Cisco Secure Email Threat Defense リリースノート

はじめに

このドキュメントには、Cisco Secure Email Threat Defense の製品の更新、使用上の警告、および既知の問題に関する情報が含まれています。

2021 年 7 月 12 日から 2022 年 9 月 29 日までの Cisco Secure Email Cloud Mailbox のアーカイブリリースノートは、https://www.cisco.com/c/en/us/td/docs/security/cloud-mailbox/release-notes/cloud-mailbox-release-notes-archive.html [英語] から検索できます。

製品アップデート

2023 年 6 月 19 日

拡張機能

- メッセージルールをステータスでフィルタ処理して、アクティブまたは無効なルールを表示または非表示にすることができます。

修正済みの問題

- 軽微なバグ修正。

2023 年 6 月 9 日

拡張機能

- メッセージグラフとクイックフィルタが更新されました。
  - 1 日の始まりが週単位のビューで明確に強調表示されるようになり、特定の日を掘り下げることができます。
  - メッセージのフィルタ処理に使用できるリンクであることを示すために、脅威と方向のメトリックが青色で表示されます。

修正済みの問題

- 軽微なバグ修正。

2023 年 5 月 19 日

拡張機能

- このリリースで Cisco Secure Email Threat Defense パブリック API が導入されました。API を使用すると、安全でスケーラブルな方法でプログラムからデータにアクセスして使用することができます。API ドキュメントについては、https://doc.api.etd.cisco.com/ を参照してください。

修正済みの問題

- 軽微なバグ修正。

2023 年 5 月 11 日

拡張機能

- 2023 年 5 月 11 日以降に作成されたビジネスについては、スパムとグレイメールの分析がデフォルトでオフになります。この設定は、[ポリシー(Policy)] ページで調整できます。
- メッセージグラフとクイックフィルタ
  - [メッセージ(Messages)] ページの上部に、脅威とメッセージのグラフィカル表示が表示されます。
  - 脅威とカテゴリのブレークアウトにより、合計を表示し、脅威を簡単にフィルタ処理できます。
  - 検疫の合計が表示され、フィルタ処理できます。
  - メッセージの方向の合計が表示され、フィルタ処理できます。
- ホームページの [スキャンされたメッセージ(Messages Scanned)] グラフが、1 時間(日次表示)、3 時間(週次グラフポイント)、および 1 日(週次 X 軸ラベル)のカスタム期間を持つ [メッセージ(Messages)] ページにピボットするようになりました。

修正済みの問題

- 軽微なバグ修正。

2023 年 4 月 20 日

拡張機能

- Secure Malware Analytics の検出が [判定の詳細(Verdict Details)] パネルに [悪意のある侵入兆候(Malicious Behavioral Indicators)] のテクニックとして表示されます。
- Secure Endpoint の検出が [判定の詳細(Verdict Details)] パネルに [低スコアのファイルレピュテーション(Low File Reputation)] のテクニックとして表示されます。
- メッセージ受信者がソートされ、影響力の高い人員が最初にリストされます。

修正済みの問題

- 軽微なバグ修正。

2023 年 4 月 13 日

拡張機能

- Secure Email Threat Defense はさらに SecureX と統合されています。特定の監視可能なメッセージを統合型製品の SecureX ピボットメニューから直接隔離できるようになりました。さらに、ピボットを使用して、Secure Email Threat Defense で検索を開始できます。ピボットできる観測対象は次のとおりです。
  - [電子メールアドレス(Email Address)]
  - [電子メールメッセージ ID(Email Message ID)]
  - [電子メールの件名(Email Subject)]
  - [ファイル名(File Name)]
  - [送信者 IP(Sender IP)]
  - [SHA 256(SHA 256)]
  - [URL(URL)]

2023 年 3 月 22 日

拡張機能

- メッセージソースとして Cisco Secure Email Cloud Gateway を使用するビジネス向けの新しい認証なしモードが導入されました。この可視性のみのモードを使用すると、Microsoft への認証を行わずに、トラフィックを Secure Email Threat Defense に送信できます。このモードでメッセージを修復することはできません。この構成をサポートするように、新しいビジネスの初期設定フローと [ポリシー(Policy)] ページの設定が更新されています。

