국방혁신기술보안협회 회원사 방문 프로젝트

제6회 K-SAEM Emerging Tech&Talk

- 회원사 : ㈜시큐레이어
- 일　시 : 2023. 12. 06. (수) 16:00
- 장　소 : ㈜시큐레이어 본사
- 참석자 : 서태진 예)소장 (前 합참지휘통신참모부장) 등 8명

SecuLayer

제6회 K-SAEM Emerging Tech&Talk

시 간	내 용
16:00~16:30 (30분)	도착 및 환담
16:30~17:30 (60분)	회사 및 기술 소개
17:30~18:00 (30분)	이동
18:00~20:00 (2시간)	식사 및 간담회

SecuLayer

시큐레이어 회사 및 기술 소개

2023.12 / ㈜시큐레이어

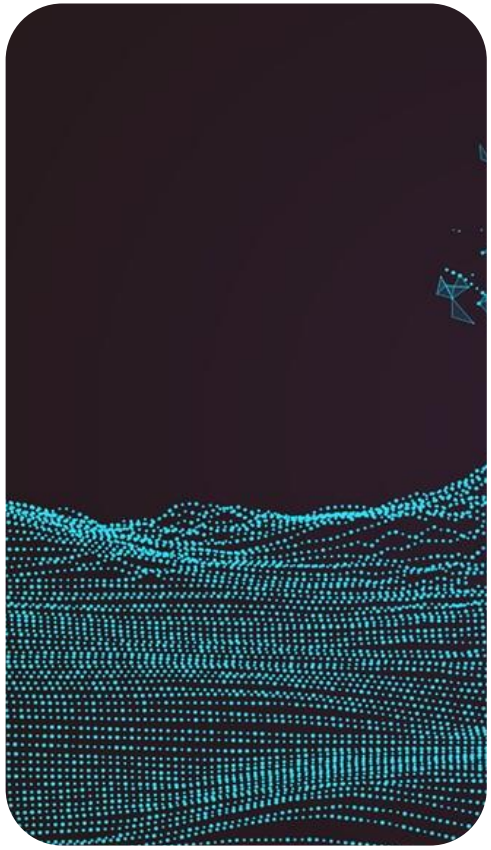
벤처기업인증

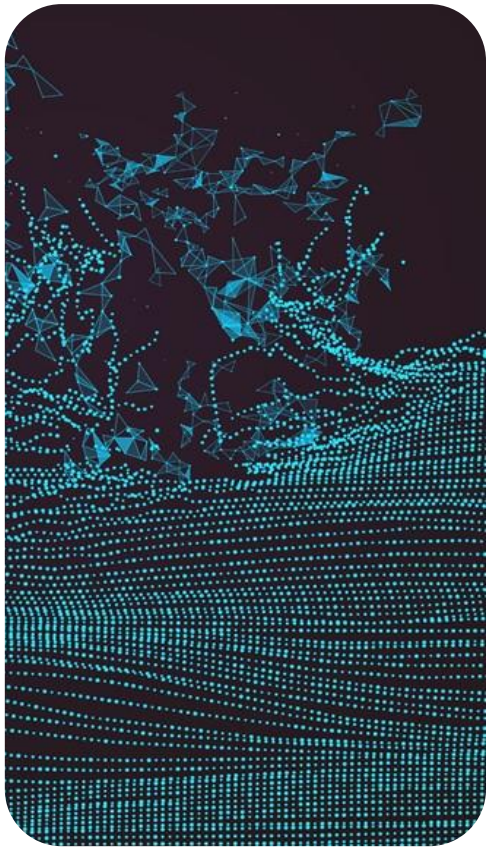
기술혁신형중소기업

SecuLayer

INDEX

SecuLayer





Ⅰ. 회사 소개

1 회사 개요

2 주요 연혁

3 조직 구성

ISO 27001
BUREAU VERITAS
Certification

SecuLayer

Ⅰ. 회사 소개

1. 회사 개요

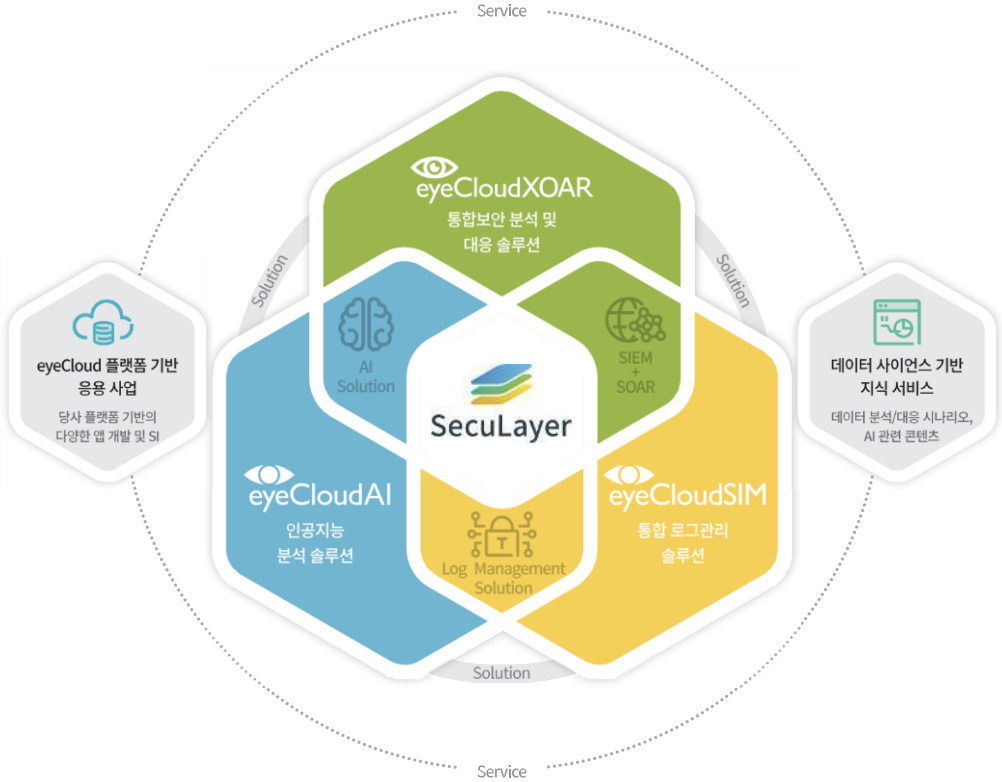
기술 중심의 기업으로 각종 수상, 특허, 매출 등 지속적으로 높은 성장과 확실한 전문성을 확보

개요

SecuLayer

- 회사설립 | 2012년 2월
- 기업형태 | 벤처기업(중소기업)
- 업 종 | 소프트웨어 개발 및 공급
- 사업분야 | 빅데이터, 인공지능 기술 활용 통합 보안 관제 솔루션 제공

사업 영역



상훈/인증/특허


기술혁신형 중소기업 확인서(2015)

행정자치부장관 표창장

대한민국 소프트웨어 품질대상(금상/2015)


ISO27001 인증서(2014)


특허증 (40종 보유)

2021년 통합관제 솔루션 개발 기술 우량 기술 기업 인증과
대한민국 ICT Innovation Awards 과학기술정보통신부장관 표창

Security Intelligence Platform

"데이터의 이해를 통해 더 안전한 세상을 만듭니다"

Ⅰ. 회사 소개

2. 주요 연혁

2012

㈜시큐레이어 설립, 국내최초 빅데이터 기반 SIEM 출시

- 클러스터링 기반 분산 처리 기술 등 빅데이터 분야 자체 핵심 기술을 바탕으로 ㈜시큐레이어 설립
- 국내 최초의 빅데이터 기반 보안 관제 솔루션(SIEM)인 'eyeCloudSIM' 출시
- 국가 핵심 기관인 전력거래소의 '통합 보안 관제 시스템 구축

2013

국내 최대 실시간 데이터 처리 기관에서 당사 제품 선정

- 'eyeCloudSIM v2.5'가 국내 최대 통합보안관제시스템인 행정안전부 국가정보자원관리원의 nSIMS로 선정
- 나루시큐리티와 협업하여 국방과학연구원 ' 사이버전시험 검증환경 구축기술' 개발

2014

원천 기술력 강화를 통한 각종 기술 인증 획득

- ISO27001:2013인증 획득
- 'eyeCloudSIM v2.5' CC인증, GS인증 획득
- 국가정보자원관리원 '2014년 정보보호 보강사업', nSIMS 고도화 및 nTEMS 구축
- 대전 지사 설립

2015

대한민국 SW 품질 최우수상 수상

- 제2회 '대한민국SW품질대상' eyeCloudSIM v2.5 최우수상 수상
- 기술혁신형 중소기업 (INNO-BIZ) 선정
- 침해사고 분석 대응 솔루션 'Bluebird' 출시
- 네트워크 트래픽 분석 솔루션 'TtL' 출시
- 광주 지사 설립

2016

공공/국방/금융/기업 등으로 사업 영역 확대

- 군인공제회, KB손해보험, NHN, 안랩 등의 사업 등을 수행하며 사업 영역 확대
- eyeCloudESM v2.5' EAL 3등급 CC인증 획득
- 부산광역시 차세대 통합보안관제시스템 구축
- 서울시 1, 2 권역, 전북, 강원 3단계 스쿨넷 사업 구축

2017

국내 최초 빅데이터 기반 보안위협 탐지·분석 AI 출시

- 국내 최초 빅데이터 기반 보안 위협 탐지 · 분석 인공지능 플랫폼 'eyeCloudAI' 출시
- 국가정보자원관리원 인공지능 적응형 보안 시스템 구축 ISP 수행
- KDB 산업은행 차세대 정보 시스템 구축 개발 사업 수행

2018

국내 최초 보안 관제 자동화 플랫폼 SOAR 출시

- 보안 오케스트레이션 자동화 및 대응(SOAR) 솔루션 'eyeCloudXOAR' 출시
- '2018 ICT 특허 경영 대상' 단체부문 은상 수상
- 하반기인기상품 eyeCloudSIM 5년 연속 선정 (전자신문)
- 국가정보자원관리원 인공지능기반 차세대 보안 시스템 구축 수행
- 대검찰청 빅데이터 기반 보안관제시스템 구축
- 헌법재판소 데이터센터 장비 등 확충 사업 수행

2019

대한민국 사랑받는 기업 정부 포상 중소벤처기업부 장관상 수상

- '제7회 대한민국 사랑받는 기업 정부 포상' 장관상 수상
- 청년친화강소기업(임금, 일생활균형, 고용안정) 선정 (고용노동부)
- 국방과학연구소 정보보호시스템 도입 사업 수행
- 국가정보자원관리원 인공지능 기반 차세대 보안 시스템 구축 수행
- 해양수산부 사이버 안전 센터 종합 분석 시스템 고도화 사업 수행
- 통일부 빅데이터 기반 차세대 보안 관제 시스템 구축
- 롯데카드 통합 로그 시스템 고도화 구축

2020

eXtended SOAR 플랫폼 eyeCloudXOAR V4.0 출시

- AutoML, XAI 등 최신 기술을 적용하는 IITP '데이터 특징과 문제를 정의하는 빅데이터 분석 모델 추천 자동화 기술 개발' 연구 과제 수주
- 국가정보자원관리원 인공지능 기반 차세대보안시스템 3차 구축
- 중앙부처 최초의 SIEM,AI,SOAR 통합 구축 사업인 문화체육관광부 "자동화 기반의 차세대 보안관제시스템 구축 사업" 수행
- 통일부 "외부위협정보 연계 보안 관제 및 분석 시스템 구축 사업" 수행
- 한국도로공사 "국토교통정보센터 통합 로그 관리 시스템 구축" 수행
- 롯데글로벌로지스 통합 로그 관리 솔루션 구축

2021

'2021 대한민국 ICT Innovation Awards' 수상

- '2021 대한민국 ICT Innovation Awards' 과학기술정보통신부 장관상 수상
- 법무부, 해양수산부, KT, 매그나칩반도체 등 SOAR 시스템 구축 확대
- IITP 'AI 빅데이터 기반 사이버 보안 오케스트레이션 및 자동 대응 기술 개발' 수주
- 2021년 SIEM 조달시장 'eyeCloudSIM' 매출 1위 달성

2022

AutoML, XAI 등 최신 AI 기술을 기반으로 사업 영역 확장

- 조직병리 비임상시험을 위한 인공지능기반 의료 영상 분석 플랫폼 수행
- KISA 악성의심 도메인 분석 시스템 구축 사업 수행
- KISA 사이버보안 얼라이언스 플랫폼 구축 사업 수행
- KT Cloud 보안관제 서비스 구축 수행
- 한국교육학술정보원 4세대 지능형 나이스 구축 수행
- IBK 금융그룹 자회사 지능형 통합보안관제 시스템 구축 수행
- 대구은행 통합로그관리시스템 고도화 사업 수행
- 2022년 시장 점유율 1위 달성

2. 주요 연혁 (요약)

- 2012년 **국내 최초** 빅데이터 기반 보안관제 시스템 **SIEM** 자체 기술 개발 출시
- 2013년 **국내 최대 실시간 데이터 처리 기관**(국가정보자원관리원, 38TB/일)에서 당사 제품 선정
- 2017년 **국내 최초** 빅데이터 기반 보안위협 분석 탐지 **AI** 솔루션 자체 기술 개발 출시
- 2018년 **국내 최초** 보안 관리 자동화 시스템 **SOAR** 시스템 자체 기술 개발 출시
- 2020년 차세대 보안관제 시스템 **eXtended SOAR** 자체 기술 개발 출시
- 2022년 **AutoML, XAI** 등 최신 AI 연구(AutoAPE)를 통한 사업 영역 확장
- 2023년 **국내 최고의** 빅테이터 **처리 성능 및 클라우드** 보안 관리 기능 공인 검증

  * 무 손실 317만 EPS, 보안관리 전 기능 만점 (KOSYAS / NIRS)

- 국내 **최대 및 최다 SIEM, SOAR, AI 레퍼런스** 보유 (주요 정부 기관, 국방, 금융, 통신, 기업 등)

국제 정보보안 인증 ISO/IEC 27001:2013 | CC인증 | GS인증 | 특허등록 | ICT특허경영대상 표창

대한민국 SW제품품질대상 | 기술혁신형중소기업 | 기업부설연구소 | 벤쳐기업인증 | 청년스마트 중소기업 선정

Ⅰ. 회사 소개

3. 주요 고객사

공공기관, 금융기관, 기업 등 약 600+ 고객

국내 시장 점유율 1위 제조사

시큐레이어의 eyeCloudSIM, SIEM 조달시장 매출 1위 기록

박남수 기자 | 승인 2022.01.06 13:40

eyeCloudSIM

[사진=시큐레이어]

[정보통신신문=박남수기자]

2021년 국내 SIEM 조달 시장에서 시큐레이어(대표이사 전주호)가 매출 1위를 달성했다고 밝혔다.

'조달정보개방포털' 자료를 통합보안관제, 로그관리(데이터검색), 보안SW 등 SIEM (보안정보 및 이벤트 관리)부문 제품군의 2021년 실적을 집계, 비교한 결과, 시큐레이어의 eyeCloudSIM (아이클라우드심)이 매출과 점유율면에서 모두 1위를 차지한 것으로 확인됐다.

[출처 : 정보통신신문 2022.01.06.]

