Kaspersky Threat Intelligence

kaspersky BRING ON THE FUTURE

課題

常に進化を続ける IT 上のセキュリティ脅威を追跡、分析してその被害を軽減することは、大変な作業です。あらゆる業種の企業は、IT セキュリティの脅威に関連するリスクの管理に必要な、最新の重要データの不足という事態に直面しています。

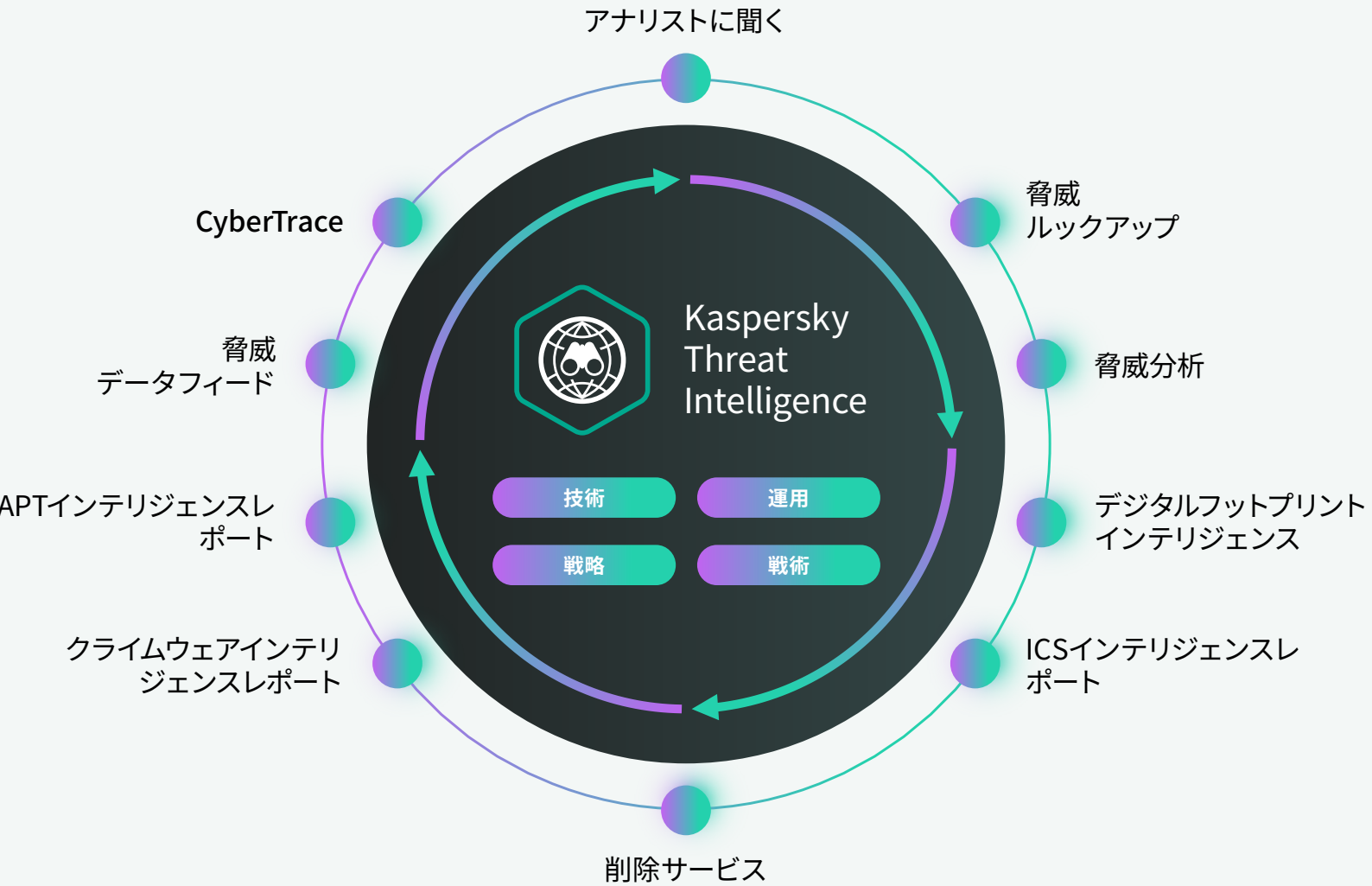
Kaspersky Threat Intelligence

カスペルスキーの脅威インテリジェンスにより、世界最高レベルのリサーチャー/アナリストのチームが提供する、サイバー脅威を軽減するために必要な情報にアクセスできます。

カスペルスキーは、サイバーセキュリティのあらゆる面に関する知識や経験、高度なインテリジェンスにより、INTERPOLや主要なCERTなどの世界有数の法執行機関や政府機関の信頼されるパートナーとなりました。Kaspersky Threat Intelligence をご利用いただきますと、技術的・戦術的・運用的・戦略的な脅威インテリジェンスに即座にアクセスできるようになります。

Kaspersky Threat Intelligenceポートフォリオには、以下のものがあります。

Threat Data Feeds、CyberTrace（脅威インテリジェンスプラットフォーム）、Threat Lookup、Threat Analysis（Cloud SandboxおよびCloud Threat Attribution Engine）、さまざまなThreat Intelligence Reportingオプション、およびオンデマンドで脅威インテリジェンスの専門知識を提供するサービス。



Kaspersky Threat Data Feeds

サイバー攻撃は日々発生しています。セキュリティの防御を突破して組織への侵入を企てるサイバー脅威は、ますます頻繁に、かつ複雑で秘密裡に行われるようになっています。攻撃者は、企業活動を妨害したり顧客に被害を与えることを目的として、巧みな侵入キルチェーン、攻撃活動、カスタマイズされた戦術/技術/手順（TTPs）を使用しています。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。

不審で危険なIP、URL、およびファイルハッシュ値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既存のセキュリティシステム（SIEM、SOAR、脅威インテリジェンスプラットフォームなど）に統合することで、セキュリティチームは初期アラートトリアージプロセスを自動化し、トリアージ専門家に十分なコンテキストを提供し、調査が必要であるか、またはさらなる調査と対応のためにインシデント対応チームにエスカレートする必要があるアラートを直ちに特定できます。

- IPレピュテーションのフィード
- ハッシュのフィード（WIN/*nix/MacOS/AndroidOS/iOS）
- URLフィード（悪意のある/フィッシング/C&C）
- ランサムウェアURLフィード
- APT IOCフィード
- 脆弱性フィード
- パッシブDNS（pDNS）フィード
- IoT URLフィード
- 許可リストフィード
- ICSハッシュのフィード
- その他

