AI 기반 오픈 XDR 구현의 시작
포괄적 관점에서 보안 운영 효율성 높이는
XDR 기반 차세대 보안관제 플랫폼(SIEM)

IGLOO

spider ExD

Background

디지털 대전환(DX) 시대의 도래, '통합'과 '효율'로 맞선다.

디지털 전환과 함께 사이버 공격자가 노릴 만한 공격 표면이 넓어지면서
신·변종 위협에 대응해야 하는 기업의 어려움은 점점 더 커지고 있습니다.

오늘날의 보안 조직은 기하급수적으로 생성되는 다양한 보안 데이터에 대한 가시성 확보를 통해,
고도화된 위협에 대한 탐지 정확성과 대응 속도를 높일 수 있어야 합니다.
그렇지만 이를 위한 보안 인력과 자원은 한정되어 있습니다.

복잡해지는 보안 환경에 발맞춰 솔루션도 변화해야 합니다.
포괄적인 관점에서 보안 운영의 효율성을 높여주는 차세대 SIEM 솔루션이 필요합니다.

가용성

보안과 관련된 모든 데이터를
안정적으로 수집/적재할 수 있는지

정확성

수집된 수많은 데이터의
신속하고 정확한 탐지/조사가 가능한지

확장성

필요한 여러 보안 기능을 쉽게 연계하며
일원화된 보안 프로세스 구현이 가능한지

높은 가용성·정확성·확장성을 토대로,
변화하는 IT 환경에 능동적으로 대응할 수 있는
차세대 보안 정보 및 이벤트 관리(SIEM) 솔루션이 필요한 시점입니다.

Overview

스파이더 이엑스디(SPiDER ExD)는 높은 수준의 가용성·정확성·확장성을 보장하는 XDR 기반 차세대 보안관제 플랫폼(SIEM)입니다.

보안 조직은 고급 수집-분석-대응-확장 기능을 통합적으로 제공하는 SPiDER ExD 도입을 통해
단일 워크플로우에서 일원화된 형태의 보안 프로세스를 구현함으로써,
기업 전반을 아우르는 가시성을 확보하고 날로 진화하는 보안 위협에 대한 대응력을 한 단계 높일 수 있게 됩니다.

SPiDER ExD와 함께 포괄적인 관점에서 보안 운영의 효율성을 극대화하고,
확장형 탐지 조사 대응(XDIR, eXtended Detection, Investigation, and Response) 체계 구현을 위한 여정을 시작해 보세요.

