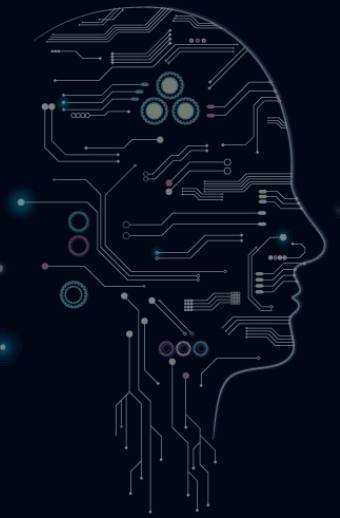
AI Leader in Cyber Security
IGLOOSECURITY

보안관제 기술
SIEM과 AI를 넘어 SOAR로



2021.12

이글루시큐리티 황범석 기술지원센터장

AI Leader in Cyber Security
IGLOOSECURITY

CONTENTS

AI Leader in Cyber Security
IGLOOSECURITY

Ⅰ. 보안관제 현황

Ⅰ. 보안관제 현황

보안관제는 무엇이고 어떠한 업무를 수행하는가

보안관제

保安管制, MSS(Managed Security Service)

1. 외부로부터의 침해시도를 예방하고 내부 정보자산을 보호하기 위해 자체 정보보호 조직 또는 전문적인 정보보안 업체를 통하여 효율적이고 효과적인 정보 보안 업무를 수행하는 것
2. 보안관제의 목적은 이기종에서 탐지되는 보안 이벤트를 수집하고 사이버 침해 공격에 대해 탐지/차단/대응 하여 사이버 침해를 사전에 예방하고 보안을 강화하는 것

24시간 265일 보안관제

- 보안 이벤트 모니터링
- 사이버 침해 대응/분석
- 홈페이지 위 · 변조 탐지 및 서비스 장애 관제
- 보안장비 운영/관리
- 보안정책 적용/관리
- 시스템 헬스 체크

사전 침해 예방

- 인트라 취약점 진단
- 모의해킹
- 최신 보안 동향 제공
- 소스코드 진단
- 보안실태 점검
- 보안 수준 진단
- 모의훈련 (악성메일 모의훈련)

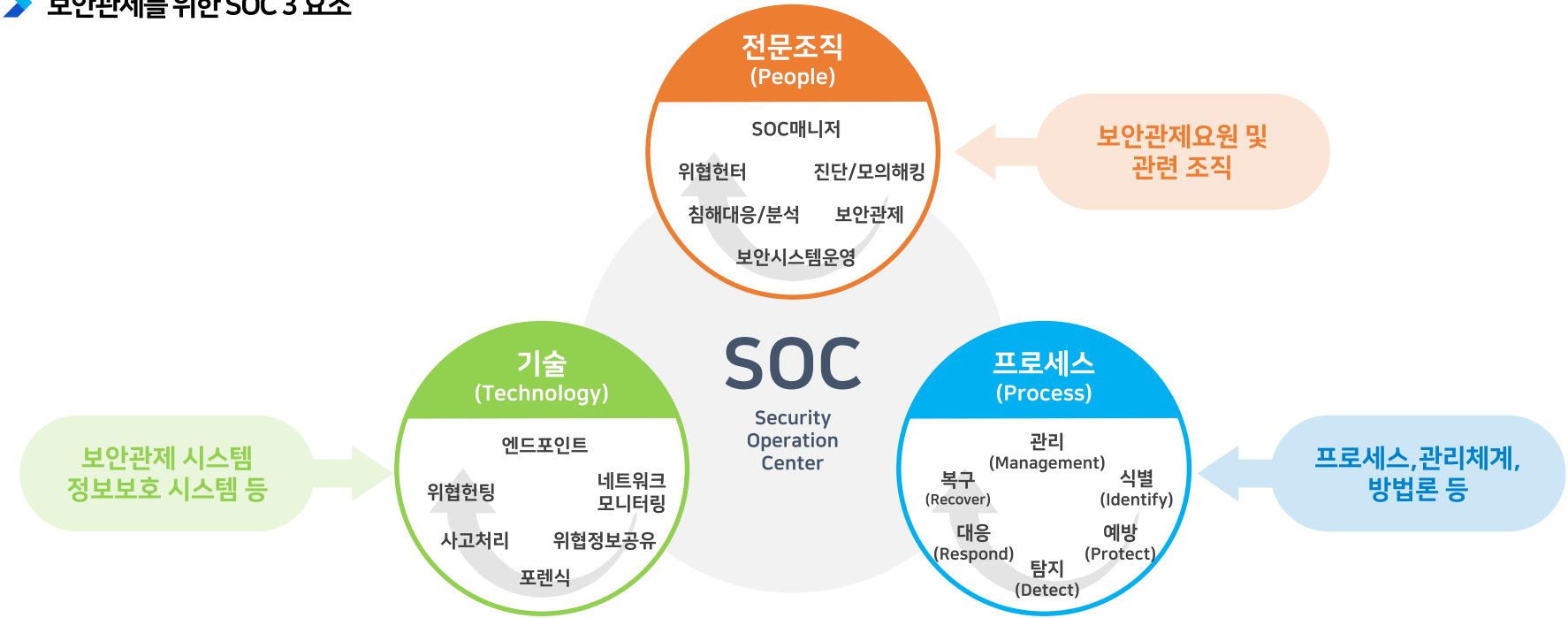
기타 정보보안 업무 지원

- 각종 인증 사전 준비 지원
- 지침/매뉴얼 개정 지원
- 정보보안 법적 대응 지원
- 보안 교육 수행

* 보안관제 업무, 이글루시큐리티

Ⅰ. 보안관제 현황

보안관제를 위한 SOC 3 요소



* Building a World-Class Security Operations Center: A Roadmap, SANS, 2015, 이글루시큐리티 재구성

Ⅰ. 보안관제 현황

보안관제 세대 별 변화

단위보안관제

Perimeter Security

- 단위 보안 솔루션 모니터링
  (FW, IDS, etc.)

