vade
FOR M365

DATA SHEET

Threat Intel & Investigation

Threat Intel and Investigationは、Vade for M365のアドオンであり、ネットワークを通過するメールによる脅威を調査して対応するための統合的な機能や情報、ツールを提供します。Vade for M365のメールログを任意のSIEM／EDR／XDRにエクスポートし、メールと添付ファイルのフォレンジック検査を実施し、ユーザから報告されたメールを調査して修復し、Vade for M365を貴社のXDR戦略に統合します。

検出、調査、対応

メールはネットワークを攻撃する進行中の脅威に関する豊富な情報源ですが、SOCにとっては、エンドポイントの無数の配列からセキュリティデータを監視して分析することが課題となっています。Threat Intel & Investigationは、SOCがフォレンジック証拠を収集し、ネットワーク全体の脅威をクロスチェックし、インシデント対応プロセスを開発するために必要な脅威インテリジェンスを提供します。

Threat Intel & Investigationによって、Vadeのフィルタリングテクノロジーの主要コンポーネントにもアクセスできるようになります。これにより、SOCはVade for M365のメールログ内の悪意のあるメールと添付ファイルをより深く掘り下げられるようになります。

サイバーセキュリティの展望が広がり、攻撃対象領域が拡大するのに合わせて、Threat Intel & Investigationは、新機能と拡張機能を活かして進化し、SOCを強化しながら、追加のテクノロジー投資の必要性を抑えます。

主な機能

- Vade for M365のメールログを任意のSIEM、XDR、EDRにエクスポートします。
- ファイルと添付ファイルを調査し、マルウェアとフィッシングのフォレンジック証拠（URL、ハッシュ、デコードされたデータ、オブジェクト、埋め込みファイル）を見つけ出します。
- ユーザから報告されたメールや類似するメール、未報告のメールを調査して対応します。
- 調査のためにメールログからメールと添付ファイルをダウンロードします。

メリット

- メールを自社のXDR戦略に統合
- 異種のメールセキュリティデータを統合
- 脅威の可視性とSOCの生産性が向上
- 脅威の調査機能が向上
- 防御態勢を改善
- メールセキュリティイベントに応答する時間を短縮

ログのエクスポート

Vade for M365のメールログは、貴社のビジネスを狙う脅威に関する一連の情報を備えています。Threat Intel & Investigationでは、VadeのREST APIを使って、Vade for M365のメールログを任意のSIEM、EDR、XDRにエクスポートします。

VadeforM365のメールログをSIEM、XDR、EDRと統合することで、メールとその他のエンドポイントが1つの画面に集約されます。豊富なデータを提供するメールログのリアルタイムビューを使うことで、SOCは、脅威を調査し、ネットワーク全体で脅威をクロスチェックし、正確に対応できるようになります。

File Inspector

File Inspectorは、ハッシュタグ、URL、オブジェクト、デコードされたデータ、JavaScriptなど、添付ファイルの悪意のある特徴や要素の詳細を明らかにします。収集された証拠を用いて脅威をクロスチェックし、脅威が企業の他の領域に広がっているかどうかを判断できます。メールログからファイルと添付ファイルを調査したり、PDFとMicrosoft Officeファイルをアップロードして調査したりすることもできます。使用できるファイルの種類は、PDF、doc、docx、xls、xlsx、ppt、pptxです。

Reported emails

エンドユーザーがOutlookアドインを介してフィッシングまたはスパムとして報告したメールは、Microsoft365の管理者による確認を受け、迅速に検知されて修復されなければなりません。Reported emailsは、Vade for M365の単一のインターフェースでユーザーが報告したメールを確認できる集約ビューを提供します。管理者は、ユーザーから報告されたメールにアラートを設定し、ユーザーから報告されたメールとそれに類似する未報告のメールの両方を迅速に調査して修復します。この処理により、他のユーザーに転送されたメールも修復されます。

メールと添付ファイルのダウンロード

メールの内容と添付ファイルを分析する機能は、メールの脅威の類型と特性を理解するために不可欠です。Threat Intel & Investigationを使用すれば、メールログからメールとその添付ファイルをダウンロードして内容を調査できます。

メールと添付ファイルのサンプルによって、チームはVadeのフィルタリングの根拠を理解し、悪意のあるメールと添付ファイルの視覚的な証拠を収集して、ユーザートレーニング用のサンプルを確保します。*

*エンドユーザー承認ワークフローが含まれています。

Vadeについて

Vadeは、人工知能を用いた脅威検出と対応技術の開発を専門とする世界的なサイバーセキュリティ企業です。Vadeの製品とソリューションは、マルウェア／ランサムウェア、スピアフィッシング／ビジネスメール詐欺、フィッシングなどのメールを介したサイバー攻撃から消費者、企業、組織を保護します。

2009年に設立されたVadeは、企業や消費者の14億個以上のメールボックスを保護し、サイバーセキュリティの向上とIT効率の最大化に役立つ、受賞歴のある製品とソリューションを、ISP、中小企業およびMSPの市場に提供しています。

Contact Vade

sales@vadesecure.com

当社HPからVade for M365のデモをお申込みください

vadesecure.com