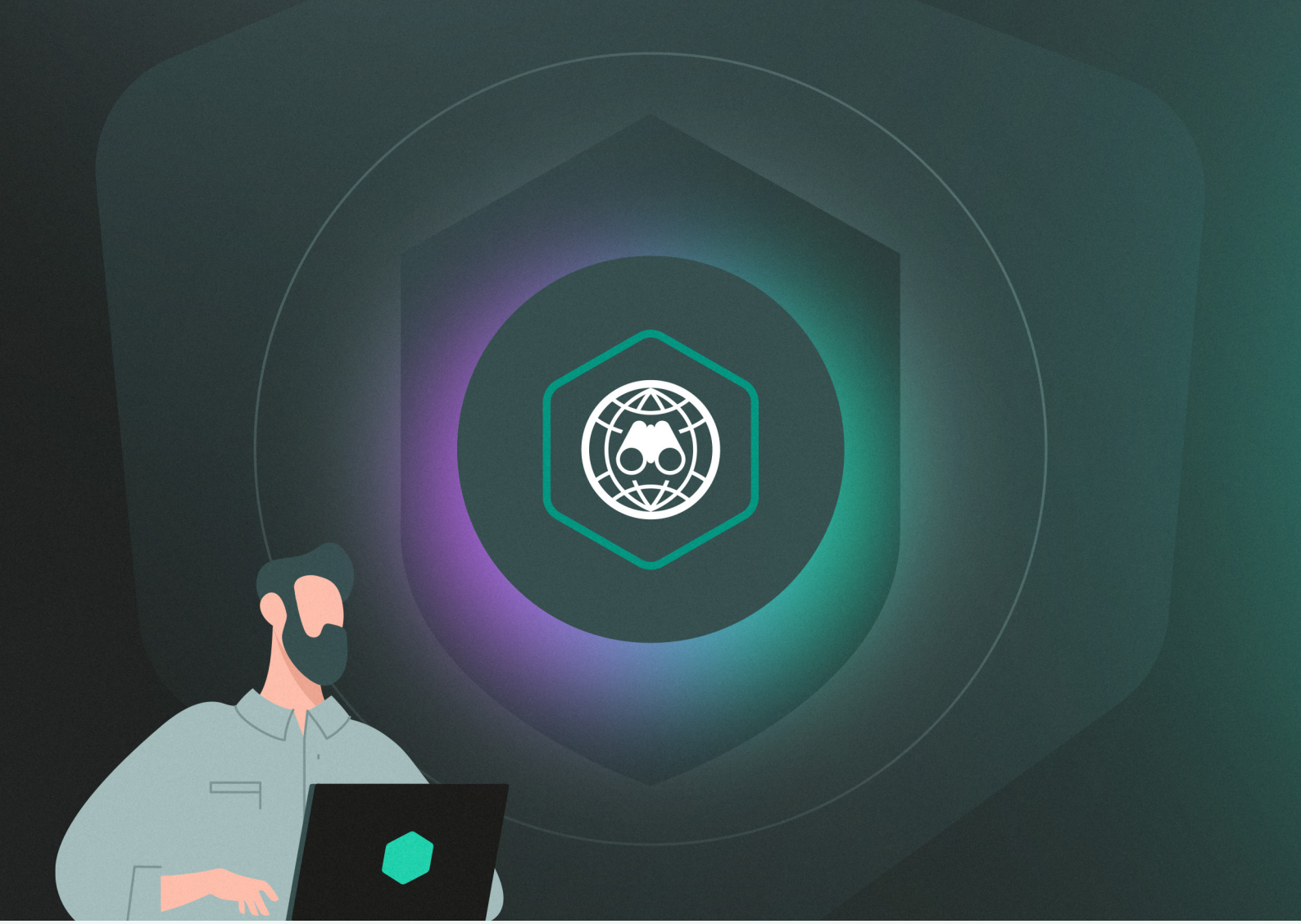

Kaspersky Threat Intelligence

脅威インテリジェンスソースの評価

kaspersky BRING ON THE FUTURE

詳しくはkaspersky.co.jpをご覧ください
#bringonthefuture

はじめに

攻撃対象が拡大し、脅威が高度化する中で、インシデントに対応するだけでは十分ではありません。ますます複雑になる環境は、攻撃にさまざまな機会を与えます。各産業および各組織は、保護対象となる独自のデータを所有し、一連のアプリケーションや技術などを使用します。このため、膨大な数の変数が攻撃を実行する可能性のある方法に導入され、毎日新たな方法が現れます。

