AhnLab TIP

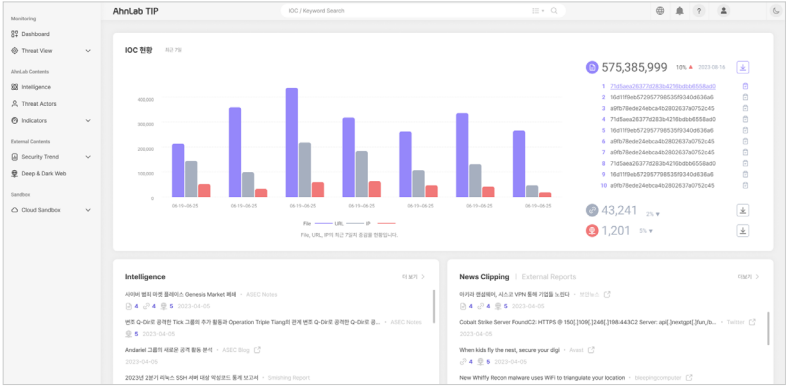
고도화된 사이버 위협에 대응하는 차세대 위협 인텔리전스 플랫폼

긴급하고 중요한 위협에 대응할 수 있도록 가시성과 조치 방법을 제공해
최적의 의사결정 지원

개요

AhnLab TIP(Threat Intelligence Platform)은 안랩의 악성코드 대응 전문 기술과 노하우를 바탕으로 위협 상관 관계 분석 및 정교한 위협 정보를 제공합니다. 발생한 혹은 발생할 위협의 배경과 목적을 포괄적으로 분석해 합리적인 의사결정을 내릴 수 있도록 안랩만의 차별화된 위협 인텔리전스를 제공해 드립니다.

"전문 기술과 노하우가 결합된 탁월한 시큐리티 인프라 기반"
THREAT INTELLIGENCE PLATFORM



포괄적인 위협 인텔리전스 프로세스

- 다양한 출처로부터 수집된 정보를 유형 별로 분류해 체계적으로 저장
- 인공지능과 동적 분석 시스템을 활용한 다차원 분석 진행
- 의사결정자, 상위 관리자, 실무자 별 상황에 맞는 위협 인텔리전스 제공

위협의 상관 관계 분석

- 다양한 위협 분석 정보와 영향도 파악을 통한 능동적인 대응 가능
- 위협 간 상관관계 분석을 통해 여러 위협에 대한 탐지와 대응의 격차 해소
- 키워드 등록을 통한 고객 맞춤형 위협 정보 확인 및 대응
- 제공되는 위협 인텔리전스를 보안 구축 프로세스에 반영

더 많은 위협 정보 제공

- '비공개 출처 정보' 모니터링 및 상관관계 분석
- 현재 뿐 아니라 발생할 위협을 예측해 보안 정책 수립
- 위협 대응 솔루션 및 방법을 제시해 방어 역량 강화
- 상시적인 공격 동향 모니터링

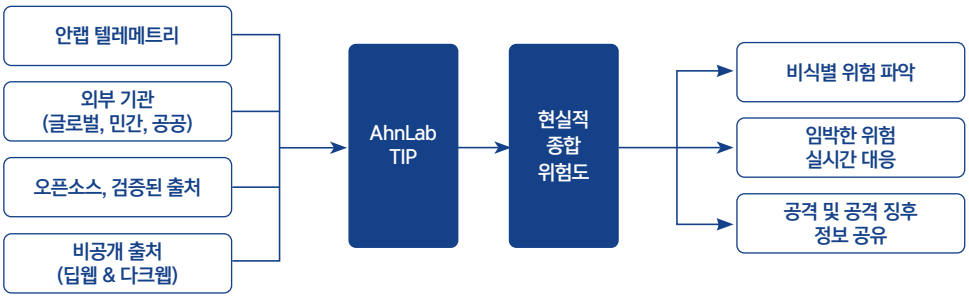
출시배경

기존의 위협 정보(Threat Information)는 평면적인 위협 데이터가 다양한 소스로부터 제공되어, 분석과 대응 효율성이 떨어지고 보안 담당자의 주관적 판단에 의존할 수밖에 없었습니다.

비공개 출처(딥웹 & 다크웹) 정보 확인이 어려움

도입효과

AhnLab TIP는 단일 채널에서 다양한 위협 인텔리전스를 제공함으로써, 고객사의 보안 담당자가 최신 위협 정보와 정교한 분석 결과를 바탕으로 위협에 대한 가시성을 확보하고 확산 여부와 조직 영향도를 파악해 빠르게 대응할 수 있도록 해드립니다.



