클라우드 기반 사이버 위협 헌팅 플랫폼+

SOMMA

SOMMA

SOMMA

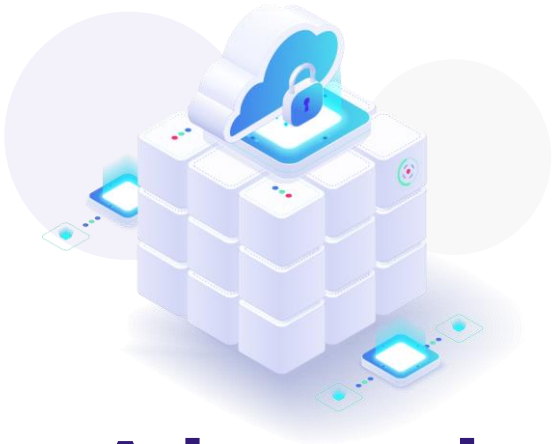
01

Advanced Cyber Threats

Advanced Cyber Threats

SOMMA

전통적인 보안 솔루션을 우회하는 지능형 APT 공격!



Advanced Persistent Threat

Targeted & Zero-day
- 타겟 환경에 특화된 공격 기법 활용
- 알려지지 않은 취약점을 통해 침투

Living Off The Land
- 운영체제에서 제공하는 기본 도구를 활용해 공격 수행
- 알려진 정상 프로그램을 통해 공격 수행

File-less attack
- 디스크에 흔적을 남기지 않고, 메모리상에서 모든 공격을 수행
- Script based attack
- Reflective Loading
- Process hollowing

Supply Chain Attack
- 신뢰 되는 소프트웨어, 하드웨어의 공급과정에 악성코드 등을 삽입
- 악성코드가 감염된 상태로 최종고객에게 배포되는 형태

Traditional Security Model

SOMMA

전통적인 보안 패러다임 (경계의 보안)을 **무력화**


SOMMA
MONSTER
Managed Threat Hunting Platform

MONSTER

공격자의 행위를 추적하고, 알려지지 않은 위협을 찾아냅니다.

고도화된 사이버 위협에 대응하기 위해 데이터 수집, 위협 분석 및 탐지, 추적, 대응까지의 과정을 자동화

01	Threat Hunting에 최적화된 양질의 데이터 셋 확보	02	엔드-포인트 행위 기반 위협 탐지 및 추적	03	사이버 위협 탐지 및 대응에 특화된 보안 플랫폼

Secure Visibility → Behavior Analysis → Detect Threats → Respond Threats → Anomaly Detection → Fully Automated

지속적인 가시성확보

- 위협 분석에 필요한 데이터 확보필수

행위기반 데이터분석

- 행위 및 행위 문맥 기반 상세분석

위협 탐지 & 대응

- 인텔리전스 TTP 기반 위협 행위 탐지
- 비정상 행위 탐지
- AI기반 위협 행위 탐지

자동화

- 반복적이고, 지속적인 위협탐지

MONSTER

Threat Hunting에 필요한 엔드-포인트 행위 데이터 및 휘발성 데이터를 **수집,가시성을 확보합니다.**

수집된 데이터를 위협분석에 **최적화된 형태로 관리하고, 위협분석 및 추적을 자동화합니다.**

Event Collector

(Active Probe) Monster Event Collector

3rd Party Event Logs

Security System

External Intelligence

Analytic Cloud

Collect

Event Cluster

Filter | Normalization

Fast Data Load

LOAD

Big Data Cluster

Monster Data Platform API

Access Control

Threat Analysis Engine

- Intelligence Driven Threat Hunting
- Anomaly Behavior Detection
- TTP Driven Threat Hunting