국내 최초 및 최다 레퍼런스 보유 제조사 (SIEM, AI, SOAR)

행정안전부 국가정보자원관리원 · 국토교통부 · 해양수산부 · 행정안전부 · 문화체육관광부 · 통일부

법무부 · 국세청 · 관세청 · 방위사업청 · 공정거래위원회 · KISA 한국인터넷진흥원

한국전력공사 · 헌법재판소 Constitutional Court of Korea · 경찰청 사이버안전국 CYBER BUREAU · 근로복지공단 · 부산광역시 BUSAN METROPOLITAN CITY · NIA 한국정보화진흥원

국방전산정보원 Defense Computing Information Agency · 대한민국육군 Republic of Korea Army · 대한민국공군 REPUBLIC OF KOREA AIR FORCE · 한미연합사 · 군인공제회 MILITARY MUTUAL AID ASSOCIATION · 군인공제회 C&C

신한카드 · 신한저축은행 · 신한캐피탈 · KDB산업은행 · KB손해보험 · 키움증권

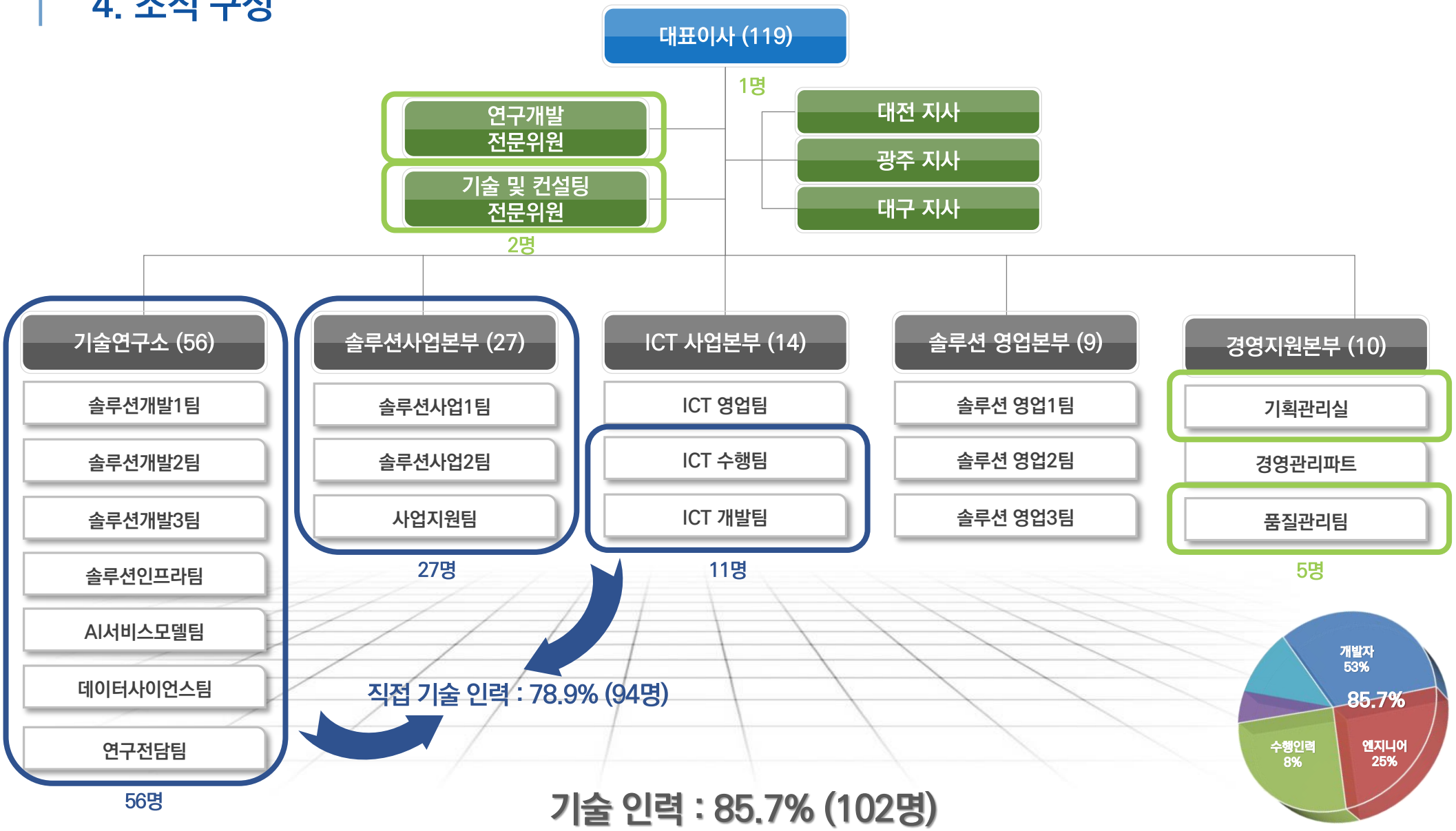
IBK기업은행 · IBK 시스템 · 농협정보시스템 · NH농협손해보험 · 한화생명 · KYOBO 교보생명

에스원 · kt cloud · NHN Cloud · 경북대학교 · 우미건설 · Magnachip

- **국방 분야**

국방전산정보원, 한미연합사령부, 제4284부대, 제3707부대, 제9965부대, 육군본부, 방위사업청(지상전술C4I, 성능개량사업), 국군지휘통신사령부, 국방과학연구소, 국군의무학교, 공군 청주기지, 공군 29전대, 공군 오산기지, 공군 제20전투비행단, 군인공제회, 군인공제회C&C 등

4. 조직 구성



※ 2023년 11월 기준

시큐레이어는?

앞선 자체 기술력으로 업계 트렌드와 시장을 선도하는 기업

최근 언론 보도

시큐레이어의 eyeCloudSIM, SIEM 조달시장 매출 1위 기록

박남수 기자 | 승인 2022.01.06 13:40

[사진=시큐레이어]

[정보통신신문=박남수기자]

2021년 국내 SIEM 조달 시장에서 시큐레이어(대표이사 전주호)가 매출 1위를 달성했다고 밝혔다.

'조달정보개방포털' 자료를 통합보안관제, 로그관리(데이터검색), 보안SW 등 SIEM (보안정보 및 이벤트 관리)부문 제품군의 2021년 실적을 집계, 비교한 결과, 시큐레이어의 eyeCloudSIM (아이클라우드심)이 매출과 점유율면에서 모두 1위를 차지한 것으로 확인됐다.

[출처 : 정보통신신문 2022.01.06.]

시큐레이어, 클라우드·AI 신기술 적용 사업 연이어 수주

발행일 : 2023-07-27 12:00

국가정보자원관리원·한국인터넷진흥원·한국거래 등 대형 사업 수주

<시큐레이어 eyeCloudXOAR V4.0 이미지. 사진=시큐레이어.>

AI 기반 빅데이터 분석과 자동화 솔루션 전문기업 시큐레이어는 작년에 이어 올해도 국가정보자원관리원 대구 클라우드센터, 한국인터넷진흥원, 한국거래소 등 상반기에 진행된 클라우드, AI 등 신기술 적용 대형 사업을 잇달아 수주했다고 27일 밝혔다.

금번 수주 사업들은 국내 보안 분야에서 다년간 쌓아온 사업 수행 경험을 통해 체계화된 자체 수행 조직을 보유한 시큐레이어가 주사업자로서 자사 솔루션인 eyeCloudXOAR, eyeCloudAI 제품을 적용해 수행할 예정이다.

우선 국가정보자원관리원 대구 클라우드센터 사업은 별도 공인된 클라우드 관련 기능과 성능 테스트를 통해 엄격하게 제품을 선정했다.

시큐레이어의 eyeCloudXOAR 제품은 모든 테스트 항목에서 만점을 획득해 클라우드 빅데이터 기술을 인정 받았으며 특히, 성능 테스트에서는 국내 최초로 399만 EPS(Event Per Second)의 벽을 깨뜨려 우수성을 확인했다.

또 한국인터넷진흥원 사이버위협 공동대응 플랫폼 구축 사업은 한국인터넷진흥원과 민간과의 협업을 바탕으로 사이버위협에 대한 정보 공유와 통합 분석을 통해 보다 정확하고 신속한 대응을 위한 공공·민간 공동 대응 플랫폼이다.

새로운 개념의 공동 대응 플랫폼은 시큐레이어의 빅데이터 통합 처리 및 공유 기술과 자동화 기술이 적용된 제품을 기반으로 구성해 사이버위협에 대한 사각지대 해소와 선제 대응이 가능하다.

한국거래소 역시 각종 증권, 선물 등의 안전한 거래를 위해 시큐레이어의 eyeCloudXOAR를 선정했다. eyeCloudXOAR는 자체 빅데이터 플랫폼인 eyeCloud Platform을 기반으로 SIEM과 SOAR를 통합한 새로운 eXtended SOAR 개념의 제품이다. 다양한 장비에서 발생하는 대량의 데이터를 데이터 소스와 분석 방식에 제한없이 가장 효율적으로 분석할 수 있는 하이브리드 분석 도구를 제공하고 있다.

[출처 : 전자신문 2023.07. 27.]

시큐레이어의 SIEM·SOAR 제품, KISA 실전형 사이버훈련장 표준 교육 도구로 선정

김대성 기자 kdsung@dt.co.kr | 입력 : 2023-08-08 14:01

eyeCloudXOAR

과학기술정보통신부(장관 이종호, 이하 '과기정통부')와 한국인터넷진흥원(원장 이원태, 이하 'KISA')이 판교에서 공동 운영 중인 '실전형 사이버훈련장(Security-GYM)'에 AI 기반 빅데이터 분석 및 자동화 솔루션 기업 시큐레이어(대표 전주호)의 eyeCloudXOAR 제품이 SIEM, SOAR 분야의 정보보호 교육 도구로 선정되었다.

실전형 사이버훈련장은 지난해 7월 정부가 발표한 '사이버보안 10만 인재양성 계획'의 하나로 확대 추진되고 있으며, 침해사고 상황에 대한 충분한 이해와 함께 실습 훈련을 할 수 있어 구직자 및 재직자 들로부터 매년 높은 교육 수요가 있다.

과기정통부와 KISA에서 '사이버보안 10만 인재 양성' 목표 달성을 위해 전년도보다 2배 이상의 교육생을 수용할 수 있도록 ㅅ실전형 훈련장의 교육훈련 서버를 증설 하고 ㅅ실시간 해킹 방어 훈련 등 교육과정을 7개에서 19개로 확대하며ㅅ특히, 다양한 정보보호 제품 실습을 위한 제품군 2종에서 12종으로 추가 구비했다.

이번 사업은 구직자 및 재직자를 대상으로 최근 발생한 해킹 시나리오 기반으로 가상의 침해사고환경을 구축하고, 침해사고 조사, 침해 공격. 방어훈련, 상용 정보보호 제품군을 활용한 실습 등 수준별 교육 과정을 편성 및 지원한다.

실전형 사이버침해 대응 과정 중 '일방향 침해사고 방어 및 분석 훈련'은 가상의 기업 인프라 환경의 침투를 방어하고, 침투 사례에 대한 취약점 정보수집·분석을 통한 대책을 수립할 수 있는 방향으로 훈련을 진행한다. '양방향 실전 공방 훈련 과정'은 가상의 기업환경에 접속해 팀별로 할당된 인프라에 대한 방어와 동시에 상대 인프라를 공격하는 절차와 방법을 훈련하면서 실질적인 침투사고에 대응할 수 있는 능력을 배양한다.

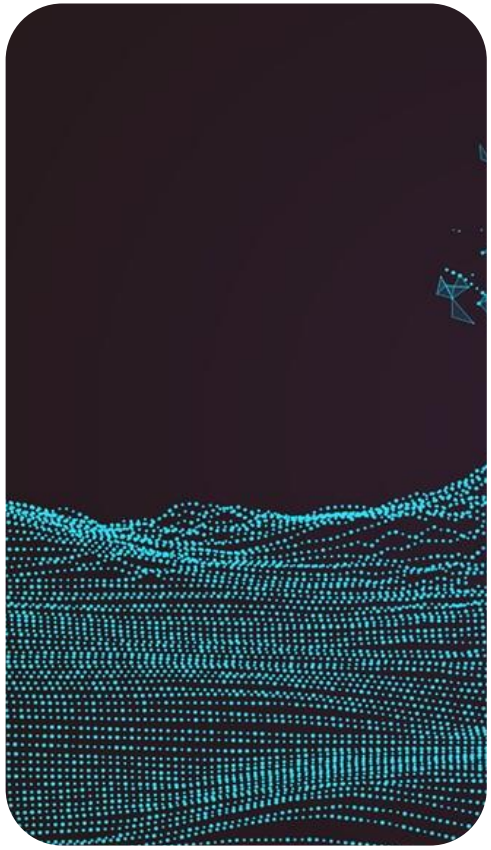
시큐레이어의 전주호 대표는 "eyeCloudXOAR 소프트웨어가 KISA와 과기정통부에서 진행하는 사업에 정보보호 교육 도구로 선정되어, 우리나라의 정보보호 역량 강화에 기여할 수 있게 되어 기쁘다"며, "날로 고도화되며 지능화되는 사이버 공격에 대응하기 위해서는 사이버 침해 대응 전문인력의 양성이 무엇보다 중요하며, 금번 KISA에서 진행하는 교육의 참가자들은 당사 입사시에 가점을 주어 전문인력 양성에 앞장 서겠다"고 전했다. 김대성기자 kdsung@dt.co.kr

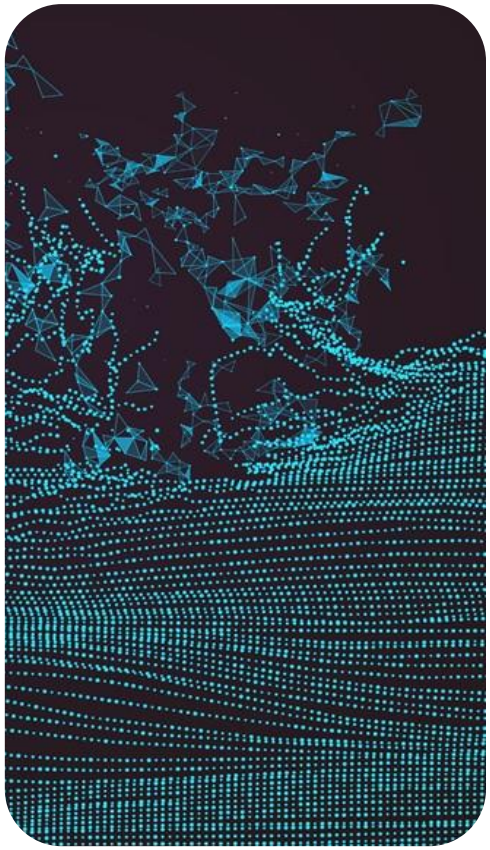
[출처 : 전자신문 2023.08. 28.]