修正済みの問題

- 2023 年 3 月 12 日の夏時間の調整で導入されたグラフの表示方法に関する問題が解決されました。

2023 年 3 月 15 日

拡張機能

- [ユーザ プロファイル(User Profile)] メニューから、Secure Email Threat Defense システムステータスページへのリンクを使用できます。

修正済みの問題

- 軽微なバグ修正。

2023 年 2 月 27 日

拡張機能

- [ポリシー(Policy)] ページに、スパムとグレイメールの分析と修復をオンまたはオフにする新しいオプションがあります。オフにすると、スパムとグレイメールおよび無用なメールのパネルとオプションが削除されます。
  - 既存のアカウントについては、スパムとグレイメールの分析がデフォルトでオンになります。
  - Cisco SEG 構成の今後のアカウントについては、スパムとグレイメールの分析がデフォルトでオフになります。スパムとグレイメールの分析は、SEG によってすでに実行されています。
- 影響力の高い人員リストの個人用に構成された情報からの逸脱は、有害と判定されたメッセージの [判定の詳細(Verdict Details)] パネルで [テクニック(Technique)] として識別されます。

修正済みの問題

- 一部のお客様の環境で、Secure Email Threat Defense に到達する前に HTTP ヘッダーが削除されるというログインの問題が発生していました。この問題は解決されました。

2023 年 2 月 8 日

修正済みの問題

- 軽微なバグ修正。

2023 年 1 月 31 日

拡張機能

- ホームページに、日次と週次のデータの表示を切り替えるオプションがあります。
- [ポリシー(Policy)] ページの [インポートされたドメイン(Imported Domains)] セクションに、インポートされたドメインの総数と自動修復用にマークされたドメインの数が表示されます。リストには、部分一致検索でリストをフィルタ処理できる検索機能があります。
- 影響レポートの開始日が編集可能になりました。これにより、30 日の範囲、またはカレンダーの月ビューの月の最初の日付を選択できます。
- [メッセージ(Messages)] ページのフィルタで、フィルタがいつ適用されたかが示されます。フィルタの設定をデフォルトに簡単に戻せるように、ページの上部に新しい [すべてリセット(Reset All)] リンクが追加されています。[フィルタのリセット(Reset Filters)] ボタンは、使いやすいようにフィルタパネルの下部にあります。
- タイムラインビューに、受信、修復、再分類などのイベントの秒数が表示されるようになりました。
- 再分類のホバーテキストに日付と時刻が表示されるようになりました。
- 初期フィールドトライアルの新機能:影響力の高い人員リスト
  - 管理者は、最大 100 人のリストを作成して Talos に送信し、表示名と送信者の電子メールアドレスをさらに精査することができます。
  - **注**:今すぐリストを構築すると、今後のリリースで [判定の詳細(Verdict Details)] に [ユーザのなりすまし(User Impersonation)] のテクニックが表示されるようになります。

修正済みの問題

- 軽微なバグ修正。

2022 年 12 月 15 日

拡張機能

- [メッセージ(Messages)] ページのフィルタを使用して、送信者の IP アドレスで検索できるようになりました。
- 通知に [すべて消去(Clear All)] ボタンが追加されました。
- [設定(Settings)] > [ダウンロード(Downloads)] > [EML ダウンロード(Download EML)] ページで、メッセージの件名をクリックしてメッセージに簡単に戻ることができます。

修正済みの問題

- 軽微なバグ修正。

2022 年 11 月 17 日

拡張機能

- [メッセージ(Messages)] ページの [送信者(Sender)] 列の名前が [送信者(表示名/フレンドリ名)(Sender (Display Name/Friendly From))] に変更されました。

