Service Provisions

Awareness Academy Service Provisions

Below you will find a detailed description of the services that can be used within the framework of the IT-Seal Awareness Academy. The service modules that are only included in selected packages are marked with corresponding badges. Additional bookable modules are marked as “optional”.

Lite | Basic | Professional | Premium

Detailed Description of the Service Modules

IT-Seal Awareness Engine

Basic | Professional | Premium

The IT-Seal Awareness Engine forms the technological core of your Awareness Academy in the Auto Pilot. It regularly evaluates the security behaviour of your participants and decides on this basis which groups of participants are to be trained and how. Each participant receives exactly as much training as necessary and at the same time as little as possible.

The “Employee Security Index” (ESI®) serves as the awareness indicator. At the start of the Awareness Academy, a target security level is defined (target ESI®). Based on this, the IT-Seal Awareness Engine decides in each three-month cycle which participant groups receive which further training measures, or which participant groups can take a break.

Possible training measures are described below and include among other things spear phishing simulations, e-training modules, short videos, awareness materials, classroom training and online seminars.

The IT Seal Awareness Engine also ensures that all participants are trained according to their needs. For example, spear phishing emails from the IT-Seal spear phishing engine build on each other in their level of difficulty. They are individually selected by the IT Seal Awareness Engine for each participant based on their current learning level.

The target ESI® differs depending on the package booked: “Basic” = 70, “Professional” = 80, “Premium” = 90.
The IT-Seal Awareness Engine is not available in the “Lite” package.

IT-Seal Spear-Phishing-Engine

Lite | Basic | **Professional** | Premium

The patented IT-Seal Spear-Phishing-Engine allows you to send spear-phishing emails in different difficulty levels.

Spear phishing simulations are particularly effective in changing the security behaviour of participants: Firstly, by creating an effect of "self-awareness", the mindset of "no one is going to attack me anyway" can be overcome. Secondly, phishing simulations offer the possibility to convey brief, relevant, learning content in the form of nano-learning: On the IT-Seal explanation page, the participant learns interactively how he could have recognised that this email was fake. Thirdly, a spear phishing simulation based on the IT-Seal Spear-Phishing-Engine facilitates the measurement of the current Employee Security Index (ESI®).

The IT-Seal Spear-Phishing-Engine automatically adapts realistic phishing scenarios to your company and your participants. For this purpose, spear phishing e-mails are sent in different levels of difficulty, in which, inter alia, high-quality spear phishing (à la Emotet / QBot) is realised with the simulation of falsified internal e-mail traffic. For this purpose, we use company-specific fake domains and imitated e-mail signatures. In addition, the spear phishing e-mails refer to the recipient's position, department and industry. File attachments and dynamic phishing links with various obfuscation techniques are used. The file attachments used are regularly checked for relevance and currently include .docm and .xlsm. In the test phase at the start of your project, we check together which attachments are suitable for your company. Of course, no third-party software is ever installed via our attachments. They only communicate with our server to register the opening of the attachment.

Spear phishing e-mails based on OSINT information are also possible[1] (see "OSINT analysis & OSINT phishing").

The engine is constantly updated with current attack scenarios, which are automatically integrated into your Awareness Academy.

OSINT Analysis & OSINT Phishing[1]

The OSINT analysis aims to examine the online presence of your company and the participating employees for information that could be used by attackers. The information found is then used by the IT-Seal spear phishing engine for particularly sophisticated attack simulations.

Company OSINT

Lite | Basic | **Professional** | Premium

Company profiles on the employer rating portal kununu (kununu.com) can be automatically searched for employee benefits for the company OSINT. On the other hand, other publicly accessible sources (e.g. website or social media) can also be used to obtain information about benefits. The benefits found, such as employee discounts, home office or canteen, are then used in realistic spear phishing simulations.

[1] OSINT phishing is available in German only.

Employee OSINT

Lite (optional) | Basic (optional) | Professional (optional) | Premium

IT-Seal exclusively searches publicly accessible sources that are predominantly used professionally for the attack potential check, The information found is evaluated as part of the attack potential analysis and a summary evaluation of the attack surface is created.

