최신 보안 위협과 공격 기법에 대한 핵심 정보를 제공하는
이글루 사이버 위협 인텔리전스(Cyber Threat Intelligence)

KLU: Threat Intelligence

IGLOO

Background

고도화되는 보안 위협, 위협 정보의 공유와 공동 대응의 필요성 대두

디지털 트랜스포메이션이 가속화됨에 따라, 보안 관리자들의 고민은 더욱 깊어지고 있습니다.
지금까지 경험하지 못했던 정교하고 전략적인 기법을 동원해 조직의 약점을 파고드는 공격자들이 늘어나고 있기 때문입니다.

날로 고도화되는 보안 위협에 위협 정보의 공유와 공동 대응의 필요성은 높아졌고,
사이버 위협 인텔리전스(Cyber Threat Intelligence)가 차세대 보안 대책으로 주목받게 되었습니다.

About CTI

CTI(Cyber Threat Intelligence)란,
전 세계에서 일어나는 모든 위협 정보를 수집하고 분석한 다음 여기서 얻은 지식을 활용해 사이버 위협에 대응하는 것을 말합니다.

고도화되는 사이버 위협에 대응하기 위해 위협 정보의 공유와 공동 대응의 필요성이 대두된 이후,
해외 CTA(Cyber Threat Alliance)나 국내 한국인터넷진흥원의 C-TAS(Cyber Threats Analysis System)는
보다 효율적인 분석을 위한 움직임들의 결과라고 볼 수 있습니다.

이제 CTI는 보안에서 가장 중요한 대응책 중에 하나이며,
보안운영센터(SOC)를 운영하는 기관과 기업에게 국내 환경에 맞는 CTI 선택은 '필수'입니다.

이글루코퍼레이션은 2016년 'K-Center'에 이어 2018년 'KLU: Threat Intelligence'까지,
누구보다 발 빠르게 위협 인텔리전스를 제공하고 있습니다.

2013

Gartner,
Threat Intelligence 정의

"현재 존재하거나 발생이 임박한 위협에 대한 증거 기반의 지식이며, 위협 대응에 관한 결정사항을 알려줄 수 있어야 한다."