국내 최초 SIEM, SOAR, AI 제품 출시

국내 최대 및 최다 레퍼런스 보유

국내 시장 점유율 1위 제조사





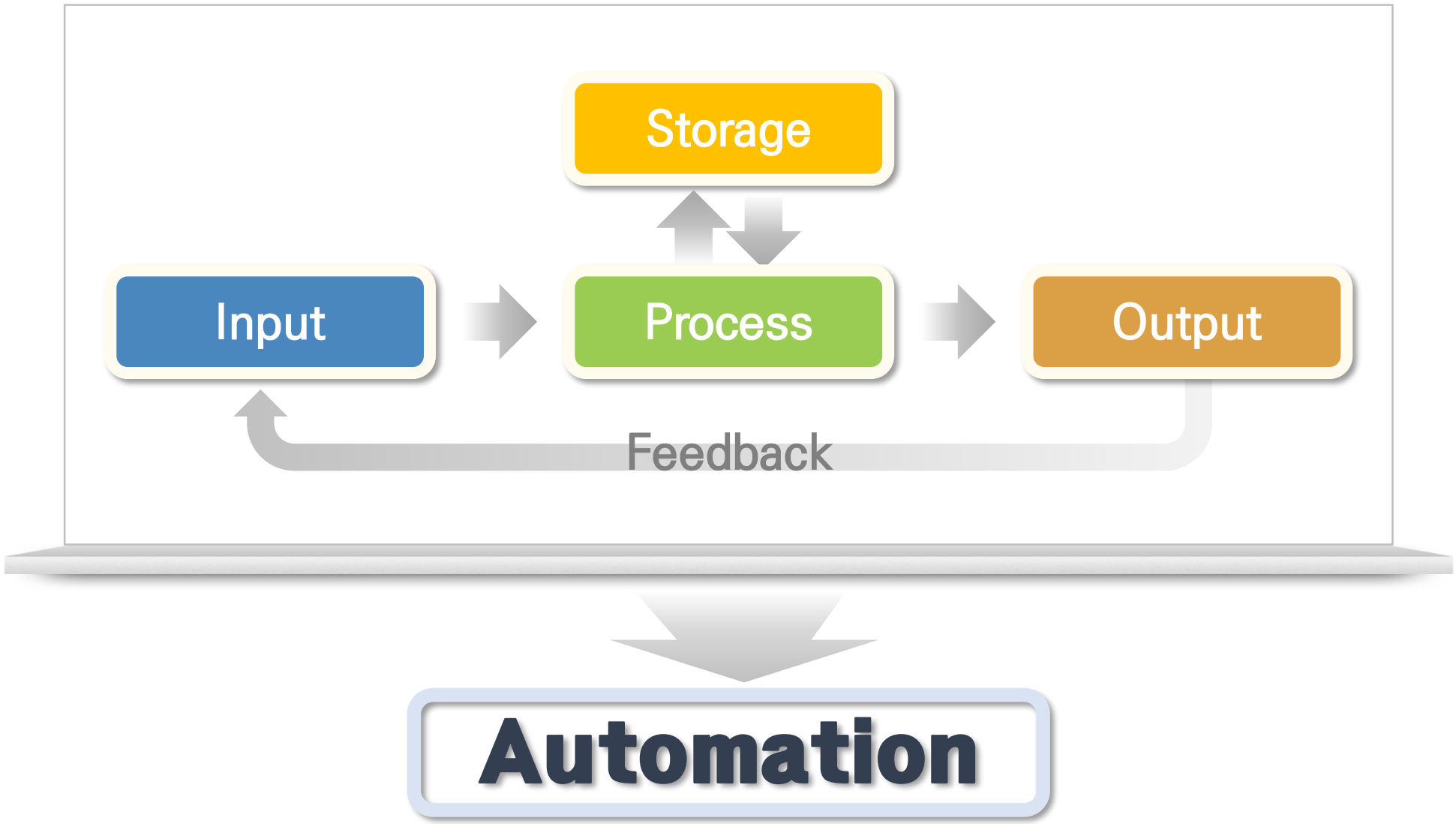
Ⅰ. 기술 소개

1. 보안관제 시스템이란?
2. 패러다임의 변화
3. eXtended SOAR
4. AI
5. 아키텍쳐 (Architecture)

SecuLayer

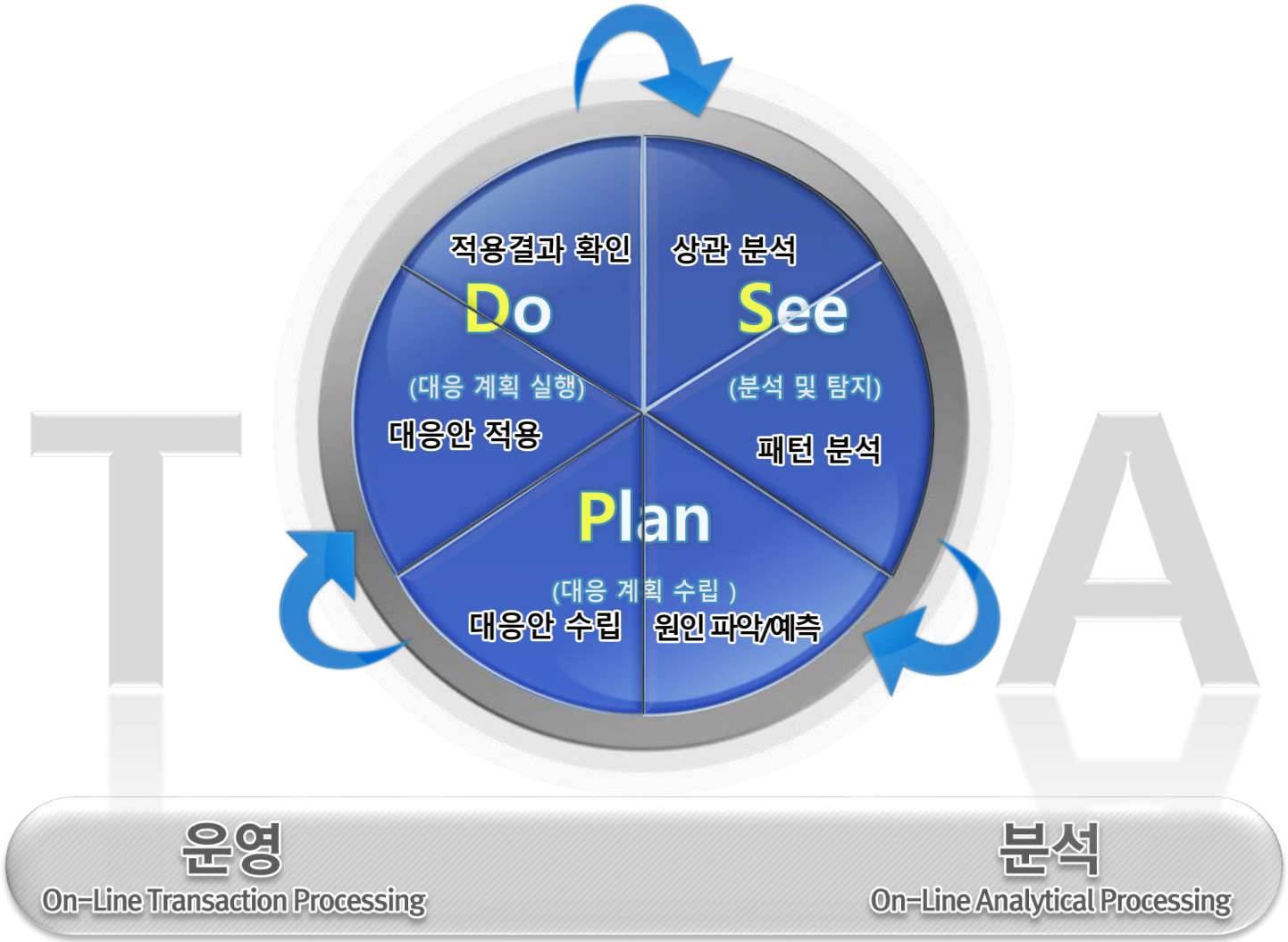
1. 보안관제 시스템 이란 ?

System



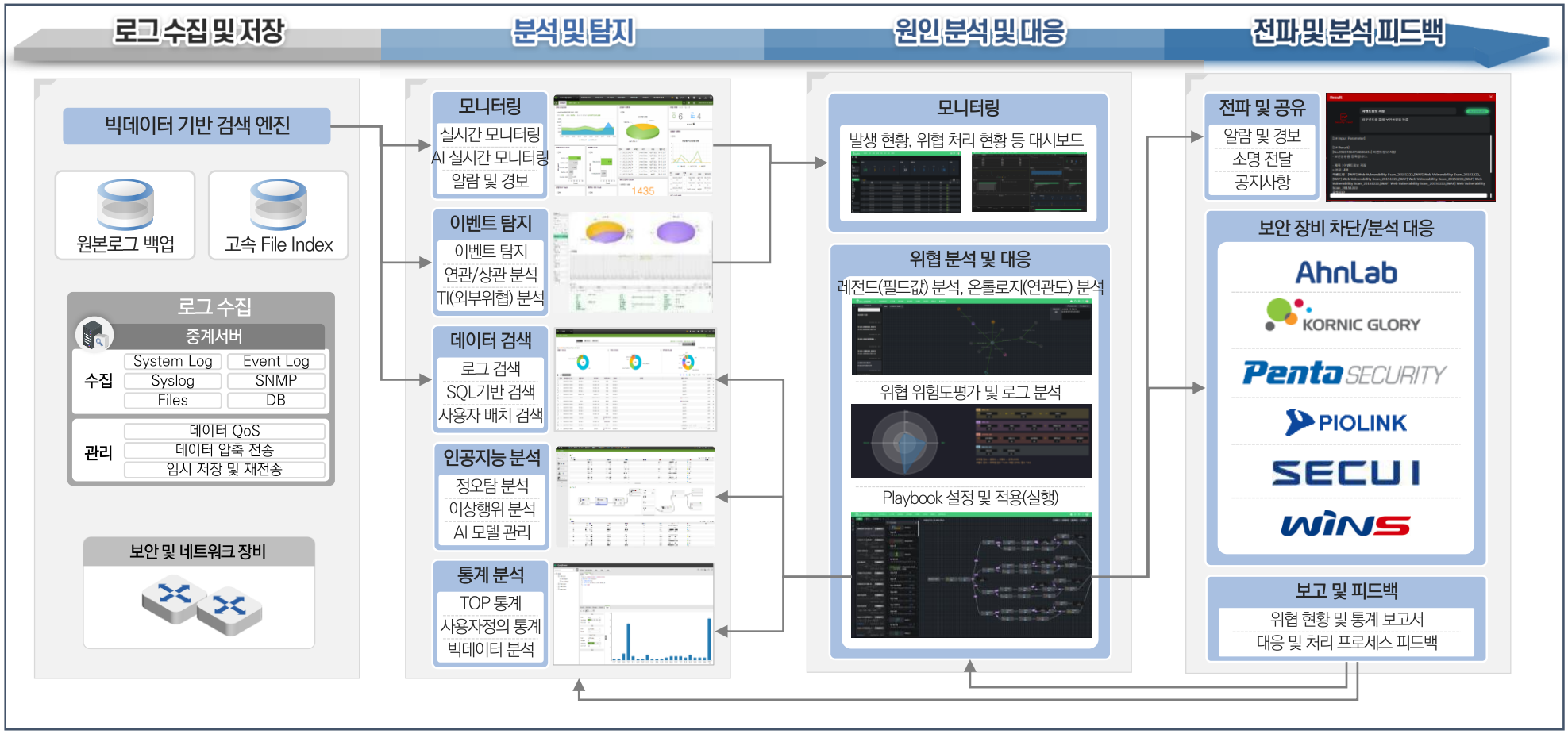
1. 보안관제 시스템 이란 ?

보안관제업무 프로세스

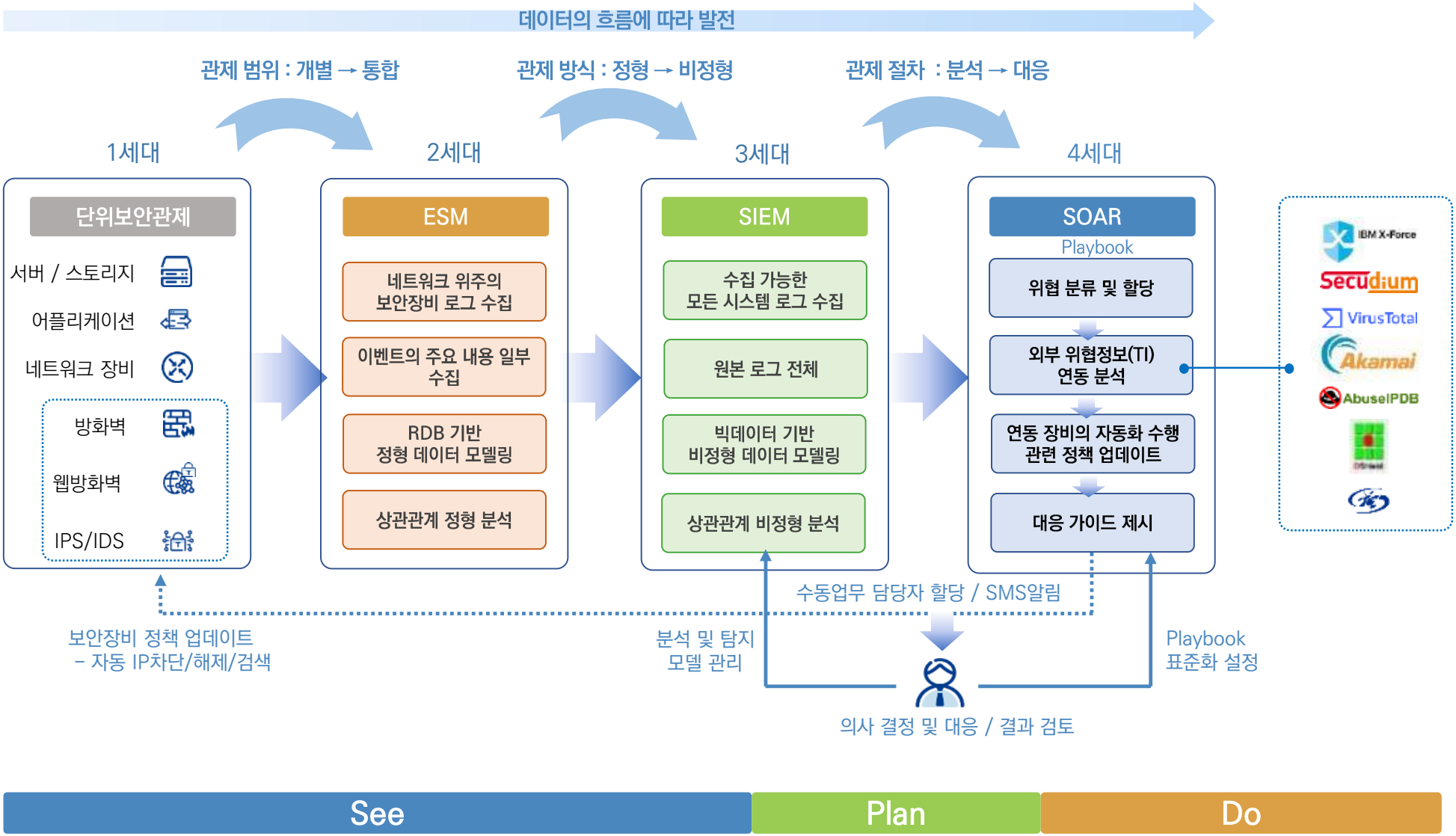


1. 보안관제 시스템 이란 ?

