IT-SEAL
Part of HORNETSECURITY group

IT SECURITY
MADE IN GERMANY

Awareness Academy

Gemeinsam zur nachhaltigen Sicherheitskultur

Featureübersicht

demo.it-seal.de
Anmeldung zu Ihrer persönlichen Phishing Awareness-Simulation und Ihrem E-Learning-Testzugang

Made with ♡ in Security Valley Darmstadt

Academy-Features im Detail

Featureübersicht der Awareness Academy Pakete

Die Awareness-Academy bietet Ihnen einen Rundum-Sorglos-Service, um eine nachhaltige Sicherheitskultur zu etablieren. Die Hauptunterschiede der Leistungspakete Basic, Professional und Premium liegen in der Höhe des anvisierten Ziel-ESI® sowie den dafür notwendigen Trainingsmaßnahmen. Im Paket Lite wird lediglich Ihr aktuelles Sicherheitslevel einmalig oder fortlaufend gemessen und reported. Eine Zielvereinbarung mittels Ziel-ESI® ist dafür nicht vorgesehen, da Sie bereits eigene Maßnahmen unternehmen, um Ihre Mitarbeitenden in Sachen IT-Sicherheit zu schulen und zu sensibilisieren. Ein Wechsel zwischen den Paketen ist möglich. Die detaillierte Beschreibung der Leistungen finden Sie in den Leistungsbestimmungen.

ESI® und Ziel-ESI® (Employee Security Index)

	Einmalig oder dauerhaft messen	Dauerhaft messen & trainieren		
Features	**Lite**	**Basic**	**Professional**	**Premium**
ESI® und Ziel-ESI® (Employee Security Index): Ihr Benchmark Der ESI® ist ein wissenschaftlicher Benchmark, um die Sicherheitskultur branchenübergreifend messen zu können. Mit dem Ziel-ESI® wählen Sie Ihr Sicherheitsniveau, das als gemeinsame Ziel-Vereinbarung gilt. Dabei wird jede Gruppe kennzahlenbasiert und bedarfsgerecht trainiert. Erreicht eine Gruppe den Ziel-ESI®, kann das Training pausiert werden, bevor der ESI® erneut gemessen wird. Gruppen, die mehr Unterstützung benötigen, erhalten mehr Hilfestellung durch zusätzliche Trainings. Als KPI benchmarkt Sie der ESI® im Vergleich zu Unternehmen derselben Branche und Größe.	ESI®	70 Ziel-ESI®	80 Ziel-ESI®	90 Ziel-ESI®

Awareness Engine

Features	Lite	Basic	Professional	Premium
Awareness Engine: Unser technologisches Herzstück Die Awareness Engine ist unser technologisches Herzstück und wertet live das Sicherheitsverhalten Ihrer Teilnehmer aus. Sie ist immer aktiv, wobei einzelne Gruppen aktiv oder pausiert sind. Sie entscheidet auf Basis des Ziel-ESI®, welche Gruppen welches Training zu welchem Zeitpunkt erhalten. Jede Teilnehmer-Gruppe erhält dadurch genau so viel Training wie nötig, aber gleichzeitig so wenig wie möglich.		✓	✓	✓
Training PLUS-Option *Single User Booster:* Teilnehmer mit zusätzlichem Lernbedarf werden intensiver trainiert, auch wenn sie zu Gruppen gehören, die bereits auf einem gutem Sicherheitslevel sind. *Productivity Booster:* Umgekehrt erhalten Teilnehmer ein reduziertes Training, wenn sie bereits auf einem guten Sicherheitslevel sind – unabhängig von ihrer Gruppe.			✓	✓
Full-Service durch unsere Awareness-Expert:innen Die strukturierte Kommunikation mit den Stakeholdern ist der Schlüssel zu einer nachhaltigen Sicherheitskultur. Dabei unterstützt Sie Ihr persönlicher Awareness Consultant mit Best Practices von hunderten erfolgreichen Kunden bei der Einrichtung und Pflege Ihres Security-Awareness-Programms. Dazu gehört die interne Kommunikation mit den Stakeholdern (Mitarbeiter:innen, Geschäftsführung, Betriebs- oder Personalrat, Datenschutzbeauftragte, IT-Support), die Konfiguration des Projekts, Unterstützung beim Whitelisting und bei Testmails sowie Material zur internen Ankündigung.	✓	✓	✓	✓

