IGLOO

AI-Driven Open XDR과 함께하는

변화하는 보안 환경 대응

이글루코퍼레이션 전략기획팀

이규환 수석부장

IGLOO

Contents.

IGLOO

AI-Driven Open XDR과 함께하는 변화하는 보안 환경 대응

1. 변화하는 보안 환경

격변하는 세상, 변화하는 보안 환경(1)

* 2025년 사이버 보안 위협 및 기술 전망 보고서(이글루코퍼레이션, 2024)

격변하는 세상, 변화하는 보안 환경(2)

국내 보안 환경의 주안점

기술

AI보안

AI를 보안에 어떻게 활용할 것인지,
그리고 AI를 활용한 공격을 어떻게 막을 것인지

XDR

전통적인 SIEM, SOAR, 엔드포인트 보안이 아닌 XDR로의 귀결,
그리고 네이티브 XDR과 오픈 XDR

정책

Zero Trust

기존의 신뢰를 바탕으로 한 레거시 보안 체계가 아닌,
ZeroTrust 환경에서 어떻게 새로운 보안 체계를 만들 것인가?

N2SF(National Network Security Framework, 국가망보안체계)

국가망보안체계에 맞춘 다양한 활동과 정책 변화에 대한 대응

시장

보안업체간 협업

제로트러스트, 나아가 N2SF를 수행하기 위해서는
혼자서는 불가능

정부에서도 협업 기조를 끌고 가는 중(K-시큐리티 얼라이언스 등)이며,
민간에서도 적극적으로 협업체계 구축 중

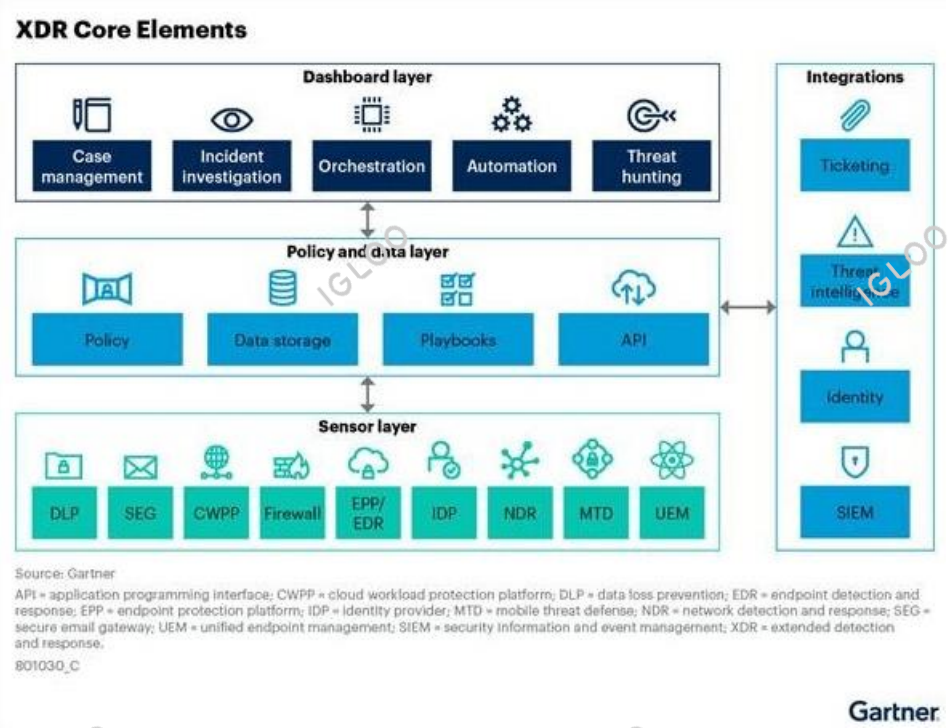
IGLOO

AI-Driven Open XDR과 함께하는 변화하는 보안 환경 대응

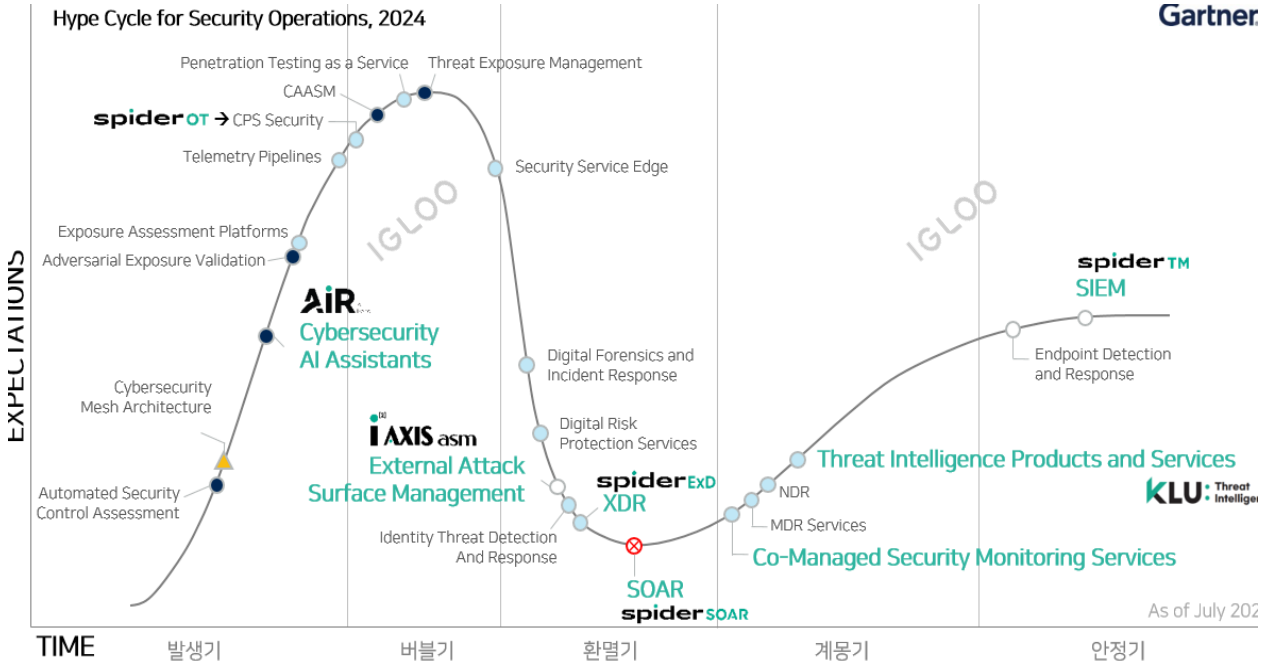
2. AI-Driven Open XDR

XDR 개요

XDR(eXtended Detection and Response, 확장 탐지 및 대응)
→ 데이터를 자동으로 수집하고 상호 연결하는 통합 보안 사고 감지 및 대응 플랫폼 *by Gartner*



* Market Guide for Extended Detection and Response (Gartner, 2024)



* Hype Cycle for Security Operations(Gartner, 2024, 이글루코퍼레이션 재구성)

