Proofpoint Security Awareness Enterprise

Renforcer la résilience des utilisateurs en adoptant une approche axée sur les menaces

Principaux avantages

- Réduisez de 40 % le nombre de clics sur des emails malveillants en moins de six mois.
- Montrez à votre RSSI les indicateurs d'une réduction des risques.
- Induisez des changements de comportement grâce à une expérience d'apprentissage personnalisée.
- Analysez automatiquement les menaces signalées par les utilisateurs sans alourdir la charge informatique.

Proofpoint Security Awareness Enterprise vous aide à relever l'un des défis les plus pressants auxquels sont confrontées toutes les entreprises : réduire le risque de sécurité posé par les collaborateurs. D'après le rapport State of the Phish 2023 de Proofpoint, notre étude annuelle sur le phishing, 98 % des entreprises ont mis en place des formations de sensibilisation à la sécurité informatique. Il semble donc que leur importance soit largement reconnue. Mais les formations seules ne permettent pas toujours d'obtenir des résultats probants.

Pour qu'un programme de sécurité soit efficace, les utilisateurs doivent s'impliquer activement dans le processus d'apprentissage et être capables de faire des choix judicieux dans des situations réelles. Qui plus est, leurs comportements doivent avoir un impact mesurable sur la sécurité.

Proofpoint Security Awareness Enterprise peut s'avérer utile. Le cadre ACE, notre approche globale de la sensibilisation à la sécurité informatique, permet de résoudre cette problématique. Ce cadre pédagogique s'articule autour de trois étapes clés : évaluer la vulnérabilité des utilisateurs, modifier leur comportement et évaluer l'efficacité du programme. Notre solution améliore l'efficacité opérationnelle et permet aux administrateurs de la sécurité de mettre le programme à l'échelle pour bénéficier d'une portée mondiale.

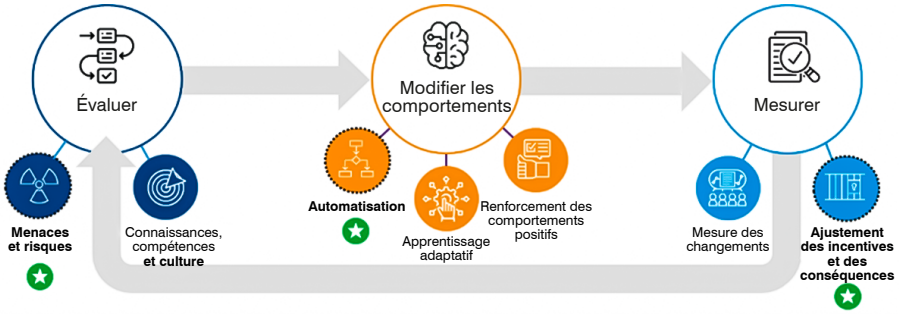

Figure 1. Le cadre ACE

Tirez parti d'une threat intelligence de pointe

Proofpoint Security Awareness Enterprise est optimisé par notre threat intelligence enrichie, collectée auprès de notre vaste clientèle. Nous l'utilisons pour vous aider à créer un programme de formation efficace, afin que vous puissiez mener des campagnes de simulations d'attaques de phishing sophistiquées qui imitent les attaques réelles. Vous pouvez identifier vos VAP™ (Very Attacked People, ou personnes très attaquées) et les sensibiliser aux menaces qui les ciblent, observer le comportement des utilisateurs lorsqu'ils sont confrontés à des menaces réelles, ainsi que mettre en lumière les tendances d'attaque dans des newsletters envoyées aux collaborateurs.

Évaluez la vulnérabilité des utilisateurs

Proofpoint Security Awareness Enterprise vous aide à évaluer les connaissances, les compétences et les croyances de vos utilisateurs en matière de cybersécurité. Il indique également leur niveau d'attractivité en tant que cibles. Toutes ces informations vous aident à identifier les utilisateurs hautement vulnérables ainsi qu'à déterminer leur capacité à adopter les bons comportements. Vous pouvez ainsi vous faire une idée précise des collaborateurs qui ont le plus besoin d'être formés et créer un programme personnalisé en fonction de leurs lacunes et de leur comportement prévu.

