AI Leader in Cyber Security

IGLOOSECURITY

뉴노멀시대, 변화하는 보안위협

SOAR를 통한 보안관제 전략

이글루시큐리티 전략기획팀 이규환 부장

AI Leader in Cyber Security
IGLOOSECURITY

CONTENTS

AI Leader in Cyber Security
IGLOOSECURITY

Ⅰ. 보안관제 현황 및 SOAR의 필요성

Ⅰ. 보안관제 현황 및 SOAR의 필요성

변화하는 위협환경

이글루시큐리티 전망 2021년 5대 보안 위협	포스트 코로나 시대 도래, 비대면 플랫폼 노린 보안위협 대두	'코로나19' 팬데믹 이슈 악용한 공격 급증	IT와 OT 환경의 안전성 확보 조치: 융합보안관제	AI 활성화를 위한 기술한계 극복: eXplainable AI(XAI)	이글루시큐리티 전망 2021년 5대 보안 기술·방법론
OT 영역을 노리는 사이버위협 증가	인공지능(AI)의 양면성	금전적인 목적의 사이버공격 증가: 랜섬웨어를 넘어 디도스(DDoS)로	데이터 경제 (Data Economy) 활성화와 정보주체 결정권 확립의 양립	보안관제 효과성 극대화 기술: SOAR	온택트(Ontact) 시대의 디지털 신뢰 (Digital Trust) 전략

* 2021년 보안위협·기술전망, 이글루시큐리티

Ⅰ. 보안관제 현황 및 SOAR의 필요성

보안관제의 어려움 증대

보안관제의 어려움 증대

- 보안 위협은 정교하게 진화하고, 대응해야 할 컴플라이언스는 늘어나며,
- 보안 운영 환경이 감당하기 힘든 수준으로 복잡해지고, 이로 인해 분석할 데이터는 증가하고 있다.

- **그러나, 이를 대응하여 분석할 보안관제인력은 한계에 다다르고 있다.**

관리적 측면

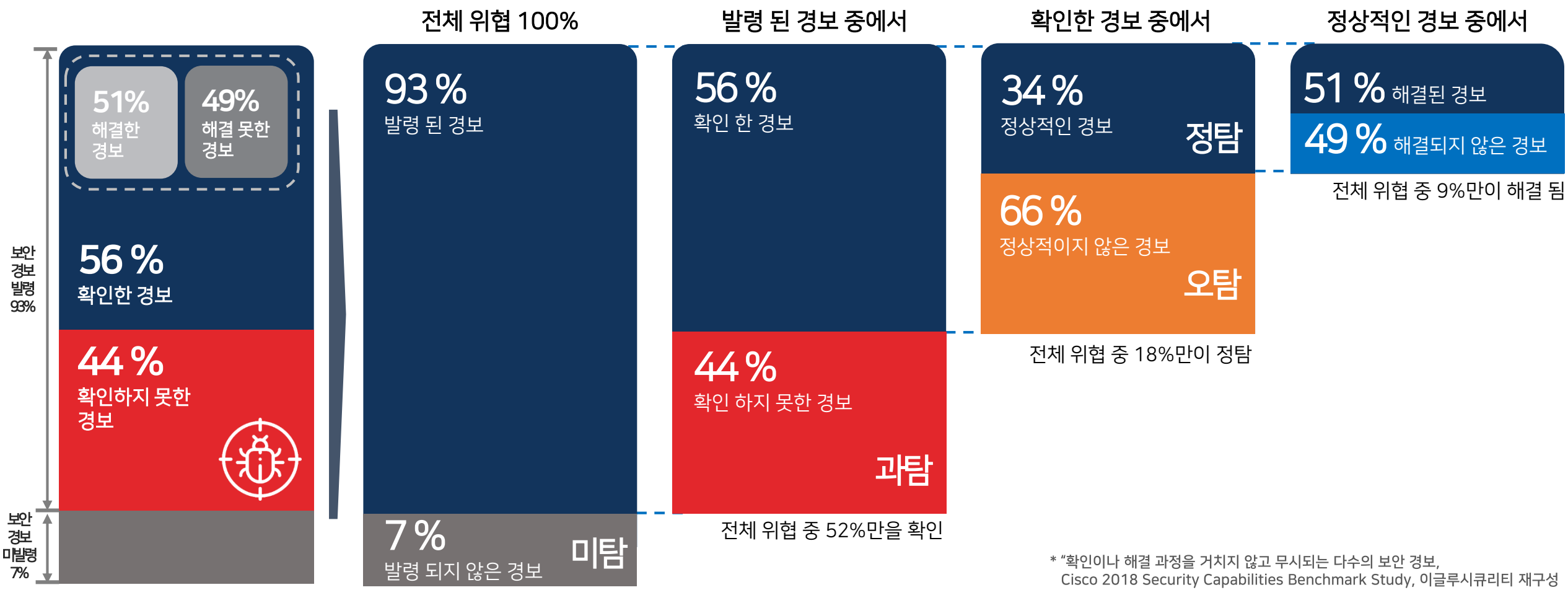
- IT 인프라 복잡성 증가에 따른 공격요인 증가
- 대응해야 하는 컴플라이언스의 증가
- 보안 예산 부족으로 인한 보안 담당 인력 부족

