サイバー犯罪インテリジェンスプラットフォーム

XARVIS

XARVIS（ザービス） は 、AI 基盤サイバー犯罪捜査プラットフォームです。 本プラットフォームは、ディープ・ダークウェブやTelegramなどのサイバー犯罪に関するヒドゥンチャネルからデータを収集し、統合的にモニタリングを行います。ユーザーは、捜査のデータを確保するために必要な元データとコンテキストをひとつのプラットフォーム上で取得可能になります。

昨今のサイバー犯罪では種類と量が急激に増加しており、限られた捜査リソースでの対応には困難があります。
XARVISは、手動での調査プロセスを簡素化し、調査時間短縮のための専用ツールとしてAI基盤のデータ分析を提供します。

AI

DarkBERT

世界初のダークウェブ特化型AI言語モデル

600万以上のダークウェブページで
学習させたDarkBERTは、
ダークウェブ上に存在する非構造化
データの処理に優れています。

ビッグデータ

膨大なサイバー犯罪情報

ディープ・ダークウェブ
Telegram
暗号資産
ソーシャルメディア

法執行機関向けのソリューション「XARVIS」

ヒドゥンチャネルのモニタリング

ディープ・ダークウェブ、Telegramなどの
ヒドゥンチャネルを継続的にモニタリングし、
リアルタイムで新たな脅威情報の取得が可能です。

違法行為の追跡

さまざまなチャネルから収集された過去のデータと
リアルタイムデータの分析を通じて違法取引の追跡や
犯罪活動に関するインテリジェンスを蓄積します。

脅威アクターの識別

調査ツールを活用して脅威アクターの隠された繋がり
を見つけ出します。
より多くの手がかりを収集し、容疑者を追跡します。

安全保障の強化

特定の国を標的としたサイバー攻撃や社会的脅威を
引き起こす犯罪行為など、様々な脅威を包括的に把
握します。

暗号資産の追跡・分析

ダークウェブインテリジェンスを活用して発信元のIPを追跡し、正確な位置情報を把握します。
暗号資産に隠された重要なインサイトを提供します。

XARVISコア機能

カスタマイズ脅威ダッシュボード

AI基盤の脅威データおすすめシステム

- AIを活用して脅威リスクを算出
- リスクの高いコンテンツを選別し優先的に表示

Telegramモニタリング

Telegramで収集された最新のコンテンツとデータをモニタリング

- 公開・非公開チャネルへのアクセス
- キーワード検索
- ファイルダウンロード

ソーシャルメディアブラウザー

ソーシャルメディア上のユーザー名を検索し、脅威アクターとの関係性を分析します。

- 主要プラットフォーム（Facebook、Instagram、WhatsApp、VK、Discordなど）をカバー

プロファイリングツール「DarkSpider」

潜在的な脅威アクターを識別するためのユーザープロファイリングツール

- 国別・産業別の脅威アクター規模の推移
- 脅威情報の視覚化

クロノロジカルブラウザー

コンテンツを収集し、変更内容をクロノロジカルに（時系列で）提供します。

- ヒドゥンチャネルへの安全なアクセス
- 修正・削除された内容まで追跡し元データを確保

マルチドメインクロス分析

散在する情報を結び付け、包括的なインサイトを収集します。

- カスタマイズ可の視覚化された関係値グラフ
- 暗号資産取引との統合

暗号資産の追跡と分析

暗号資産の追跡・分析機能を持つ「CryptoAnalyzer」は、ウォレット間の取引概要を提供し、特定の暗号資産アドレスの位置情報まで特定します。

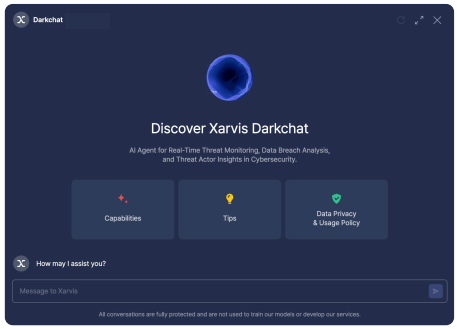
トランザクション追跡

- ダークウェブに関する様々なウォレットの自動トランザクション追跡。
- サポートしている暗号資産の種類として、BTC、ETH、AVAXが含まれます。

ジオトレース(GeoTrace)

- 暗号資産アドレスから個人の位置情報を正確に特定します。
- ビットコインウォレットアドレス関連のIP

DarkCHAT：サイバー犯罪AIチャットボット



AI基盤のデータ分析・対応

- 迅速なエンジニアリングによる包括的な結果の取得
- 最新・関連データ漏洩の発見
- 影響を受け得る産業別の統計的インサイト

関連データの提案（XARVIS内）

- XARVISデータベース内の関連データとリダイレクトリンクを提供

S2W

glosales@s2w.inc /s2w_official /@s2winc

www.s2w.inc/ja /company/s2winc /S2WLAB