Kaspersky Threat Data Feeds

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、アクセス頻度など）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」という疑問に答えて攻撃者を特定することがより簡単になり、迅速な意思決定を行い、アクションを起こすことができます。

主な強化ポイント

データフィードは、世界中の知見に基づいてリアルタイムで自動的に生成され（Kaspersky Security Networkは、213を超える国々の膨大な数のエンドユーザーをカバーするすべてのインターネットトラフィックのかなりの割合を可視化します）、高い検知率と精度を提供します。

実装のしやすさ。カスペルスキーが提供する補助的なドキュメント、サンプル、技術専任の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。

世界中のセキュリティアナリスト、世界的に著名なGReATや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。

収集とデータ処理

データフィードは、Kaspersky Security Network や当社独自の Web クローラー、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、類似性ツール、ふるまいプロファイリングなど、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。

HTTPS、TAXII、アドホックな配信メカニズムを介したシンプルかつ軽量な普及フォーマット（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組み込みを手軽に実現します。

すべてのフィードは、優れたフォールトトレランスインフラストラクチャにより生成、監視され、継続的な可用性を維持します。

誤検知だらけのデータフィードには価値がないため、フィードの配信前にさまざまな検証とフィルタリング処理を実施して100%精査済みデータを配信します。

メリット

絶えず更新される脅威存在痕跡（IOC）情報と実用的なコンテキスト情報により、ネットワーク防御ソリューション（SIEM、ファイアウォール、IPS/IDS、セキュリティプロキシ、DNSソリューション、APT対策）を強化し、サイバー攻撃に対する洞察を提供し、攻撃者の目的、能力、標的を明らかにします。主なSIEM製品（HP ArcSight、IBM QRadar、Splunkなど）およびTIプラットフォームが完全にサポートされています

初期トリアージプロセスを自動化することで、お客様のインシデント対応およびフォレンジック能力を改善、促進し、セキュリティアナリストに十分なコンテキスト情報を提供し、さらなる調査と対応のために調査が必要であるか、またはインシデント対応チームにエスカレートする必要があるアラートを直ちに特定します。

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。感染した資産をすばやく検知して、ブランドレピュテーションを保護し、競争優位を維持し、事業機会を確保します。

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。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。

Kaspersky CyberTrace

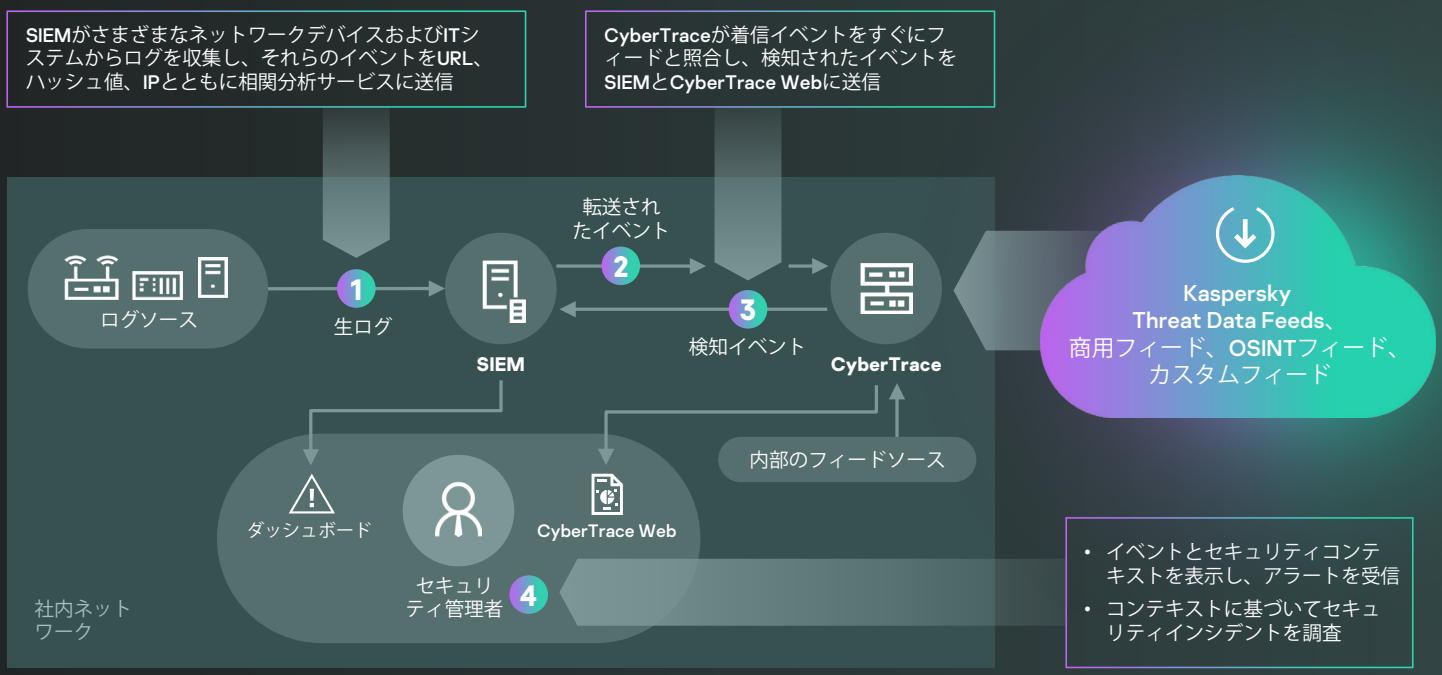
最新の機械可読の脅威インテリジェンスをSIEMシステムなどの既存のセキュリティコントロールに統合することで、セキュリティオペレーションセンターは初期のトリアージプロセスを自動化できます。また、十分なコンテキストに基づくセキュリティ分析が可能になるので、調査が必要であるか、またはさらなる調査と対応のためにインシデント対応チームにエスカレートする必要があるアラートを直ちに特定できるようになります。しかし、脅威データフィードの数や、使用可能な脅威インテリジェンスの供給元が増え続けるなか、どの情報が自社に適しているかを判断するのは容易なことではありません。脅威インテリジェンスにはさまざまな形式があり、莫大な数の侵入の痕跡（IoC）が含まれているため、SIEMやネットワークセキュリティコントロールで処理するのは困難です。