Realtime Threat Analysis

Continuous Threat Analysis

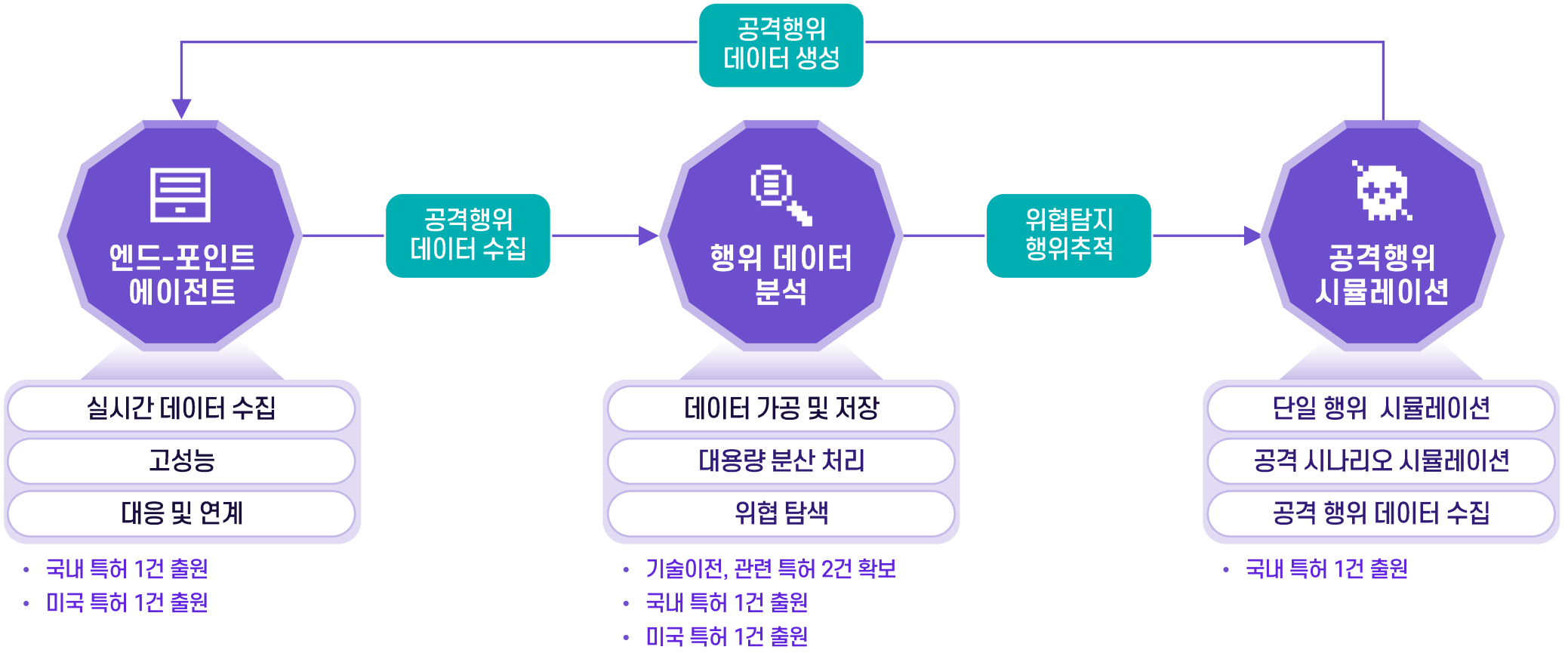
STIX | TAXII

Reference

Alert and Response

MONSTER

Endpoint Visibility – Data Analysis On Cloud – Adversarial Emulation



- 국내 특허 1건 출원
- 미국 특허 1건 출원

- 기술이전, 관련 특허 2건 확보
- 국내 특허 1건 출원
- 미국 특허 1건 출원

- 국내 특허 1건 출원

Core technology of MONSTER

SOMMA

엔드-포인트 에이전트

실시간 데이터 수집

- 시스템의 모든 행위 실시간 모니터링
- 위협분석에 필요한 행위 데이터 수집
- 휘발성 데이터 수집

고성능

- 가벼운 모니터링 엔진
  분당 20만 건 실시간 처리
- 행위 데이터 축약 기술을 통해
  시스템 부하 최소화
- 국내 특허 1건 출원
- 미국 특허 1건 출원

대응 및 연계

- 서버 연동 및 온라인
- 정책으로 네트워크 실시간 제어
- 발생 위협에 신속 대응

솔루션화

ANY-Office

애니 오피스 (원격근무관리 솔루션)

- 원격근무 관리용 솔루션 (2020년 TIPS 프로그램 선정)
- 화이트리스트/블랙리스트 기반 엔드-포인트 제어기능
- 원격근무 단말의 사이버위협 탐지 서비스를 통합한 솔루션
- 기존 엔터프라이즈 솔루션 – 보안 솔루션 연동을 통한 시장 진입 전략

Nanny-On | AhnLab SMB PLACE

DocuONE | OfficeKeeper

비즈니스

- 한국주택토지공사 외주 업체 관리용 시범 도입 (2020년)
- 400 유저규모 추가 도입 예정 (2021년)

LH 한국토지주택공사

- 싱가폴 보안 업체
- 엔드-포인트 모니터링&제어 기술 공급 (2019년)

uppsalasecurity

- AI 학습용 데이터 셋 생성 사업에 활용 (2020년)
- 능동형 허니팟 시스템 구축사업에
  엔드-포인트 모니터링 에이전트 공급 (2020년)

