More security,
More freedom

AhnLab TIP

차세대 위협 인텔리전스 플랫폼

표준제안서

AhnLab

목차

01.
제안 배경

1. 사이버 위협의 증가 및 변화
2. 이제 보안도 ‘Intelligence’ 로
3. Threat Intelligence의 필요성

사이버 위협의 증가 및 변화

국내·외 사이버 공격 사례로 살펴 본 사이버 공격 위협의 분류 및 특징은 다음과 같습니다.
단순 해킹부터 타깃화 된 APT(Advanced Persistent Threat)까지 **광범위한 형태로 빠르게 진행**되고 있습니다.

사이버 공격 위협 유형

- P2P/메신저 통한 정보유출
- C&C 접속
- 불법적인 계정/권한 탈취
- 알려지지 않은 악성코드 유입
- 단순 해킹 시도
- OS/웹/애플리케이션 취약점 공격
- 대상 지정 공격 (APT 공격)
- 네트워크 취약점 공격
- 하드웨어와 소프트웨어 조작
- 비인가 행위
- 원치 않는 메일
- 정보 조작
- 위조된 인증서의 생성 및 사용
- 원격 조작(실행)
- 불법적인 접근 시도
- 사회공학적 공격
- 무차별 대입
- 불법적인 소프트웨어 설치

위협의 변화

공격의 신속성
신형 변종 악성코드 배포 주기↑

지속성
지속적으로 전체 시스템 통제

치명적
데이터 암호화, 대규모 시스템 감염

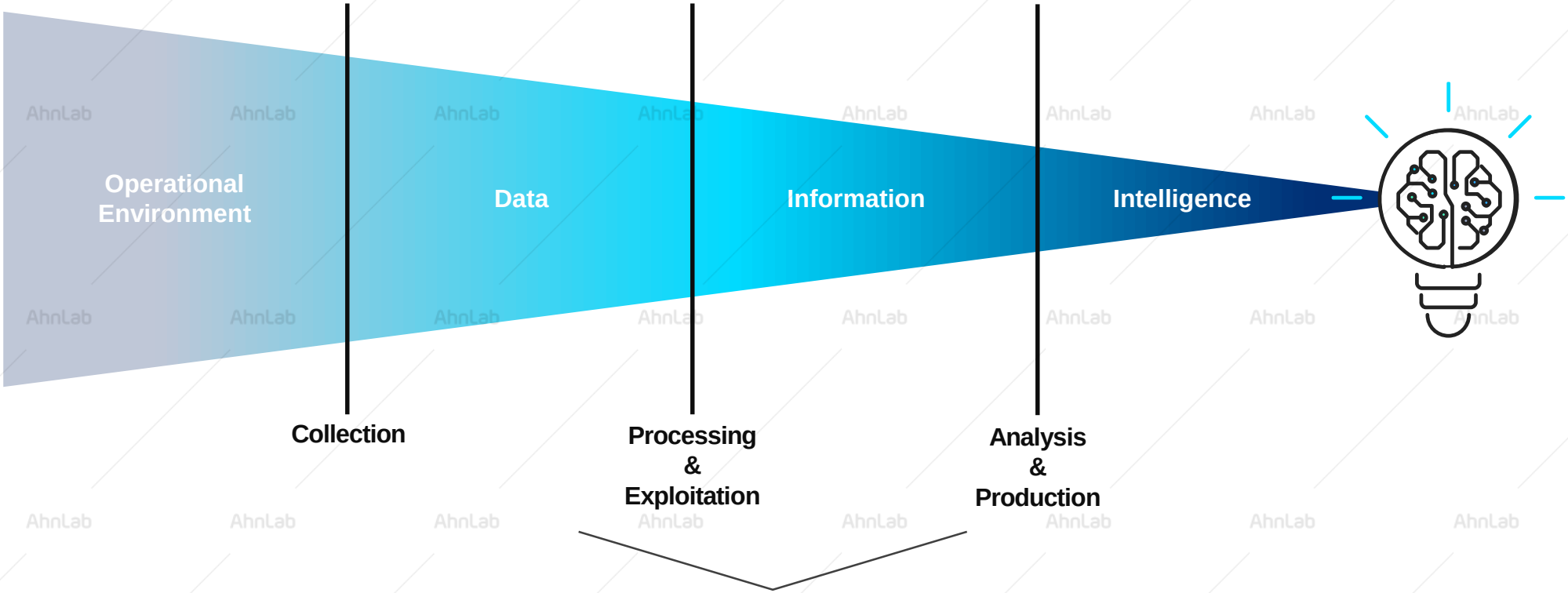
지능적
사람의 심리를 이용

내부 자산

이제 보안도 Intelligence 로…

사이버 공격이 한층 정교해지고 그 범위 또한 확대되고 있습니다. 1건의 이상 징후를 놓치는 것만으로도 사회기반시설 및 서비스 인프라가 다운되거나 기업의 주요 정보가 유출되는 등의 대형 보안 사고로 이어질 수 있어, 위협 인텔리전스 필요성이 증가하고 있습니다.

위협 인텔리전스 (Threat Intelligence)



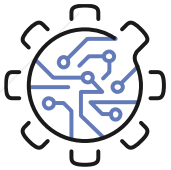
온라인 상에서 대량으로 생산되고 확산되는 위협 정보를 큐레이션(Curation) 및 분석하여, 위협에 신속하고 효과적으로 대응할 수 있는 서비스 필요성 증가

Threat Intelligence의 필요성

최근 사이버 공격은 방법이 복잡해지고 공격 경로가 동적화 되어, 전통적인 정적 분석 결과를 기반으로 만들어지는 침해 지표(IOC)만으로는 탐지 및 차단에 한계가 있습니다. 이에, 위협 인텔리전스 서비스 도입이 필요한 시점입니다.

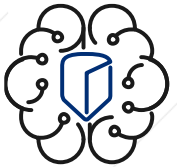
위협 인텔리전스 (Threat Intelligence)

Threat Information이 아닌 Threat Intelligence로
다변화하는 위협 정보에 대한 대응 필요



기술
Tactical
일반적인 정보

관리
Operational
정보의 조합, 공유



전략
Strategic
공격 전략, 사용된 기술,
공격 절차의 종합적인 분석

EASY ← 사이버 위협 정도 난이도 → DIFFICULT

악성 IP 주소	웹쉘 샘플	보안 취약점	해킹 도구		
악성 Domain 주소 +	악성코드 +	탐지 패턴 +	PoC 코드 +	침해사고 분석 사례 +	TTP