Kaspersky CyberTraceは、脅威データフィードとSIEMソリューションのシームレスな統合を可能にする脅威インテリジェンスプラットフォームです。このプラットフォームは、アナリストが既存のセキュリティ業務のワークフローで脅威インテリジェンスを効果的に活用するために役立ちます。また、任意の脅威インテリジェンスフィード（カスペルスキー、その他の製造元、OSINT、または独自の顧客フィード）をJSON、STIX、XML、およびCSV形式に統合し、多数のSIEMソリューションやログソースとの設定不要の統合をサポートします。

Kaspersky CyberTraceは、脅威インテリジェンスを効率的に運用可能にするための一連の製品を提供します。

- 全文検索が可能な指標データベースと高度な検索クエリーによる検索能力により、コンテキストフィールドを含めて、全指標フィールドへの複雑な検索を実行できます。
- 各指標についての詳細情報のページから、さらに詳しい分析結果を取得できます。各ページには、1つの指標について、すべての脅威インテリジェンスサプライヤーからの情報が表示され（重複するものは排除）、アナリストが脅威についてコメントしたり、その指標に関する内部の脅威インテリジェンスを追加したりすることができます。
- 調査グラフを使うと、CyberTrace内に保管されたデータや検知を視覚的に調査し、脅威に共通する特徴を発見することができるようになります。
- 指標エクスポート機能は、ポリシーリスト（ブロックリスト）のようなセキュリティコントロールに設定されている指標のエクスポートや、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の間での脅威データの共有に対応しています。
- IoC のタグ付けをすることで管理が容易になります。あらゆるタグを作成して、そのウエイト （重要度） を指定できます。また、そのタグを IoC を手動でタグ付けするのに使うこともできます。これらのタグやウエイトに基づいてIoCを分類、フィルタリングすることもできます。
- 履歴相関機能（レトロスキャン）では、過去に検査済みのイベントの観測データに最新のフィードを適用して分析し、以前は発見されなかった脅威を見つけることができます。
- フィルターはSIEMソリューションに検知イベントを送信し、ソリューションや分析に対する負荷を軽減します。
- マルチテナント機能は、MSSPや大企業のユースケースをサポートします。
- 統合フィードの効果を測定するフィード利用統計やフィードインターセクションマトリクスは、最も重要な脅威インテリジェンスサプライヤーを選択する際に役立つ機能です。
- HTTP RestAPIを使用した脅威インテリジェンスのルックアップと管理が可能です。

ツールは内部プロセスを使用して着信データの解析と照合を行うので、SIEMのワークロードが大幅に軽減されます。Kaspersky CyberTraceは受信したログやイベントを解析して、結果データをすぐにフィードと照合し、脅威を検知した場合は独自のアラートを生成します。ソリューション統合のおおまかなアーキテクチャを以下の図に示します。



Kaspersky CyberTraceおよびKaspersky Threat Data Feedsを使用すると、セキュリティアナリストは以下のことを実行できます。

- 大量のセキュリティアラートを効率的に抽出し、優先順位を付ける
- トリアージや初期対応プロセスを向上させ、促進させる
- 企業にとって重大なアラートを直ちに特定し、IRチームにエスカレートする内容に関して、詳細な情報に基づいた決定を行う
- インテリジェンスに基づいてプロアクティブな防御を構築する

Kaspersky Threat Lookup

サイバー犯罪に国境はなく、技術力は急速に向上しています。サイバー犯罪者はダークウェブのリソースを使用して標的を脅かすことで、攻撃はますます巧妙になります。セキュリティの防御を突破するために新たな方法を試行するサイバー脅威は、ますますひんぱんに、かつ複雑で秘密裡に行われるようになっています。攻撃者は企業活動の妨害、情報資産の窃取やその取引先への損害などを目的として、巧みなキルチェーンと標的ごとにカスタマイズした戦術: Tactics、テクニック: Techniques、手順: Procedures（TTPs）を使用します。

Kaspersky Threat Lookupは、さまざまなサイバー脅威やそれらの関係についてカスペルスキーが得た知識のすべてを、単一の強力なWebサービスに一元化しています。目的は、セキュリティチームにできる限り多くのデータを提供し、組織が影響を受ける前にサイバー攻撃を防ぐことです。URL、ドメイン、IPアドレス、ファイルハッシュ値、脅威名、統計/ふるまいのデータ、WHOIS/DNSデータ、ファイル属性、地理位置情報データ、ダウンロードチェーン、タイムスタンプなど、最新の詳細な脅威インテリジェンスがプラットフォームで取得されます。これにより新たな脅威を世界規模で可視化し、組織を保護するとともに、インシデント対応能力を大幅に高めることができます。

主な強化ポイント

信頼できるインテリジェンス: Kaspersky Threat Lookupは、実用的なコンテキストで強化された、信頼性の高い脅威インテリジェンスデータを提供することができます。カスペルスキーは、アンチマルウェアテスト[1]の分野をリードし、誤検知がほぼゼロの最高レベルの検知率を提供することで、比類なきセキュリティインテリジェンス品質を実証します。

脅威ハンティング: 攻撃を事前に防ぎ、検知し、対処することで、その影響や頻発を最小限に抑えます。攻撃をできるだけ早く追跡し、積極的に排除します。脅威を早期発見すれば、損害を抑え、速やかに修正を実行し、ネットワーク運用をすぐに通常どおりに戻すことができます。

インシデント調査: 調査グラフは、Threat Lookupに保存されたデータと検知を視覚的に確認できるようにすることで、インシデント調査を促進します。URL、ドメイン、IP、ファイル、およびその他のコンテキスト間の関係をグラフィカルに表現するため、インシデントの全容を理解し、その根本原因を特定できます。

マスター検索: 単一の強力なインターフェイスで、すべてのアクティブな脅威インテリジェンス製品と外部リソース（OSINT IoC、ダークウェブおよび表層ウェブを含む）の情報を検索します。

簡単に使用できるWebインターフェイスやRESTful API: 必要に応じて、Webインターフェイスから（Webブラウザを介して）、またはシンプルなRESTful APIにアクセスして、サービスをマニュアルモードで使用できます。

さまざまなエクスポート形式: IOC（侵害の痕跡）または実用的なコンテキストを、広く使用されているより調整された機械可読の共有形式（STIX、OpenIOC、JSON、Yara、Snort、CSV）にエクスポートして、脅威インテリジェンスからメリットを得たり、運用ワークフローを自動化したり、SIEMなどのセキュリティコントロールと統合したりできます。