spider ExD

수집
분산 저장·검색을 지원하는
클러스터 기반의 빅데이터 아키텍처

분석
실시간 분석, 대용량 상관분석을
지원하는 진화된 분석

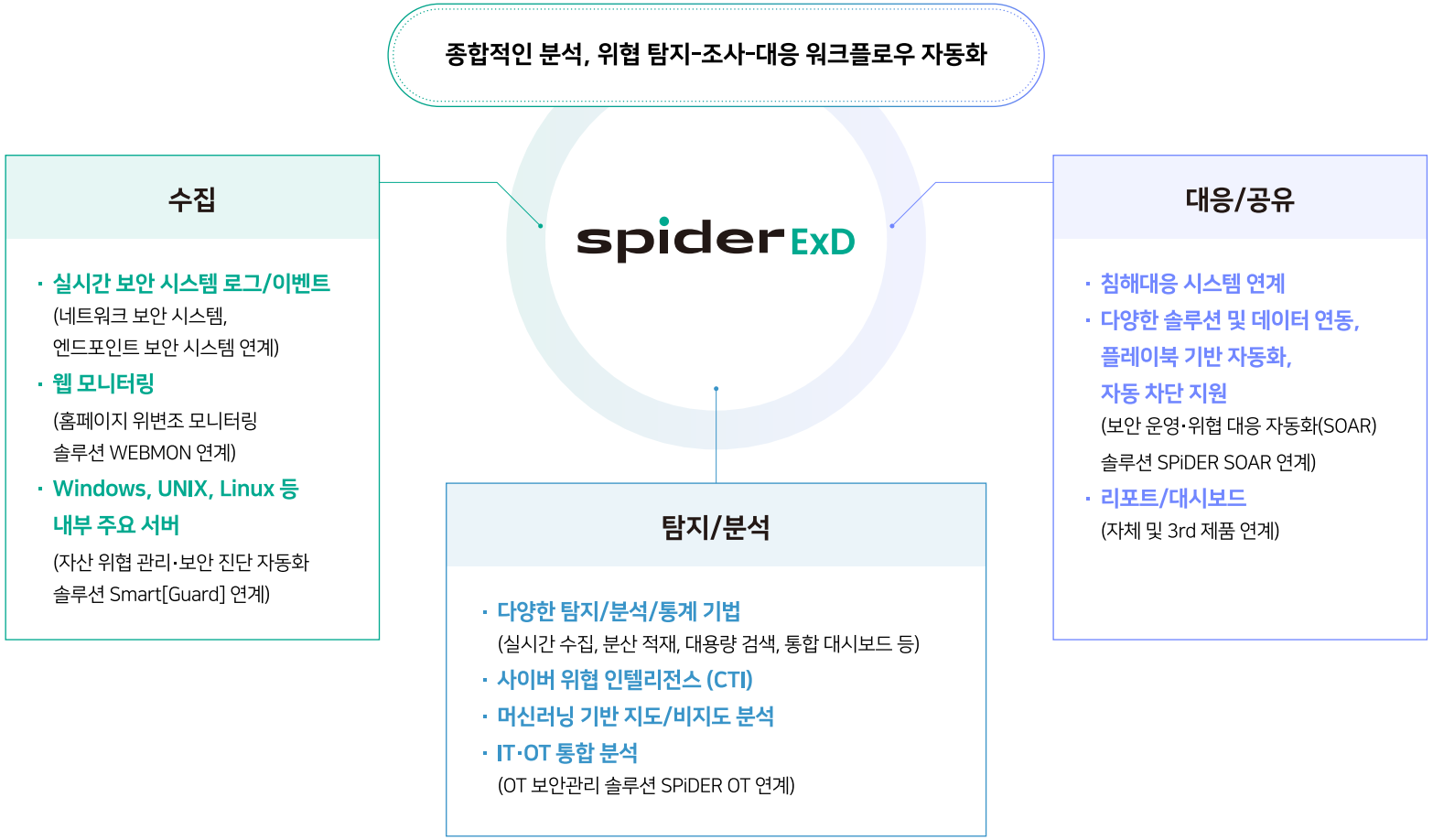
대응
침해대응시스템 및
보안 운영·위협 대응 자동화(SOAR)
연계를 통한 자동 대응

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

Why SPiDER ExD

SPiDER ExD는 보안 기능의 자유로운 확장 및 통합을 지원하는 가장 포괄적인 SIEM 솔루션입니다.
컨테이너 서비스를 중심으로 한 플랫폼 및 UI 통합을 통해, 확장형 탐지 조사 대응(XDIR) 아키텍처를 구축할 수 있습니다.

- **보안 위협 데이터 수집 범위 확장**, **다양한 탐지·조사 기법 적용**, **보안 운영 및 대응과 관련된 업무 자동화** 등 보안 조직의 요구사항에 맞춰 지속 확장 가능
- 포괄적 관점에서 방대한 보안 데이터 및 내외부 위협 인텔리전스를 유기적으로 연계하여 탐지·조사 및 대응함으로써, 보안 운영 및 위협 대응의 효율성 극대화

