# バージョン12リリースノート

Flowmon ADS

注：VerUP時には再起動、及びファイルチェックが行われる場合があります。

| Ver.No | リリース日 | 追加機能 |
|---|---|---|
| Ver.12.03.01 | 2024/5/29 | 修正された不具合 |
| | | インポートされたIP情報は、「一般IP情報」の他のタブに関係なく表示されるようになりました。 |
| | | 関連するエンドポイントは、バイナリ値（0 - 非アクティブ、1 - アクティブ）を含むアクティブフィールドを返すようになりました。 |
| | | マスターユニットは、サービスポータルからの更新（6時間ごとに発生）後に何らかの変更があった場合にのみ、ブラックリストとBPATTERNをプッシュします。 |
| | | 名前の3番目の位置に "x "文字があるフィルターが削除されなくなりました。 |
| | | SVRNAメソッドの実装が調整され、TCP SYNフラグのみを持つリクエストフローを失敗としてカウントするようになりました。 |
| | | SuspiciousExtServiceが、ローカル範囲内のパブリックIPアドレスに対しても正しく動作するようになりました（LANフィルタに追加した場合）。 |
| | | ユーザー権限設定でユーザーに割り当てられているフィルター名のみが表示されるようになりました。 |
| | | 新機能 |
| | | 新たに追加された２つのウィジェットにより、セキュリティ体制を強化し、最も重要な脅威に焦点を当てることが容易にできるようになりました。 |
| | | Flowmon ADSウィジェットのIPアドレスとメソッドのコンテキストメニューを拡張し、ダッシュボードやレポートから解析画面への遷移がシームレスになりました。 |
| | | 個々のテナントのための独立したデータスペースと、別々のコンフィギュレーションを利用可能にするマルチテナント機能が追加されました。 |
| | | DNSトラフィックの異常を検出する方法を改善しました。 |
| | | 特定のサブメソッドを無効にすることができるようになりました。 |
| | | イベント詳細画面に、関連性の高いTOP20のターゲットを表示する機能が追加されました。 |
| | | 解析の概要セクションを有効/無効にすることができるようになりました。 |
| | | Flowmon ADS 12.3以降、Flowmon ADSで設定された分散アーキテクチャ(DA)は、Flowmonコンフィギュレーション・センターで設定された同等のFlowmon DAなしでは動作しません。FlowmonコンフィギュレーションセンターでDAを設定するか、Flowmon ADSでDAを無効にしてください。 |
| | | MISPサーバーへの接続は、Flowmonプロキシ設定を尊重するようになりました。 |
| | | 既知の不具合 |
| | | REST APIコールは、ユーザーが作成されたテナントでのみ機能します。現在のところ、テナントを切り替えるAPIコールはありません。つまり、ベーステナントの管理者は、REST APIを使用しREST APIコールは、ユーザーが作成されたテナントでのみ機能します。現在のところ、テナントを切り替えるAPIコールはありません。つまり、ベーステナントの管理者は、REST APIを使用して設定を調整するためにサブテナントに切り替えることはできません。て設定を調整するためにサブテナントに切り替えることはできません。 |
| | | 複数のブラウザタブで作業し、1つのタブで別のテナントに切り替える場合、テナントが手動で切り替えられていないタブで変更を行うと予期しない問題が発生するため、他のタブを更新する必要があります。 |
| | | Delete events after パラメーターは、12.3.0より低いバージョンで検出されたイベントに対して正しく機能しません。この問題は安定版リリース前の 12.3.x で修正される予定です。 |
| Ver.12.02.01 | 2023/11/29 | 修正された不具合 |
| | | MITRE ATT&CK マトリックスのチャプターの列が常に PDF ページサイズに合い、はみ出さないようになりました。 |
| | | サードパーティのCurlライブラリ CVE-2023-38545の脆弱性を修正しました。 |
| | | イベントの証跡の添付フローで、ローカル時間ではなくサーバー時間が表示されるようになりました。 |
| | | 解析の概要でホストを表示するには、脅威スコアが以前の値に比べて少なくとも+20%増加する必要があります。 |
| | | トリガーされたトラフィック記録の開始時間が、ユーザーガイドでより詳しく説明されるようになりました。 |
| Ver.12.02.00 | 2023/10/5 | 修正された不具合 |
| | | Flowmon ADSからエクスポートされたCSVファイルに、UTF-8 BOMが含まれるようになりました。これによって、日本語のCSVファイルをExcelで開く際に発生していた問題が修正されました。 |
| | | チェコ語版ユーザーガイドの「Delete events marked as false positives」の翻訳を修正しました。 |
| | | フィルタの内容の変更が、対応する誤検知除外ルールに正しく反映されるようになりました。 |
| | | 新機能 |
| | | IDSイベントの調査を効率化するため、新しいIDSイベント解析が導入されました。 |
| | | 解析の概要と脅威スコア機能が追加されました。 |
| | | IPアドレスに対応するアプリケーションやプラットフォームに関する情報が提供されるようになりました。 |
| | | ブラックリストは望ましくないアプリケーションやシャドーITとの通信を警告するために利用できるようになりました。 |
| | | ライセンス制限により処理されなかったフローが表示されるようになりました。 |
| | | DICTATTACKメソッドが改善されました。 |
| | | SCANSメソッドが改善されました。 |
| | | ユーザーガイドオンラインプラットフォームから入手できるようになりました。 |
| | | REST API ユーザーガイドに変更履歴が追加されました。 |
| | | デフォルトの外部サービスにVirusTotalが追加されました。 |
| | | MITRE ATT&CKマッピングがバージョン13に更新されました。 |
| | | 無効化されたメソッドに関するSYSCHECK警告メッセージの重大度が増加し、syslogレポートがトリガーされるようになりました。 |
| | | PHPがバージョン8.1にアップグレードされ、Flowmon 12.3およびFlowmon Packet Investigator 12.2と互換性があります。 |
| Ver.12.01.03 | 2023/7/17 | 修正された不具合 |
| | | BPATTERNSのメソッドインスタンスの編集および保存時にエラーが発生する問題が修正されました。 |
| | | ASNまたはホスト名のみの誤検知除外は、フィルタが削除されても削除されなくなりました。 |
| | | DHCPANOM: サブメソッドOversendingClientIPの誤検知除外が正しく適用されるようになりました。 |
| | | XMLファイルのインポートでインポートされた誤検知除外が、選択されたメソッドインスタンスを正しく反映するようになりました。 |
| Ver.12.01.02 | 2023/5/10 | 修正された不具合 |
| | | 過去5分間に0バイトのフローのみを受信した場合、ADS処理エンジンが再起動する不具合が修正されました。 |
| | | ADS12.1へのアップデート後、MISPサーバーのIP（hosts）ブラックリストが正しく動作するようになりました。以前は、ブラックリストが更新されるまで、ブラックリストは動作しませんでした。 |
| | | 新機能 |
| | | REFLECTDOS: DoS攻撃を増幅するためのSLPプロトコルの悪用（CVE-2023-29552）を検出するために拡張されました。 |
| Ver.12.01.01 | 2023/3/14 | 修正された不具合 |
| | | API: REST API ドキュメントのフィルタ章が改善されました。 |

| | | |
|---|---|---|
| | | フィルタ作成時の invert と atomize アクションが修正されました。 |
| | | 特殊文字「&」、「"」、「>」、「<」が名前フィールドに正しく表示されるようになりました。 |