2014

정부, C-TAS 가동

과기정통부와 KISA는 각종 사이버 위협 정보의 수집·분석·공유체계를 고도화한 사이버 위협정보 분석·공유시스템 'C-TAS' 가동

2016

K-Center 서비스

이글루코퍼레이션 SIEM에 신속한 사이버 위협 대응을 위한 Knowledge Center 서비스

2017

CTA 출범

글로벌 보안기업들의 사이버위협연합(CTA)의 공식 출범

2018

KLU: Threat Intelligence

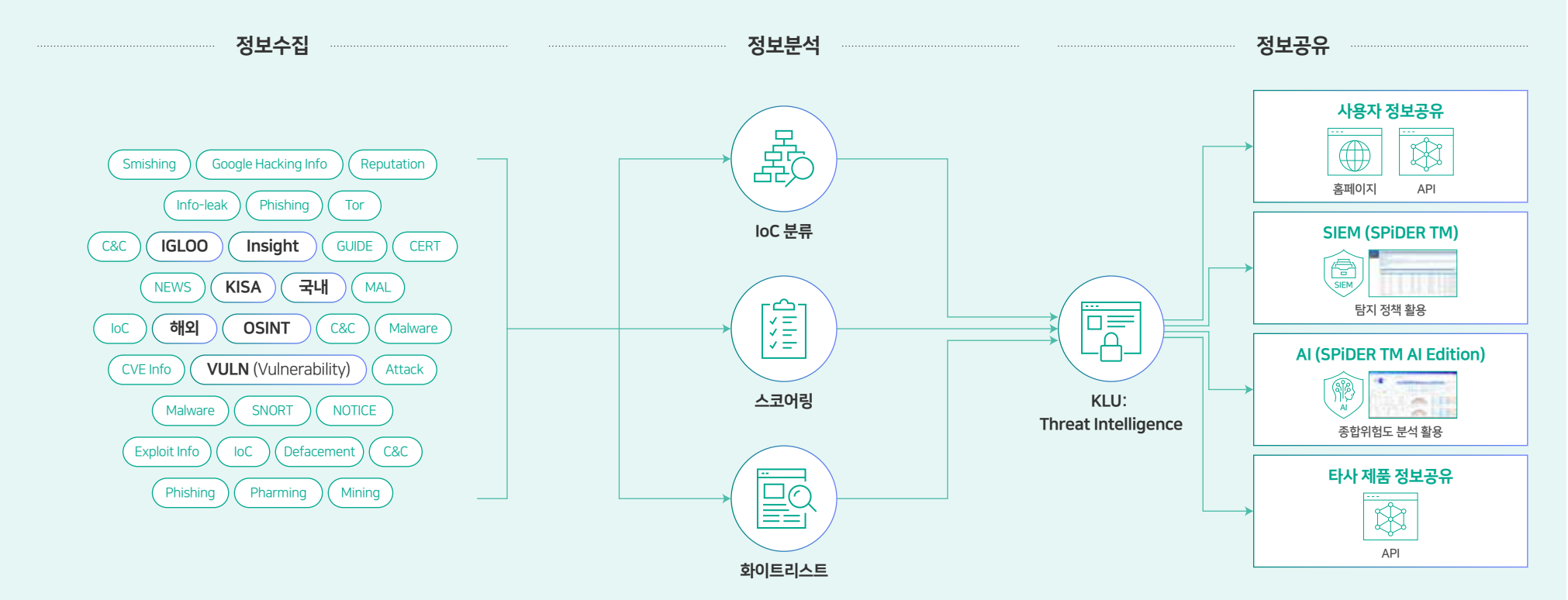
KLU: Threat Intelligence 정식 서비스 출시

Overview

KLU: Threat Intelligence는
글로벌 최신 위협 정보를 실시간으로 수집하고 공유하는 사이버 위협 정보 공유 시스템입니다.

이글루코퍼레이션은 사이버 공격을 사전에 예방하고, 공격을 탐지하며 공격자를 신속하게 식별하는 데 도움을 주기 위해 국내외 기업·기관에서 수집한 보안 위협 정보를 지속적으로 공유하고 있습니다.

기업 및 기관을 노리는 보안 위협에 맞서 공격의 맥락과 목적 등을 간파해 선제적인 대응이 가능하도록 수집한 위협 정보 중 고객사와 연관이 있는 상세 정보를 선별하여 제공합니다.



Why IGLOO CTI

01

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, 배포합니다.

02

고객의 요구와 환경에 따른 맞춤형 사이버 위협 인텔리전스

3가지 유형으로 나누어 서비스 정책을 운영합니다.

· 웹 서비스
CTI 웹 서비스를 통한 정보공유

· 연계 서버 구축
고객사 CTI 연계 시스템 구축

· 플랫폼 구축
고객사 CTI 시스템 구축

03

다양한 제품과 연동 가능한 사이버 위협 인텔리전스

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

04

머신러닝 기반 위협 정보 스코어링 고도화

· 위협 정보의 생명 주기를 고려한 고품질의 정보 전달을 위해, 머신러닝 기술을 적용한 위협 정보 스코어링 기법을 KLU: Threat Intelligence에 적용하고 있습니다.

Features

KLU: Threat Intelligence — 이글루 코퍼레이션 제품

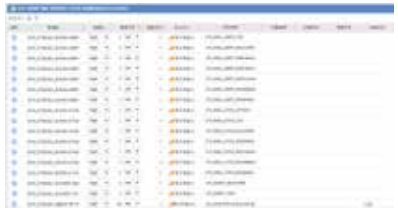
KLU: Threat Intelligence

API 통신

SIEM(빅데이터 기반 보안관제 체계)