KISA

Core technology of MONSTER

SOMMA

행위 데이터 분석

데이터 가공 및 저장

- 메타데이터 생성/저장
- 데이터 파이프라인 관리

대용량 분산 처리

- Monster Data Platform API
- 독립적인 데이터 접근 API 제공
- 수평 확장 가능한 구조의
- 분산 데이터베이스 지원
- 빅데이터 처리 효율 향상

위협 탐색

- 실시간, 지속적, 반복적 위협 탐색
- 인텔리전스 기반 위협 탐색
- TTP(Tactics Techniques Procedures) 기반 위협 탐색
- Machine Learning/AI 기반 비정상 행위 탐색
- 기술이전, 관련 특허 2건 확보
- 국내 특허 1건 출원
- 미국 특허 1건 출원

기술 고도화

인텔리전스 활용 기술 고도화

- 국가보안 연구소 기술 이전(특허 2건, TTA 표준 1건)
- ㈜세인트 시큐리티, malwares.com 인텔리전스 서비스 협약
- ㈜안랩, 악성코드 데이터 사용 협약

데이터에 기반한 위협 탐지/대응 고도화

- 군 사이버보안 관련 R&D 사업에서 다수 기술력 검증 (2016-현재)
- 한국인터넷 진흥원, 클라우드 보안서비스 고도화 사업 (2020년)
- **MITRE Attack Evaluation 참가 (2021년)**

AhnLab | NSR | SAINT SECURITY | 한화시스템/시스템 | 국방과학연구소 Agency for Defense Development | LIG 넥스원 | KISA 한국인터넷진흥원

비즈니스

End-Point 위협 관리 서비스 (Pre-Sales)

- 무인화기기 위협 보안 관리서비스 공동개발 협력 (롯데정보통신)
- SMB 대상 관리형 보안 서비스 협력 (㈜안랩)
- 외주 협력업체 단말기 위협 관리 서비스 (한국토지주택공사)
- 엔드-포인트 위협 관리 서비스 미국 시장 진출 협력 (WeBridge, Inc.)

AhnLab | uppsalasecurity | webridge | 롯데정보통신 | CM | KISA 한국인터넷진흥원 | LH 한국토지주택공사

Core technology of MONSTER

SOMMA

공격행위 시뮬레이션

단일 행위 시뮬레이션

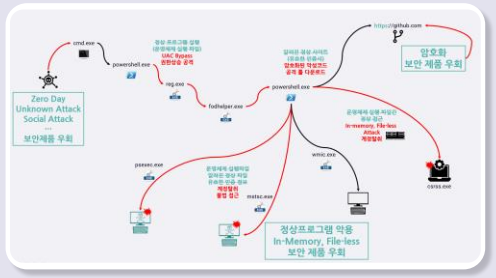
- MITRE ATT&CK 기반 단일 공격행위 시뮬레이션

공격 시나리오 시뮬레이션

- 실제 발생한 APT 공격을 Cyber Range 상에서 공격자의 전략(Tactics), 기술(Techniques), 과정(Procedures)를 시뮬레이션

공격 행위 데이터 수집

- 공격행위 시뮬레이션을 통해 위협분석에 필요한 데이터를 생성하고, 자사 솔루션의 취약점을 개선



솔루션화

CHEIRON

MITRE ATT&CK 기반 공격 기술 시뮬레이션

APT 공격 시나리오기반 공격 시뮬레이션

MITRE ATT&CK 기반 공격 기술 시뮬레이션

- 현재 자사 MONSTER 플랫폼의 탐지엔진 고도화에 활용
- 사용자 편의성을 개선, 향후 자체 솔루션화 계획

국방과학연구소 Agency for Defense Development | LIG 넥스원 | 한화시스템/시스템 | ATT&CK®

비즈니스

데이터셋 생성 용역 사업 등에서 활용

- 군 사이버 보안 관련 R&D 사업에서 다수 활용
- 한국인터넷 진흥원, 사이버보안 빅데이터 AI 데이터셋 구축 사업 (2020년)

국방과학연구소 Agency for Defense Development

고도화된 사이버 위협 관련 교육 사업

- 군 사이버 보안 관련 교육사업에서 활용
- MITRE ATT&CK 기반의 사이버 위협 헌팅 교육

Why Data on Cloud is BETTER?

Cloud 에 모여 있는 **DATA** 가 SOMMA 의 경쟁력입니다.

