Osservatorio
Attacchi Digitali
in Italia

PROPOSAL OF SPONSORSHIP OAD 2025

AN INIZIATIVE OF aipsi

IMPLEMENTED BY malabo ICT Advisory

January 2025

Summary

1. THE OAD INITIATIVE

The Italian acronym OAD, Osservatorio Attacchi Digitali in Italia, indicates the annual survey of the digital attacks on IT systems, and their security measures, in Italy, provided by AIPSI, Associazione Italiana Professionisti Sicurezza Informatica (https://www.aipsi.org/), Italian Chapter of the world-wide no profit ISSA (Information System Security Association, https://www.issa.org/).

The OAD survey started in 2008 with the acronym OAI, Osservatorio Attacchi Informatici in Italia, changed in OAD in 2016. With the 2025 edition, this initiative covers **eighteen years of consecutive survey**.

Operationally OAD/OAI has been always implemented by **Malabo Srl** (www.malaboadvisoring.it), and in the last years is **a key initiative** of AIPSI, that sets up, guides, supports all the OAD initiative, and publishes the OAD final report, **ensuring its quality and independence** (also from the Sponsors).

OAD is the only initiative in Italy carried out with a strictly anonymous survey addressed to all companies, of every product sector and size, and to Public Administrations, via an online web questionnaire with pre-set answers that can be filled out with any modern browser.
The questionnaire is typically addressed to IT Systems Managers (CIOs), System Administrators, IT Security Managers (CISOs), Third Parties who manage the digital security of their customers, and for small and very small organizations, the top managers (CEOs) and/or owners which decide strategies, budget and plans for their information system and their cyber security.

The OAD main objective is to analyze and spread as much as possible the actual reality of cybersecurity and of intentional digital attacks on the information systems of companies and public bodies in Italy, as well as the security measures in place. The OAD questionnaire is anonymous, independent, authoritative and freely accessible by any person who operates and/or decides in the field of digital security.
The availability of correct and updated information on cybersecurity and digital attacks "local to Italy" is fundamental for the growth of knowledge and culture on these topics and for a concrete help, especially for small organizations, in the assessment of digital risks and in the choice of the most suitable prevention and protection security measures.

The OAD contributes to the awareness and knowledge of digital security for all users and decision makers of information systems, which is one of the objectives of AIPSI and ISSA (see https://www.issa.org/about-issa/ and https://www.aipsi.org/associazione/perche-aipsi.html). Due to its importance in terms of communication, awareness and training on cybersecurity, OAD is part of the Italian national strategic initiative Digital Republic[1], as highlighted in https://repubblicadigitale.associazione.gov.it/it/i-progetti/.

Thirteen OAD/OAI annual reports have been published (their covers in fig. 1): these reports cover the seventeen consecutive years of online surveys carried out, from 2007 to 2023. It should be noted that the year of the OAD Report refers to the previous year during which the digital attacks indicated in the questionnaire were detected.
The most recent OAD reports have an “executive summary” both in Italian and in English.

[1] National strategic initiative promoted by the Italian Department for Digital Transformation of the Presidency of the Council of Ministers within the framework of the "Italy 2025" strategy: it aims to combat the cultural digital divide in the Italian population, to support maximum digital inclusion and encourage education on future technologies, accompanying the country's digital transformation process.

All OAI/OAD reports can be downloaded free of charge from the specific web site created for this initiative, https://www.oadweb.it/. A part of this site is in English: https://www.oadweb.it/en/.
This site archives and makes available to anyone interested all the documentation (in some cases also video recordings) of the various events, organized by AIPSI or in which it participated, where the data emerging from the various OAD surveys were presented and discussed.

As highlighted in fig. 1, on the covers of each report, since 2012, there are the logos of the Sponsors and the presentation sheet of each Sponsor is included as an attachment within the report (Attachment C, see §2.2).