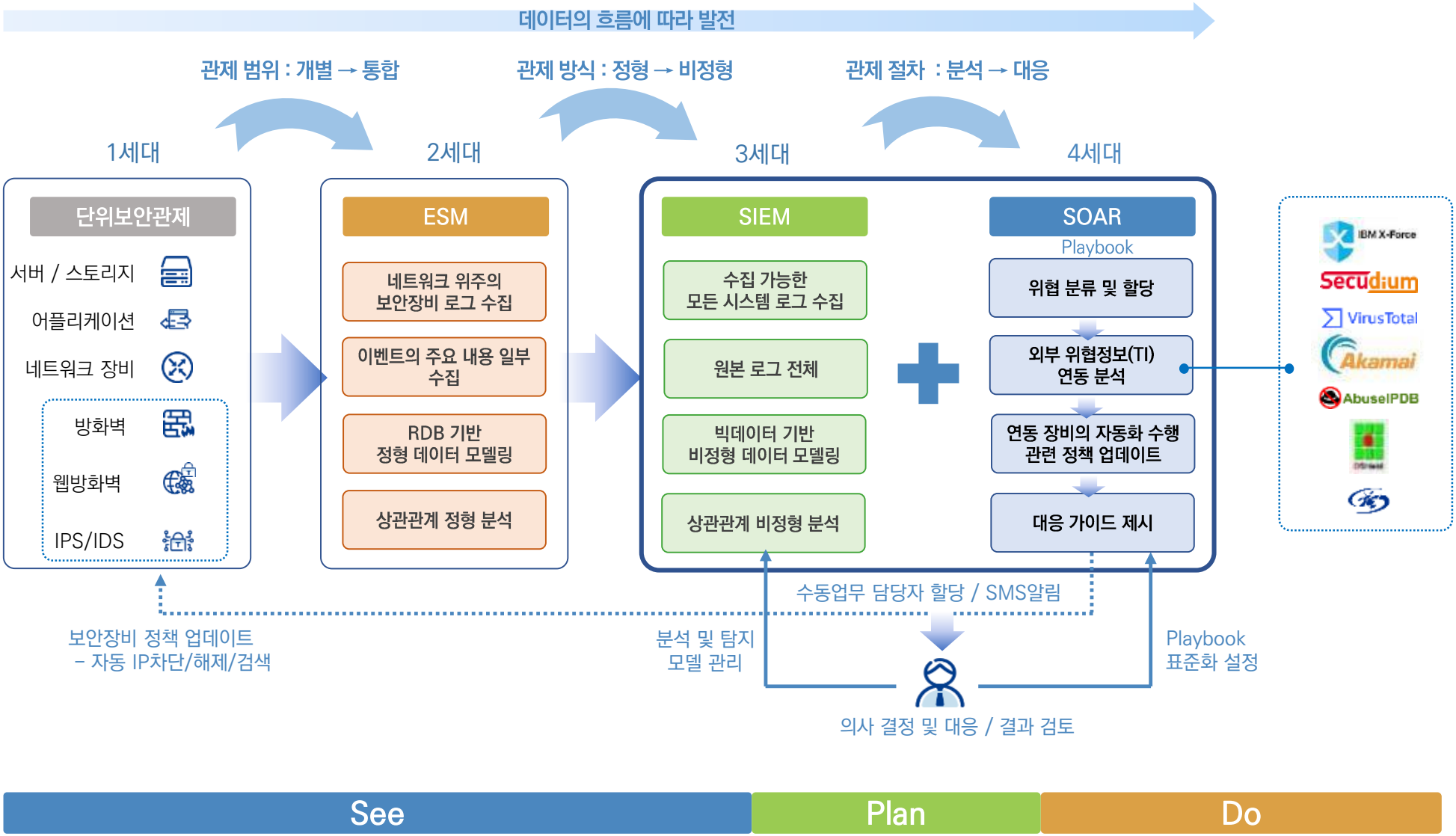
보안관제업무 시스템



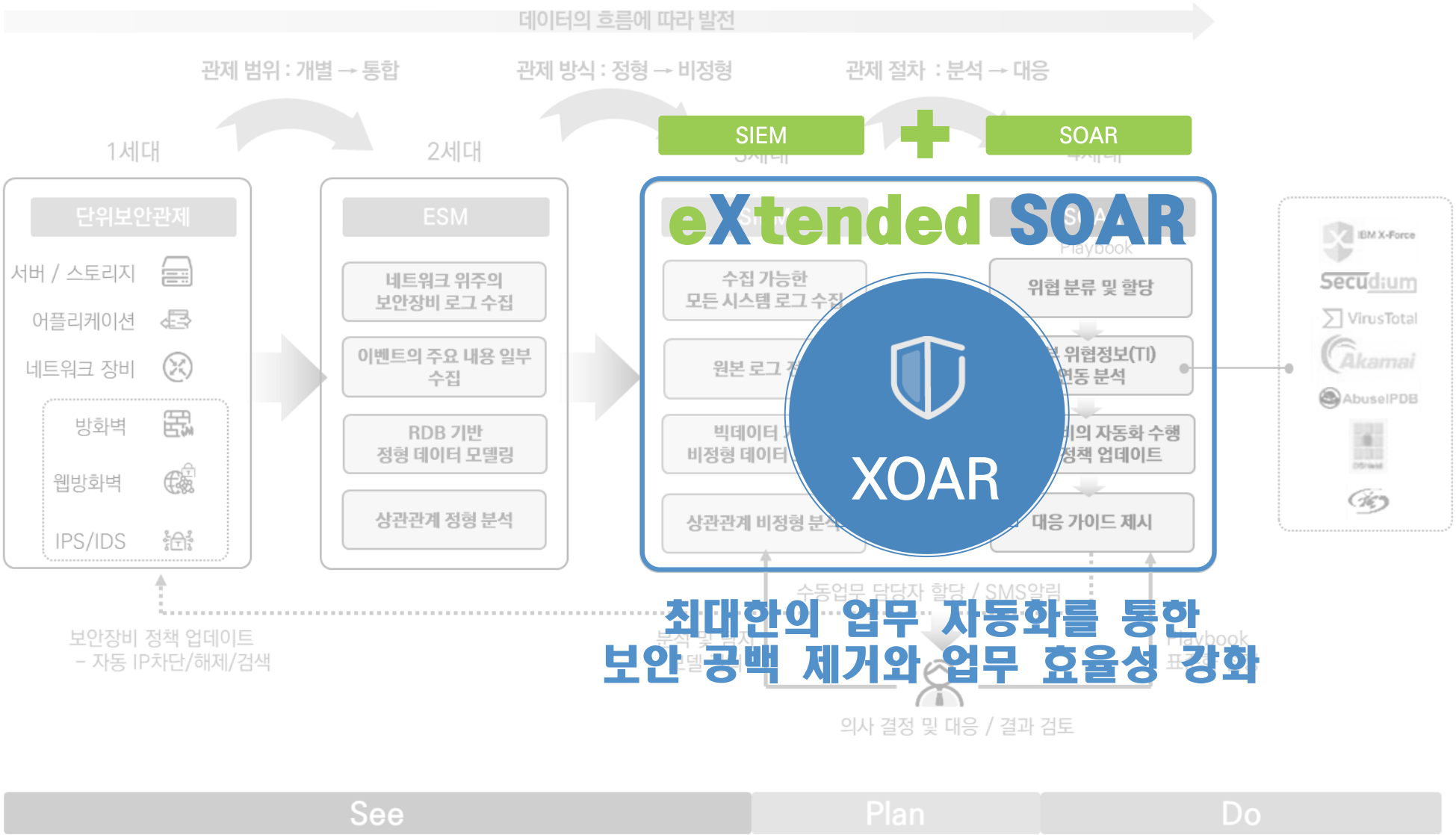
2. 패러다임의 변화


데이터의 흐름에 따라 발전
관제 범위 : 개별 → 통합
관제 방식 : 정형 → 비정형
관제 절차 : 분석 → 대응
1세대
단위보안관제
서버 / 스토리지
어플리케이션
네트워크 장비
방화벽
웹방화벽
IPS/IDS
2세대
ESM
네트워크 위주의 보안장비 로그 수집
이벤트의 주요 내용 일부 수집
RDB 기반 정형 데이터 모델링
상관관계 정형 분석
3세대
SIEM
수집 가능한 모든 시스템 로그 수집
원본 로그 전체
빅데이터 기반 비정형 데이터 모델링
상관관계 비정형 분석
4세대
SOAR
Playbook
위협 분류 및 할당
외부 위협정보(TI) 연동 분석
연동 장비의 자동화 수행 관련 정책 업데이트
대응 가이드 제시
IBM X-Force
Secudium
VirusTotal
Akamai
AbuseIPDB
수동업무 담당자 할당 / SMS알림
보안장비 정책 업데이트
- 자동 IP차단/해제/검색
분석 및 탐지 모델 관리
Playbook 표준화 설정
의사 결정 및 대응 / 결과 검토
See
Plan
Do

2. 패러다임의 변화


데이터의 흐름에 따라 발전
관제 범위 : 개별 → 통합
관제 방식 : 정형 → 비정형
관제 절차 : 분석 → 대응
1세대
단위보안관제
서버 / 스토리지
어플리케이션
네트워크 장비
방화벽
웹방화벽
IPS/IDS
2세대
ESM
네트워크 위주의 보안장비 로그 수집
이벤트의 주요 내용 일부 수집
RDB 기반 정형 데이터 모델링
상관관계 정형 분석
3세대
SIEM
수집 가능한 모든 시스템 로그 수집
원본 로그 전체
빅데이터 기반 비정형 데이터 모델링
상관관계 비정형 분석
4세대
SOAR
Playbook
위협 분류 및 할당
외부 위협정보(TI) 연동 분석
연동 장비의 자동화 수행 관련 정책 업데이트
대응 가이드 제시
IBM X-Force
Secudium
VirusTotal
Akamai
AbuseIPDB
수동업무 담당자 할당 / SMS알림
보안장비 정책 업데이트
- 자동 IP차단/해제/검색
분석 및 탐지 모델 관리
Playbook 표준화 설정
의사 결정 및 대응 / 결과 검토
See
Plan
Do

2. 패러다임의 변화

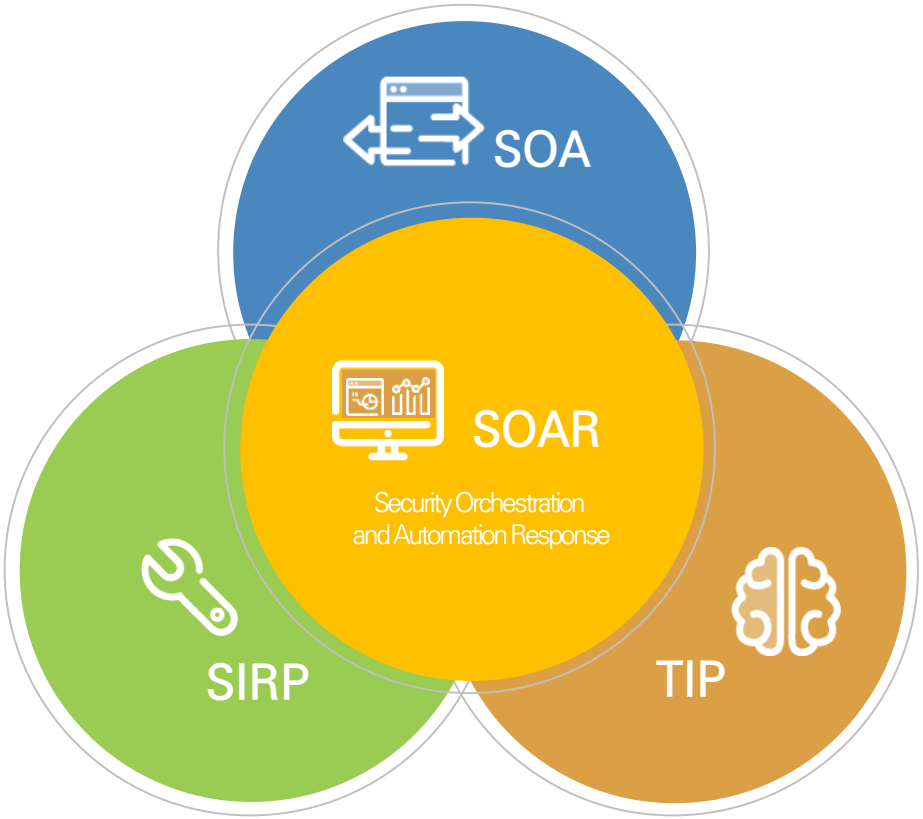

데이터의 흐름에 따라 발전
관제 범위 : 개별 → 통합
관제 방식 : 정형 → 비정형
관제 절차 : 분석 → 대응
1세대
2세대
SIEM
SOAR
단위보안관제
서버 / 스토리지
어플리케이션
네트워크 장비
방화벽
웹방화벽
IPS/IDS
ESM
네트워크 위주의 보안장비 로그 수집
이벤트의 주요 내용 일부 수집
RDB 기반 정형 데이터 모델링
상관관계 정형 분석
eXtended SOAR
수집 가능한 모든 시스템 로그 수집
위협 분류 및 할당
위협정보(TI) 연동 분석
대응 가이드 제시
XOAR
IBM X-Force
Secudium
VirusTotal
Akamai
AbuseIPDB
보안장비 정책 업데이트
- 자동 IP차단/해제/검색
최대한의 업무 자동화를 통한
보안 공백 제거와 업무 효율성 강화
의사 결정 및 대응 / 결과 검토
See
Plan
Do

3. eXtended SOAR (SIEM)

	ESM (2세대)	SIEM (3세대)
수집대상	네트워크 위주 보안 장비	수집 가능한 모든 시스템
수집내용	일부 정형 로그 (국정원 포맷)	원본 로그 전체
저장소	R-DB	File DB
모델링	정적 모델링	동적 모델링
분석방식	정형 분석 (Structured Query Language)	비정형 분석 (Unstructured Query Language)

3. eXtended SOAR (SOAR)

Automation For Orchestration



SOA

Security Orchestration and Automation
보안 오케스트레이션 및 자동화
조직내에 있는 여러 가지의 장비를 적절히 배치하여 Workflow를 관리하는 기법