Native XDR과 Open XDR

보안관제, 나아가서 통합보안관리를 위한 XDR

Management & Governance

관리&거버넌스

MG.SL 서비스수준관리
- 평가지표 개발
- 미흡/개선사항 도출

MG.MP 지침/절차 개정
- 보안관제 운영지침/절차 개정
- 중장기 발전방향 도출

MG.WS 근무체계 관리
- 근무체계 도출
- 근무체계 개선 및 적용

MG.SE 평가
- 평가항목 도출
- 미흡/개선사항 도출

MG.CE 인증
- 정보보호관리체계 인증
- 지속적인 관리 및 개선

MG.SP SOC보호 및 시스템운영
- SOC 물리보호체계 구축
- 내부시스템 운영/관리

Identify

식별

ID.AM 자산관리
- 자산 목록화
- 자산 R&R, 가치평가

ID.BE 비즈니스환경분석
- 외부연계 목록화
- 비즈니스 영향분석

ID.GV 법적요건
- 관련 법/규정 이해와 관리
- 정보보안정책 확립

ID.RA 위험식별 및 관리
- 내·외부 위협 식별
- 문서화 및 위험허용 관리

ID.SO 운영관리
- 관제 범위/대상 파악
- 직무별 업무소요량 산정

Protect

예방

PR.VA 취약점진단
- 진단대상 목록화
- 취약점도출 및 대응방안 마련

PR.DT 모의침투/인식훈련
- 모의침투/인식훈련방법수립및시행
- 대응체계 이슈도출및대응체계 최적화

PR.SH 보안시스템 최적화
- 보안시스템 정책점검
- 이슈사항 도출 및 정책최적화

PR.PP 대응체계 수립
- 분야별 대응체계 수립
- 대응체계 점검 및 개발

PR.IS 정보공유
- 글로벌 위협수집
- 정부공유체계 수립

Detect

탐지

DE.EC 보안이벤트 수집
- 관제대상 이벤트 및 로그 수집
- 위험도 산정 및 경보설정

DE.DA 탐지 및 분석
- 보안이벤트 모니터링
- 상세분석 및 초동대응

DE.RA 대응 및 조치
- 상황전파 및 추가대응
- 보고 및 종결

DE.PH 탐지프로세스관리 및 정책최적화
- 탐지프로세스 관리
- 탐지정책 최적화

Respond

대응

RS.IA 침해사고 분석
- 접수 및 위험도 분석
- 자체분석 / CERT지원

RS.IP 침해사고 대응
- IP차단 및 격리
- 과거이벤트 분석

RS.CO 상황전파
- 보고체계 및 상황전파
- 정보공유 및 협업

RS.MI 확대방지
- 침입경로 및 취약점 상세분석
- 프로파일링 (공격기법 및 위협)

RS.IM 개선
- 침해사고 프로세스 검토
- 개선사항 업데이트

Recover

복구

RC.RP 복구계획
- 분야별 복구계획 수립
- 지속적인 관리 및 개선

RC.IM 개선
- 개선사항 통합
- 복구전략 업데이트

RC.CO 커뮤니케이션
- 비상연락망 현행화
- 단계별 보고체계 점검

보안관제방법론에서의 XDR의 역할

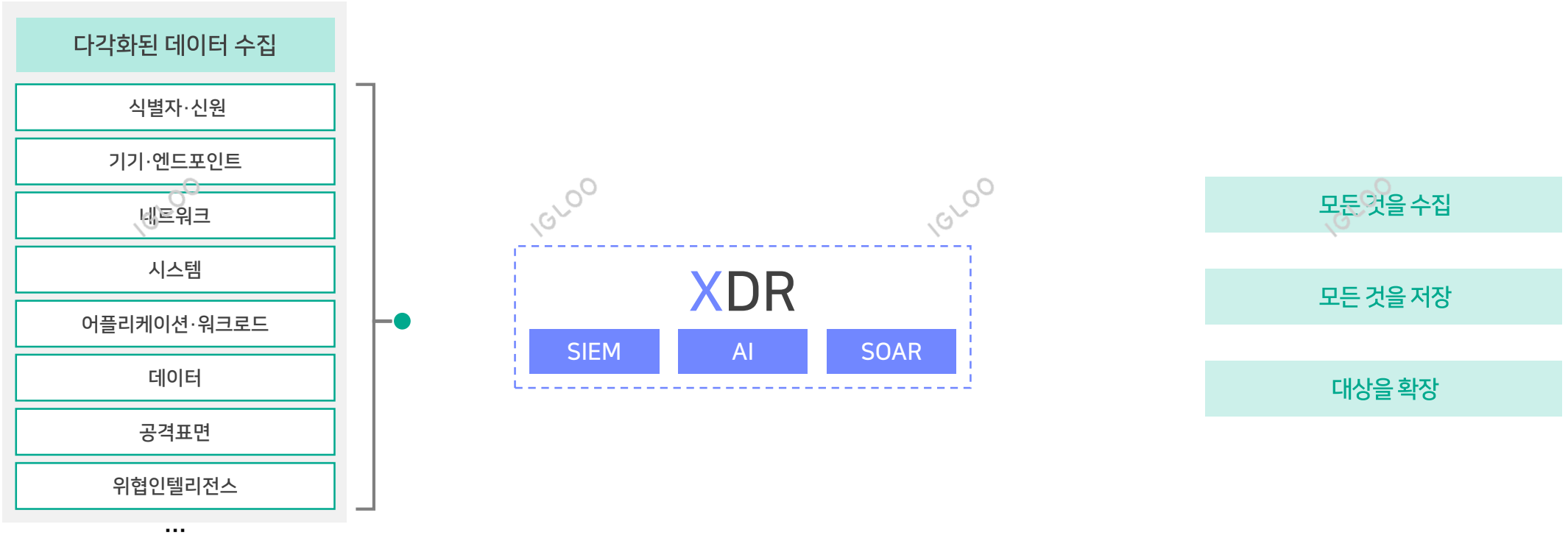
이글루가 생각하는 XDR

XDR은 솔루션의 관점에서는 SIEM, AI, SOAR의 결합
그리고, 보안운영의 관점에서는 통합보안운영 및 관제의 노하우의 결합

이글루가 생각하는 XDR

X의 기능에서는 모든것을 식별해야 합니다. 여기에서 모든것은 기존의 보안장비가 아닌, 보안과 관련된 모든것을 뜻합니다.

