## 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。



- 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。



3) Pi	ogress <sup>-</sup> Flowr	mon' 🗸 🛛 Dashb	oards Reports	Topologies Preset:	s		⑦ ¢ 5	John Base tenant 😦
Map \	iew MITRE	E Default	LoadMaster S	SecOps Status S	ocial Networks NetOps	s Office 365 QoS		Last 24 hours 🗸 🔞
All	Sources				Last 24 hour	rs (generic time span) 🗸 🎄	New widget	×
	100M -						Category Historical Trends Data to display	٣
L	Sep 25 14:00	16:00 18:00	20:00 22:00	Sep 26 2:00 4:	Compared to 2	10:00 12:00	Widget name	
1	Now 1 week ago	19.11 Mb/s 9.98 Mb/s	8.53 Mb/s 4.78 Mb/s	▲ +3.75 Mb/s (+78.5%)	<ul> <li>+6.18 Mb/s (+263.4%).</li> <li>+2.43 Mb/s (+103.6%).</li> </ul>	<ul> <li>→ +6.11 Mb/s (+252.2%)</li> <li>→ +2.36 Mb/s (+97.4%)</li> </ul>	Al Sources Data range	
3	2 weeks ago 3 weeks ago	7.09 Mb/s 10.19 Mb/s	2.35 Mb/s 2.42 Mb/s		•		Visualisations	•
202	3-09-25 13:44 - 2	2023-09-26 13:44						

- 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。

Progress'	SOLUTIONS • PRODUCTS • SUPPORT & S	ERVICES • RESOURCES • PARTNERS • COMPAN	Y · Q   L   C   READY TO TALK?
Progress Documentation > Flowmon All Products + Search	٩		
Products			B
Flowmon	Flowmon Anomaly Detection System (ADS)	Flowmon Application Performance Monitoring (APM)	Flowmon Packet
Flowmon DDoS Defender	Flowmon Data Retention	Additional Resources	

- 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。

Progress Flowmon' ^	Dashboa	irds Reports	Topologies	Presets	
Dashboards and Reports	>	Analysis		Simple list	
Monitoring Center	>	Events	>	By MITRE ATT&CK	
Anomaly Detection System	>	Report Chapters		By hosts	
Packet Investigator	>	Settings	>	Aggregated view	
Configuration Center	>	Logs			
		Help	>		
Return to homepage					

