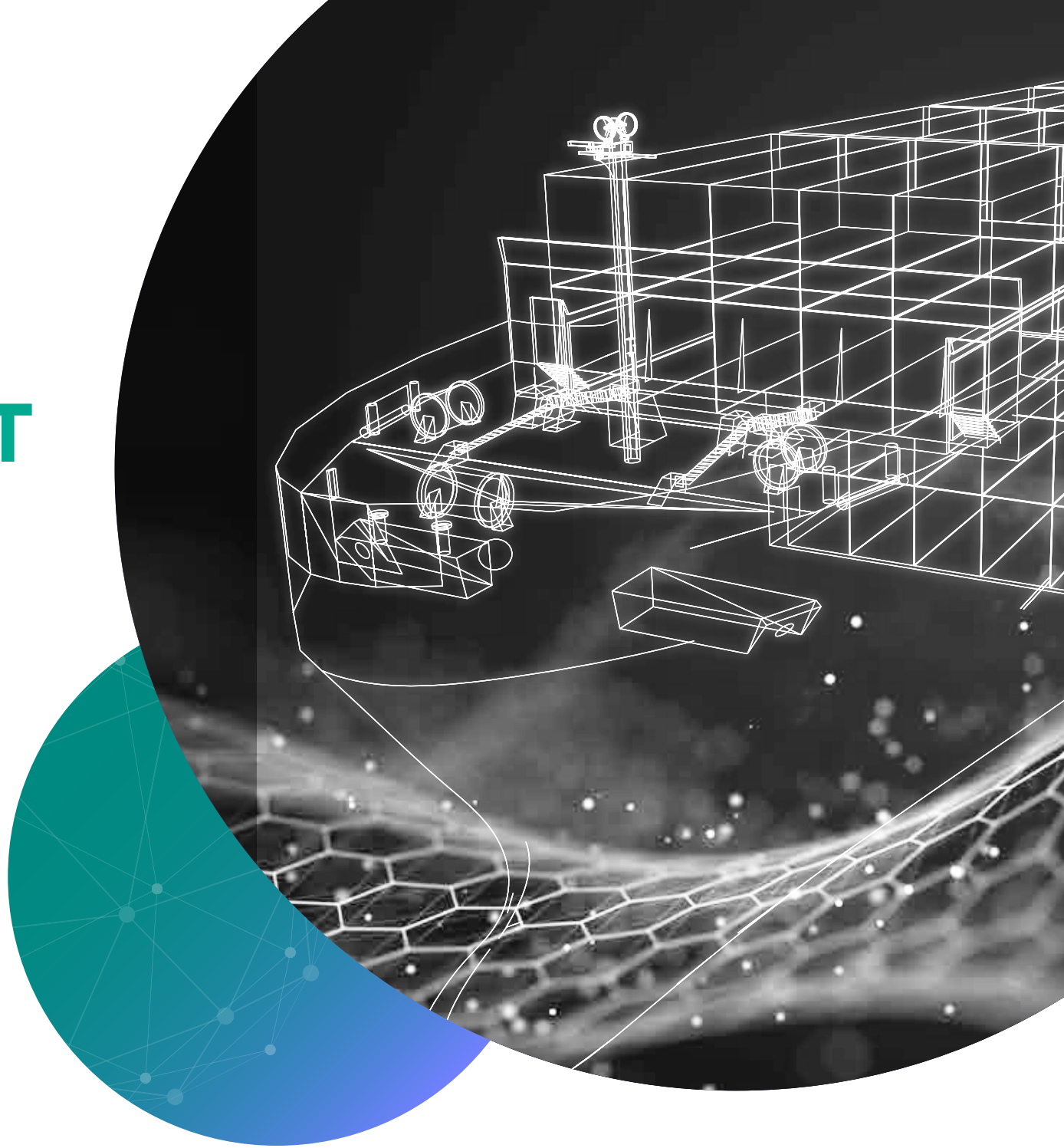
IT와 OT 영역을 통합적으로 아우를 수 있는 있는 융합보안관제 체계 구현