The following sources are included in the search:

- Linkedin.com
- Xing.com

Publicly accessible data sources that are used less for professional than predominantly for private purposes or are otherwise to be assigned to the private sphere are explicitly excluded from the search by IT-Seal. Information from the following websites, in particular, but not exclusively shall not be used:

- Facebook.com
- Instagram.com
- Twitter.com

Furthermore, the collection, or evaluation, of data within the meaning of Section 9(1) GDPR is explicitly excluded.

The search of the aforementioned publicly accessible sources for information essentially includes participant-related data, e.g. the number of contacts, former employers, interests, knowledge and hobbies.

The individual information that IT-Seal obtains from the search of the publicly available sources is explicitly not passed on to the Client, unless presented in the reporting.

The results of the data search are abstracted and processed for individualised attacks.

Spear-Phishing E-Mails: Level 1–3

Lite | Basic | Professional | Premium

The levels of spear phishing e-mails are based on standardised classifications: the higher the level, the more time an attacker needs. The automated selection of spear phishing e-mails is based on individual person, department, company and industry scenarios. Just like real attackers, they use, potentially dangerous links, fake login pages, macros and encrypted file attachments.

Proposal system for new scenarios

Lite | Basic | Professional | Premium

Let's develop the IT-Seal spear phishing engine further together by giving us your ideas for phishing scenarios for your company or industry. Our phishing experts check all suggestions for feasibility and difficulty level.

The submitted suggestions as well as current attacks in circulation are used to implement new phishing emails every month. These are automatically integrated in your Awareness Academy.

Individual Spear Phishing Mails

Lite (optional) | Basic (optional) | Professional (optional) | Premium

IT-Seal creates individual phishing e-mails for your awareness training, designed in line with your wishes. The “Premium” package includes three phishing e-mails individually designed for your organisation. This service can be booked as an option in all other packages.

IT-Seal explanation page: Most Teachable Moment

Lite | Basic | Professional | Premium

We deliver relevant learning content at the time the learning has the greatest effect, i.e. the moment the participant has fallen for a phishing email.

Nano-learning is used to teach how an e-phishing e-mail can be used on the interactive explanation page, with individual training content for the e-mail that has just been simulated. In that respect, clear signs of recognition as well as psychological tricks of the attackers are shown.

Branding included: By default, your logo is displayed on the explanation page to strengthen the users’ trust in the site. Furthermore, we also offer the possibility of customizing, so you have the opportunity to store your own texts and hyperlinks there.

Falsified login pages

Lite | Basic | Professional | Premium

Credential phishing uses fake login pages to check how many participants enter their login data on a fake website. Of course, no login data are ever forwarded to our servers during our phishing simulation. All packages include use of the three default login pages, based on Microsoft Login, SAP Netweaver and Dropbox.

The creation of a customer-specific login page based on an HTML template can be booked as an option.

Reporter Button Outlook Add-In

Lite | Basic | Professional | Premium

The IT Seal Reporter Button is an Outlook add-in for desktop and mobile. It simplifies the reporting process for real attacks while providing positive feedback for correctly detected phishing simulations. The internal IT support is relieved with supporting information and automated response processes. In the Awareness Manager, one can see how many of the simulated phishing e-mails have been reported by employees. The Reporter Button is available in German and English.

Technical requirements for usage: Outlook client version from at least 2021, Outlook Retail license from at least 2019 or Exchange Online / Office 365 as well as Outlook Web Access, Outlook for Macintosh and Mobile.

E-Training Modules

Lite (optional) | Basic | **Professional** | Premium

The IT-Seal e-training modules provide participants with basic information about various IT security awareness topics in an entertaining, clear and understandable way.

The training focuses on content that can be directly recognised and implemented by technical laypersons in everyday life. 1-3 learning modules are available in the form of interactive e-training sessions, short videos or PDF files for each topic. In addition, we also offer refresher modules to help participants recall the content they have already completed.

- **Interactive e-training sessions** are, at all times, divided into several modules of 2 to 10 minutes each (with the exception of the module on data protection, which is about 20 minutes long). The progress is saved so that each module can be worked on by the participant in a single or in several sessions.
- In the **short videos**, the motivation of the learners is addressed and increased in 60 to 90 seconds and individual learning objectives are repeated and deepened.
- Our **PDF's** contain supporting information for the e-trainings, which your employees can save for quick access or print out.
- To refresh the knowledge of your employees, we offer refresher modules, so-called **memo rays**. These briefly and clearly summarize the learning content of training modules that have already been completed.

