KELAGROUP

KELA ULTRARED SLING

脅威インテリジェンスの"次の一手"｜KELA CTIプラットフォームが描く、先を読む防御の未来

Davidi Carmiel
Co-Founder & CEO

Itsik Kesler
CTO

山路 樹
サイバー脅威インテリジェンスエキスパート

KELA Press Conference ｜ 2026年11月5日

2026 ©KELA K.K. | All rights reserved. | KELAcyber.com ULTRARED.ai SLINGscore.com

Davidi’s Welcome Message



KELA

日本における脅威シグナル

2つの異なる脅威トラック：10月にKELA CONTROLにより特定

トラック1・データ窃盗ストリーム

日本のWebおよびAPI資産へのプロービング

約400 **10日間で偵察された日本の組織数（679ホスト、9月29日～10月8日）**

- 同一サーバーが、確認された求人プラットフォームの侵害（最大390万件のメール）に関与
- JPCERT/CCがIPを公表後（10月8日）、Google Cloud Tokyoの141ノードへ移動。KELAが追跡
- 確認された被害組織は1社。残りは調査対象のリード

トラック2・ランサムウェアストリーム

日本のVPNポータルをスキャンするQilinアフィリエイト

12 **1時間以内にスキャンされた日本のGlobalProtect VPNポータル数（8月8日）**

- 他地域で数時間以内にQilinによる暗号化に至ったCVE-2026-0257に一致
- Qilin関連の2つ目のサーバーが10月までVPNポータルのスキャンを継続
- Qilinは日本で最も活発なランサムウェア：10月10日までの30日間で13被害中4件

2つのトラック、2つの防御手法: Qilinの指標ではデータ窃盗を検知できず、逆もまた同様です

出典: *KELA「Qilin and Japan: Attackers Probing Japanese Networks」（2026年10月）、KELA CONTROL* ネットフロー、パッシブDNS、証明書データ。スキャンは標的化を示すものであり、侵害そのものを示すものではありません。

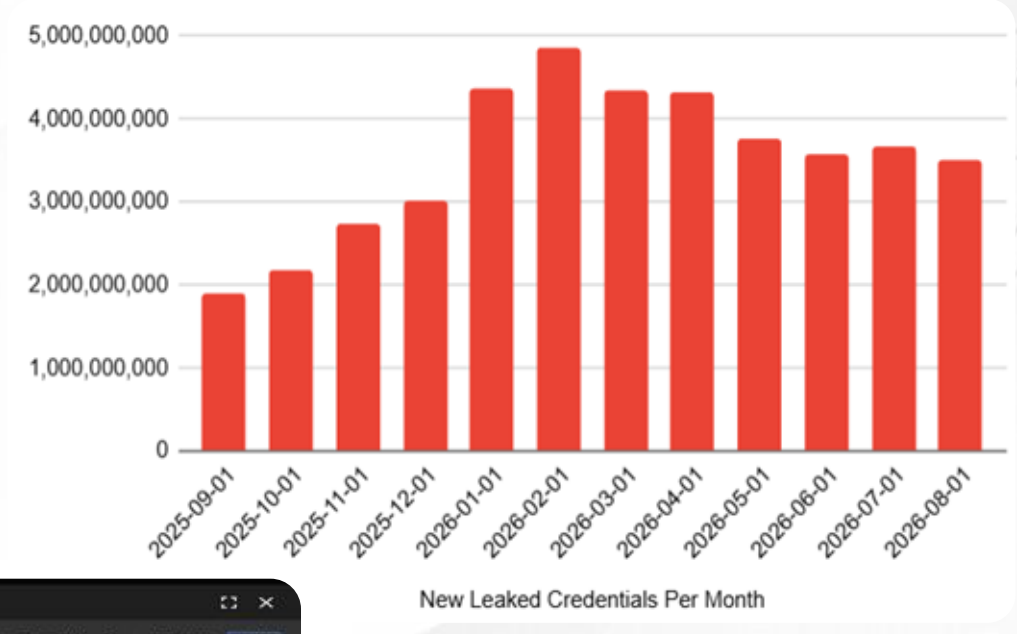
KELA

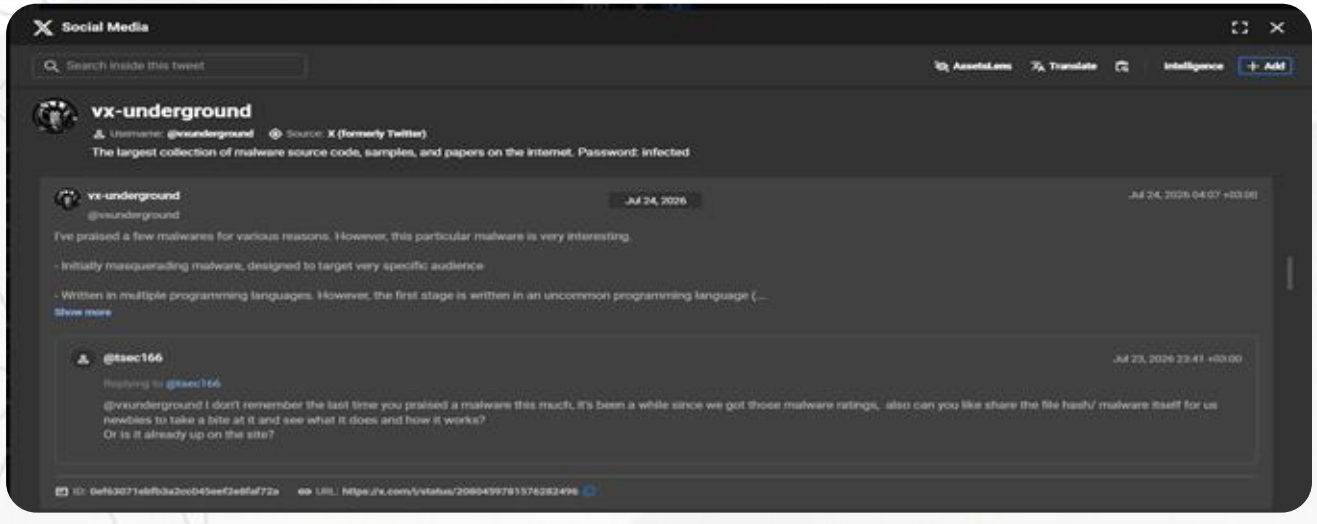
© 2026 KELA. All rights reserved.