修正済みの問題

- 軽微なバグ修正。

2022 年 11 月 9 日

拡張機能

- メッセージソースとして Cisco Secure Email Cloud Gateway を使用できるようになりました。この初期リリースでは、サポートは Microsoft O365 メールボックスに限定されています。この構成をサポートするように、新しいビジネスの初期設定フローと [ポリシー(Policy)] ページの設定が更新されています。
- ブランドのなりすましの検出がサポートされるようになりました。構成の変更は必要ありません。現在 1500 のブランドがインデックスに登録されており、今後さらに追加される予定です。
- ホームページのダッシュボードに、過去 24 時間のビジネスの状態をすばやく表示する新しいウィジェットとグラフがあり、フィルタ処理されたメッセージのリストにすばやくピボットできます。内容は次のとおりです。
  - 脅威:BEC、詐欺、フィッシング、悪意のある検出の数が表示されます。
  - 無用なメール:スパムとグレイメールの検出のスパークライングラフが表示されます。
  - スキャンされたメッセージ:メッセージトラフィックのグラフが表示されます。

  - 侵害された可能性のあるアカウント：組織内から脅威メッセージを送信していることが確認された内部アドレスがリストされます。
  - クイックメッセージフィルタ：レトロスペクティブ判定、隔離状態のメッセージ、およびメッセージルールが適用されたメッセージへのクイックリンクが表示されます。
- Secure Email Threat Defense の新しいステータスページは https://ciscosecureemailthreatdefense.statuspage.io で利用できます。登録すると、ステータスに変化があったときに更新情報を受け取ることができます。

修正済みの問題

- 軽微なバグ修正。

2022 年 10 月 25 日

拡張機能

- Cisco Secure Email Cloud Mailbox は、Cisco Secure Email Threat Defense に名前が変更されました。この名前は、インターフェイス、ドキュメント、およびマーケティング資料全体で、段階的に変更されます。

修正済みの問題

- 軽微なバグ修正。

使用上の注意

Microsoft Excel のセルサイズの制限

Microsoft Excel では、セルあたり 32,767 文字の制限があります。データを CSV にエクスポートしてから Excel で開くと、文字数制限を超えるデータは次の行に移動されます。

Microsoft アカウントに姓が含まれていない場合、Microsoft で Security Cloud Sign On にサインインできない

Microsoft 365 では、アカウントに名前と姓を定義する必要はありません。姓が含まれていない Microsoft アカウントで認証しようとすると、Security Cloud Sign On は次のエラーを返します。

400 Bad Request. Unable to create the user. Required properties are missing.

この問題を回避するには、Microsoft 365 アカウントに姓と名の両方が定義されていることを確認します。

メッセージを手動で再分類すると、トレンドが遅延する

メッセージを手動で再分類すると、[トレンド（Trends）] ページに変更が反映されるまでに最大で 1 時間の遅延が生じることがあります。

既知の問題

Microsoft 許可リストと安全な送信者

Microsoft の MSAllowList フラグにおける最近の変更により、個々のユーザがメールボックス内の許可リストを設定することを組織が許可しており、メッセージがユーザの許可リストに含まれる場合、Microsoft 許可リストが Cisco Secure Email Threat Defense で常に適用されることはありません。

Cisco Secure Email Threat Defense でこれらの設定を適用する場合は、[ポリシー(Policy)] ページの [スパムまたはグレイメールと判定された Microsoft Safe Sender メッセージを修復しない(Do not remediate Microsoft Safe Sender messages with Spam or Graymail verdicts)] チェックボックスをオンにします。Safe Sender フラグは、スパムとグレイメールの判定では適用されますが、悪意とフィッシングの判定では適用されません。つまり、スパムまたはグレイメールと判定された Safe Sender メッセージは修正されません。

一部のインスタンスで組織 BCC が入力されない

メッセージの [組織 BCC(Organization-BCC)] フィールドは、BCC がユーザのドメイン内のメールボックスを対象とする場合に入力されます。社内メッセージでは、このフィールドがメッセージに明示的に設定されています。着信メッセージでは、これはメッセージヘッダーから推測されます。

一部の受信者が混合メールに含まれていない

混合メッセージ(内部受信者と外部受信者を含むメール)の場合、UI にはすべての受信者が表示されるわけではありません。

カンバセーションビュー

カンバセーションビューを使用すると、次の問題が発生する場合があります。

- 追加のメッセージがない場合でも、[+] 記号はクリックするまで表示されたままです。
- 水平ノードは 9 個に制限されています。

翻訳について
このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。