AI, 빅데이터 기반, 글로벌 최고 수준의 사이버 위협 인텔리전스 전문 기업

SANDS Lab

2023년 8월

MDX MAX M/X malwares.com

Disclaimer

본 자료의 재무정보는 한국채택국제회계기준에 따라 작성된 영업실적 입니다.

본 자료에 포함된 '예측정보'는 개별 확인 절차를 거치지 않은 정보들입니다. 이는 과거가 아닌 미래의 사건과 관계된 사항으로 회사의 향후 예상되는 경영현황 및 재무실적을 의미하고, 표현상으로는 '예상', '전망', '계획', '기대', '(E)' 등과 같은 단어를 포함합니다. 위 '예측정보'는 향후 경영환경의 변화 등에 따라 영향을 받으며, 본질적으로 불확실성을 내포하고 있는 바, 이러한 불확실성으로 인하여 실제 미래 실적은 '예측정보'에 기재되거나 암시된 내용과 중대한 차이가 발생할 수 있습니다. 또한, 향후 전망은 PRESENTATION 실시일 현재를 기준으로 작성된 것이며 현재 시장상황과 회사의 경영방향 등을 고려한 것으로 미래 시장환경의 변화와 전략수정 등에 따라 변경될 수 있으며, 별도의 고지 없이 변경 될 수 있음을 양지하시기 바랍니다.

본 자료는 투자자들의 투자판단을 위한 참고자료로 작성된 것이며, 본 자료의 활용으로 인해 발생하는 손실에 대하여 회사 및 회사의 임원들은 그 어떠한 책임도 부담하지 않음을 알려드립니다.(과실 및 기타의 경우 포함)

SANDS Lab

CONTENTS

AI, 빅데이터 기반, 글로벌 최고 수준의 사이버 위협 인텔리전스 전문 기업

SANDS Lab

Prologue

01 ▪ 사이버 위협에 따른 피해 급증
02 ▪ CTI(Cyber Threat Intelligence)란?
03 ▪ 사이버 보안 기술 Paradigm Shift
04 ▪ CTI 시장 본격적 개화
05 ▪ Corporate Identity

SANDS Lab

01 사이버 위협에 따른 피해 급증

단 한번의 클릭으로, 사이버 범죄 피해 금액 연간 최대 7조 달러 손실 위험

사이버 위협의 고도화, 첨단화에 따른 피해 확대로 진보된 사이버 보안 기술 필요성 대두

① 하나의 기업이 사이버 침해 시도를 경험한 평균 횟수	270 건
② 한 번 이상 실제 사이버 공격의 피해를 경험한 기업 비중	86 %
③ 연 간 사이버 범죄로 인한 피해 금액	7 조달러
④ 랜섬웨어 공격으로 인한 피해 금액	200 억달러
⑤ 사이버 공격으로 인한 기업 데이터 피해 금액	400 만달러

※자료: 2021년 기준, 미래에셋증권, 하나증권

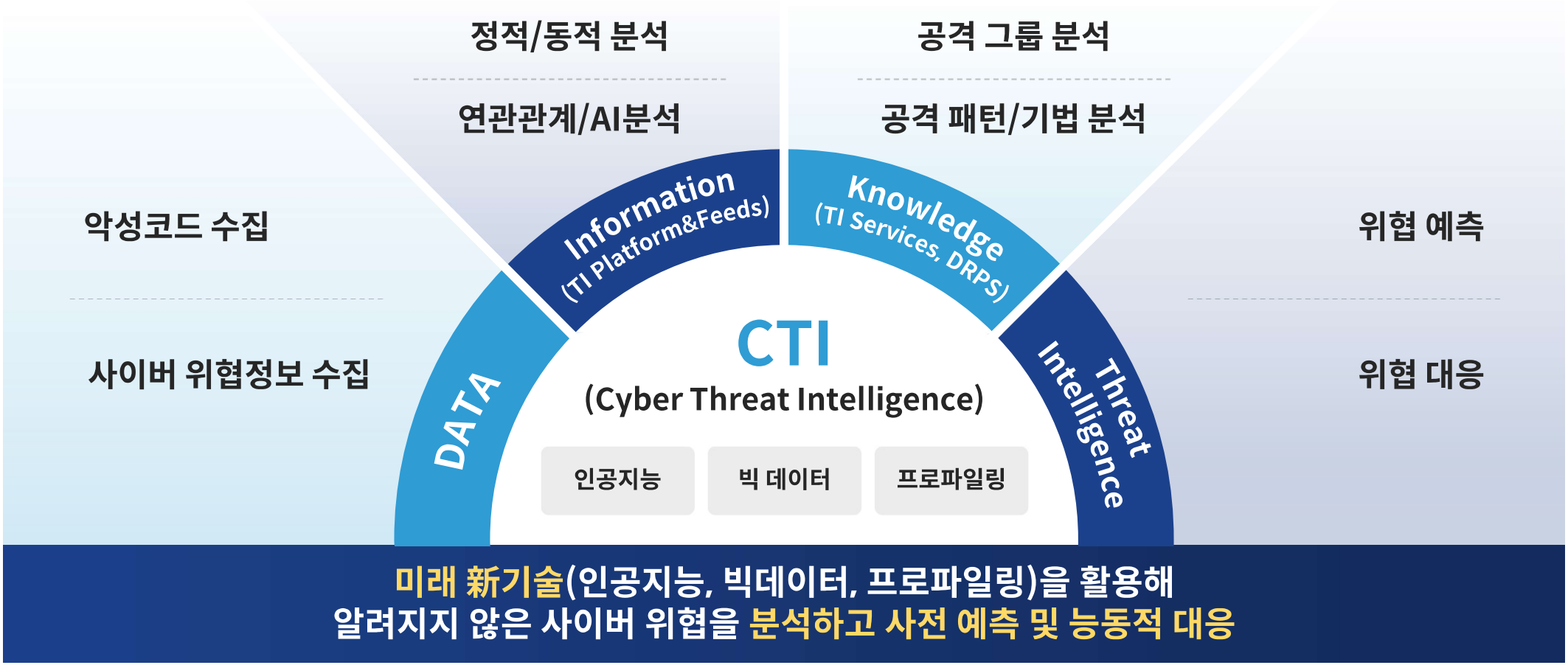
고도화, 첨단화 되는 사이버 위협에 능동적 대응 가능한 지능형 사이버보안 솔루션에 대한 필요성 증대

02 CTI(Cyber Threat Intelligence)란?

첨단화 되는 사이버 위협에 대응하기 위한 차세대 사이버 보안 기술, CTI

CTI (Cyber Threat Intelligence)?

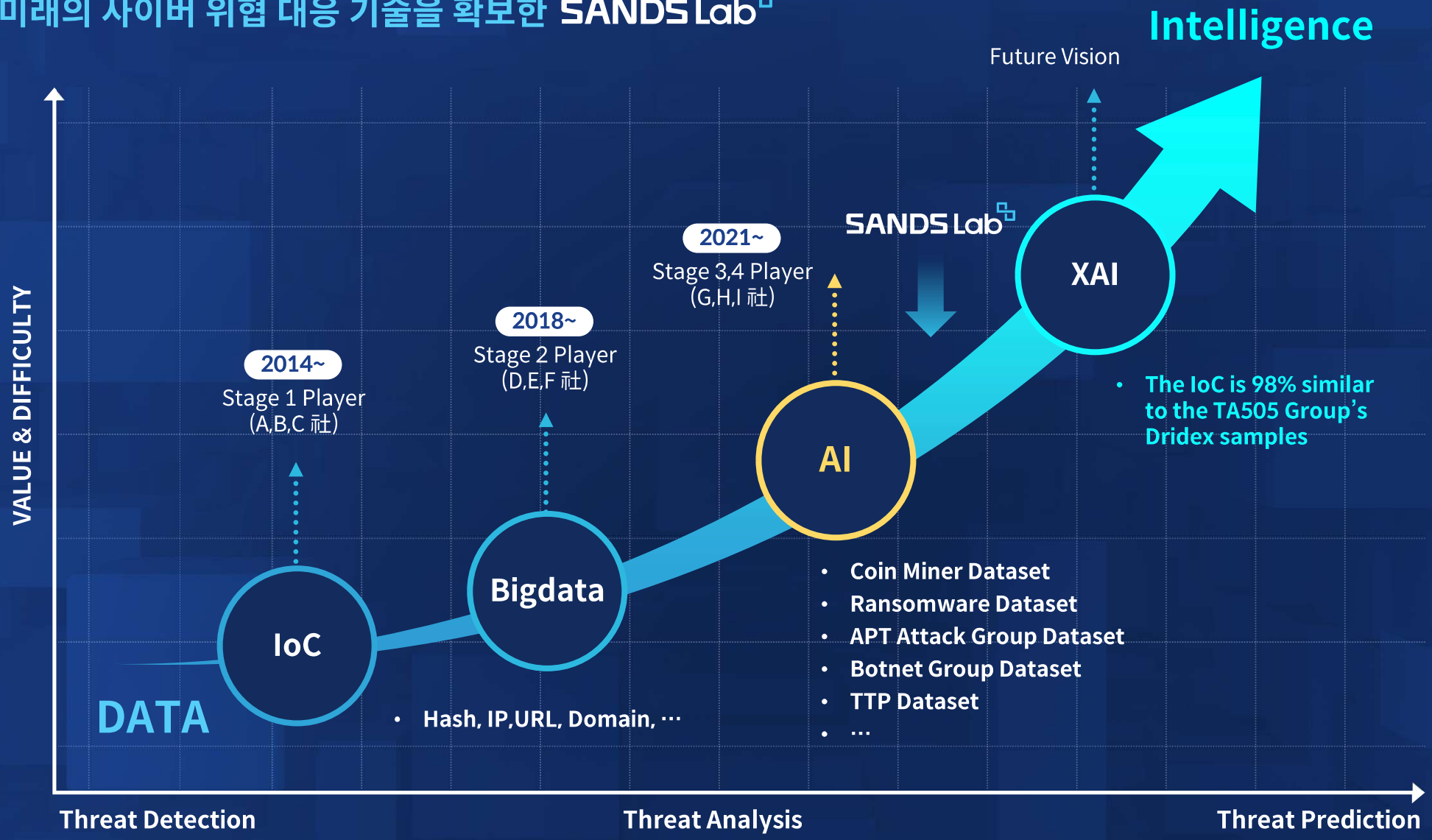
각종 사이버보안 위협 데이터를 분석 → **공격의도, 목적 및 방식 등을 식별하고 효과적인 대응을 위해**
보안 전문가들이 오랜 시간 분석하고 대응해온 지식과 의사결정에 대한 경험의 산출물