가시성 확보

- 침해 사고 대응 준비도
- 발생한 행위의 정확한 분석과 추적이 가능

지속적인 위협 탐색

- 최신 인텔리전스 과거 위협 탐색
- **과거의 데이터를 현재의 기술로 분석**

수집은 한번, 분석은 여러 번

- 인텔리전스 기반 탐지
- TTP 기반 위협 탐지
- ML/AI기반 탐지

SOMMA

02

Market & Business Strategy

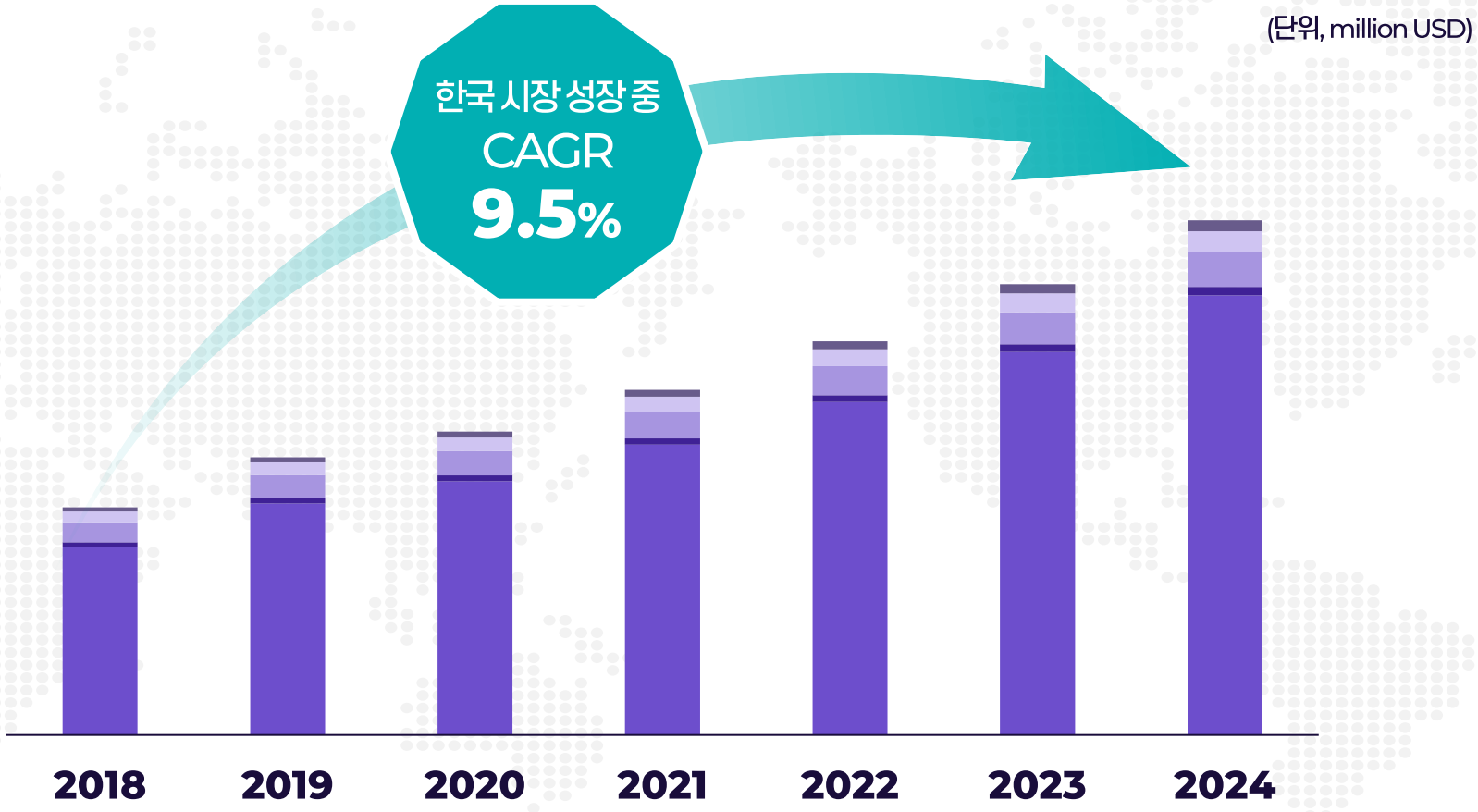
엔드-포인트 보안 / 지능형 보안시장 (EDR, MDR, XDR, MSS)은 **성장 중**입니다.