OT 보안 관리 솔루션

spider OT



IGLOO

Background

디지털 전환이 가속화됨에 따라, 스마트 선박, 스마트 팩토리, 스마트 빌딩 등의 주요 설비 제어와 관련된 OT(운영 기술, Operational Technology) 보안의 중요성이 대두되고 있습니다. OT 환경을 노린 보안 사고 발생 시에는 전 세계 경제 활동과 국가 시스템을 뒤흔드는 큰 피해가 발생할 수 있습니다.
또한, IT(정보 기술) 네트워크와 OT의 접점이 점점 넓어지면서, 이를 노리는 보안 위협도 증가하고 있기 때문에 가용성 확보에 중점을 둔 OT 환경에 최적화된 보안 체계 구축의 필요성이 부각되고 있습니다.

IT, OT 환경을 아우르는 보안 역량

OT 침해 사고는 IT 환경 기반 악성코드를 통해 발생하므로,
OT는 물론 IT 보안 위협에 대한 이해와 대응 역량 필요

이기종 보안 이벤트에 대한 통합 분석·관리 역량 보유

OT 보안은 OT 환경에 대한 정확한 현황 파악에서 시작

특정 OT 환경에 최적화된 솔루션 개발 역량 보유

물리 보안 기업 및 관계사와의 협업을 통해,
스마트선박·스마트팩토리·스마트빌딩 보안 역량 강화

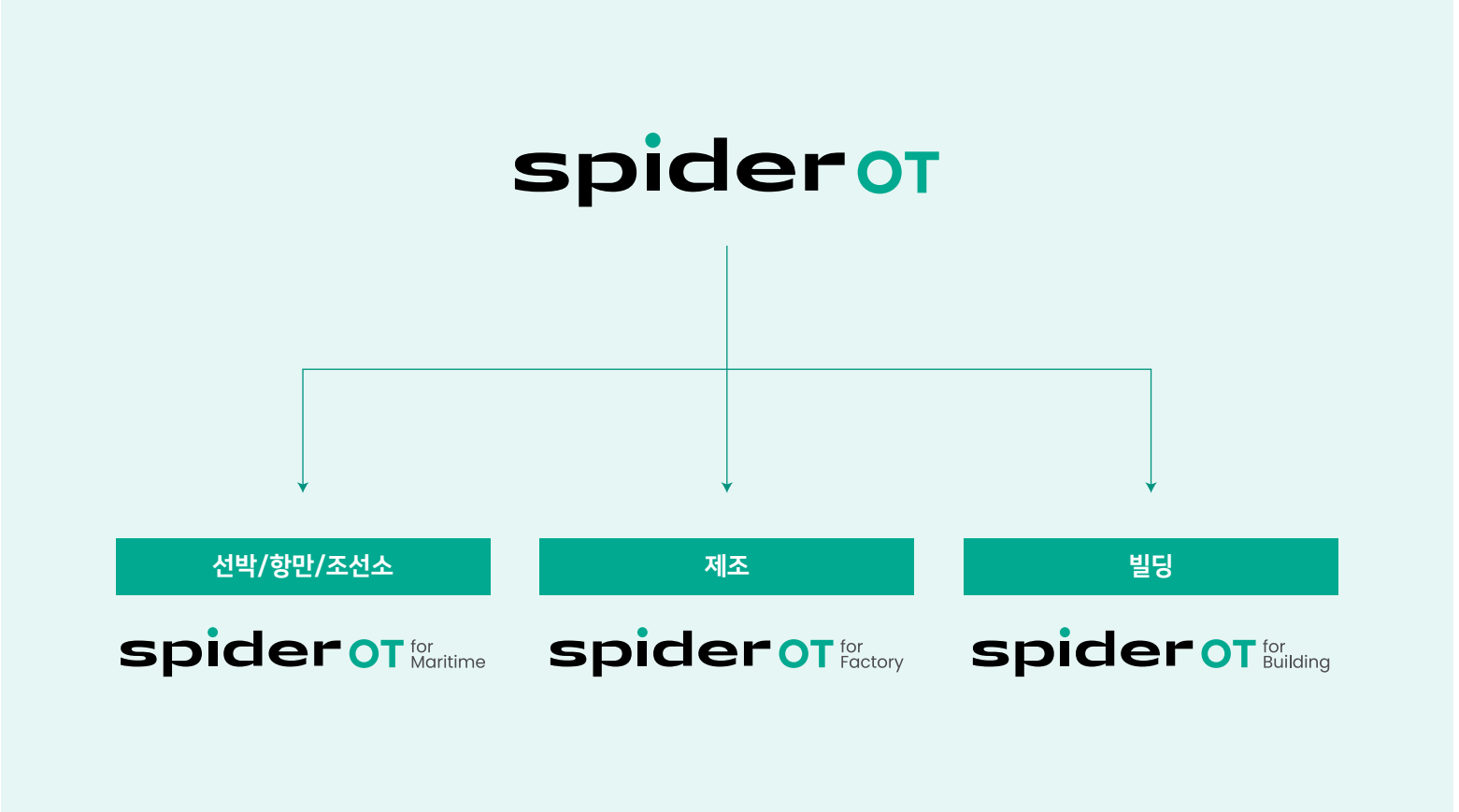
IT 영역 **OT 보안솔루션** OT 영역

IT, OT 영역을 중앙에서 통합적으로 아우를 수 있는
융합보안관제 체계 구현

Overview

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 제공합니다. 보안 담당자들은 SPiDER OT를 통해 IT 보안 장비와 OT 자산을 식별하고, 프로토콜을 분석하는 OT 센서 및 OT 보안 솔루션에서 수집한 이기종의 보안 이벤트를 통합 관리할 수 있을 뿐만 아니라, OT와 IT를 아우르는 위협 분석 및 가시성 확보로 OT 보안 위협에 대한 선제적인 대응이 가능합니다.