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)。

3 Progress' Flowmon'	Anomaly Detection System +			🌲 🖛 🖌 🚱 😁 admin (Base tenant) 👻	DProgress'F	lawmon' 🗸 🛛 Dash	vboærds Reports Topologies Pr	004CS					D 4 0	John 😝
Q. Anatosia	Date IDS data source	Source IP	Targets	Q. CHOOSE EVENTS BY ID	Security board	0							Last 24 ho	ours v 🐵
Events				-	The latest 10 m	ew events	La	st 24 hours (generic time span)	× 0.0	Top 10 IDS event	s by priority	st 24 hours (gen	eria time span)	0.0 -1
Report Chapters	METHODS IDS CATEGORIES				DNSANDMALY.	DNS traffic anomaly	Ol 101	2023-09-26		Event type	Nume	Event sour	Targets	
Settings		Showe.	PRIORITIES CATEGORIES	莊 Categories	ONSQUERY	DNS query volume anomaly	Ot 17	2023-09-26 11:14:15		Misc activity	ET USER, AdENTS Microsoft Device Metadata Retrieval Client User-Agent	<b>DI</b> 91- 18	<b>1 36</b> at 111	***
E Logs				Type category name to fitter Q	ALIENDEV	New or alien device	<b>Di</b> 7	2023-09-26		Misc activity	ET USER_AGENTS Microsoft Device	Q6		
<ul> <li>About</li> </ul>				Potential Corporate Prixe	ICMPWNOM	ICMP anomaly		2023-09-26 11:11:27	***		User-Agent ET USER, AGENTS			
				Generic Protocol Command	ALIENDEV	New or allen device	<b>OI</b> 11	2023-09-26		Misc activity	Microsoft Device Metadata Retrieval Client	Q 7	Be 0	-45 -11
	196 -		A	0 () Misc activity	ONSQUERY	DNS query volume anomaly	Q	2023-09-26 11.04.01		-	ET USER_AGENTS Microsoft Device	-		
			Λ	© 💽 Not Suspicious Traffic 🛛 🌑	ANOMALY	Behavior anomaly		11.03.00		Misc activity	Metadata Retrieval Client User-Agent	Q1 4	-	1994 (11)
	0 5eg 21 00 10 5eg 21 00.00 5eg 22 00	00 beg 23-00-00 5ep 24	30.00 544 25-00.00 Kep 24-00:00	O Undefined	ANOMALY	Behavior anomaly	Ct .1	11.03.00		Misc activity	ET USER, AGENTS Microsoft Device Metadata Retrieval Client	<b>9</b> 1 16	i 🖬	
		10 11 15 - 2022 20 26 11 16		werd events over 202	DNSANDMALY. 2023-09-25 11:1	DNS traffic anomaly 6 - 2023-09-26 11.16	OI - 100-425 OI 11-4018	2023-09-26 11.03:00		Misc activity	ET USER_AGENTS Microsoft Device Metadata Retrieval Client	Q 2** 4		
	Origination Protection	0	]	2 1	Top 10 IDS even	nt types by priority and c	ount La	at 24 hours (generic time span)	~ Q Ø	Misc activity	User-Agent ET USER_AGENTS Microsoft Device Metadata Retrieval Client	Q1 *	-	
	> (w) Attempted Information Leak	.0		4 个						O Mer article	ET USER AGENTS Microsoft Device	B1- 4		-
	> () Generic Protocol Command Decode	13	Λ	181 个						6 mic story	Metadata Retrieval Chent User-Agent			
	> 🕦 Misc activity	0		123 🔨						Misc activity	ET USERCAGENTS Microsoft Device Metadata Retrieval Client	Q	·	- 16
	> () Not Suspicious Traffic	11		~~~~ 60 A	Event type			Hambe	r of events	-	ET USER AGENTS Microsoft Device		1.1	
	> (c) Undefined	0	٨	3 个	Minc a	ctivity			17	e wise activity	Metadata Retrieval Client User-Agent			1000 111

#### 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) でも詳細をご覧いただくことができます。

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、サポートボ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。



- 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



- 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。





ລາ	Progress Flowmon 2	> Anomaly Detecti	on System 👻			
		Date	Perspective	IP addresses		
Q,	Analysis	Last 24 hours 🐱	Security issues 🗸		APPLY MORE FILTERS	
		SIMPLE LIST	BY MITRE ATT&CK	BY HOSTS	AGGREGATED VIEW	
۲	Report Chapters					
۵	Settings	> 🕢 64 📼	10.100.28.40 fam Int	۹)	As source:      43     43	As target: 93
Ê	Logs	> @ 61 📼	192.168.3.176 (	)	🗏 As source: 37	♦ As target: 31
0	About	> ③ 60 📼	10.100.28.41 @··		🚍 As source: 12	♦ As target: 22
		> @ 60 📮	10.100.16.21 (u )		As source: 47	As target: 72
		> 🕕 51 📮	10.100.32.28 (P°		As source: 2	As target: 2
		> 🕕 51 📼	10.100.32.26 (13 •		📱 As source: 🛛 2	♦ As target: 2
		> 🛈 46 🖵	10.100.32.142 ( 🕫		📱 As source: 🚺	♦ As target: 1
		> 🕕 42 📼	10.100.58.22 (s		🗏 As source: 🚺	♦ As target: 3
		> 🕕 42 📮	t) 10.100.58.21 ( 👘		📱 As source: 🙎	♦ As target: 5
		> 🕕 42 📮	t) 10.100.33.140 (ulat - 1)		📱 As source: 🙎	♦ As target: 1