| | | インターネットサービスプロバイダー（ISP）のテンプレートを適用すると、企業ネットワークのデフォルト設定が削除されない問題を修正しました（LANフィルタ,Operational issues, and Security issuesパースペクティブ）。 |
| | | ユーザー エクスペリエンスに対するマイナーな修正と改善がされました。<br>- ブラックリストのファイルは、CR EOL形式でアップロードできるようになりました。<br>- データ フィード列が正しく並べ替えられるようになりました。<br>- 誤検知除外にて「誤検知除外イベントの削除：すべて」が正しく機能するようになりました。<br>- ADS アプライアンス ログのサイズが小さくなりました。<br>- 無効なアトミックフィルタをインポートするときのエラー メッセージが改善されました。 |
| | | 新機能 |
| | | リモートアクセスアプリケーションの活動を検出するためのカスタムブラックリストとして、以下のブラックリストを追加することができます。<br>- IPベースのブラックリスト：<br>https://services.flowmon.com/reputation/optional/applications-ioc_ip.csv<br>- ドメインベースのブラックリスト：<br>https://services.flowmon.com/reputation/optional/applications-ioc_domain.csv |
| Ver.12.01.00β | 2023/1/31 | 修正された不具合 |
| | | SCANSメソッドのメソッド固有のパラメータとオプションのパラメータが正しく表示されるようになりました。 |
| | | SVRNA メソッドは、「イベント証跡」で正しいフローを表示するようになりました。 |
| | | 「検出方法に割り当て」機能の使用状況が記録され、「ログ」ページで使用状況を確認できるようになりました。 |
| | | 新機能 |
| | | DNS over HTTPS（DoH）トラフィックを検出するための新しいメソッド「DOHDET」が追加されました。<br>DoHトラフィックは、ネットワーク監視ツールから隠れるため、悪意のある活動や通信を隠すために使用することができます。<br><br>このメソッドは、DoH 通信とサーバを検出する 2 つのサブメソッドで構成されます。<br>- 1つ目のサブメソッドは、既知の DoH サーバのリストに基づいています。<br>- この方法は、DoHサーバを正確に検出するためにSNI情報に依存するため、HTTPS情報を有効にしたFlowmon Probeが必要です。<br>- フロー データで SNI を有効にするには、Flowmon ユーザガイドの 4.3.1 高度な設定 と 5.1 FMC設定 を参照してください。<br>- 2つ目のサブメソッドは、フロー データの行動パターンを検査する高度なアルゴリズムを使用しています。<br>- SNIが利用できない場合、既知のDoHサーバとの通信にサブメソッドが適用されます。<br>- SNIを必要とせず検出が機能しますので、Flowmon プローブは必要ありません。<br><br>備考：<br>- このメソッドは、自動的にアクティブ化されず、定義されたパースペクティブ (デフォルトのパースペクティブを含む) に追加されません。<br>- このメソッドは、設定 → 処理 → メソッドで有効にすることができます。<br>- 検出されたイベントを表示するには、設定 → 処理 → [パースペクティブにて手動で本メソッドをパースペクティブに追加する必要があります。 |
| | | 以下のメソッドについて、検出精度の向上とユーザへのチューニングオプションの追加を目的として、改良、拡張、または再構築を行いました。<br><br>RDPDICT：<br>- 本メソッドは、RDP プロトコルの現在のバージョンに対する攻撃を確実に検出するように改訂されました。<br>- ユーザが検出を調整できるように、新しいメソッドのパラメータが導入されました。<br><br>TEAMVIEWER：<br>- DNSドメイン名が利用できない場合にASN（Autonomous System Numbers）を新たに利用することで、この手法の精度を向上させた。<br>- TEAMVIEWER メソッドで ASN を使用するには、フロー データにASN情報を含む必要があります。<br>- Flowmon Probeからのフローデータは、設定に基づきASNでエクスポートすることができます。<br>（Configuration center ＞モニタリングポート＞ 高度な設定にて設定可能）<br>- サードパーティーのフローソースがフローデータにASNをエクスポートすることができない場合、FlowmonCollector側でフローにASNを拡張することができます。<br>- この機能は、Configuration center＞ FMC設定＞ ASにて有効にすることができます。<br><br>DNSANOMALY：<br>- ForbiddenServer サブメソッドで、ローカル DNS サーバがパブリック DNS サーバと通信したときの誤検出を排除するために、許可されていないサーバとの通信の検出からローカル DNS サーバを除外できるようになりました。<br>- これを行うには、「PolicyExceptions」という新しいパラメータに、ローカルDNSサーバを使ったフィルタを割り当てます。<br><br>RANDOMDOMAIN：<br>- メソッドが処理するトラフィック（DNS、HTTP/HTTPS、またはその両方）を指定するパラメータを追加しました。<br>- これにより、例えば、ランダムドメインとのHTTP(S)通信のみをレポートし、DNS 変換のみとの通信はレポートしない（または、パースペクティブでDNSトラフィック用の別のメソッドインスタンスを使用することにより、<br>より低い優先度でレポートする）ことができます。<br><br>BLACKLIST：<br>- IP ブラックリスト形式には、ブラックリストに登録された IP アドレスに関する追加情報を提供するオプションのコメント フィールドが含まれるようになりました。コメントは「イベント詳細」に表示されます。 |
| | | IP アドレスの「一般情報」の詳細が拡張されました。<br>- ブラックリストに登録されたIPアドレスに対して「一般情報」を表示した場合、そのIPアドレスが属しているすべてのブラックリスト名とコメントが詳細に表示されるようになりました。<br>- 変更により、CSVファイルにIPアドレスと自身のコメントを追加することで、ブラックリストに登録されたIPアドレスにコメントを追加することも可能になりました。<br>- このCSVファイルは、ADSのカスタムブラックリストとして追加することができ、コメントは「一般情報」の詳細に表示されます。<br>- カスタム ブラックリストは 6 時間ごとに更新されるため、多少の遅延が生じる場合があります。 |
| | | イベントテーブルにカスタマイズ可能な列を追加して、「イベント詳細」を開かなくても重要な情報を表示できるようにしました。<br>- IP ビュー テーブル (イベント テーブル) は、テーブル ヘッダーからカスタマイズできるようになりました。<br>- 以下の列を表示/非表示にすることができるようになりました。<br><br>「Method Instances」、「 Comments」、「 Categories. 」<br>- 「イベント」 ページの既存のテーブル カスタマイズ オプション ( 簡易リスト、ホスト別、MITRE 別) は、同じ列で拡張されました。<br>- イベントのコンテキスト メニューには、イベントにコメントを追加するオプションも含まれるようになりました (カテゴリを割り当てる既存のオプションに追加されました)。<br>- 管理者以外のユーザも、イベントにコメントを追加したり、カテゴリを割り当てたりできるようになりました。<br>- これを有効にするには、設定 ＞ システム設定＞ 一般設定にて設定できます。<br>- 現在、この設定はブラウザのクッキーに保存されています。 |
| | | イベント証跡 から Monitoring Center ＞ 解析への直接リンクが追加され、イベント調査が合理化されました。<br>- リンクを使用すると、Monitoring center＞ 解析への新しいタブが開きます。<br>- 解析は事前に設定されており (対応する期間、プロファイル、チャネル)、フィルタも事前に入力されています。 |
| | | MITRE ATT&CK マッピングがバージョン 11 に更新されました。<br>- MITRE ATT&CK v11 のプリセットは、Dashboard and Reportsで利用できます。 |