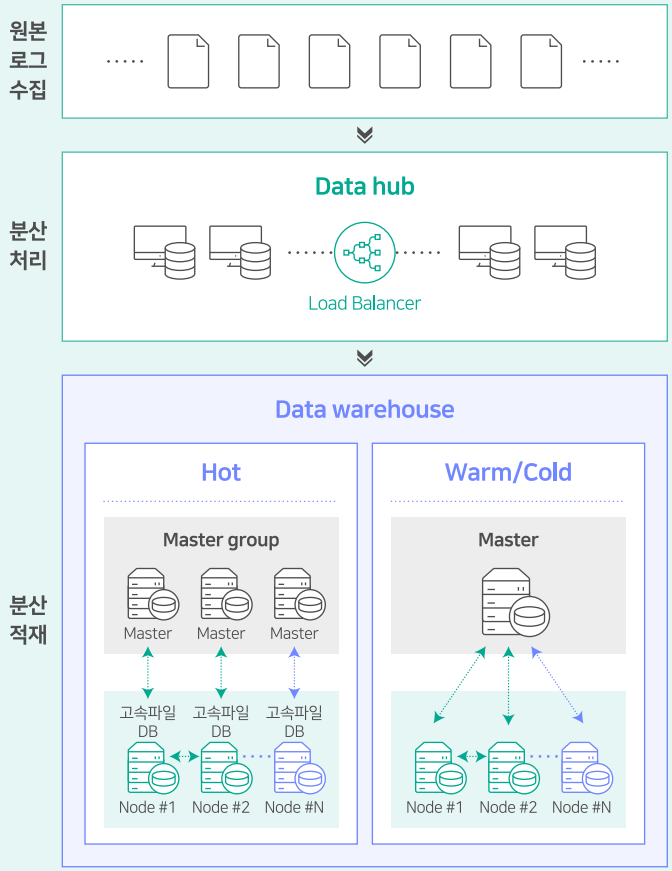


Features

A. 고가용성 보장

클러스터(Cluster) 기반의 빅데이터 아키텍처 및 레플리카(Replica) 기능을 토대로, 서비스 안정성 확보

- 클러스터 기반 병렬적 노드(Node) 확장 및 분산 저장·검색 기능을 통한 수평적 대용량 확장 지원
- 데이터 복제 저장 및 압축·암호화·백업 기능을 통한 데이터 보호 및 장애 대응 지원



클러스터 기반 병렬적 노드 확장

- 관제 대상, 로그 증가에 따른 확장성 보장(Scale-Out)
- 신규 노드가 추가되는 경우 기존 데이터 노드와 저장 용량을 균일하게 분산할 수 있는 기능
- 서비스 중단 없이 확장에 소요되는 시간을 최소화하고, 중앙 관리 기능을 통해 관리의 편의성 보장

분산 저장/검색

- 정제된 이벤트 로그를 각 데이터 노드에 조건(Default: Day) 단위별로 분산 적재(저장)

복제 저장

- 데이터 전처리 후 이벤트 로그를 2개 이상 분산 저장하여, 저장 장치 장애 시에도 중단 없이 운영
- 저장 데이터와는 별개로 복제본을 생성 및 저장하게 되며, 다른 데이터 노드에 분산 적재(저장)
- 데이터 노드(서버) 장애 발생 시, 복제 데이터를 이용한 자동 복구

압축/암호화/백업

- 저장된 로그 데이터는 디스크 저장 공간을 효율적으로 사용하기 위해 압축 저장
- 콜드(Cold) 데이터의 경우 파일 단위로 암호화하여 저장
- 백업 설정 정책에 따른 데이터 백업 및 삭제 관리

Features

B. 데이터 검색 편의성 및 분석 정확성 강화

한 단계 강화된 적재 및 검색 기능을 토대로, 높은 수준의 데이터 분석 정확성 확보

- 정규 표현식 및 실시간 파싱을 통한 수집·적재로 검색 편의성 및 분석 정확성 향상
- 복합적으로 설정한 기준 및 원본 정보를 포함한 고급 로그 검색 기능 지원
- 실시간 및 검색 기반 분석 기능 제공

사용자 정의 파서를 통한 원본로그의 정규화 적용

파서 정보

인덱스로 저장되어
검색 및 분석 용도로 활용

데이터 검색
편의성 향상

※ 로그 정규화 방식:

- 원본로그의 가공 없이 정규 표현식, 구분자 등 원하는 방식으로 로그 포맷을 정의하여 검색 및 분석에 활용
- 수집된 로그는 검색 및 분석을 위해 실시간 파싱 기능을 제공
- 원본 형태의 로우 데이터(Raw data)와 파싱된 데이터를 함께 저장
- 수집된 로그의 분석 효율성을 위해 부가적인 정보를 추가하거나 변환할 수 있는 기능 제공

실시간 분석 및 탐지

실시간
데이터

인메모리 기반 분석 엔진

- 임계치 초과 여부
- 제외 조건
- 대응 조건
- 필드 별 조건 비교
- 평판 DB 비교
- 동일 조건(분포)

분석 정확성 향상

경보 이벤트

- 근거 데이터#1
- 근거 데이터#2
- 근거 데이터#3
- 근거 데이터#4

정규화를 통한 수집·적재

- 사용자 정의 파서 기능을 통해 원본로그를 별도의 개발 없이 정규 표현식으로 필드 별 설정 지원
- 이를 통해 생성된 인덱싱 필드들은 검색 및 분석 용도로 활용되어 데이터 검색 편의성 및 분석 효율성 향상

강화된 로그 검색

- 복합적으로 설정한 기준으로 로그 검색 가능 (AND, OR, NOT 등)
- 원본 로그, 인덱싱된 모든 필드에 대한 표출 및 국가 정보, 유해 IP 정보 등 해당되는 부가 정보를 함께 제공
- 사용자 정의 검색, 대화형 검색 등 다양한 검색 기능 제공

실시간 분석 및 탐지

- 신속한 분석을 위한 인메모리(In-Memory) 방식의 실시간 로그 분석 및 탐지 기능으로 분석 정확성 향상
- SIEM과 AI 분석 모델을 통합하는 확장형 분석 엔진으로 고급 분석 기능 지원

심화된 검색 기반 분석

- 수집 로그의 모든 필드에 대한 특정 조건 및 정규 표현식 등 다양한 분석 조건 설정 지원
- 탐지 룰 별 예외 조건 기능을 제공하며 특정 요일, 시간에 대한 예외 처리 가능
- 수집된 데이터를 토대로 평판 DB를 구성하여, 해당 DB의 데이터를 통한 분석 기능 제공

Features

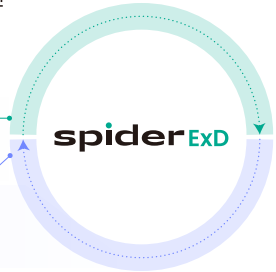
C. 폭넓은 확장성 제공

플랫폼 형태 아키텍처로 기능 확장 및 추가 용이

- API를 통한 내부 모듈 및 외부 시스템 연동 지원
- 파트너 협업을 통해 기능 지속 확장 가능

SPiDER ExD를 중심으로
이기종 솔루션 및 시스템의 자유로운 연동 지원

기능의 확장을 통한 통합 플랫폼화로,
빈틈없는 가시성 확보 및 보안 운영 효율성 극대화



Open API 연동 솔루션

- SOAR: 보안 운영·위협 대응 자동화
- AI: 머신러닝 기반 지도/비지도 분석 지원
- 취약점 진단: 취약점 진단 솔루션 연계 및 결과 연계
- 위협 인텔리전스(CTI): 위협 정보 및 위험 IP, URL, IoC, 탐지 정책 연계
- 대시보드: 사용자 정의 대시보드
- 정보보호 포털: 연계 기관 대응을 위한 포털
- 정보보호 솔루션: 차단 및 정책 연계
- 자산관리 솔루션 및 시스템 관리 솔루션 연계
- 정규화된 데이터를 메시지큐에 저장하여 내부 모듈 및 외부 솔루션과 연동 기능 제공