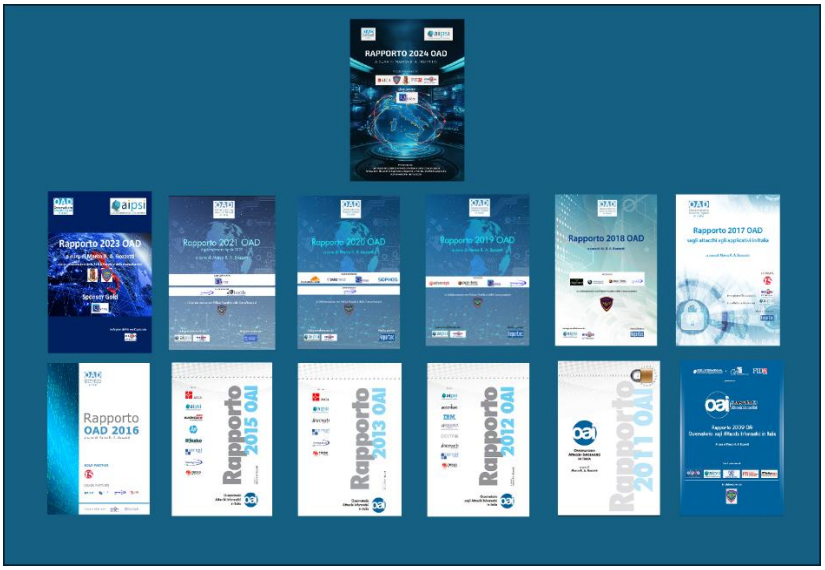

Fig. 1 The covers of the published OAD-OAI reports

The potential respondents to the OAD questionnaire are informed of the 2025 OAD survey and invited to fill in it through the various communication channels of AIPSI, of the patronizing associations and of the Sponsors (websites, events, social networks, e-mails, articles and banners, etc.).
In previous editions, the number of possible respondents contacted was estimated to be in the order of 5,000-6,000 people, mostly belonging to the world of companies, services, professional firms, public administrations, universities and high schools.

The number of reports downloaded from the OAD website or distributed via email, file transfer, file sharing, etc. has gradually increased over the years, reaching a number per edition of **over 3000** (three thousand) in the last three years. This data is provided by the precise number of downloads made from the aipsi.org and oadweb.it websites, and does not take into account the direct forwarding of the OAD final Report to interested parties by Sponsors, Patrons and those who had already downloaded it. Estimating these forwardings, it is reasonable to estimate that the Report has been distributed, in the latest editions, among **4000 - 5000 people**.
For example, with regard to the OAD 2024 Report, to date **3373 downloads** have been recorded between the AIPSI website and the OAD website, a significant number due to the possibility of downloading it without having to first log in to the site, and therefore be registered.

Also for OAD 2025 it will be possible to download the final report, which will be available on the AIPSI and OAD websites, without having to register.

2. OAD 2025

The 2025 OAD survey will have a reduced and simplified questionnaire so as to reduce the time needed to complete it, while maintaining significant content for the analysis of the phenomenon of intentional digital attacks in the business sector and ensuring continuity with the main information collected in the previous editions.
For these reasons the online questionnaire, strictly anonymous, of OAD 2025:

- will contain only two questions on the attacks detected in 2024 in reference to the types of attacks and to the groups of attack techniques (see §2.1.1), so as to be able to have general trend data on the attacks (what is attacked and with which techniques) from 2007 to 2024;
- the in-depth questions will only concern the attacks suffered in 2025 on **web applications** and on **OT, Operational Technology**;
- questions on the digital security measures present in the information systems will be optional.

The first two questions, about the attacks suffered, will be mandatory for all respondents: for those who have not detected attacks, the related questions will be automatically skipped thanks to the application that supports the online questionnaire, based on a specific configuration made by Malabo on the open source software Limesurvey.
Questions regarding the type of company/entity to which the Information System subject to the answers belongs, the most feared future attacks, the role of the compiler of the questionnaire will also be mandatory. There are also mandatory all the questions related to the type of respondent company/entity, to the most feared future attacks and to the role of the questionnaire compiler.

Upon completion of the entire questionnaire, including the optional part on the security measures in place, a qualitative **macro evaluation of the security level** is automatically provided: a level that emerges from the answers provided, and that depends, in general, from the type of company and from its needs for digital security. This macro-assessment is of particular interest especially for small and very small organizations.

As in previous years, AIPSI will try to establish patronage with associations of the various product sectors (as well of the local and central public administrations), and of specific professions (for example lawyers, notaries, accountants, doctors, CIOs, CISOs, DPOs, etc.).
AIPSI will also try to expand the number of media used, and to obtain a more incisive involvement of newspapers to raise awareness of the 2024 OAD survey and of its final report, and, first of all, to promote the compilation of the questionnaire .
AIPSI will hold specific events with some of the patronizing associations, and if the number of respondents per product sector allows it (>100), to carry out specific analyzes for these sectors.

Please note that **AIPSI cannot guarantee** complete coverage of the various product sectors, and even less can it guarantee the effective and active collaboration of the patronizing associations.

