Proofpoint Managed Security Awareness — Enterprise

Bénéficiez d'une ressource experte dédiée qui se consacre à vos objectifs de cybersécurité

Consacrez-vous à vos activités métier principales et confiez-nous la conception et l'exécution de vos programmes de formation et de sensibilisation à la sécurité informatique, ainsi que la génération de rapports. Proofpoint Managed Security Awareness — Enterprise vous offre une ressource dédiée qui se consacre entièrement à votre programme, pour une activité continue et une attention soutenue à la cybersécurité.

Avec Proofpoint, la mise en œuvre de programmes de sensibilisation à la sécurité informatique est à la fois simple et efficace. Nous adoptons une approche personnalisée, rigoureuse et éprouvée, qui mobilise vos utilisateurs tout au long de l'année. Notre expertise et notre connaissance approfondie des bonnes pratiques nous permettent d'élaborer des programmes de qualité.

Planification

Notre équipe d'experts se chargera de gérer votre programme de sensibilisation à la sécurité informatique. Au lancement du programme, vous rencontrerez toutes les semaines votre interlocuteur désigné au sein de l'équipe. Cette personne sera votre représentant personnel vis-à-vis de l'équipe et votre point de contact principal. Vous travaillerez ensemble pour concevoir et mettre en œuvre un programme spécifique en accord avec la culture et les objectifs de votre entreprise.

Intégration

Votre spécialiste de l'intégration attitré prendra rendez-vous avec vous et, grâce aux informations de notre questionnaire d'intégration, vous aidera à mettre en œuvre et à configurer les éléments suivants :

- Listes d'autorisation
- Synchronisation des utilisateurs
- PhishAlarm
- Authentification unique

Identification des besoins

Des réunions seront organisées avec votre contact pour vous permettre d'échanger au sujet de vos préoccupations en matière de cybersécurité et des menaces auxquelles vous êtes confronté, ainsi que de communiquer vos préférences en ce qui concerne les différentes activités de sensibilisation à la sécurité informatique. Vous aborderez notamment les programmes de formation, les tests d'intrusion et les simulations d'attaque de phishing, mais aussi les résultats du programme sur la longueur, ainsi que les retours et les problèmes en termes d'organisation.

Vous pourrez faire part de vos objectifs de sensibilisation à la sécurité informatique à court et moyen terme, afin qu'ils servent de lignes directrices pour l'élaboration d'un programme personnalisé. Ces discussions initiales permettront d'établir un ensemble d'objectifs de programme clairement définis.

Nous aborderons ensuite les premières initiatives visant à susciter l'engagement des principales parties prenantes, comme les ressources humaines et le département informatique. Votre contact vous procurera une série de guides, outils et modèles qui serviront tout au long du programme, à savoir :

- Guide de bonnes pratiques
- Calendrier de bonnes pratiques
- Modèles de simulation d'attaque de phishing
- Modèles de notification pour les formations à suivre
- Modèles de communication pour l'équipe informatique et le service d'assistance

Pour déterminer à quel point vos utilisateurs sont vulnérables aux attaques, votre contact exécutera des campagnes de simulation d'attaque de phishing parallèlement aux évaluations des connaissances.

Communications

Il est vivement recommandé d'élaborer un plan de communication mûrement réfléchi à l'intention des principales parties prenantes. Ce plan doit définir les attentes correspondant aux objectifs poursuivis par le programme. Il doit aussi renseigner un point de contact à même de répondre à vos questions et préoccupations. L'équipe Proofpoint peut aider à informer l'équipe informatique et le service d'assistance du calendrier de déploiement des campagnes de sensibilisation. Cette notification leur procurera des informations détaillées sur les campagnes et les groupes d'utilisateurs concernés, ce qui leur permettra de se préparer à répondre aux questions et demandes des utilisateurs. En outre, nous pouvons mettre à votre disposition des modèles de messages pour vous aider à communiquer efficacement avec vos utilisateurs à propos de votre programme de sensibilisation à la sécurité informatique. Une telle initiative peut favoriser l'acceptation et la mobilisation des utilisateurs face à des expériences d'apprentissage essentielles.

Composantes du programme de sensibilisation à la sécurité informatique

Votre programme de sensibilisation à la sécurité informatique peut inclure les modules suivants, selon vos produits sous licence :

- Évaluations des connaissances
- Simulations d'attaques
- Formations
- Supports de sensibilisation
- Outils de renforcement

Pour en savoir plus sur les produits de notre solution Proofpoint Security Awareness Training, consultez la page suivante : **http://www.proofpoint.com/fr/products/security-awareness-training**.

