조직에 최적화된 보안 업무 자동화 구현

**보안 운영·위협 대응 자동화(SOAR) 솔루션**

# spider SOAR

IGLOO

## Background

### 다가온 보안 운영 자동화 시대 어떻게 실현할 수 있을까?

디지털 트랜스포메이션 가속화에 따라 IT 인프라의 복잡성도 높아지면서, 기존의 방어 체계로는 예측하기 어려운 복합적인 사이버 공격도 증가하고 있습니다. 그러나 이에 맞설 전문 인력과 시간, 자원은 한정되어 있는 것이 사실입니다. 한정된 인력으로 수많은 IT 인프라와 컴플라이언스에 대응하고자 기업이 도입하는 보안 솔루션 수도 늘고 있지만, 이는 근본적인 해결책이 되기는 어렵습니다. 날로 진화하는 보안 위협과 기하급수적으로 쌓이는 보안 정보, 점점 늘어나는 보안 솔루션 속에서, 되레 관리 업무가 늘어나고 대응 프로세스의 복잡성이 심화되는 어려움이 발생할 수 있기 때문입니다.

이러한 배경에서 보안관제센터(SOC, Security Operation Center)의 복잡성을 해소하고 보안관리 업무의 효율성을 높여주는 **보안 운영·위협 대응 자동화(SOAR, Security Orchestration, Automation and Response) 솔루션**의 중요성이 더욱 높아지게 되었습니다.

### 그러나 막상 SOAR를 도입하기 위해 여러 요소를 검토하다 보면, 예상치 못한 난관에 부딪히게 됩니다.


SOAR의 진정한 가치는 단일 솔루션으로서의 기능보다 보안 환경 전반을 아우르는 프로세스 개선에 있습니다. 그리고 이는 보안 전문가가 실제로 잘 사용할 수 있는, 활용도 높은 자동화가 가능할 때 비로소 실현될 수 있습니다.

하지만 현실적으로는 국내 보안 환경과 조직에 최적화된 플레이북(Playbook)이 미비할 뿐만 아니라 기존에 구성되어 있는 솔루션 및 시스템 과의 연동 문제로 오늘날 많은 기업들은 SOAR의 도입을 망설이고 있습 니다. 또 이미 솔루션을 도입했다 하더라도, 위의 문제는 여전히 남아 만족할 만한 성과를 얻지 못하고 있습니다.

제품 도입만으로 보안 운영 프로세스를 자동화하여 실질적인 성과를 낼 수 있는 SOAR 솔루션은 많지 않습니다.

## Overview

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

spider SOAR

**보안 운영·위협 대응 자동화**
(Security Orchestration, Automation and Response)

**오케스트레이션 (Orchestration)**
다양한 솔루션 및 데이터 연동

**자동화 (Automation)**
플레이북 기반 분석 및 자동화 대응

**이벤트 대응 (Event Response)**
자동 차단 및 다양한 보안 대응 지원
(네트워크 격리, 취약점 패치, IP 자동 차단, 위협헌팅 등)

**케이스 관리 (Case Management)**
위협 중심 분석 및 대응 프로세스

## Why SPiDER SOAR

**01** 정확도 높은 자동 위협 탐지 가능

### AI 지도학습 모듈을 활용한 인공지능 기반 자동화 대응

· 실제 관제 환경에 최적화된 AI 정오탐 판단 위험 모델 보유
· AI 기반의 정오탐 판단 모듈로 통합위협관리(TMS), 침입방지시스템(IPS), 웹방화벽(WAF)의 페이로드(Payload) 데이터 정오탐을 판단하여 자동 대응
· AI 시스템 예측 결과에 대한 침해대응 프로세스 자동화로
① 초동분석 및 대응시간 단축, ② 사이버침해 대응능력 강화

**02** 자동화된 선제적 대응 가능

### 위협 인텔리전스(Cyber Threat Intelligence) 연계를 통한 대응

· CTI와의 연계를 통해 선제적 자동 대응 체계 마련
- 구축형 CTI를 통해 상위 중앙관제센터에서 배포하는 수백 개의 차단 권고 IP와 위협 정보를 실시간으로 수집
- 구축형 CTI가 없는 경우, SOAR에서 직접 상위기관 CTI나 IGLOO CTI에 접속하여 실시간으로 위협 정보 수집