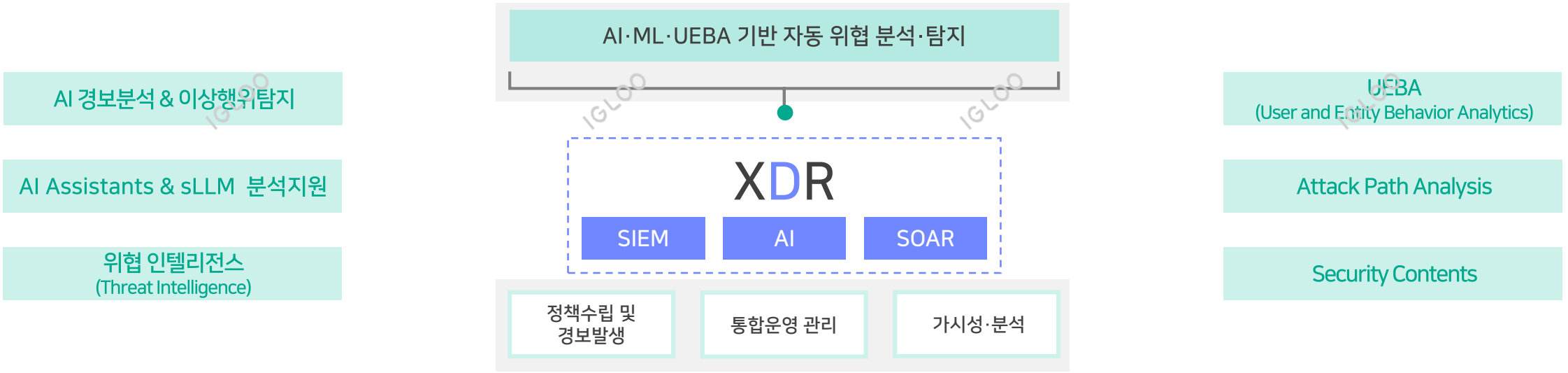
기존의 네트워크보안장비의 보안 요소를 넘어 제로트러스트의 핵심요소, 최근에 지속적으로 이슈가 되고 있는 공격표면이나 위협인텔리전스 등 모든 것을 수집하고 분석할 수 있어야 합니다.



이글루가 생각하는 XDR

D의 기능에서는 수집한 모든것을 탐지, 분석할 수 있어야 합니다.

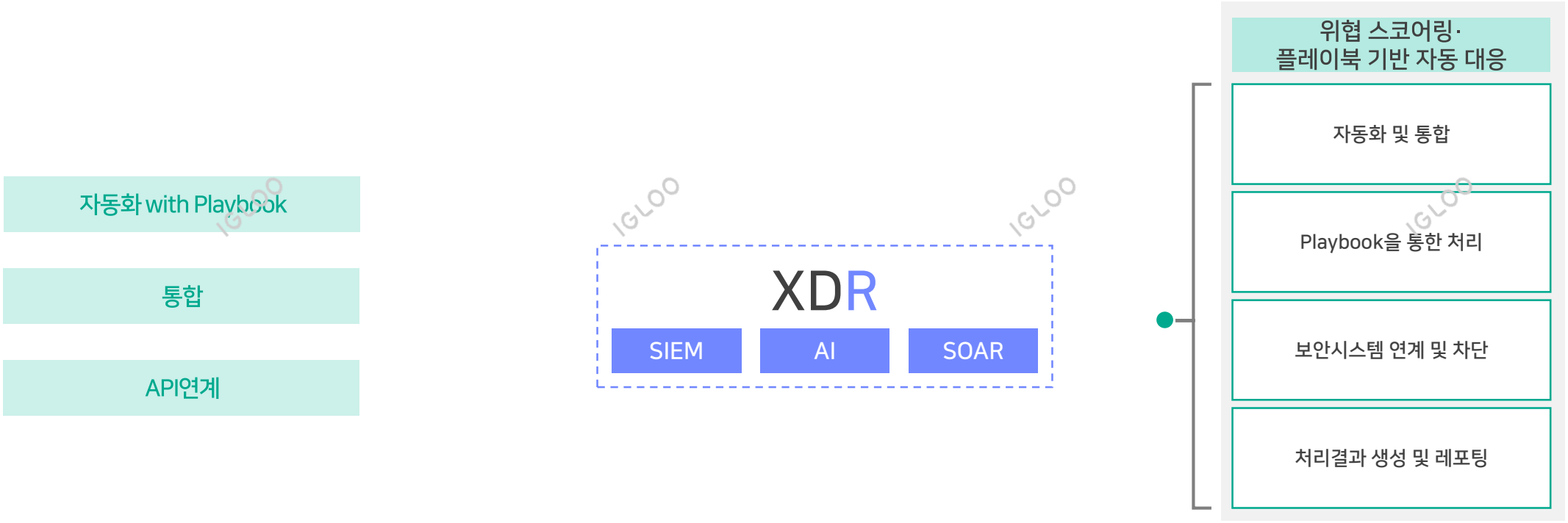
이를 위해서는 AI, ML, UEBA 기반 자동 위협 분석 및 탐지를 수행해야 하고
이러한 부분은 단순히 기능적인 요소가 아닌, 보안운영 및 관제에 대한 노하우가 반영 되어야 합니다.



