

2018年11月7日

MENDEL v3.2 では、ネットワーク全体を概観する新機能が追加されて、ネットワーク管理がしやすくなり、ネットワーク全体の状態を簡単に把握できるようになりました。

新機能

- ネットワークの概要、検出された脅威、およびリスク順に並べたホストを表示可能な新しい管理ダッシュボード
- データと情報を改善および簡略化した新しいセキュリティ・ダッシュボード
- 複数のセンサーからの情報を表示可能
- **Telnet**、**LDAP**、および **SNMP** の各プロトコルの分析に対応
- フロー内のアプリケーション・データの検索機能
- **Juniper Networks** 製ファイアウォールと統合

改善点

- **HTTP** リクエストに含まれるホスト名からホストを特定する機能を強化した
- サブネット・フィルタにより、**MENDEL** 内で定義されているサブネットかそれ以外のサブネットかをフィルタリングできるようにした
- 複数のセンサーからのデータを重複を省いて表示できるようにした
- アプリケーション・データのユーザー・パスワードをプロトコル解析で表示されないようにした
- フロー内のアプリケーション・データのレンダリングを強化した
- **Netflow** フローを一方向送信できるように改善した
- **Netflow** プロトコルの数値型の処理を改善した
- インシデント管理でコメントする際にユーザーをウォッチャーに追加した
- システム情報にセンサー名と **IP** アドレスを追加した
- **IP** ダイアログにダブルクリックで **IP** アドレスを選択するオプションを追加した
- ダッシュボードのメイン画面に新しいバージョンについての情報メッセージを追加した
- ファイアウォール・プラグイン統合を改善して考えられるエラー状態をすべて解決できるようにした
- インストール・ウィザードの使用言語を英語、チェコ語、中国語（簡体字と繁体字）、日本語から選択できるようにした

バグ修正

- 一部のアプライアンスでパケットが欠落する問題を修正した
- イベントのスクリーン画面の詳細表示に関する問題を修正した
- メモリ使用量のモニタリングに関する問題を修正した
- 無効な **IP** アドレスによるインストールの問題を修正した
- データ・インポート時の無効な日付形式に関する問題を修正した
- **SMTPS** フローの無効な検出に関する問題を修正した
- **IDS** コンポーネントのさまざまなセキュリティ問題を修正した

- 外部ホストおよびサブネットの設定が誤判定される問題を修正した
- 標準以外のポートのサービスの通知に関する問題を修正した
- データベース停止中の **IDS** および **Neflow** のデータ保存に関する問題を修正した
- ホスト名の割り当てに関する問題を修正した
- 速度の遅い接続時の設定の読み込みに関する問題を修正した
- ホスト・アナライザーが表示されない問題を修正した
- システム名サーバーの設定が失われる問題を修正した
- フィルタのサービス・タイプの妥当性が正しく検証されない問題を修正した
- プロキシ設定の再設定に関する問題を修正した
- センサー・コレクター・モデルのアップグレード・ステータスの通知に関する問題を修正した
- センサーとコレクターの接続に関する問題を修正した
- ソース **IP** アドレスと宛先 **IP** アドレスによるフィルタリングに関する問題を修正した
- **LEEF** フォーマットのエクスポート時のタイムアウトが長い問題を修正した
- **[Service]** ダイアログからリダイレクトした後のサービスのフィルタリングに関する問題を修正した
- データ・キャプチャのフィルタリング時の問題を修正した
- センサーの **SPAN** ポートの問題を修正した
- ホスト名のネットワーク・ゲートウェイへの割り当てに関する問題を修正した
- 長く続いているフローの通知に関する問題を修正した
- インシデントにリンクを挿入する場合の問題を修正した
- フィルタのサブネットの妥当性検証に関する問題を修正した
- 誤判定の説明に英語以外の文字が使用された場合の問題を修正した
- 特定のホスト名の誤判定に関する問題を修正した
- 通知メールのインシデントへのリンクを修正した
- システム再起動後のデータベースのメンテナンスに関する問題を修正した
- インストール・プロセス中の新規ディスク・パーティションの作成に関する問題を修正した
- 未使用および重複の **IDS** シグネチャを削除した
- 新規ユーザーのロギングに関する問題を修正した
- ステータス・モニタ・イベントのページネーションに関する問題を修正した
- フロー詳細の **SMTPS** アプリケーション・データの表示に関する問題を修正した
- 停止時のセンサーからの通知に関する問題を修正した
- プラグインの設定に関する問題を修正した
- **SMB** セキュリティ・パラメータの分析時の問題を修正した
- 特殊な **DHCP** メッセージの分析時の問題を修正した
- **IDS** イベント詳細のテーブル設定の保存に関する問題を修正した
- センサーからセントラル・イベント管理へのデータの通知に関する問題を修正した
- データ処理の復元に関する問題を修正した