カスペルスキー
脅威インテリジェンス

kaspersky

カスペルスキー脅威インテリジェンス

絶えず進化し続ける情報セキュリティにおける脅威を追跡、分析、解析、軽減する作業には、非常に大きな労力が必要です。あらゆる業界の企業で、情報セキュリティの脅威に付随するリスクへの対処に必要な最新情報と適切なデータが不足しています。

カスペルスキー
サイバーセキュリティサービス

カスペルスキー
脅威インテリジェンス

脅威データフィード
CyberTrace
APT インテリジェンスレポート
デジタルフットプリントインテリジェンス
脅威情報ルックアップ
クラウドサンドボックス
ICS 脅威インテリジェンスレポート

カスペルスキー
脅威ハンティング

カスペルスキー
セキュリティトレーニング

カスペルスキー
インシデントレスポンス

カスペルスキー
セキュリティアセスメント

Kaspersky の脅威インテリジェンスサービスを利用することで、お客様は、世界有数のリサーチャーとアナリストのチームが提供する、脅威を軽減するために必要なインテリジェンスをご利用いただけます。

サイバーセキュリティのあらゆる側面に関する深い知識、経験、情報により、Kaspersky は世界有数の警察機関および政府機関（インターポールや主要 CERT など）からパートナーとして信頼されています。このインテリジェンスを、お客様の組織で活用いただけます。

Kaspersky が提供する脅威インテリジェンスサービスには以下のものが含まれます：

- 脅威データフィード
- CyberTrace
- APT インテリジェンスレポート
- デジタルフットプリントインテリジェンス（個別顧客に特化した脅威情報）
- 脅威情報ルックアップ
- クラウドサンドボックス
- ICS 脅威インテリジェンスレポート

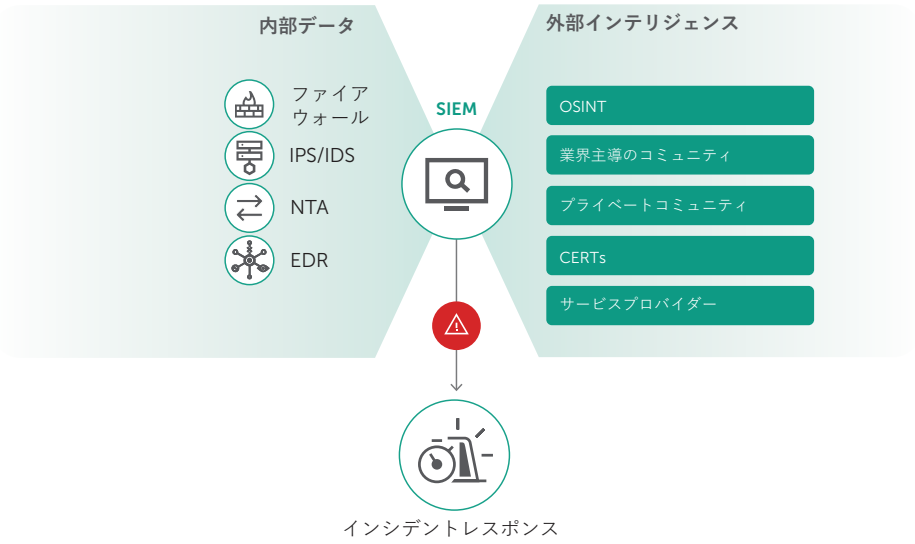
脅威データフィード

サイバー攻撃は絶えず行われています。サイバー脅威は、**標的の防御を突破しようと**、頻度、複雑度、難読度において常に進化しています。攻撃者は、標的のビジネスを中断させる、あるいはその顧客にダメージを与えるために、侵入するための複雑な**キルチェーン**、活動、およびカスタマイズされた**戦術（Tactics）、技術（Techniques）、手順（Procedures）、すなわち TTP を駆使しています。**今や、脅威インテリジェンスに基づいた新しい方法を保護対策に導入しなければならないことは明白です。

危険な可能性がある疑わしい IP、URL、ファイルハッシュ値に関する情報が含まれた最新の脅威インテリジェンスフィードを SIEM などの既存のセキュリティ管理システムに統合することで、セキュリティチームは最初のアラートトリアージのプロセスを自動化したうえで、調査が必要なアラートや、インシデントレスポンスチームにエスカレーションして詳細な調査と対応を行う必要のあるアラートを直ちに特定するために必要なコンテキスト情報を担当者に提供できます。

長年の実績があり信頼されたカスペルスキー脅威データフィードは、大規模セキュリティベンダーや大手企業により、高品質のセキュリティ製品開発や**ビジネスの保護**に利用されています。

図 1：外部脅威インテリジェンスの運用



コンテキスト情報

各データフィード内のすべてのレコードに**実用的なコンテキスト情報**(脅威名、タイムスタンプ、地理的位置情報、感染した Web リソースの解決済み IP アドレス、ハッシュ値、知名度など)が付加されます。コンテキスト情報によって「より広い視野」が得られ、その後の検証や、幅広いデータの利用法が可能になります。データをコンテキスト情報とともに考察することで、**「誰が」、「何を」、「どこで」、「いつ」という疑問**に答えることが容易になり、その結果、攻撃者を特定して、**自社に固有の**タイムリーな意思決定を下して行動に移すことができます。

データフィード

フィードの構成は以下のとおりです:

- **IP レピュテーションフィード** – 疑わしいホストや悪意のあるホストを対象とした IP アドレスとコンテキスト情報のセットです。
- **悪意のある URL およびフィッシング URL フィード** – 悪意のあるリンクおよびフィッシングサイトを対象とします。
- **ボットネット C&C URL フィード** – デスクトップボットネット C&C サーバーおよび関連する悪意のあるオブジェクトを対象とします。
- **モバイルボットネット C&C URL フィード** – モバイルボットネット C&C サーバーを対象として、C&C と通信している感染したマシンを特定します。
- **ランサムウェア URL フィード** – ランサムウェアオブジェクトをホストするリンクまたはランサムウェアオブジェクトからアクセスされるリンクを対象とします。
- **脆弱性データフィード** – セキュリティ上の脆弱性と、関連する脅威インテリジェンス(脆弱なアプリやエクスプロイトのハッシュ値、タイムスタンプ、CVE、パッチなど)のセットです。
- **APT IoC フィード** – APT 攻撃を実行するために攻撃者が使用する悪意のあるドメイン、ホスト、IP アドレス、ファイルを対象とします。
- **パッシブ DNS (pDNS) フィード** – ドメイン名からそれに対応する IP アドレスを導出する DNS による名前解決の結果が含まれたレコードのセットです。
- **IoT URL フィード** – IoT デバイスに感染するマルウェアのダウンロードに使用された Web サイトを対象とします。
- **マルウェアハッシュフィード** – 危険で蔓延している新しいマルウェアを対象とします。
- **ICS ハッシュ値データフィード** – 産業用制御システム(ICS)で使用されるデバイスに感染する悪意のあるオブジェクトを検知するためのファイルハッシュ値と、対応するコンテキスト情報のセットです。
- **モバイル向けの悪意のあるハッシュフィード** – Android および iPhone を対象とする悪意のあるオブジェクトの検知をサポートします。
- **許可リストデータフィード** – サードパーティの製品とサービスの正規ソフトウェアに関する体系的知識を提供します。

