KELA
TARGETED CYBER INTELLIGENCE

お客様を標的としているサイバー攻撃を未然に防ぐために
元イスラエル国防軍インテリジェンス部隊に在籍していた
サイバーセキュリティ専門家がダークネットを調査し、
適切な対処方法をアドバイス

お客様のこんな悩みを解決します！

- 情報の流出による被害を事前に察知したい。
- リモートワークにより社内システムへの外部接続が増加しているが、ネットワーク脆弱性があるか外部から調査してほしい。
- 自社がサイバー攻撃のターゲットになっているかを調査したい。
- サイバーセキュリティの専門家の支援が欲しい。

リモートワークにおける
標的型脅威インテリジェンス調査サービス

リモートワーク環境に移行したお客様に関する情報を弊社の標的型脅威インテリジェンス・偵察プラットフォームを利用し、インターネット全体（ディープウェブ、ダークウェブを含む）を調査し、脅威情報を分析及びレポートを行うサービスとなります。

1. 調査対象セッティング

お客様と調査対象のミーティングを行い、調査対象のセッティングを行います

IPレンジ、ドメイン名、機密情報・システム情報取引先、提携先、クラウドプロバイダーなど

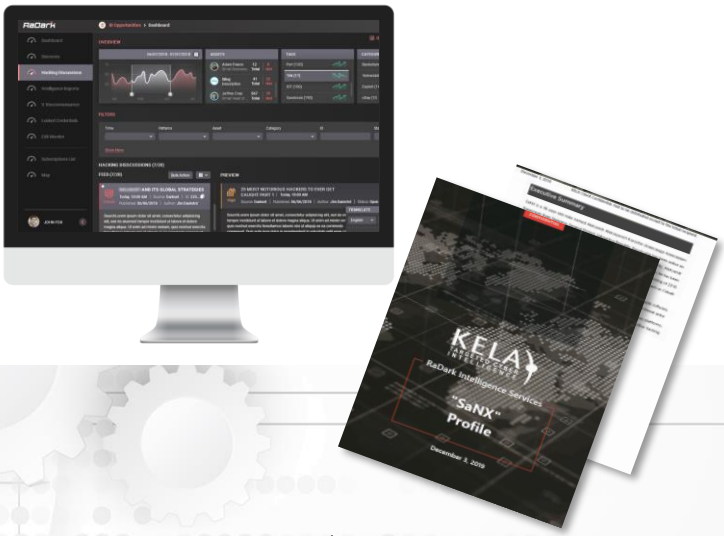
2. 調査対象に対するリサーチ、分析レポート作成

KELA独自の脅威インテリジェンスプラットホームに収集された情報をKELAの脅威インテリジェンス専門家が調査および分析を行います。さらにご要望により、必要な脅威分析レポートを作成します。

3. 分析レポートの結果報告/オンラインミーティング

収集された情報から作成された調査・分析レポートを元にKELAの脅威インテリジェンス専門家による対処方法も含めた結果報告ミーティングを行います。

対処が必要な脅威については、弊社がお客様に代わって対処することも可能です。



＊ご提供価格および詳細につきましては、下記までご問い合わせください。

japan@ke-la.com　お問い合わせ　www.kela.co.jp