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

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

4세대

Ⅰ. 보안관제 현황

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

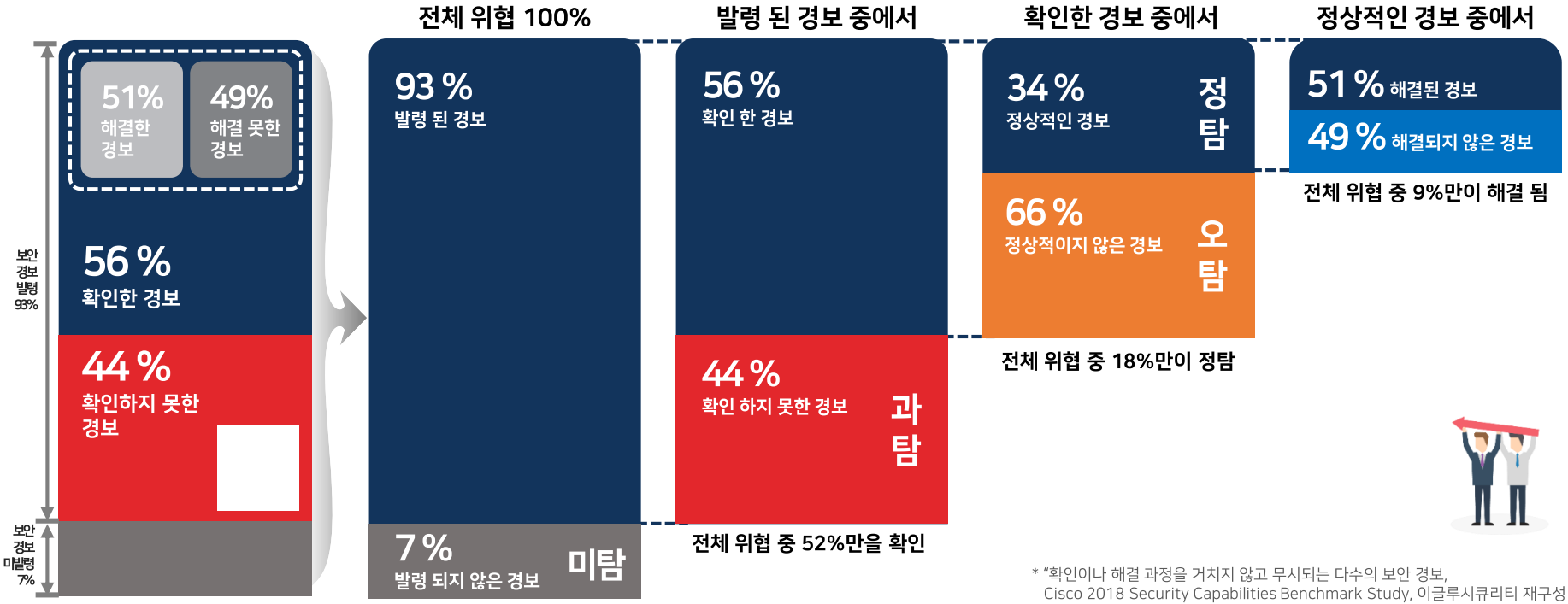
- IT 인프라 복잡성 증가에 따른 공격요인 증가
- 대응해야 하는 컴플라이언스의 증가
- 보안 예산 부족으로 인한 보안 담당 인력 부족

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

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

보안관제의 자동화 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

보안관제의 자동화 필요성 대두

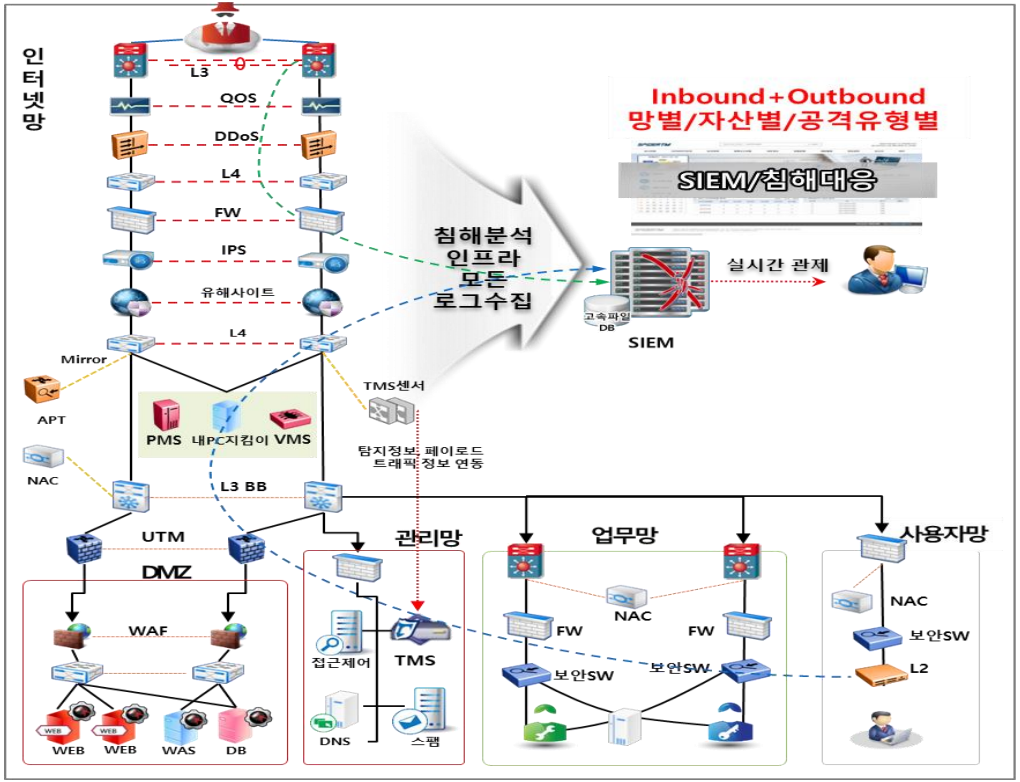
AI Leader in Cyber Security
IGLOOSECURITY