Alongside the classic e-training sessions, our training portfolio also includes quizzes for testing knowledge – so called Quick Checks. Quick checks are rolled out as a follow-up to a training session and are designed to provide a fun way to check one's level of knowledge and refresh concepts that are in danger of being forgotten.

The language availability of the e-training modules is stated in the appendix.

The “Basic”, “Professional” and “Premium” packages contain all the content available at IT-Seal.
The e-training modules can be booked as an option in the “Lite” package.

Learning content can be rolled out either via IT-Seal's Security Hub or in a separate LMS.

Awareness Materials

Lite (optional) | Basic (optional) | **Professional** | Premium

The awareness materials are aimed at repeatedly drawing the attention of participants to important rules of IT security behaviour in everyday life. At the start of the Awareness Academy you will therefore receive a package of awareness posters, depending on the number of participants.

A basic level of awareness can be achieved and thus attention can be increased in everyday life with the help of awareness materials such as posters and flyers. Awareness materials are available in German only.

Online Seminars

Lite (optional) | Basic (optional) | Professional | Premium

Our experience has shown that in many cases supplementary training is an effective means of imparting knowledge and permanently improving security behaviour.

In online seminars, participants with special training needs are taught the basics of secure behaviour in the workplace by our awareness consultants. This includes the role of the participant in IT security, how attackers act (including live phishing), how to recognise attacks and how to protect oneself.

A social engineering awareness training course comprises an online seminar of 60 minutes. The number of participants is generally unlimited. Online seminars are available in German and English.

Classroom Training

Lite (optional) | Basic (optional) | Professional (optional) | Premium

In contrast to online seminars, our classroom trainings offer participants the opportunity to ask questions in a protected environment. Our awareness consultants can then respond to the participants' questions even more individually.

In classroom training, our awareness consultants teach participants with special training needs the basics of secure behaviour in the workplace. This includes the role of the participant in IT security, how attackers act (including live phishing), how to recognise attacks and how to protect oneself.

At the beginning of the workshop, each participant will receive training materials and a certificate upon completion of the workshop. The number of participants is limited to 20 for each training session. Classroom training is only available in Germany, in German or English. IT-Seal decides on a case-by-case basis whether a classroom training or an online seminar is most suitable for the project situation.

Individual Branding: Geared Towards Your Company

Lite | Basic | Professional | Premium

Adjusting the learning content in line your corporate branding strengthens the image of the participants and increases their trust in the content.

If you wish, we can adjust the Security Hub, including the e-training modules and awareness materials, in line with your corporate identity and adopt your colours and logo.

Individual Configuration: Geared Towards Your Employees

Lite | Basic | Professional | Premium

Configure the awareness training according to your individual ideas or add your own content: From the number of simulated e-mails (phishing intensity) to individual text elements in your e-training sessions.

Languages

Lite | Basic | Professional | Premium

Our **Phishing Simulation** is available in the following languages:

- German, Swiss German, English, French, Italian, Dutch, Turkish, Spanish, Hungarian, Polish, Portuguese, Romanian, Czech, Slovak and Chinese.

The IT-Seal **Explanation Page** is available in the following languages:

- German, English, French, Italian, Spanish, Turkish, Portuguese, Hungarian, Polish, Romanian, Chinese, Czech, Danish, Arabic, Croatian, Hindi, Japanese, Dutch, Norwegian, Swedish, Slovak and Russian.

The **Security Hub** is available in the following languages:

- German, Chinese, English, French, Italian, Polish, Portuguese, Romanian, Spanish, Czech, Turkish and Hungarian

The **Awareness Manager** is available in the following languages:

- German and English

All available languages are included in the packages.

The languages available for the E-Training modules can be found in the appendix "E-Training modules". All available languages are included in all packages.

