KnowBe4
Human error. Conquered.

Critères de sélection pour évaluer les prestataires de formation sur la sensibilisation à la sécurité

Critères de sélection pour évaluer les prestataires de formation sur la sensibilisation à la sécurité

Sommaire

INTRODUCTION

L'offre des prestataires de formation sur la sensibilisation à la sécurité (SAT) est aussi variée qu'innovante. Ce marché a considérablement évolué au cours des dernières années. Désormais, les RSSI et les responsables de la sécurité veulent s'assurer que leur programme SAT modifie le comportement des utilisateurs et permet à leur organisation de comprendre, de réduire et de surveiller les cyberrisques liés aux employés.

Un fournisseur SAT doit fournir une plateforme répondant à ces besoins, mais encore :

- approfondir votre réflexion sur la culture de la sécurité et la gestion du risque humain ;
- fournir les outils nécessaires pour favoriser et mesurer les changements de comportement ;
- veiller à ce que vos utilisateurs deviennent le pare-feu humain de votre organisation et la dernière ligne de défense contre les cyberattaques et les violations de données.

Ce livre blanc résume ce que vous devez prendre en compte pour évaluer les plateformes SAT, et dresse la liste des sept fonctionnalités essentielles que tout prestataire SAT doit proposer pour aider votre organisation à atteindre ses objectifs.

ÉVALUER LES PLATEFORMES DE SENSIBILISATION À LA SÉCURITÉ

De nombreux programmes SAT traditionnels ne tiennent pas compte du décalage entre connaissance, intention et comportement. Autrement dit, ce n'est pas parce que vous communiquez des informations et des renseignements sur la sensibilisation à la sécurité à vos utilisateurs qu'ils en tirent des enseignements ou y prêtent attention.

L'information seule ne change pas les actes. Au bout du compte, les individus tendent à emprunter la voie de la facilité ou retombent dans leurs anciennes habitudes. Assurez-vous que les principales parties prenantes de votre organisation comprennent ces trois réalités avant d'évaluer un prestataire SAT.

- **Une personne peut être sensibilisée à un sujet et ne pas s'en soucier**
  Ce n'est pas en submergeant les employés d'informations, de données et de procédures qu'ils vont se soucier de la sensibilisation à la sécurité. Lorsqu'ils reçoivent une recommandation de sécurité, la plupart des employés la « prennent en considération » en la confrontant à d'autres priorités.

- **Aller à l'encontre de la nature humaine est un combat perdu d'avance**
  Si les attentes de votre politique ne cadrent pas avec les réalités comportementales que nous venons d'évoquer, votre programme SAT ne répondra probablement pas à ces attentes. Au bout du compte, il s'agit de former et de communiquer des attentes à des êtres humains, pas de programmer des données dans un ordinateur.

- **Ce que font vos employés compte plus que ce qu'ils savent**
  Les connaissances seules ne suffisent pas à éviter qu'une organisation ne soit victime d'une violation. C'est le comportement de tout un chacun qui permet de renforcer le dispositif de sécurité d'une organisation ou mène à une violation. Mettez l'accent sur le comportement et ne vous contentez pas de communiquer des informations et des politiques.

SEPT ÉLÉMENTS ESSENTIELS QU'UN PRESTATAIRE SAT DOIT FOURNIR

Lorsque vous évaluez des prestataires SAT, vérifiez qu'ils proposent les sept éléments suivants. Cela vous aidera à choisir un programme SAT efficace à court terme et à préparer l'avenir en vous aidant à anticiper de futurs développements.

1 Un contenu varié et attrayant

Assurez-vous que le prestataire SAT prend en charge l'apprentissage mobile afin que les utilisateurs puissent assimiler le contenu et faire les exercices en déplacement.

Le contenu est essentiel. C'est le volet informatif de tout programme SAT. Fuyez les solutions toutes faites. Chaque utilisateur est attiré par un style de contenu différent qui correspond à ses propres préférences. Gardez ce point à l'esprit lorsque vous évaluez les plateformes SAT. Pour parvenir à modifier les comportements et à forger une solide culture de la sécurité dans votre organisation, il est essentiel de proposer une gamme de contenu adaptée aux différents groupes d'employés. Cherchez une plateforme SAT dotée d'une large bibliothèque régulièrement mise à jour, de contenu SAT multilingue, contenant des modules interactifs, des vidéos, des jeux, des affiches, des bulletins d'informations, des évaluations, etc.