Grâce à Proofpoint Security Awareness Enterprise, vous pouvez :

- Identifier les lacunes au moyen de tests rapides et concis basés sur notre threat intelligence enrichie
- Exécuter des tests de phishing qui intègrent les menaces observées en circulation
- Analyser la vulnérabilité des collaborateurs sur la base de leur participation, de leurs performances et de la probabilité qu'ils soient ciblés par une attaque
- Identifier les croyances en matière de sécurité pour déterminer comment encourager les collaborateurs à adopter les bons comportements
- Identifier les VAP et les collaborateurs qui se laissent le plus piéger lorsque la solution est intégrée à la plate-forme Proofpoint

Déterminez le niveau de connaissances de vos utilisateurs

Nos évaluations adaptatives vous aident à déterminer le niveau de connaissances de vos utilisateurs et les points qui leur posent problème. Les évaluations sont des modules de formation spécifiques à la fois concis et précis. Vous pouvez faire votre choix parmi une large sélection de tests qui répondent à des objectifs spécifiques et parmi des modules de microapprentissage présentant différents niveaux de difficulté.

Anticipez le comportement de vos utilisateurs

Nos simulations d'attaques de phishing vous permettent de vous assurer que vos utilisateurs sont prêts à faire face aux menaces réelles. Proofpoint s'appuie sur la threat intelligence issue des plus de 2,6 milliards d'emails que nous analysons chaque jour. Cette visibilité nous permet de vous proposer des milliers de modèles de phishing qui simulent plusieurs types de menaces. Vous pouvez également personnaliser vos propres modèles en fonction des types de menaces observées dans votre environnement, ainsi qu'inscrire automatiquement à des formations les utilisateurs qui échouent lors d'une simulation d'attaque de phishing.

Découvrez les croyances de vos utilisateurs

Pour instaurer une culture solide de la sécurité informatique, vous devez identifier les croyances de vos utilisateurs en matière de cybersécurité. Nos évaluations de la culture vous aident à déterminer l'état actuel de votre culture de la sécurité informatique. Elles utilisent de courts questionnaires qui vous permettent d'analyser et de mesurer les trois principaux facteurs qui contribuent à cette culture : la responsabilité, l'importance et l'autonomisation. Vous pouvez ainsi personnaliser le programme pour modifier les croyances de vos collaborateurs et les encourager à mettre en pratique ce qu'ils apprennent.

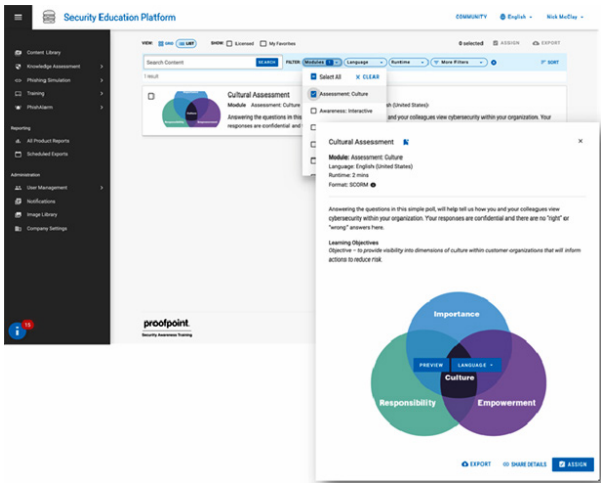

Figure 2. Évaluations de la culture et filtrage et bibliothèque de contenus améliorés

Identifiez les utilisateurs les plus à risque

Lorsqu'elle est intégrée à la plate-forme Proofpoint Threat Protection, notre solution vous aide à identifier vos VAP et les collaborateurs qui se laissent le plus piéger. Grâce à ces informations, vous pouvez proposer des formations ciblées à vos utilisateurs les plus attaqués en fonction des menaces qui les visent. Notre intégration avec Nexus People Risk Explorer vous offre encore plus d'informations sur vos utilisateurs les plus à risque. Elle évalue leur vulnérabilité, l'indice d'attaque (Attack Index) et les privilèges métier. Vous pouvez ainsi axer votre programme et vos ressources sur les risques réels pesant sur votre entreprise.

Pour en savoir plus sur les formations ciblées de Proofpoint Security Awareness, consultez la fiche solution **Comment Proofpoint Security Awareness Training stimule l'engagement des utilisateurs**.