Administration and Setup

Lite | Basic | Professional | Premium

Your personal awareness consultant supports you in successfully setting up your security awareness programme. This includes internal communication with stakeholders (data protection officer, staff or works council, IT support, participants, management), configuration of the project, support with whitelisting and test e-mails as well as various materials for internal announcement and data protection-friendly project implementation.

Security Hub

Lite | Basic | Professional | Premium

The Security Hub brings together the personal learning content of employees centrally and conveniently in one place. Employees are logged in automatically and do not have to remember any access data. They have access to their booked and assigned e-training and other learning content. The Security Hub saves all intermediate training statuses and employees can also view completed learning content at any time. Employees can also view a personalised evaluation of the phishing e-mails they have received from IT-Seal. The FAQ section also provides employees with information from our knowledge database. Employees can use the Security Hub to make use of their right of objection and adapt it flexibly.

Live Dashboard: Awareness Manager

Lite | Basic | Professional | Premium

The IT-Seal Awareness Manager gives you access to a dashboard that gives you an insight into the current status of the simulation and training progress and the current security behaviour of the participants at any time.

In the Awareness Manager, you can view phishing and e-training results in a secure environment, evaluate the current ESI® at company and group level, and share files in an encrypted manner. In addition, there is a whitelisting guide including an interactive whitelisting test. You can also unlock a phishing overview for IT support, where they can check whether a message reported as an attack is part of our phishing simulations or not.

Summary of the results and Recommendations for Action in Regular Reports

Lite | Basic | Professional | Premium

In addition to the live view in the IT-Seal Awareness Manager, interim reports are produced at 3-month intervals and presented by your personal Awareness Consultant. This includes evaluations according to user groups, the development of the ESI® over time and concrete recommendations for action for your company.

The results are broken down into the individual groups, but not into individual participants.

In-depth Analysis and Interpretation of the Results

Professional | Premium

Your Awareness Consultant examines the results in detail and develops in-depth insights into participant behaviour, the handling of fake login pages, the evaluation of managers, particularly effective psychological tricks as well as an industry benchmark.

When booking an OSINT analysis (Professional (Optional), Premium), you will be shown how strongly the participant groups are present in the publicly accessible sources.

Reports for the Management

Professional | Premium

As IT Security Officer, it is important to inform your contacts briefly and precisely about how the security level is currently developing and what progress you have been able to achieve.

With regard to reporting to the management/board, your personal Awareness Consultant will prepare an adapted report with the results and progress as well as specific next steps every 3 months.

Reports for Team Leaders and Managers

Premium

Team leaders and managers are seen as multipliers for the security culture or they can also completely undermine it. To utilise the potential of the managers and strengthen the security culture, your awareness consultant prepares separate reports for the team leaders of the groups with a particular need to catch up. In this respect, both the departmental results and concrete tips for communicating with the team members are provided.

Company Certificate as Proof of Auditing According to ISO 27001

Lite | Basic | Professional | Premium

You receive a company certificate that can be used as proof for security audits (ISO27001, TISAX, BSI IT Basic Protection, …) and for customers.

Rules of Procedure Set Out in Writing

Lite (optional) | Basic (optional) | Professional (optional) | Premium

We provide you with a template for the documentation of your Rules of Procedure for your organisational handbook to meet the requirements of auditors. This documents when and how security behaviour is trained and what measures are taken in the case of a group of participants with a particular need to catch up.

CISO Workshop on Security Culture

Optional

In conjunction with an experienced specialist, a workshop is held once a year, as required, in which current challenges to the security culture are discussed and further recommendations for action to increase the security culture are developed.

Contaminated Data Storage Devices (USB sticks)

Lite (optional) | Basic (optional) | Professional (optional) | Premium

IT-Seal prepares USB sticks with a manipulated file and measures how often the file is opened. The USB sticks can be sent by post to persons/mailboxes selected by the Client. Alternatively, they are made available to the Client by IT-Seal to be placed on site by the Client. The “Premium” package includes 15 USB sticks per quarter for every 500 employees booked. In the other packages, scales of 15 USB sticks each can be booked.

Telephone Phishing Campaign (Vishing)

Lite (optional) | Basic (optional) | Professional (optional) | Premium

Vishing stands for “Voice Phishing” and is increasingly used by criminals to build up additional pressure and stress, for example in CEO fraud. We simulate this attack path to help you discover weak points in your company's security concept. If necessary, we train your employees, to close these vulnerabilities.

