Cyber Guru

Cyber Guru Phishing add-on

PHISHPRO

EXTENSIONS DE FONCTIONNALITES

Cyber Guru Phishing, grâce à son modèle exclusif et innovant d'apprentissage automatique spécifiquement conçu pour la formation et l'entraînement, est capable de proposer une approche personnalisée et surtout adaptative et automatique, ce qui rend la formation beaucoup plus efficace et fonctionnelle pour faire face aux nouvelles techniques d'attaque cyber.

C'est précisément pour former les utilisateurs à différentes techniques d'attaque cyber que Cyber Guru propose l'Add-on **PhishPro**, qui étend les simulations d'attaque à deux composants numériques particulièrement intéressants pour les cybercriminels, les **clés USB** et les **codes QR**. L'Add-on offre également une formation anti-hameçonnage adaptative avec la fonctionnalité **Adaptive Learning Remediation**.

SIMULATION D'ATTAQUE USB

SIMULATION D'ATTAQUE QR CODE

ADAPTIVE LEARNING REMEDATION

Simulation d’attaque USB

En utilisant ce type particulier de simulation, il sera possible d’étendre la formation anti-phishing et de former le personnel à une utilisation consciente des dispositifs USB.

L’extension d’attaque par clé USB permet aux superviseurs de :

- Créer une clé USB contenant un fichier Microsoft Word “malveillant”.
- Accéder à un rapport, présent dans le tableau de bord de Remédiation et alimenté à chaque ouverture du fichier Word, qui mettra en évidence le nombre de fois où le Word a été ouvert.
- Analyser combien d’utilisateurs, en plus d’insérer la clé USB dans le dispositif, ont également accepté d’exécuter la macro Word, une action particulièrement dangereuse pour la sécurité qui exposerait l’organisation à un niveau supplémentaire de risque cybernétique.

Simulation d’attaque QR code

En utilisant ce type particulier de simulation, il sera possible d’étendre la formation anti-phishing et de former le personnel sur les risques qui pourraient se cacher derrière un QR code malveillant.

L’extension d’attaque QR code permet de réaliser des campagnes de simulation organisées de cette manière :

Les superviseurs auront la possibilité de créer des QR codes "malveillants" et de les distribuer au sein de l'organisation selon deux méthodes :

- Le QR Code pourra être imprimé et distribué. Le balayage, l'ouverture du lien associé au QR Code, ainsi que toute saisie d'informations supplémentaires sur la page d'atterrissage vers laquelle mène le lien du QR Code, seront surveillés.

- Le QR Code pourra être distribué via les habituelles campagnes de phishing de Cyber Guru Phishing par courriel.

Adaptive Learning Remedation

Avec ce type particulier de remédiation adaptative, il sera possible d’effectuer des actions de formation personnalisées envers les utilisateurs qui ont besoin de contenus éducatifs dédiés et axés sur la reconnaissance de la menace dont ils sont victimes.

À partir du tableau de bord de remédiation, les superviseurs pourront donc attribuer des contenus de formation dédiés à ce type d’utilisateurs définis comme “faibles” ou répondant à des critères similaires, fournissant ainsi une formation spécifique et axée sur la reconnaissance de la menace du phishing.