| | | ADS の GUI が更新され、Progress のブランドに合わせて新しい色とロゴが追加されました。 |
| Ver.12.00.04 | 2022/11/22 | 修正された不具合 |
| | | 誤検知除外の並び替えが正しく動作するようになりました。 |

| | | |
|---|---|---|
| | | 設定ウィザードで「一般的な企業（最大500台のコンピュータ）、TCPフラグなしのフローデータ」を適用する際にRANDOMDOMAIN、TEAMVIEWER、TORが有効になるように修正されました。 |
| | | 日本語版でHIGHTRANSFのイベントの詳細の転送済みデータ量が正しく表示されるようになりました。 |
| Ver.12.00.03 | 2022/6/1 | 修正された不具合 |
| | | 誤検知除外のルールを、SIPデータフィードに適用すると、処理エンジンが再起動してしまう不具合を修正しました。 |
| | | パースペクティブでメソッドインスタンスを選択すると、設定が保存できない不具合を修正しました。 |
| | | 既知の不具合 |
| | | チェコ語と日本語のユーザーガイドはPDFにエクスポートすることができません。 |
| | | 設定ウィザードにて「会社のネットワーク」の「一般的な企業(最大500台のコンピュータ)、TCPフラグなしのフローデータ」テンプレートを使用した設定を行うと、RANDOMDOMAINメソッドはデフォルトでインアクティブに設定されます。Ver.12.00.04にてデフォルトでアクティブに設定される予定です。 |
| Ver.12.00.02 | 2022/5/10 | 修正された不具合 |
| | | IDS Collectorのメモリ割り当て量が多すぎる原因で、パフォーマンスが低下する不具合を修正しました。 |
| | | RANDOMDOMAINのメソッドインスタンスが自動的に作成されるようになりました。<br>- このメソッドは、定義されたパースペクティブ（デフォルトのパースペクティブを含む）には自動的に追加されません。<br>検知されたイベントを表示するには、手動でメソッドをパースペクティブに追加する必要があります。 |
| | | 新機能 |
| | | チェコ語と日本語のユーザーガイドを追加しました。 |
| | | 既知の不具合 |
| | | ADSのユーザーガイドに新たに追加された説明は、チェコ語と日本語に翻訳されていないものがあります。 |
| Ver.12.00.01β | 2022/4/6 | 修正された不具合 |
| | | TELNETメソッドは、TCPおよびUDPトラフィックに制限されるようになりました。 |
| | | MULTICASTメソッドで検出されたイベントに、マルチキャストアドレスの説明を再度表示するようにしました。 |
| | | イベント証跡で「添付されたフロー」のフローテーブルのヘッダーが、RANDOMDOMAINメソッドに対して正しく表示されない問題を修正しました。 |
| | | Flowmon ver12にFlowmon APMをインストールされている場合、Flowmon ADSが正しくインストールされない不具合を修正しました。 |
| | | 既知の不具合 |
| | | チェコ語と日本語のユーザーガイドは現在利用できず、今後リリースされる12.0.x（安定版より前のバージョン）で利用可能になる予定です。 |
| | | 12.00.00バージョンで変更されたメソッドのイベント詳細は、現在日本語では利用できず、今後リリースされる12.0.x（安定版以前のバージョン）で利用可能になる予定です。 |
| Ver.12.00.00β | 2022/3/2 | 修正された不具合 |
| | | 設定ウィザードで、IPアドレス範囲 172.16.0.0/12 の LAN フィルタが正しく作成されない不具合を修正しました。 |
| | | BPATTERNメソッドインスタンスが定義されていない場合、システムメッセージで警告メッセージの原因となる古いBPATTERNは処理されなくなりました。 |
| | | ADSのREST APIドキュメントが更新され、さまざまな問題とドキュメントの不一致が修正されました。 |
| | | DHCPANOMALYメソッドのServerChange サブメソッドに関する不具合を修正しました。 |
| | | これにより、現在のMACアドレスが更新されず、イベント詳細にて以前のMACアドレスと現在のMACアドレスが同じに表示されてしまう不具合を修正しました。 |
| | | DAモードで期限切れのライセンスを更新した後、ADSが停止してしまう不具合を修正しました。 |
| | | イベント詳細で「トラフィックレコード」タブが表示されない不具合を修正しました。 |
| | | 誤って設定されたシステムで、多数のイベントがある場合、GUIが応答しなくなる問題を修正しました。 |
| | | HIGHTRANSFメソッド：TransferThresholdパラメーターの制限が正しく動作されない不具合を修正しました。 |
| | | 新機能 |
| | | ランダムドメインを自動的に検出するための新しいメソッド「RANDOMDOMAIN」が追加されました。<br>これは、マルウェアに感染したデバイスがコマンド＆コントロールサーバーと通信していることを示すことができます。<br>- このメソッドは、第2レベルのドメイン名の複数のプロパティを解析し、ランダムなドメイン名パターンが使用されているかどうかを評価します。<br>- このメソッドでは、「HTTPホスト名」または「DNSフィールド」を含めているフローが必要です。「HTTPホスト名」または「DNSフィールド」を有効にするには、Flowmonユーザガイドを参照してください。 |
| | | 以下のメソッドは、検出精度を高め、ユーザに分かりやすい情報を提供するために、改良、拡張、または再構築しました。<br>TOR：<br>- TORネットワークを利用した悪意のある通信を検出する際に正確な結果が得られるように、TORメソッドを再構築しました。このメソッドは現在、2つのサブメソッドで構成されています。<br>- ClientDirectAccessサブメソッド ：TORネットワークへのアクティブな接続があるネットワーク内のデバイスを検知します。（TORブラウザ、TORベースのOSディストリビューション、またはTORに接続する他のクライアントを介して）<br>- ServerAccessサブメソッド：TORネットワークから監視対象デバイス（インターネットからアクセス可能なサーバなど）への接続試行を検知します。<br>ANOMALY：<br>- 予測値の計算が改善され、メソッドの精度が向上しました。<br>- イベントの詳細が変更され、現在値と以前値ではなく、現在値と予測値の間の増加分が表示されるようになりました。<br>- SCANS：<br>- SCANSメソッドは、 TCP connect scanを検知するように拡張されました。<br>- スキャンが成功したときにフローを分析することにより、TCP SYNスキャンの検知精度を改善しました。（サービスはスキャンされたポートでリッスンしています）<br>- SYN\|RSTを持つフローが必要です。 |
| | | 誤検知除外ルールの定義は、きめ細かいチューニングを可能にするため、新しいオプションが追加されました。<br>- ユーザは、誤検知除外でAS番号（Autonomous System Number）とFQDN（Fully Qualified Domain Name）を定義することにより、正当な自律システム（Microsoft、Google、Amazonなど）やドメイン（*office365.comなど）のトラフィックをメソッドの処理から除外することができるようになりました。<br>- 定義されたAS番号のすべてのトラフィックは、それぞれのAS番号（それらに紐づけられたIPアドレス範囲）に対する処理から除外されます。<br>- 誤検知除外のルールでAS番号を使用するには、フローデータにAS番号が含まれている必要があります。<br>Flowmonプローブからのフローデータは、設定に基づきAS番号でエクスポートされます（ Configuration Center > モニタリングポート > 高度な設定で確認できます）。<br>サードパーティーのフローソースがフローデータにAS番号をエクスポートしていない場合、Flowmonコレクター側でAS番号を使用して、フローを拡張することができます。この機能は、Configuration Center > FMC 設定 > ASにあるFlowmon Collectorで有効にすることができます。<br>- HTTP/HTTPSおよびDNSトラフィックのみが、それぞれのFQDNの処理から除外されます。<br>- 誤検知除外のルールでFQDNを使用するには、「HTTPホスト名」または「DNSフィールド」を含めているフローが必要です。この機能を有効にするには、Flowmonユーザーガイドの「4.3.1高度な設定」および「5.1FMC設定」を参照してください。<br>- 誤検知除外のルールをすべてのメソッドインスタンスまたは選択したメソッドインスタンスに適用できるようになりました。 |