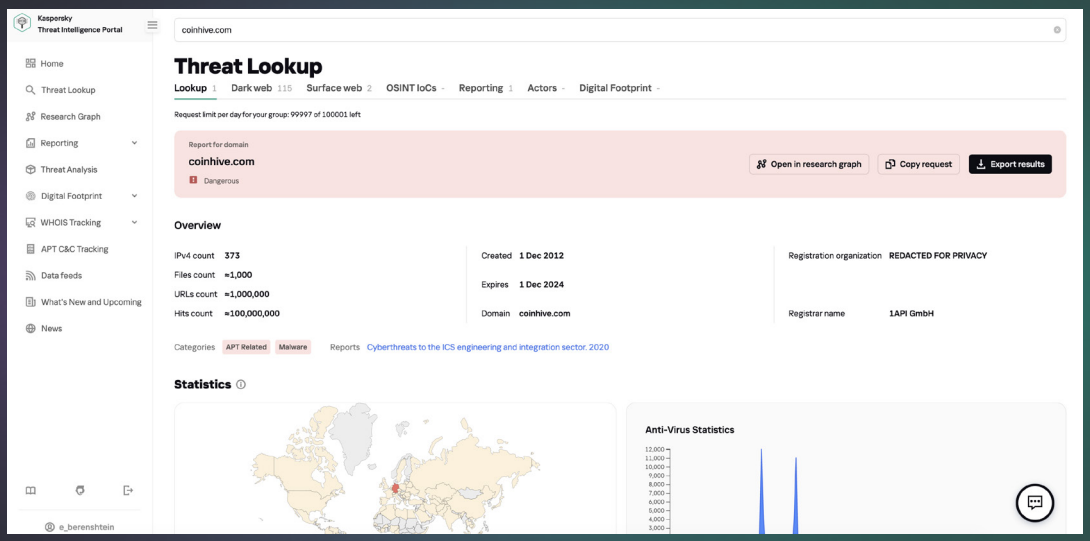
メリット

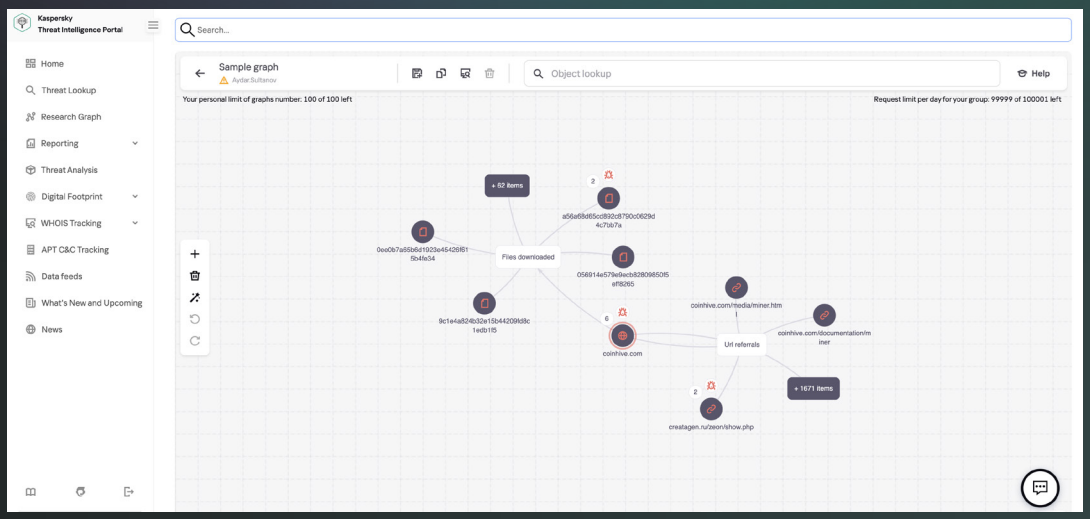
高度に検証された脅威のコンテキストを使用して、脅威の兆候について詳細に調査することで、攻撃に優先順位を付け、ビジネスにとって極めて大きなリスクとなる脅威の緩和に集中できるようにします。

