Kaspersky Threat Data Feeds

kaspersky bring on the future

Kaspersky Threat Data Feeds

Kaspersky Threat Data Feeds

サイバー攻撃は日々発生しています。サイバー脅威は常にその頻度、複雑性、難読性を高めながら、組織の防御を突破しようとしています。攻撃者は、複雑な侵入キルチェーン、キャンペーン、カスタマイズされた戦術、テクニック、手順（TTP）を使用して、貴社のビジネスの混乱や顧客への被害を発生させます。保護には、脅威インテリジェンスに基づいた新しい方法が必要なことは明らかです。

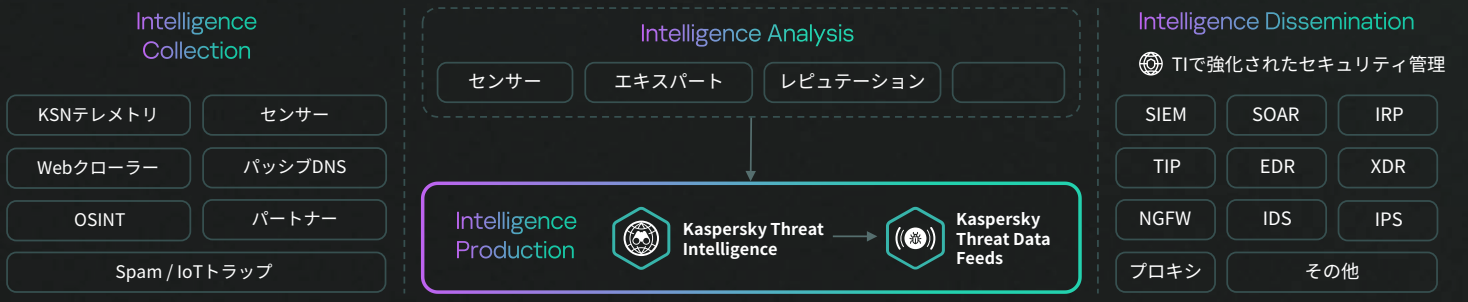
不審かつ危険なIPアドレス、URL、ファイルハッシュに関する情報を含む最新の脅威インテリジェンスフィードを、SIEM、SOAR、脅威インテリジェンスプラットフォームなどの既存のセキュリティシステムに統合することで、セキュリティチームは初期アラートのトリアージプロセスを自動化することができます。同時に、トリアージの担当者には、調査やインシデントレスポンスチームへのエスカレーションが必要なアラートをすぐに特定するために十分なコンテキストを提示することができます。

コンテキストデータ

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、優先順位付けするのに役立つ次の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
- 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
- 位置情報
- 普及度など

仕組み



Kaspersky Threat Data Feedsは、多様かつ信頼性が高い複数のKasperskyの情報源からデータを集約しています：

Kaspersky Security Network

世界4億人以上の参加者が任意で提供する匿名のサイバー脅威データを収集、分析する先進的なクラウドインフラにより、ビッグデータ分析、機械学習、エキスパートの専門知識を活用して、新種の脅威に最速で対応します。

Webクローラー

各種の情報源から新しいマルウェアと合法的なサンプルを収集しています：情報源には、OSINT、Kasperskyのアナリストによる調査、およびマルウェアからURLを抽出する当社独自の自動処理システムと分析システムなどがあります。

ボットネット追跡システム

専任のボットネット調査チームは、ボットの設定を抽出し、通信プロトコルをリバースエンジニアリングし、コマンドセンターからのコマンドを監視することで、有益な脅威インテリジェンスを獲得しています。

スパムトラップ

毎年、当社のフィッシング対策システムは、5億件以上のフィッシングリンクのクリックと1億6,000万件以上の悪意のあるメール添付ファイルのクリックを阻止しています。こうしたデータの抽出と追加により、当社のデータストリームをリッチ化しています。

パートナー

当社は、他のベンダーやサイバーセキュリティ組織と悪意のあるサンプルを共有するパートナーシップに参加しています。

センサー

ハニーポット、シンクホール、ITW攻撃を傍受するその他の方法です。（例：IoTデバイス、脆弱なシステム、ソフトウェアなど。）Kasperskyのアナリストは攻撃の試行と攻撃者の手法を調査し、セキュリティ侵害インジケーターを抽出し、他のデータソースにリンクします。