SIRP

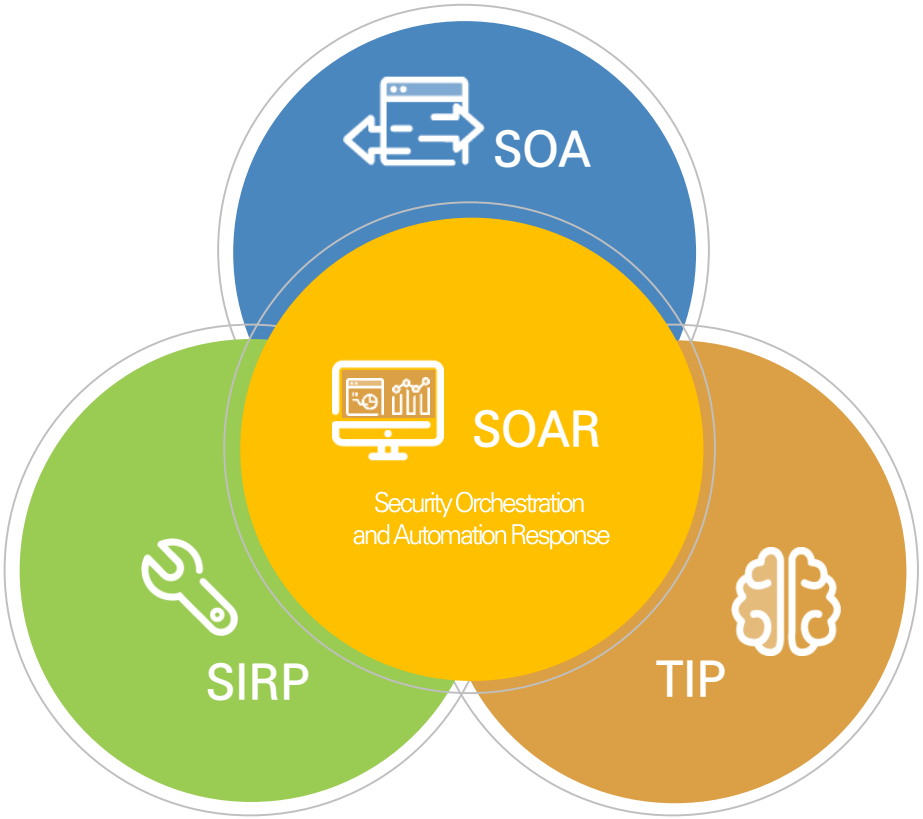
Security Incident Response Platform
보안 사고 대응 플랫폼
SIEM에서 탐지된 위협에 대한 대응 지원 플랫폼

TIP

Threat Intelligence Platform
위협 인텔리전스 플랫폼
위협 인텔리전스 중 상황에 맞춘 구체적인 Action 제시

3. eXtended SOAR (SOAR)

Automation For Orchestration



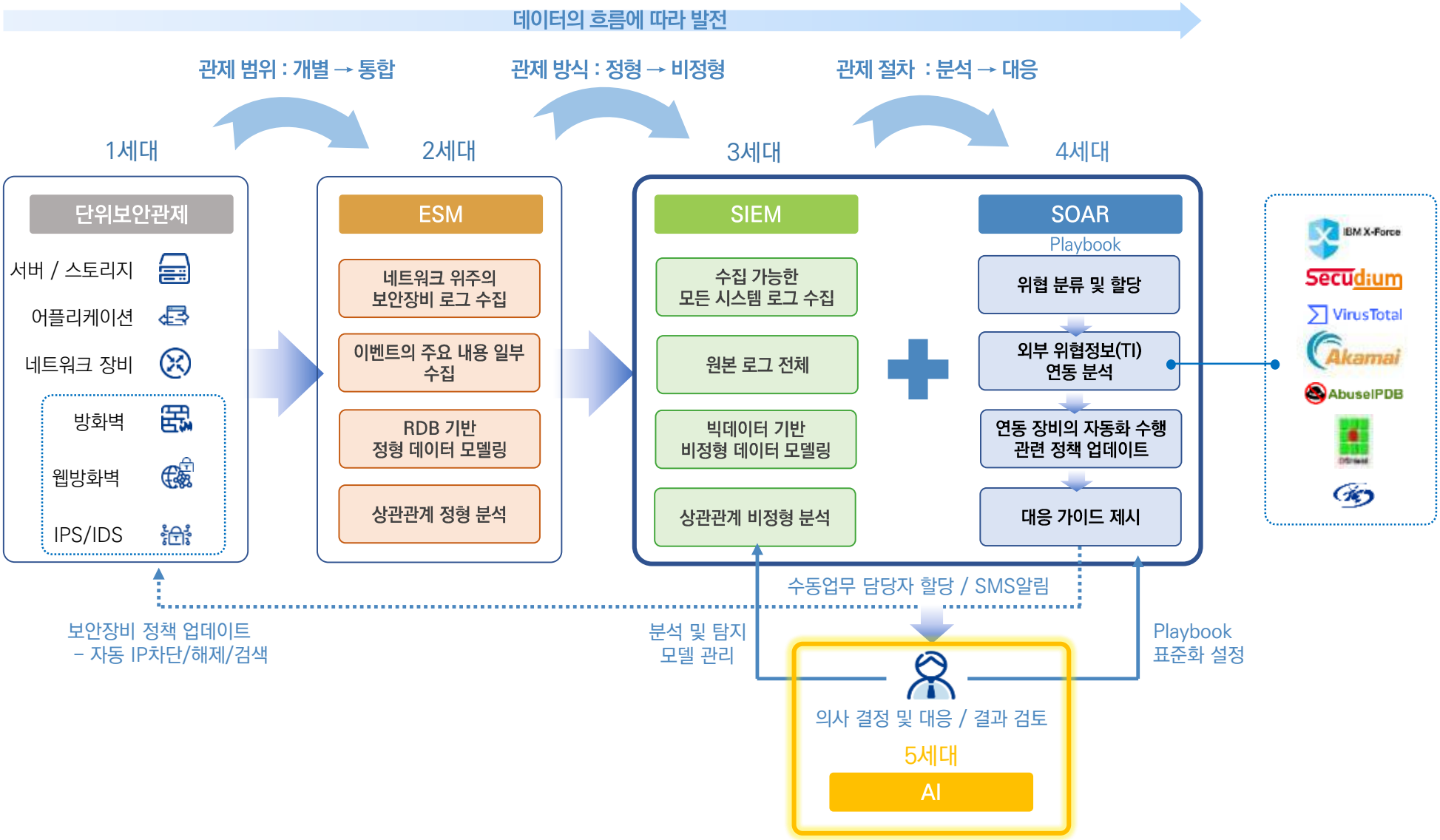
Workflow Systemization

Read Only → Read & Write

Deep (AI) & Wide (TI)

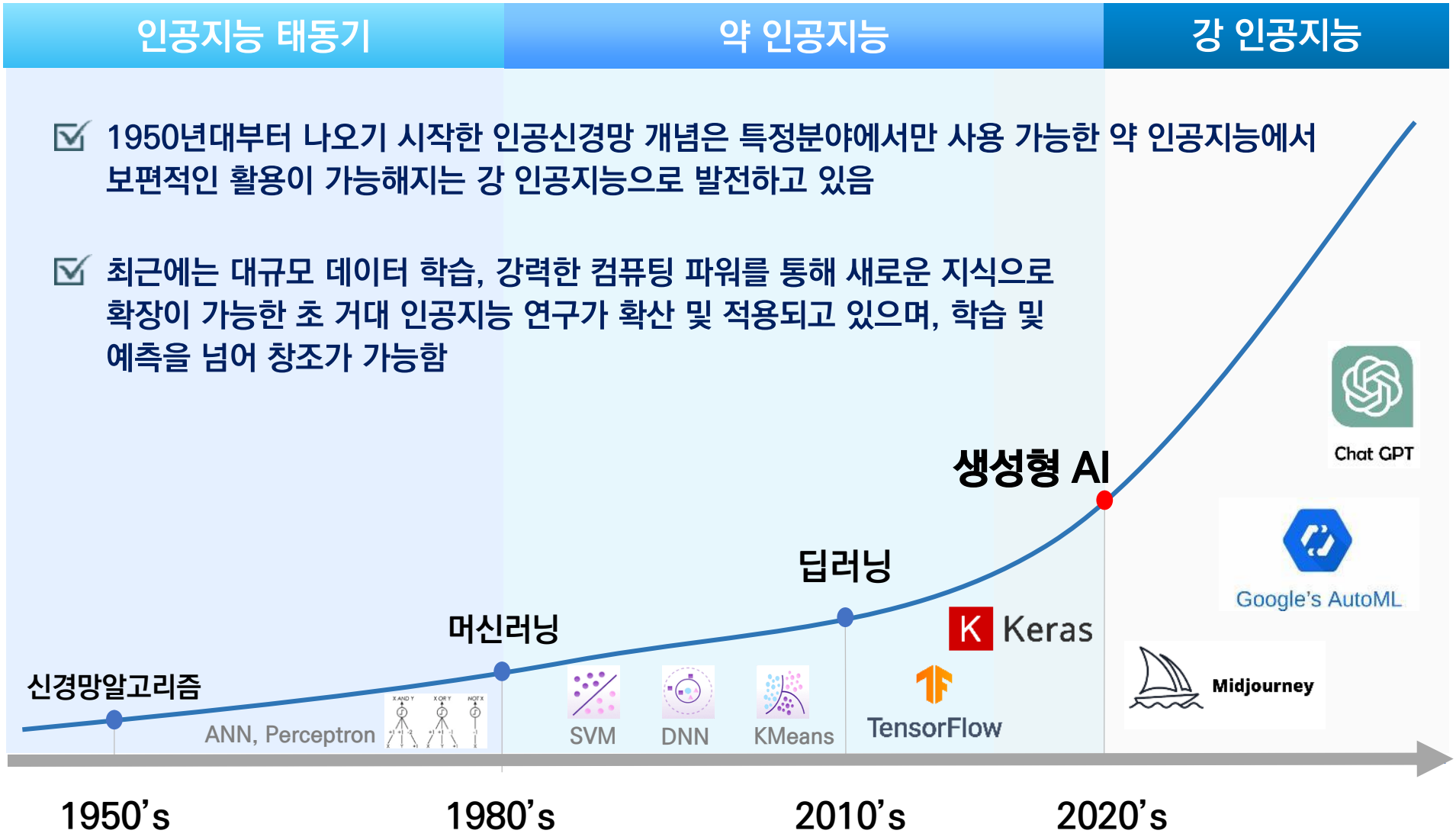
2018 Gartner, Inc.(ID : 322580)

4. AI


데이터의 흐름에 따라 발전
관제 범위 : 개별 → 통합
관제 방식 : 정형 → 비정형
관제 절차 : 분석 → 대응
1세대
단위보안관제
서버 / 스토리지
어플리케이션
네트워크 장비
방화벽
웹방화벽
IPS/IDS
2세대
ESM
네트워크 위주의 보안장비 로그 수집
이벤트의 주요 내용 일부 수집
RDB 기반 정형 데이터 모델링
상관관계 정형 분석
3세대
SIEM
수집 가능한 모든 시스템 로그 수집
원본 로그 전체
빅데이터 기반 비정형 데이터 모델링
상관관계 비정형 분석
4세대
SOAR
Playbook
위협 분류 및 할당
외부 위협정보(TI) 연동 분석
연동 장비의 자동화 수행 관련 정책 업데이트
대응 가이드 제시
IBM X-Force
Secudium
VirusTotal
Akamai
AbuseIPDB
수동업무 담당자 할당 / SMS알림
보안장비 정책 업데이트
- 자동 IP차단/해제/검색
분석 및 탐지 모델 관리
Playbook 표준화 설정
의사 결정 및 대응 / 결과 검토
5세대
AI

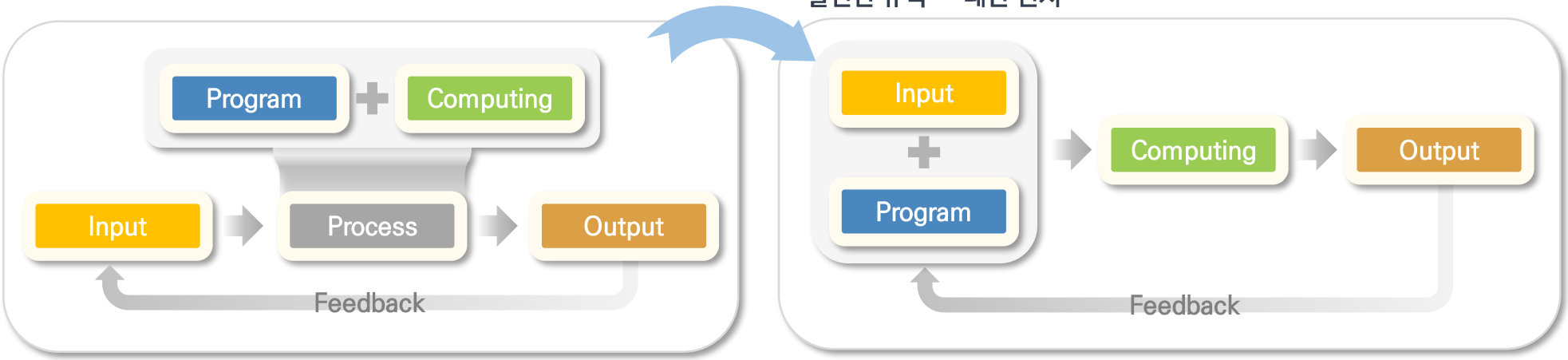
4. AI

발전 과정

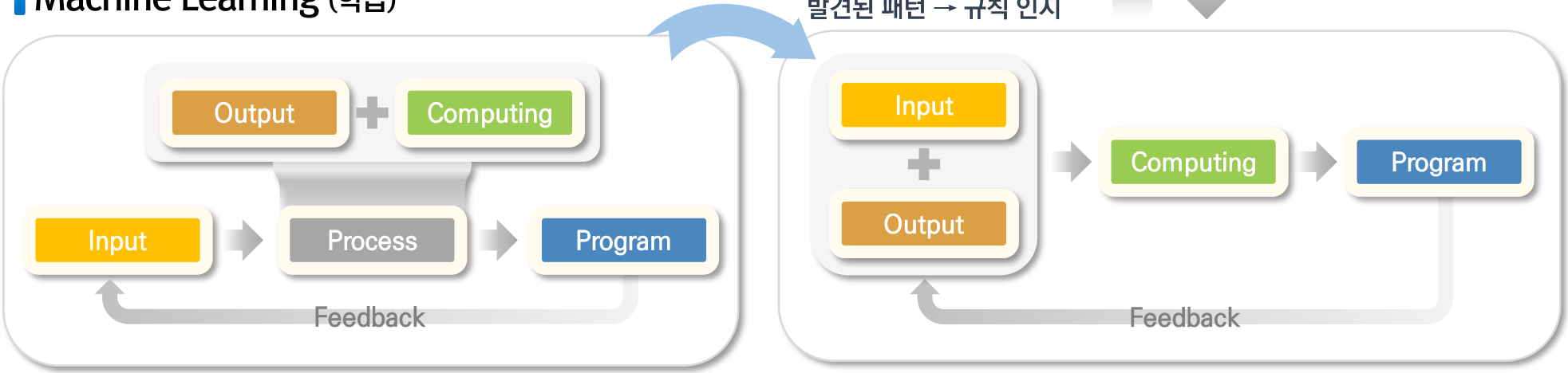

인공지능 태동기
약 인공지능
강 인공지능
1950년대부터 나오기 시작한 인공신경망 개념은 특정분야에서만 사용 가능한 약 인공지능에서 보편적인 활용이 가능해지는 강 인공지능으로 발전하고 있음
최근에는 대규모 데이터 학습, 강력한 컴퓨팅 파워를 통해 새로운 지식으로 확장이 가능한 초 거대 인공지능 연구가 확산 및 적용되고 있으며, 학습 및 예측을 넘어 창조가 가능함
생성형 AI
Chat GPT
Google's AutoML
Midjourney
딥러닝
Keras
TensorFlow
머신러닝
SVM
DNN
KMeans
신경망알고리즘
ANN, Perceptron
1950's
1980's
2010's
2020's

4. AI

Traditional System (추론)



Machine Learning (학습)