SANDS Lab

02 CTI(Cyber Threat Intelligence)란?

단순 데이터를 넘어, 차별화된 기술력을 기반으로 미래의 사이버 위협 대응 기술을 확보한 SANDS Lab



03 사이버 보안 기술 Paradigm Shift

사이버 보안 기술 Trend는 CTI 중심으로 패러다임이 이동 중이며,
샌즈랩은 CTI의 근간이 되는 Data를 확보하고 이를 활용한 차별화 된 비즈니스 모델 보유

사이버 보안 기술 Trend

	Lv. 01 (~2010년)	Lv. 02 (~2016년)	Lv. 03 (~2020년)	Lv. 04 (2021년~)
	알려진 공격 제한적 대응	알려진 공격 대응	알려지지 않은 공격 제한적 대응	알려지지 않은 공격 대응
대응 기술	**기본 보안 솔루션** ▪ 방화벽, 보안관제 ▪ IDS ▪ 안티바이러스(백신)	**보안 관제 고도화** ▪ 데이터 수집 ▪ 연관 분석 ▪ ESM, SIEM	**차세대 분석** ▪ 악성코드 행위분석 ▪ 이상 행위 탐지 ▪ EDR, SOAR	**CTI(사이버 위협 인텔리전스)** ▪ 인공지능/빅데이터 ▪ 프로파일링/역추적 ▪ 초거대 AI/생성형 AI
국내 Player	A사, E사, S사, W사	E사, T사	G사, A사, C사	SANDS Lab

차별화 된 CTI Business Model

수익구조	Lv. 01 ~ Lv. 03 Player	VS	Lv. 04 Player	
			데이터 사업	솔루션 사업
	Only 솔루션 판매		API (기존 시스템과 연계) / Feed (수집 정보 역제공) / Dataset (Big Data 공급)	MDX / MAX

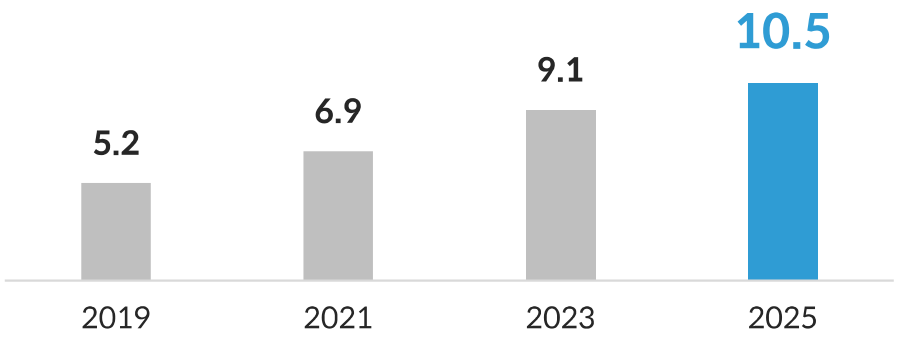
SANDS Lab

04 CTI 시장 본격적 개화

글로벌 사이버 범죄 피해 규모 증가에 따라 가파르게 성장하고 있는 CTI 시장 전망

글로벌 사이버 범죄 피해 규모

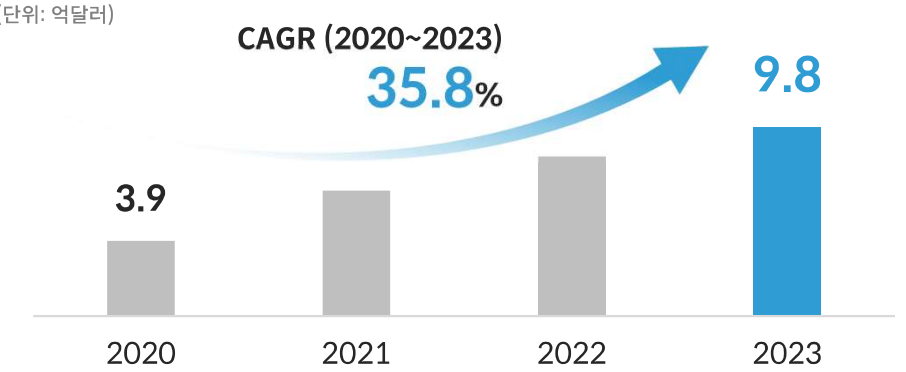
(단위: 조달러)



※자료: 사이버시큐리티벤처스

글로벌 CTI 시장 전망

(단위: 억달러)



※자료: Frost&Sullivan

Big Tech 기업들의 CTI 역량 내재화

회사명	기업특징/주력사업	피인수 CTI 기업	인수시기	인수금액 (단위: 달러)
AT&T (미국)	세계 최대 통신 기업	AlienVault (스페인)	2019	-
Everbridge (미국)	기업 소프트웨어 기업	NC4 (미국)	2019	8,300만 (약, 1천억)
ZeroFox (미국)	CTI 전문 기업	Vigilante (미국)	2021	-
Splunk (미국)	세계 최대 SIEM 기업	TruSTAR (미국)	2021	-
Microsoft (미국)	세계 최대 소프트웨어 기업	RiskIQ (미국)	2021	5억 (약, 6천억)
Outpost24 (스웨덴)	사이버보안 위험 관리 기업	Blueliv (스페인)	2021	-
Rapid7 (미국)	모의해킹 전문 기업	InSights (미국)	2021	3억 3,500만 (약, 4천억)
HelpSystems (미국)	비즈니스 인텔리전스, 보안 및 규정 준수 분야 전문 기업	PhishLabs (미국)	2021	-
DomainTools (미국)	CTI 전문 기업	Farsight Security (미국)	2021	-
Google (미국)	세계 최대 소프트웨어 기업	Siemplify (미국)	2021	5억 (약, 6천억)
		Mandiant (미국)	2022	54억 (약, 7조)

05 Corporate Identity

차별화 된 기술력과 축적된 빅데이터를 기반한 글로벌 최고의 CTI 전문 기업

CTI 1st Mover

- 국내 최초 인텔리전스 퍼블릭 서비스 런칭
- 위협 프로파일링 관련 R&D 과제 및 선도 기술 수행
- 국내 최초 **보안분야 AI 적용 신기술(NET) 인증**
- 초거대 AI, 생성형 AI 연동을 통한 진보된 인텔리전스 제공

다양한 매출 확대 전략 추진

- 母회사 **케이사인과의 시너지**
- **총판 체계 구축**을 통한 공공, 일반분야 매출 확대 본격화
- 연동 솔루션 출시로 CTI 도입 기술적 진입 장벽 낮춤
- 자체 클라우드 데이터센터 구축
- 5G, C-ITS, BAS 등 신사업 추진
- 차별화 된 **해외 시장 진출** 전략

글로벌 수준의 기술 경쟁력 확보

- 전체 인력의 **84**% R&D 비중으로 기술 중심의 조직 구성
- **95**여개의 핵심 기술 특허 출원 및 포트폴리오 구성을 통한 지식재산권 확보
- CTA (Cyber Threat Alliance) 활동을 통해 글로벌 수준의 인텔리전스 퀄리티 입증

실적 성장 본격화

- 데이터 기반 수익 구조로 **원가 구조 개선**
- 기업의 중장기 Risk Management 관점에서 **CTI 필요성 증대**
- 생성형 AI 연동을 통한 자동화된 보안 위협 대응 프로세스 수립. 이를 통한 **RPA 시장 연계 성장**

SANDS Lab

CHAPTER

I Company Overview

01 회사 개요

Company Profile

회사명	주식회사 샌즈랩
대표이사	김기홍
설립일	2004년 11월 1일
자본금	15억원 (2023년 상반기 기준)
임직원	38명 (2023년 상반기 기준)
주요 사업	사이버 보안 위협 인텔리전스 등 소프트웨어 개발 및 공급
본사	서울시 강남구 선릉로 577 4층
홈페이지	www.sandslab.io

CEO Profile

대표이사 김 기 홍

- 연세대학교 컴퓨터/산업공학 학사
- 現) ㈜샌즈랩 대표이사
- 국무총리 표창 (2016년)
- 과학기술부장관 표창 (2021년)
- 과학기술부장관 표창 (2022년)

주요 임원 Profile

성명	직책	담당업무	주요 경력
정철호	상무	사업부 총괄	▪ 성균관대학교 정보공학과 학사 ▪ (주)NSHC MSSP 사업본부 이사
하수헌	이사	영업 총괄	▪ 익사이트스토아코리아 기술부 ▪ K2network US Tech팀 ▪ 제이컴정보 사업본부
박성은	이사	연구개발 총괄	▪ 아주대학교 컴퓨터공학 박사 ▪ 소리나무솔루션 수석연구원 ▪ ㈜케이사인 수석연구원
이창주	이사	경영지원 총괄	▪ 중앙대학교 회계학 학사 ▪ 잘만테크 재경팀 ▪ ㈜케이사인 재경팀

02 성장 스토리

인공지능, 빅데이터, 프로파일링 등 차세대 기술을 활용해
글로벌 기술경쟁력 확보 및 세계 수준의 CTI 기업으로 도약

설립기 2003~2012

CTI 원천기술 확보

2003
- 연세대학교 학생 벤처 창업

2004
- 법인 전환 및 사명 변경
  ((주)세인트시큐리티)

