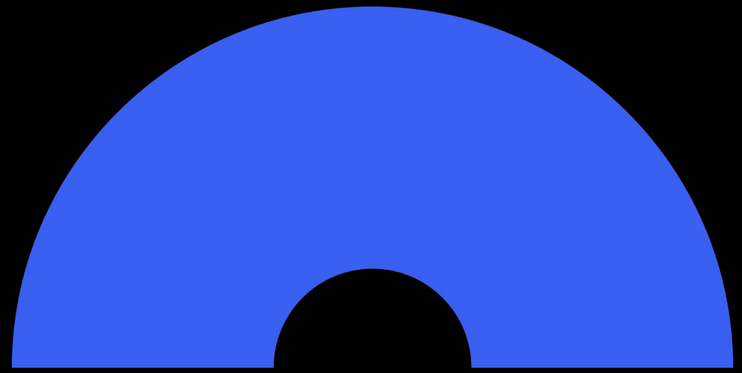
제품
소개서



uppsalasecurity

웁살라 시큐리티

싱가포르 380 Jalan Besar, #11-05 ARC 380, Singapore 209000

대한민국 서울시 강남구 삼성로 100길

아시아 테크의 중심 싱가포르에 본사를 둔 웁살라 시큐리티는
숙련된 금융 보안 전문가들로 구성된 블록체인 사이버 보안 회사입니다.
블록체인 기술을 기반으로한 사이버 보안 솔루션을 서비스 하고 있습니다.

Threat Intelligence

보안위협정보

Sentinel Portal	센티넬 포털
TRDB	위협 평판 데이터베이스
Crypto Address Crawler System	암호화폐 주소 크롤러 시스템
ICF API	TRDB(위협 평판 데이터베이스) 외부 접속용 API
TOMS API	내부망 구축형 로컬 TRDB(위협 평판 데이터 베이스)

보안 위협은 항상 역동적으로 진화하고 있습니다. 기술이 발전하고 새로운 기술이 도입됨에 따라 보안위협은 더욱 다양한 방법으로 끊임없이 진화하여 시장과 사회에 새로운 위협과 보안 취약성을 만들어 내고 있습니다. 피싱 URL 및ID 도난 및 도용, 악성 코드, 스캠, 멀웨어 등은 개인과 집단에게 피해를 입히는 대표적인 보안위협의 예 입니다.

센티넬프로토콜은 이러한 보안 위협 정보들을 수집하고 이에 대응하기 위한 블록체인 기반의 Threat Intelligence 플랫폼을 만들었고, 이를 통해 암호화폐 등 기타 디지털 자산에 발생하는 위협에 대해 선제적으로 대처하고자 합니다.

—

Sentinel Portal

TRDB

Crypto Address Crawler System

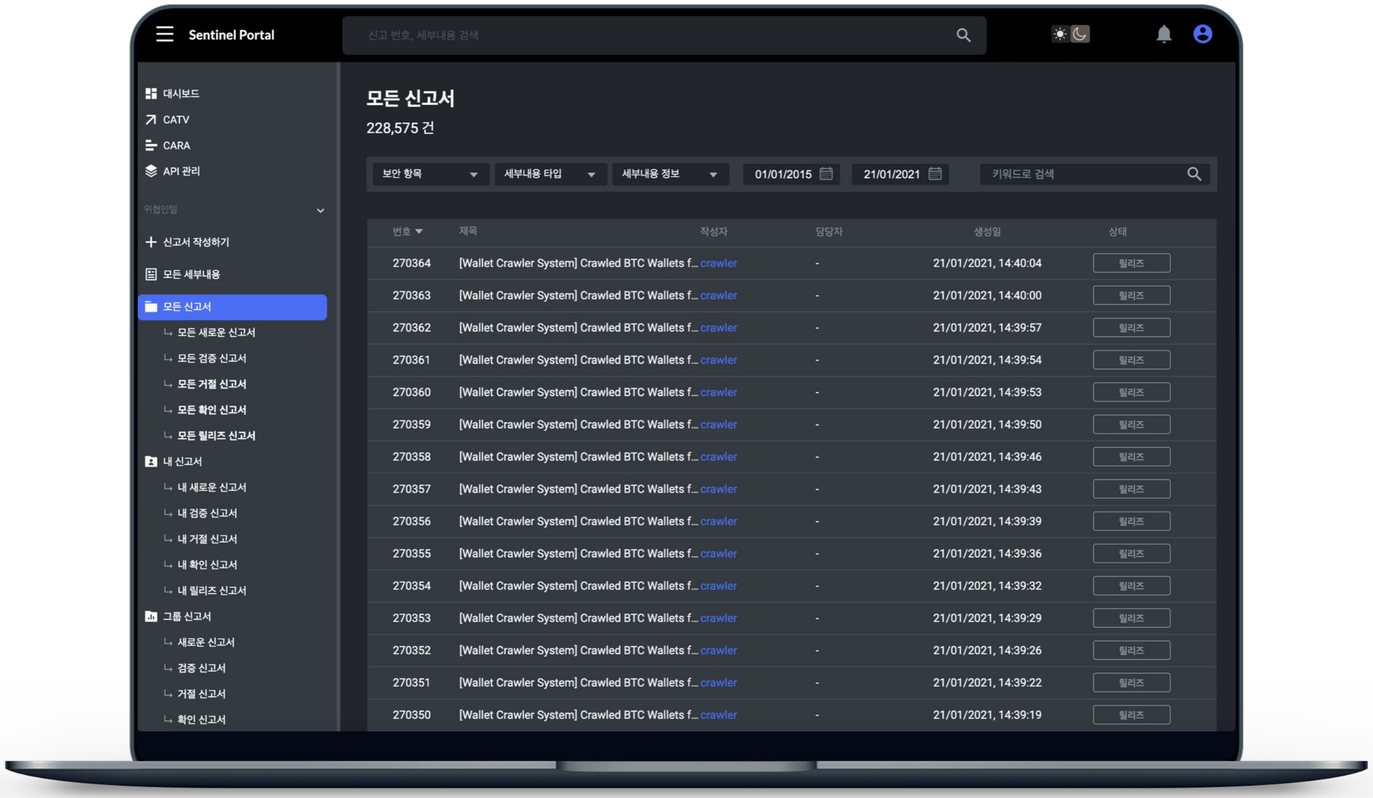
ICF API

TOMS API

Sentinel Portal

센티넬 포털

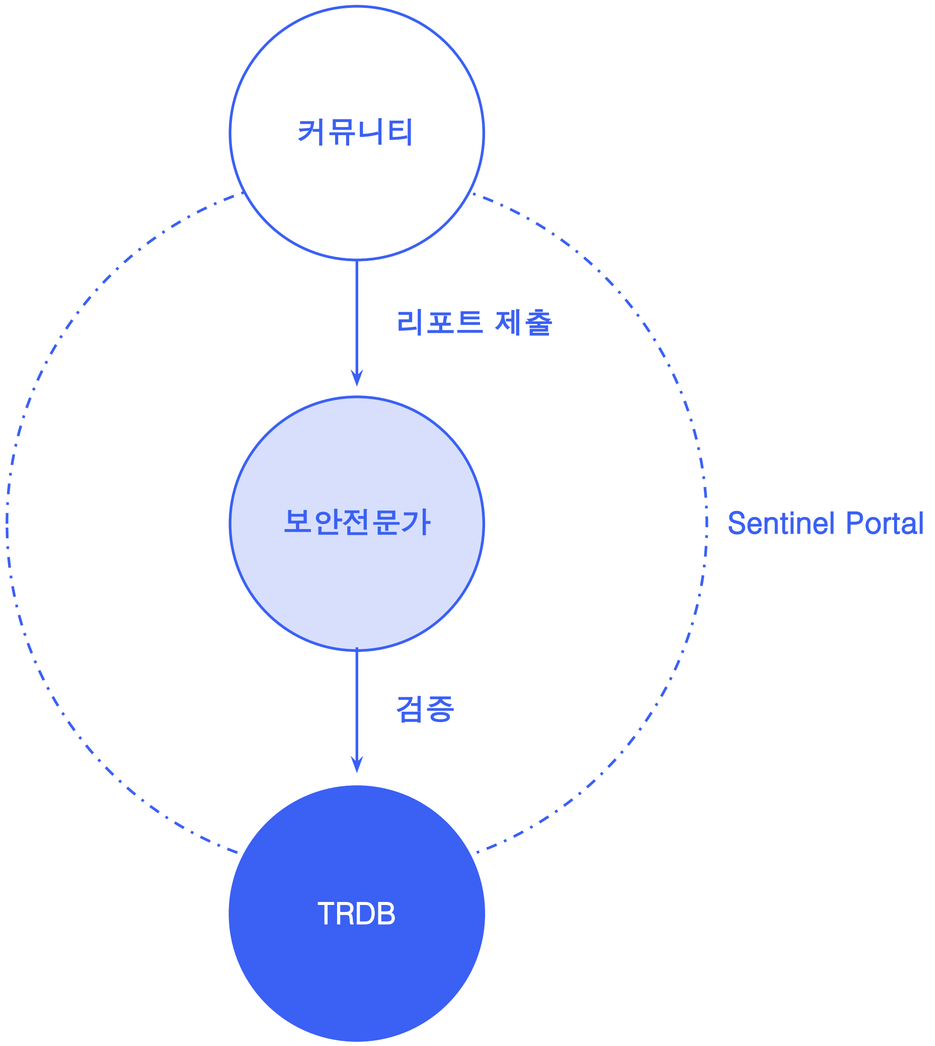
센티넬 포털은 집단지성을 활용해 보안위협을 모으기 위한 보안 플랫폼입니다. 사용자는 센티넬 포털에서 해킹, 사기 등 다양한 공격행위에 대해 리포트를 작성할 수 있습니다. 제출된 리포트는 웁살라시큐리티의 보안전문가들이 분석하고 검증합니다.



어떻게 작동하나요?

Sentinel Portal은 집단 지성을 활용, 보안 위협 정보를 모으기 위한 원스톱 플랫폼으로서 사용자가 멀웨어, 해킹, 사기 및 부정 행위와 관련된 보안 사고를 직접 보고할 수 있는 창구 입니다.

웁살라시큐리티의 보안 전문가들은 포털을 통해 제출된 각 사건 리포트를 분석, 추적 및 검증합니다. 각 리포트가 검토되어 유효한 것으로 인정되는 경우, 각종 보안 사고 및 위협에 관련된 데이터는 그 피해자들의 프라이버시를 침해하지 않는 범위에서 블록체인 상의 Threat Reputation Database (TRDB)내에 저장됩니다.