Tactic, Technique, Procedure

02.
AhnLab TIP

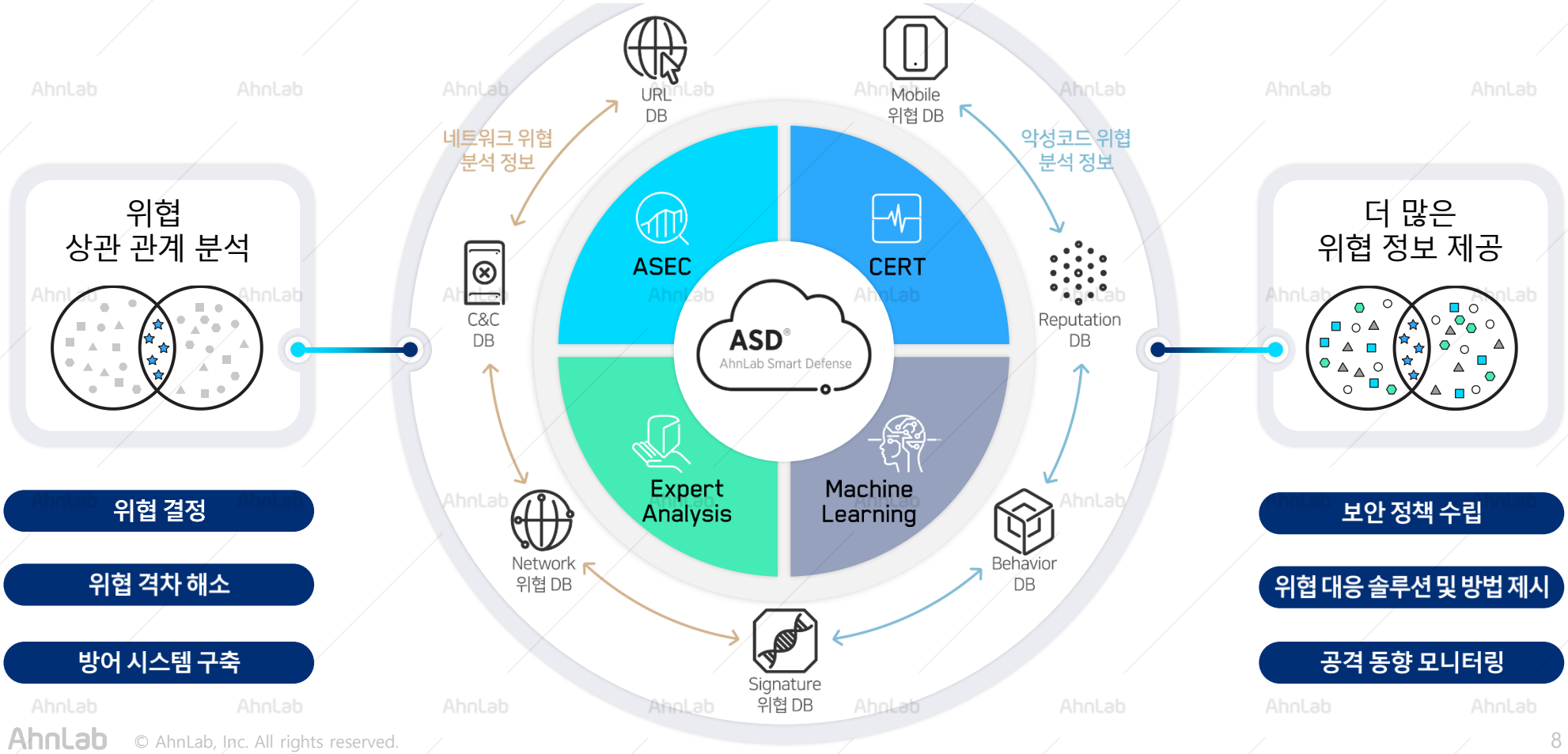
1. 개요
2. 도입 효과
3. 활용 방안
4. 주요 기능

개요(1/2)

AhnLab Threat Intelligence Platform(AhnLab TIP)는 안랩의 악성코드 대응 전문 기술과 노하우를 바탕으로 위협 상관관계 분석 및 풍부한 위협 정보를 제공합니다.

전문 기술 및 노하우가 결합된 탁월한 시큐리티 인프라 기반의

THREAT INTELLIGENCE PLATFORM



- 위협 결정
- 위협 격차 해소
- 방어 시스템 구축

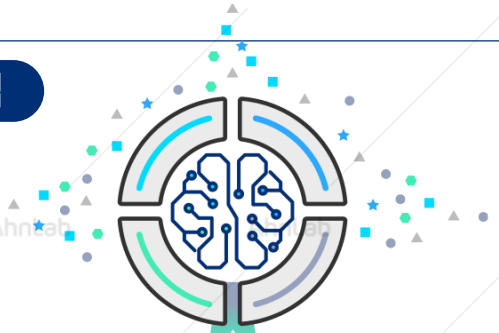
- 보안 정책 수립
- 위협 대응 솔루션 및 방법 제시
- 공격 동향 모니터링

개요(2/2)

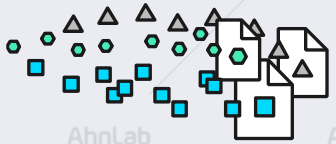
AhnLab TIP는 발생한(할) 위협이 왜, 어떤 목적으로 발생하고 진행되는지 포괄적으로 분석 및 해석하여 의사결정을 내릴 수 있도록 안랩만의 차별화된 위협 정보를 제공해 드립니다.

① 위협 정보 수집

AhnLab Threat Intelligence Platform



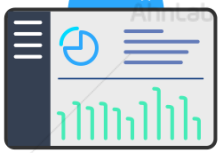
- AhnLab Telemetry (NW,EP, Mobile, etc.)
- Threat Research & Analysis Team
- ASEC / CERT
- Security Partners
- Web Crawlers
- Botnet Monitoring
- Cloud Sandbox
- Open Source
- SNS, etc. .....



수집 정보를 유형별로 분류하여 체계적으로 저장

② 위협 정보 분석

TI Infrastructure



- 수집 정보의 유입 정보 분석
- 수집 정보의 평판 검증
- 수집 정보의 정적 분석
- 수집 정보의 행위 정보/동적 분석
- 통계 및 연관성 분석

- 위협 데이터셋 생성
- 침해사고 데이터 및 분석 정보 분류
- 사이버 위협 관련 실시간 이슈 정보 분류

③ 위협 정보 제공

고객사

식별되지 않은 추가 위험을 예측하기 위해 의사결정자에게 제공되는 정보

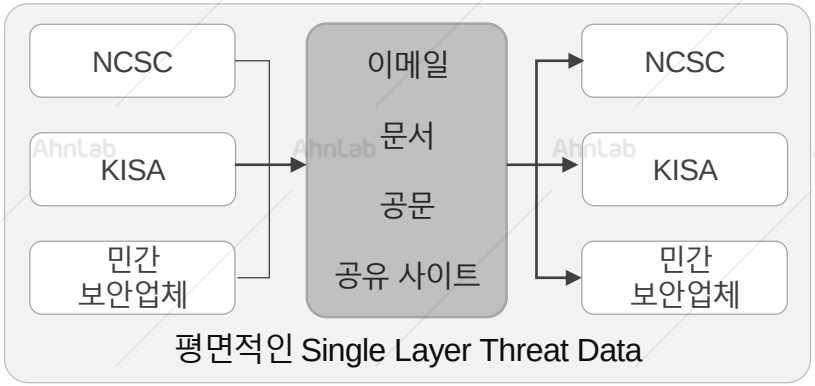
임박한 위험에 대응하기 위해 상위 관리자에게 제공되는 정보

공격 및 공격 징후에 대응하기 위해 보안 실무자들에 제공되는 침해 지표와 같은 정보

도입 효과

AhnLab TIP는 단일 채널에서 다양한 위협 정보를 제공함으로써 고객사의 보안 담당자가 보안 위협을 빠르게 파악하고 대응할 수 있게 해드립니다.