이글루코퍼레이션은 인공지능(AI), 보안 정보 및 이벤트 관리(SIEM) 등의 보안 솔루션 개발을 통해 축적한 이기종 보안 이벤트 분석 역량을 활용하여, 해양·제조·건설 산업 영역별로 특화된 OT 보안 전략을 제시합니다.



About SPiDER OT

선박/항만/조선소

spider OT for Maritime

스파이더 오티 포 마리타임(SPiDER OT for Maritime)은 선박 환경에 최적화된 보안 기능을 제공하는 선박 통합보안관리 솔루션입니다. 선박 네트워크 중 비정상 행위에 대한 지표를 수립하고, 이를 토대로 판단한 사이버 위협 정보와 대응 가이드를 제공합니다.

또한, 선박 네트워크와 보안 정책에 대한 철저한 분석을 기반으로 선박에 특화된 보안성과 안정성, 사용자 편의성을 보장합니다. IT 비전문가 선원도 사이버 위협 및 자산 현황의 이상 유무를 손쉽게 인지 및 모니터링할 수 있도록, 필수 기능 중심의 직관적인 메뉴를 구성했습 니다. 기존 제품과는 다른 선박 내 독립적인 로그 수집·이벤트 분석 방식 적용으로, 위성통신 네트워크가 과점 되는 트래픽 이슈도 해소했습니다.

2024년 의무 적용되는 선박 사이버 보안 규정 (IACS E26, E27)에 선제 대응하기 위해 선박 IT 서비스 전문사 ㈜포스텍과 업무 협약을 맺고 선박의 사이버 복원력을 높이는 보안 솔루션을 공급하고 있습니다.

제조

spider OT for Factory

스파이더 오티 포 팩토리(SPiDER OT for Factory)는 제조업(공장)에 특화된 OT 보안관리 솔루션으로 IT/OT에 대해 통합보안관리가 가능한 OT SIEM과 OT 센서가 함께 구성된 제품입니다.
IT 영역의 다양한 정보보호 제품군과 로그 연동을 하며 OT 영역의 네트워크 트래픽을 수집하여 프로토콜을 분석하고 이를 통합대시보드로 관리가 가능합니다.