The campaign that will be undertaken by AIPSI with all these interlocutors, and the reduction in the number of questions in the online questionnaire, should lead to an increase in the total number of respondents: but it is not possible to guarantee the Sponsor a predetermined extension of the pool of respondents (and then of readers of the Final Report) for the various sectors.

2.1. The questionnaire OAD 2025

As already indicated in the previous paragraph, the 2025 questionnaire will be focus on the intentional attacks detected in 2024 on **web applications** and on the world of **OT, Operational Technology**.

The OAD 2025 online questionnaire, with predefined answers to select, will be structured with about a hundred questions collected in 8 sections, many of which are optional and "skippable" during compilation. In some sections there are subsections to better articulate and contextualize the various questions. Furthermore, in some sections there are non-visible "questions" that perform calculations on the selected answers for the evaluation of the security level of the IT system object of the answers.
The sections considered in the 2025 questionnaire:

- S1 - Brief information on the respondent's Company/Entity
- S2 - Digital attacks of any kind on the Information System detected throughout 2024
- S3 - In-depth analysis of attacks on the Information System's websites and web applications
- S3B - In-depth analysis of attacks on the Information System's OT systems and equipment
- S4 - Most feared attacks in the near future
- S5 - Macro characteristics of the Information System to which the respondent refers
- S6 - Technical measures in place for the digital security of the entire Information System (6 questions)
    - S6.1 - Physical digital security measures
    - S6.2 - Identification, Authentication and Authorization measures
    - S6.3 - Measures for the security of local and geographic networks, including Internet connections
    - S6.4 - Application security measures of the Information System
    - S6.5 - Technical measures of digital security for data protection
    - S6.6 - Technical tools for the control and management of the digital security of the IS
    - S6.7 - Security in OT systems in use
- S7 - Organizational measures of digital security in the Company/Entity of the respondent
- S8 - Role of the respondent
- S10 - Calculations (not visible) and final real-time presentation of the macro assessment of the IS security level to those who complete the answers including those of Sections 6 and 7.

The answers related to the attacks will be mandatory, while these on existing security measures will be optional, but required to have the macro evaluation of the security level.
If no attacks have been detected, the online questionnaire system automatically skips the related questions and moves on to the next ones.

2.1.1 The questions on the detected attacks

The two general and mandatory questions, necessary to guarantee continuity with those of the previous seventeen years on the spread of intentional digital attacks in Italy, concern:

- the **types/families of digital attacks**, that refer to what is attacked:
    - Physical destruction of ICT devices or their parts
    - Theft of mobile user devices (smartphones, tablets, etc.)
    - Theft of fixed ICT devices or their parts (PCs, servers, storage systems, etc.)
    - Theft of information from fixed ICT systems
    - Theft of information from mobile user systems

  - Attacks on the identification, authentication and authorizations of the users
  - Attacks on networks, local and geographic, fixed and wireless, and on DNS
  - Attacks on individual ICT systems as a whole (from user devices to storage servers and cloud services)
  - Attacks for unauthorized modifications to application programs and their configurations
  - Attacks for unauthorized modifications to the information processed by ICT systems
  - Deniel of Services/Distributed DoS attacks (DoS/DDoS)
  - Attacks on the parts of our IT system outsourced in cloud or in housing/hosting services
  - Attacks on the OT, Operational Technology, systems of your IT system (Internet of Things, industrial automation and robotics, etc.)
  - SUPPLY CHAIN attacks caused by vulnerabilities in interconnected suppliers and/or customers.
- the families of **attack techniques**, which refer to the attack's modes in terms of which technical techniques were used:
  - Physical attack
  - Malicious and unauthorized collection of information
  - Malicious scripts and programs
  - Autonomous agents
  - Toolkits
  - Botnets and similar
  - Use of Artificial Intelligence tools
  - Use of two or more attack techniques, including APTs, Advanced Persistent Threats.

Detailed questions about detected attacks on web and on OT, will include:

- whether the systems attacked are on premise, outsourced in hosting or in the cloud, or in a mix between outsourcing and on premise;
- the probable attack techniques used (listed above) and, in greater detail for web environments, which vulnerabilities were probably exploited by referring to the OWASP top 10 in the case of the most serious attack suffered;
- the most serious technical and economic impacts experienced by the most serious attack;
- the possible reasons for the most serious attack;
- the maximum time to recover after suffering the most serious attack.

2.1.2 The questions on the digital security measures in place

As previously indicated, all these questions will be optional. However, it would be advisable to be compiled, so as to obtain:

- a checklist of digital, technical and organizational security measures that could or should be implemented on the information systems of the respondent;
- a macro qualitative analysis of the existing security level, based on the answers provided, with the list, among these answers, of those that highlight the most serious shortcomings. In practice, a first indication of the main improvements in digital security that should be made.

