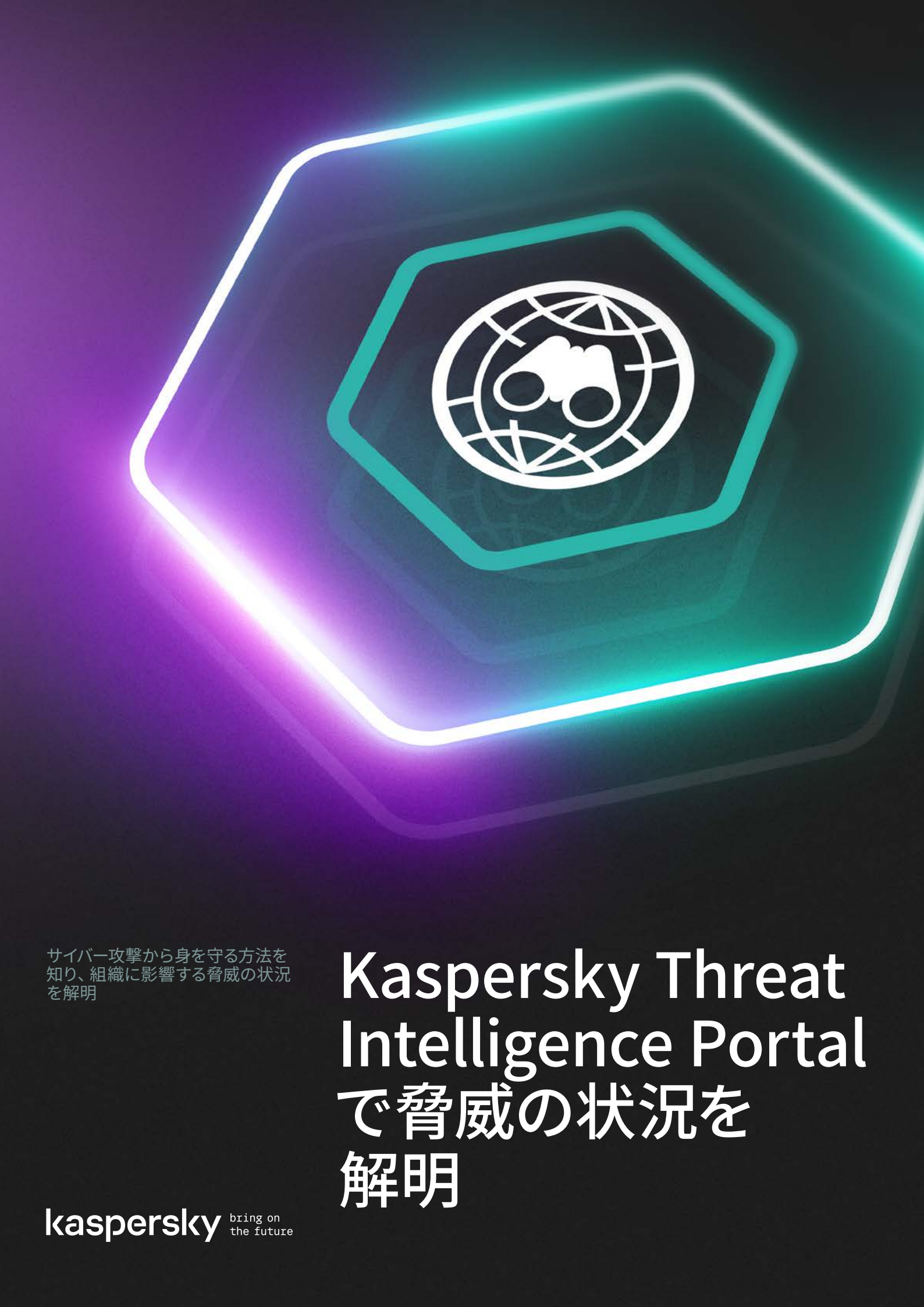


サイバー攻撃から身を守る方法を知り、組織に影響する脅威の状況を解明

Kaspersky Threat Intelligence Portalで脅威の状況を解明

kaspersky bring on the future

Kaspersky
Threat Intelligence
Portal

Kaspersky Threat Intelligence Portalで解明される、組織に影響する脅威の状況

世界的な脅威の状況は常に変化しており、新しい攻撃手法が毎日のように登場し、既知の攻撃手法もより巧妙化が進んでいます。今日、情報セキュリティチームにとってますます重要になっているのは、即座に対応が要求される脅威の効果的な優先順位付けです。しかし、自社のビジネス、業界、地域にとって関連性が特に高い脅威には、どのように注力すべきでしょうか？