OT 센서는 공정, 제어망에 영향이 없도록 패시브 미러링 (Passive Mirroring) 방식으로 OT 자산을 자동 수집 하며, 수집된 자산 정보는 퍼듀 모델(Purdue Model) 기준으로 자동 분류하여 자산 상세정보를 제공합니다.

다양한 센서 제품과 연계가 가능하며, 각 제어, 공정 시스템에 특화된 사이버 위협정보와 탐지 정책을 제공합니다.

빌딩

spider OT for Building

스파이더 오티 포 빌딩(SPiDER OT for Building)은 스마트빌딩에서 운영되는 재난관리 솔루션과 IT 정보보호 솔루션을 연계하여 통합으로 관리합니다. 위협관리를 위한 SOP 대응 시나리오와 3D 시각화된 실시간 모니터링을 제공하며, 옵션으로 OT 센서 등 다양한 제품과 연계가 가능합니다.

스마트빌딩의 모델을 3D 시각화 제공하고, 층별 시스템을 레이어로 구성하여 알람 상황 정보를 실시간으로 파악할 수 있습니다.
화재, 시설관리, 출입통제, CCTV 등의 재난관리 정보와 랜섬웨어, 웹해킹, 악성코드, 제어시스템 공격 등의 사이버 공격 정보를 통합하여 스마트빌딩에서의 요구하고자하는 최적의 통합 모니터링 방안을 제공합니다.

Why SPiDER OT

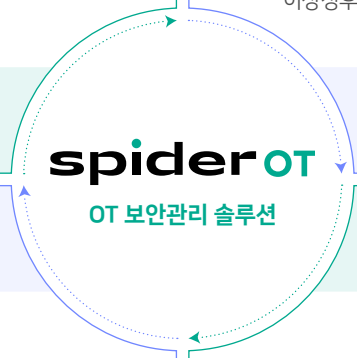
IT 보안	ICS/OT 보안	IoT 보안
방화벽(Firewall), 침입탐지/방지시스템(IDS/IPS), DDoS, 통합위협관리(TMS), 웹방화벽(WAF), Anti-virus, 네트워크 접근 제어(NAC), Etc	원격감시 제어시스템(SCADA), 프로그래밍 제어장치(PLC), 긴급경보 방송시스템(EWS), 운전자용 전산기(OWS), 분산 제어시스템(DCS), 인간·기계 인터페이스(HMI), Etc	출입관리, CCTV, 방재, 냉난방 공조시스템(HVAC), Etc

01 융합보안관리
Convergence Security Management

- IT 보안장비, OT 센서 및 OT 보안솔루션을 연동하여 제어시스템에서 발생되는 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 통합관리

02 가시성 및 효과성 관리
Visibility & Effectiveness Management

- 사용자 정의 OT 관제맵을 통해 통합관제, 보안관제, 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



03 위협 분석 관리
Threat Analysis Management

- 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)

04 실시간 이벤트 관리
Real-Time Event Management

- 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

Features

SPiDER OT는 다양한 OT 시스템에 대한 폭넓은 가시성을 확보하고, 이를 IT 영역과도 아울러
OT 자산에 대한 정밀한 제어 및 감시가 가능하도록 하는 OT 환경에 최적화된 통합보안관제 솔루션입니다.

데이터 수집 및 분석

IT 보안시스템 연계 및 보안 데이터 수집 (SYSLOG/API 연동 등)