글로벌 엔드-포인트 보안 시장

'24년 17,684M (약 20조원)

(참고 자료 : Forecast Gartner 2020 3Q)

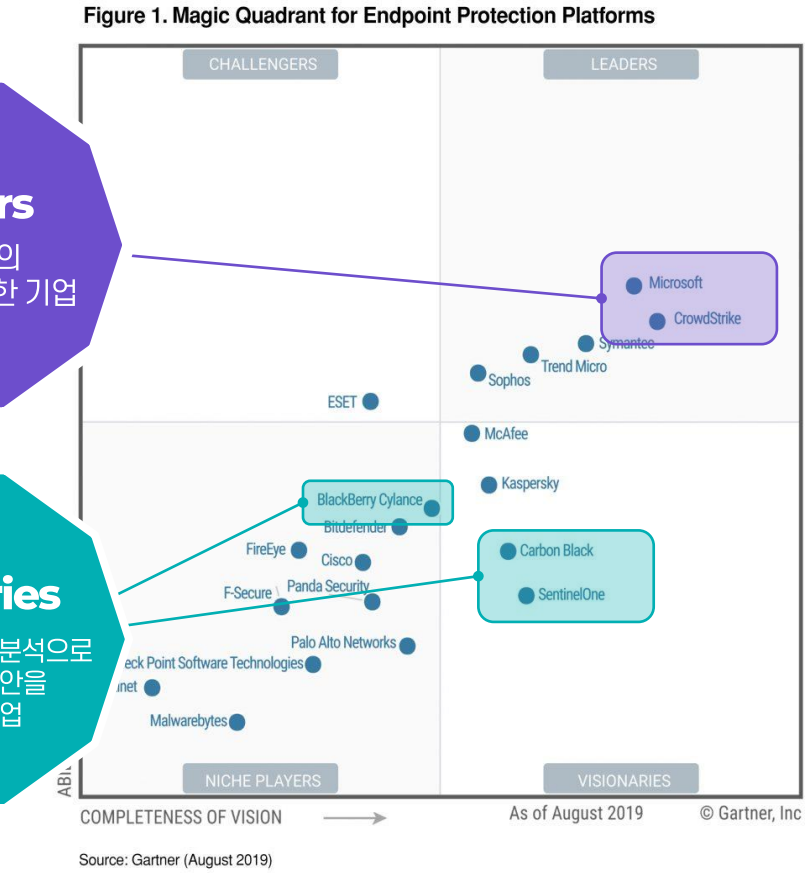
- GLOBAL
- KOREA
- JAPPAN
- APAC
- Emerging APAC



데이터 확보 – 분석 능력이 비즈니스의 성패를 좌우합니다.

Leaders
Endpoint의
가시성을 확보한 기업

Visionaries
정보 수집 및 위협 분석으로
Endpoint 보안을
제시하는 기업



엔드-포인트 데이터 수집-분석에 기반한 업체들이 크게 성공

- Microsoft 는 보안제품 벤더가 아니었지만, 운영체제의 Telemetry 데이터를 통한 EDR 솔루션으로 Leaders 그룹에 포지셔닝

㈜쏘마는 다년간 엔드-포인트 데이터 수집-분석에 필요한 원천기술 확보

- 군 사이버 보안 관련 R&D 사업에 자사 원천 기술 활용 다수 (국방과학연구소, LIG넥스원, 한화 시스템)
- 국내 정보 기관 보안시스템 구축에 자사 원천 기술 활용 (5,000 동시 사용자)
- 해외 보안업체에 자사 원천기술 공급 (싱가폴, Uppsala Security, Inc)

원천기술을 활용한 다양한 서비스/솔루션 런칭 계획

Business Map

MONSTER

Managed Threat Hunting Service

관리형 보안 서비스(MDR/XDR)

- Security As A Service
- 고도화된 사이버 위협에 가장 효과적이고 능동적인 대안을 제시
- 데이터에 기반한 전문가 서비스 제공

ANY-Office

원격 근무 관리 솔루션

- 원격근무 환경 관리 시장 성장세
- MONSTER 플랫폼을 활용한 부가 솔루션
- 기존 엔터프라이즈 솔루션 연계
- MONSTER 관리형 보안 서비스 연계로 고객 다변화와 부가 매출을 목표

CHEIRON

공격 행위 시뮬레이터 (BAS)

- 보안 컨설팅/평가
- 최신 사이버 공격 데이터셋 생성
- 공격 탐지 기술 고도화
- MONSTER 관리형 보안 서비스의 경쟁력강화와 추가 매출 목표

1 Threat Hunting 교육

2 Threat Intelligence Feed

3 Incident Response

침해 사고 대응 서비스

- 이미 발생한 사고의 원인분석과 대책 수립
- 가시성 확보, 행위 분석, 위협 추적에서 확실한 경쟁력 확보

4 Threat Hunting On-Demand

능동형 위협 평가 서비스

- 침해 사고 발생 전 보안성 평가
- 사이버 위협에 능동적 사전 평가
- 가시성 확보, 위협 분석에 필요한 모든 기술을 가진 자사의 경쟁력을 극대화 할 수 있는 형태의 서비스

Achievements

확보한 원천기술들을 통해 **다양한 분야의 고객들과 성과**를 만들어내고 있습니다.