Réfléchissez, en outre, à proposer une formation personnalisée basée sur le rôle ou des préférences de chacun. Une formation n'insistera probablement pas sur les mêmes points selon qu'elle s'adresse au personnel d'un centre d'appel ou aux membres d'une équipe informatique. Le contenu doit prendre en compte ces différences. Le style d'apprentissage de chaque utilisateur de votre organisation est différent : certains retiendront mieux le contenu traité dans des vidéos amusantes de trois minutes tandis que les cadres de votre organisation peuvent se sentir infantilisés par une telle approche. Lorsque vous évaluez les différentes plateformes SAT, la variété des approches est un critère de sélection essentiel pour vous permettre de présenter vos sujets de formation de base sous une forme adaptée à chacun.

Enfin, le déploiement du contenu de formation pour les utilisateurs est un critère tout aussi important que le contenu lui-même. Assurez-vous que le prestataire SAT prend en charge l'apprentissage mobile afin que les utilisateurs puissent assimiler le contenu et faire les exercices en déplacement. De plus, une interface administrative facile à utiliser vous permettant d'attribuer, de suivre, de mesurer et de rendre compte des efforts de formation est essentielle pour que vous puissiez tirer des conclusions pertinentes et utiles sur l'augmentation ou la diminution du risque et identifier les secteurs de votre organisation nécessitant un effort accru. Recherchez également des plateformes SAT flexibles qui vous permettront d'intégrer des contenus tiers personnalisés.

2 Localisation

La localisation est un processus essentiel qui consiste à traduire le contenu, mais aussi à proposer des exemples, des visuels et des éléments interactifs adaptés à la région des utilisateurs. C'est un processus approfondi qui va bien au-delà de la simple traduction du contenu et qui est crucial pour les organisations ayant une implantation mondiale et un personnel multilingue.

Choisir un prestataire SAT qui permette à vos utilisateurs de sélectionner la langue ou la région dans laquelle ils sont situés ou qu'ils préfèrent est un facteur primordial pour leur permettre d'assimiler et de mettre en œuvre le contenu de formation. Vérifiez que le prestataire SAT propose des localisations de qualité et fait appel à des experts locaux en la matière pour garantir la pertinence du contenu et des exemples.

3 Structure et automatisation

Le SAT ne constitue pas un exercice ponctuel. Pour mettre en place une culture de la sécurité, vous devez proposer un programme continu de formation et de tests, suivis de renforcement. En outre, gardez à l'esprit que l'apprentissage se compose de trois niveaux différents lorsque vous élaborez un programme SAT. La plateforme SAT que vous choisissez doit impérativement proposer le contenu et les outils appropriés pour cibler et dispenser chaque phase d'apprentissage.

- **Apprentissage formel et structuré** (**10 %)** : cette composante correspond à des éléments tels que la formation en classe, la formation en ligne déployée via un système de gestion de l'apprentissage (LMS), à des journées de formation, etc.

- **Apprentissage informel (20 %)** : demander conseil à d'autres équipes, collaborer, regarder des vidéos ou lire sont autant d'exemples de ce type d'apprentissage.

- **Apprentissage par l'expérience (70 %)** : cet aspect correspond principalement aux opportunités d'apprentissage quotidiennes, via des interactions sociales sur le lieu de travail, lors de l'application de procédures de travail ou de la culture d'une entreprise ou d'un département.

90 % des apprentissages d'une personne se produisent en dehors de tout cadre formel structuré.

