Progress Flowmon ADS 12.3 の新機能

一般的に企業の情報システム部門は、より効率的にネットワークの可視性、異常を検知できるようプロセスを合理化することができるソリューションを求めています。
Flowmon Anomaly Detection System (ADS)の最新のアップデートは、お客様が抱えるこのような懸念に対応することを目的として開発されています。本記事では、Flowmon ADS 12.3 がお客様の組織の脅威分析とサイバーセキュリティ戦略を改善する手助けとなり得る情報についてご紹介します。

Dashboard and Reports の解析概要と脅威スコアウィジェット

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。

解析の概要

ダッシュボード機能では、「解析の概要」ウィジェットを利用し、選択期間と過去を比較し、何が変化したか、脅威的なホストのセキュリティ状況がどのように変化しているかを確認することができます。このウィジェットは、「ダッシュボード」または「レポート」チャプターに追加することができます。

注：解析概要ウィジェットを編集時に、表示内容（フロー、イベント、脅威スコア、メソッド）を選択できます。また、メソッドコードを正式名称に切り替えることもできます（「DOHDET」から「DoH サーバとの通信」など）。

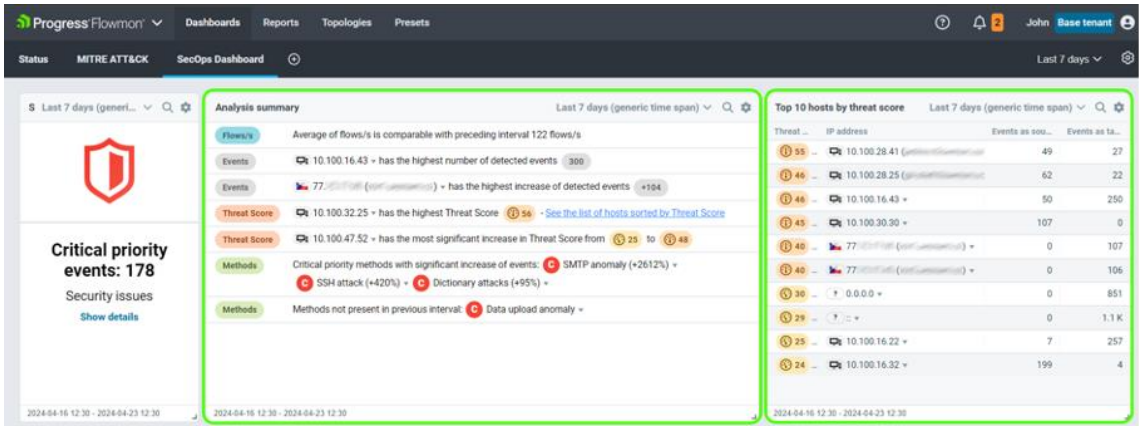


図 1: Flowmon ダッシュボード上の 2 つの新しいウィジェット
左側が解析の概要、右側が脅威スコア。

脅威スコア

脅威スコアは最も脅威的なホストを特定し、調査作業の優先順位付けに役立ちます。検出されたイベントの数、優先度、ターゲットの数など、さまざまな要因から判定されます。また、脅威スコアは MITRE ATT&CK フレームワークの戦術を使用し、わかりやすく表示します。図 1 の右側が、Flowmon ダッシュボード上の脅威スコアウィジェットです。脅威スコアでソートされた TOP10 のホストを表示しています。

新しいウィジェットを有効にする方法

ダッシュボードに新しいウィジェットを追加するには、ダッシュボードの下部にある[新しいウィジェット]ボタンを押下するか、レポートの作成または編集時に[新しいチャプター]ボタンで追加できます。

合理化されたイベント解析ワークフロー

Flowmon ダッシュボードは、現在のセキュリティ状況の概要を提供します。これにより、次の調査ステップの優先順位を決めることができ、多くの場合 Flowmon ADS の解析結果はネットワーク内の状況把握に役に立ちます。

本アップデートでは、Flowmon ADS ウィジェットの IP アドレスとメソッドのドリルダウンメニューを拡張し、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できるようになりました。新しいドリルダウンメニューから目的の IP アドレスやメソッドをクリックし、オプションを選択するとイベント画面へ遷移します。