| | | 添付されたフローはイベントの詳細で表示され、検知されたイベントの解析を改善しました。<br>- 「フローの添付」は、システムがイベントを検知したフローを基にしたリストです。<br>「フローの添付」機能はデフォルトでは無効になっています。この機能を有効にするには、設定 > システム設定 > ストレージ設定 に移動し、「フローの添付」を有効にします。<br>- 添付フローの機能を有効にすると、イベント詳細 > イベント証拠のサブタブに表示されます。<br>- Monitoring Centerに保存されているフローを表示するイベント証跡は「MONITORING CENTER」のサブタブで、添付されたフローは「添付されたフロー」のサブタブで確認することが可能です。 |

| | | |
|---|---|---|
| | | カスタムパターンでMITRE ATT＆CKの戦術とテクニックにマッピングできるようになりました。<br>SYSCHECKメソッド：<br>- Event floodのパラメーターは、設定ミスによりあまりにも多くのイベントを検知し、システムパフォーマンスに影響を与えるメソッドを無効にする際に、より厳しくなりました。<br>- パラメーターのデフォルト設定は、5分間に最大100イベント、1時間に最大1000イベントに変更されました。この値は、設定 > 処理 > SYSCHECKメソッド > インスタンスの編集で設定することができます。 |
| | | ADSのREST APIを改訂および拡張しました。<br>- ADSのREST APIに SNMP 及び Syslogのエンドポイントが追加されました。<br>- 詳細な情報についてはADSのREST API ドキュメントを参照してください。 |
| | | Flowmon OS 12.0との互換性を追加しました。 |
| | | 既知の不具合 |
| | | チェコ語と日本語のユーザーガイドは現在利用できず、今後リリースされる12.0.x（安定版より前のバージョン）で利用可能になる予定です。 |
| | | 12.00.00バージョンで変更されたメソッドのイベント詳細は、現在日本語では利用できず、今後リリースされる12.0.x（安定版以前のバージョン）で利用可能になる予定です。 |

# バージョン11リリースノート

Flowmon ADS

注：VerUP時には再起動、及びファイルチェックが行われる場合があります。

| Ver.No | リリース日 | 追加機能 |
|---|---|---|
| Ver.11.04.02 | 2021/11/22 | 修正された不具合 |
| | | 誤検知除外にてフィルタ名にカンマが含まれていても問題が発生することはなくなりました。 |
| | | 週次のメール通知が、カレンダーの週と一致しない問題を修正しました。 |
| | | Dashboard＆ReportsでMITRE ATT&CKチャプターをCSVとしてエクスポートする時、「戦術のみ表示」オプションがエクスポートされない問題を修正しました。 |
| | | 既知の不具合 |
| | | イベント詳細のメソッド固有の属性の一部が二重に表示され、異なるフォーマットになっています。この問題は、複数のメソッド（サブメソッド）で発生します。（DHCPANOM、DICTATTACK、IPV6TUNNELなど） |
| | | レポートをCSVでエクスポートする際に、チャプター設定の「すべてのシリーズ」チェックを外さない限り、「フロー概要」チャプターにデータが含まれない（チャプターの編集 > ウィジェット > 時系列グラフ > すべてのシリーズ）。 |
| Ver.11.04.01 | 2021/10/26 | 修正された不具合 |
| | | DA (Distributed Architecture) モードにおいて、スレーブコレクターでメモリを大量に消費する問題を修正しました。 |
| | | MISPブラックリストが正しく更新されるようになりました。 |
| | | 誤検知除外の使用状況の更新は、誤検知ルールが大量にあるインストール用に最適化されました。<br>更新が遅いと、フローチャートにピークが生じる可能性がありました。 |
| | | 新機能 |
| | | チェコ語と日本語のユーザーガイドを追加しました。 |
| | | 既知の不具合 |
| | | イベント詳細のメソッド固有の属性の一部が二重に表示され、異なるフォーマットになっています。この問題は、複数のメソッド（サブメソッド）で発生します。（DHCPANOM、DICTATTACK、IPV6TUNNELなど） |
| | | レポートをCSVでエクスポートする際に、チャプター設定の「すべてのシリーズ」チェックを外さない限り、「フロー概要」チャプターにデータが含まれない（チャプターの編集 > ウィジェット > 時系列グラフ > すべてのシリーズ）。 |
| Ver.11.04.00 | 2021/9/30 | 修正された不具合 |
| | | ANOMALYメソッドは、イベント詳細にてソースの通信ピア（peers）の数を正しく表示するようになりました。 |
| | | 新機能 |
| | | 誤検知除外：<br>- 誤検知除外のルール処理が再実装され、検出されたイベントではなく、ルールがフローデータに直接適用されます。<br>この変更により、ベースラインの精度が向上したり、イベント詳細の提供する情報の信頼性が向上したり、システムのパフォーマンスが向上します。<br>- 検出メソッドがフローデータを処理する前に、バックエンドで誤検知除外のルールが適用されるようになりました。<br>- 「時間の妥当性」パラメーター（ 以前の名前は「検知時間」）は、誤検知除外のルールが評価されるタイミングで<br>制限されます。「時間の妥当性」の間隔内の開始時刻を持つルールに一致するフローデータのみがドロップされます。<br>- 新しい誤検知除外の使用状況チャートが追加され、誤検知除外の使用数が置き換えられます。<br>これは、過去24時間は10分間隔、過去7日間は1時間間隔でのルール使用量を示しています。<br>- 誤検知除外ルールの評価がシステムパフォーマンスに与える影響は少なくなりました。 |
| | | 検知メソッド（メソッドインスタンス）：<br>- 検知メソッド（メソッドインスタンス）は、パースペクティブ定義の一部として構成して、より詳細なイベントレポート構成を<br>提供できるようになりました。<br>- パースペクティブの「高度なフォームで表示」では、異なるメソッドインスタンスに異なる優先順位を設定することができます。 |
| | | イベントのチャート：<br>- イベントのチャートは、より快適な色で表示され、チャートとメソッドの凡例の間をナビゲートしやすくなりました。<br>- イベントのチャートは、「最新」と「コントラスト」の2つのモードが用意されました。<br>最新：<br>- このモードは、読みやすさを向上させるためにグラデーションが調整されたチャートです。<br>- メソッドの凡例がチャートの色に対応するようになり、ナビゲーションが改善されました。<br>コントラスト：<br>- このモードでは、イベントのチャートとメソッドの凡例に勾配を使用せず、最高の読みやすさとナビゲーションを実現します。<br>- ユーザは、イベントチャートの設定アイコンをクリックすることで、チャートモードを選択することができます。<br>上記の設定は一時的なものです。<br>永続的な設定では、「ユーザ設定」ページにて変更することができます。 |
| | | Syslogメッセージ：<br>- Syslogメッセージは、メソッドインスタンス名（すべてのメソッドの場合）とブラックリスト名（BLACKLISTメソッドの場合）で拡張され、ユーザがSIEMなどのサードパーティツールでSyslogメッセージをフィルタリングおよび<br>処理できるようになりました。<br>- Flowmon ADSによって生成されるすべての可能なイベントのサンプルメッセージは、Kempポータル(https://support.kemptechnologies.com/) で入手することができます。 |