データソースの拡大

サイバー犯罪ソースを常に把握し、インテリジェンスを実用的に

- **2,100万台以上**の感染デバイス情報
- **約1,240億件**の漏洩クレデンシャル
- 新しい**Cookieデータセット** – MFAバイパスに使用されるセッションCookieに注力 - 月間**約1億5,000万件**！
- **X (旧Twitter)** のカバレッジを追加
- その他関連するコミュニケーションプラットフォームの継続的な監視





6つの新機能

2026年Q4 新機能

3つの方向性（2026年第4四半期にかけて順次展開）

01 AIネイティブ

KELA AI

プラットフォーム内でのサマリー生成、クライアント資産や脅威に関する文脈情報、オープンチャット機能（逐次提供開始）

Brand Control

AI駆動によるブランド悪用の高度な分析

02 統合 & 連携

KELA MCP

顧客独自AIアシスタントにKELAインテリジェンスを組み込み

Integrations Portal

ワークフロー構築：インサイトを行動へ転換

03 リアルタイム早期警戒

Indicators Research

IP、ドメイン、URL、ハッシュに対する明確な判定

Vulnerability Intelligence

自社資産への脅威の兆候を瞬時にアラート通知

Plus: 統合分析プラットフォーム CONTROLが一般提供開始
（KELAリサーチャーが運用するCICマネージドサービスのオプションあり）

KELA

© 2026 KELA. All rights reserved.

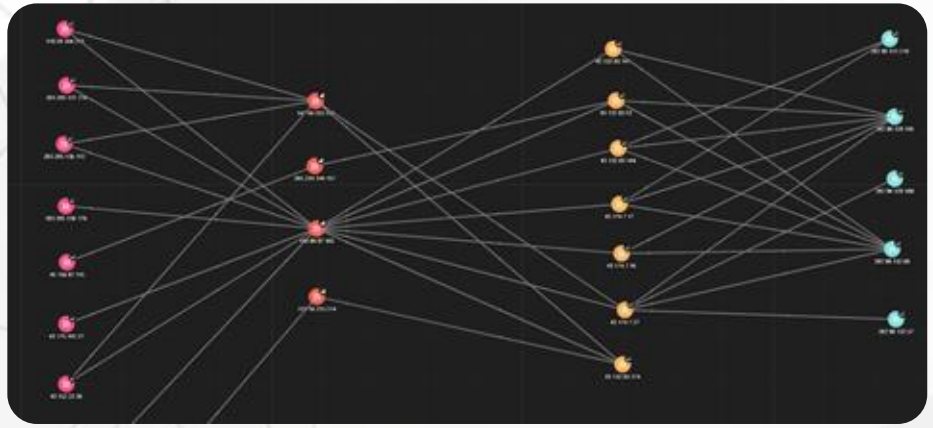
CONTROL プラットフォーム

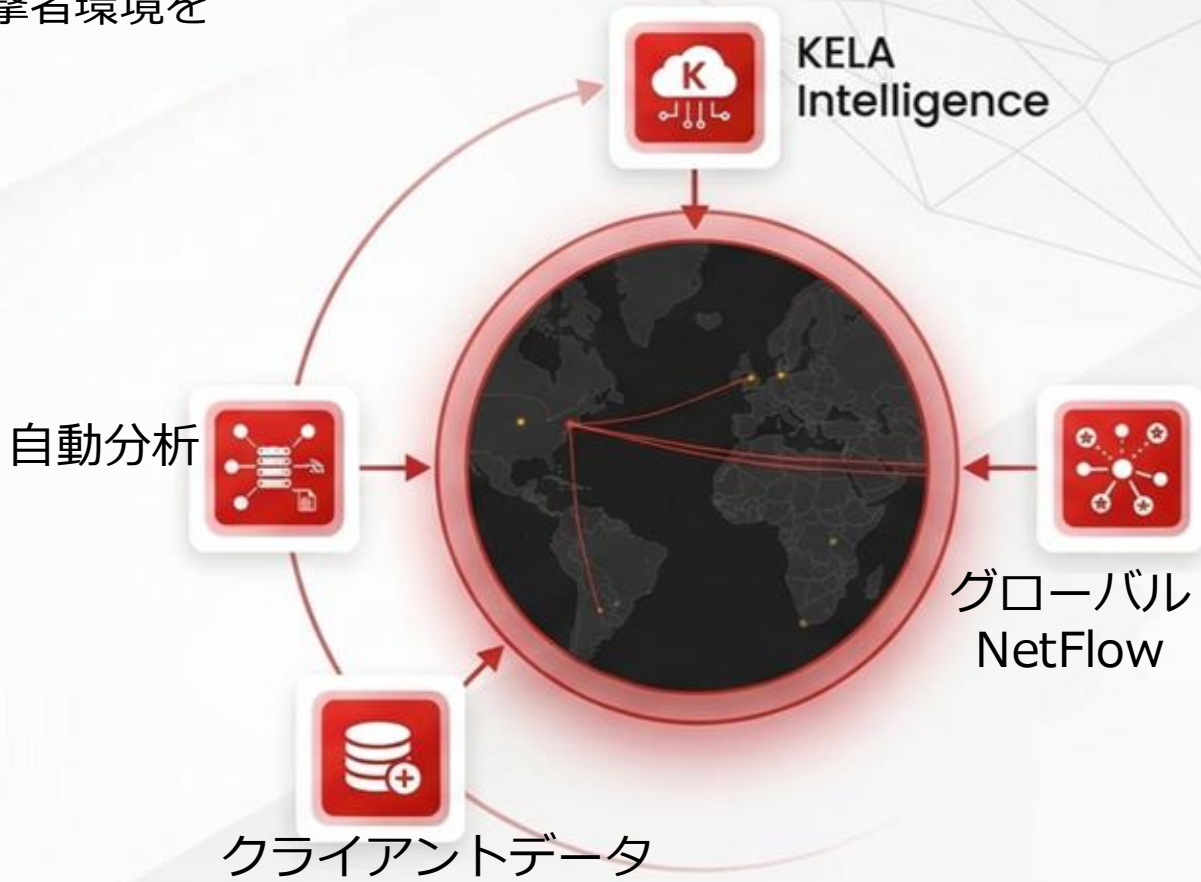
ネットワークトラフィックとインテリジェンスに基づく高度な融合リサーチ

- **ターゲット型インフラリサーチ**
  専用のデータ融合プラットフォームを使用して、疑わしい攻撃者環境を調査します。

- **包括的なデータ統合**
  KELAのインテリジェンスをグローバルNetFlowログやクライアント側の情報源とシームレスに融合します。

- **自動エンティティマッピング**
  異なるデータポイントを即座に相関分析し、隠れた関連性や高精度な検出事項を明らかにします。





CONTROL + CIC（サイバーインテリジェンスセンター）

一般提供開始

一般提供開始（KELAのリサーチャーが脅威ハンティングを実行）

CONTROL プラットフォーム

- KELAのインテリジェンスをグローバルNetFlowおよびクライアントデータと融合
- 攻撃者のインフラストラクチャとその関連性を自動的にマッピング
- 微弱なシグナルを高精度な検出結果へと転換

