DATASHEET

KELA

EMPOWERED BY KELA

IDENTITY GUARD

不正アクセスされたアカウント情報を能動的に保護

あらゆるモノが高度につながりあう現在のデジタル社会において、組織のデジタル資産を保護することは最優先の課題となっています。

クラウドサービスプロバイダーは常に不正アクセスのリスクにさらされており、いまやあらゆる規模の企業が、激しさを増す脅威に慢性的に脅かされています。その一方で、アンダーグラウンドのサイバー犯罪者が集うダークウェブのマーケットでは、**不正アクセスされたアカウント情報**が販売されています。

マーケットで販売されているアカウント情報は、悪意あるアクターが企業のネットワークに侵入して機密データを窃取し、大規模な被害をもたらす足掛かりに悪用されています。

IDENTITY GUARD

不正アクセスされたアカウント情報を能動的に保護するリアルタイムなソリューション

KELAのIDENTITY GUARDは、不正アクセスされたアカウント情報の中から**お客様組織のFQDN*と関連がある**情報（ドメインやサブドメイン、SaaS上でご利用中のアカウントなど）を特定します。本モジュールは大量のデータセット（ボット数：1,000万台超、アカウント数：3億件超）を監視し、お客様組織の情報を特定した後は、関係者の皆様にリアルタイムなアラート＆実際の対応に役立つ有用な情報を送信し、効率的な脅威対応を行えるよう支援します。

また、既存のセキュリティ製品やサービスともシームレスに連携し、不正アクセスされたアカウント情報やマルウエアに感染した端末の検知作業を自動化します。

**FQDN*（完全修飾ドメイン名）は、DNSの階層構造において、全てを表記したドメイン名。ドメインとサブドメインの両方が含まれており、インターネット上での正確な位置情報を示します。*

主な機能＆特長

簡単なセルフ・セットアップ

監視対象アセット提案機能で簡単にセットアップし、インシデントにもスピーディに対応することができます。

重大度に基づいた分類

不正アクセスされたアカウント情報を重大度に基づいて自動で分類し、適切なトリアージとリソースの割り当てを実現します。

Webhookによる自動化で効率性を向上

インテグレーション作業を簡素化することで、モジュールとチーム、アプリ間におけるスムーズなコミュニケーションを実現。直感的なセットアップマニュアルが様々なワークフローのシームレスな立ち上げをサポートします。

SaaSアカウントの保護

クラウドサービス上で使用している企業アカウントのセキュリティを強化します。

不正アクセスのリスクをより効率的＆効果的に管理

監視＆検知

少ないリソースでも効率的に監視：
少人数のセキュリティチームでも、不正アクセスされたアカウント情報を効率的に監視し、リスクを緩和することができます。

直感的なフィルタリング：
ユーザーフレンドリーなインターフェースで、重大度や脅威、サードパーティプロバイダー、サービスの種類、その他様々な条件に基づいたフィルタリングを実行することができます。

不正アクセスされたアカウント情報を検知＆フィード：
重大度のレベルを表示したり、ステータス（解決済み／未解決など）を更新することもできます。

情報を分かりやすく可視化：
選択したフィルタリング条件に基づいてセグメント化した統計データを分かりやすいグラフ形式にして表示することで、情報に基づいた効率的な対応を支援します。

詳細な背景情報：
不正アクセスされたアカウント情報を検知した場合、関連するサービスや脅威、その他の詳細情報も表示します。

データの最適化＆即時対応

関連のあるデータに特化：
IDENTITY GUARDは、選択されたフィルターと重大度に基づいて、データの検知・トリアージ（優先順位付け）を行います。セキュリティチームが最も影響を受ける領域に対応し、効率的な改善策を実行できるようサポートします。

実用性：
お客様に関連のある重要な情報のみを表示・配信します。

リアルタイムなアラート：
Webhookを使ってアラートを即時送信することにより、タイムリーなインシデント対応を実現します。

即時対応の自動化：
Webhookに対応したアプリケーションを使って、改善ワークフローを開始することができます。

タイムリーなアラート：
直感的なマニュアルを使って、Webhookによるアラート通知を設定することで、重大なイベントや緊急アップデートの発生時にも、精度の高いタイムリーなアラートを受信することができます。

容易なインテグレーション：
Webhookによる自動通知機能を取り入れた複雑なインテグレーションを、簡単に実装することができます。また、シンプルなルールを基にプレイブック（上限数なし）を作成し、Slackなど様々なエンドポイントアプリケーションや社内のセキュリティシステムと連携して、ワークフローを開始することができます。

インシデント対応＆管理

インシデントチケットのトラッキング：
インシデントのチケットを、ステータスに応じてフィルタリングすることができます。現在の対応ステータスを把握したり、今後の監査対応にご利用いただけます。過去のインシデントを検証する必要が生じた場合にも、簡単に情報を取得することができます。

ボットプロファイルの閲覧：
重要なボットのデータをKELAのプラットフォーム上で簡単に確認することができます。インシデントと関連のあるボットの詳細情報を閲覧し、インシデントの分析を深化することができます。

一括アクション：
簡単な操作でWebhookの作成やインシデントのステータス変更を実行し、合理的＆効率的にインシデントを管理することができます。

KELA

無料トライアルを開始

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