kaspersky

「Kaspersky CyberTrace」のご紹介
～SIEMと脅威データフィードを統合したサイバー攻撃対策～

2023年01月19日
株式会社カスペルスキー
セールスエンジニアリング本部

V1.0

Kaspersky CyberTrace とは

Kaspersky CyberTrace

- Firewall、Proxy、Mailサーバーなどのログと脅威データを高速に突合し脅威分析を容易にするツール
- 主要なSIEMとの連携プラグインを用意
- OSINT 脅威データの使用も可能*
- 読み込んだ脅威データを検索するlookup機能 *

＊CyberTraceのライセンスタイプにより使用出来る機能が異なります。
P25を参照

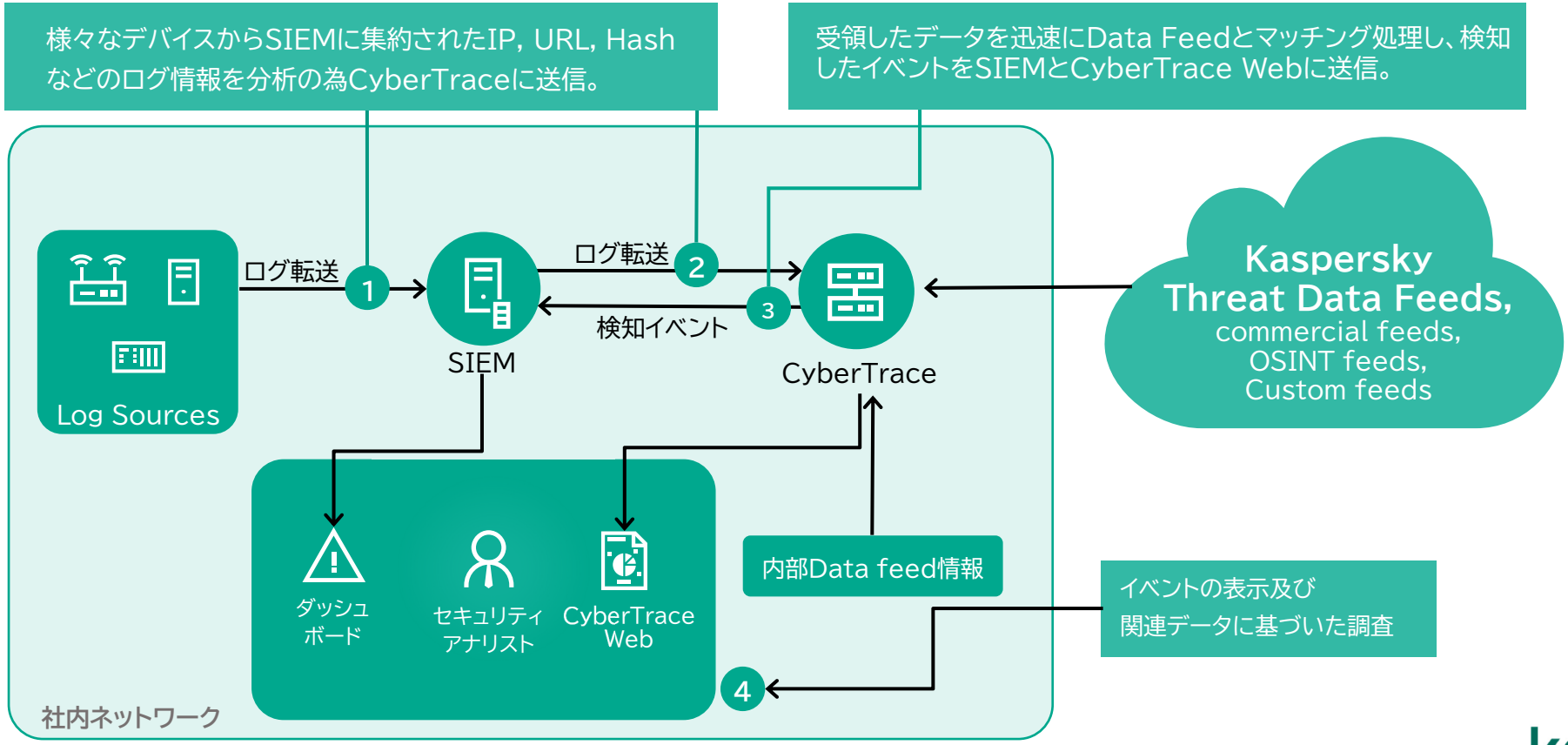
kaspersky

Kaspersky CyberTrace とは

SIEMと脅威インテリジェンスを統合、効率的なデータ照合を実現

・既存のSIEMなどのセキュリティワークフローと脅威データフィードを統合することで、SIEMに集められたログと
カスペルスキーの脅威データベース：Threat Data Feedsを自動的に照合し、リアルタイムな「状況認識」を実現します。

・受信したデータの解析・照合はCyberTrace内部で処理する為、SIEMのパフォーマンスに影響を及ぼすことがありません。



Kaspersky Threat Data Feed：脅威データフィード

Kaspersky CyberTrace

高品質なIoCとコンテキスト情報を提供

・膨大なレピュテーション情報と標的型攻撃などの様々な脅威を調査・分析する専門チームのナレッジを統合し、絶えず更新されるC&Cサーバーや悪意のあるURL、マルウェアのハッシュ値などのIoCとサイバー脅威に関する最新情報を提供。

脅威データフィード名	フィードに含まれる情報
Malicious URL	悪意のあるリンクやウェブサイトを含むコンテキストを持つURLマスクのセット
Phishing URL feed	フィッシング・リンクやウェブサイトを含むコンテキストを持つURLマスクのセット
Botnet C&C URL Feed	デスクトップ・ボットネットのC&Cサーバーや関連する悪意のあるオブジェクトを含むURLマスクのセット
Malicious Hash Feed	最も危険で広く普及している新興のマルウェアに対応するコンテキストを持つファイルハッシュのセット
Mobile Malicious Hash Feed	AndroidおよびiPhoneのモバイルプラットフォームに感染する悪意のあるオブジェクトを検出するために対応するコンテキストを持つファイルハッシュのセット
Mobile Botnet C&C Feed	モバイル・ボットネットのC&Cサーバのコンテキストを含むURLのセット
IP Reputation Feed	疑わしいホストや悪意のあるホストのさまざまなカテゴリを示すコンテキストを持つIPアドレスのセット
Ransomware URL feed	ランサムウェアのリンクやWebサイトを含むURL、ドメイン、ホストのセット
IoT URL Data Feed	IoTデバイスに感染するマルウェアのホスティングに使用されるサイトのコンテキストを含むURLセット。マルウェアのハッシュ値も提供
ICS Hash Data Feed	産業用制御システムのインフラストラクチャ(ICS)を攻撃するために使用される悪意のあるオブジェクトに対応するコンテキストを持つファイル・ハッシュのセット
APT URL Feed	悪意のあるAPTキャンペーンで使用されるインフラストラクチャの一部であるドメインのセット
APT IP Feed	悪意のあるAPTキャンペーンで使用されるインフラストラクチャの一部であるIPアドレスのセット
APT Hash Feed	APTアクターがAPTキャンペーンを行う際に使用する悪意のあるアーティファクトをカバーするハッシュのセット

