vade
FOR M365

Sécurisation de la collaboration : une nouvelle approche de la sécurité des suites de productivité

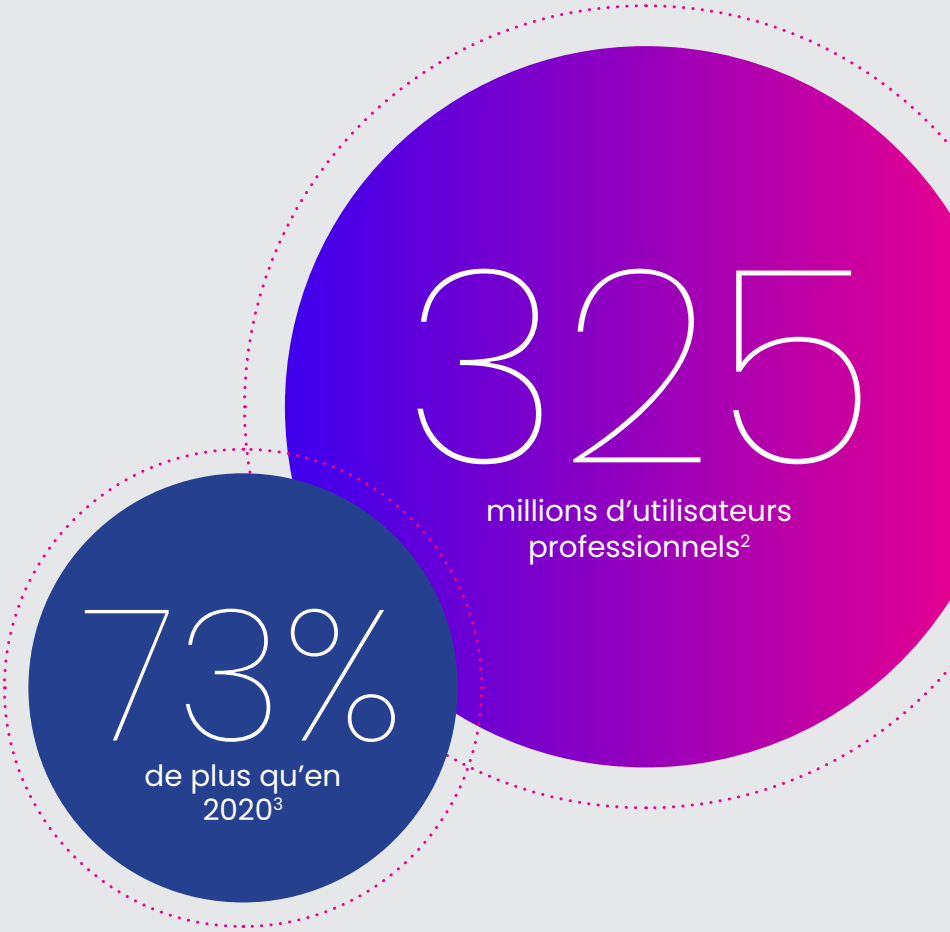
Table des matières

INTRODUCTION

La COVID-19 a révolutionné le fonctionnement des organisations de toutes tailles et de tous les secteurs. En effet, dès le début de la pandémie, les gouvernements les ont poussées à adopter le télétravail et la collaboration à distance. C'est ainsi que presque du jour au lendemain, le monde du travail est passé d'interactions physiques à des interactions numériques. Cette évolution soudaine a entraîné l'adoption rapide de suites de productivité comme Microsoft 365 et Google Workspace pour faciliter la communication et la collaboration.