Like a real attacker, we simulate attacks by telephone and check, for example:

- Whether employees pass on access data and passwords
- Whether employees can be tricked into installing software or opening files
- Whether employees pass on personal data about themselves or their colleagues.

The “Premium” package includes 20 calls per quarter to selected target persons for every 1,000 employees booked. In the Lite, Basic, and Professional packages vishing calls can also be booked optionally. The dial attempts are limited to a number of 4 attempts per call. The resolution after a vishing call is optional. Here we resolve the situation and confirm the behaviour or give tips on how to deal correctly with vishing.

Social Engineering Site Visit

Lite (optional) | Basic (optional) | Professional (optional) | Premium

The social engineering site visit is an on-site inspection at the customer's premises. A social engineering specialist conducts an inspection of the customer's object and checks the customer's technical organizational security concept. This involves a systematic search, from the outside in, for possible weak points that a social engineer could use to gain access to the company and then to security areas, IT, production or other neuralgic areas.

The on-site visit lasts approximately 6-8 hours. After the execution of the inspection, the social engineering inspector prepares a report on the identified potential vulnerabilities and makes recommendations for further actions. If more than one object is involved or if this object is too large for a one-day walk-through, another day may be necessary.

The social engineering inspection is included in the "Premium" package for 30 employees or more once a year.

Social Engineering Penetration Test

Lite (optional) | Basic (optional) | Professional (optional) | Premium (optional)

The aim of the penetration test is to examine the physical and technical-organizational security measures of an object from the perspective of an attacker. Possible identified weaknesses are tested for vulnerability using a simulated attack scenario.

The outcome of the penetration test is presented to you in a report. The results are anonymized so that neither names nor photos of persons appear.

Our approach

The approach to physical social engineering penetration is divided into four phases:

1. OSINT (Open Source Intelligence) and Basic Exploration

The purpose of the OSINT and basic exploration phase is to provide a basic overview of the possible objects of attack and possible methods of attack. The phase aims to find suitable access points to the target object as well as determine a method of attack, so that detailed planning can begin in the following phase.

We conduct OSINT as follows:

- Evaluation of information provided by the client on their own websites, blogs and social media etc.
- Identification of employees of the target organisation in business social networks.
- Collecting newspaper articles on current issues, framework agreements, events and campaigns of the organisation.
- Researching external companies to support the target organisation (suppliers, technical support and facility management, etc.)

We carry out basic exploration as follows:

- Exploration of the surrounding area of possible target objects and access points.
- Exploration of the immediate area, with documentation of the infrastructure and security measures at the property
- Inspection of the target properties in a defined way
- Observation of suitable target objects, with the aim of obtaining information about the daily routine (where do colleagues spend their breaks together, their evening work, delivery services, cleaning staff and maintenance companies etc.)?
- Documented approach of possible target persons

2. Specific Exploration and Education

The Specific Exploration and Clarification phase is the main focus of the preparations. In this respect, specific exploration is carried out for the selected method and information is provided on and in the object. Possible access points are identified and documented. Connections to persons are established if required by the method of attack.

Possible methods of attack:
(Wishes/restrictions can be taken into account after consultation)

Person:

- Identification of target persons
- Addressing and establishing contact
- Creating common ground (rapport)
- Build up legend

Third party company:

- Identifying the company
- Addressing the third-party company in a defined way
- Collect information (names, access authorisation and in-processing procedure)
- Photographing of work clothes etc.

Self-infiltration:

- Legend as third-party company
- Place advertisement
- Act as applicant
- Act as a parcel service
- Request information
- And much more.

Authorised access:

- Obtain access by initiating employees.
- Requesting access in a defined manner (e.g. occupational health and safety inspection)
- Disrupting the internet and posing as an internet/telephone technician
- Use fake access authorisation

3. Attack

The attack is carried out on the basis of the knowledge gained in the previous phases. At this stage, the exact procedure, targets, persons, times and habits are known.

The following specifics should be considered during the attack:

- Hardly any attack can be planned 100%. Therefore, the tester's creativity and flexibility are required.
- If desired, the attacks are documented with cameras in order to later generate information from conversations and the video material.
- Highly classified and internal information of the target organisation can be used after consultation.