#### 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。

110	Per	perfre	Swarts #	Turgette					O DEDOK EVEN	187-0							
late 24	Anyo w	inantifed-	3		APPERT MORE FAILURE												
	uur I	PMIRATICS	e mens	AUGREGATED VEM													
			-														
	82 28	AL PACTORN AN	ENTITIE 8	NUMBER	SCARCE	8796	Tweet's	APPLICATIONS	DASAFEE	ALL IP ADDRESSES BY COUNTRY	BY IP	BY APPLICATION					
	44040 U 15	10.00 MA	anece .	Theest	Shi 1834644 (42.C.)	A new device fills, address to the line base detected based at his 5° address.			<b>Intent</b>				-	-			
1	A0340 11 15	2000 AU	and a	Phasel	Oc 183465164(L)	A new decore (blic), addresse (bl.m			brut								
	*104 H 11	NU AI	abetr 1	Planet	RE 18246-62941.3	A new device blief, address, Vo			belock.	E ? Unknown (9)							
	4000 H 10	000 DN	GINEMAD 1	Distants	69 10 10 10 14 21	A high amount of TOP DEB traffic transferred, doils uncl. 13 42 408. data mentioned 1422 72 828.	66 103163248 Ge 100366510		Detail	(CR) 10.30.200.100 (CR) 10.1	00.16.21	10.100.16.22		<b>1</b>		154.40.100.170	<b>R</b> 172.16.2.2
,	***** = 11	000 M			55 11 10 18 O Line .	The following conduct of packate: 2001 BMH that have based in the restricted (AMA in 1717 BBE), where then the predicated field? A packate; Packates permitty the devices 114/58/88	64 16 10 20 20 10 10 10 16 16 20 20 20 26 16 16 20 20		trial	QL 172.16.3.248 QL 172.	) 16.4.209	(Unknown)		(unknown)		(unknown)	(unknown)
	-en : 7			konstillere	Be 18 10 19 20	The following arrests of data. UNI SNI has been resident in the methods (2014) in SNI 2020, many that the predenal EUC 77 MAE, fee	64 10 1014 65 10 1024 66 10 10224	3a = Clauff fan (228) Leigi indeline (427) Leili fan Spolonaume (Nedrong	et sent	(unknown) (unknown	)	<ul> <li>(unknown)</li> </ul>	Υ				
						incomed by the device, VIN UR.	65 10 100 38 O (ale-see			P R Facebook Network Applance (FNA) (3)	(hade not) -			Deale part	-		(anahanik anan)
7	PERSON IN THE	10 10 AM	decr 1	and gen	6 11 10 14 0 10	Plantition of particular of data 2 are only been been as in the behavior (basis a 208-2015 more than the predicted T58 kill bill). Data setting the denice 2 31 GB.	65 10 10 10 44 (p =		behad.		food files			.noconcrony -			accounty -
•	eens a 20	0.003 NT	aau (	konstfadet	6e ni 101 52.27	The bilineary random of packets of VAR N has been reserved in the second (Static IIII) TAA structure the problem (VARIE) packets Radials assessibly the doctor 2010/2011	No. 10:003         Solution         1           Solution         1         Solution         1           Solution         1         Solution         1           Solution         1         Solution         1	34 - Charline (200) 14 Orabitre (201) Seco 14 B Tree Spectromation (Indensing	er wur	(unknown) -	<b>1</b>	(unknown) -					
	eares 11 11	2004 A	-	-	Di taminini	Burnituded artische besch Autoriset. Their artische weis successivel. Gammel kan preis 1. sattempter 4. sattemie 123-15 Kill, maanmel aptimal- 542 Kill, folde kangete 1. sittempter 16, optimal 36.28 Kill, maanmel sattemie 1564 Kill.	61 10 10 20 4 Dates ov 61771		beaut.	C Scogle Cloud Platform (2)							
- 10	****** 11 25	2010-25 AU	iner/	Phanet	NR (834652951.)	A new desire Mild' address in			brief		onen.com) •			contention()			
	***** 1. 10	100 A	aneor .	Thereil	SS TEDRATOR(.)	A new device band address 21277777 (\$ 522) has loss detailed have detailed			Mad.	P & Groate (2)							
tr.	ACTIN 11 77	NA DIG N	aners a	Theast	45 10308-6648(L)	A new denias PERC address, PD			brief.								
18	***** T	A1	mari d	Theorem	Dr 10100 (441.)	A new device \$550 address Con- Ind \$1 has been detected			bred .	🍽 G		<b>M</b> 6	625 av 110.1	.net) -			
- 18	Permit 71	565 B	HET 1	ana y	NR 15.549.67.599	Distributed article has lower detected. This attack was successful fouriest torpate. 5. secondst 2, uplicat: 19.14. Will maximal optical 9.97 MIX and storpets 1, advergets 13, uplicad 41.09.000 insecond uplicad 511.58.	0 300348-2		Nut								
15	**210 U 15	AL AL	Deci i	Preset	Ge 1834634/682.3	A new device [Min] address [((arrow of [*)(4)) has been conscised based on by \$* address			belast.								
16	retor 1 13	2010 100	ormest o	lene y	Re 10.9928-0	Tanatamat 2.51-58, sp pear transfer 2.51-58	Dr 16 10 12 21		brint .								
4					125 (1996) (1997) (1997)		BR 10 100 28 41 64										