Kaspersky Threat Intelligence Portal

［Threat Landscape］セクションで、ユーザー固有の脅威の状況を評価することができます。このセクションは、特定の業界や地域を標的とする攻撃者に関する情報の提供に特化して設計されており、検知技術とグローバルな脅威インテリジェンスの統合も行います。これにより、想定される攻撃者が関連する脅威、戦術、テクニック、手順（TTP）に関する、包括的で最新のコンテキストを得ることができます。

［Threat Landscape］セクションから得られる、脅威に関する情報は次の通りです：

- 地理的な情報
- 業界
- 脅威の種別
- 脅威アクター
- テクニック、戦術、手順（TTP）
- 攻撃者が使用する悪意のあるソフトウェア
- 関係するセキュリティ侵害インジケーター（IoC）

脅威インテリジェンスデータの収集には、Kasperskyが25年以上にわたってサイバー犯罪対策に使用してきた各種のエキスパートシステムがリアルタイムで使用されています：Kaspersky Security Networkはその代表的なシステムの1つで、世界中の何百万人ものユーザーから匿名データを同意を得た上で収集し、1日あたり何百万ものファイルを自動処理します。他にも、Webクローラー、ボットファーム、スパムトラップ、ハニーポット、センサー、パッシブDNS、オープンウェブおよびダークウェブの情報源、パートナーなどからも情報を収集しています。当社はこの四半世紀にわたってこのデータを使用しており、独立系機関によるテストや外部評価で常に最高点を獲得しています。収集されたデータは、Kasperskyの脅威リサーチチームによって慎重に分析され、サンドボックス、ヒューリスティックエンジン、類似性チェックツールなどの最新自動システムで処理され、検証済みの最新情報となります。

詳細はこちら

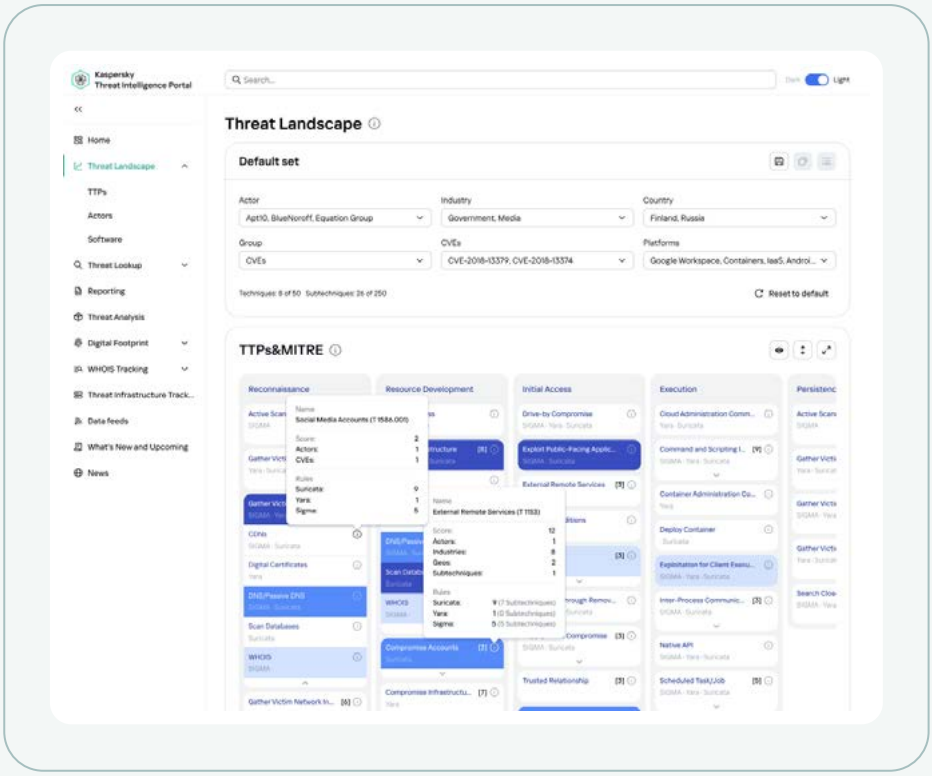
仕組み

当社は毎日、数十万もの悪意のあるファイルサンプルを処理し、その地理的情報と業界データを抽出しています。その後、Kasperskyの社内システムが関連するTTPを抽出し、既知のサイバー犯罪グループやマルウェアにファイルを属性付けします。[Threat Landscape] セクションもまた、世界中のKasperskyのエキスパートリサーチャーチームから寄せられる実際のインシデントデータの集積に基づいています。