SPiDER TM(SIEM) 위협 DB에 데이터 연동 후 탐지 정책 활용

01 예방활동 데이터 수집



02 탐지 정책 적용

03 보안관제 실시간 관제 탐지 내역 확인

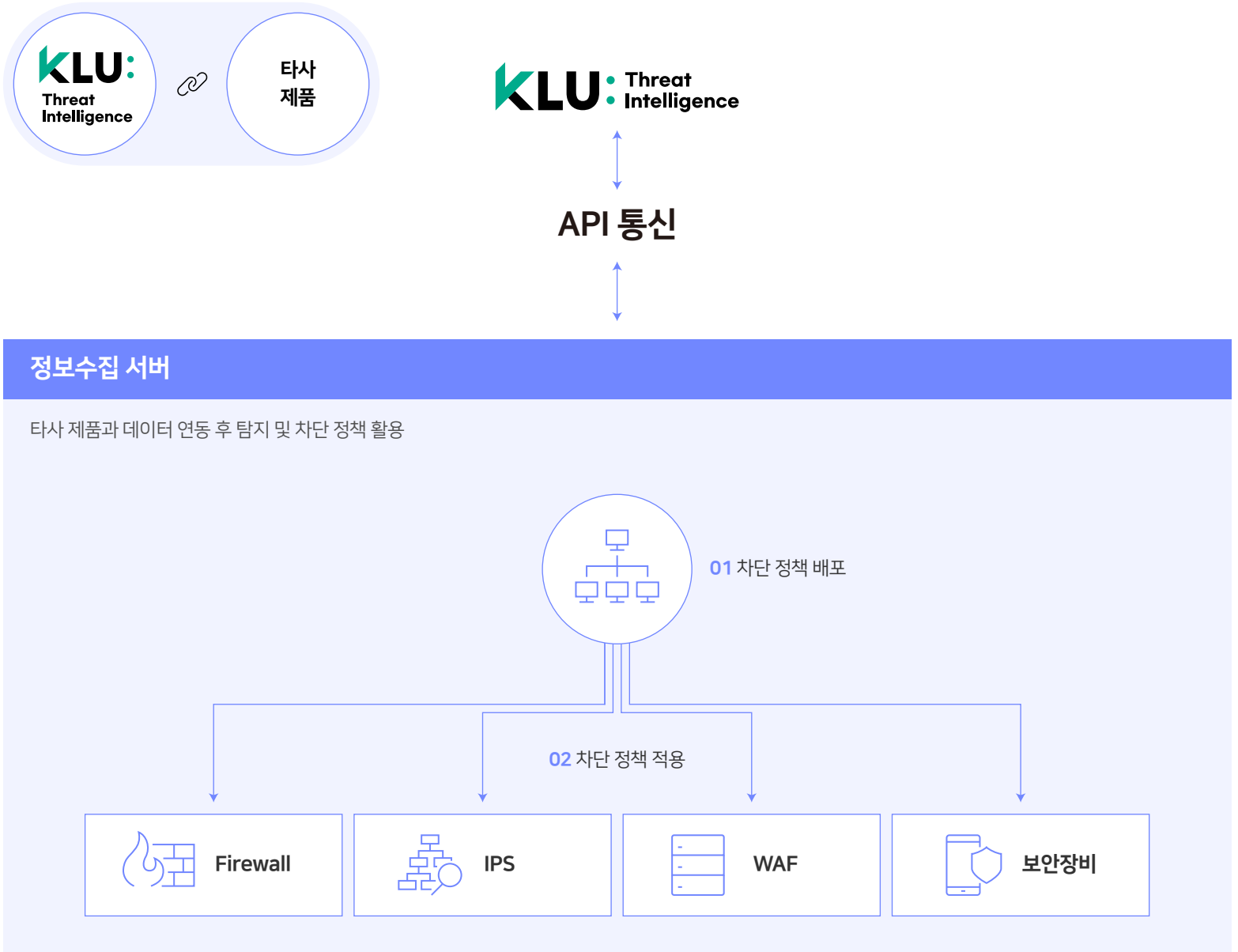
AI(인공지능 기반 보안관제 체계)