—

Sentinel Portal

TRDB

Crypto Address Crawler System

ICF API

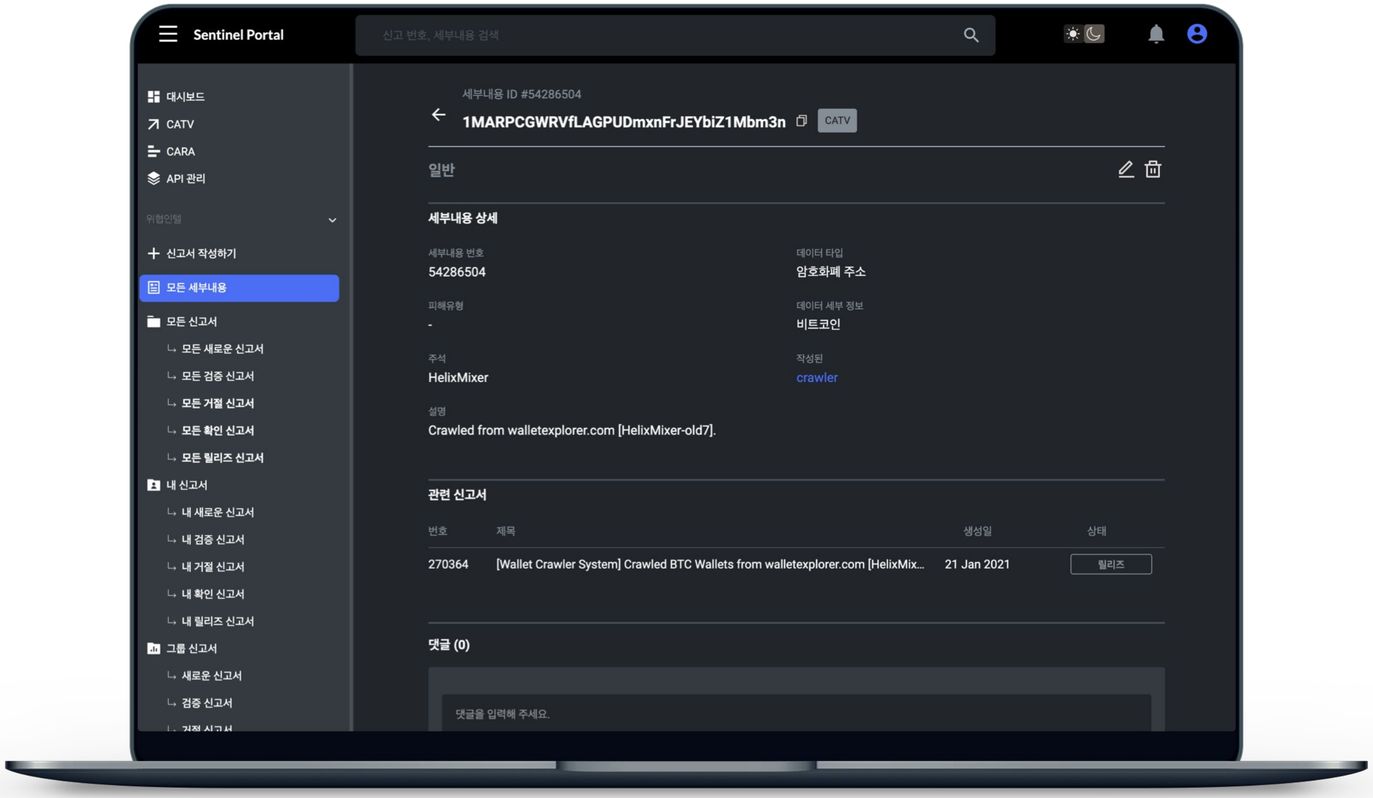
TOMS API

TRDB

Threat Reputation Database

위협 평판 데이터베이스

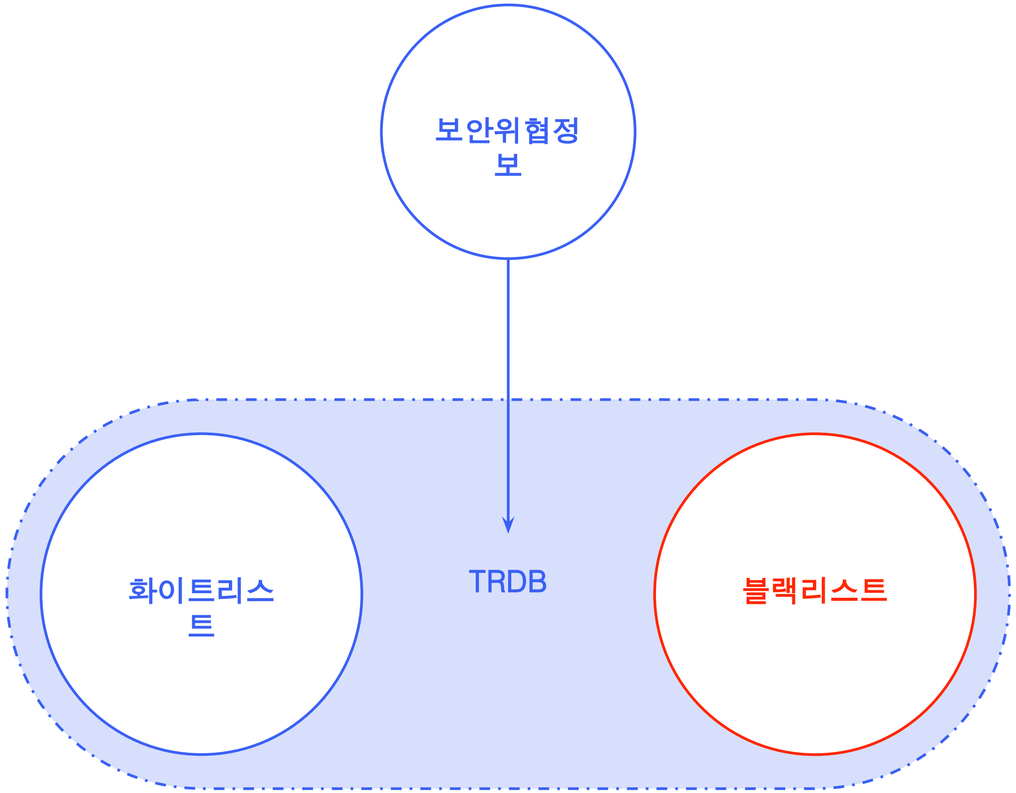
TRDB는 암호화폐 거래소, 지갑, 결제 서비스, 트위터, IT 및 사이버보안 회사 등 다양한 소스로부터 검증된 크라우드소싱 기반의 보안 정보를 저장합니다.



어떻게 작동하나요?

TRDB는 암호화폐 거래소, 지갑, 결제 서비스, 트위터, IT 및 사이버보안 회사 등 다양한 소스로부터 검증된 크라우드소싱 기반의 보안 정보를 저장합니다. TRDB는 화이트리스트와 블랙리스트의 형태로 구분하여 저장하는데 암호화폐 거래소의 경우 TRDB와 CATV를 활용하여 도난당한 암호화폐를 추적하고, 거래 위험을 관리할 뿐만 아니라 보안 규정을 준수할 수 있습니다.

이를 통해 사기 및 해킹과 관련된 악성 지갑주소 뿐만 아니라 크립토재킹, 보이스 피싱 등과 같은 온라인상의 악의적 활동으로부터 디지털 자산을 더욱 안전하게 보호할 수 있습니다.



* 크립토재킹(Cryptojacking): 일반인 PC를 암호화폐 채굴에 이용하는 신종 사이버 범죄

—

Sentinel Portal

TRDB

Crypto Address Crawler System

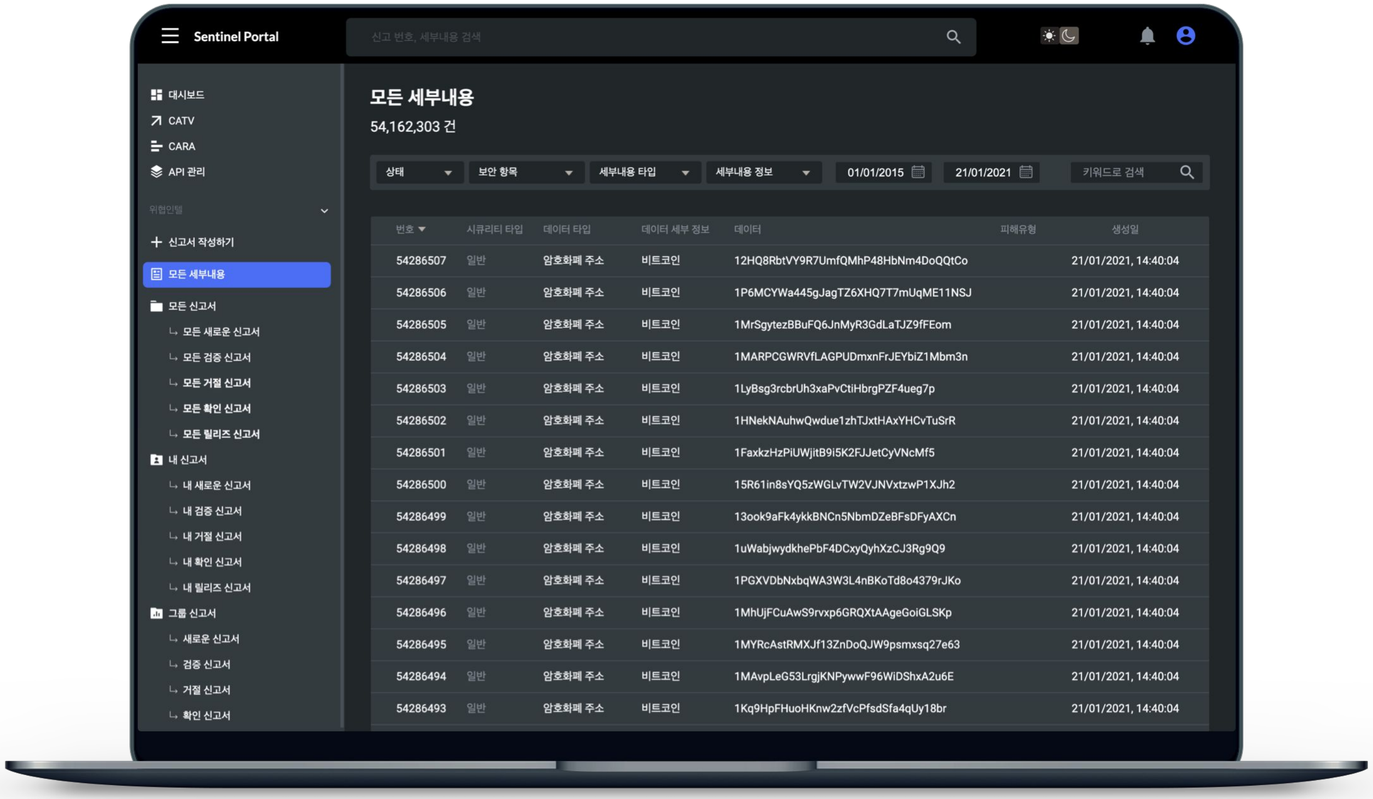
ICF API

TOMS API

Crypto Address Crawler System

암호화폐 주소 크롤러 시스템

웁살라 시큐리티의 암호화폐 주소 크롤러 시스템은 실시간으로 비트코인, 이더리움 등 암호화폐 지갑 데이터를 탐지하고 수집합니다. 보이스 피싱이나 해킹 등 범죄에 연루된 암호화폐 지갑들을 빠르게 수집하고 분석합니다.

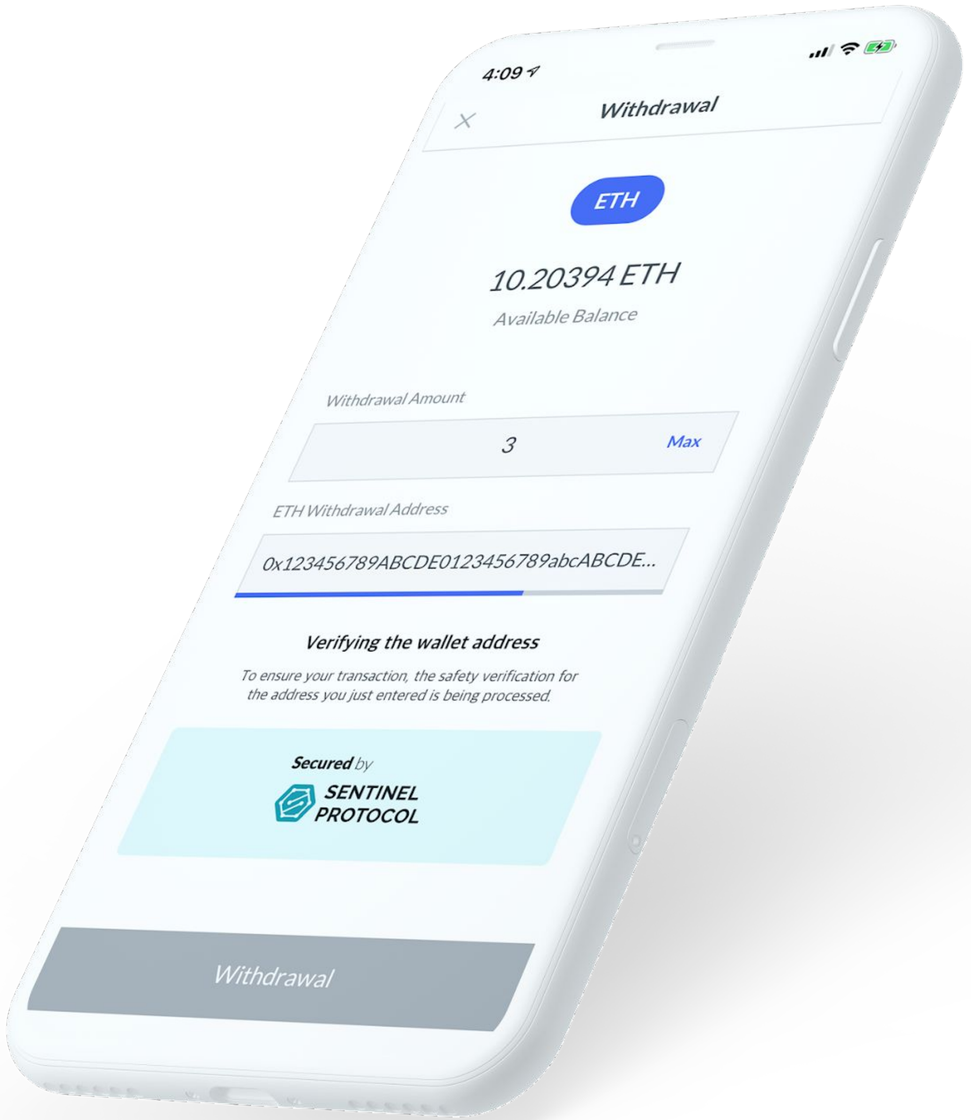


ICF API

Interactive Cooperation Framework

TRDB(위협평데이터베이스) 외부 접속용 API

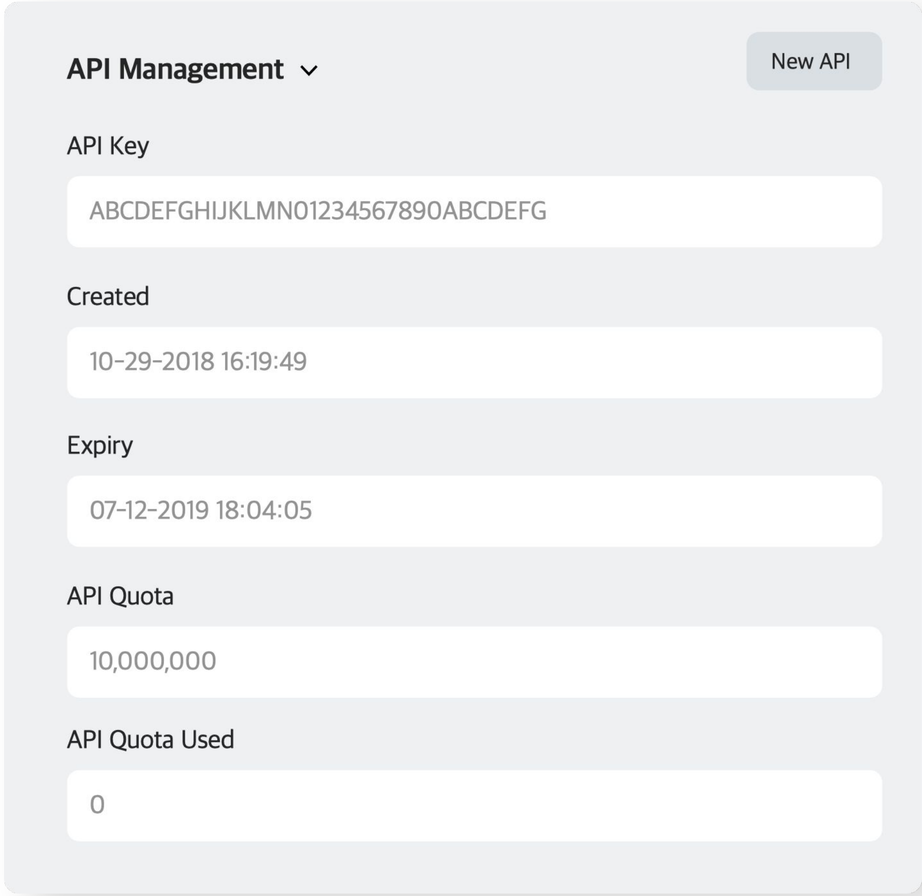
ICF 는 API로서 금융 소프트웨어와 결합하여
암호화폐와 같은 디지털 자산을 사기나 스캠으로부터
보호하기 위해
개발된 솔루션입니다.