Image: state of the state		near the						78
Image: state stat		EVENTS #				Show:	PRIORITIES METHODS	Type method name to filter
Image: state stat		3						
								O () HIGHTRANSF
Image: state stat								
Image: market with a state		1						
Image: 14.1       Option: 1000       Option: 10000       Option: 1000       Option: 10000       Option: 10000       <		0	21.00 5ep.	n ao	DR-DD	08:00 12:00	13.00	
Image: Control of Contro	0	EVENTS BY PRIORITY	023-09-24 15-57 - 2023-09-25 15-58					verall events count: 6
Image: Distribution of the second of the	-	M ANOMALY						/ 4 *
				4 events of the	he type ANOMALY from 1 source IP addresses d	detected		
		SOURCE IP ADDRESS	SOURCE IP FILTERS	EVENTS COUNT				
Image: Second		✓ □ 10.100.52.22						2 RELATED EVE
Intermine to the second of th				Detected	4 events of the type ANOMALY from 10.100.5	52.22		
Image: 1 mode				Night	ttime			
Image: All of the second of		1/20 10.00	25.00	00.00	0100		10.00	
Image: 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1 - 1		2023-09-24	2000 2200	2023-09-25	04:00		1000 1200	14:00
Image: Section 1       Source P ACTING       Source P ACTING <td< td=""><td></td><td>ID DETECTION LAST TIME UPDATE</td><td>DETAIL</td><td>TARGETS</td><td></td><td>APPLICATIONS</td><td>DATA FEED METHOD INSTANCE</td><td>COMMENTS</td></td<>		ID DETECTION LAST TIME UPDATE	DETAIL	TARGETS		APPLICATIONS	DATA FEED METHOD INSTANCE	COMMENTS
<ul> <li></li></ul>		#42609 E 2023-09-25 2023-09-2 15:43:01 15:43:01	The following number of packets: 4745679 has be network (that is 350.766% more than the predicte Packets received by the device: 3646188.	en received in the 11052803 packets). (Di 10.10.9.5 (Di 10.100.2.9 more		2x = CloudFlare (CDN) 1x O Vodafone (ISP/Telco) 1x Time Synchronization (Technology)	Default Default	
		#42611 2023-09-25 2023-09-2 15:43:01 15:43:01	The following amount of data: 5.98 GiB has been (that is 582.755% more than the predicted 896.77 the device: 5.09 GiB.	eceived in the network (CR) 10.10.9.5 MiB). Data received by (CR) 10.100.2.9 more		2x - CloudFlare (CDN) 1x O Vodafone (ISP/Telco) 1x S Time Synchronization (Technology)	Default Default	
1       2000 1		#37065 [2] 2023-09-25 2023-09-3 06:08:00 06:08:00	The following number of packets: 2324096 has be network (that is 245.573% more than the predicte Packets received by the device: 1655387.	en received in the 📴 10.100.2.9 1672533 packets). 🔤 10.100.28.41 (j. more	- 6)	2x + CloudFlare (CDN) 1x O Vodafone (ISP/Telco) 1x Time Synchronization (Technology)	Default Default	
Normal Reside		#37067 [2 2023-09-25 2023-09-2 06-08:00 06-08:00	The following amount of data: 2.74 GiB has been (that is 453.851% more than the predicted 505.84	eceived in the network (R) 10.100.2.9 MiB). Data received by (R) 10.100.28.41 (P)	-) -	2x - CloudFlare (CDN) 1x O Vodafone (ISP/Telco)	Default Default	
Rule       Rule       Rule       Rule       Rule         INTS BY FIGURY       20       2023-09-24 15.45       Overall events on the type SSHDCT from 25 source P adventees detected       0       <			the device: 2.31 Gib.	more		1x Time Synchronization (Technology)		
International and a state of the state		Showing 1 - 4 of 4						
SOURCE P ALOR RES 500 CE P ALOR RES 500 CE P ALOR RES 100 CE P ALO	SRVNA	華 2023-09-24 15:44 - 2023-0	9-25 15:45				Overall	l events count: 1003