II. 빅데이터 SIEM과 AI를 통한 관제 업무 프로세스

Ⅱ. 빅데이터 SIEM과 AI를 통한 관제 업무 프로세스

Ⅱ. 빅데이터 SIEM과 AI를 통한 관제 업무 프로세스

빅데이터 SIEM 어떤 공격을 탐지/분석 할 것인가



탐지 및 로그 분석 방법

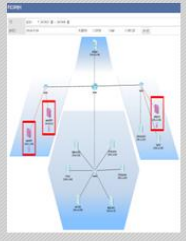
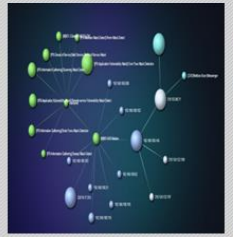
- 외부->내부 침해 공격 대응
  - 네트워크 보안장비와 웹서버 중심으로 실시간 모니터링 및 탐지
- DDoS
  - 주요장비 : DDoS + L4 + FW + IPS + TMS + WEB서버
  - 분석로그 : 탐지로그 + BPS, PPS + 자원현황 + Access log
- 웹해킹
  - 주요장비 : TMS + IPS + WAF + WEB서버 + 웹쉘 + FW
  - 분석로그 : 탐지로그(페이로드) + Access log + 웹쉘 파일무결성
- 악성코드(랜섬웨어) 감염
  - 주요장비 : 스팸 + APT + TMS +VMS + DNS + FW + IPS + 유해사이트 + NAC + 보안스위치 + PMS
  - 분석로그 : APT공격 매일 + 파일다운로드 + 탐지로그 + IP인증 + ARP Poisoning + Scan + 감염 여부 + 내부->외부 트래픽
- 내부 정보유출 & 비인가 접근 공격
  - 주요장비 : 접근제어+NAC+IPS+Server+FW +DB보안+DRM&DLP
  - 분석로그 : 감사 로그 + SecureLog,wtmp + 정책로그 + 탐지로그 Scan + BlueForce + IP인증 + ARP Poisoning
- 정책 감사(&비인가 접근)
  - 주요장비 : 접근제어 + DB보안 + FW + NAC.....
  - 분석로그 : 로그인 정보 및 정책 변경 감사 로그 수집

Ⅱ. 빅데이터 SIEM과 AI를 통한 관제 업무 프로세스

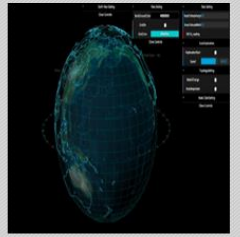
빅데이터/AI를 통한 알려진/알려지지 않은 공격 통합보안관제 프로세스

예방 ▶ 탐지 ▶ 분석 ▶ 검증 ▶ 예측 ▶ 침해사고대응

1단계	2단계	3단계	4단계	5단계	6단계	7단계
위협정보 (TI)	경보 (Alert)	1차분석 (빅데이터)	Payload 분석 (Packet분석)	검증 (바이러스, 가상화분석)	의사결정 /기계학습 (AI)	침해사고 대응





AI Leader in Cyber Security
IGLOOSECURITY

III. 보안관제 대응 자동화 전략

III. 보안관제 대응 자동화 전략

보안관제를 위한 다양한 솔루션

단위 보안시스템

이기종 보안로그

SIEM

실시간
위협 탐지

SOAR

자동 분석
및 대응

보안관제센터

보안관제

관제요원

CTI(위협 인텔리전스)

글로벌 위협
최신 정보

인공지능(AI)