기술적 측면

- 신규 보안위협 증가로 인한 보안솔루션 복잡도 증가
- 보안솔루션 경보 급증으로 보안관제 업무 급증
- 보안 전문인력 부족 및 성숙도 부족에 따른 휴먼에러(Human Error) 증가

Ⅰ. 보안관제 현황 및 SOAR의 필요성

경보의 홍수 앞에 선 보안관제



* "확인이나 해결 과정을 거치지 않고 무시되는 다수의 보안 경보,
Cisco 2018 Security Capabilities Benchmark Study, 이글루시큐리티 재구성

Ⅰ. 보안관제 현황 및 SOAR의 필요성

보안관제의 대응 한계

**"일반적인 규모의 SOC는 1주일에 약 17,000개의 경보를 받고 있으며,
매년 오탐(false positive)을 추적하는 데 21,000시간을 소비한다."**

- Cost of Malware Containment report, Ponemon Institute -

보안 환경 변화 및 증가된 탐지 데이터 대응과정에서
보안관제요원의 분석 및 대응은 한계에 도달

Ⅰ. 보안관제 현황 및 SOAR의 필요성

SOAR 필요성 대두

위협에 대응하기 위한 보안관제 전략의 변화

- 보안관제의 패러다임이 변화 됨에 따라 Zero Trust 기반의 차세대보안관제 대응이 필요하고, AI 및 위협정보(TI, Threat Intelligence)활용을 통한 Orchestration과 Automation 필요성 급증
- Zero Trust 보안관제 환경에서는 “단순 소모적인 수작업 보안관제 업무 절감” 및 “위협 수준에 맞는 명확한 보안이벤트 대응” 요구 증가

위협 대응 레벨 자동 분류, 관제 노하우 기반 Playbook을 통한 유기적 대응 자동화를 위한

SOAR 필요성 대두

Security Orchestration, Automation and Response, 보안 오케스트레이션 · 자동화 및 대응

AI Leader in Cyber Security
IGLOOSECURITY

II. SOAR의 기능

(Security Orchestration, Automation and Response)

Ⅱ. SOAR의 기능 (Security Orchestration, Automation and Response)

SOAR 개념

SOAR

(Security Orchestration, Automation and Response)

**다양한 사이버 위협에 대해, 대응 수준을 자동으로 분류하고
표준화된 업무 프로세스에 따라
보안 업무 담당자와 솔루션이 유기적으로 협력할 수 있도록 지원하는 플랫폼**

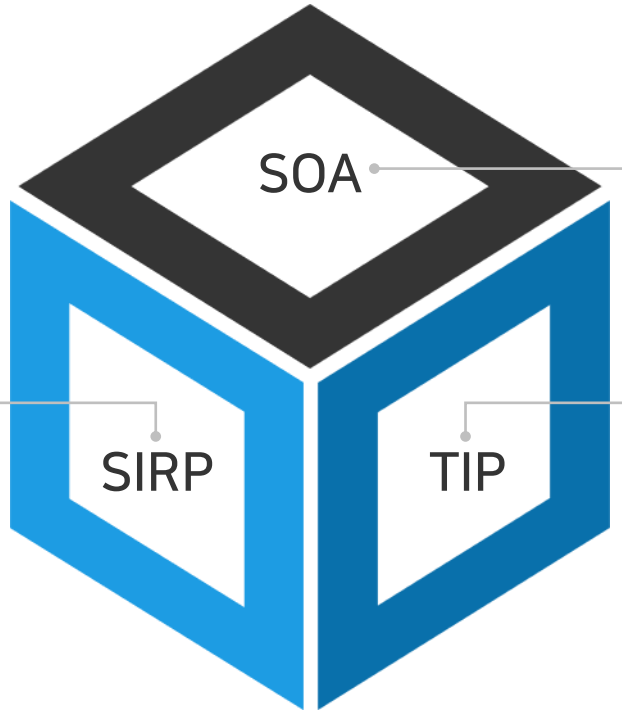
* SOAR 정의, Gartner(2018)

