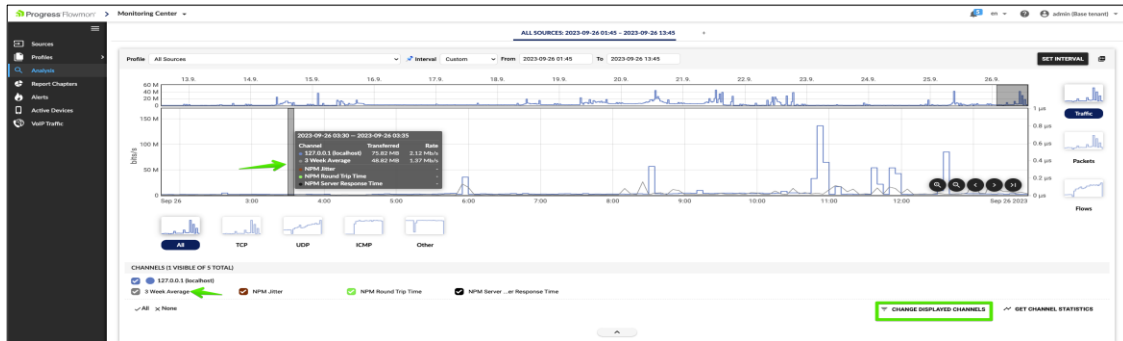


Flowmon 新バージョン ver.12.03 情報

1. トレンド分析機能が追加（3 Week average）

トレンド分析機能は、現在のネットワークトラフィックの状況を過去のトラフィック・トレンドと簡単に比較し、情報を得ることができる新機能です。日々のトラフィック状況と比較することで異常を発見し、トラフィックが時間とともにどのように変化しているか可視化可能です。また、ネットワークのキャパシティ・プランニングを行う際にも、有効活用いただけます。



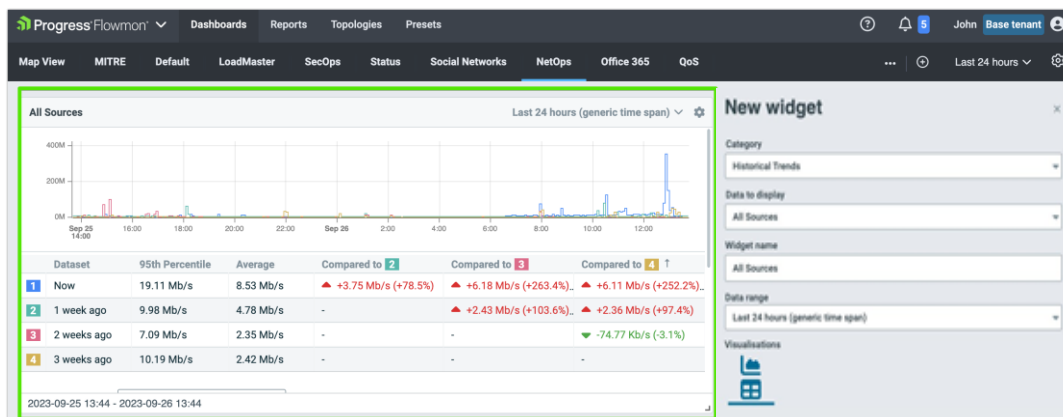
アクティベート方法：

1. Flowmon Monitoring Center > 解析にアクセスします。
2. 表示されているチャンネルの変更をクリックします。
3. Show 3 Week Average line チェックボックスが選択されていることを確認します。
4. グラフ下のチャンネルの 3 Week Average チェックボックスを有効にします。
5. 3 Week Average line がメインチャートに表示されます。



アクティベート方法：

1. Flowmon Monitoring Center > プロファイルにアクセスします。
2. 一つ目のチャート下の、過去の傾向タブを選択します。
3. 希望の間隔を指定し、期間の設定をクリックします。
4. チャート上で設定した間隔とチャート下の表で比較した過去のトレンドを表示します。