정/오탐
자동 판단

대시보드/리포트

가시성 확보
대응현황 보고

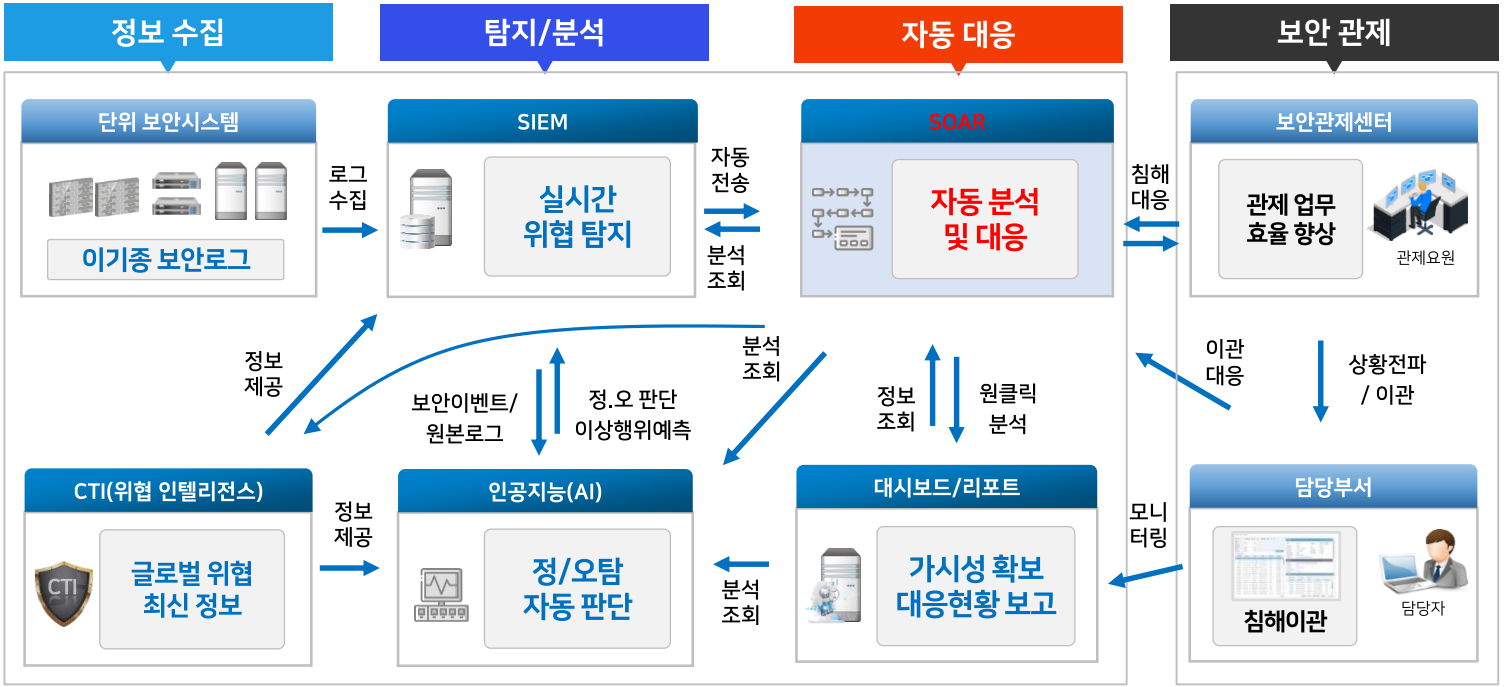
담당부서

침해이관

담당자

III. 보안관제 대응 자동화 전략

보안관제솔루션의 유기적 연계를 통한 보안관제 대응 자동화

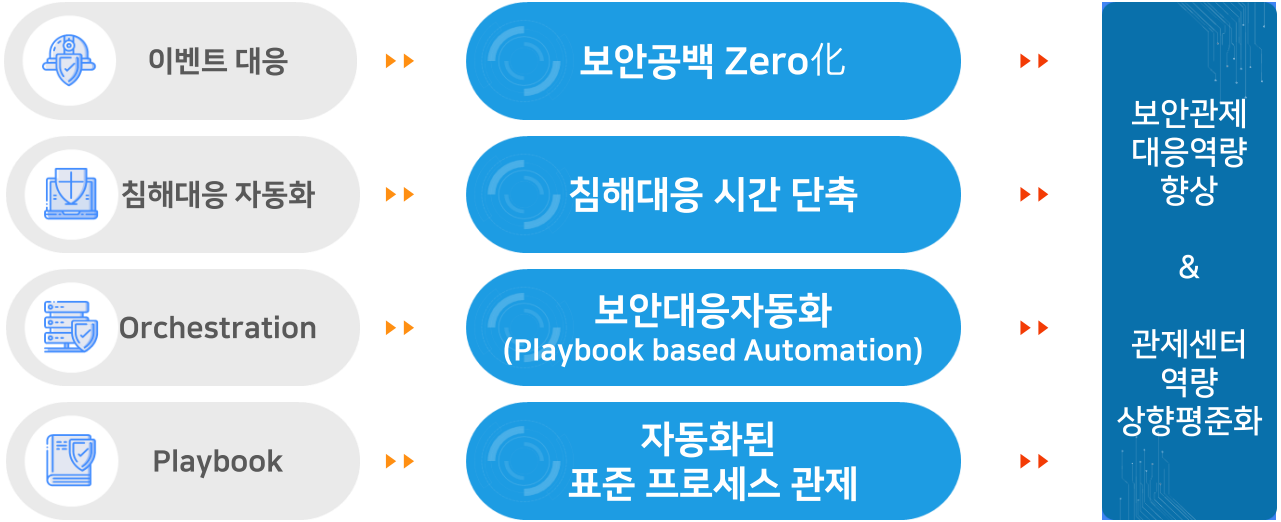


Ⅲ. 보안관제 대응 자동화 전략

보안관제 대응 자동화를 통한 기대효과

보안관제 대응 자동화 기대 효과

- 기존 보안관제 업무 진행 체계 개선을 통한 보안관제 대응역량 향상
  : 긴 시간 대응, 불규칙적인 대응 품질, 프로세스 가시성 부족, 단순 반복 작업
- 보안관제 대응 자동화 업무 프로세스 도입으로 관제센터 역량 상향 평준화
  : 보안관제 및 분석 품질의 상향 평준화, 프로세스 가시성 확보, 보안관제 전문인력 재편성(모니터링 → 상세분석)