kaspersky

SIEMとの連携

Kaspersky CyberTrace

プラグインを使用して、主要SIEMとの統合が「簡単に」実施可能

・CyberTraceのインストールパッケージに含まれるSIEM用プラグインを使用することで、簡単にSIEMとの連携が可能。

＜プラグイン対応SIEM一覧＞

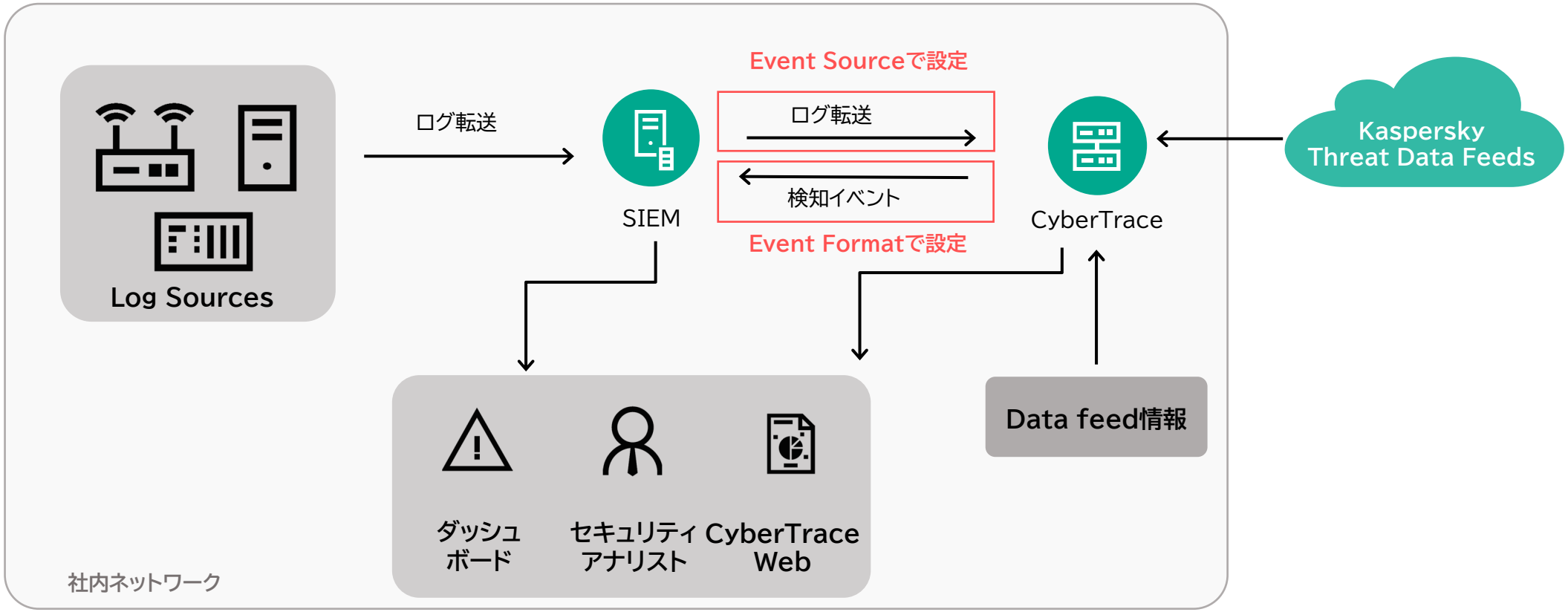
SIEM	Supported
ArcSight An HP Company	✓
splunk>	✓
QRadar®	✓
LogRhythm™	✓
RSA NetWitness	✓

kaspersky

基本設定

抽出条件と出力データ条件を設定するだけで利用可能

・「Event Source（ログから取得するデータの抽出条件）」と「Event Format（脅威検出時のSIEMへの出力データ条件）」を設定することでSIEMからCyberTraceに転送されたログと脅威データフィードの照合が可能になります。



データ抽出:Event Source とは

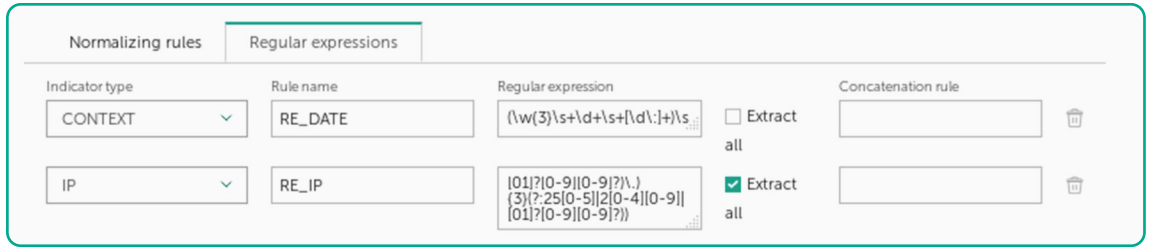
Kaspersky CyberTrace

SIEMから転送されたログから取得するデータの抽出条件

・SIEMからCyberTraceに転送されたログから脅威データフィードと照合したいIPアドレス・URL・ハッシュ値の情報や脅威検知時のアラートに表示したい日時・デバイスIDなどの情報をログから抽出するために定義された正規表現のルールのこと。

・ログ形式ごとのEvent Source設定をすることで、異なるデータ形式のログがCyberTraceに転送された場合でも、必要なデータの 抽出が可能。

<データ抽出ルール例>



Indicator type	ログから抽出されるデータのタイプ。 URL/MD5/SHA1(256)/HASH/IP/DOMAIN/CONTEXTから選択
Rule Name	ルール名。データ出力時はルール名を「%」で囲むことで変数として使用可能
Regular expression	データ抽出の為の正規表現
Extract all	チェックボックスがON ：正規表現に当てはまるデータをログ内の全て抽出。 チェックボックスがOFF：正規表現に1つでもデータが当てはまった段階で処理を終了。
Concatenation rule	連結ルール（詳細はページ9に記載）