이글루가 생각하는 XDR

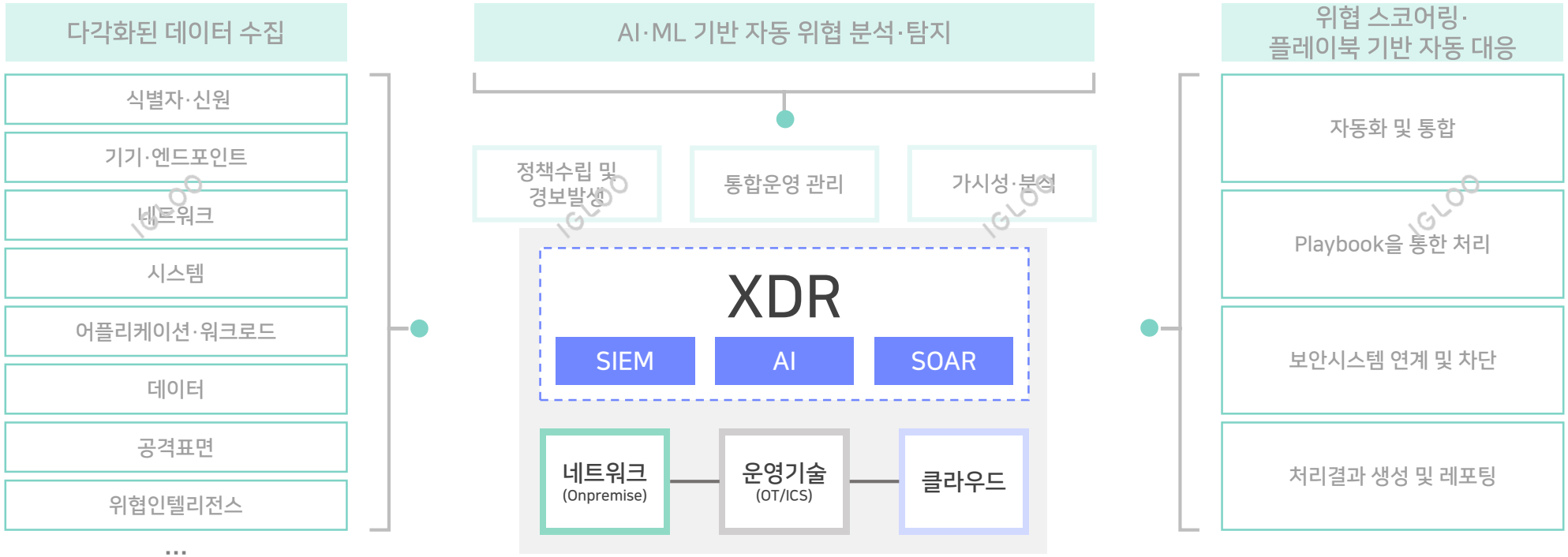
R의 기능에서는 자동대응이 핵심 요소입니다.

여기에는 Playbook을 활용한 SOAR의 기능을 통해 보안 오케스트레이션 및 자동화가 이루어집니다.
보안운영인력이 운영 시 불필요한 요소는 자동화 하고, 이를 통해 보안운영의 성숙도를 향상 시킬 수 있습니다.