Mise en œuvre

Les simulations d'attaque Proofpoint établissent un point de référence initial réaliste de la vulnérabilité de votre entreprise sur différents vecteurs d'attaque. Pour déterminer à quel point vos utilisateurs sont vulnérables aux attaques, votre contact exécutera des campagnes de simulation d'attaque de phishing parallèlement aux évaluations des connaissances.

Simulations d'attaque de phishing

Votre contact sera l'administrateur « sur le terrain » de l'outil d'évaluation associé aux simulations d'attaque de phishing. Nous choisirons ensemble les modèles de simulation et les messages éducatifs pour chaque campagne. Nous déterminerons également avec vous, avant chaque campagne, la portée de la simulation et les utilisateurs concernés. Une simulation d'attaque de phishing en aveugle sera envoyée à vos utilisateurs au début de la période de licence afin de définir des données servant de point de référence initial. Par la suite, nous exécuterons des simulations d'attaque de phishing, accompagnées de messages éducatifs, pendant toute la durée de votre licence. Ces messages éducatifs offrent un retour immédiat et efficace aux utilisateurs qui tombent dans le piège.

Campagne USB de simulation d'attaque de phishing

Votre contact créera la campagne USB de simulation d'attaque de phishing. Nous configurerons, planifierons et lancerons chaque campagne selon le plan défini avec votre contact dans le cadre de votre accord de licence. Nous configurerons les noms des fichiers leurres qui devront être placés sur les clés USB et sélectionnerons ou personnaliserons le message éducatif. Nous vous enverrons ensuite le fichier ZIP contenant les éléments nécessaires via Secure Share. Vous devrez alors vous procurer les clés USB et charger les fichiers à l'aide de la feuille de calcul fournie, afin d'organiser leur déploiement. Une fois les clés USB déployées, votre contact vous fournira des rapports d'activité selon un calendrier établi.

Évaluations des connaissances

Les évaluations des connaissances que nous réalisons déterminent le niveau de connaissances de vos collaborateurs et permettent de mesurer l'efficacité de la formation. Il est recommandé de réaliser une évaluation des connaissances portant sur des thèmes généraux au début de la période de licence, puis diverses évaluations complémentaires en fonction des résultats de la première. Cette méthodologie vous aidera à cibler les domaines à risque que vous avez identifiés.

Modules de formation

Proofpoint affectera des modules de formation à vos utilisateurs qui sont tombés dans le piège des simulations d'attaque de phishing. Ces formations peuvent inclure des modules liés à vos produits sous licence. Nous créerons également des formations destinées à tous les utilisateurs, qu'ils aient réussi ou échoué à la simulation, pour que chacun puisse bénéficier d'un apprentissage.

À l'approche de l'échéance fixée pour une formation donnée, nous enverrons des rappels aux utilisateurs concernés. De plus, nous déterminerons l'état des connaissances des utilisateurs afin de planifier les prochaines évaluations et formations à suivre.

Votre contact affectera aux utilisateurs des modules de formation sur la sécurité et la conformité, dont certains feront par ailleurs l'objet d'une inscription automatique. Les formations à suivre seront composées de plusieurs modules, selon les domaines à risque identifiés.

REMARQUE : si vous utilisez votre propre système d'apprentissage (LMS, Learning Management System) pour une partie ou l'intégralité des formations à suivre, l'administration des utilisateurs LMS, les attributions LMS et la génération de rapports LMS seront gérées par vos soins, et non par votre contact. Les jaquettes de formation et l'inscription automatique aux formations ne sont pas disponibles pour les modules LMS.

Renforcement

PhishAlarm propose un renforcement par encouragement aux utilisateurs qui signalent des attaques de phishing potentielles. Le module d'extension PhishAlarm permet d'alerter d'un simple clic les équipes de sécurité et de réponse aux incidents de la présence d'emails suspects. Ce signalement limite la durée et l'impact des attaques de phishing actives, tout en renforçant les comportements appris dans le cadre de votre programme de sensibilisation à la sécurité informatique. Il constitue par ailleurs un indicateur important pour le suivi du comportement des utilisateurs, ainsi que de leur sensibilisation à la sécurité et de leur engagement. Les supports de sensibilisation à la sécurité informatique sont conçus pour renforcer les principes fondamentaux enseignés par nos modules de formation. Ils permettent de mettre en avant les bonnes pratiques et d'améliorer l'ancrage des connaissances. Proofpoint adaptera les supports de sensibilisation à la sécurité informatique en fonction des lacunes relevées lors des évaluations des connaissances.