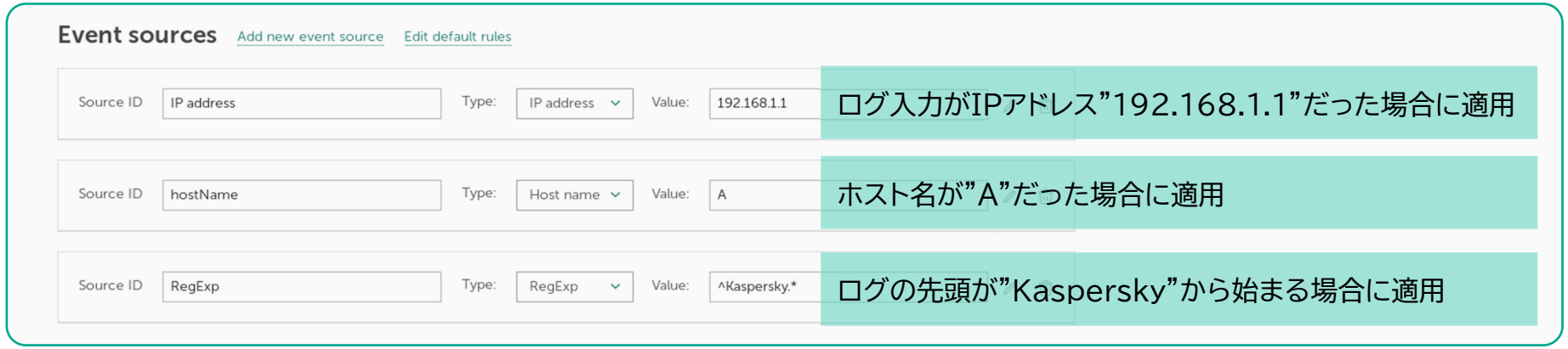
kaspersky

データ抽出:複数のEvent Source作成

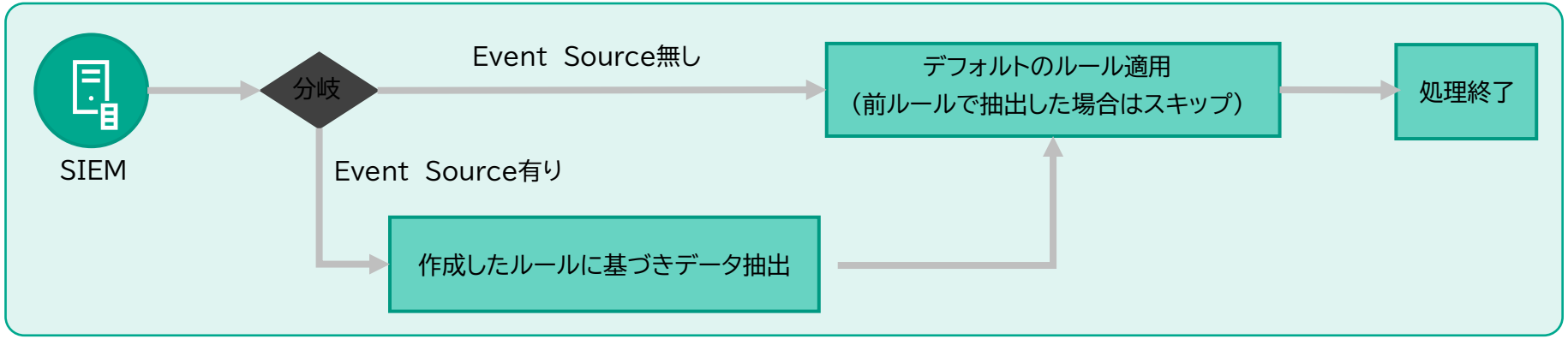
Kaspersky CyberTrace

複数の入力元・データ形式の異なるログでも脅威データベースと照合可能

・複数の入力元からログが転送される場合や同一SIEMから異なるデータ形式のログが転送される場合でも、入力元のIPアドレス・ホスト名やログ内のキーワードごとに適用するEvent Sourceを指定することで、柔軟なデータ抽出が可能です。



<照合処理フロー>



kaspersky

データ抽出：同一SIEMから転送される異なる形式のログ

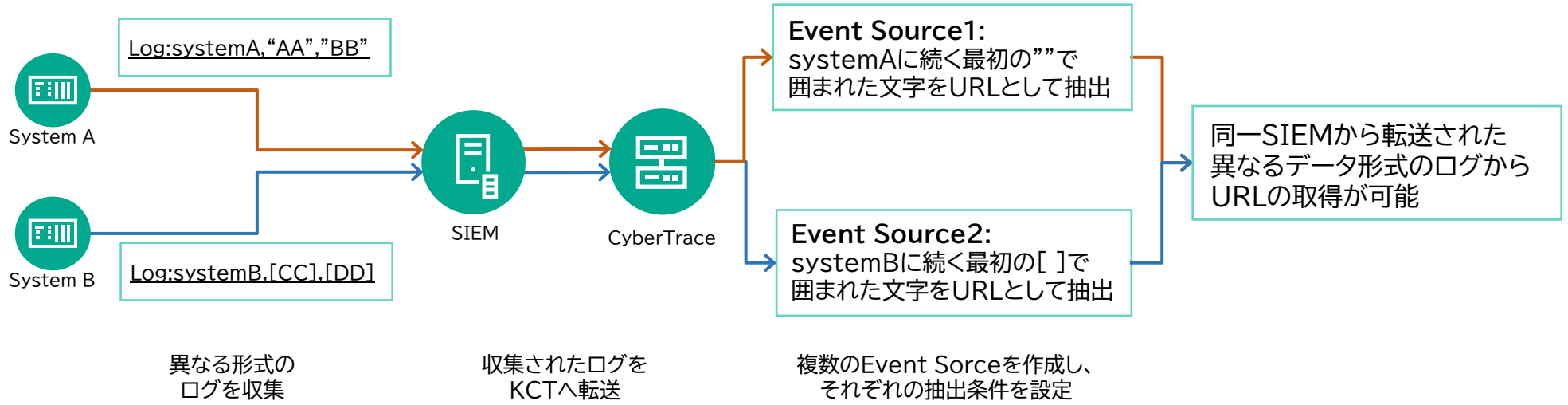
Kaspersky CyberTrace

複数の入力元・データ形式の異なるログでも脅威データベースと照合可能

・ログ内の特定のキーワードからどの抽出ルールを適用するか設定することが可能です。

→同一SIEMから転送された異なるデータ形式のログに対しても適切な抽出ルールが選択され、必要な情報の抽出が可能です。

シナリオ：



kaspersky

データ抽出：連結ルールを使用したデータの並び替え/一部出力

Kaspersky CyberTrace

抽出したデータを自由に並び替え、必要なところのみを出力

・CyberTraceは設定した正規表現にマッチした文字列に#nを付与します。

連結ルールに指定した#nの順にデータが再形成されて出力される為、抽出したデータの並び替えや不要なデータの削除が可能です。

→異なるデータ形式のログも形式を揃えて出力可能

<例:ログから日時を変数”date”に抽出する正規表現を設定した場合>

Log： ”Wed Apr 1 9:30:10”,user@demo.co.jp,”http://xxx.xx.xx

#1 #2 #3 #4 #5 #6

正規表現：(?:”)(¥w{3})¥s(¥w{3})¥s(¥d{1,2})¥s(¥d{1,2}):(¥d{1,2}):(¥d{1,2})(?:”)