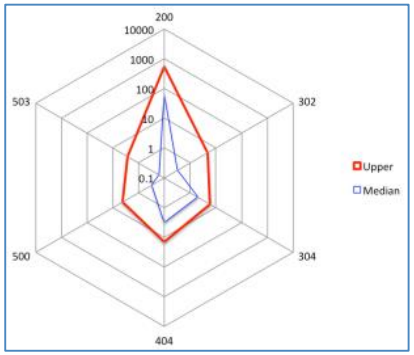


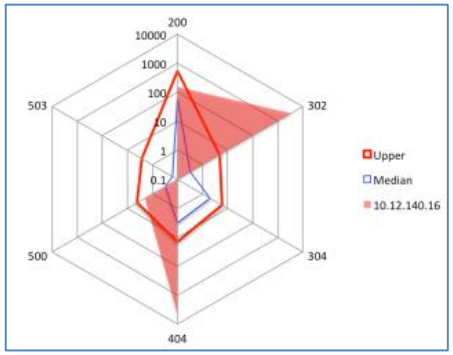
4. AI

Classification (Profiling)

- 모집단 내의 대상들에 대한 비슷한 패턴 분류

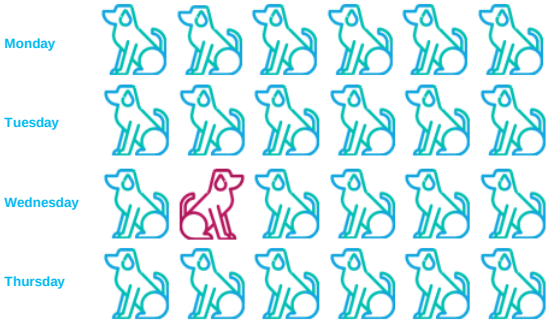
- Outliers in population (using entity profiling)





Anomaly Detection (Unusual)

- 비슷한 분류내에서 다른 대상들과 비교해 보기 드문 행동 패턴 탐지



- Unusual rates in “categories” of events (Single-Metric, Multi-Metric, Time Series)

4. AI

방식 및 용도에 따른 분류

분류

- Classification (지도학습) : DNN, CNN, RNN 등
- Clustering (비지도학습) : Kmeans, DBSCAN 등

패턴 인지 : 이미지 인식, 이상행위탐지 등

예측

- 회귀분석 (Linear 및 Polynomial Regression 등)
- 지도학습 ↔ 비지도학습 상호 보완적 운용

규칙 분석에 따른 수치 예측 : 주식전망 분석 및 투자, 장애 예측 등

생성

- Transformer, GAN 등
- 지도학습 ↔ 비지도학습 상호 보완적 운용

조합을 통한 콘텐츠를 생성 : 언어 생성, 이미지 생성 등

4. AI

생성형 AI

챗GPT 등 생성AI가 일으킬 수 있는 문제

데이터 오류	**챗GPT** 사실과 다른 내용 존재하지 않는 논문 인용
윤리 문제	**이루다(2021년), 테이(2016년)** 인종·소수자 혐오 발언
사이버 범죄 악용 가능성	**챗GPT** 텍스트 입력만으로 악성 코드 생성 가능
저작권 침해	**코파일럿** 자동 코드 생성 AI 서비스의 저작권 침해 논란

출처: 지민구 기자, 전남혁 기자, '증세 써내자 병 오진한 챗GPT, 근거 물으니 가짜 논문 제시', 2023.02.07.

국내외 규제 현황

- ☑ 이탈리아 : 챗 GPT 전면 금지
- ☑ EU : 인공지능법 제안
  (AI 정의, AI 위험수준 분류 및 분류별 의무,
  생성AI 학습 데이터 저작권 공개 의무화 등)
- ☑ 중국 : 챗 GPT 전면 금지,
  생성형 AI 관리 지침 초안 발표
- ☑ 미국 : AI 시스템 규제안 검토
- ☑ 캐나다 : 챗 GPT의 개인 정보 침해 여부 조사 검토
- ☑ 독일·프랑스·아일랜드 : 챗 GPT 금지 방안 검토
- ☑ 대한민국 : 챗GPT 등 생성형 AI 활용 보안 가이드라인,
  AI 개인정보보호 자율점검표 마련

국정원 / 국내의 경우, 법적인 규제보다는 가이드라인 및 자율 점검 권고
*** 국가정보원(국가보안기술연구소), 개인정보보호위원회**

4. AI

구분		분석	
		위협으로 탐지 O	위협으로 탐지 X
실제	위협/이상행위	정탐	오탐 (미탐)
	정상	오탐 (과탐)	정탐

4. AI

	SIEM	AI
분석방식	로그 상관 분석	패턴 인지 분석
탐지모델	시나리오 기반 룰셋	AI 학습 모델
탐지대상	알려진 위협	알려지지 않은 위협도 가능 (비지도 학습)

인공지능 기반
패턴 인지 분석시

❖ 단순 반복 업무의 기계적 처리 가능

정오탐 분석/분류

하루 2만건 분석에 필요한 인력

X 650 명 (1명당 / 30건 처리)

❖ 알려지지 않은 위협도 탐지

이상행위 탐지

비지도 • 강화 학습을 통한 신종 위협 탐지

숙련된 분석가가 장기간 분석
해야할 위협을 기계적으로 처리

4. AI

시큐레이어 AI 연구 및 개발

2021~2024 AI·빅데이터 기반 사이버 보안 오케스트레이션 및 자동 대응 기술 개발

사이버공격에 대한 선제적 대응을 위해 보안관제센터 全 업무 프로세스의 자동화(탐지→위협분석→대응) 및 AI를 활용하여 사이버 위협 의심정보를 자동 분류 할 수 있는 기술 개발 / 총 사업비 111억 규모

2020~2023 데이터 특징과 문제 정의를 인지하는 빅데이터 분석모델 추천 자동화 기술 개발

비전문가도 손쉽게 빅데이터를 분석 활용할 수 있도록 AutoML기술과 XAI를 활용한 빅데이터 분석모델 추천 자동화 기술 및 시스템 개발 / 총 사업비 75억 규모

2017~2020 진화형 사이버방어 가시화 기술 개발

지능형 사이버 자가 방어를 위한 인공지능 기반 다계층 고해상도 사이버방어 가시화 기술 개발
총 사업비 32억 규모

2015~2018 고급분석을 이용한 실시간 위험관리시스템 개발

금융부정행위 탐지를 위한 빅데이터 분석 프레임워크 및 시스템 개발/ 총 사업비 14억 규모

2015년 부터 인공지능/빅데이터 분석 관련 연구 **11건**

국가 연구과제 **총 340억 수행**

4. AI

시큐레이어 AI 연구 및 개발 (AutoAPE 연구)

AutoAPE

'AutoAPE'는 AutoML과 XAI 기술을 활용하여 인간(Human)의 DNA와 가장 흡사한 유인원 수준의 AI를 학습시켜 스스로 판단하여 가장 적절한 인공지능 모델을 추천하는 기술을 개발하겠다는 목표

4. AI

시큐레이어 AI 연구 및 개발 (AutoAPE 연구)

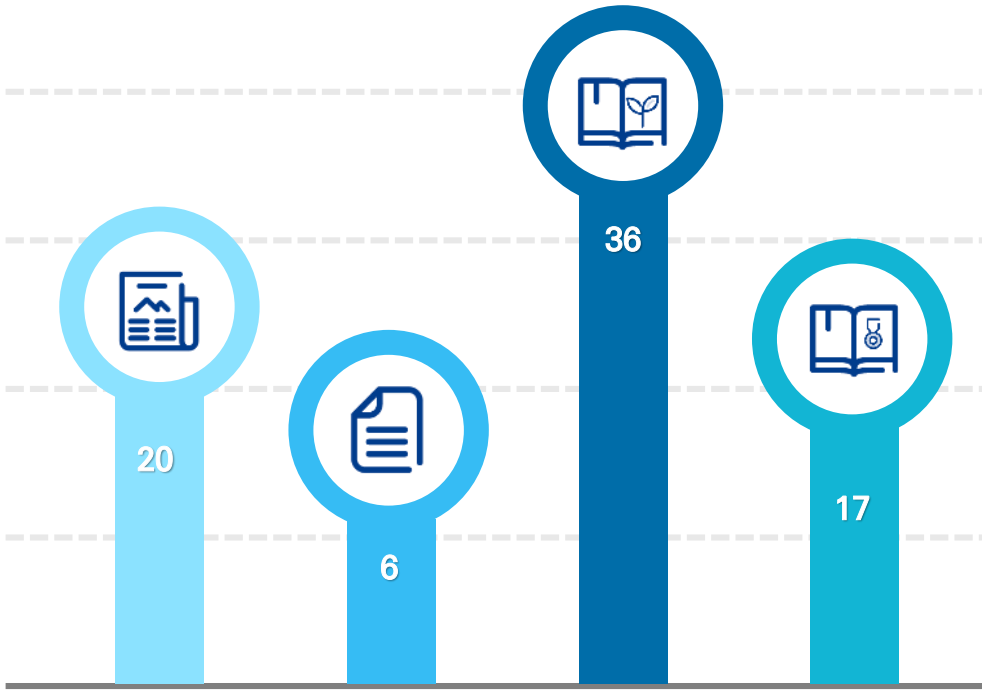
- 연구기간 2020년부터 2022년 총 3년간 관련 기술에 대한 다양한 성과 창출
- 숫자를 위한 성과가 아닌 질적으로 높은 수준의 성과를 달성(ImpactFactor, SMART 특허 가치평가 진행)

SCI급 논문 20건 게재 완료
(ImpactFactor : 평균 3.03)

기타 학술대회 논문 6건 게재
(한국인터넷정보학술대회)

특허출원 36건 달성
(HPO기술, XAI기술 외)

특허등록 17건 달성
(SMART 평가 지수 : B등급 이상)



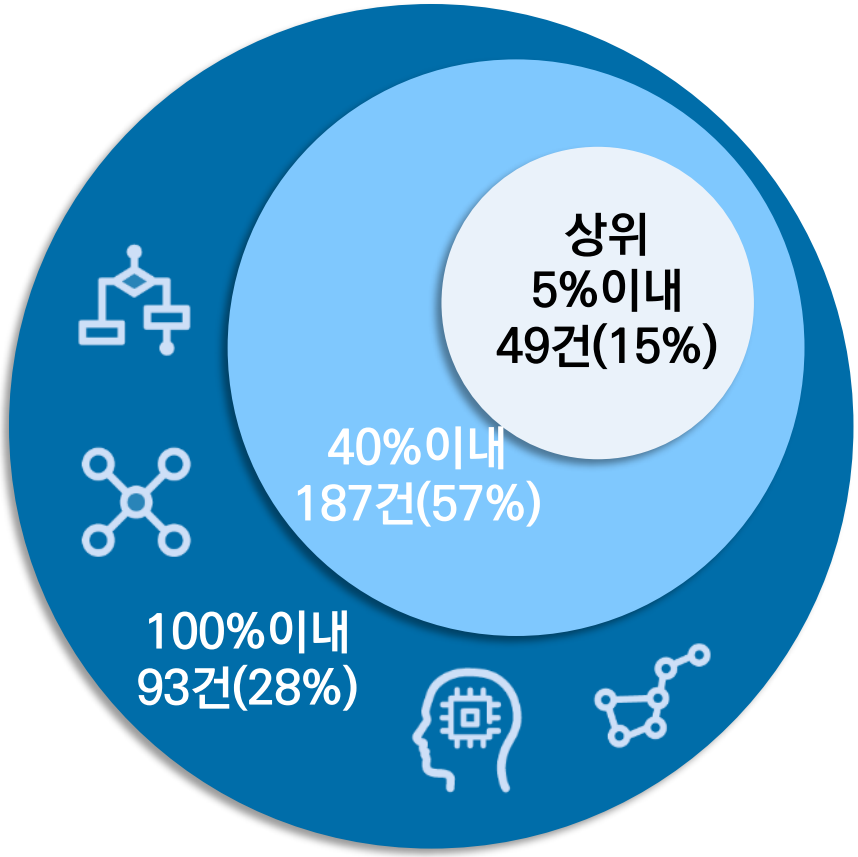
개발 성과(2020년 ~2022년 3년 기준)

4. AI

시큐레이어 AI 연구 및 개발 (Kaggle 인공지능 대회)

kaggle

Kaggle(캐글)이란? 전 세계 데이터 사이언스 경진대회 플랫폼, 600개 이상의 다양한 데이터 분석 대회



- 'AutoAPE' 모델 훈련을 위해 다양한 데이터가 모여 있는 Kaggle과 Dacon 인공지능 대회 수행
- 매년 100개 이상의 데이터 분석 경진대회 수행
  2020년~2023년 3년간 출전한 인공지능 경진대회
  총 329건
- 다양한 데이터에 대한 학습 경험으로 지식 데이터베이스 생성, 데이터 특징에 맞는 인공지능 모델 자동 추천 가능

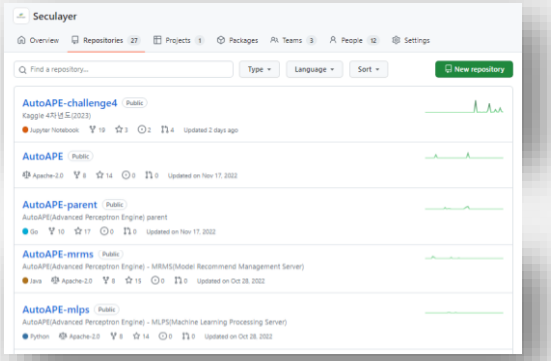
4. AI

시큐레이어 AI 연구 및 개발 (오픈소스 & 커뮤니티 사이트 운영)

GitHub

오픈소스 연구로 진행, 관련 내용을 시큐레이어 MS 산하의 GitHub를 통해 공개중
누구든지 접근하여 사용할 수 있으며, 공개를 통한 데이터확보 및 플랫폼 강화 목적