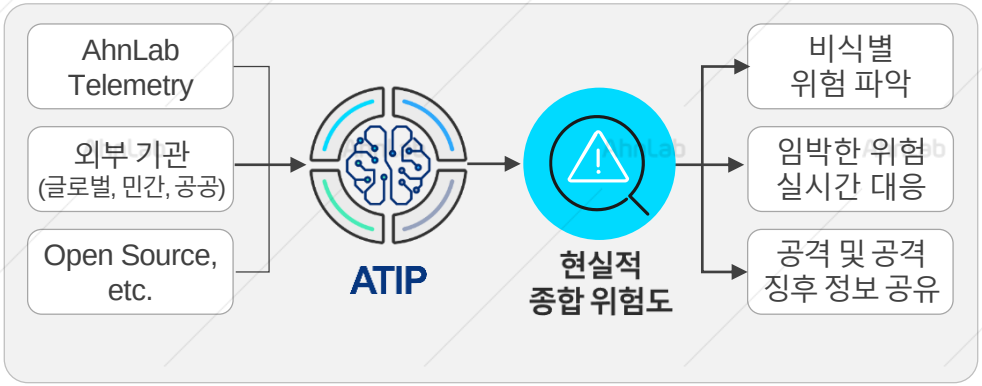
AS-IS



보안 담당자의 주관적 판단에 의존한 위협 대응

- 보안 정책 표현 불일치로 인한 재생성
- 다양한 정보 공유로 중복 소요 발생
- 사람에 의한 정보 수집의 한계
- 정보 공유가 사후 대응 체계로 편성됨
- 최신 위협 정보의 실시간성 결여
- 신규 위협 정보에 대한 대응 기간 과다 소요
- 신규 취약점 정보 공유 지연

TO-BE



자체 보안 대응력 강화 – 정략적, 정성적 판단 기준 제공

위협 분석 확산, 영향도 확인
> 이상 행위 탐지, 의심 위협 탐지 시 자체적인 위협 분석 및 대응

위협 차단 유입, 확산 방어
> 다양한 위협 시나리오 설계 및 테스트

탐지 및 대응 정책 강화
> 새로운 악성/의심 탐지 정책 및 패턴 실시간 적용

활용 방안 – 기업 내부 보안 전략 수립 (비식별 위험 파악)

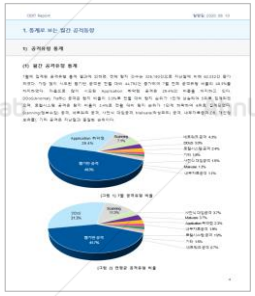
AhnLab TIP는 식별되지 않은 추가 위험을 예측하기 위해 의사 결정권자에게 제공하는 정보를 전달합니다.
기업에서는 내부 보안 전략 수립 시 이를 활용할 수 있습니다.

해당 정보를 기반으로 조직을 효과적으로 보호하고
전략적 우선 순위에 부합하는 사이버 보안 투자 진행 가능

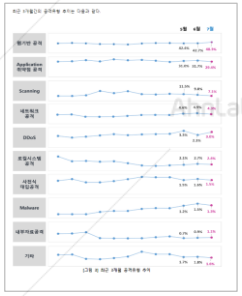
연도별 주요 보안 위협 전망 | 보안 위협 트렌드 확인 | 산업군별 위협 유형 | 주요 보안 이슈 확인

보안 위협 트랜드에 대한 정보 제공

공격 유형 통계(주/월/년)



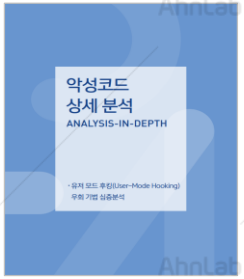
공격 유형 추이



산업군별 공격 유형

신규 취약점 정보

보안 이슈 / 악성코드 상세 분석 정보 제공



보안 위협 전망

활용 방안 – 보안 대책 수립 및 대응 (임박한 위협 대응)

AhnLab TIP는 임박한 위험에 대응하기 위해 상위 관리자에게 제공되는 정보를 전달함으로써 기업의 보안 담당자는 침해사고 사전 예방 및 피해 최소화를 위해 능동적으로 대처할 수 있습니다.

TI 포털을 통한 위협 인지
(Cognition)

TI 포털을 통한 정보 획득

- 보안 위협 통계
- 침해 사고 분석 정보
- 공격 시도 분석 정보
- 악성코드 (샘플) 정보
- 취약점 정보
- RSS Feeds / SNS 정보

신종 사이버 위협 정보에 대한
정례화된 수집·분석 자료 (리포트 등)

수집된 대량의 정보 중 위협 인텔리전스
(도메인, IP, 해시 정보, 파일 정보 등)

고위험 사이버 공격 징후 및 연관성 정보

기업 내 자산 영향도 분석
(Analysis)

- 영향 받는 자산 분석
  (정보시스템 및 데이터)
- TI 정보 기반 취약성 분석
  (관리적, 기술적, 물리적)
- TI 정보 기반 대응책 분석
  (해당 취약성 보호 대책)

단기 대책 수립 및 대응
(Plan & Action)

- 사전/사후 보호 대책 수립
  (정보시스템 및 데이터)
- 보호 대책 실행
  (악성코드, 취약점 대응)
- 사전 예방 대책 실행

**임박한 위협 정보 확인을 통해
침해사고 사전 예방 및 피해 확산 최소화**

활용 방안 – 위협 대응 (1/2)

공격 및 공격 징후에 대응하기 위해 보안 실무자들에게 제공되는 침해 지표 등의 정보를 전달합니다.
기업 보안 담당자는 이러한 정보를 내부 시스템의 차단 리스트로 활용할 수 있습니다.

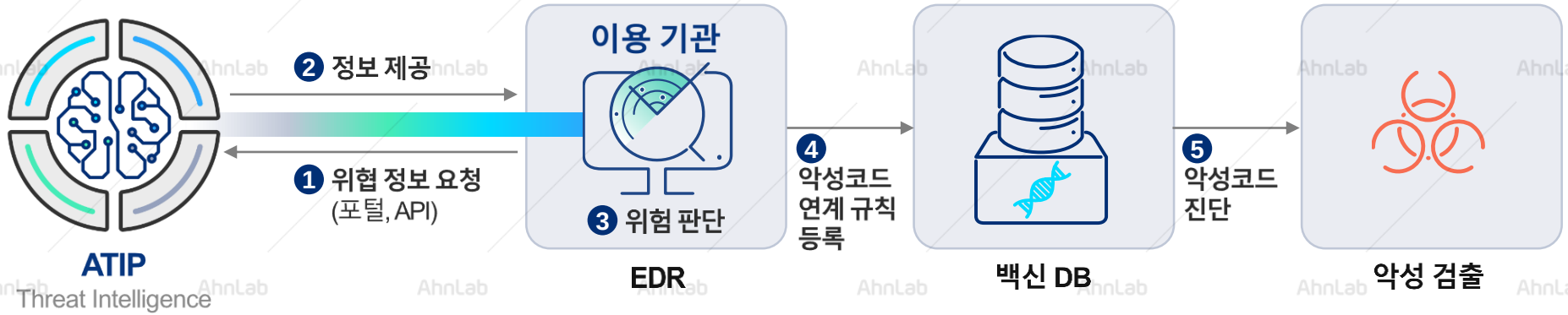
활용 방안 : 위협 IP 차단 리스트(Blocklist) 적용 – 위험도 파악 후 사내 IPS, IDS, F/W 등에 차단 리스트로 적용

- 위협 정보가 수집될 경우 해당 정보와 보안 관제 대상과의 연관성 확인
- 해당 위협 정보가 관제 대상에 피해를 입힐 우려가 있다고 판단되는 경우 IPS 등에 공격을 식별할 수 있는 탐지 정책 적용 후 모니터링 수행
- 실제 위협이 발생했거나 가능성이 높은 경우 방화벽이나 APT 솔루션에 차단 정책을 설정하여 위협 발생 최소화

활용 방안 – 위협 대응 (2/2)

공격 및 공격 징후에 대한 정보를 제공합니다. AhnLab EDR을 사용 중인 기업이라면 연계 규칙 등록을 통해 신종 악성코드 대응 및 차단을 더 효과적으로 수행할 수 있습니다.