＝格納されるデータ

変数”date”：”**Wed Apr 1 9:30:10**”（正規表現に一致した一連のデータが格納されます）

分割データ：「#1=Wed / #2=Apr / #3=1 / #4=9 / #5=30 / #6=10」）（マッチした順に#nの番号が付与されます）

①並び変え

例）連結ルールに[#4:#5:#6 #1/#2/#3]と指定

⇒”9:30:10 Wed/Apr/1”に並び替えて出力

②一部出力

例）連結ルールに[#4:#5:#6]と指定

⇒9:30:10のみ出力 Wed,Apr,1は出力しない

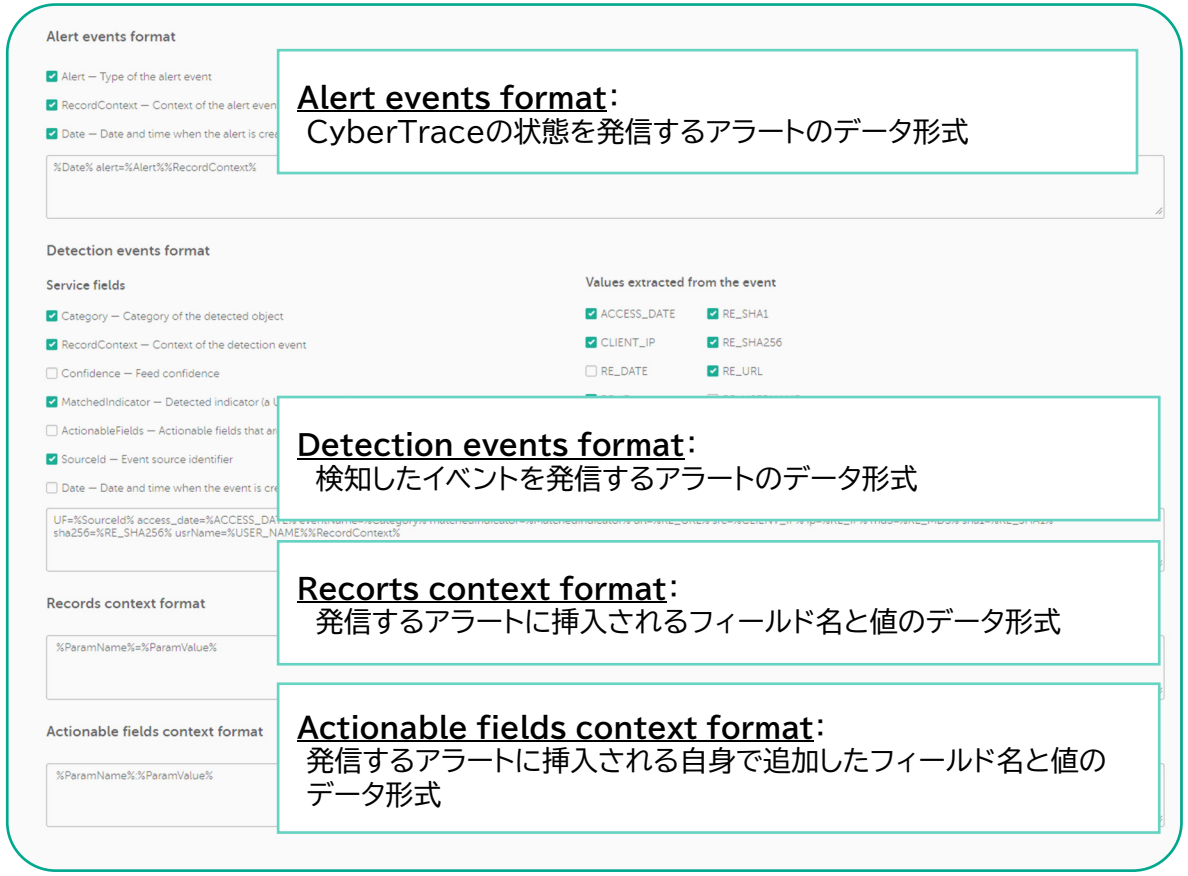
kaspersky

データ出力:Event Format とは

Kaspersky CyberTrace

脅威検知時にSIEMにさまざまな情報を送付

・脅威検知時にSIEMに発信するアラートのフォーマット設定のことで、変数を組み合わせることでSIEMに適用されたEvent Source名、検知したIoCに関する情報、ログの日時といった様々な情報を送付することが可能です。



<Event Format 使用可能変数一覧>

%Alert%	アラートの形式
%RecordContext%	イベントの追加パラメータ イベントのタイプに応じて異なるデータを生成
%Category%	フィールド要素のカテゴリ属性
%ParamName%	フィールド名
%ParamValue%	フィールド値
%MatchedIndicator%	検出されたIndicator(URL,ハッシュまたはIPアドレス)に関する値
%ActionableFields%	脅威インテリジェンスフィードで設定したActionableFieldsの値
%SourceId%	Event SourceのID