2008
- 한국인터넷진흥원 봇넷 과제 수주

2009
- 기업부설연구소 설립
- ETRI DDos 대응 기술 과제 수주
- 악성코드 자동 분석 과제 수주

2011
- 악성코드 분석 시스템 출시 및 CC 인증 획득

2012
- 기술혁신형 중소기업 인증

성장기 2013~2017

시장 진출 및 경영 안정화

2013
- VirusTotal (Google 社) 협약

2014
- malwares.com 출시

2015
- (주)파이오링크 투자 유치
- K-Global 300 선정

2016
- 악성코드 全생명주기 프로파일링 과제 수주
- 중기청, NAVER 공동 기술 개발
- 독일 R&S 회사 협력
- 국무 총리 표창
  (산업 발전 공로)

2017
- MNX CC 인증 획득
- (주)케이사인 투자 유치
- CTA 가입 승인

도약기 2018~

Global Top-Tier CTI 전문기업 도약

2018
- MAX 출시 및 SE Labs, AV-Comparatives 해외 인증

2020
- 세계 최초 동형암호 기반 악성코드 탐지기술 성공
- 5G 스마트 시티 R&D 과제 수주
- 국방부 프로젝트 수주

2021
- C-ITS R&D 과제 수주
- 국내 최초 한국인터넷진흥원 침해사고, 악성코드 분야 데이터셋 사업 수주
- 과학기술부 장관 표창
  (인텔리전스 핵심 기술 개발 공로)
- ISO 9001:2015 인증 획득
- 산업통상자원부 NET
  (신기술 인증) 획득

2022
- 기술특례상장 기술성 평가 'A' 등급 획득
- 한국인터넷진흥원 위협 프로파일링, 어플리케이션 보안, 능동형보안관제데이터셋사업수주
- 과학기술부 장관 표창
  (사이버 위협 정보 최다 공유 공로)
- 산업통상자원부 NET
  (신기술 인증) 획득

2023
- 코스닥시장 기술특례상장

03 Platform 및 솔루션 소개

CTI Platform malwares.com 중심으로 MDX, MNX, MAX 등 다양한 솔루션 제공

서비스

CTI Platform
malwares.com™

사이버 위협 인텔리전스 제공 서비스

- 위협 정보 실시간 분석 및 제공
- 인공지능, 빅데이터 기술 등을 활용하여 정확도 높은 분석 정보 제공
- 공격그룹, 공격기법 등 차원 높은 사이버 위협 인텔리전스 제공

솔루션

MDX

다양한 전자문서 or 비실행형 파일의 APT 공격에 사용되는 인공지능 기반 제로데이 공격 탐지 솔루션

- 사내 업무용 시스템과 연동하여 APT 공격에 대응

MNX

IT/OT 네트워크 모니터링을 통한 자산 가시성 확보 및 인공지능 기술을 활용한 위협징후 식별 솔루션

- 네트워크 구간 상에서 전달되는 파일에 대한 위험을 조기 식별하여 대량 확산 방지

MAX

인공지능 기반 안티바이러스(스마트백신) 솔루션

- 사용자 PC 및 모바일 기기에 설치되어 직접 위협을 식별하고 대응

Business Model

API

- 기존 보안 제품 및 다양한 서비스와 연계 및 연동하여 자동 분석 체계 구축

데이터셋

- 공격그룹, 공격기법, 랜섬웨어, 악성코드 등 既분석 된 사이버 위협 인텔리전스 데이터 제공

Feed

- 수집되고 분석된 다양한 분석 정보들 중 고객사가 필요로 하는 위협 정보 역제공

Intelligence

- 연관 관계 분석
- 공격자 그룹 식별 및 자동 탐지 패턴 생성
- 머신러닝 기반 악성코드 탐지
- 악성코드 프로파일링을 통한 추적

04 R&D 인프라

**차별화된 기술 경쟁력 확보를 위한 R&D 인력에 대한 투자(전체 84% 비중),
기술 특허 및 NET(신기술 인증) 등 다양한 지적재산권 다수 확보**

개발자 및 엔지니어 인력

전문 개발 인력

총 인원(38명)의
84%
(2023년 상반기 기준)

특고급 개발자 비중
34%
(2023년 상반기 기준)

지적재산권 현황

특허권 저작권

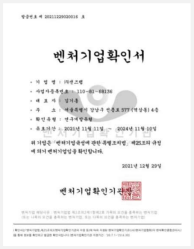
등록특허	출원특허	전체특허
48건	47건	95건
미국 1건 일본 2건	미국 20건 PCT 2건	해외 25건

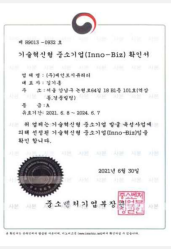
저작권 29건

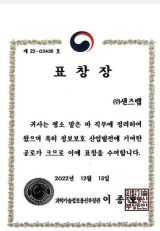
전문 인증 및 수상

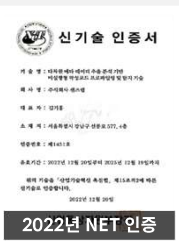
인증 11건

수상 8건









NET 인증[1)] 신기술 국가 인증 제도

※주1) 신기술(NET) 인증은 국내에서 최초로 개발되거나 기존 기술을 혁신적으로 개선해 상용화와 기술 거래를 촉진한 우수 기술을 대상으로 부여

SANDS Lab

CHAPTER

II Investment Highlights

01 ▪ CTI 1st Mover, “SANDS Lab”

02 ▪ 글로벌 최고 수준의 Big Data 수집/분석 역량

03 ▪ 핵심 기술 바탕 신속/정확한 사이버 위협 탐지

04 ▪ 경쟁사 대비 독보적 비교우위

05 ▪ CTA 가입을 통해 검증된 기술력

06 ▪ 고객사 Reference 확보

01 CTI 1st Mover, "SANDS Lab"

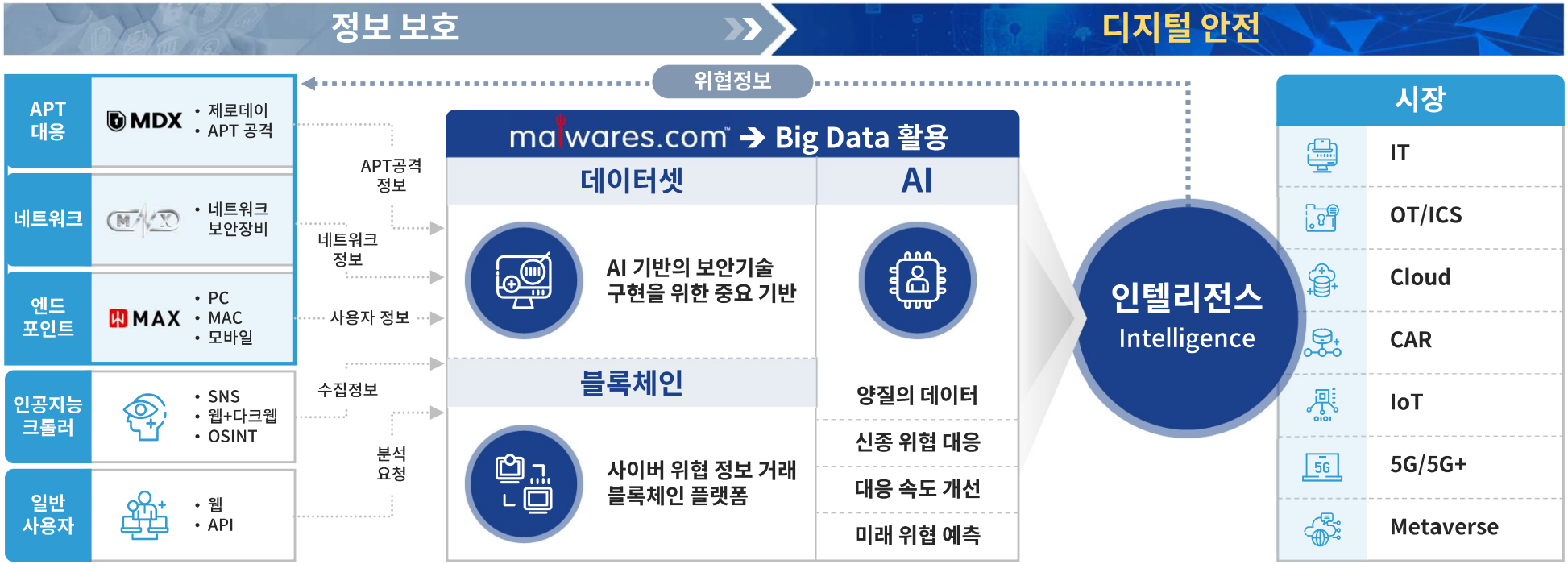
국내 CTI 1st Mover로서 디지털 안전을 위한 차별화된 사이버 보안 관련 비즈니스 모델 보유

국내최초

2015년	2018년	2020년	2021년	2022년
인텔리전스 퍼블릭 서비스 런칭	머신러닝 기반 안티 바이러스	동형 암호 기반 악성코드 분석 기술 확보	바이너리 역공학 기반 공격자 프로파일링 기술 개발 및 NET 인증	다차원 메타데이터 추출 분석 기반 비실행형 악성코드 프로파일링 및 탐지 기술 개발

