vade FOR M365

DATA SHEET

DIGICOM SOLUTIONS

Détection des menaces basée sur l'IA et réponse aux incidents pour Microsoft 365

POURQUOI – La scalabilité, la réduction des coûts et la standardisation proposées par Microsoft 365 ont rendu Microsoft très populaire pour les business de toute taille. Sa notoriété auprès des cybercriminels pose de nombreux problèmes. Entre les attaques de phishing dynamiques et les ransomware de plus en plus difficiles à repérer, les menaces véhiculées par email sont devenues la première porte d'entrée vers la suite Microsoft 365. Les enterprises ont donc besoin d'une solution capable de repérer ce que Microsoft laisse passer.

SOLUTION – Vade for M365 offre une protection soutenue par l'IA contre les cyberattaques dynamiques véhiculées par email qui ciblent Microsoft 365. Vade for M365 est une solution basée sur l'API qui offre une expérience native dans Microsoft 365 et présente un taux de blocage 10 fois plus de menaces avancées que Microsoft.

AVANTAGE – L'intégration de l'API procure un avantage architectural par rapport aux solutions concurrentes, rendant Vade for M365 invisible aux yeux des cybercriminels dans les requêtes d'enregistrement MX, ce qui représente un atout crucial dans la sécurité de la chaîne logistique. De plus, l'intégration de l'API s'accompagne de fonctionnalités post-réception efficaces qui assurent une protection continue, avec des capacités de réponse aux incidents et une formation de sensibilisation des utilisateurs automatisée facile à intégrer dans votre offre de sécurité managée.

Avantages

- **10 fois plus de menaces bloquées par rapport à Microsoft**
- **Bloque les attaques sophistiquées en temps réel**
- **Neutralisation automatique post-réception**
- **Facile à déployer et à gérer**
- **Expérience native dans Outlook sans quarantaine externe**
- **Options de licence flexibles adaptées à votre entreprise**

Blocage des menaces dynamiques inconnues dans Microsoft 365

Vade for M365 exécute une analyse comportementale en temps réel de la totalité de l'email ; et ce grâce à une combinaison de technologies soutenues par l'IA qui vont plus loin que la simple analyse des signatures pour identifier des menaces inconnues et encore inédites.

Grâce à l'exploitation des données et des retours des utilisateurs issus de plus d'un milliard de messageries protégées dans le monde, le filtre d'email est mis à jour chaque minute et continuellement affiné, garantissant ainsi un taux de précision élevé.

Détection basée sur l'IA

- Protection contre le phishing
- Protection contre le spear phishing/BEC
- Protection contre les malwares et les ransomwares

Fonctionnalités post-réception

- Auto-remédiation
- Formation de sensibilisation des utilisateurs automatisée
- Boucle de rétroaction intégrée pour les utilisateurs finaux et les administrateurs

Capacités de réponse aux incidents

- Intégration SIEM et outils SOC
- Remédiation automatique des menaces post-réception
- Affichage d'une bannière d'alerte de spear phishing

Rapidité de déploiement et de configuration

- Déploiement en quelques minutes
- Assimile les paramètres Microsoft Exchange
- Aucune modification des enregistrements MX
- Paramètres faciles à activer/désactiver

Protection contre le phishing

Nos technologies de détection du spear phishing classent les menaces en fonction de leur typologie, notamment : les arnaques au président, les arnaques aux impôts, les demandes de virement, les arnaques à l'avocat et les contacts initiaux. Des technologies combinées basées sur l'IA, comprenant le traitement du langage naturel et des algorithmes de détection des usurpations, analysent les éléments d'un email susceptibles de révéler des anomalies et des schémas suspicieux, notamment :

- URL cachées
- Redirections d'URL
- URL à retardement
- Usurpation du nom
- Domaines voisins
- Images distantes
- Images et logos de marques altérés

Protection contre le spear phishing et le BEC*

Nos technologies de détection du spear phishing classent les menaces en fonction de leur typologie, notamment : les arnaques au président, les arnaques aux impôts, les demandes de virement, les arnaques à l'avocat et les contacts initiaux. Des technologies combinées basées sur l'IA, comprenant le traitement du langage naturel et des algorithmes de détection des usurpations, analysent les éléments d'un email susceptibles de révéler des anomalies et des schémas suspicieux, notamment :

- Adresses email et domaines usurpés
- Noms affichés factices
- Trafic de messagerie anormal
- Contenu textuel suspect

* En cas de suspicion de spear phishing, Vade affiche une bannière d'avertissement personnalisable.

Protection contre les malwares et les ransomwares

Notre technologie de détection des malwares et ransomwares vise les caractéristiques malveillantes des emails, pages web, fichiers partagés et pièces jointes, y compris les fichiers exécutables, les codes suspicieux, les macros malveillantes et les URL. Loin de se contenter d'une simple analyse de la signature, notre détection comportementale des malwares comprend les fonctionnalités suivantes :

- Vade for M365 analyzes mAnalyse comportementale basée sur le machine learning
- Analyse heuristique des emails, pages web et pièces jointes
- Analyse en temps réel des pièces jointes (PDF, Word, Excel, PPT)
- Analyse des fichiers hébergés (OneDrive, SharePoint, Google, WeTransfer)

Fonctionnalités post-réception et capacités de réponse aux incidents

Technologie basée sur l'IA, améliorée par les utilisateurs et conçue pour les admins débordés

- **Auto-Remediate -** Solution de réponse aux incidents entièrement intégrée qui scanne continuellement les emails post-réception et supprime automatiquement les messages des boîtes de réception dès la détection d'une nouvelle menace. Les administrateurs peuvent également neutraliser des messages manuellement en un clic.
- **Threat Coach™ -** Propose une formation automatisée et contextualisée pour corriger le comportement d'un utilisateur qui ouvre un email de phishing ou clique sur un lien de phishing. Grâce à des exemples réels d'email de phishing, Threat Coach enrichit l'apprentissage structuré avec du contenu de formation adapté qui permet de renforcer les bonnes pratiques.
- **Threat Intel & Investigation –** Threat Intel and Investigation est un module complémentaire premium pour Vade for M365 qui permet aux SOC d'exporter les journaux d'emails de Vade for M365 vers n'importe quel SIEM, XDR, ou EDR, de procéder à un examen approfondi des mails et des pièces jointes et d'intégrer Vade for M365 à leur stratégie XDR (détection et réponse étendues).
- **Boucle de rétroaction intégrée -** Transforme les retours des utilisateurs en informations stratégiques sur les menaces permettant de renforcer en permanence l'efficacité du filtre et de la fonction Auto-Remediate. La boucle de rétroaction permet aux administrateurs de signaler les emails à Vade depuis la console d'administration et aux utilisateurs de signaler les emails grâce au bouton Signaler le hameçonnage de Microsoft Outlook.
- **Journaux d'emails et rapports - O**ffre une visibilité immédiate sur les menaces détectées et neutralisées avec les tableaux de bord, rapports et journaux en temps réel. Les administrateurs peuvent garder un œil sur le trafic d'emails, repérer les menaces liées à des événements actuels et neutraliser les emails en un clic.

À propos de Vade

- 1 milliard de boîtes mails protégées
- 100 milliards d'emails analysés / jour
- 1400+ partenaires dans le monde
- Renouvellement annuel de 95%
- 18 brevets internationaux actifs

Contact

Digicom Solutions Sàrl
027 722 70 71
info@digicom-solutions.ch