Analyse

Combinés, les résultats de l'évaluation des connaissances, des campagnes de simulation d'attaque de phishing et des rapports PhishAlarm de signalement d'emails dangereux offrent une vue globale du niveau de connaissances des utilisateurs et de leur vulnérabilité aux attaques. Grâce à ces données, vous pouvez identifier les principaux domaines à risque et élaborer un plan ciblé de renforcement des connaissances des collaborateurs.

Votre contact examinera les résultats après chaque évaluation et formation à suivre. Les résultats seront comparés aux performances précédentes pour dégager les tendances à l'amélioration et identifier les problématiques (anciennes ou nouvelles) à cibler. Les propriétés incluses dans le rapport (qui ont été définies lors de la session de planification initiale) seront analysées pour identifier la corrélation entre le risque, d'une part, et les départements internes, les zones géographiques, les rôles ou les directions d'équipe, d'autre part. Cette analyse sera ensuite examinée lors des sessions de stratégie et planification continue, afin de déterminer les étapes suivantes dans le parcours de formation. Votre contact vous fournira une analyse comparative au niveau sectoriel et des études de référence, lorsque c'est possible.

Analyse des VAP

Si vous disposez de Proofpoint Targeted Attack Protection (TAP), votre contact exécutera les tâches suivantes :

- Identification des collaborateurs les plus souvent pris pour cible au sein de votre entreprise
- Segmentation de vos VAP en fonction des données sur les menaces ciblées
- Création d'activités de formation et de sensibilisation pour les VAP, en fonction des menaces identifiées
- Analyse des VAP et de leurs performances dans le cadre du programme de sensibilisation à la sécurité informatique au fil du temps

Génération de rapports

Des rapports seront générés de manière sécurisée pour chaque activité tout au long du déroulement du programme. L'API de gestion des résultats vous permet également de créer des tableaux de bord via l'outil de veille stratégique de votre choix.

Calendrier du programme de sensibilisation à la sécurité informatique

Le calendrier ci-dessous est une proposition de mise en œuvre de notre méthodologie de formation continue. Il sera adapté en fonction de vos produits sous licence, de la durée du programme, ainsi que de vos besoins et objectifs spécifiques.

Du 1er au 3e mois

	1ER MOIS	2E MOIS	3E MOIS
Évaluation des connaissances	Évaluation des connaissances de référence 1 Communication initiale		
Phishing	Phishing à l'aveugle 1	Campagne 1 avec inscription automatique	
Formation		Formation avec inscription automatique	Utilisateurs qui ne se laissent pas piéger par les simulations d'attaque
Support de renforcement		Thème sélectionné	

Du 4e au 6e mois

	4E MOIS	5E MOIS	6E MOIS
Évaluation des connaissances			
Phishing	Campagne 2	Campagne 3	Campagne 4
Formation		Formation supplémentaire	Utilisateurs qui ne se laissent pas piéger par les simulations d'attaque
Support de renforcement		Nouveau thème	

Du 7e au 9e mois

	7E MOIS	8E MOIS	9E MOIS
Phishing		Campagne 5	Campagne 6
Formation	Utilisateurs qui ne se laissent pas piéger par les simulations d'attaque		Formation supplémentaire*
Support de renforcement		Nouveau thème	

Du 10e au 12e mois

	10E MOIS	11E MOIS	12E MOIS
Évaluation des connaissances			Évaluation des connaissances supplémentaire 1
Phishing	Campagne 7	Campagne 8	

* Les thèmes de formation supplémentaires sont déterminés en fonction des résultats des évaluations des connaissances. Les clés USB de simulation d'attaque de phishing peuvent être obtenues à tout moment pendant la durée de la licence.

« Proofpoint Managed Security Awareness » remplace « Managed Proofpoint Security Awareness Training ».

EN SAVOIR PLUS

Pour plus d'informations, visitez notre site à l'adresse : **proofpoint.com/fr**.

À PROPOS DE PROOFPOINT

Proofpoint, Inc. est une entreprise leader dans le domaine de la cybersécurité et de la conformité qui protège les ressources les plus importantes et les plus à risques des entreprises : leurs collaborateurs. Grâce à une suite intégrée de solutions cloud, Proofpoint aide les entreprises du monde entier à stopper les menaces ciblées, à protéger leurs données et à rendre leurs utilisateurs plus résistants face aux cyberattaques. Les entreprises de toutes tailles, y compris 75 % des entreprises de l'index Fortune 100, font confiance aux solutions de sécurité et de conformité de Proofpoint centrées sur les personnes, pour diminuer leurs risques les plus critiques via les emails, le cloud, les réseaux sociaux et le Web. Pour plus d'informations, rendez-vous sur **www.proofpoint.com/fr**.