Ⅲ. 보안관제 대응 자동화 전략

보안관제 대응 자동화를 통한 기대효과

보안관제 대응 자동화 기대 효과

- 기존 보안관제 업무 진행 체계 개선을 통한 보안관제 대응역량 향상
  : 긴 시간 대응, 불규칙적인 대응 품질, 프로세스 가시성 부족, 단순 반복 작업
- 보안관제 대응 자동화 업무 프로세스 도입으로 관제센터 역량 상향 평준화
  : 보안관제 및 분석 품질의 상향 평준화, 프로세스 가시성 확보, 보안관제 전문인력 재편성(모니터링 → 상세분석)

탐지 분석 업무 Flow 예시

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

AI Leader in Cyber Security
IGLOOSECURITY

IV. 보안관제 대응자동화의 핵심 SOAR

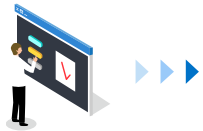
(Security Orchestration, Automation and Response)

Ⅳ. 보안관제 대응 자동화의 핵심 SOAR (Security Orchestration, Automation and Response)

XDR 개념

XDR

XDR(eXtended Detection & Response)



- EDR(Endpoint Detection and Response) 또는 SIEM 관련 기업에서 처음 언급하였으나, Gartner에서 정의 및 언급을 하면서 새로운 보안 플랫폼으로 자리 잡기 시작
- XDR의 X(Extended)의 의미를 자사 솔루션과 연계하여 업체마다의 홍보의 수단으로 활용

* EDR의 확장, SIEM의 확장, etc..

* XDR: Enterprise-Scale Detection and Response(Coretex)

Ⅳ. 보안관제 대응 자동화의 핵심 SOAR (Security Orchestration, Automation and Response)

