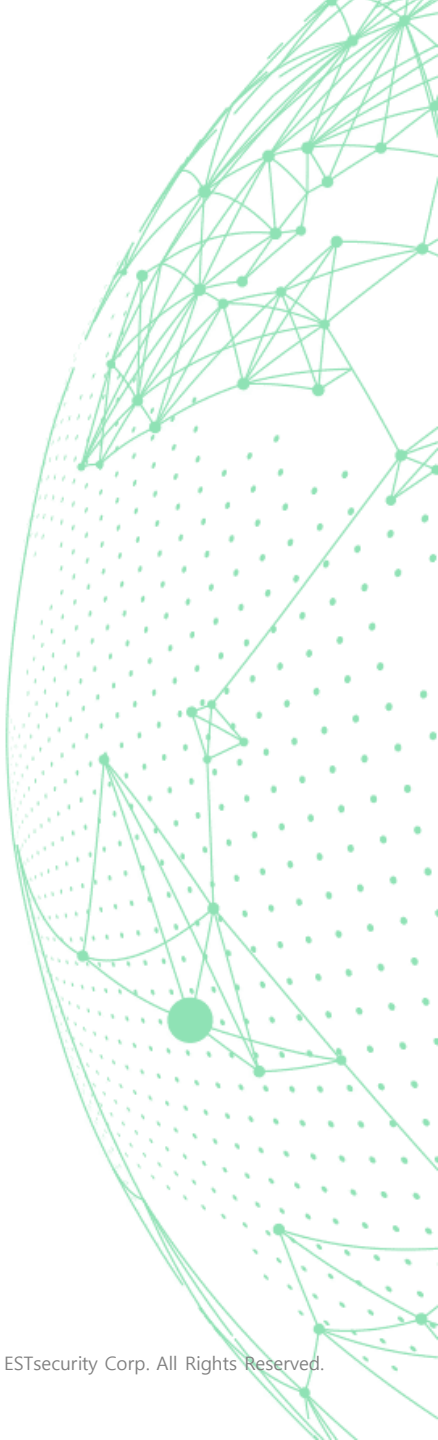
ESTsecurity | Company Introduction 2018

ESTsecurity providing the best intelligent security solution utilizing A.I



Index

01 이스트시큐리티 OVERVIEW

- CEO GREETING MESSAGE
- 회사 개요
- 이스트시큐리티 연혁
- 이스트시큐리티 조직도

CEO | SANGWON CHUNG

이스트시큐리티는 세계적인 지능형 통합보안업체가 되는 것을 목표로, 이스트소프트에서 2017년 1월 자회사로 독립했습니다.

이스트시큐리티는 국내 최다 사용자를 확보하고 있는 '알약'을 통해 지난 10여 년간 대한민국의 PC 엔드포인트 보안 영역에서 첨병 역할을 해왔고, 모바일에서도 '알약 안드로이드'를 통해 500만 사용자의 스마트폰을 보호해 오고 있습니다.

이제 PC뿐만 아니라 우리를 둘러싼 모든 기기가 서로 연결되어 더욱 편리한 삶을 만들어 주지만, 상대적으로 모든 것이 연결될수록 개인, 기업 및 공공기관의 정보들은 위험에 더 노출되고 있으며 취약점을 악용하려는 수법 또한 고도화되고 있습니다. 뿐만 아니라 전 세계적으로 하루 100만개 이상의 악성코드가 새로 생성되며, 양적인 측면에서도 우리 사회 곳곳을 위협하고 있습니다.

이렇게 질적, 양적으로 진화되는 악성 행위에 대항하기 위해서는 새로운 기술 패러다임의 적용이 필요하며, 이에 이스트시큐리티 AI 기술에 기반한 지능형 통합보안 기술과 서비스를 개발하여 고도화된 악성 위협들을 방어하려고 합니다. 이스트시큐리티는 단지 국내 시장만을 염두에 두고 있지 않습니다. 아시아, 유럽, 미국을 아우르는 글로벌 시장에서도 유수의 보안 업체들과 겨룰 수 있는 세계적인 지능형 통합보안업체로 성장할 것입니다.

이스트시큐리티의 기술과 서비스로 더욱 안전한 세상이 되도록 저희 임직원은 최선을 다하겠습니다.

감사합니다.

이스트소프트 대표이사

정 상 원

서울대학교 수학과 졸업
前 ㈜이스트소프트 알툴즈 사업본부장
前 ㈜줌인터넷 부사장
現 ㈜이스트소프트 대표이사
現 ㈜이스트시큐리티 대표이사 겸직

01

OVERVIEW

회사개요 | Making world more secure.

국내 1위 엔드포인트 보안 기업 이스트시큐리티는 가장 강력하고 안전한 엔드포인트 보안 솔루션을 제공하며, 국내 보안 업계에서 성능과 품질을 인정받아 1,400만 명의 개인 사용자뿐만 아니라 다수의 정부, 교육기관, 기업고객을 확보하고 있습니다. 새로운 도약을 위해 이스트소프트로부터 분사한 이스트시큐리티는 더욱 강력한 '지능형 보안 솔루션 '을 제공하는 기업으로 성장하겠습니다.

회사명	(주)이스트시큐리티 (ESTsecurity Corp.)
대표 이사	정 상 원
법인설립일	2017년 1월 3일
본사소재지	서울특별시 서초구 반포대로 3 (서초동 1464-30) 이스트빌딩
사업분야	보안 SW 개발 및 서비스
임직원 수	118명 (2017.10월말 현재)
홈페이지	www.estsecurity.com

이스트시큐리티 연혁

1993	이스트소프트 시작
2000	인터넷디스크 1.0 출시
2007	알약 1.0 출시
2009	알약 2.0 출시 (기업용), 국제CC인증 획득
2010	시큐어디스크 출시, 알약 안드로이드 1.0 출시

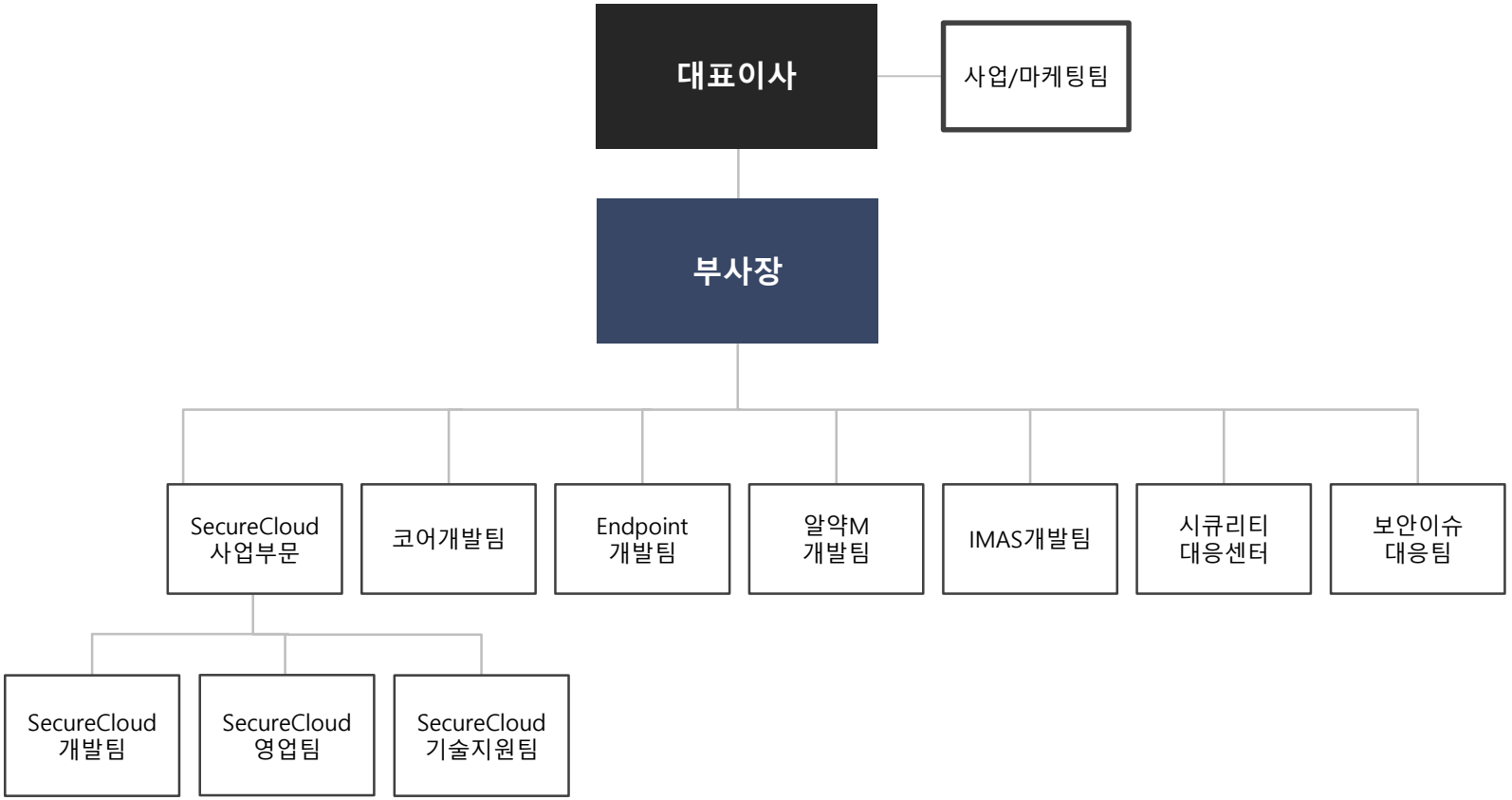
- 1993.10. ㈜이스트소프트 설립
- 2000.01. 인터넷디스크 1.0 출시
- 2007.12. 알약 1.0 출시
- 2008.02. 인터넷 디스크 5.0, 행정업무용 소프트웨어 선정 (한국소프트웨어산업협회)
- 2008.12. 2008 총결산 히트상품 - 보안솔루션부문 마케팅상 (디지털타임스)
- 2009.09. 인터넷 디스크 6i 출시
- 2009.09. 알약 2.0 기업용 버전 출시
- 2009.12. 알약 국제공통평가기준(CC)인증 획득
- 2010.07. 시큐어디스크 출시
- 2010.07. 알약 2.5 기업용/서버용 버전 출시
- 2010.12. 알약 안드로이드 1.0 출시
- 2010.12. 인터넷디스크 앱 출시 (iPhone)
- 2011.11. 인터넷디스크 앱 출시 (Android)
- 2011.07. 알약 안드로이드 'IT 혁신상품 대상' (디지털데일리)