ICF API는 무엇인가요?

ICF는 기업의 금융 소프트웨어 어플리케이션들과 결합하여 혐의거래나 금융사기으로부터 암호화폐 등 디지털 자산을 보호하기 위해 개발된 센티넬프로토콜의 API솔루션입니다.

ICF API는 사용자가 거래를 완료하기 전, 센티넬프로토콜의 위협평판데이터베이스(TRDB)에 저장된 화이트리스트 및 블랙리스트 정보와 대조하여 거래상대방에 대한 위협을 사전에 즉시 판별함으로써 금융사기범죄로부터 고객의 디지털 자산을 보호합니다.



어떻게 작동하나요?

ICF API를 사용하는 암호화폐 거래소 및 가상 자산 서비스 제공업체(VASPs)는 트랜잭션 발생 직전, 센티넬프로토콜의 위협 평판 데이터베이스(TRDB)를 통해 특정 지갑 주소, URL, 도메인 또는 텔레그램 ID의 보안 위험성 여부를 확인 후 해당 결과에 따라 트랜잭션을 완료하게 됩니다. 밀리 세컨드 단위 내에 즉시 수행되는 TRDB 조회 결과에 따라 '주의' 또는 '경고'가 확인될 경우, 보류 중인 트랜잭션을 즉시 거부 및 종료할 수 있으며, 반대로 경고 수준이 낮거나, 화이트리스트로 검증된 지갑주소의 경우 안심하고 암호화폐를 송금할 수 있습니다. 이처럼 사전에 위협요소가 있는지 미리 판별할 수 있을 뿐만 아니라 사후에도 다른 의심스러운 행적들이 감지되는지 확인할 수 있습니다.

이전에 안전한 지갑으로 확인됐던 주소가 거래에 사용된 후 의심스러운 행동이 포착된다면, 해당 내용은 보안위협으로 인지되어 TRDB에 보고, 블랙리스트에 추가됩니다.

현재까지는 해커들이 탈취 & 사기편취 한 자금을 중앙 집중화된 거래소(CEX)나 분산화된 거래소(DEX) 등으로 전송하여 현금화를 시도하면 이를 막을 수 있는 방안이 없었습니다. 하지만 모든 이해 당사자들이 ICF API를 이용해 연합하고 악의적인 보안위협에 공동 대처함으로써, 악성 행위를 사전에 차단하고 도난당한 암호화폐의 흐름을 파악한다면, 이를 기반으로 원래 소유자에게 반환할 수 있는 근거가 될 수 있습니다.

왜 ICF API 인가요?

블록체인 생태계가 활성화되고 전통적 기업들의 블록체인 시장 진입이 늘어남에 따라, 암호화폐 거래의 안정성을 보장받기 원하는 블록체인 기업들의들의 요구가 커지고 있으며, FATF 규제안에 발맞춰 점차 강화되고 있는 암호화폐 관련 자금세탁방지(AML), 테러자금조달차단(CFT) 규정으로 규제 감독기관 역시 공신력 있는 데이터를 지속적으로 요구하고 있는 실정입니다.

또한 컴퓨터, 서버의 컴퓨팅 자원을 훔쳐 암호화폐 채굴에 악용하는 '크립토재킹' 또는 '악의적 마이닝 멀웨어' 등 정교한 형태로 진화된 다양한 악성 공격에 대한 해결책 역시 시급한 상황입니다.

국제표준 표현규격인 STIX 준수

전통적 사이버 보안 업계에서 범용적으로 사용하는 ' 사이버 보안위협정보 표준 '인 STIX 표준을 준수하는 검색 필드를 제공합니다. 거래 암호화폐 주소, 암호화폐 주소, 보안위협 범주, 보안위협 하위 유형, 보안위협 ID 등 STIX표준에서 지정한 항목을 최대 10개까지 조건을 걸어 검색할 수 있습니다. 때문에 ICF API을 사용하는 기업 고객의 경우 전세계에 널리 사용되는 표준 포맷을 준수하고 있으므로, 별도의 사내 보안규정에 따른 감사를 추가적으로 받거나, 보안 검사에 대한 이중투자를 하실 필요가 없습니다.

왜 ICF API 인가요?

크라우드소싱 기반의 최신위협정보 공유

ICF API는 집단지성 기반의 TRDB에 취합된 최신 보안 위협 정보를 실시간 공유하여 사용자가 멀웨어, 피싱 및 혐의거래 관련 지갑 주소, URL 및 도메인에 대해 검증이 완료된 화이트리스트 및 블랙리스트 정보를 제공받을 수 있게 합니다.

모든 금융소프트웨어와의 높은 호환성

ICF API의 주요 특징 중 하나는 플랫폼의 독립성입니다. 모든 암호화폐 거래소, 지갑, DApp 또는 암호화폐 트랜젝션 관련 애플리케이션 등, 다양한 고객군의 니즈에 맞게 커스터마이즈 되어 손쉽게 결합할 수 있으며 보안 규정에 대한 검사를 신속하게 수행할 수 있습니다.

누가 사용하면 좋은가요?

ICF API는 국제적 표준 표현 규격인 STIX를 사용하여 어떤 소프트웨어와도 쉽게 호환이 가능합니다. 따라서 모든 디지털 자산 서비스 사업자(VASP)에게 제공 가능하며 고객사 내부 보안 규정 검사를 신속하게 수행, 암호화폐 거래의 안전성을 극대화시킵니다.

암호화폐 거래소, Dapp(분산어플리케이션) 프로젝트 팀, 지갑 서비스 제공자, 커스터디 사업자 모두 사용 가능하며 메인넷 및 신규 블록체인 사업을 추진 중인 기업에게는 표준 컴플라이언스 또는 익스플로러의 역할도 수행 가능 합니다. 또한 CATV와 결합 시 암호화폐 거래추적 및 분석 기능을 통해 사기범죄 수사의 증적자료로 활용 가능하므로 사법금융기관에서도 활용할 수 있습니다. 이뿐만 아니라 글로벌 Fortune500대 기업 중 2개 회사와 협력하여 블록체인 생태계 사업의 보안요소기술로서 검증을 받고 있습니다.

OCTA SOLUTION

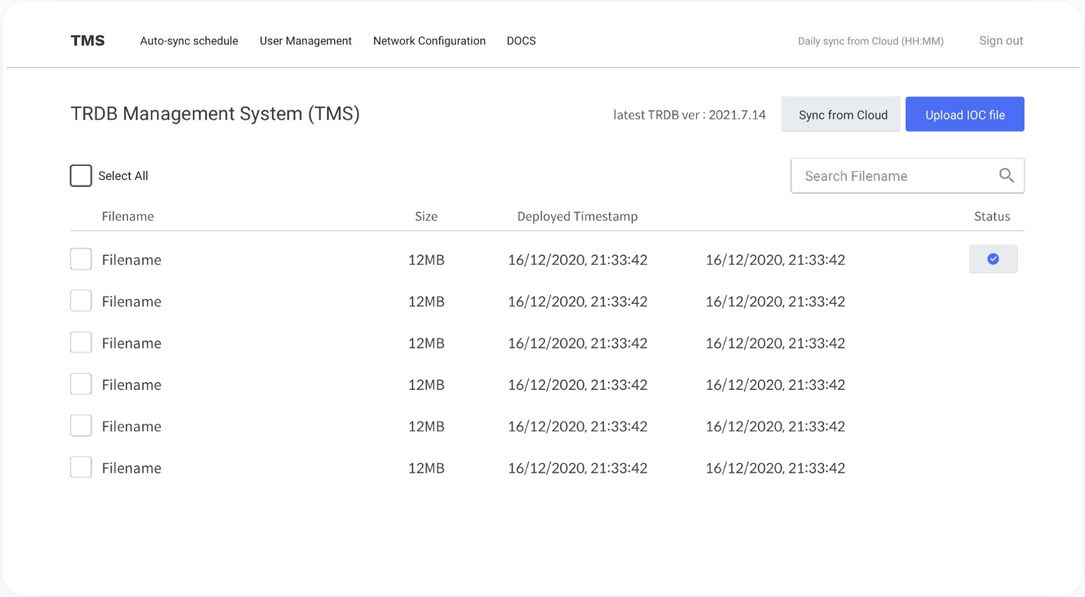
옥타 솔루션, RegTech 기반 컴플라이언스 솔루션

Hexlant.

헥슬란트, 블록체인 연구소

parsiq

파시크, 블록체인 분석 플랫폼

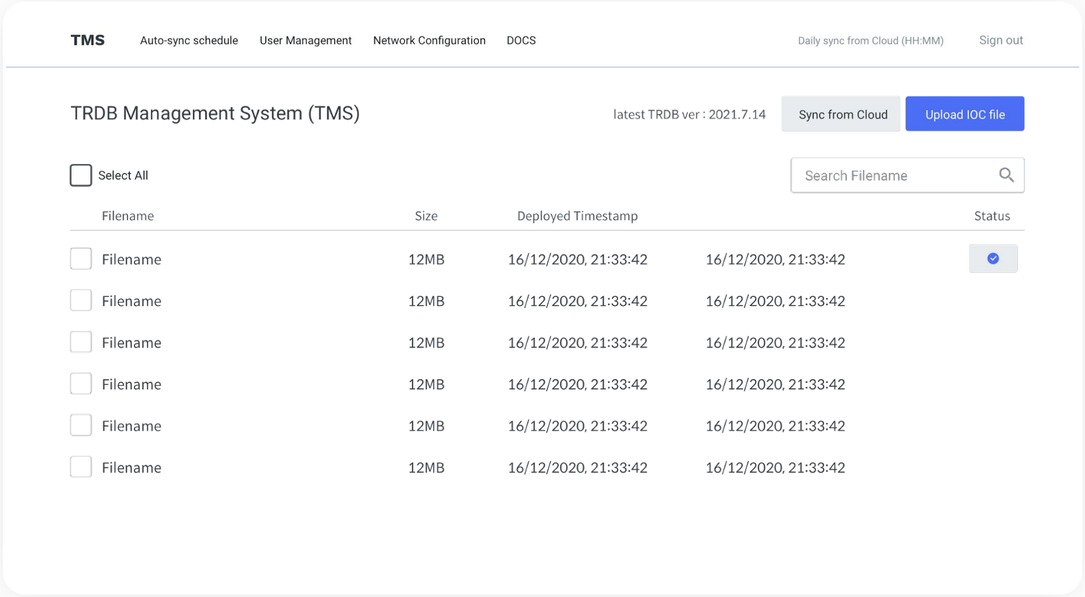


TOMS API

Threat Reputation Database On-premise Management System

내부망 구축형 로컬 TRDB (위협 평판 데이터 베이스)

2021년 3월에 출시된 TOMS API는 엄격한 최신 규제 요구 사항을 충족하도록 설계되었으며, 최근 급격히 증가한 온프레미스 솔루션에 대한 수요에 적극적으로 대응합니다.



TOMS의 주요 기능에는 최신 위협 인텔리전스 데이터가 포함되어있으며 RESTful API를 통해 다양한 형태의, 애플리케이션 및 서비스와 함께 유연하게 연동이 가능합니다. 또한 온프레미스 특성에 맞게, 조직의 내부 컴퓨터 네트워크에서 인터넷 연결 없이도 위협 평판 데이터베이스(TRDB)에서 호스팅되는 최신 보안 인텔리전스 데이터에 액세스가 가능합니다.

정부의 상위 기관, 금융 기관 및 금융 소프트웨어 애플리케이션들은 가장 선도적으로 엄격한 규제 프레임워크를 준수해야 하기때문에 TOMS API가 제공하는 서비스를 통해 데이터 개인 정보 보호 및 보안을 강화에 보다 유연하게 대응할 수 있습니다.

