



Osservatorio
Attacchi Digitali
in Italia

PROPOSAL OF SPONSORSHIP OAD 2026

AN INIZIATIVE OF  **aipsi**

IMPLEMENTED BY



April 2026

Summary

1. THE OAD INITIATIVE	3
2. OAD 2026	3
2.1. The questionnaire OAD 2026	4
2.2 OAD 2025 Report	4
3. OAD 2025 SPONSORSHIP	4
3.1 Why sponsoring OAD 2026 is worth it	6
4. THE INTELLECTUAL PROPERTY OF OAD 2025	7
5. HOW TO JOIN THE SPONSORSHIP OF OAD 2025	7
OAD 2026 SPONSORSHIP FORM	8
Annex 1 – Operational Plan for OAD 2026	9
Annex 2 - The OAD 2026 Questionnaire	10
Annex 2.1 - Questions on Detected Digital Attacks	10
Annex 2.2 - To thank the respondents to the OAD 2026 questionnaire	11
Annex 3 - The OAD 2026 Report	12
AIPSI, Associazione Italiana Professionisti Sicurezza Informatica	13

1. THE OAD INITIATIVE

OAD – Digital Attack Observatory in Italy is the leading Italian observatory for the ongoing analysis of intentional digital attacks and the security level of information systems in businesses and public administrations.

In 2026, OAD reached 19 consecutive years of surveys, confirming its uniqueness in the national landscape for its continuity, authoritativeness, and ability to provide a concrete snapshot of the evolution of digital security in the country.

The survey is conducted by Malabo, a management consulting firm specializing in ICT, responsible for implementing the online questionnaire, processing the collected data, and drafting the final report, under the guidance of AIPSI, the Italian Association of Digital Security Professionals.

AIPSI defines and oversees the initiative's structure, publishes the final report, and guarantees its quality, independence, and authority, including with respect to its sponsors.

OAD is currently the only initiative in Italy based on an anonymous online survey targeting companies of all sizes and sectors, as well as public administrations, with the aim of collecting real, comparable data useful for understanding the spread of digital attacks and the actual level of adoption of the main digital security measures.

The questionnaire is aimed specifically at:

- CIOs and information systems managers
- system administrators
- CISOs and cyber managers
- third parties who manage digital security on behalf of clients
- top decision-makers in smaller organizations.

OAD's objective is twofold: on the one hand, to measure and analyze the phenomenon of digital attacks in Italy in an independent, continuous, and authoritative manner; on the other, to contribute to the diffusion of a broader culture of digital security by providing the market with local, reliable, and freely accessible information.

The availability of "local to Italy" data on detected attacks, key vulnerabilities, and the most widespread protective measures represents concrete support for organizations, especially small and medium-sized ones, in assessing cyber risk and defining prevention and protection actions, also in accordance with the main national and international regulatory frameworks.

Over the years, OAD has consolidated its growing capacity for dissemination and impact. Its published annual reports have become a reference tool for professionals, companies, organizations, media, and institutional stakeholders interested in digital security issues.

In recent years, the number of copies downloaded per edition has exceeded one thousand.

For sponsors, OAD therefore represents not only support for an initiative of value for the country, but also a qualified platform for visibility, positioning, and relationships with a highly profiled community of ICT and cyber professionals and decision-makers.

2. OAD 2026

The 2026 edition of the OAD was created with a specific goal: to increase participation and further enhance the survey's ability to produce useful, readable, and current market insights.

For this reason, the 2026 OAD questionnaire has been significantly simplified and reduced, both in terms of the number of questions and the structure of the responses, to reduce completion time and encourage broader participation, without compromising the quality and significance of the data collected.

Annex 1 provides a rough schedule of the various OAD planned activities for 2026.

Please note that AIPSI cannot guarantee the effective and active collaboration of the sponsoring associations, resulting in a significant response from their members and consequently significant coverage of various product sectors.

AIPSI intends to increase the number of companies/institutions completing the online questionnaire by:

- significantly reducing and simplifying the number of questions and answers available in the new online questionnaire (see Annex 2)
- **free one-year AIPSI membership**, worth €50.00, for those who complete the questionnaire
- the promotional campaign that AIPSI will launch with the involvement of its Patrons and Sponsors.