활용 방안 : 신종 악성코드 대응 및 차단 – 사내 EDR 시스템에 악성코드 연계 규칙 (이름, 경로, 해시(Hash)값 등) 등록



- 위협 정보가 수집될 경우 해당 정보와 내부 자산과의 연관성 확인
- 해당 위협 정보가 내부 자산에 피해를 입힐 우려가 있다고 판단되는 경우
  EDR 등의 사용자 정의 규칙 설정을 통해 위협 종류, 행위, 공격 흐름에 대한 가시성 확보 및 적절한 대응
- 설정된 위협 정보 탐지 및 모니터링 수행

주요 기능

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.

AhnLab Threat Intelligence Platform

01 정교한 위협 인텔리전스

- IOC(Indicator Of Compromise) Feeds
- Threat Lookup

02 Cloud Sandbox

- 의심스러운 파일 또는 URL에 대해 다양한 플랫폼 환경에서 실시간 분석

03 Contents

- 정기 보고서 / 이슈 보고서
- 위협 통계
- 보안 권고문
- 뉴스 클리핑
- ASEC Blog

주요 기능 – 주요 증거 수집 및 제공 항목

AhnLab TIP는 발생한(할) 위협이 왜, 어떤 목적으로 발생하고 진행되는지 포괄적으로 분석 및 해석하여 의사결정을 내릴 수 있도록 안랩만의 차별화된 위협 정보를 제공해 드립니다.

주요 증거 수집 및 제공 항목

악성코드 분석 노하우와 자체 시큐리티 인프라를 통한 최신의 위협 정보 수집

- APT Feeds
- C&C Feeds
- IP Reputation
- URL/Domain Reputation
- Phishing Feeds

- File Reputation
- Malware Feeds

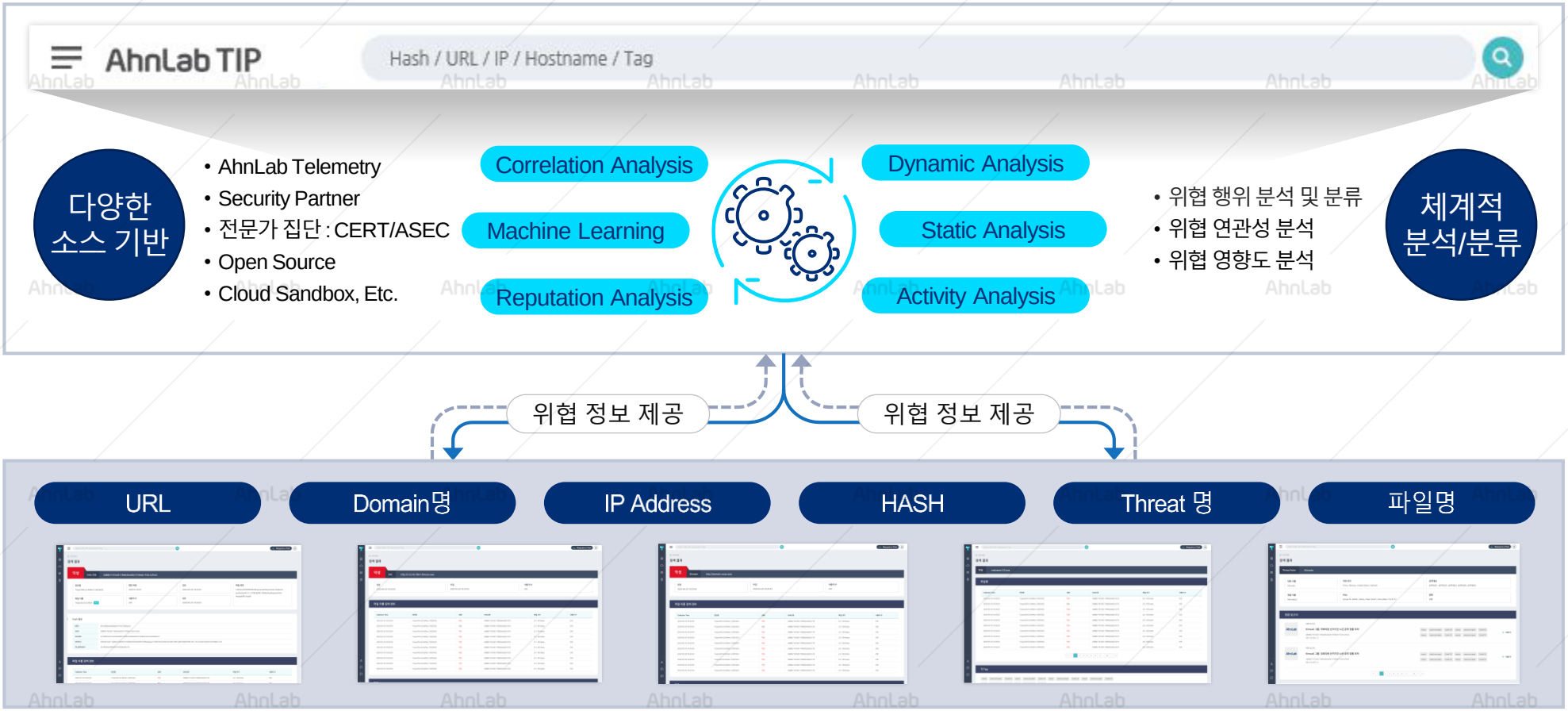
- 정기 보고서 / 이슈 보고서
- 위협 통계, 보안 권고문
- 국내 / 해외 주요 보안 뉴스

주요 기능 – Threat Lookup

수집된 위협 데이터에서 생성된 침해 지표(IOC)를 기반으로 중요하고 긴급한 위협에 대응할 수 있는 가시성과 조치 방법 등
의사 결정을 지원하는 관점에서 정보를 제공합니다. 이를 통해 조직은 보안 위협과 탐지를 통한 대응 사이의 차이를 좁힐 수 있습니다.

검색 - Threat Lookup

위협 정보 분석 최적화



주요 기능 – IOC Feeds (1/2)

안랩에서 제공하는 침해지표(IOC)는 악성코드의 정적, 동적 분석 정보를 활용하여 초기 분석 시 알려진 악성코드의 실행 흔적을 탐지하거나 조직 내부 망의 추가적인 감염 시스템을 찾는데 최적화되어 있습니다.

IOC(Indicators of Compromise) Feeds

위협 정보 분석 최적화

호스트

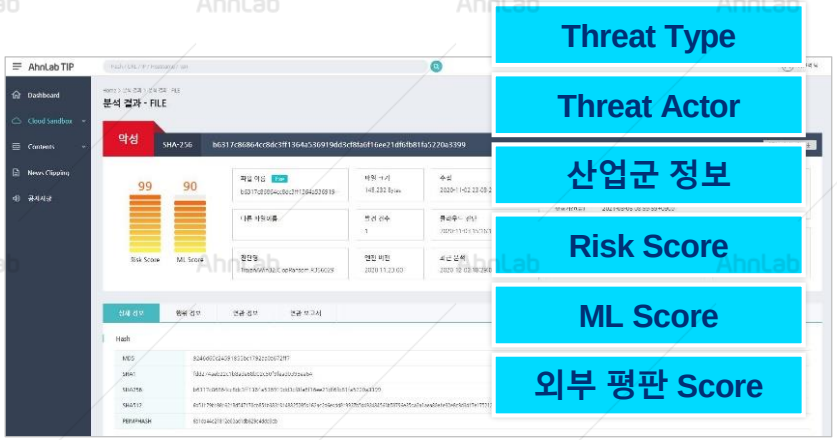
- 악성코드 파일 관련 정보(이름, 해시값, 사이즈 등)
- 악성코드 파일 관련 연관 행위 정보
- 악성코드의 파일 위치 및 서비스 등록 여부
- 악성코드 등과 관련된 레지스트리, 이벤트 로그 등

