

バージョンアップリリースノート

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 | 変更箇所 |
|--|------------|--|
| Ver.12.00.03 | 2022/06/01 | 修正された問題 |
| | | 誤検知除外のルールを、SIP データフィールドに適用すると、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。 |
| | | 既知の問題 |
| | | 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。 |
| Ver.12.00.02 | 2022/05/10 | 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。 |
| | | 新着情報 |
| | | チェコ語と日本語のユーザーガイドを追加しました。 |
| | | 修正された問題 |
| | | 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。 |
| Ver.12.00.01β | 2022/04/06 | 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。 |
| | | - 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。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。 |
| | | 既知の問題 |
| | | 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。 |
| | | 修正された問題 |
| Ver.12.00.00β | 2022/03/02 | 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。 |
| | | 既知の問題 |
| Ver.12.00.00β | 2022/03/02 | 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。 |
| | | 新着情報 |
| | | 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。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。 |
| | | - 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。 |
| - このメソッドでは、「HTTP ホスト名」または「DNS フィールド」を含んで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。 | | |
| - TOR : | | |
| - 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。 | | |
| - 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） | | |
| - 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。 | | |
| - ANOMALY : | | |
| - 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。 | | |
| - 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。 | | |

| ver.No | リリース日 | 変更箇所 |
|--|-------|---|
| | | <ul style="list-style-type: none"> - SCANS : - SCANS メソッドは、TCP connect scan を検知するように拡張されました。 - 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) - 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。 |
| | | <ul style="list-style-type: none"> - 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。 - 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。 - 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。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) 。 - 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。 - 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。 - 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。 - 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。 |
| | | <ul style="list-style-type: none"> - 「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。「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。 - 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。 - Monitoring Center に保存されているフローを表示するイベント証拠は「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。 |
| | | SYSCHECK メソッド : |
| | | <ul style="list-style-type: none"> - 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。 - 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。 |
| | | <ul style="list-style-type: none"> - 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。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。 |
| | | 修正された問題 |
| | | 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。 |
| 既知の問題 | | |
| 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。 | | |
| 修正された問題 | | |
| 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。 | | |

Ver.11.04.02

2021/11/22

| ver.No | リリース日 | 変更箇所 |
|--------------|------------|---|
| | | <p>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。</p> <p>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。</p> <p>既知の問題</p> <p>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）</p> <p>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）。</p> |
| Ver.11.04.01 | 2021/10/26 | <p>新着情報</p> <p>チェコ語と日本語のユーザーガイドを追加しました。</p> <p>修正された問題</p> <p>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。</p> <p>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。</p> <p>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。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す。</p> <p>既知の問題</p> <p>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）</p> <p>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）。</p> |
| Ver.11.04.00 | 2021/09/30 | <p>新着情報</p> <p>誤検知除外：</p> <ul style="list-style-type: none"> - 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。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。 - 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。 - 「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。 - 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。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。 - 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。 <p>検知メソッド（メソッドインスタンス）：</p> <ul style="list-style-type: none"> - 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提供できるようになりました。 - 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。 <p>イベントのチャート：</p> <ul style="list-style-type: none"> - 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。 - 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。 - 最新： <ul style="list-style-type: none"> - 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。 - 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。 - コントラスト： <ul style="list-style-type: none"> - 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。 <p>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。上記の設定は一時的なものです。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。</p> <p>Syslog メッセージ</p> <ul style="list-style-type: none"> - 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処理できるようになりました。 - 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。 <p>MITRE ATT&CK:</p> <ul style="list-style-type: none"> - 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 |

| ver.No | リリース日 | 変更箇所 |
|---------------|------------|--|
| | | <p>ことを示すようになりました。</p> <p>- MITRE ATT&CK マッピングを最新バージョン 9 に更新しました。</p> <p>イベント証跡</p> <p>- 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。</p> <p>- 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。</p> <p>製品使用状況データの収集：</p> <p>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。</p> <p>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。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。</p> <p>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。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。</p> <p>修正された問題</p> <p>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。</p> <p>既知の問題</p> <p>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）</p> <p>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。</p> |
| Ver.11.03.03 | 2021/09/08 | <p>修正された問題</p> <p>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。</p> <p>既知の問題</p> <p>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）</p> |
| Ver.11.03.02 | 2021/7/7 | <p>新着情報</p> <p>Dashboard and Reports に MITRE ATT&CK のプリセットが追加されました。</p> <p>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。</p> <p>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。（各 MITRE ATT&CK 戦術のチャプタを含みます。）</p> <p>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。</p> <p>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。</p> <p>修正された問題</p> <p>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。</p> <p>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。</p> <p>既知の問題</p> <p>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）</p> |
| Ver.11.03.01β | 2021/06/23 | <p>新着情報</p> <p>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）。</p> <p>チェコ語と日本語のユーザーガイドを追加しました。</p> <p>REST API ガイドが ADS バージョン 11.3 に更新されました。</p> <p>修正された問題</p> <p>「<」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。</p> <p>イベント処理のパフォーマンスが改善されました。</p> <p>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。</p> <p>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。</p> <p>既知の問題</p> <p>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）</p> |
| Ver.11.03.00β | 2021/05/17 | <p>新着情報</p> <p>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。</p> |

