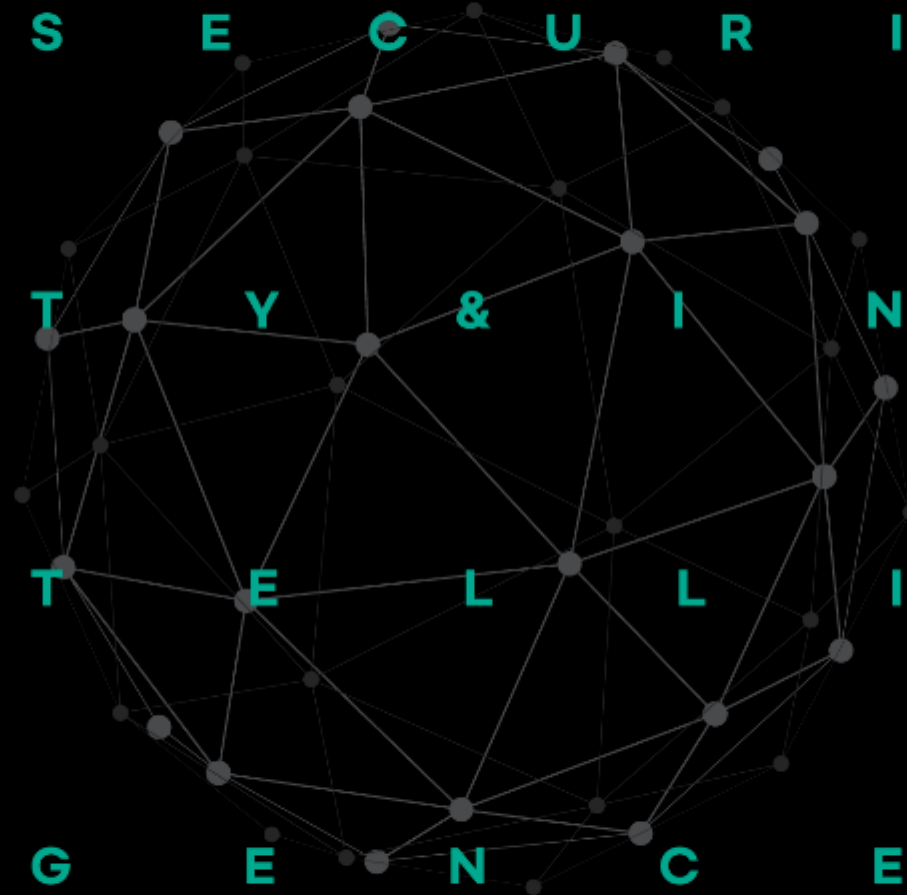


IGLOO
Corporation
Company
Brief



Stimulate innovation in your
organization and improve cyber
professionals' skills with a smarter way

About **IGLOO** Corporation

01 Overview
기업 개요

02 Vision
비전

03 History
연혁

04 Business Areas
사업 영역

4-1 솔루션
4-2 서비스

05 Core Competencies
핵심 경쟁력

06 Fact sheets
이글루 성과

07 Customers
고객사

08 Overseas Business
해외 사업

09 Contacts
문의

1999년 보안 벤처 기업으로 시작...
인공지능, 빅데이터, 클라우드 분야를 아우르는
종합 IT 기업으로 도약



이글루코퍼레이션은 1999년 창립 이래, 조직의 업무 환경, 업무 수행 방식의 혁신을 앞당기고 보안성을 강화할 수 있는 핵심 기술 구현에 집중하여 왔습니다.

이글루코퍼레이션은 지속적인 연구개발(R&D) 투자를 통해, 인공지능(AI), 보안 운영·위협 대응 자동화(SOAR), 위협 인텔리전스(CTI), 운영 기술 보안(OT), 전문 보안 서비스를 아우르는 다각화된 사업을 전개하며, 보안 시장의 성장을 이끌어왔습니다.

기업명	(주)이글루코퍼레이션	대표이사	이득춘	본사	서울특별시 송파구 정의로8길 7
설립일	1999년 11월 2일	직원수	1,037명 (2023년 사업보고서 기준)	대전지사	대전광역시 유성구 죽동로 297번길 38
상장일	2010년 8월 4일	홈페이지	www.igloo.co.kr	광주지사	광주광역시 서구 풍금로 59
				일본법인	東京都千代田区岩本町3-4-3
사업영역	<ul style="list-style-type: none">- AI (분류형·설명형·생성형)- 클라우드 보안- SIEM (보안 정보 및 이벤트 탐지 분석)- 위협 인텔리전스(CTI) 기반 전문 서비스- SOAR (보안 운영·위협 대응 자동화)- 전문 보안 서비스 (보안관제, 보안컨설팅, 침해사고 분석)- OT (운영 기술 보안)				



AI 기반 보안 운영 · 분석 플랫폼 기업

인공지능(AI)을 핵심 성장 동력으로 삼은 이글루코퍼레이션은 지속적인 연구개발 투자 확대를 통해 **고유의 분류형·설명형 AI 기술**을 확보하였습니다. 2023년에는 챗GPT를 적용한 국내 최초의 보안 서비스인 '에어(AiR)'를 출시하며, 보안에 특화된 **생성형 AI 역량 강화**에 속도를 붙였습니다.

2024년 이글루코퍼레이션은 **SIEM-SOAR-AI 등 핵심 보안 영역의 유기적인 통합**에 기반한 '확장형 탐지 조사 대응 인사이트(XDIR Insights)' 구축 지원에 힘을 실을 계획입니다. **수많은 기능 연동·추가가 용이한 플랫폼 구조**로 IT 환경의 변화 및 조직 환경에 최적화된 보안성을 확보할 수 있습니다.

더 나아가, **핵심 보안 요소에 분류형·설명형·생성형 AI 기술을 적용하며, 보안 운영 및 분석의 효율성을 극대화할 전략**입니다. 데이터 중심의 AI 역량과 보안 분석가의 눈높이에 맞춘 자연어 형태의 가이드를 토대로, 보안분석가들이 보다 정확하고 빠른 의사결정을 내릴 수 있도록 지원하겠습니다.

03 History

끊임없는 변화 속에서
새로운 기회를 찾아내는 기업,

이글루코퍼레이션

이글루코퍼레이션은 보안 벤처 기업에서
인공지능, 클라우드, 빅데이터 분야를 아우르는
종합 IT 기업으로 도약했습니다.