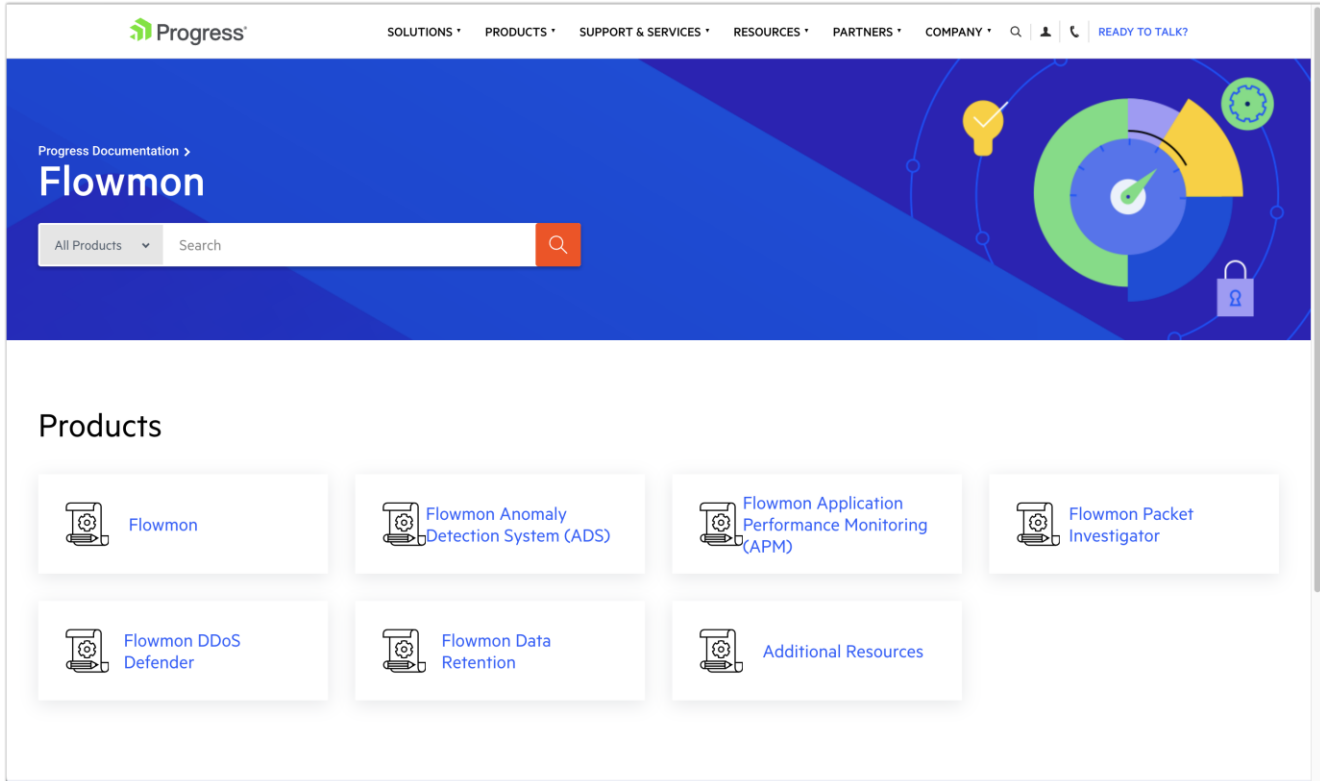


アクティベート方法：

1. Flowmon **Dashboards and Reports** にアクセスします。
2. ウィジェットに使用する予定のタブを選択します。
3. **カテゴリを過去の傾向に変更**します。
4. 通常のウィジェットと同様に、他の項目を設定します。
5. ウィジェット作成ダイアログの最後の部分で、必要なデータと**視覚化**を設定します。
6. **ウィジェットの作成**をクリックします。

2.新しいドキュメントプラットフォーム

Flowmon ユーザーガイドが移行され、より迅速に検索・閲覧ができる特別な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。アプライアンスには、ユーザーガイドの PDF 版が残っており、ネットワークからオンラインドキュメントにアクセスできない場合は、代わりに PDF が開きます。このプラットフォームには、Flowmon に関するその他多くの文書が含まれております。