국내 유일 2년 연속 보안 분야 NET 인증

미래기술을 활용한 차별화 된 CTI



02 글로벌 최고 수준의 Big Data 수집/분석 역량

분석 데이터 수량, 위협 정보 수량, 수집량 등 압도적인 Big Data 확보

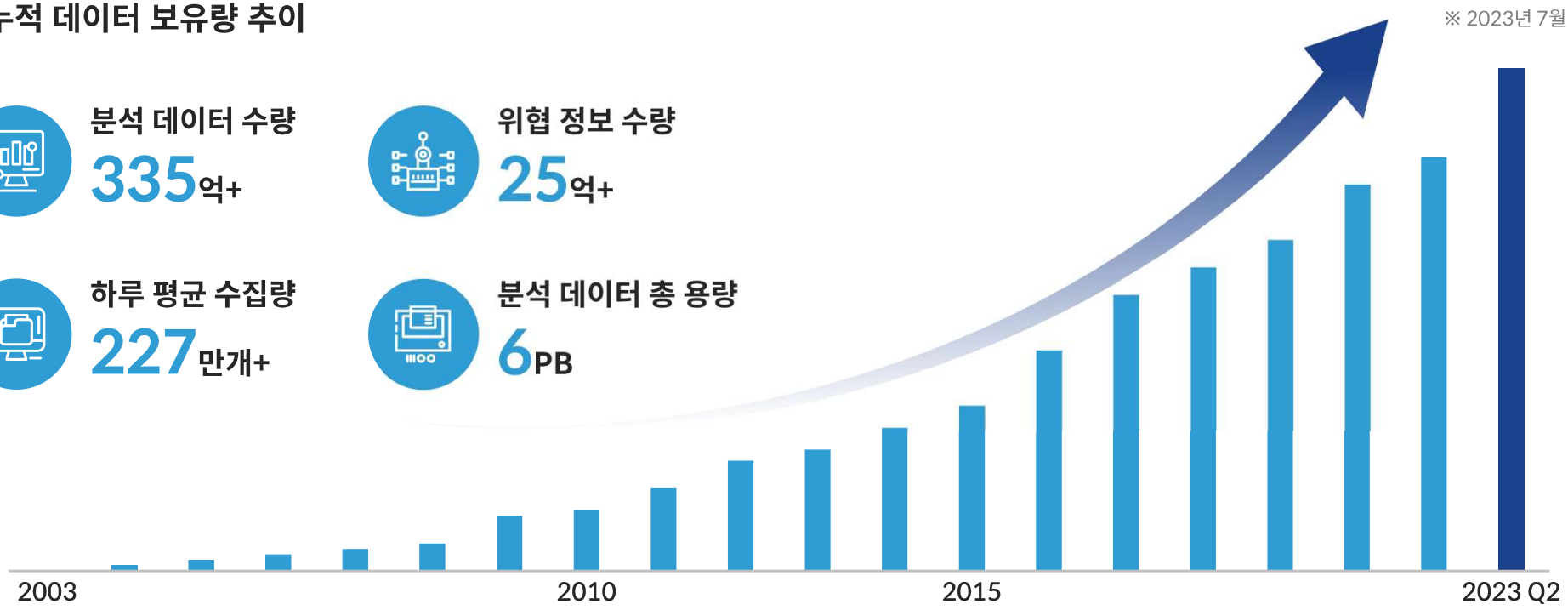
malwares.com™ = AI 기반의 사이버 위협 분석 및 하이퍼 인텔리전스 제공 플랫폼

- 위협 수집 및 분석 기술
- 인공지능 기술
- 프로파일링 기술
- 연관관계 추적 기술
- 빅데이터 플랫폼 기술

누적 데이터 보유량 추이

※ 2023년 7월 기준

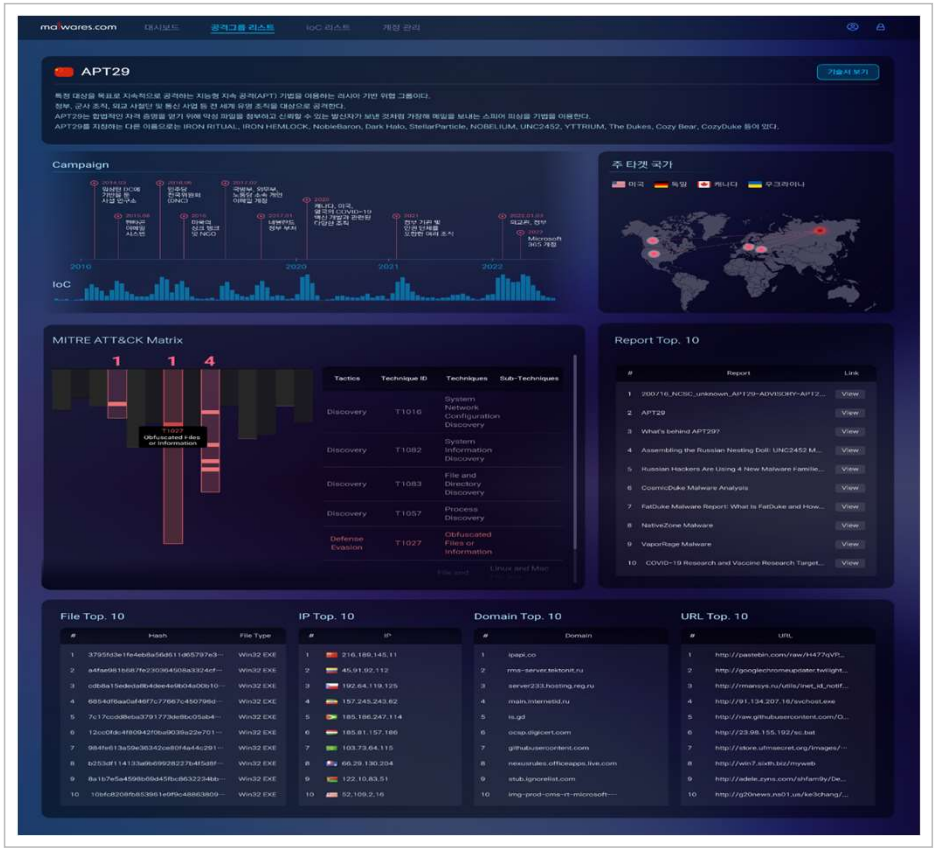
- 분석 데이터 수량: 335억+
- 위협 정보 수량: 25억+
- 하루 평균 수집량: 227만개+
- 분석 데이터 총 용량: 6PB

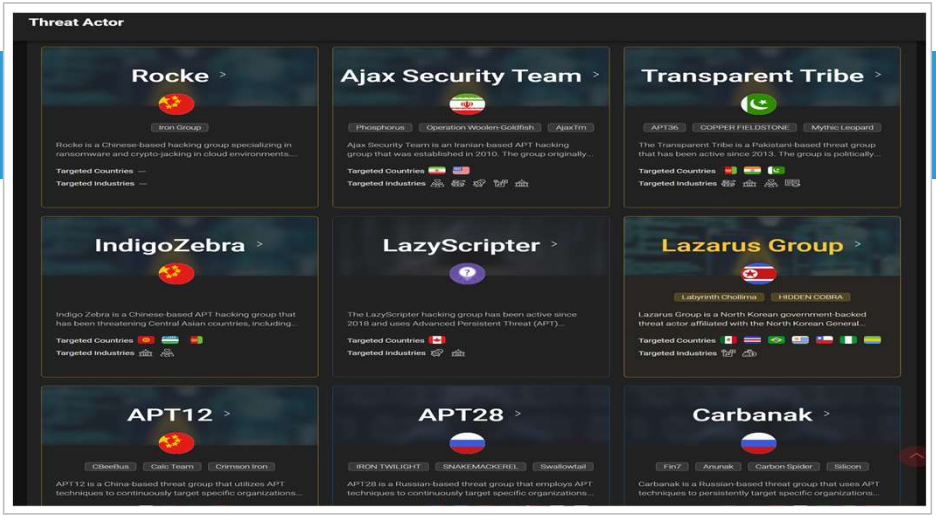


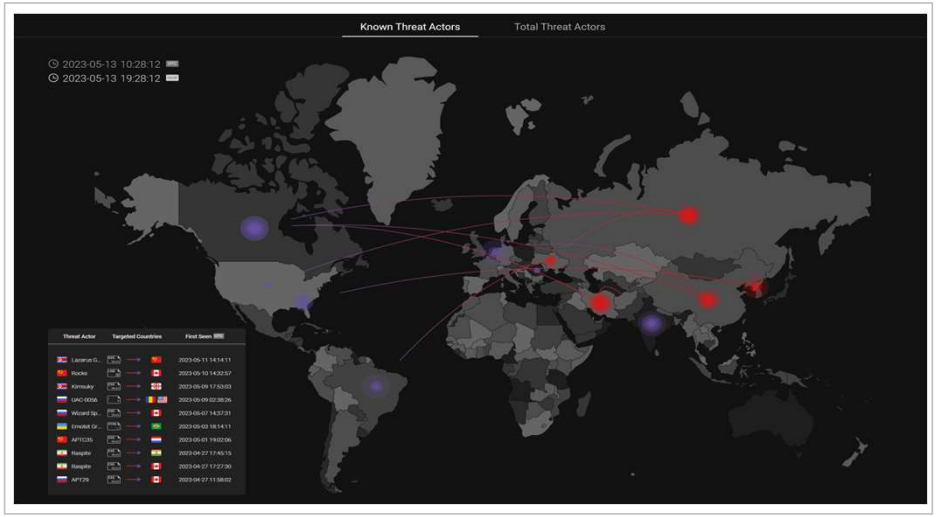
02 글로벌 최고 수준의 Big Data 수집/분석 역량

全세계에서 현재에도 활동중인 사이버 공격 그룹 에 대한 실시간 추적과
공격 기법, 공격에 사용된 서버정보 등을 실시간 분석하여 고객이 대응할 수 있는 정보 제공