Ⅱ. SOAR의 기능 (Security Orchestration, Automation and Response)

SOAR 구성

SOAR 구성

- SOAR는 사이버위협 대응 레벨 자동 분류 및 대응 자동화를 위해 관제 노하우 기반 Playbook을 통하여 다음과 같이 SOA, SIRP, TIP의 구성으로 결합되어 유기적으로 동작



SOA Security Orchestration and Automation, 보안 오케스트레이션 및 자동화

- 보안 오케스트레이션 및 자동화
- 솔루션 간 연동 복잡성 해소 업무 처리 시간 단축
- 수많은 보안 솔루션을 운영 관리하는 업무 부담 해소

SIRP Security Incident Response Platforms 보안사고 대응 플랫폼

- 보안사고 대응 플랫폼
- 대응 프로세스 표준화
- 인력 간 역량 격차 축소
- 전문 인력 부족 문제 해결

TIP Threat Intelligence Platforms, 위협 인텔리전스 플랫폼

- 위협 인텔리전스 플랫폼
- 위협 데이터 수집/분석
- 분석 효율화
- 단순 반복적 업무량 절감

Ⅱ. SOAR의 기능 (Security Orchestration, Automation and Response)

보안관제 세대 별 변화와 SOAR의 위치

단위보안관제
Perimeter Security

- 단위 보안 솔루션 모니터링

1세대

통합보안관제
Data Security

- 관제 범위 확대
  (트래픽, 취약점, 웹, etc.)
- ESM 기반 보안관제
  (Enterprise Security Management)

2세대

빅데이터보안관제
Trust Security

- 빅데이터 기반 시나리오 관제
- SIEM 기반 보안관제
  (Security Information and Event Management)