＋

CONTROL向け CICマネージドサービス

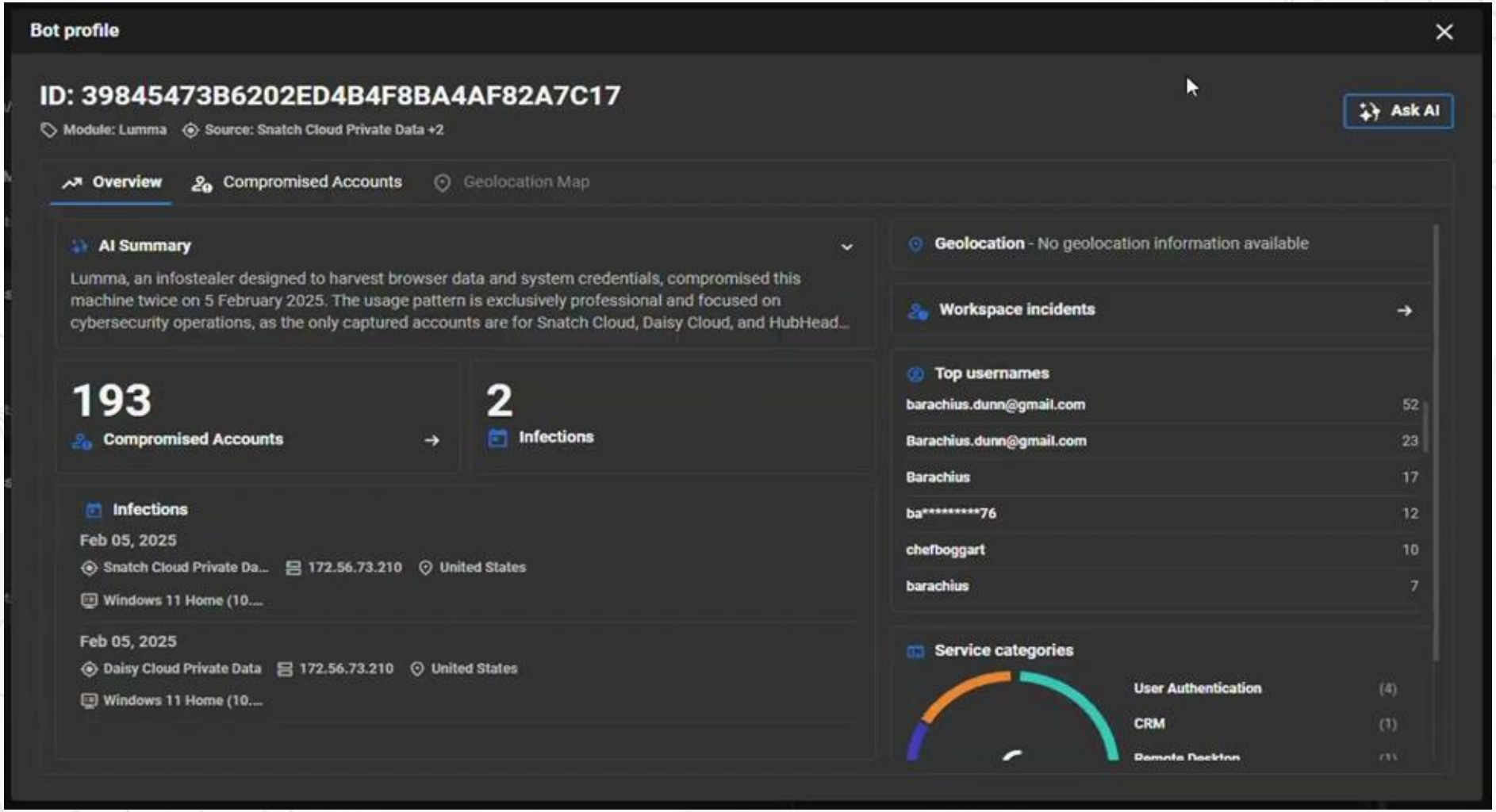
- KELA Cyber Intelligence Centerのリサーチャーがお客様に代わってハンティングを実行
- 貴社を標的とする疑わしい攻撃者環境を調査
- 推奨アクション付きの優先度付けされた検出結果

© 2026 KELA. All rights reserved.

KELA AI

早期アクセスを逐次開始

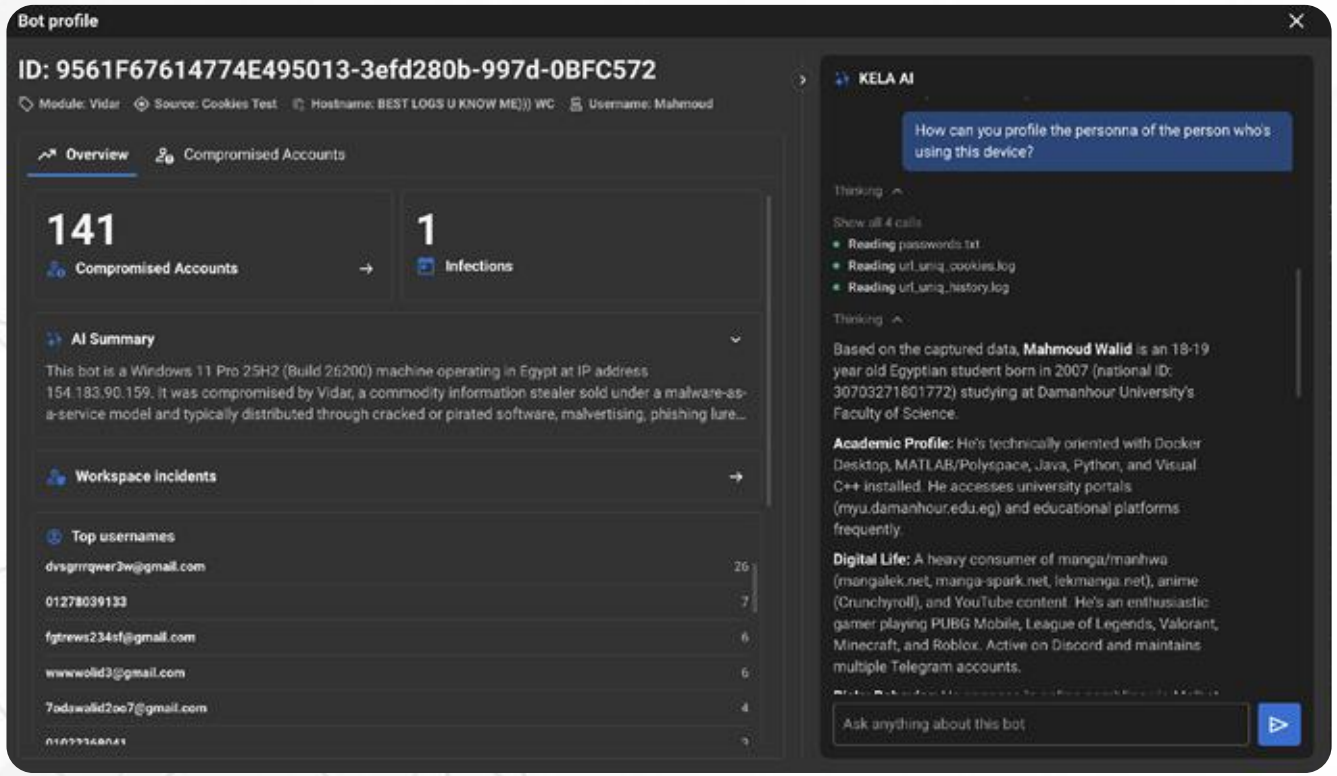
KELAプラットフォームから直接利用できる新たなAI機能
— **要約機能**および**対話型ユーザーチャットを搭載**