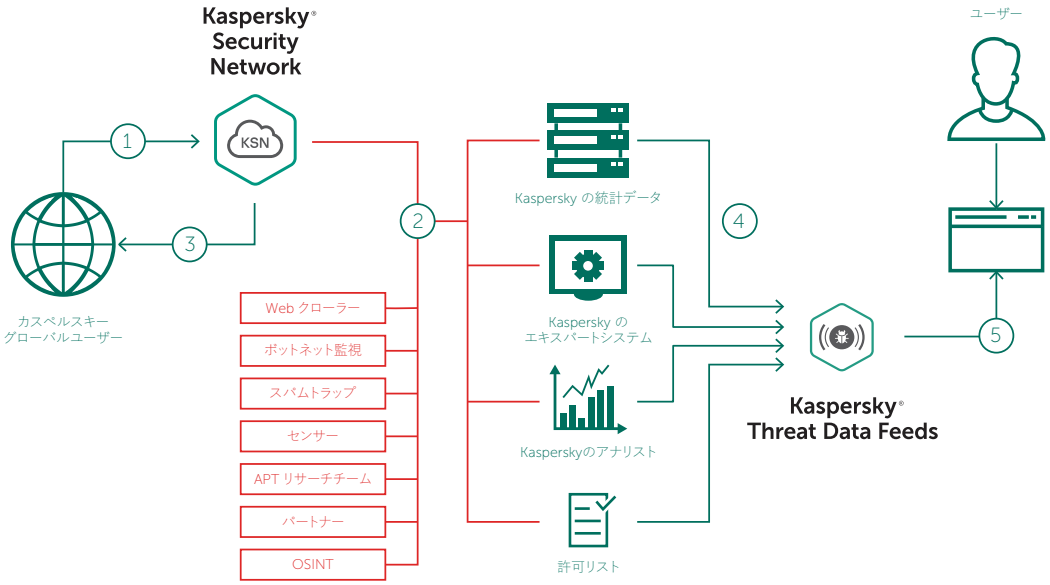


図 2:カスペルスキー脅威インテリジェンスのソース

サービスの概要

- **誤検知**がいくつもあるデータフィードには価値がありません。そのため、十分に精査されたデータが配信されるように、フィードをリリースする前に大量のテストとフィルターを適用しています。
- データフィードは、世界中から収集された調査結果に基づいて、リアルタイムで自動的に生成されます（Kaspersky Security Network は、213 を超える国と地域から数千万にのぼるエンドユーザーを対象として、インターネットの全トラフィックのうち、かなりの割合のトラフィックを把握しています）。そのため、高い**検知率**と精度を実現しています。
- すべてのフィードは耐障害性の高いインフラストラクチャによって生成、監視されており、**継続的可用性**を確保しています。
- データフィードによって、フィッシング、マルウェア、エクスプロイト、ボットネット C&C の URL、その他の悪意のあるコンテンツをホストするために使用されている **URL を即座に検知**できます。
- さまざまなトラフィック種別（Web、メール、P2P、IM など）、あるいはモバイルプラットフォームを標的とした**マルウェア**も**すぐに検知**して特定できます。
- シンプルな軽量の**配布**形式（**JSON、CSV、OpenIoC、STIX**）で **HTTPS** や任意の方法によって配信されるため、フィードをセキュリティソリューションに容易に統合できます。
- 世界中の**セキュリティアナリスト**、業界をリードする **GReAT チームや最先端の研究開発チームのセキュリティエキスパート**など、数百人に及ぶ専門家がこれらのフィードの生成に携わっています。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られます。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。
- **実装のしやすさ。**Kaspersky が提供する補助的なドキュメント、サンプル、専任のテクニカルアカウントマネージャー、テクニカルサポートのすべてが一体となって、容易な統合を可能にします。

収集と処理

データフィードは、Kaspersky Security Network や当社独自の Web クローラーであるボットネット監視サービス（ボットネットおよびその標的とアクティビティを 24 時間 365 日監視するサービス）、スパムトラップ、調査チーム、パートナーなどの信頼性の高い異種混在のソースを融合して、そこから集積されます。

次に、集積されたすべてのデータがリアルタイムで慎重に調査され、複数の前処理手法によってふるい分けされます。その手法として、統計的な基準、サンドボックス、ヒューリスティックエンジン、近似ツール、ふるまいプロファイリング、アナリストによる検証、許可リスト検証などが利用されます：

利点

- 絶えず更新される侵害の痕跡（IOC）と実用的なコンテキスト情報によって SIEM、ファイアウォール、IPS/IDS、セキュリティプロキシ、DNS 解決、APT 対策などの**ネットワーク防御ソリューションを強化**することで、サイバー攻撃に関する知見を得て、攻撃者の意図、能力、標的についてより深く理解できるようになります。主要な SIEM（ArcSight、QRadar、Splunk など）に対応しています。
- **周辺機器やエッジネットワーク機器のマルウェア対策を強化**します（ルーター、ゲートウェイ、UTM アプライアンスなど）。
- 脅威に関連する有意義な情報と標的型攻撃の背景にあるグローバルな知見をお客様のセキュリティ / SOC チームに提供することで、**お客様のインシデントレスポンスおよびフォレンジック能力を改善、強化**します。ホストやネットワークでのセキュリティインシデントをより効率的かつ効果的に診断、分析し、未知の脅威に対する社内システムからのシグナルの優先順位を付けることで、インシデント対応の時間を最小限に抑え、重要なシステムやデータが不正アクセスを受ける前に、キルチェーンを遮断することができます。
- 新しいマルウェアやその他の悪意のある脅威について直に得た情報を活用して、**先手を打ってお客様の防御体制を強化し、侵害を防止**します。
- **標的型攻撃の軽減**に役立ちます。戦術的、戦略的脅威インテリジェンスを利用して、目の前の特定の脅威に対抗するために防御戦略を適応させることで、セキュリティ体制を強化できます。
- 脅威インテリジェンスを利用して、**ネットワークやデータセンターにホストされている悪意のあるコンテンツを検知**できます。
- 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。**感染した資産を素早く検知することで、競争優位や事業機会の喪失を防ぎ、ブランドへの評価を維持します。
- コマンド & コントロールプロトコル、IP アドレス、悪意のある URL、ファイルハッシュ値などの脅威の兆候について詳細に調査し、さらに専門家によって検証された脅威のコンテキスト情報を付加することで、攻撃に優先順位を付け、IT 支出やリソースの割り当てに関する意思決定を向上できるようにします。また、**ビジネスにとって極めて大きなリスクとなる脅威を軽減することにお客様が集中できるようにサポート**します。
- 当社の専門知識とコンテキストに関する実用的なインテリジェンスを利用して、Web コンテンツフィルタリング、スパム / フィッシングブロックなどの**お客様の製品およびサービスが提供する保護機能を強化**できます。
- **マネージド・セキュリティ・サービス・プロバイダー（MSSP）として**、業界をリードする脅威インテリジェンスをお客様の顧客向けの高品質サービスとして提供することで、お客様のビジネスの成長に貢献します。**CERT として**、お客様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。