2.1. The questionnaire OAD 2026

The strictly anonymous OAD 2026 online questionnaire (see details in Annex 2):

- maintains two key questions on attacks detected in 2025, ensuring historical continuity and trend analysis from 2007 to 2025
- simplifies and makes the section on existing technical and organizational security measures optional
- aims to improve the completion experience and, consequently, the volume and quality of responses.

An additional valuable element is that, upon completion of the entire questionnaire, **a macro-assessment of the digital security level resulting from the responses is automatically returned**, contextualized to the type of organization and its IT system, along with the relevant technical and organizational security measures.

This is a particularly interesting feature, especially for SMEs and microenterprises, as it makes the initiative not only informative but also immediately useful for participants.

As in previous editions, OAD 2026 will be supported by a network of free patronages with trade associations, professional bodies, and representatives from various economic and professional sectors.

The goal is to further expand the promotional campaign's reach and engage vertical communities, increasing the project's relevance and representativeness.

While it is not possible to guarantee a predetermined distribution of responses by sector in advance, the project's structure, simplified questionnaire, and the activation of partners and sponsors make OAD 2026 an initiative with strong potential for visibility and penetration among a highly qualified audience.

2.2 OAD 2025 Report

The planned structure for the 2026 OAD Report, similar in content to the final reports of previous years, is detailed in Appendix 3.

A specific chapter is dedicated to data provided by the Italian Postal Police and Cybersecurity Service. This data, as in previous years, will cover attacks on Italian critical infrastructure, attacks on the banking and financial sectors, and digital terrorism.

3. OAD 2025 SPONSORSHIP

Sponsorship of OAD 2026 is designed to offer partner companies **qualified visibility**, **authoritative positioning**, and **concrete opportunities** for engagement with an audience of professionals, decision-makers, and stakeholders from the ICT and cyber world.

Three partnership options are available.

1. **Silver Sponsorship**, the basic one with a prize of **€ 2.000,00 + VAT**, which entitles to:
 - a) the Sponsor logo on the online questionnaire and on the cover of the OAD 2026 Report
 - b) **one A4 page presentation of the Sponsor** in the Annex C of the final Report (see Annex 3), with institutional information and a highlight of his products/services for the digital security
 - c) the availability of the figures and graphs in high definition of the 2025 Report for any publications (blogs, websites, social networks, on paper, etc.) by the Sponsor, with the obligation to always show, for each published figure, the brand **©OAD 2026** (present in the figures and graphs provided, and not to be deleted)
 - d) the visibility of the Sponsor's logo in all the AIPSI presentations on OAD
 - e) the Sponsor logo on the OAD and AIPSI web pages to download the OAD 2026 Report; the promotion of the 2026 survey and of the final report on social networks and other media in which OAD, AIPSI, Malabo and the various Patrons and Sponsors are active.A single invoice of **€2,000.00 + VAT** is issued to the Silver Sponsor by AIPSI upon receipt of the order; payment must be made within 30 days of the invoice date.
2. **Gold Sponsorship**, with a prize of **€ 5.000,00 +VAT**. In addition, and/or in modification to what is provided for the Silver one, it entitles to:
 - a) a larger size of the Sponsor logo on the cover of the Report and on the AIPSI and OAD websites such as Gold Sponsor
 - a. **two A4 pages** in its presentation in Annex C of the OAD 2026 Report
 - b. the inclusion of the logo and the link to the Sponsor website on the home page of the AIPSI website under the heading "Sponsor AIPSI 2026"
 - b) the participation of a representative of the Sponsor at the Round Table of the (hybrid) webinar that will present the OAD 2026 Report.Payment can take place in a single tranche or in two. Two invoices can be issued to the Gold Sponsor by AIPSI, the first of **€3,000.00 + VAT** upon receipt of the order, the second of **€2,000.00 + VAT** upon publication of the Final Report. Payment must be made within 30 days of the invoice date.
3. **Diamond**, with a prize of **€ 10.000,00 +IVA**. In addition, and/or in modification to what is provided for the Gold one, it entitles to:
 - a) an even larger size of the Sponsor's logo on the cover of the 2026 Report and on the AIPSI and OAD websites such as Diamond Sponsor
 - b) **three A4 pages** in its presentation in Annex C of the OAD 2025 Report
 - c) the possibility for a top manager of the Diamond Sponsor to participate in the AIPSI Board of Directors, without the right to vote, but suggesting/proposing specific initiatives
 - d) a specific AIPSI-Sponsor event/webinar, which content will be agreed and, in any way, will include some of the results of the OAD 2025 survey, that are significant for the Sponsor. The webinar may use the AIPSI platform or the one provided by the Sponsor itself