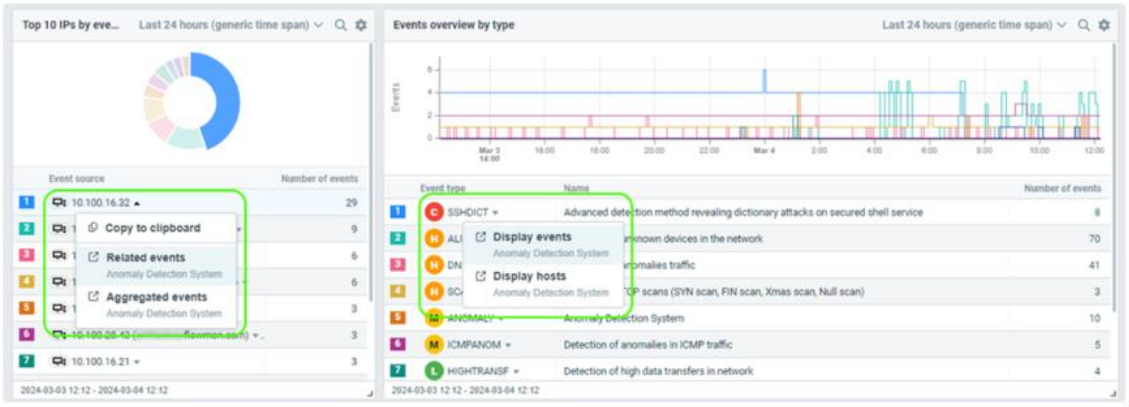


図 2：IP アドレスとメソッドの新しいドリルダウンメニュー

メニューからオプションを選択すると、Flowmon ADS のイベント画面に移動し、関連する項目が自動入力され、結果が表示されます。

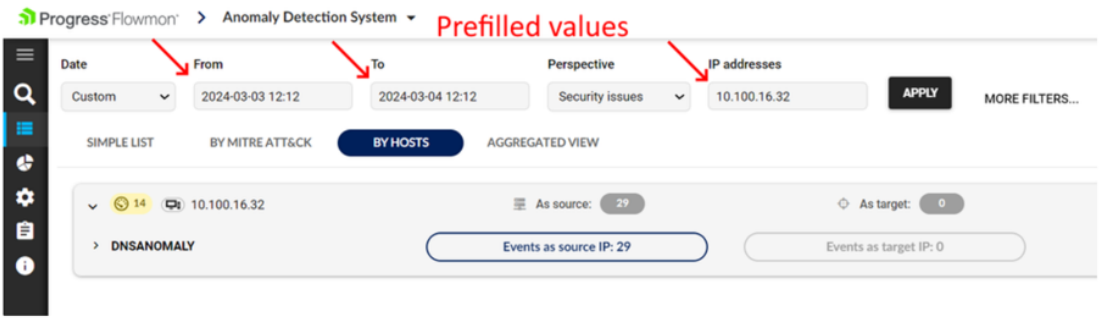


図 3：ADS のイベント画面

関連項目は自動で入力されます。ダッシュボードまたはレポートから遷移できます。

マルチテナント

マネージドサービスプロバイダー(MSP)は通常、複数の組織にサービスを提供しています。12.3 リリースでは、1 つの Flowmon デプロイメント上で、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。ADS は現在、Flowmon Configuration Center で定義されたテナントをサポートしていますが、MSP は 1 つの Flowmon で複数のクライアントを管理することができます。

Flowmon Configuration Center では、テナントがアクセスできるフローソース、またはプロファイルを指定できます。ADS ではこれらのプロファイルを特定のデータフィードに割り当て、ユーザはアクセスを許可されたデータのみを表示できます。また、REST API も更新され、エンドポイントには関連するテナントの情報を提供する「tenantId」フィールドが含まれるようになりました。

