kaspersky BRING ON THE FUTURE

Kaspersky CyberTrace

情報セキュリティアナリストが日々処理するセキュリティアラートは、指数関数的に増加しています。このような莫大な量のデータの分析では、アラートの優先順位付け、トリアージ、検証を効果的に行うことはほとんど不可能です。多数のセキュリティ製品からひっきりなしに警告ランプが点滅する状況では、重要なアラートが埋もれやすくなり、アナリストは疲弊します。ログ管理およびセキュリティ分析ツールであるSIEMを使用してセキュリティデータを収集し、関連するアラームすべての相関関係を明らかにすれば、追加検査を要するアラートの数を減らすことは可能です。しかし、それでもまだセキュリティアナリストにかかる過剰な負担は軽減されません。

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。

効果的なアラートトリアージと分析を可能にするには

セキュリティオペレーションセンターで、SIEMシステムのような既存のセキュリティコントロールに、最新の機械可読脅威インテリジェンスを統合すると、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、調査が必要なアラートや、インシデント対応チームに調査と対応を依頼する必要のあるアラートをすぐ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。JSON、STIX、XML、CSVの形式の任意の脅威インテリジェンスフィード（カスペルスキー、その他のベンダー、OSINTの脅威インテリジェンスフィードまたは自社のカスタムフィード）と統合できます。また、購入後すぐにさまざまなSIEMソリューションやログソースと統合できます。

Kaspersky CyberTrace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。着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。

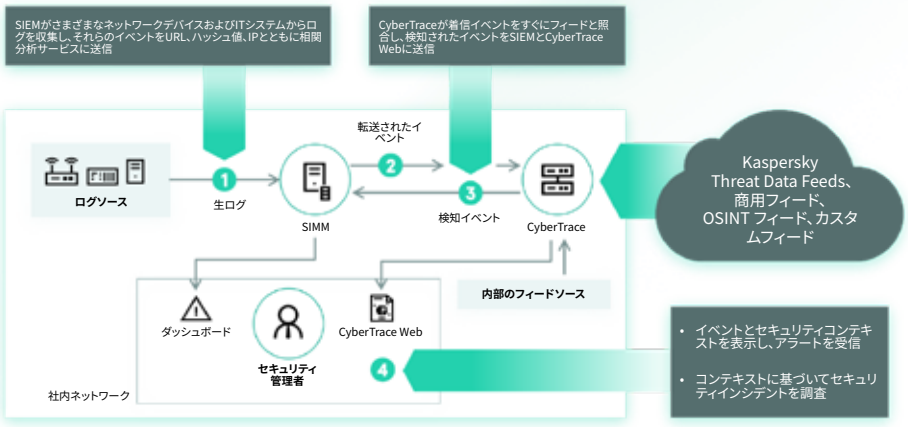

図1.Kaspersky CyberTraceの統合図

製品機能一覧

Kaspersky CyberTraceは、脅威インテリジェンスを活用した効果的なアラートトリアージと初期対応を可能にする各種の機能を提供します。これらの機能は以下のとおりです。

- 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。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。インテリジェンスサプライヤー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がシンプルになります。
- 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。その指標が検知された場合、検知日についての情報と検知リストへのリンクが表示されます。