- e) the creation of a specific article, in collaboration with some AIPSI leaders, that will be published in one or more magazines, chosen from those of the AIPSI and/or used by the Sponsor; this article will be published also on the AIPSI and OAD websites.

Payment can take place in a single tranche or in two. Two invoices can be issued to the Diamond Sponsor by AIPSI, the first of **€6,000.00 + VAT** upon receipt of the order, the second of **€4,000.00 + VAT** upon publication of the Final Report. Payment must be made within 30 days of the invoice date.

3.1 Why sponsoring OAD 2026 is worth it

Sponsoring OAD 2026 means associating your brand with one of the most authoritative and ongoing initiatives in Italy on the topic of digital security, while simultaneously gaining high-quality visibility, authority, and opportunities to connect with a highly relevant audience.

For a sponsor, OAD 2026 represents a concrete opportunity to:

- strengthen your positioning in an authoritative and independent context
- increase brand visibility among professionals, decision-makers, and influencers in the ICT and cyber world
- enhance your company profile within an authoritative Report, known and consulted for years by more than just small and micro-organizations
- oversee an ecosystem of events, webinars, and content related to the initiative
- associate your brand with a project with high cultural, reputational, and informational value for the Italian market.

A distinctive feature of OAD 2026 is the immediate provision to participants of a macro-assessment of the level of digital security resulting from their responses. This makes the project particularly effective in terms of awareness and activation: those who complete the questionnaire immediately perceive the concrete value of the initiative and, in the event of critical issues in the information system covered by the responses, can identify the sponsors as qualified interlocutors capable of supporting improvement processes.

From this perspective, the OAD 2026 sponsorship is not merely a communication activity, but an investment capable of effectively combining brand awareness, authority, reputation, and commercial proximity to a high-value target.

For these reasons, sponsorship can be viewed not only as an alternative to other forms of promotion, but as a solution that is often more efficient, more qualified, and more consistent with the positioning objectives of companies operating in the digital security market.

Another attractive aspect of the OAD 2026 sponsorship is **its cost-effectiveness in terms of the quality of visibility achieved**, especially when compared to traditional online promotion tools.

Unlike paid digital advertising, which requires ongoing investment to maintain coverage and results over time, **the OAD 2026 sponsorship allows, with a defined and predetermined investment, coverage of multiple moments, multiple channels, and multiple opportunities to engage with a highly targeted audience, consistent with the digital security market.**

The Sponsor not only acquires promotional space, but also associates its brand with a consolidated, independent, and authoritative initiative, gaining visibility in the online questionnaire, the Final Report, the AIPSI and OAD websites, presentation events, webinars, communication materials, and subsequent content dissemination activities. It is therefore a comprehensive and long-lasting presence, which goes well beyond the logic of simple temporary advertising.

From a financial perspective, this translates into **greater investment efficiency**, particularly for companies operating in ICT, cybersecurity, and related professional services, as sponsorship allows them to reach an already qualified audience of professionals, decision-makers, influencers, and potential clients, significantly reducing the dispersion typical of generalist online campaigns.

Added to this is another valuable factor: **the persistence of the communication effect**. While an online advertising campaign tends to wear off once the invested budget expires, the OAD 2026 sponsorship continues to generate returns in terms of visibility and positioning thanks to the circulation of the Report, downloads, reuse of content at events and conferences, ongoing consultation of published materials, and the stable association of the brand with a recognized source in the Italian digital security landscape.

Sponsorship therefore allows not only an institutional presence, but also a more direct and relevant connection with an audience potentially interested in cybersecurity solutions, services, and expertise.

