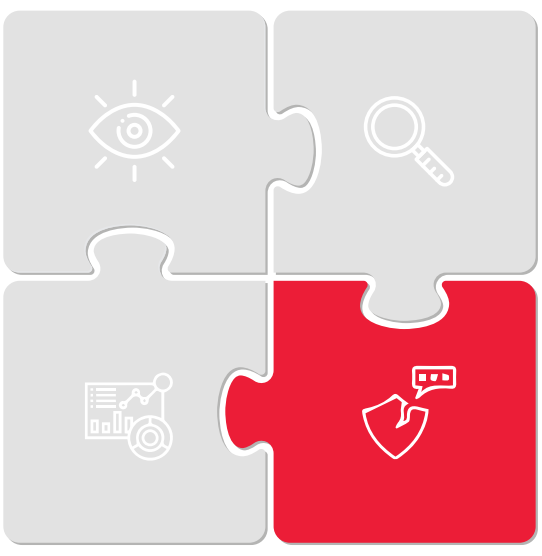
DATASHEET

TECHNICAL INTELLIGENCE

サイバー犯罪活動に悪用されうるIPアドレスやドメインを検知

概要



KELAのTECHNICAL INTELLIGENCEモジュールは、非公開のフォーラムや違法マーケット、サイバー犯罪商品を専門とする自動売買ショップ、サイバー犯罪者の使用するインスタントメッセージチャンネル、その他様々なソースをクローリングして、侵害・悪用されている可能性のあるIPアドレスやドメインをお客様に通知します。本モジュールは、現在お客様が使用されている他のセキュリティ製品とも容易に連携していただけます。（本モジュールのデータは、KELAのAPI経由で機械可読式フィードとしてご提供しております。）

サイバー犯罪者に侵害されたネットワーク資産は、今後攻撃用インフラストラクチャ（C2サーバーなど）として悪用されたり、フィッシング攻撃のベクトルとして利用される可能性があります。
自組織のネットワーク資産を監視し、侵害状況をいち早く把握するツールとして、KELAのTECHNICAL INTELLIGENCEをご活用ください。

仕組み

データ収集

自動化されたKELAのサイバーインテリジェンステクノロジーが、アンダーグラウンドのサイバー犯罪社会に投稿されたメッセージや画像の他、様々なデータ形式で流通する情報を継続的に収集します。

分析・抽出

収集したデータを背景情報やソースの信頼性に基づいて分析し、侵害された可能性のある資産を検出してIPアドレスやドメインなどの指標を表示します。

データの正規化

検知した資産やその背景情報、STIXなどのMRTI*を、KELAやSnowflakeのAPI経由で機械可読形式の構造化データとしてご提供します。*機械可読型脅威インテリジェンス

プロアクティブな防御の支援

侵害が検知された資産へのアクセス状況をTECHNICAL INTELLIGENCEモジュールで監視し遮断することで潜在的リスクをプロアクティブに解消していただけます。

ユースケース

実用的な脅威インテリジェンス

KELAのTECHNICAL INTELLIGENCEで実用的なサイバー犯罪脅威インテリジェンスを入手し、お客様のネットワークインフラストラクチャが侵害されたり、悪用される事態を未然に阻止することが可能となります。

脅威ハンティング能力の強化

KELAのTECHNICAL INTELLIGENCEを調査業務に取り入れることで、お客様の脅威ハンティング能力を強化していただけます。

特長

シームレスな連携

TECHNICAL INTELLIGENCEの機械可読形式データは、お客様が現在使用されているSIEMやSOAR、その他様々なセキュリティ製品とも簡単に連携していただけます。
（STIXフォーマットやその他のフィールド形式にてご利用いただけます。）

広範なカバー領域

KELAのTECHNICAL INTELLIGENCEには、広範なサイバー犯罪ソースから収集されたリアルタイムな情報が含まれています。
お客様と関連のあるサイバー脅威について、最新のインテリジェンスをご利用いただけます。

最新情報をリアルタイムに取得

脅威アクターが侵害し、サイバー犯罪コミュニティ等で言及したIPアドレスやドメインの最新情報をリアルタイムに入手することで、自組織を防御することが可能となります。事前の対策をとり、お客様を狙いうる攻撃者の先を行く一助としてご活用ください。

背景情報を取り入れたインテリジェンス

脅威アクターが組織の資産を侵害する手法やインテリジェンスソースの詳細を知ることで、各脅威に対する理解を深めていただけます。

www.kelacyber.com/ja / marketing@ke-la.com / 03-6634-7836