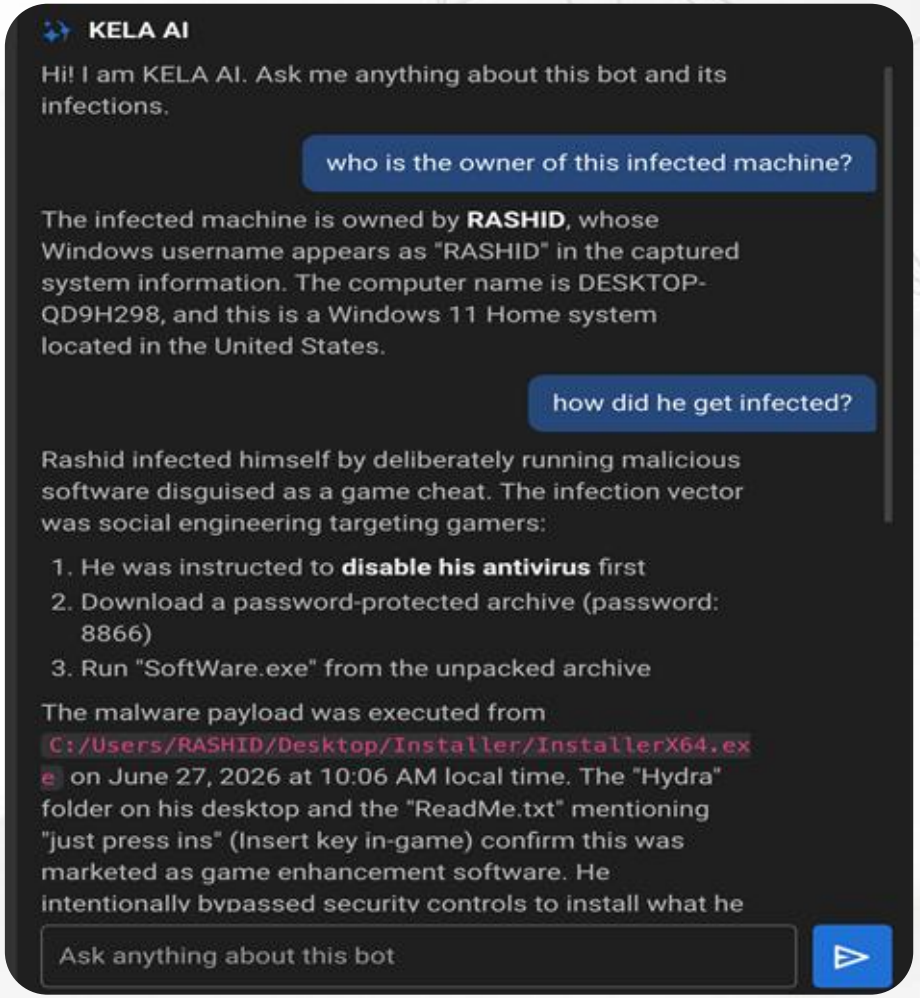
KELA AI

早期アクセスを逐次開始

KELAプラットフォームから直接利用できる新たなAI機能
ー 要約機能および対話型ユーザーチャットを搭載



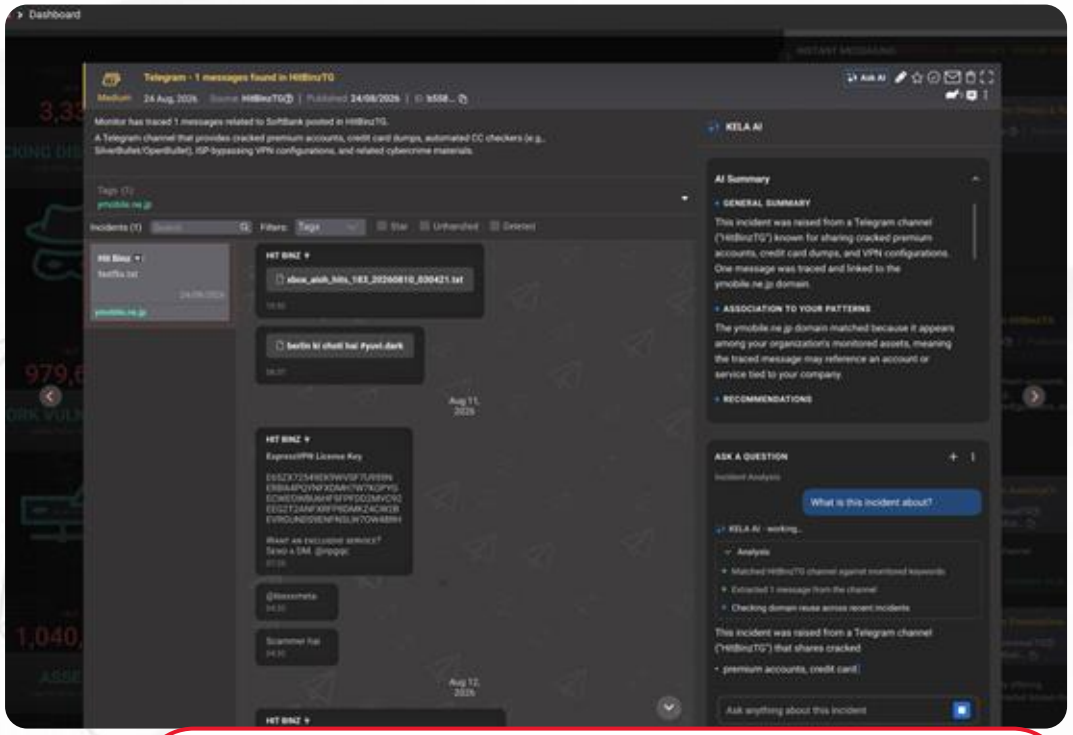
要約とオープンチャットを備えた
インフォスティーラー（感染端末）情報



KELA AI

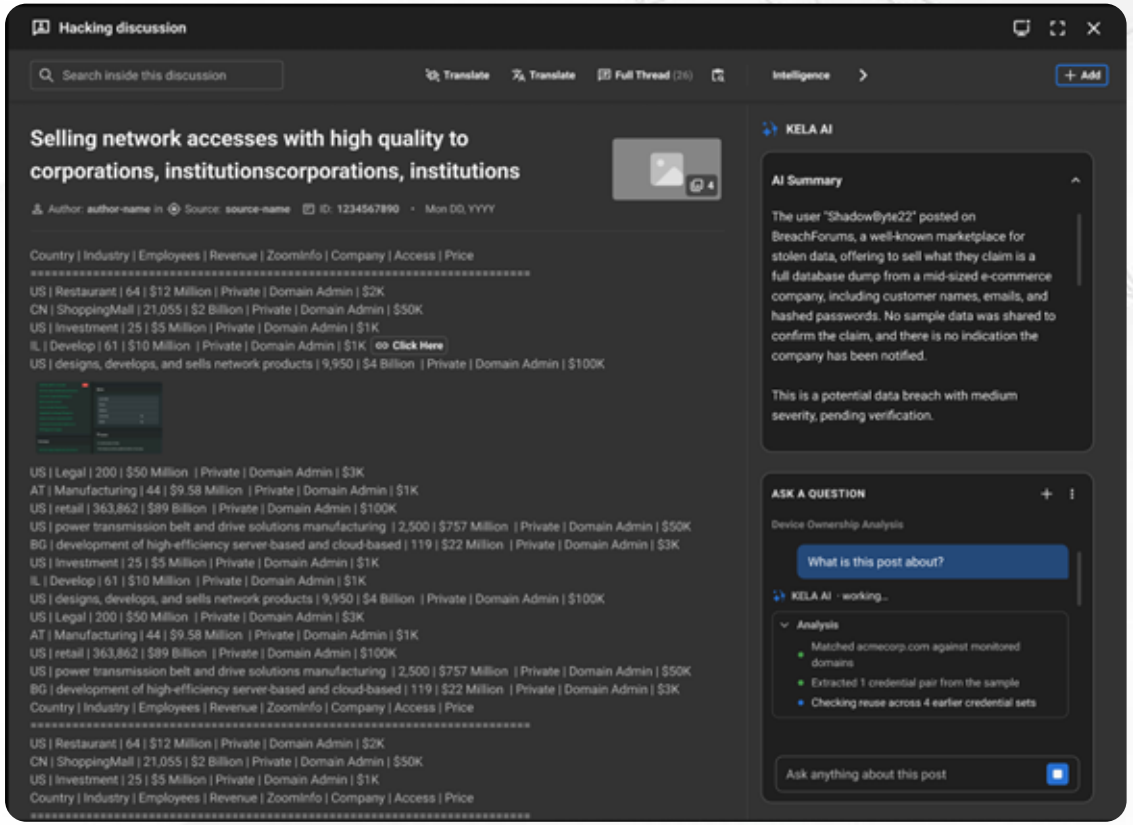
早期アクセスを逐次開始

KELAプラットフォームから直接利用できる新たなAI機能
― 要約機能および対話型ユーザーチャットを搭載



MONITORアラートに含まれる内容:

- **要約**
- **クライアント資産の文脈情報**