kaspersky

脅威データフィード設定

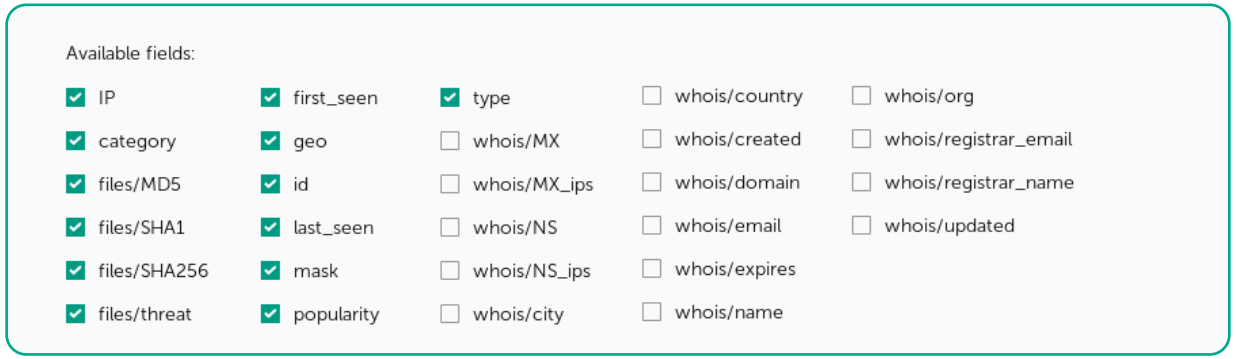
Kaspersky CyberTrace

フィルター条件設定・サードパーティ製の脅威データフィード追加などの柔軟な設定

データ抽出・出力設定以外にも脅威データフィードの使用フィールドを選択したり、フィルター条件を設定することが可能です。

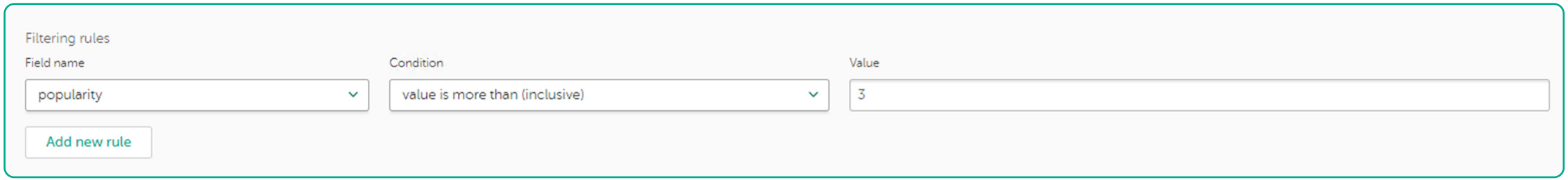
①使用フィールドの選択

-Web UIからチェックボックスのOn/Offを切り替えることで使用するデータの選択が可能です。



②フィルタルールの追加、編集、削除

・フィールドと値(単数・複数・範囲)を設定することでルールのフィルター条件を設定可能です。



kaspersky

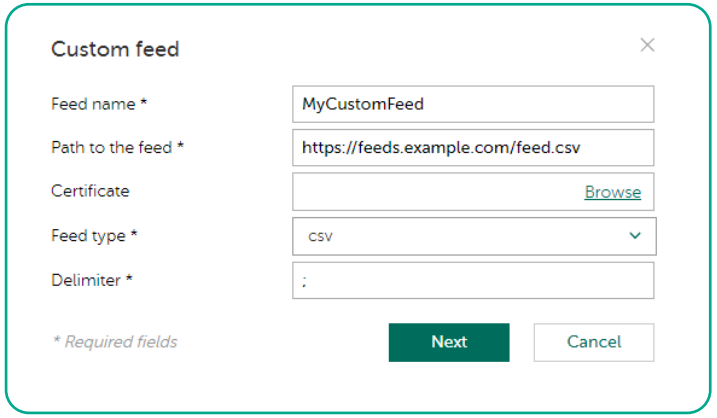
脅威データフィード設定

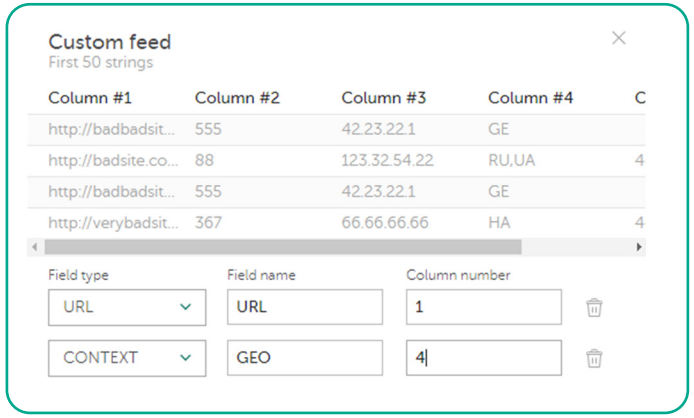
Kaspersky CyberTrace

③Custom Feed

・追加したいフィードのパス・フィールド情報を登録することで、サードパーティ製の脅威データフィードを追加可能です。

・アップデート周期は30分～24時間で設定可能です。





④False Positive list

・登録数の上限無しで検知対象から除外したいURL・ハッシュ値・IPアドレスを登録可能です。

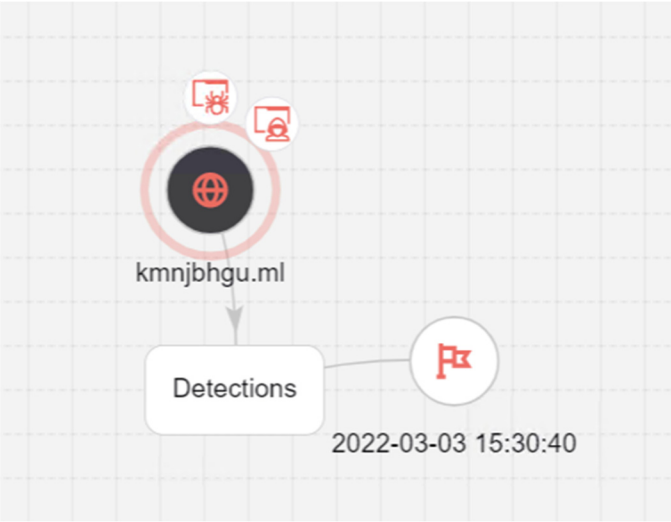
kaspersky

Reseach Graph機能

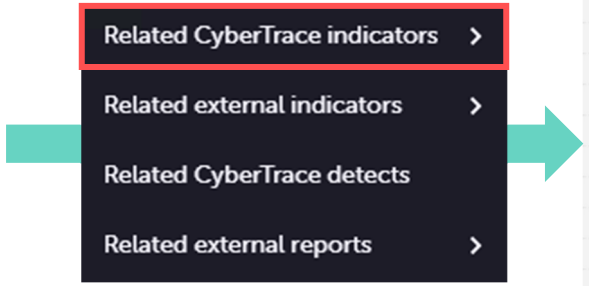
Kaspersky CyberTrace

グラフで脅威を可視化、検知した脅威の関連性と攻撃の全体像を把握

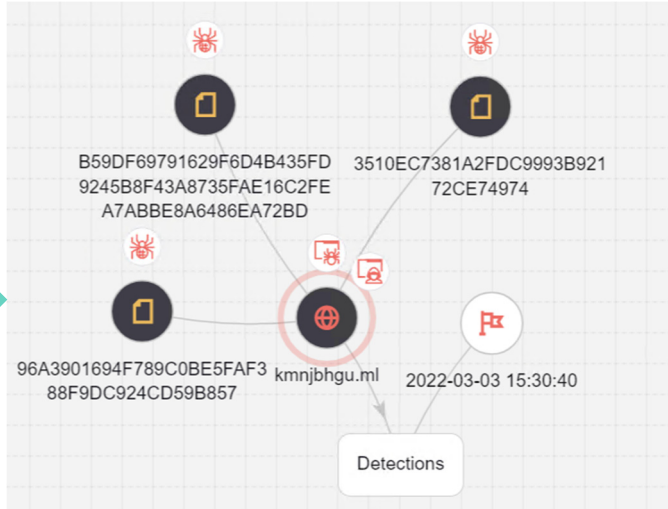
・検知した脅威からグラフを作成し、既知のインジケーター（URL、ドメイン、IPアドレス）との関連性を視覚化することで、インシデントの全体像と規模の把握が可能です。
また、別サービス「Threat Lookup」と連携することで悪意のあるインジケーターに関連する情報の取得が可能です。