네트워크

- 악성코드를 다운로드 받거나 통신하는 URL
- 악성코드를 제어하거나 정보를 탈취하는 IP 주소(C&C)
- 악성코드가 외부 통신에 사용하는 암호화 방식 및 디지털 인증서 등

취약점

- 소프트웨어 및 시스템, 네트워크의 취약점



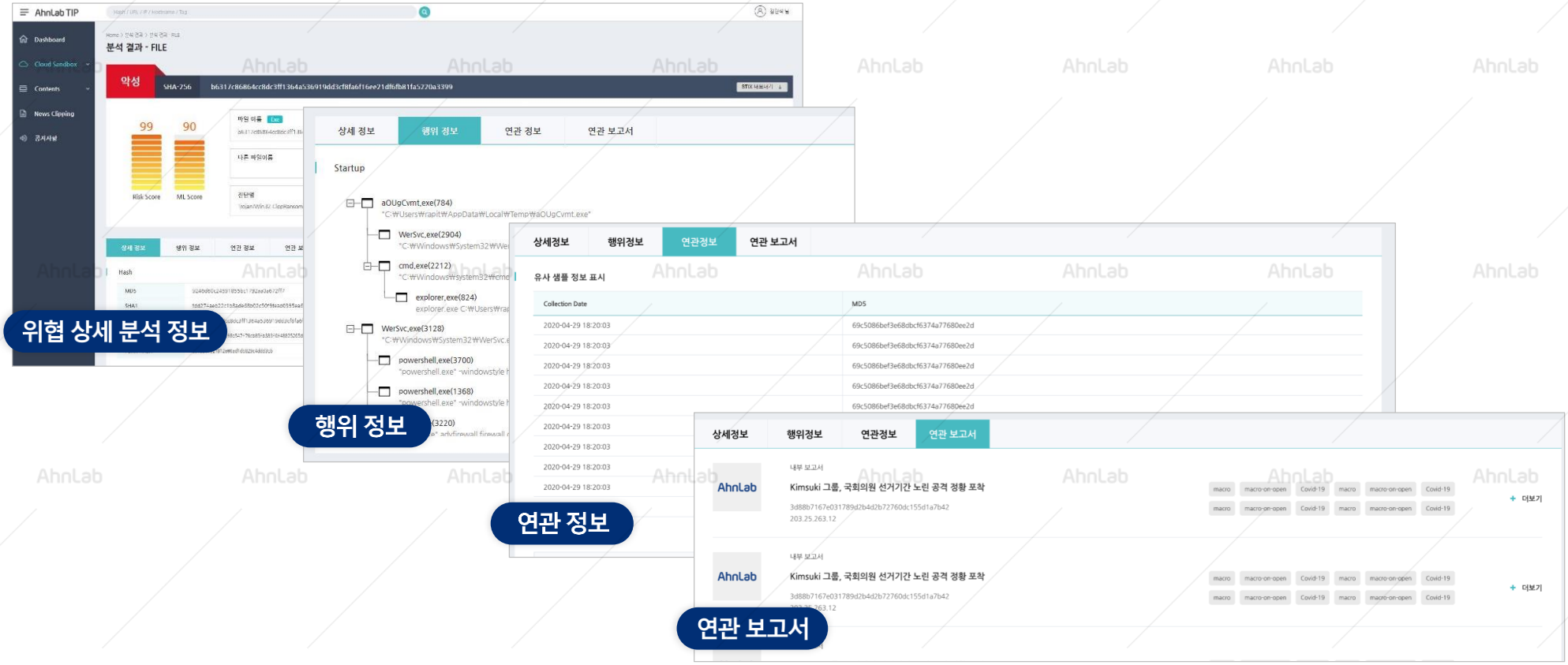
기대 효과

- 위협 정보 자료를 통해 관련성, 적시성, 정확도, 비교 가능성, 일관성, 명확성, 신뢰성 확보
- 분석을 통해 악성코드 유입 경로, 대응 정책, 안랩 제품 또는 고객사 운용 타 솔루션 기반의 조치 방안 마련

주요 기능 – IOC Feeds (2/2)

더욱 정교해진 위협에 대응하기 위해 세부 위협 정보 뿐만 아니라 행위 정보, 연관 정보, 연관 보고서를 통해 신뢰성 있는 탐지 및 대응이 가능해 집니다.

