Kaspersky Threat Lookup

kaspersky BRING ON THE FUTURE

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し、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。

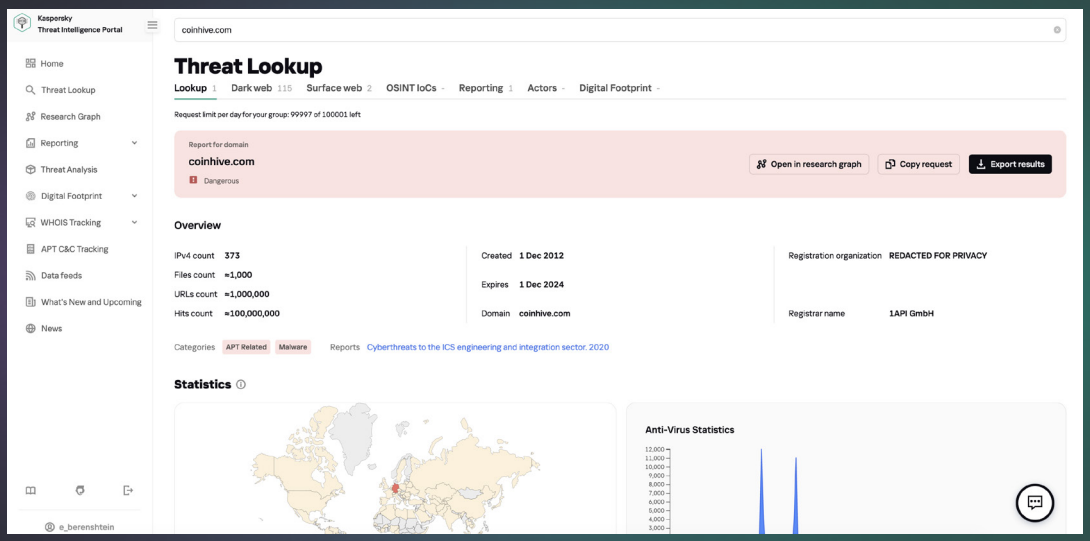
メリット

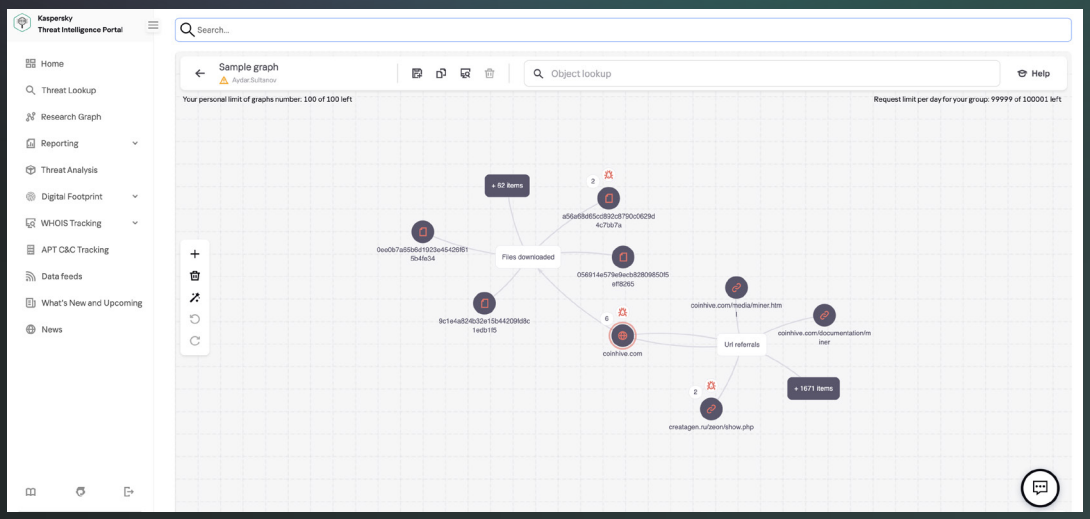
高度に検証された脅威のコンテキストを使用して、脅威の兆候について詳細に調査することで、攻撃に優先順位を付け、ビジネスにとって極めて大きなリスクとなる脅威の緩和に集中できるようにします。

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 Threat Lookup

詳しくはこちら

www.kaspersky.co.jp

© 2022 AO Kaspersky Lab.登録商標およびサービスマーク
はそれぞれの所有者に帰属します。