Comme vous pouvez le constater, 90 % de l'apprentissage s'effectue en dehors de tout cadre formel et structuré. De nombreux programmes SAT échouent parce qu'ils se concentrent uniquement sur les 10 % initiaux de l'apprentissage. Assurez-vous que votre programme SAT s'adresse à ces trois niveaux d'apprentissage et que la plateforme associée vous offre des outils pour cibler ces trois niveaux. Proposer une courte vidéo sur le mot de passe directement sur la page de changement de mot de passe de votre organisation, afin qu'elle soit facilement disponible en cas de besoin est un parfait exemple d'une telle démarche.

Pour finir, l'automatisation est également un critère essentiel. Un prestataire SAT doit inclure des éléments d'automatisation dans son programme pour faciliter l'approvisionnement d'utilisateurs afin que les campagnes de formation puissent être programmées plusieurs semaines à l'avance sans nécessiter aucune action de la part des administrateurs. Cette automatisation doit également améliorer la simplicité d'utilisation et le retour sur investissement en rationalisant le temps nécessaire à la gestion du programme et en distribuant plus efficacement le contenu approprié à chaque utilisateur en temps opportun. Enfin, la plateforme doit également proposer une gestion automatisée des événements pour apporter une formation circonstancielle ou de rattrapage « juste à temps » et produire des rapports planifiés à la direction.

4 Tests

Si la formation est la clé de voûte de tout programme SAT, c'est en testant les utilisateurs pour voir comment ils réagissent aux simulations d'hameçonnage que vous déterminerez si vous parvenez à modifier les comportements en matière de sécurité et à réduire le risque humain. Un utilisateur va-t-il cliquer dans un e-mail, le signaler ou ne rien faire ?

De plus, vous devez fournir aux utilisateurs un moyen simple de signaler les e-mails d'hameçonnage afin d'aider votre organisation à renforcer sa résilience. Ce dispositif de signalement permet à votre équipe informatique de se tenir informée des attaques potentielles ciblant votre organisation et d'en avertir tout le personnel le cas échéant.

La plupart des plateformes SAT contiennent différents types de simulations et de modèles d'hameçonnage ainsi que des outils pour les utilisateurs finaux qui permettent de signaler les hameçonnages, mais le diable se cache dans les détails. Veillez à choisir un prestataire SAT qui garde une longueur d'avance sur les menaces et propose, par conséquent, des modèles d'e-mails d'hameçonnage s'appuyant sur des exemples réels.

Si un employé échoue à un test d'hameçonnage simulé, la plateforme SAT doit proposer une formation « juste à temps » afin de tirer des enseignements de cet incident spécifique pendant qu'il est encore frais dans l'esprit de l'utilisateur.

De même que pour la diffusion du contenu et le développement de programmes, l'automatisation et de l'apprentissage automatique sont des atouts considérables pour les programmes de simulation d'hameçonnage. La plateforme de simulation d'hameçonnage du prestataire doit utiliser l'apprentissage automatique pour recommander et distribuer des modèles d'hameçonnage pertinents et personnalisés en fonction de la formation et de l'historique d'hameçonnage de l'utilisateur, mais être également capable de reconnaître les véritables e-mails d'hameçonnage et de les transformer en modèles de simulations.

5 Statistiques et rapports

Un autre moyen de déterminer l'efficacité de votre programme SAT pour modifier les comportements et réduire le risque humain est d'effectuer des mesures et d'établir des rapports. C'est d'ailleurs indispensable pour permettre à la direction d'évaluer la réussite de votre programme de sensibilisation à la sécurité.

Vous devez savoir dans quelle mesure votre programme remplit ses objectifs et pouvoir montrer clairement les progrès effectués pour conserver le soutien de votre direction. Un prestataire qualifié vous fournira une solide plateforme de rapports et d'analyses pour proposer à votre organisation de mesurer les indicateurs les plus importants. Cette plateforme doit notamment vous permettre de générer des rapports exécutifs afin que les responsables du programme SAT puissent créer des rapports sur mesure pour la direction.

Identifiez également les prestataires qui proposent une évaluation de la culture de la sécurité et du risque humain. Les statistiques des programmes SAT traditionnels sont généralement centrées sur les taux d'achèvement, les performances aux questionnaires, les mesures d'engagement, etc. Il est essentiel de pouvoir mesurer le profil de risque de chaque personne et de chaque département afin de décider des ajustements nécessaires pour la formation en vous basant sur des données chiffrées. Vous devriez être en mesure d'évaluer l'évolution du risque de votre organisation au fil du temps et de mesurer véritablement les performances de votre programme de formation afin de comprendre les améliorations à apporter pour renforcer votre pare-feu humain.