Defense Security

사이버보안 툴

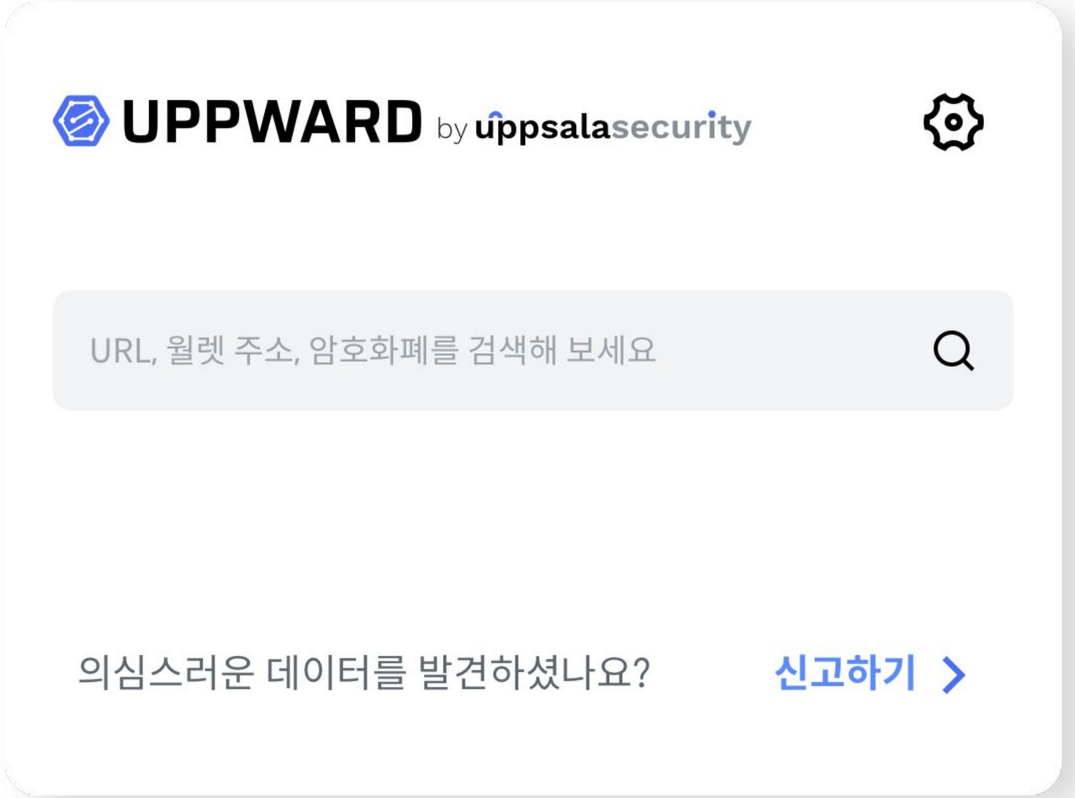
UPPward 웁워드 보안 툴

Sentinel Protocol Dapp 센티넬 프로토콜 디앱

최근 몇 년 사이, 기업과 조직에게 주요한 화두로 다루어 졌던 사이버 보안 이슈는 이제 모든 인터넷 사용자들의 일상적인 문제로 대두되었습니다. 때문에 센티넬프로토콜은 사용자들이 피싱, 크립토 재킹과 같은 사이버 공격을 받거나, 악성코드에 감염되기 전에 선제 방어 및 예방을 할 수 있는 더 확실한 보안 솔루션을 제공하고자 Defense security 를 개발하였습니다.

사용자는 센티넬 프로토콜이 제공하는 사이버 보안 툴을 개인 PC 및 브라우저에 손쉽게 다운 받아 사용할 수 있으며, 센티넬프로토콜의 위협 평판 데이터베이스(TRDB)를 통해 크라우드 소싱된 최신 사이버 보안 위협 (안전한 URL과 도메인, 악의적인 URL, 온라인 지갑주소의 블랙리스트 등) 정보및 알람을 제공받을 수 있습니다.

UPPward



UPPward

UPPward Security Tool

웁워드 보안 툴

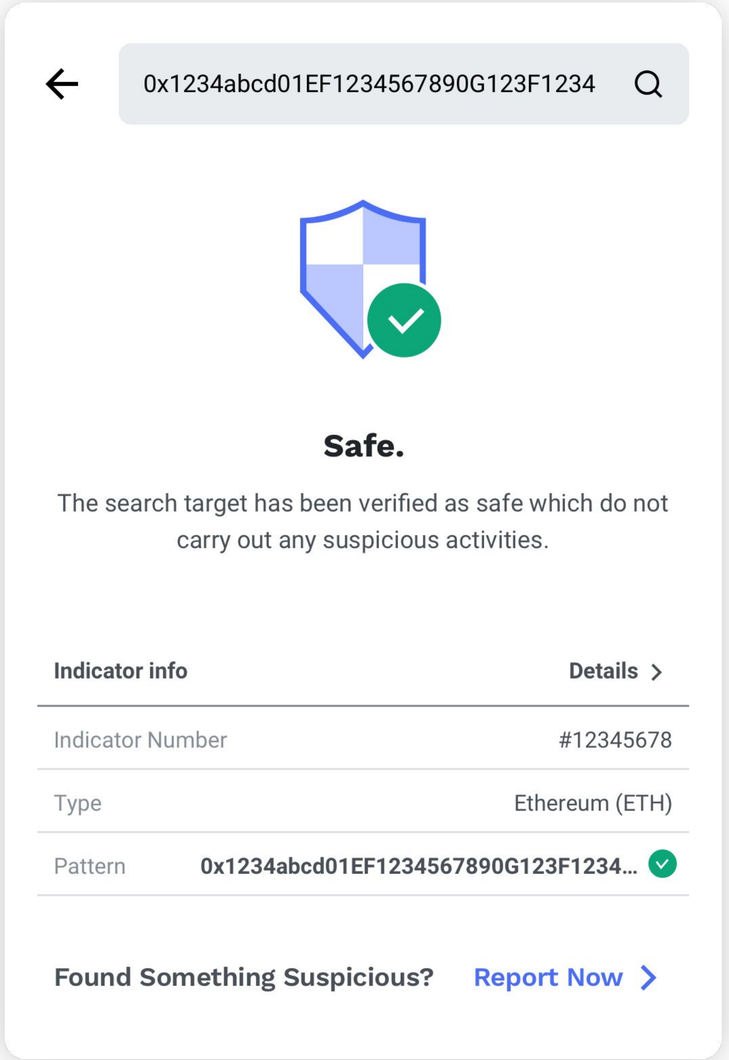
웁워드는 모든 사람들이 웹 브라우저 안에서 무료로 사용할 수 있는 사기 방지 보안 툴 입니다. 웁워드는 별도의 회원가입 없이 웹사이트, 트위터, 암호화폐 주소 등의 진위 정보를 모든 사용자에게 쉽고 빠르게 제공합니다.

UPPward 는 무엇인가요?

UPPward 브라우저 익스텐션은 스캠 &. 사기 방지 보안툴입니다.
사용자가 접속하고 있는 웹사이트(URL)와 센티넬 프로토콜의
위협 평판 데이트베이스(TRDB)를 상호 참조하여 능동적으로
데이터의 안정성을 판별 후, 해당 URL이 위협정보일 경우
사용자에게 경고합니다.

사용자들은 직접 UPPward 검색창에 URL, 혹은 암호 화폐 지갑
주소 등을 검색함으로써 안전한 정보인지 확인할 수 있고,
위협정보로 의심되는 사건들은 웁살라시큐리티의 보안전문가에게
신고할 수도 있습니다.

UPPward는 웹사이트 내의 지갑주소를 스캔하여 혐의거래와
연관성이 있는 블랙리스트 지갑주소가 감지되는 경우 빨간색으로
표시해 의심스러운 정보임을 알려줍니다.



어떻게 작동하나요?

위협정보 알림

사용자가 접속해 있는 웹사이트에 따라 브라우저 오른쪽 상단에 있는 웁워드 아이콘의 색깔이 달라집니다.

암호화폐 주소 하이라이트

암호화폐 주소 하이라이트 기능은 웹사이트에서 TRDB에 블랙리스트로 등재된 지갑주소를 감지합니다. 블랙리스트 지갑 주소가 감지되면 웁워드는 해당 지갑 주소를 빨간색으로 하이라이트 함과 동시에, ‘Suspicious’ 로 표시하여 의심스러운 주소라는 것을 알립니다.

의심스러운 정보 신고

사용자들은 웁워드 검색창 하단에 있는 “Report Now”를 클릭하여 웁살라 시큐리티의 보안 전문가인 센티넬 에게 의심스러운 데이터, 해킹, 피싱 정보 등을 신고할 수 있습니다. 사용자가 신고한 리포트는 웁살라시큐리티 보안전문가들의 분석&검증을 거치게 되며 유효한 것으로 인정될 경우 블록체인 상의 TRDB에 저장되고 해당 블랙리스트 데이터는 사용자에게 실시간으로 공유됩니다.

쉽고 빠른 검색

사용자는 URL, 도메인, 암호화폐 주소, 트위터 ID 및 이메일 주소를 검색창에 입력하여 관련 위협을 확인할 수 있습니다. 웁워드는 사용자가 입력한 값과 TRDB의 데이터를 대조 후 정상적인 정보인지 위협 정보인지 판단합니다.

어떻게 작동하나요?

정상

화이트리스트에 포함되어 있습니다.
정상적인 활동이 가능합니다.

주의

TRDB에서 확인되지 않고,
화이트리스트 또는 블랙리스트에
모두 등록되어있지 않은 웹사이트
입니다. 중요한 정보를 입력해야 하는
경우 주의가 필요합니다.

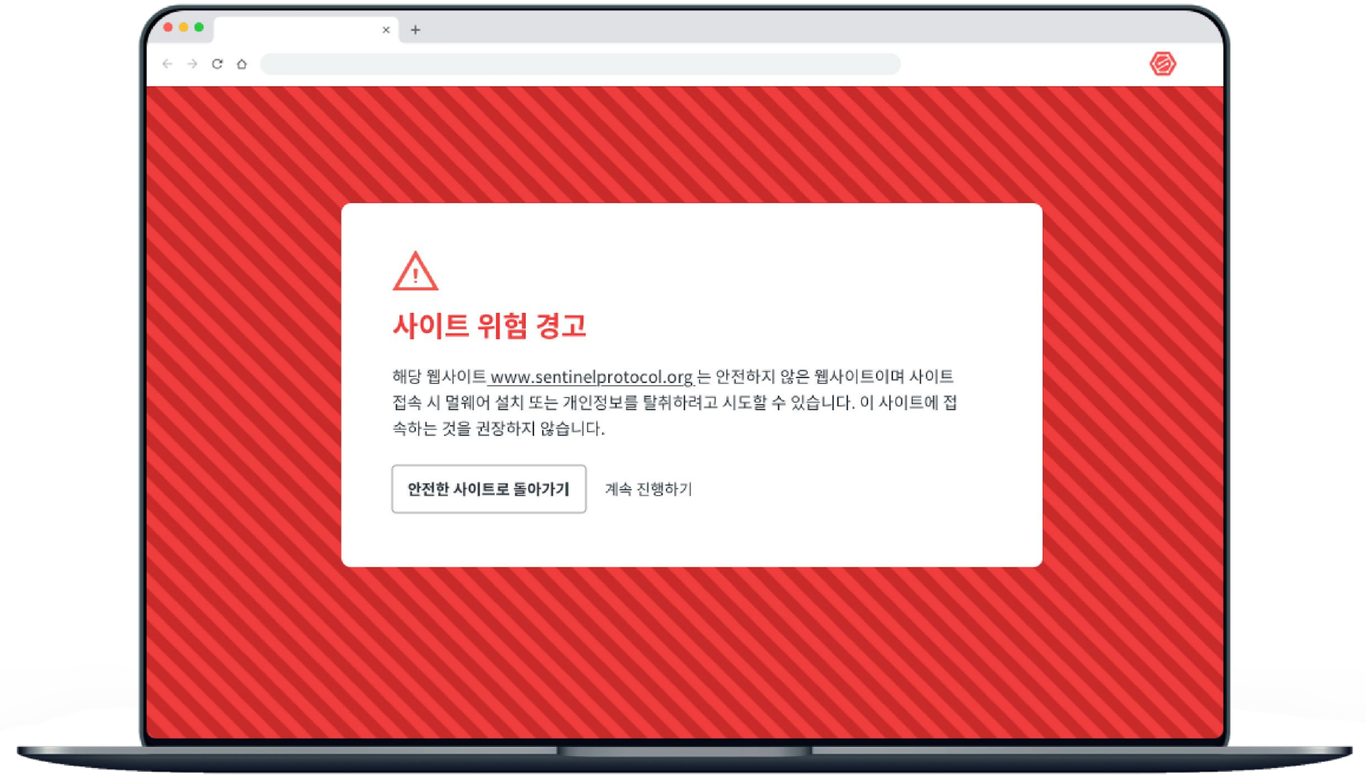
위험

블랙리스트에 포함되어 있습니다.
개인정보 입력 등 을 권장하지
않습니다.

왜 UPPward 인가요?

의심스러운 데이터 사전 차단

ICO 회사의 피싱 웹사이트는 접속자의 개인정보를 탈취하고 사용자의 디바이스를 멀웨어에 감염시키며, 악성 지갑주소로의 송금을 유도합니다. UPPward는 웹 브라우저상에서 이러한 악의적인 웹사이트 방문 시 경고 메세지를 주고, 거래가 완료되기 전에 상대방의 지갑주소의 안전성을 파악, 이를 사용자에게 알림으로써 사기피해를 예방할 수 있도록 돕습니다.