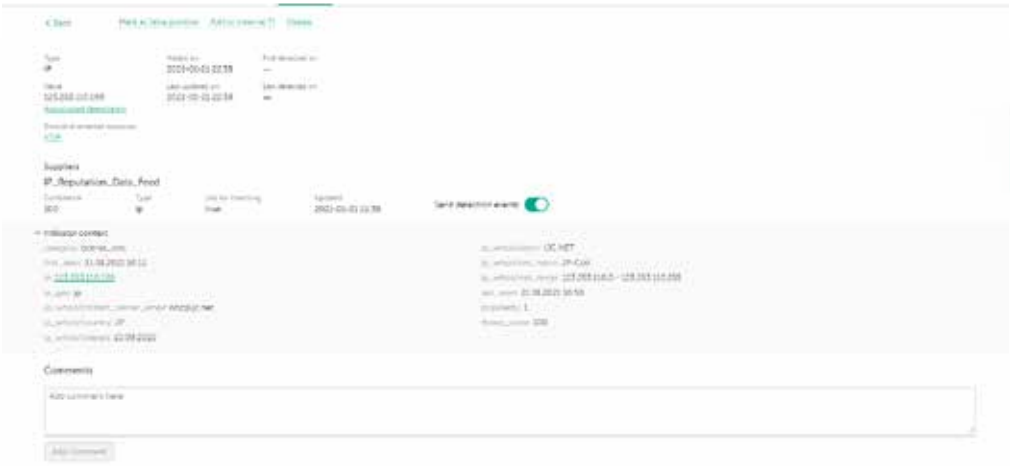

図2.各指標について、すべての脅威インテリジェンスサプライヤーからの詳細情報を表示

- 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。調査グラフは URL 、ドメイン、 IP 、ファイル、その他の調査中に遭遇したコンテキスト間の関係を図にして視覚化します。そのグラフには以下のような機能が含まれます：変形、ミニグラフ、ノードのグループ分け、手動でのリンクの追加、指標の追加、グラフ上でのノードの検索。