- **推奨される対策手順**
- **オープンチャット機能**



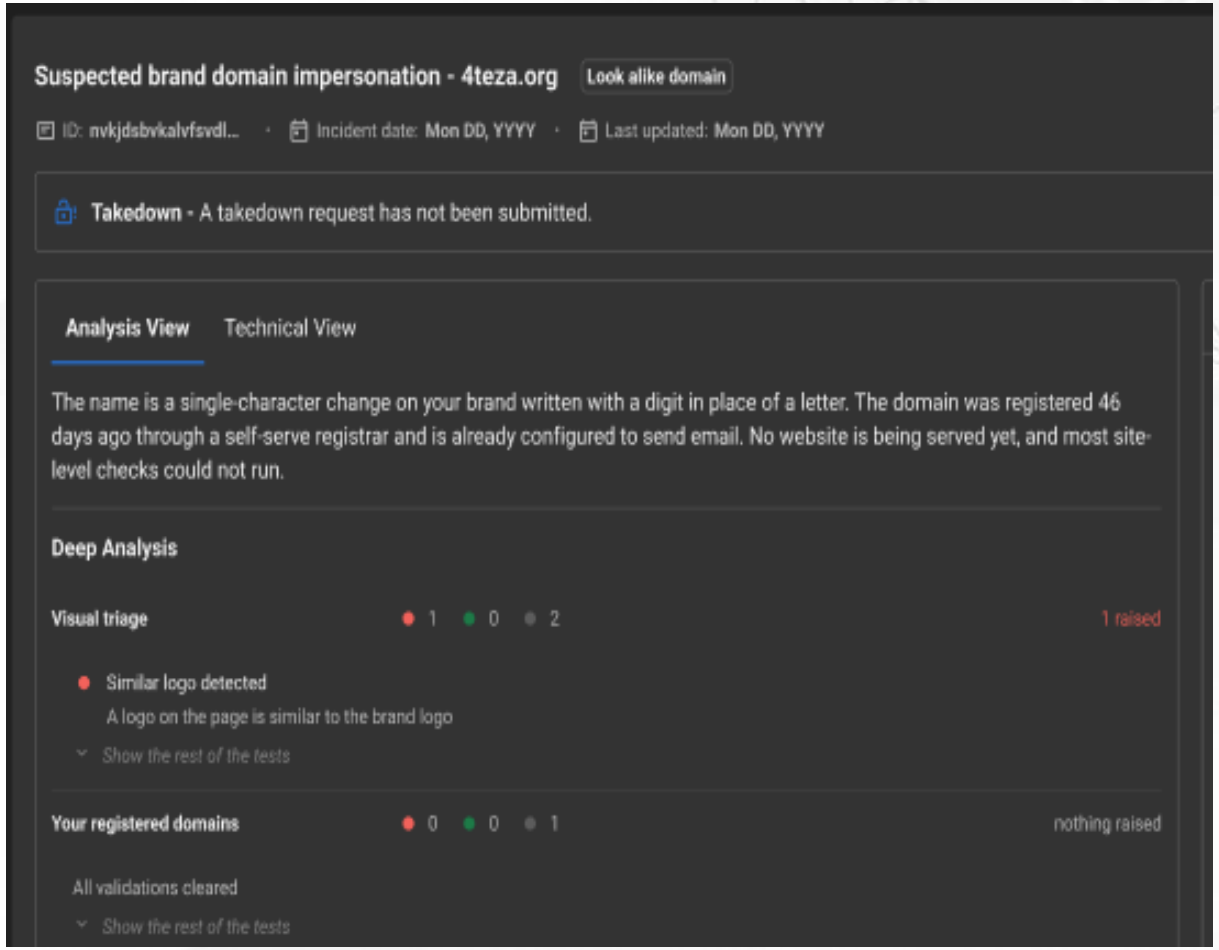
要約とオープンチャット機能を備えた投稿調査

Brand Control

AI-NATIVE

高度な分析: ブランド悪用とノイズを判別するAI

- ブランドに対する**なりすましの試み**を検知（なりすましWebサイト、類似ドメイン等）
- **AI**を活用し、すべての検知結果を高度に分析
- 新機能「**分析ビュー**」— アラートの発生理由や深刻度の設定根拠を確認可能
- **技術面と視覚面**の双方向から検証を行い、なりすましを特定
- プラットフォームから直接**テイクダウン（削除要請）**を実行



KELA

© 2026 KELA. All rights reserved.