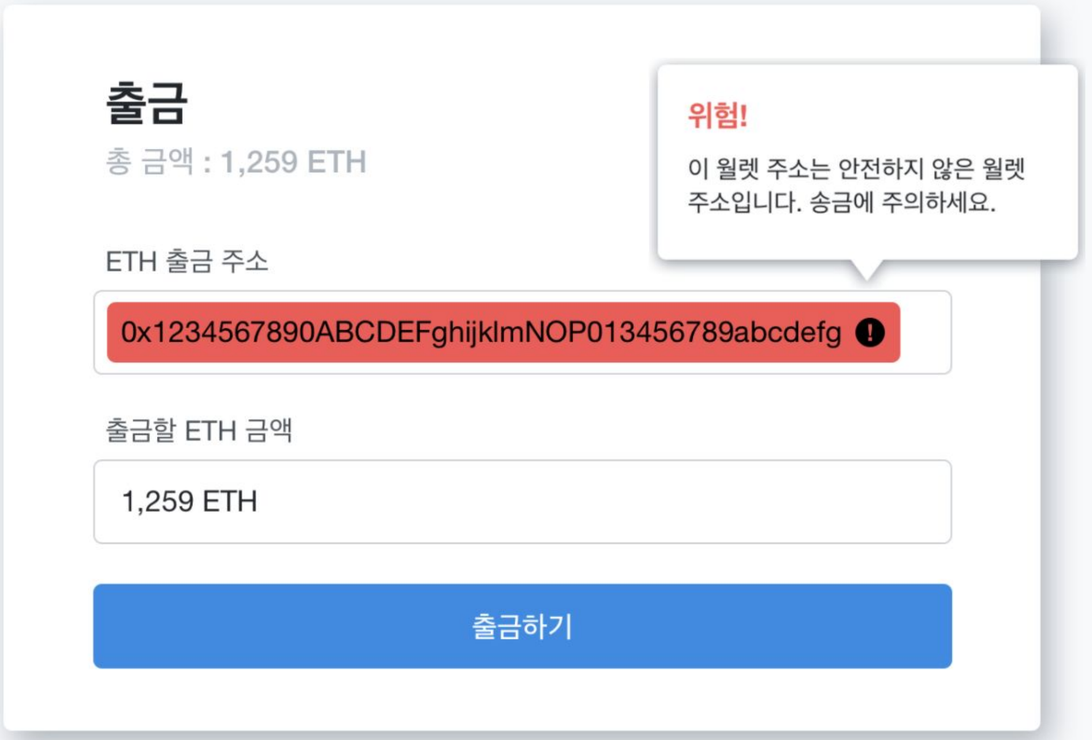
왜 UPPward 인가요?

최고의 보안 전문가들이 인증

UPPward를 통해 제공되는 위협정보와 데이터는 최고수준의 보안 전문가들이 직접 분석 및 검증하여 데이터의 유효성을 평가하고 승인합니다.

집단지성을 통한 최신위협정보 공유

사용자들이 의심거래나 사기, 해킹 등의 사건을 UPPward 를 통해 직접 제보할 수 있으며, 동시에 신고된 내용 중 유효한 것으로 확인된 URL, 지갑 주소 등은 다른 사용자들이 같은 피해를 입지 않도록 실시간 공유함으로써 2차 피해를 예방합니다. 또한 유효한 데이터를 신고한 사용자에게 보상을 제공하는 리워드 프로그램을 통해 실생활에서 보다 널리, 적극적으로 사용될 수 있도록 할 예정입니다.



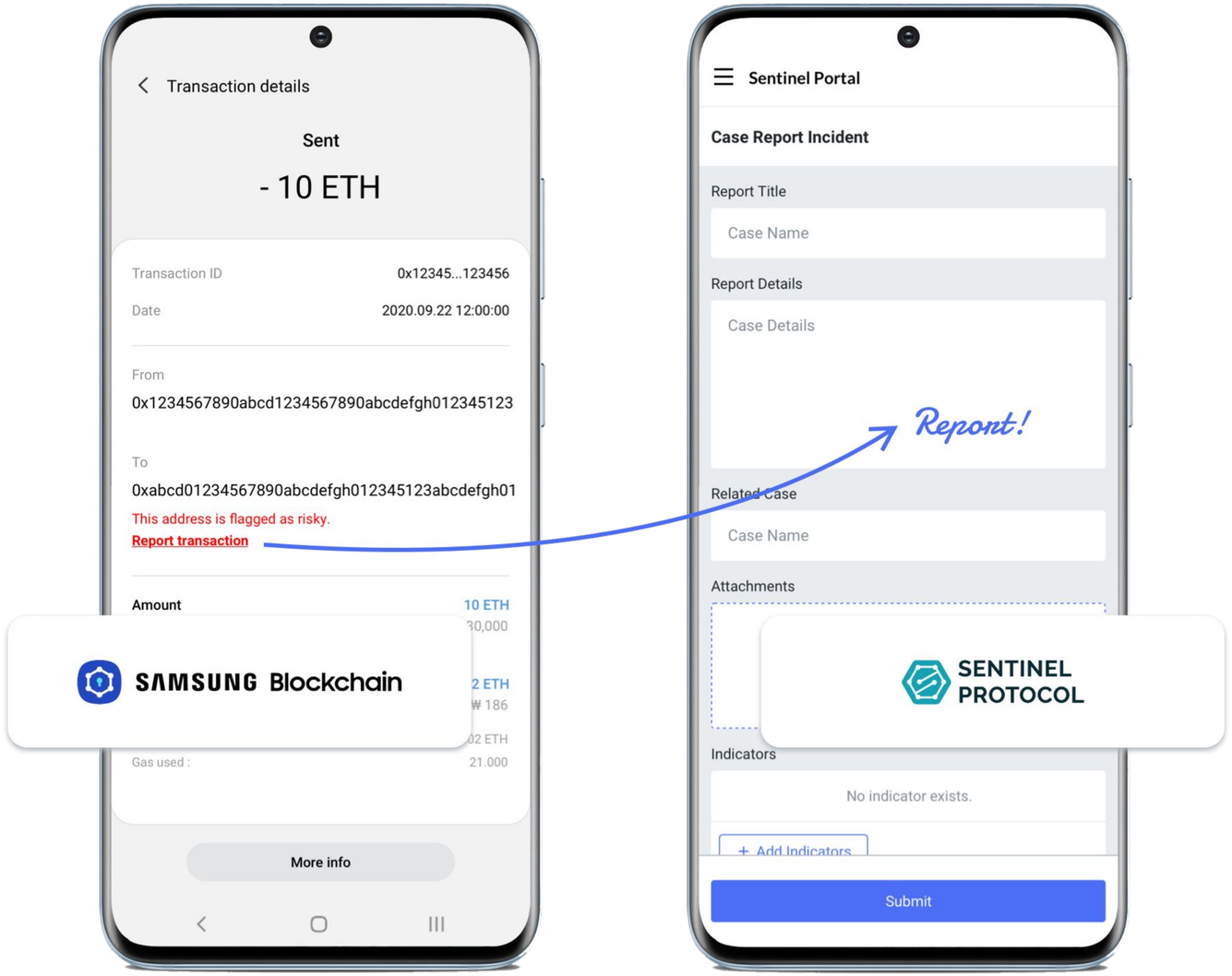
Uppsala Security's AML

SAMSUNG Blockchain

웁살라시큐리티 AML 통합 보안 서비스, 전세계 19개국 삼성 블록체인 월렛 이용자 지원

삼성전자에서 출시한 최신 핸드폰 기종(갤럭시 S10 시리즈 이상)을 사용하는 삼성 블록체인 월렛 글로벌 이용자에게 웁살라시큐리티 AML 통합 보안 서비스를 실시간으로 지원하고 있습니다.

서비스 지원 국가
노르웨이, 대한민국,
덴마크, 독일, 루마니아, 미국, 브라질, 스웨덴, 스위스, 스페인, 싱가포르,
아이슬란드, 영국, 오스트리아, 캐나다, 포르투칼, 필리핀, 핀란드 (2020년 12월 기준)

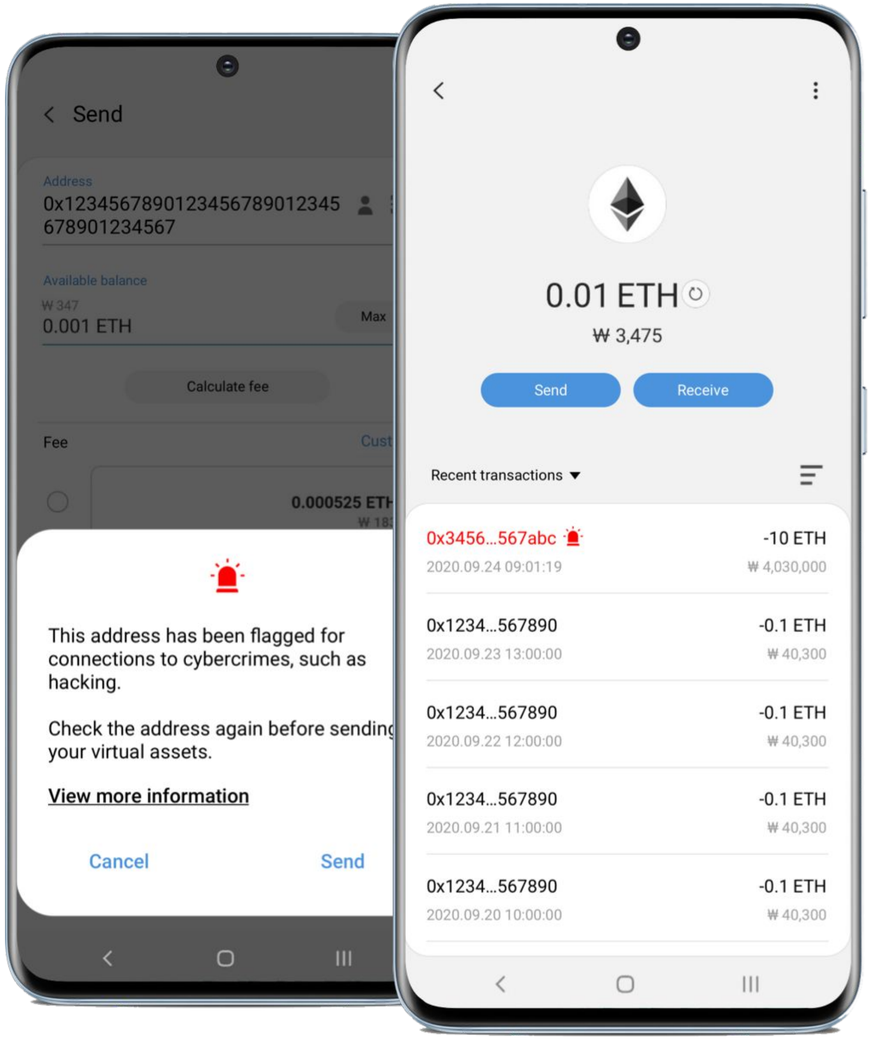


삼성 블록체인 월렛 맞춤 웁살라시큐리티의 독보적 AML 통합 보안 서비스

1. 가상자산 송금 전 안전한 월렛인지 사전 검증
센티넬프로토콜의 위협 데이터베이스(TRDB)
를 통해 송금하고자 하는 상대방의 지갑 주소가 해킹, 스캠, 다크웹 등
범죄에 사용된 이력이 있는지 사전 조회하여, 안전성이 검증된 거래를 할 수 있습니다.

2. 이용자 모르게 일어난 위험거래 탐지 및 Push Notification
센티넬프로토콜의 AML 솔루션을 통해 블랙리스트 지갑과의 위험 거래 탐지 즉시 이용자에게 푸시 알림을 통해 경고합니다.

3. 자금세탁과정 추적해 피해 이용자에게 증적자료 제공
삼성 블록체인 월렛 이용자가 의심스러운 월렛 또는 위험거래를 발견 시, 월렛에
연동된 센티넬 포털사이트를 통해 신고하거나추적 의뢰를 할 수 있으며,
필요시 경찰 및 사법기간에 신고할 수 있으며
필요시 경찰 및 사법기간에 신고할 수 있는 '거래 추적 보고서'를 증적
자료로 제공받을 수 있습니다.



Data Analytic Tools

데이터 분석 툴

CARA 크립토 분석 위험도 평가

CATV 암호화폐 추적 보안 솔루션

실제 해커들은 암호화폐 탈취 후 자금을 세탁하는 과정에서 텀블링과 믹싱 (Tumbling and Mixing) 기술을 이용해 거래기록을 감추기 때문에 자금의 흐름을 수동으로 따라가는 것은 막대한 시간과 노력이 필요한 일이며, 경우에 따라서는 추적 자체가 불가능하기도 합니다.
하지만 센티넬프로토콜의 데이터 분석 툴은 암호화폐 거래의 자동 매핑 기능을 통해 신속한 혐의거래 추적이 가능하며, 거래내역 리포트 자동 생성 기능으로 간편하게 사후보고 및 실시간 데이터 공유를 할 수 있습니다.

뿐만 아니라 센티넬 프로토콜은 인공지능(AI) 머신러닝 모듈을 추가해 비정상 행위가 발생한 거래를 선제적으로 분석하고 해킹 등의 사고에 실시간으로 대응할 수 있도록 개발을 진행하고 있으며, 이는 FATF 규제안의 핵심인 위험 기반 접근 (Risk based Approch:RBA)을 준수하는 AML/CFT 솔루션이 됩니다.

