脅威インテリジェンス
プラットフォーム

Kaspersky CyberTrace

kaspersky bring on the future

Kaspersky CyberTrace

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連携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。

アラートの効果的なトリアージと分析を実現

サイバーセキュリティのアナリストが処理するアラートの数は、爆発的に増加しています。分析するデータがこれほど大量になると、効果的なアラートの優先順位付け、トリアージ、検証はほぼ不可能となります。

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、不要なアラートの中に重要なアラートが埋もれてしまい、アナリストは疲弊してしまいます。SIEMやその他のセキュリティ分析ツールは、イベントを関連付け、アラートの数を減らすのに役立ちますが、セキュリティアナリストの負荷は依然として非常に高いままです。

SIEMシステム

機械可読な最新の脅威インテリジェンスをSIEMシステムのような既存のセキュリティ管理に連携させることで、セキュリティ担当者は最初のトリアージプロセスを自動化できます。これにより、詳細な調査やレスポンスのためにインシデントレスポンスチームへのエスカレーションが必要なアラートをすぐに特定するのに十分なコンテキストを得ることができます。

しかし、脅威データフィードと利用可能な脅威インテリジェンス提供元の数が増え続けているため、組織にとってどの情報が適切かを判断するのが難しくなっています。脅威インテリジェンスは多様な形式で提供され、膨大な数のセキュリティ侵害インジケーター（IoC）が含まれているため、SIEMやネットワークセキュリティ管理ツールによる処理も困難になっています。