ユーザーガイドのテナントの章では、ADS でマルチテナント環境を使用するための具体的な要件について説明しています。特に、Syslog および SNMP レポートを使用している場合、テナントに 1 秒あたりのフロー（FPS）制限を適用したい場合、バージョン 12.3 にアップグレードできない場合、また ADS 12.3 でのマルチテナントの仕組みについて詳しく知りたい場合は、本内容をご覧ください。
ADS12.3 にアップデートした後も、以前のシングルテナントモードで Flowmon を使用することもできます。12.3 にアップデートする際、現在の設定を変更する必要はありません。ただし、マルチテナントでクライアントをサポートするオプションがあります。

マルチテナントを有効にする方法

Flowmon ADS でテナントを有効化するには、Configuration Center＞システム＞ユーザ設定＞テナントメニューに記載されている手順をご確認ください。

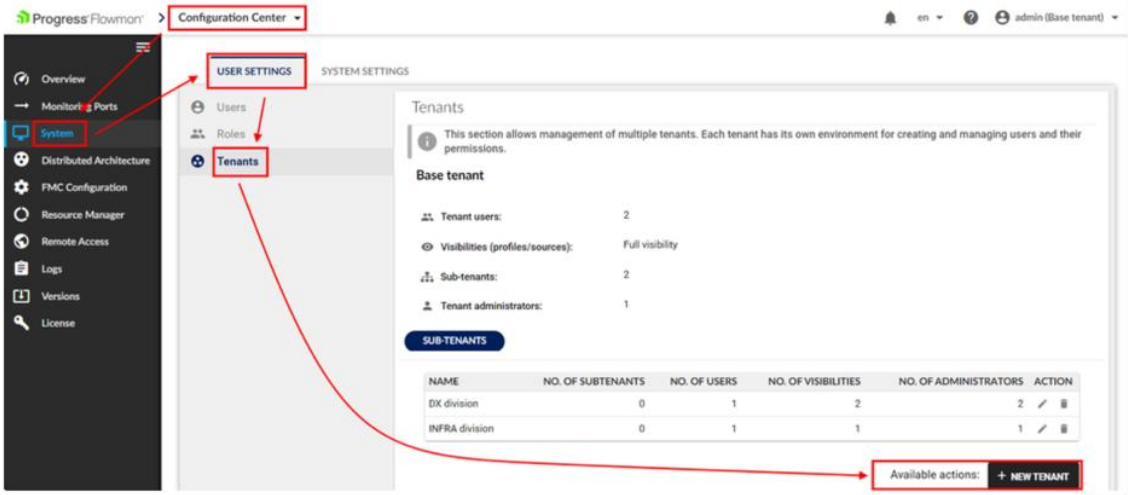


図 4：テナント管理画面への移動

必要なテナントを作成後、それぞれに新しい役割とユーザを作成する必要があります。特定のテナントに切り替えてから、そのユーザで役割とユーザを作成します。その後、ADS の管理画面に切り替え、各テナントの要件に合わせて設定します。
テナントの構成と設定に関する詳細は、Flowmon および Flowmon ADS のユーザーガイドの「テナントについて」に記載されています。

DNS トラフィックの検出改善

ADS 12.3 では、お客様からのフィードバック、最新のネットワークにおける DNS 用 TCP 使用量の増加を考慮し、DNS トラフィックの異常を検出する方法を改善しました。
修正点は以下の通りです：

・「DNSANOMALY」の「TCPDNS」サブメソッドに「IgnoreInternal」という新しいパラメータが追加されました。このパラメータを有効にすると、宛先 IP が外部であることを確認する追加チェックが行われます。これは、監視対象ネットワーク内で TCP プロトコル経由の、大規模な DNS 転送検出を取り除くのに役立ちます。

・ADS 12.3 では、「TCPTransferLimit」パラメータ範囲が拡大され、5 分間に 100MB までの TCP トラフィックが許容されるようになり、サブメソッドの感度が向上しました。

・「DNSANOMALY」の「UnusualServer」サブメソッドが更新され、「ClientsToExclude」という新しいパラメータが追加されました。このパラメータにより、ユーザはクライアントドメインを解決しようとする DNS サーバなど、DNS クライアントとして動作することがある DNS サーバを指定することができます。