—

CARA

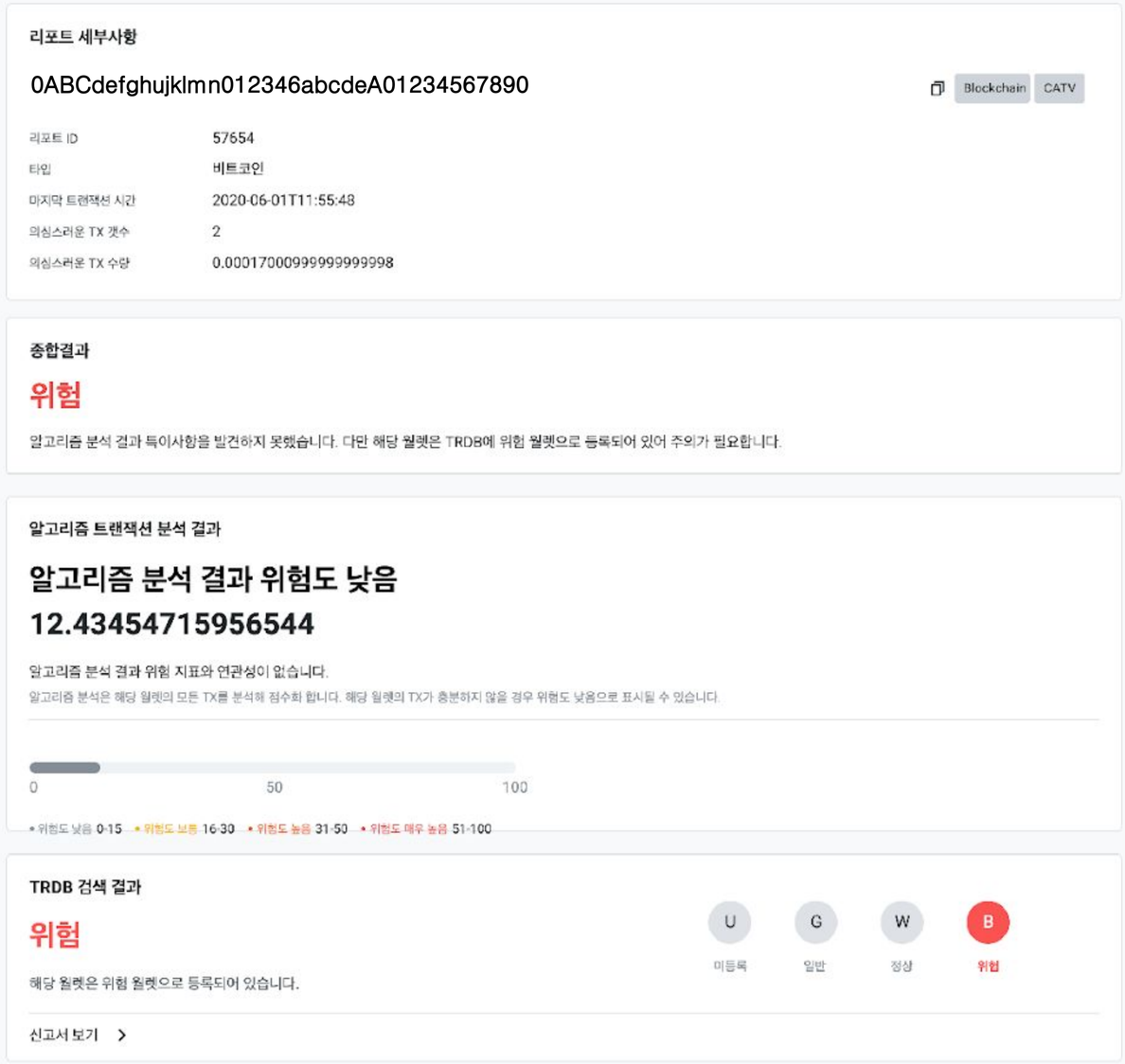
CATV

CARA

Crypto Analysis Risk Assessment

크립토 분석 위험도 평가

CARA(Crypto Analysis Risk Assessment)는 알려진 위험지갑과 알려지지 않은 위험지갑에 대한 패턴 분석을 기반으로 머신러닝 라고리즘에 사용하여 특정거래의 위험수준을 판단하는 AI 기반의 위험평가솔루션 입니다.



CARA 는 무엇인가요?

CARA는 거래 지갑의 행동패턴을 분석 & 학습해 암호화폐 거래에 대한 위험평가를 예측합니다.

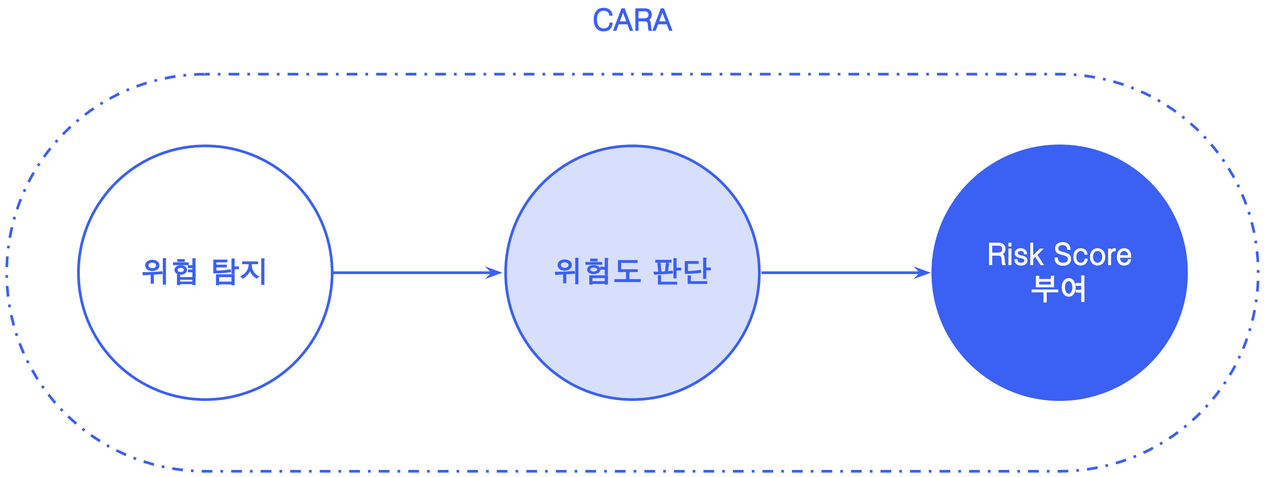
CARA는 이미 알려져 있는 의심거래지갑과 정상거래지갑의 행동을 지속적으로 분석학습하는 머신러닝 알고리즘을 사용해 특정 암호화폐주소의 위험 수준을 판단하고, 그 위험도를 사용자에게 알려주는 암호화폐 거래 위험평가솔루션입니다.

CARA는 FATF(Financial Action Task Force)에서 권장하는 위험 기반 접근 방식(RBA)을 준수하며, 풍부한 데이터 학습을 통해 해킹, 사기, 돈세탁, 테러자금 등 디지털 자산을 탈취하려는 모든 종류의 악의적 행위를 사전에 파악하는 직관력, 즉 식스센스(the sixth sense)를 탑재한 디지털 자산관리 솔루션이라 할 수 있습니다.

***웁살라시큐리티는 2020년 9월 과학기술정보통신부 주최 'AI 데이터 가공 바우처 사업'의 수요기업으로 선정되어, 공급 기업인 'NSHC'로부터 다크웹 관련 위협 데이터를 제공받아 CARA(Crypto Analysis Risk Assessment)의 AI 서비스 고도화를 진행 완료하였습니다.**

어떻게 작동하나요?

CARA는 머신러닝 모듈을 통해 혐의거래 지갑과 정상거래 지갑의 과거 행동패턴을 정밀하게 학습하고, 거래형태에 따라 암호화폐 지갑의 위험수준을 판별하는 자체 평가 기준을 갖게 됩니다. 이를 통해 CARA는 단순히 디지털 자산과 주요 데이터를 탈취하는 잠재적 위협을 탐지하는 데에서 한 걸음 더 나아가 거래의 형태를 통해 위험도를 판단, Risk Score를 부여함으로써 특정 암호화폐 주소에 대한 위험 평가를 제공합니다.



인공지능(AI)과 머신러닝은 사이버보안 산업뿐 아니라 다른 디지털 생태 계에서도 선도적인 솔루션으로 인식되고 있습니다.
센티넬프로토콜은 이미 자사 위협평판 데이터베이스인 TRDB에 크라우드소싱된 보안 위 협 데이터를 축적해오고 있으며 현재까지 약 6,300만개의 (2022년 2월 기준) 지표와 카운트를 보유하고 있으며 실시간으로 추가되고 있습니다.

이는 신뢰할 수 있는 머신러닝 알고리즘과 AI 기반의 사이버 보안 솔루션을 개발하는데 핵심적인 역할을 수행하고 잠재적 위협을 탐지하며, 한 걸 음 더 나아가 암호화 지갑 주소에 대한 위험 평가를 제공합니다.

왜 CARA 인가요?

우리는 수 많은 디바이스들이 서로 연결되어 데이터를 교환하고 또 새로운 가치를 만들어내는 세상에 살고 있습니다. 하지만 이는 악의적 해킹과 사기 등, 알려진 혹은 알려지지 않은 수많은 사이버 위협으로 부터 개인과 기업의 디지털 자산이 취약해질 수 있다는 것을 의미합니다.
블록체인 보안회사인 CiperTrace의 암호화폐 자금세탁방지 리포트에 따르면, 해킹, 도난, 탈취, 사기와 연루된 자금이 2019년 중반까지 사십억 달러를 초과할 것이라고 예측됩니다. 이러한 상황을 해결하기 위해 자금세탁과 테러자금에 효과적으로 대응할 수 있는 신뢰도 높은 솔루션이 필요합니다.

CARA는 국제자금세탁방지기구 Financial Action Task Force (FATF) 권고안의 핵심인 위험기반접근법(RBA, Risk-based Approach) 을 준수하는 AML/CFT 솔루션으로 사용자가 자금세탁이나 테러리스트 자금조달 혐의를 받는 암호화폐 주소를 사전에 파악하는데 도움을 줍니다.

누가 사용하면 좋은가요?

암호화폐 거래소, Dapp(분산어플리케이션) 프로젝트 팀, 지갑 서비스 제공자, 커스터디 사업자 모두 사용 가능하며 디지털 스페이스에서 사이버 안전에 관심이 있는 사람이면 누구나 CARA의 잠재적인 사용자라고 할 수 있습니다.

센티넬 프로토콜은 특히 개인이 제3자를 이용하지 않아도 자산을 저장거래할 수 있는 분산화된 블록체인 세상에서 사이버 보안의 책임은 개인과 기업 모두에게 중요하다고 생각합니다.
CARA는 해킹, 사기, 자금 세탁, 테러 자금 지원 또는 디지털 자산을 기반하는 기타 모든 유형의 악의적인 행위를 사전에 파악하는 직관력, 즉 식스센스(the sixth sense)를 탑재한 디지털 자산관리 솔루션이라 할 수 있습니다.

CARA는 현재, 비트코인(BTC), 이더리움(ETH) 및 ERC-20, 라이트코인(LTC), 트론(TRX), 이오스(EOS), 스텔라(XLM), 리플(XRP), 비트코인 캐시(BCH), 바이낸스 코인(BNB), 바이낸스 스마트 체인(BSC) 및 카르다노(ADA) 지갑주소들에 대한 서비스를 지원하고 있습니다.

—

CARA

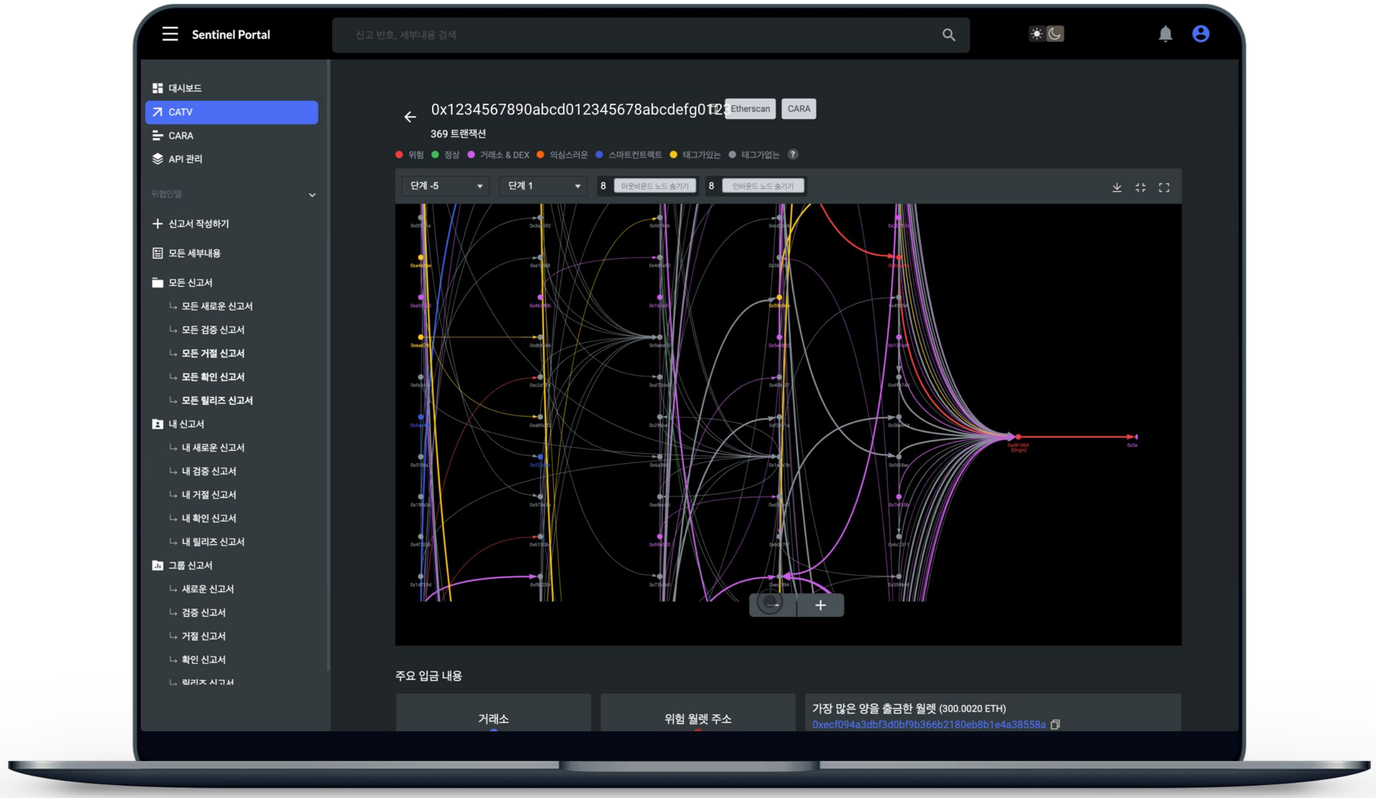
CATV

CATV

Crypto Analysis Transaction Visualization

암호화폐 추적 보안 솔루션

CATV(Crypto Analysis Transaction Visualization)는
특정 지갑이 어디에서 자금을 받아 어디로 송금하는지,
암호화폐 거래 흐름을 보여줌으로써 통찰력을 제공하는
암호화폐 거래 추적 보안 툴입니다.