| ver.No | リリース日 | 変更箇所 |
|--|------------|--|
| | | 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。 |
| | | 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、マトリッ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ード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。 |
| | | 修正された問題 |
| | | 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。 | | |
| 既知の問題 | | |
| 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 | 2021/04/28 | 修正された問題 |
| | | 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ーガイドが再度利用できるようになりました。 |
| Ver.11.02.02 | 2021/03/10 | 新着情報 |
| | | 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。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。 |
| | | 注釈 |
| | | 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.No | リリース日 | 変更箇所 |
|--------------|------------|---|
| | | <p>既知の問題点</p> <p>日本語のユーザガイドはまだご利用になれません。</p> |
| Ver.11.02.01 | 2021/02/25 | <p>修正された問題</p> <p>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。</p> <p>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。</p> <p>注釈</p> <p>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)。</p> <p>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)。</p> |
| Ver.11.02.00 | 2021/01/27 | <p>新着情報</p> <p>解析でのイベントチャートの表示を改良しました。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。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。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 を割り当てることが可能となりました。</p> <p>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 (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)。</p> <p>マッピングは、ATT&CK v7: https://attack.mitre.org/versions/v7/ に対応しています。</p> <p>マッピングは過去にさかのぼって行われなかったため、ADS 11.2 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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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 フィンガープリントは Configuration Center で有効にすることが可能:</p> <p>Flowmon Probe > モニタリングポート > 高度な設定 > TLS JA3 フィールド</p> <p>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</p> <p>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。</p> <p>JA3 のブラックリストはこちらから入手可能となります: https://services.flowmon.com/reputation/ja3malware/list.csv</p> <p>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。</p> <p>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。</p> <p>BPATTERNS の 1 秒あたりのフロー (fps) 性能が向上しました。</p> <p>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。</p> <p>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)。</p> <p>詳細は Flowmon ADS スペックシートをご参照ください。</p> <p>“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。</p> <p>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。</p> <p>修正された問題</p> <p>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。</p> |
| Ver.11.01.05 | 2021/03/10 | <p>新着情報</p> <p>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。</p> |

| ver.No | リリース日 | 変更箇所 |
|--------------|------------|---|
| | | <p>フローペ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。</p> <p>修正された問題</p> <p>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。</p> <p>“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。</p> |
| Ver.11.01.04 | 2021/02/25 | <p>修正された問題</p> <p>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。</p> <p>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。</p> <p>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。）</p> |
| Ver.11.01.03 | 2021/02/15 | <p>新着情報</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>修正された問題</p> <p>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。</p> |
| Ver.11.01.02 | 2021/1/21 | <p>新着情報</p> <p>フィルタの操作が大幅に高速化されました。</p> <p>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。</p> <p>修正された問題</p> <p>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。</p> <p>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。</p> |
| Ver.11.01.01 | 2020/12/03 | <p>新着情報</p> <p>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。</p> <p>Flowmon OS 11.1.0 との互換性を追加しました。</p> <p>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。</p> <p>チェコ語と日本語のユーザガイドを追加しました。</p> <p>修正された問題</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>既知の問題点</p> <p>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。</p> |
| Ver.11.01.00 | 2020/09/30 | <p>新着情報</p> <p>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。</p> <p>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。</p> <p>誤検出エンジンが刷新されました。</p> <p>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。</p> <p>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。</p> <p>使用統計情報が簡素化されました。</p> <p>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。</p> <p>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。</p> <p>修正された問題</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>既知の問題点</p> |

| ver.No | リリース日 | 変更箇所 |
|---|------------|---|
| | | 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 | 2020/12/01 | 修正された問題 |
| | | 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 | 2020/10/09 | 新着情報 |
| | | Flowmon のサブライセンスに対応しました。 |
| | | 修正された問題 |
| | | Hyper-V ブ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。 |
| | | 既知の問題点 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 | 2020/09/30 | 新着情報 |
| | | 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。 |
| | | 修正された問題 |
| | | 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。 |
| | | 既知の問題点 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 | 2020/08/31 | 新着情報 |
| | | 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。 |
| | | 修正された問題 |
| | | 50 チャン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。 |
| | | 既知の問題点 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 | 2020/08/04 | 修正された問題 |
| | | 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 | 2020/07/22 | 新着情報 |
| | | 「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トからのフローは、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。 |
| | | 修正された問題 |
| | | 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。 |
| 既知の問題点 日本語のユーザガイドはまだご利用できません。 その他： 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 | 2020/07/08 | 修正された問題 |
| | | 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。 |