| | | MITRE ATT&CK：<br>- イベント詳細画面ではMITRE ATT&CKに関連性の無いイベントはFlowmonカテゴリに分類され、明確に関連性が無いことを示すようになりました。<br>- MITRE ATT&CKマッピングを最新バージョン9に更新しました。 |
| | | イベント証跡：<br>- イベント証跡からエクスポートできるTXTファイルの内容と書式を改善しました。<br>- このファイルには、イベント属性を含む、イベント詳細の全情報が含まれています。 |
| | | 製品使用状況データの収集：<br>製品を改善するために、アプライアンスのコンフィグレーションに関する個人を特定できないデータのみを収集する機能、（使用統計、有効な機能、一般的な構成など）が導入されました。<br>Flowmonアプライアンスに保存された、あるいはアプライアンスによって処理された顧客データを収集することはありません。<br>収集されたデータは、コンフィグレーションセンター ＞システム＞システム設定 ＞メンテナンス ＞製品使用状況データの収集にて確認することができます。<br>製品使用状況データを有効にしますと、収集されたデータは安全な通信チャネルを介して外部サーバーに送信されます。<br>本機能はデフォルトで有効になっており、コンフィグレーションセンター ＞ システム ＞システム設定＞ メンテナンス＞ 製品使用状況データの収集より無効にすることができます。 |
| | | 既知の不具合 |
| | | イベント詳細のメソッド固有の属性の一部が二重に表示され、異なるフォーマットになっています。この問題は、複数のメソッド（サブメソッド）で発生します。（DHCPANOM、DICTATTACK、IPV6TUNNELなど） |
| | | チェコ語と日本語のユーザーガイドは現在提供されておらず、今後リリースされる11.4.x（安定版より前のバージョン）で提供される予定です。 |
| Ver.11.03.03 | 2021/9/8 | 修正された不具合 |
| | | IDS イベントの詳細が IDS イベントブラウザで正しく表示されるようになりました。 |
| | | 既知の不具合 |
| | | イベント詳細のメソッド固有の属性の一部が二重に表示され、異なるフォーマットになっています。この問題は、複数のメソッド（サブメソッド）で発生します。（DHCPANOM、DICTATTACK、IPV6TUNNELなど） |
| Ver.11.03.02 | 2021/7/7 | 修正された不具合 |
| | | イベント証跡にポート23（UDP）トラフィック上で検出されたTELNETイベントのフローが正しく含まれるようになりました。 |
| | | ANOMALYメソッドで「増加(パーセント)」属性が負の数の場合に、大きなパーセント増加を表示しなくなりました。 |

| | | |
|---|---|---|
| | | 新機能 |
| | | Dashboard and ReportsにMITRE ATT&CKのプリセットが追加されました。<br>このプリセットは、MITRE ATT&CKマトリックスのチャプタを含む複雑なMITRE ATT&CKレポートの作成を支援し、　　インフラの状態を迅速に報告します。<br>これは、個々の攻撃者の戦術を示し、対応するイベントの番号/リストとともに表示します。<br>（各MITRE ATT&CK戦術のチャプタを含みます。）<br>戦術のチャプタには、その特定の戦術にマッピングされた検出イベントの詳細なリストが含まれています。 |
| | | Flowmon ADSは、Kemp Technologies, Inc.が提供する他の製品やコンテンツに合わせて、新しいカラーパレットとロゴを使用しています。 |
| | | 既知の不具合 |
| | | イベント詳細のメソッド固有の属性の一部が二重に表示され、異なるフォーマットになっています。この問題は、複数のメソッド（サブメソッド）で発生します。（DHCPANOM、DICTATTACK、IPV6TUNNELなど） |
| Ver.11.03.01β | 2021/6/23 | 修正された不具合 |
| | | 「 < 」および「 > 」記号が、メソッドのインスタンス名に使用できない問題を修正しました。 |
| | | イベント処理のパフォーマンスが改善されました。 |
| | | ADSのアップグレードの失敗につながる問題を防ぐために、ADSのアップグレード中はイベント処理を停止するようになりました。 |
| | | COUNTRYメソッドで検出対象の国が1つしか選択されていない場合にエラーが発生する問題を修正しました。 |
| | | 新機能 |
| | | 解析とイベント機能でDS-Lite形式のIPアドレスのフィルタリングが使用できるようになりました (例： ::ffff:8.8.8.8)。 |
| | | チェコ語と日本語のユーザーガイドを追加しました。 |
| | | REST APIガイドがADSバージョン 11.3 に更新されました。 |
| | | 既知の不具合 |
| | | イベント詳細のメソッド固有の属性の一部が二重に表示され、異なるフォーマットになっています。この問題は、複数のメソッド（サブメソッド）で発生します。（DHCPANOM、DICTATTACK、IPV6TUNNELなど） |
| Ver.11.03.00β | 2021/5/17 | 修正された不具合 |
| | | MULTICASTの検出メソッドで、/23以上のネットワークにおいて、.255で終わるすべてのIPアドレスがブロードキャストトラフィックとして検出されなくなりました。 |
| | | 集約ビューでメソッド名がクラスター化するまれな問題を修正しました。 |
| | | HIGHTRANSFメソッドで検出されたすべてのケースのイベントで、転送されたデータの正しい値が詳細に表示されるようになりました。 |
| | | 新機能 |
| | | MITRE ATT&CKのフレームワークを使用したイベントの可視化、レポート、解析機能を拡張する新機能が追加されました。 |
| | | MITRE ATT&CK のウィジェットがDashboard and Reportsに追加され、ユーザがセキュリティの状況を迅速に把握できるようになりました。 |
| | | MITRE ATT&CK マトリックスには、検出されたイベント数と、対応する戦術とテクニックがマッピングされており、インタラクティブなウィジェットで表示されるようになりました。<br>このウィジェットでは、マトリックス全体（戦術とテクニック）、または戦術のみを視覚化できるようになりました。 |
| | | ウィジェットから新しいMITRE ATT&CKのイベントタブ「BY MITRE ATT&CK」を表示し、さらにドリルダウンして解析することができるようになりました。 |
| | | 「BY MITRE ATT&CK」タブは、Flowmon Anomaly Detection System＞イベントを拡張し、検出されたイベントに関する新しいビューを提供できるようになりました。 |
| | | 検出されたイベントは各MITRE ATT&CKの戦術ごとに集約されます。各戦術を展開すると、個々のイベントのリストが表示されるようになりました。 |
| | | リストには、各戦術の合計数と検出されたイベントが表示されます。検出されたイベントがない戦術は表示されなくなりました。 |
| | | MITRE ATT&CKの2つの新しいチャプタがレポートに表示されるようになりました。 |
| | | 「MITRE ATT&CK Matrix」のチャプタは、ダッシュボードのウィジェットに対応しており、マトリクス全体または戦術のみを可視化することもできるようになりました。 |
| | | MITRE ATT&CKチャプタは、チャプタ設定で指定された戦術から BY MITRE ATT&CKのビューに対応するようになりました。 |
| | | Flowmon Anomaly Detection System＞イベントの「さらに多くのフィルタ」で、MITRE ATT&CK techniquesが拡張され、このフレームワークを使ったイベント解析に役立つようになりました。 |
| | | 事前定義ダッシュボードのSecOpsにMITRE ATT＆CKウィジェットが追加されるようになりました。（新規に作成した定義済みのSecOpsダッシュボードにのみ適用されます。） |
| | | 誤検知外の定義に追加された「Detection time(検出時間)」パラメータでは、誤検出ルールを適用する特定の日や時間帯を設定できるようになりました。この時間間隔で検出されたイベントは、誤検出としてマークされます。このオプションは、その時間間隔の間にトリガーされたイベントにのみ適用されます。更新されるイベントはこのオプションの影響を受けません。このオプションは、ターゲットフィルタやIPアドレスと一緒に使用することができなかった従来の「イベント時間」パラメータを置き換えるものです。 |