SPiDER TM AI Edition(AI SIEM) 인텔리전스 DB에 데이터 연동 후 종합위험도 분석 활용

01 위협 인사이트 이벤트 탐지

02 위협 인사이트 상세내용 확인

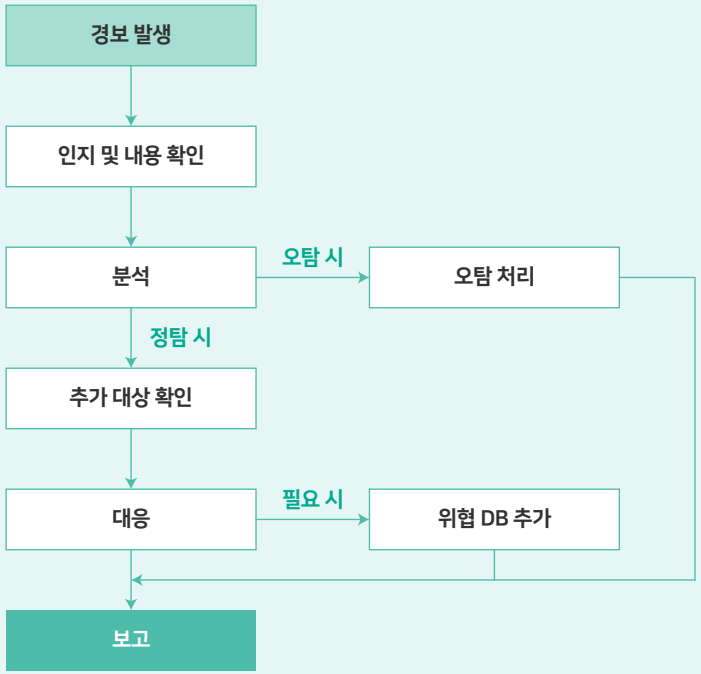
Features


KLU: Threat Intelligence
타사 제품
KLU: Threat Intelligence
API 통신
정보수집 서버
타사 제품과 데이터 연동 후 탐지 및 차단 정책 활용
01 차단 정책 배포
02 차단 정책 적용
Firewall
IPS
WAF
보안장비

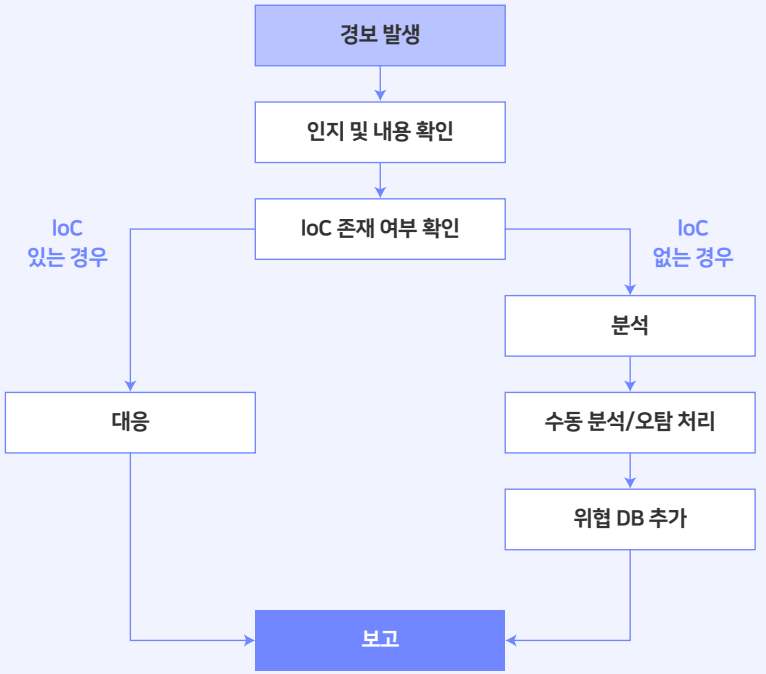
Benefits

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

AS-IS (수동분석) | 보안 경보 당 분석 시간 평균 30분~1시간



TO-BE (자동분석) | 분석 시간 평균 5분~10분



1999년 보안 벤처 기업으로 시작한 이글루코퍼레이션은 국내 최초 보안 정보 및 이벤트 관리(SIEM) 솔루션을 시작으로 수많은 정보보호 핵심 중추 기관과 기업에 보안 솔루션 및 서비스를 제공하며 정보보안 시장의 성장을 이끌어왔습니다. 또한, 디지털 전환 시대 흐름에 맞는 꾸준한 기술 고도화 및 미래 기술 준비를 통해 사업 영역을 확장해 나가며 보안을 넘어 인공지능, 클라우드, 빅데이터 분야를 아우르는 종합 IT 기업으로 성장했습니다. 이글루코퍼레이션은 세계의 고객에게 고유의 보안과 데이터 역량에 기반한 최적의 솔루션, 서비스를 제공하며 급변하는 비즈니스 환경에 최적화된 혁신적인 디지털 경험을 선사하는 기업으로 나아가고자 합니다.

서울특별시 송파구 정의로8길 7 한스빌딩 6층 | TEL 02-3452-8814 | FAX 02-3452-8815 | www.igloo.co.kr

IGLOO