3세대

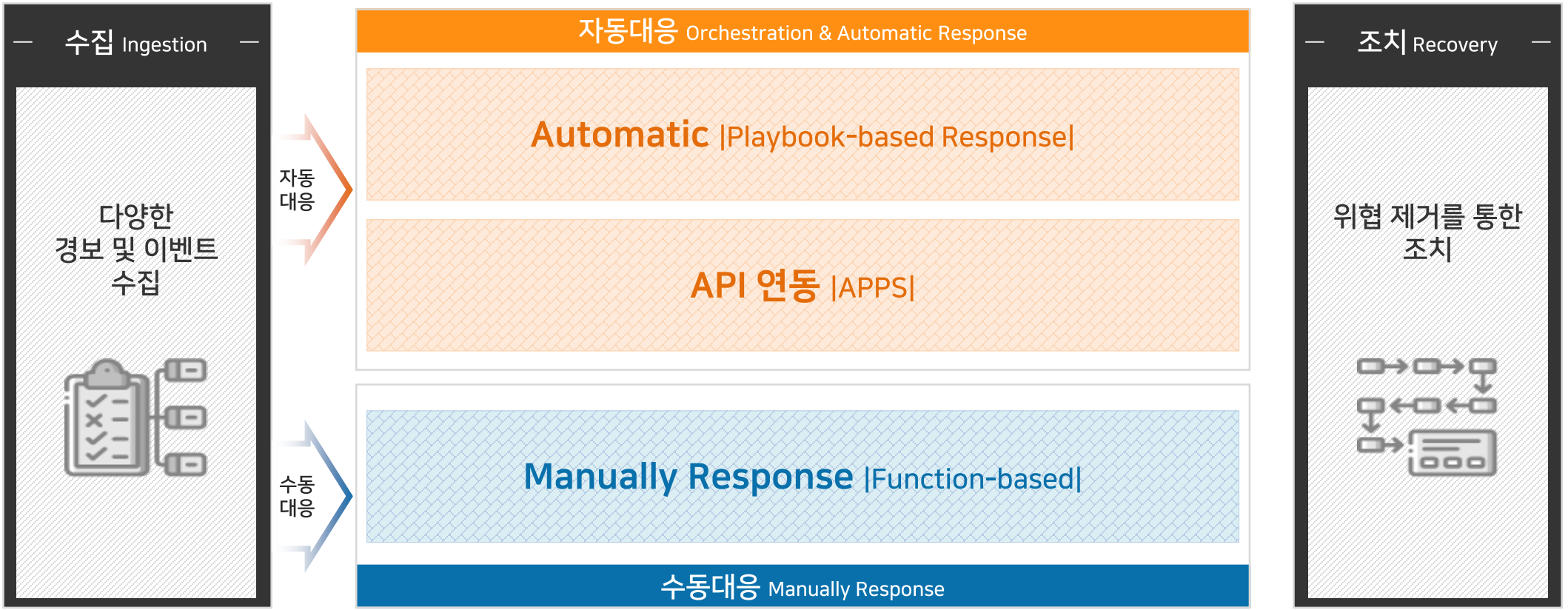
차세대보안관제
Zero Trust

- 머신러닝(AI) 기반 이상행위 탐지
- 위협정보 관제연동
  (TI, Threat Intelligence)
- SOAR 기반 자동화 대응

4세대

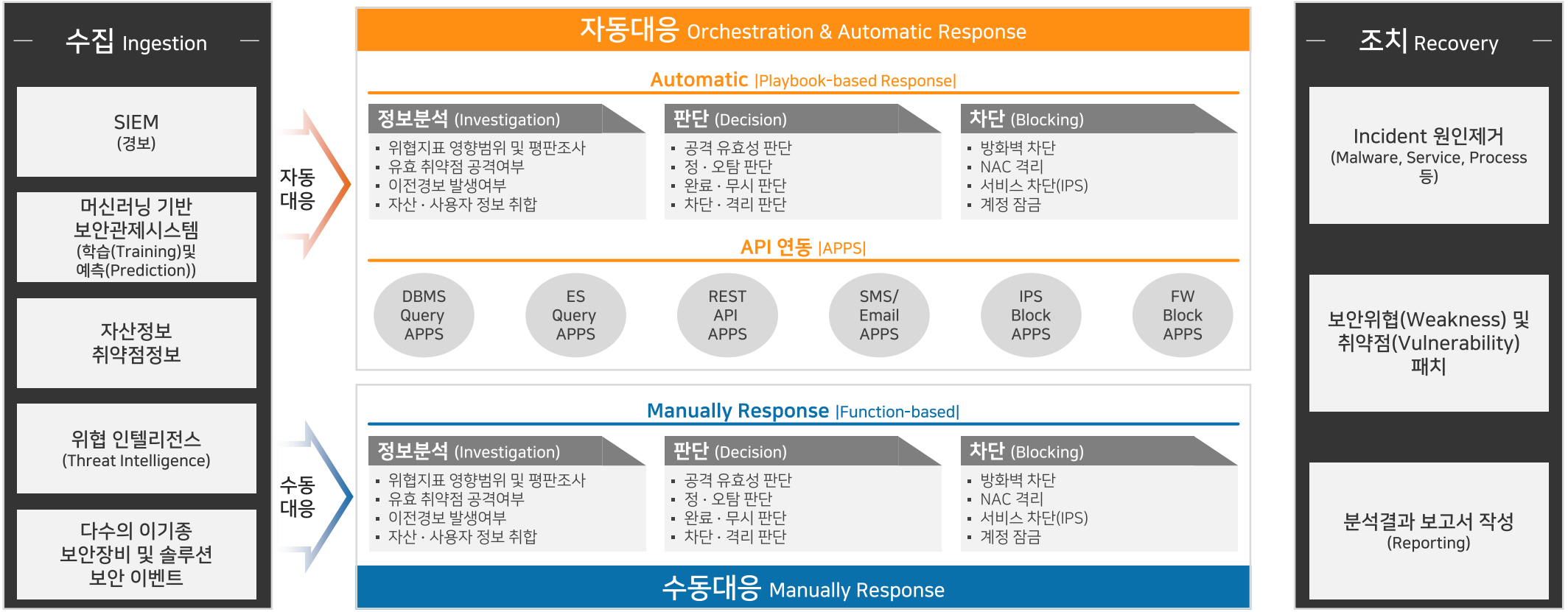
II. SOAR의 기능 (Security Orchestration, Automation and Response)

SOAR를 통한 대응 아키텍쳐



Ⅱ. SOAR의 기능 (Security Orchestration, Automation and Response)