Academy-Features im Detail

Awareness Engine

	Einmalig oder dauerhaft messen	Dauerhaft messen & trainieren		
Features	**Lite**	**Basic**	**Professional**	**Premium**
Security Hub: One-Stop-Shop für Training & Kommunikation Damit wir am besten lernen, benötigen wir eine bequeme und konsistente Lernerfahrung. Der Security Hub fasst die persönlichen E-Trainings Ihrer Mitarbeiter:innen zentral an einem Ort zusammen. Dabei setzen wir auf individuelle Lernpfade, denn wir wissen, wie individuell jeder Einzelne lernt. Mitarbeiter:innen können ihre E-Trainings an jedem Ort aufrufen und die eigenen Phishing-Szenarien Revue passieren lassen. Ihre Mitarbeiter:innen werden automatisch per Magic Link eingeloggt und müssen sich keine Zugangsdaten merken.	✓	✓	✓	✓
"Most Teachable Moment": Aufklärung im richtigen Moment Der „Most Teachable Moment" ist pädagogisch und didaktisch ein wertvoller Moment, um besonders effektiv zu lernen und Mitarbeiter:innen über das potenziell schadhafte Fehlverhalten aufzuklären. Beispielsweise zeigt eine interaktive Erklärseite anhand der tatsächlich geklickten Phishing-Mail auf, worauf zu achten ist und welcher psychologische Trick angewendet wurde.	✓	✓	✓	✓
Interaktive E-Trainings, die Spaß machen Das IT-Seal E-Training vermittelt Teilnehmern unterhaltsam, kurzweilig und verständlich Inhalte zu Sicherheitskultur, Informationssicherheit und Datenschutz in Form von E-Learnings, Kurzvideos, Quick-Checks und Most-Teachable-Moments.	optional	✓	✓	✓
Unternehmenszertifikat als Nachweis für ISO 27001 u.ä. Sie erhalten ein Unternehmenszertifikat, das als Nachweis für Sicherheitsaudits (ISO27001, TISAX, BSI IT-Grundschutz, etc.) und für Kunden dient. Weiter erhalten Mitarbeiter:innen Teilnahmezertifikate im Security Hub zum download.	✓	✓	✓	✓
Individuelles Branding: Auf Ihr Unternehmen angepasst Die Anpassung des E-Trainings, des Security Hubs und der Benachrichtigungs-Mails an Ihr Unternehmensbranding stärkt das Image bei den Mitarbeiter:innen. Zusätzlich erhält die Erklärseite Ihr Unternehmenslogo, um Misstrauen vorzubeugen.	✓	✓	✓	✓
Individuelle Konfiguration: Auf Ihre Mitarbeiter:innen angepasst Konfigurieren Sie das Awareness-Training nach Ihren individuellen Vorstellungen oder ergänzen Sie eigene Inhalte: Von der Anzahl der simulierten E-Mails (Phishing-Intensität) bis hin zu individuellen Textelementen in Ihren E-Trainings.	✓	✓	✓	✓
Online-Seminare & „Bleib wachsam!"-Awareness-Material In interaktiven Online-Seminaren bekommen Teilnehmer:innen die Grundlagen sicheren Verhaltens am Arbeitsplatz durch einen Awareness-Coach vermittelt. Mit Hilfe der Awareness-Materialien, wie Poster und Flyer, kann ein Grundbewusstsein erreicht und somit die Aufmerksamkeit im Alltag erhöht werden.	optional	optional	✓	✓
Präsenzschulungen & Social-Engineering-Standortbegehung In Präsenzschulungen erhalten Teilnehmer:innen die Grundlagen sicheren Verhaltens am Arbeitsplatz persönlich bei Ihnen vor Ort vermittelt. Für den Social-Engineering-Penetrationstest nehmen wir die Rolle eines Angreifers ein und prüfen, wie angreifbar Ihr Standort ist.	optional	optional	optional	✓
Telefonangriffe (Vishing) & manipulierte USB-Sticks Mit gefakten Telefonangriffen versuchen wir sensible Informationen herauszufinden oder Zahlungen anzuweisen. Dabei klären wir die betroffenen Mitarbeiter:innen direkt und sensibel auf. Manipulierte USB-Sticks werden als weiterer Angriffsvektor eingesetzt.	optional	optional	optional	✓