| | | イベント詳細の属性が、人間が読める形式で表示されるようになりました。属性は、共通の属性とメソッド固有の属性に分かれています。各属性には、名前、説明、およびフォーマットされた値があります。複数の値を持つ属性については、フルテキスト検索が可能です。 |
| | | データフィードを設定する際にシャドープロファイルを選択できるようになりました。 |
| | | IDSイベントブラウザの読み込み速度が向上しました。 |
| | | IDSイベントブラウザで集約されたイベントに、最大500個のIDSイベントが含まれるようになりました。IDSイベントブラウザのイベントチャートには、検出されたIDSイベントの総数が引き続き表示されます。 |
| | | 既知の不具合 |
| | | イベント詳細のメソッド固有の属性の一部が二重に表示され、異なるフォーマットになっています。この問題は、複数のメソッド（サブメソッド）で発生します。（DHCPANOM、DICTATTACK、IPV6TUNNELなど） |
| | | チェコ語と日本語のユーザーガイドは現在ご利用になれません。 |
| Ver.11.02.04 | 2021/4/28 | 修正された不具合 |
| | | Samba拡張機能を有効にしても「DICTATTACK: SambaProtocol」のサブメソッドの誤検出が発生しなくなりました。 |
| | | BPATTERNSおよびカスタムパターンイベントのイベント詳細に、誤検知除外ルールによって削除されたターゲットの数が含まれるようになりました。 |
| | | Syslogで破損したIDSイベントを受信すると、IDSイベントの処理が停止していた問題を修正しました。 |
| | | チェコ語でのユーザガイドが再度利用できるようになりました。 |
| Ver.11.02.02 | 2021/3/10 | 新機能 |
| | | ADSイベントのマッピングに使用されるMITRE ATT&CKマトリックスがバージョン7からバージョン8へ更新されました。<br>バージョン8は、新たに検出されたイベントに対してのみ行われます。今回の更新以前に検出されたイベントは、バージョン7に基づいてマッピングされます。 |
| | | 既知の不具合点 |
| | | 日本語のユーザガイドはまだご利用になれません。 |
| | | 注意事項 |
| | | 本バージョンには、同日にリリースされたVer.11.01.05からの変更点が含まれています（詳細は「過去のリリース - バージョン11.01.05」をご参照ください）。 |
| Ver.11.02.01 | 2021/2/25 | 修正された不具合 |
| | | イベントをCSVファイルでエクスポートした際、ヘッダーがずれてしまう問題を修正しました。 |
| | | DHCPANOMALY（サブメソッド：ServerChangeでのみ発生）において、現在のMACアドレスが更新されず、イベント詳細に以前と現在で同じMACアドレスが表示されていた問題を修正しました。 |
| | | 注意事項 |
| | | 本バージョンには、Ver.11.01.03からのパフォーマンスの最適化が含まれています（詳細は「以前のリリース - バージョン11.01.03」をご参照ください）。 |
| | | 本バージョンには、同日にリリースされたVer.11.01.04からの変更点が含まれています（詳細は「過去のリリース - バージョン11.01.04」をご参照ください）。 |
| Ver.11.02.00 | 2021/1/27 | 修正された不具合 |

| | | |
|---|---|---|
| | | VPNのイベントでソースIPを持たない場合エラーが発生し、ADSが動作しなくなることがある問題を修正しました。 |
| | | 新機能 |
| | | 解析でのイベントチャートの表示を改良しました。 |
| | | イベントチャートが補間曲線で平滑化されるようになりました。 |
| | | MITRE ATT&CKのtactics and techniquesは、ADSの検出（サブ）メソッドにマッピングされ、ユーザに追加のコンテキストを提供するようになりました。 |
| | | ADSの検出イベントにMITRE ATT&CKをマッピングし、ユーザに追加のコンテキストを提供するようになりました。 |
| | | 最も正確なマッピングを実現するために、文脈的解析が行われます。<br>そのため、同じサブメソッドの異なるイベントに異なるMITRE ATT&CKのtactics and techniquesを割り当てることができます。<br>また、イベントの展開状況に応じて、1つのイベントに複数のtactics and techniquesを割り当てることも可能となりました。 |
| | | 検知方法やサブメソッドの中には、どのMITRE ATT&CKのtactics and techniquesにも割り当てられていないものが存在します<br>（例えば、適切なtactics や techniquesが存在しない場合や、その方法が構成上の問題を検知する場合など）。 |
| | | マッピングは、ATT&CK v7: https://attack.mitre.org/versions/v7/ に対応しています。 |
| | | マッピングは過去にさかのぼって行われないため、ADS11.2へのアップデート前に検出されたイベントは、MITRE ATT&CKのどのtactics and techniquesにも割り当てられません。 |
| | | JA3フィンガープリントを用いて、暗号化されたトラフィック解析が可能となりました。 |
| | | JA3フィンガープリントはBLACKLIST メソッドを拡張し、暗号化されたトラフィックに含まれる悪意のある通信を検出するようになりました。 |
| | | JA3フィンガープリントは、新しいJA3ブラックリストのデータフォーマットを使用して、ローカルまたはリモートのブラックリストとして追加できるようになりました。 |
| | | フローレコードにはJA3フィンガープリントのパラメータが必要（Flowmon Probe提供）であり、JA3フィンガー |
| | | フローレコードにはJA3フィンガープリントのパラメータが必要（Flowmon Probe提供）であり、<br>JA3フィンガープリントはConfiguration Centerで有効にすることが可能：<br>Flowmon Probe ＞ モニタリングポート ＞ 高度な設定＞ TLS JA3フィールド<br>Flowmon Collector ＞ FMC設定 ＞ フローのデータベースフィールド＞ TLS JA3フィールド |
| | | JA3フィンガープリントを使用すると、正当なアプリケーションと悪意のあるアプリケーションのJA3フィンガープリントが衝突する可能性があるため、誤検出の原因となる可能性があります。ユーザは以下のリンクからJA3ブラックリストをダウンロードし、ローカルのブラックリストとして追加すると、必要に応じて編集することができます。ブラックリストをリモートで設定した場合、ブラックリストの内容をローカルで設定した場合のように自由に編集することはできませんが、リモートではJA3フィンガープリントのブラックリスト提供者から自動的にリストを取得/更新します。 |
| | | JA3のブラックリストはこちらから入手可能です：https://services.flowmon.com/reputation/ja3malware/list.csv |
| | | 脅威情報共有プラットフォームのMISPに対応するようになりました。 |
| | | MISPインスタンスをリモートブラックリストとしてADSに接続することで、MISPのIoCフィードからブラックリストを自動的に作成し、悪意のある通信を検知できるようになりました。 |
| | | BPATTERNSの1秒あたりのフロー（fps）性能が向上しました。 |
| | | BPATTERNSの1秒あたりのフロー（fps）性能が向上しました。<br>ADS Business以上のモデルをお持ちのすべてのお客様に、パフォーマンスの向上をもたらします。<br>最大パフォーマンスが15kから25kfpsに向上しました（EnterpriseとUltimateモデルで有効）。<br>詳細はFlowmon ADSスペックシートをご参照ください。 |
| | | “サービスタイプ”のブラックリストで、任意のプロトコルに対してキーワードに“ANY”を使用できるようになりました。 |
| | | P2P Supernodesのブラックリストは、利用時に制限があるため削除しました。 |