過去数年にわたり、弊社は異なる種別の脅威と異なるタイプの攻撃者の間の境界が不鮮明になっていくのを見てきました。以前は限られた数の組織にとって脅威だった方法とツールが市場に広く出回っています。この例として、Shadow Brokersグループによるコードのダンプがあります。これにより、その種の洗練されたコードにアクセスできなかった犯罪グループが高度な脆弱性攻撃を自由に使えるようになります。別の例としては、標的型サイバー攻撃（APT）活動の登場があります。これは、サイバースパイではなく、盗みが主な目的です。APTグループが関わる他の活動のための資金を得るためにお金を盗み出します。その他にも、さまざまな攻撃があります。

新たなアプローチが必要です。

以前は限られた数の組織にとって脅威だった方法とツールが市場に広く出回っています。

高度な標的型攻撃の犠牲になる企業が増えているため、正しい防御のために新たな方法が必要なことは明らかです。自身を守るために、事業者は絶えず変化する脅威の環境に対して常にセキュリティ制御を適用し、攻撃を受ける前に対処しておく必要があります。これらの変化に対応する唯一の方法は、効果的な脅威インテリジェンスプログラムを構築することです。

脅威インテリジェンスは、すべての産業や地域のさまざまな規模の企業により確立されたセキュリティ運用の重要なコンポーネントになっています。脅威インテリジェンスは、人間が読み取れる形式と機械可読の形式で提供され、インシデント管理サイクルを通じて有益な情報でセキュリティチームをサポートし、戦略的な意思決定を通知します（図1）。

ただし、外部脅威インテリジェンスに対する需要の高まりにより、大量の脅威インテリジェンスの製造元が生まれ、各製造元がさまざまなサービスを提供しています。大規模で競争の激しい市場には、無数の複雑なオプションが用意されており、組織にとって適切なソリューション選ぶことが非常に複雑になり、激しいストレスを感じる場合があります。