2011	알약 '2012년 세계에서 주목 받을 국산SW 30선' 선정, '英 체크마크 보안인증', VB100 국제 보안 인증 획득	• 2011.07. 알약 '2012년 세계에서 주목 받을 국산SW 30선' 선정 (한국SW전문기업협회) • 2011.07. 알약 2.5 '英 체크마크 보안인증' 획득 (Westcoast lab) • 2011.10. 알약 안드로이드 프리미엄 출시 • 2011.11. 알약 'VB100 국제보안인증' 획득(Virus Bulletin)
2011	알약 2012 대한민국 대표 브랜드 대상	• 2011.11. 알약 2011 하반기 히트상품 (디지털타임스) • 2012.04. 알약 2012 대한민국 대표 브랜드 대상 (한경닷컴, Imbc, 동아닷컴) • 2012.07. 인터넷디스크 6i 행정업무용 SW선정 • 2012.12. 알약 2012 히트상품 (디지털타임스)
2014	알약 안드로이드 1,000만 다운로드	• 2013.05. 알약 3.0 & ASM 3.0 국제공통평가기준(CC)인증 획득 • 2013.05. 알약 3.0 Server 국제공통평가기준(CC)인증 획득 • 2014.09. 알약 안드로이드 1,000만 다운로드 돌파
2016	IMAS, 알약PMS, 알약 내PC지키미 출시	• 2016.04. IMAS 공개 • 2016.11. 알약 PMS, 알약 내PC지키미 출시

2017 이스트시큐리티 분사

- 2017.01. 이스트시큐리티 분사
- 2017.01. 랜섬쉴드 클라우드 1.0 출시
- 2017.01. 랜섬쉴드 PC 1.0 출시

이스트시큐리티 조직도 | ORGANIZATION CHART



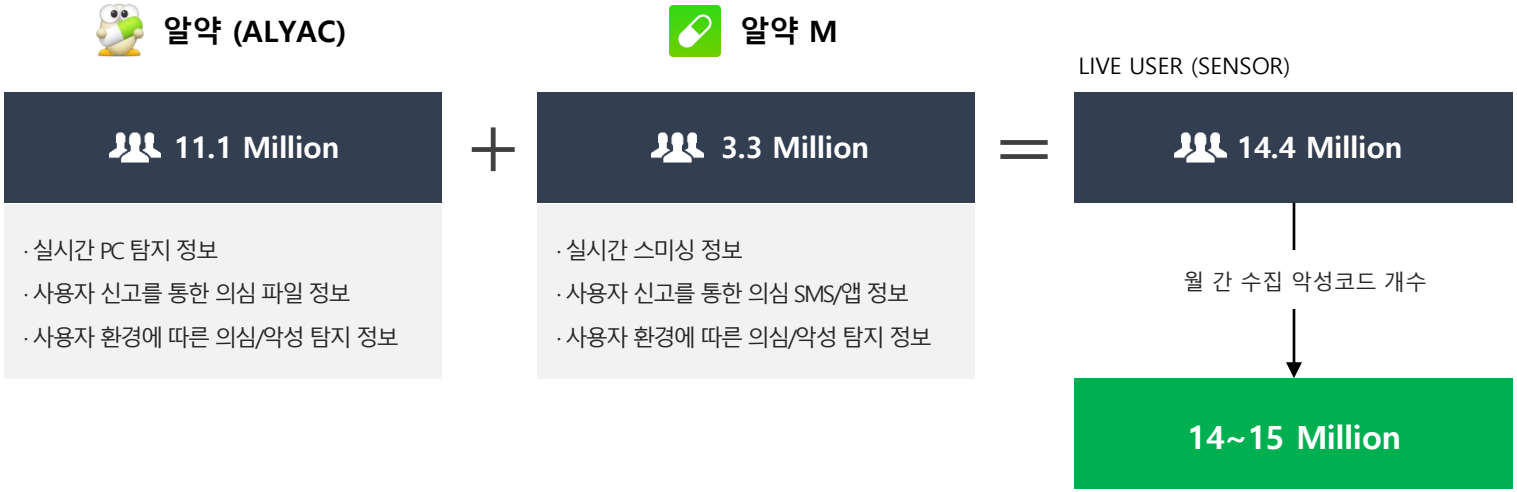
02 이스트시큐리티의 특장점

- 국내 1위 / 1400만 USER
- 보안위협분석 전문가 집단
- 인공지능 기술력

국내 1위 ANTI VIRUS 사업자

1,400만 : 사용자 수 & 월간 탐지 악성코드 개수

이스트시큐리티의 대표 제품인 알약과 알약M은 1,400만 사용자가 사용하는 강력한 브랜드 인지도를 가진 국내 대표 Anti Virus 프로그램 입니다.
이스트시큐리티는 해당 엔드포인트 솔루션을 통해 PC 기준 월 간 1,400~1500만 건, 모바일 기준 월간 4만 건 이상의 국내 최대 수준의 악성코드 DB를 상시 업데이트/관리 하고 있습니다. 이러한 실 사용자(Sensor)와 수집하는 대규모 악성코드DB는 차세대 사업을 위한 핵심 자원으로 활용 됩니다.