SOURCE IP ATURES       SOURCE IP ATURES       Destrict Output         Die 10.99 224       Centre of the type SSHDDCT from 10.972.82.4       Centre of the type SSHDDCT from 10.972.82.4       Centre of the type SSHDDCT from 10.972.82.4         10.90       2000       2000       2000       0000       0000       1000       2000       Applications         10.90       EFTECTION       MART       DETAL       TARGETS       APPLICATIONS       DATA FEED       METHOD INSTANCE       COMMENTS         10.90       15.90.00       200.90       200.90       200.90       0.000       0.600       0.600       1000       2000       Comments         10.90       EFTECTION       MART       DETAL       TARGETS       APPLICATIONS       DATA FEED       METHOD INSTANCE       COMMENTS         10.90       15.90.00       200.90       200.90       0.90       10.100.28.40 (x, n = n)       Default	y			66 events of the type SSHDIC	T from 25 source IP addresses detected			
Dick 1.09 224     CERTION 109 2284       Description       Description       100 0 2000 0000 0000 0000 0000 0000 000		SOURCE IP FILTE	RS EVEN	IS COUNT				
Definition 10928284         Support of the type SSHDET from 10928284         Internation 1000000000000000000000000000000000000	SOURCE IP ADDRESS							2 RELATED EVEN
Neghttime       Control table columns         16:00       20:00       20:00       20:00       00:00       00:00       00:00       06:00       06:00       10:00       2:00       2:00       2:00       0:00	SOURCE IP ADDRESS							
Neptime         Second Sec	SOURCE IP ADDRESS			Detected 2 events of the	type SSHDICT from 10.99.28.24			
16:00 2023-07-37     18:00     20:00     20:00     00:00     02:00     04:00     06:00     08:00     10:00     12:00     If defined instance in commentations in commentations       10     DETECTION IVEGAT     DETAL     TARGETS     TARGETS     TARGETS     APPLICATIONS     DATA FEED     METHOD INSTANCE     COMMENTS       422591     02:00-02     20:00-02     Commentations     Sciencessific     Sciencessific     Sciencessific     Sciencessific     Commentations       42591     02:00-02     20:00-02     Commentations     Sciencessific	SOURCE IP ADDRESS			Detected 2 events of the	: type SSHDICT from 10.99.28.24		~	Customize table columns
D         DETERTION         LAT         DEFL         TARGETS         TARGETS         APPLICATIONS         DATA FEED         METHOD INSTANCE         COMMENTS           #4258 0         2023-0925	SOURCE IP ADDRESS			Detected 2 events of the Nighttime	type SSHDICT from 10.99.28.24		<u> </u>	Customize table columns
ID         TIME         DEFAUL         DEFAUL         TARGETS         APPLICATIONS         DATAFEED         MEHOD INSTANCE         COMMENTS           #42598         2023.09.25	SOURCE IP ADDRESS ©1 10.99.28.24 16:00 2023-09-24	18.00 20.0	0 22:00	Detacted 2 events of the Nighttime 0:00 02:00 023-09-25	type SSHDICT from 10.99.28.24 04.00 06.00	08.00	10:00 12:00	Customize table columns Applications Method instance Comments
#42598       2023-09-75	SOURCE IP ADDRESS (B) 10.99.28.24 16:00 2023-09-24 DETECTM	18:00 20:0	0 22:00	Detacted 2 events of the Nighttime 0.00 02:00 923-09-25	e type SSHDICT from <b>10.99.28.24</b> 04.00 06.00	08:00	10.00 12.00	Customize table columns Customize table columns Applications Method instance Comments Comments Categories