・「DNSQUERY」メソッドが改良され、TCP トラフィックで送信された DNS リクエストに対して、より正確な情報を提供できるようになりました。UDP プロトコルで有効な 1 つのリクエストを 1 つのパケットとしてカウントするのではなく、TCP トラフィックで 1 つのリクエストを 1 つのフローとしてカウントするようメソッドを調整しました。この変更により、TCP プロトコルで送信された DNS リクエストの誤検知数が減少します。

DNSANOMALY メソッドに関連する変更は、設定画面で行うことができます。また、DNSQUERY の変更のために設定を変更する必要はありません。

メソッドインスタンス設定でサブメソッドをオフにする方法

最新のメソッドインスタンス設定では、特定のサブメソッドを無効にすることができます。これは特定のサブメソッドが必要でない場合、特に役立ちます。また、デプロイやチューニングの過程で一時的に検出をオフにすることもできます。以前は特定のコンフィギュレーション・パラメータを使用して、いくつかのサブメソッドをオフにすることができました。すべてのメソッドは、Flowmon ADS＞ 設定＞ 処理＞ メソッドから無効にすることができます。

イベント属性に上位ターゲットを追加

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。これらのターゲットは静的なものではなく、新しい情報が入手可能になると動的に変更され、最新の関連データを提供します。これらのターゲットの関連性は、使用する検出方法によって異なります。例えば、BITTORENT、COUNTRY、DIRINET、HIGHTRANSF、PEERS、WEBSHARE のような検出方法の場合、選択されるターゲットはデータ転送率が最も高いものになります。また、その他の検出方法では、フロー数に基づいてターゲットが選択されます。ADS 12.3 では、この変更をデフォルトで有効にしています。

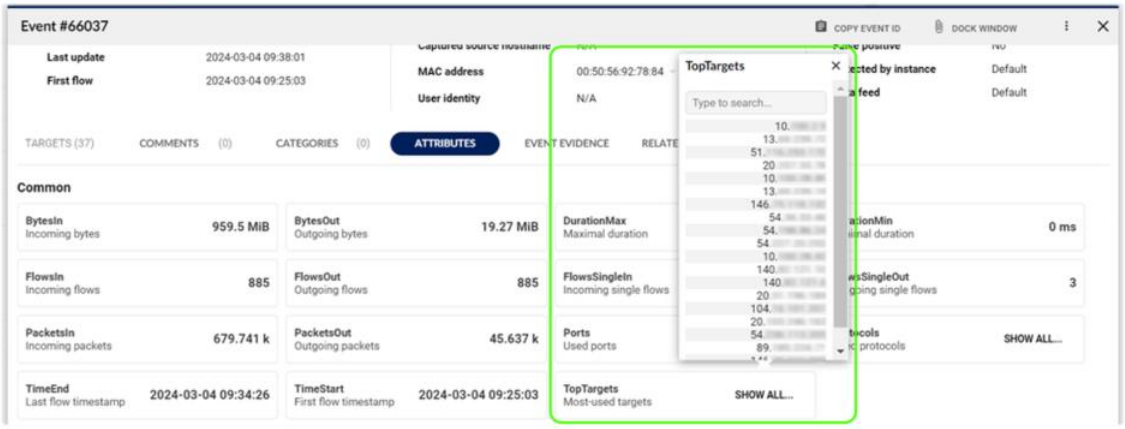
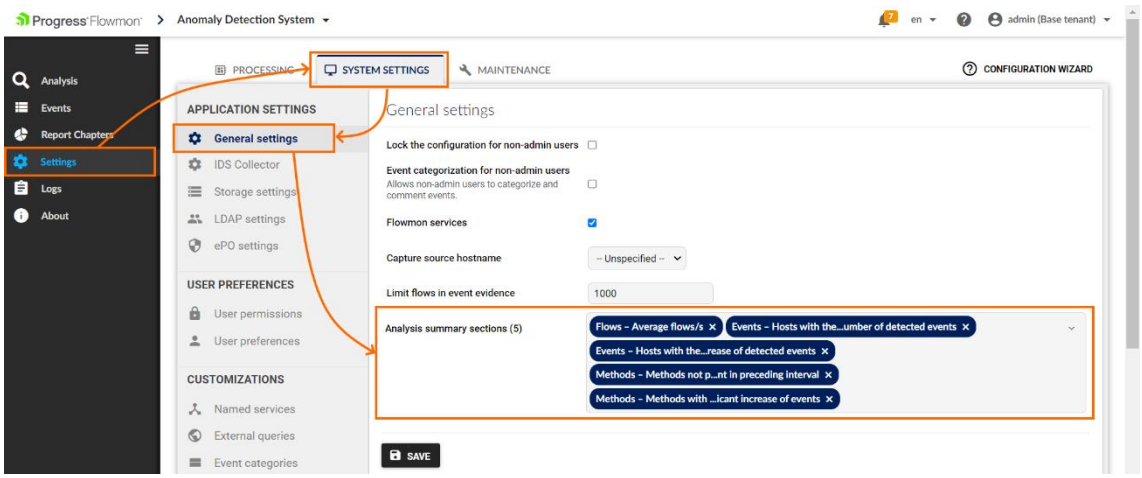