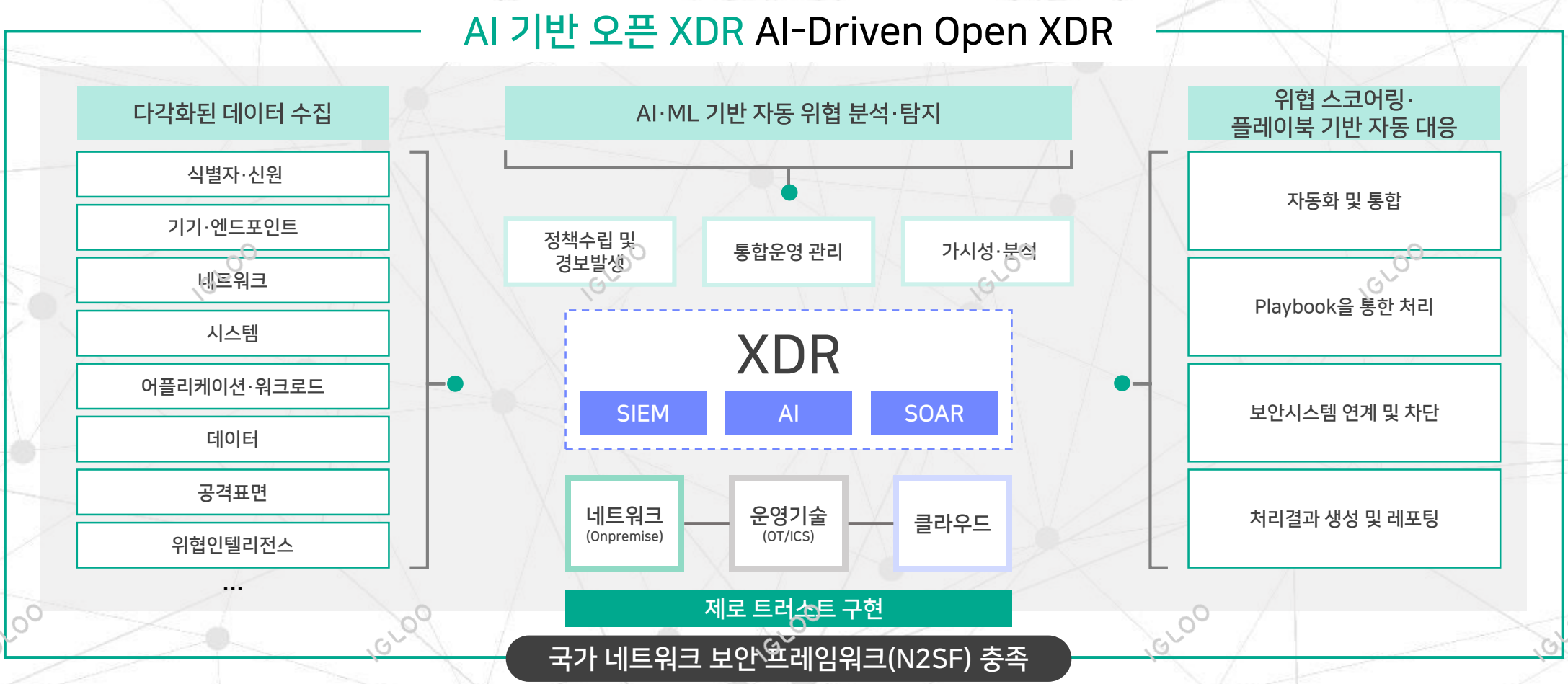
이글루가 생각하는 XDR

이러한 XDR의 가장 중요한 요소는 기존의 네트워크를 기반으로 한 레거시 보안 환경 뿐만 아니라
새로운 영역, OT/ICS와 같은 산업보안의 영역, 클라우드의 영역에서도 이러한 프로세스의 업무를 수행할 수 있어야 합니다.



