HORNETSECURITY

Fiche d'information

# NEXT-GEN SECURITY AWARENESS SERVICE

Renforcez votre pare-feu humain. Créer une culture de sécurité durable.

Notre service prochaine-generation, Security Awareness Service permet à vos employés d'apprendre grâce à des simulations réalistes de spear phishing et à une formation en ligne utilisant l'intelligence artificielle, en les sensibilisant aux risques et aux menaces de cybersécurité. Ils apprennent efficacement à se protéger et à protéger leur entreprise. Entièrement automatisé et facile à utiliser.

**Faits clés:**

- **Référence à la sensibilisation intelligente (ESI[MD])**
- **Formation en ligne en fonction des besoins**
- **Spear-Phishing-Engine**

## L'Employee Security Index (ESI[MD]) – Référence à la sensibilisation

- ESI[MD] - Employee Security Index est une référence unique dans l'industrie qui permet de mesurer et de comparer en permanence le comportement des employés en matière de sécurité dans l'ensemble de l'entreprise et contrôle les besoins individuels en formation en ligne.

## FORMATION EN LIGNE ADAPTÉE AUX BESOINS EN UTILISANT L'AWARENESS ENGINE

Le Awareness Engine est le cœur technologique de notre Security Awareness Service et offre la bonne dose de formation pour chacun : chaque utilisateur reçoit autant de formation que nécessaire et le moins possible.

- Mise à disposition des contenus de formation en ligne pertinents en fonction des besoins
- Option Suramplificateur pour les utilisateurs qui ont besoin d'une formation en ligne plus intense
- Contrôle entièrement automatisé de la formation en ligne

## SPEAR-PHISHING-ENGINE

- Simulation de spear phishing réaliste et personnalisée de différents niveaux de difficulté – afin que les employés puissent se familiariser avec les attaques les plus sophistiquées.
- Les scénarios de spam récents vous redirigent également vers de fausses pages de connexion et contiennent des fichiers joints avec des macros ainsi que des courriels avec des historiques de réponse.

À venir : en combinaison avec les solutions Hornetsecurity 365 Total Protection ou Spam and Malware Protection, le trafic de messagerie individuel peut même être inclus dans la simulation de spear phishing pour reproduire des attaques encore plus sophistiquées.

HORNETSECURITY

Fiche d'information

### LE CONTROL PANEL - DASHBOARD

- Le Awareness Dashboard donne un aperçu de tous les indicateurs importants des groupes de formation et des employés ainsi que du succès de la formation grâce à ESI[MD].
- Historique et prévisions ESI[MD]: Comment le ESI[MD] à l'échelle de l'entreprise a-t-il progressé jusqu'à présent et comment va-t-il évoluer ?
- Configurez et adaptez la formation sur la sensibilisation aux besoins de votre entreprise.

### LA SECURITY HUB

- Accès centralisé à tous les contenus d'apprentissage : les employés trouveront tous les contenus d'apprentissage de manière centralisée dans la Security Hub : des cours en ligne aux courtes vidéos, modules de remise à niveau et aux jeux-questionnaires.
- Contenus d'apprentissage et cours en ligne en plusieurs langues.
- L'approche de ludification encourage les utilisateurs à « donner le meilleur d'eux-mêmes ».

## SECURITY AWARENESS SERVICE - CARACTÉRISTIQUES PRINCIPALES

**Des attaques de spear phishing générées automatiquement et personnalisées, avec différents niveaux de difficulté. Y compris de fausses pages de connexion et des fichiers joints avec des macros.**

- Niveau 7 - La lecture cachée de la boîte aux lettres
- Niveau 6 - Historique des réponses aux courriels
- Niveau 5 - L`usurpation de domaine
- Niveau 4 - Titre d'emploi et division
- Niveau 3 - Entreprise et OSINT (intelligence de sources ouvertes)
- Niveau 2 - Spam par la direction (Niveau C)
- Niveau 1 - Distribution massive de spam

Scénarios de spam de niveaux 6 et 7 prévus pour une extension ultérieure.
Prérequis : Spam and Malware Protection ou 365 Total Protection.

### Awareness Engine

- Mode de formation automatique : le contenu de la formation est automatiquement déployé aux utilisateurs et aux groupes à la demande.
- Utilisateur unique et suramplificateur de productivité : les utilisateurs ayant des besoins d'apprentissage supplémentaires sont formés de manière plus intensive et utilisateurs ayant un très bon niveau de sécurité, en revanche, sont moins formés.
- Embarquement automatique des nouveaux utilisateurs (nécessite LDAP/AD Sync.)
- Mode de formation manuel : il est possible de déployer manuellement les modules de formation aux groupes et aux utilisateurs.