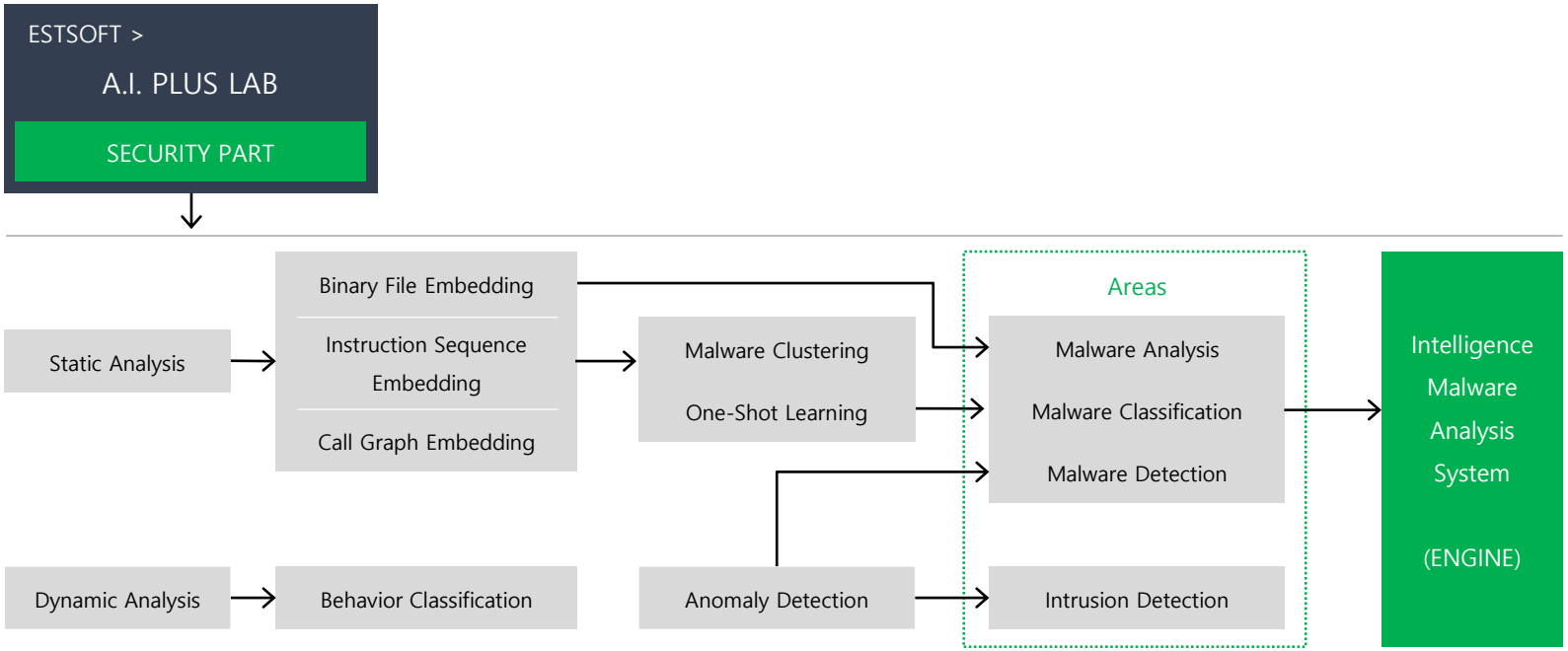
전문 백신 업체 10년의 노하우

이스트시큐리티는, 10년간 백신 제품 운영을 통해 다양한 악성 샘플에 대한 전문적인 분석 노하우와 더불어 이슈 대응 능력을 지닌 분석 전문가 집단 및 개발자 집단을 내부에 보유하고 있습니다.

보안 위협 분석 전문가 집단	커널 개발자 + 분석가 집단	A.I. Solution 개발자 집단
시큐리티 대응센터	코어 개발팀	Threat Inside 개발팀
보안이슈 대응팀		A.I. PLUS LAB
윈도우/안드로이드 /URL 분석 연구팀		

국내 최고 수준의 인공지능(Deep Learning)기술력

이스트소프트의 인공지능 연구소인 A.I. PLUS LAB에서는 보안 분야에 포커스 된 전담 인력이 편재되어 있으며, 다년간 연구를 통해 축적된 이스트소프트의 Security 기술은 이스트시큐리티의 '보안 위협 지식 검색(CTI Search Service) 서비스' 에 적용됩니다.



국내 최고 수준의 인공지능(Deep Learning)기술력

TECHNOLOGY	DEFINITION	Target Area
Binary File Embedding	바이너리 파일 전체로부터 CNN을 기반으로 한 딥러닝으로 패턴을 학습하여 유사한 벡터를 표현함으로써, 파일 내의 어떤 부분에 악성코드가 존재하더라도 악성 여부를 판단할 수 있습니다.	• Malware Analysis • Malware Classification • Malware Detection
Instruction Sequence Embedding	바이너리 파일에 존재하는 명령어 시퀀스와 바이너리 시퀀스로부터 다양한 악성코드에서 유사하게 등장하는 유의미한 시퀀스 패턴을 찾아 학습하고 이를 바탕으로 악성 행위의 유형과 위치를 탐지할 수 있습니다.	• Malware Analysis • Malware Classification • Malware Detection
Call Graph Embedding	함수의 호출 관계를 바탕으로 실질적으로 유사한 부분 그래프로 구성된 함수들을 유사한 벡터로 표현함으로써, 함수 심볼을 난독화하거나 부분 함수를 분리해내더라도 원래 함수와 유사성을 탐지해낼 수 있습니다.	• Malware Analysis • Malware Classification • Malware Detection
Malware Clustering	다양한 벡터 임베딩을 활용하여 여러 가지 기준으로 유사한 악성코드들을 클러스터링합니다. 나아가 기존에 사람이 분류하던 체계보다 더 일관된 기준으로 새롭게 탐지 명을 부여할 수 있습니다.	• Malware Analysis • Malware Classification • Malware Detection
One-shot Learning	새롭게 발견되어 아직 샘플이 부족한 악성코드라 하더라도 손쉽게 딥러닝 모델에 추가하여 빠르게 대응할 수 있습니다.	• Malware Analysis • Malware Classification • Malware Detection
Behavior Classification	수행된 프로세스의 동적 실행의 결과로 얻은 데이터로부터 해당 프로세스가 어떤 행위를 하는지 분류합니다.	• Malware Detection • Intrusion Detection
Anomaly Detection	데이터 또는 행위가 관측되는 확률 분포를 학습하여 해당 확률 분포에서 거의 발생하지 않는 사건을 탐지합니다.	• Malware Detection • Intrusion Detection

03 이스트시큐리티의 주요 제품

- 알약
- 알약M
- 시큐어디스크
- Threat Inside

이스트시큐리티 사업 영역 | BUSINESS AREA

이스트시큐리티는 '안티 바이러스(Anti-Virus)제품을 주축으로 한 엔드포인트 보안 사업에 기반을 두고 있으며, 확장된 사업영역으로 모바일 보안, 인텔리전스 보안 및 문서 보안 사업을 영위하고 있습니다.

	정의	대표 제품	제품 라인업
엔드포인트 보안	실시간 바이러스와 악성 코드 차단 및 치료	알약	• 알약 • ASM • 알약 패치관리(PMS) • 알약 내PC지키미 • 알약 익스플로잇쉴드 • 알약 레거시 프로젝터
모바일 보안	악성코드 및 스파이앱 탐지/치료, 청소 기능. 스팸, 스미싱 문자 감시/차단	알약M	• 알약M
인텔리전스 보안	인공지능 악성코드 분류 엔진 기반 '보안 위협 지식 검색 (CTI Search Service) 서비스'	Threat Inside	• Threat Inside
문서 보안	자료 유출/유실 방지, 랜섬웨어 대응 및 문서 중앙 통합관리가 가능한 차세대 문서 보안 솔루션	시큐어디스크	• 시큐어디스크 • 인터넷디스크 • 랜섬쉴드 엔터프라이즈

엔드포인트 보안 | Making world more secure.

알약

월 사용자 수 **1,100만 명의 국내 1위 백신 프로그램 알약**은 지속적인 탐지와 대응을 실현하는 강력한 통합 보안 솔루션으로 진화하였습니다.

알약은 위협 요소의 탐지와 방어, 대응 단계 전반을 가시화하여 제공하며, 각 단계에 최적화된 솔루션을 구축하여 랜섬웨어, 보안 취약점, 기타 알려지지 않은 공격까지 모든 보안 위협에 빈틈없이 대응할 수 있습니다.

01 강력한 악성코드 탐지

- 트리플 엔진(Tera, Botdefemder,Sophos) 동시 구동으로 더욱 완벽한 탐지율 제공
- 바이러스는 물론 애드웨어, 루트킷 같은 악성코드 파일검사 및 치료

02 실시간 감시

- 실시간으로 악성코드 침입 탐지 및 방어
- 인증되지 않은 프로그램 설치 중 악성코드 설치 시 실행 중지 및 감염 사실 알림

03 사전방역 및 랜섬웨어 차단기능

- 우수한 행위 기반 탐지 기술 바탕으로 사전 방역 기능 제공
- 사용자 파일 암호화 사전 차단
- 감염 의심 파일 수집하여 랜섬웨어 탐지 DB 강화

04 자가보호

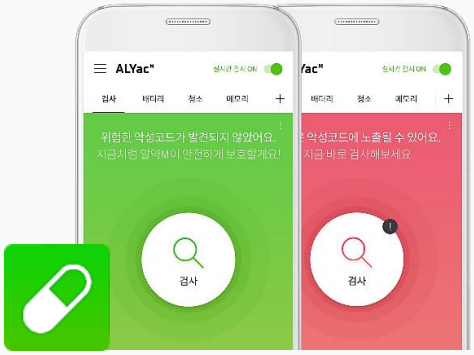
- 알약을 무력화 시키는 악성코드로 부터 파일과 프로세스를 스스로 보호
- 해킹 툴의 다양한 공격까지 방어

모바일 보안 | Making world more secure.