1999

(주)이글루코퍼레이션 설립

2000s

정보보안 시장 개척

- '00 **SIEM** 국내 최초 보안 정보 및 이벤트 관리(SIEM) 솔루션 출시
- 보안관제** 보안관제 서비스 개시
- '04 정부 통합전산센터 보안사업 참여

2010s

정보보안 시장 선도

- '10 **상장** 코스닥 시장 상장
- '11 **보안관제** 보안관제 전문업체 지정
- '14 **컨설팅** 지식정보보안컨설팅 전문업체 지정
- '17 **해외사업** 일본 법인 'CIC' 등록
- CERT** 평창동계올림픽 침해사고 대응팀(CERT) 운영사업 수주
- '18 **AI** '대구 AI 기반 지능형 보안관제 체계' 구축 프로젝트 완료
- '19 **AI** 국내 최초 AI 보안관제 솔루션 출시

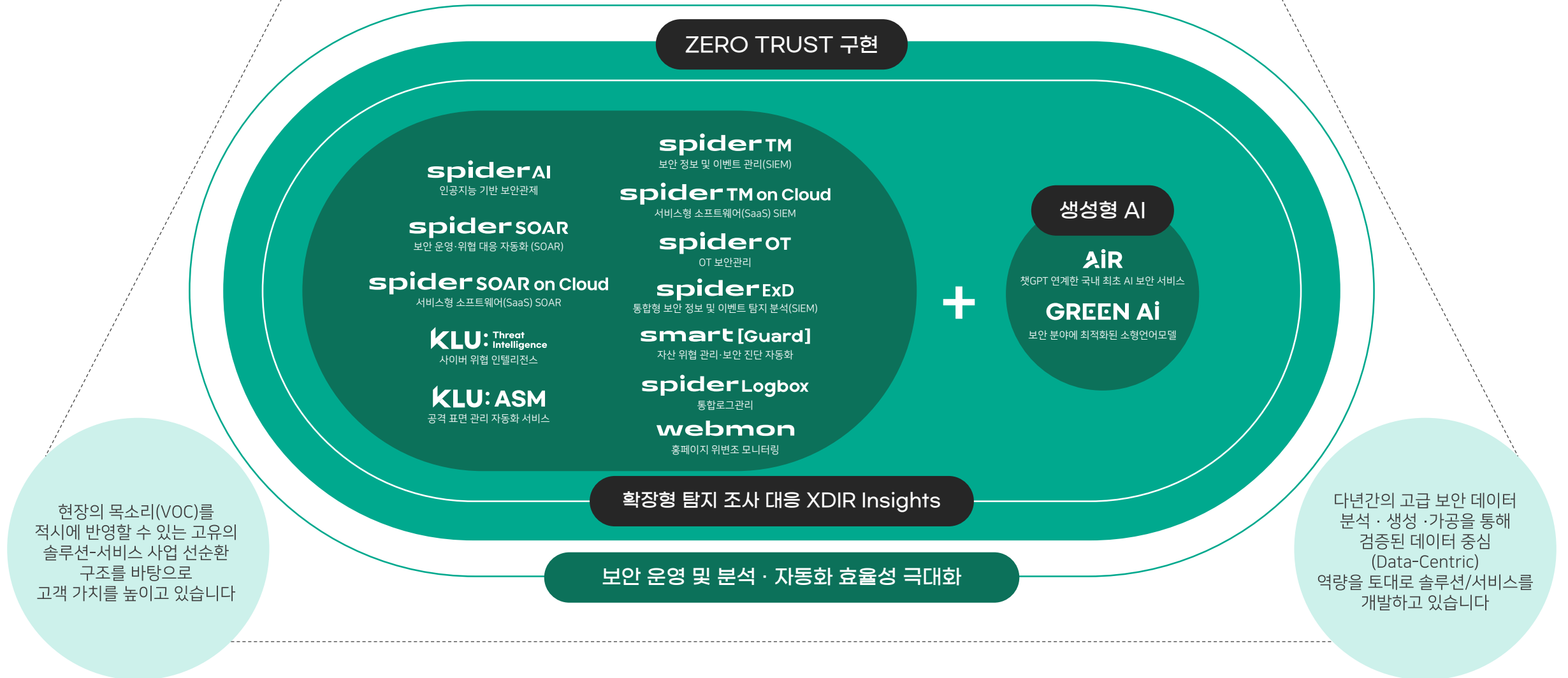
2020s

인공지능·클라우드·빅데이터 기술 기반 리더 기업 도약

- '20 **AI** '2020년 인공지능 기반 지자체 보안관제시스템 확대 구축 사업' 수주
- 해외사업** 미얀마 국립사이버보안센터(NCSC)에 SIEM 솔루션 수출
- Cloud** MS 애저(Azure) 파트너 계약 체결... 클라우드 보안 사업 경쟁력 강화
- '21 **SOAR** 보안 운영·위협 대응 자동화(SOAR) 솔루션 출시
- OT** OT 보안관리솔루션 'SPiDER OT' 출시
- CLOUD** MS 애저 마켓플레이스 통해 클라우드 기반 SIEM 제공
- 인수** 소프트웨어 테스트 전문기업 코드마인드 인수
- 인수** 클라우드 데이터센터 최적화 전문기업 파이오링크 인수
- '22 **AI** KISA '사이버보안 인공지능 데이터셋(침해사고 분야) 구축 사업' 침해사건 재현 분야 완료
- 사명변경** '(주)이글루코퍼레이션'으로 사명 변경
- AI** KISA '사이버보안 인공지능 데이터셋 (능동형 보안관제 분야) 구축 사업' 수주
- AI** 자율주행 보안 특허 취득
- '23 **OT** 포스텍과 손잡고 '선박 특화 OT 보안 사업' 확장
- 해외사업** 42억 원 규모 키르기스스탄 사이버안전센터 구축 사업 수주
- AI** 생성형 AI 포함 하이브리드 AI 탐지모델 서비스 'AiR' 출시
- 특허** SIEM·AI·SOAR·CLOUD 관련 특허 취득
- 특허** 언어 모델 활용해 AI 효율성 높이는 특허 기술 취득
- 개발역량** 개발자 컨퍼런스 'IDC 2023' 성료
- SOAR** SOAR 솔루션 최초 국가정보원 보안기능확인서 획득
- OT** 산자부 선박 사이버안전성 평가 및 통합보안관리 솔루션 개발 과제 수주
- CTI** KLU:ASM 출시, 에이아이스페라와 MOU 체결
- SOAR** 활용성 높은 플레이북 공유하는 SOAR 커뮤니티 오픈

'제로 트러스트'를 구현하는 확장형 탐지 조사 대응(XDIR) 체계 구축 지원

이글루코퍼레이션은 핵심 보안 영역이 유기적으로 통합된 XDIR 체계 도입 및 고유의 생성형 AI 기능 결합을 통해, 보안 운영·분석 업무의 효율성을 극대화하고 있습니다.



보안 운영·분석의 효율성을 높이는 다양한 정보보안 솔루션 제공

고객이 조직에 최적화된 핵심 보안 기능을 적시에 도입하고
보안 효율성을 극대화할 수 있도록 지원합니다.

