IT-SEAL
Part of HORNETSECURITY group

IT SECURITY
MADE IN GERMANY

Awareness Academy

Together for a sustainable security culture

Feature overview

demo.it-seal.de
Your personal registration for the phishing awareness simulation and your E-Learning test access

Made with ♡ in Security Valley Darmstadt

Academy feature details

Feature overview of the Awareness Academy packages

The Awareness Academy offers you an all-round carefree service to establish a sustainable security culture. The main differences between the Basic, Professional and Premium packages lie in the level of the targeted ESI® and the training measures required to achieve it. In the Lite package, only your current security level is measured once or on an ongoing basis and reported. There is no target agreement using Target ESI® for this, as you are already taking your own measures to train and raise awareness of IT security among your employees.

It is possible to switch between the packages. You will find a detailed description of the services in the attached service provisions.

ESI® and Target ESI® (Employee Security Index)

	Measure once or permanently	Measure & train permanently		
Features	**Lite**	**Basic**	**Professional**	**Premium**
ESI® and Target ESI® (Employee Security Index): Your Benchmark The ESI® is a scientific benchmark to measure security culture across industries. With the Target ESI®, you choose your security level, which is a common target agreement. This involves training each group based on metrics and needs. When a group reaches the Target ESI®, training can be paused before the ESI® is measured again. Groups that need more support receive more assistance through additional training. As a KPI, the ESI® benchmarks you against companies of the same industry and size.	ESI®	70 Target ESI®	80 Target ESI®	90 Target ESI®

Awareness Engine

Features	**Lite**	**Basic**	**Professional**	**Premium**
Awareness Engine: Our technological heart The Awareness Engine is our technological heart and provides the live analysis of the security behavior of your participants. It is always active, with individual groups active or paused. Based on the target ESI®, it decides which groups receive which training at which time. Each participant group therefore obtains just as much training as necessary, but at the same time as little as possible.		✓	✓	✓
Training PLUS-Option **Single User Booster:** Participants with additional learning needs are trained more intensively, even if they belong to groups that are already at a good security level. **Productivity Booster:** Conversely, participants receive reduced training if they are already at a good security level - regardless of their group.			✓	✓
Full-Service by our awareness experts Structured communication with stakeholders is the key to a sustainable security culture. Your personal awareness consultant will support you with best practices from hundreds of successful customers in setting up and maintaining your security awareness program. This includes internal communication with stakeholders (employees, management, works or staff council, data protection officers, IT support), configuration of the project, support with whitelisting and test mails as well as material for internal announcements.	✓	✓	✓	✓

Academy feature details

Awareness Engine

	Measure once or permanently	Measure & train permanently		
Features	**Lite**	**Basic**	**Professional**	**Premium**
Security Hub: One-Stop-Shop for training & communication To ensure an optimal learning effect, we need a convenient and consistent learning experience. The Security Hub combines your employees' personal e-training in one central location. We focus on individual learning paths because we know how each individual learns. Employees can access their e-training sessions from any location and review their own phishing scenarios. Your employees are automatically logged in via Magic link and do not have to remember any access data.	✓	✓	✓	✓
"Most Teachable Moment": Awareness at the right moment The „Most Teachable Moment" is a valuable pedagogical and didactical moment for effective learning and for informing employees about potentially harmful misconduct. For example, an interactive explanation page uses the actual phishing e-mail clicked to show what to look out for and what psychological trick was used in the process.	✓	✓	✓	✓
Interactive e-trainings that are fun to use IT-Seal e-trainings provide participants with entertaining, easy-to-understand content on security culture, information security and data protection in the form of e-learning sessions, short videos and most teachable moments.	optional	✓	✓	✓
Company certificate as proof for ISO 27001, etc. You will receive a company certificate as proof for security audits (IS027001, TISAX, BSI IT-Grundschutz, ...) and for customers. Employees can also download certificates of participation from the Security Hub.	✓	✓	✓	✓
Individual branding: customized for your company Adapting the e-training, the Security Hub and the notification e-mails to your corporate branding strengthens your image among employees. In addition, the explanation page with your company logo prevents any feelings of mistrust.	✓	✓	✓	✓
Customized configuration: Adapted to your employees Configure the awareness training according to your individual requirements or add your own content: From the number of simulated emails (phishing intensity) to individual text elements in your e-trainings.	✓	✓	✓	✓
Online seminars & „Stay alert!" awareness material In interactive online seminars, participants are taught the basics of secure behavior in the workplace by an awareness coach. With the help of awareness materials, such as posters and flyers, a basic awareness can be achieved and thus the attention in everyday life can be increased.	optional	optional	✓	✓
Face-to-face training & social engineering site visits In face-to-face training sessions, participants are taught the basics of secure workplace behavior in person at your site. For the social engineering penetration test, we assume the role of an attacker and check how vulnerable your site is.	optional	optional	optional	✓
Phone attacks (vishing) & manipulated USB sticks With fake telephone attacks, we try to obtain sensitive information or instruct payments. We inform the affected employees directly and sensitively. Manipulated USB sticks are used as another attack vector.	optional	optional	optional	✓

Patented Spear-Phishing-Engine

	Measure once or permanently	Measure & train permanently		
Features	**Lite**	**Basic**	**Professional**	**Premium**
Patented Spear Phishing Engine: The Best Phishing Simulation Based on freely available information, our patented Spear Phishing Engine generates individually tailored phishing attacks (spear phishing/dynamite phishing). This is fully automated: Each employee recieves individual scenarios at individual points in time.	✓	✓	✓	✓
Company OSINT: Open Source Intelligence Our company OSINT searches your website, job portals, employer rating portals or professional social networks for individual company characteristics. The information obtained serves as the basis for company-specific spear phishing e-mails.	✓	✓	✓	✓
Employee-OSINT: Open-Source-Intelligence Our employee-OSINT searches professional social networks for usable information. We collect information from your employees who have not set their privacy settings correctly. The obtained information is used as a basis for employee-specific spear phishing emails.	optional	optional	optional	✓
Spear phishing mails: Level 1–3 The level of our spear phishing mails is based on standardized classifications (the higher the level, the greater the time required by an attacker). The automated selection of spear phishing mails is based on individual person, department, company, and industry scenarios. Just like real attackers, they use potentially dangerous links, fake log ins, pages and macros.	✓	✓	✓	✓
Outlook-Add-In: Reporter Button The Reporter Button serves as a reporting tool and simplifies the reporting process for real attacks. It also provides positive feedback for detected phishing simulations.	✓	✓	✓	✓
Custom spear phishing emails We create phishing emails that are individually designed according to your specific needs.	optional	optional	optional	✓

Employee friendliness & data protection

Features	**Lite**	**Basic**	**Professional**	**Premium**
Security and Privacy by Design Collaboration and data protection are paramount, which is why the results of the phishing simulation are always analyzed on a group basis. From the very beginning, our process and database structures have been created according to the principle of „Security and Privacy by Design“.	✓	✓	✓	✓
Respectful and sensitive communication From the beginning, we have understood that we need to involve all employees step by step, communicating in a respectful and sensitive manner. Together with your employees, we want to work on achieving the goal of a sustainable security culture.	✓	✓	✓	✓
Individual opt-out solutions In order to make processes as data protection-friendly as possible, your employees can opt out of certain measures via the Security Hub. This gives you the opportunity to address each participant individually and in line with their wishes.	✓	✓	✓	✓

Made with ♡
in Security Valley Darmstadt

IT-SEAL
Part of **HORNETSECURITY** group