#1301         2023-09-25         2023-09-25         2023-09-25         2023-09-25         2023-09-25         Control target stark, has been detected. This attack was successful.         Option         Default         Default         Default           #1301         2228-06         140612         2         Stream of targets 2, attempts 33, upload 180.82 Kill, maximal upload.         Option 1010028.40 (fg+i-b-A         seet)         Default         Default         Default           Stream of 1.2 of 2         53 KB         Stream of targets 2, attempts 33, upload 180.82 Kill, maximal upload.         Option 1010028.131         Default         Default	SOURCE IP ADDRESS D(10.99.28.24 16.00 2023-09-24 ID DETECTING	18:00 20:0 ION LAST UPDATE DETAIL	0 22:00	Detected 2 events of the Nighttime 0.00 02:00 02:00 TARGETS	a type 55HDICT from <b>10.99.28.24</b> 04.60 06:00	08:00 STATE	10.00 12.00 D METHOD INSTANCE C	Customize table columns Customize table columns Customize table columns Customize table columns Comments Categories COMMENTS
9.53 Kdl.	SOURCE IP ADDRESS D) 10.99.28.24 16.00 2023-09-24 ID DETECTION #42598 [2] 2023-09-1 15.42.00	18:00         20:0           ION         LAST         DETAIL           UPDATE         Detable datack         Corrent targets: 1, KB; total targr	0 2200 2200 2200 2200 2200 2200 2200 2	Detected 2 events of the Nighttime 0000 02200 02200-25 TARGETS 6 (SR) 10.100.28.40 (4, ) a)	t type 55HDICT from <b>10.99.28.24</b> 04:00 06:00	06.00 State APPLICATIONS DATA FEE Default	10.00 12.00 ID METHOD INSTANCE C Default	Customize table columns Applications Method instance Comments Categories COMMENTS
	SOURCE IP ADDRESS GI 12.99.28.24 16.00 2023-09-24 ID DETECTION #42598 12 2023-09-24 15.42.00 441301 12 2023-09-1 12.226.66	18:00         20:0           ION         LAST UPDATE         DETAIL           25         20:0:9-75 15:5:00         Commot targets 1, Keil           25         20:0:9-75 15:6:00         Commot targets 1, Keil           25         20:0:9-25 20:0:9-25         Commot targets 1, Keil, Instrument	0 22:00 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	Detected 2 events of the Nighttime 0.00 023-09-25 TARGETS (6) 53: 10.100.28.40 (s	Hype 55HDICT from 10.99.28.24	08:00 APPLICATIONS DATA FEI	10.00 12.00 ID METHOD INSTANCE C Default Default	Customize table columns  Applications  Applications  Comments  Categories  COMMENTS
	SOURCE IP ADDRESS Gi 10.99.28.24 16.00 2023-09-24 ID DETECTM 184200 #41301 [2] 2023-09-3 184200 #41301 [2] 2023-09-3 184200 841301 [2] 2023-09-3 184200 184000 184000 18400 18400 18400 184000 18400 18400 184	18.00         20.0           ION         LAST UPDATE         DETAIL           25         2023-09-25 15 4:200         Distributed attack Current targets 1, activatiat attack is local based attack           25         2023-09-25 14:06:122         Distributed attack RE ford largets: 9.53 KB.	0 2200 2 has been detected. This attack was successful attempts & update 22.24 KB, maximal update 5.6 , attempts & guidade 22.24 KB, maximal update 4.6 attempts & update 27.24 KB, maximal update 4.6 attempts & update 27.24 KB, maximal update 4.6 attempts & update 27.24 KB, maximal update 4.6 attempts & Update 190.82 KB, maximal update 4.6 attempts & 33, update 190.82 KB, maximal update 4.6 attempts & 34, update 190.82 KB, update 190.8	Detected 2 events of the Nighttime 1023-09-25 7ARGET5 6 (B): 10.100.28.40 (s. , u) 100: 10.100.28.40 (s. , u) 100: 10.100.28.40 (s. , u)	t type 55HDICT from <b>10.99.28.24</b> 04.00 06:00	OBSO STATE	1000 1200 ED METHOD INSTANCE C Default Default	Customize table columns Applications Method Instance Comments Categories COMMENTS