인공지능(AI) 기반 보안관제	보안 운영·위협 대응 자동화(SOAR)		운영기술(OT) 보안	자산 위협 관리·보안 진단 자동화
<p>spiderAI</p> <p>보안 특화 AI 알고리즘과 데이터를 토대로 사이버 공격에 대한 대응력을 높여주는 인공지능 기반 보안관제 솔루션</p>	<p>spiderSOAR</p> <p>보안 위협 대응 프로세스를 자동화하여 보안 업무의 효율성을 높이는 보안 운영·위협 대응 자동화 솔루션</p> <p>높은 활용성과 안정성이 검증된 플레이북을 공유하는 'SOAR 커뮤니티' 지원</p>	<p>spiderSOAR on Cloud</p> <p>클라우드 환경에 최적화된 서비스형 소프트웨어(SaaS)방식의 SOAR 솔루션</p> <p>등록 마켓플레이스 KT클라우드 NHN클라우드</p>	<p>spiderOT Maritime Building Factory</p> <p>정보기술(IT)과 운영기술(OT) 영역을 포괄한 자산 식별-탐지-분석 기능을 제공하는 OT 보안 관리 솔루션</p> <p>2024년 1월부터 의무 적용된 선박 보안 규정 (IACS E26, E27)을 준수하는 해사 특화 솔루션 지원</p>	<p>smart [Guard]</p> <p>온프레미스, 하이브리드·멀티 클라우드 환경을 아우르는 자산 위협 관리·보안 진단 자동화 솔루션</p>
보안 정보 및 이벤트 탐지 분석(SIEM)			홈페이지 위변조 모니터링	
<p>spiderTM</p> <p>고유의 보안관제 수행 경험 및 빅데이터 활용 역량이 집약된 SIEM 솔루션</p>	<p>spiderTM on Cloud</p> <p>클라우드 환경에 최적화된 서비스형 소프트웨어(SaaS) 방식의 SIEM 솔루션</p> <p>등록 마켓플레이스 Microsoft Azure AWS KT클라우드 NHN클라우드</p>	<p>spiderExD</p> <p>단일 워크플로우에서 통합적인 고급 탐지-분석-대응 기능을 제공하는 차세대 SIEM 솔루션</p> <p>2024년 상반기 출시 예정</p>	<p>webmon</p> <p>종합 모니터링을 통해 웹사이트·홈페이지 위변조 발생을 탐지하는 홈페이지 위변조 모니터링 솔루션</p>	

보안 운영·분석의 효율성을 높이는 다양한 정보보안 서비스·콘텐츠 제공

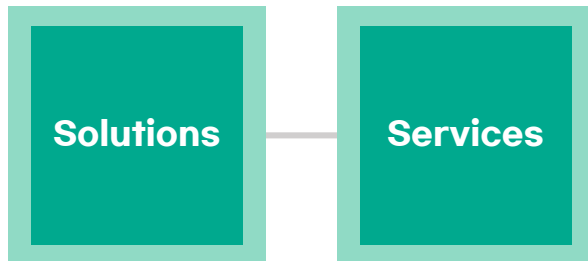
고객이 보안 위협에 대한 걱정 없이 핵심 비즈니스에 집중할 수 있도록, 조직의 정보 자산을 노리는 공격 및 잠재적인 위협 요인을 선제 탐지하고 대응합니다. 또한, 고유의 데이터 수집-가공-검증-활용 역량을 토대로 조직에 최적화된 핵심 사이버 위협 인텔리전스를 제공하고 있습니다.

분류형·설명형·생성형 AI 기술 기반 AI 탐지 모델 서비스	위협 인텔리전스(CTI) 기반 전문 서비스	클라우드 보안 서비스 (클라우드 보안 운영, SaaS)	전문 보안 서비스	보안 교육 서비스 '이글루 스쿨'
 <p>생성AI연계한 국내최초AI보안서비스</p> <p>분류형·설명형·생성형 AI 기술을 바탕으로 AI 모델의 예측 결과 및 근거를 자연어 형태로 설명해 주는 서비스</p>	 <p>KLU: Threat Intelligence 최신 보안 위협과 공격 기법에 대한 핵심 정보 제공</p> <p>KLU: ASM 외부에 노출된 IT 자산 정보를 실시간 파악·관리하는 공격 표면 관리(ASM) 서비스</p>	<p>클라우드 보안관제</p> <p>클라우드 보안 체계 구축-운영 지원</p> <p>클라우드 기반 SIEM, SOAR 공급</p>	<p>보안관제</p> <p>보안컨설팅</p> <p>침해사고 분석</p>	<p>정보보안 관리자/담당자 대상</p> <p>이글루 임직원 대상</p>
	<p style="text-align: center;">+</p> <p>(2024) Ransomware, Dark Web 등 신규 제품 출시 예정</p>	<p style="text-align: center;">+</p> <p>(2024) 클라우드 네이티브 보안 서비스 연계 및 서비스형 보안(SaaS) 확대 공급</p>		

AI 기반 보안 운영·분석 플랫폼 확장을 위한 핵심 역량 보유

업무 효율성·편의성 높이는 솔루션-서비스 선순환 구조 정립

솔루션 기능 많기만 하면 좋은 건가요?
현장의 니즈를 반영한 실질적 개선을 통해,
솔루션의 완성도, 사용자 편의성을 높입니다



솔루션 또는 서비스 사업만 별도 전개하는 다른 기업과는 달리,
이글루코퍼레이션은 자사의 보안 솔루션을 구축·운영하여
업무를 수행하는 현장 보안 요원들의 목소리(VoC)를 토대로,
솔루션의 완성도를 지속적으로 높이고 있습니다.

고유의 AI·보안 데이터 수집-가공-검증-활용 기술 확보

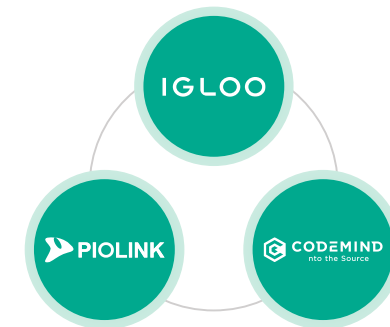
고도화된 AI 기반 보안 솔루션·서비스?
양질의 보안 데이터가 있을 때
비로소 그 가치를 발휘할 수 있습니다



이글루코퍼레이션은 정보보안 및 데이터 전문가로 구성된
별도의 조직 운영을 통해, 시그마를·플레이북·위협 모델 등을
아우르는 양질의 보안 데이터를 생성하고 있습니다.
또한, 이를 목적에 부합하는 머신러닝 모델에 적합한 형태로
변환한 AI 학습 데이터도 제공하고 있습니다.

이글루패밀리 기업과 함께 미래 성장 동력 발굴 가속

이글루패밀리의 목적에 따라,
유기적으로 결합 및 확장될 수 있는
다각화된 역량을 보유하고 있습니다



이글루코퍼레이션은 클라우드 데이터센터 최적화 전문기업
'파이올링크', 소프트웨어 테스트 전문 기업 '코드마인드'와 함께,
AI, 빅데이터, 클라우드, 소프트웨어 테스트 등의 핵심 역량을 결
집하며, 조직의 혁신을 이끄는 새로운 먹거리 발굴에 속도를 붙
이고 있습니다.