알약M

누적 다운로드 수 1,400만을 돌파한 모바일 보안 앱 1위 알약 안드로이드는 강력한 모바일 보안 및 메모리 최적화 등 편의 기능을 제공하여 모바일 환경을 안전하고 쾌적하게 만드는 모바일 통합 관리 앱 입니다.

2015년도 국내 최초로 클라우드 검사 기능을 도입하여 최신, 변종 악성코드를 실시간 탐지 및 치료가 가능한 알약 안드로이드는 새로운 모바일 보안의 길을 열어가고 있습니다.



01 악성앱 실시간 감시/치료

- 악성 앱 설치로 느려지거나 정상 사용이 어려울 때 검사하기
- 신규 앱 설치 및 업데이트, 실행 시 앱 안전도 정보 제공
- 유명 게임 으로 위장된 악성코드 포함 리패키징 앱 설치 시 위험 알림

02 스미싱(Smishing) 문자 메시지 감시 및 차단

- 스미싱 감시 및 스팸 감시 기능
- 위험 메시지 즉시 차단

03 더 빠르고 안전한 사용을 위한 스마트폰 최적화

- 불필요하게 실행중인 앱을 종료시키는 메모리 최적화
- 임시 저장 캐시 데이터 및 불필요한 파일을 한번에 삭제 청소

04 효율적인 폰 전력 사용을 돕는 배터리 관리

- 현재 배터리 상태를 한 눈에 보고, 배터리 사용 앱 정보 확인 및 종료
- 초절전/고속 충전/숙면 최적 모드 제공

문서보안 | Making world more secure.

시큐어디스크

2017 기술유출방지시스템구축 지원사업에서 **2년 연속 1위 사업자**로 선정된 시큐어디스크는 모든 자료를 중앙서버로 강제 이관 및 저장하여 자료유출/유실을 원천적으로 막고, 보안정책을 통해 안전하고 철저하게 문서를 관리할 수 있는 문서 보안 솔루션 입니다.

최근 랜섬웨어 감염, 내부자 자료 유출 등으로 기업의 중요한 문서 자산이 유실 또는 유출돼 피해를 입는 보안 사고가 빈번히 발생하는 가운데, 시큐어디스크는 보안 성능과 안정성을 입증 받은 제품으로서 회사의 디지털 문서 자산을 보호하기 위한 가장 안전한 선택이 될 것입니다.

01 내부자료 유출 원천 차단 환경

- 관리자가 설정한 보안 정책에 따라 로컬 저장 매체 유출 차단
- 화면 캡쳐, 클립보드 복사, 출력 등 기타 유출 경로 차단
- 웹메일, 웹하드, 메신저 등 온라인 매체에 대한 파일 첨부 행위와 같은 온라인 유출 차단

02 시큐어디스크 서버 통합 저장 환경

- 문서 중앙화를 통한 업무 연속성 보장
- 데이터 유출 방지를 위한 자료 암호화 기술 적용
- 관리자에 의한 사용자 보안 실시간 적용
- 부서별 특성에 맞는 정책 수립을 위한 폴더별 접근 권한 관리

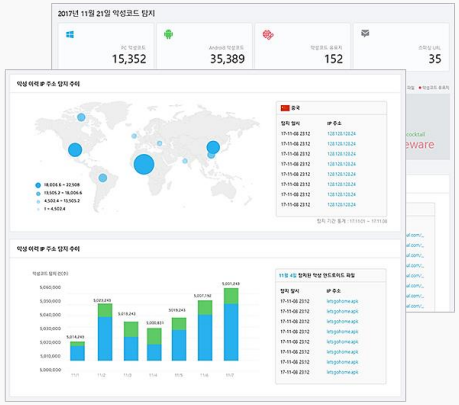
03 랜섬웨어 방지

- 버전 별 문서 관리를 통해 삭제 또는 덮어쓰기로 문서가 유실되거나 랜섬웨어로 인해 변조되더라도 빠르고 쉽게 복구
- 관리자 보안 정책 상 비인가 프로그램의 접근 원천 차단하여 랜섬웨어가 중요 문서를 강제적으로 변조하여 저장하는 것을 방지

인텔리전스 보안 | Making world more secure.

Threat Inside

Threat Inside는 '보안 위협 지식 검색 (CTI Search Service) 서비스' 로서, 사이버 보안 담당자를 대상으로 보안 위협 정보와 이에 특화된 대응 정보를 제공합니다.
24시간 언제든지 의심되는 파일이나 정보들을 분석하고 악성 여부나 종류를 자동으로 판별하여, 기하급수적으로 늘어나고 있는 신/변종 악성코드들을 탐지하고 대응하는 최상의 방법을 제공합니다.



01 강력한 A.I. 엔진

- 국내1,440만 이상의 실 사용자(LIVE USER)를 통해 수집되는 악성/정상 샘플을 활용.
- 알려지거나 혹은 알려지지 않은 악성코드에 대한 악성 여부를 99% 확률로 판단 가능한 딥러닝 기반의 추론 엔진을 개발

02 분석 시스템

- 24시간 언제나 분석 의뢰 및 실시간 결과 확인 가능
- 인공지능/정적/동적/URL&IP/평판/유사도/통계분석 등 다양한 방식의 악성코드 분석 시스템을 통해 다각도의 풍부한 분석 정보를 제공

03 보안위협전문가가 작성한 Deep Insight 컨텐츠

- 이스트시큐리티 내 숙련된 보안분석전문가들이 직접 악성코드 별로 분석 및 기록한 결과와 대응 노하우들을 분류 결과와 매칭된 검색 결과로 제공함으로써, 검증된 정확한 정보로 빠른 보안 위협 대응이 가능

04 SECURITY+A.I. : Threat Inside 소개

- 보안에 인공지능을 더하다.

잘 알려진 두 가지 문제

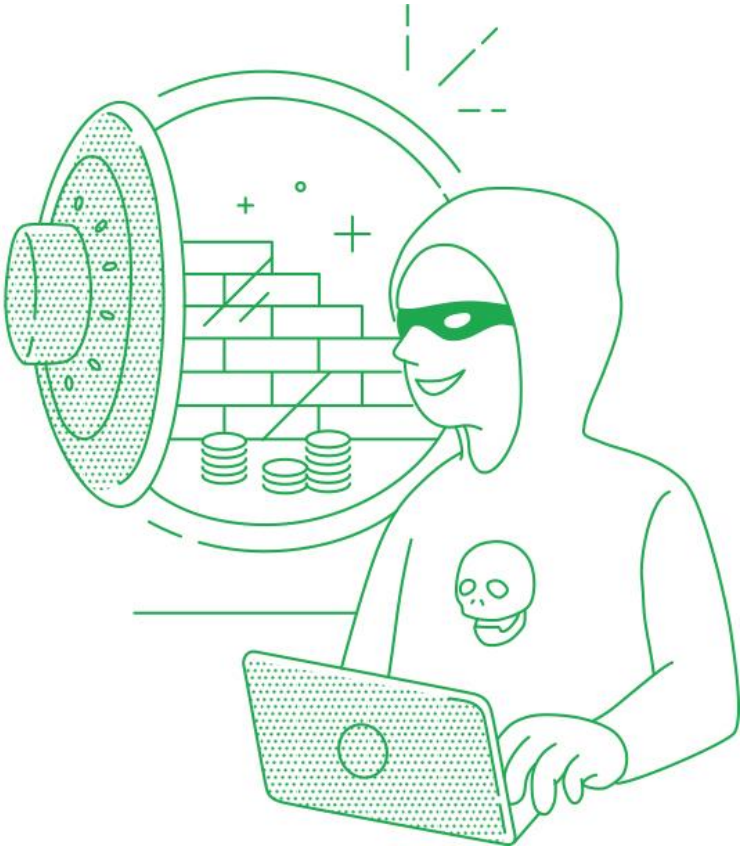
1. APT 지능화/고도화 공격

"예전의 침해 사건들은 엄청난 양의 포렌식 아티팩트를 남겼었고, 공격자의 행동을 식별하는 것은 아주 쉬운 일이었습니다."