KELA MCP

2026年9月提供開始

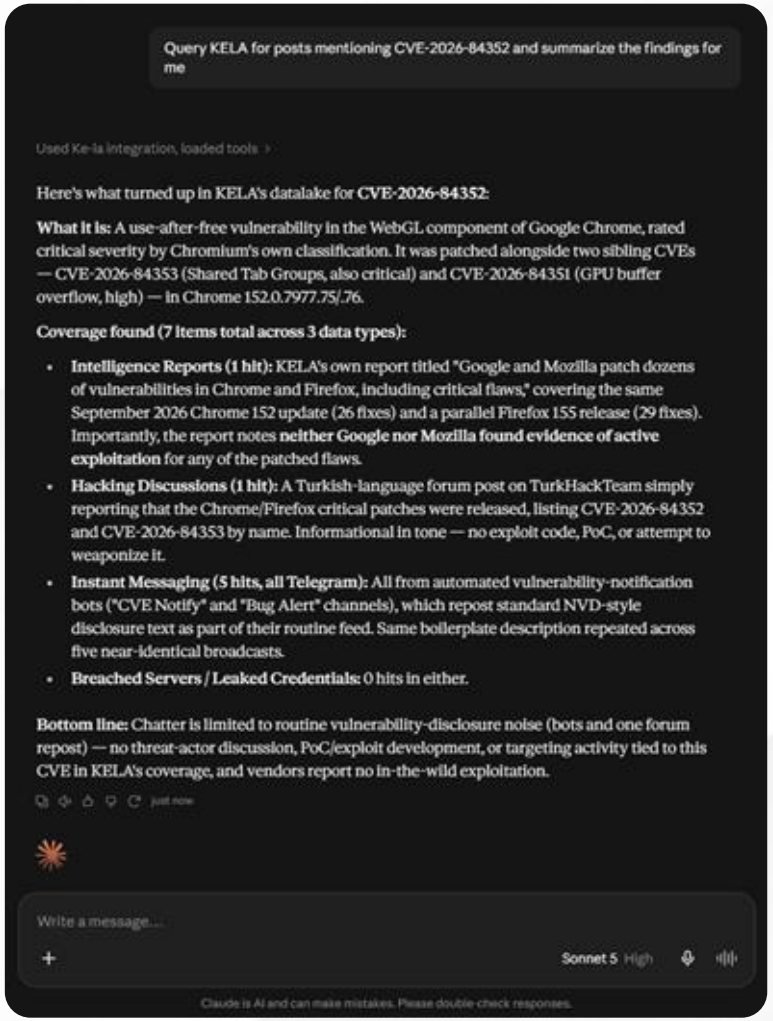
KELAプラットフォームの情報を顧客のAI 環境 へ直接取り込み

KELAの新たな MCPサポート により、プラットフォームをAIアシスタントへ直接接続可能に。

AIからあらゆるKELAモジュールにクエリ投稿可能：

- Investigate — KELAデータレイク（投稿、メッセージ等）への検索・クエリ実行
- Threat Actors — 脅威アクターのプロファイル、TTP、最新の活動状況の把握
- Threat Landscape — 関連イベント情報、アップデート、分析レポートの抽出
- Identity Guard — 侵害クレデンシャル情報など最新のインシデント情報および全データの確認