CATV 는 무엇인가요?

Threat Reputation Database (위협평판 데이터베이스, TRDB)를 기반으로 암호화폐 거래이후 디지털 자산의 흐름 추적, 분석 그리고 시각화를 제공합니다. CATV는 사용자들이 알려진 사이버 범죄에 의도치 않게 연루되는 것을 막고, 자신이 모르는 사이 돈세탁이나 테러 자금조달에 동참하게 되는 것을 방지할 수 있습니다.

어떻게 작동하나요?

CATV의 핵심 기능은 도난 자금을 포함한 블록체인 상의 암호화폐를 추적하는 것입니다. 특정 지갑 주소를 입력하면 원클릭만으로 자금을 추적하고 자동으로 요약된 거래 흐름도를 확인할 수 있습니다.
이를 통해 사용자들은 입력한 지갑 주소에서 시작된 송금 거래가 얼마나 진행되었는지 추적할 수 있으며, 동시에 해당 지갑주소까지 자금이 어떻게 흘러 들어왔는지 유입 경로의 추적도 가능합니다. 이때 각 거래에 TRDB 의 정보가 반영되어 각 거래에 대한 위험을 시각적으로 제공합니다. 뿐만 아니라 그래픽에사용된 전체 거래의 리스트가 제공되며, 이를 통해 추가 분석 및 보고서를 작성하는데 활용할 수 있습니다.

Threat Reputation Database (위협평판 데이터베이스, TRDB)

TRDB에는 암호화폐 거래소, 지갑 회사, 디지털 자산 보관 서비스 업체, 결제 서비스 업체, IT 및 사이버 보안 회사를 포함한 다양한 소스로부터 수집된 검증된 보안 정보가 들어 있습니다.

왜 CATV 인가요?

현금과는 달리 디지털 자산은 추적이 가능하지만, 해커에 의해 도난 당하거나 사기 행각을 통해 탈취될 수 있으며, 물리적인 형태가 없기 때문에 언제 어디서든 이동이 가능합니다. 이러한 디지털 자산의 특징을 바탕으로 CATV는 다음과 같은 솔루션을 제공합니다.

거래 추적의 자동화 및 신속화

해킹, 사기 등으로 암호화폐 및 디지털 자산을 도난 당했을 경우, 지갑과 각 거래 내역을 일일이 수동 조회할 필요 없이, 도난당한 자금의 흐름을 자동으로 조회해 시각적 그래프로 나타냄으로써 신속한 분석이 가능하도록 합니다.

보안위협정보 실시간 제공

CATV 툴을 포함한 모든 센티넬프로토콜 솔루션의 핵심에는 Threat Reputation Database (TRDB)가 있습니다. 사용자는 실시간으로 업데이트되는 크라우드 소싱 기반의 TRDB 최신 보안 위협정보를 제공받게 됩니다.

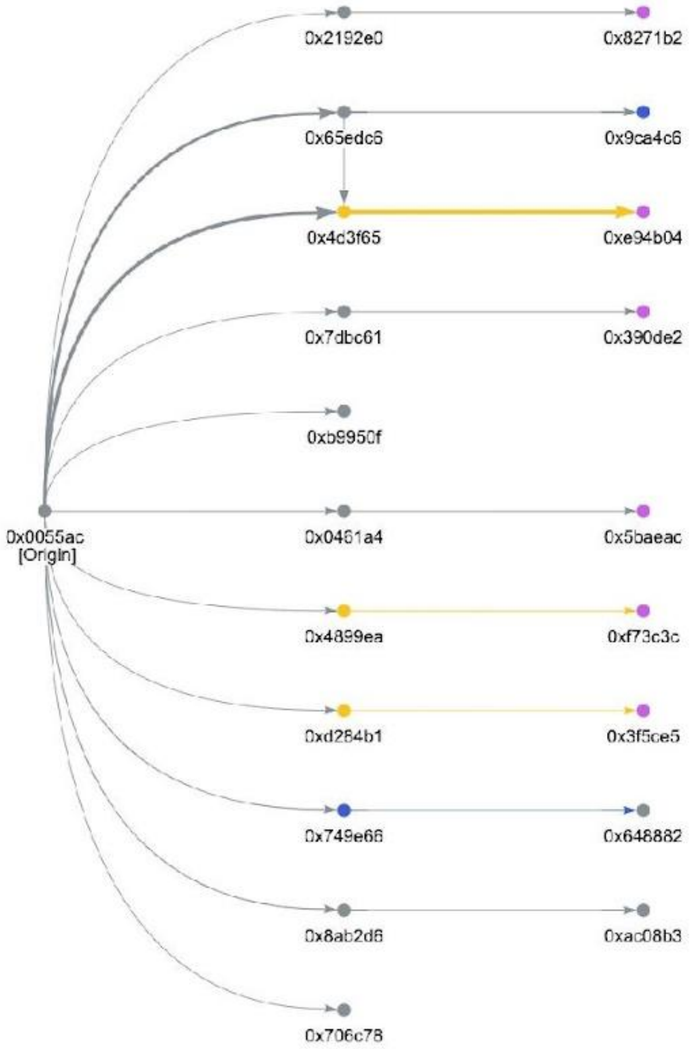
왜 CATV 인가요?

자금세탁방지와 테러자금조달방지에 기여

CATV툴은 사이버범죄에 연루된 암호화폐가 거래소등으로 유입될 경우 이에 대한 정보를 사법당국과 암호화폐 거래소등 관련 기관에게 제공함으로써 암호화폐 거래소가 자금세탁의 창구가 되지 않도록 하는 데에 기여할 수 있습니다.

거래내역 리포트 자동생성

시각화 된 그래프에 해당하는 전체 거래내역 리스트를 기반으로 관련 리포트를 자동으로 생성할 수 있습니다. 이를 통해 자금 이동에 대한 통찰력를 제공하며, 신속한 분석이 가능하도록 합니다.

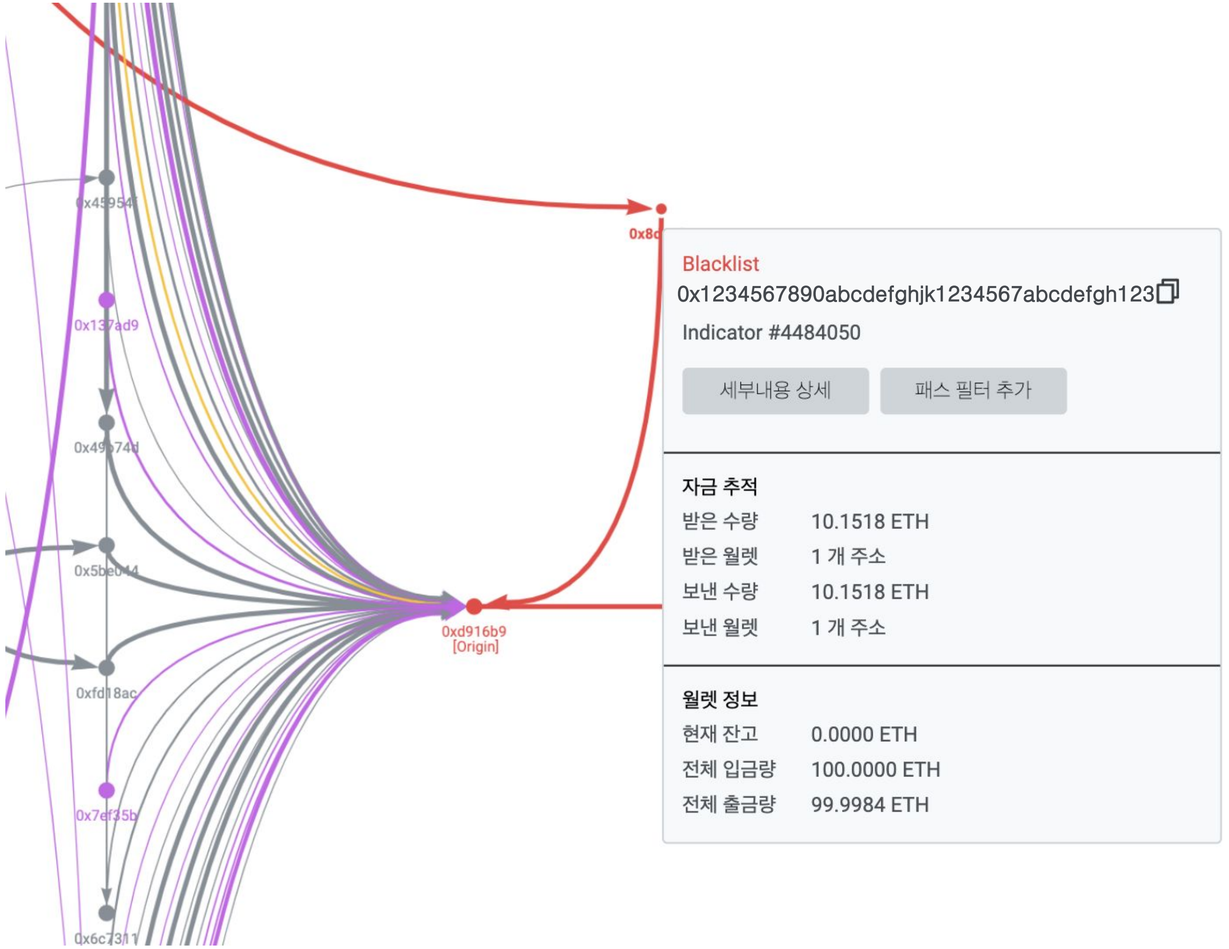


누가 사용하면 좋은가요?

CATV는 기업과 개인 모두 사용 가능합니다. 암호화폐를 다루는 모든 조직 및 개인들에게 사이버 범죄자들 과의 부주의한 거래를 막고 반테러 자금 조달(CTF, Counter-Financing of Terrorism) 및 자금세탁방지(AML, Anti-Money Laundering)에 도움을 줄 수 있습니다.

* CATV 지원 가능 토큰

비트코인(BTC), 이더리움(ETH) 및 ERC-20, 라이트코인(LTC), 트론(TRX), 이오스(EOS), 스텔라(XLM), 리플(XRP), 비트코인 캐시(BCH), 바이낸스 코인(BNB), 바이낸스 스마트 체인(BSC) 및 카르다노(ADA) (2022년 2월 기준)



CATV 사용자 가이드

https://www.youtube.com/watch?v=07YMeULoDJU

Professional Services

전문 서비스

SWAP 지갑 주소 분석요약 프로파일링

DATS 디지털자산 추적 서비스

움살라 시큐리티는 역동적으로 변화하는 기술혁신 시대에 고객이 선제적으로 비지니스 리스크를 관리하고 컴플라이언스를 준수하여 경쟁력을 갖출 수 있도록 고객 맞춤 암호화폐 거래 위험 평가 레포트 서비스를 제공합니다.

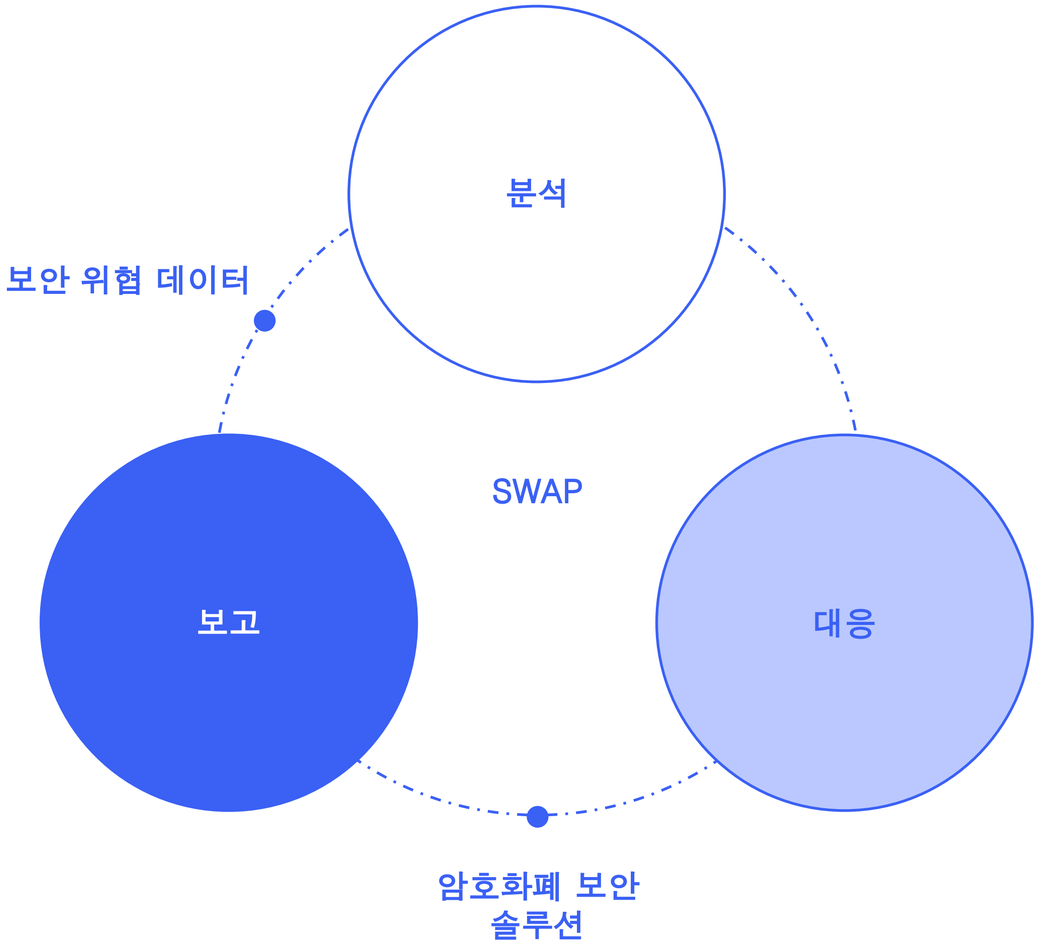
SWAP

SWAP

Summary Wallet Analytical Profiling

지갑 주소 분석요약 프로파일링

자사가 수집보유하고 있는 보안 위협 데이터(Threat Intelligence)와 암호화폐 보안 솔루션을 바탕으로 잠재적인 혐의거래와 리스크를 분석, 사전에 보고함으로써 고객이 전략적으로 리스크 대응을 하고 비즈니스 목표를 달성할 수 있도록 지원합니다.