| Ver.11.01.05 | 2021/3/10 | 修正された不具合 |
| | | サーバからの応答がない場合、クライアントが「DHCPANOMALY: FakeServer」の サブメソッドからDHCPサーバに通信しようとする際の検出を除外しました。 |
| | | “Appタグ”列が空欄の場合、「イベント証跡」に表示されないように修正されました。 |
| | | 新機能 |
| | | イベントフローの解析を改善するために、「イベント詳細」の「イベント証跡」に「フロー受信時間」が追加されました。「フロー受信時間」は、Configuration Center＞ FMC設定＞ フローのデータベースフィールド＞ コレクタが受信したタイムスタンプフロー、のチェックが有効になっている場合のみ表示されます。 |
| | | フローベアリングのタイムアウトを60秒から75秒に変更し、反対方向のフローの遅延による誤検出を減らしました。 |
| Ver.11.01.04 | 2021/2/25 | 修正された不具合 |
| | | 設定＞ 処理＞ パースペクティブ設定で、データフィードが正しくソートされるようになりました。 |
| | | 高負荷のアプライアンス上で非常にまれにADSの機能が停止してしまう問題を修正しました。 |
| | | イベント証跡の'Data feed IP'の項目名を'Flow source IP'に変更し、Monitoring Centerの用語と一致するように修正しました。（※英語版のみの対応です。） |
| Ver.11.01.03 | 2021/2/15 | 修正された不具合 |
| | | ICMPANOMメソッドの一部でセグメンテーションエラーが発生し、システムに高負荷がかかっていた問題を修正しました。 |
| | | 新機能 |
| | | 様々なパフォーマンスの最適化により、「イベント詳細」と「イベント証跡」のダウンロード時間が短縮され、複数のイベントを分析する際のシステムの応答性が向上されました。 |
| | | イベント詳細とそれに対応するイベント証跡のダウンロード時間を短縮し、特にイベント証跡の中で期間が長くフロー量が多いイベントのダウンロード時間が短縮されました。 |
| | | イベント詳細で対応するタブを開いた後に、イベント証跡がダウンロードされるようになりました。 |
| | | イベント証跡 は、開始時刻ではなく受信時刻に従って Monitoring Center から最初の 1000 (変更可能なデフォルト値) のフローを取得できるようになりました。この修正により、フローの読み込みが非常に速くなりましたが、フローの数が制限値を超えた場合、開始時刻に応じてMonitoring Centerでソートされたフローのリストと比較すると、遅延したフローがイベントの証跡として表示されなくなることがあります。 |
| Ver.11.01.02 | 2021/1/21 | 修正された不具合 |
| | | 多数のイベントの処理中にフィルタが複数回編集された場合に、アプリケーションが数分間フリーズする問題が修正されました。 |
| | | 誤検知除外の設定を設定ファイルから正しくインポートされるように修正しました。 |
| | | 新機能 |
| | | フィルタの操作が大幅に高速化されました。 |
| | | 脅威インテリジェンスのデータが拡張されたため、クォータの管理でADSが要求するディスクの下限値が増加しました。 |
| Ver.11.01.01 | 2020/12/3 | 修正された不具合 |
| | | データフィードが設定ファイルから正しくインポートされるようになりました。 |
| | | クライアントとサーバのタイムゾーンが同じではない場合、解析ページにはサーバの設定時刻が表示されます。 |
| | | 解析の優先度別イベントの各イベントの「IPをフィルタに追加」にて、事前に設定した情報が表示されない問題を修正しました。 |
| | | 解析の優先度イベントが表示される前にグラフが表示されていた問題を修正しました。 |
| | | 新機能 |
| | | 正しく一度に複数のフィルタにIPアドレスを追加できるようになりました。 |
| | | Flowmon OS 11.1.0との互換性を追加しました。 |
| | | Flowmon OS 11.1以降をご利用の場合、GUI上で新しいRest APIガイドを利用できるようになりました。 |
| | | チェコ語と日本語のユーザガイドを追加しました。 |
| | | 既知の不具合点 |

| | | |
|---|---|---|
| | | バージョン 11.1 で導入された変更は、チェコ語と日本語のユーザガイドに反映されていません。 |
| Ver.11.01.00 | 2020/9/30 | 修正された不具合 |
| | | 文字 '&' が CSV エクスポートで正しく表示されるようになりました。 |
| | | データフィードの名前は、UI内のすべての場所で適切に翻訳されるようになりました。 |
| | | syslogメッセージのフォーマットがCEF標準に一致するように調整されました。 |
| | | 新機能 |
| | | ストリーム処理において、プロキシ相関が再実装されました。詳細については、ユーザガイドの「データフィード」の章を参照してください。 |
| | | イベントの視覚化のAdobe Flashは、Javascript D3ライブラリをベースにした新しいものに置き換えられました。 |
| | | 誤検出エンジンが刷新されました。 |
| | | イベントが複数の誤検知除外ルールに一致した場合に、誤検知除外ルールが適切に適用されるようになりました。 |
| | | ユーザは、指定されたターゲットで誤検知除外のタイムスタンプを定義することができなくなりました。 |
| | | 使用統計情報が簡素化されました。 |
| | | プロファイル'live'の名前が'All Sources'に変更され、FMCの命名規則に対応するようになりました。 |
| | | プロファイルのグループ名がデータフィードの編集画面に表示されるようになりました。 |
| | | 既知の不具合点 |
| | | 日本語のユーザガイドはまだご利用できません。 |
| Ver.11.00.11 | 2020/12/1 | 修正された不具合 |
| | | SIPフローの処理中にSIPデータフィードの再起動につながるバグを修正しました。 |
| | | フィルタを使用した誤検知除外の設定を設定ファイルから正しくインポートされるように修正しました。 |
| | | BROKENSENメソッドが膨大なCPUを使用しデッドロックが発生する問題を修正しました。 |
| | | 実行時に使用可能なマシン メモリが変更されたために、データ フィードが再初期化されない問題を修正しました。 |
| Ver.11.00.10 | 2020/10/9 | 修正された不具合 |
| | | Hyper-Vプラットフォームでデータフィードが実行されない問題を修正しました。 |
| | | 新機能 |
| | | Flowmonのサブライセンスに対応しました。 |
| | | 既知の不具合点 |
| | | イベントが複数の誤検知除外ルールに該当した場合、一部の誤検知除外ルールが適用されない場合があります。（Flowmon ADS 11.1で修正されました） |
| Ver.11.00.09 | 2020/9/30 | 修正された不具合 |
| | | IPアドレスのコンテキストメニューから「IDSイベントの閲覧」が正しく開かない問題を修正しました。 |
| | | 新機能 |
| | | データベースが最大サイズに達した場合、バックエンドエンジンが適切に復旧し、処理停止を防ぐようになりました。 |
| | | 日本語のユーザガイドを公開しました。 |
| | | 既知の不具合点 |
| | | イベントが複数の誤検知除外ルールに該当した場合、一部の誤検知除外ルールが適用されない場合があります。（Flowmon ADS 11.1で修正予定） |
| Ver.11.00.08 | 2020/8/31 | 修正された不具合 |
| | | 50チャネル以上割り当てられたデータフィードでBPATTERNSが処理されない問題を修正しました。 |
| | | Flowmon ADS 11よりも前に生成されたイベントに対して、イベント証跡が適切に動作するようになりました。 |
| | | 新機能 |
| | | Flowmon ADS Standardライセンスのデータフィードの最大数が1から3に増加しました。 |
| | | 既知の不具合点 |
| | | イベントが複数の誤検知除外ルールに該当した場合、一部の誤検知除外ルールが適用されない場合があります。（Flowmon ADS 11.1で修正予定） |
