kaspersky bring on the future

Kaspersky
Threat Intelligence

Kaspersky Threat Data Feeds

概要

フィードに含まれる情報

Kasperskyが提供するフィードのエントリには、脅威をすぐに確認し優先順位付けできるコンテキストデータが含まれています。

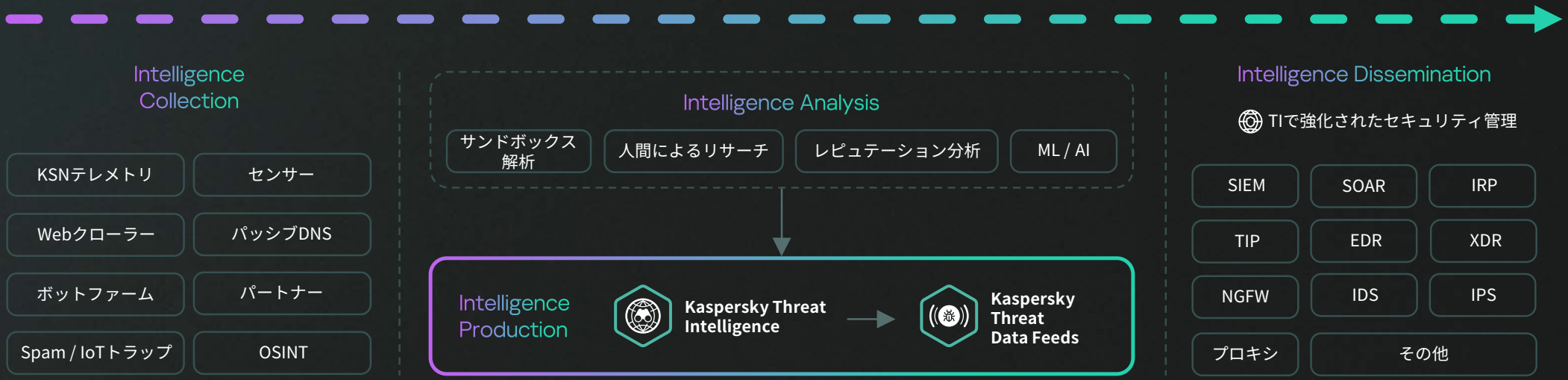
- 脅威の名称
- 悪意のあるWebリソースの確立されたIPアドレスとドメイン名
- 悪意のあるファイルのハッシュ
- 脆弱性のあるオブジェクトと侵害されたオブジェクトの識別子
- MITRE ATT&CK分類による攻撃の戦術、テクニック、手順
- タイムスタンプ
- 地理的位置
- 普及度など。

Kaspersky Threat Data Feedサービスは、リアルタイムの脅威インテリジェンス情報を提供することで、産業組織のネットワークやシステムをサイバー脅威から保護します。データフィードには既知のマルウェア、フィッシングサイト、最新の脆弱性やエクスプロイト、その他のサイバー脅威に関する情報が含まれています。組織はこの情報を利用して、悪意のあるトラフィックのブロック、セキュリティソフトウェアのアップデートなど、サイバー攻撃から身を守るための対策を講じることができます。

データは、Kaspersky Security Network、当社のクローラー、ボットネット脅威監視サービス（24時間365日体制で、標的のボットネットとその活動を監視）、スパムトラップ、リサーチャーやパートナーからのデータなど、信頼性の高い各種の情報源から収集されます。

収集された情報はすべて、サンドボックス、統計的分析とヒューリスティック分析、類似サンプル検索ツール、ふるまいプロファイリング、エキスパートによる分析など、各種の事前処理方法を使用してリアルタイムで慎重にチェックされ、参照可能な状態に整理されます。

データフィードは、イベントに関する一般的な情報を収集し、詳細を掘り下げるのに役立ちます。また、「攻撃者が誰で、どんな攻撃を、どんな場所から、どんな理由で行っているのか」という点とその攻撃の発生源を特定することで、短時間での意思決定を可能にし、どんな複雑な脅威からでも企業を守ります。