IOC(Indicators of Compromise) **Feeds** 위협 정보 분석 최적화

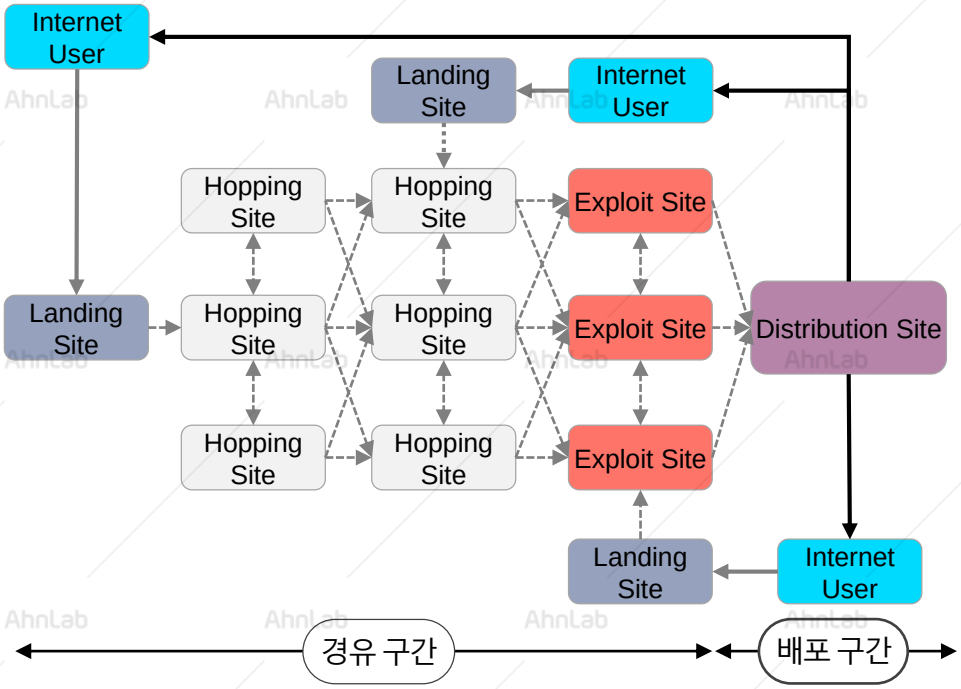


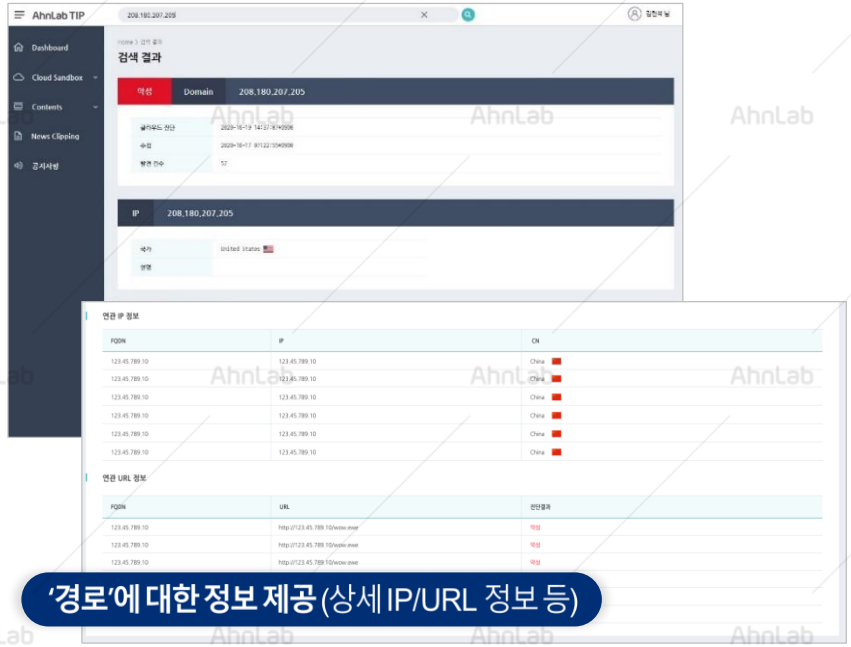
주요 기능 – 악성코드 경유 및 유포 경로 파악

악성코드 탐지 결과를 바탕으로 경유지 웹사이트 별로 위험도를 측정합니다.
이를 활용해 웹사이트의 악성코드 대응 관리·분석의 효율성을 증대시키는데 목적이 있습니다.

악성코드 경유 및 유포 경로 파악

위협 정보 분석 최적화





'경로'에 대한 정보 제공 (상세 IP/URL 정보 등)

기대 효과

- 위협 정보 자료를 통해 관련성, 적시성, 정확도, 비교 가능성, 일관성, 명확성, 신뢰성 확보
- 분석을 통해 악성코드 경로 및 유포 경로, 대응 정책, 안랩 제품 또는 고객사 운용 타 솔루션 기반의 조치 방안 마련

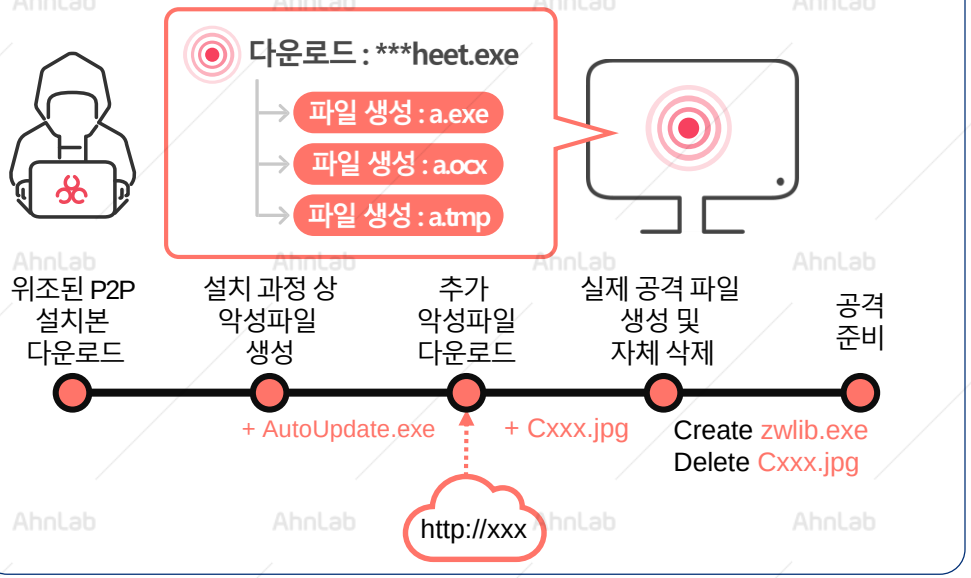
주요 기능 – 위협 이벤트 및 공격 흐름도 제공

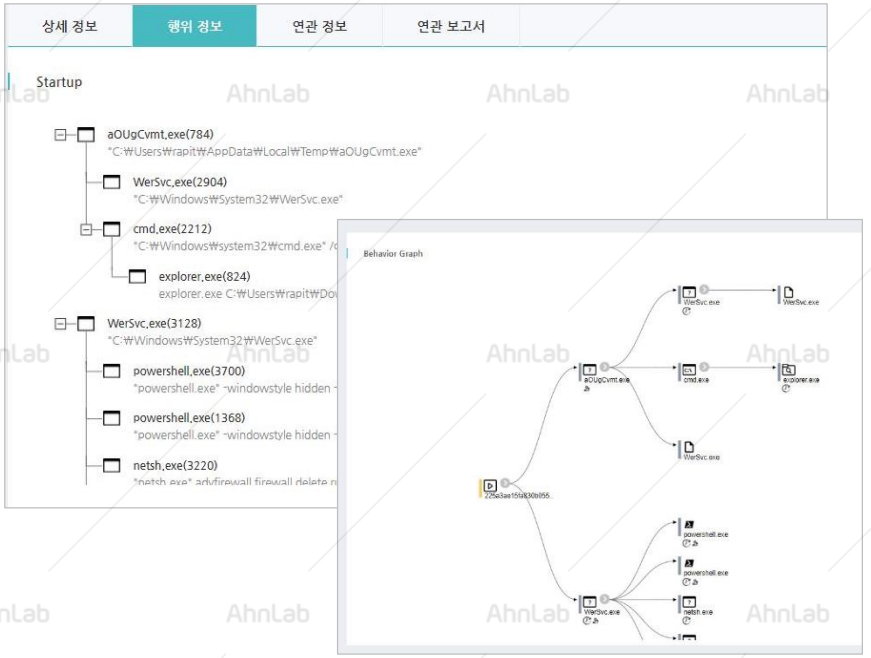
AhnLab TIP는 공격 흐름도와 함께 상세한 정보를 제공하며 위협 종류, 행위 및 공격 단계에 따라 적절한 대응 및 조치 방안을 제시합니다.

위협 이벤트 및 공격 흐름도 제공

위협 정보 분석 최적화

위협 행위 연관 정보 제공





기대 효과

- 피해 최소화를 위한 골든타임 확보
- 위협의 종류, 유입 경로, 주요 행위, 연관 관계, 위험도, MITRE ATT&CK 정보, 인증서 정보, 위협 정보 링크 등에 대한 상세한 확인 및 대응 가능

주요 기능 – 더 정교한 분석을 위한 Cloud Sandbox

최신 악성코드들은 정교한 은닉 기술이 도입되거나 새로운 변종 악성코드가 출현하는 경우 등가 많습니다.
Cloud Sandbox는 악성코드를 실제로 실행시켜 분석하는 방법으로, 메모리 덤프 분석과 실제 행위 관찰을 통해 변종에도 빠르게 대응 가능합니다.