検知情報からグラフの作成が可能
ただし、この状態では検知した悪意あるURLと
検知したログ情報のみが表示



検知した悪意あるURLに関連する
既知のインジケーターを取得



悪意あるURLに関連する
既知のインジケーターがグラフに表示

悪意あるURLからダウンロードされた
ファイルのハッシュ値やIPアドレスを返した
DNSサーバー等の情報との関連性を可視化

kaspersky

Retrospective(Retro)スキャン機能

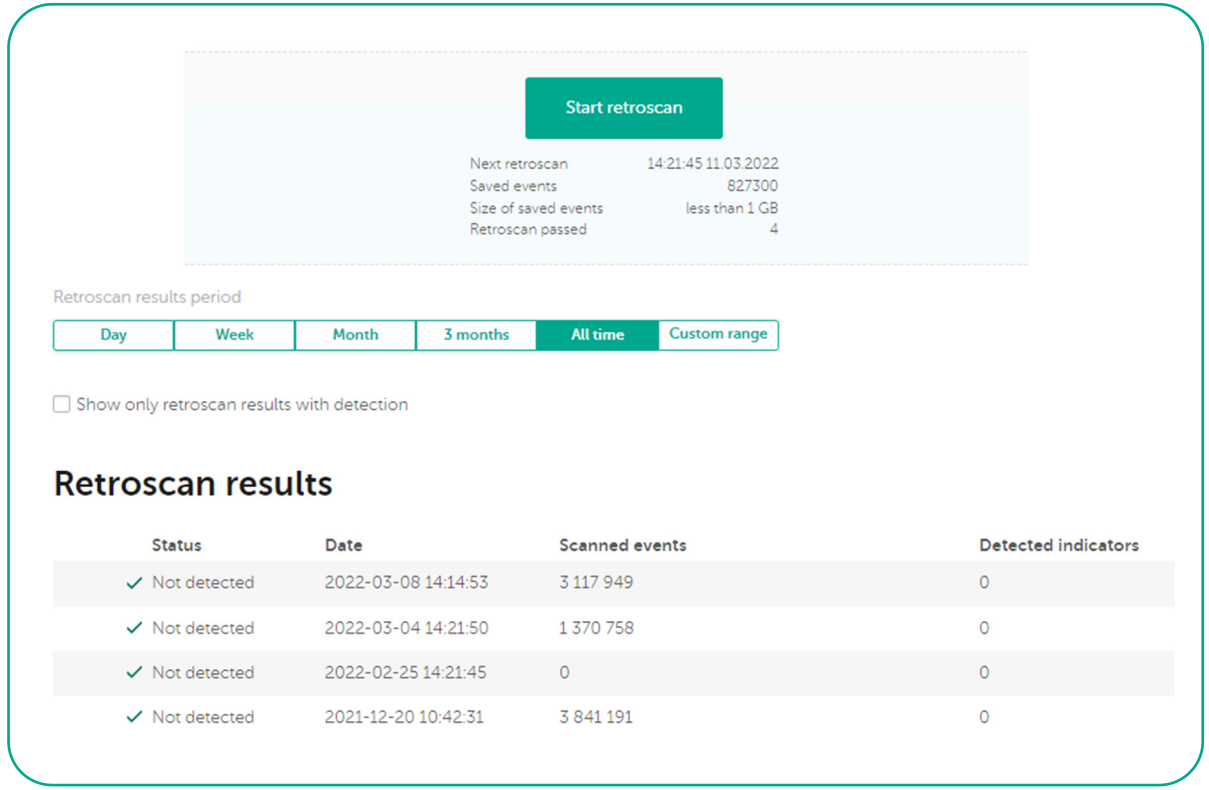
Kaspersky CyberTrace

一度スキャンしたログと最新の脅威データフィードを再度照合し、新たな脅威を検知

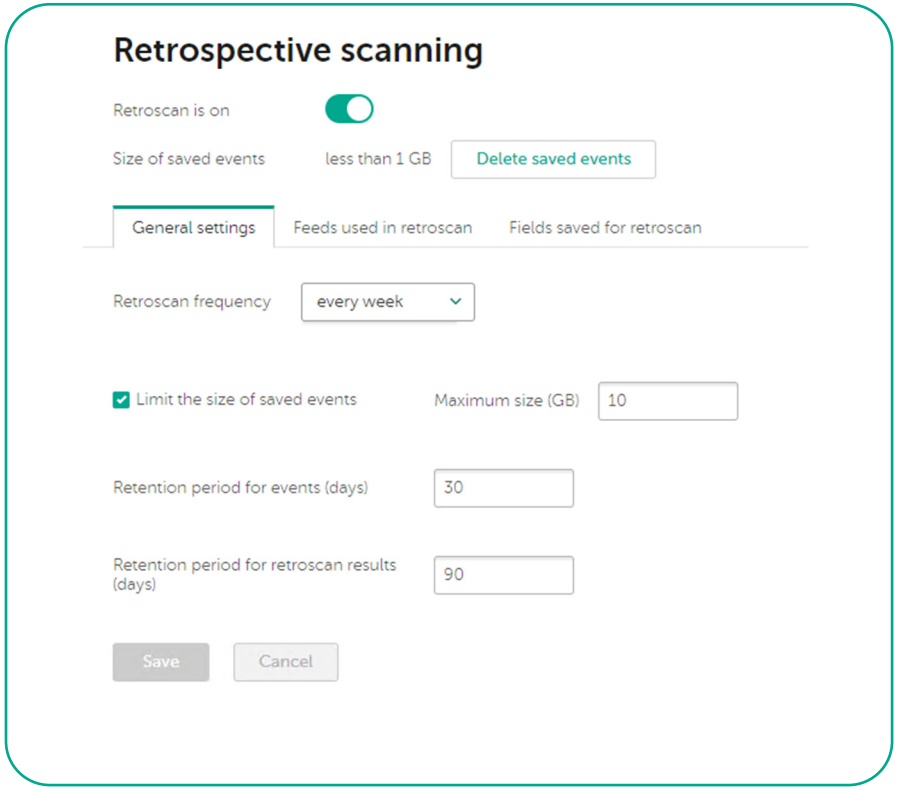
脅威が検知されなかったログを一定期間保持し、設定された周期ごとに再度ログと脅威データフィードを照合します。