 

 1
 #2068
 2
 2023-08-02 131:4:02
 G
 UPLOAD
 General
 General
 Image: China Telecom IDC (Hosting)
 Uploaded: 13.26 MiB, downloaded: 1.55 MiB, port(s): 443.
 Image: China Telecom IDC (Hosting)
 Default

 2
 #983
 2
 2023-08-02 12:53:38
 G
 BLACKLIST
 Host
 Image: China Telecom IDC (Hosting)
 Known attackers, attempts: 1, uploaded: 44 B, downloaded:
 Image: China Telecom IDC (Hosting)
 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。



:

ລາ	Progress <sup>-</sup> Flowmon <sup>*</sup>	> Anomaly Dete	ction System 👻				🌲 en 👻	🙆 \varTheta adm	in (Base tenan
۹	<b>⊟</b> Analysis	Date	Perspective	Source IP	Targets	APPLY	MORE FILTERS	୍ <b>CHOO</b>	SE EVENTS BY
	Events Report Chapters	SIMPLE LIST	BY MITRE ATT&CK	BY HOSTS	AGGREGATED VIEW	_			
\$	Settings	🛓 EXPORT EV	ENTS TO A CSV FILE	OPEN IN A NEW	TAB				
Ê	Logs		DETAIL		TARGETS		APPLICATIONS		DATA FEED
	ADOUT		A new device (MAC address: or has been detected based on its	IP address.				Customize table	columns
			A new device (MAC address: 0) has been detected based on its A new device (MAC address: av	۹۵) IP address. ههه)				Detection time Last update	
			has been detected based on its A high amount of TCP DNS traff data sent: 12.62 KiB, data receiv	IP address. ic transferred, /ed: 962.72 KiB.	<ul> <li>172.16.3.248</li> <li>192.168.0.173</li> </ul>	ст. Т		<ul> <li>Event subtype</li> <li>MITRE ATT&amp;CH</li> </ul>	( tactic
		ion.com) –	The following number of packet been sent in the network (that is than the predicted 964714 pack sent by the device: 1655868.	s: 2681894 has 177.998% more tets). Packets	<ul> <li>10.100.28.41 (j)</li> <li>10.100.28.44 (2)</li> <li>10.100.52.22</li> </ul>	i)		Applications	( techniques
		~	The following amount of data: 5 been received in the network (th more than the predicted 896.77 received by the device: 5.09 GiB	5.98 GiB has hat is 582.755% MiB). Data	<ul> <li>□ 10.10.9.5</li> <li>□ 10.100.2.9</li> <li>□ 10.100.28.41 (i*a</li> <li>□ 10.100.28.43 (%b · , more</li> </ul>	• • •	2x - CloudFlare (CD 1x O Vodafone (ISP/ 1x Time Synchron	<ul> <li>Method instand</li> <li>Comments</li> <li>Categories</li> </ul>	ce
		ion.com) –	The following amount of data: 2 been sent in the network (that is than the predicted 755.68 MiB). device: 2.31 GiB.	2.99 GiB has 305.02% more Data sent by the	10.100.28.41 (bzen	n)			Default
			The following number of packet been received in the network (th more than the predicted 105280 Packets received by the device:	s: 4745679 has hat is 350.766% 33 packets). 3646188.	I0.10.9.5         I0.100.2.9         I0.100.28.41 (%).         I0.100.28.43 (rm	୍ ) କ ଜଣ) କ	2x CloudFlare (CDI 1x O Vodafone (ISP/ 1x Time Synchroni	N) Telco) ization (Technology)	Default