The OAD 2025 survey of digital security measures in place will refer to the following measures:

- **Technical measures**
  - Digital security architecture, integrated with the IT system architecture, which may include Zero Trust, SASE, SOAR, etc.

  - Physical countermeasures
  - Identification, Authentication, Authorization (IAA)
  - Local and geographic networks' countermeasures
  - Logical protection of each ICT system (as a whole)
  - Application protection
  - Data protection
- **Organizational measures**
  - Digital security structures, roles, skills, certifications
  - Digital security policies and procedures
  - Digital security contracts and clauses with Third Parties
  - Awareness of digital security at all levels of the organizational structure
  - Auditing
- **Management and governance measures**
  - Digital security control and monitoring (operational management)
  - Strategic governance
  - Disaster Recovery.

Further questions in the questionnaire will concern:

- type and macro characteristics of the respondent's company/entity: product sector, number of employees, organizational structure for cybersecurity and primary needs for security measures for its activities (this question is asked at the beginning of the survey)
- How attacks were detected and managed when they occur
- types of attacks most feared in the near future.
- role of the questionnaire compiler.

2.2 OAD 2025 Report

The final report will be published and made available free of charge to all interested parties on the OAD and AIPSI websites, within the expected timeframes indicated in §5.
The Report will initially have an Executive Summary in Italian and English.
A specific chapter will be dedicated to the data provided by the Postal and Telecommunications Police, relating to the whole 2023. These data will concern, as in previous years, digital attacks on Italian critical infrastructures, digital attacks on the world of banking and finance, digital terrorism .

The final report will also include the following attachments:

- Annex A - Methodological aspects of the 2024 OAD survey
- Annex B - Glossary of the main terms and acronyms on cyber attacks
- Annex C - Sponsor Profiles (an "institutional" sheet for each Sponsor, of 1, 2 or 3 pages in A4 format depending on the type of sponsorship, see §8)
- Attachment D - Sponsor Profiles (logo, website URL, 3-4 lines of description)
- Annex E - References and sources
- Annex F - Profile of the Author(s) of the 2024 OAD Report
- Attachments G, H - Profiles of AIPSI and Malabo Srl

The 2024 OAD Report, as soon as it is available (see §6), will be downloadable free of charge from the OAD website (https://www.oadweb.it/en) and from the AIPSI website (https://www.aipsi.org), within the timeframes foreseen and indicated in §2.3.

As an example of a final report, and its summary, see the OAD 2023 Report:
https://www.aipsi.org/eventi/eventi-in-programma/902-aipsi-ha-pubblicato-il-rapporto-oad-2023-ora-scaricabile.html

All previous OAD/OAI reports are archived, and downloadable, year by year from
https://www.oadweb.it/it/rapporti-e-relativi-convegni.html

2.2.1 The desired and expected prefaces in the OAD 2025 Report

As for the 2024 edition, the OAD 2025 Report will have prefaces by well-known players in the Italian digital security scene, such as representatives of the most important Italian institutions. Prefaces are expected from the Director of the Postal Police Service and Cyber Security, and from the Department of Digital Transformation of the Presidency of the Council of Ministers, already had in 2024.
AIPSI will try to have prefaces also from ACN, AIGID and/or other Italian/European institutions involved in digital security.
These prefaces are essential for the recognition of the authoritativeness and validity of the OAD survey and Report, and thus help its dissemination especially in Italian Public Administrations and institutional offices.

3. TO THANK THE RESPONDENTS TO THE 2024 OAD QUESTIONNAIRE

Who will complete the 2023 OAD Questionnaire will be able to download for free two issues of the ISSA Journal magazine, reserved for AIPSI-ISSA Members.
The decision of which numbers to use of the ISSA Journal is currently underway, in order to select the two numbers with the topics of greatest interest to the Italian respondents.

4. OAD 2025 SCHEDULING

The overall framework of the activities planned for OAD 2025 is divided, month by month, into the following activities:

- **JANUARY 2025**
  - Setting up of the OAD 2025 initiative within AIPSI
  - Drafting sponsorship and patronage proposals and sending them to the potential interested companies and associations

- **FEBRUARY 2025**
  - Design and installation-activation of the online questionnaire on the oadweb.it platform
  - Start of promotional campaign for questionnaire's compilation
  - Contacts for patronages and sponsorships

- **MARCH – APRIL- MAY 2025**
  - Campaign for questionnaire's compilation
  - Contacts for patronage and sponsorships

- **JUNE 2025**
  - The online questionnaire system should be closed, depending on whether and when the minimum number of respondents (necessary for an anonymous web survey) will be reached.
    - If not reached, AIPSI will carry out a further specific promotion for the compilation of questionnaires person by person, in particular with reference to CIOs and CISOs
  - Start the analysis and the data processing of all the information collected by respondents.