| ver.No | リリース日 | 変更箇所 |
|---------------|------------|--|
| | | <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>既知の問題点</p> <p>日本語のユーザガイドはまだご利用になれません。</p> <p>その他</p> <p>イベント処理のパフォーマンスが向上しました。</p> <p>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。</p> <p>データフィールド設定で「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。</p> <p>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。</p> |
| Ver.11.00.04β | 2020/06/03 | <p>新機能</p> <p>新しいストリーム処理</p> <p>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。</p> <p>振る舞い検知がより速くなりました。</p> <p>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。</p> <p>検出されたイベントは遅延なく通知されます。</p> <p>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。</p> <p>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。</p> <p>正しいイベントソースを特定するために通信インシエータの識別を改善しました。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>すべての検出メソッドが再構築されました。</p> <p>TEAMVIEWER メソッドの機能を改善しました。</p> <p>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。</p> <p>DHCPANOM メソッドの機能を改善しました。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>BROKENSEN メソッドを再設計しました。</p> <p>旧式のメソッドである ICGUARD、LATENCY、DNSREVERSE、INSTMSG を削除しました。</p> <p>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。</p> <p>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。</p> <p>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）</p> <p>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。</p> <p>データフィール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。</p> <p>SuperFast 機能とフィルタブースタ機能を削除しました。</p> <p>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変わりました。</p> <p>既知の問題</p> <p>日本語のユーザガイドはまだご利用になれません。</p> <p>Flowmon Dashboard and Reports</p> <p>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。</p> <ul style="list-style-type: none"> ● 優先度別のイベント概要 ● タイプ別のイベント概要 ● 優先度とイベント数による上位 10 件のイベントタイプ ● Security status <p>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。</p> <p>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。</p> |

| ver.No | リリース日 | 変更箇所 |
|---------------|------------|---|
| | | <p>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。</p> <p>注意事項</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> <p>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。</p> |
| Ver.10.01.01 | 2020/06/24 | <p>修正された問題</p> <p>PDF スケジュール レポートがタイムアウトしないようになりました。</p> <p>「対話型のイベント視覚化」画面の [関連イベント]と[集約されたイベント]がオプションメニューから正常に動作するようになりました。</p> <p>長い名前のデータフィールドが存在する場合にも、デフォルトレポートの作成が正常に行えるようになりました。</p> <p>新規に開いたモーダルウィンドウが常にフォアグラウンドに表示されるようになりました。</p> <p>Syslog メッセージに出力されるイベントからは IP アドレスのルーティングプレフィックスを表示しなくなりました。</p> |
| Ver.10.01.00β | 2020/04/21 | <p>修正された問題</p> <p>FlowmonOS バージョン 11 に対応しました。</p> |
| Ver.10.00.06 | 2020/06/23 | <p>修正された問題</p> <p>非常にまれなケースで電子メールレポートを送信できない問題を修正しました。</p> <p>イベント属性のオーバーフローが原因でバッチ処理が失敗する問題を修正しました。</p> <p>CSV レポートで、チャプタの構成で指定されたすべてのフィルタが考慮されるようになりました。</p> <p>イベント証跡画面でフィルタに指定した整数値が適切に機能するようになりました。</p> <p>イベント画面の[簡易リスト]、[ホスト別]の検索結果でソースとターゲットを選択時にオプションメニューが表示されるようになりました。</p> |
| Ver.10.00.05 | 2020/03/23 | <p>Syslog メッセージに含まれる詳細メッセージ部の区切り文字をカンマ区切りからセミコロン区切りに変更しました。</p> <p>修正された問題</p> <p>Syslog メッセージの重要度を表す数値がユーザガイドの記載と異なっていた問題を修正しました。</p> <p>優先度 : 変更前 → 変更後</p> <p>-----</p> <p>重要 : 2 → 10</p> <p>高 : 4 → 8</p> <p>中 : 6 → 6 (※変更なし)</p> <p>低 : 8 → 4</p> <p>情報 : 10 → 2</p> <p>「レポートのスケジューリング」においてカスタムインターバルの「終了」時間が「00:00」になっていた問題を「23:59」になるように修正しました。</p> <p>イベントマトリックスのチャプターを「レポートの作成」で CSV にエクスポートした際、正しい日付でイベントが表示されない問題を修正しました。</p> <p>英語表示以外の UI においてデフォルトレポートが作成できない問題を修正しました。</p> <p>チャンネルを仮想データフィールドとして使用する設定をした際、設定画面とダッシュボードでの表記が異なる問題を修正しました。</p> |
| Ver.10.00.04 | 2020/02/03 | <p>データベースサイズの大きいアプライアンスにおけるダッシュボードの読み込み速度が改善されました。</p> <p>修正された問題</p> <p>IP アドレスのメニュー項目[一般情報]に誤ったブラックリスト名が表示される問題を修正しました。</p> <p>仮想データフィールドからのイベントがパースペクティブに正しく割り当てられない問題を修正しました。</p> <p>仮想データフィールドが有効な場合において、Syslog メッセージが適切に送信されない問題を修正しました。</p> <p>[説明]が記載されていないカスタムブラックリストをアップロードできない問題を修正しました。</p> <p>プラグインの再起動後にカスタムブラックリストが正しく機能しない問題を修正しました。</p> <p>イベント処理の失敗を引き起こす可能性のあるイベント解析の問題を修正しました。</p> <p>既知の不具合</p> <p>[デフォルトレポートの作成]ボタンは日本語では正常に動作しません。</p> <p>制限事項</p> <p>Flowmon ダッシュボードの Flowmon ADS ウィジェットの機能を改善するには、Flowmon OS をバージョン 10.3.2 以上にアップグレードしてください。</p> <p>Flowmon ダッシュボードで Flowmon ADS レポートを PDF へ手動エクスポートした場合、アイコンが表示されず、オーバーフローします (Flowmon OS ver.10.03.03 で修正されます)。</p> |