In summary, OAD 2026 offers sponsors:

- a visible presence throughout the initiative's entire lifecycle
- access to a qualified community sensitive to cyber issues
- brand association with authoritative, highly informative content
- opportunities for networking, thought leadership, and communication before, during, and after the Report's publication.

4. THE INTELLECTUAL PROPERTY OF OAD 2026

The intellectual property and copyrights of the entire initiative OAD 2026, including the online questionnaire and the contents, figures and graphs of the OAD 2026 Report, belong, as for the previous editions, to AIPSI and Malabo Srl which allow their use to Sponsors, with the obligation to cite the source on the figures and graphs of the Report using the brand ©OAD 2026.

5. HOW TO JOIN THE SPONSORSHIP OF OAD 2026

Simply **complete the following application form**, sign it by the person with the necessary signing authority (preferably with a digital signature), and send it via certified email (PEC) to **aipsi@gigapec.it**.

Upon receipt, AIPSI will contact the designated contact to finalize the operational and administrative aspects and issue the relevant invoice.

Sponsorship applications remain open until 2-3 weeks before the publication of the Final Report. After this deadline, it will no longer be possible to guarantee the inclusion of the sponsor profile in the Report and the logo on the cover.

It is understood that early confirmation allows the Sponsor to benefit from a longer period of visibility, starting with the questionnaire promotion campaign and throughout the duration of the communication activities related to OAD 2026.

OAD 2026 SPONSORSHIP FORM

This form, completed and signed, has to be sent in e-mail to aipsi@gigapec.it

Our Company confirms to AIPSI its sponsorship of OAD 2026 with the choice selected below, that implies the related rights and conditions detailed in this proposal.

(Please, place a cross in the chosen box)

- | | | |
|--------------------------|---------------------|-------------------|
| ☐ | Silver Sponsorship | € 2.000,00 + VAT |
| ☐ | Gold Sponsorship | € 5.000,00 + VAT |
| ☐ | Diamond Sponsorship | € 10.000,00 + VAT |

Company:

Address:

City:

Postal Code:

VAT:

Company E-mail (possibly REM for Europe):

We will issue a purchase order to AIPSI: NO/YES **ORDER NUMBER:**

Operational contact person

First Name: **Last Name:**

Phone: **Mobile:** **E-mail:**

Responsible/Manager with signing power

First Name: **Last Name:**

Business role:

Phone: **Mobile:** **E-mail:**

Responsible/Manager signature:

Place : **Date:**

Annex 1 – Operational Plan for OAD 2026

The overall schedule of activities planned for OAD 2026 is as follows (this schedule is tentative and subject to change):

- **MARCH 2026**
 - Development of the OAD 2026 initiative within the AIPSI Steering Committee, with the support of OAD creator Marco R. A. Bozzetti and his company Malabo.
 - Development by Malabo of the new OAD 2026 questionnaire and related testing with a Working Group for OAD 2026 specifically created within AIPSI.
 - Drafting sponsorship proposals and requests for free patronage and sending them to potential interested companies and organizations.
- **APRIL 2026**
 - Launch of the online questionnaire on the oadweb.it platform
 - Promotional campaign begins for completing the questionnaires
 - Contacts for sponsorships and sponsorships
- **MAY – JULY 2026**
 - Promotional campaign continues for completing the questionnaires
 - Contacts for sponsorships and sponsorships continue.
- **AUGUST 2025**
 - Closure of the online questionnaire
 - Processing of data collected from the online questionnaires
 - Beginning of drafting of the OAD 2026 Final Report
- **SEPTEMBER 2026**
 - Completion of the OAD 2026 Final Report
 - Launch of the promotional campaign for downloading the OAD 2026 Report by the Patrons' and Sponsors' contacts, as well as any interested parties contacted through AIPSI's various multimedia channels.
 - AIPSI videoconference or "hybrid" event (in-person and remote videoconference) for the official presentation of the OAD 2026 Report, with a roundtable discussion of the data emerging with representatives of the Gold and Diamond Sponsors.
- **SEPTEMBER-DECEMBER 2026**
 - Drafting and/or assistance in drafting notes and articles in various media outlets relating to the OAD 2026 Report and the published data.
 - Possible creation of webinars and articles for Gold and Diamond Sponsors
 - Periodic provision to Sponsors of download data for the 2026 OAD Report (number of downloads, not the name of the downloader, since the download will not require the downloader's login).