ホストやネットワーク上のセキュリティインシデントをより効率的/効果的に診断、分析し、未知の脅威に対する内部システムからの信号に優先順位を付けます。

インシデント対応機能と脅威ハンティング機能を強化し、重大なシステムやデータが侵害される前にキルチェーンを破壊します。

[1]kaspersky.com/top3





以下のことが実行できます

Webベースのインターフェイス、またはRESTful APIを介した脅威の兆候を検索します

証明書、一般的に使用される名前、ファイルパス、または関連するURLなどの詳細情報を調査して、新たな疑わしいオブジェクトを発見します

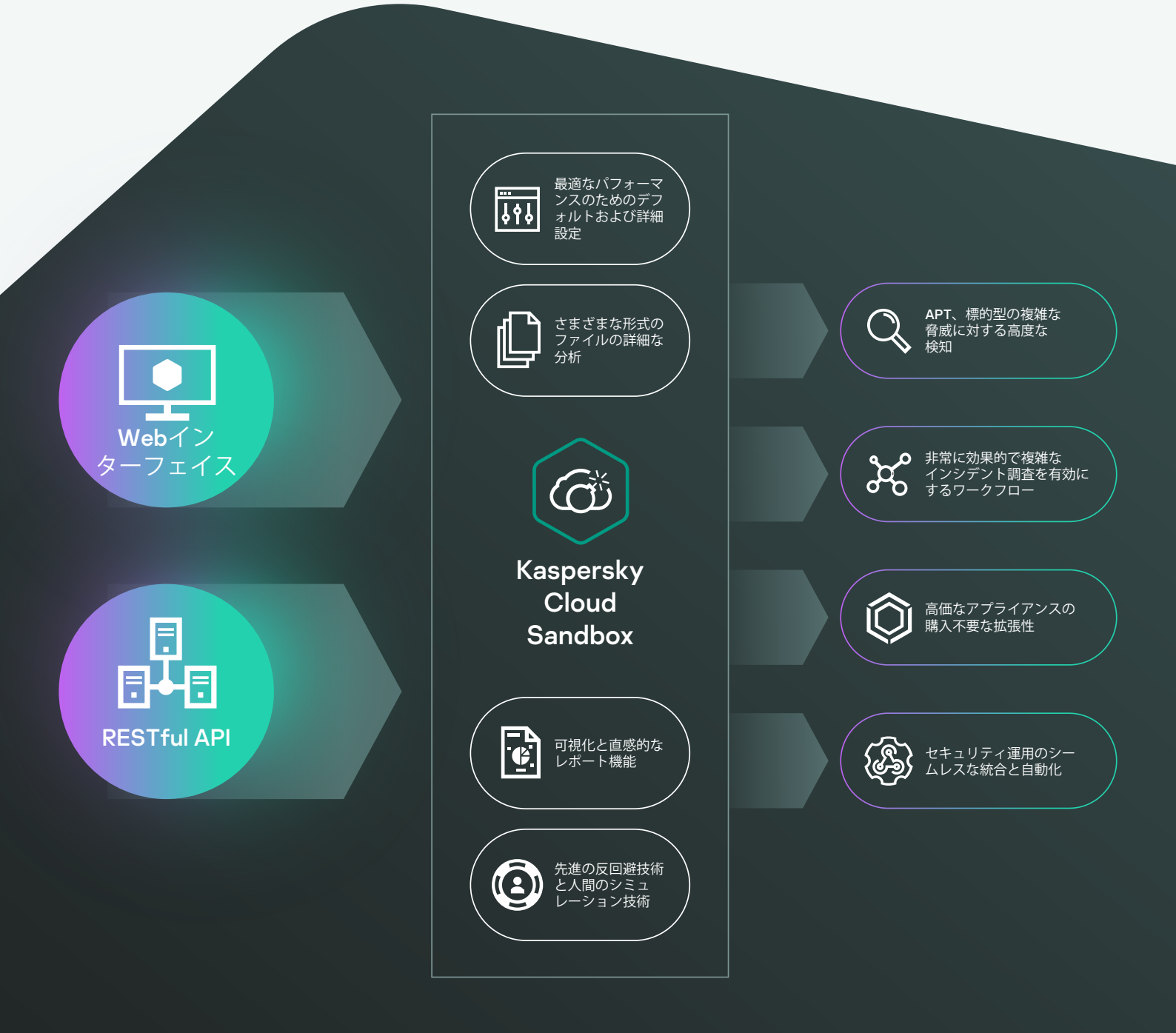
発見したオブジェクトが拡散されているのか、固有のものかチェックします

オブジェクトが悪意あるものとして処理される理由を理解できます

Kaspersky Cloud Sandbox

従来型のAVツールを使用して、現在の標的型攻撃を防ぐことができます。アンチウィルスエンジンは、既知の脅威とその亜種のみを防ぐことができます。一方、巧妙な攻撃者は、自動検知を逃れるために自在にあらゆる方法を駆使します。情報セキュリティインシデントからの被害は急増し続けており、重大な損害を受ける前に、迅速に対応し、脅威に対抗す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、情報処理能力を駆使した意思決定を行うと同時に、プロセスメモリやネットワークアクティビティなどを分析することは、今日の洗練された標的型攻撃やカスタマイズされた脅威を理解するための最適なアプローチとなります。統計データに最新の変更されたマルウェアの情報が欠落していても、強力なツールであるサンドボックス技術により、ファイルサンプルの発生源の調査、ふるまい分析に基づいたIOCの収集、未確認の悪意あるオブジェクトの検知が可能になります。



包括的なレポート

- DLLの読み込みと実行
- ドメイン名やIPアドレスとの外部接続
- 作成、変更、削除されたファイル
- 明らかにされたすべてのIOC（侵害の痕跡）に関する実用的なコンテキストを含む詳細な脅威インテリジェンス
- プロセスメモリダンプおよびネットワークトラフィックダンプ（PCAP）
- HTTPおよびDNSのリクエストとレスポンス
- 作成された相互拡張（相互排除）
- RESTful API
- 修正、作成されたレジストリキー
- 実行ファイルが作成したプロセス
- スクリーンショット
- **その他**

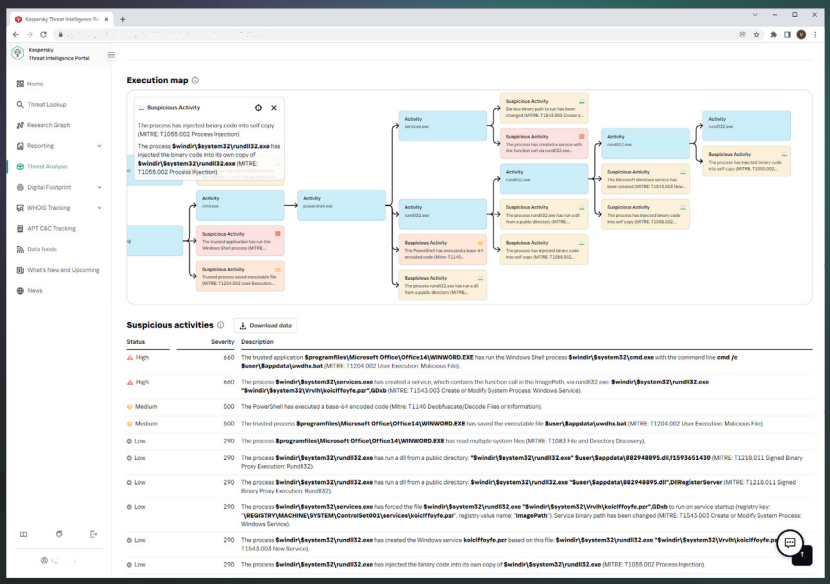
事前対策による脅威の検知と軽減

マルウェアはその実行が検知されないようにするために、さまざまな方法を使用します。システムが必要なパラメータを満たしていない場合、悪意あるプログラムはほぼ確実に自分自身を破壊し、痕跡を残すことはありません。悪意のあるコードの実行に対して、サンドボックス環境はエンドユーザーの通常のふるまいを正確に装うことができる必要があります。

Kaspersky Cloud Sandboxは、ペタバイトの統計データ（Kaspersky Security Networkとその他の専用システムによる）、ふるまい分析、極めて堅固な反回避技術から収集した脅威インテリジェンスを、自動クリッカー、ドキュメントのスクロール、およびダミープロセスなどの人間をシミュレートする技術と組み合わせたハイブリッドアプローチを提供します。

この製品は、社内サンドボックスラボで開発され、10年以上にわたり進化を続けています。技術には、20年を超える脅威の研究から取得したマルウェアのふるまいに関するすべての知識が組み込まれています。これにより、毎日36万を超える悪意のある新しいオブジェクトを検知して、お客様に業界トップレベルのセキュリティソリューションを提供します。

