vade
FOR M365

DATA SHEET

Threat Intel & Investigation

Threat Intel and Investigation est un module complémentaire pour Vade for M365 qui fournit les intégrations, informations et outils nécessaires pour analyser les emails menaçant vos réseaux et y répondre. Exportez les journaux d'email Vade for M365 vers n'importe quel SIEM/EDR/XDR, réalisez des investigations numériques des emails et des pièces jointes, analysez et remédiez les emails signalés par des utilisateurs, et incorporez Vade for M365 à votre stratégie XDR.

Détection, investigation et réponse

Les emails constituent une mine d'informations sur les menaces auxquelles vos réseaux font face, mais les SOC ont toutes les peines du monde à surveiller et analyser les données de sécurité sur un grand nombre de terminaux. Threat Intel & Investigation fournit les informations sur les menaces dont vos SOC ont besoin pour recueillir des preuves techniques, recouper les menaces sur leurs réseaux et mettre au point des processus de réponse aux incidents.

Threat Intel & Investigation fournit par ailleurs l'accès à tous les composants clés de la technologie de filtrage Vade, qui permet à votre SOC d'approfondir l'analyse des emails malveillants et des pièces jointes dans vos journaux d'email Vade for M365.

Le monde de la cybersécurité évolue, et les surfaces d'attaque ne cessent de s'étendre. Threat Intel & Investigation s'adaptera à ces changements avec de nouvelles fonctions et améliorations qui aideront votre SOC à gagner en efficacité et limiteront la nécessité d'investir dans de nouvelles technologies.

FONCTIONS CLÉS

- **Exportation** des journaux d'email **Vade for M365** vers n'importe quel SIEM, XDR ou EDR
- **Analyse des fichiers et pièces jointes** pour découvrir des preuves techniques de la présence de malwares ou de phishing (URL, hachage, données décodées, objets, fichiers embarqués)
- **Analyse et réponse** aux emails signalés par les utilisateurs, ainsi que les emails qui leur ressemblent, mais sont passés inaperçus
- **Téléchargement des emails et pièces jointes** depuis les journaux pour analyse

AVANTAGES

- **Intègre** l'email à votre stratégie XDR
- **Centralise** des données de sécurité de l'email disparates
- **Améliore** la visibilité sur les menaces et la productivité des SOC
- **Renforce** les capacités d'analyse des menaces
- **Améliore** les dispositifs de défense
- **Diminue** le temps de réponse aux évènements de sécurité de l'email

Exportation de journal

Les journaux d'emails de Vade for M365 renferment de nombreuses informations sur les menaces qui visent votre entreprise. Grâce à Threat Intel & Investigation, vous pouvez exporter vos journaux d'email Vade for M365 vers n'importe quel SIEM, EDR ou XDR avec l'API REST de Vade.

L'intégration de vos journaux d'emails Vade for M365 à votre SIEM, XDR ou EDR vous permet d'examiner vos emails et autres points d'entrée depuis un espace centralisé. Bénéficiez d'une vue en temps réel de vos journaux d'email, et utilisez les informations recueillies pour permettre à vos SOC d'analyser les menaces, de les recouper entre vos différents réseaux et d'y répondre avec précision.

File Inspector

L'outil d'inspection des fichiers File Inspector révèle des informations sur les composantes et caractéristiques malveillantes des pièces jointes, comme le hachage, les URL, les objets, les données décodées et le code JavaScript. Les éléments de preuve ainsi recueillis peuvent être utilisés pour déterminer si les menaces détectées ont atteint d'autres activités de l'entreprise. Vous pouvez inspecter les fichiers et pièces jointes dans les journaux d'email ou bien importer les PDF et fichiers Microsoft Office pour analyse. Les types de fichiers acceptés sont PDF, doc, docx, xls, xlsx, ppt et pptx.

Emails signalés

Les emails signalés en tant que phishing ou spam par les utilisateurs finaux via le module complémentaire Outlook doivent être examinés par les administrateurs Microsoft 365 afin d'être triés et remédiés au plus vite. La fonction Emails signalés fournit une vue agrégée des emails signalés par les utilisateurs dans une seule et même interface de Vade for M365. Les administrateurs peuvent configurer des alertes pour les emails signalés par les utilisateurs, et analyser et remédier rapidement les emails signalés, ainsi que les emails qui leur ressemblent, mais qui sont passés inaperçus. Cette action entraînera aussi la remédiation des emails qui ont pu être transférés à d'autres utilisateurs.

Téléchargement des emails / pièces jointes

La possibilité d'analyser le contenu des emails et leurs pièces jointes est essentielle pour comprendre les typologies et caractéristiques des menaces par email. Avec Threat Intel & Investigation, vous pouvez télécharger des emails et leurs pièces jointes directement depuis vos journaux d'emails pour en inspecter le contenu.

Les exemples d'emails et pièces jointes permettent à votre équipe de comprendre la logique de filtrage de Vade, de collecter des preuves visuelles de la présence d'emails malveillants et de leurs pièces jointes et de les réemployer dans le cadre de la formation des utilisateurs.*

* Workflow d'approbation des utilisateurs finaux inclus.

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 organisations contre les attaques véhiculées par email, y compris les malwares/ransomwares, le spear phishing, les attaques Business Email Compromise et le phishing.

Fondée en 2009, Vade protège plus d'un milliard de messageries professionnelles et personnelles et propose aux marchés des FAI, PME et MSP des solutions et produits acclamés qui permettent de renforcer la cybersécurité et d'accroître l'efficacité informatique.

Contact Vade

sales@vadesecure.com

Demandez une démonstration de Vade for M365 sur

vadesecure.com

vade