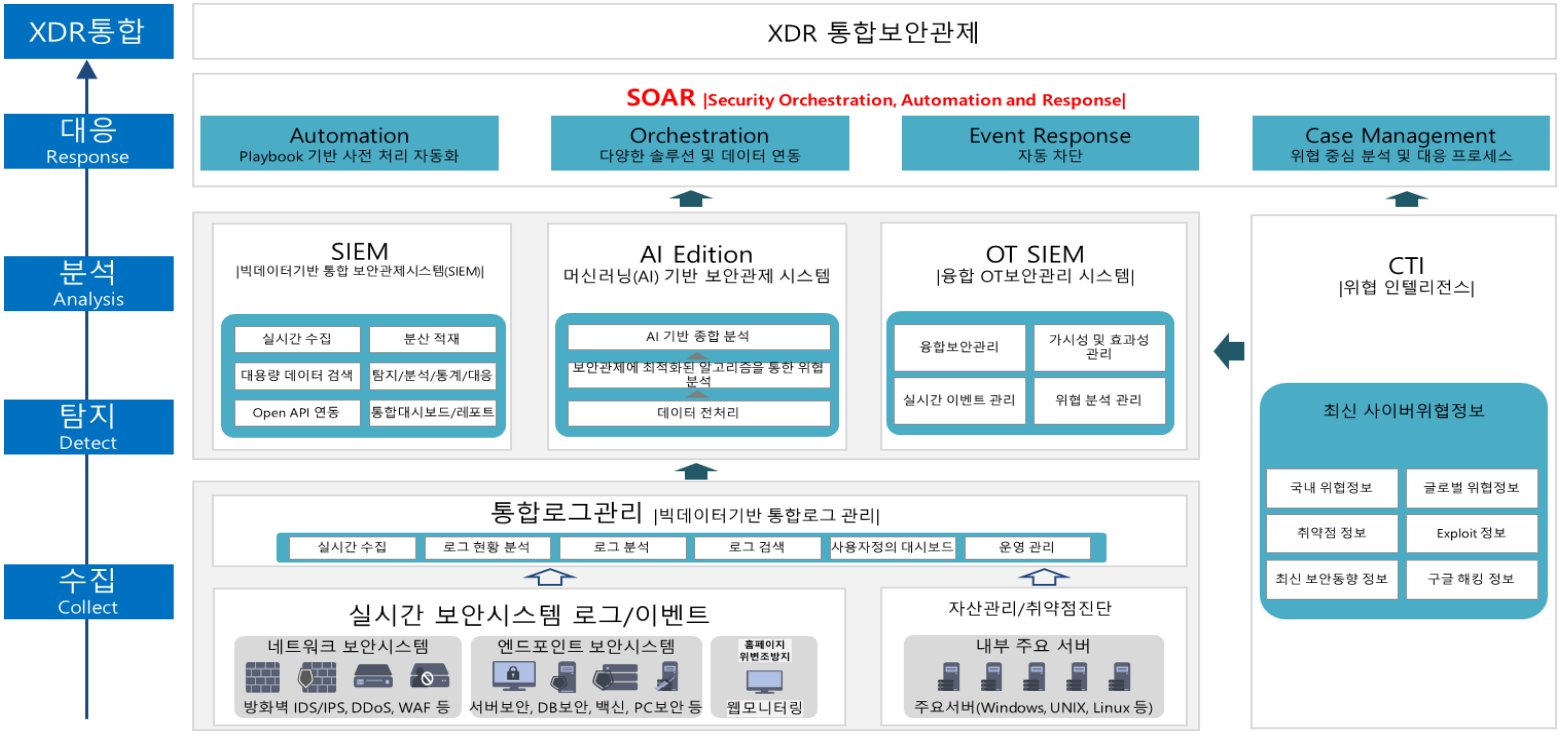
XDR을 통한 통합보안관제 확장 개념

XDR 통합보안관제

- **탐지 및 대응 확장 (Extended Detection, Analysis and Response)**
  - SOAR를 통해 Playbook 기반의 자동 대응 구현
  - 머신러닝(AI) 기반 탐지 및 분석을 통해 지능형 분석을 수행
- **위협 인텔리전스 확장 (Extended Information & Intelligence)**
  - 위협인텔리전스(Cyber Threat Intelligence) 수집을 통한 위협 정보 공유 및 활용
  - 자산정보 및 취약점정보 수집을 통한 분석 활용
- **Collection 확장 (Extended Collection Target)**
  - NDR, Endpoint(EDR) 이벤트 수집을 통해 분석을 위한 기초 데이터 확보
- **보안관제 영역 확장 (Extended Managed Security Spectrum)**
  - 보안관제 대상을 외부 위협 뿐만 아니라 내부 위협영역까지 확장

Ⅳ. 보안관제 대응 자동화의 핵심 SOAR (Security Orchestration, Automation and Response)

XDR 통합보안관제시스템 아키텍쳐



Ⅳ. 보안관제 대응 자동화의 핵심 SOAR (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
(XDR 통합보안관제의 핵심)

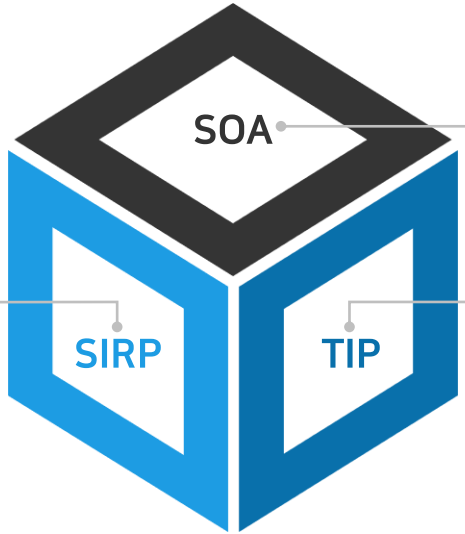
* SOAR 정의, Gartner(2018)

Ⅳ. 보안관제 대응 자동화의 핵심 SOAR (Security Orchestration, Automation and Response)

SOAR 구성

SOAR 구성

- 다양한 사이버 위협에 대해, 대응 수준을 자동(Automation) 으로 분류하고, 업무 표준화
- 프로세스에 따라 보안 업무 담당자와 솔루션이 유기적으로 협력(Orchestration)할 수 있도록 지원하는 플랫폼(Platform) (‘Gartner)



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

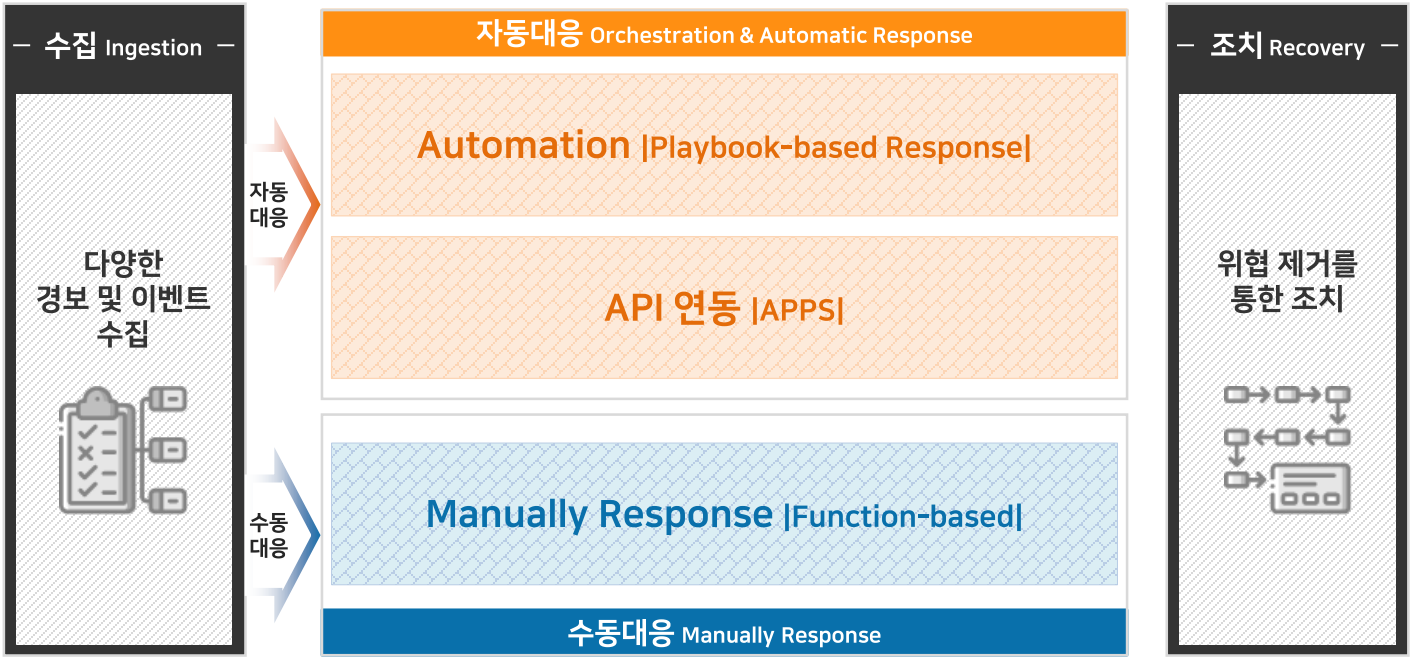
- 보안사고 대응 플랫폼
- 대응 프로세스 표준화
- 인력 간 역량 격차 축소
- 전문 인력 부족 문제 해결