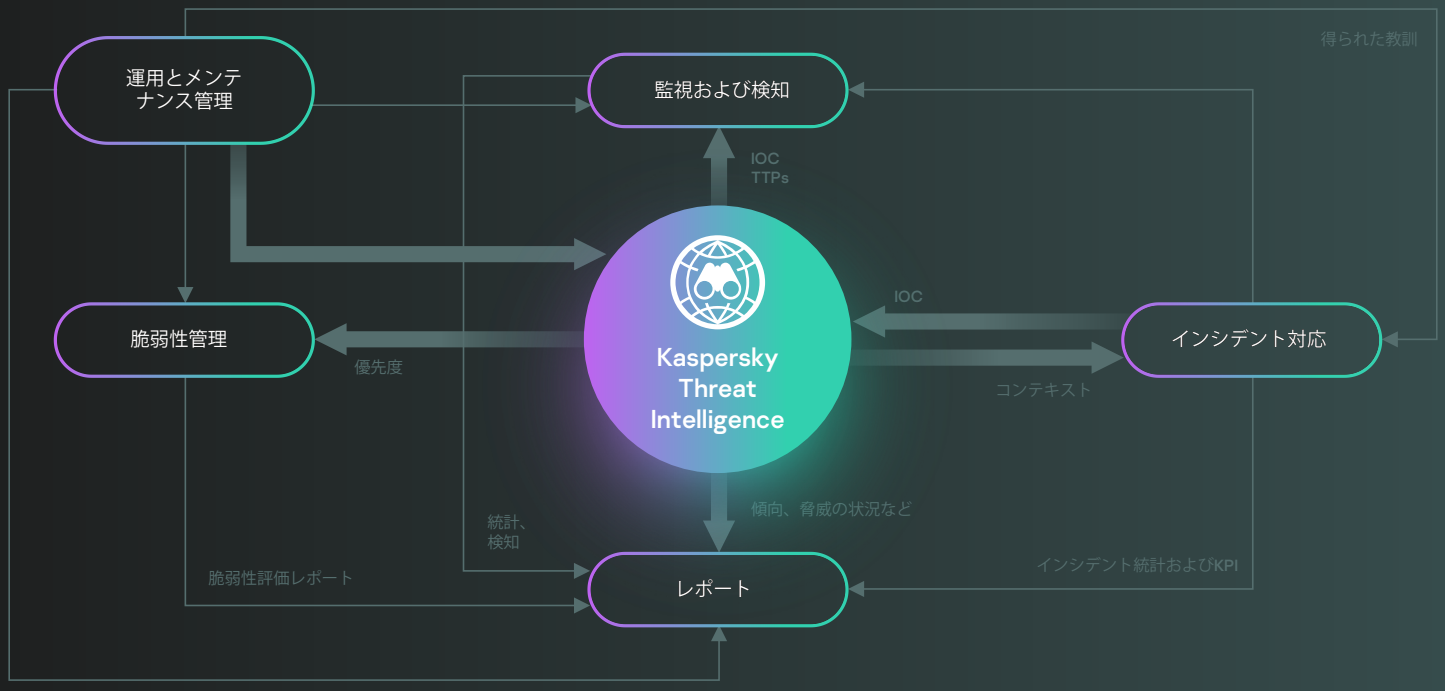

図1

脅威インテリジェンス主導のセキュリティ運用

お客様のビジネスのためにカスタマイズされていない脅威インテリジェンスは、状況を悪化させる可能性があります。現在、多くの企業で、セキュリティアナリストはプロアクティブな脅威ハンティングや対応を行う代わりに、誤検知を分類することに大半の時間を過ごしています。このため、検知時間が大幅に増加しています。セキュリティ運用に無関係で不正確な情報を与えることで、誤ったアラートの数がさらに増加し、応答機能、そして会社のセキュリティ全体が深刻な悪影響を受けることになります。

最適なインテリジェンスはどこにあるか…

数多くの脅威インテリジェンスソースを評価し、組織に最も関連しているものを特定し、それらを効果的に運用するには、どうすればいいのでしょうか？ほとんどすべての製造元が最高だと主張している情報を伴うおびただしい数の無意味なマーケティングをナビゲートするには、どうすればいいのでしょうか？

これらの質問は、もっともですが最初に尋ねる質問ではないはずです。派手なメッセージと高い理想に魅了され、多くの組織は、外部製造元がある種の強力な透視能力を提供すると信じています。しかし、価値ある情報のほとんどは、企業ネットワークの境界内に存在しているということを見落としています。

侵入検知や防御システム、ファイアウォール、アプリケーションログ、およびその他のセキュリティ制御のログから得られるデータは、企業ネットワーク内で何が起こっているかを明らかにします。組織に固有の悪意のある活動のパターンを特定できます。通常ユーザーとネットワークのふるまいを差別化し、データアクセスアクティビティの痕跡を維持することができます。

図2
外部脅威インテリジェンスの運用

攻撃者のように考える

効果的な脅威インテリジェンスプログラムを構築するために、企業は（セキュリティオペレーションセンターを確立済みの企業も含む）攻撃者として思考し、最も可能性の高い標的を特定し、保護する必要があります。脅威インテリジェンスプログラムから真に重要な情報を取得するには、重要な資産とは何か、そして組織の目的を達成するために不可欠なデータセットとビジネスプロセスとは何か、を明確に理解する必要があります。これらの最も重要な要素を特定することで、企業はその周囲にデータ収集ポイントを確立し、収集したデータを外部入手可能な脅威情報を使用してさらにマッピングできます。情報セキュリティ部門が通常持っている限定的なリソースを検討し、組織全体をプロファイリングすることは大変な作業です。解決策は、リスクベースのアプローチを採用し、最初に最も影響を受けやすい標的に焦点を当てることです。