SWAP은 무엇인가요?

핵심 위험요인, 사전 파악해 알려주는 암호화폐 거래 위험 분석 보고서

Summary Wallet Analytical Profiling (SWAP)은 암호화폐 프로젝트 기업의 비즈니스 역량 강화와 규정 준수를 위한 웁살라시큐리티 의 고객 맞춤 서비스로, 모든 지갑 주소와 거래 패턴을 360°다각도로 심층 분석해 '암호화폐 거래 위험 평가 리포트'를 제공합니다.

해당 보고서는 자사의 암호화폐 추적 보안 솔루션인 Crypto Analysis Transaction Visualization(CATV)와 인공지능(AI) 머신러닝 기반 암호화폐 위험 평가 툴인 Crypto Analysis Risk Assessment (CARA)를 통해 거래 흐름과 패턴을 선제적으로 분석, 잠재적 블랙리스트 지갑과 의심스러운 혐의거래의 위험 수치 및 등급 등을 알려줍니다.
또한 지원하는 메인넷 12종에 대한 월.일별 거래량 수, 또는 거래 기여정도를 세분하여 보여줌으로써 고객의 리스크 관리와 컴플라이언스를 준수를 돕습니다.

왜 SWAP인가요?

웁살라 시큐리티의 암호화폐 보안 솔루션과 차세대 거래 모니터링 툴은 의심되는 암호화폐 지갑의 위험수치와 등급을 선제적으로 분석함으로써 사용자들이 능동적으로 비즈니스 리스크를 관리하는데 도움을 줍니다.

또한 보고서에 정리된 내용들은 고객들이 추후 모델링과 보고 시스템 으로 사용할 수 있도록 직관적이고 이해하기 쉬운 표와 데이터로 추출되기 때문에 더 이상 수작업으로 보고서를 작성하느라 시간과 에너지를 낭비할 필요가 없습니다. SWAP은 고객들로 하여금 비즈니스 리스크를 줄이고, 규정을 준수하며, 생산성을 높이는 비즈니스 의사 결정을 할 수 있도록 최적의 맞춤 ‘암호화폐 거래 평가 레포트’를 제공합니다

SWAP은 어떻게 작성되나요?

웁살라 시큐리티는 자사의 암호화폐 보안 솔루션을 바탕으로, 고객사의 암호화폐 거래내용을 분석하여 하기와 같이 다양한 위험 지표 등을 작성합니다.

기본적으로는 매 분기 말에 '분기별 보고서'가 작성되어 발송됩니다.
그 밖에 고객이 온디맨드(On-Demand) 보고서를 요청하는 경우, 보고서 발송 시기나 기타 특이사항 등 은 별도로 협의가 가능합니다.

위험 지표

- 일별 혹은 월별로 분류된 암호화폐 거래 건수(Count)와 거래량 (Volume)
- 암호화폐 월별 거래 건수와 거래량의 시각화 그래프와 각 항목의 총 합
- 암호화폐 월별 거래 건수와 거래량이 높은 지갑들에 대한 위험 수치와 위험 등급 평가
- 블랙리스트 지갑과 직/간접적 접촉이 있었던 지갑리스트, 혐의거래로 의심되는 거래

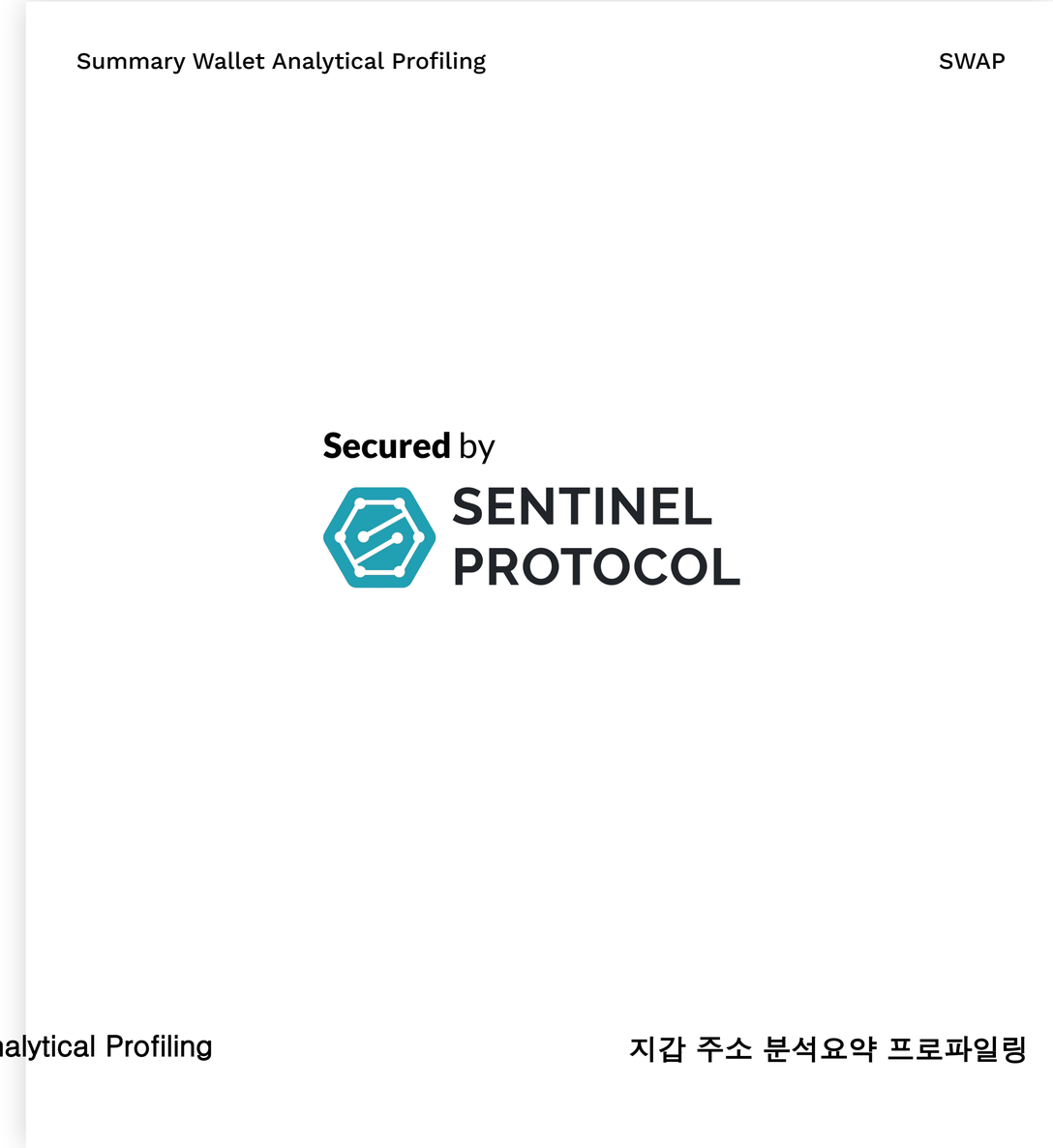
누가 사용하면 좋은가요?

암호화폐 기업의 안전성 검증 지표, 기업 IR 홍보로도 활용 가능

“자사의 토큰이 현재 자금세탁, 혹은 암호화폐 혐의거래 등에 연루되어 있는지, 혹은 가까운 미래에 그럴 가능성이 있는지?” 고민하는 암호화폐 기반의 모든 기업들은SWAP서비스를 이용할 수 있습니다.

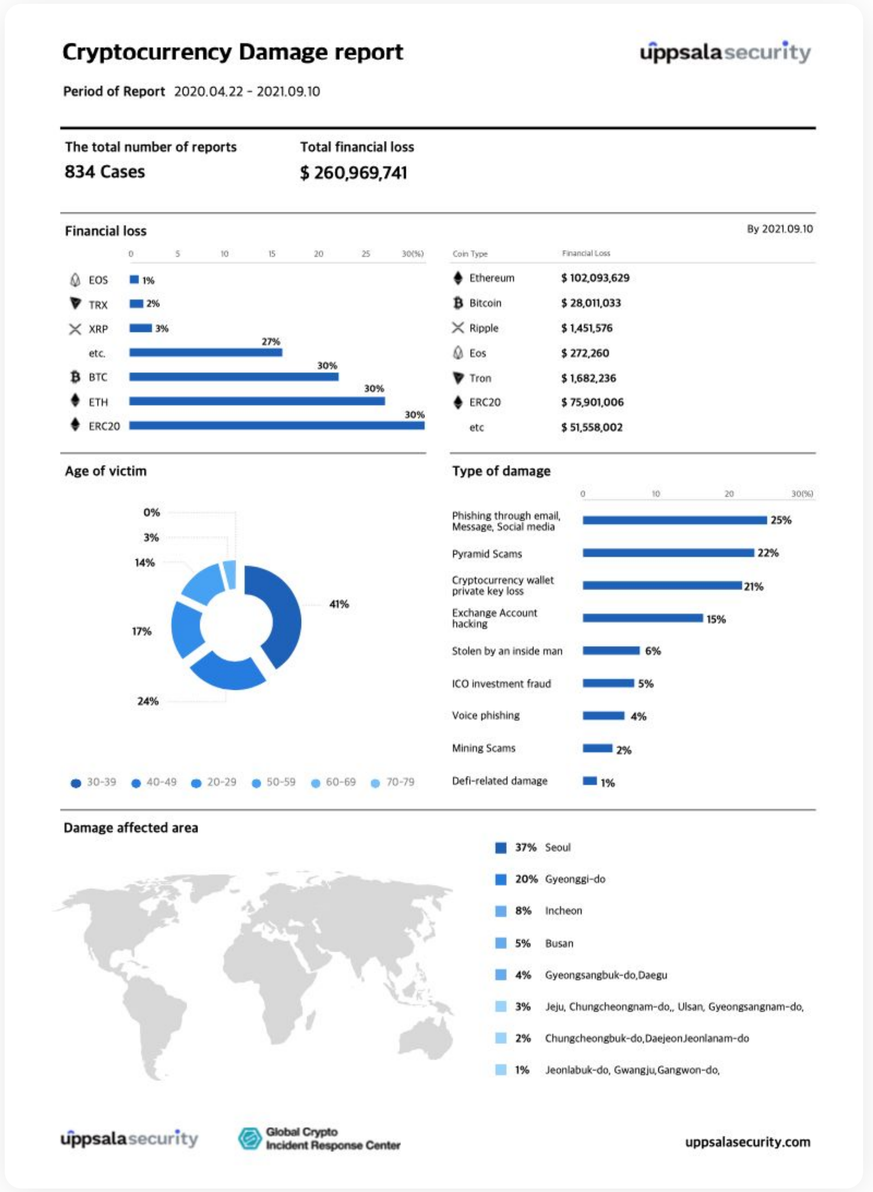
뿐만 아니라 해당 보고서를 통해 자사의 암호화폐 거래에 대한 무결성과 보안 규제 준수를 증명할 수 있으며, 거래 안전성을 검증받은 보고서를 바탕으로 대외홍보 및 기업IR에 활용할 수 있습니다.

웁살라 시큐리티의 기존 솔루션을 이용하고 있는 고객의 경우, SWAP 보고서 서비스를 추가로 신청할 수 있으며, SWAP 서비스만 별도 이용하고자 하는 기업 고객의 경우 info@uppsalasecurity.com 으로 연락 주시기 바랍니다.



악의적인 범죄활동에 희생되고, 디지털 자산에 막대한 손해를 입었던 기업과 개인들은, 이제 웁사라시큐티가 제공하는 전용 신고양식을 통해 해당사건을 직접 보고할 수 있습니다.
Uppsala Security의 전문 조사관은 당사의 핵심 솔루션 TRDB,CATV, CARA를 활용하여 도난당한 디지털 자산을 추적하고 분석합니다.

전문 조사관의 분석 및 조사 이후의 결과들은 상세한 추적 보고서로 제작되어 의뢰인(피해자)에게 제공됩니다. 사건 피해자 추가 법적 조치를 위해 당사자 거주 국가의 수사 관할권에 맞는 해당 법 집행 기관에 해당 사고를 신고하고, 본 추적 보고서를 함께 제출할 수 있습니다.



As updated in February 2022

Decentralized Solutions for Cyberspace Security.

Contact

info@uppsalasecurity.com

Website

www.uppsalasecurity.com

uppsalasecurity