D. 고도화된 위협 탐지 및 대응

고급 위협 탐지 기능 제공, 추가 기능 및 연동 지원

- 정확하고 신속한 보안 위협 인사이트 도출을 위한 다양한 기본 탐지 및 조사 기능 제공
- (기본 제공) 내장된 사이버 위협 인텔리전스(CTI) 서비스 '클루(KLU:)' 기능을 통해, 최신 신변종 위협에 대한 대응력 향상
- (선택 사항) AI 보안 어시스턴트 '에어(AiR, AI Road)' 연동을 통해, 보안 데이터 분석의 정확성을 높이고 적합한 대응 방안 도출 가능

고급 탐지·조사 기능 제공

머신러닝 기반 분석 & MITRE ATT&CK 대시보드

- 머신러닝 기반 지도/비지도 분석, 위협 헌팅(Threat Hunting), 마이터 어택(MITRE ATT&CK) 프레임워크 분석 프로세스 등 다양한 기본 탐지 및 조사 기능을 통해 고도화된 위협 탐지 가능

위협 정보 연계 기능 제공

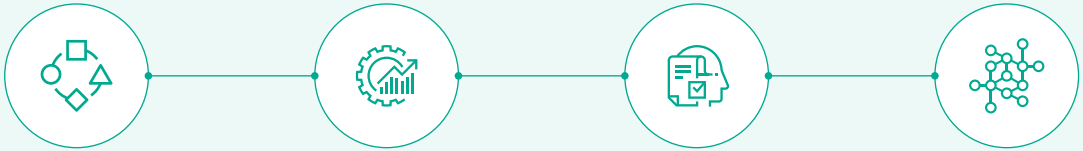
KLU: 사이버 위협 인텔리전스 'KLU: Threat Intelligence'

- 유해 IP/URL, 악성코드 해시값/취약점에 대한 관리 기능 제공
- 보안 기업에서 직접 제공하는 보안 뉴스, 취약점 정보 등 보안 콘텐츠의 자동 업데이트를 통해 최신 위협 상황에 대한 효과적인 대응 지원
- 기본 탑재된 CTI를 통해, 위협 정보를 실시간으로 연계 및 공유함으로써 신속 정확한 조사 지원

Benefits

SPiDER ExD의 도입으로 확장된 탐지, 다양해진 분석, 빨라진 대응을 경험해 보세요.

방대한 보안 데이터의 수집, 정확도 높은 분석, 자동화된 대응 프로세스 구현, 폭넓은 보안 기능 연계·확장을 통해
전체 공격 표면을 포괄하는 통합된 가시성을 확보하고, 시시각각 변화하는 IT 환경에 능동적으로 대응할 수 있게 됩니다.



수집

방대한 보안 데이터
수집 및 저장·처리

분석

수집된 데이터 간의
연관 관계 분석 정확성 향상

대응

위협 탐지·대응
효율성 극대화

통합

변화에 선제 대응 가능한
확장·연계

SPiDER ExD는 **포괄적 관점에서 보안 운영 효율성을 극대화**함으로써
더욱 강력하고 효과적인 보안체계를 구축할 수 있도록 도와줍니다.

이글루코퍼레이션은 1999년 창립 이래, 조직의 업무 환경 및 업무 수행 방식의 혁신을 앞당길 수 있는 핵심 기술 구현에 집중하여 왔습니다. 국내 최초의 보안 정보 및 이벤트 관리(SIEM) 솔루션 출시를 시작으로, 인공지능(AI), 보안 운영·위협 대응 자동화(SOAR), 위협 인텔리전스(CTI), 운영 기술 보안(OT), 전문 보안 서비스를 아우르는 다각화된 사업을 전개하며, 보안·인공지능·클라우드·빅데이터 분야를 아우르는 종합 IT 기업으로 성장했습니다. 이글루코퍼레이션은 고유의 AI 기반 보안 운영·분석 플랫폼을 바탕으로, 급변하는 비즈니스 환경에 최적화된 해결책을 제시하는 핵심 조력자 역할을 지속 수행하고자 합니다.

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

IGLOO