Si la pandémie est aujourd'hui terminée, le monde professionnel moderne ne semble pas vouloir revenir en arrière. 40 % des organisations mondiales ont ainsi conservé des modes de travail hybrides, et ce nombre ne cesse d'augmenter.[1]

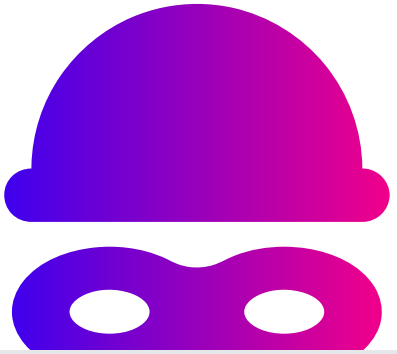
Aujourd'hui, Microsoft 365 est la suite de productivité la plus populaire au monde, avec plus de **345 millions d'utilisateurs professionnels,[2] soit presque 73 % de plus qu'en 2020.**[3] De son côté, Google Workspace continue de gagner des parts de marché et est désormais la deuxième suite de productivité la plus utilisée.[4] Le boom de ces deux outils n'est pas passé inaperçu des cybercriminels. Microsoft et Google sont ainsi respectivement les 1re et 2e marques les plus usurpées lors d'attaques de phishing.[5]



1. Gartner. "Gartner Forecasts 39% of Global Knowledge Workers Will Work Hybrid by the End of 2023." https://www.gartner.com/en/newsroom/press-releases/2023-03-01-gartner-forecasts-39-percent-of-global-knowledge-workers-will-work-hybrid-by-the-end-of-2023
2. Microsoft. "Earnings Release Q3 2022." https://www.microsoft.com/en-us/investor/earnings/fy-2022-q3/press-release-webcast
3. Microsoft. "Microsoft FY20 First Quarter Earnings Conference Call." https://www.microsoft.com/en-us/Investor/events/FY-2020/earnings-fy-2020-q1.aspx
4. Gartner. "Google Workspace Continues to Slowly Take Market Share From Microsoft Office and Office 365." https://www.gartner.com/en/documents/4004066
5. Vade. "Phishers' Favorites 2022 Year-in-Review: The 20 Most Impersonated Brands in Phishing Attacks." https://www.vadesecure.com/en/ebook-phishers-favorites-2022-year-in-review

Les hackers s'appuient sur les intégrations prises en charge par ces plateformes, et en particulier celles liées à l'email. En effet, les employés utilisent l'email pour effectuer de nombreuses tâches. Ouverture de documents à modifier, participation à des fils de messages instantanés ou accès à des pièces jointes volumineuses : l'email ne leur sert pas seulement à échanger des messages. Cette évolution a fait de l'email un vecteur plus intéressant pour les cybercriminels et le rend donc plus risqué pour les utilisateurs.

Par exemple, les hackers peuvent élaborer des campagnes de phishing qui semblent liées à des outils de productivité pour pousser leurs victimes à télécharger des malwares ou divulguer leurs identifiants. Après un premier exploit réussi, les hackers peuvent aussi exploiter les comptes compromis pour procéder à une reconnaissance interne et lancer des attaques plus ciblées et personnalisées qui tirent parti de l'intégration entre applications d'emails, de messages instantanés, de partage de fichiers et de stockage de documents.



La position des organisations est aujourd'hui plutôt précaire, car elles dépendent de ces outils pour chaque facette de leur activité. S'ils les font bénéficier d'une hausse appréciable de productivité, ils les rendent aussi plus vulnérables face aux conséquences dévastatrices des cyberattaques, notamment sur les plans financier, juridique, réputationnel et réglementaire. Pour combattre efficacement les cybermenaces émergentes, les organisations doivent donc adopter des solutions de cybersécurité adaptées aux réalités de l'espace de travail moderne, qui sécurisent les modèles dynamiques de collaboration.

Pour le dire autrement, elles ont besoin d'une cybersécurité collaborative.

FACTEURS À L'ORIGINE DE LA MULTIPLICATION DES MENACES

Si les suites de productivité ont su capter l'intérêt des cybercriminels, d'autres facteurs aggravent la situation des organisations. Nous pouvons notamment citer les modèles économiques malveillants, les technologies qui renforcent les capacités des cybercriminels et les contraintes de ressources.

1 **La montée en puissance du PhaaS**

L'émergence du Phishing-as-a-Service (PhaaS) et du Ransomware-as-a-Service (RaaS) a vraiment transformé la nature des menaces. Les cybercriminels expérimentés peuvent désormais développer et vendre des kits de phishing et ransomwares élaborés à des acteurs malveillants qui n'ont pas les compétences, l'envie ou le temps de le faire eux-mêmes.