| | | 「データフィードの編集」画面の「FPSの上限値/下限値の設定」項目でフロー数は0～200,000の範囲であると説明されていますが、正しくは0～100,000です。 |
| | | 日本語のユーザガイドはまだご利用できません。 |
| Ver.11.00.07 | 2020/8/4 | 修正された不具合 |
| | | Flowmon ADSログのローテーションを妨げる問題を修正しました。（ディスク上のスペースを確保するために古いログを削除します。） |
| Ver.11.00.06β | 2020/7/22 | 修正された不具合 |
| | | 11.0.5にアップグレードした後、新しいパラメータの無効なデフォルト値によって生じた不正なタイムスタンプのレポートを修正しました。 |
| | | 集約されたイベントおよび関連イベントをすべてのモーダルウィンドウから開くことができるようになりました。 |
| | | ICMPプロトコルに基づくメソッドのトラフィックの記録フィルタを修正しました。 |
| | | 新機能 |
| | | 「タイムスタンプ」という用語は、実際の意味を反映するために「検出時間」という用語に置き換えられました。（英語版のみ） |
| | | 規格外のフロー期間を持つエクスポータからのフローは、処理をしない代わりに300秒に短縮して処理されるようになりました。 |
| | | 以前のバージョンからの無効なカスタムパターン設定が処理されるとユーザに適切に通知されるようになりました。 |
| | | 既知の不具合点 |
| | | 日本語のユーザガイドはまだご利用できません。 |
| | | カスタムパターン設定で正規表現が許可されなくなりました。 |
| | | データフィード設定で「アクティブなプロキシ」オプションが有効になっている場合、v11より古いバージョンのFlowmon ADSからのアップグレードができなくなりました。 |
| Ver.11.00.05β | 2020/7/8 | 修正された不具合 |
| | | イベントターゲットの誤検知除外ルールが正しく評価されるようになりました。 |
| | | 既存のFlowmon ADSレポートのFlowmon Dashboard and Reportsへの移行は、すべてのケースで機能するようになりました。 |
| | | Flowmon Dashboard and ReportsのCSVエクスポートに関する問題を修正しました。 |
| | | VPNの使用を検出するVPNメソッドが機能するようになりました。 |
| | | フローチャートと集約ビューに、以前のバージョンのFlowmon ADSのデータが正しく表示されるようになりました。 |
| | | 集約ビューをイベントターゲットから開くことができるようになりました。 |
| | | 検出エンジンは、パケット数が0のフローを処理できるようになりました。 |
| | | イベント証跡に表示されるフローの時間範囲を修正しました。 |

| | | |
|---|---|---|
| | | 既知の不具合点 |
| | | 日本語のユーザガイドはまだご利用になれません。 |
| | | イベント処理のパフォーマンスが向上しました。 |
| | | メソッド検出の問題を回避するために、規格外のフロー期間（300秒を超える）のフローは処理されない場合があります。 |
| | | データフィード設定で「アクティブなプロキシ」オプションが有効になっている場合、v11より古いバージョンのFlowmon ADSからのアップグレードができなくなりました。 |
| | | イベントあたりの最大ターゲットは1000に制限されています。 |
| Ver.11.00.04β | 2020/6/3 | 新機能 |
| | | トラフィックの処理性能（1 秒あたりのフロー）が全体的に大幅に向上しました。 |
| | | 振る舞い検知がより速くなりました。 |
| | | 5分毎のバッチ処理からFlowを受信するとリアルタイムに分析されるように変更されました。 |
| | | 検出されたイベントは遅延なく通知されます。 |
| | | 限界のない幅広い時間帯でのフローデータ分析により、検出の質が向上しました。 |
| | | 振る舞いが継続して検出されている場合は、再度新しいイベントを作成するのではなく、既存のイベントを継続的に更新するように変更されました。 |
| | | 正しいイベントソースを特定するために通信イニシエータの識別を改善しました。 |
| | | 検出されたイベントの理解を深めるための新しい説明を追加しました。 |
| | | 利用可能なすべての言語のイベント詳細テキストの翻訳を追加しました。 |
| | | メソッドにサブタイプを追加しました。これにより、1つの検出方法から様々なイベントを識別できるようになりました。 |
| | | イベント属性の表示を追加しました。属性は、UIでローカライズされたイベント詳細を構築するために使用されます。 |
| | | すべての検出メソッドが再構築されました。 |
| | | TEAMVIEWERメソッドの機能を改善しました。 |
| | | アプリケーションの起動とデスクトップの共有を区別できるようになりました。 |
| | | DHCPANOMメソッドの機能を改善しました。 |
| | | DHCPサーバのMACアドレスの変更を検出できるようになりました。 |
| | | DHCPサーバを過負荷にしているサーバをIPアドレスによって検出できるようになりました。 |
| | | DHCPサーバを過負荷にしているクライアントをMACアドレスによって検出できるようになりました。 |
| | | BROKENSENメソッドを再設計しました。 |
| | | 旧式のメソッドであるICGUARD、LATENCY、DNSREVERSE、INSTMSGを削除しました。 |
| | | DNSANOMALYメソッドから旧式の大きなUDPパケットを検出する機能を削除しました。 |
| | | 動作パターン(BPATTERNS)を処理するための新しい下位互換エンジンを導入しました。 |
| | | より長いドメインを持つブラックリストに対応しました。（31文字から63文字に拡張） |
| | | PDF/CSVレポートとダッシュボードウィジェットをFlowmon ADSモジュールからFlowmon Dashboard and Reportsに移動しました。 |
| | | データフィードの設定からアクティブなプロキシ設定を削除しました。 |
| | | SuperFast機能とフィルタブースタ機能を削除しました。 |
| | | パースペクティブの高度なフォーム設定から「部分文字列」が削除され、「サブメソッド」から選択する方式に替わりました。 |
| | | 既知の不具合 |
| | | 日本語のユーザガイドはまだご利用になれません。 |
| | | Flowmon Dashboard and Reports |
| | | レポートに以下のチャプターを使用して「CSVとしてエクスポート」を実施してもCSVにエクスポートされません。<br>- 優先度別のイベント概要<br>- タイプ別のイベント概要<br>- 優先度とイベント数による上位10件のイベントタイプ<br>- Security status |
| | | イベントマトリックスのチャプターを使用したレポートで「CSVとしてエクスポート」を実施した場合に、イベント数が正しくない／イベントの送信元フィールドが欠落していることがあります。 |
| | | チャプター「タイプ別イベント概要」で、表示されるメソッドが検出された数より少ない場合があります。 |
| | | Flowmon ADSのダッシュボードから「集約されたイベント」を選択しても、集計されたイベント画面が開かない場合があります。 |
| | | 誤検知除外ルールが有効になるまでに数分程度時間が掛かることがあります。 |
| | | 注意事項 |
| | | イベントの概念が新しくなったため、誤検知除外機能の動作が変更されました。 |
| | | 新しい誤検知除外ルールを追加すると、すべてのアクティブなイベントに影響を与えます。 |
| | | つまり履歴から始まり、まだ更新されているイベントは、新しい誤検知除外によって削除される可能性があります。 |
| | | 新しい誤検知除外ルールによりADSからのアクティブなイベントが消失することは、想定動作であることに注意してください。 |
| | | DA(Distributed Architecture)モードでFlowmon ADSの旧バージョンからアップグレードする場合は、Flowmonサポート（support@flowmon.com）にお問い合わせ頂くことをお勧めします。 |