->最新の情報が更新された脅威データフィードとスキャン済みのログを照合することで、1回目のスキャンでは検知出来なかった脅威を検知することが可能です。

<Retroスキャンメイン画面>



<Retroスキャン設定画面>



kaspersky

IoCのタグ付け

Kaspersky CyberTrace

タグを使用してIoCを分類・優先順位付け

・IoCの分類と重要度の管理の為にお客様自身で0～5段階のウェイトを指定したタグをIoCに指定することが可能です。

・付与されたタグごとまたはウエイトの合計（単数、範囲指定）をフィルター条件にIoCを検索・並び替えすることが可能です。

<付与されたタグでフィルター>

Indicators　Add　Mark as false positive　Delete

ioc_value: 192.0.2.* OR (ioc_type: md5 AND ioc_updated_date: >=01.01.2020)

指定したタグを含むIoCを一覧表示

Indicators selected: 0 of 5

Type	Value	Added	Changed	Tag (1)	Total tag weight	Suppliers
URL	xhbxjdbdn.ga	2022-03-10 13:06:31	2022-03-10 13:35:07	CRITICAL	5	Malicious_URL_Data_Feed, Ransomware_URL_Data_Feed
URL	iuqaknub.org	2022-03-09 15:35:20	2022-03-10 13:35:07	APT, CRITICAL	10	Malicious_URL_Data_Feed, Botnet_CnC_URL_Data_Feed, Ransomware_URL_Data_Feed
URL	networki.duckdn...	2022-03-10 13:34:11	2022-03-10 13:34:11	CRITICAL	5	Malicious_URL_Data_Feed

<ウエイトの合計でフィルター>

指定したウエイトの範囲に含まれるIoCを一覧表示

Type	Value	Added	Changed	Tag	Total tag weight	Suppliers
URL	xhbxjdbdn.ga	2022-03-10 13:06:31	2022-03-10 13:35:07	CRITICAL	5	Malicious_URL_Data_Feed, Ransomware_URL_Data_Feed
URL	d3etwai8fde30c....	2022-03-09 18:00:12	2022-03-10 13:35:07	DANGEROUS	4	Malicious_URL_Data_Feed, Ransomware_URL_Data_Feed
URL	iuqaknub.org	2022-03-09 15:35:20	2022-03-10 13:35:07	APT, CRITICAL	10	Malicious_URL_Data_Feed, Botnet_CnC_URL_Data_Feed, Ransomware_URL_Data_Feed
URL	psd2-kunde4453...	2022-03-10 13:34:17	2022-03-10 13:34:17	INFO	0	Phishing_URL_Data_Feed
URL	111.241.219.138	2022-03-10 13:34:17	2022-03-10 13:34:17	WARNING	3	Phishing_URL_Data_Feed

kaspersky

IoCのエクスポート

Kaspersky CyberTrace

フィルター条件に一致するIoCをエクスポート

・フィルター条件に一致するIoCをCSV形式でエクスポートするタスクが作成可能です。

・検索条件はIoC作成日(更新日)・IoCタイプ・タグ名・タグのウェイトなどから選択可能です。

＜フィルター条件例:2023年1月1日以降に更新されたIoCタイプが「MD5」のIoC ＞

Fields to export

	Field name	Condition	Value	Include	Output name
	ioc_updated_date	date is more than (inclusive)	2023-01-01	☑	ioc_updated_date
AND	ioc_type	value is equal to	MD5	☑	ioc_type
AND	ioc_value	value is non-empty		☑	ioc_value

一致するIoCを

CSV形式でエクスポート

	A	B	C
1	#ioc_updated_date	ioc_type	ioc_value
2	2023-01-19T02:52:30.241533Z	MD5	0[redacted]F1
3	2023-01-19T02:52:30.241533Z	MD5	0[redacted]F0
4	2023-01-19T02:52:30.241533Z	MD5	0[redacted]C92
5	2023-01-19T02:52:30.241533Z	MD5	0[redacted]E51
6	2023-01-19T02:52:30.241533Z	MD5	0[redacted]F7A
7	2023-01-19T02:52:30.241533Z	MD5	0[redacted]3A6
8	2023-01-19T02:52:30.241533Z	MD5	0[redacted]538
9	2023-01-19T02:52:30.241533Z	MD5	0[redacted]B0
10	2023-01-19T02:52:30.241533Z	MD5	0[redacted]14

