Progress® Flowmon®

Flowmon ADS Specification

データシート

Flowmon ADS

Flowmon 異常検出システム (Anomaly Detection System, ADS) は、人工知能と機械学習を使用してネットワークトラフィック内の見つかりにくい異常を検知するセキュリティソリューションです。従来のセキュリティ ツールを補完し、侵害の様々な段階で脅威を検出できる多層保護システムを作成します。ファイアウォール、IDS/IPS、ウイルス対策などの従来のシグネチャやルールベースの検出アプローチは、境界とエンドポイントの保護に重点を置いています。既知の悪意あるコードや振る舞いによる初期感染の検出には効果的ですが、境界やエンドポイントを超えて保護することはできません。インサイダー脅威や未知の脅威が発生する可能性がある広大な領域が残ったままとなります。

データ侵害やデータ窃盗には、このギャップがしばしば悪用されます。インサイダー脅威は、侵害の兆候を示すわずかな異常を検知しないと発見できません。Flowmon ADS は、Flowmon Probe 上で動作する Suricata IDS と統合して、検出機能の範囲を拡張・強化し、振る舞いベースの異常とインシデントの検出に追加のコンテキストを提供できます。この仕様は、オンザフライでデータを処理する新しいストリームベースの検出エンジンに基づく Flowmon ADS バージョン 11.2 以降のバージョンに有効です。

		Lite FP-ADS-L	Standard FP-ADS-S	Business FP-ADS-B	Coporate FP-ADS-C	Enterprise FP-ADS-E	Ultimate FP-ADS-U
データ処理	**ローデータ**	NetFlow v5/v9, IPFIX, NetStream, jFlow, cflowd					
	外部情報	Flowmon Threat Intelligence (レピュテーションデータベース、侵害の指標)、whois、IP ツール、Web リンク					
	振る舞い検知	機械学習、適応ベースライン、振る舞い分析、ヒューリスティックス					
	IDS 検出	Flowmon Probe で実行される Suricata IDS との統合は組み込み済み					
イベントレポート	**レポートと警告**	メール、PDF/CSV、syslog、SNMP、パケットキャプチャトリガー、スクリプトトリガー					
	SIEM サポート	(syslog での) CEF形式の使用、SNMP トラップ					
パフォーマンス指標[1]	**ストリームデータ処理 (フロー/秒)**	100	1,000	5,000	20,000	50,000	100,000
	振る舞いパターン処理 (フロー/秒)	100	1,000	5,000	20,000	25,000	25,000
	データフィード	1	3	5	20	50	100
	必要なメモリ (GB)	4	8	16	32	64	128
	必要な CPU コア数	1	2	4	8	16	24
ユーザーインタフェース	**イベントの視覚化**	イベント分析ツリー、タイムライン、詳細、証拠、インタラクティブ					
	サードパーティー統合	IBM QRadar App, LDAP/AD, McAfee ePO					

[1] 秒あたりのフロー数は、双方向フローに集約される前の単方向フローデータに関する数値です。検出メソッドの設定が、多数のメソッドインスタンスを含み、多くのアクティブなデータフィードが割り当てられていると、パフォーマンス問題が発生する可能性があります。パフォーマンスは、Flowmon ADS に必要な量のメモリを提供できる、標準の設定 (すべての検出方法が有効、メソッドごとに1つのメソッドインスタンス、プロキシ相関が無効) でのものです。

プロキシ相関を有効にすると、パフォーマンスが示された値の50%まで低下する可能性があります。プロキシ相関の使用はストリームエンジンに限られるので、影響が出るのはストリームデータ処理のパフォーマンスだけです。必要なメモリは、Flowmon ADS が消費するメモリのみについての値です。Flowmon アプライアンスの合計メモリは、Flowmon ADS の値の2倍にすることが推奨されています。Flowmon ADS に割り当てられるメモリが不十分だと、フローデータのローリングメモリに保存される履歴情報が十分でなく、個々のイベントの詳細を分析するためのデータが不足する可能性があります。

Flowmon ADS は、メモリが不足すると、データ処理を続行するためにフローを保存する容量を動的に減らします。必要な CPU コア数は、Flowmon ADS のみに割り当てられる CPU コア数であり、ハイパースレッディングを含みます。CPU コア数を減らすと、パフォーマンスが低下する可能性があります。

総合パフォーマンスは、すべてのアクティブなデータフィードを組み合わせて処理した場合の、1秒あたりの最大フロー数を示します。ストリーム処理では、1時間のフロー/秒の平均値がしきい値を超えると、制限が適用されます。振る舞いパターン処理では、5分間のフロー/秒の平均値がしきい値を超えると、制限が適用されます。つまり、ごく短時間のしきい値を超えるフロー急増やトラフィックバーストがあっても、処理は制限を受けずに続行されます。

振る舞いパターン（BPATTERNS）処理のパフォーマンスは、この検出メソッドに割り当てられたすべてのアクティブなデータフィードで処理されるフローの1秒あたりの最大量です。パフォーマンスはデータフィード間で均等に負荷分散され、使用可能な容量内で処理される5分間のバッチの最初のフローの値です。しきい値による制限は、5分間のバッチに適用されます。BPATTERNS エンジンは、フローデータのバッチ処理に基づいています。

データフィードは、Flowmon Collector からフローデータを受け取ります。データフィードは、異なるネットワークセグメント（LAN、DMZ など）または異なる組織 (テナント) からのデータを論理的に分離します。1つのデータフィードに対して、各検出メソッドの複数のインスタンスを定義できます。各データフィードとメソッドインスタンスの内部コンテキストと分類子が計算され、分離された状態で保持されます。

Flowmon Threat Intelligence は、プレミアムのクラウドベースのサービスです。このサービスは、レピュテーションデータ、最近の攻撃者・感染したホスト・ボットネットコマンドなどの侵害の兆候、そしてコントロールセンターを提供します。この情報は、BLACKLIST メソッドによる疑わしいネットワーク通信の検出の基礎データとして使用されます。Flowmon Threat Intelligence は、振る舞い分析の原則を使用して既知の脅威やゼロデイ攻撃を検出するための振る舞いパターンも更新します。

.

プログレスについて

プログレス（Nasdaq：PRGS）は、テクノロジーが牽引する世界において専心的にビジネスを推進し、多くの企業がイノベーションのサイクルを加速し、躍進して業績を向上させていくプロセスを支援します。プログレスは信頼できるプロバイダーとして、インパクトが大きいアプリケーションを開発、展開、管理するための最高の製品を提供し、お客様は必要なアプリケーションとエクスペリエンスを開発し、適切な手法で展開し、すべてを安全かつ確実に管理することが可能になります。1,700のソフトウェア会社と350万の開発者を含め何十万もの企業が目標達成のために確信を持ってプログレス製品を利用しています。詳細については www.progress.com をご覧ください。また、LinkedIn、YouTube、Twitter、Facebook、Instagram へのフォローをお願いいたします。

プログレス・ソフトウェア・ジャパン株式会社
〒106-0047
東京都港区南麻布4-11-22 南麻布T&F ビル
www.flowmon.com/jp
sales_japan@progress.com

Progress