当社のThreat Intelligence Portalの一部として、Cloud Sandboxは脅威インテリジェンスワークフローにおいて重要なコンポーネントです。Threat Lookup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/ふるまいのデータ、WHOIS/DNSデータなど、最新の詳細なインテリジェンスを取得し、Cloud Sandboxはその知識を分析サンプルから生成されたIOCとリンクします。



非常に効果的で複雑なインシデント調査を実行して、脅威の性質を迅速に把握し、相互に関連する脅威の兆候について掘り下げながら、それらを結びつけていくことが可能です。

検証では、特にマルチステージ攻撃の場合に、リソースを大量に消費します。Kaspersky Cloud Research Sandboxは、インシデント対応やフォレンジックアクティビティを向上させ、高価なアプライアンスを購入したり、システムリソースを気にしたりすることなく、ファイルを自動処理するための拡張性が提供されます。

カスペルスキーAPTインテリジェンスレポート

カスペルスキーのAPTインテリジェンスレポートのお客様は、弊社が実施した調査結果および確認された情報（確認されたすべてのAPTの完全な技術データ（さまざまな形式）や、公表されない脅威に関するデータなど）に継続的にアクセスすることができます。レポートにはエグゼクティブサマリーが含まれており、経営幹部レベル向けのわかりやすい情報を提供します。関連するAPTを説明し、関連するIOCとYARAルールを含むAPTの詳細な技術説明も含まれています。これにより、セキュリティリサーチャー、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、およびAPTリサーチャーに脅威に対してすばやく正確に対応できる実用的なデータを提供できます。

弊社の専門家は、サイバー犯罪グループの戦術で検知した変化を直ちにお客様に通知します。セキュリティ防御におけるさらなる強力な調査および分析コンポーネントであるKasperskyの完全なAPTレポートデータベースにもアクセスできます。

メリット

MITRE ATT&CK
レポートで説明されているすべてのTTPsは、MITRE ATT&CKにマッピングされ、対応するセキュリティ監視のユースケースを開発して優先順位を付け、ギャップ分析を実行し、関連するTTPsに対する現在の防御をテストすることで、検知と応答を向上させることができます。

非公開APTの情報
さまざまな理由により、すべての有名な脅威が既知になっているとは限りません。しかし、弊社はそれらすべての脅威をお客様と共有します。

権限付きアクセス
一般公開する前に、調査中に最新の脅威に関する技術的説明を受信

遡及的分析
サブスクリプション中は、以前発行されたすべてのプライベートレポートにアクセスできます。

技術データへのアクセス
openIOCやSTIXなどの標準的な形式で使用可能なIOCの詳細なリスト、および弊社のYARAルールへのアクセスを含む

攻撃者のプロファイル
発生源となる疑わしい国と主なアクティビティ、使用されたマルウェアファミリー、対象となる産業と地域、使用されたすべてのTTPsの説明（MITRE ATT&CKへのマッピングあり）を含む

継続的なAPT活動のモニタリング
APT配信の情報、IOC、コマンド&コントロール用インフラなどの調査中に、実用的な情報にアクセス可能

RESTful API
セキュリティワークフローのシームレスな統合と自動化

Kaspersky Digital Footprint Intelligence

ビジネスが発展するにつれて、IT環境はより複雑になり、配信する情報も増え、直接管理せずに、または所有権を使用せずに、広く配信されたデジタルプレゼンスを保護するという課題が現れます。動的で相互接続された環境により、企業は大きなメリットを得ることができます。ただし、相互接続が増え続けることにより、攻撃対象も広がります。攻撃者が巧妙になるにつれ、組織のオンラインプレゼンスの状態を正確に把握するだけでなく、その変化も追跡することが重要です。そして、デジタル資産の漏洩に関する最新情報に対応する必要があります。

組織はセキュリティ運用において、さまざまなセキュリティツールを使用していますが、それでもデジタル脅威は現れます。このため、ダークウェブフォーラムに存在するサイバー犯罪者のインサイダー活動、計画、攻撃スキームを検知/軽減する機能が必要です。セキュリティアナリストが企業のリソースに対する攻撃者の視点を調査し、攻撃者が利用する潜在的な攻撃ベクトルを迅速に検出し、必要に応じて防御を調整できるようにするために、カスペルスキーはKaspersky Digital Footprint Intelligenceを作成しました。

組織に対する攻撃を開始する最適な方法とは？最も効率的な攻撃方法とは？ビジネスを標的にしている攻撃者が利用する情報とは？知らぬ間にインフラが侵害されていませんか？

Kaspersky Digital Footprint Intelligenceがこれらの質問にお答えします。当社の専門家がお客様に対する攻撃の現状の全体像を提示し、悪用されやすい弱点を特定して、過去や現在の攻撃、さらに計画されている攻撃のエビデンスを明らかにします。

製品により、以下が提供されます。

- 非侵入型の方法を使用したネットワーク境界インベントリ: 攻撃の入り口となり得るお客様のネットワークリソースと公開サービスを特定（境界に意図せずに残された管理インターフェイス、設定ミスのサービス、デバイスのインターフェイスなど）。
- 既存の脆弱性に対するカスタマイズされた分析: CVSSベーススコアに基づいた詳細なスコア計算と包括的なリスク評価、パブリックエクスプロイトの可用性、ペネトレーションテストの経験、ネットワークリソースの位置（ホスト/インフラストラクチャ）。
- アクティブな標的型攻撃や計画されている攻撃、企業、産業、事業地域を標的にしたAPT活動の特定、開始、分析。
- 企業、パートナー、利用者を標的にした脅威の特定。影響を受けたシステムが攻撃に使用されます。
- Pastebinサイト、パブリックフォーラム、ブログ、ショートメッセージチャンネル、制限されたアンダーグラウンドオンラインフォーラムやコミュニティを慎重に監視し、侵害されたアカウント、情報漏えい、または計画されている組織に対する攻撃を発見する。

主な強化ポイント

Kaspersky Digital Footprint Intelligenceは、表層ウェブ、ディープウェブ、ダークウェブの自動/手動分析と組み合わされたOSINT技術と、内部カスペルスキーのナレッジベースを使用して、対応可能な対策と推奨事項を提供します。

製品はKaspersky Threat Intelligence Portalから入手できます。年間のリアルタイム脅威アラートが記載された四半期レポートを購入するか、6か月間アクティブなアラートが記載された単一のレポートを購入できます。