データフィードの使用方法

フィード名	予防	検知	調査
悪意のあるURLデータフィード	•	•	•
ランサムウェアURLデータフィード	•	•	•
フィッシングURLデータフィード	•	•	•
ボットネットC&C URLデータフィード	•	•	•
モバイルボットネットC&C URLデータフィード	•	•	•
悪意のあるハッシュデータフィード	•	•	•
モバイルデバイスを標的とする悪意のあるハッシュデータフィード	•	•	•
IPレピュテーションデータフィード	•	•	•
フィッシングURLデータフィード	•	•	•
脆弱性データフィード	•	•	•
ICS脆弱性データフィード	•	•	•
ICS脆弱性データフィード（OVAL形式）		•	
ICSハッシュデータフィード	•	•	•
pDNSデータフィード			•

フィード名	予防	検知	調査
Suricataルールデータフィード		•	
Cloud Access Security Broker（CASB）データフィード		•	
APTハッシュデータフィード		•	•
APT IPデータフィード		•	•
APT URLデータフィード		•	•
APT Yaraデータフィード		•	•
オープンソースソフトウェアの脅威データフィード	•	•	•
クライムウェアハッシュデータフィード		•	•
クライムウェアURLデータフィード			•
クライムウェアYaraデータフィード			•
Sigmaルールデータフィード	•		
ネットワークセキュリティIPデータフィード	•	•	
ネットワークセキュリティURLデータフィード	•	•	
ネットワークセキュリティWebフィルタリングデータフィード	•	•	

Kaspersky Threat Data Feedsのリストは継続的に更新され、拡大を続けています。

Kaspersky Threat Data Feedsの説明

商用フィード

商用フィードには、網羅性が最も高い情報が集積されており、サブスクリプションへの登録により使用が可能となります。情報は定期的に更新されます。フィードの種類によって、更新の頻度は数分から数時間の幅があります。リストに記載されたデータフィードに加えて、ニーズに合わせてカスタマイズしたフィードの作成も可能です。

フィード名	フィードの説明	インジケーターのタイプ	ユースケース
悪意のあるURLデータフィード	マルウェアの配信元であるWebリソース	マスク	• 情報セキュリティ管理システムは公開されており、外部の情報源によるリッチ化がその目的です。これらのストリームをSIEM / SOAR / IRPに接続することで、ユーザーは現在の脅威にタイムリーに対応し、インシデントを調査する際に追加のコンテキストを作成することができます。 • ネットワークおよびメールセキュリティシステム（たとえば、NGFW / IDS / IPS / メール / Webセキュリティ）との連携により、データフィードが提供するIOCによってネイティブのセキュリティ管理機能がリッチ化され、サイバーインシデントの防止を支援します。
ランサムウェアURLデータフィード	ランサムウェアの配信元であるWebリソース		
フィッシングURLデータフィード	フィッシングWebリソース		
ボットネットC&C URLデータフィード	ボットネットC&Cサーバーと関連する悪意のあるオブジェクト（ボット）		
モバイルボットネットC&C URLデータフィード	C&Cモバイルボットネットサーバーと関連する悪意のあるオブジェクト（ボット）		