- **JUNE-JULY 2025**
  - Processing of data collected from online questionnaires
  - Drafting of the 2025 OAD Report and its publication
  - Starting of the promotional campaign for the download of the 2025 OAD Report
  - Possible AIPSI "hybrid" event (physical and remote meeting in audio video conference) for the official presentation of the 2025 OAD Report with a round table to discuss the survey results with the representatives of the Gold and Diamond Sponsors (this event could be moved to September).

- **AGOST-SEPTEMBER 2025**
  - Drafting of notes and articles in the various media relating to the 2025 OAD Report
  - Webinars for Gold and Diamond Sponsors.

- **SEPTEMBER-DECEMBER 2025**
  - Periodic provision to Sponsors of the data for the 2025 OAD Report downloads (number of downloads, not the name of the person who downloaded it, since the download will not require the login of the person who downloads it)
  - AIPSI presentations, in various events, of some results from the 2025 OAD survey.

5. WHY IT IS WORTH SPONSORING OAD 2025

The sponsorship of OAD 2025 allows any company/institutions, in particular ICT and cyber security companies, to obtain important and qualified visibility of their brand and of their products/services, thanks to the Sponsor sheets published in the Annex C of the Report (see §2.2), their logo on the cover and in the numerous presentations of the OAD results in the AIPSI various events and webinars. Visibility accentuated by **an immediate "time to market"** with those who have a negative

assessment of the digital security level, and have immediately the references of the sponsoring companies which can help in the hardening the digital security level of the information system.

The sponsorship contributes also actively to support the only Italian online survey via web on digital security and make Sponsor company and their brands known to the thousands of AIPSI interlocutors who read the reports and articles on OAD, and who participate in the various events of the association: all potential customers of the Sponsors.
The AIPSI events help the diffusion of the OAD data and, above all, their circulation in the qualified business communities of decision makers and "ICT influencers". All this allows Sponsors to obtain large visibility.

6. OAD 2025 SPONSORSHIP

AIPSI allows the following types of sponsorships:

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 2025 OAD Report;
   b) **one A4 page presentation of the Sponsor** in the Annex C of the 2025 Report (see §2.2), with institutional information and an highlights 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 2025** (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's logo on the OAD and AIPSI web pages to download the OAD 2024 Report; the promotion of the 2024 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 as Gold Sponsor;
   a. **two A4 pages** in its presentation in Annex C of the OAD 2025 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 2025”;
   b) the participation of a representative of the Sponsor at the Round Table of the (hybrid) webinar that will present the OAD 2025 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 2025 Report and on the AIPSI and OAD websites as Diamond Sponsor;
    b. **three A4 pages** in its presentation in Annex C of the OAD 2025 Report;
    c. the possibility of participating and collaborating in defining the questions and answers in the 2025 OAD questionnaire, if registration takes place by 15/02/2025;
    d. the possibility for a top manager of the Diamond Sponsor to participate in the AIPSI Board of Directors, suggesting/proposing specific initiatives;
    e. 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;
    f. 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.

7. THE INTELLECTUAL PROPERTY OF OAD 2025

The intellectual property and copyrights of the entire initiative OAD 2025, including the online questionnaire and the contents, figures and graphs of the OAD 2025 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 2025**.

8. HOW TO JOIN THE SPONSORSHIP OF OAD 2025

To join the sponsorship of OAD 2025, simply complete all the entries in the **membership form on page 13**, sign it by the person with signing powers, scan it and send the signed and scanned form by email as an attachment to **aipsi@gigapec.it**. After receiving the form, the applicant Sponsor will be contacted by telephone/e-mail, and the related invoice will then be issued by AIPSI.

8.1 Time frame available to sign up for the sponsorship

The time frame for signing this offer goes from January 2025 to June 2025, but practically it has the limit of **2-3 weeks before the OAD 2025 Report will be published**, so that the Sponsor's presentation sheet can be edited and inserted in the Attachment C, and its logo on the cover of the Report.

It is important to highlight that the sooner the Sponsor will confirm its sponsorship, the longer its logo and link will be visible and followed by visitors to the websites, social networks, events that will promote OAD 2025.

OAD 2024 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 2024 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***: .....

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