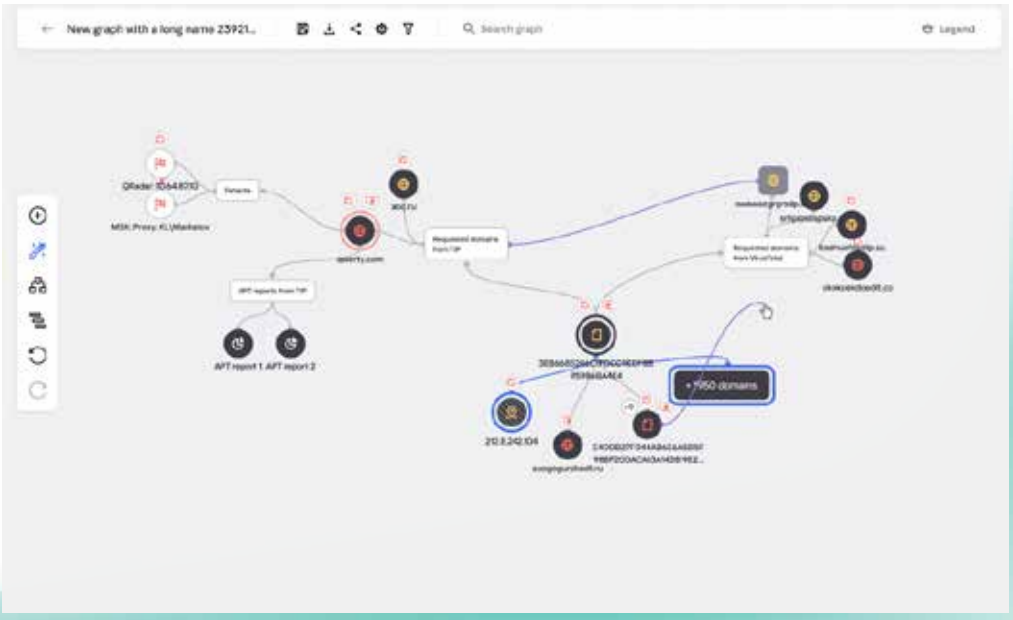

図3.調査グラフ

- 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。

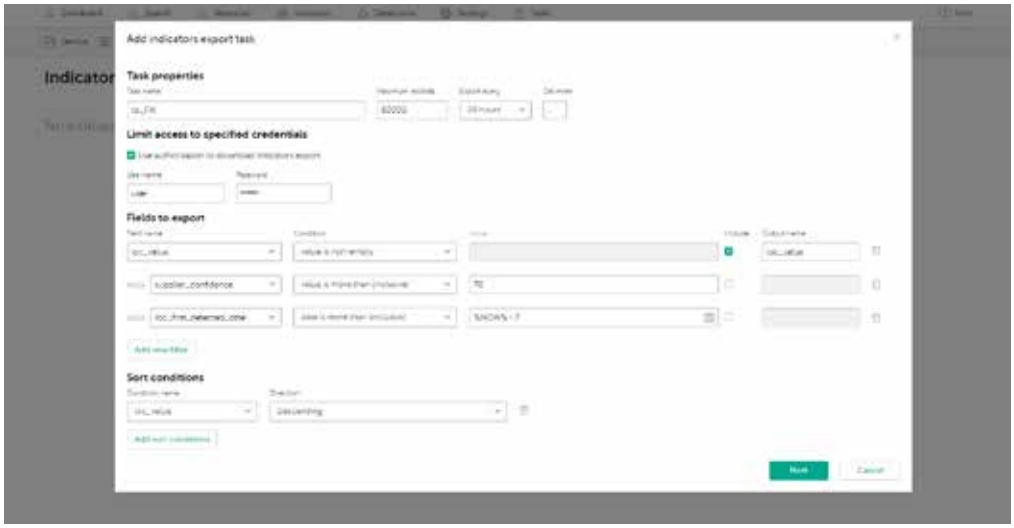

図4.指標エクスポートタスク

- 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。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。

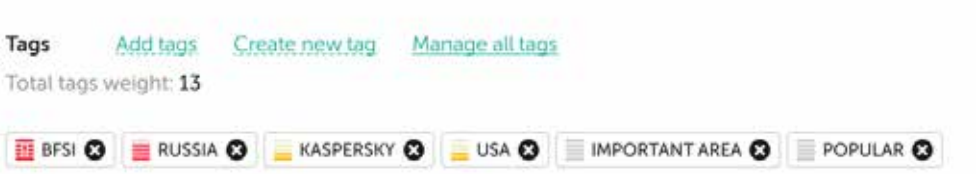

図5.IoC タグ

- 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。すべての履歴検知がレポートに記録されるので、将来これらを調査に使用することも可能です。
- 検知イベントをSIEMソリューションに送信する際にフィルターを適用することで、SIEMへの負荷や、アラート処理で疲弊しているアナリストの負担を軽減できます。この機能を使用すると、インシデントとして扱う必要のある最も危険な検知イベントのみをSIEMに送信できます。その他の検知イベントはすべて内部データベースに保存され、根本原因分析や脅威ハンティングに利用できます。
- マルチテナント機能は、MSSPや大企業のユースケース、たとえば、サービスプロバイダー（本社）が多様な支社（テナント）からのイベントを個別に処理する必要がある場合などに役立ちます。この機能を使用すれば、1つのKaspersky CyberTraceインスタンスをさまざまなテナントの複数のSIEMソリューションに接続して、各テナントに使用するフィードを設定できます。