Modifiez le comportement des utilisateurs

Une fois que vous avez établi une ligne de base des connaissances, des comportements et des croyances de vos utilisateurs, vous pouvez commencer à modifier leurs comportements à risque. Proofpoint Security Awareness Enterprise vous aide à induire des changements de comportement grâce à des formations et activités de renforcement personnalisées. Vous pouvez ainsi apporter à chaque personne les connaissances dont elle a besoin et lui proposer du contenu adapté à sa situation. Cela vous permettra d'optimiser le temps limité dont vous disposez pour former les utilisateurs et d'accroître l'impact de cette formation.

Grâce à Proofpoint Security Awareness Enterprise, vous pouvez :

- Motiver les utilisateurs en leur offrant une expérience d'apprentissage personnalisée
- Créer des formations concises et spécifiques pour chaque objectif d'apprentissage
- Proposer du contenu attrayant tenant compte du paysage actuel des menaces
- Accroître l'efficacité de l'apprentissage grâce à des formations pertinentes proposées au moment opportun

Utilisez un cadre adaptatif et des modules de microapprentissage

Proofpoint Security Awareness Enterprise utilise un cadre d'apprentissage adaptatif. C'est tout le contraire d'une approche universelle. Le cadre propose des formations à la sécurité informatique suivant un barème progressif à quatre niveaux, allant des principes de base à des concepts avancés. Vos utilisateurs peuvent donc suivre les formations dont ils ont besoin avec le niveau de difficulté approprié.

Le cadre adaptatif s'accompagne également de modules de microapprentissage. Ces modules d'une durée de trois minutes sont concis et répondent à des objectifs d'apprentissage spécifiques. Vos utilisateurs bénéficient ainsi d'une formation continue et facile à assimiler. De plus, les formations sont personnalisées selon des facteurs individuels tels que le rôle, le style d'apprentissage, les compétences, le niveau de vulnérabilité et la langue du collaborateur.

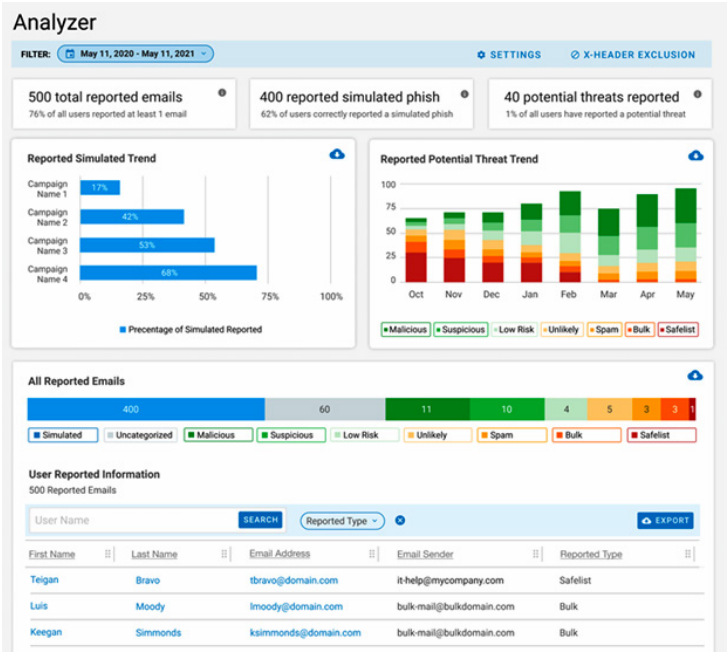

Figure 3. Analyse en temps réel des comportements face aux simulations d'attaques de phishing et aux menaces réelles

Proposez du contenu axé sur les menaces et des formations au moment opportun

Les tendances et les tactiques du paysage actuel des menaces orientent le contenu de Proofpoint Security Awareness Enterprise. Vous pouvez ainsi mieux préparer vos utilisateurs à faire face aux menaces réelles en circulation. Nos alertes hebdomadaires sur les menaces décrivent les dernières attaques observées au sein de notre clientèle, tandis que nos alertes Attack Spotlight améliorent votre programme avec des formations proposées au moment opportun.