Le PhaaS et le RaaS ont ainsi multiplié le nombre de cybercriminels actifs et élargi la disponibilité et l'accessibilité de campagnes sophistiquées. Ces deux systèmes ont contribué au renforcement de l'activité et de la dangerosité des menaces et forcé les organisations à muscler leurs mesures de sécurité.

2 **L'utilisation de l'IA à des fins malveillantes**

Dans le monde de la cybersécurité, l'intelligence artificielle (IA) a longtemps permis d'équilibrer les forces en présence. Les hackers possèdent en effet un avantage intrinsèque, car ce sont eux qui décident contre qui déployer des cyberattaques, à quel moment et par quel canal. Mais avec l'IA, les organisations ont pu adopter une stratégie de cybersécurité proactive pour éviter les menaces par email et autres formes de cyberattaques, les détecter et y répondre. Cette stratégie reste un facteur important de croissance de l'IA dans la cybersécurité, un marché qui devrait atteindre **133,8 milliards de dollars en 2030.**[6]

Si les outils basés sur l'IA ont renforcé la cybersécurité des organisations, ils ont aussi ouvert de nouvelles vulnérabilités. En effet, ces outils qui protègent les organisations des cybermenaces permettent aussi aux hackers de lancer des attaques plus fréquentes, ambitieuses et sophistiquées. Les chercheurs de Vade ont par exemple découvert que certains sont capables de créer des kits de phishing sophistiqués, notamment des modèles de phishing accompagnés de code malveillant, en seulement quelques secondes.

On voit ici que l'IA peut devenir une arme essentielle pour les hackers. Les opérateurs de PhaaS peuvent exploiter cette technologie pour accélérer la production de leurs kits, répondre à davantage de clients et se développer. Dans le même temps, l'IA permet aussi de créer un réseau PhaaS plus facilement pour les hackers moins talentueux. En limitant le besoin en connaissances et compétences spécialisées, l'IA multiplie les réseaux PhaaS, la disponibilité de kits de phishing et la cybercriminalité en général. Enfin, cet exemple n'en est qu'un parmi d'autres : l'IA est génératrice de valeur pour les hackers par de nombreux aspects.

6. Acumen Research and Consulting. "Artificial Intelligence in Cybersecurity Market Analysis." https://www.acumenresearchandconsulting.com/artificial-intelligence-in-cybersecurity-market

3

Les difficultés en lien avec les ressources humaines et la technologie

Alors même que les cybercriminels sont de plus en plus nombreux et actifs, les organisations continuent de rencontrer des difficultés pour recruter les spécialistes en informatique dont elles ont besoin. Une organisation sur trois ne dispose ainsi pas d'un nombre suffisant d'analystes des menaces, et près de quatre sur dix ont besoin de davantage d'administrateurs de sécurité informatique.[7]

Cette difficulté est aggravée par les outils de cybersécurité classiques, qui n'offrent pas une protection appropriée contre les menaces sophistiquées et inconnues. D'après une étude commandée par Vade, presque 77 % des PME se contentent de la sécurité de l'email de base incluse dans leur suite de productivité. 69 % des personnes interrogées ont par ailleurs avoué avoir été victimes d'une violation de données sérieuse liée à une menace contenue dans un email dans les 12 mois précédents.[8] Ces chiffres sont très inquiétants, d'autant plus que l'email reste le principal vecteur des cyberattaques et un des principaux moyens d'exploiter les suites de productivité.