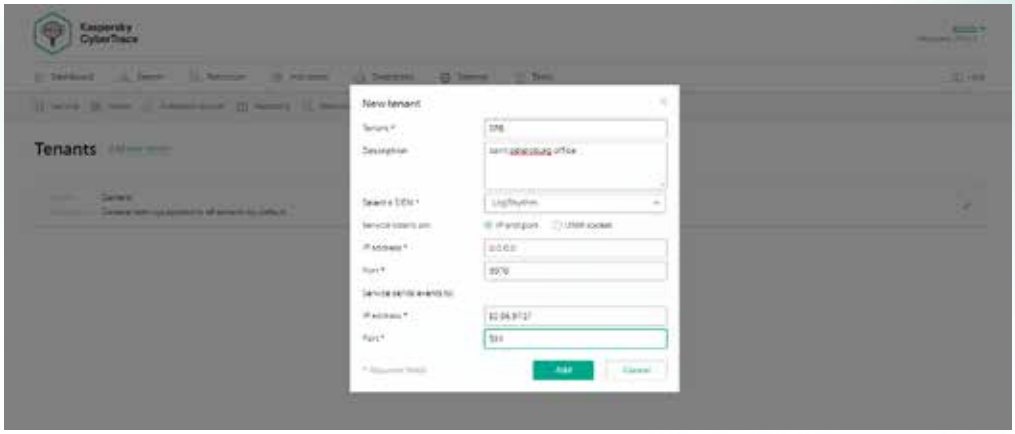

図 6.新規テナントの作成

- 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判断する際に役立つ機能です。

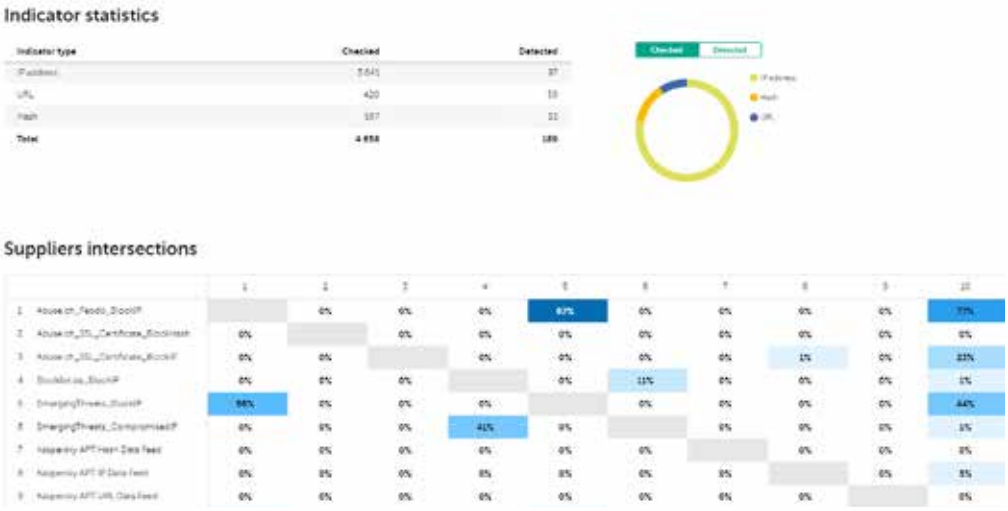

図 7.指標統計とフィードインターセクションマトリクス

その他の製品機能:

- 多様なSIEMソリューションに対応するSIEMコネクタにより、脅威検知に関するデータを可視化して管理
- 詳細な脅威調査に役立つ指標（ハッシュ、IPアドレス、ドメイン、URL）のオンデマンドルックアップ
- フィードに対する高度なフィルタリング
- ログとファイルの一括スキャン
- WindowsおよびLinuxプラットフォーム向けのコマンドラインインターフェイス
- スタンドアロンモードでは、Kaspersky CyberTraceがネットワークデバイスなどの多様なソースからログを受信して解析
- この他にもさまざまな機能があります

- 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。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、自動化やオーケストレーションを実現できます。
- Kaspersky Unified Monitoring and Analysis Platform（KUMA）との統合が可能です。この統合にはWeb UIの統合（単一UI）も含まれます。

Kaspersky CyberTrace と Kaspersky Threat Data Feedsは別々に使用することもできますが、併用すると、脅威検知機能が大幅に向上します。サイバー脅威に対するグローバルな可視性を活用することで、セキュリティオペレーションを強化できます。Kaspersky CyberTrace と Kaspersky Threat Data Feedsの併用により、以下のことが可能になります。

- セキュリティアラートを効果的に抜き出し、優先順位を判断する
- アナリストの作業負荷を軽減し、疲弊を防ぐ
- 重大アラートを即座に特定し、インシデント対応チームに報告すべきアラートについて、より多くの情報に基づき適切に判断する
- 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

サイバー脅威ニュース:www.securelist.com
ITセキュリティニュース：business.kaspersky.com
中小企業向けITセキュリティ kaspersky.co.jp/business
大規模企業向けITセキュリティ：kaspersky.co.jp/enterprise
脅威インテリジェンスポータル：opentip.kaspersky.com

www.kaspersky.co.jp

実証済みの品質、独立性、透明性をお約束します。カスペルスキーは、安全な世界を作り上げ、テクノロジーを活かして人々の暮らしを良くすることを目指しています。そのために、世界中の誰もがテクノロジーの無限の恩恵を受けることができるよう、セキュリティサービスを提供しています。安心できる未来のために、サイバーセキュリティをお届けします。

詳しくは、kaspersky.com/transparency をご覧ください。

Proven.
Transparent.
Independent.