kaspersky

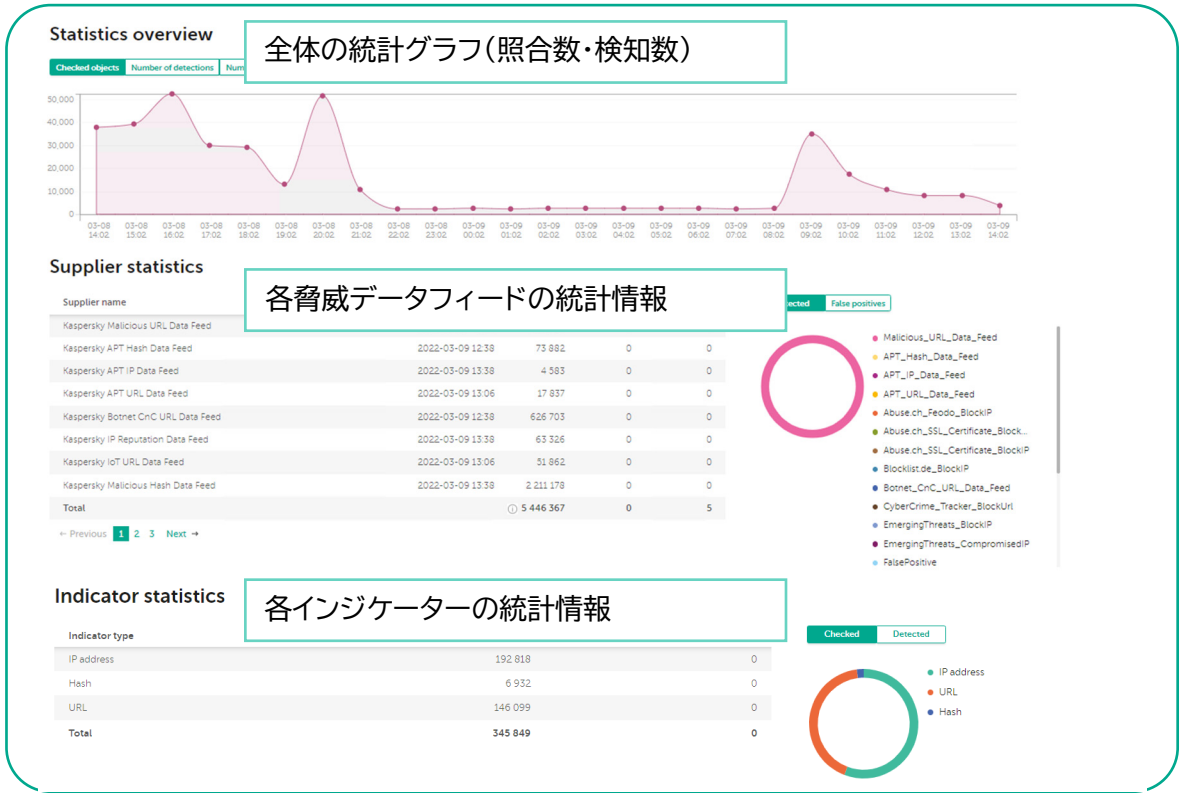
Web UI

Kaspersky CyberTrace

CyberTraceの照合情報・脅威データフィード情報をグラフで可視化

■ダッシュボード

・各脅威データフィードの統計情報(レコード数・検知数)や各インジケーター(URL・ハッシュ・IPアドレス)の統計情報(照合数・検知数)をダッシュボードから確認可能です。



kaspersky

Web UI

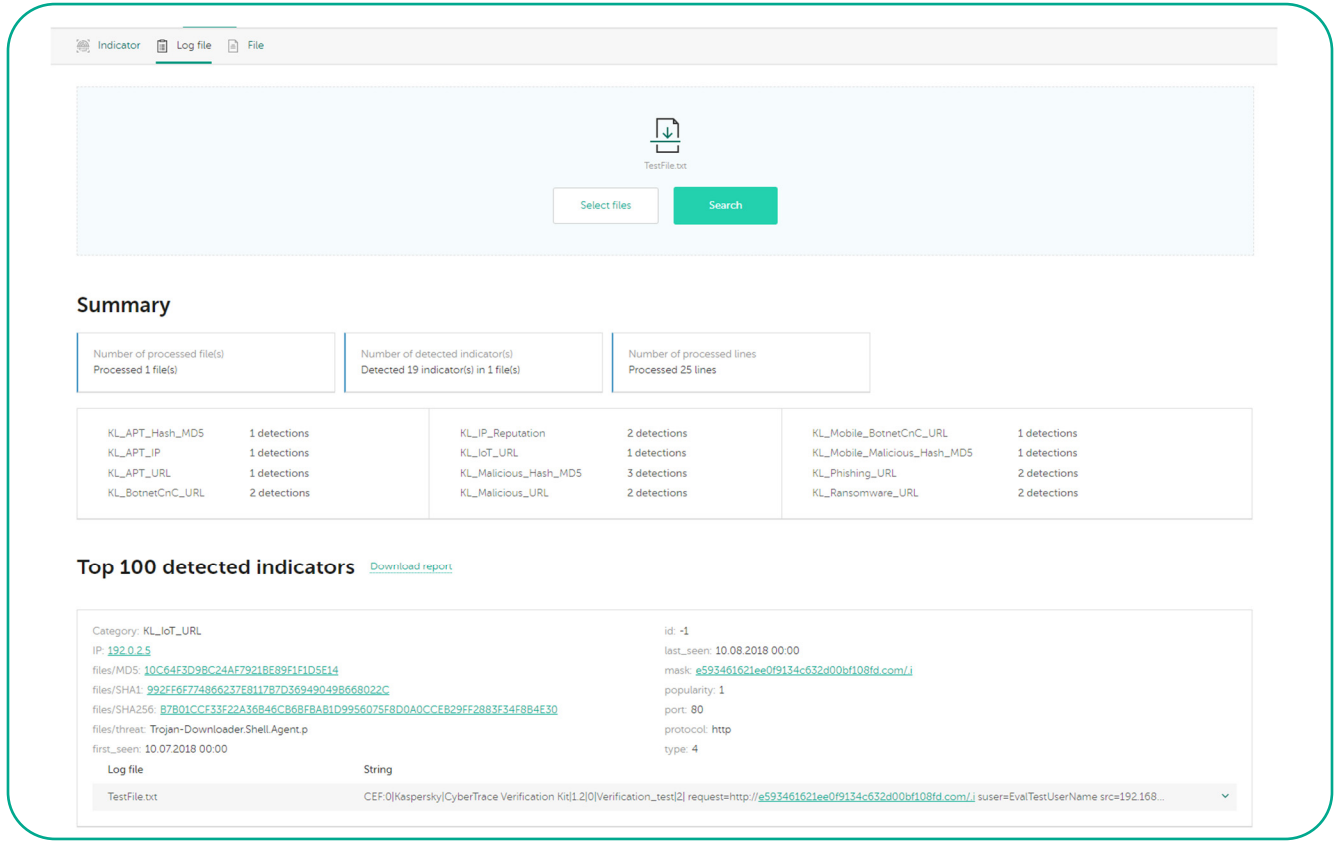
Kaspersky CyberTrace

特定のキーワード・ハッシュ値を脅威データフィードから検索

■Lookup機能

・URL/ハッシュ/IPアドレスをキーワードに脅威インテリジェンス情報を検索することが可能です。

-直接入力による単一検索・ログファイルに含まれるIoCの複数検索・ファイルハッシュ値の3種類の方法で検索



kaspersky

ライセンス体系

Kaspersky CyberTrace

・CyberTraceは適用するライセンスによって利用出来る機能が以下の通り異なります。

	EPS limit(※2)	IoCの ダウンロード上限	Lookup機能	サードパーティ製 脅威データフィードの 使用	マルチユーザー	マルチテナンシー	IoCの エクスポート
Community Edition (無償)	250	100万個まで (脅威データレコード数)	○	○	×	×	○
Feed matcher (有償)(※1)	無制限	無制限	×	×	×	×	×
MSSP feed matcher (有償)	※3	無制限	×	×	×	○	×
TI platform (有償)	無制限	無制限	○	○	○	○	○
MSSP TI platform (有償)	※3	無制限	○	○	○	○	○

※1: Threat Data Feedsをご契約の場合、無償での提供となります。

※2: EPS = Event Per Second。1秒間に照合可能なイベント数のことで、ライセンスで定義された数値を超えた照合は出来ません。

※3: 契約時にお客様環境に適した数値のライセンスが発行されます。

kaspersky

kaspersky