공개 저장소 운영

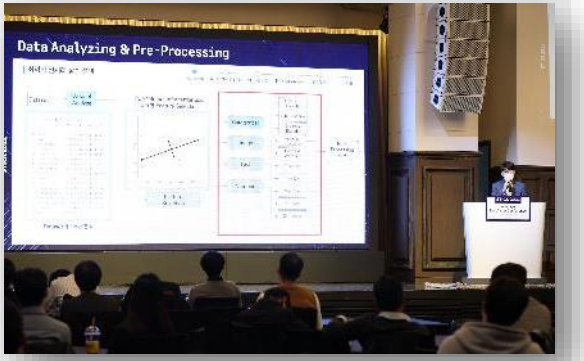


- AutoAPE관련 공개 GitHub 저장소 17개 운영
- 관련 저장소 STAR 150개, 연구 기여자 93명

커뮤니티 사이트 오픈

- AutoAPE 연구 성과 홍보 및 오픈소스 사용 가이드
- 연구 전반에 대한 설명과 고객지원을 위한 창구 마련

기술 세미나 STICK2023

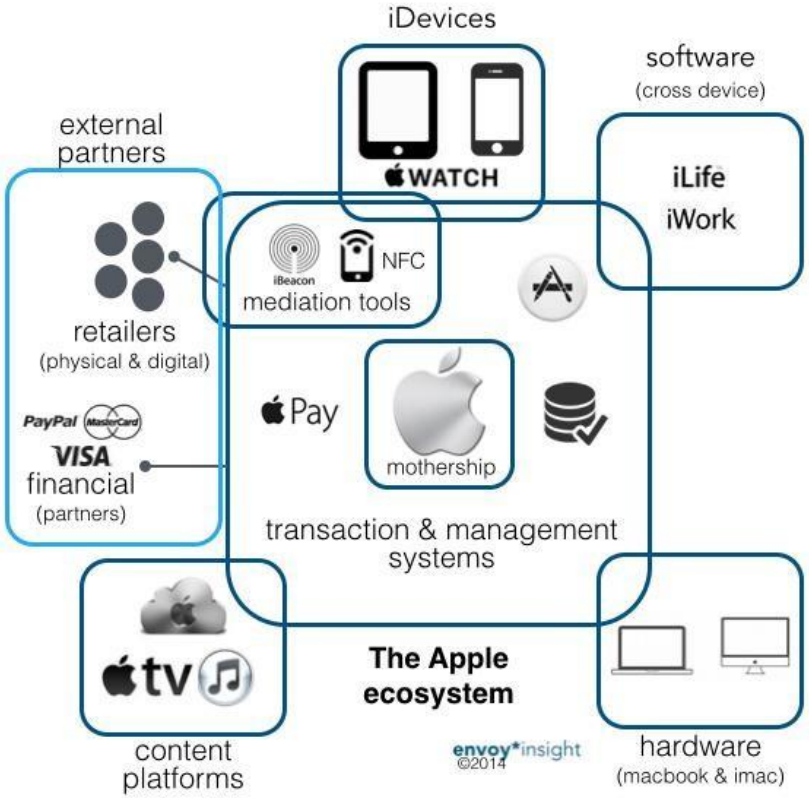


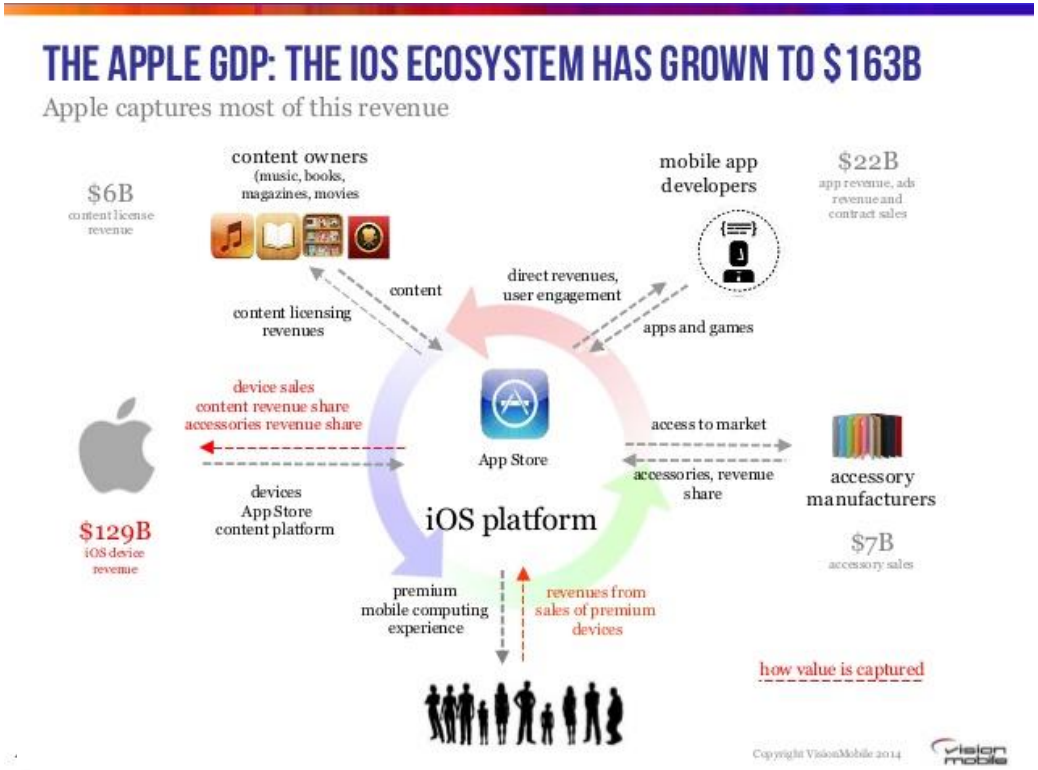
- 연구 내용을 대중에게 홍보하기 위한 세미나 개최
- AutoML, XAI, 정보보안 동향 등 다양한 주제 발표

5. 아키텍쳐 (Architecture)

Ecosystem

Apple Ecosystem

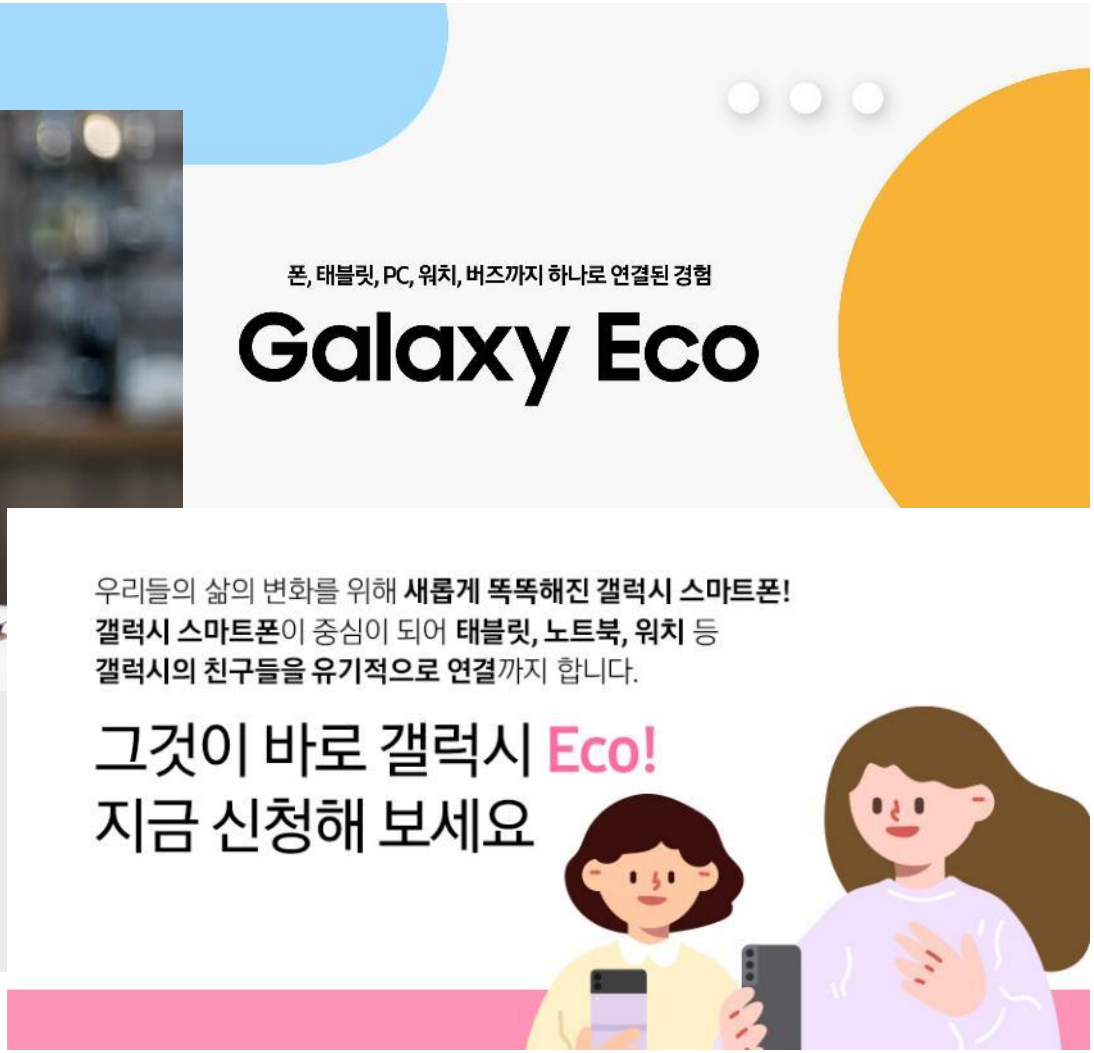




5. 아키텍쳐 (Architecture)

Ecosystem

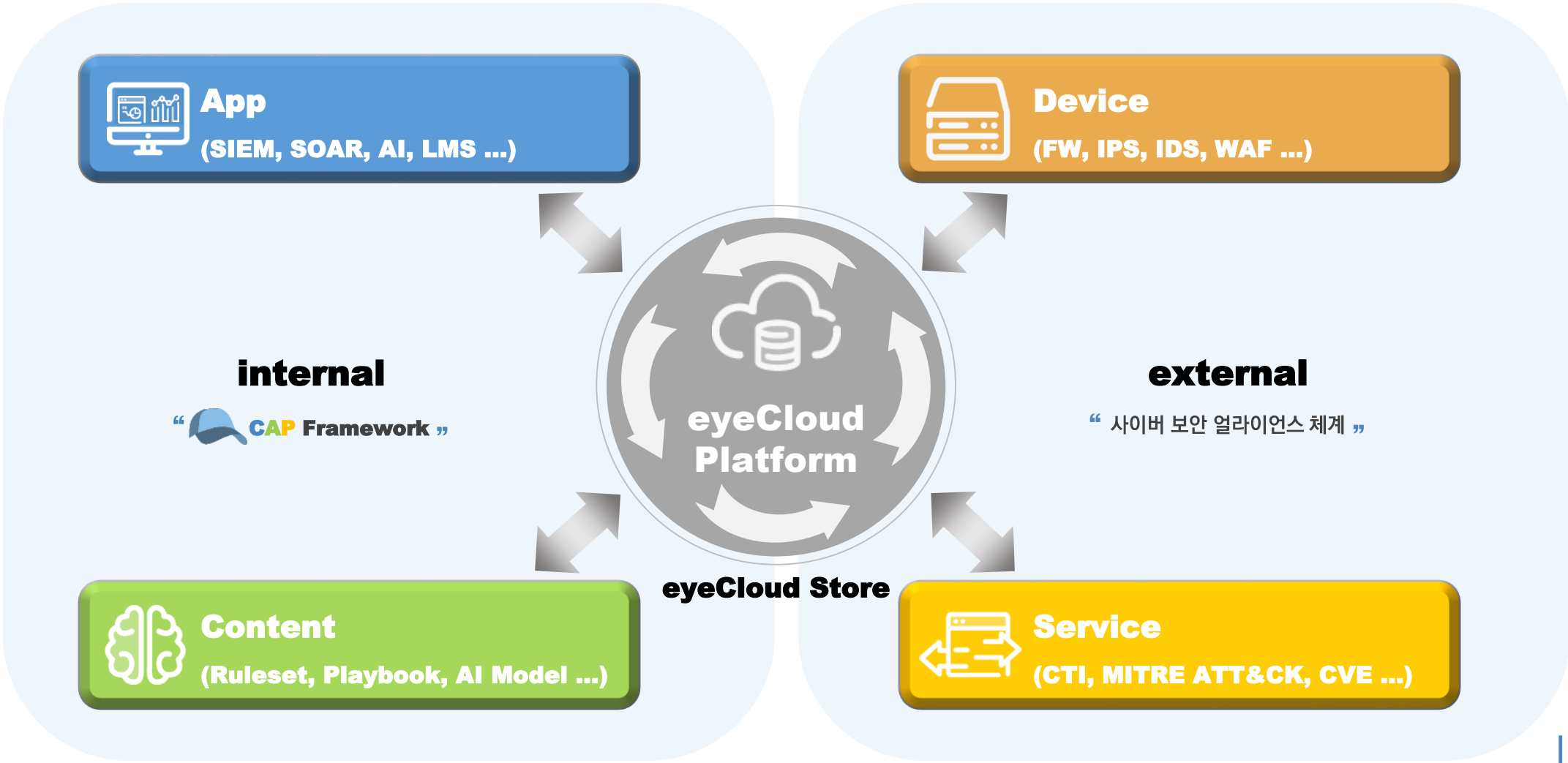
Galaxy Ecosystem



5. 아키텍쳐 (Architecture)

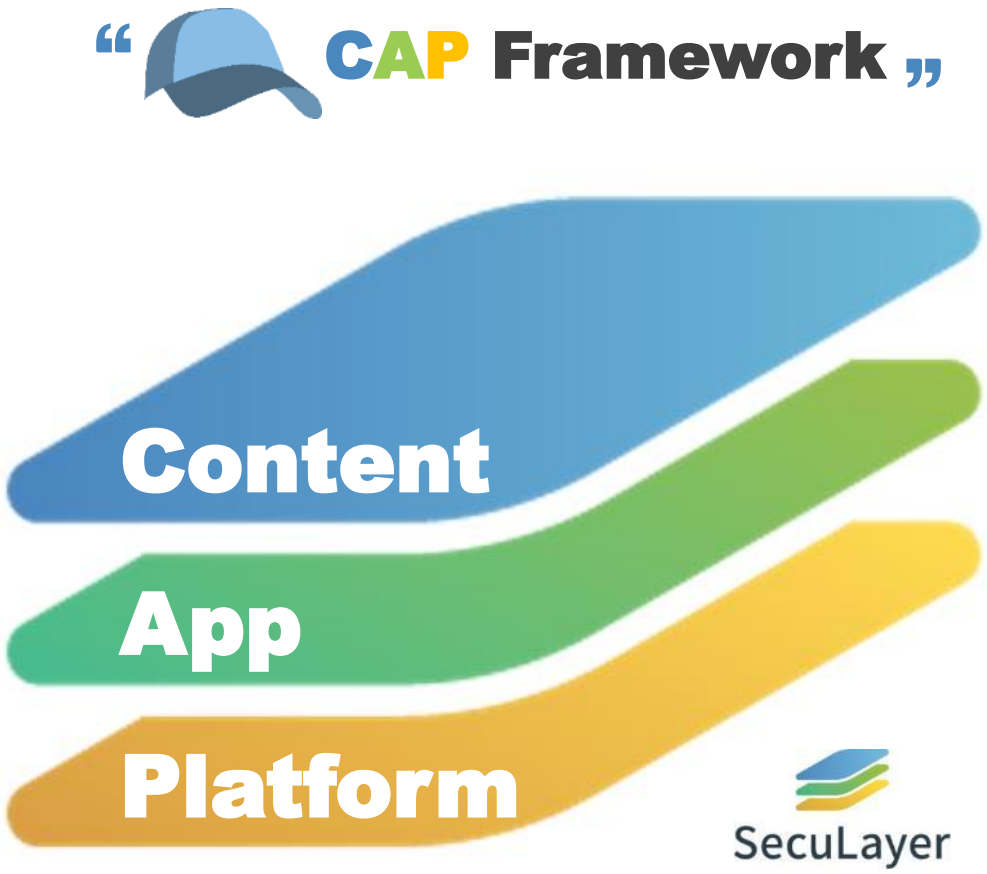
eyeCloud Ecosystem

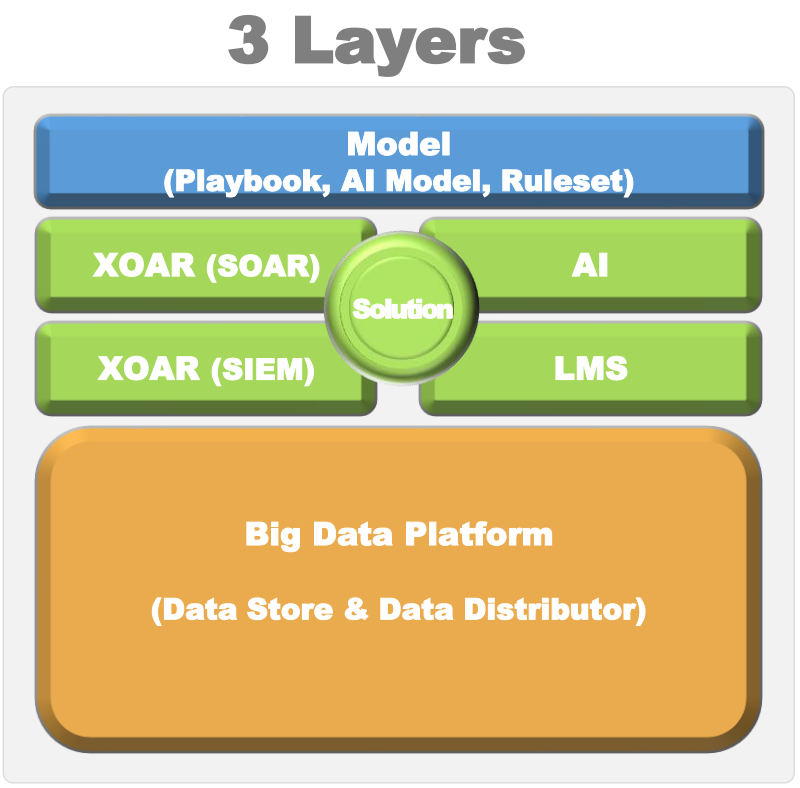
eyeCloud Platform 기반의 정보보호 운영 생태계



5. 아키텍쳐 (Architecture)