해커들의 공격 방식은 날로 지능화/고도화되고 있으며, 안티바이러스나 방화벽과 같은 전통적인 보안 제품들만으로는 모든 공격을 막아내는 것이 힘듭니다.

해커들은 더 이상 단순한 스매시 엔드 그랩(Smash and grab) 공격을 수행하지 않으며, 덜 망가뜨리고, 더 털어가는(Less Smash, More Grabby) 공격을 수행합니다.

또한, 탐지, 조사 및 복구가 더 어려워진 공격은 환경에 계속 남아있을 가능성이 높으며, 이는 더 막대한 양의 금융 정보가 탈취되고 있음을 의미합니다.



잘 알려진 두 가지 문제

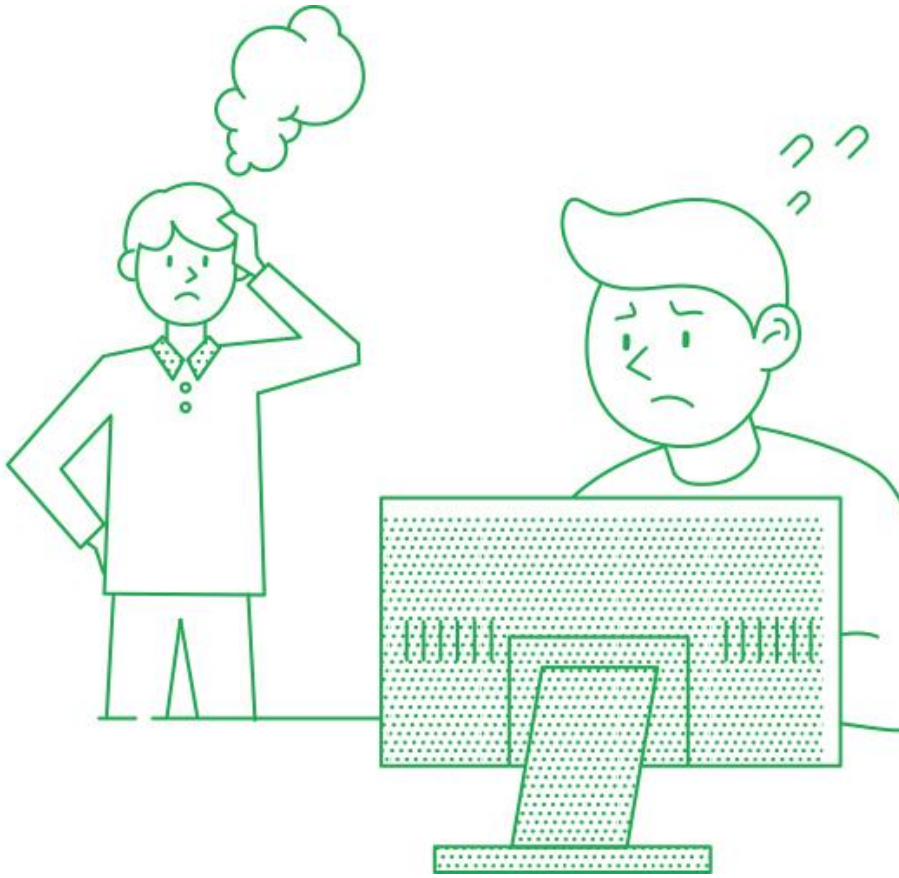
2. 전문보안인력의 부족

"부족한 전문 인력으로 지능적이고 고도화된 공격의 징후를 감지하고 즉각적이며 적절한 대응을 한다는 것은 무리가 있습니다."

몇 년 전과는 비교가 안 되게 늘고 있는 신/변종 악성코드나 데이터 트래픽의 양 그리고 각종 보안 시스템에 쌓이는 이벤트/로그들은 더 이상 인간이 분석하기에는 불가능한 분량으로 늘어가고 있습니다.

해커들은 다양한 방법으로 기업에 대한 공격을 압도적으로 수행하며, 수분 안에 데이터를 해킹하지만, 보안 담당자로서는 이러한 침해와 데이터 유출을 발견하고 조치하는데 며칠씩 매달려야 하는 어려움이 있습니다.

게다가 표적이 되는 공격 대상은 대부분 보안 전문가가 많지 않은 일반 기관이나 단체라 부족한 인력의 문제는 더더욱 크게 도드라져 나타났습니다.



풀리지 않는 문제

3. 솔루션을 도입했더니, 일만 늘었어요.

"심해에 있는 빙산을 꺼내게 되면 그걸 처리하는 건 담당자 몫이죠 기타 주변 솔루션 없으시면 걍 묻어주시는거 추천요"

일단 제가 낭패본다는 케이스가 운영리소스가 엄청 나요. 주 목적은 위협적인 행위를 탐지한다 이거인데. 그 다음 스탭은 각 기업 보안담당자 몫으로 떨어지죠. 아직 타 제품과 연동 부분도 확실하지 않고 이벤트는 나오는데 그걸 추적하고 처리할수 없는 상황이면 빚 좋은 개살구가 될거에요. 2달간 poc했을때 인터넷망에서 실제 악의적인 트래픽을 찾아내긴 했었는데 엔드포인트 백신이 먼저 찾아처리했던 기억도 나네요.

yff****

내부 네트워크 인사이트 기능은 좋습니다 사후 포렌식 활용성도 좋고
다만 악성행위에 대한 검증이 수동으로 필요한 상황이라 윗분들 말씀처럼 인력리소스가 엄청납니다

ill*******

보완재로 사용한다면 나쁘진않은듯. 비싼건 흠. 말처럼 인공지능같지않음. poc해보시길.