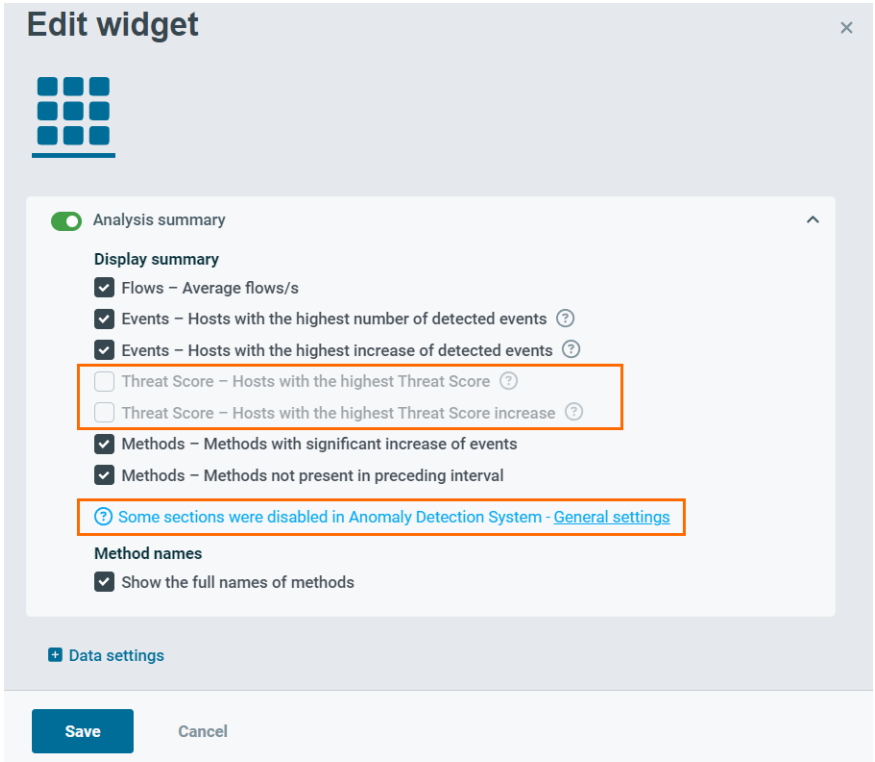
図 5：イベント詳細画面に表示される TOP 20 のターゲット

その他の変更

Flowmon ADS> 設定> システム設定> 一般設定で、解析の概要セクションを無効にすることができます。この設定はグローバルで、Dashboard and Reports の解析の概要ウィジェットに表示されるデータに影響します。特定のセクションが不要な場合、または解析ページの読み込み速度が低下している場合は、この設定を使用してください（この場合、「脅威スコア」セクションは最もリソースを消費するため、無効にすることを推奨します）。



解析の概要セクションは、一般設定で有効/無効を設定できます。



※解析の概要ウィジェットに無効にしたセクションは表示されなくなります。