샌즈랩 Intelligence



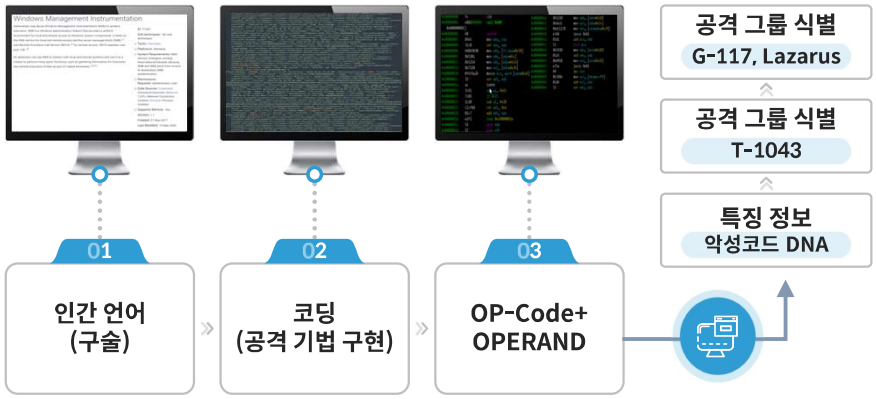




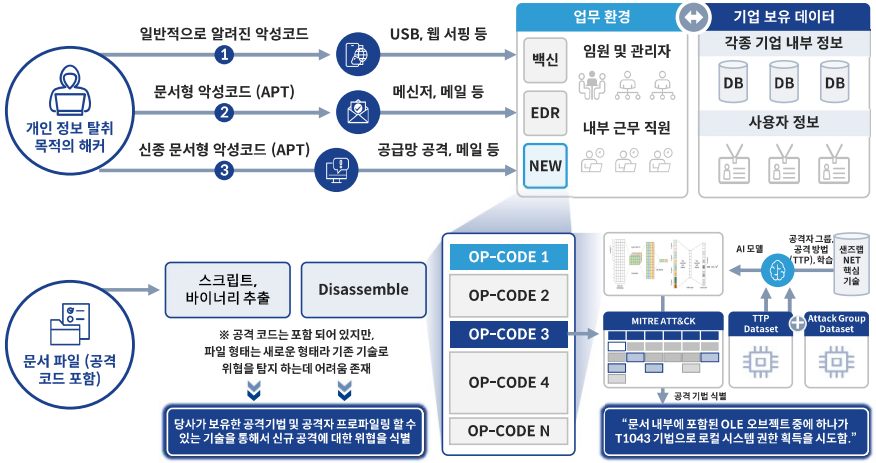
03 핵심 기술 바탕 신속/정확한 사이버 위협 탐지

자체 개발 프로파일링 기술 기반 공격자 그룹 자동 식별 → 분석 시간 단축으로 고객사 효율 극대화

바이너리 역공학 기반 공격자 프로파일링 기술



다차원 메타데이터 추출 분석 기반 비실행형 악성코드 프로파일링 및 탐지 기술



기존 공격 기법, 공격자 그룹 식별	vs	신기술 기반 공격 기법, 공격자 그룹 식별
5 일	99 % 단축	10 분

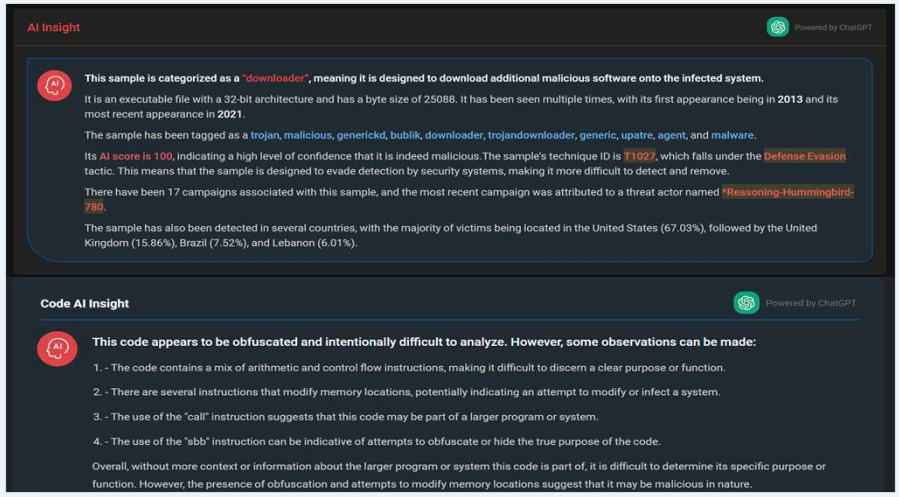
고객사 Benefit

- 신속,정확한 판단
- 리소스 활용 극대화
- 비용 절감

03 핵심 기술 바탕 신속/정확한 사이버 위협 탐지

생성형 AI 기술을 이용한 사이버 위협 인텔리전스 활용성 극대화 → 자연어 기반의 위협 설명을 통한 이해력 강화

차별기능	내 용
공격기법 식별	• 공격기법별 사용되는 코드 특징 추출 및 빅데이터화 • 빅데이터에 의해 학습된 인공지능 모델 • 프로파일링 기술을 통해 악성코드의 특징 추출
공격그룹 식별	• 기존 발견된 악성코드에서 발견된 코드 특징 연관성 추적 • 그룹별 주 사용 공격기법을 식별하여 빅데이터화 • 빅데이터 내 연관 정보 기반 공격그룹 식별



인사이트 예시

01 북한 Kimsuky 공격그룹이 악성 행위를 수행하기 위해 주로 사용하는 공격기법과 패턴

02 탐지 우회를 하기 위해서 주로 사용되는 T-ID 기법과 관련된 공격 방법

03 TA505 공격그룹의 활동 기간에 대한 추세

04 특정 사회 이슈 키워드를 이용한 국내 정부 기관 대상의 APT 공격량 급증

05 특정 기업이 보유한 지적 재산 (설계, 제조 등) 유출을 위한 중국, 베트남에서 APT 공격 수행

04 경쟁사 대비 독보적 비교우위 ① Platform

BigData, AI 등 차세대 기술과 접목한 프로파일링 新기술 바탕의
사이버 보안 위협에 능동적 대응이 가능한 글로벌 수준 최고의 인텔리전스 플랫폼

malwares.com 비교우위

국내 1위, 아시아 1위
(방문자, API 쿼리 수, 데이터 보유량 기준)

매일 227만개 이상 파일, 25억개 이상 위협정보
335억개 이상 프로파일링 정보 제공

매일 103,000 페이지뷰,
평균 3,700만 API 쿼리 처리

자체 개발 AI 모델로 악성코드
프로파일링 정보 제공

MITRE ATT&CK TPP 모델 기반 T-ID
공격기법, 공격자 그룹 정보 제공

기능분류		malwares.com	글로벌 경쟁사 G社
수집 및 검색	서비스 형태	공개/고객 전용	공개/고객 전용
	1일 수집량	평균 약 200만개	평균 약 300만개
	분석 가능 파일 크기	2GB	650MB
파일 분석	리얼 환경 동적 분석 기술	O	X
	머신러닝 기반 악성 분석	O	X
	머신러닝 기반 악성코드 분류	O	X
	STIX포맷 인터페이스 제공	O	X
프로 파일링	프로파일링 정보 제공	O	X
	공격 그룹 정보 제공	O	X
	공격 그룹 클러스터링 정보 제공	O	X
	공격 기법 정보 제공	O	X
편의기능	Feed 기능	O	O
	API	O	O
	추가 인텔리전스 보고서 제공	O	△

04 경쟁사 대비 독보적 비교우위 ① Platform

BigData, AI 등 차세대 기술과 접목한 프로파일링 新기술 바탕의
사이버 보안 위협에 능동적 대응이 가능한 글로벌 수준 최고의 인텔리전스 플랫폼

malwares.com™ 비교우위

	malwares.com™	글로벌 M 社	글로벌 C 社
① 공격 그룹 (Known)	**510여개**	210여개	370여개
② 공격 그룹 (Unknown)	**14만개**	10만개	15만개
③ 자동화	**자동화 + AI**	자동화 + 분석가	자동화 + AI + 분석가
④ 분석 대응	**없음**	티켓 (30개)	티켓 (15개)
⑤ API	**제공**	제공	제공
⑥ 제품 (솔루션)	**MNX, MDX 연동**	없음	XDR 제품 있음
⑦ 고객사	**80여개**	8,000개	15,000개
⑧ 협력사	**구축중**	100여개	300여개

04 경쟁사 대비 독보적 비교우위 ② 솔루션

18년 간 축적된 노하우 및 탁월한 기술력을 통해 신속·신뢰할 수 있는
정확한 탐지, 대규모 빅데이터 수집 역량 등 제품 경쟁력으로 연결

MDX 비교우위

문서형 악성코드 평균 탐지율 **99.4%**

최소 **24**시간 최대 **180**시간 빠른 탐지

민간전자문서 유통 시스템 내부 검증 결과 탐지율 **95.9%**

기능분류		MDX	해외 A社	국내 B社	국내 C社
기반 기술	비실행형 파일 분해 검사	O	O	O	O
	AI 기반 분석	O	X	X	X
	디스어셈블 분석	O	X	O	X
	지원 파일 종류	42종	17종	12종	9종
	제로데이 공격 탐지	O	X	△	X
	분석 시간	3~5초	30초	12초	1분
	운영 방법	소프트웨어, 클라우드, 자체장비	소프트웨어	자체장비	소프트웨어, 자체장비
인텔리전스	공격기법 정보 제공	O	X	X	X
	공격자 정보 제공	O	X	X	X
	인텔리전스 연동	O	O	△	X

MNX 비교우위

DPDK 기반 **100**Gpbs 네트워크 트래픽 무손실 수집기능

경쟁사 대비 2배 큰 파일 수집 가능 최대 **200** 메가 경쟁사 평균 64 메가

380개가 넘는 IT/OT **L7프로토콜** 식별

기능분류		MNX	해외 A社	해외 B社	국내 C社
수집	DPDK	O	X	X	X
	DPI	O	X	X	X
	자산식별	O	X	X	X
식별	어플리케이션	500종	40종	35종	65종
	프로토콜	380종	12종	7종	10종
	OT 프로토콜지원	O	별도 장비	X	X
분석	파일 분석	O	O	O	O
	이상 징후 분석	O	△	O	△
	위협 설명	O	△	△	X
기록	PCAP 보관 및 분석	O(90일)	X	X	X
	메타데이터 추출	O	O	X	X

05 CTA 가입을 통해 검증된 기술력

전세계 유수의 보안 업체들로 구성된 CTA 가입으로 글로벌에서 인정받은 CTI 역량

What is CTA (Cyber Threat Alliance) ?

