

OpenText Core Security Awareness Training

Réduire l'exposition aux risques par le biais des utilisateurs internes

Principaux avantages

- 20 % de logiciels malveillants en moins par rapport aux clients qui utilisent OpenText Core Endpoint Protection
- Administration et gestion des campagnes aisées
- Mises à jour de formation pertinentes et fréquentes avec un contenu utile, interactif et efficace
- Solution intégrée pour les MSP et les PME avec gestion multi-tenant
- Gestion automatisée de la formation et création de rapports de conformité au niveau de l'individu, du groupe et de la société

Ce n'est pas un hasard si le phishing est la méthode préférée des pirates informatiques. Ce type d'attaque facile à déployer enregistre un taux de réussite de 74 % parmi les entreprises américaines¹. Et les cybercriminels ciblent des entreprises de toutes tailles. Un simple clic involontaire de la part d'un utilisateur sur un lien de phishing permet en effet aux criminels d'accéder à l'ensemble des ressources d'un réseau, voire au-delà dans certains cas. C'est également la raison pour laquelle les formations de sensibilisation à la sécurité et les simulations de phishing sont un élément essentiel pour les entreprises qui veulent transformer les utilisateurs finaux, de maillon faible de la chaîne de sécurité, en une première ligne de cyberdéfense véritablement résiliente.

La meilleure sécurité au monde ne peut pas empêcher un employé, qu'il travaille sur site ou à distance, de laisser involontairement la porte d'entrée du réseau grande ouverte. OpenText™ Core Security Awareness Training permet aux entreprises d'aider les utilisateurs finaux à identifier et à signaler les tentatives de phishing, d'éviter les risques, de respecter les exigences de conformité réglementaire et de prévenir les cyberattaques modernes grâce à une formation régulière s'inscrivant dans une approche de défense multicouche, dans le but de devenir cyberrésilientes.

Réduire les risques avec OpenText Core Security Awareness Training

Suivez l'évolution des menaces et les nouveaux vecteurs d'attaque

OpenText Core Security Awareness Training fournit la formation et les tests continus, pertinents et mesurables dont les entreprises ont besoin pour limiter les comportements à risque des utilisateurs et devenir cyberrésilientes. Son simulateur de phishing complet propose une bibliothèque de modèles en constante évolution, basée sur des scénarios concrets. Les modèles sont catégorisés et régionalisés pour faciliter leur utilisation, tandis que la randomisation du calendrier permet une livraison échelonnée pour maximiser l'impact de la campagne.

OpenText Core Security Awareness Training est une offre SaaS (Software-as-a-Service) entièrement basée sur le cloud. Les administrateurs peuvent gérer la formation et les simulations de phishing via la même console qu'OpenText™ Core Endpoint Protection et OpenText™ Core DNS Protection, offrant ainsi une expérience unique avec une faible charge de gestion. Une formation adéquate des utilisateurs permettra de réduire le nombre d'incidents de sécurité auxquels l'entreprise est confrontée, ce qui réduira à son tour les coûts ainsi que les pertes en termes de productivité et d'interruptions de service. D'après les observations que nous avons réalisées sur de véritables clients, les entreprises qui utilisent OpenText Core Security Awareness Training en plus de la sécurité de leurs nœuds d'extrémité enregistrent 20 % de logiciels malveillants en moins que celles qui déploient uniquement notre protection des nœuds d'extrémité, sans formation.

¹ Venure Beat 2021, Phishing attacks get smarter as targets struggle to keep up

Console unique et multi-client qui vous permet de lancer facilement des formations sur un ou plusieurs sites

Fonctionnement

OpenText Core Security Awareness Training inclut un système de gestion de l'apprentissage (LMS) hautement automatisé qui facilite et optimise la gestion des formations. Grâce à son intégration à Microsoft® Azure Active Directory, OpenText Core Security Awareness Training permet aux administrateurs d'automatiser l'importation des utilisateurs cibles et d'en assurer la synchronisation. L'assistant de configuration simple d'emploi facilite la création de simulations de phishing et de campagnes de formation. Quelques minutes suffisent pour attribuer un nom à une campagne, choisir les destinataires souhaités, sélectionner le contenu et lancer la campagne. Les administrateurs peuvent planifier une séquence de plusieurs formations et simulations de phishing sur une période donnée. En outre, les administrateurs qui gèrent plusieurs clients ou sites, tels que les MSP, peuvent mettre en oeuvre et gérer ces programmes à l'échelle mondiale pour plusieurs clients. Les fonctionnalités de planification, de randomisation du calendrier de livraison et de rappels et rapports automatisés simplifient le lancement de campagnes de sensibilisation à la sécurité continues et responsables, qui améliorent efficacement le comportement des utilisateurs au fil du temps.

OpenText Core Security Awareness Training

L'intégration d'Azure AD facilite la gestion de la formation des utilisateurs, tandis que l'assistant de création de campagne réduit le temps et le coût d'administration des programmes de sensibilisation à la cybersécurité. Le LMS intégré permet de suivre la participation de chaque utilisateur, ce qui favorise la capacité de responsabilisation et la mesurabilité des formations en cybersécurité. Notre rapport exécutif de synthèse de campagne met en évidence les données de campagne et les résultats de la formation. Un tableau de bord de formation unique affiche toutes les campagnes en cours ou terminées, tandis qu'un workflow intuitif de gestion des campagnes permet aux administrateurs de composer et de lancer rapidement et facilement une formation multi-client.

OpenText Core Security Awareness Training est un programme de sensibilisation à la sécurité prêt à l'emploi où vous gérez la liste des utilisateurs : nous nous chargeons de leur envoyer chaque mois des campagnes de formation et de simulation de phishing.

Transformer les utilisateurs finaux, de maillon faible de la chaîne de sécurité, en une première ligne de cyberdéfense véritablement résiliente

Formation continue, pertinente et mesurable pour limiter les comportements à risque des utilisateurs et devenir cyberrésilient

OpenText Security Solutions réunit les meilleures solutions de sa catégorie pour aider votre entreprise à rester cyberrésiliente. OpenText peut vous aider à prévenir les menaces et à vous en protéger, et vous permettre d'atténuer les risques en détectant et en réagissant rapidement, puis en récupérant les données en toute simplicité. Vous réduisez ainsi leur impact et assurez votre conformité au regard de l'évolution des réglementations.

Le vaste catalogue de formations d'OpenText Core Security Awareness Training est mis à jour chaque mois pour couvrir une grande variété de sujets liés à la sécurité et à l'entreprise dans tout un éventail de formats. Vous pouvez recevoir des statistiques de campagnes de phishing et générer des actions par utilisateur ainsi que d'autres rapports afin de mesurer la progression et le retour sur investissement. Dans une récente analyse des simulations de phishing auprès des clients, 11 % des utilisateurs avaient cliqué sur le premier e-mail de phishing. Lors de la 6e simulation, le taux de clics était passé à 6 %, et à la 18e simulation, il s'établissait à 4 %. La formation OpenText Core Security Awareness Training peut aider à renforcer la cyberrésilience parmi les utilisateurs grâce à des sujets recommandés par l'infrastructure de cybersécurité du NIST.