6 Sondages et évaluations

Les employés peuvent avoir le sentiment qu'une formation formelle et continue de sensibilisation à la sécurité est hors de propos et considérer que la cybersécurité est du ressort des services informatiques. Il est donc crucial de comprendre quelles sont les attitudes adoptées au sein de votre organisation et de quelle manière elles évoluent avec le programme SAT. Cela vous aidera à identifier les domaines où vous obtenez de bons résultats et ceux qui nécessitent de prendre des mesures correctives. Vous pourrez également évaluer par la même occasion les progrès réalisés en matière de culture de la sécurité. Cette approche diverge totalement des statistiques classiques évoquées précédemment, car elle analyse les préférences, les opinions et l'état d'esprit.

Les sondages et évaluations doivent mesurer non seulement les sentiments et les attitudes, mais également les connaissances et les compétences. Toute plateforme SAT devrait offrir la possibilité d'effectuer une évaluation des compétences et des sondages sur la culture de la sécurité afin de mesurer les connaissances et les aptitudes de vos utilisateurs en matière de sécurité, et dresser un état des lieux global de la culture de la sécurité au sein de votre organisation. L'objectif est d'identifier les utilisateurs qui comprennent le mieux comment réagir à une situation donnée et qui sont capables de faire le bon choix. Par ailleurs, votre plateforme SAT devrait vous permettre de comparer votre organisation à des structures comparables au sein de votre secteur d'activité et de réaliser des évaluations selon des critères scientifiques afin de mesurer avec précision les progrès réalisés.

Elle devrait également inclure la possibilité de mesurer le score de risque humain des employés. L'objectif ultime est d'être en mesure de gérer le risque humain. Une fois que vous comprenez le profil de risque d'une personne ou d'un département, vous pouvez adapter la formation et recueillir de précieuses informations sur les points à améliorer dans votre programme de sécurité afin de renforcer par la même occasion la situation de votre organisation en matière de sécurité.

7 Au-delà de la sensibilisation à la sécurité

Au cours des dernières années, le secteur des prestataires SAT a connu une mutation fondamentale. Les principaux prestataires sont passés d'offres axées uniquement sur la formation des utilisateurs à des plateformes qui abordent désormais des questions plus globales telles que l'instauration d'une culture de la sécurité au sein d'une organisation et la gestion du risque humain.

Vous devez choisir un partenaire SAT qui vous permet non seulement d'atteindre vos objectifs immédiats, mais qui peut également vous accompagner dans le futur. Gardez ces différents éléments à l'esprit lorsque vous évaluez un prestataire SAT :

- **Concentrez-vous sur la sensibilisation, le comportement et la culture de la sécurité**
  Votre objectif suprême doit être de réduire le risque humain. D'après les études de Forrester Research*, vous devez vous associer à des prestataires qui quantifient et calculent le risque humain en fonction du comportement de l'utilisateur. La sensibilisation à la sécurité devient donc la pierre angulaire pour construire votre culture de la sécurité.

- **Le prestataire propose-t-il une gamme de services qui permet à votre organisation d'aller au-delà de la sensibilisation à la sécurité ?**
  Comme nous l'avons souligné précédemment, la sensibilisation à la sécurité est l'axe principal autour duquel se construit la culture de la sécurité de votre organisation, sans nécessairement en être la seule composante. La détection et la réponse humaines, les plateformes SOAR, la réaction aux incidents et le renseignement sur les menaces sont autant d'autres éléments clés qui peuvent compléter à l'avenir votre feuille de route en matière de culture de la sécurité. Assurez-vous que le prestataire que vous choisissez peut répondre à vos besoins actuels, mais aussi à vos besoins futurs.