連携

Kaspersky CyberTraceでは、JSON、STIX、XML、CSV形式のあらゆる脅威インテリジェンスデータフィードを使用することができます：

1. Kasperskyの脅威データフィード
2. 他のベンダーのデータフィード
3. OSINTまたはカスタマイズされたフィード

顧客の利便性を考慮し、CyberTraceは多くのSIEMソリューションやログの提供元とすぐに連携させることが可能となっています。

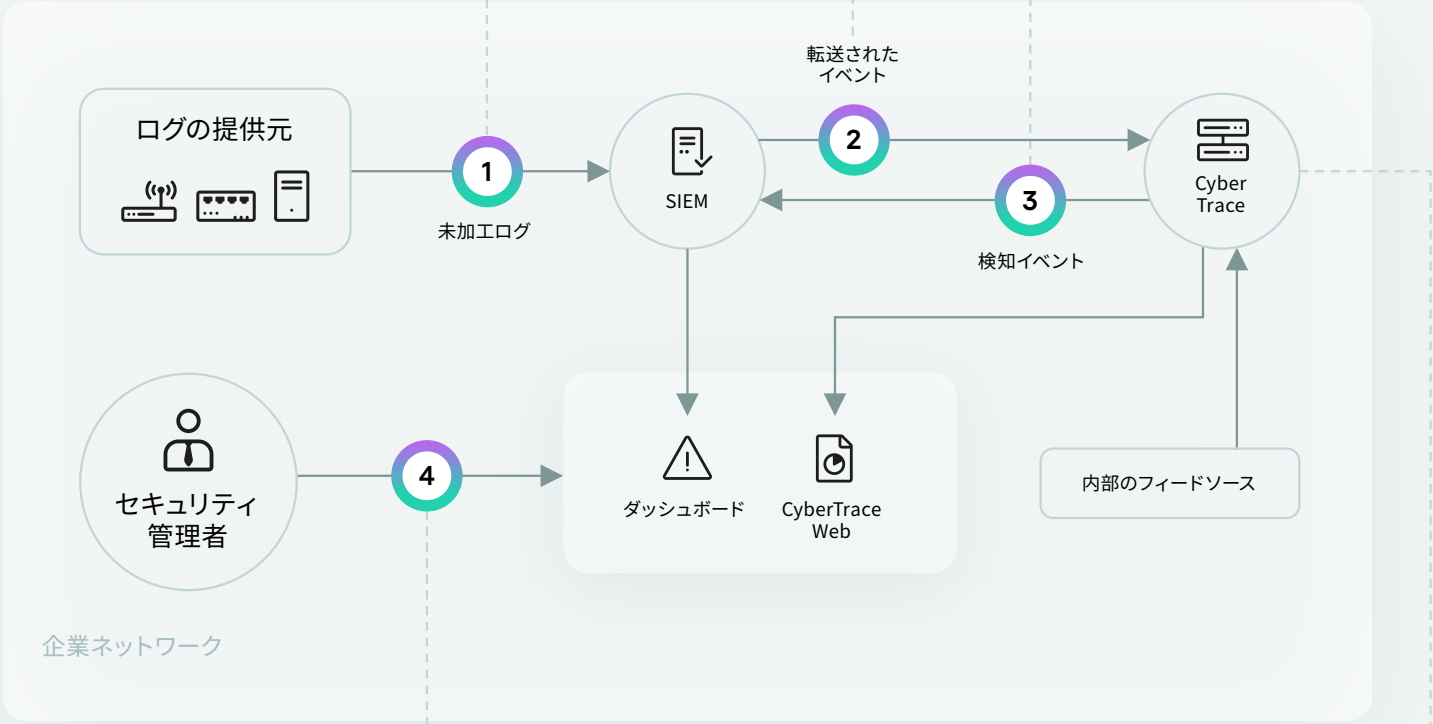
Kaspersky CyberTraceの連携スキーム

Kaspersky CyberTraceは、受信データの解析と照合の処理工程を追加することで、SIEMの機能を強化し、SIEMの作業負荷を大幅に軽減します。イベントをデータフィードの情報と照合して脅威を特定し、検知したインシデントに有益なコンテキストを提供します。ソリューション連携の概略アーキテクチャを下図に示します。

SIEMは、複数のネットワークデバイスやITシステムからのイベントログを集約します

URL、ハッシュ、IPを含むログがCyberTraceに送信され、詳細な分析が行われます

CyberTraceが着信イベントをすぐにフィードと照合し、検知されたイベントをSIEMとCyberTrace Webに送信します



- イベントとセキュリティコンテキストを表示し、アラートを受信
- コンテキストに基づいてセキュリティインシデントを調査

Kaspersky Threat Data Feeds、商用フィード、OSINTフィード、カスタムフィード

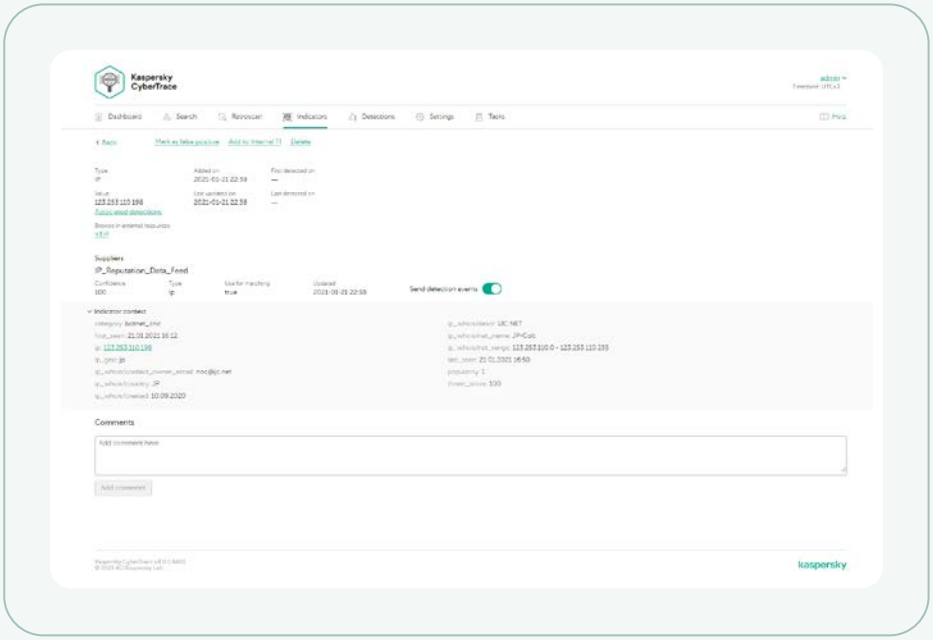
製品機能

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。機能は次の通りです：

詳細情報をすべての脅威インテリジェンス提供元からの脅威インジケーターについて表示

全文検索や高度な検索クエリを使用した検索機能を実装するインジケーターデータベースにより、すべてのインジケーターフィールド（コンテキストのフィールドを含む）を横断した複雑な検索が可能です。インテリジェンスの提供元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簡素化されます。

