uppsalasecurity

人々に安心感を与えるテクノロジー

Uppsala Securityの使命は、暗号犯罪の発生を防止すること、そして、発生した際は被害を軽減することにあります。そのためにUppsala Securityは、使いやすく簡単に導入できる暗号セキュリティソリューションとして賞を獲得した実績あるSentinel Protocolをお求めやすい値段で提供しています。セキュリティの悪用を防止する鍵は、脅威に関する情報をグローバルにいかに速く収集、検証、および共有できるかにあります。

コアセキュリティテクノロジー

Sentinel Portal

個人および組織を対象としたUppsala SecurityのワンストッププラットフォームであるSentinel Portalを使用すると、セキュリティの専門家が、悪意のある攻撃、マルウェア、詐欺、および不正な活動に関連する疑わしいインシデントを調査および分析できます。Sentinel Portalでユーザーが疑わしいネットワークインシデントをレポートすると、それに応じてセンチネルと呼ばれるUppsala Securityのセキュリティのエキスパートが分析および検証を行います。

Threat Reputation Database (TRDB)

ブロックチェーンベースのThreat Intelligence Database (TRDB)は、特定の暗号アドレス、URL/URI/ドメイン、およびソーシャルメディアアカウントに関連するシステムの脅威に関する情報が保存された、当社の中核となる分散エコシステムです。Uppsala Securityのセキュリティのエキスパートが、クラウドソースデータを分析、検証してホワイトリストおよびブラックリストに分類します。TRDBデータはすべて、防御セキュリティ、リスクベース分析、および規制コンプライアンス用のツールを使用してUppsala Securityのコミュニティとリアルタイムで共有されます。

Twitter Crawler System

Twitter Crawler Systemは、認識パターンマッチングアルゴリズムを使用してTwitter上の悪意のある行為に関わる脅威インジケータを探して収集する役目を果たします。この革新的なテクノロジでは、新しいフィッシィングリンクが作成されてから見つかってブラックリストに載せられるまで、ほぼリアルタイムに近い数分しかかかりません。Twitter Crawler Systemは、偽のアカウントを正確にフィルターにかけて除外し、ユーザーが偽のウォレットアドレスを使用してなりすまし者に資金を送信することを徹底的に防止します。

Crypto Address Crawler System

Crypto Address Crawler Systemは、自社開発した三段論法アルゴリズムを活用して、悪意のある暗号アドレスと悪意のない暗号アドレスを収集して分類します。悪意のあるハッキング、詐欺、および不正な活動に関連する悪意のあるウォレットは、Uppsala Securityが提供する暗号通貨セキュリティツールを使用してフィルターにかけて除外できます。

防御セキュリティ用のツール

Interactive Cooperation Database API (ICF-API)

Interactive Cooperation Database API (ICF-API)を使用すると、ユーザーがソフトウェアアプリケーションをTRDB (Threat Intelligence Database)と統合できるようになります。これにより、統合したソフトウェアアプリケーションを使用してTRDBに動的に問い合わせ、問い合わせに対する回答を数ミリ秒以内で受け取ることができます。この回答には、特定のウォレットアドレス、URL/URI/ドメイン、またはソーシャルメディアアカウントがTRDB内で安全/危険のどちらとして分類されているかが示されています。ICF-APIを使用すると、暗号資産の保護に関する脅威インテリジェンス情報を動的に取得し、フィッシィング/マルウェアに関連するウェブページを回避し、政府の規制に準拠することができるよう、任意のソフトウェアアプリケーションフレームワークを強化することが可能です。国際的に認められたフレームワークとその標準形式を活用することで、政府組織や仮想資産サービスプロバイダ、およびその他の企業は冗長な脅威検証プロセスを解消し、プロセスを自動化し、生産性を最適化できます。

UPPward

UPPwardと呼ばれるUppsala Securityのブラウザ拡張機能は、フィッシィング/マルウェア、暗号詐欺、および不正からユーザーをリアルタイムで保護します。また、これらの機能により、疑わしいネットワークアクティビティやハッキングインシデントをUppsala Securityのセキュリティのエキスパートが分析および検証できるようユーザーが簡単にレポートできるようになります。UPPwardにより、ユーザーが現在参照しているURL/URI/ドメインがTRDB (Threat Intelligence Database)で安全と危険のどちらとして定義されているかが自動的に示されるため、ユーザーは安全なインターネット閲覧体験を楽しむことができます。また、ユーザーは、TRDBに動的に問い合わせることで、特定のウォレットアドレスまたはソーシャルメディアアカウントがTRDBで危険として分類されているかどうかを確認できます。UPPwardブラウザプラグインは数秒でインストールできます。このプラグインは、Chrome、Brave、Edge、およびFireboxの各ブラウザ上で動作します。UPPwardは無料で利用できます。

Tools for Risk Based Analytics

Crypto Analysis Risk Assessment (CARA)

A.Iおよび機械学習アルゴリズムを活用した直感的で使いやすいソリューションであるCARAは、ウォレットの過去の取引を分析し、既知の危険ウォレットと安全ウォレットによって示された学習行動を活用することで、特定の暗号アドレスに関するリスクスコアを生成する役割を果たします。暗号通貨を扱う企業にとっては、CARAはサイバー犯罪者、マネーロンダリング犯罪者、およびテロリストとの不注意な取引を解消する上で役に立ちます。CARAには、GUIまたはRESTful APIを介してアクセスできます。CARAは、BTC、ETH、ERC-20、ADA、BNB、BCH、EOS、LTC、TRX、XLM、およびXRPの使用をサポートしています。

Crypto Analysis Transaction Visualization (CATV)

CATV (Crypto Analysis Transaction Visualization)と呼ばれる暗号取引科学探査ツールは、ユーザーが指定したウォレットで受信する取引/ウォレットから送信する取引の両方を追跡およびレポートします。CATVにより、指定したウォレットとやり取りが行われた様々なタイプのウォレットやトークンのフローが表示された画像が素早く生成されます。このため、混乱や混合などの疑わしいフロー動作、またはTRDB内のブラックリストに載せられたウォレットとの過去の取引をユーザーが分析する上で役に立ちます。CATVには、GUIまたはAPIを介してアクセスできます。CATVは、BTC、ETH、ERC-20、ADA、BNB、BCH、EOS、LTC、TRX、XLM、およびXRPの使用をサポートしています。

Professional Services

Summary Wallet Analysis Profiling (SWAP)

暗号通貨リスク管理および規制コンプライアンスを向上させるために、SWAP (Summary Wallet Analytical Profiling)は、一連のカスタマイズ可能な分析レポートセットをタイムリーに生成します。このレポートには、企業のエンドユーザーの暗号アドレスおよび取引履歴に基づいて主なビジネスリスクを強調した、時宜を得た綿密な洞察が記載されています。
次世代の人工知能を活用したSWAPを使用すると、深い分析インサイトに素早くアクセスできるため、企業のリスクを軽減しながら、企業の生産性、サービスレベル、および意思決定を改善し、戦略的なビジネスの目標を達成する上で役に立ちます。SWAPは、BTC、ETH、ERC-20、ADA、BNB、BCH、EOS、LTC、TRX、XLM、およびXRPの使用をサポートしています。

ウェブサイト	uppsalasecurity.com	
連絡先	info@uppsalasecurity.com	
ソーシャルアカウント	**Twitter**	twitter.com/UPPSentinel
	Telegram	t.me/newofficialsentinelprotocol
	Facebook	www.facebook.com/sentinelprotocol
	LinkedIn	www.linkedin.com/company/uppsalafoundation