글로벌 사이버 보안 업체들 간
사이버 보안 위협 정보를 교류하기 위한 얼라이언스

Charter Members

- CHECK POINT
- CISCO
- FORTINET
- paloalto NETWORKS

Affiliate Members

avast	NEC	SK 쉴더스
cloudbric	NTT	SOPHOS
DRAGOS	SANDS Lab	Symantec
JUNIPER NETWORKS	RAPID7	TENTRIS
McAfee	Scitum	Telefónica Tech
MORPHISEC	Security Scorecard	verizon

“ 글로벌 보안 업체에 당사 기술력 입증 ”

» 글로벌 수준의 인텔리전스 퀄리티 입증 보안 업체에게 데이터 제공 中, 상위권 랭킹

05 CTA 가입을 통해 검증된 기술력

2023년 8월

Camp David Summit (한,미,일) 에서 사이버 보안 위협 정보 공유 및 관련 실무 협의 중요성 강조

AUGUST 18, 2023

The Spirit of Camp David: Joint Statement of Japan, the Republic of Korea, and the United States

BRIEFING ROOM › STATEMENTS AND RELEASES

Furthermore, we reaffirm our commitment to the complete denuclearization of the Democratic People's Republic of Korea (DPRK) in accordance with

우리는 불법적인 대량살상무기 및 탄도미사일 프로그램에 자금을 지원하는 북한의 불법적인 사이버 활동에 대해 우려를 표명한다. 우리는 북한의 사이버 위협에 대응하고 사이버를 이용한 제재 회피를 차단하기 위해 국제사회를 포함한 협력을 추진하기 위한 새로운 3국 워킹 그룹을 설립할 것을 발표한다.

actions that pose a grave threat to peace and security on the Korean Peninsula and beyond. We express concern regarding the DPRK's illicit cyber activities that fund its unlawful WMD and ballistic missile programs. We announce the establishment of a new trilateral working group to drive our cooperation, including with the international community, to combat DPRK cyber threats and block its cyber-enabled sanctions evasion. Japan, the ROK, and the United States remain committed to reestablishing dialogue with the DPRK with no preconditions. We a
respect for human r
the immediate resol
unrepatriated prisor
Audacious Initiative
peace.

- **Trilateral Working Group on DPRK Cyber Activities:** The United States,

북한 사이버 활동에 관한 3국 워킹 그룹: 미국, 일본, 대한민국은 북한의 불법 수익 창출과 악의적인 사이버 활동에 대응하기 위한 노력을 조율하기 위해 미국, 일본, 대한민국 정부 기관으로 구성된 새로운 3자 북한 사이버 활동 실무그룹을 설립하기로 결정했습니다. 실무그룹은 정보 공유, 북한의 암호화폐 사용, 도난, 세탁에 대한 대응 조율, 외교 및 산업계 참여를 통한 북한의 수익 창출을 위한 IT 노동자 활용 문제 해결, 악의적인 사이버 행위자 활동 방해에 중점을 둘 것입니다.

engagement; and disrupting malicious cyber actor operations.

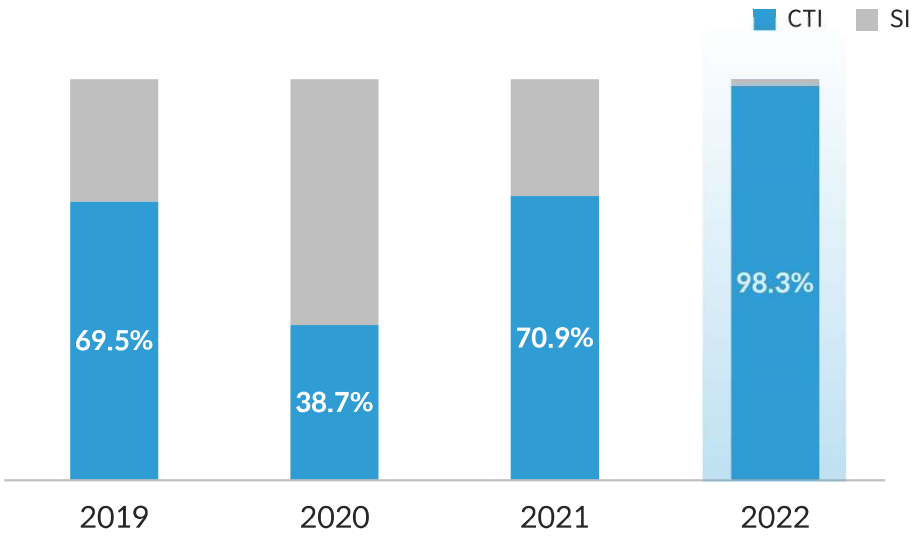
KISA 한국인터넷진흥원 + 대한민국 국방부 Ministry of National Defense + CYBER THREAT ALLIANCE

SANDS Lab CTI (위협 정보 공유)

06 고객사 Reference 확보

보안업체, 공공, 민간, 금융 등 다양한 고객사 보유 및 CTI 중심의 매출 구조 확보

매출 비중 추이



CTI(데이터셋) 수주 현황

2020년
- 악성코드 및 앱 데이터 자동 수집 시스템 개발
- 보안산업 데이터셋 가공 및 공유 시스템 개발
- PC 원격 보안점검 운영

2021년
- 사이버보안 인공지능 데이터셋 (악성코드 분야) 구축
- 사이버보안 인공지능 데이터셋 (침해사고 분야) 구축
- 정보보호 데이터셋 가공 모듈 개발 및 공유 플랫폼 연계시스템 개선 용역
- 내PC돌보미 서비스 운영 (위협 분석 및 인텔리전스 점검 도구 제공)

2022년
- 사이버보안 인공지능 데이터셋 (위협 프로파일링 분야) 구축
- 사이버보안 인공지능 데이터셋 (능동형 보안관제 분야) 구축
- 사이버보안 인공지능 데이터셋 (어플리케이션 보안 분야) 구축

2023년
- 사이버보안 인공지능 데이터셋 최신화 및 고도화 구축

총, 누적 금액 10,588백만원

부문별 고객사

보안업체	INZENT	SOMMA	S2G	NSHC	LSIT 엘에스정보기술(주)	nurilab	금융	kakaobank	CashBucks	
	FINSECURITY	ZeinSoft	ESTsecurity	ATEK	IT NOMADS			농협정보시스템		
공공	중앙선거관리위원회	국토교통부	NSR 국가보안기술연구소		민간	HYUNDAI AutoEver	NEXON	MT COMMUNICATION	SC&S	
	KISA 한국인터넷진흥원	대한민국 국방부	TS 한국교통안전공단			solideo (주)솔리데오시스템즈	POLARIS OFFICE	고려대학교 KOREA UNIVERSITY	JOINTREE	

SANDS Lab

CHAPTER

III Growth Strategy

01 ▪ 케이사인과의 Synergy

02 ▪ 매출 확대 본격화

03 ▪ 클라우드 데이터센터 구축

04 ▪ 신사업 추진

05 ▪ 해외 시장 진출

06 ▪ Vision

01 케이사인과의 Synergy

母회사 케이사인과의 시너지 기반 공공, 일반분야 시장지배력 확대

공공, 일반분야 Target으로 매출 확대 본격화

공공분야
(정부 부처, 시도 및 지자체, 주요 관공서 등)

일반분야 (금융, IT, SI 등)

기술 Synergy	영업 Synergy	전략 Synergy
차세대 보안 기술 (BAS 등) 공동 개발로 시장 공략 박차	케이사인 기존 고객사 활용을 통한 시장 공략	임원들간의 지속적인 전략 교류를 통해 시장 지배력 강화

SANDS Lab | CTI, 보안 솔루션 전문 그룹사 | KSIGN (주) 케이사인

세계 수준의 CTI 전문 기업 + 국내 Top-tier 보안 솔루션 전문 기업

02 매출 확대 본격화 ❶ 공공 분야

사이버 보안을 위한 정부의 적극적인 정책 바탕 공공분야 사업 확대

정부의 사이버 보안 육성 정책 확대

K-사이버 방역 추진 전략

중점 추진과제	주요 내용
디지털 안심 국가기반 구축	• 사이버보안 대응체계 고도화
	• 수요자 중심 디지털보안 역량 강화
보안 패러다임 변화 대응 강화	• 차세대 융합보안 기반 확충
	• 신종 보안위협 및 AI 기반 대응 강화
정보보호산업 육성 기반 확충	• 디지털보안 핵심기술 역량 확보
	• 정보보호산업 성장 지원 강화
	• 디지털보안 혁신인재 양성
	• 디지털보안 법제도 정비

2023년까지 총 **6,700**억원 투자

12대 국가전략기술 선정 및 육성

12대 전략기술		• 사이버보안
로드맵	단기(~5년)	• AI기반 보안관제 · 자동대응 등 원천기술 개발 • ICT 장비 · SW취약점 신속 분석 · 대응 기술
	중장기(5~10년)	• 미래 디지털 인프라 사이버 보안체계 자립화
세부 중점 기술		• 데이터 · AI보안 • 네트워크 · 클라우드 보안 • 디지털 취약점 분석 · 대응(공급망 보안) • 신산업 · 가상융합 보안

2022년 12대 국가전략기술로 사이버보안 선정 및 향후 적극적 육성

※자료: 과학기술정보통신부

공공분야 사업 추진 현황

A사	• 데이터셋 구축 사업 및 유지보수 • 사이버 위협 통합 탐지 체계 구축 • 빅데이터 기반의 해킹 사고 추적 및 분석 시스템 구축 • 메타버스 기반 사이버 위협 예측, 분석 통합 플랫폼 구축
B사	• 차세대 자동차 정보 관리 시스템 • V2X 국가자율협력주행 인증관리체계 구축
C사	• 차세대 지방행정공통시스템-클라우드 전환 보안 분야
D사	• K-에듀 통합플랫폼 구축-클라우드 보안/ 네트워크 APT
E사	• 건축서비스산업 정보체계 구축-클라우드 네트워크 보안