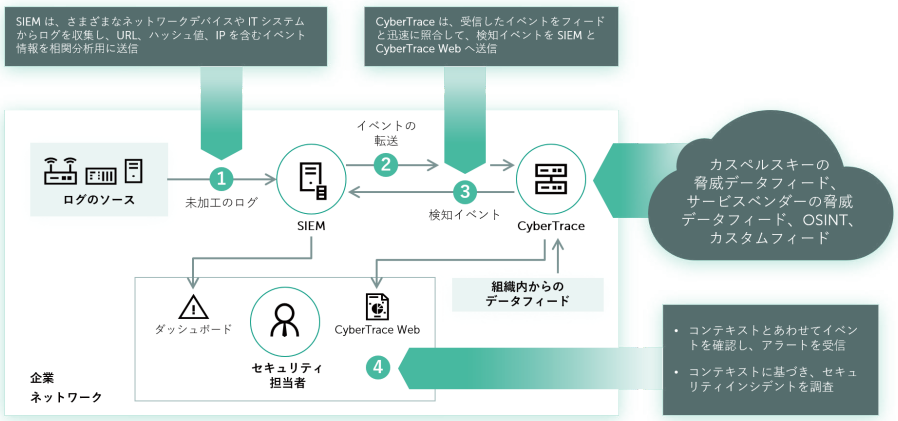
CyberTrace

機械で判読可能な最新の脅威インテリジェンスを SIEM などの既存のセキュリティ管理システムに統合することで、セキュリティオペレーションセンターでは最初のトリアージプロセスを自動化し、調査が必要なアラートや、インシデントレスポンスチームにエスカレーションして対応を行う必要があるアラートを直ちに特定するためのコンテキスト情報をセキュリティアナリストに提供できます。その一方で、脅威データフィードや利用できる脅威インテリジェンスのソースは増加し続けているため、自社に関係のある情報を見極めることが困難になっています。脅威インテリジェンスがさまざまな形式で提供され、そこに膨大な数の侵害の痕跡(IOC)が含まれることから、SIEM やネットワークセキュリティ管理システムですべてを処理することが難しくなっています。

Kaspersky CyberTrace は、脅威データフィードと SIEM ソリューションをシームレスに統合することで、アナリストが既存のセキュリティ運用ワークフローで脅威インテリジェンスをより効果的に活用できるように支援する、脅威インテリジェンスのプラットフォームです。Kaspersky、他のベンダー、OSINT からの脅威インテリジェンスフィード、カスタムのフィードなど、お客様が使用するさまざまな形式(JSON、STIX、XML、CSV)の脅威インテリジェンスフィードと統合し、SIEM ソリューションやログソースともすぐに統合することが可能です。

Kaspersky CyberTrace が、受信したデータの解析と照合を行うことで、SIEM の負荷を大幅に軽減できます。また受信したログとイベントを解析し、解析結果のデータとフィードを速やかに照合して、脅威検知に関する独自のアラートを生成します。下の図は、このソリューションの統合アーキテクチャの概要を示しています。

図 3:Kaspersky CyberTrace の統合スキーム



製品機能

Kaspersky CyberTrace には、脅威インテリジェンスを運用してアラートのトリアージと初期対応を効果的に行うために、次の機能があります。

- 全文検索および高度な検索クエリの使用が可能な痕跡データベースでは、コンテキストフィールドを含むあらゆるインジケーターフィールドに対し、複雑な検索を実行できます。またインテリジェンスサプライヤ別に結果をフィルタリングできるため、脅威インテリジェンスの分析プロセスを簡略化することができます。
- ページには各痕跡に関する詳細な情報が掲載されるため、分析を掘り下げることも可能です。こうしたページには、あらゆる脅威インテリジェンスサプライヤから得られる痕跡に関する情報が掲載されるため(重複は排除)、アナリストはそこにコメントを追加して脅威に関するディスカッションを実施し、その痕跡に関する社内の脅威インテリジェンスを強化することができます。痕跡が検出されると、その検出日に関する情報および検出リストへのリンクが提示されます。
- この痕跡のエクスポート機能では、ポリシーリスト(ブロックリスト)などのセキュリティ管理システムに痕跡セットをエクスポートすることも、Kaspersky CyberTrace のインスタンス間または他の TI プラットフォームと脅威データを共有することも可能です。
- 履歴相関機能(逆スキャン)では、最新のフィードを使用して、以前にチェックしたイベントの識別可能データを分析することで、以前には特定できなかった脅威を見つけることができます。検出データの履歴はレポートに掲載されるため、将来の調査に役立てることができます。
- 検出イベントを SIEM ソリューションに送るためのフィルターもあるため、その負荷も、またアナリストによるアラート対応の負荷も軽減できます。 これにより、インシデントとして扱うべき危険な検出結果のみを SIEM へ送ることができます。その他の検出結果はすべて、根本原因の分析や脅威ハンティングの際に使用できるよう、内部データベースに保存されます。

- マルチテナンシーは、MSSP や大企業のユースケースに対応しているため、サービスプロバイダー（本部）がテナント（支部）のイベントに個別に対処する必要がある場合に便利です。これにより、1 つの Kaspersky CyberTrace インスタンスをさまざまなテナントの SIEM ソリューションと関連させることができ、また各テナントで使用するフィードを設定することもできます。
- フィード利用統計は、統合されたフィードとフィード交差マトリックスの効果を測定でき、価値の高い脅威インテリジェンスサプライヤを特定する際に役立ちます。
- HTTP RestAPI では、脅威インテリジェンスの検索および管理が可能です。また Rest API を使用することで、Kaspersky CyberTrace を複雑な環境に簡単に統合して、自動化やオーケストレーションに役立てることができます。

Kaspersky CyberTrace とカスペルスキー脅威データフィードは個別に使うことも可能ですが、組み合わせて使用することでサイバー脅威のグローバルな動向を把握して、セキュリティ対策を強化することができ、お客様の脅威検知能力が大幅に向上します。Kaspersky CyberTrace とカスペルスキー脅威データフィードにより、以下が可能になります。

- セキュリティアラートの中から重要なアラートを効果的に選別して優先順位を決定する
- アナリストの作業負荷を軽減し、燃え尽き症候群を回避する
- 重要なアラートを即時に特定し、インシデントレスポンスチームにエスカレーションすべきアラートを情報に基づき判断する
- プロアクティブでインテリジェンス主導型の防御を確立する

カスペルスキー APT インテリジェンスレポートのメリット:

- **専用アクセス:**最先端の脅威に関する技術的な情報を、公開前の調査段階で入手できます。
- **非公開の APT 情報:**注目を集めるすべての脅威が公開の対象となるわけではありません。被害を受けた組織やデータの機密性、脆弱性解消のプロセス、または関連する法執行機関の活動により公開されない脅威もあります。しかし、カスペルスキー APT インテリジェンスレポートの利用者には、発見されたすべての脅威が報告されます。
- **詳細な関連データ:**侵害の痕跡(IOC)が標準形式(openIOCやSTIX)で提供される他、Yaraルールも利用可能。
- **サイバー犯罪組織のプロファイル:**特定のサイバー犯罪組織に関する概要(拠点と思われる国、主な活動、使用されたマルウェア群、標的となった業界や地域、使用された TTP (戦術・技術・手順)の説明、MITRE ATT&CK フレームワークへのマッピングなど)を提供します。
- **MITRE ATT&CK:**レポートに記載されている TTP は、MITRE ATT&CK フレームワークにマップされています。対応するセキュリティ監視のユースケースを作成および優先順位付けし、関連性のある TTP に対するギャップ分析と現行の防御テストを行うことで、検知と対応を強化できます。
- **継続的な APT 活動の監視:**実用的なインテリジェンスに調査段階からアクセスできます(APT 分類、IOC、C&C インフラストラクチャに関する情報)。
- **過去レポート:**サービス期間中は、以前に発行されたレポートも閲覧できます。
- **RESTful API:**システム連携を可能にする API を利用し、セキュリティワークフローを自動化できます。

APT インテリジェンスレポート

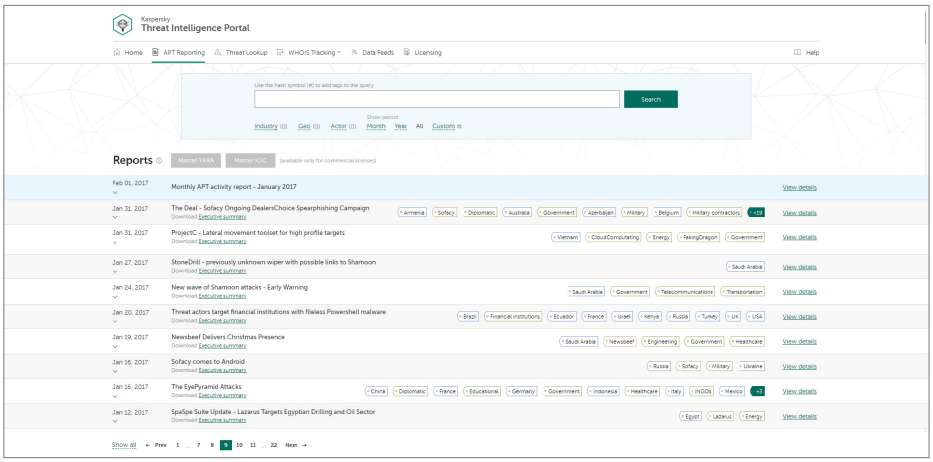
注目度の高いサイバースパイ活動の認識と知識を高める、包括的かつ実用的な Kaspersky のレポート提供サービスです。

インテリジェンスレポートで提供される情報を活用することで、新しい脅威と脆弱性に素早く対応でき、既知の経路からの攻撃のブロック、高度な攻撃によるダメージの軽減や、セキュリティ戦略の強化が可能になります。

Kaspersky はこれまで重大な APT 攻撃をいくつも発見してきましたが、発見されたすべての攻撃が公開されるわけではなく、公表されないものも多くあります。

カスペルスキー APT インテリジェンスレポートでは、発見されたすべての APT に関して、Kaspersky の調査内容が報告されます。これには、公開されることのない脅威情報も含まれています。各レポートには、関連する APT に関する情報をわかりやすくまとめた、経営層向けのエグゼクティブサマリーが含まれています。また、エグゼクティブサマリーの後に APT の詳しい技術説明と関連する IOC および Yara ルールの情報が続きます。この情報から、セキュリティ調査チーム、マルウェアアナリスト、セキュリティエンジニア、ネットワークセキュリティアナリスト、APT 調査チームは、関連する脅威に対して迅速かつ的確に対応するための実用的な情報を得ることができます。

Kaspersky のエキスパートは、業界をリードする高いスキルと実績を持つ APT ハンターであり、サイバー犯罪者グループが戦術を変更した場合は、ただちにお客様に警告を送ります。また、お客様は、セキュリティ強化に有用なリサーチや分析が含まれる、Kaspersky の APT レポートデータベースにアクセスできます。



注 - 購読にあたっての制限事項

本サービスのレポートに含まれる情報の機密性と固有性により、レポートの購読は信用ある政府、公共団体、民間団体に限定させていただいております。

デジタルフットプリントインテリジェンス

事業の成長とともに IT 環境は複雑化し規模が拡大する中、企業は、広範囲に分散されたデジタルプレゼンスを直接制御したり、所有したりせずに保護しなければならないという課題に直面しています。企業は、相互接続された動的な環境から、プロセスの最適化、製品の品質向上、顧客エクスペリエンスの改善、競争力の維持という大きなメリットを引き出すことができます。その一方で、相互接続がますます進むにつれて、攻撃対象領域も拡大しています。攻撃者はさらに巧妙になっていることから、組織はそのオンラインプレゼンスの全容を正確に把握するだけでなく、そこでの変化も追跡して、脅威にさらされているデジタル資産に対応しなければなりません。

セキュリティ対策としてさまざまなセキュリティツールを使用しても、デジタル脅威を完全に排除することは困難であり、内部関係者のアクティビティや、ダークウェブ上のフォーラムでのサイバー犯罪者の計画と攻撃スキームなどを検知および緩和する能力が求められます。Kaspersky では、カスペルスキーデジタルフットプリントインテリジェンスの提供を通じて、セキュリティアナリストが攻撃者の視点に立って社内のリソースをチェックし、攻撃者が利用できる潜在的な攻撃経路を見つけることで、防御を適切に調整できるよう支援します。

組織に攻撃を仕掛けるためにもっとも有効な方法は何でしょうか。組織に対する費用対効果に優れた攻撃方法は何でしょうか。標的を絞った攻撃者は、どのような情報を利用できるでしょうか。インフラストラクチャへの不正侵入がすでに発生しているでしょうか。

カスペルスキーデジタルフットプリントインテリジェンスは、これらの疑問に答えるだけにとどまりません。Kaspersky のエキスパートが現在の攻撃状況を総合的につなぎ合わせて、悪用可能な弱点を特定し、過去/現在/将来の攻撃の痕跡を明らかにします。

OSINT の手法と、攻撃対象領域、ディープウェブおよびダークウェブの自動分析と手動分析、さらには Kaspersky 内部のナレッジベースを組み合わせて作成されたオーダーメイドのレポートでは、すぐ実行につなげることができる有用な情報と推奨事項が提供されるため、潜在的な攻撃経路数を最小限に抑制して、デジタルリスクを軽減することができます。レポートには以下が含まれます。