isf*****

감사합니다 결국 머신러닝을 사용해서 위협적인 행위를 탐지하지만 사람의 일을 줄여 주진 못하는가 보네요 ㅜㅜㅜ

BSE***

너무 잘 탐지해서 조치할게 많아짐
유입경로가 분석되 버려서 그거 조치하느라 빡셈

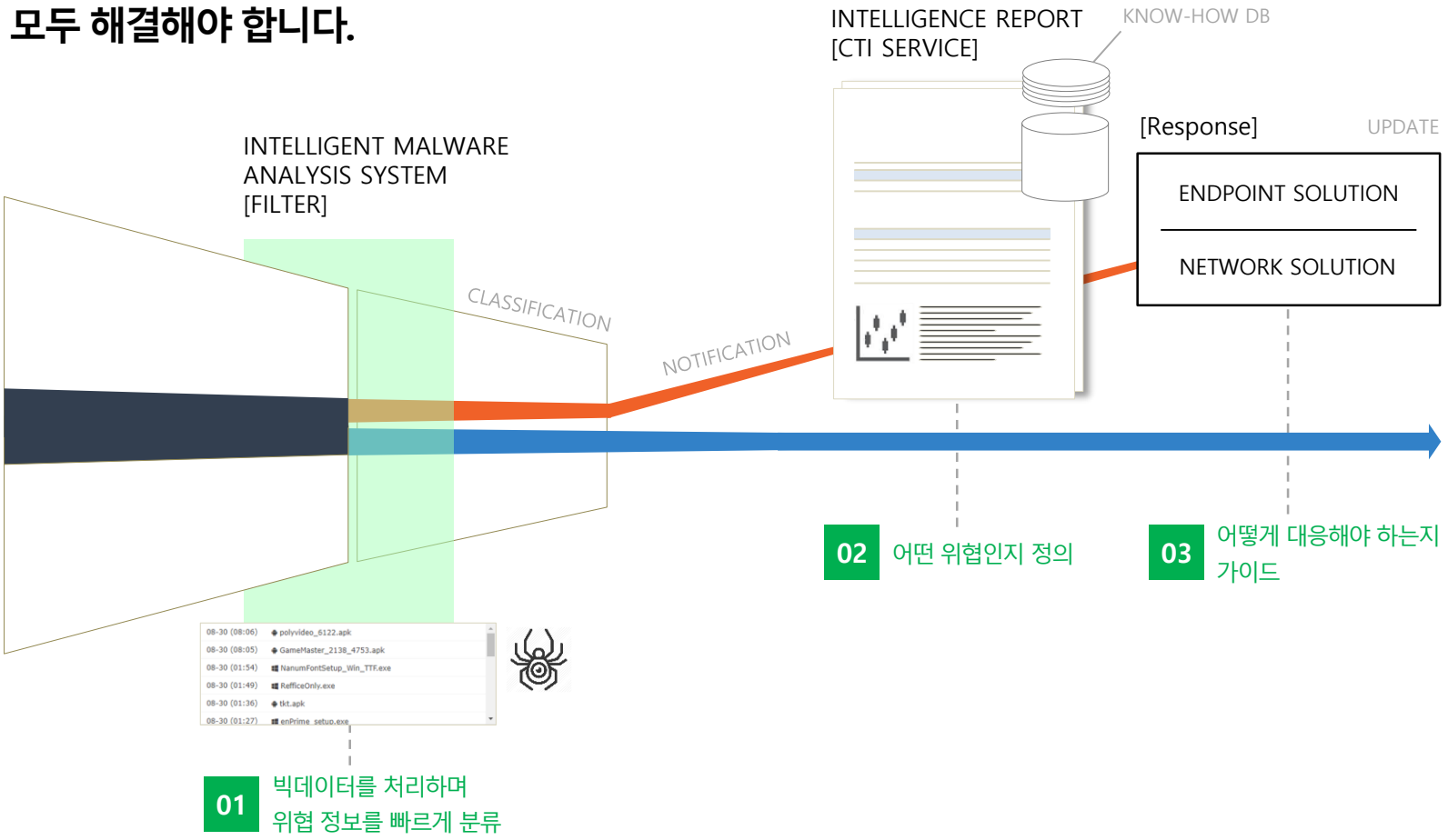
kt****

솔루션 구매 이후 이력 채용이 필수각
침해사고 분석 경험이 있는 중급 이상의 인력이 매일 튜닝해 가면서 모니터링 필요

ㅍㅂ***

세 가지 문제

모두 해결해야 합니다.



보안에 인공지능을 더하다

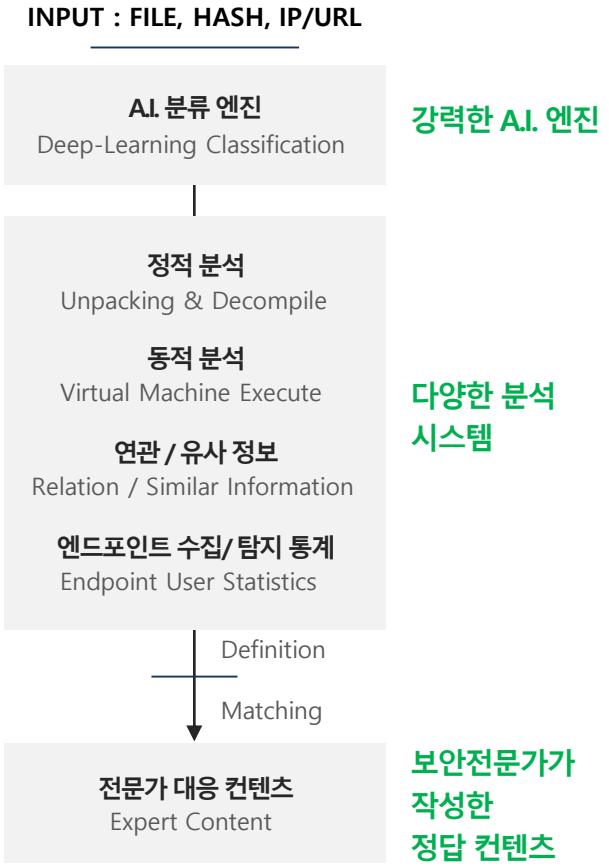
Threat Inside는,

이스트시큐리티는 2017년 KISA, 금보원, 경찰청 등에 악성코드 분석 시스템 구축 프로젝트(又 IMAS: Intelligent Malware Analysis System)를 S.I 사업으로 진행해 개발한 바 있습니다.

이 시스템을 더욱 고도화 해 이스트시큐리티는, 알약 1,440만의 실 사용자(LIVE USER)를 통해 수집되는 악성/정상 샘플을 활용해, 알려지거나 혹은 알려지지 않은 악성코드에 대한 악성 여부를 99% 확률로 판단 가능한 새로운 딥러닝 기반의 추론 엔진을 개발하였습니다.

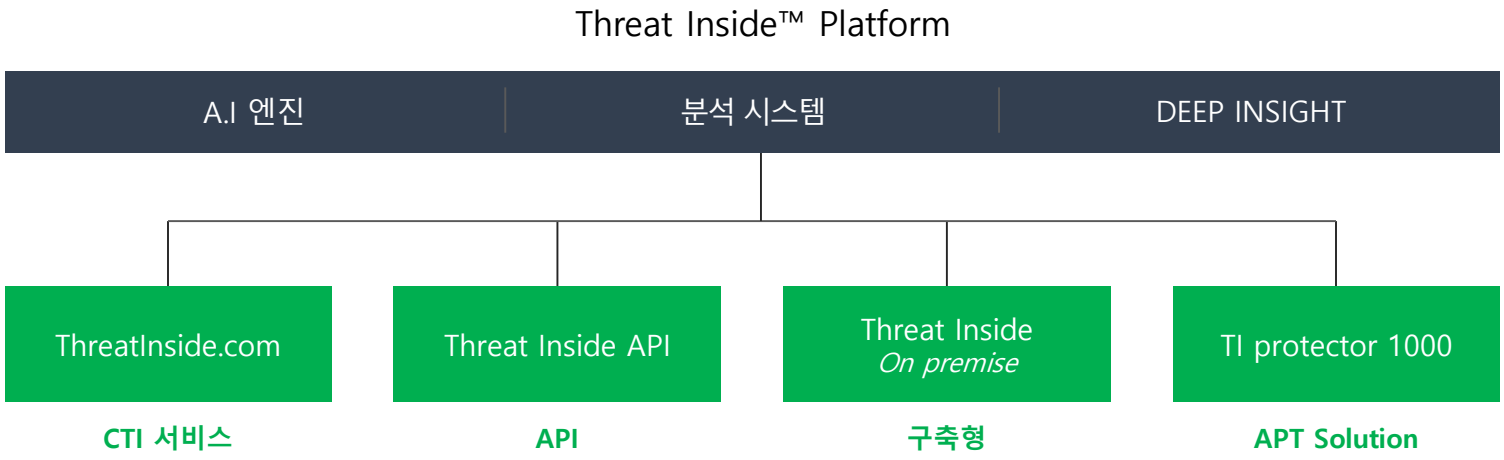
더해 이스트시큐리티는 대규모의 악성코드 데이터를 심도 깊게 다뤄본 숙련된 보안 위협분석 전문가 집단을 보유하고 있습니다. 이들로부터 다년간 확보된 증거 기반 지식(Cyber Threat Intelligence)과 대응 노하우를 전산 DB화하고, 판별된 악성코드 분류 검색 결과로 매칭해 제공함으로써, 보안 담당자들이 온라인 바다 속에서 정보를 찾아 헤매거나, 정보의 신뢰성에 대해 검토 받지 않은 상태에서 불안한 조치를 취하는 일이 없도록 기업 내부의 빠른 의사결정과 보안 이슈의 해결을 돕고 있습니다.

현재 클라우드 기반의 서비스는 2018년 상반기 정식 상용화를 준비하고 있으며, 분석 엔진 등을 HW에 탑재한 어플라이언스 형식의 제품 판매도 함께 준비하고 있습니다.