* The Forrester Wave : Sensibilisation à la sécurité et solutions de formation, T1 2022

LISTE DE CONTRÔLE DES PRESTATAIRES SAT

- ☐ Une bibliothèque de contenus d'apprentissage fournie et variée
- ☐ La localisation
- ☐ Une plateforme largement automatisée de formation et de simulation d'hameçonnage
- ☐ Votre prestataire offre-t-il la possibilité de charger votre propre contenu de formation ou de télécharger du contenu de sa plateforme ?
- ☐ Une plateforme de déploiement de la formation dotée de capacités d'automatisation
- ☐ La possibilité de charger du contenu tiers sur la plateforme de formation/le système de gestion de l'apprentissage
- ☐ Une plateforme de simulation d'hameçonnage flexible, proposant des modèles variés, personnalisables et localisés
- ☐ L'intégration de l'automatisation, de l'intelligence artificielle et de l'apprentissage automatique aux plateformes de formation et de simulation d'hameçonnage
- ☐ Des capacités robustes de test et d'évaluation pour mesurer les connaissances des utilisateurs et l'impact de la formation
- ☐ Des fonctionnalités intuitives de statistiques et de création de rapports pour mesurer votre retour sur investissement
- ☐ Des fonctionnalités de rapports exécutifs

CONCLUSION

Toutes ces capacités constituent une base solide pour que le programme SAT de votre organisation puisse modifier le comportement des utilisateurs et permette à votre structure de véritablement comprendre, réduire et surveiller les cyberrisques. Le SAT servira de plateforme pour développer une compréhension plus large de la culture de la sécurité et de la gestion du risque humain, et pour transformer vos utilisateurs en véritable pare-feu humain de votre organisation.

CLIQUEZ ICI En savoir plus sur la de KnowBe4
Formation sur la sensibilisation à la sécurité Kevin Mitnick

Ressources supplémentaires

Test de sécurité gratuit relatif à l'hameçonnage
Découvrez le pourcentage de Phish-Prone (pourcentage de vulnérabilité à l'hameçonnage) de vos employés, en profitant de votre test de sécurité gratuit relatif à l'hameçonnage.

Programme automatisé de sensibilisation à la sécurité gratuit
Créez un programme de sensibilisation à la sécurité, personnalisé pour votre organisation.

Outil Phish Alert Button gratuit
Un seul clic suffit désormais à vos employés pour signaler les attaques par hameçonnage de manière sécurisée.

Outil Email Exposure Check (EEC) gratuit
Identifiez avant les pirates les adresses e-mail à risque de vos utilisateurs.

Outil Domain Spoof Test gratuit
Déterminez si les pirates peuvent usurper une adresse e-mail de votre domaine.

À propos de KnowBe4

KnowBe4 est la plus grande plateforme de formation sur la sensibilisation à la sécurité et de simulation d'hameçonnage au monde. Née du constat selon lequel l'aspect humain de la sécurité était largement négligé, KnowBe4 a pour objectif d'aider les organisations à gérer la menace permanente de l'ingénierie sociale par le biais d'une approche globale et innovante de la formation sur la sensibilisation.

Cette méthode intègre un dispositif de test de référence basé sur des simulations d'attaques réelles, une formation interactive au contenu stimulant, un système d'évaluation continue reposant sur un état des lieux des points forts de l'entreprise. Elle a pour but de développer une organisation plus résiliente, ayant pour priorité la sécurité.

Dans le monde entier, des dizaines de milliers d'organisations de tous les secteurs d'activité utilisent la plateforme KnowBe4, y compris dans des domaines très réglementés tels que la finance, la santé, l'énergie, l'administration et les assurances. Elles mobilisent ainsi leurs utilisateurs finaux, qui constituent leur dernière ligne de défense, et leur permettent de prendre des décisions plus avisées en matière de sécurité.

Pour en savoir plus, consultez la page www.KnowBe4.com

KnowBe4
Human error. Conquered.

KnowBe4 NL, BV | Papendorpseweg 99, 3528 BJ Utrecht, Pays-Bas
Tél. : +31 (0)30 7996074 | www.KnowBe4.com | E-mail : Sales@KnowBe4.com

08D03K01