- ネットワーク活動を阻害しないようにしてネットワーク境界を検査し、攻撃の侵入口として利用される可能性があるサービス（境界上に意図せずに残された管理インターフェイス、適切に設定されていないサービス、デバイスのインターフェイスなど）を特定
- 既存の脆弱性に関するオーダーメイドの分析、および CVSS 基本値（ベーススコア）、公開されているエクスプロイトの利用可能性、侵入テストの結果、ネットワークリソースの場所（ホスティングまたはインフラストラクチャ）に基づく、詳細なスコアと総合的なリスク評価
- 企業と、企業が属する業界および事業を展開する地域を標的とした、活動中の標的型攻撃、現在計画中の攻撃、APT 活動の特定、監視、分析
- お客様の顧客、パートナー、サービス利用者を標的とした脅威がある場合は、感染システムが攻撃に使用される可能性があるため、その痕跡を確認
- Pastebin サイト、公開フォーラム、ソーシャルネットワーク、インスタントメッセージチャネル、アクセスが制限されたアンダーグラウンドのオンラインフォーラムやコミュニティを慎重に監視することで、お客様の組織を標的としたアカウントへの不正アクセス、情報漏洩、攻撃が計画および話し合われているかどうかを確認

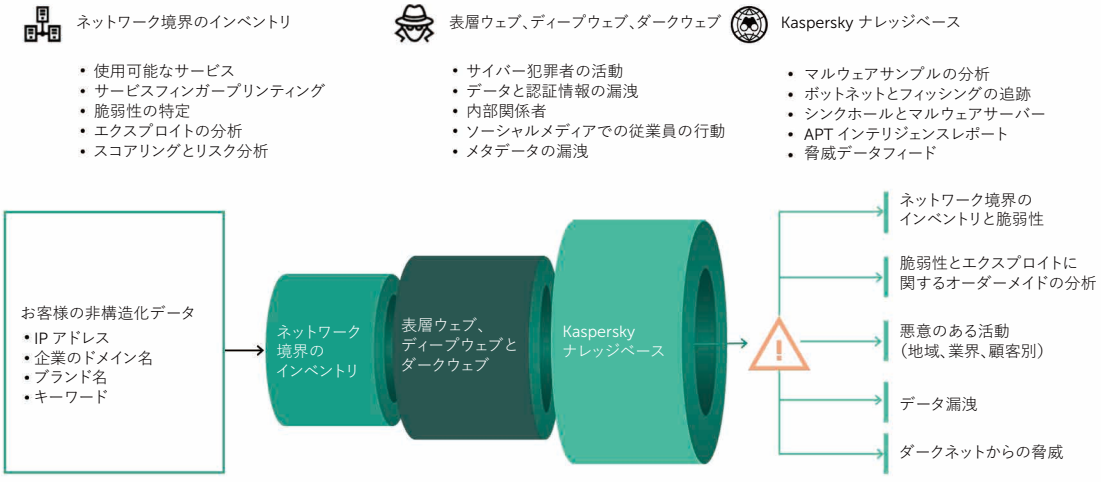
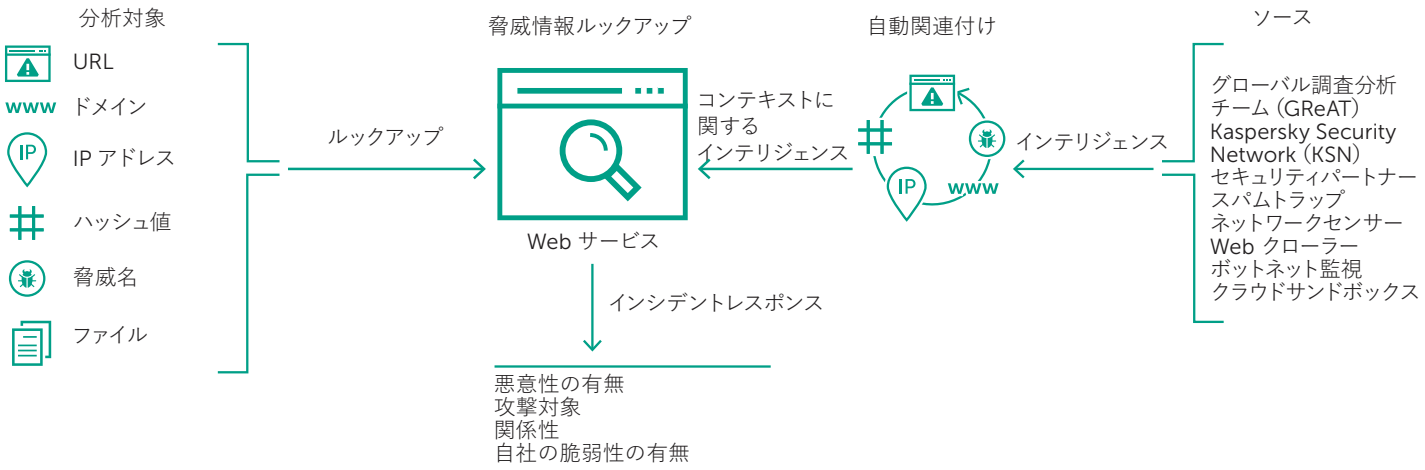


図 4：カスペルスキーデジタルフットプリントインテリジェンス

ポータルでのレポート提供と新情報の通知

カスペルスキーデジタルフットプリントインテリジェンスは、ネットワークリソースとサービスの整合性と可用性に影響を与えないようにして調査します。レポートは、カスペルスキー脅威インテリジェンスポータルで確認できます。このポータルは Kaspersky が 20 年以上にわたって収集した脅威インテリジェンスをまとめたアクセスポイントで、新しい情報が使用できるようになるとすぐに通知が送信されます。API の提供により、カスペルスキーデジタルフットプリントインテリジェンスをサードパーティのタスク管理システムと統合して、ワークフローの管理に必要な時間を大幅に削減できます。

脅威情報ルックアップ



サービスの概要

- **信頼できるインテリジェンス：**カスペルスキー脅威情報ルックアップの主な特徴として、脅威インテリジェンスデータの信頼性が高く、実用的なコンテキスト情報が付属していることが挙げられます。Kaspersky 製品はアンチマルウェアテスト[1] の分野でトップの評価を獲得しており、セキュリティインテリジェンスデータの比類のない質の高さが、最高水準の検知率と極めて低い誤検知率によって実証されています。

- **脅威ハンティング：**先を見越した予防、検知、対処を行うことで、攻撃の影響や頻度を最小限に抑えることができます。可能な限り早期に攻撃を追跡し、積極的に排除します。脅威の発見が早いほど与えられるダメージも小さく、速やかに修復して、ネットワーク運用を通常状態に戻すことができます。

- **さまざまなエクスポートフォーマット：**侵害の痕跡（IOC）や実用的なコンテキスト情報を機械判読可能なフォーマット（STIX、OpenIOC、JSON、Yara、Snort のほか CSV にも対応）にエクスポートでき、脅威インテリジェンスの十分な活用、運用ワークフローの自動化、SIEM などのセキュリティ管理システムへの統合が可能です。

- **使いやすい Web インターフェイス、RESTful API：**このサービスは、Web インターフェイス（Web ブラウザー）経由で手動モードで利用することも、RESTful API 経由でアクセスすることもできます。