보안에 인공지능을 더하다

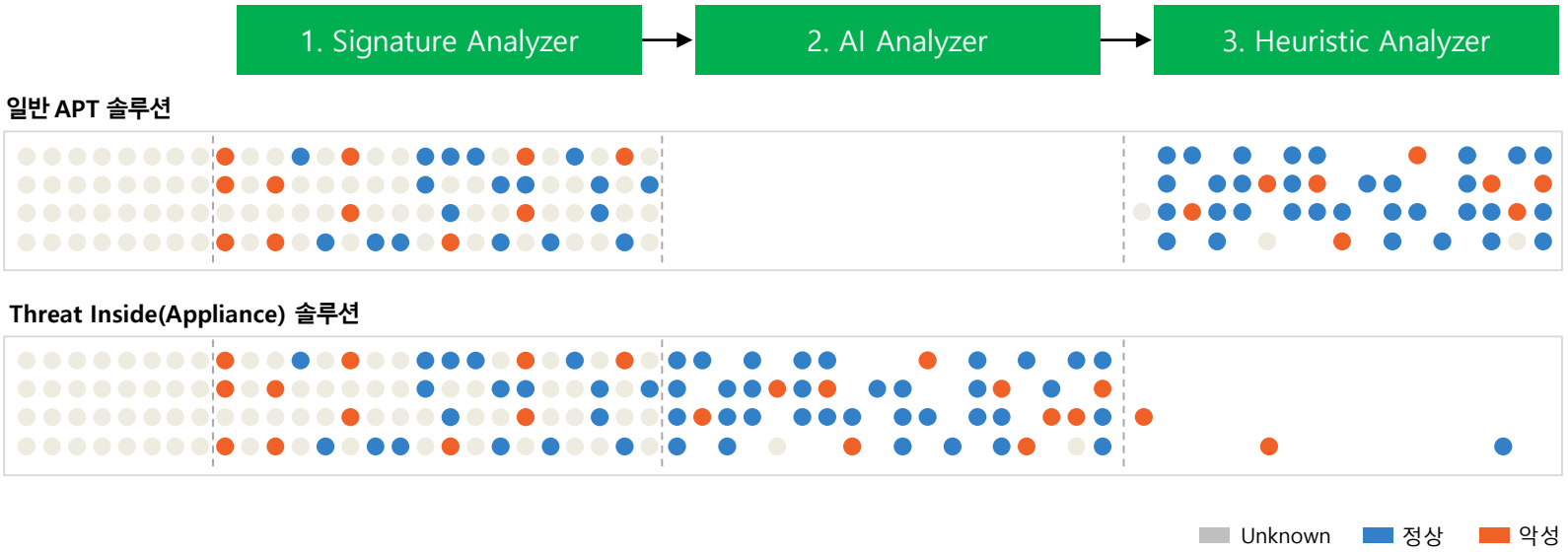
Threat Inside는, 다음과 같이 구성되어 있습니다.



보안에 인공지능을 더하다

Threat Inside APT Solution은,

기존의 어플라이언스들은 시그니쳐 기반의 분석 다음으로 휴리스틱 분석 단계로 넘어가 동적 분석 등에 많은 시간과 리소스를 사용해야 했습니다.
Threat Inside Appliance는 시그니쳐 분석기와 휴리스틱 분석기 사이에 AI 분석기를 배치함으로써 휴리스틱 분석기로 넘어가는 분석량을 최소화 하며, 높은 퍼포먼스를 낼 수 있도록 설계 되었습니다.



CTI REPORT

Threat Inside Deep Insight 페이지에서는,

다음의 분석 결과를 확인할 수 있습니다.

A.I. 분석결과

샘플 개요	악성 여부, 파일 크기, 타입, 전체 태그, 해시 다운로드 기능을 제공합니다. (※ PDF 보고서, 샘플 원본, PCAP 파일 등)
A.I. 분석 결과	악성 및 위험도에 대해 스코어링 된 정보를 제공합니다.
클러스터링	AI를 통해 클러스터링 된 그룹 정보와 그룹 내 거리 값을 통해 속성 정보를 가이드합니다.
유사 샘플	AI.엔진을 통해 인접한 샘플 리스트와 유사 수치 정보를 제공합니다.

CTI REPORT

전문가 컨텐츠

샘플 개요	악성코드 카테고리와 관련된 개요. 설명
A.I. 분석 결과	악성코드 카테고리와 관련된 이미지 전체
클러스터링	카테고리에 대한 사건을 기록한 히스토리를 타임라인 형태의 정보로 제공
유사 샘플	카테고리 특성에 따른 감염 경로와 증상에 대한 설명
샘플 개요	★ 카테고리에 대한 대응 방안 제공 / 보안 담당자 대응 방안 별도 제공
A.I. 분석 결과	카테고리 내 샘플들에 대한 제품 탐지 추이 제공
클러스터링	카테고리 내 샘플 리스트를 제공하여 추가분석 정보로 활용
유사 샘플	★ 카테고리 내 대표 샘플에 대해 전문가 코드 분석을 단계별로 제공

CTI REPORT

정적 분석 결과

- PE 정보
- 버전 정보
- 섹션 정보
- API Call 그래프
- 임포트 정보
- 익스포트 정보
- 리소스 정보
- 문자열

동적분석 결과

- 분석 타임라인
- 주요 행위정보
- 탐지 흐름도
- 행위 고급분석
- 네트워크 정보
- 문자열
- 분석환경

URL/IP분석 결과

- URL 개요
- 네트워크 지도
- 탐지 흐름도
- 히스토리 요약
- 악성히스토리
- 관련히스토리
- 사이트 히스토리

평판 분석

- 워드클라우드
- 백신 탐지

연관성 분석

- 인텔리전스 그래프
- 연관 샘플 리스트
- 샘플 비교 분석

샘플 통계

- 제품 탐지 통계
- 샘플 유포지
- 시스템/네트워크 행위
- 탐지/파일이름

Threat Inside

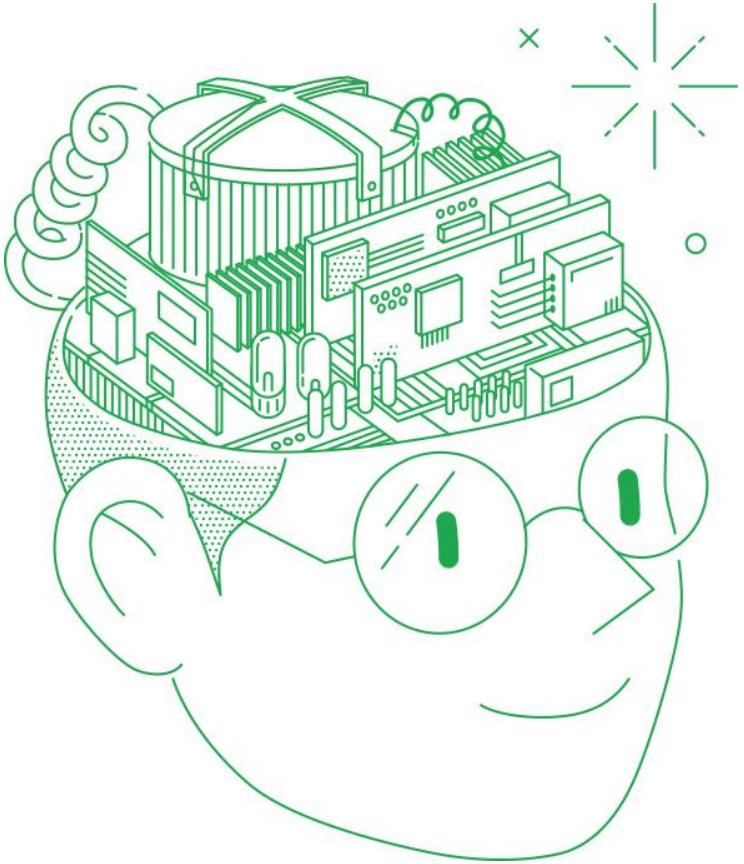
Threat Inside를 사용하는 것은
숙련된 보안위협분석가를 고용하는 것과 같습니다.

강력한 CTI 서비스

보안 담당자에게 저녁 있는 삶을 만들어 드리겠습니다.

Threat Inside 는 '보안 위협 지식 검색 (CTI Search Service) 서비스' 로서, 사이버 보안 담당자를 대상으로 보안 위협 정보와 이에 특화된 대응 정보를 제공합니다.

24시간 언제든지 의심되는 파일이나 정보들을 분석하고 악성 여부나 종류를 자동으로 판별하여, 보안 담당자가 정확하고 신속한 판단을 내릴 수 있도록 돕습니다.