06 Fact sheets

이글루코퍼레이션은 보안 운영·분석 효율성 향상을 위한 다각화된 솔루션·서비스를 제공하며, 고객의 보안 환경을 강화하는 조력자 역할을 수행하고 있습니다. 또한, 최신 기술과 방법론을 적시에 적용할 수 있는 고유의 특허 기술과 데이터 역량 확보를 통해, 조직의 비즈니스 경쟁력을 높일 수 있도록 지원하고 있습니다.

25
years

보안 역량, 노하우

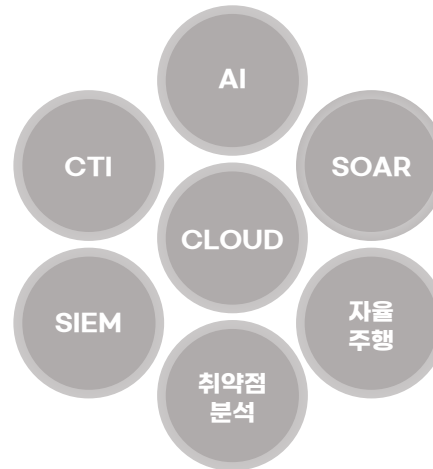
보안 운영·분석 효율성을 극대화한
국내외 핵심 사업 수행

- CERT 평창동계올림픽 침해사고 대응팀(CERT) 운영
- AI 국내 공공기관 최초의 AI 기반 사이버침해대응시스템
- AI '대구 AI 기반 지능형 보안관제 체계' 프로젝트 완료
- AI AI 기반 지자체 보안관제시스템 확대 구축 사업 진행
- CLOUD 국내 최대 규모 AWS 고객사 대상 클라우드 보안관제 수행
- 해외사업 르완다 정보보호 구축 프로젝트 진행
- 해외사업 에티오피아 국가사이버안전센터 구축
- 해외사업 42억 원 규모 키르기스스탄 사이버안전센터 구축 사업 수주
- OT 산자부 선박 사이버안전성 평가 및 통합보안관리 솔루션 개발 과제 수주
- 자율주행보안 '다부처 공동 암호화 사이버위협 대응기술 개발사업' 참여

45+

최근 3년간 취득 특허 수

미래 동력 발굴 및 우수 신기술 선점을
위한 고유의 특허 기술 확보



∞

무한한 가치를 창출하는 데이터 기반 인텔리전스

AI-SOAR-SIEM 등 핵심 영역의 가치를
높이는 검증된 데이터 역량 보유

- CTI 기반 고급 위협 콘텐츠 KLU: 서비스 제공
- 사이버보안 AI 데이터셋 구축
- KISA '사이버보안 인공지능 데이터셋 구축 사업' 수행 (침해사고, 능동형 보안관제 등)
- '데이터 바우처 지원사업' 공급기업 선정 ('22-현재)

07 Customers

이글루코퍼레이션은 국내외 수많은 조직에게 보안성 강화를 위한 솔루션·서비스를 제공하며, 고유의 AI 기반 보안 운영·분석 역량을 인정받았습니다.

	금융	공공	제조/서비스
솔루션	<p>DGB금융그룹, IBK시스템, KB국민은행, KT, LG유플러스, SK텔레콤, 광주은행, 금융감독원, 다올투자증권, 대한무역투자진흥공사 (KOTRA), 동부생명, 동양생명보험, 롯데손해보험, 수협은행, 신용회복위원회, 이베스트증권, 토스페이먼츠, 하나카드, 한화손해보험</p>	<p>강원도교육청, 건강보험심사평가원, 경기도교육청, 경상남도교육청, 경상남도청, 경상대학교, 경상북도, 경상북도교육청, 경제인문사회연구회, 경찰청, 고용노동부, 공군본부, 공군작전사령부, 공무원연금공단, 과학기술정보통신부, 관세청(인천세관), 광주광역시교육청, 광주광역시청, 국가기록원, 국가보훈처, 국가철도공단, 국군방첩사령부, 국군지휘통신사령부, 국립경찰병원, 국립생태원, 국방부, 국토안전관리원, 국토정보공사, 국회, 기상청, 대한상공회의소, 병무청, 보건복지부, 부산광역시교육청, 부평구청, 사이버작전사령부, 산림청, 상수도사업본부(인천), 서귀포시청, 서울시교육청, 서울특별시, 소방청, 소상공인시장진흥공단, 순천대학교, 식품의약품안전처, 여성가족부, 연구구청, 영남대학교, 외교부, 우정사업본부, 육군본부, 제주대학교, 제주시청, 창원시청, 한국원자력연구원, 한국폴리텍대학교, 한국해양대학교, 환경부</p>	<p>GS리테일, SK바이오사이언스, SNT중공업, STX엔진, 금호타이어, 에코프로, 오송첨단의료산업진흥재단, 유한양행, 티머니, 현대백화점, 현대오일뱅크, 현대중공업</p>
서비스	<p>KDB생명보험, NH투자증권, SC제일은행, 교보생명보험, 금융감독원, 동양생명보험, 라이나생명보험, 롯데손해보험, 메리츠화재, 미래에셋대우, 미래에셋증권, 비씨카드(운영), 수협은행, 카카오페이, 토스페이먼츠, 한국증권금융, 한국투자증권, 현대캐피탈</p>	<p>경기도교육청, 고려대학교의료원, 국토교통부, 국회도서관, 국회사무처, 기상청, 대구사이버대학, 도로교통공단, 보라매병원, 서울대학교병원, 서울도시가스, 서울도시가스, 서울시교육청, 서울신용보증재단, 성균관대학교, 성남시청, 연세대학교, 연세의료원, 외교부, 우정사업본부, 재외동포재단, 중소기업중앙회, 한국교육학술정보원, 한국국제교류재단, 한국도로공사, 한국원자력안전재단, 한국인터넷진흥원, 한국장학재단, 항공교통본부</p>	<p>LG에너지솔루션, 고진모터스, 교보문고, 금호타이어, 네오엠비즈, 다나와, 대한항공, 아우디폭스바겐코리아, 애경그룹, 여기어때컴퍼니, 이스타항공, 제주항공, 진학사, 차바이오텍, 코오롱아우토, 현대백화점, 현대오일뱅크, 현대오일뱅크, 홈앤쇼핑</p>

이글루코퍼레이션은 국내를 넘어 전 세계를 무대로 활약하고 있습니다.

대규모 공적개발원조(ODA) 사업 진행을 통해 축적한 노하우를 토대로 해외 시장에서 새로운 사업 기회를 발굴하고 있습니다.

IN Japan

2010년 일본 보안 시장에 진출한 이글루코퍼레이션은 높은 인지도, 검증된 기술력을 토대로 가시적인 성과를 기록하고 있습니다.

'10 일본 지사 설립 / '17 일본 별도 법인 CIC(Cyber Infinity Corporation) 설립

IN Central Asia

이글루코퍼레이션은 2023년 42억 원 규모의 키르기스스탄 국가 통합 사이버안전센터 구축 사업을 수주하며 글로벌 경쟁력을 입증했습니다.