**03** 경보 탐지 중심에서 침해대응/상세 분석 중심의 체계 구현 가능

### MITRE ATT&CK 프레임워크 연계를 통한 대응

· MITRE ATT&CK 프레임워크 분석 앱을 통해 공격 현황에 대한 가시성 확보
- 공격의 전체 범위를 표현하여 해커가 어떤 공격을 했으며, 다음에 어떤 액션을 취할 가능성이 높은지를 예측하고 분석하는 프로세스 마련
- 공격 IP, 테크닉 아이디(TID), 전술명, 위협 그룹 등을 검색하여 상세 분석 수행
- 기간 조회를 통해 장기간에 걸친 공격의 흐름과 변화 파악

**04** 전반적인 보안 프로세스 자동화로 인한 대응 속도 향상 가능

### SOAR to SOAR를 통한 기관 연계 대응
**(상위기관-소속기관 간 연계 및 자동 차단 대응)**

· SOAR to SOAR 연계를 통해 실시간 자동 및 긴급 차단 체계 마련
- 상위 기관-하위 기관 SOAR간 이관 티켓, 공격IP, 공지 사항 등 동기화
- 차단 권고 IP들의 자동 배포 및 실시간 차단으로
① 대응력 향상, ② 단순 반복 작업 및 중복 업무 최소화

**05** 높은 활용도 및 효과성 지속 유지 가능

### 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

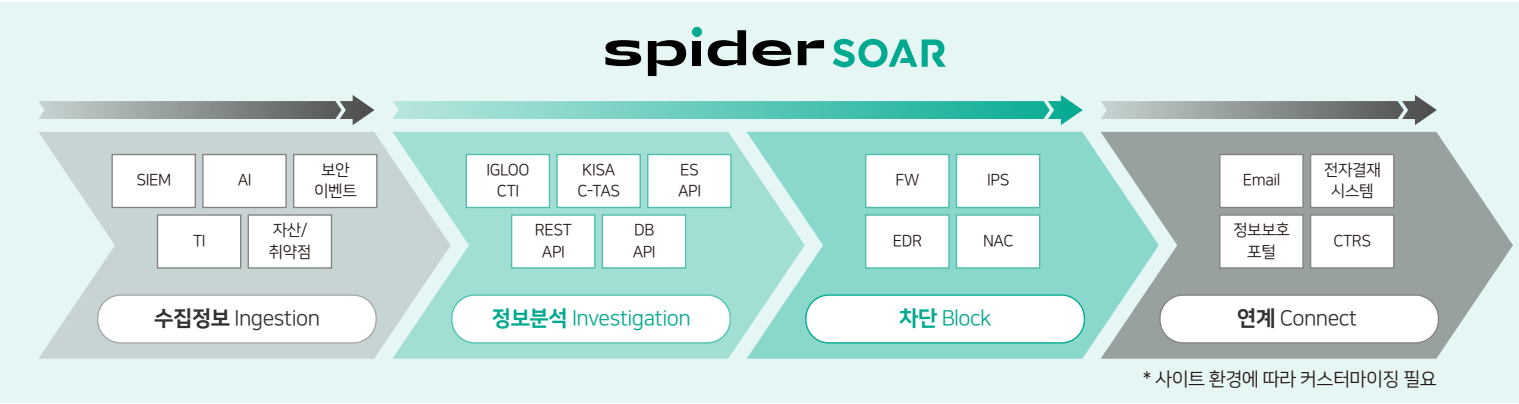
## SPiDER SOAR Architecture

이글루코퍼레이션은 다년간의 보안관제센터(SOC) 운영 경험을 바탕으로 보안 정보 및 이벤트 관리(SIEM), 위협 인텔리전스(Threat Intelligence) 등 국내 보안 조직들이 도입한 각종 보안 솔루션과 업무 시스템 간의 긴밀한 연동을 지원합니다.
위협 탐지부터 차단, 격리 조치까지 아우르는 일원화된 침해대응 프로세스를 구현하고, 보안 환경 전반에 걸친 자동화를 가능하게 합니다.