Pendant que les organisations se débattent avec ces problèmes constants de ressources humaines et technologiques, les cyberattaques leur coûtent cher. Le cabinet McKinsey prévoit que les cyberattaques feront chaque année pour 10,5 mille milliards de dollars de dégâts d'ici 2025, soit 3 fois plus qu'en 2015.[9] Les PME et fournisseurs de services managés (MSP) assument une bonne partie de ces coûts, car les PME sont victimes de deux fois plus de cyberattaques et violations de données que les grandes entreprises.[10]

Adopter une cybersécurité collective est la seule solution pour faire face aux nouvelles menaces. Ce modèle intégré, coordonné et continu combine intelligences artificielle et humaine pour assurer une protection contre les cybermenaces les plus sophistiquées de notre époque.

de dégâts
d'ici 2025

7. CyberEdge Group. "2022 Cyber Defense Report." https://cyber-edge.com/cyberthreat-defense-report-2022/
8. Vade. "The Time for MSPs is Now: The 2022 SMB Cybersecurity Landscape Report." https://info.vadesecure.com/en/the-2022-smb-cyber-security-landscape-report-survey-results
9. McKinsey. "New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers." https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers
10. Verizon. "2022 Data Breach Investigations Report." https://www.verizon.com/business/resources/reports/dbir/

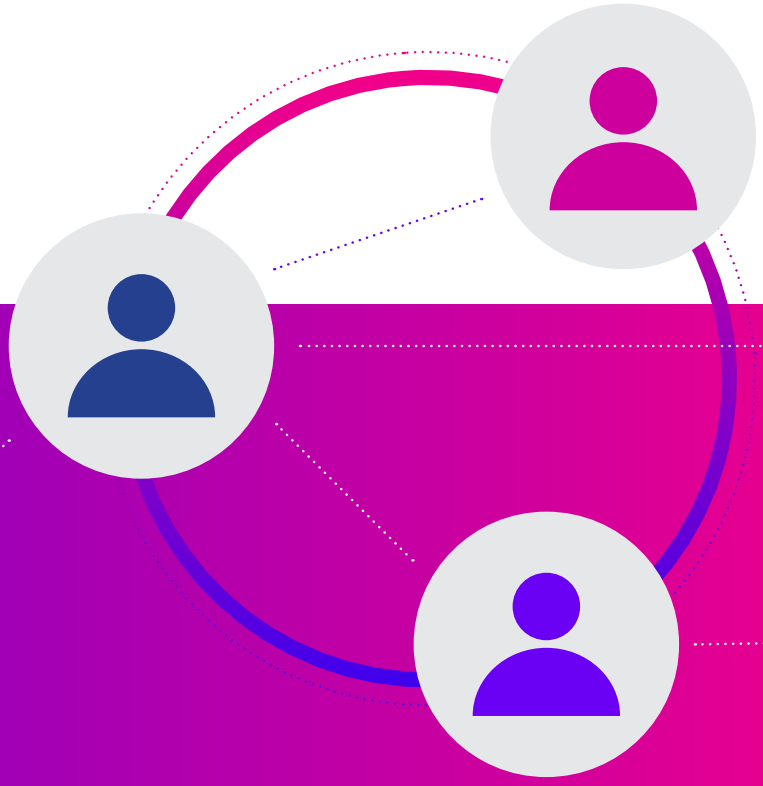
SÉCURISATION DE LA COLLABORATION

Les suites de collaboration constituent le principal, voire parfois le seul moyen de communication au sein des entreprises. La collaboration paraît sans fin, les utilisateurs sont submergés par un flux constant de communications. Lassés des emails, alertes, notifications de réunion et autres messages instantanés, ils se montrent moins vigilants et peuvent facilement se faire piéger par les cybercriminels.

Les experts en cybersécurité recommandent depuis longtemps d'adopter une sécurité à plusieurs niveaux. L'idée consiste à multiplier les solutions de sécurité pour qu'elles se complètent. Lorsqu'un niveau cède, un autre peut ainsi prendre le relais. Mais cette stratégie n'est pas une panacée. À un moment ou à un autre, toutes les solutions échoueront.