対応AIアシスタント：
Claude • ChatGPT • Gemini • Copilot

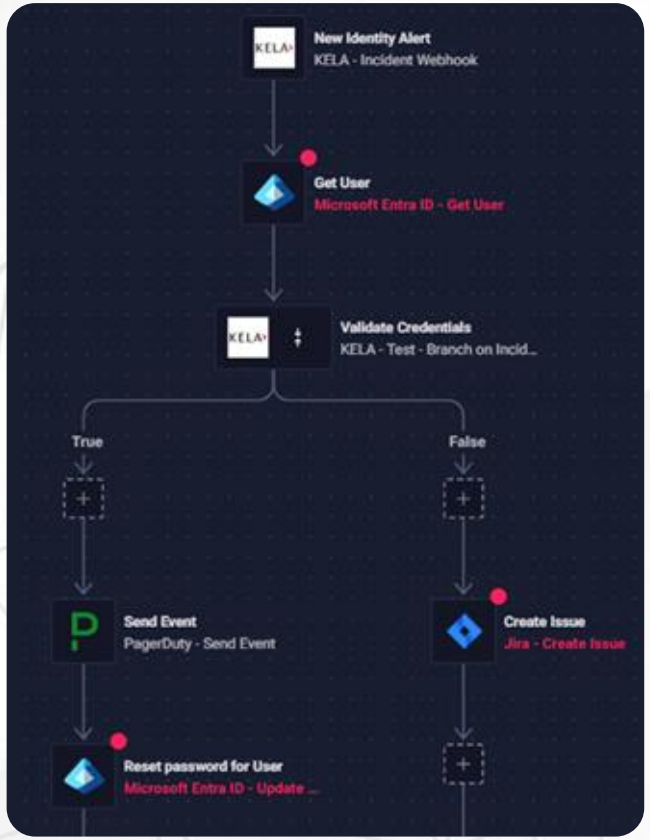


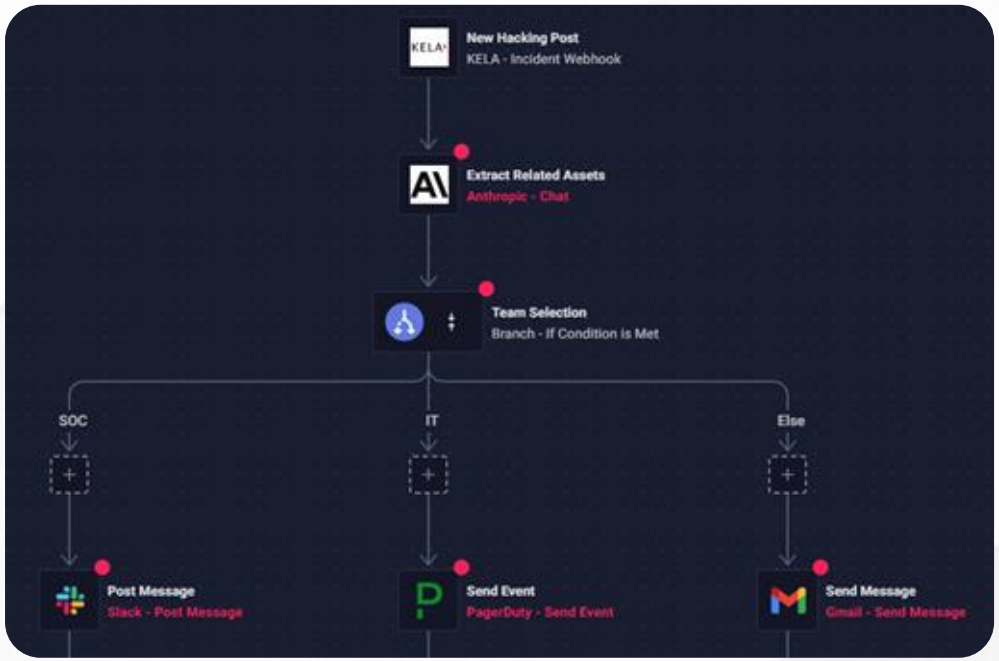


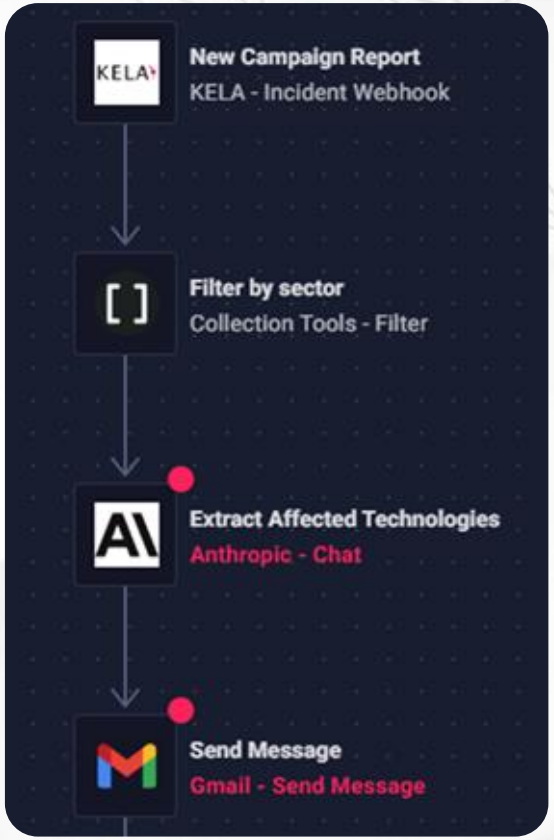
Workflow Builder

新 インテグレーションポータル - インサイトからアクションへ

KELAプラットフォームから直接、軽減策、検証、アクションを計画



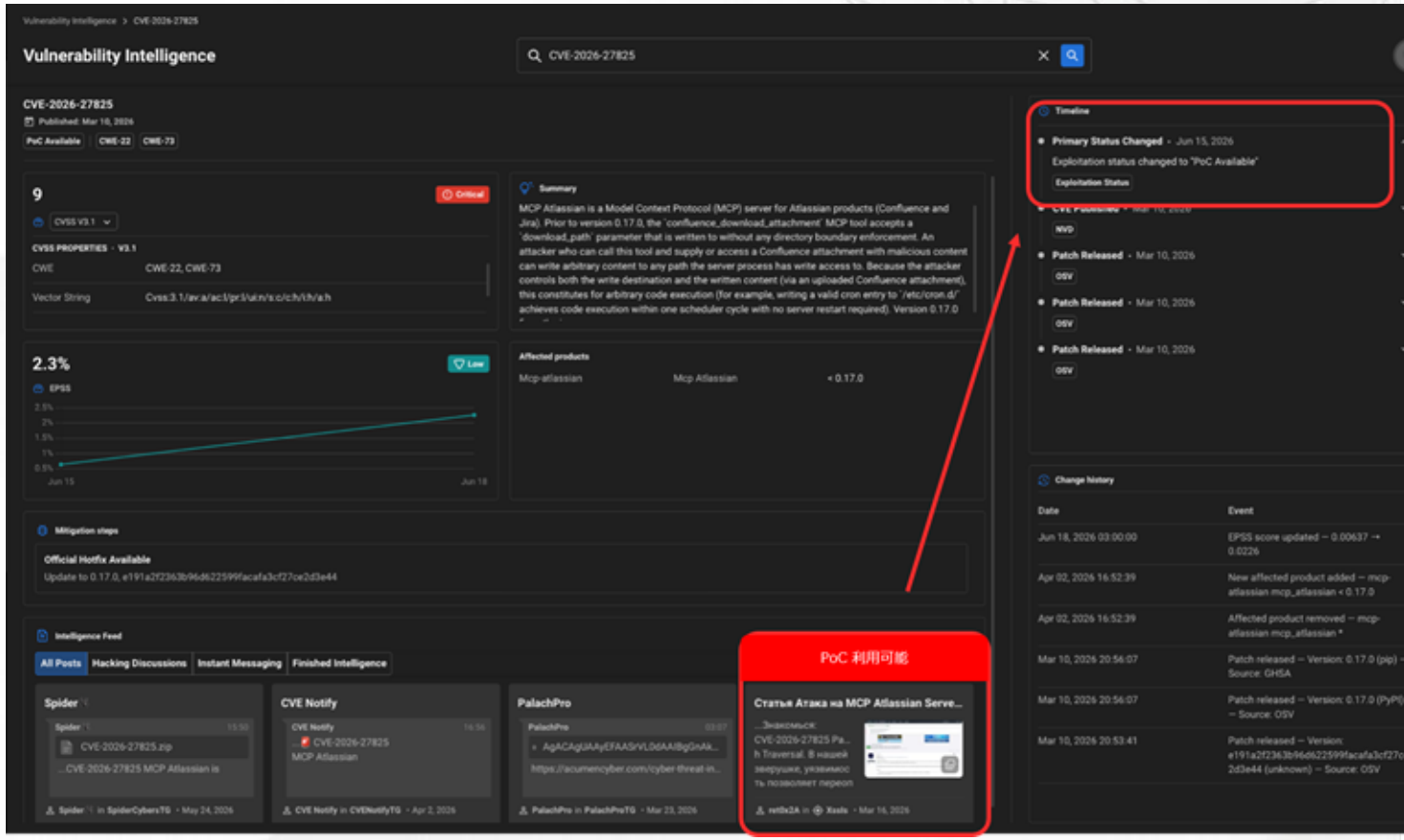




Vulnerability Intelligence

攻撃者が**実際に悪用・話題にしている**脆弱性を可視化

- 任意のCVE、脆弱性、アプリケーションを検索し、公式の詳細情報と現実世界の脅威アクティビティを併せた**統合ビュー**を取得
- KELAのCTIデータレイクからの**PoC販売、ゼロデイ、技術的議論**などを含むアンダーグラウンドのシグナル
- 脆弱性の全**ライフサイクル追跡** ― ステータス変更、影響を受ける製品、タイムラインを1箇所で管理
- **Popularity Risk Score** ― 従来のCVSS深刻度を超え、投稿量・コンテンツ・最新性に基づく新たな優先順位付けレイヤー



