- Experience in OT - background & history in OT
- Expert OT SOC
- Gold partners (MS, GCP, AWS, SentinelOne, CrowdStrike, Palo Alto Networks, HarfangLab, etc.)
- Multiple partners - tech/partners agnosticism
- Diversity/sovereignty - ability to work with local technology vendors and develop proprietary security solutions (x5)
- OT sec - vulnerability operations center
- OT sec - field operations for OT
- OT - qualifications (ISO, etc.)
- IT sec - proprietary cybersecurity threat intelligence (CTI) feeds (x3)
- IT sec - capacity to share own CTI services
- IT sec - INTERCERT/FIST contribution.
- IT sec - CERT or CSIRT offering capacity
- Special capabilities or services that set the company apart from competitors

## PAC RADAR REPORT LICENSE

### **PAC RADAR "Leaders in IT/OT Cybersecurity in France 2025"**

#### **Unlimited reprint rights**

Within the framework of the license with unlimited reprint rights the customer receives a PAC RADAR short report, a PAC RADAR graphic, and a PAC RADAR badge. Their usage and distribution to external parties is expressly permitted, without any limitations. The customer is entitled to use the contents of this PAC RADAR short report as well as the PAC RADAR graphic and badge, either completely or partially (e.g., individual text sections or graphics), for all marketing and communications purposes.

In any usage and distribution, all contents of the PAC RADAR short report, the PAC RADAR graphic, and the PAC RADAR badge must always be marked with the "PAC" source reference. However, the contents must not be manipulated or deployed in such a way that changes the context.

The usage rights defined within the license with unlimited reprint rights refer to the PAC RADAR short report, the PAC RADAR graphic, and the PAC RADAR badge, however, under no circumstances include the usage of the contents of the full version of the PAC RADAR report.

Moreover, copyright conditions for the PAC RADAR apply (see [About the PAC RADAR](#)).

## ABOUT THE PAC RADAR

The PAC RADAR is protected by Pierre Audoin Consultants (PAC) GmbH's copyright.

The PAC RADAR is a graphical representation and written analysis of the positioning of various IT providers within a defined market segment at a specific point in time. The positioning and characterization of selected companies within the PAC RADAR is conducted on the basis of an analytical assessment of criteria which PAC previously defined for this analysis.

The selection, positioning, and characterization of companies within the PAC RADAR is not subject to any vested interests whatsoever. PAC does not support any providers that are represented in the PAC RADAR, and does not give any recommendations to technology users. The PAC RADAR represents a result from market research only and must not be taken as a recommendation for action.

The contents of the PAC RADAR have been created with utmost diligence and care. However, PAC cannot be held responsible for any errors or omissions.

PAC excludes all express or implied claims, also if derived from warranties with respect to the PAC RADAR report, including any implied warranties of merchantability or fitness for a particular purpose.

The PAC RADAR may only be used for a license fee and with the consent of PAC. Moreover, the use and publication of the contents and the results of the PAC RADAR are subject to the "Terms & Conditions for the Usage of Pierre Audoin Consultants' SITSI® License."

Copyright Pierre Audoin Consultants (PAC) GmbH 2025. All rights reserved.

More on [www.pac-radar.com](http://www.pac-radar.com).

## ABOUT PAC

We are a content-based company with a consulting DNA. PAC is the leading European consulting and analyst firm supporting software & IT service vendors worldwide. Since 1976, we have helped our clients to understand market dynamics, grow their revenue and raise their profile. Our unrivalled understanding of European markets, and deep research coverage help key market players to define their strategy, optimize their go-to-market and increase market share. PAC is an analyst-led consultancy with a team of over 100 experts across Europe. We provide market research and analysis on more than 30 countries worldwide, delivered through our portfolio pillars, Guidance, Insights, and Visibility, and our renowned SITSI® research platform.

More on [www.pacanalyst.com](http://www.pacanalyst.com).