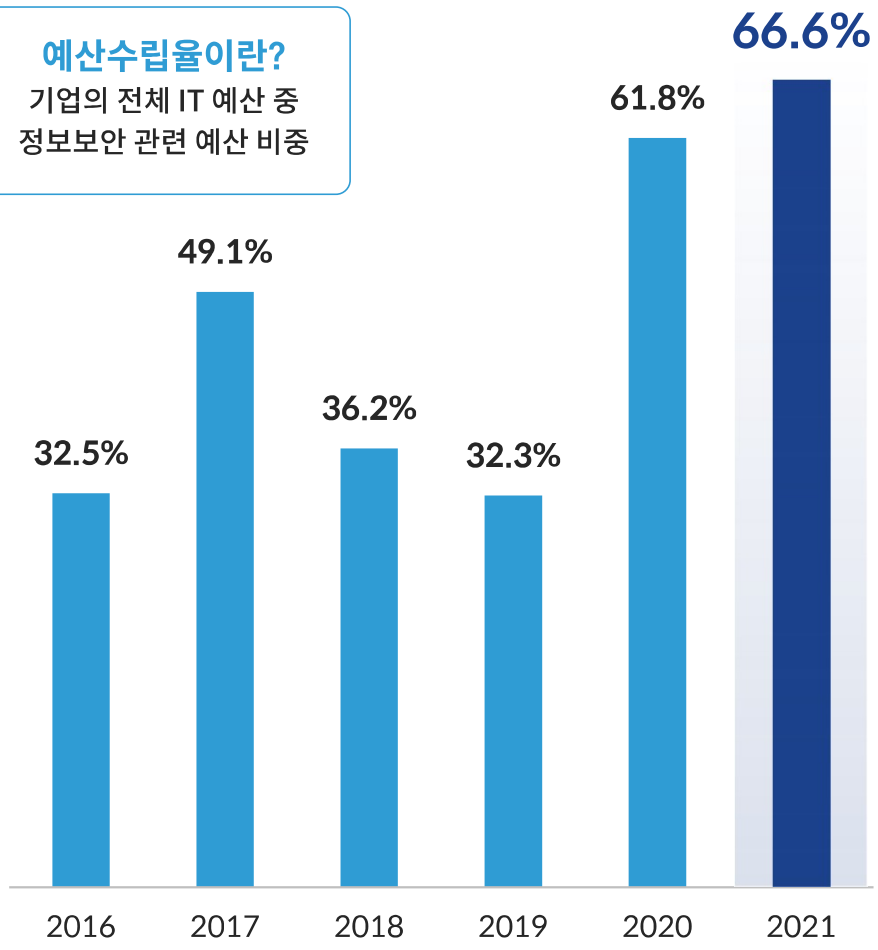
정부 부처, 시도 및 지자체, 주요 관공서 등
총, **647**개 기관 영업 진행

02 매출 확대 본격화 ② 일반 분야

기 확보된 레퍼런스 적극 활용해 금융, IT, SI 등 다양한 분야로 시장 확대

기업의 정보보안 예산수립율

예산수립율이란?
기업의 전체 IT 예산 중
정보보안 관련 예산 비중



일반(금융/IT/SI 등) 사업 추진 현황

금융

최신 보안 기술 도입을 통해 높은 수준의
보안 시스템 구축 Needs 대응

주요 기업 Reference 활용

NEXON HYUNDAI AutoEver kakaobank

파트너사 통해
금융 및 민간기업 영업망 확보

일반 (IT/SI 등)

- 보안관련 기업 12개사와 협약 체결 및 11개사와 논의 진행 중
- ERP 3개사 협약 논의 중

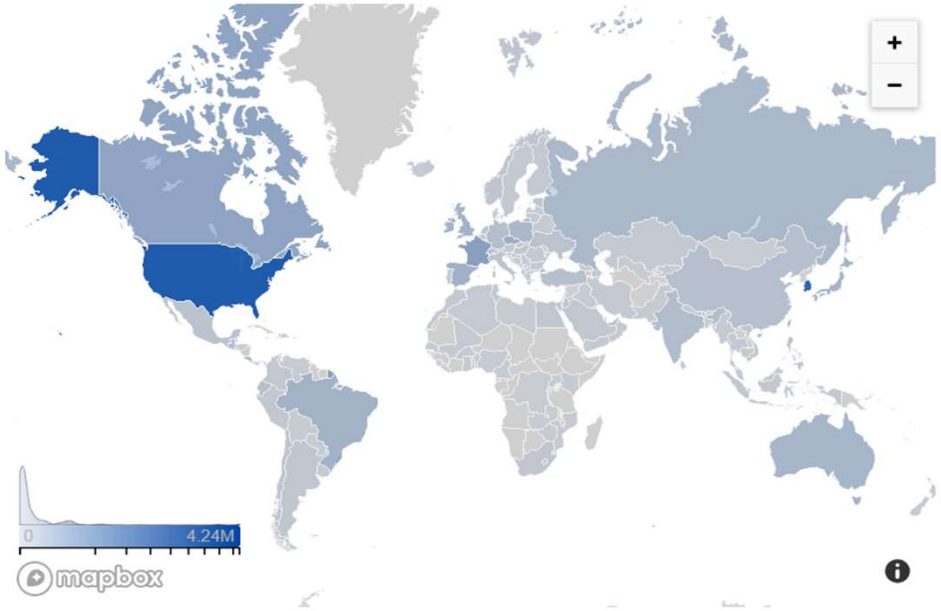
DOUZONE 더존비즈온 영림원소프트랩 (주)이노가드

- 헬스케어 2개사 협약 논의 중

ezCaretech INFINITT Healthcare

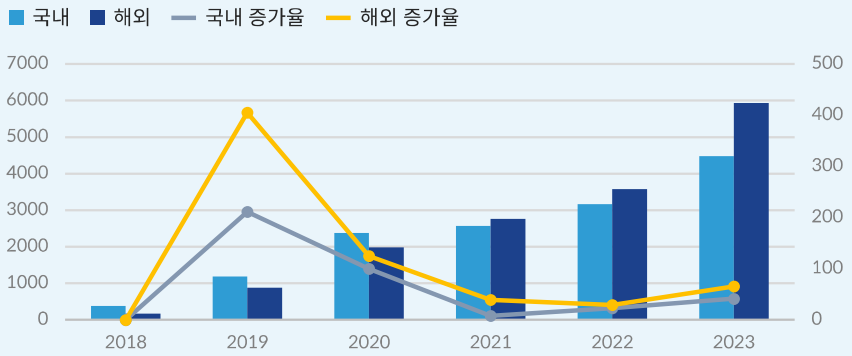
02 매출 확대 본격화 ❸ malwares.com 글로벌 사용량 급증

malwares.com 글로벌 사용량 및 실사용자, API 모든 수치들이 성장 추세

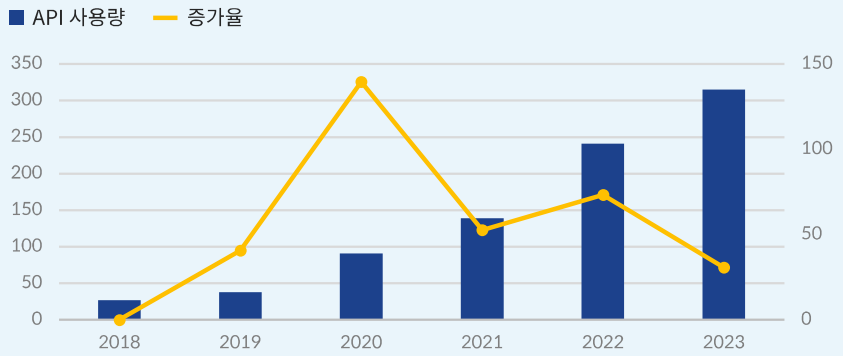


1	United States	4.24M
2	Korea, South	3.47M
3	France	632.04k
4	Canada	532.23k
5	Czech Republic	321.91k
6	Spain	249.52k
7	Taiwan	245.03k
8	United Kingdom	224.55k
9	Brazil	223.75k
10	Japan	214.31k

malwares.com 사용자 증가



API 사용량 증가



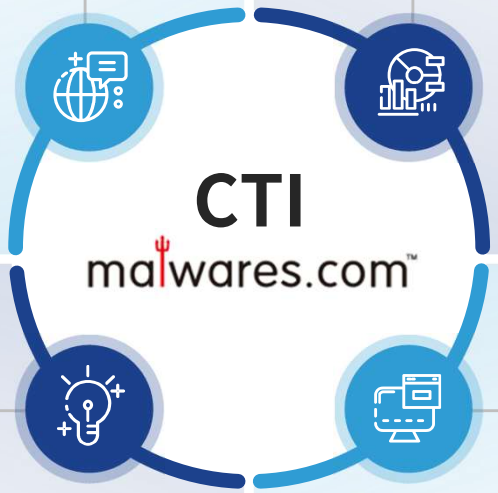
02 매출 확대 본격화 ④ 국내 사업 활성화

01 Feed

- **K기관, S금융사, K금융사, H기업 등 당사 보유한 위협 정보에 대해서 역제공 받는 서비스에 대해서 검토 및 BMT 진행 중 (공공, 금융, 일반 포함)**
- 국내외 주요 보안 관제, 솔루션 업체와 연동하여 위협 정보 역제공을 통한 역추적 기능 개발 진행

03 Dataset

- **한국인터넷진흥원 50억 규모 2023년 사이버보안 분야 인공지능 데이터셋 구축 사업 수주 (23년 6월, 당사 수주 금액 33억)**
- 데이터셋 실증 사업 사전 신청 업체 (S社, H기관 등 100개 이상 확보) → 추후 당사 고객으로 전환 가능
- 과학기술정보통신부 사이버 보안분야 생성형 AI 개발 사업 연동 → 당사 구축 데이터셋을 이용한 차세대 사업 진행