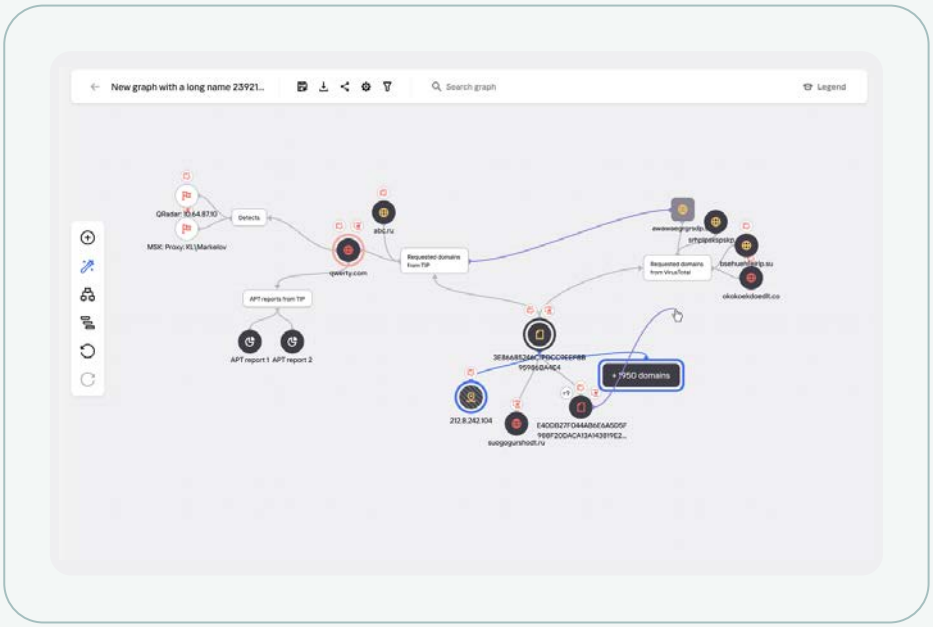
国家/政府/金融コンピューター緊急対応チーム（CERT）、TIベンダー、コミュニティからのメールサブスクリプションやPDF文書は、CyberTraceのIoCの提供元として使用することができます。IOCは、メール本文と添付ファイル（XML、CSV、JSON、PDF）の両方から抽出できます。IMAP/POP3サーバーや、PDFファイルを集めたローカル/共有フォルダーをフィードソースとして使用することができます。



各インジケーター詳細情報のページで、さらに詳細な分析結果を確認できます。各ページには、1つのインジケーターについてすべての脅威インテリジェンス提供元からの情報が表示され（重複する情報は除外されます）、アナリストが脅威についてコメントしたり、そのインジケーター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。そのインジケーターが検知された場合、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。

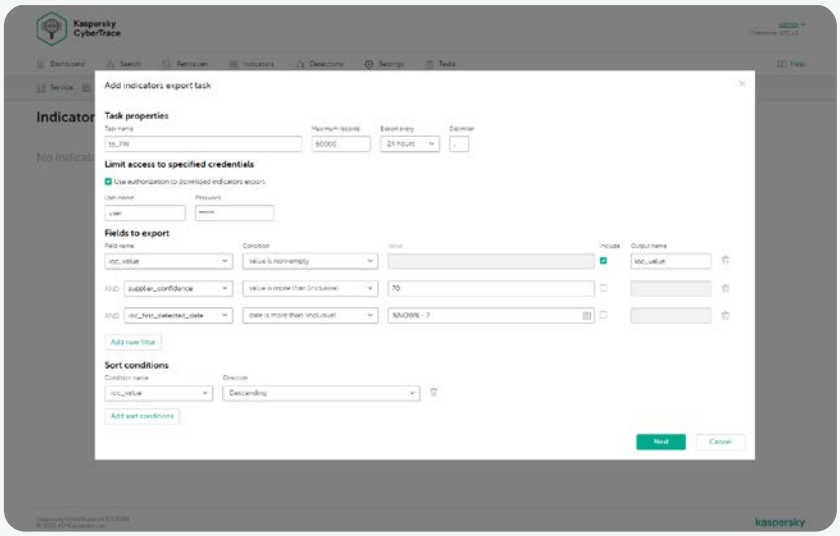
調査グラフ

調査グラフを使用すると、 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。グラフに実装される機能は次の通りです：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、インジケーターの追加、グラフ上でのノードの検索。VirusTotalからの調査グラフにおけるIoCのリッチ化をサポートしています。