今日のサイバー犯罪に国境はなく、技術的な能力も急速に高まっており、サイバー犯罪者がダークウェブのリソースを活用して標的を恐怖に陥れるなど、攻撃は巧妙になる一方です。サイバー脅威は、標的の防御を突破しようと次々と新たな試みが行われ、頻度、複雑度、難読度において常に進化しています。攻撃者は、標的のビジネスを中断させ、資産を窃取し、あるいはその顧客にダメージを与えるために、その活動において複雑なキルチェーン、およびカスタマイズされた戦術（Tactics）、技術（Techniques）、手順（Procedures）、すなわち TTP を駆使しています。

カスペルスキー脅威情報ルックアップは、サイバー脅威に関して Kaspersky が収集し続けているデータとそれらの間にある相互関係を単一の強力な Web サービスにまとめたものです。お客様のセキュリティチームに対して、影響を受ける前にサイバー攻撃を防止できるよう、可能な限り多くのデータを提供することを目的としています。URL、ドメイン、IP アドレス、ファイルハッシュ値、脅威名、統計的データまたはふるまいデータ、WHOIS データ、DNS データ、ファイル属性、地理的位置情報データ、ダウンロードチェーン、タイムスタンプなどに関する最新の脅威インテリジェンスの詳細情報を取得できます。その結果、新しい脅威のグローバルな動向を把握し、組織の保護とインシデントレスポンス能力の強化に役立てることができます。

カスペルスキー脅威情報ルックアップによって提供される脅威インテリジェンスは耐障害性の高いインフラストラクチャによってリアルタイムで生成、監視されており、継続的可用性と一貫したパフォーマンスが確保されています。世界中のセキュリティアナリスト、世界的に著名な GReAT チームや最先端の研究開発チームのセキュリティエキスパートなど、数百人に及ぶ専門家が、実態に即した価値ある脅威インテリジェンスの生成に携わっています。

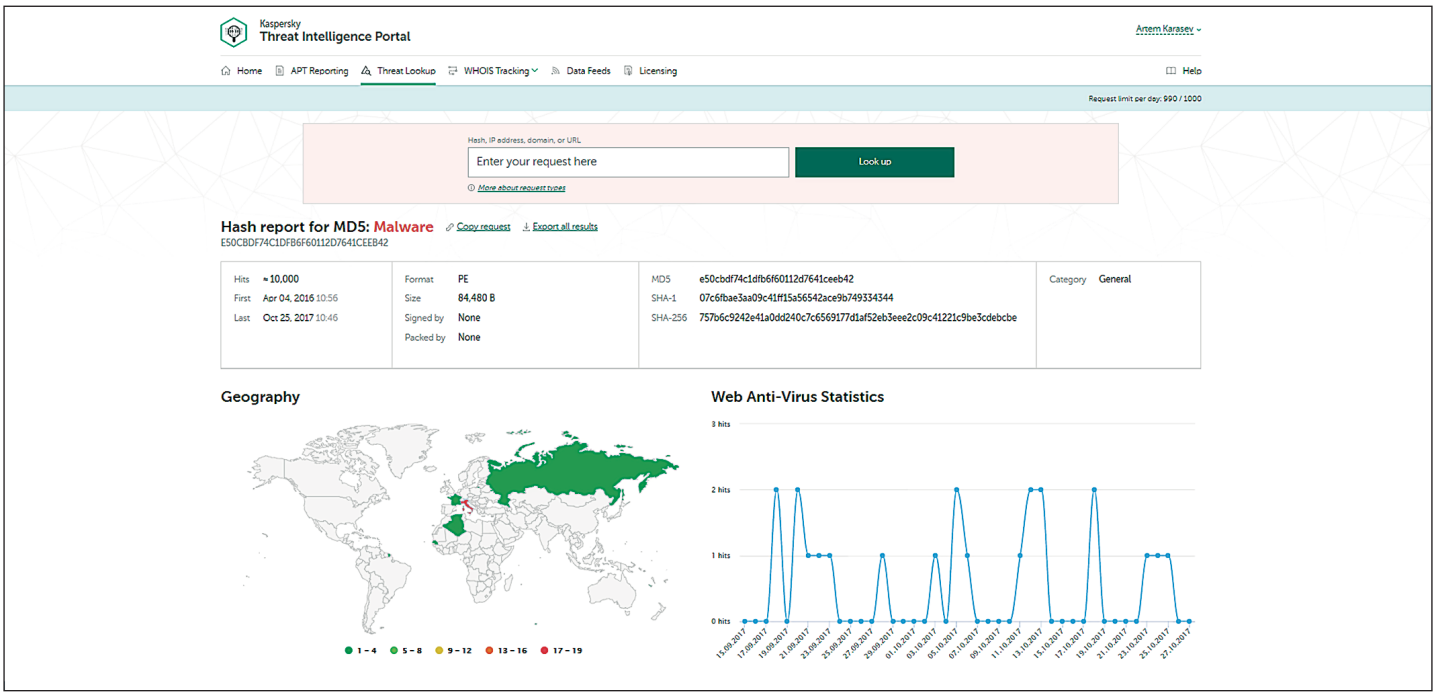
主な利点

- 脅威に関連する有意義な情報と標的型攻撃の背景にあるグローバルな知見をお客様のセキュリティ / SOC チームに提供することで、**お客様のインシデントレスポンスおよびフォレンジック調査を支援**します。ホストやネットワークでのセキュリティインシデントをより効率的かつ効果的に診断、分析し、未知の脅威に対する社内システムからのシグナルの優先順位を付けることで、インシデントレスポンスの時間を最小限に抑え、重要なシステムやデータが侵害される前に、キルチェーンを遮断することができます。

- IP アドレス、URL、ドメイン、ファイルハッシュ値などの**脅威の兆候について詳細に調査**し、さらに高度に検証された脅威のコンテキスト情報を付加することで、攻撃に優先順位を付け、スタッフやリソースの割り当てに関する意思決定を向上し、ビジネスにとって極めて大きなリスクとなる脅威の軽減に集中できるようにします。

- **標的型攻撃の軽減：**脅威インテリジェンスを利用して、脅威に対抗するための防御戦略を適応させることで、セキュリティインフラストラクチャを強化できます。

1 http://www.kaspersky.co.jp/top3



このサービスでできること

- Web インターフェイスまたは RESTful API 経由で脅威の兆候を検索する
- オブジェクトを悪意のあるものとして扱うべき理由を理解する
- 検知されたオブジェクトは広範に拡散されているか、固有のものであるかを確認する
- 証明書、共通名、ファイルパス、関連 URL などの高度な詳細情報を調査し、新たな疑わしいオブジェクトを発見する

これらは一部の例に過ぎません。関連性が高く粒度の細かいインテリジェンスデータを集めた、この充実した持続的なソースを活用できる方法は色々とあります。

敵と味方を知ること。そして、悪意がないと立証されているファイル、URL、IP アドレスを見分けて、調査スピードを上げることが大切です。1 秒 1 秒が重大になるときに、信頼済みオブジェクトの分析のために時間を無駄にできません。