ODA사업 진행을 통해 축적한 노하우를 토대로 정부 차원에서 보안운영센터(SOC)에 속도를 붙이고 있는 국가 대상의 ODA 사업 등의 신규 기회를 발굴하고 있습니다.

또한 정보보안 수요가 급증하고 있는 인도네시아, 캄보디아 등과의 현지 파트너십 체결을 통해, 해당 국가의 고객 니즈에 부합하는 XDR 라인업 및 SaaS형 AI·CTI 서비스를 제공할 방침입니다.

IGLOO IN WORLD

이글루코퍼레이션은 앞으로도 세계의 고객에게 고유의 보안과 데이터 역량에 기반한 최적의 솔루션, 서비스를 제공할 계획입니다.

- '12 르완다 정보보호 구축 프로젝트 수주
- '14 에티오피아 국가사이버안전센터 구축
- '16 인도네시아 중앙은행 통합보안관제 시범사업 수주
- '16 UAE 정보보안 기업에 보안관제 서비스 수출
- '19 두바이 엑스포 공식 파트너인 UAE 협력사와 정보보안 컨설팅 워크샵 진행
- '19 베트남 1위 ICT기업 FPT 텔레콤과 보안관제 사업 진행을 위한 MOU 체결
- '20 미얀마 국립사이버보안센터(NCSC)에 SIEM 솔루션 수출
- '23 키르기스스탄 국가 통합 사이버안전센터 구축 완료

09 Contacts

서울특별시 송파구 정의로8길 7 (문정동 640-3) 한스빌딩 6층

지하철

8호선 문정역 4번출구 도보 10분

3호선 가락시장역 8번출구 도보 15분

버스

문정로데오거리입구 하차 후 길건너 도보 7분 내외



대표전화 02)3452-8814

팩스 02)3452-8815

홈페이지 www.igloo.co.kr

문의하기 솔루션 solbizteam@igloo.co.kr

서비스 servicebiz@igloo.co.kr

 www.igloo.co.kr

 [igloocorporation](https://www.facebook.com/igloocorporation)

 [@IGLOOCorporation](https://www.youtube.com/@IGLOOCorporation)

 @이글루코퍼레이션

Thank you.

Stimulate innovation in your
organization and improve cyber
professionals' skills with a smarter way

About Solutions & Services

01 AI

SPiDER TM AI Edition
AiR

02 SIEM

SPiDER TM & SPiDER TM on Cloud
SPiDER ExD

03 SOAR

SPiDER SOAR
SOAR 커뮤니티

04 OT

SPiDER OT (Maritime/Building/Factory)
SPiDER OT for Maritime

05 위협 인텔리전스(CTI) 기반 전문 서비스

KLU: Threat Intelligence
KLU: ASM

06 전문 보안 서비스

보안관제
보안컨설팅
침해사고 분석

07 전문 보안 교육

이글루스쿨

spiderAI

'스파이더 티엠 에이아이 에디션(SPiDER TM AI Edition)'은 보안 지능화를 구현하는 AI 보안관제 솔루션입니다. 고유의 AI 및 보안 역량이 집약된 보안 특화 AI 알고리즘과 데이터를 토대로, 고도화된 사이버 공격에 대한 대응력을 한 단계 높여줍니다.

여러 사이트에 최적화된 AI 솔루션 개발 및 운영 역량

- 국내 최초 AI 보안관제 솔루션 개발
- 핵심 공공기관/기업에 AI 솔루션 공급
- 대형 사이트 AI 보안관제 담당

업계를 선도하는 AI·보안 데이터 전문가

- 보안 데이터셋, AI 알고리즘 개발 전담팀 보유
- '설명가능한 AI' 등 다수의 AI 특허 보유 (20+)

AI의 정확성과 신뢰성을 높이는 AI 학습 데이터셋 구축 역량

- 대규모 위협 대응 경험 기반 데이터셋 개발
- KISA 사이버보안 데이터셋 구축 사업 참여 ('22-)

지능형 보안
체계 수립



인공지능(AI)
정확성·신뢰성
향상

침해 분석·대응 역량 강화
보안 이벤트 분석 효율성 향상 및 고위험
이벤트 적시 대응 신·변종/잠복형 위협 탐지

데이터 중심(Data-Centric) AI 기술력 확보
기존 탐지 모델 검증 및 성능 개선
고품질의 신규 모델 구축 및 모델 개선



'에어(AiR)'는 '분류형·설명형(XAI, eXplainable AI)·생성형 AI(Generative AI)' 기술을 토대로 특정 보안 데이터에 대해 AI 모델이 판단한 근거를 자연어 형태로 알려주는 '하이브리드 탐지 모델' 서비스입니다. 사용자들은 AI 모델이 특정한 예측을 내린 기준 확인을 통해 AI 답변의 신뢰도를 평가하고, 자연어 형태의 설명을 토대로 AI 답변에 대한 이해도를 높일 수 있습니다.

IGLOO 분류형 모델 정·오탐 분류모델: IDS/IPS, WAF

- 이글루코퍼레이션에서 자사 장비 데이터를 활용해 자체 개발한 양질의 학습 데이터를 학습한 AI 모델이 스스로 판단 기준을 세워 공격 유/무를 판단

IGLOO 설명형 모델 SHAP, 시그니처 기반

- AI 탐지 분류 모델의 결과 예측 과정에 영향을 미친 공격 특징(feature)의 중요도를 보여주며, 이를 통해 AI 모델이 그러한 결과를 내놓은 이유를 확인

생성형 모델 오픈AI의 챗GPT

- 챗GPT가 자체 데이터를 토대로 판단한 자연어 형태의 설명+
- 이글루코퍼레이션의 AI 모델(분류형/설명형)이 내놓은 결과를 챗GPT와 연계한 자연어 형태의 답변을 확인

온라인
웹페이지



RESTful
API

보안 조직 전문성 강화

- 분류형·설명형·생성형의 답변을 비교 확인함으로써 지식 격차를 해소
- 3개의 AI 답변으로 언제나 최상의 조치 실행 가능

다양한 보안장비 연동을 통한 대응 효율 강화

- 자사 제품 및 타사 제품(SIEM, SOAR, 포털, 기존 정보보호 제품 등)과의 연동을 지원
- SPiDER SOAR의 플레이북 생성 효율성 및 강화 효과

spider™

'스파이더 티엠(SPiDER™)'은 이글루코퍼레이션의 보안 경험과 빅데이터 활용 역량이 집약된 보안 정보 및 이벤트 관리(SIEM) 솔루션입니다. 최초 탐지부터 로그 분석까지 일원화된 관제 환경 구성을 통해 보안 운영 업무의 기민성과 효율성을 높이고, 인프라 전반에 대한 폭넓은 가시성을 확보할 수 있도록 지원합니다.