#予防

#検知

#調査

フィード名	フィードの説明	インジケーターのタイプ	ユースケース	
悪意のあるハッシュデータフィード	典型的な悪意のあるファイルのハッシュ	ハッシュ	• インフラセキュリティシステム（エンドポイントセキュリティ、サーバーセキュリティ、メール/Webセキュリティ）との連携により、マルウェアのダウンロードや実行を防止し、既に活動中のマルウェアを検知します。 • SIEM / SOAR / IRPシステムとの連携により、ユーザーは現在の脅威に短時間で対応し、インシデントを調査する際に追加のコンテキストを作成することができます。	#予防 #検知 #調査
モバイルデバイスを標的とする悪意のあるハッシュデータフィード	モバイルOS（AndroidとiOS）用の典型的な悪意のあるファイルのハッシュ			
IPレピュテーションデータフィード	各種の疑わしい悪意のあるIPアドレスのカテゴリ	IP	• ネットワークおよびメールセキュリティシステム（NGFW / Mail Security）との連携により、セキュリティ侵害インジケーターのネイティブデータベースに現在の脅威に関するデータを追加することで、サイバーインシデントの防止に役立ちます。 • SIEM/SOAR/IRPクラスのシステムとの連携により、ユーザーは現在の脅威にすぐに反応し、インシデントを調査する際に追加のコンテキストを作成することができます。	#予防 #検知 #調査
フィッシングURLデータフィード	IoTデバイス（IP カメラ、スマート掃除機、ティーポット、コーヒーメーカーなど）を標的とする悪意のあるソフトウェアを配布するWebリソース	マスク		
脆弱性データフィード	企業向けソフトウェアの脆弱性	CVE	• 脆弱性スキャナーおよび資産管理システムとの連携による脆弱なインフラ要素の特定。 • エンドポイント保護システムと連携し、深刻な脆弱性を含むソフトウェアの起動を防止。 • 脆弱なソフトウェアの起動を検知。 • 調査の支援。 • 脆弱性による影響の緩和のための推奨事項。	#予防 #検知 #調査
ICS脆弱性データフィード	ICSソフトウェアおよびハードウェアや、プロセス管理インフラで使用する企業ソフトウェアに存在する脆弱性			

フィード名	フィードの説明	インジケーターのタイプ	ユースケース	
ICS脆弱性データフィード（OVAL形式）	ICSソフトウェアの脆弱性を自動的に検索するためのルール	OVALチェック	• よく使用されるソフトウェアの脆弱性のスキャナーをリッチ化し、ICSソフトウェアの脆弱性を検知します。	#検知
ICSハッシュデータフィード	ICSに脅威をもたらす一般的な悪意のあるファイル	ハッシュ	• OTネットワークの境界において、悪意のあるハッシュデータフィードを使用するシナリオと同様です。 • OTネットワーク内部で危険な可能性のあるファイルを検知します。	#予防 #検知 #調査
pDNSデータフィード	一定期間における、ドメインと対応するIPアドレスの DNSルックアップの記録	IP、FQDN	• サイバーインシデントを調査する際にコンテキストを提供	#調査
Suricataルールデータフィード	ネットワークトラフィックにおける各種の脅威カテゴリ（APT、ボットネットC&C、ランサムウェアなど）を検知するためのルール	Suricataルール	• NGFW/IDS/IPS/NTA/NDRシステムと連携し、悪意のある活動を検知するルールをリッチ化します。	#検知
Cloud Access Security Broker（CASB）データフィード	一般的なクラウドサービスに関連するドメインおよびホスト	マスク	• CASBソリューションを構築します。特に、クラウドサービスのアクセスポリシーを設定します。	#検知

フィード名	フィードの説明	インジケーターのタイプ	ユースケース	
APTハッシュデータフィード	APT 攻撃グループが標的型攻撃の実行に使用するファイルのハッシュ	ハッシュ	• インフラセキュリティシステム（エンドポイントおよびサーバーセキュリティ）との連携により、マルウェアのダウンロードと実行を防止し、既に活動中のマルウェアを検知します。 • ネットワークおよびメールセキュリティシステム（たとえば、NGFW / IDS / IPS / メール / Webセキュリティ）との連携により、データフィードが提供するIOCによってネイティブのセキュリティ管理機能がリッチ化され、サイバーインシデントの防止を支援します。 • SIEM / SOAR / IRPクラスのシステムとの連携により、ユーザーはインシデントを調査する際に追加のコンテキストを作成でき、標的型攻撃やAPTグループのメンバーに関連する現在の脅威に短時間で対応することができます。	#検知 #調査
APT IPデータフィード	標的型攻撃に関連するインフラ要素に関する情報	IP		
APT URLデータフィード		マスク		
APT Yaraデータフィード	標的型攻撃で使用するファイルを識別するためのYARA ルール	YARAルール	• 組織のインフラにおける標的型攻撃の兆候を事前に検索します。 • サイバーインシデントの調査時に役立ちます。	#検知 #調査
オープンソースソフトウェアの脅威データフィード	脆弱性、悪意のある機能、または政治的な動機による機能の侵害（特定の地域でのブロック、政治的なスローガンなど）を含むオープンソースソフトウェアパッケージ	パッケージ名とバージョン	• セキュアな開発プロセス（DevSecOps）の一環として、開発されたソフトウェアの構成要素の分析を目的として設計されています。サプライチェーン攻撃からのソフトウェアの保護、脆弱性の早期の検知と除去、政治的な指向性を持ち未発表の機能（NVD）の使用を防止します。	#予防 #検知 #調査