“정량적 & 정성적 판단 기준을 제공해 자체 보안 대응력 강화”

영향도 및 확산 정도 확인

이상 행위 혹은 의심 위협 탐지 시 자체적인 분석 및 대응

유입 및 확산 방어

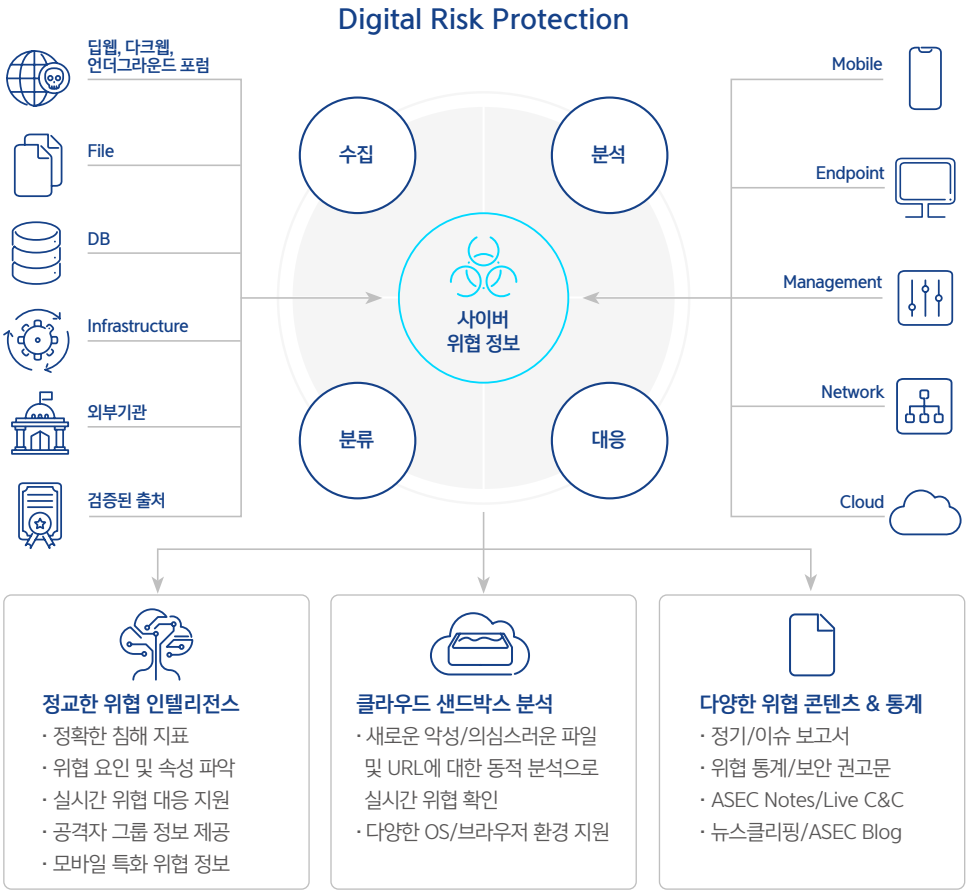
다양한 위협 시나리오 설계 및 테스트

탐지 및 대응 정책 강화

새로운 악성·의심 탐지 정책 및 패턴 실시간 적용

주요기능

AhnLab TIP를 통한 정보 식별의 목적은 허가 받지 않은 정보 수집, 취약점을 이용한 보안 통제 무력화 / 우회 및 정보 유출 등 공격 행위에 빠르게 대응하는 것입니다. 이를 위해 정교한 위협 인텔리전스, 클라우드 샌드박스를 활용한 동적 위협 정보 분석 및 다양한 위협 인텔리전스 콘텐츠를 제공합니다.



AhnLab TIP는 아래의 주요 기능들을 '중앙 집중형 단일 대시보드'로 제공합니다. 단일 대시보드에서 모든 IOC(Indicators of Compromise) 확인 및 검색이 가능하며, 심각도 및 신뢰 수준별로 IOC를 요약해 위협 대응 우선순위 설정에 기여합니다.