SOAR를 통한 대응 아키텍쳐

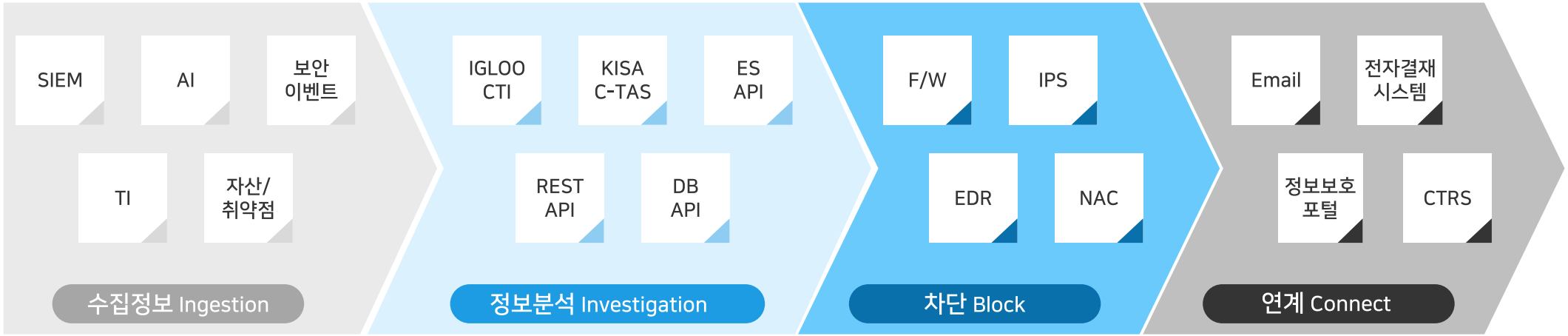


Ⅱ. SOAR의 기능 (Security Orchestration, Automation and Response)

SOAR 주요 기능 > Orchestration

01 이기종 보안솔루션 연동을 통한 보안관제 Orchestration 구현

- 이기종 보안솔루션 및 업무 시스템 연동
  (SIEM, 머신러닝기반 보안관제시스템, 위협인텔리전스(Threat Intelligence), 정보자산·취약점관리 시스템, API:APPs, 관제지원시스템 등)
- 수집정보(Ingestion), 정보분석(Investigation), 차단(Block) 연동을 통해 보안관제 환경에서 수집, 탐지 뿐 아니라 차단, 격리 조치까지의 일괄 수행을 통한 작업 효율성 향상



* 사이트 환경에 따라 상이할 수 있음

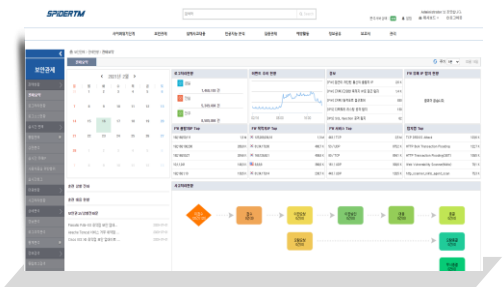
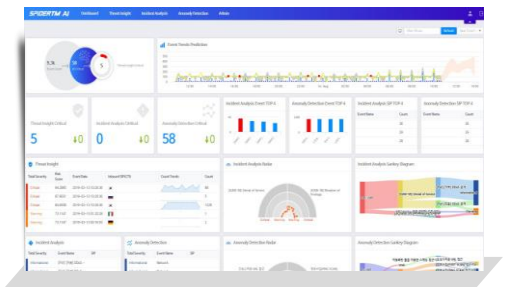
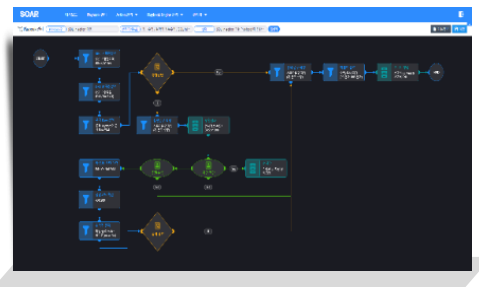
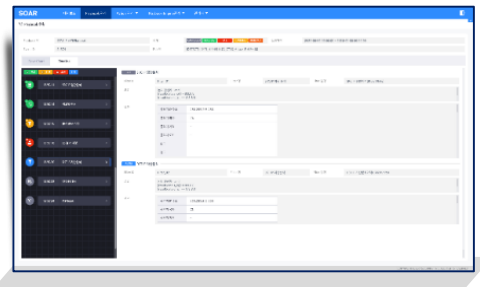
Ⅱ. SOAR의 기능 (Security Orchestration, Automation and Response)

SOAR 주요 기능 > Playbook

02 관제 노하우를 반영한 Playbook 기반 대응 프로세스

- Playbook은 탐지부터 대응까지 일련의 관제의 흐름을 담고 있으며, SOAR의 핵심 요소라 할 수 있음
- Playbook을 통한 단순 반복 업무의 최소화 및 보안관제 효율 증대
- 관제 노하우를 반영한 Playbook 적용이 필수
  (국내 보안관제센터 운영 노하우가 반영 된, 보안관제에 최적화 된 Playbook 보유 여부가 중요)