Patentierte Spear-Phishing-Engine

	Einmalig oder dauerhaft messen	Dauerhaft messen & trainieren		
Features	**Lite**	**Basic**	**Professional**	**Premium**
Patentierte Spear-Phishing-Engine: Die beste Phishing-Simulation Auf Basis frei verfügbarer Informationen generiert unsere patentierte Spear-Phishing-Engine individuell zugeschnittene Phishing-Angriffe (Spear-Phishing/Dynamite Phishing). Dies erfolgt vollautomatisiert: Jeder Mitarbeiter:in erhält zu individuellen Zeitpunkten individuelle Szenarien.	✓	✓	✓	✓
Unternehmens-OSINT: Open-Source-Intelligence Unser Unternehmens-OSINT durchsucht Ihre Website, Jobportale, Arbeitgeberbewertungsportale oder berufliche Soziale Netzwerke nach individuellen Unternehmensmerkmalen. Die gewonnenen Informationen dienen als Grundlage für unternehmensspezifische Spear-Phishing-Mails.	✓	✓	✓	✓
Mitarbeiter-OSINT: Open-Source-Intelligence Unser Mitarbeiter-OSINT durchsucht berufliche Soziale Netzwerke nach verwertbaren Informationen. Dabei sammeln wir Informationen Ihrer Mitarbeiter:innen, die ihre Datenschutzeinstellungen nicht korrekt gesetzt haben. Die gewonnen Informationen dienen als Grundlage für mitarbeiterspezifische Spear-Phishing-Mails.	optional	optional	optional	✓
Spear-Phishing-Mails: Level 1–3 Die Level unserer Spear-Phishing-Mails basieren auf standardisierten Einteilungen (je höher das Level, desto höher der Zeitaufwand eines Angreifers). Die automatisierte Auswahl der Spear-Phishing-Mails erfolgt über individuelle Personen-, Abteilungs-, Unternehmens- und Branchenszenarien. Sie nutzen genau wie echte Angreifer potenziell gefährliche Links, gefälschte Login-Seiten und Makros.	✓	✓	✓	✓
Outlook-Add-In: Reporter Button Der Reporter Button dient als Melde-Tool und vereinfacht den Meldeprozess für reale Angriffe. Er liefert zudem eine positive Rückmeldung für erkannte Phishing-Simulationen.	✓	✓	✓	✓
Individuelle Spear-Phishing-Mails Wir erstellen Phishing-Mails, die nach Ihrem Wunsch individuell konzipiert sind.	optional	optional	optional	✓

Mitarbeiterfreundlichkeit & Datenschutz

Features	**Lite**	**Basic**	**Professional**	**Premium**
Security and Privacy by Design Der Mitarbeiter- und Datenschutz steht im Vordergrund, weshalb die Ergebnisse der Phishing-Simulation stets gruppenbasiert ausgewertet werden. Unsere Prozess- und Datenbankstrukturen sind von Anfang an nach dem Prinzip „Security and Privacy by Design“ entwickelt worden.	✓	✓	✓	✓
Respektvolle und sensible Kommunikation Wir haben von Anfang an verstanden, dass wir alle Mitarbeiter:innen Schritt für Schritt abholen müssen und dabei respektvoll und sensibel kommunizieren. Gemeinsam mit Ihren Mitarbeiter:innen möchten wir an einem Strang ziehen und das Ziel einer nachhaltigen Sicherheitskultur erreichen.	✓	✓	✓	✓
Individuelle Opt-Out-Lösungen Um die Prozesse so datenschutzfreundlich wie möglich zu gestalten, können Ihre Mitarbeiter:innen über den Security Hub bestimmten Maßnahmen widersprechen. Dadurch erhalten Sie die Möglichkeit, jeden Teilnehmer individuell und wunschgerecht abzuholen.	✓	✓	✓	✓

Wir freuen uns auf ein persönliches Gespräch mit Ihnen!

Tel.: 06151 862 70 00
E-Mail: kontakt@it-seal.de

IT-Seal GmbH | Hilpertstr. 31 | 64295 Darmstadt | www.it-seal.de

Made with ♡ in Security Valley Darmstadt

IT-SEAL
Part of HORNETSECURITY group