TIP Threat Intelligence Platforms, 위협 인텔리전스 플랫폼

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

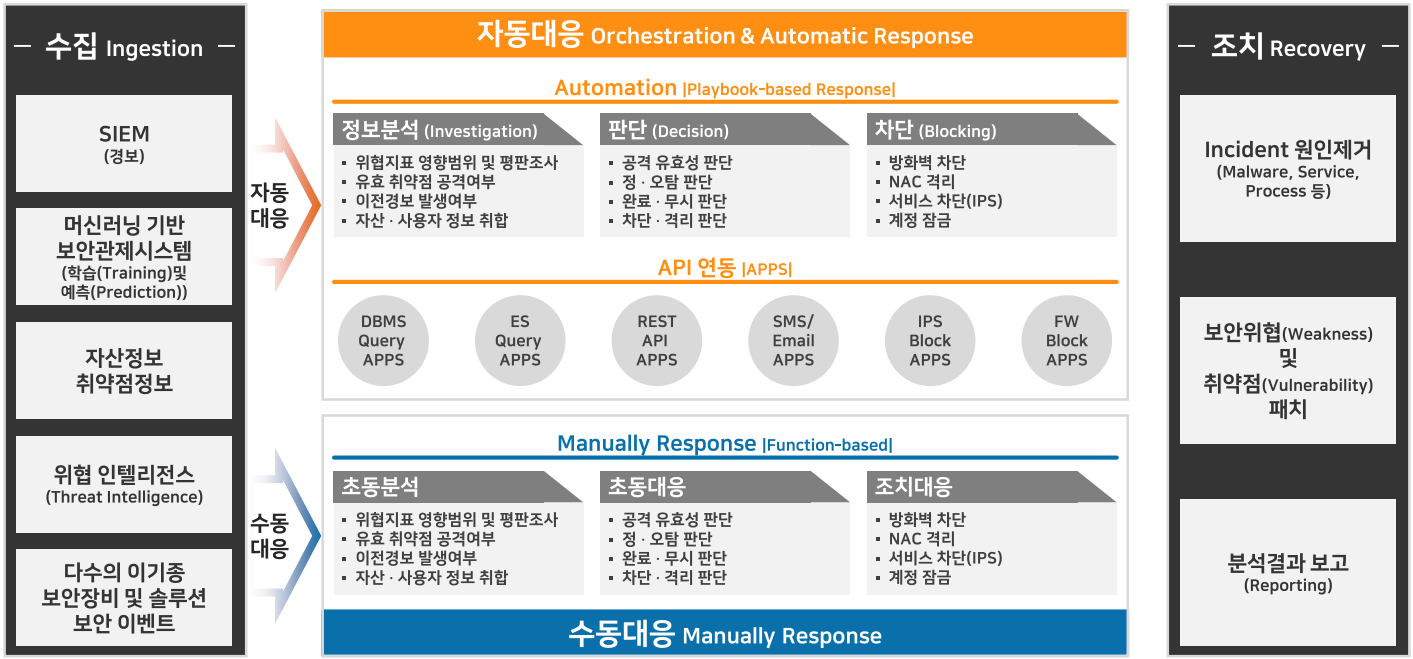
Ⅳ. 보안관제 대응 자동화의 핵심 SOAR (Security Orchestration, Automation and Response)

SOAR 서비스 개념



Ⅳ. 보안관제 대응 자동화의 핵심 SOAR (Security Orchestration, Automation and Response)

SOAR 서비스 개념



Ⅳ. 보안관제 대응 자동화의 핵심 SOAR (Security Orchestration, Automation and Response)

SOAR 기능 구성

DASHBOARD	CASE 선별	INCIDENT 대응	PLAYBOOK 관리	보안관리
SOAR 침해대응 전체 현황	자동대응 효율 위한 CASE 선별/ 그룹 누적 및 Playbook 매핑	화면기반 수동 Incident 대응 및 자동/수동 결과조회	Playbook 및 API Service 등록/수정/삭제	시스템 설정 및 보안업무 지원 기능 관리
Visualization	Automatic Ticket	Automation Response	Orchestration & Creation	Security Support

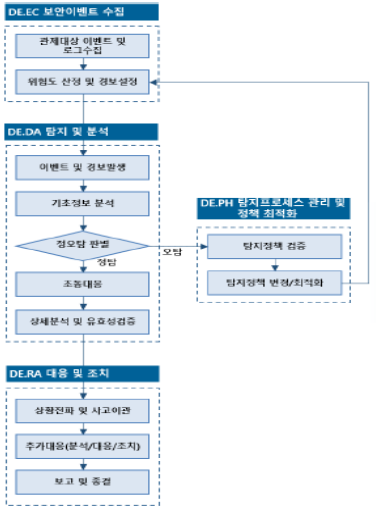
Ⅳ. 보안관제 대응 자동화의 핵심 SOAR (Security Orchestration, Automation and Response)