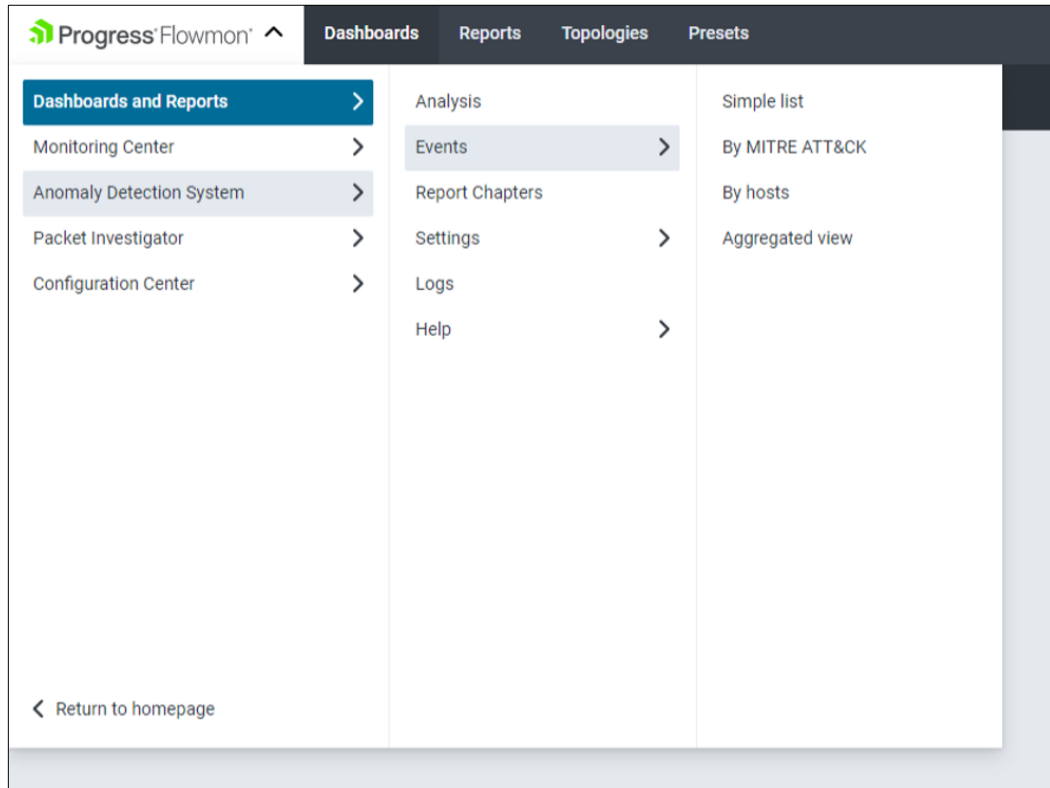


アクティベート方法：

1. いずれかの Flowmon モジュールのページにアクセスします。
2. ヘルプアイコンをクリックし、ユーザーガイドをクリックします。または、直接こちらにアクセスします。 <http://docs.progress.com/>。
3. Progress のオンラインドキュメント用プラットフォームが開きます。

3. Dashboards and Reports の新しいナビゲーションメニュー

このリリースでは、Dashboards and Reports の機能画面へのアクセスを統一し簡素化することで、使いやすさとユーザーエクスペリエンスを向上させています。コンソールの左側に新しいメニューが追加され（下図参照）、インストールされているすべてのモジュールを通じて、Flowmon プラットフォーム内を素早く移動することが容易になりました。

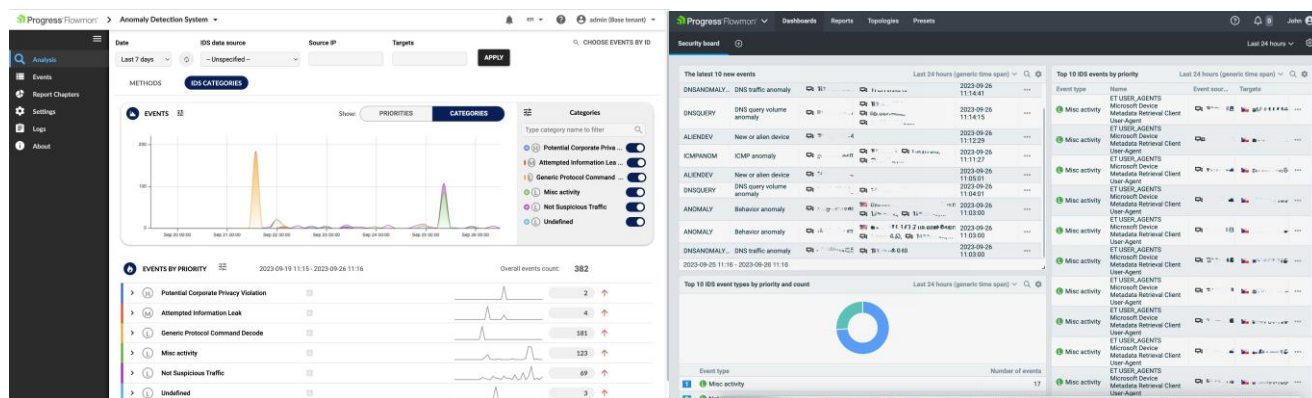


Dashboards and Reports での通知エクスペリエンスは、より直感的になり、他の Flowmon モジュールと連携するようになりました。

4.新しい Intrusion Detection System (IDS) イベント解析

IDS イベントの調査を効率化するため、異常検知システムと同じビジュアルとワークフローを備えた新しい IDS イベント解析を導入します。IDS イベントの詳細には、関連する IDS イベントと関連するフローも含まれ、フローレベルでの迅速な解析のために、FMC (Flowmon Monitoring Center) 解析へのリンクがあります。ダッシュボードには IDS 関連のウィジェットを配置でき、レポートには IDS 関連のチャプターを配置できます。

注: 解析ワークフローとドリルダウンは同じですが、IDS イベントは ADS イベントと同じイベントパイプラインには従いません。例えば、IDS イベントに基づいてカスタムアクションを設定することはできません (Flowmon Probes から syslog を使用して IDS イベントを直接送信することは可能ですが、ADS からの syslog レポートは現在カスタムアクションとして利用できない等)。



注意事項:

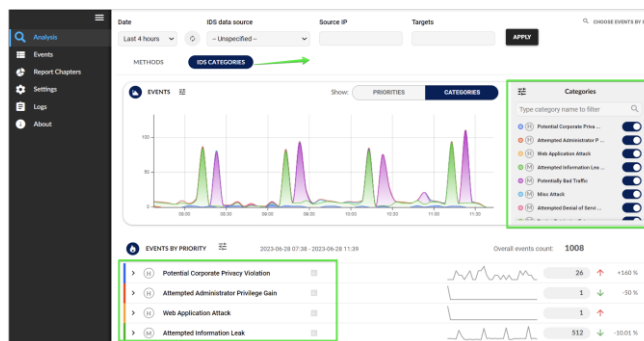
この機能は、Flowmon IDS Probe パッケージを Flowmon Probe にインストールし、Flowmon ADS で IDS コレクタを有効にすることで有効になります。Flowmon IDS Probe パッケージのダウンロードおよびインストール、設定、チューニングの詳細については、こちらの[ブログ記事](#)をご覧ください。

また、[サポートポータル](#) (Knowledge → Flowmon Integrations → Flowmon IDS Probe) でも詳細をご覧ください。

IDS コレクタをアクティブにします ([Anomaly Detection System 設定] → [システム設定] → [IDS Collector] に移動)。

アクティブをクリックします。解析に戻ります。

注: IDS コレクタを有効にしたにもかかわらず、IDS イベントが表示されない場合は、上記のブログ記事を読み、サポートポータルを確認してください。正しく設定されていない可能性があります。



アクティベート方法:

1. Flowmon Dashboards and Reports で新しいウィジェットを作成します。
2. カテゴリで Intrusion Detection System を選択します。
3. ニーズに応じて他のパラメータを選択します。
4. 作成をクリックし、ウィジェットの作成を完了します。

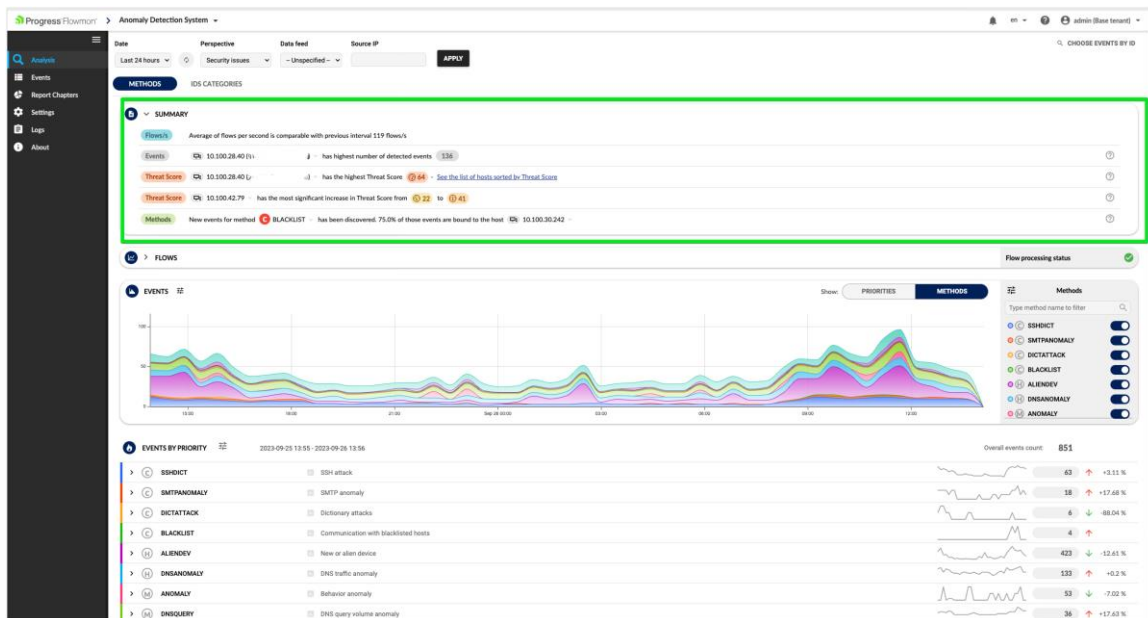
5. 脅威スコアの判定

脅威スコア機能は、重要な脅威アクターや関心のあるホストに焦点を当てるのに役立ちます。脅威スコアの計算では、特定のホストで検出されたイベントの数、優先度、これらのイベントに含まれるターゲットの数、イベントに割り当てられた MITRE ATT&CK フレームワークの戦術など、さまざまな側面を考慮します。ネットワーク内のどのアクターが最も疑わしく、最も注意を払う必要があるかを知ることができます。

Flowmon は、選択された時間間隔の中で最も重要な発見や注目すべき出来事を集約し、数行に要約します。この機能は、作業の優先順位をつけ、最も重要な発見に集中できるように設計されています。解析では、選択した時間間隔における最も重要な発見と注目すべきイベントの自動概要が含まれるようになりました。また、重要な脅威アクターまたは関心のあるホストに優先順位を付けて焦点を当てるのに役立つ、まったく新しい脅威スコアも含まれています。