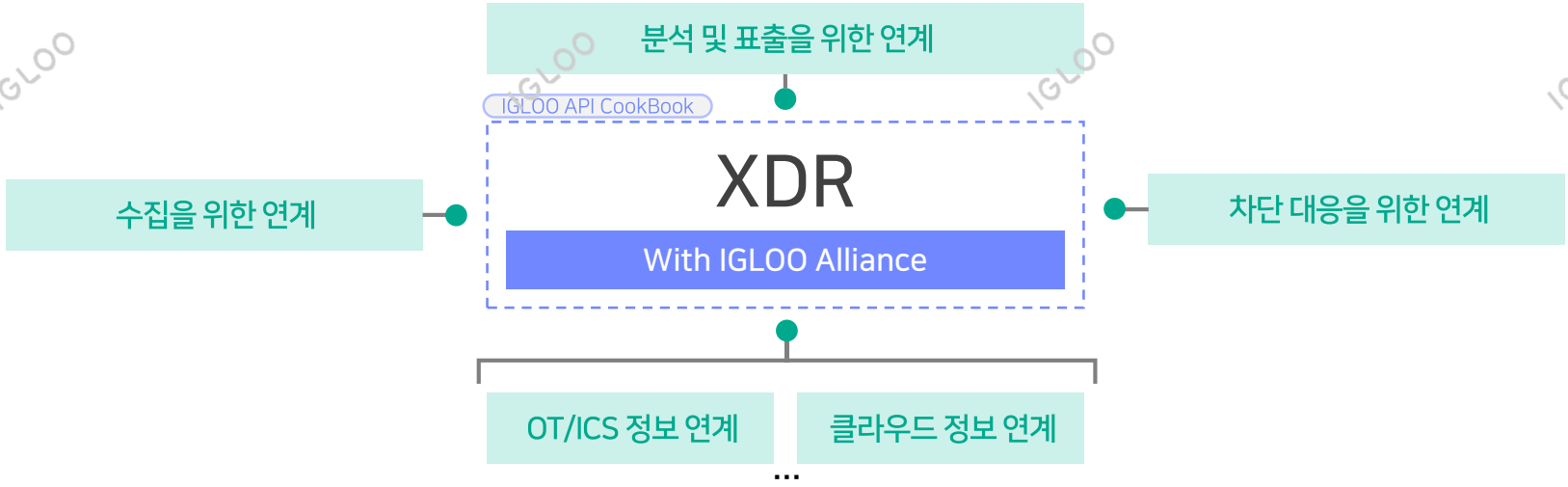
이글루가 생각하는 XDR

지금까지 말씀드린 XDR의 전략은 이글루만의 오픈 XDR 전략(AI-Driven Open XDR)으로 구현했으며
이를 통해 보안 운영·분석·대응 효율성을 극대화할 수 있습니다.