Cloud Sandbox

동적 위협 정보 분석 최적화

위협 탐지 현황

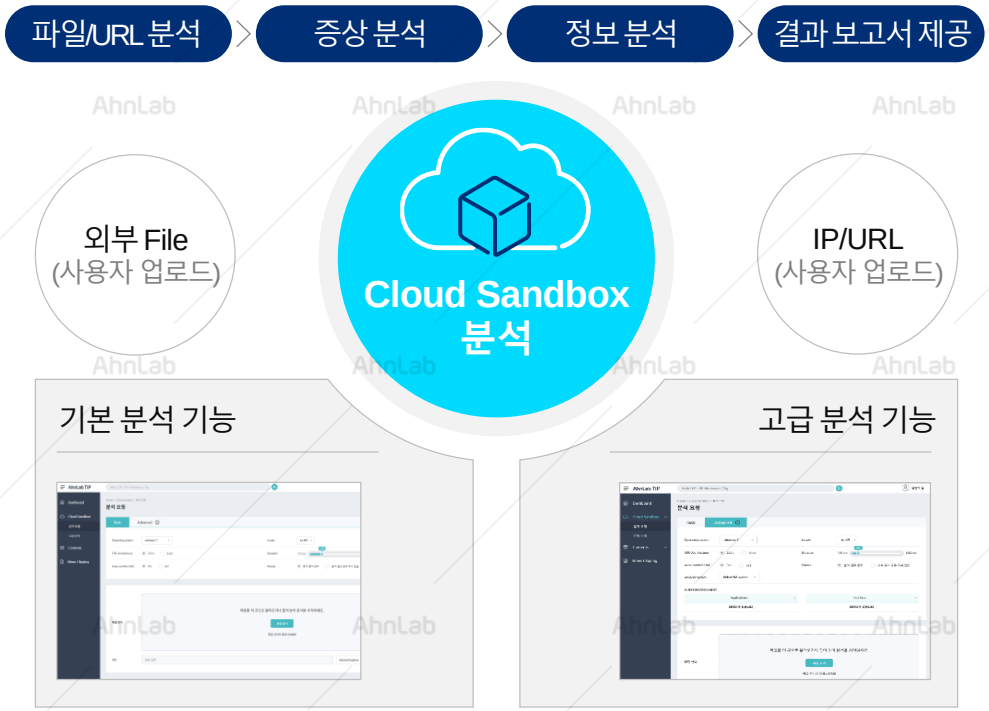
- 경로별 위협 탐지 현황
- 위협 수집 현황 및 상태

분석 환경

- 멀티 OS 환경 / 브라우저 환경 기반 분석 현황
- 상용 사용 프로그램 기반 분석 현황
  - 파일 포맷별 자동 실행 프로그램 기반 분석

분석 결과

- Known/Unknown 위협 현황 정보
- 악성 활동의 자동연결 시각화, 공격의 범위, 타임라인 등
- 행위별 위협 수준 정보



기대 효과

- 내부에 알려지지 않는 파일에 대한 보안 위협 · 취약점을 사전에 분석함으로써 보안 사고 예방에 기여

주요 기능 – 정기 보고서 / 이슈 보고서

위협 정보를 신속히 전달하여, 동일한 또는 유사 사고 확산을 방지하고자 주기적으로 위협 정보 보고서를 제공해 드립니다.

정기 보고서 / 이슈 보고서

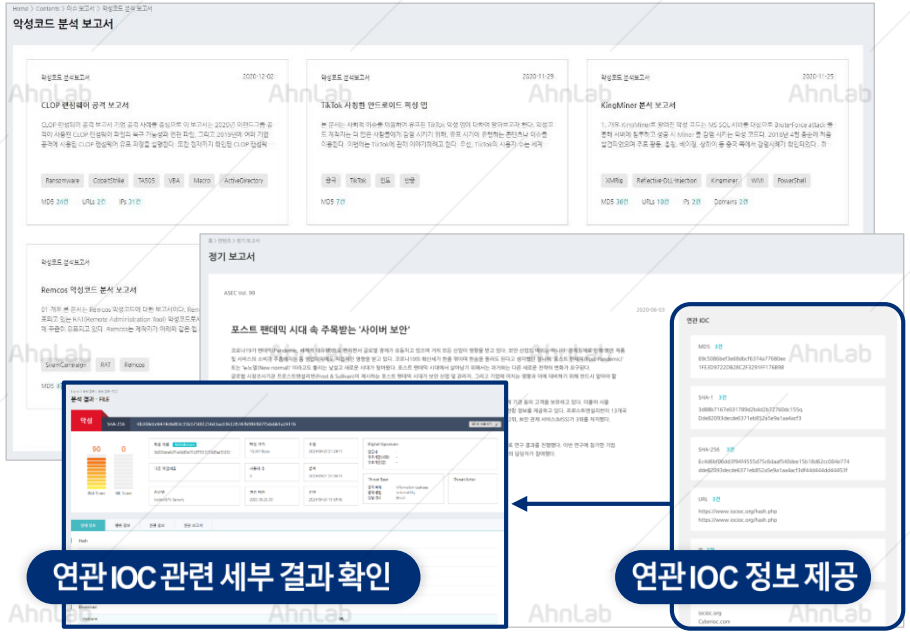
주기적 위협 정보 공유

정기 보고서

- IT 보안 관련 국내외 주요 사건, 이슈, 동향 뿐만 아니라 보안전문가들의 전문적인 의견, 조언을 바탕으로 사이버 공격에 대처할 수 있는 대응책 제공

이슈 보고서

- 유관 기관 및 기업에서 보안을 수행하기 위해 발생된 특정 이슈에 대한 보안 전문가들의 전문적인 의견, 조언으로 대상 사이버 공격에 대처할 수 있는 대응책 제공



기대 효과

- 최근 사이버 위협 트렌드를 설명한 보고서를 통해 사이버 위협 동향 및 예방 정보 확인 가능

주요 기능 – 위협 통계

악성코드 추이 관련 효과적이면서 신속한 대응에 대한 관심이 증가하고 있습니다.
향후 리스크를 유발할 수 있는 요소를 사전에 예방하기 위해 최적화된 통계 정보를 제공하고 있습니다.

위협 통계

위협 현황 분석 최적화

악성코드 통계

- 악성코드 수집 통계
- 악성코드 주요 유형별 수집 통계 / 수집 Top 10 정보 등

산업군 별 악성코드 영향도 통계

- 산업군별 악성코드 진단(피해) 통계
- 산업군별 네트워크 공격 유형 통계 등

Threat Type 별 통계

- Threat Type별 악성코드 진행 통계
  - 공격 피해 / 공격 기법 / 공격 (감염) 경로

기대 효과

- 악성코드에 대한 추이 → 지속 → 중복 → 동향 정보 실시간 파악

주요 기능 – 보안 권고문

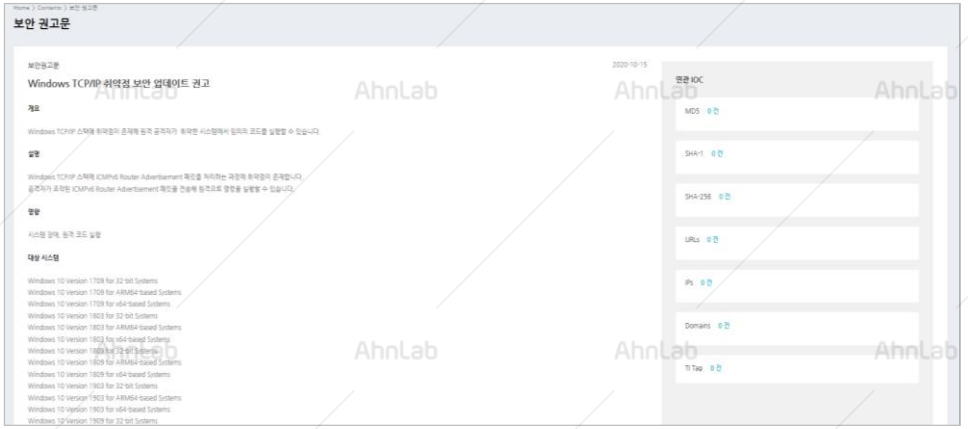
상용 소프트웨어에서 발생된 취약점 관련, 신속한 대응에 대한 관심이 증가하고 있습니다.
향후 리스크를 유발할 수 있는 요소를 사전에 예방하기 위해 보안 권고문 및 연관 위협 정보를 제공해 드립니다.