Kaspersky のミッションは、あらゆる種類のサイバー脅威から世界を守ることです。このため、また、インターネットを安全なものにするため、脅威インテリジェンスをリアルタイムで共有し、利用できるようにすることが不可欠です。データとネットワークを効果的に保護し続けるための中核を成すのは、情報へのタイムリーなアクセスです。カスペルスキー脅威情報ルックアップを利用すれば、このようなインテリジェンスを効率的かつ容易に入手することができます。

主な機能:

- ロード済み、実行済み DLL
- 排他制御(ミューテックス)
- 変更、作成されたレジストリキー
- ドメイン名および IP アドレスによる外部接続
- HTTP、DNS のリクエストとレスポンス
- 実行ファイルによって作成されるプロセス
- 作成、変更、削除されたファイル
- プロセスメモリダンプ、ネットワークトラフィックダンプ
- スクリーンショット
- 判明した侵害の痕跡(IOC)に関する脅威インテリジェンスと実用的なコンテキスト情報
- RESTful API

主な利点:

- APT、標的型脅威、複雑な脅威の高度な検知
- 非常に効果的で複雑なインシデント調査を実行できるワークフロー
- コストのかかるアプライアンスの購入もシステムリソースに関する懸念も不要なスケーラビリティ
- 現行のセキュリティ対策とのシームレスな統合と自動化

クラウドサンドボックス

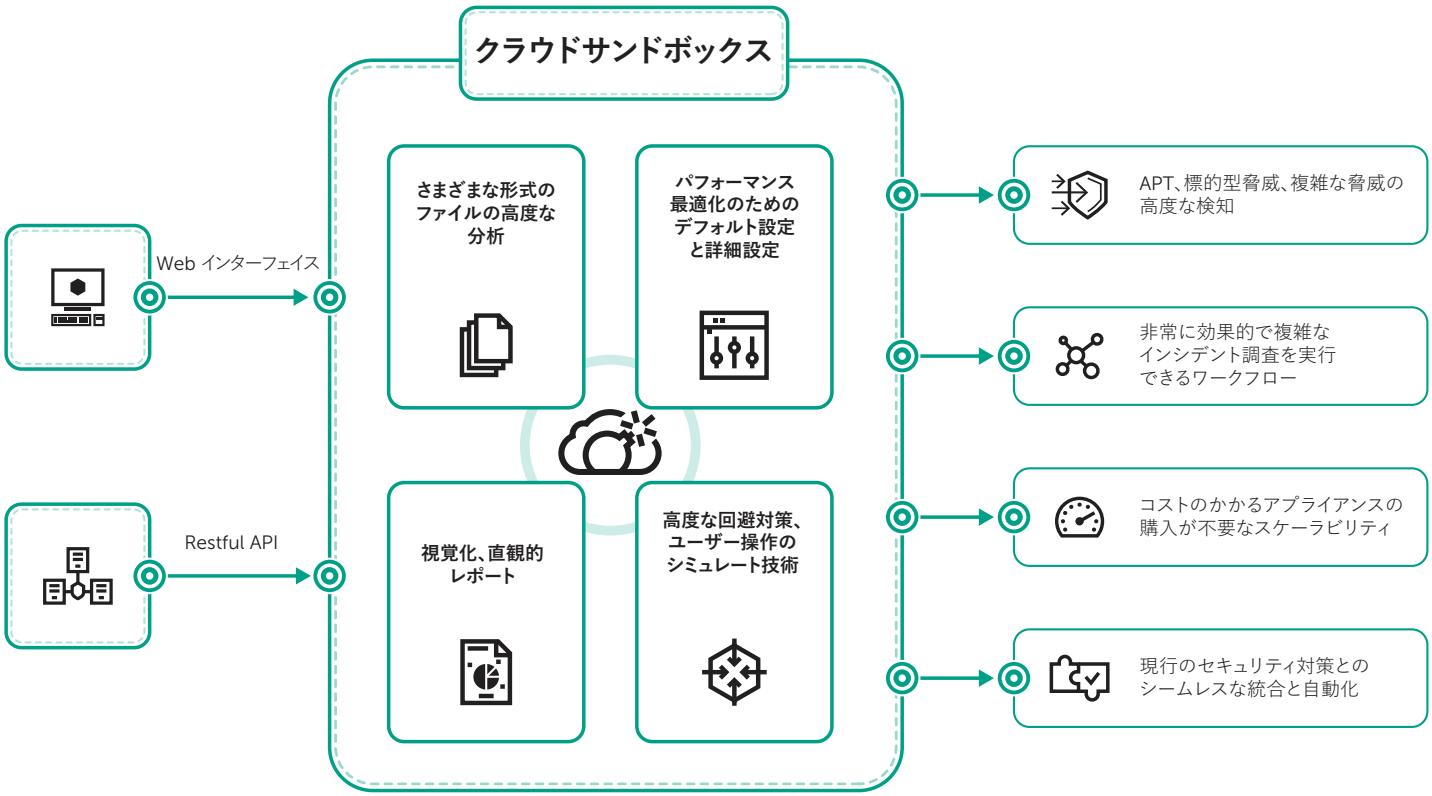
従来型のウイルス対策ソフトウェアだけで今日の標的型攻撃を予防することは難しくなってきています。アンチウイルスエンジンは既知の脅威やその亜種を阻止することしかできず、豊富な知識を持つサイバー犯罪者はあらゆる手段を自在に利用して自動検知をすり抜けます。情報セキュリティインシデントによる損害が今も急増していることから、大きな損害が発生する前に、瞬時に脅威を検知して脅威に対して迅速に対応および対抗できることがますます重要になっています。

ファイルのふるまいに基づいてインテリジェントな判断を行うこと、およびそれと並行してプロセスメモリ、ネットワークアクティビティなどを分析することが、目標に合わせて洗練された現在の標的型脅威を理解する上で最適なアプローチです。統計的データには、つい最近に修正されたマルウェアに関する情報が含まれていない可能性があります。一方、サンドボックス技術は、ファイルサンプルの発生源を調査し、ふるまい分析に基づいて IOC を収集し、未知の悪意のあるオブジェクトを検知できる強力なツールとなります。

セキュリティの防御をくぐり抜ける脅威に対する、先を見越した軽減対策

現代のマルウェアは、悪意のある動作の存在を知らせる可能性のあるコードを実行しないように、あらゆる策を講じています。標的のシステムに必要なパラメータが揃っていない場合、悪意のあるプログラムは自らを削除し、一切の痕跡を残さないようにすることがあります。そのため、悪意のあるコードを実行するには、サンドボックス環境が通常のエンドユーザーのふるまいを正確に模倣できる必要があります。

カスペルスキークラウドサンドボックスは、Kaspersky Security Network やその他のシステムによって得られた数ペタバイトにおよぶ統計的データから収集した脅威インテリジェンス、ふるまい分析、信頼性の高い回避対策と、自動クリック、文書スクロール、ダミープロセスなどのユーザー操作のシミュレート技術を組み合わせたハイブリッドアプローチを採用しています。そのため、未知の脅威を検知するための最適なツールに仕上がっています。