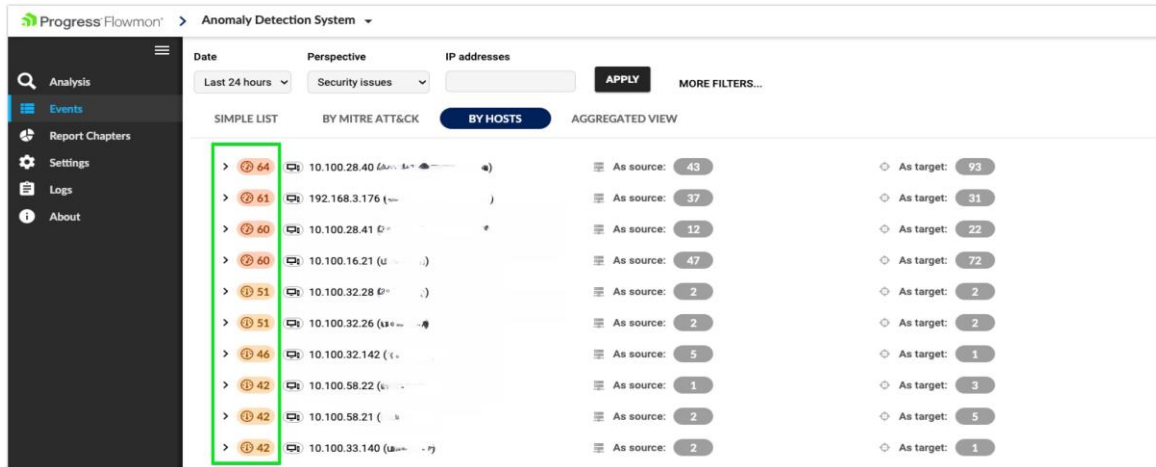
解析概要のハイライト：

- 解析概要は、選択された時間間隔を考慮し、同じ長さの前の間隔と比較します
- イベント数が最も多い、または増加したホスト
- 脅威スコアが最も高い、または増加したホスト
- 前回のインターバルには存在しなかったイベントまたはメソッドが大幅に増加したメソッド
- 平均フロー/秒の増減。ライセンス制限により処理されなかったフロー数



アクティベート方法：

1. Flowmon Anomaly Detection System 解析にアクセスします。
2. 脅威スコアは、解析の概要で利用できます。



アクティベート方法 :

1. Flowmon Anomaly Detection System イベントにアクセスします。
2. ホスト別をクリックします。

6.IP マッピングへのアプリケーション

Flowmon ADS は、IP アドレスを対応する SaaS アプリケーションやプラットフォームにマッピングするためのネットワークインテリジェンスを提供します。これにより、イベント解析と調査のプロセスが簡素化されます。

特定の IP アドレスのアプリケーションまたはプラットフォームに関する情報は、ユーザが外部 IP アドレスを見ることができる ADS の、あらゆる場所で利用できるようになりました。（Event Evidence を除く）。

[一般 IP 情報]に、アプリケーション名とロゴ、カテゴリ、ホームページ、および説明を含むアプリケーションタブが含まれるようになりました。イベント詳細のターゲットウィンドウとタブに、マップされたアプリケーションによってターゲットにされたイベントを集約するアプリケーション別ビューが含まれるようになりました。

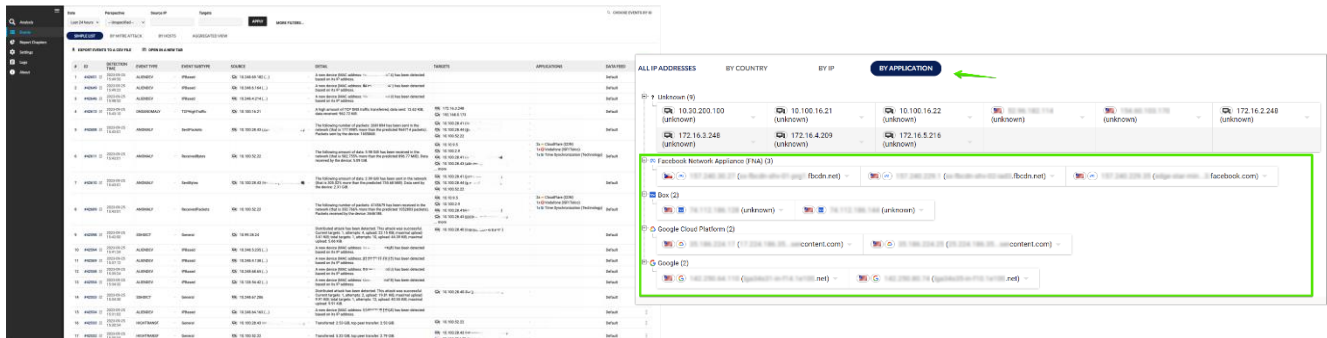
IP アドレスの横に表示されるアイコン/ビジュアルのデザインが変更されました :

- ・国アイコン/アプリケーションアイコン/ブラックリスト IP アイコン

注 : アプリケーションから IP へのマッピングは、有効な Standard または Extended サポートでのみ利用可能です。

注 : アプリケーションから IP へのマッピングは、ADS モジュールでのみ利用可能です。ADS 関連のウィジェットや Flowmon Dashboards and Reports およびレポートのチャプターでは使用できません。

