FICHE PRODUIT

Mimecast - protection avancée contre les BEC

Bloquez les compromissions d'e-mail professionnelles avec une solution de sécurité e-mail alimentée par l'IA, offrant une protection intégrée pour vos communications.

Le Problème

L'e-mail est au cœur des affaires, que ce soit pour échanger des informations sensibles ou faciliter des transactions majeures. Avec une telle dépendance à l'e-mail, la messagerie d'entreprise devient une cible de prédilection pour les compromissions d'e-mail professionnelles (Business Email Compromission - BEC) qui cherchent à exploiter ces communications sensibles. Les leurres de BEC évoluent constamment, nécessitant des outils qui ne reposent pas sur des signatures ou des heuristiques, d'où l'utilisation de solutions basées sur l'IA. Le défi posé par la combinaison de ces technologies est la complexité et la quantité de données à interpréter, tout en nécessitant une surveillance et un paramétrage humains constants en raison du grand nombre de faux positifs générés par les solutions uniquement basées sur l'IA.

La Solution

Pour prévenir les menaces BEC, les équipes de sécurité ont besoin d'une approche qui intègre plusieurs solutions éprouvées. Cette stratégie d'intégration doit prendre en compte les flux de menaces, les protocoles d'authentification des e-mails et les capacités avancées d'IA pour détecter les anomalies et identifier les e-mails suspects.

Alors que les attaques sans charge utile deviennent plus sophistiquées, il est impératif que vos méthodes de protection apprennent et s'améliorent en continu. Bloquez les compromissions d'e-mail professionnelles avancées avec une IA soutenue par des milliards de signaux, conçue pour détecter les menaces évolutives. Notre plateforme unifiée protège vos communications, assurant signaux faibles, une protection contre tout type d'attaque – pas seulement le BEC. Donnez aux administrateurs une visibilité sur les menaces ciblant vos utilisateurs et des informations exploitables pour prendre des décisions éclairées grâce à des tableaux de bord intuitifs et une modélisation des politiques de sécurité.

2,9 MILLIARDS

de dollars de pertes dues à la BEC en 2023*

25%

des attaques à motivation financière utilisent le BEC**

Ce que vous permet Mimecast

- **Détectez les attaques sans charge utile.** Bloquez les menaces avancées de compromission d'e-mail professionnel avec une IA avancée.
- **Renforcez les défenses avec une protection intégrée.** Une plateforme pour protéger les outils collaboratifs d'entreprise contre tout type d'attaque.
- **Obtenez une visibilité sur les menaces ciblant vos utilisateurs.** Donnez aux administrateurs les moyens de prendre des décisions éclairées avec des informations directement exploitables.

* https://www.ic3.gov/Media/PDF/AnnualReport/2023_IC3Report.pdf
** https://www.verizon.com/business/resources/reports/dbir/

Fonctionnalités	Détails
Graphe social	• Analyse de la relation hierarchique entre l'expéditeur et les destinataires au sein de l'organisation • Analyse de la réputation des communications entrantes/sortantes et des messages signalés par les utilisateurs • Vérification de domaine des courriels gratuits, récemment enregistrés et des typosquatting de marques communes
Analyse des messages	• Détection du langage spécifique aux menaces dans les courriels liés à des catégories de menaces BEC spécifiques, telles que les demandes d'aide pour une tâche, les faux virements bancaires, l'urgence, les changements de canaux de communication et les escroqueries liées aux cartes cadeaux, aux banques et à la finance. • Concentration sur la compréhension du contexte, des nuances et des implications du message afin d'interpréter avec précision l'intention réelle.
Analyse de la ligne d'objet	• Détection du langage spécifique aux menaces dans les courriels liés à des catégories de menaces BEC spécifiques, telles que les demandes d'aide pour une tâche, les faux virements bancaires, l'urgence, les changements de canaux de communication et les escroqueries liées aux cartes cadeaux, aux banques et à la finance. • Concentration sur la compréhension du contexte, des nuances et des implications du message afin d'interpréter avec précision l'intention réelle.
Administration	• Vue structurée et consolidée des informations critiques • Explication des détections offrant des preuves détaillées et les utilisateurs impactés • Identification des principaux utilisateurs ciblés affichant ceux qui reçoivent fréquemment des menaces BEC • Recherche à travers les menaces pour déterminer l'échelle et la gravité • Support pour des politiques et actions BEC personnalisables pour soutenir la tolérance au risque organisationnelle
Modélisation des politiques	• Évaluation de l'impact d'une modification du niveau de sensibilité • Comparaison des e-mails traités pour déterminer le statut de chaque niveau de sensibilité

Cas d'utilisation de la protection avancée contre les BEC

Se défendre contre les menaces BEC
Éliminez les menaces BEC en identifiant les activités suspectes et en créant un graphique social des interactions entre les utilisateurs, en analysant les expressions à risque et l'intention sémantique afin de déterminer l'objectif d'un e-mail.

Protection complète contre les BEC
La défense contre les menaces BEC ne peut pas s'appuyer uniquement sur l'IA pour identifier les modèles et les anomalies. Cela nécessite une approche combinant l'IA et des indicateurs éprouvés provenant des signatures et des flux de menaces, garantissant que les attaques sont stoppées au point de détection plutôt que de compter uniquement sur l'IA comme dernière ligne de défense.

Comprendre ce qui est bloqué et pourquoi
Être capable de trier facilement une détection BEC est important. Chaque détection de la protection avancée contre les BEC de Mimecast liste non seulement la politique qui a déclenché la détection, mais également les caractéristiques du risque qui ont conduit au verdict. En conséquence, les administrateurs passent moins de temps à déterminer la cause.

Modélisation simplifiée des politiques
Il n'est pas possible d'adapter constamment les politiques du BEC. Grâce à l'analyse historique des messages, identifiez l'impact d'un de l'historique changement de politique et déterminez les messages potentiels capturés par chaque niveau de sensibilité.