02 API

- **신규 버전 malwares.com 런칭 (23년 7월)**
- **malwares.com 순사용자 증가 (런칭 이후 8% 증가)**
  한국인터넷진흥원 사이버보안 분야 데이터셋 실증 사업과 연계하여 70여개 넘는 기업 사용자 사전 확보
- **ChatGPT 연동 API, AI API 등 신규 API 8종 개발**
- 파트너 API 개발을 통해 국내외 주요 보안 솔루션들과 분석 정보 공유 및 연동
- **유료 결제 서비스 시작 (글로벌 결제 가능)**
- UI/UX 개선으로 사용자 편의성 확대

04 Intelligence

- **초거대 AI, 생성형 AI 와 연동한 자연어 기반의 위협 인텔리전스 서비스 시작 (국내외 특허 30여건 출원)**
- AVAR, VirusBulletin 등 국제 컨퍼런스에 당사가 보유한 데이터와 인공지능 기술을 통한 추적 사례 발표를 통한 글로벌 진출 바탕 마련
- **가트너, CTA 등 다양한 전문가 집단으로 부터 당사 인텔리전스 서비스의 효과성 증빙 (한미일 정상 회담 등)**
- 당사 인텔리전스와 연동된 MNX, MDX 솔루션의 클라우드 서비스 시장 진출을 통해 글로벌 저변 확대 (진행 중)

03 클라우드 데이터 센터 구축

당사 주력 사업인 CTI의 안정적인 서비스 제공을 위해 필수적인 자체 클라우드 데이터 센터 구축

클라우드 데이터 센터 건립 계획

착공일	2023년 하반기
위치	(미정)
투자 금액	약, 130억원 (공모자금 활용)
준공 예정일	2025년 하반기
활용 방안	• 안정적인 서비스 제공 • 글로벌 전용 회선을 통한 위협 정보 제공

투자 세부 내역

(단위: 백만원)

구분	내역		금액
시설	인텔리전스 클라우드 센터 및 지원시설 보증금	공용면적 1,155㎡ 공용면적 198㎡	3,850
	전용 네트워 구성 및 모니터링 도구	-	700
	비상발전 시스템	-	500
	온도 및 내부환경 관리시스템	-	300
구성 장비	오브젝트 스토리지 5PB	5대	4,750
	데이터베이스 클러스터링 서버	50대	1,500
	분석 모듈 가상화 서버	3대	900
기타	기타관리비품 및 유지보수	-	500
합계			13,000

2023	2024	2025	
1단계	2단계	3단계	4단계
▪ 자체 스토리지 구축 ▪ 클라우드 서비스 정리	▪ 고전력 IDC 이전 ▪ 고성능 장비 입고	▪ 대기업 IDC 임대 활용 ▪ 회선 서비스 증가	▪ 클라우드 데이터센터 구축 ▪ 글로벌 직접 회선 구축

04 신사업 추진 ❶ 스마트시티 플랫폼&C-ITS 인프라 보안

5G 기반 스마트시티 및 C-ITS 보안 강화 기술 개발

5G 기반 스마트시티 플랫폼

스마트시티 보안 ISSUE

01	02	03
IoT 기기 보안성 미고려	365일 24시간 작동	외부 공격에 취약

5G 기반 스마트 시티 보안 강화 플랫폼 개발

IoT 장비 — 차세대 스마트허브 기술 → 5G 네트워크

⊕

스마트허브 관리 운영 서버 기술

서비스 개발 진행

C-ITS 인프라 보안 강화 기술 개발

인프라 보안 강화 ISSUE

01	02	03
인프라 보안성 강화 중요성 확대	비통제 모의해킹 위험성	인프라 가상복제 모의해킹 대두

C-ITS 인프라 보안 강화 기술 개발

AI기술 (방어전략수립)

C-ITS Real Infra

상암, 세종시 등 시범 도시 대상으로 수행 중

서비스 개발 진행

가상 환경 시뮬레이션 도구

AI기술을 통한 공격, 방어 자동화 프레임워크

04 신사업 추진 ② BAS(공격 방어 시뮬레이션) 개발

취약점 사전 식별 및 악성코드를 통한 공격 경로 사전 확보를 위한 AI 기반 시뮬레이션 솔루션 개발

모의해킹 현황

공격 대응을 위해 모의 해킹 진행
BUT, 주관성으로 낮은 일관성

Market Needs

- 장기간 지속적인 **수행 가능성**
- 인력의 기술과 **상관없는 일관성**
- 공격 Simulation의 **자동화**

BAS (Breach and Attack Simulation)

Breach and Attack Simulation

전체적인 공격 위협과 단계별로 수행 가능하여
포괄적인 범위의 위협 시뮬레이션을 수행하는 시스템

When?

- 운영되는 보안 솔루션에 대한 일관성을 확보할 경우
- 체계적이며 빈번한 테스트가 필요할 경우
- 사전에 확인 가능한 효과적인 방법론이 필요할 경우

광범위한 컨트롤 및 **자산 테스트 가능**

공격자의 행동과 내부자를 직접적으로 **테스트 가능**

특정 그룹, 특정 악성코드 **시뮬레이션 가능**

보안팀 대응능력 **훈련 가능**

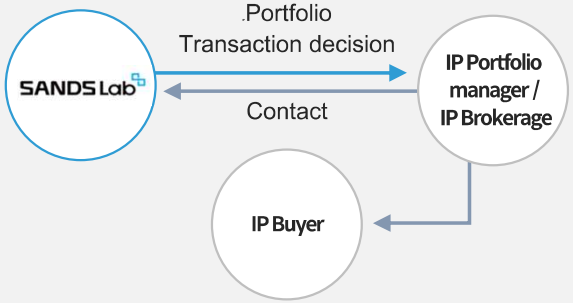
05 해외 시장 진출

기존 업체들과 차별화 된 샌즈랩만의 고유 방식을 통해 Global Market 진입

SANDS Lab

해외 특허 로열티 기반의 **OEM 전략**	클라우드 마켓플레이스를 통한 **글로벌 진출**	malwares.com 웹기반 **글로벌 결제 연동**

특허 기반 기술 로열티



특허 매각 중심의 해외 문화 적극 이용
OEM 라이센싱 전략 → 제품 개발 부담 감소

클라우드 마켓플레이스

Azure aws

23년 2분기 → 23년 3분기 → 23년 4분기 ▶

MDX 판매 / malwares.com 판매 / ... / MNX 판매

MS, Amazon 등
메이저 플랫폼 업체와 협력

malwares.com 상품 결제 페이지 개선

[API 및 데이터셋 상품 제공]

- 제공 서비스 차등화
- 고객 Needs에 따른 패키지 선택 가능
- 쉽고 빠른 결제 서비스

CTA 등 검증된 인텔리전스 제공 현지
법인 설립 부담 최소화, 기술 중심의 사업

RSA

샌즈랩은 2023년 4월 미국 샌프란시스코에서 열린 RSA 2023에 참여하여 글로벌 인텔리전스 전문 업체와 북미 시장 진출, OEM 계약 등 다양한 논의를 진행하였으며 10개가 넘는 기업과 NDA 계약 후 현재 본격적인 데이터 검증, 비즈니스 모델 논의 등을 진행 중임

06 Vision

Global Top Class CTI 기업 도약

매출 Quantum Jump

2025

해외 시장 매출 비중 확대

- 샌즈랩만의 특화된 방식으로 해외 시장 진입
- 클라우드 전환 시대를 통한 마켓플레이스 매출 증대
- 해외 OEM 라이센싱을 통한 기술 영업 기회 창출

2024

클라우드 데이터 센터 구축 및 신사업 기술 개발 완료

- CTI 플랫폼 구축 및 지속적 R&D 기반신기술 개발
- 안정적 글로벌 서비스를 위한 자체 클라우드 데이터 센터 구축
- 차세대 핵심 기술 및 제품 개발 완료

2023

국내 시장 선점 및 성장 발판 본격화

- 데이터셋 실증 사업 통한 공공 및 일반분야 고객 확보
- 코스닥 상장을 통한 경영 투명성 확보 및 홍보를 통한 서비스 및 제품 활성화

SANDS Lab

Appendix

01 ▪ 요약 재무제표

SANDS Lab

01 요약 재무제표

(단위: 백만원)

재무상태표

구분	2020	2021	2022	2023.2Q
유동자산	3,632	6,955	7,454	38,203
비유동자산	1,884	1,043	2,322	3,052
자산총계	5,516	7,998	9,776	41,255
유동부채	1,382	3,068	7,751	1,999
비유동부채	-	62	27	13
부채총계	1,382	3,130	7,778	2,012
자본금	600	1,200	1,200	1,509
자본잉여금	6,227	5,627	5,796	41,814
기타자본항목	-	-	(5,194)	(3,410)
이익잉여금	(2,693)	(1,959)	196	(670)
자본총계	4,134	4,868	1,998	39,243

SANDS Lab

01 요약 재무제표

(단위: 백만원)

손익계산서

구분	2020	2021	2022	2022.2Q	2023.2Q	반기 대비 증감률(%)
영업수익	5,247	5,414	9,299	1,448	1,588	10%
영업비용	5,340	4,925	7,210	2,481	3,461	40%
영업이익	(93)	489	2,089	(1,033)	(1,873)	(81)%
영업외수익	103	71	53	11	393	3,327%
영업외비용	57	14	28	3	113	3,072%
법인세차감전 순이익	(47)	546	2,114	(1,025)	(1,593)	(55)%
당기순이익	(47)	734	2,115	(797)	(866)	9%

23년 7월 1일 이후 수주 확정 매출액 약50억

(한국인터넷진흥원 사이버보안 AI 데이터셋 33억 및 국민연금 10억 계약완료 / 국민연금 추가 사업 10억 진행중)