## Features

### 01 이기종 보안 솔루션의 유기적 연동을 통한 **자동화된 침해대응 프로세스 운영**

· 국내·외 다양한 보안 솔루션 및 업무 시스템 연동 지원
· 수집정보(Ingestion), 정보분석(Investigation), 차단(Block) 연동 APP 연계 모듈 개발
· 위협 대응 단계 수행 보안 솔루션의 API 연동을 통해 보안관제 환경에서 수집, 탐지뿐 아니라 차단, 격리 조치까지의 일괄 수행을 통한 작업 효율성 향상




* 사이트 환경에 따라 커스터마이징 필요

### 02 20여 년 보안관제 노하우가 축적된 **플레이북(Playbook) 제공**

· 공공·민간·국방 등 다양한 산업 군의 고객사에서 성공적으로 수행한 다년간의 보안관제 경험이 집약된 플레이북
  - 이글루코퍼레이션 전문 조직과의 협업 및 커뮤니케이션을 통해 SOAR를 활용한 관제 체계에 관제 노하우 적용
  - 보안관제에 최적화된 플레이북 지속 개발 및 SOAR 반영
· 플레이북을 통한 단순 반복 업무 최소화 및 보안관제 효율 향상

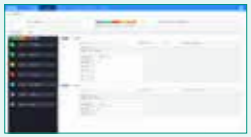

Playbook Workflow Design


Playbook Workflow Chart 편집기


Playbook 상태 모니터링


Playbook Filter Action Component 설정

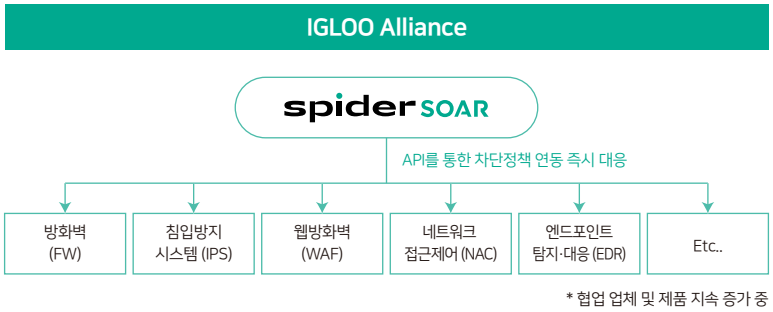

API:APPs 설정


Playbook 처리결과 상세 조회

## Features

### 03 국내 최대 규모의 보안 솔루션 연동을 통한 자동 차단

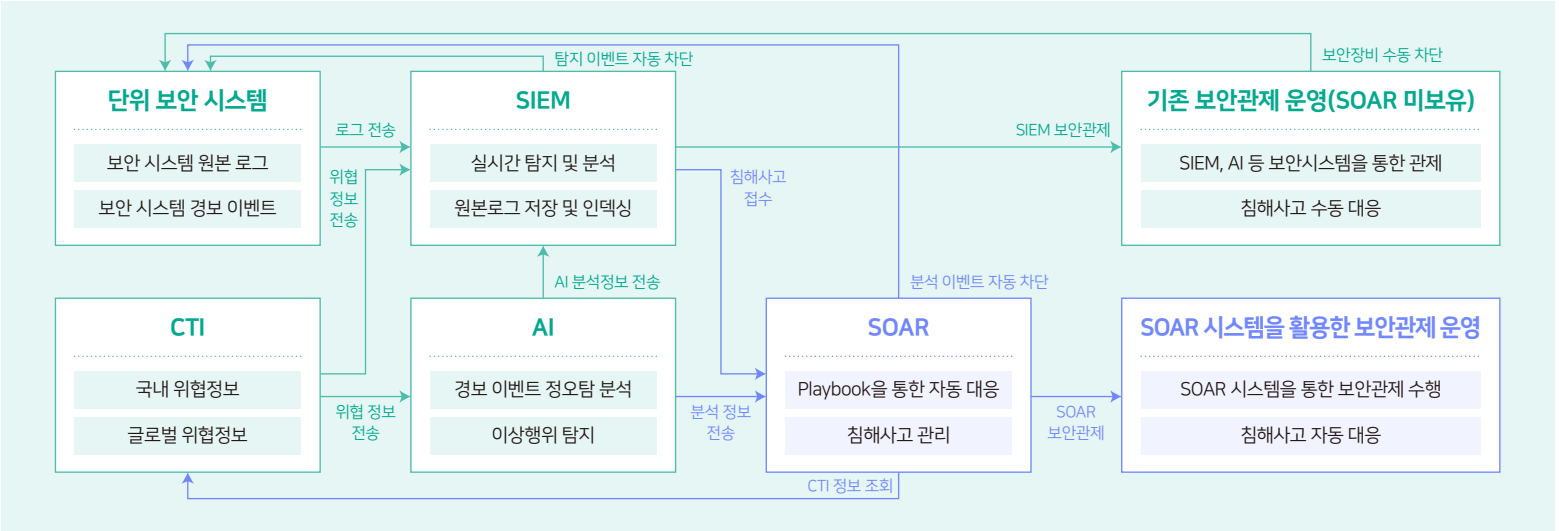
· IGLOO Alliance 협약 모델 운영 중
· 국내 최대 규모의 보안솔루션 연동 및 자동 차단
· 방화벽(FW), 침입방지시스템(IPS), 네트워크 접근제어(NAC) 등
자동차단을 위한 다양한 제품군 연동
※ SECUI(방화벽), WINS(IPS), 안랩(방화벽, IPS), 파이오링크(WAF) 등
국내 최다 사이트 구축 보안 솔루션 연동 지속 확대