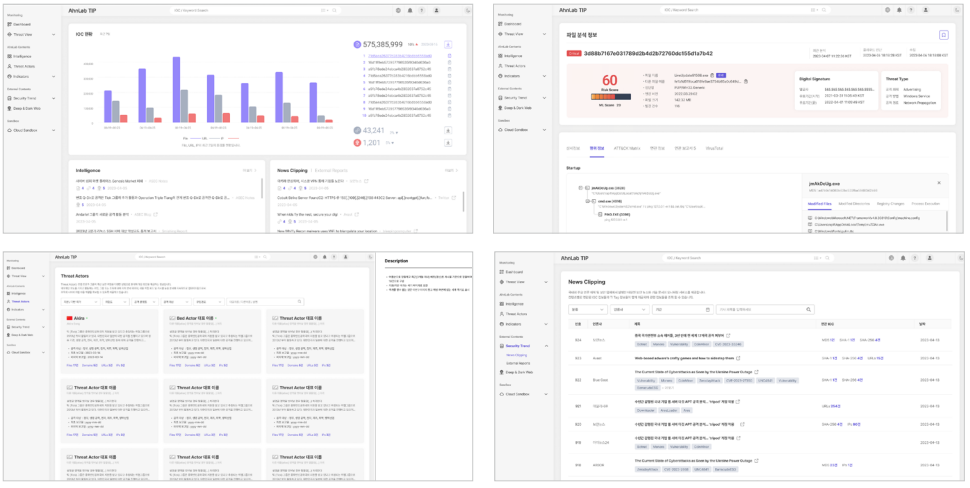
정교한 위협 인텔리전스	· Threat Lookup: URL, 도메인, IP, 해시, 위협 종류, 공격자 등의 정보 제공 · IOC 피드를 통한 위협 정보 분석 최적화 · 악성코드 경유 및 유포 경로 파악을 통해 대응 효율성 제고 · 위협 이벤트 및 공격 흐름도를 제공해 대응/조치 방안 제시 · 최적화된 별도 RESTful API 제공을 통한 제품 및 서비스 연동 · 딥/다크웹상에서 수집된 정보 기반 위협 연관 분석
클라우드 샌드박스 분석	· 경로별 위협 탐지 현황 및 수집 현황 제공 · 멀티 OS 환경/브라우저 환경 및 사용 프로그램 기반 분석 · 위협 현황 정보 시각화 및 행위별 위협 수준 정보 제공 / 폭 넓은 파일 유형 지원
다양한 위협 콘텐츠	· 최신 보안 위협을 분석하는 과정에서 수집 및 분석된 정보 공유 · 정기 & 이슈 보고서를 통해 주기적으로 위협 동향 정보 공유 · 다양한 위협 통계 정보를 제공해 현황 분석 최적화 · 악의적인 의도를 가지고 활동하는 개인, 그룹 또는 조직에 대해 자체 분석 데이터 확보 · 유포량이 많은 악성코드를 선별하여 자동 분석 시스템을 통해 확인된 C&C 정보 제공 · 취약점, 영향 받는 제품, 대응 방안을 담은 보안 권고문 공유 · 국내외 주요 보안 뉴스 등 위협 연관 정보 제공
비공개 출처에서 수집된 위협 정보	· Tor/IP2 네트워크 출처 정보, 유출된 이메일 및 파일 내용 정보 · 중요 크리덴셜 유출 정보 / 침해되어 유출된 데이터 셋 정보

활용방안

안랩의 위협 인텔리전스 플랫폼 활용 'TIP'

A. 실시간 보안 위협 대응 및 보안 전략 설계

침해지표는 물론 공격 유형, 공격자 정보, 신규 취약점 분석 정보, 비공개 출처 정보 등 다양한 위협 트렌드를 습득해 기업 내부 보안 전략 설계



B. 다양한 API 연동을 통한 포괄적인 위협 대응 역량 강화

다양한 보안 제품 및 서비스와 연동해 신종 악성코드 대응 & 실시간 차단

이 밖에, AhnLab TIP를 아래와 같이 활용하시면 도입 효과를 극대화할 수 있습니다.

기업 내부 보안 전략 설계	· 미래 위협 예측 정보를 통해 다가올 위협 현황을 보안 전략에 반영 · 전략적 대응 우선 순위를 설정해 사이버 보안 투자 진행
보안 대책 수립 임박한 위협 대응	· AhnLab TIP 플랫폼을 통해 신규 사이버 위협 분석 정보 획득 · 임박한 위협에 영향 받는 자산, 취약성 분석 및 대응책 마련 · 취합한 정보를 바탕으로 사전 예방 대책 실행 및 피해 최소화
포괄적인 위협 대응 역량 강화	· IP / Domain / URL 위험도 파악 후 IPS, IDS, 방화벽 등에 차단 리스트로 적용 · SOAR 및 XDR 시스템 연계를 통해 파일, IP, URL 등에 대한 실시간 위협 검증 · 국내외 주요 보안 뉴스를 분석해 사회적 보안 이슈에 신속하게 대응

경기도 성남시 분당구 판교역로 220 (우)13493
홈페이지: www.ahnlab.com
대표전화: 031-722-8000 팩스: 031-722-8901

AhnLab