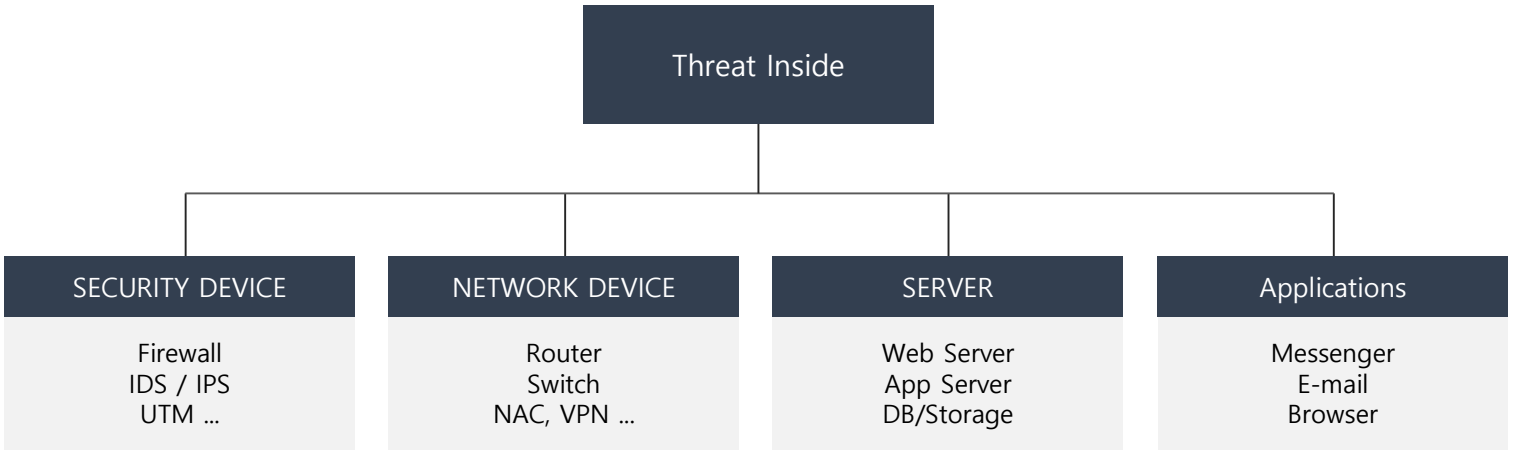


05 Threat Inside Case Study

- 금융보안원
- 경찰청
- KISA

Threat Inside

久 IMAS: Intelligent Malware Analysis System



- Security Devices, Network Devices, Server, Application 등 보안 위협요소가 존재하는 모든 센서에 적용 가능
- 센서에서 수집된 모든 정보에서 위협요소가 존재하는 샘플을 분석하고 악성 여부 판단을 포함한 리포트 제공

Threat Inside

레퍼런스 1. 금융보안원

- KOREA
- FINANCIAL SECURITY INSTITUTE (금융보안원)
- 대한민국의 신뢰할 수 있는 금융환경 조성을 위하여 설립된 금융보안 전담 기관

NEEDS

해킹, DDoS, 악성코드, 정보 유출 등 다양한 사이버 침해사고를 감지하고 대응할 수 있는 솔루션이 필요

✓ 대한민국 주요 금융기관과 관련된 다양한 샘플을 수집하여 악성 여부를 검증하는 시스템
✓ 샘플 수집부터 분석 및 결과를 제공하는 과정에 자동화 프로세스 적용

Threat Inside

레퍼런스 2. 경찰청

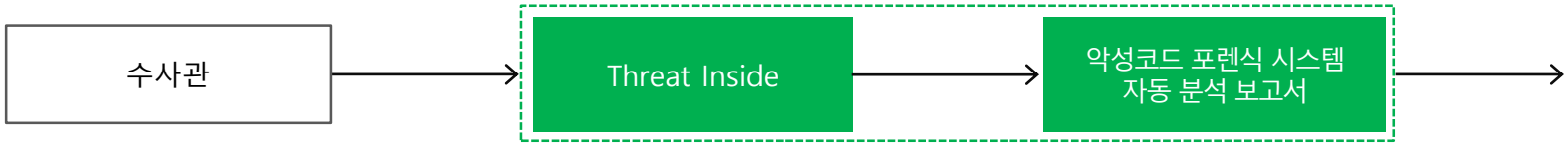
- KOREA
- KOREAN NATIONAL POLICE AGENCY
- 대한민국 치안 업무를 관장하는 중앙행정기관

NEEDS

증가하는 사이버 범죄에 대응하기 위한 상세분석 리포트 및 유사/연관 샘플 분석 솔루션이 필요

- ✓ 사이버 수사 업무와 관련된 파일의 악성 여부 검증을 위한 시스템
- ✓ 경찰청 업무 프로세스와 연관된 문석 정보를 제공하여 분석 결과를 효율적으로 활용할 수 있도록 도움

- 사건 관련 샘플 분석 요청



- 이해하기 쉬운 요약 정보 제공
- 전문 분석관을 위한 상세 정보 제공
- 유사 사전 목록 제공

Threat Inside

레퍼런스 3. 한국인터넷진흥원

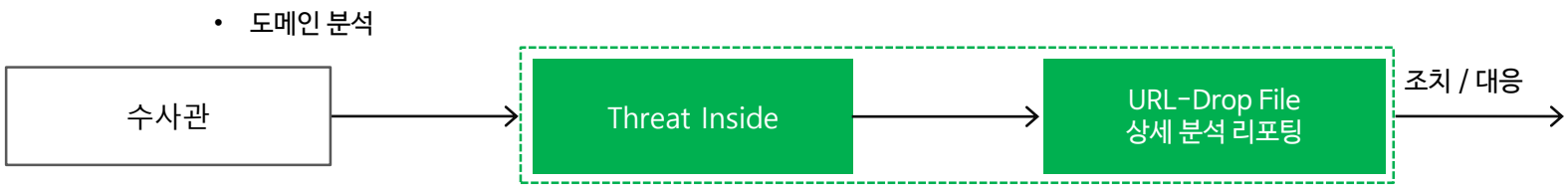
- KOREA
- KOREAN INTERNET & SECURITY AGENCY
- 대한민국 글로벌 리더를 지향하는 인터넷 정보보호 진흥 기관

NEEDS

국내 도메인을 통해 유포되는 악성코드를 탐지하고 대응하기 위한 정적/동적 분석 솔루션 필요

✓ 국내 도메인에 대해 일일 2,000만 도메인 분석

✓ 기존에 운영하고 있던 시그니쳐 기반 탐지가 아니라, 신규 유포지를 탐지할 수 있는 차세대 분석 솔루션 필요



- URL 탐지흐름도
- 사용된 취약점, Exploit Kit 분석
- Drop-File 상세 연계 분석
- 종합 인텔리전스 리포팅

06 APPENDIX

- 특허 내역

특허 | Making world more secure.

구분	등록번호	등록일	발명의 명칭	등록권자
1	10-0996839	2010-11-22	컴퓨터백신데이터베이스 자동검증시스템 및 검증방법	이스트소프트(50%), 이스트시큐리티(50%)
2	10-1174635	2012-08-10	자동화된 악성코드 긴급대응시스템 및 방법	이스트소프트(50%), 이스트시큐리티(50%)
3	10-1191914	2012-10-10	웹스토리지서비스를 제공하는 파일관리시스템의 파일관리방법	이스트소프트(50%), 이스트시큐리티(50%)
4	10-1402057	2014-05-26	위험도계산을 통한 리패키지 애플리케이션의 분석시스템 및 분석방법	이스트시큐리티(100%)
5	10-1404882	2014-05-30	행위를 기반으로 한 악성코드 분류 시스템 및 분류방법	이스트소프트(45%), 이스트시큐리티(55%)
6	10-1462311	2014-11-10	악성코드 차단방법	이스트소프트(15%), 이스트시큐리티(85%)
7	10-1483859	2015-01-12	백신의 상태를 모니터링하는 관리시스템을 이용한 악성코드 차단방법	이스트소프트(35%), 이스트시큐리티(65%)
8	10-1483901	2015-01-12	인트라넷 보안시스템 및 보안방법	이스트소프트(80%), 이스트시큐리티(20%)
9	10-1490442	2015-01-30	이동통신단말기, 이동통신단말기에서의 악성문자메시지 차단방법 및 시스템	이스트시큐리티(100%)
10	10-1710918	2017-02-22	사용자파일을 암호화하는 악성코드의 모니터링 장치 및 방법	이스트소프트(50%), 이스트시큐리티(50%)
11	10-1737794	2017-05-15	사용자파일을 암호화하는 악성코드의 모니터링 장치 및 방법	이스트소프트(50%), 이스트시큐리티(50%)

감사합니다

ESTsecurity
이스트소프트 서울시 서초구 반포대로 3 이스트빌딩 (우) 06711