パッシブDNS

ホスティング組織やISPなどの信頼できるサードパーティから、世界規模でデータを収集しています。

OSINT

攻撃者のデータは、ニュース配信、ソーシャルメディア、公開レポート、ダークウェブなど、一般に公開されている情報源から自動的に収集されます。このデータを使用して、敵対者のインフラを探索し、新しい悪意のあるサンプルを調査して継続的に知識ベースを追加しています。

検知されたインジケーターは、自動処理システム内で多段階のスクリーニングプロセスにかけられます。このシステムでは、実際の信頼されたファイルと悪意のあるファイルの数億件ものサンプルに基づいてトレーニングされた信頼性評価技術と機械学習モデルを使用して、誤検知を排除しています。インジケーターはそれぞれ、複数のサンドボックスでも分析され、そこからTTP、ネットワーク上のふるまい、OS上のふるまい、その他多数の関係性など、さらに数十の属性が抽出されます。

これらすべてにより、Kaspersky Threat Intelligenceは戦術レベルの強力なインテリジェンス情報源となり、企業の脅威監視センターを強化し、組織の最前線で攻撃者を検知することができるようになります。

主な特徴

データフィードは、世界中の調査結果に基づいてリアルタイムで自動的に生成され、**高い検知率と精度を実現します。**

実装や統合を簡単に行うことができます。補足ドキュメント、サンプル、専任のテクニカルアカウントマネージャーやKasperskyのテクニカルサポートによる支援を組み合わせることで、この簡便性が実現されます。

HTTPS、TAXII、またはアドホックな配信メカニズムを介したシンプルな軽量な配信形式（JSON、CSV、OpenIoC、STIX）により、セキュリティソリューションへのフィードの**統合が容易**になります。代表的なSIEMおよびTIプラットフォームを完全にサポートしています。

誤検知の多いデータフィードは価値がありません。そのため、フィードを公開する前に非常に広範囲にわたるテストとフィルタリングを行い、**100%精査されたデータが配信されるようにしています。**

世界各国のセキュリティアナリストを含む数百人のエキスパートや、GReATや研究開発チームの世界に名だたるセキュリティエキスパートが、これらのフィードの生成に貢献しています。セキュリティ担当者には、**最高品質のデータ**から生成された重要情報とアラートが送信されます。必要以上の兆候データや警告が大量に流入するリスクはありません。

すべてのフィードは、高度な耐障害性インフラによって生成および監視されており、**継続的な可用性を確保しています。**

メリット

1. SIEM、ファイアウォール、NGFW、IPS/IDS、セキュリティプロキシ、DNSソリューション、APT対策などのネットワーク防御ソリューションを強化します。また、セキュリティ侵害インジケーター（IOC）を継続的に更新し、実用的なコンテキストを提供することで、サイバー攻撃に関する洞察力を高め、攻撃者の意図、能力、標的についてより深く理解することができます。

2. 初期のトリアージプロセスを自動化することで、インシデントレスポンスとフォレンジック能力を改善し、加速させます。また、セキュリティアナリストに十分なコンテキストを提供することで、調査やインシデントレスポンスチームへのエスカレーションが必要なアラートをすぐに特定できるようにします。

3. 感染したマシンから機密情報を含む資産や知的財産が外部に流出するのを防ぎます。感染した資産をすばやく検知してブランドの評判を保護し、競争上の優位性を維持して事業機会の損失を防ぎます。

4. MSSPとして、業界をリードする脅威インテリジェンスをプレミアムサービスとして顧客に提供することで、ビジネスを成長させることができます。

5. CERTとして、組織のサイバー脅威の検知および特定能力を強化、拡張します。

Kaspersky Threat Intelligence

Kaspersky Threat Intelligenceにより、世界トップクラスのアナリストやリサーチャーが収集した幅広い情報へのアクセスが可能となります。このデータを活用することで、今日のサイバー脅威に効果的に対抗できます。

当社は、サイバー脅威の研究における深い知識と豊富な経験、そしてサイバーセキュリティのあらゆる側面に対する独自の洞察力を備え、最新の戦術的、実用的、戦略的な脅威インテリジェンスを提供しています。これにより当社は、インターポールや各種のCERTユニットをはじめ、世界中の法執行機関や政府機関から信頼されるパートナーとなっています。そして、これらすべての情報は、Kaspersky Threat Intelligence Portalを通じて、関連性のある実用的なデータとしてご利用いただけます。

Kaspersky Threat Intelligence

詳細はこちら

www.kaspersky.co.jp

#kaspersky
#bringonthefuture