注 : 外部 IP がアプリケーションにマッピングされます。Flowmon が一致を検出した場合、アプリケーションが追加され、そうでない場合は空白になります。



EVENTS BY PRIORITY 2023-09-24 15:57 - 2023-09-25 15:58 Overall events count: 6

ANOMALY 4 events of the type ANOMALY from 1 source IP addresses detected

Detected 4 events of the type ANOMALY from 10.100.52.22

Nighttime

ID	DETECTION TIME	LAST UPDATE	DETAIL	TARGETS	APPLICATIONS	DATA FEED	METHOD INSTANCE	COMMENTS
#42609	2023-09-25 15:43:01	2023-09-25 15:43:01	The following number of packets: 4745679 has been received in the network (that is 320.76% more than the predicted 1052903 packets). Packets received by the device: 3646188.	10.10.9.5 10.100.2.9	2x = CloudFlare (CDN) 1x = Vodafone (SP/Telco) 1x = Time Synchronization (Technology)	Default	Default	
#42811	2023-09-25 15:43:01	2023-09-25 15:43:01	The following amount of data: 5.98 GiB has been received in the network (that is 582.75% more than the predicted 896.77 MiB). Data received by the device: 5.09 GiB.	10.10.9.5 10.100.2.9	2x = CloudFlare (CDN) 1x = Vodafone (SP/Telco) 1x = Time Synchronization (Technology)	Default	Default	
#37065	2023-09-25 06:08:00	2023-09-25 06:08:00	The following number of packets: 2324096 has been received in the network (that is 245.57% more than the predicted 672533 packets). Packets received by the device: 1655387.	10.100.2.9 10.100.28.41 (i)	2x = CloudFlare (CDN) 1x = Vodafone (SP/Telco) 1x = Time Synchronization (Technology)	Default	Default	
#37067	2023-09-25 06:08:00	2023-09-25 06:08:00	The following amount of data: 2.74 GiB has been received in the network (that is 453.85% more than the predicted 505.84 MiB). Data received by the device: 2.31 GiB.	10.100.2.9 10.100.28.41 (i)	2x = CloudFlare (CDN) 1x = Vodafone (SP/Telco) 1x = Time Synchronization (Technology)	Default	Default	

Showing 1 - 4 of 4

EVENTS BY PRIORITY 2023-09-24 15:44 - 2023-09-25 15:45 Overall events count: 1003

SSHDICT 66 events of the type SSHDICT from 25 source IP addresses detected

Detected 2 events of the type SSHDICT from 10.99.28.24

Nighttime

ID	DETECTION TIME	LAST UPDATE	DETAIL	TARGETS	APPLICATIONS	DATA FEED	METHOD INSTANCE	COMMENTS
#42598	2023-09-25 15:42:00	2023-09-25 15:42:00	Distributed attack has been detected. This attack was successful. Current targets: 1, attempts: 6, upload: 22.24 KiB, maximal upload: 5.66 KiB, total targets: 1, attempts: 6, upload: 22.24 KiB, maximal upload: 5.66 KiB.	10.100.28.40 (i)		Default	Default	
#41301	2023-09-25 12:26:06	2023-09-25 14:06:12	Distributed attack has been detected. This attack was successful. Current targets: 1, attempts: 2, upload: 12.92 KiB, maximal upload: 6.46 KiB, total targets: 2, attempts: 33, upload: 180.82 KiB, maximal upload: 9.53 KiB.	10.100.28.40 (i) + 10.100.56.131		Default	Default	

Showing 1 - 2 of 2

Customize table columns: Applications, Method instance, Comments, Categories

#	ID	DETECTION TIME	EVENT TYPE	EVENT SUBTYPE	SOURCE	DETAIL	TARGETS	DATA FEED
1	#2068	2023-08-02 13:14:02	UPLOAD	General	10.99.18.149 China Telecom IDC (Hosting)	Uploaded: 13.26 MiB, downloaded: 1.55 MiB, port(s): 443.		Default
2	#983	2023-08-02 12:53:38	BLACKLIST	Host		Known attackers, attempts: 1, uploaded: 44 B, downloaded: 264 B, frequently used ports: 80.	10.100.24.18	Default

アクティベート方法：

アプリケーションマッピングは、有効なサポートを受けている顧客に対しては自動的に有効になり、ユーザインタフェースに表示されます。手動で有効にすることもできます：

1. Anomaly Detection System にアクセスします。
 2. 解析にアクセスします。
 3. 優先度別のイベントで、検出方法を展開し、ソース IP を展開します。
 4. テーブルの列をカスタマイズするアイコンをクリックします。⇒
 5. アプリケーションチェックボックスを選択します。
- ※テーブルの「アプリケーション」列が表示されます。IP アドレスによっては、アプリケーションが空白の場合もあります。

Progress Flowmon > Anomaly Detection System

Date: Last 24 hours | Perspective: -- Unspecified -- | Source IP: | Targets: | APPLY | MORE FILTERS...