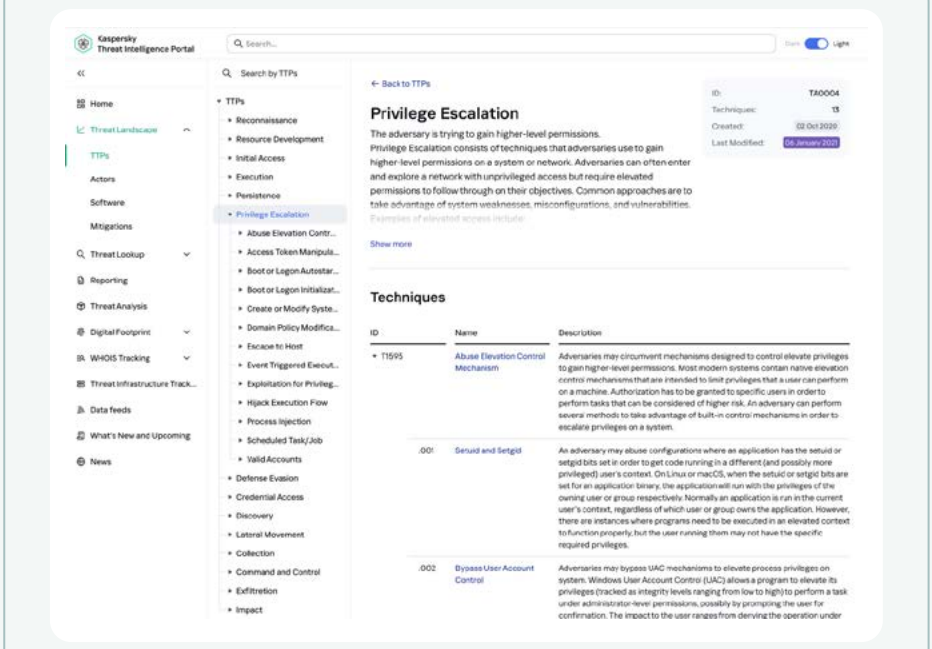
フィルターの適用により、Kaspersky Threat Intelligence Portalユーザーは、 MITREATT&CKフレームワークに準拠した独自の脅威の状況の把握し、想定される敵対者に関する最新情報を入手することができます。入手可能な情報は次の通りです：攻撃に使用される可能性が高いテクニック、戦術、手順、それらを使用するアクター、マルウェア、およびTTPの詳細な説明、攻撃の詳細な説明を含むレポートです。最終的には、アクターのテクニックが成功裏に実行されるのを防止するための特定の推奨事項に基づいて、緩和策を講じることができます。