- 프로세스 제어
- 네트워크 제어
- 실시간 정책 적용
- 행위데이터 수집
- 위협 대응

엔드-포인트 에이전트

- 엔드 포인트 정책 관리
- 사이버 위협 인텔리전스 통합
- 행위 데이터 처리
- 위협 탐지 및 분석

빅 데이터 처리

행위 데이터 분석

- 실시간 위협 분류 기술 (TTP 탐지 엔진)
- 사이버 위협 인텔리전스 기반 탐지
- 비 정상 행위 식별 (Anomaly Detection)
- 위협객체 행위 추적

공격행위 시뮬레이션

- 최신 APT 공격 시나리오 시뮬레이션
- TTP 기반 단일 악성행위 시뮬레이션
- Living Off The Land 방식 시뮬레이션

Achievements

SOMMA

확보한 원천기술들을 통해 다양한 분야의 고객들과 성과를 만들어내고 있습니다.

보유 기술 활용 실적

민간

AhnLab, 지란지교시큐리티, SAINT SECURITY

군

국방과학연구소, ROK CYBER COMMAND, 한화시스템/시스템, LIG 넥스원

공공

LH 한국토지주택공사, INNOPOLIS 연구개발특구진흥재단, KISA 한국인터넷진흥원, NSR 국가보안기술연구소

해외

uppsalasecurity

2018.04	국방과학연구소	• 지능형 침입추론 및 사이버위협 분석 시스템 개발
2018.06	(주) 세인트시큐리티	• 상용 위협 인텔리전스 연동을 통한 악성코드 탐지 기술 협약 체결
2018.09	국방과학연구소	• APT 공격 시뮬레이터 개발
2019.01	주식회사 안랩	• 악성코드 데이터 베이스 사용 및 악성코드 탐지 기술 공유 협약 체결
2019.02	Uppsala security (해외)	• Monster Platform 기술 공급 및 제품 공동 개발
2019.04	국방과학연구소	• 위협 탐지 시스템 평가용 위협 데이터 생성 용역 수행
2019.07	국방과학연구소	• 사이버 위협 지능형 분석 및 예측기술 R&D 사업 수행
2020.04	국방과학연구소	• APT 공격 탐지 관련 기술 R&D 사업 수행
2020.04	국방과학연구소	• 실시간 메모리 분석 기술 관련 R&D 사업 수행
2020.07	한국인터넷진흥원	• 사이버보안 빅데이터 AI 데이터셋 구축사업
2020.08	한국인터넷진흥원	• 능동형 사이버 위협정보 수집 시스템 구축 사업, Monster Platform 공급 (100 User 라이선스)
2020.08	한국토지주택공사	• 빅데이터 플랫폼 도입사업, Monster Platform 공급
2021.05	한국인터넷진흥원	• 사이버보안 인공지능 데이터셋(침해사고 분야) 구축
2021.06	국방과학연구소	• Autonomous Cyber Red team/Blue team Architecture 개발
2021.09	대덕연구개발특구	• CTI의 효율적 활용을 통한 능동적 사이버위협 탐지시스템 후속 고도화 개발
2021.12	국방과학연구소	• 지능형 침입 추론 및 사이버 위협 기술 분석
2022.05	한국인터넷진흥원	• 비대면 서비스 보안 강화 시범 사업 개발

믿고 맡길 수 있는 기술 경쟁력을 보유하고 있습니다.

개발대상 기술(제품, 서비스 등) 관련 지식재산권

출원국	출원 및 등록번호	지식재산권(특허)명	비고
한국	C-2018-006383	• 몬스터 에이전트	
한국	C-2019-010324	• Monster Threat Inspector	
한국	C-2019-010323	• Monster Threat Hunting Engine	
한국	C-2019-010321	• Monster Event Collector	
한국	C-2019-010322	• Monster Analytic Cloud	
한국	C-2019-010325	• Monster Analytic API	
한국	C-2019-010326	• ARES	