위협탐지 ▸▸ 위협분석 ▸▸ 플레이북 작성 및 적용 ▸▸ 대응결과

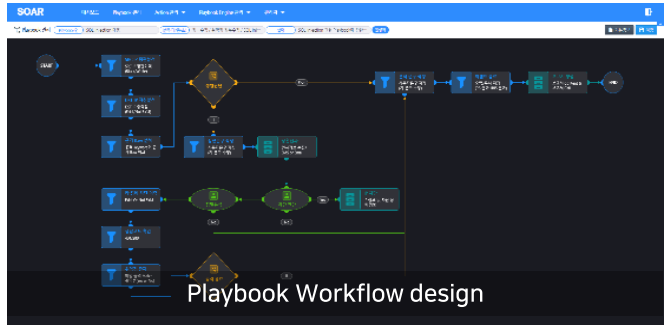





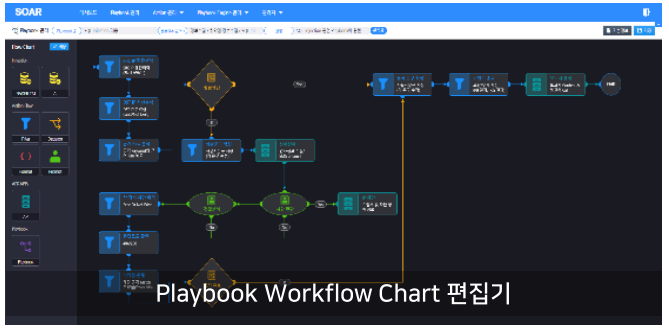
* 보안관제 노하우를 보유한 업체 또는 전문조직의 지속적인 Playbook 개발 및 지원 시 효율 극대화

Ⅱ. SOAR의 기능 (Security Orchestration, Automation and Response)

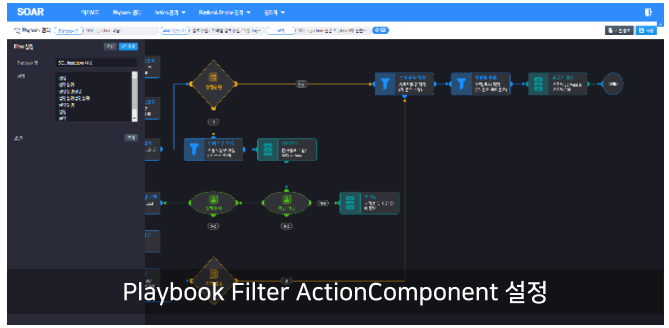
SOAR 주요 기능 > Playbook

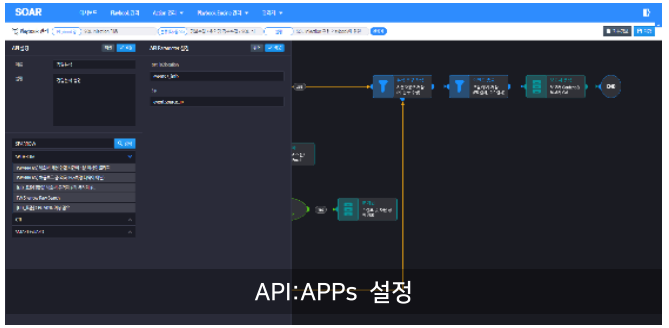
02 관제 노하우를 반영한 Playbook 기반 대응 프로세스

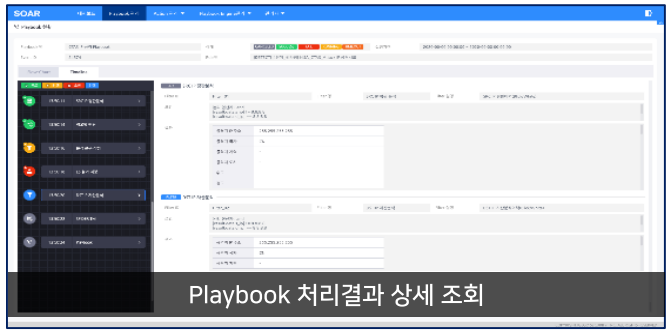

Playbook Workflow design


Playbook Workflow Chart 편집기


Playbook 상태 모니터링


Playbook Filter ActionComponent 설정


API:APPs 설정


Playbook 처리결과 상세 조회

Ⅱ. SOAR의 기능 (Security Orchestration, Automation and Response)