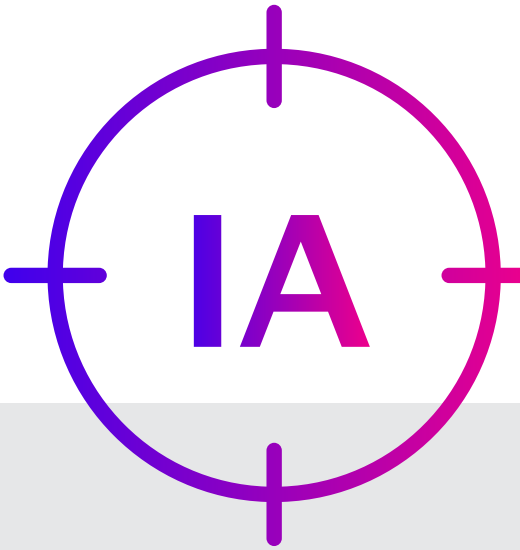
Pour sécuriser la collaboration, il est nécessaire d'affronter une vérité gênante : aucune solution ne peut détecter 100 % des menaces. Une telle approche place la réponse aux incidents aux avant-postes de la stratégie de sécurité et fait des utilisateurs un niveau de protection supplémentaire. En effet, les utilisateurs, qui sont certes les principales cibles des cyberattaques, peuvent fournir une protection supplémentaire, mais aussi les informations sur les menaces nécessaires à une amélioration continue de la sécurité.

Un modèle de cybersécurité collaborative combine ainsi les forces des utilisateurs et de la technologie en mettant en place une boucle d'amélioration tout en préparant dès le départ la réponse aux menaces qui parviennent à contourner vos défenses. Il se compose des éléments suivants, qui sécurisent la collaboration tout au long du cycle de vie des menaces.



Détection des menaces basée sur l'IA

La détection des menaces basées sur l'IA recourt au machine learning et à l'apprentissage profond pour analyser les menaces, et reconnaître les schémas et les obfuscations que les analyses classiques de l'URL ne voient pas. Cette détection se compose de plusieurs fonctions et capacités, notamment :



Algorithmes d'IA

Ces algorithmes se présentent sous différentes formes et vous protègent contre différents types d'attaques.

- Le **machine learning** analyse les éléments contenus dans les emails, les liens et les pièces jointes pour repérer des caractéristiques et schémas uniques, tels que des redirections, du code obfusqué et des URL temporaires.
- La **Computer Vision** analyse les images, comme les QR codes qui cachent des liens malveillants, les logos de marques altérés et les images hébergées à distance.
- Les modèles de **natural language processing** détectent les tournures grammaticales, mots et expressions subtils typiques des attaques de spear phishing.

Données

L'efficacité de l'IA dépend entièrement des données à partir desquelles elle est entraînée. Elle a ainsi besoin d'ensembles de données de grande qualité et statistiquement significatifs. Par « grande qualité », nous entendons des données représentatives, capturées en temps réel et actualisées en continu à partir de sources artificielles et humaines. Par « statistiquement significatifs », nous voulons dire que l'ensemble doit être suffisamment important pour être représentatif.

Boucle d'amélioration continue

L'IA dépend de l'intelligence des data scientists, des analystes en cybersécurité et des utilisateurs. Ce sont les data scientists qui créent les algorithmes à l'origine des filtres de l'IA. Les analystes en cybersécurité, quant à eux, se basent sur les informations sur les menaces pour affiner l'IA et lui permettre de détecter et neutraliser les menaces avec précision, tout en limitant les faux positifs et négatifs.

Enfin, les utilisateurs sont nécessaires pour actualiser en continu les algorithmes en signalant des données nouvelles et émergentes, par exemple des interactions suspectes avec des menaces qui n'ont pas encore été rencontrées. En collectant des informations sur les menaces et en signalant activement les interactions douteuses, les utilisateurs participent plus efficacement à l'amélioration de la détection des menaces et la réponse basées sur l'IA. Ce type d'intelligence humaine, qui crée une boucle d'amélioration continue, est indispensable à l'IA.

CAPACITÉS DE RÉPONSE AUX INCIDENTS

Pour créer un modèle de sécurité à plusieurs niveaux, les organisations ont besoin d'une technologie qui permet de répondre précisément et rapidement aux incidents de sécurité. Cette technologie doit offrir les capacités suivantes :

Remédiation automatique. Si une menace par email contourne la détection initiale ou devient active après sa remise, la remédiation automatique l'élimine directement des boîtes de réception en s'appuyant sur les nouvelles informations à sa disposition. L'IA est ensuite entraînée pour repérer plus efficacement les menaces similaires à l'avenir via un modèle d'auto-apprentissage qui ne demande aucune intervention humaine.