Lorsque Proofpoint Security Awareness Enterprise est intégré à la plate-forme Proofpoint, vous pouvez afficher des avertissements contextuels pour vos utilisateurs et renforcer les comportements positifs. Les messages éducatifs expliquent aux utilisateurs pourquoi ils ne devraient pas cliquer sur un lien dans le cadre d'une simulation d'attaque de phishing. Les avertissements intégrés à l'application en cas d'emails suspects leur signalent les messages potentiellement malveillants. Enfin, le bouton « Report Suspicious » (Signaler comme suspect) déclenche notre workflow Proofpoint Closed-Loop Email Analysis and Response (CLEAR) automatisé, qui fournit aux utilisateurs un feedback personnalisé sur l'email qu'ils ont signalé.

Évaluez l'impact du programme

Vous devez être capable d'évaluer l'impact de votre programme de sensibilisation à la sécurité informatique sur votre sécurité. Proofpoint Security Awareness Enterprise fournit des indicateurs comportementaux qui mettent en évidence les performances de vos collaborateurs et du programme. Vous pouvez ainsi évaluer clairement l'impact du programme sur votre sécurité. Par exemple, nos clients ont observé une diminution de 40 % du nombre de clics sur des menaces réelles en seulement six mois. Ils ont également constaté que le nombre d'emails signalés par les utilisateurs avait triplé. Vous pouvez présenter ces indicateurs de réduction des risques à votre RSSI pour lui démontrer l'efficacité du programme et obtenir son accord pour investir davantage dans celui-ci et le développer.

Grâce à Proofpoint Security Awareness Enterprise, vous pouvez :

- Surveiller le comportement des utilisateurs en ce qui concerne le signalement des menaces réelles
- Comparer des indicateurs clés avec ceux d'autres entreprises de votre secteur
- Démontrer un changement positif des comportements des utilisateurs pour obtenir l'adhésion de la direction

Surveillez les comportements face aux simulations et aux emails réellement malveillants

Notre tableau de bord destiné aux RSSI montre l'impact des formations sur le comportement de vos collaborateurs. Il surveille les signalements effectués par les utilisateurs pour des emails réellement malveillants et montre l'évolution au fil du temps. De cette façon, vous pouvez comprendre comment leur comportement s'est amélioré. Des indicateurs tels que le taux de signalement des emails suspects et la précision de ces signalements vous aident à mesurer les performances des utilisateurs au-delà du taux d'achèvement des formations.

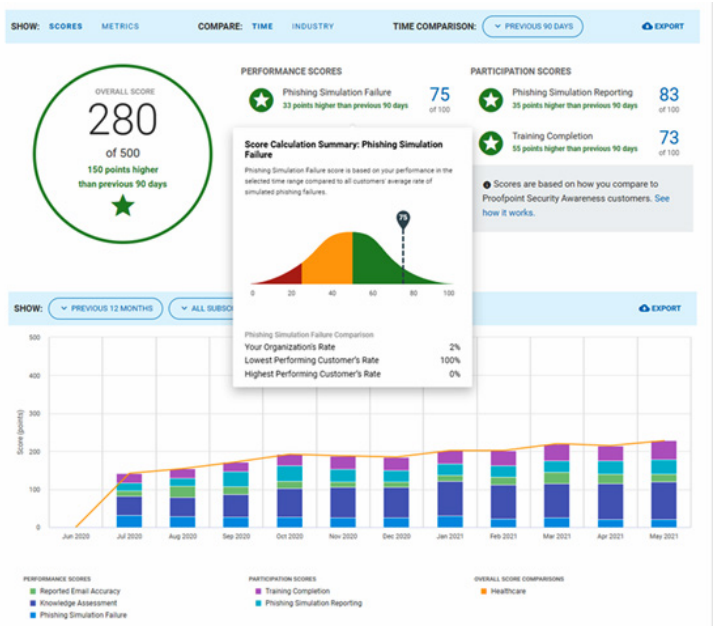

Figure 4. Suivi des performances du programme dans le récapitulatif des scores intégré au tableau de bord destiné aux RSSI

Comparez vos résultats à ceux d'autres entreprises de votre secteur

Le tableau de bord destiné aux RSSI compare également les performances de votre programme à celles d'autres entreprises de votre secteur. Il vous permet de voir les changements de comportement de vos utilisateurs, par exemple le pourcentage de collaborateurs qui signalent des emails suspects. Vous pouvez ainsi comparer leur taux de précision aux taux enregistrés par d'autres entreprises, ce qui vous permet d'évaluer l'impact de votre programme par rapport à ceux de vos homologues et de mettre en avant son efficacité.