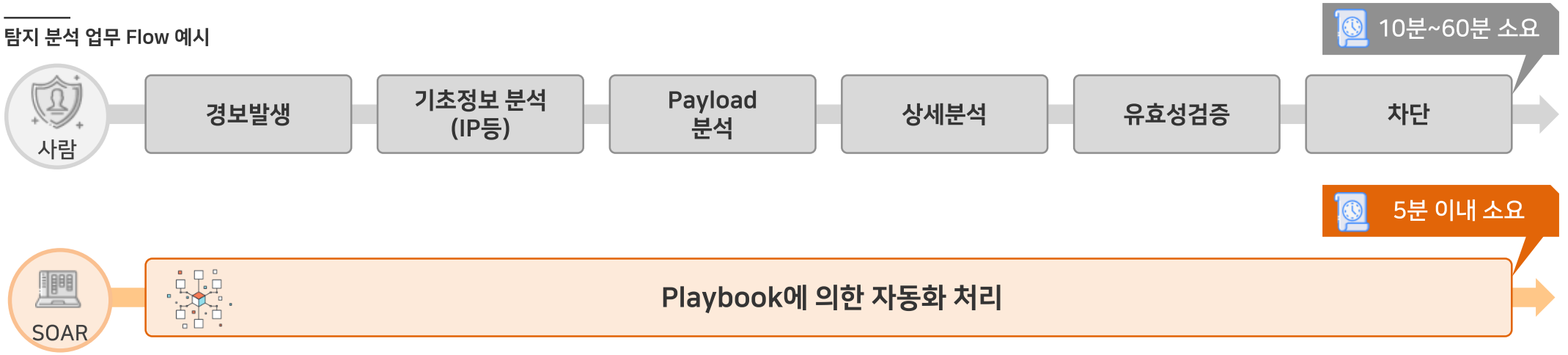
SOAR 주요 기능 > Automation and Response

03

차단 및 대응 프로세스 자동화를 통한
보안관제센터 대응 프로세스 효율 향상

- 단위 보안솔루션(F/W, IPS, NAC 등)과의 연동을 통한 자동 차단
  (국내 보안관제센터에서 운영 중인 다양한 차단 가능 솔루션과의 연동이 가능해야 함)
- 신속한 대응 및 분석을 위한 보안관제센터 프로세스의 Real-Time Alert Automatic Response
- 이벤트 분석 시, 수행하는 단순·반복적인 업무의 표준화·자동화를 통해 위협 대응 시간 최소화

탐지 분석 업무 Flow 예시



* 평균대응시간(MTTR, Mean Time To Response) 기준, 사이트에 따라 상이함

Ⅱ. SOAR의 기능 (Security Orchestration, Automation and Response)

SOAR 도입 기대효과

01 단순·반복 업무 자동화를 통한 관제업무 고도화

- 단순·반복 업무에 소요된 시간 단축을 통해 분석업무 등 고도화 된 관제업무를 위한 인력 투자 가능
- 다양한 솔루션 연동을 통한 통합적이고 유기적인 대응

02 사이버 위협 대응 품질 상향평준화

- 위협 대응 시간 최소화 및 신속한 의사 결정
- Playbook 기반의 표준화된 대응 체계를 통한 경보이벤트 선별 및 대응 즉각 수행

03 업무 프로세스 가시성 확보

- MTTR(Mean Time to Repair, 평균 복구 시간), MTTD(Mean Time to Diagnostic, 평균 진단 시간), ROI(Return on Investment, 업무생산성) 지표화 가능

기존의 보안관제

- 긴 시간 대응
- 불규칙적인 대응 품질
- 프로세스 가시성 부족
- 대부분의 인력이 단순 반복 업무에 투입

SOAR 기반 보안관제

- 대응시간 단축 및 신속한 의사 결정
- 대응 품질의 상향 평준화
- 프로세스 가시성 확보
- 사람 판단이 필요한 분석 업무 등의 전문업무 투입
- 수동 & 자동 실시간 관제 대응 가능
- MTTR, MTTD, ROI 지표화

AI Leader in Cyber Security
IGLOOSECURITY

III. SOAR 도입 시 고려사항

III. SOAR 도입 시 고려사항

SOAR 도입 시 고려사항 > 1) 제조사

01 국내 환경
- SOAR 제공 업체가 국내 보안관제센터 환경과 보안관제를 잘 알고 있는지?

02 노하우
- SOAR 제공 업체가 보안관제 서비스를 수행하며, 보안관제 노하우가 반영 된 Playbook을 제공하는지?

03 지원 체계
- SOAR 운영을 위한 Playbook 제공 등 지속적인 지원 서비스를 제공하는지?

III. SOAR 도입 시 고려사항

SOAR 도입 시 고려사항 > 2) 제품 기능

04 **연계**

- 국내 보안관제센터에서 운영 중인 다양한 보안 솔루션과의 연계를 통한 자동대응이 가능한지?

05 **편의성**

- 보안 분석 및 대응 자동화를 위한 자유로운 Playbook 커스터마이징 및 재사용 기능을 제공하는지?