빅데이터 기반 통합 보안 시스템 구축을 통해
고도화된 보안 환경 마련 및 효율적이고 안정적인 IT 인프라 운영관리를 위한 기반 확보

spiderExD

'스파이더 이엑스디(SPIDER ExD)'는 높은 수준의 가용성·정확성·확장성을 보장하는 보안 정보 및 이벤트 탐지 분석(SIEM) 솔루션입니다. 고급 수집-분석-대응-확장 기능을 통합적으로 제공하는 SPiDER ExD를 통해 단일 워크플로우에서 일원화된 형태의 보안 프로세스를 운영함으로써, 기업 전반을 아우르는 가시성을 확보하고, 날로 진화하는 보안 위협에 대한 대응력을 한 단계 높일 수 있게 됩니다.

종합적인 분석, 위협 탐지-조사-대응 워크플로우 자동화

수집

분산 저장·검색을 지원하는 클러스터 기반의 빅데이터 아키텍처

분석

실시간 분석, 대용량 상관분석을 지원하는 진화된 분석

대응

침해대응시스템 및 보안 운영·위협 대응 자동화(SOAR) 연계를 통한 자동 대응

확장

수집·분석·대응·공유 모듈의 응용프로그램인터페이스(API)를 통한 확장 가능한 플랫폼



포괄적 관점에서 보안 운영 효율성 극대화함으로써
더욱 강력하고 효과적인 보안체계를 구축

spiderSOAR

'스파이더 소아(SPiDER SOAR)'는 보안 위협 대응 프로세스를 자동화하여 보안 업무의 효율성을 높이는 보안 운영·위협 대응 자동화(SOAR) 솔루션입니다. 검증된 플레이북(Playbook) 제공 및 국내외 이기종 보안 솔루션 간 긴밀한 연동 지원을 통해, 활용도 높은 자동화 기능을 제공합니다.

정확도 높은 자동 위협 탐지 가능
**AI 지도학습 모듈을 활용한
 인공지능 기반 자동화 대응**

자동화된 선제적 대응 가능
위협 인텔리전스 연계를 통한 대응

경보 탐지 중심에서 침해대응/상세
 분석 중심의 체계 구현 가능
**MITRE ATT&CK 프레임워크
 연계를 통한 대응**

전반적인 보안 프로세스 자동화로 인한
 대응 속도 향상 가능
SOAR to SOAR를 통한 기관 연계 대응

활용도 높은 플레이북을 지속 배포하는 SOAR 커뮤니티 운영

- 실제 보안운영 현장에서 활용할 수 있는 전문화된 플레이북 지속 개발·배포
- 다양한 보안 위협 유형 및 조직 상황에 부합하는 플레이북 선별 및 적용 가능



보안 대응 자동화

- 보안 대응 프로세스의 자동화를 통해 대응 역량 향상
- 플레이북 기반 동일한 품질의 분석 결과 도출을 통해 대응 역량 상향 평준화

보안 운영의 성숙도 향상

- 전문가의 상세 분석으로 보안 체질 개선
- SOC 자동화 트랜스포메이션으로 차세대 보안 성숙도 향상

spiderSOAR 커뮤니티

보안 관제 요원 및 보안 분석가들이 각 조직 상황과 공격 대응에 최적화된 플레이북을 손쉽게 선별 및 적용할 수 있도록 최신 플레이북을 공유하는 SOAR 커뮤니티입니다.

각 조직에 최적화된 플레이북 적용 통해,
실질적으로 의미 있는 보안 운영 자동화(SOA) 구현

플레이북을 손쉽게 찾고 적용할 수 있는
사용자 중심의 UI/UX 적용

이글루코퍼레이션 보안 전문가들이 검증한
플레이북 제공으로 높은 안정성과 활용성 보장

최신의 플레이북을 한눈에 알아보기 쉽게 간략하게 표출



<SOAR 커뮤니티 메인 페이지>

사용자의 선별 및 적용의 편의성을 높인 그리드 형태의 카테고리



<플레이북 매트릭스 화면 >

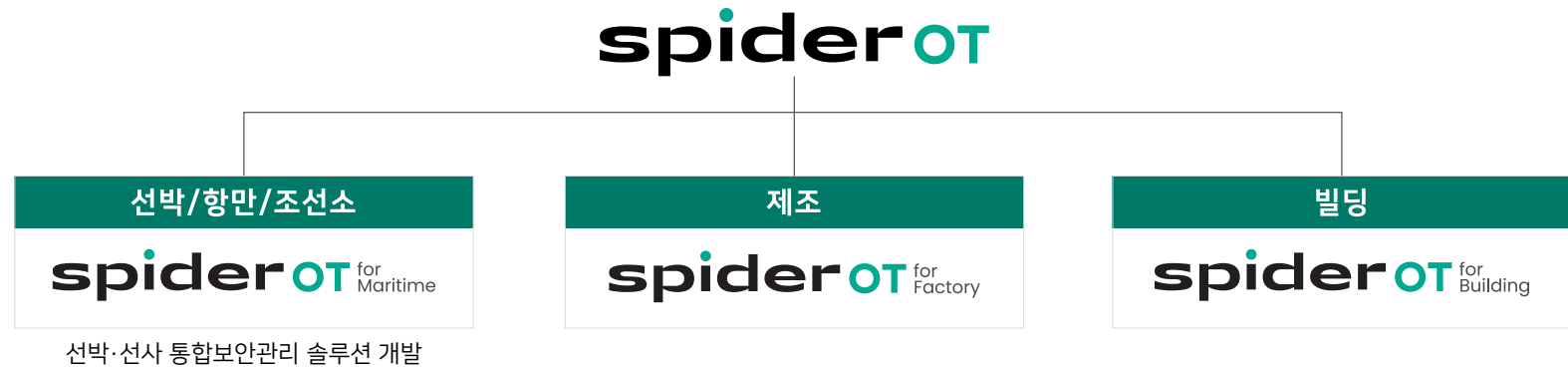


- 플레이북 생성 및 관리의 부담을 절감
- 공격 대응 프로세스의 복잡성을 해소하여 업무 효율성을 높임

spiderOT

‘스파이더 오티(SPiDER OT)’는 이글루코퍼레이션의 이기종 보안 이벤트 통합 분석 기술과 노하우를 토대로 IT와 OT 영역을 포괄하는 자산 식별-보호-탐지-대응 보안 기능을 제공하는 OT 보안 관리 솔루션입니다. IT 보안 장비와 OT 자산을 식별하고, 보안 이벤트를 통합 관리할 수 있을 뿐만 아니라, IT와 OT를 아우르는 위협 분석 및 가시성 확보로 OT 보안 위협에 대한 선제적인 대응이 가능합니다.