OT 센서/DPI 연계 시 OT 데이터 수집

■ **자산현황 식별**
- 네트워크 패킷 분석을 통한 자산 정보 식별

데이터 정규화

원시로그 파싱로그

■ **정형데이터 파싱**
- 정규표현식, Key, 구분자 파싱
- 사용자 정의 파싱 지원

■ **자산정보 현행화**
- 수집 자산 정보 목록화 DB 적용
- 미수집 자산정보 식별

로그 관리

■ **로그 검색**
- 로그 검색
- 이기종 연계 검색
- 멀티레벨/통계기반 등 다차원 로그분석

■ **자산정보 관리**
- 자산정보 관리 기능 제공 (등록/수정/삭제)
- 일괄 관리 기능 지원

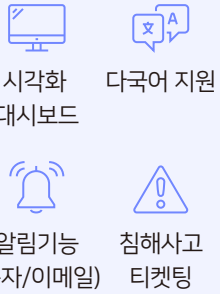
실시간 모니터링

■ **실시간 모니터링**
- 공격유형, 위험도에 따른 실시간 모니터링

■ **경보 분석**
- 근거 이벤트 및 공격 유효성 분석

■ **자산 및 네트워크 운영 모니터링**
- 자산 및 네트워크 통신 이상유무 탐지

통합 모니터링 UI



■ **통합 모니터링 UI**
- 네트워크 토폴로지맵
- 시각화 하이라이트

■ **자산현황 시각화**
- 이상 경보 시각화
- 등록된 자산 정보를 대시보드에 연계

Features

OT 센서 (Option)

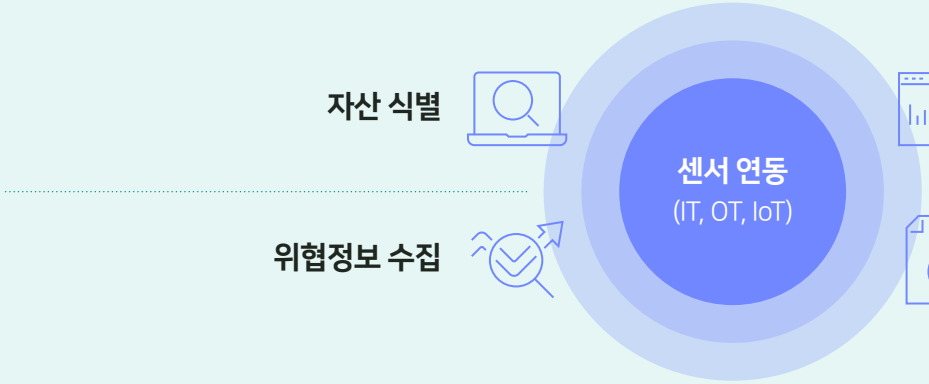
OT 센서는 각 계층별 제어시스템 자산을 식별하고 산업전용 프로토콜 트래픽을 분석하여 위협정보를 수집하며 OT망 내 잠재적 위협을 탐지합니다.
또한, Yara 및 Snort 탐지정책을 설정함으로써 위협에 신속하게 대응이 가능합니다.

자산 식별

- 패시브 미러링(Passive Mirroring) 방식을 통한 OT 자산 자동수집
- 수집된 자산 자동분류 및 자산현황 통계 제공
- 네트워크 토폴로지 자동 구성 및 자산 타입에 따른 통계정보 제공
- 식별된 자산을 CSV 파일로 Export하여 자산관리의 편의성 제공

탐지정책 설정

- Rule set 기반의 Alert을 통한 MITRE ATT&CK 탐지 정보 제공
- 다양한 벤더사의 SIEM과 연동 API를 제공
- 최신 시그니처 업데이트 파일을 제공하여 인터넷이 되지 않는 네트워크에서 최신 시그니처 수동 업데이트 가능