Annex 2 - The OAD 2026 Questionnaire

The OAD 2026 online questionnaire is in Italian, with predefined answers to choose from. It is structured with a total of 47 questions divided into 8 sections, of which 28, those on existing security measures, are optional. Therefore, only 19 questions are mandatory.

Sections 1, 4, 5, and 6 contain hidden "questions" that perform calculations on the selected answers to assess the overall security level of the information system being answered.

The sections considered in the OAD 2026 questionnaire, with the number of questions per section in brackets:

- S1 - Brief information on the respondent's company/organization (4)
- S2 - Digital attacks of any kind on the information system detected throughout 2025 (2)
- S3 - Most feared attacks in the near future (3)
- S4 - Macro-characteristics of the information system to which the respondent refers (10)
- S5 - Technical measures in place for the digital security of the entire information system
 - S5.1 - Inventory of the IS's ICT resources and basic architecture of digital security tools (3)
 - S5.2 - Access and account protection (2)
 - S5.3 - Patches, anti-malware, antivirus, EDR, endpoint protection (3)
 - S5.4 - Networks, firewalls, remote access (2)
 - S5.5 - Backup and business continuity (4)
 - S5.6 - Digital Security Monitoring and Log Management (2)
 - S5.7 - Vulnerability and Incident Management (2)
- S6 - Main Organizational Measures for Digital Security (9)
- S7 - Role of the Respondent (1)
- S10 - Calculations (not visible) and final real-time presentation of the macro-assessment of the SI security level to those who complete the responses, including those in Sections 6 and

Completing the entire questionnaire, including the optional sections, automatically provides a **macro-assessment of the digital security level** that emerges from the responses provided, along with a list of the selected responses that are most critical and impactful on this assessment.

Annex 2.1 - Questions on Detected Digital Attacks

The two general questions, necessary to ensure continuity with those of the previous seventeen years on the prevalence of intentional digital attacks in Italy, concern:

- **Attack types** (what is being attacked), which include the following 15 attack groups (families):
 - Destruction and/or PHYSICAL compromise of FIXED ICT devices or their parts
 - Theft of FIXED ICT devices or their parts
 - Theft of MOBILE ICT devices owned by the company/organization and used by its employees/collaborators
 - Information theft from specific FIXED ICT systems (PCs, servers, storage systems, etc.) of the Information System, including outsourced/cloud-based systems

- Information theft relating to the company/organization from MOBILE systems (PDAs, smartphones, tablets, etc.) whether owned by the company/organization or by the end user using them as part of a BYOD approach
 - Attacks on identification, authentication, and control End-user and privileged access
 - Attacks on local and wide-area networks, both fixed and wireless, including Internet connections, and DNS during 2022
 - Attack and/or unauthorized use of ENTIRE IT SYSTEMS (from PCs to physical and virtual hosts). including outsourced or cloud-based systems
 - Malicious and/or unauthorized modifications to the APPLICATION PROGRAMS and their configurations, including outsourced and cloud-based systems
 - Malicious and/or unauthorized modifications to the INFORMATION processed by the IT System's applications, including those outsourced/cloud-based systems
 - Saturation (DoS, DDoS) of the IT System's digital resources, including those outsourced/cloud-based systems
 - Attacks on its own digital systems/services in the CLOUD or otherwise OUTSOURCED at third-party providers
 - Attacks on OT and Operational Technology (OT) systems, including IoT/IIoT systems, industrial automation systems (SCADA, DCS, PLC, etc.), and robotics
 - Supply Chain attacks caused by vulnerabilities in interconnected suppliers and/or customers
 - Attacks on Artificial Intelligence-based systems/services/applications
- Families of **attack techniques** (how it is attacked):
 - Physical attack
 - Malicious and unauthorized collection of information
 - Malicious scripts and programs
 - Autonomous agents
 - Toolkits
 - Botnets and similar
 - Use of Artificial Intelligence tools and techniques
 - Use of two or more attack techniques, including APTs (Advanced Persistent Threats).