Remédiation manuelle. Une réponse aux incidents efficace nécessite également la capacité de remédier manuellement aux emails, notamment en neutralisant les menaces et en normalisant les emails qui n'en sont pas. Efficacité et rapidité sont ici clés. Les emails auxquels il faut remédier doivent pouvoir être localisés rapidement et traités simplement.

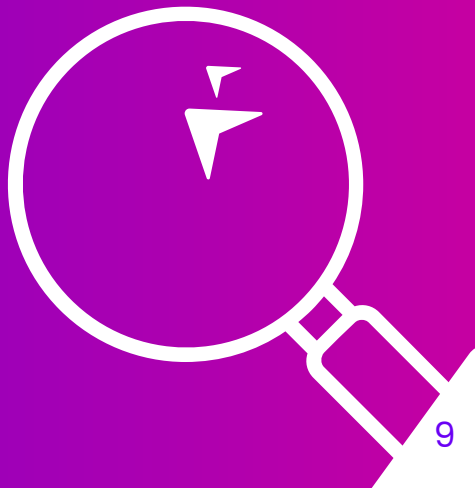
INFORMATIONS SUR LES MENACES ET ANALYSES

Une réponse aux incidents efficace dépend aussi de votre capacité à réunir des informations sur les menaces et à réaliser des analyses sur l'ensemble de votre réseau. Avec ces capacités de détection et de réponse, vous avez aussi besoin de solutions qui vous permettent d'analyser les menaces signalées par les utilisateurs, de réunir des données techniques et d'intégrer les informations à vos différents outils de cybersécurité.

Réponse aux incidents basée sur les utilisateurs. Les utilisateurs constituent une source d'informations essentielle. Votre solution doit donc leur permettre de signaler facilement les emails suspects et permettre aux administrateurs de les étudier en temps réel pour remédier à ces emails.

Analyse et inspection sécurisées des fichiers. La possibilité de télécharger et d'examiner en toute sécurité des emails potentiellement malveillants sans faire courir de risque aux administrateurs est particulièrement importante. Vous pouvez ainsi étudier des données techniques et les utiliser pour déterminer dans quelle mesure la menace a pu se propager dans votre réseau.

Intégrations aux systèmes SIEM, SOAR et XDR. L'email constitue le principal vecteur d'attaque et la principale source d'informations sur les menaces. Par conséquent, votre solution doit permettre l'importation des journaux d'emails dans les systèmes SIEM (Security Information and Event Management), SOAR (Security Orchestration and Automated Response) et XDR (Extended Detection and Response).



FORMATION DE SENSIBILISATION AU PHISHING

L'erreur humaine est la principale cause de violations de données.[11] Dans le cadre de cyberattaques, les interactions humaines concernent la plupart du temps des emails, et l'une des meilleures protections est donc une solution de formation de sensibilisation au phishing. Lorsque vous évaluez de telles solutions, intéressez-vous aux programmes qui présentent ces caractéristiques, qui permettent d'améliorer la mémorisation et l'application des connaissances.

Automatisation
Les utilisateurs ont besoin d'une formation ne nécessitant pas d'intervention humaine. En automatisant la formation, vous vous assurez de répondre aux besoins de vos utilisateurs sans alourdir la charge de travail d'administrateurs déjà bien occupés.

Personnalisation
Les exemples contextuels adaptés au monde réel optimisent la mémorisation et l'application des connaissances. C'est pour cette raison que vos utilisateurs ont besoin d'une formation imitant leurs expériences numériques du quotidien plutôt que d'exemples génériques qui ne sont pas représentatifs des menaces auxquelles ils sont confrontés au jour le jour dans leur travail.

Régularité et adéquation
La formation doit être permanente pour garantir que les utilisateurs se souviennent de ce qu'ils apprennent et connaissent les nouvelles tendances et techniques. Elle doit donc être actualisée en permanence et dispensée en continu et en fonction des besoins, dès qu'un utilisateur fait face à une tentative de phishing.