| ver.No | リリース日 | 変更箇所 |
|--|------------|---|
| Ver.10.00.03 | 2020/01/06 | [HIGHTRANSF]メソッドのしきい値の最大値を増加しました（1GB から 1TB）。 |
| | | ユーザガイドに小規模な改善を実施しました。 |
| | | 修正された問題 |
| | | 仮想データフィードのイベントが適切に表示されない問題を修正しました。 |
| | | Flowmon ADS 10.0 にアップグレードする前に Flowmon IDS Collector がインストールされたアプライアンスで、IDS イベントブラウザが動作するようになりました。 |
| | | ユーザガイドの日本語版の全文検索が正しく機能するようになりました。 |
| | | Flowmon OS のローカルディスクのカスタムブラックリストは、Windows の行末記号（CRLF）を使用して CSV でインポートできるようになりました。 |
| | | 欠落していた翻訳を追加しました。 |
| | | 構成の変更後にページが自動で更新されるようになりました。 |
| | | 制限事項 |
| | | Flowmon ダッシュボードの Flowmon ADS ウィジェットの機能を改善するには、Flowmon OS を少なくともバージョン 10.3.2 にアップグレードしてください。 |
| Flowmon ダッシュボードで Flowmon ADS レポートを PDF へ手動エクスポートした場合、アイコンが表示されず、オーバーフローします（Flowmon OS ver.10.03.03 で修正されます）。 | | |
| Ver.10.00.02β | 2019/12/04 | 日本語のユーザガイドが利用可能になりました。 |
| | | ダッシュボードに送信元 IP アドレスの国旗とドメイン名が表示されるようになりました。 |
| | | 修正された問題 |
| | | ダッシュボードとイベント画面で正しいタイムゾーン（サーバー側）が使用されるようになりました。 |
| | | [IP の一般情報]が正しく機能するようになりました。 |
| | | ユーザガイドのチェコ語版での検索が、すべての場合に機能するようになりました。 |
| | | 既知のバグ |
| | | 日本語版のユーザガイドの全文検索のインデックスに一部の単語が欠落していますが、次のバージョンで修正される予定です。 |
| | | 制限事項 |
| | | Flowmon ダッシュボードの Flowmon ADS ウィジェットの機能を改善するには、少なくとも Flowmon OS を ver.10.3.2 にアップグレードしてください。 |
| Flowmon ダッシュボードで Flowmon ADS レポートを PDF へ手動エクスポートした場合、アイコンが表示されず、オーバーフローします（Flowmon OS ver.10.03.03 で修正されます）。 | | |
| Ver.10.00.01β | 2019/11/18 | チェコ語のユーザガイドが利用可能になりました。 |
| | | PDF 形式で完全なユーザガイドをダウンロードできるようになりました。 |
| | | FTR トラフィックレコードの起動に失敗した際のエラーメッセージを改善しました。 |
| | | 修正された問題 |
| | | ダッシュボードからのドリルダウン調査のイベント数の概要が正しく表示されない問題を改善しました。 |
| | | すべての Flowmon ADS 9.5 バージョンからのアップグレードが可能になりました。 |
| | | PDF フォーマットでスケジュールされたレポートが正しく生成されない問題を修正しました。 |
| | | ブラックリストの更新時間が正しく表示されない問題を修正しました。 |
| | | [ADS 管理者]ロールを持つユーザがログページを表示できるようになりました。 |
| | | 既知のバグ |
| | | チェコ語版のユーザガイドの検索が正しく機能しない場合があります。 |
| | | 制限事項 |
| | | ユーザガイドは英語版とチェコ語版でのみ利用可能です。 |
| Flowmon ダッシュボードの Flowmon ADS ウィジェットの機能を改善するには、少なくとも Flowmon OS を ver.10.3.2 にアップグレードしてください。 | | |
| Flowmon ダッシュボードで Flowmon ADS レポートを PDF へ手動エクスポートした場合、アイコンが表示されず、オーバーフローします（Flowmon OS ver.10.03.03 で修正されます）。 | | |
| Ver.10.00.00β | 2019/10/31 | ユーザインターフェイスが分析に重点を置いて完全に再設計されました。また、簡単な微調整を実施しました。 |
| | | 新しいフィルタ管理機能の追加、独自の評価フィードの実装、利用できる外部サービスを拡張しました。 |
| | | Syslog メッセージ機能がデータフィードとパースペクティブインジケータによって拡張されました。 |
| | | IDS コレクタを搭載しました。 |
| | | ユーザガイドを HTML で入手できるようになりました。Flowmon ADS ユーザインターフェイスからアクセス可能で、全文検索をサポートしています。 |
| | | 制限事項 |
| | | ユーザガイドは英語版のみで利用可能です。 |
| Flowmon ダッシュボードの Flowmon ADS ウィジェットの機能が制限される場合があります（Flowmon OS バージョン | | |

