SANDS Lab

사이버 위협 인텔리전스 전문 기업. 샌즈랩

The #1 Cyber Threat Intelligence

CONTENTS

01 Company History

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

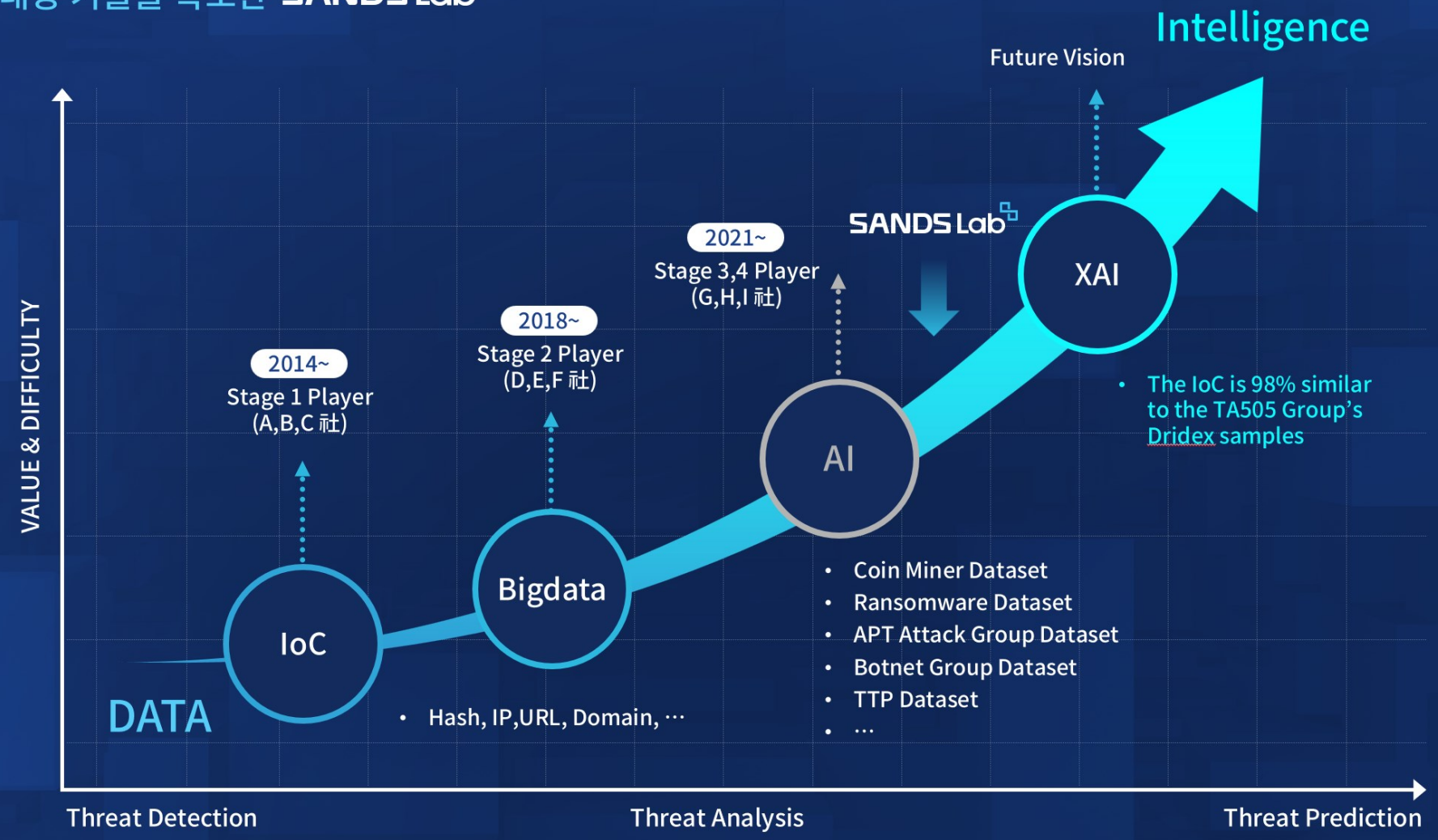
도약기 2018~
Global Top-Tier CTI 전문기업 도약

- **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

SANDS Lab

01 Corporate Identity History

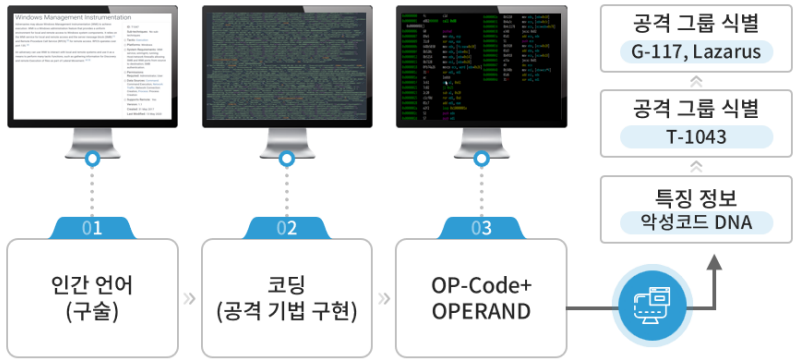
단순 데이터를 넘어, 차별화된 기술력을 기반으로 미래의 사이버 위협 대응 기술을 확보한 SANDS Lab



02 Artificial Intelligence Technology

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

SANDS Lab

02 Big Data Technology