융합보안관리	가시성 및 효과성 관리	위협 분석 관리	실시간 이벤트 관리
<ul style="list-style-type: none"> IT 보안장비, OT 센서 및 OT 보안솔루션을 연동하여 제어시스템에서 발생하는 OT 위협 및 비정상 행위 탐지 OT 네트워크 내 통신에 대한 사업 프로토콜의 이상 정보 수집, 분석, 시각화를 통한 신속한 대응 빅데이터 기반의 IT-OT 이기종 보안이벤트를 연관 필드 검색 및 보안정책 적용으로 통합 관리 	<ul style="list-style-type: none"> 사용자 정의 OT 관제맵을 통해 통합관제, 보안 관제, OT 운영관제 등 자유롭게 시각화 설정 센서를 통한 제어시스템 내 OT 자산 식별로 자산 종류 및 통신 상황에 대한 가시성 확보 OT 자산에 대한 동작 및 통신에 대한 실시간 학습으로 이상징후 모니터링 및 위협경보 제공 	<ul style="list-style-type: none"> 위협정보시스템(Cyber Threat Intelligence) 연동을 통한 국내외 위협정보에 대한 선제적인 대응체계 구축 시그니처 기반 위협 탐지 및 경보 상관관계 분석으로 보안 위협 대응 강화 YARA 및 Snort Rule 기반 보안정책 적용으로 신규 위협에 대한 대응 강화 (OT 센서) 	<ul style="list-style-type: none"> 실시간 처리 기술을 통한 Real-Time 보안관제 (In-Memory 방식의 실시간 스트림 처리 기술 (CEP) 적용) 빅데이터 기반 기술 적용을 통해 대규모 이벤트의 실시간 상시 모니터링 및 분석 관제에 최적화된 대시보드 시각화를 통한 신속한 침해사고 대응 강화



선박·선사 통합보안관리 솔루션 개발

IT와 OT 영역을 중앙에서 통합적으로 아우를 수 있는 융합보안관제 체계 구현

spider OT for Maritime

'스파이더 오티 포 마리타임(SPiDER OT for Maritime)'은 선내 능동 보안 환경 구현을 지원하는 SIEM 솔루션입니다. 선박 네트워크 중 비정상 행위에 대한 지표를 수립하고, 이를 토대로 판단한 사이버 위협 정보와 대응 가이드를 제공합니다.

NEW

[UR E26/UR E27 2024년 의무 적용]

국제선급협회(IACS)가 선박의 사이버 복원력 향상을 위해 마련한 공통규칙

해사 운영기술(OT) 환경에 최적화된 보안 솔루션 필요

해상에서 검증된 가용성, 정확성, 확장성으로 선박 보안 운영 효율성 극대화



사이버 위협 분석 관리	IT & OT 자산 관리	이벤트 및 로그 모니터링
<ul style="list-style-type: none"> 사이버 보안 탐지 정책 업데이트 지원 빅데이터 기반 로그 이벤트의 실시간 모니터링 정보 분석 	<ul style="list-style-type: none"> IT 및 OT 자산 정보 통합관리 자산 상태 및 네트워크 모니터링 다양한 자산의 이벤트 관리 	<ul style="list-style-type: none"> 수집된 로그/이벤트 기반의 비정상 행위 탐지, 정책 기반 사이버 보안 위협 알람 생성

이글루코퍼레이션은 조선·해양 노하우를 보유한 포스텍, KR(한국선급) 등 전문 기업과의 협력을 통해, 다양한 OT 프로토콜과 운영체제, 시스템에 대한 폭넓은 가시성을 확보하고 최적화된 보안 체계를 구축하는 보안 컨설팅-진단-서비스를 제공하고 있습니다.

CTI를 토대로 적과 나에 대한 핵심 단서를 제공하는 위협 전문 브랜드 '클루(KLU:)'

KLU:는 이글루코퍼레이션의 위협 정보 수집·선별·가공 역량이 집약된 위협 인텔리전스 전문 브랜드입니다. 이글루코퍼레이션은 위협 헌팅, 다크웹, 랜섬웨어 등 조직이 필요로 하는 핵심 영역을 추가하며, 다각화된 CTI 서비스를 지속 제공할 계획입니다.



‘클루 쓰렛 인텔리전스(KLU: Threat Intelligence)’는 사이버 상에서 발생하는 다양한 위협 정보에 대한 분석을 통해, 고객사와 연관이 있는 상세 정보를 선별·제공하는 서비스입니다.

국내 환경에 최적화된 사이버 위협 인텔리전스

- 20여 년 이상 수백 개 고객사들의 정보보호시스템을 운영한 경험과 노하우를 토대로 탐지에 실질적으로 활용할 수 있는 고품질의 위협 정보를 수집, 분석, 배포

고객의 요구와 환경에 따른 맞춤형 사이버 위협 인텔리전스

- 웹 서비스 (CTI 웹 서비스를 통한 정보공유)
- 연계 서버 구축 (고객사 CTI 연계 시스템 구축)
- 플랫폼 구축 (고객사 CTI 시스템 구축)

다양한 제품과 연동 가능한 사이버 위협 인텔리전스

- 이글루코퍼레이션 보안 정보 및 이벤트 관리 (SIEM) 솔루션의 위협 데이터베이스(DB)에 연동하여, 탐지 정책에 활용
- 이글루코퍼레이션 AI 보안관제 솔루션의 인텔리전스 DB에 데이터 연동하여, 종합위험도 분석에 활용
- 타사 제품과 데이터 연동 후 탐지 및 차단 정책에 활용

머신러닝 기반 위협 정보 스코어링 고도화

- 위협 정보의 생명 주기를 고려한 고품질의 정보 전달을 위해, 머신러닝 기술을 적용한 위협 정보 스코어링 기법을 KLU:에 적용

이글루코퍼레이션 제품
(SIEM, AI)



타사
제품

국내외 위협 정보와 자체 보안관제센터에서 수집된 각종 위협 정보를 데이터베이스(DB)화하고, 보안관제시스템과 연계함으로써 최신 보안 위협 예방 체계를 구축하고 관제 프로세스를 개선합니다

KLU:ASM

'클루 에이에스엠(KLU: ASM)'은 전 세계 네트워크에 흩어져 있는 조직의 수많은 IT 자산을 실시간으로 확인 및 조치할 수 있게 지원하는 위협 인텔리전스 기반 공격 표면 관리 자동화 서비스입니다.

고객 자산 자동 탐지

- 고객이 알고 있는 자산과 알지 못하는 자산까지 전체 인터넷 대상으로 스캔
- 사용중인 IP 주소와 열려 있는 모든 Port에서 운용 중인 네트워크 자산 전체를 탐지

자산 및 취약점 위험도 스코어링

- AI 머신러닝을 통한 자체 알고리즘을 통해 실시간 탐지된 모든 자산을 5단계의 위험 스코어링으로 시각화
- 보안 담당자는 시각화된 스코어링을 통해 사이버 위협 우선순위를 지정하여 빠르고 정확하게 보안 위협에 대응

위협 인텔리전스 검색엔진 및 AI 탐지 모델 서비스 연동

- 사이버 위협 인텔리전스 (KLU: Threat Intelligence) 검색엔진과 연동
- 분류형·설명형·생성형 AI 탐지 모델 서비스 'AiR'와 연동

클라우드 기반 웹 인터페이스

- SaaS 형태의 ASM 제품으로 도입 시 고객사 서버 내에 하드웨어 또는 소프트웨어를 설치하거나 구축할 필요가 없음
- 고객사의 PC, 태블릿, 모바일 기기의 브라우저를 통해 웹 인터페이스로 빠르고 쉽게 공격표면관리 솔루션 사용

단 한 개의 도메인 제공으로,
연결된 모든 IT 자산을 둘러싼 잠재 위협 가시성을 확보할 수 있습니다.