보안 권고문 – 글로벌 취약점 정보, 대응 정보, 보안 권고 내용 등 예·경보 정보 제공 — 주기적 위협 정보 공유

보안 권고문

- 상용 소프트웨어에서 발견된 취약점들과 관련된 내용
  - 취약점 / 취약점 공식 관리 번호 등
- 영향 받는 제품 정보 (제품명 / 버전 정보)
- 대응 방안 (패치 업데이트 등)

다양한 신규 취약점 공격에 대한 보안 권고문 제공



기대 효과

- 동종 업종이나 관련 분야 상호간 사이버상에서 발생하는 위협과 취약점 등의 문제에 관한 정보를 분석하고
- 문제를 유발하는 행위가 발생된 경우 이를 관계 기관에 신속하게 확인하여 주요기반시설에 대한 공격을 효과적으로 예방/탐지/대응

주요 기능 – 뉴스 클리핑

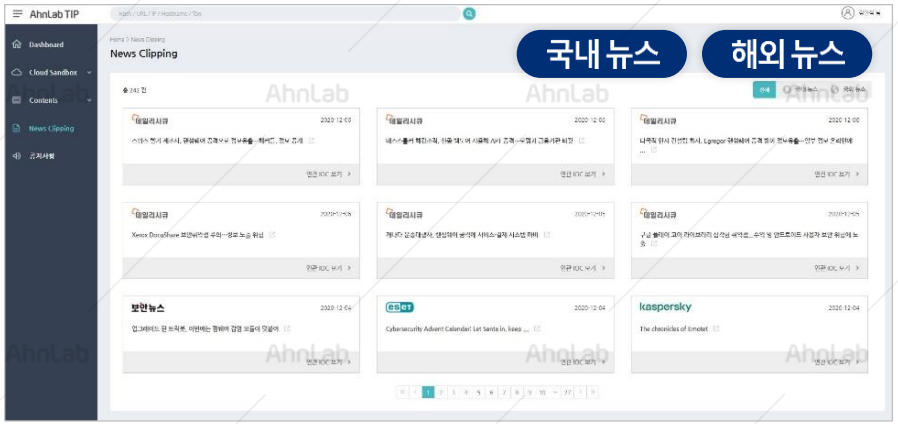
사회적 보안 이슈 발생 상황을 빠르게 확인 후 내부 자산에 대한 방어 조치를 위한 세부 정보를 신속하게 제공합니다.

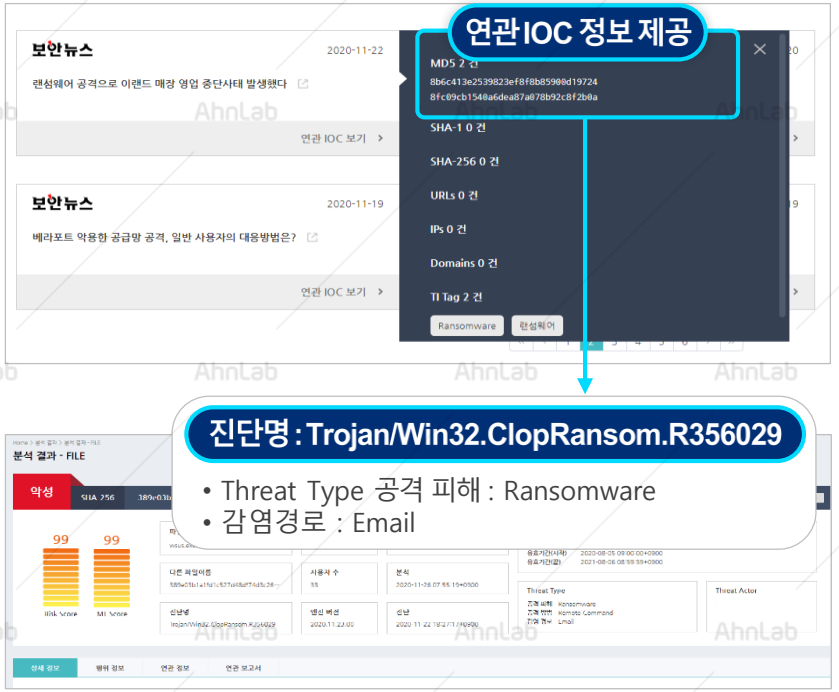
뉴스 클리핑

사회적 보안 이슈 공유

국내외 뉴스 연관 정보 제공

- 국내·외 뉴스 및 미디어와 관련된 연관 정보 제공
  ※APT, 해킹, 바이러스, 취약점 등 검색어 기반 관련 정보 분류
  ※주요 보안 기사와 링크 + 연관 IOC 보기 기능 제공
- 국내·외 해커 그룹이 운영하는 블로그 및 소셜 사이트 링크





기대 효과

- 언론 기사 등 사회적 이슈 발생 시 '뉴스 기사' + '세부 정보', '연관 IOC 정보' 및 '연관 정보' 등을 통한 실시간 사전·사후 위협 대응 가능

주요 기능 – 보안관제/운영 연동을 위한 API

AhnLab TIP는 별도 API를 제공하여 다양한 보안 관리 제품과 손쉽게 연동 가능하며, 위협에 대한 실시간 확인이 가능합니다.

Threat Intelligence APIs – RESTful API

보안 관제 / 운영 연동 최적화

서비스 제공 대상

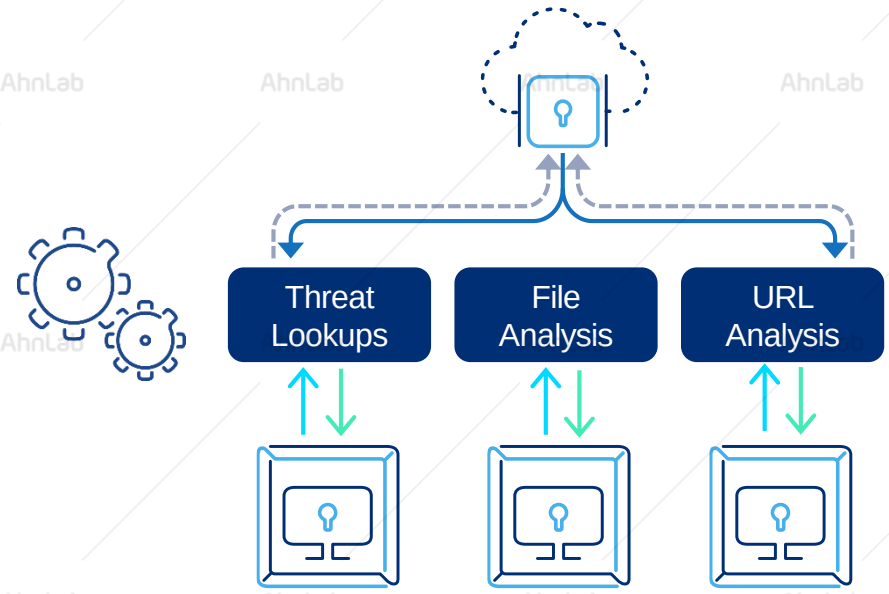
- ATIP Advance 등급 이상 이용 고객
  * 세부 가격 등급은 TIP 홈페이지 참고

주요 내용

- Threat Lookups

서비스 프로세스

서비스 신청 → RESTful API, 연동 KEY 제공 → API 연동 → 요청 및 결과 실시간 확인



기대 효과

- 보안 관리 제품과의 연동을 통하여 빠른 위협에 대한 대응 가능

More security,
More freedom

㈜안랩
경기도 성남시 분당구 판교역로 220 (우) 13493
대표전화 : 031-722-8000 | 구매문의 : 1588-3096 | 전용 상담전화 : 1577-9431 | 팩스 : 031-722-8901 | www.ahnlab.com

AhnLab TIP

AhnLab

www.ahnlab.com
www.facebook.com/AhnLabEP
www.youtube.com/user/OfficialAhnLab