このサービスは、当社のラボ内で 10 年以上にわたって進化を遂げてきたサンドボックステクノロジーをもとに開発されています。このテクノロジーは、Kaspersky が 20 年間継続している脅威の研究によって判明したマルウェアのふるまいに関する知識を取り込んでいます。当社が毎日 35 万件以上の新たな悪意のあるオブジェクトを検知して、業界をリードするセキュリティソリューションを提供できるのも、この知識があるからです。

カスペルスキークラウドサンドボックスは、お客様の脅威インテリジェンスワークフローを完結させる最後のコンポーネントです。脅威情報ルックアップが URL、ドメイン、IP アドレス、ファイルハッシュ値、脅威名、統計的データまたはふるまいデータ、WHOIS データ、DNS データなどに関する最新の脅威インテリジェンスの詳細情報を引き出すものであるのに対して、クラウドサンドボックスは、その知識を、分析対象サンプルによって生成された IOC に関連付けるものです。

このサービスによって、効果的に複雑なインシデント調査を実施して、脅威の特性について即座に理解し、詳細情報を確認しながらそれぞれを結び付けて、相互に関連する脅威の兆候を明らかにすることができます。

インスペクションは、特に対象が多段階攻撃である場合に非常にリソースを消費する作業です。カスペルスキークラウドサンドボックスは、インシデント対応とフォレンジック分析のための理想的なツールであり、コストのかかるアプライアンスの購入もシステムリソースに関する懸念も不要で、自動的にファイルを処理できるスケーラビリティを備えています。

レポートに含まれるもの

- **エグゼクティブサマリー:**
  - 脅威の緊急性や、脆弱性の重大度の評価
  - 脅威や脆弱性の説明
  - タイムライン
  - 地域、国、業界での分布状況
  - リスク軽減に関する推奨事項
- **分析結果の詳細な説明**
- **脅威に関するレポート:**
  - 攻撃方法
  - 使用されるエクスプロイト(ある場合)
  - マルウェアの説明
  - C&C インフラストラクチャおよび手順の説明
  - 攻撃対象者分析
  - データ流出分析
  - 要因
- **脆弱性に関するレポート:**
  - 公開されているエクスプロイトの利用可能性
  - 実際の攻撃におけるエクスプロイトの形跡
  - 脆弱性を特定するための手法
  - 脆弱性の悪用を可能にするセキュリティ上の問題に関する技術的分析
  - 考えられる攻撃経路(他の脆弱性やセキュリティ上の欠陥と合わせて利用される可能性あり)
  - 影響を受ける製品や製品バージョンの評価
  - 地域、国、業界への脆弱な製品の展開に関する予測
- **まとめ**
- **付録**
  技術的分析、重要な IOC、その他の関連する情報

産業用制御システム(ICS)脅威インテリジェンスレポート

カスペルスキー ICS 脅威インテリジェンスレポートでは、産業組織を標的とした悪意ある活動に関する詳細なインテリジェンスを提供し、注意を喚起するとともに、一般的な産業用制御システム(ICS)および基盤技術において発見された脆弱性に関する情報を提供します。レポートは Web ベースのポータルに掲載され、すぐに利用することができます。

提供されるレポートのタイプ

1. **APT レポート。**産業組織を標的とした新たな APT 活動および大量攻撃活動に関する情報、ならびに現在進行中の脅威に関する最新情報をレポートします。
2. **脅威の状況。**地域、国、業界に特有の情報も含め、脅威に対する ICS のセキュリティレベルおよび ICS のリスクに影響するような、新たに発見された重大な要素など、ICS への脅威の状況に関する大きな変化をレポートします。
3. **発見された脆弱性。**ICS、産業用 IoT、およびさまざまな業種のインフラストラクチャにおいて一般的に使用されている製品で Kaspersky が特定した脆弱性についてレポートします。
4. **脆弱性の分析と軽減。**インフラストラクチャの脆弱性を特定し、軽減するため、Kaspersky のエキスパートからの実用的な推奨アクションを提供します。

脅威インテリジェンスデータを使ってできること

レポートされた脅威を**検出および回避**することで、ソフトウェアやハードウェアコンポーネントなど重要な資産を保護し、技術プロセスの安全性と継続的な運用を確保します。

産業環境においてユーザーが特定した悪意ある活動や疑わしい活動と、Kaspersky のリサーチ結果を**照らし合わせる**ことで、ある活動が、レポートされた悪意ある活動によるものであることを確認し、その脅威を特定し、問題に早急に対応します。

脆弱性の範囲および重大度に関する正確な評価に基づいて産業用制御システムの**脆弱性評価を実施**することで、パッチ管理や Kaspersky が推奨する脅威回避策の実施を、情報に基づいて意思決定できます。

攻撃に使用される戦術、技術、手順、新しく発見された脆弱性、およびその他の脅威状況の重要な変化に関する情報を**活用**でき、以下が可能になります。

- レポートされた脅威やその他の同様の脅威によるリスクを特定および評価すること。
- 生産の安全性および技術プロセスの継続性を確保できるように、産業用インフラストラクチャに対する変更を計画および設計すること。
- 実際に発生したケースに対する分析に基づいてセキュリティ認識活動を実施し、スタッフのトレーニングシナリオを作成したり、レッドチーム(攻撃側)対ブルーチーム(防御側)の演習プランを策定したりすること。
- サイバーセキュリティへの投資およびオペレーションの回復力確保について、情報に基づく戦略的な意思決定を行うこと。

サービスのメリット

特典

- **非公開の情報：**サイバーセキュリティの担当者はサイバーセキュリティ活動を計画および実施するために不可欠となる情報（公開されていないものも含め）を取得することができます。
- まだリサーチや調査が完了しておらず、情報が公開されていない段階でも、**脅威に関する技術的な情報に早期にアクセスできます**。
- 悪意ある側に悪用されるリスクを回避するため、公のドメインには掲載されない可能性のある情報に、**特別にアクセスできます**（脆弱性を実証するために製造元のみに共有されるソフトウェアの情報は含まれないことがあります）。

実用性

- **新たな脅威への迅速な対応：**提供される情報およびツールを活用することで、新たな脅威や脆弱性に迅速に対応でき、高度な攻撃や既知の経路からの攻撃に関するリスクを軽減できます。
- ICS サイバーセキュリティのオペレーションのための技術的情報：このサービスでは、自動化ツールと連携して、脆弱性評価、インシデント検出、対応および調査活動に使用できる、侵害の痕跡（IOC）が提供されます。

完全性

- **過去の分析：**サービス期間中は、以前に発行されたレポートも閲覧できます。
- **悪意ある活動への継続的な監視：**調査中の実用的な情報のほか、TTP の変化や新たに検出されたツールセットの IOC といった新しい発見事項に関する最新情報を提供しています。

容易

- **自動：**レポート情報は、自動化されたサイバーセキュリティプロセスに組み込むことができます。
- **複数の業界標準に対応：**IOC は、OpenIOC、STIX、YARA、SNORT といった形式で提供されます。

サイバー脅威に関する最新情報（英語）：www.securelist.com
大企業向けセキュリティに関する情報：www.kaspersky.co.jp/enterprise-security

www.kaspersky.co.jp

kaspersky BRING ON THE FUTURE