| ver.No | リリース日 | 変更箇所 |
|--------------|------------|--|
| | | 10.3.2 で対処されます)。 Flowmon ダッシュボードのレポート機能において、Flowmon ADS が制限される場合があります (Flowmon OS のバグ修正で処理されます)。 既知のバグ ダッシュボードからのドリルダウン調査のイベント数の概要が正しく表示されない場合があります。 |
| Ver.9.05.11 | 2019/10/21 | Syslog および SNMP 経由のイベントレポートのパフォーマンスが最適化されました。 修正された問題 SCANS メソッドのフローが欠落する問題を修正しました。 |
| Ver.9.05.09 | 2019/09/23 | 修正された問題 多数のイベント処理に対応するために、誤検知除外機能に使用するカウンタのサイズを増やしました。 |
| Ver.9.05.08 | 2019/09/02 | 誤検知除外機能の動作中にイベントが削除された場合に警告処理が追加されました。 修正された問題 Flowmon OS 10.3 の Flowmon ダッシュボードが正しく表示されるようになりました。 フランス語でのイベントの CSV エクスポートに対応しました。 新しいパースペクティブに対する評価が改善されました。 |
| Ver.9.05.07β | 2019/08/16 | 誤検知除外機能の統計処理バッチのパフォーマンスが改善されました。 Flowmon OS による IP アドレスに関する地理情報の表示が改善されました。 Flowmon OS 10.3 のサポートが可能となりました。 修正された問題 イベントの詳細情報内の誤検知除外機能により削除されたターゲット情報が改善されました。 誤ったタイムゾーンで検索された IDS イベントが改善されました。 イベント処理中のイベント詳細の表示をブロックしました。 |
| Ver.9.05.06 | 2019/06/25 | より迅速な誤検知と見通しの評価ができるようになりました。 修正された問題 期限切れのフロータイムスタンプが誤ったイベントタイムスタンプ正規化する問題を修正しました。 |
| Ver.9.05.05 | 2019/06/20 | 新しいイベントの最適化処理が可能になりました 修正された問題 IPv6 アドレス ffff : ... : ffff がフィルタに存在する場合、イベント処理が機能しない問題を修正しました。 誤検知ルール使用カウンタの最大値に達したときにイベント処理が機能しない問題を修正しました。 データ処理用データベースの起動が遅れていた問題を修正しました。 管理者以外のユーザが CSV ファイルのレポートをエクスポートすることができない問題を修正しました。 |
| Ver.09.05.04 | 2019/05/24 | FlowmonOS 10.2 のサポートが可能となりました。 修正された問題 ADS 分散アーキテクチャが有効になっている場合、特殊な環境下において誤検知機能が作動しない問題を修正しました |
| Ver.9.05.03β | 2019/04/17 | 修正された問題 Syslog/SNMP イベント報告が遅延する問題を修正。 仮想ソースが有効になっていると Syslog/SNMP イベントレポートが機能しない問題を修正。 http ホスト名に基づくブラックリストが機能しない問題を修正。 イベント詳細ダイアログで、既存のイベント誤検知ルールを評価してしまう問題を修正。 |
| Ver.9.05.02β | 2019/03/26 | 修正された問題 FMC で NEL/NSEL 拡張が有効になっている場合に間違った国コードになる問題を修正。 データフィールド All が選択されていると CSV レポートが機能しない問題を修正。 メールイベントレポートが機能しない問題を修正。 Flowmon OS 10.1.3 でのイベント証跡の破損を修正。 メソッドを無効にしたときにメッセージにコロンが表示されない問題を修正。 注：Syslog Machine Readable Detail は、属性にも統一単位 (KiB) を使用します。 注：Flowmon OS ver.10.01.04 より古いバージョンの Flowmon コンフィグレーションセンターでは、ブランディング機能により PDF レポートのロゴを変更することができません。 |
| Ver.9.05.01β | 2019/02/22 | 修正された問題 E メールへの送信が失敗するという問題において、PDF のスケジュールされたレポートを修正しました。 ワイルドカードを使用した False Positive ルールにより処理が停止する問題を修正しました。 注：PDF レポートのロゴは現在ブランディングでは変更できません |
| Ver.9.05.00 | 2019/02/07 | ダッシュボードの概要ページを以下の通り再設計しました。 時間内のイベント数とフロー数/秒の新しいグラフを表示。 グラフの下に表示されるイベントの種類は無制限です。 |