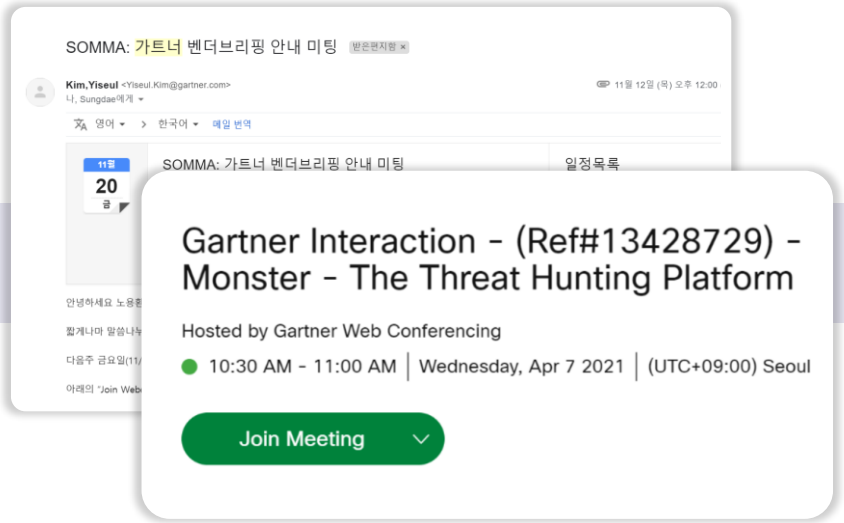
믿고 맡길 수 있는 기술 경쟁력을 보유하고 있습니다.

개발대상 기술(제품, 서비스 등) 관련 지식재산권

출원국	출원 및 등록번호	지식재산권(특허)명	비고
한국	10-2265955	악성 코드 실행 방지를 위한 악성 코드 탐지 방법 및 도메인 생성 알고리즘 탐지 방법	등록
한국	10-2276345	컴퓨터 내 행위 이벤트 축약 방법	등록
한국	10-2381150	원격 근무 환경을 위한 보안관리 시스템 및 방법	등록
한국	10-2395134	플레이 북 형태의 모의공격도구 구현 장치 및 방법	등록
미국	17/474,420	Security management system and method for remote working environment	출원
미국	17/122,261	Method for compressing behavior event in computer and computer device therefor	출원
미국	17/120,868	Malware detection method for preventing execution of malware, method for detection domain generation algorithm and computer device therefor	출원
한국	10-1818006	행위 정규화를 통한 악성코드 고속탐지 및 시각화 방법 및 이를 이용한 장치	기술이전
한국	10-1964592	보안위협 정보 공유 장치 및 방법	기술이전

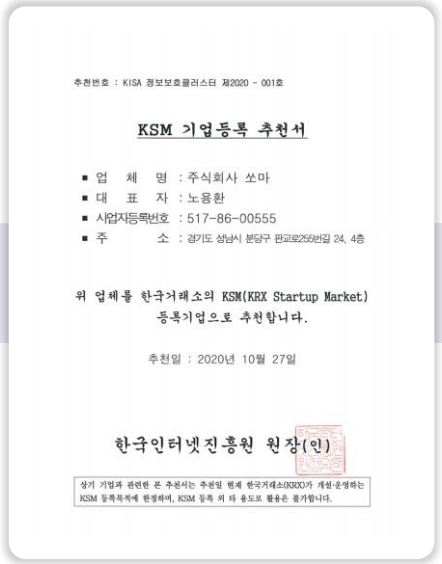
Achievements

사이버위협 대응에 필요한 원천기술을 확보했고, 기술력을 인정받고 있습니다.