* 협업 업체 및 제품 지속 증가 중

### 04 경보탐지에서 침해대응 중심으로 SOAR 기반 보안관제 프로세스 구축

· 기존의 SIEM 경보 기반 탐지 중심의 보안관제가 아닌, SOAR 기반 대응 중심의 보안관제 프로세스 구성
· SIEM과 인공지능시스템(AI)과의 효율적인 운영을 위한 최적의 연계방안 구성
· SOAR 기반 침해대응 분석 및 대응 지원을 위한 프로세스 및 대시보드 구성

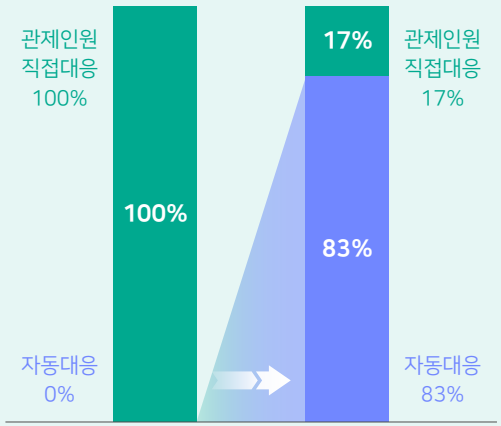


## Benefits

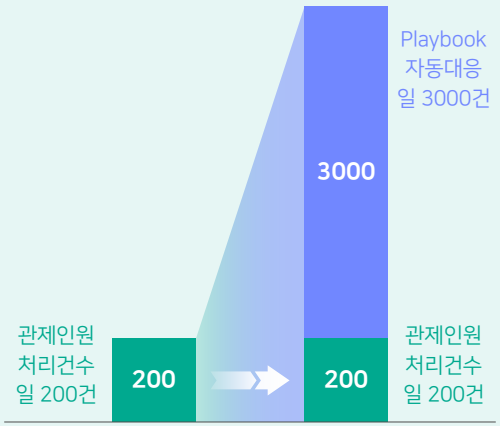
### 보안관제 효율성 향상

SPiDER SOAR는 국내 수많은 고객사에서 실제로 활용되고 있는 플레이북을 바탕으로 탐지된 공격에 대한 자동 분석·대응 기능을 제공함으로써 위협 대응에 소요되는 시간을 최소화하고 보안 인력 역량 편차 문제를 해결해 줍니다. SOAR 적용을 통해 보안 전문가들은 단순 반복적인 업무 처리에서 벗어나 분석 업무와 같이 보안 전문가의 판단이 반드시 요구되는 중요도 높은 업무에 집중하게 되면서 보안관제의 효율성을 극대화할 수 있습니다.

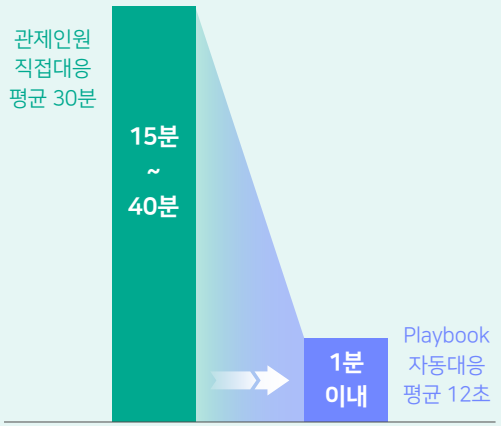
**위협 분석 및 대응 자동화**




**대응(티케팅) 건수**
(일일 자동 차단 IP 1,400개)




**위협 대응 시간**
(탐지→분석→보안장비 차단 시간)




* SOAR 도입 전후 관제 효과성 분석 (이글루코퍼레이션 운영 사이트 기준)

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