

DTS

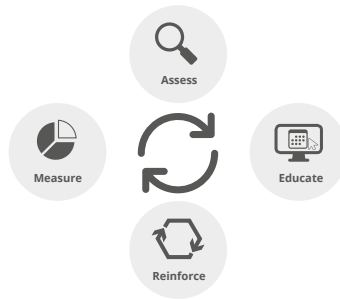
Managed Security Awareness Training

Managed Security Awareness Training

Die moderne IT-Bedrohungslandschaft weist neben technischen Faktoren eindeutig eine Reihe von menschlichen Elementen auf. Dieser „Faktor Mensch“ ist ein beliebtes Ziel für Cyberangriffe. Ein Großteil dieser Attacken beginnt mit einer E-Mail. Zwar gibt es Technologien zur Erkennung und Blockierung gefährlicher E-Mails, die letzte Sicherheitsinstanz ist der Endbenutzer. Sie gilt es als finale Hürde zu überwinden, denn mit ihnen steht und fällt die Sicherheit von sensiblen Unternehmensdaten. Aus diesem Grund sind Security Awareness Trainings unverzichtbar, um die Wahrscheinlichkeit erfolgreicher Phishing- oder Ransomware-Angriffe durch effektive Bedrohungs-simulationen und weiterbildende Maßnahmen zu verringern.

Unser DTS Managed Security Awareness Training ist einzigartig auf diesem Gebiet und nutzt Risikoinformationen und wissenschaftliche Lernprinzipien, um die richtige Ausbildung zur richtigen Zeit an die richtigen Personen zu vermitteln. Wir stärken nicht nur Ihre letzte Verteidigungslinie erheblich. Sie profitieren von unserer Erfahrung im Umgang mit der branchenführenden Proofpoint Security Awareness Training (PSAT) Lösung und sorgen gleichzeitig für eine Entlastung Ihrer Ressourcen.


- Ganzheitliches Security Awareness Training
- Gemeinsame Erarbeitung eines Trainingsplans
- Erstellung & Auswertung modulbasierter Assessments
- Zuweisung der im Trainingsplan festgelegten Trainingsmodule
- Quartalsweise Jour Fixe zum Review der Lernergebnisse
- Quartalsweise Phishing Simulationen
- Schulung administrativer Mitarbeiter
- Deutscher Support via DTS (9/5 Support Hotline)



Das PSAT beruht auf einer vierteiligen Methodik, erfunden von drei Forschern und Fakultätsmitgliedern der Carnegie Mellon University. Bei ihren Forschungen für die National Science Foundation und das Verteidigungsministerium erkannten sie, dass traditionelle Schulungsmethoden nicht wirksam sind, um das Risiko und die Anfälligkeit für Cyberangriffe zu reduzieren. Stattdessen entwickelten sie ein kontinuierliches Training, mit kurzen, interaktiven und spielbasierten Schulungen sowie dem Einsatz von simulierten Phishing-Angriffen. Dies hat sich bei Verhaltensänderungen nachweislich als wirksamer erwiesen.

Um eine erfolgreiche Einführung der Lösung zu gewährleisten, nehmen wir Sie direkt an die Hand. Von der Planung der Einführung bis zur Entwicklung eines individuellen Trainingsplans – Sie profitieren von unseren zahlreichen Kundenprojekten und Best Practices. Nach der erfolgreichen Einführung und initialen Planung der Lösung, übernehmen wir für Sie die weitere Verwaltung der Plattform und kümmern uns um die Bereitstellung der im Trainingsplan abgestimmten Maßnahmen. Hierzu zählen die Zuweisung von Wissens-Assessments sowie der abgestimmten Trainingsmodule zu verschiedenen Themenbereichen. In quartalsweise geplanten Jour Fixe Terminen besprechen wir mit Ihnen die Ergebnisse der Maßnahmen, nehmen Anpassungen des Trainingsplans vor, planen Phishing Simulationen und geben weitere Empfehlungen.

Um bei Ihren Mitarbeitenden zusätzliche Security Awareness für reale Bedrohungen zu schaffen, wie z. B. Phishing-Angriffe, erstellen wir für Sie simulierte Phishing-Nachrichten. Mit diesen ist es wiederum möglich, Mitarbeitenden aufzuzeigen, wie täuschend echt Angreifer heutzutage E-Mails fälschen.

<p>Right People</p>  <p>Only company that can identify people receiving actual attacks and map the training they need to take.</p>	<p>Right Education</p>  <p>Targeted training improves skills to defend against threats received. Proven learning science approaches ensure longer learning retention.</p>	<p>Right Time</p>  <p>Training delivered is based upon actual threats or responses to assessments to ensure relevancy and timelines.</p>
--	---	--