SIMPLE LIST | BY MITRE ATT&CK | BY HOSTS | AGGREGATED VIEW

EXPORT EVENTS TO A CSV FILE | OPEN IN A NEW TAB

DETAIL	TARGETS	APPLICATIONS	DATA FEED
A new device (MAC address: 08:00:27:11:11:11) has been detected based on its IP address.			
A new device (MAC address: 08:00:27:11:11:11) has been detected based on its IP address.			
A new device (MAC address: 08:00:27:11:11:11) has been detected based on its IP address.			
A high amount of TCP DNS traffic transferred, data sent: 12.62 KiB, data received: 962.72 KiB.	172.16.3.248 192.168.0.173		
The following number of packets: 2681894 has been sent in the network (that is 177.998% more than the predicted 964714 packets). Packets sent by the device: 1655868.	10.100.28.41 10.100.28.44 10.100.52.22		
The following amount of data: 5.98 GiB has been received in the network (that is 582.755% more than the predicted 896.77 MiB). Data received by the device: 5.09 GiB.	10.10.9.5 10.100.2.9 10.100.28.41 10.100.28.43 ... more	2x CloudFlare (CDN) 1x Vodafone (ISP/Telco) 1x Time Synchronization (Technology)	
The following amount of data: 2.99 GiB has been sent in the network (that is 305.02% more than the predicted 755.68 MiB). Data sent by the device: 2.31 GiB.	10.100.28.41 10.100.28.44 10.100.52.22		Default
The following number of packets: 4745679 has been received in the network (that is 350.766% more than the predicted 1052803 packets). Packets received by the device: 3646188.	10.10.9.5 10.100.2.9 10.100.28.41 10.100.28.43 ... more	2x CloudFlare (CDN) 1x Vodafone (ISP/Telco) 1x Time Synchronization (Technology)	Default

Customize table columns

- Detection time
- Last update
- Event subtype
- MITRE ATT&CK tactic
- MITRE ATT&CK techniques
- Applications
- Data feed
- Method instance
- Comments
- Categories

#	ID	DETECTION TIME	EVENT TYPE	EVENT SUBTYPE	SOURCE	DETAIL	TARGETS	APPLICATIONS	DATA FEED
1	#42651	2023-09-25 15:49:50	ALIENDEV	IPBased	10.248.69.182 (...)	A new device (MAC address: 08:00:27:11:11:11) has been detected based on its IP address.			Default
2	#42649	2023-09-25 15:49:22	ALIENDEV	IPBased	10.248.6.164 (...)	A new device (MAC address: 08:00:27:11:11:11) has been detected based on its IP address.			Default
3	#42646	2023-09-25 15:48:52	ALIENDEV	IPBased	10.248.4.214 (...)	A new device (MAC address: 08:00:27:11:11:11) has been detected based on its IP address.			Default
4	#42613	2023-09-25 15:48:10	DNSANOMALY	TCPHighTraffic	10.100.16.21	A high amount of TCP DNS traffic transferred, data sent: 12.62 KiB, data received: 962.72 KiB.	172.16.3.248 192.168.0.173		Default
5	#42608	2023-09-25 15:43:01	ANOMALY	SentPackets	10.100.28.43	The following number of packets: 2681894 has been sent in the network (that is 177.998% more than the predicted 964714 packets). Packets sent by the device: 1655868.	10.100.28.41 10.100.28.44 10.100.52.22		Default
6	#42611	2023-09-25 15:43:01	ANOMALY	ReceivedBytes	10.100.52.22	The following amount of data: 5.98 GiB has been received in the network (that is 582.755% more than the predicted 896.77 MiB). Data received by the device: 5.09 GiB.	10.10.9.5 10.100.2.9 10.100.28.41 10.100.28.43 ... more	2x CloudFlare (CDN) 1x Vodafone (ISP/Telco) 1x Time Synchronization (Technology)	Default
7	#42610	2023-09-25 15:43:01	ANOMALY	SentBytes	10.100.28.43	The following amount of data: 2.99 GiB has been sent in the network (that is 305.02% more than the predicted 755.68 MiB). Data sent by the device: 2.31 GiB.	10.100.28.41 10.100.28.44 10.100.52.22		Default
8	#42609	2023-09-25 15:43:01	ANOMALY	ReceivedPackets	10.100.52.22	The following number of packets: 4745679 has been received in the network (that is 350.766% more than the predicted 1052803 packets). Packets received by the device: 3646188.	10.10.9.5 10.100.2.9 10.100.28.41 10.100.28.43 ... more	2x CloudFlare (CDN) 1x Vodafone (ISP/Telco) 1x Time Synchronization (Technology)	Default

