

Cyber AI Platform

Antigena Email

Développez l'immunité de votre boîte de réception

Aperçu

- ✓ Technologie auto-apprenante : s'intéresse à l'humain, pas seulement à l'adresse e-mail
- ✓ Identifie les e-mails malveillants qui échappent aux outils traditionnels
- ✓ Efficace contre les attaques les sophistiquées, y compris l'ingénierie sociale
- ✓ Déploiement virtuel rapide

Menaces par e-mail interceptées par Antigena Email

- Hameçonnage ciblé
- Ingénierie sociale et usurpation d'identité
- Piratage du compte de messagerie d'entreprise
- Piratage de compte dans la chaîne d'approvisionnement
- Fuite de données externes
- Logiciels malveillants nouveaux et inconnus

“ Nous avons été choqués par la quantité de choses qui échappaient à nos outils traditionnels et qui étaient interceptées par Antigena Email.

- CTO, Bunim/Murray Productions ”

De nouvelles menaces pour la messagerie apparaissent

Les attaques par e-mail sont de plus en plus sophistiquées, et l'utilisation agressive de l'IA menace de faire exploser la gravité des attaques dans un avenir proche.

De nouvelles attaques contournent régulièrement les outils traditionnels de sécurité de la messagerie. Dans un monde où les chaînes d'approvisionnement sont de plus en plus complexes et les employés de plus en plus éparés et mobiles, le recours à une approche auto-apprenante basée sur l'IA pour protéger la messagerie s'avère plus que jamais nécessaire.

“

Un changement de mentalité accompagné d'innovation est plus que jamais nécessaire pour sécuriser la messagerie moderne dans le paysage des menaces actuel.

”

- Gartner

La première boîte de réception au monde capable de s'auto-défendre

Antigena Email est la première solution de cyber IA au monde pour la boîte de réception. En apprenant le « modèle comportemental normal » de chaque utilisateur et de chaque correspondant, la technologie développe une compréhension évolutive du facteur humain derrière chaque communication par e-mail.

Là où les outils de défense traditionnels se demandent si les éléments d'un e-mail ont déjà été observés lors d'attaques antérieures, Antigena Email est la seule solution capable de détecter de façon fiable si l'interaction d'un utilisateur donné avec un e-mail précis est inhabituelle, dans le contexte de son « modèle comportemental normal », de celui de ses pairs et de l'organisation toute entière.

Cette connaissance contextualisée permet à l'IA de prendre des décisions fiables et de neutraliser toutes les attaques qui passent par la messagerie, des faux e-mails « clean » incitant les destinataires à effectuer des paiements frauduleux aux tentatives d'hameçonnage ciblé particulièrement sophistiquées.

Comprendre l'humain derrière la messagerie électronique

Inspiré par le système immunitaire humain, Antigena Email utilise l'intelligence artificielle au cœur de la technologie Darktrace pour développer une compréhension de l'identité de chaque utilisateur interne et externe en analysant les communications entrantes et sortantes, ainsi que les communications latérales qui restent en interne.

En traitant les destinataires comme des individus dynamiques et des pairs, Antigena Email détecte de façon unique les déviations subtiles de la « normalité », qui révèlent que des e-mails à l'apparence bénigne sont sans aucun doute malveillants.

Scénario d'utilisation : Piratage de compte dans la chaîne d'approvisionnement

L'une des attaques les plus difficiles à détecter est la prise de contrôle de compte, au cours de laquelle un criminel pirate les informations de connexion d'un contact de confiance pour accéder à sa boîte de réception.

Une fois infiltré, l'attaquant peut accéder à l'historique des correspondances et peut ainsi produire des e-mails particulièrement convaincants, en intégrant à la conversation un lien malveillant ou une pièce jointe infectée au moment opportun.

Tandis que les outils de défense traditionnels eux supposent qu'il s'agit d'un utilisateur de confiance, Antigena Email lui s'aperçoit que ce n'est pas le cas. Le logiciel analyse chaque e-mail dans le contexte des modèles comportementaux normaux qu'il a appris et détecte les écarts les plus subtils. Les facteurs déterminants incluent (sans toutefois s'y limiter) :

Emplacement de connexion inhabituel – Antigena Email peut extraire l'adresse IP géolocalisable de l'expéditeur authentique afin de déterminer si cet emplacement est rare par rapport au modèle comportemental normal habituel de l'utilisateur. Même si un emplacement de connexion rare ne déclenche pas nécessairement une alerte ou une action de réponse autonome, il est comptabilisé dans le calcul global du système et dans le score d'anomalie.

Rareté des liens – Les utilisateurs partagent souvent des liens vers les sites Web qu'ils consultent et auxquels ils font confiance. En observant ces liens dans le trafic e-mail latéral, Antigena Email peut identifier les liens et domaines rares dans le contexte de l'organisation. Cette approche est également utile dans d'autres scénarios, pour déterminer par exemple si le domaine de messagerie d'un expéditeur donné a été observé dans les liens partagés en interne.

Destinataires inhabituels – Antigena Email modélise de façon graphique les relations entre les utilisateurs internes et externes et leurs pairs et comprend chaque lien à un niveau granulaire. Si l'attaquant envoie plusieurs e-mails à de nombreux destinataires au sein de l'organisation, Antigena Email peut évaluer la probabilité que ce groupe spécifique reçoive un e-mail provenant de la même source.

Anomalies de comportement – Au fil du temps, Antigena Email apprend comment les différents expéditeurs construisent leurs e-mails, en analysant à la fois les métadonnées cachées dans les e-mails et les modèles récurrents dans le corps des messages. En appliquant l'IA à chaque e-mail entrant, Darktrace identifie les écarts subtils susceptibles de révéler que l'e-mail n'a pas été envoyé par le véritable propriétaire du compte.

En corrélant ces indicateurs faibles, Antigena Email calcule rapidement un score d'anomalie complet, qui détermine avec certitude que l'e-mail est malveillant et neutralise l'attaque avant qu'elle n'ait un impact.



Découvrez Antigena Email dans votre propre environnement avec un essai gratuit de 30 jours.



Réserver une démonstration
dès maintenant