表層/ダークウェブを検索し、資産に脅威をもたらし、制限されたアンダーグラウンドのコミュニティやフォーラムに機密データを漏洩させるグローバルセキュリティイベントに関するほぼリアルタイムの情報を提供します。年間ライセンスは、外部リソースやカスペルスキーのナレッジベースを1日あたり50件検索できます。

Kaspersky Digital Footprint Intelligenceは、Kaspersky Takedown Serviceを使用して単一のソリューションを形成します。年間ライセンスでは、悪意のあるドメインやフィッシングドメインの削除を年に10回リクエストできます。

Kaspersky ICS Threat Intelligenceレポート

Kaspersky ICS Threat Intelligenceレポートは、産業組織を標的にした悪意のある活動に関する綿密なインテリジェンスを提供し、それらに対する認識を深めることができるようにします。さらに、最も普及している産業制御システムや基本技術で発見された脆弱性に関する情報を提供します。Webベースのポータルからレポートが配信されるため、すぐにサービスの使用を開始できます。

サブスクリプションに含まれるレポート

1. **APTレポート。**産業組織を標的にした新しいＡＰＴと大量の攻撃活動に関するレポート、およびアクティブな脅威に関する最新情報。
2. **脅威の状況。**産業制御システムの脅威の状況の大きな変化、ICSセキュリティレベルに影響する新たに発見された重要な要素、脅威に対するICSの漏洩に関するレポート（地域、国、産業固有の情報を含む）。
3. **脆弱性の発見。**産業制御システムで使用されている最も一般的な製品、IIoT（Industrial Internet Of Things）、およびさまざまな産業のインフラストラクチャにおいてカスペルスキーが特定した脆弱性に関するレポート。
4. **脆弱性分析と軽減。**弊社のアドバイザリは、お使いのインフラにある脆弱性を特定し、軽減するために、カスペルスキーのエキスパートからの実用的な推奨事項を提供します。

脅威インテリジェンスデータにより以下のことが実行できます。

検知と防止

報告された脅威を検知および防止して、ソフトウェアおよびハードウェアコンポーネントを含む重要な資産を保護し、技術プロセスの安全性と継続性を確保します

関連付け

産業向けの環境で検知した悪意のある不審な活動をカスペルスキーの調査結果と関連付けることで、報告された悪意のある活動が検知の要因であると断定し、脅威を特定して、インシデントに迅速に対応します

実行

脆弱性の範囲と重大度の正確な評価に基づいた産業環境と資産の脆弱性評価を実行し、パッチ管理について情報に基づいた決定を行い、カスペルスキーが推奨するその他の予防策を実装します

活用

攻撃技術、戦略、手順に関する情報、最近発見された脆弱性、およびその他の重要な脅威の状況の変化に関する情報を活用して、以下のことを実行します

- 報告された脅威やその他の同様の脅威により発生するリスクの特定と評価
- 産業用インフラストラクチャの変更を計画、設計し、生産の安全性と技術プロセスの継続性を確保
- 実世界の事例分析に基づいたセキュリティ意識活動を実行し、個人用トレーニングシナリオを作成し、チーム対抗の演習を策定
- サイバーセキュリティに投資し、運用の回復力を確保するための、情報に基づいた戦略的決定

脅威の継続的な調査

脅威の継続的な調査を通じて、カスペルスキーは攻撃者やサイバー犯罪者が出入りする世界中のクローズドのコミュニティやダークウェブの犯罪者フォーラムを発見、侵入、監視しています。カスペルスキーのアナリストは、このアクセスを利用して、もっとも有害で悪名高い脅威のほか、特定の組織を挟撃にした脅威を率先して検出・調査できます。

カペルスキー、アナリストに聞く

サイバー犯罪者は企業を標的とする洗練された攻撃手法の開発を続けています。急激に変化する不安定な今日の脅威状況では、ますます俊敏化するサイバー犯罪技術が利用されています。企業は、非マルウェア攻撃、ファイルレス攻撃、自給自足/環境寄生型攻撃、ゼロデイ脆弱性攻撃や、それらすべてを組み合わせた複合的な脅威、APT に類似した攻撃、標的型攻撃による複雑なインシデントに直面しています。

業務に深刻な被害をもたらすサイバー攻撃が蔓延する中、以前にも増してサイバーセキュリティの専門家が重要になっていますが、このような人材を見つけて確保するのは簡単なことではありません。信頼できるサイバーセキュリティチームが社内にいるとしても、高度な脅威との戦いに単独で挑むことを常に期待することはできません。**社外のエキスパートの支援を要請できる体制が必要になります。**外部の専門知識に頼ることで、複雑な攻撃やAPT攻撃に利用されるおそれのある攻撃ルートを割り出し、それを排除することができる根本的な対策に関して、実用的なアドバイスが得られることがあります。

Ask the Analyst の成果物

(統合されたリクエストベースのサブスクリプション)

Kaspersky Ask the Analyst サービスは、カスペルスキーの脅威インテリジェンスポートフォリオを拡張するもので、お客様が現在直面している脅威や関心をお持ちの脅威に関するガイダンスやインサイトをお求めいただけます。このサービスでは、カスペルスキーの高度な脅威インテリジェンス機能と調査機能をそれぞれの企業に固有のニーズに合わせて調整することで、お客様の組織を標的とする脅威に対するレジリエントな防御態勢の構築を可能にします。

APT とクライムウェア

公開されたレポートや継続中の調査に関する追加情報(APT またはクライムウェアのインテリジェントレポートに付加) [1]

マルウェア解析

- マルウェアのサンプル解析
- その他の是正措置に関する推奨事項

脅威、脆弱性、関連する IoC に関する説明

- 特定のマルウェアファミリーに関する基本的な説明
- 脅威に関する追加のコンテキスト(関連するハッシュ、URL、CnC など)
- 特定の脆弱性に関する情報(重大度や、カスペルスキー製品が対応できる防御メカニズム)

ダークウェブインテリジェンス[2]

- 特定のアーティファクト、IP アドレス、ドメイン名、ファイル名、メールアドレス、リンク、画像についてダークウェブで調査
- 情報の検索と分析

ICS関連リクエスト

- 公開レポートに関する追加情報
- ICS脆弱性情報
- 地域/産業ごとのICS脅威統計および傾向
- 規制または基準に関するICSマルウェア分析情報

[1] APT やクライムウェアに関するインテリジェンスレポートを現在利用しているお客様のみ

[2] Kaspersky Digital Footprint Intelligence サブスクリプションに既に含まれています

本サービスのメリット

専門知識を補足

業界のエキスパートにオンデマンドで相談できるため、希少なフルタイムの専門家を探し出して採用するための投資が不要

調査を加速

調整された詳細なコンテキスト情報に基づいてインシデントのスコーピングと優先順位付けを効果的に実施

迅速に対応

カスペルスキーのガイダンスに従って脅威と脆弱性に迅速に対応し、既知の経路からの攻撃をブロック

仕組み

Kaspersky Ask the Analyst は別個にご購入いただくことも、他の脅威インテリジェンスサービスの付加サービスとしてご購入いただくこともできます。