フィード名	フィードの説明	インジケーターのタイプ	ユースケース	
クライムウェアハッシュデータフィード	Kasperskyのクライムウェアレポートで説明されている不正なキャンペーンで使用されたファイルのハッシュ	ハッシュ	• 侵入者の不正な動作に関連する悪意のある活動を検知します。 • 脅威データフィードに含まれる追加情報の提供により、インシデントの解決を支援します。	#検知 #調査
クライムウェアURLデータフィード	Kasperskyのクライムウェアレポートで説明されている不正なキャンペーンに関連するインフラ要素に関する情報	マスク		
クライムウェアYaraデータフィード	Kasperskyのクライムウェアレポートで説明されている不正なキャンペーンで使用するファイルを特定するためのYARAルール	YARAルール	• 組織のインフラにおける不正キャンペーンの兆候を事前に探します。 • サイバーインシデントの調査時に役立ちます。	#調査
Sigmaルールデータフィード	悪意のある活動を検知するためのYAML形式のルール	SIGMAルール	• SIEM/EDRとの連携により、悪意のある活動を検知します	#検知
ネットワークセキュリティIPデータフィード	NGFWの警告/拒否リスト用の IP アドレスのリスト	IP	• ネットワークセキュリティ管理（NGFW）との連携により、保護レベルを向上します	#検知 #予防

フィード名	フィードの説明	インジケーターのタイプ	ユースケース	
ネットワークセキュリティURLデータフィード	NGFWの警告/拒否リスト用の URLの一覧	URL	• ネットワークセキュリティ管理（NGFW）との連携により、保護レベルを向上します	#検知 #予防
ネットワークセキュリティWebフィルタリングデータフィード	NGFWの警告/拒否リストのカテゴリ化されたドメインのリスト	URL	• ネットワークセキュリティ管理（NGFW）との連携により、保護レベルを向上します	#検知 #予防

デモフィード

デモフィードは評価目的でのみ使用可能です。データのサンプルは制限されており、情報量が大幅に削減され、更新頻度も低くなっています。フィードの構造は商用フィードの形式と類似していますが、一部異なる場合があります。

- IPレピュテーションデータフィード（デモ版）
- ボットネットC&C URLデータフィード
- 悪意のあるハッシュデータフィード（デモ版）
- APT IPデータフィード（デモ版）
- APT URLデータフィード（デモ版）
- Sigmaルールデータフィード（デモ版）
- APT ハッシュデータフィード（デモ版）
- Suricataルールデータフィード（デモ版）
- Suricataルールデータフィード（デモ版）
- ICS脆弱性データフィード（デモ版）
- ICS脆弱性データフィード（OVAL形式）（デモ版）
- クライムウェアハッシュデータフィード（デモ版）
- クライムウェアURLデータフィード（デモ版）

デモのご依頼はこちら

Kaspersky Threat Intelligence

既存のシステムをサポートする豊富なコンテキスト

Kasperskyの脅威データフィードは、SIEMシステム、侵入検知システム、セキュリティプロキシなど、既存のセキュリティ対策の検知能力を強化します。

詳細はこちら

www.kaspersky.co.jp

© 2024 AO Kaspersky Lab.
登録商標およびサービスマークは、各所有者の財産です。