内部の脅威インテリジェンスソースが定義され、運用可能になると、企業は外部情報を既存のワークフローに追加しようと考え始めます。

信頼の問題

外部脅威インテリジェンスソースは信頼レベルに応じて変化します。

オープンソースは無料で入手できますが、多くの場合、それらはコンテキストが欠落し、大量の誤検知が発生します。

商用脅威インテリジェンスソースは、より信頼性が高くなりますが高額のアクセス権を購入する必要があります。

まずは、Financial Services Information Sharing and Analysis Center（FS-ISAC）などの産業固有のインテリジェンス共有コミュニティにアクセスすることが最適な方法です。これらのコミュニティは、非常に有用な情報を提供しますが、制限があり、アクセスするために会員登録が必要な場合があります。

外部脅威インテリジェンスソースを選択する際の原則は、量より質です。一部の組織は、統合できる脅威インテリジェンスソースが多ければ多いほど、より多くの情報を可視化できると考えています。これは、たとえば商用ソースなど、組織に固有の脅威プロファイルに応じてカスタマイズされた脅威インテリジェンスを提供する信頼性の高いソースについては当てはまる場合があります。そうでない場合、無関係の情報によりセキュリティ運用に重大なリスクが発生します。

専門の脅威インテリジェンスの製造元が提供した情報では、内容が重複することは非常にわずかです。これら製造元のインテリジェンスソースと収集方法は異なるため、提供される洞察はある側面において一意になります。たとえば、ある製造元は、特定の地域で主要な存在であるため、その地域から発生した脅威の詳細を提供しますが、別の製造元は特定の種別の脅威の詳細を提供します。このため、両方のソースにアクセスできるようにすることは、一緒に使用する場合はメリットがあり、全体像をより明らかにし、より効果的な脅威ハンティングとインシデント応答ミッションをガイドするために役立ちます。ただし、これらの種類の信頼できるソースは、慎重な事前評価が必要なことに留意してください。提供されたインテリジェンスが組織固有のニーズやユースケース（セキュリティ運用、インシデント対応、リスク管理、脆弱性管理、レッドチームサービスなど）に適しているか確認してください。

商用脅威インテリジェンス製品を評価する際に考慮する問題

さまざまな商用脅威インテリジェンス製品を評価するための共通の基準はありませんが、いつくかの留意点があります。

お客様の企業は、すでにいくつかのセキュリティ制御が導入されており、関連付けられたプロセスが定義され、使用方法を把握しているツールを用いて脅威インテリジェンスを使用することが重要であると思われます。このため、既存のセキュリティ運用との脅威インテリジェンスのスムーズな統合をサポートする配信方法、統合メカニズム、形式を探してください。

グローバルに展開するインテリジェンスを探してください。攻撃に国境はありません。南米の企業を標的にした攻撃がヨーロッパで開始されます。またこの逆の攻撃も行われます。製造元はグローバルに情報を調達し、ばらばらに見える活動をまとまりのある活動にまとめていますか？この種の情報は、適切なアクションを実行することに役立ちます。

コンテキストはデータからインテリジェンスを作ります。コンテキストのない脅威指標は、価値がありません。「なぜ、これが重大なことなのか」という重要な質問に答えることのできるプロバイダを探す必要があります。関係コンテキスト（例: 検知されたIPアドレスに関連付けられたドメイン、または特定のファイルがダウンロードされたURLなど）は、付加価値をもたらし、インシデント調査を促進し、ネットワーク内で新たに取得した関連する「侵害の痕跡」を発見することで、すぐれたインシデント「スコーピング」をサポートします。

長期的なセキュリティ計画を通知するために、以下のようなより戦略的なコンテンツを求めている場合:

- 攻撃傾向の高度な表示
- 攻撃者が使用する技術と方法
- 意図
- アトリビューションなど

地域や産業で複雑な脅威を発見し、調査し続けている実績のある脅威インテリジェンスプロバイダを探してください。そのリサーチ機能をお客様の会社の条件に合わせてカスタマイズするプロバイダの能力も重要です。

結論

カスペルスキーは、20年以上にわたり、脅威の研究に集中してきました。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グローバル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に対しても耐性を保てるようにサポートします。

Kaspersky Threat Intelligence

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。