Feature-Übersicht unserer Awareness-Pakete

SoSafe
Cyber Security Awareness

Alle Pakete werden als Jahreslizenz verkauft.
Die Kosten richten sich nach Anzahl der zu schulenden Nutzer sowie dem gewünschten Leistungsumfang.
Gerne beraten wir Sie zu dem am besten passenden Paket.

(S) Starter

Basis-Absicherung zu den Grundlagen der IT-Sicherheit

(B) Business

Effektive IT-Sicherheitsschulung für den Mittelstand

(E) Enterprise

Umfassendes Awareness-Training inkl. Simulation zielgerichteter Angriffe

(P) Premium

Full-Service-Lösung mit passgenauem Content und Aussehen

✓ inkludiert ○ optional

Konfiguration & Auswertung	S	B	E	P	
Setup via Self-Service	✓				Kundenseitige Konfiguration der Kampagne (Auswahl aus Vorlagen) und Umsetzung der technischen Voraussetzungen (Anleitungen werden bereitgestellt).
Setup-Unterstützung durch SoSafe		✓	✓	✓	Beratung bei Konfiguration, Unterstützung beim Einrichten technischer Voraussetzungen (Whitelisting), Bereitstellung Kommunikationsvorlagen, Nutzermanagement (Zu-/Abgänge) & Datenqualitätssicherung.
Auswertung	✓	✓	✓	✓	Zugriff auf SoSafe Manager Portal mit Reporting-Dashboard zur Auswertung aller Kennzahlen (z.B. Klickrate in der Phishing-Simulation, Absolvierungsrate beim E-Learning).
Auswertung nach Nutzergruppen		✓	✓	✓	Auswertung der Kennzahlen nach Nutzergruppen.
ISO 27001 Reporting			✓	✓	Konforme Auswertung für ein ISO 27001 Audit.
Experten-Auswertung				✓	Detailliertere Auswertungsmöglichkeiten nach multiplen Nutzermerkmalen (z.B. Standort, Landesgesellschaft, Funktion, Hierarchiestufe).
Benchmarking		✓	✓	✓	Benchmarking (alle Kennzahlen der Standard-Auswertung) im Vergleich zum Durchschnitt aller Kunden.
Experten Benchmarking			✓	✓	Weitere Benchmarks (Branche, Unternehmensgröße).
Datenexport		✓	✓	✓	Möglichkeit zum Export der Auswertungsdaten der Phishing-Simulation (CSV-Datei).
Nutzerfeedback		✓	✓	✓	Anzeige des Feedbacks der Nutzer sowie Möglichkeit zum Export als CSV-Datei.
Monitoring & Beratung			✓	✓	Überwachung der Awareness-Maßnahme und Bereitstellung von Handlungsempfehlung aufgrund der Daten.
Endnutzer-Support (E-Mail und Nutzerportal)	✓	✓	✓	✓	Schnelle, unkomplizierte Hilfe bei Fragen Ihrer Endnutzer via Wissensdatenbank. E-Mail-Support gemäß unseres SLA.
Admin-Support (E-Mail oder Telefon)	✓	✓	✓	✓	Support für Administratoren via E-Mail oder Telefon gemäß unseres SLA.
Phishing-Simulation					
Phishing-Simulation (Best-Practice-Paket à 12 Templates)	✓	✓	✓	✓	Versand von 12 Phishing-Mails aus unseren Best-Practice-Paketen (passgenau für Ihre Branche und mit individueller Ansprache je Nutzer). Randomisierter Versand über das Jahr hinweg zu definierten Geschäftszeiten.
Spear-Phishing-Simulation (+ 3 individuelle Templates)			✓	✓	Zusätzlich 3 individuell für das Kundenunternehmen erstellte Phishing-Templates (z.B. Nachbildung CEO-Fraud) für die Phishing-Simulation.
Expertenkonfiguration Simulation			✓	✓	Anpassungen der Versandzeiten, z.B. Einplanung von Pausen wegen Urlaub, Berücksichtigung von Zeitzonen.
Branding Lernseiten			✓	✓	Anpassungen der edukativen Aufklärungs-/Lernseiten: Logo, Aufklärungstext, Farbgebung.
Differenzierte Ausspielung				✓	Gezieltes Training durch Zuordnung ausgewählter Phishing-Mail-Templates zu spezifischen Nutzergruppen.
E-Learning					
Zugriff SoSafe Lernplattform	✓	✓	✓	✓	Zugriff auf die SoSafe Lernplattform für alle Nutzer.
Kontinuierliche Updates	✓	✓	✓	✓	Fortlaufende inhaltliche Aktualisierung der Lernmodule auf den neuesten Stand der Best Practices im Cyber Security Bereich.
Lernvideos	6	6	6	6	Awareness-Videos à jeweils ca. 3 Minuten.
Interaktive Lernmodule	6	10	20	20	Vertiefende, interaktive Lernmodule à 4-8 Minuten jeweils mit kurzem Abschlussquiz (4 Fragen).
Zertifikat		✓	✓	✓	Zertifikat über alle bestandenen Lernmodule (nur verfügbar bei Nutzung des E-Learnings über die SoSafe Lernplattform).
SCORM-Streaming			✓	✓	Zugriff auf Lernvideos und vertiefende Lernmodule als SCORM-Container zur Einbindung in ein kundeneigenes Learning-Management-System.
Einschätzungstest			✓	✓	Fragebogen zur Ersteinschätzung des Wissenstandes jedes einzelnen Nutzers.
Optionale Features					
Phishing-Melde-Button		○	○	✓	Office Add-In für Exchange 2016 oder Office 365 (siehe SLA) für zusätzliche Schaltfläche in Outlook zur Meldung verdächtiger E-Mails an definiertes Postfach beim Kunden.
Internationales Paket (14 Sprachen verfügbar)		○	○	○	12 fixe Best-Practice Templates und Lernseiten, alle Lerninhalte (Lernvideos, vertiefende Lernmodule) sowie Phishing-Melde-Button in den verfügbaren, weiteren Sprachen.
Platzhalter im E-Learning		○	○	✓	In die E-Learning Inhalte werden über Platzhalter kundenspezifische Regelungen und Richtlinien integriert, z.B. Vorgaben zur Mindestlänge von Passwörtern.
Branding des E-Learnings		○	○	✓	Die E-Learning Inhalte, die Lernplattform und das Zertifikat werden im Stile Ihrer Corporate Identity (Logo und Farben) zur Verfügung gestellt.
Weitere Sprachen für 3 individuelle Templates für Spear-Phishing-Simulation			○	○	Übersetzung der 3 individuellen Templates und der Lernseiten in eine weitere Sprache.
Ausgedruckte Poster (Offline Paket)		○	○	○	Druckvorlagen für Poster, Screensaver; keine kundenspezifischen Anpassungen; Druck und Versand der Poster an bis zu 5 unterschiedliche Adressen.
Single-Sign-On		○	○	○	Single-Sign-On für Microsoft Azure AD oder Google G Suite.
Voice-Phishing / Vishing-Simulation		○	○	○	Automatisierte Simulation von Attacken per Telefon.

Unsere E-Learning-Module umfassen unter anderem Themen wie Passwörter, Spam & Phising, Apps, Webseiten, Datenschutz, (Un-)sichere Datenschutztypen, Soziale Netzwerke und viele weitere.

Im Leistungsumfang ist stets eine Sprache (Deutsch oder Englisch) inkludiert. Zusätzliche Sprachen können über die optionalen Features hinzugebucht werden.