アクティベート方法：

1. Anomaly Detection System にアクセスします。
2. イベントにアクセスします。
3. テーブルの列をカスタマイズするアイコンをクリックします。⇒
4. アプリケーションチェックボックスを選択します。

7. 処理不能フローに関する通知

ライセンスの処理性能を超えて処理されなかったフローは、解析概要だけでなく、解析ページのフローチャートにも表示されるようになりました。



アクティベート方法：

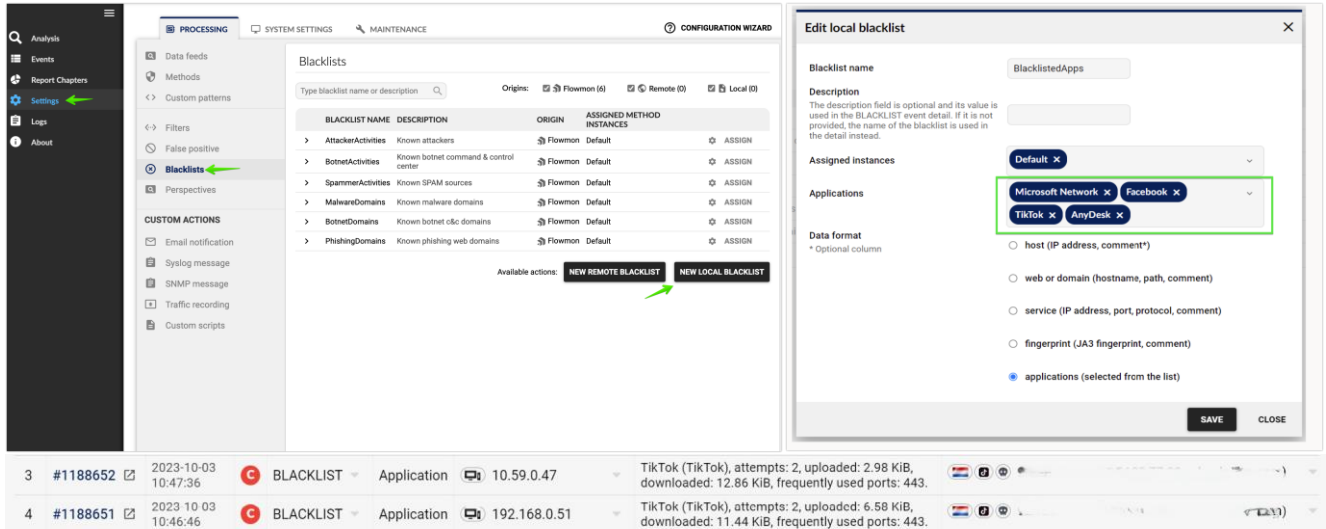
1. この機能はすべてのユーザーに対して有効です。ライセンス制限を超えると、解析ページの概要にこの行が表示されます。

8. アプリケーション・ブラックリスト

新しいアプリケーション・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ます。

AnyDesk（リモートアクセスアプリケーション）、DropBox（ファイル共有）、TikTok（ソーシャルネットワーク）など、1,500 のアプリケーションと 30 のカテゴリのリストから、アプリケーションとの通信を簡単にアラートできます。

注：アプリケーション・ブラックリストは、有効なサポートをご利用のお客様にご利用いただけます。



The screenshot shows the Flowmon interface with the 'Blacklists' section selected in the left sidebar. The main panel displays a table of existing blacklists and two buttons: 'NEW REMOTE BLACKLIST' and 'NEW LOCAL BLACKLIST'. The 'NEW LOCAL BLACKLIST' button is highlighted with a green arrow. An 'Edit local blacklist' dialog box is open on the right, showing the configuration for a new blacklist named 'BlacklistedApps'. The 'Applications' section in the dialog is highlighted with a green box, showing selected applications: 'Microsoft Network', 'Facebook', 'TikTok', and 'AnyDesk'.

BLACKLIST NAME	DESCRIPTION	ORIGIN	ASSIGNED METHOD INSTANCES
AttackerActivities	Known attackers	Flowmon	Default
BotnetActivities	Known botnet command & control center	Flowmon	Default
SpammerActivities	Known SPAM sources	Flowmon	Default
MalwareDomains	Known malware domains	Flowmon	Default
BotnetDomains	Known botnet c&c domains	Flowmon	Default
PhishingDomains	Known phishing web domains	Flowmon	Default

アクティベート方法：

1. Anomaly Detection System にアクセスします。
2. 設定→ブラックリスト → 新しいローカルブラックリストを選択します。
3. アプリケーションブラックリストタイプを選択します。
4. リストからアプリケーションを指定します。
5. ブラックリストを作成後、それを BLACKLIST 検出メソッドに割り当てます。

9. DICTATTACK 検出方法の改善

Flowmon ADS の検知方法の改善は、継続的なプロセスです。今回の ADS12.2 リリースでは、様々なネットワークプロトコルを狙ったディクショナリ攻撃を検出する DICTATTACK メソッドを改善しました。この改良により、長時間接続における誤検出が減少し、HTTP や HTTPS などのサービスや、複数のネットワークポートを使用するネットワークサービスに対して、より正確な検出結果が得られるようになります。