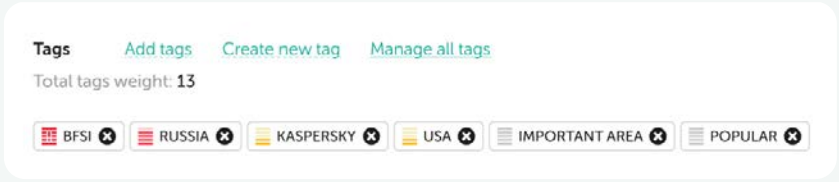
インジケーターのエクスポートタスク

インジケーターのエクスポート機能では、エクスポートしたIoCをポリシーリスト（ブロックリスト）などのサードパーティ製セキュリティ管理ツールにネイティブに統合することが可能であり、Kaspersky CyberTraceインスタンス間や他のTIプラットフォームとの脅威データの共有にも対応しています。



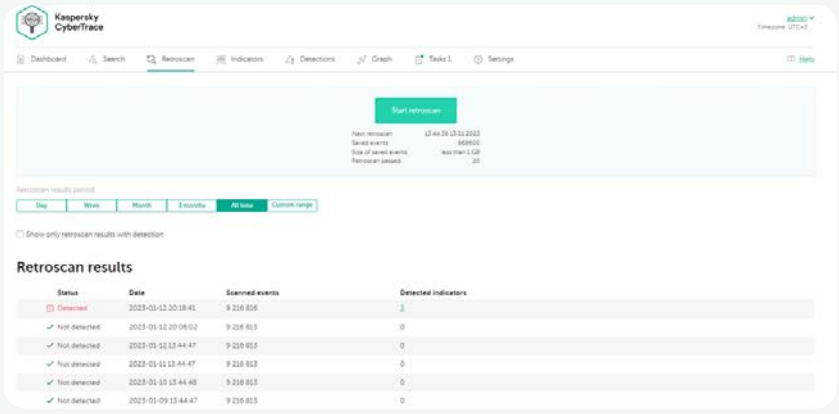
IoCタグ

IoCにタグを付与することで、管理が容易になります。任意のタグを作成し、その重み（重要度）を指定して、IoCに手動でタグを付与するために使用できます。また、タグとその重みに基づいて、IoCの並び替えやフィルタリングを行うことも可能です。



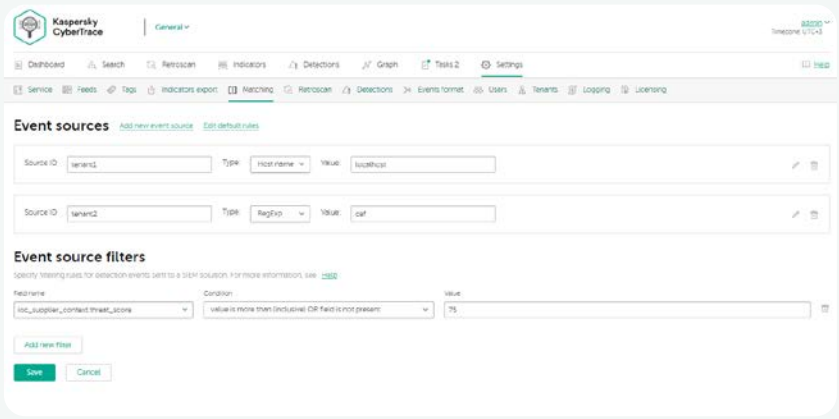
レトロスキャン機能

履歴の関連付け機能（レトロスキャン）を使用すると、最新のフィードを使用して以前にチェックしたイベントの観測値を分析し、以前に検知された脅威を見つけることができます。すべての検知履歴がレポートに記録されるので、将来の調査にこれらを使用することも可能です。