| ver.No | リリース日 | 変更箇所 |
|--------------|------------|--|
| | | <p>自動更新は更新ボタンで有効にできます。</p> <p>誤検知ルールを無効にして再度有効することができます。</p> <p>選択したオプションで誤検知ルールが作成された場合、イベントを削除できます。</p> <p>ADS 分散アーキテクチャがアクティブな場合、Syslog/SNMP は、マスターノードから送信されます。</p> <p>Flowmon Traffic Recorder ver.10(アダプティブバッファ)に対応し、履歴の記録を開始できます。</p> <p>修正された問題</p> <p>グラフにイベントが表示されないという問題において、[イベント]ページの集計ビューが修正されました。</p> <p>DNSREVERSE メソッドの遅延イベントを修正しました。</p> <p>注：Syslog マシンの読み取り可能な詳細は一時的に変更されます（単位は以前のように統一されていません）。</p> |
| Ver.9.04.02 | 2018/11/9 | <p>データフィールド設定のバグを修正しました。</p> <p>（バージョン 9.04.01 で「仮想ソースとしてのチャンネル」オプションが変更された場合）</p> <p>最新のユーザガイド（日本語）を掲載しました。</p> |
| Ver.9.04.01 | | <p>無効な XML 設定のインポートを修正しました（データフィールドセクション）</p> <p>分散アーキテクチャモードでのデータフィールドの予期しない無効化を修正しました。</p> |
| Ver.9.04.00 | | <p>ADS 分散アーキテクチャ設定ウィザード (kads-wizard.py) を追加しました。</p> <p>アトミックフィルタをリレーショナルに変換するための新しい関数。</p> <p>既存のデータフィールドをすべての検出方法に割り当てるための新機能。</p> <p>データフィールドページで欠けているプロフィール/チャンネルのシグナル伝達を改善しました。</p> <p>ADS イベントデータベースに関する稀な問題を修正しました。</p> |
| Ver. 9.03.00 | | Flowmon OS 10 に対応いたしました。 |
| Ver.9.02.02 | 2018/10/24 | <p>Flowmon OS 9.01.06 で ADS の以前のバージョンをアップグレードする機能が追加されました。</p> <p>（Flowmon ADS は、Flowmon OS がバージョン 9.02.01 以降にアップグレードされるまで無効になります）</p> <p>MAC アドレスの検出（イベントソース IP として 127.0.0.1 の場合）が修正されました。</p> <p>Flowmon OS 9.02.02 以降のイベント報告を修正（動作していない）しました。</p> <p>Flowmon OS 9.02.02 以降のブラックリストの表示を修正（予期しないエラー）しました。</p> |
| Ver.9.02.01β | | <p>イベント詳細の詳細およびソース MAC アドレスを使用した syslog レポートが拡張されました。</p> <p>syslog メッセージの変更点：</p> <p>- 新しいフィールドを追加しました smac = XX : XX : XX : XX : XX : XX</p> |
| Ver.9.02.00β | | <p>削除された機能「脅威（集約されたイベント）」。</p> <p>新しい言語（ドイツ語、フランチャイズ、スペイン語）のサポートを追加。</p> <p>ユーザグループ（FCC ロール、ADS タブ）に ADS 管理者権限を与える機能を追加。</p> <p>簡単にフォーム設定を複製するための「名前を付けて保存」機能が新しく追加されました。</p> <p>計算データベース（セキュリティパッチ）が更新されました。</p> <p>BPATTERNS - 新しいパラメータ "Activation"（新しく追加されたパターンのデフォルトステータス）が追加されました。</p> <p>CSV ファイルへのエクスポートを修正しました（最大イベント数）。</p> |
| Ver.9.01.03 | 2018/5/24 | <p>電子メールレポートに GPG 暗号化/署名のサポートを追加（FM 9.01.03 より）しました。</p> <p>拡張された RESTful API : カスタムスクリプトとレポート</p> <p>長い章名を持つ PDF レポートの構成エクスポートを修正しました（間違った名前切り捨てにより、インポート後に依存関係が失われる不具合を修正）。</p> <p>ADS ライセンスを下位モデルに変更した時の、データフィールドのアクションの不具合を修正しました。</p> <p>HONEYPOT メソッドの IgnoreAccessFrom パラメータを修正しました。</p> <p>今後の FM 10.00.00 (NoDataException) との互換性が修正されました。</p> |
| Ver.9.01.01 | 2017/11/1 | Flowmon OS 9.00.04 以上でのイベントエビデンスへのフローロードが改善されました。 |
| Ver.9.01.00β | | <p>新しい検出方法 DICTATTACK（辞書攻撃の一般的な検出）</p> <p>レポートに CSV 形式のエクスポートを追加</p> <p>カスタムパターンの強化された機能（Having 節、イベントソースの選択、ヘルプの追加）</p> <p>フィルタ、パースペクティブ、データフィールドの削除に関連するすべてのアクションに関する警告が改善されました。</p> <p>SNMP イベントレポートの改善（複数のレポート、FCC SNMP ターゲットグループのサポート）</p> <p>ダッシュボードページにデータロードの信号を追加（ドリルダウン）</p> <p>ADS Ultimate ライセンスのサポートを追加</p> <p>修正された syslog イベントレポート形式（Syslog UDP 送信者が使用されている場合、ホスト名が不明）</p> <p>脅威のリスニングイベント（rest / ads / threats / <id> / events はコード 302 を返すことがある）のための固定 RESTful API クエリ</p> <p>イベントの詳細でのトラフィック記録ファイルのダウンロードを修正しました（「同じイベント間隔」が設定されている場合）</p> |
| Ver.9.00.01β | | 多数のフロー・ソースに対する最適化された処理パフォーマンス（統計的オーバーヘッドを削減） |