The attack can be supported in various ways, depending on the method used.

These include:

- Wire-tapping (by arrangement)
- Elicitation technique (by arrangement)
- False statements
- Disrupting internet connections with the help of jammers (by arrangement)

4. Evaluation, Presentation and Training

The Evaluation, Presentation and Training phase forms the conclusion of the penetration test. In an internal process, the execution of the attack is reconciled with the planning basis and compared with the results of other tests. A documentation of the work steps is presented to the customer. The presentation to the client is comprehensive, under the premise of being able to provide the client with a detailed picture of the detected situation.

Our standards in the phase evaluation, presentation & training

Evaluation:

- Each attack is documented in writing in a situation description
- All identified weak points are evaluated
- Each object is additionally evaluated individually
- Exploration = attack
- Psychological evaluation of the exploited human weaknesses

Presentation:

- The report is handed over to the client without the names of the tested target persons, unless otherwise discussed
- Image and sound material is destroyed after the test but can be viewed by the Customer beforehand if desired
- At the Customer's request, the results of the penetration test can be presented as a lecture

Training: Half-day workshop following completion of the tests (optional)

In a concluding half-day workshop, the lessons learned from the penetration test are discussed with a group of persons to be determined and further conclusions/measures are discussed.

Contract for order data processing

In addition to the present offer, the parties enter into a contract providing for the order data processing in accordance with data protection law.

Individual Opt-Out Solutions

Lite | Basic | Professional | Premium

To make the processes data protection-friendly, your employees have various options to object to certain measures. This gives you the opportunity to meet each participant individually and as desired and counteract possible concerns.

Reference

The Client agrees that his name may be mentioned by IT-Seal as a reference client and that his logo may be used on the website and advertising materials as a reference.

Data Protection, Obligation to Maintain Secrecy

The parties agree that protection of employees must play a central role. Anonymised results and data shall be forwarded to the Client. The information collected during the social engineering awareness measures will be stored in abstract form.

The Client undertakes to use all working documents made available for using of this offer only for internal company use, not to pass them on to third parties and not to pass on any content relating to the subject matter of the offer to third parties in any form.

Appendix: Content listing of our available languages

E-Training modules

Topic	Qty. Modules	Languages (ISO-639-1)	Languages - planned
IT and me: An introduction	1	DE, EN, FR, CS, PL, IT, TR, ES, ZH, PT, JA, RO, HU	
Social Engineering	1	DE, EN, FR, CS, PL, IT, TR, ES, ZH, PT, JA, RO, HU	
E-mail security	1	DE, EN, FR, CS, PL, IT, TR, ES, ZH, PT, JA, RO, HU	
Passwords and authentication	1	DE, EN, FR, CS, PL, IT, TR, ES, ZH, PT, JA, RO, HU	
Social media	1	DE, EN, FR, CS, PL, IT, TR, ES, ZH, PT, JA, RO, HU	
Vishing (telephone phishing)	1	DE, EN, FR, CS, PL, IT, TR, ES, ZH, PT, JA, RO, HU	
Secure in the Home Office	1	DE, EN, FR, CS, PL, IT, TR, ES, ZH, PT, JA, RO, HU	
Data protection	1	DE, EN, FR, CS, PL, IT, TR, ES, ZH, PT, JA, RO, HU	
Protection classes	2	DE, EN	FR
Reporting incidents	3	DE, EN	FR
Mobile security	2	DE, EN	FR
Information secure on the Internet	2	DE, EN	FR
Reporter button	1	DE, EN	
Macros	1	DE, EN, FR[2]	
Falsified login pages	1	DE, EN, FR[2]	
Setting an example of information security as a leader	1	DE, EN, FR[2]	

[2] French subtitles

Quick checks

Topic	Languages (ISO-639-1)	Languages - planned
IT and me	DE, EN	
Passwords and authentication	DE, EN	
Protection classes	DE, EN	
E-mail security	DE, EN	

Memo rays (refresher modules)

Topic	Languages (ISO-639-1)	Languages - planned
Vishing	DE, EN	
Phishing	DE, EN	