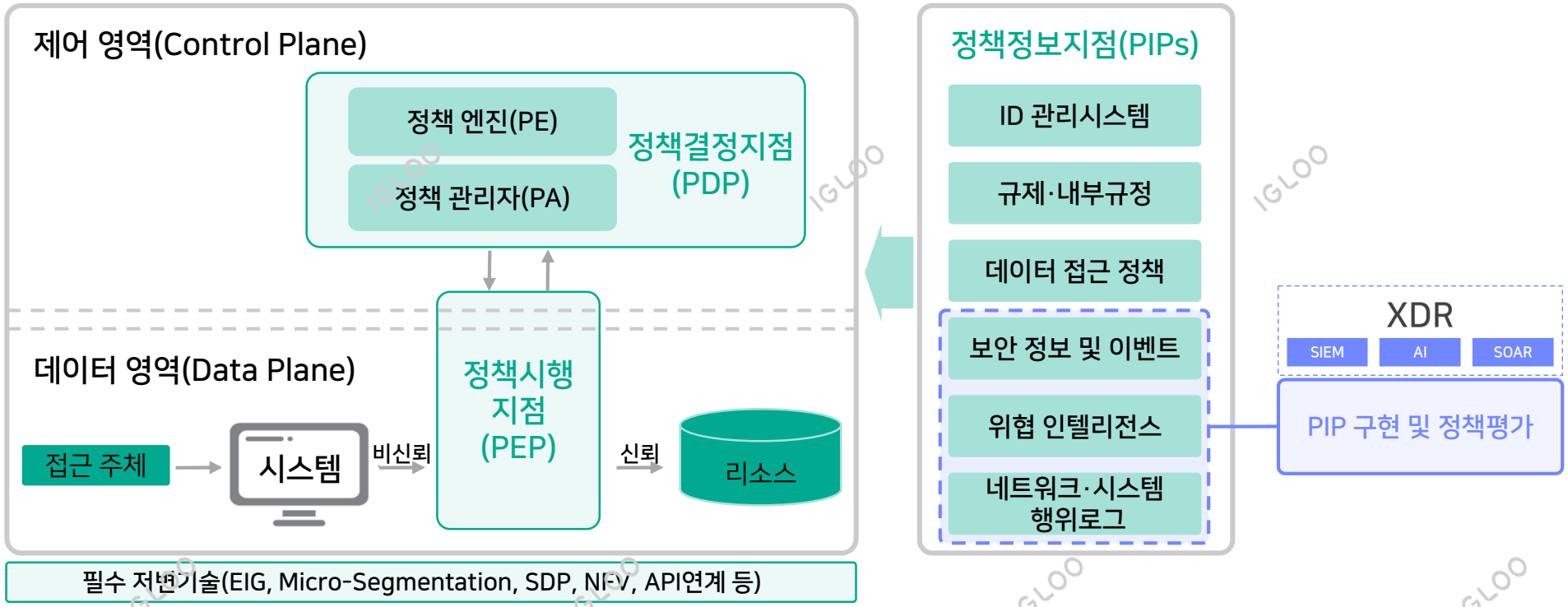
그리고 Alliance

Open XDR의 가장 중요한 요소는 연계 그리고 협업



Zero Trust에서는…

Zero Trust 환경에서 XDR은 정책 정보 지점에서 PIP 구현 및 정책 평가를 수행



N2SF(국가 네트워크 프레임워크, National Network Security Framework) 에서는…

N2SF 환경에서 XDR은 정보의 흐름을 모니터링 하고 분석하기 위한 핵심 역할을 수행

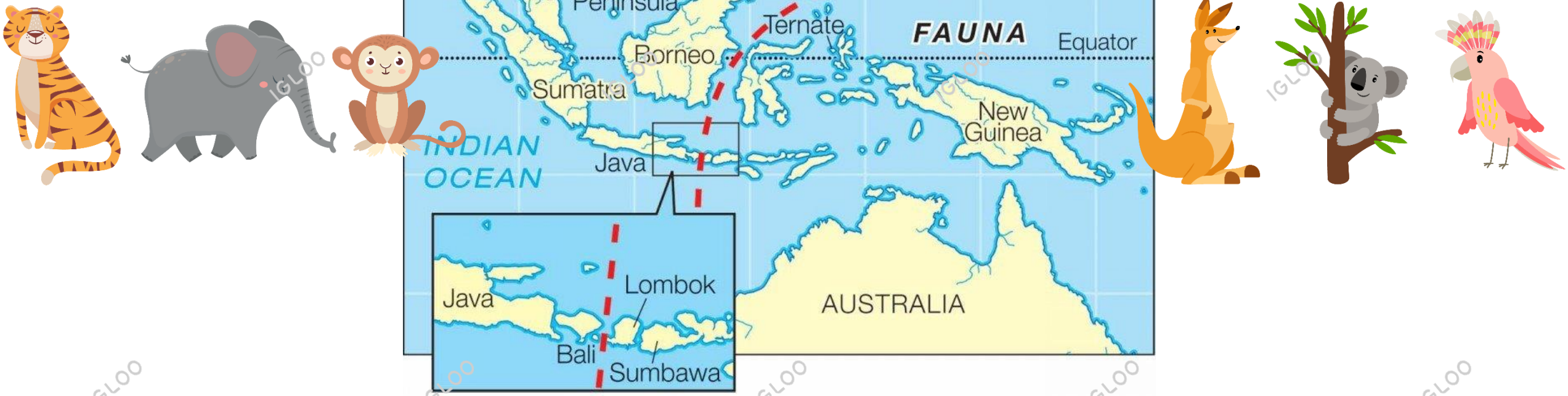
[국가 망 보안체계(N2SF)]

IGLOO

AI-Driven Open XDR과 함께하는 변화하는 보안 환경 대응

3. 마무리

그거 아세요? - 월리스선(Wallace line) 이야기



보안업체의 DNA, 그리고 이글루코퍼레이션

이글루코퍼레이션은
보안 조직의 어려움을 해결하는 조력자이자
새로운 비즈니스 기회를 제시하는 길잡이입니다.

이글루에게 물어보세요