| ver.No | リリース日 | 変更箇所 |
|---------------|-----------|--|
| | | アップグレード後に固定フローソースが停止する（「実行していない」状態が表示される） |
| | | Flowmon モバイルダッシュボードアプリケーションのウィジェット表示を修正しました |
| | | 固定イベントの有効期限（Delete Events After パラメータで定義された時間より前に発生する可能性があります） |
| | | すべてのフローソースまたはフィルタを削除した後のユーザインターフェイスの問題を修正しました。 |
| | | 改善されたユーザガイド（検出方法の再編成、オペレーティングシステムテーブルのカスタムパターンへの追加） |
| Ver.9.00.00β | | Flowmon OS 9.x プラットフォーム（データ処理、システムサービスなどの新しいデータベース）に最適化されています。 |
| Ver.8.02.05 | 2017/7/27 | 日本語版ユーザガイドをアップデートしました。 |
| Ver.8.02.04 | 2017/2/16 | Flowmon OS バージョン 8.03 以上でのイベント証拠の表示を修正しました。 |
| | | ・MAC アドレスコンテキストメニューの固定ラベル |
| | | ・特殊な記号を使用した外部 IP サービス URL の修正 |
| | | IP アドレス割り当て（望ましくない IP 部分文字列一致）に対する DNS 名を修正しました。 |
| | | イベントエビデンスでのフィルタリングのパフォーマンスが向上しました。 |
| Ver.8.02.03 | 2017/1/18 | 特別な場合の UPLOAD メソッドの検出を修正しました（pairwise オプションを無効にしました） |
| | | ダッシュボードの概要図の月の名前の翻訳が修正されました |
| | | SCANS – RST / ACK スキャンの実験的検出を削除。 |
| Ver.8.02.02 | | ブラックリストイベントベースのホスト名の詳細を修正（変換するバイト数の合計） |
| Ver.8.02.01 β | | データ処理のデータベースの起動処理を修正 |
| | | 長文の DNS レコードの表示を修正 |
| | | 自動 IP アドレス名前変換が無効になったとき、誤検知除外処理の修正 |
| | | 双方向フローに関連した、検知メソッドの修正（IPV6TUNNEL, SRVNA, DNSANOMALY,) |
| | | BLACKLIST - "malware domains" の情報で、"malware activities" を変更しました。 |
| Ver.8.02.00 β | | パフォーマンスの改善（双方向フローに切り替え） |
| | | フローサンプリングの拡張（ペアフローの対策） |
| | | フローの重複の解析拡張（異なるソースからのフローのみを比較） |
| | | 逆引き DNS レコードの取り込みメソッドを変更（ページレンダリング中にリアルタイム処理） |
| | | MULTICAST - MAC アドレスベースの検知を追加 |
| | | REFLECTDOS - 新規 TFTP 攻撃の検知を追加（TrivialFTP パラメータ） |
| | | SMTAPANOMALY - 新規パラメータ IgnoreSYNflows 追加（検知から SYN フローを除外） |
| | | SYSHECK - 新規パラメータ DeactivateOnFlood 追加（大量のイベント発生時に無効にするメソッド） |
| Ver.8.01.02 | | SNMP 経由のイベントレポートの修正 |
| | | 存在しないプロファイルチャンネルでフローソースの設定の保存処理を修正 |
| | | 誤検知除外処理の修正（名称に特殊なフィルタ記号が含まれる場合） |
| | | イベントエビデンスタブ上のメニューオーバーレイの修正 |
| | | イベントの集約表示の拡大表示を修正 |
| Ver.8.01.01 | | AdBlock browser プラグインによるブロックされた機能 "Show filters for IP" の修正 |
| | | "Edit user" 表示中の "Renamer settings" の保存を修正 |
| Ver.8.01.00 | | 新分散アーキテクチャ（複数の ADS がインストール環境のリンクの可能性） |
| | | 大規模ブラックリストのサポートを追加（C&C ドメインリスト |
| | | メールイベントレポート中の日付フォーマットの選択オプションの追加 |
| | | PDF チャプタ"Events by priority"中のイベントソートのためのオプションの追加 |
| | | メインメニューの表示の更新 |
| | | ロングテーブルでの新フローティングヘッダー表示 |
| | | 新機能 "Show filters for IP"（IP アドレスの文章メニュー） |
| | | "Event detail" 拡張表示（メソッドインスタンスの名称追加） |
| | | 最新のダウンロードされたブラックリストの表示拡張（ページを追加） |
| | | "Event Evidence" テーブルの拡張（新規のフィールド、apptag コードからアプリケーション名変換） |
| | | NATDET - IP アドレスの背後の NAT の発見する新たなメソッドの追加 |
| | | BLACKLIST - イベント詳細の拡張（ブラックリストされたドメインの表示） |
| Ver.8.00.05 | | syslog メッセージの SMTAPANOMALY メソッドの説明が消える問題の修正 |
| Ver.8.00.04 | | スケジュールド PDF レポートの修正(送信) |
| | | プロキシ相関関係の修正と拡張(設定ミスについての注意を追加) |
| Ver.8.00.03 | | HTML イベントレポートの拡張（イベント詳細に関連する IP アドレスの代わりにホスト名を利用） |
| | | アップグレード中、SCANS メソッドの DetectOnlyKnown のオプション設定が上書きされる問題の修正 |
| Ver.8.00.02 | | 翻訳のミスを修正（アップグレード後のキャッシュのリフレッシュ） |
| | | バックグラウンドで起動する ADS データベースの修正(システム起動がブロックされた) |