11. A Verizon. "2022 Data Breach Investigations Report." https://www.verizon.com/business/resources/reports/dbir/

VADE FOR M365

Vade for M365 est une solution de sécurité de l'email collaborative pour Microsoft 365 qui bloque les menaces avancées véhiculées par les emails et y remédie grâce à un moteur d'IA collaborative qui intercepte les éléments que Microsoft laisse passer. Le moteur d'IA de Vade est continuellement alimenté par les informations issues de plus de 1,4 milliard de messageries protégées, conjuguées à des millions de signalements d'utilisateurs quotidiens et à l'expertise de nos analystes en cybersécurité.

Vade for M365 couvre l'intégralité du cycle de vie des emails.

- Intercepte les menaces manquées par Microsoft grâce à des capacités de détection de pointe.
- Offre la visibilité, les outils et la technologie dont vous avez besoin si une menace parvient jusqu'aux boîtes de réception.
- Crée une boucle d'amélioration continue entre les utilisateurs et la technologie.
- Aide les utilisateurs à reconnaître et signaler les emails de phishing.
- Habitue les utilisateurs à contribuer plus efficacement à la boucle d'amélioration continue.

Fonctions et capacités clés

Anti-Phishing
Les algorithmes de machine learning et de Computer Vision exécutent des analyses comportementales, contextuelles et visuelles des emails et pages web afin d'identifier les attaques de phishing.

Protection contre les malwares et les ransomwares
Des algorithmes prédictifs et des analyses heuristiques examinent à la fois les comportements et le code pour détecter les malwares et ransomwares qui se cachent dans les emails, pièces jointes et fichiers hébergés.

Anti-Spear Phishing
Les algorithmes de détection des anomalies et de traitement du langage naturel décèlent les tentatives d'usurpation et les schémas malveillants dans les emails de phishing.

Classification du graymail
Les emails non prioritaires, comme les notifications des réseaux sociaux et des applications, encombrent les boîtes de réception des utilisateurs et nuisent à leur productivité. Vade relègue les emails non prioritaires dans des dossiers de graymail pour libérer les boîtes de réception, ainsi que le temps et l'attention des utilisateurs.

Auto-remédiation
Analysez en permanence les boîtes aux lettres et supprimez automatiquement les menaces après qu'elles ont été remises.

Formation automatique des utilisateurs
Proposez des formations au phishing contextuelles qui se déclenchent automatiquement lorsqu'un utilisateur interagit avec un email malveillant.

Threat Intel & Investigation
Triez les emails signalés par les utilisateurs et remédiez-y, décortiquez les emails et pièces jointes et exportez des journaux vers n'importe quel SIEM/SOAM/XDR.

Intégration native de Splunk
Exportez vos journaux d'email Vade for M365 vers Splunk sans écrire une seule ligne de code.

Solution intégrée et low-touch
Bénéficiez d'une sécurité de l'email intégrée nativement à Microsoft 365 et qui vient renforcer EOP et Microsoft Defender for Office 365. Notre solution se déploie en quelques minutes et ne nécessite pas de modifier sa configuration par la suite. Aucune modification des enregistrements MX ou de mise en place d'une quarantaine externe n'est nécessaire.

RESSOURCES

Fiche d'information : Vade for M365

Livre blanc : Microsoft 365 : Protégez votre entreprise face aux nouvelles menaces

À PROPOS DE VADE

Vade est une entreprise internationale de cybersécurité spécialisée dans le développement de technologies de détection et de réponse aux menaces grâce à l'intelligence artificielle. Les produits et solutions de Vade protègent les consommateurs, les entreprises et les administrations contre les attaques véhiculées par email, telles que les malwares/ransomwares, le spear phishing, les attaques Business Email Compromise et le phishing.

Créée en 2009, Vade protège 1,4 milliard de messageries professionnelles et personnelles et propose aux marchés des FAI, PME et MSP des solutions et produits reconnus qui permettent de renforcer la cybersécurité et d'optimiser l'efficacité informatique.

Suivez-nous sur
Twitter et **LinkedIn**

Inscrivez-vous à nos alertes blog :
www.vadesecure.com/fr/blog

Copyright ©2023 Vade