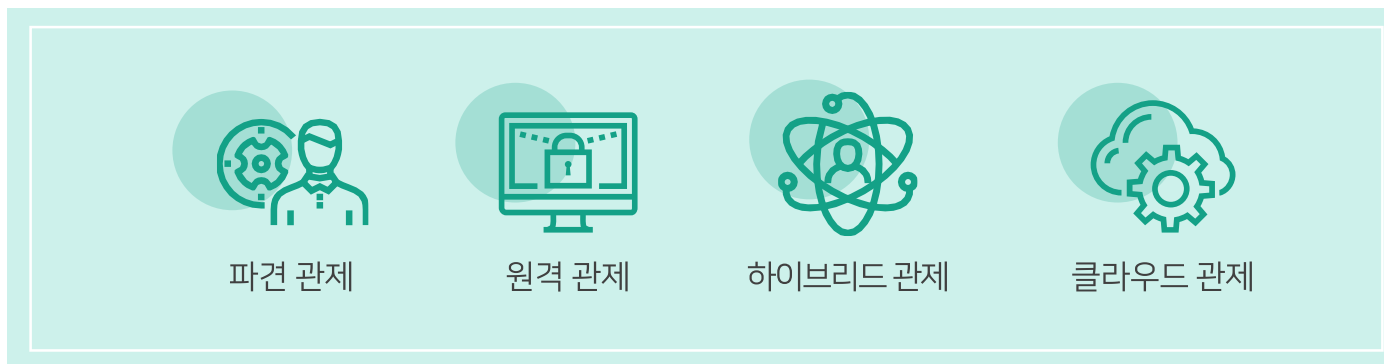


KLU: ASM 도입으로 '적이 노릴 만한 내 정보'를 간편하고 정확하게 파악하세요

전 세계 네트워크에 흩어져 있는 조직의 IT 자산을 실시간으로 확인하고 문제점을 신속히 조치함으로써, 고도화된 공격에 대한 방어력을 한 단계 높일 수 있습니다.

보안관제서비스

위협요소에 대한 실시간 분석 및 대응을 통해, 고객의 정보 자산을 24시간 365일 안전하게 보호합니다.



01

24시간 365일 보안관제

- 보안 이벤트 모니터링
- 사이버 침해 대응/분석
- 홈페이지 위·변조 탐지 및 서비스 장애 관제
- 보안장비 운영/관리
- 보안정책 적용/관리
- 시스템 헬스 체크

02

사전 침해 예방

- 인프라 취약점 진단
- 모의해킹
- 최신 보안 동향 제공
- 소스코드 진단
- 보안실태 점검
- 보안 수준 진단
- 모의훈련 (악성메일 모의훈련)

03

기타 정보보안 업무 지원

- 각종 인증 사전 준비 지원
- 지침/매뉴얼 개정 지원
- 정보보안 법적 대응 지원
- 보안 교육 수행

정보보안컨설팅서비스

정보보호에 대한 관리/물리/기술적 보안 위협 요소를 종합 진단하고, 고객 환경에 최적화된 대책 수립과 실질적인 개선안을 제공합니다.

					
정보보호 컨설팅	개인정보보호 컨설팅	정보보호 인증지원 컨설팅	개인정보 영향평가	주요정보통신 기반시설 컨설팅	기술적 취약점 진단 컨설팅

01

체계적 방법론 보유

- 정보보호관리 체계수립 컨설팅 방법론
- 주요정보통신기반시설 취약점 분석 평가 컨설팅 방법론
- 개인정보관리 체계수립 컨설팅 방법론
- 개인정보 영향평가 수행 방법론
- ISMS-P/ISO27001 인증 컨설팅 방법론
- 취약점 점검 컨설팅 방법론

02

사전 침해 예방

- 정보보호 전문서비스 기업 지정
- 개인정보 영향평가 수행기관 지정
- 보안관제 전문업체 지정
- ISMS 및 ISO27001 인증 보유

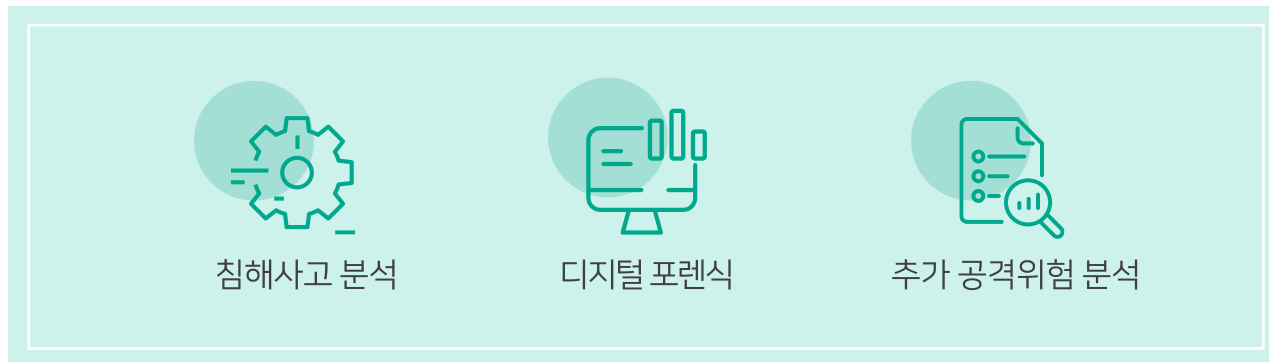
03

보안 서비스/솔루션 시너지 보유

- 솔루션/서비스 개발·구축·보안 운영을 통해 축적한 노하우 연계

침해사고 분석

침해사고 원인 분석부터 보안 강화 로드맵까지 국내외 침해사고 역량 기반의 사고 분석 서비스를 제공합니다.



01

침해사고 전문인력 보유

- 악성코드, 침해사고 분석, 클라우드, 디지털 포렌식 역량을 보유한 전문가 풀 확보

02

25년간의 침해사고 분석 역량 및 노하우 보유

- '2018년 평창동계올림픽 침해사고 대응팀(CERT) 등 주요 침해사고 분석 업무 수행

03

철저한 침해사고 원인 분석을 통한 사후 대응 방안 제시

- 조직 보안 환경 및 비즈니스 모델을 토대로, 침해사고 피해 최소화 및 보안 강화를 위한 로드맵 제시

핵심 보안 전문가 양성을 위한 '이글루스쿨' 운영

이글루코퍼레이션은 우리나라의 보안을 책임지는 핵심 보안 전문가 육성을 위해, 임직원과 고객 담당자를 대상으로 보안 교육 프로그램을 제공하는 '이글루스쿨'을 운영하고 있습니다. 숙련된 보안 전문가는 물론 초급 보안 인력까지 아우를 수 있는 세분화된 커리큘럼을 개발하고, 다년간의 실무 경험과 노하우를 보유한 강사를 초빙하여 수업을 진행하고 있습니다.