06 **수동 대응**

- 자동 대응 기능 뿐만 아니라 필요 시 보안관제요원에 의한 수동 대응 기능을 동시에 제공하는지? (사고처리, Ticketing 등)

III. SOAR 도입 시 고려사항

SOAR 도입 시 고려사항 > 3) 도입 고객

07 전담 인원

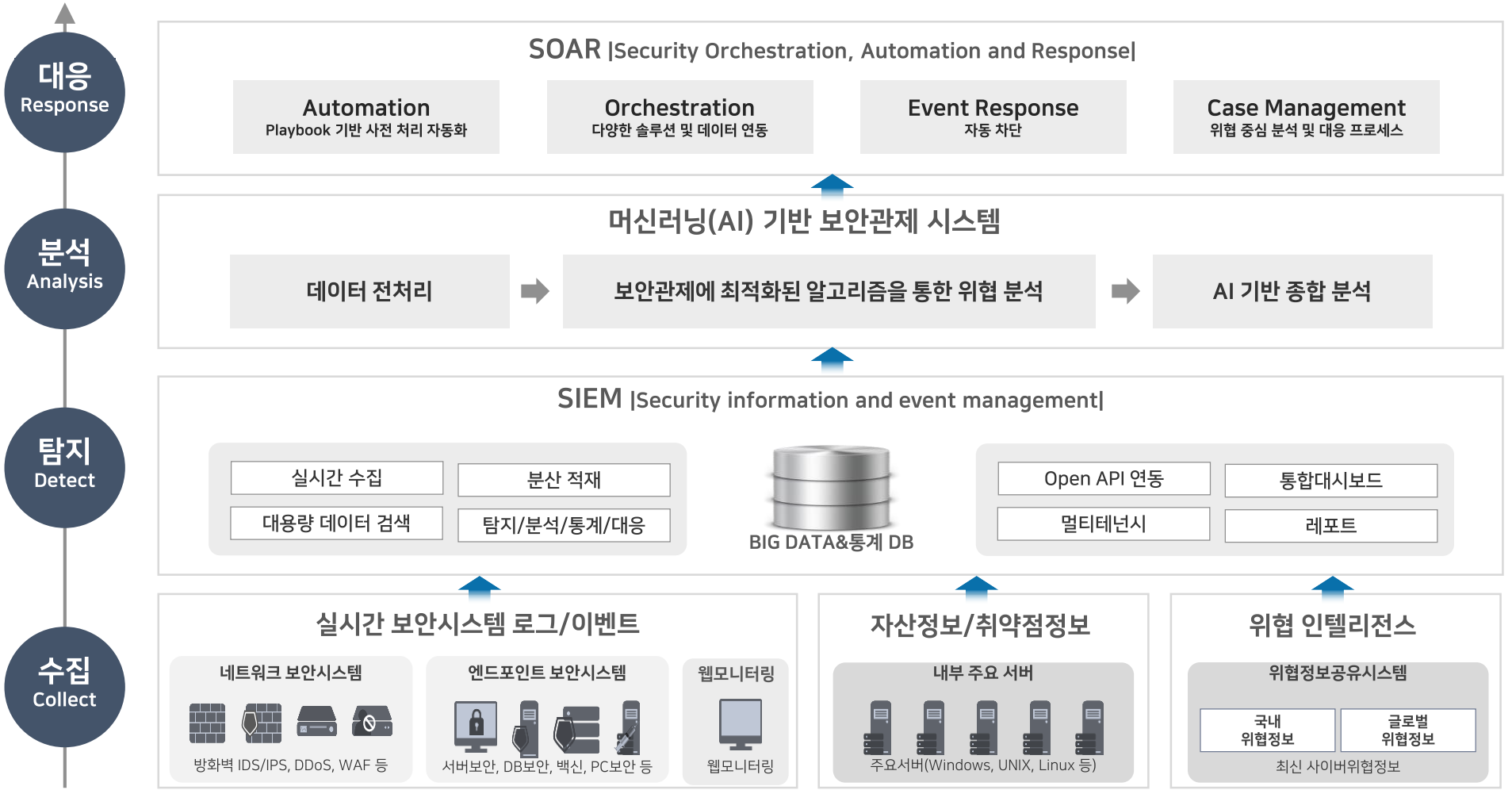
- SOAR 솔루션 도입 후 전담 인력을 배정하여,
  기존 관제 업무의 업무량 증가가 아닌, 관제 편의 증가 및 관제 품질 향상을 할 수 있도록 지원 가능한지?

08 업무 파악

- 보안 분석 및 대응 효율화가 가능한 범위 식별 및 반복적이며 시간이 다수 소요되는 업무가 파악 되어 있고, SOAR를 통해 이를 대응 할 수 있는지?

III. SOAR 도입 시 고려사항

SOAR는 만능이 아닙니다



THANK YOU

AI Leader in **Cyber Security**

IGLOOSECURITY