Annex 2.2 - To thank the respondents to the OAD 2026 questionnaire

Those who complete the OAD 2026 questionnaire can **request free one-year membership to AIPSI** by submitting the **numeric code** provided by the system in the thank-you text upon completion of the questionnaire.

This numeric code must be sent by email to aipsi@aipsi.org, requesting free one-year membership to AIPSI and providing the following information:

Annex 3 - The OAD 2026 Report

The basic structure of the OAD 2026 Report will consist of the following chapters:

- Preface(s)
- Chapter 1 - Executive Summary (in Italian)
- Chapter 1bis - Executive Summary (in English)
- Chapter 2 - The OAD 2026 Survey
 - Type of Respondent Companies/Entities
 - Macro-characteristics of the Information Systems of the Respondent Companies/Entities
- Chapter 3 - Intentional Digital Attacks
 - International (including with OECD data)
 - European (including with ENISA data)
 - Italian (ACN data)
- Chapter 4 - Digital Attacks in Italy from the OAD 2026 Survey
- Chapter 5 - The Most Feared Digital Attacks in the Near Future in Italy from the OAD 2026 Survey
- Chapter 6 - Security Measures in Place in Respondents' Information Systems from the OAD Survey 2026
- Chapter 7 - Data on "computer crime" in Italy from the Italian Postal and Cybersecurity Police
- Appendix A - Methodological aspects of the OAD 2026 survey
- Appendix B - Glossary of main terms and acronyms related to cyber attacks
- Appendix C - Sponsor Profiles (an "institutional" profile for each Sponsor, 1, 2, or 3 A4 pages depending on the type of sponsorship (Silver, Gold, Diamond, see §4)
- Appendix D - Sponsor Profiles (logo, website URL, 3-4 lines of description)
- Appendix E - References and sources
- Appendix F - Author Profile of the OAD 2026 Report
- Appendixes G, H - Profiles of AIPSI and Malabo

The OAD 2026 final report will include prefaces by the most important and well-known representatives of Italian institutions involved in digital security. A preface by the Director of the Postal Police and Cybersecurity Service is expected, and prefaces have been requested from the top officials of the Department for Digital Transformation of the Presidency of the Council of Ministers, ACN, and AGID. These prefaces are significant in acknowledging the authoritativeness and validity of the OAD Report and indirectly contribute to its dissemination, especially within Italian public administrations and institutional bodies.

A specific chapter is dedicated to data provided by the Italian Postal Police and Cybersecurity Service. This data, as in previous years, will concern attacks on Italian critical infrastructure, attacks on the banking and financial world, and digital terrorism.

As with previous years, the newly published OAD 2026 Report will be made available free of charge on the OAD website www.oadweb.it and the AIPSI website www.aipsi.org

AIPSI, Associazione Italiana Professionisti Sicurezza Informatica

A non-profit association, the Italian chapter of the global ISSA, is made up of only natural persons interested and/or operating at any level and role in the field of digital security.

The primary objective of AIPSI is the professional growth and skills of its Members and the promotion and dissemination of the culture of digital security in Italy. In this perspective, in addition to the services and events provided by ISSA, such as the monthly magazine ISSA Journal, conferences, webinars, working groups and courses in English, a global network among Members, discounts on courses and individual certifications, AIPSI provides specific services for the Italian context: some reserved for Members only, such as free mentorship for professional growth, in-depth working groups, a national network among Members, discounts on courses and individual certifications in Italy, but most are open to all interested parties: conferences and webinars, the annual OAD survey on digital attacks and security measures in companies/entities in Italy, AIPSI Giovani, the working group and the survey on female work in digital security in Italy (CSWI).

CF 9741515015 – VAT 05311540966 e-mail: aipsi@aipsi.org PEC: aipsi@gigapec.it

Registered office: Via Savona 26 - 20144 Milano

Tel: +39 02 72191512

MALABO S.r.l.

www.malaboadvisoring.it/en

Registered office: Via del Caravaggio 14 - 20144 Milano

Operational headquarters: Via Savona 26 - 20144 Milano

Tel: +39 02 72191512

E-mail: info@malaboadvisoring.it