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

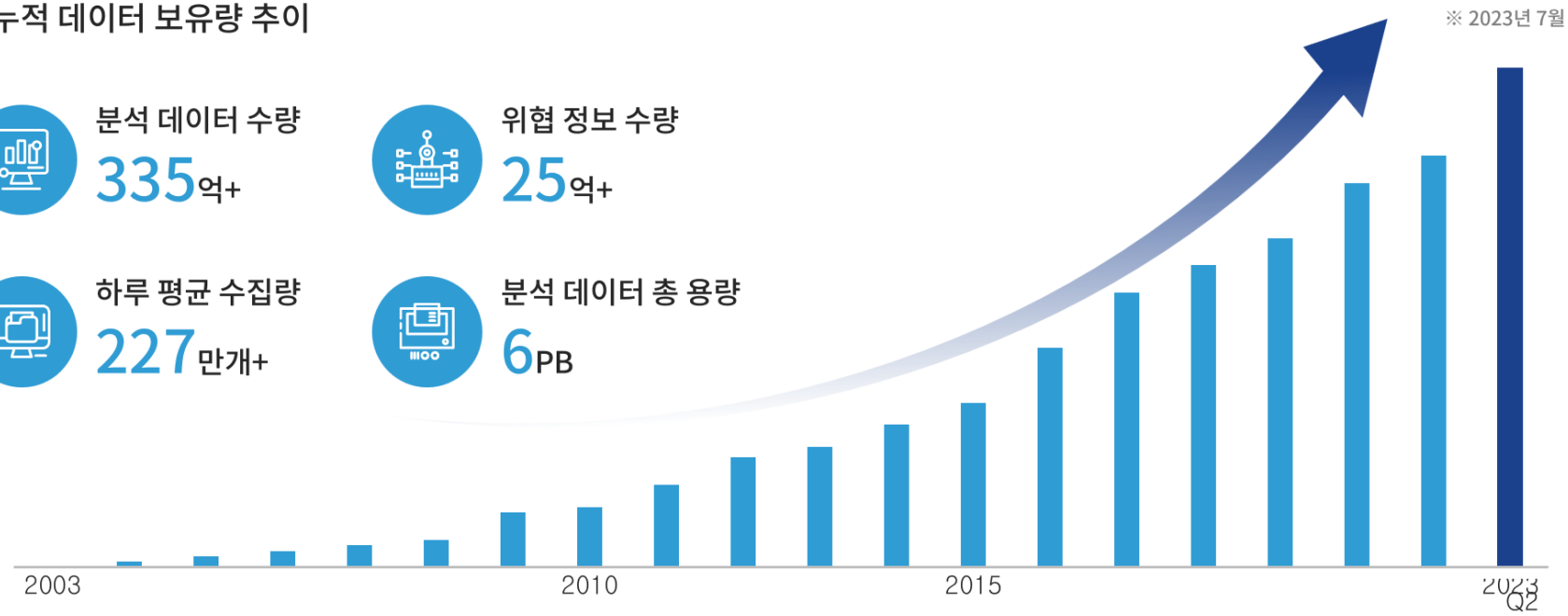
malwares.com™ = AI 기반의 사이버 위협 분석 및 하이퍼 인텔리전스 제공 플랫폼

- 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**



03 Business Overview

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

사이버 위협 인텔리전스 (CTI)

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

03 Business Service

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	△

SANDS Lab

03 Business Service

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 Event CTX 쇼케이스

사전 참가 신청 QR

SANDS Lab