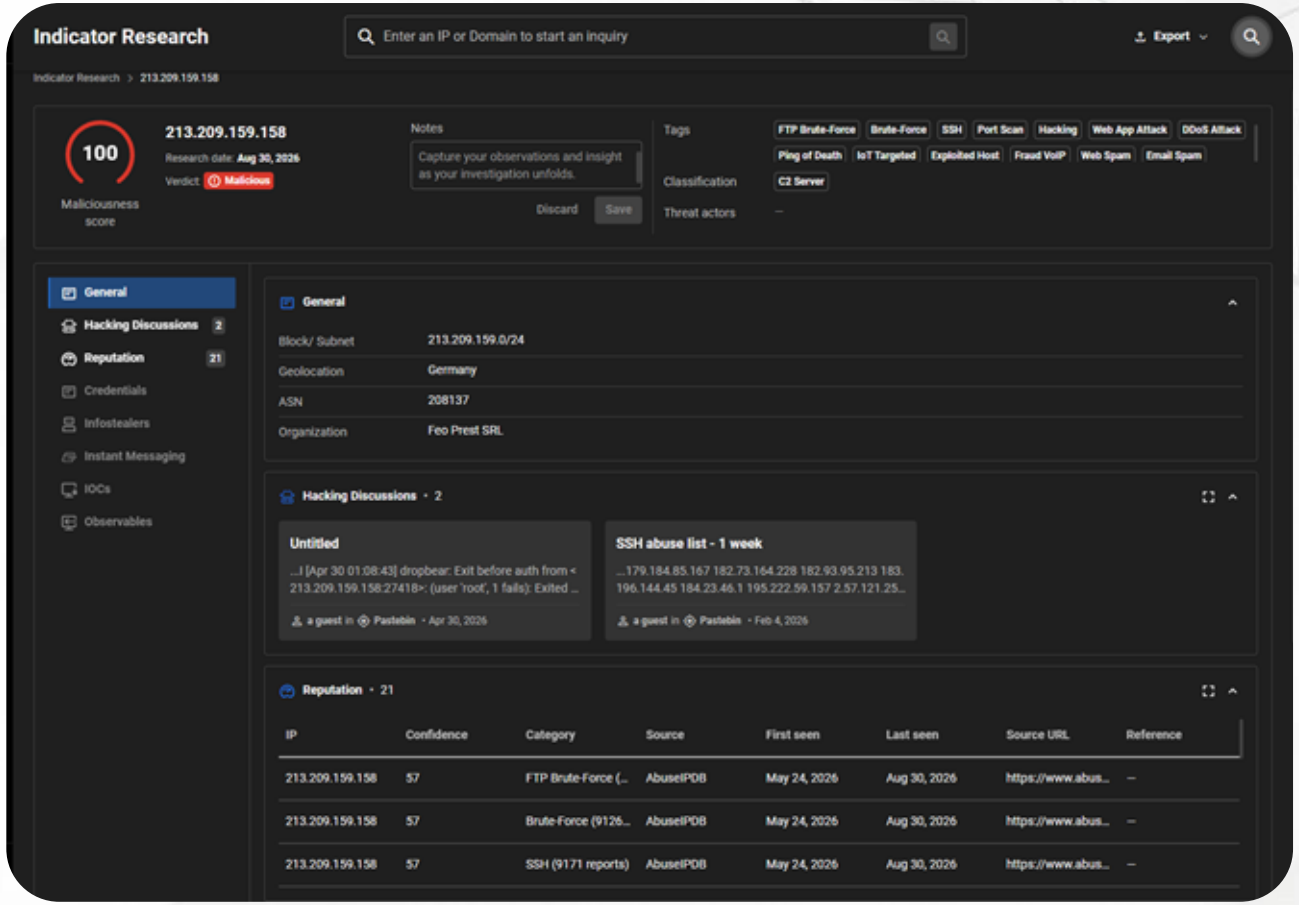
KELA

Indicator Research

2026年10月提供開始

あらゆるドメイン、IP、その他のインジケーターを 完全分析

- 単一のクエリから **IP、ドメイン、URL、ファイルハッシュなど** あらゆるインジケーターを検索
- KELAが該当インジケーターに関するすべての検出事項を自動的に収集、相関分析、要約
- 明確な **悪性 / 非悪性の判定（Verdict）** とその判定根拠を提供
- コンテキストを包含 ― 関連する脅威アクター、マルウェア、キャンペーン、過去のアクティビティ情報
- ツールを切り替えることなく、疑わしいインジケーターやアクティビティを数秒でトリアージ



脅威ハンティング　スイート

完成されたインテリジェンス

世界的なトレンドとイベント



世界中で発生する新しいトレンドや脅威を特定



実環境で実際に悪用されている脆弱性に関する実用的なインテリジェンスで優先順位付け

アクターと手法



戦術、キャンペーン、攻撃パターンに対する深い洞察により脅威アクターを解明

技術調査

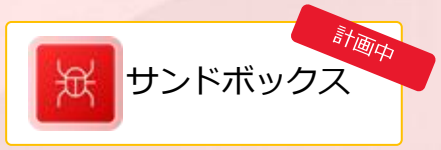
インジケーター



インテリジェンスに基づいてインジケーターを調査



セキュリティ機器向けに悪性IOCと将来悪用の可能性のあるIOCを取り込み



アクティブハンティング



新しい攻撃インフラやインジケーターを発見し、プロアクティブに脅威をハンティング



KELAのデータレイク全体でメール、テキスト、暗号資産ウォレット、画像などを調査してアクターを追跡

KELA

早期兆候への対応
日本の組織が 今できること

01
攻撃者がスキャンする対象の堅牢化（ハードニング）

トラック1：公開されているWeb/API資産

KELA: インジケーター調査、脆弱性インテリジェンス

02
リモートアクセスの厳格化

トラック2：VPNポータルと流出資格情報

KELA: 侵害されたクレデンシャル、リアルタイムモニター

03
次のシグナルを監視

攻撃の発生後ではなく、発生前に

KELA: CONTROL + CIC リサーチャー、KELA AI

KELA

© 2026 KELA. All rights reserved.

KELAGROUP

KELA ULTRARED SLING

Thank You

Questions & Discussion

www.kelacyber.com/ja

2026 ©KELA Group | All rights reserved.