主な機能

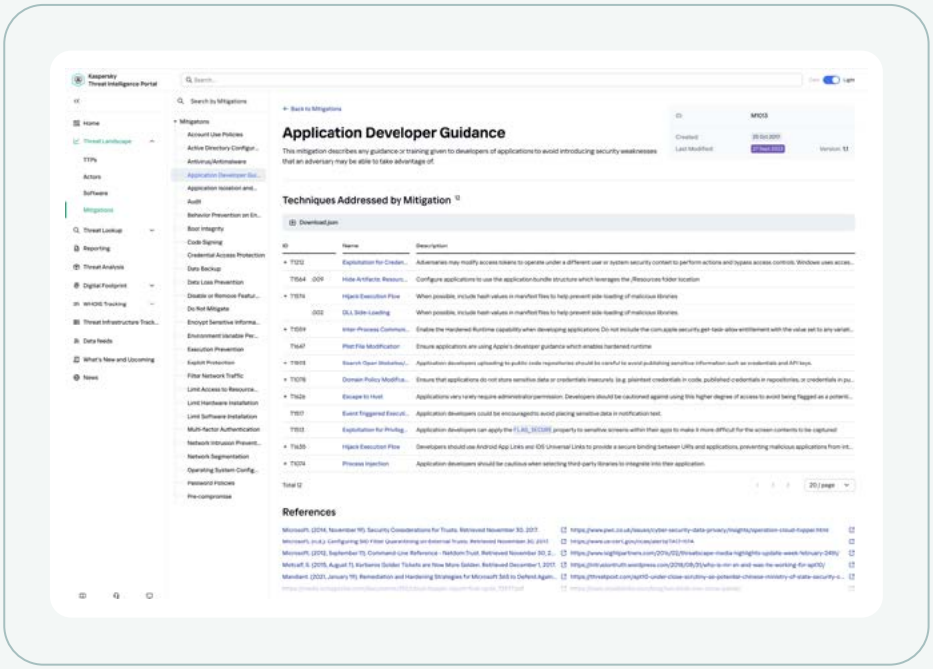
MITRE ATT&CKヒートマップを使用して、組織に固有の脅威の状況をリアルタイムで構築します。フィルターを適用することで、ユーザーは、当社のシステムとエキスパートが継続的な調査を通じて入手した過去24時間分の更新情報など、最新のデータにアクセスできます。国際的な組織のレイヤーを保存することができます。



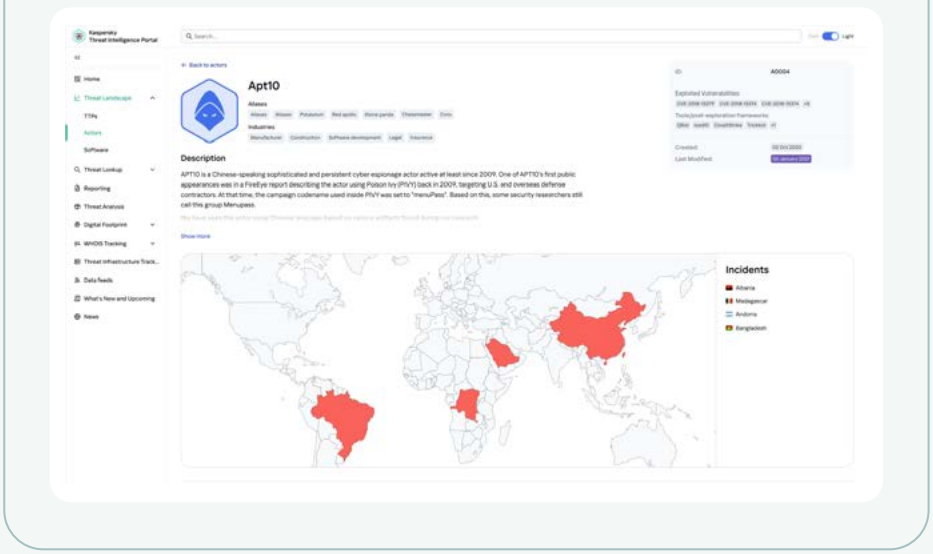
Kasperskyのエキスパートシステムに基づく、攻撃者のテクニック、戦術、手順に関するリアルタイムの最新情報。



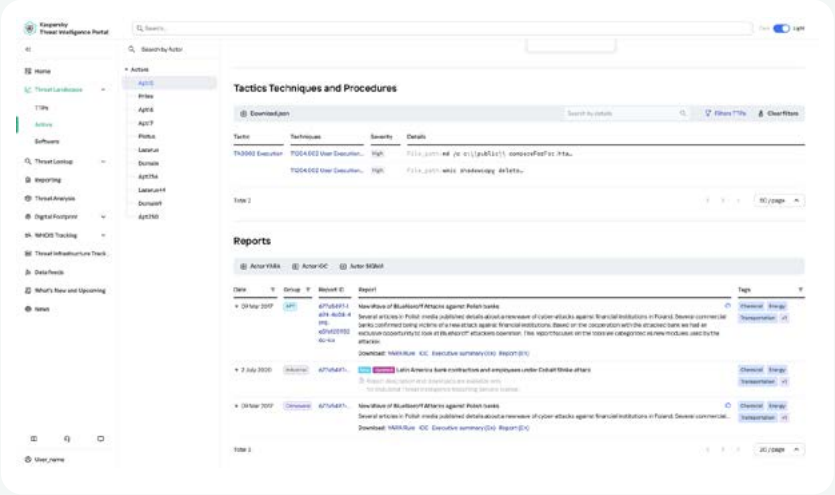
［Mitigation］セクションでは、セキュリティギャップを回避するための組織の予防措置および保護措置について詳細な説明を参照することができます。