| ver.No | リリース日 | 変更箇所 |
|---|-------|---|
| Ver.8.00.01 | | ADS ソース編集フォームでプロフィール/チャンネルの表示を修正 |
| Ver.8.00.00 | | 関連フィルタの追加 (関連情報でのフィルタ込み入ったフィルタの定義を許可) |
| | | 誤検知除外ページの IP アドレス表示の拡張 |
| | | PDF レポート用の新規チャプタ "Events by type"を追加 (タイプによる TOP 10) |
| | | PDF レポートのパーミッションの再設定(オーナー設定機能を追加) |
| | | IgnoreInternal パラメータの追加(内部ローカルセグメントの通信を無視) |
| | | BLACKLIST - DNS トラフィックでブラックリストされたドメイン名を検出するを新規に追加(Flowmon 独自 DNS フィールド設定) |
| | | DOS - syn flood と fin2-wait 攻撃を検出する機能を新規に追加 |
| | | MULTICAST - 高トラフィックを検出する機能を新規に追加(データ合計もしくは秒間での高パケットレート) |
| | | REFLECTDOS - portmap サービス経由の攻撃を検出する機能を新規に追加 |
| | | SCANS - ARP scans 検出する機能を新規に追加 |
| | | SCANS - DetectThesePorts パラメータにポートレンジ入力可 |
| | | OUTSPAM メソッドを SMTPANOMALY メソッドに名称変更 |
| | | BTTORENT MinSeeds パラメータの意味を変更 (すべてのイベントに適用) |
| | | CSV ヘフィルタをエクスポート 機能を削除 (重複のため、FCC コンフィグレーションのインポート/エクスポートでリプレイス) |
| | | 空き容量のアラートを削除(クォータ管理に定義された推奨されないデータ領域) |
| | | syslog メッセージの変更 |
| | | 短いメソッドコード後にメソッド名が長い場合の問題を修正 |
| INVEA-TECH の社名変更に伴う、会社名記述を Flowmon Networks に変更 | | |
| いくつかのメソッドのイベント推奨詳細を変更(例 : MULTICAST) | | |