Identifiez les comportements qui se répètent

Proofpoint Security Awareness Enterprise fournit des données quotidiennes sur les tests internes et les menaces externes. Par exemple, vous pouvez surveiller et identifier les comportements qui se répètent. Notre solution vous permet de filtrer et de regrouper les utilisateurs qui ont échoué plusieurs fois lors d'une simulation d'attaque de phishing au cours d'une période donnée. Les administrateurs peuvent ainsi prendre les mesures qui s'imposent, par exemple en attribuant des formations supplémentaires.

Développez votre programme et mettez-le à l'échelle

Proofpoint Security Awareness Enterprise vous permet de tirer parti de la puissance de l'automatisation et de l'évolutivité. Les processus automatisés réduisent les tâches manuelles et augmentent la flexibilité et l'efficacité de vos opérations. Notre solution vous permet également de mettre votre programme à l'échelle pour bénéficier d'une portée mondiale.

Grâce à Proofpoint Security Awareness Enterprise, vous pouvez :

- Améliorer l'expérience des administrateurs grâce à des processus flexibles et automatisés
- Vous adresser à votre public international dans la langue préférée des utilisateurs
- Proposer votre programme de sensibilisation à la sécurité informatique dans un large éventail de langues
- Adopter de bonnes pratiques et bénéficier d'une aide ininterrompue grâce aux services managés Proofpoint
- Faciliter le signalement des emails suspects par les utilisateurs et leur fournir un feedback positif
- Analyser et neutraliser automatiquement les emails signalés par les utilisateurs grâce à l'intégration avec la plate-forme Proofpoint

Prenez en charge plusieurs langues

Vous pouvez vous adresser à votre public international dans la langue préférée des utilisateurs. Proofpoint Security Awareness Enterprise prend en charge plus de 40 langues pour nos modules de formation et nos services de personnalisation. Cela inclut des sous-titres et des voix off. En outre, nous ajoutons continuellement de nouvelles langues.

Profitez d'un déploiement flexible grâce à l'administration multitenant

Avec l'administration multitenant, vous bénéficiez d'une configuration simplifiée, qui peut être déployée de manière flexible et adaptée à votre cas d'utilisation spécifique. L'équipe de sécurité de votre entreprise supervise le programme dans sa globalité. Elle prend des décisions à l'échelle du groupe. Les groupes individuels (tels qu'une succursale ou une division régionale) peuvent adapter les formations à leurs utilisateurs et à leurs exigences spécifiques. Ce workflow est idéal pour les grandes entreprises complexes avec une présence mondiale ou distribuée.

Améliorez la productivité grâce aux services managés

Proofpoint vous aide à renforcer votre équipe de sécurité et à adopter de bonnes pratiques. Grâce aux **services managés**, nous pouvons assurer les tâches quotidiennes associées à l'exécution et à l'évaluation de votre programme de sensibilisation à la sécurité informatique. Votre équipe de sécurité peut ainsi se concentrer sur ses activités métier principales. Avec les **services de personnalisation de Proofpoint Security Awareness**, vous pouvez présenter un programme propre à votre entreprise et renforcer votre culture de la sécurité informatique en personnalisant les modules de microapprentissage (logos d'entreprise, couleurs, images, texte, voix off, traduction, etc.).

Automatisez les signalements des utilisateurs et la réponse aux menaces

Lorsqu'un utilisateur signale un email suspect dans son client de messagerie, la technologie de détection des menaces Proofpoint analyse automatiquement l'email. Cela réduit votre exposition aux menaces de phishing qui pourraient échapper à vos défenses, diminue les tâches manuelles et améliore l'efficacité opérationnelle. Si notre technologie de détection des menaces identifie un email suspect comme représentant une menace et que la solution est intégrée à la plate-forme Proofpoint, notre workflow CLEAR automatisé se déclenche. Il neutralise l'email et envoie un feedback à l'utilisateur qui l'a signalé. Ce processus permet de renforcer les comportements positifs et réduit la charge de correction jusqu'à 90 % pour les administrateurs.

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**.

proofpoint.