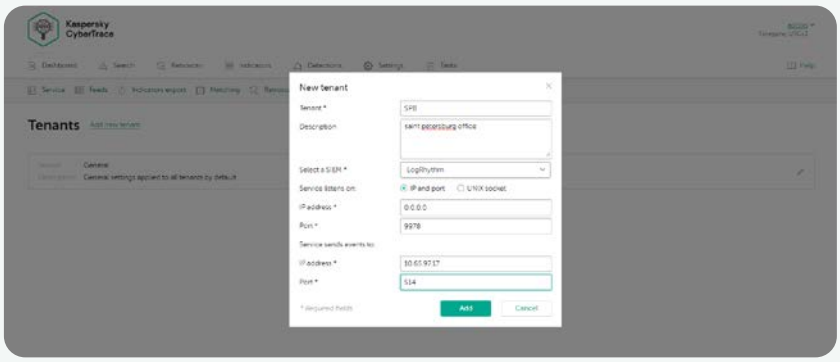
イベントソースフィルター

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使用できます。



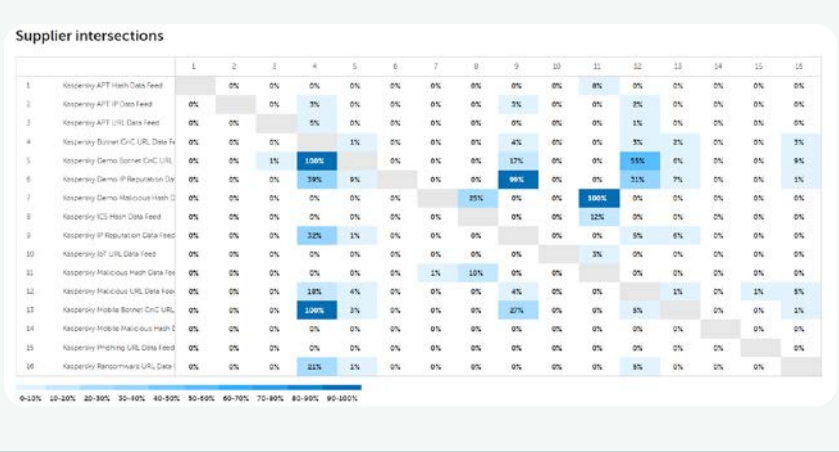
マルチテナンシーのサポート

マルチテナンシーは、MSSPや大企業のユースケースをサポートします。たとえば、サービスプロバイダー（本社）が異なる支社（テナント）からのイベントを個別に処理する必要がある時などです。これにより、1つのKaspersky CyberTraceインスタンスを異なるテナントの異なるSIEMソリューションと接続し、テナントごとに使用するフィードを設定することができます。



インジケーターの統計とフィード交差マトリクス

統合されたフィードの有効性を測定するためのフィード使用統計とフィード交差マトリックスは、最も価値のある脅威インテリジェンスの提供元の選択に役立ちます。



HTTP RestAPIによる脅威インテリジェンスの検索と管理

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行うことができます。Kasperskyのインシデント監視、分析、レスポンスプラットフォームとの統合が可能です。

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コネクターにより、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インジケーター（ハッシュ、IPアドレス、ドメイン、URL）をオンデマンドでルックアップ
- 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により、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
- その他、多数の機能を実装しています

Kaspersky CyberTraceとKaspersky Threat Data Feedsはそれぞれ単独で使用することも可能ですが、併用することで脅威検知能力を大幅に強化することができます。また、サイバー脅威の全体的な可視化により、セキュリティ運用も強化されます。

Kaspersky CyberTraceと Kaspersky Threat Data Feedsの併用により、組織が実現可能な活動：

セキュリティアラートの効果的な抽出と優先順位付け。

アナリストの作業負荷の軽減と過労の防止。

重要なアラートをすぐに特定し、より詳細な情報に基づいてインシデントレスポンスチームへのエスカレーションを決定。

インテリジェンスに基づいた予防的な防御体制の構築。

Kaspersky CyberTrace

詳細はこちら

www.kaspersky.co.jp

#kaspersky
#bringonthefuture