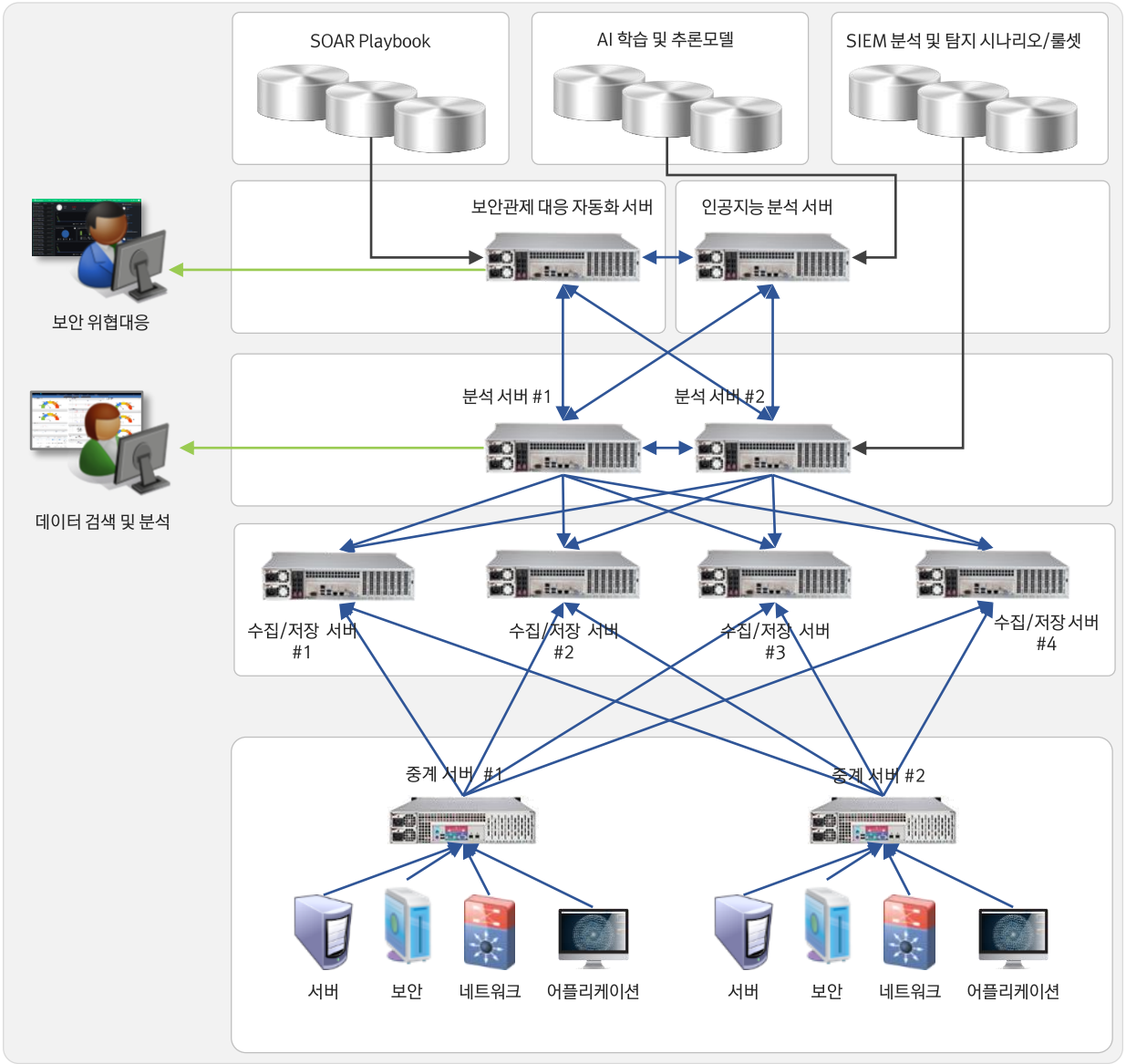
Framework

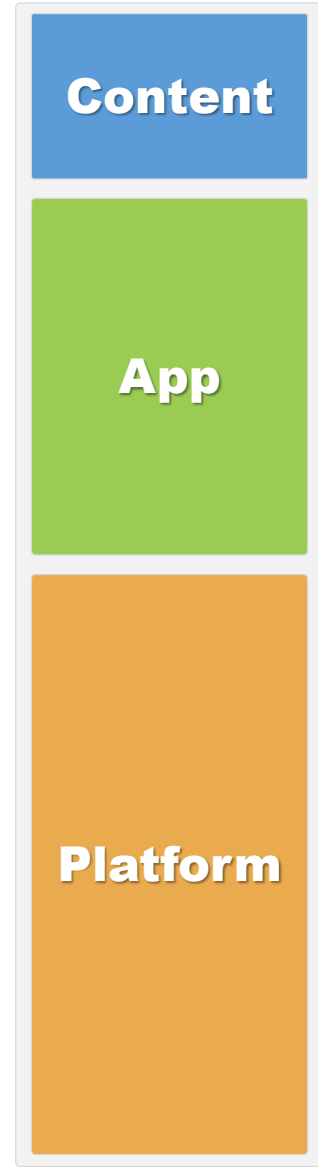




5. 아키텍쳐 (Architecture)

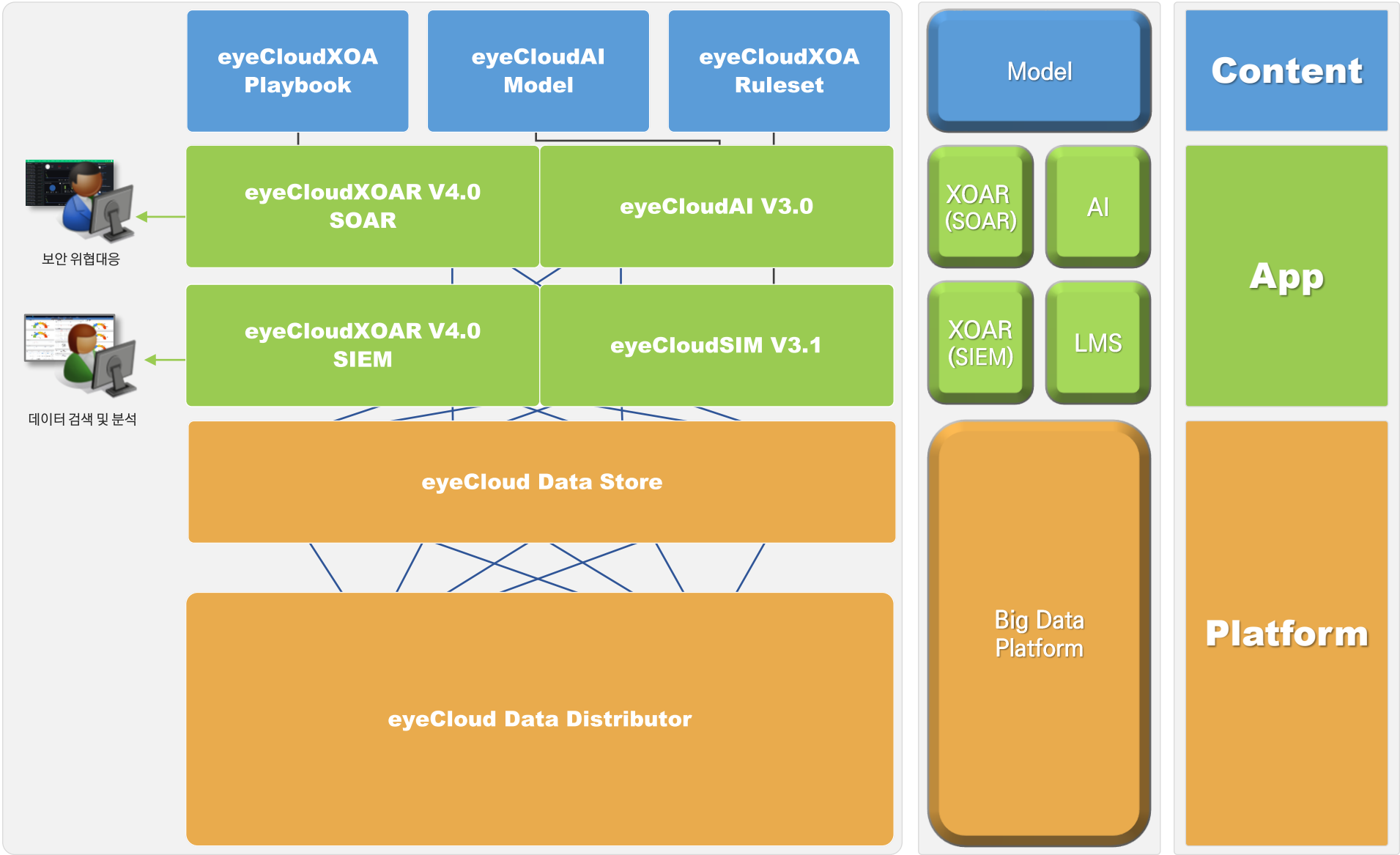
System 구성





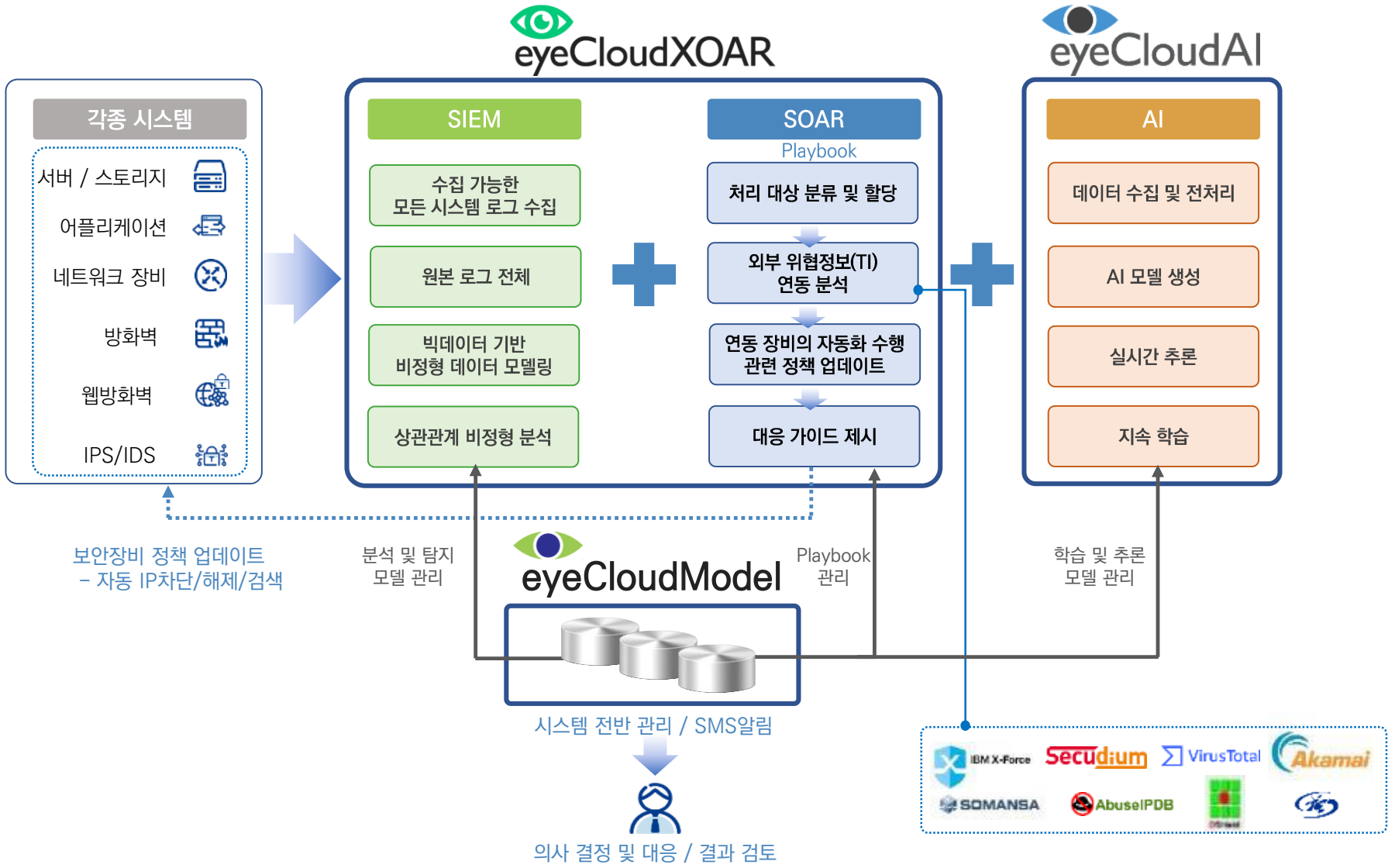
5. 아키텍쳐 (Architecture)

Software 구성



5. 아키텍쳐 (Architecture)

프로세스




RSAConference™2023
San Francisco | April 24 – 27 | Moscone Center
Stronger Together
RSAConference™
"Stronger Together"
Josh Aaron
CEO
Laura Brown
VP, Sales
Aaron Mellman
Director of Marketing
JOIN US
Apr. 24th - 27th
Moscone Center
San Francisco, Ca
More Information : meetaiden.com/events

식사 장소

일일향 (日日香)

서울 성동구 성수일로6길 47 2층

- ☑ 거리 : 561M
- ☑ 소요시간 : 8분
- ☑ 이동수단 : 도보


감사합니다.