企業のお客様のためのサポートポータルであるカスペルスキーカンパニーアカウントからリクエストをお送りいただけます。リクエストにはメールでご対応しますが、お客様の同意がある場合は必要に応じて電話会議や画面共有セッションもご用意いたします。リクエストが受諾された場合、リクエストの処理に必要な予想時間をお伝えします。

本サービスのユースケース：

- 以前に公開された脅威インテリジェンスレポートの特定の詳細情報に関する明確化
- 既に提供された IoC に関する追加のインテリジェンスを取得
- 脆弱性の詳細と、その悪用に対する防御方法の推奨を取得
- 興味のある特定のダークウェブアクティビティの追加情報を取得
- マルウェアのふるまいや、その潜在的な影響、カスペルスキーが確認した関連アクティビティに関する詳細を含む、マルウェアファミリーの概要レポートを取得
- ショートレポート経由で提供された関連 IoC の詳細な背景情報と分類に基づく、アラート/インシデントの効果的な優先順位付け
- 検知された疑わしいアクティビティが APT やクライムウェアに関連するものかどうかを特定するためにサポートを利用
- マルウェアファイルを送信し、包括的な分析を依頼して、提供したサンプルのふるまいと機能について把握

知識とリソースを拡張

Kaspersky Ask the Analyst では、カスペルスキーの中核的なリサーチャーグループに案件ベースでアクセスできます。本サービスを通じて、エキスパートと包括的にコミュニケーションを取ることで、既存の社内リソースをカスペルスキーの知識とリソースで補強していただけます。

Kaspersky Takedown Service

課題

サイバー犯罪者は、悪意のあるドメインやフィッシングドメインを作成し、企業やブランドを攻撃します。特定されたこれらの脅威をすばやく軽減できないと、利益の損失、ブランドへのダメージ、顧客からの信頼の失墜、データ漏洩などにつながります。しかし、これらのドメインの削除を管理することは、専門知識と時間を要する複雑なプロセスです。

ソリューション

カスペルスキーは、15,000種類以上のフィッシング/詐欺URLをブロックし、そのようなURLのクリックを1日当たり100万回以上防ぎます。弊社は長年にわたり悪意のあるドメインやフィッシングドメインの分析経験を有しており、ドメインに悪意があることを証明するために必要なすべての証拠を収集する方法を把握しています。弊社は削除管理に対応し、デジタルリスクを最小限に抑える迅速なアクションを実行し、お客様のチームが他の優先度の高いタスクに集中できるようにします。

カスペルスキーは、国際的な組織、国や地域の法執行機関（インターポール、欧州刑事警察機構、Microsoft Digital Crimes Unit、オランダ警察機関のNational High-Tech Crime Unit（NHTCU）、ロンドン市警察など）、およびComputer Emergency Response Teams（CERT: コンピューター緊急対応チーム）と協力することで、お客様にオンラインサービスとレピュテーションのための効果的な保護を提供します。

仕組み

企業のお客様のためのサポートポータルであるカスペルスキーカンパニーアカウントからリクエストをお送りいただけます。弊社は、必要なすべてのドキュメントを用意し、ドメインをシャットダウンするために必要な法的権利を有する関連する地方/地域の機関（CERT、登録機関など）に削除リクエストを送信します。お客様は、リクエストされたリソースが正常に削除されるまで、削除のすべての段階ごとに通知を受信します。

簡単な保護

Kaspersky Takedown Serviceは、ブランドやビジネスが損害を受ける前に、悪意のあるドメインおよびフィッシングドメインがもたらす脅威をすばやく軽減します。プロセス全体のエンドツーエンド管理により、貴重な時間やリソースを節約できます。

本サービスのメリット

世界規模の対応

悪意のあるドメインやフィッシングドメインが登録されても問題ありません。カスペルスキーは関連する法的権限を持つ地域組織からの削除をリクエストします。

エンドツーエンド管理

削除プロセス全体を管理し、お客様の負担を最小限に抑えます。

完全な可視化

リクエストの登録から削除の成功まで、プロセスの各段階に達するたびに通知します。

Digital Footprint Intelligenceとの統合

このサービスはKaspersky Digital Footprint Intelligenceと統合され、ブランド/組織に損害を与え、悪用し、偽装するよう設計された、フィッシング/マルウェアドメインに関するリアルタイム通知を提供します。単一のソリューションは包括的なサイバーセキュリティ戦略の重要なコンポーネントです。

主な利点

グローバルな脅威の可視化により、サイバー脅威のタイムリーな検知、セキュリティアラートの優先順位付け、情報セキュリティインシデントに対する効果的な対応を実行できます。

アナリストの疲弊を防ぎ、社員が真の脅威に集中できるようにサポートします。

異なる産業や地域にまたがる攻撃者による戦術、技術、および手順に対する独自の洞察により、標的型の複雑な脅威に対してプロアクティブな保護を実行できます。

軽減戦略に対する実用的な推奨事項を含むお客様のセキュリティ体制の包括的な概要を利用することで、サイバー攻撃の最大の標的として特定される領域に集中して防衛戦略を立案できます。

インシデント対応機能および脅威ハンティング機能を強化、促進することで、攻撃の「潜伏期間」を短縮し、損害発生のリスクを大幅に低下させます。

結論

最新のサイバー脅威に対抗するには、攻撃者の戦術やツールの全体像を把握する必要があります。このインテリジェンスを生み出して最も効果的な対策を特定するには、継続的な努力と高度な専門知識が必要です。数ペタバイトに及ぶ脅威に関する豊富なデータ、高度な機械学習テクノロジー、他に類を見ないほどの世界的な専門家を活用できるカスペルスキーは、世界中から集めた最新の脅威インテリジェンスでお客様を支え、過去に例のないサイバー攻撃が行われたとしても耐性を保てるようにサポートします。

FORRESTER®

Forrester Wave において外部脅威インテリジェンスサービスのリーダーとして位置付けられています（2021年）

www.kaspersky.co.jp