	ID	DETECTION TIME	EVENT TYPE	EVENT SUBTYPE	SOURCE		DETAIL	TARGETS	APPLICATIONS	DATA FEED	<b></b> -
1	#42651 🖾	2023-09-25 15:49:50	ALIENDEV	IPBased	( <b>Di</b> ) 10.248.69.182 ()		A new device (MAC address: 5. g has been detected based on its IP address.			Default	:
2	#42649 🖸	2023-09-25 15:49:22	ALIENDEV	IPBased	(Dt) 10.248.6.164 ()		A new device (MAC address: 12: 3) has been detected based on its IP address.			Default	1
3	#42646 🖾	2023-09-25 15:48:52	ALIENDEV	IPBased	(Dt 10.248.4.214 ()		A new device (MAC address: % 'a) has been detected based on its IP address.			Default	÷
4	#42613 🖾	2023-09-25 15:43:10	DNSANOMALY	TCPHighTraffic	( <b>Gi</b> ) 10.100.16.21		A high amount of TCP DNS traffic transferred, data sent: 12.62 KiB, data received: 962.72 KiB.	©1 172.16.3.248 ©1 192.168.0.173		Default	÷
5	#42608 🖾	2023-09-25 15:43:01	ANOMALY	SentPackets	<b>G</b> 10.100.28.43	۰.	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.	©i         10.100.28.41 (i/i)         1           ©i         10.100.28.44 (i/i)         8           ©i         10.100.52.22         8		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 MB). Data received by the device: 5.09 GiB.	Di 10.10.9.5           Di 10.100.2.9           Di 10.100.28.41 }           Di 10.100.28.43 \$P (r)	2x CloudFlare (CDN) 1x O Vodafone (ISP/Telco) 1x Time Synchronization (Technology	Default	:
7	#42610 🖾	2023-09-25 15:43:01	ANOMALY	SentBytes	🕞i 10.100.28.43 (n r		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 tr         tr         tr         tr           ⊕:         10.100.28.44 e+         sl1)         sl1)           ⊕:         10.100.52.22         sl1)		Default	:
8	#42609 2	2023-09-25 15:43:01	ANOMALY	ReceivedPackets	Q 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.	©i         10.10.9.5           ©i         10.100.2.9           ©i         10.100.28.41 (jn           ©i         10.100.28.43 (ra:          more        )	2x CloudFlare (CDN) 1x O Vodafone (ISP/Telco) 1x Time Synchronization (Technology	Default	1
							Right had attack has been detected. This attack one accessed if				

- 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。

Flows/s	In average 29.6% flows/s were not processed due to license limit. Average flows per second not processed: 84 flows/s	0
Events	📮 10.100.16.21 👻 has highest number of detected events 141	0
Threat Score	📮 10.100.28.41 (2) 🕫 👘 👘 👘 👘 has the highest Threat Score 😗 46 - See the list of hosts sorted by Threat Score	0
✓ FLOWS		Flow processing status
00 -1		

アクティベート方法:

1. この機能はすべてのユーザに対して有効です。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。



## **Progress** Flowmon

## 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。

B PROCESSING SYSTEM SETTINGS A MAINTENANCE ⑦ CONFIGURATION WIZARD Edit local blacklist Data feeds Blacklists Blacklist name BlacklistedApps Methods Origins: 🖾 🗊 Flowmon (6) 🖾 🕲 Remote (0) 🖾 🖺 Local (0) Type blacklist name or description Q Description <> Custom patterns e description field is optional and its value is ed in the BLACKLIST event detail. If it is not wided, the name of the blacklist is used in ORIGIN ASSIGNED METHOD INSTANCES BLACKLIST NAME DESCRIPTION 🖻 Logs ♦ Filters provid AttackerActivities Known attackers 3 Flowmon Default ASSIGN S False positiv BotnetActivities Known botnet com > St Flowmon Default ASSIGN Assigned instances Blacklists + > SpammerActivities Known SPAM sources A Flowmon Default ASSIGN Perspectives rk 🗙 Fac Applications > Mahwa eDomains Known malware domains 3 Flowmon Default ASSIGN CUSTOM ACTIONS ok 🗙 🛛 Any sk x Known botnet c&c do ¢ ASSIGN omains Known phishing web domain Data format 🖻 Email no 3 Flowmon Default host (IP address, comment\*) Syslog message INSE NEW REMOTE BLACKLIST NEW LOCAL BLACKLIST web or domain (hostname, path, comment) SNMP me Traffic recordi service (IP address, port, protocol, comment) Custom scr fingerprint (JA3 fingerprint, comment) applications (selected from the list) SAVE CLOSE 3 **#1188652** Z 2023-10-03 10:47:36 TikTok (TikTok), attempts: 2, uploaded: 2.98 KiB, downloaded: 12.86 KiB, frequently used ports: 443. - . G BLACKLIST - Application 💷 10.59.0.47 4 #1188651 2 2023 10 03 10:46:46 TikTok (TikTok), attempts: 2, uploaded: 6.58 KiB, downloaded: 11.44 KiB, frequently used ports: 443. G BLACKLIST Application 🗩 192.168.0.51 20. (123)

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。

#### 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。



×

-1