이러한 DNA를 가지고 있는 이글루코퍼레이션은 이를 위한 다양한 솔루션과 서비스를 가지고 있습니다.
이글루코퍼레이션이 추구하는 XDR전략은 무엇인지, 이를 표출하는 이글루코퍼레이션의 SPiDER ExD는 어떤 모습일지,
그밖에 이글루코퍼레이션이 여러분들에게 해줄 수 있는게 무엇인지 궁금하시다면, 이글루코퍼레이션에게 물어봐 주세요.

보안 분석·운영·관리

XDR 기반 차세대 보안관제 플랫폼 (SIEM)

spider ExD

보안 운영·위협 대응 자동화(SOAR)

spider SOAR

AI 보안 어시스턴트

AiR AI Road

웹페이지 접속 | API 연동

GPU/NPU 기반 어플라이언스 구축

보안관제

보안관제 서비스

iSOC[2]

보안관제 포털 서비스

iAXIS[2]

보안관제 특화 공격 표면 관리 서비스

iAXIS asm[2]

운영기술(OT) 보안

spider OT

위협 인텔리전스

KLU: Threat Intelligence

홈페이지 위변조 모니터링 시스템

webmon

침해사고 분석

보안 컨설팅

사이버 역량 강화 교육

IGLOO

THANK YOU