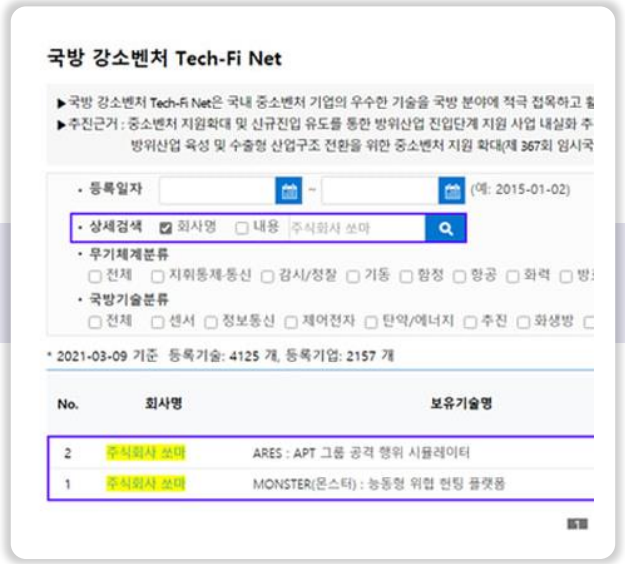
가트너 벤더 브리핑 초청

- 벤더가 가트너에 요청해도 미팅 성사가 매우 어려움
- 가트너에서 먼저 회사 및 기술 소개 요청을 받을 정도로 기술력을 인정



KRX Startup Market 등록 추천

- 한국인터넷진흥원으로부터 스타트업 비상장 주식 시장에 등록을 위한 추천받음

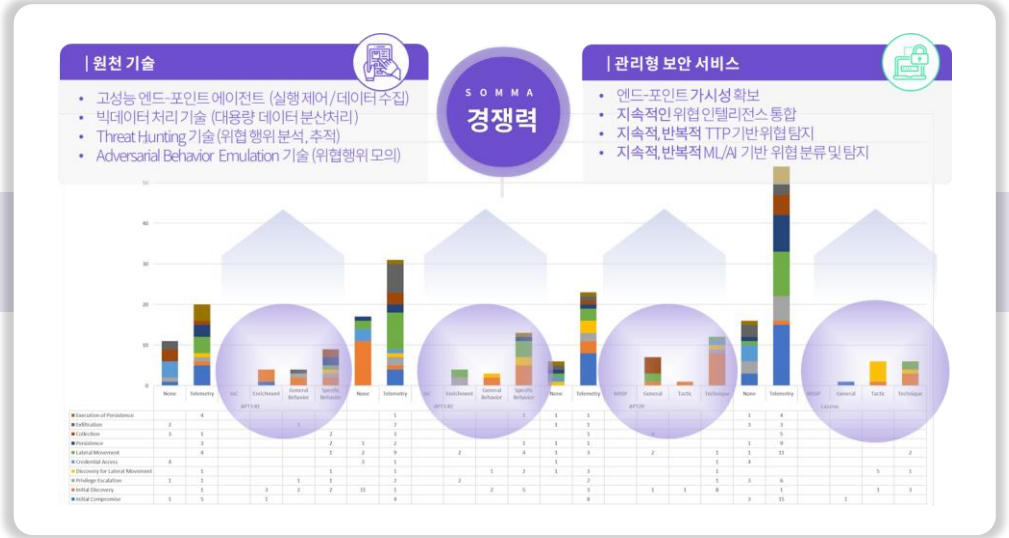


군, 방위산업 업계에서 기술력을 인정

- 대형 방위산업체 LIG넥스원과 파트너 등록 (스타트업으로는 매우 이례적)
- 국방 강소벤처로 등록, 방위산업 분야에서 기술력을 인정 받음

Achievements

기술 개발에 그치지 않고, 공식적으로 기술력을 **인정받기 위한 노력**들을 하고 있습니다.



Project Statement

ATT&CK Evaluation Collaborative Research and Development

THIS Project Statement No. One, effective April 13, 2021 ("Effective Date"), is between MITRE Engenuity, Incorporated ("MITRE Engenuity"), a Delaware charitable nonstock, not-for-profit corporation operating as a foundation with a principal place of business at 7525 Colshire Drive, McLean, VA 22102-7539 and Somma Inc. (the "Evaluation Partner"), a Korean corporation with its principal place of business at 24, Pangyo-ro 255beon-gil, Bundang-gu, Seongnam-si, Gyeonggi-do, Republic of Korea. MITRE Engenuity and the Evaluation Partner may be referred to eac
Statement.

AGREED TO AND ACCEPTED BY:	AGREED TO AND ACCEPTED BY:
Somma, Inc.	MITRE Engenuity, Incorporated
By: (Signature)	By: (Signature)
Name: Yonghwan, Roh	Name: Richard W. Gordon
Title: CEO	Title: Managing Director of Programs
Date: 04/13/2021	Date: 4/13/21

한국인터넷 진흥원, 클라우드 보안 서비스 고도화 사업 (2020년)

- 고도화된 사이버 위협에 대한 MITRE ATT&CK 기반 탐지가 가능한 유일한 제품/서비스 행위 및 행위 맥락 탐지 기술에 대한 능력을 평가받고, 인정 받음

MITRE Attack Evaluation 2021 참가

- 글로벌하게 인정 받는 고도화된 사이버위협탐지 평가로, 글로벌 보안 벤더들 위주 (글로벌 보안 벤더들과 동일하게 기술을 평가 받을 예정)
- 국내 보안 스타트업으로는 자사가 유일 (국내에서는 ㈜안랩을 제외하고는 두 번째 프로그램 참여기업)

클라우드 기반 사이버 위협 헌팅 플랫폼 **SOMMA**

Thank you

SOMMA