위협정보 수집

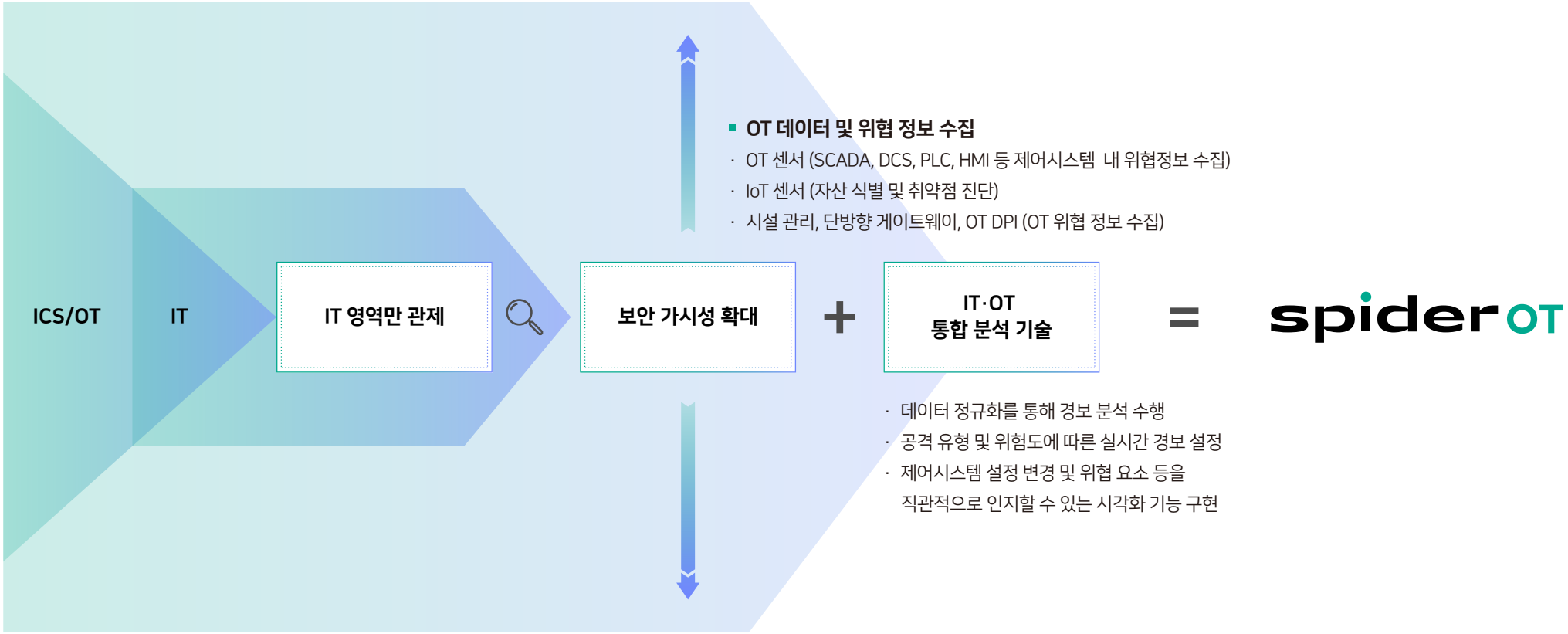
- Threat Intelligence(시그니처) 기반 위협식별로 Packet Rules (시그니처) 기반의 탐지 방법 활용 (Packet-Rule, Yara-Rule, STIX)
- 실시간 Alert 자동 갱신기능으로 악성코드 감염 상태 실시간 탐지현황 제공
- 프로그램 다운로드 및 신규 통신 연결 탐지 알람
- 자산의 펌웨어 변경 내역을 추적하여 관리 가능
- 취약점이 확인된 자산을 탐지하여 세부내용 및 발견 날짜, 조치 상태 조회 기능 제공

프로토콜 분석

- 취약 프로토콜 현황 및 목록 조회 가능
- ICS/OT 프로토콜에 대한 DPI 기능 지원 (Modbus/TCP, Ethernet/IP, FTE, VNET/IP 등)
- 패킷 아키텍쳐 구성에 포함된 내용은 모두 구분되어 저장
- 제어 프로토콜의 변수 및 기능코드를 포함해 제품 환경설정을 통한 전체 프로세스 확인 가능

Benefits

SPiDER OT는 IT 환경으로 한정돼있던 보안 영역을 OT/ICS 환경으로까지 확대시킴으로써 이기종의 OT 보안 시스템에 대한 폭넓은 가시성을 확보하고 이를 정밀하게 제어·모니터링할 수 있도록 지원하여, OT 환경에 최적화된 보안 체계를 구축합니다.



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