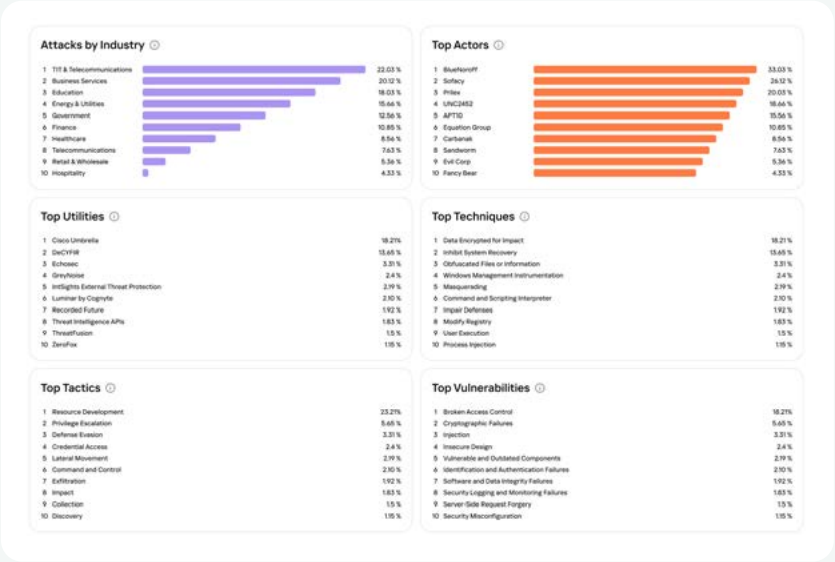
アクターおよびマルウェアのプロファイルを業界で最も大規模に収集したリポジトリと、Kaspersky のエキスパートがまとめた詳細な説明を参照できます。



MITRE ATT&CKのテクニック、戦術、手順に関連するSigma / Yara / Suricataのルールにアクセスし、組織に影響する脅威を検知します。



トップ10の統計情報を、業界、アクター、TTP、脆弱性、ソフトウェアについて表示。



日々進化し続けるサイバー脅威の世界には、多数の製品やサービスを通じて取得可能な脅威インテリジェンスデータが潤沢に存在しています。組織は、自らの脅威の状況を理解することで、関連する攻撃に対して戦略面で合理的な対策を講じ、事前に防御することが可能になります。

使用するメリット

予防的な防御アプローチ

組織に対する最も可能性の高い攻撃経路を理解し、効果的な防御戦略を策定します

攻撃対象領域の監視

攻撃者が脆弱性を悪用する前に、セキュリティ上のギャップを特定します

組織に関連する脅威に専念する

ビジネス、業界、地域に最も大きな影響を与える可能性が高い脅威に集中的に対処することができます

戦略的な計画

脅威の状況に関する情報を、投資計画や保護ツール/方法の開発に使用します

情報セキュリティ部門の効率性の向上

関連する脅威や世界的な傾向に関する情報へのアクセスにより、スタッフの作業効率を向上させ、人件費を削減します

脅威の正しい認識に基づいた防衛策

最新の脅威とその世界的な動向を認識し、効果的な防衛策を講じることができます

「彼を知り己を知らば、百戦殆うからず。彼を知らずして己を知らば、一勝一負す。彼を知らず己を知らざれば、戦う毎に必ず殆うし」

孫子

『孫子の兵法 謀攻編』より引用

Kaspersky Threat Intelligence

Kaspersky Threat Intelligenceは、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を提供します。このデータを活用することで、あらゆる組織が今日のサイバー脅威に効果的に対抗できるようになります。

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分析力を備えています。これにより、Kasperskyはインターポールや各種のCERT機関をはじめ、世界中の法執行機関や政府組織から信頼されるパートナーとなっています。Kaspersky Threat Intelligenceをご利用になることで、最新の戦術的、運用的、戦略的な脅威インテリジェンスを活用できるようになります。

Kaspersky Threat Intelligence

詳細はこちら

www.kaspersky.co.jp

#kaspersky
#bringonthefuture