Playbook 개념

PLAYBOOK(플레이북) 이란

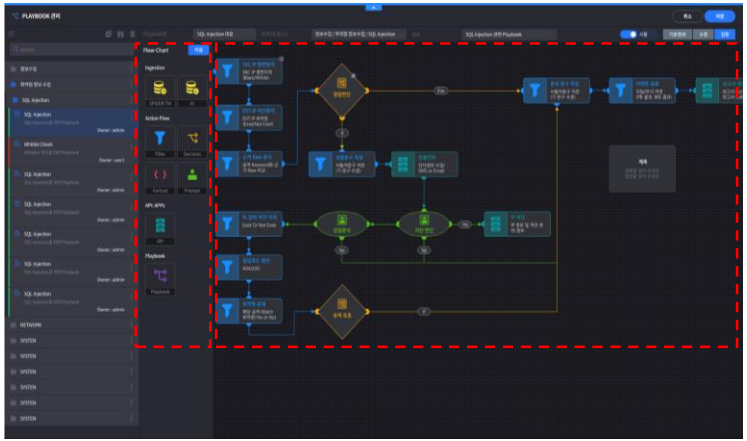
공격 유형별 대응 방안을 표준화된 업무프로세스로 사전에 정의한 자동대응 매뉴얼

관제 대응 프로세스(예시)



자동화

Playbook 기반 자동대응(예시)



Ⅳ. 보안관제 대응 자동화의 핵심 SOAR (Security Orchestration, Automation and Response)

Playbook을 통한 자동대응 예시 > 정오탐 판단을 위한 공격 IP 속성 자동 분석

활용

IPS Payload 필드에 대해 AI 정탐 판단된 공격IP 속성 분석, Anomaly, Scan등 단순 접근 및 비인가 접근 IP 속성 분석

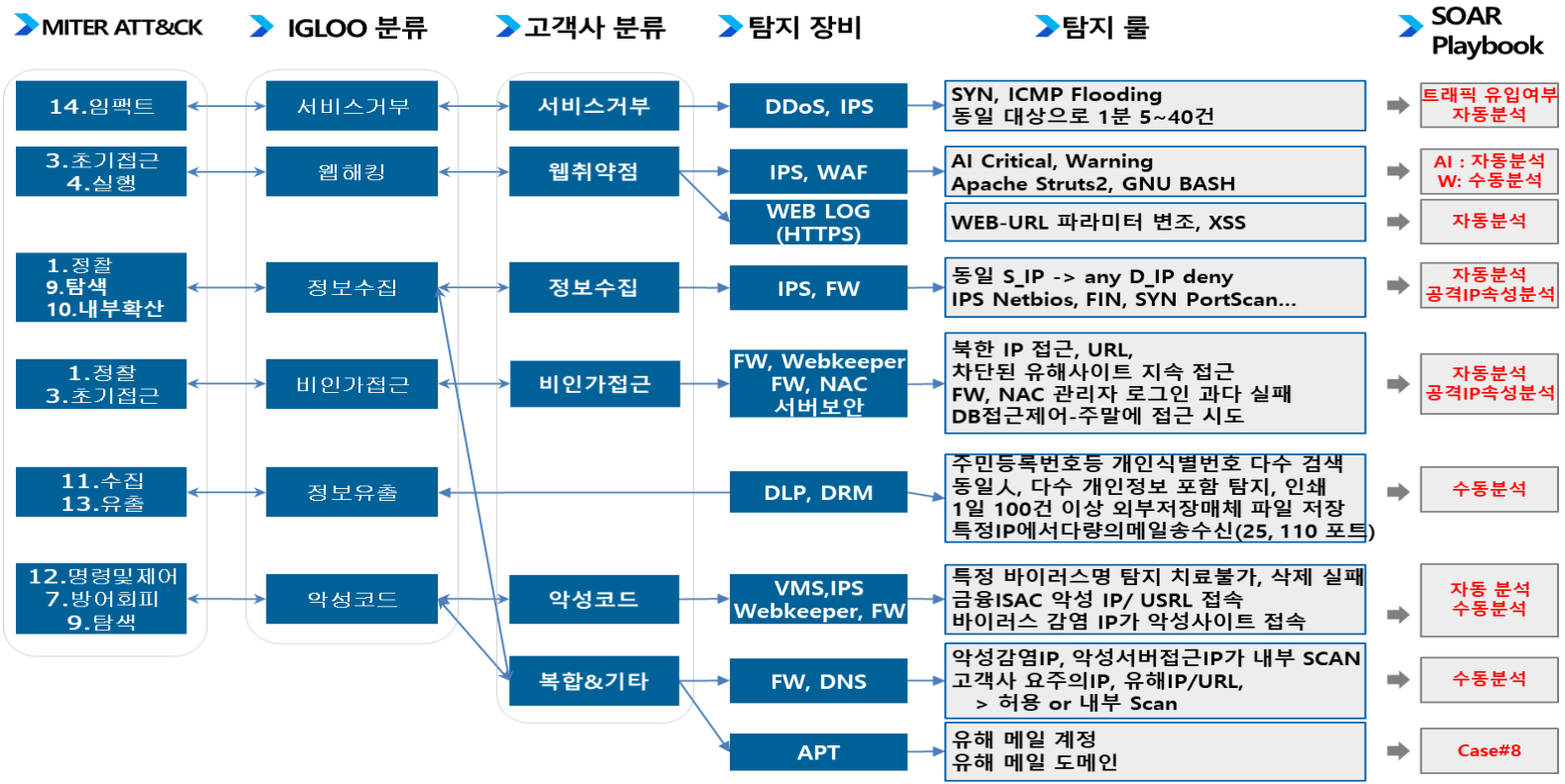
분석 API

국내외 판단, 유해IP 판단, 과거 공격이력 판단, 목적지IP 자산여부 판단

대응 API

공격IP 구간별 방화벽등 보안장비에서 자동 차단

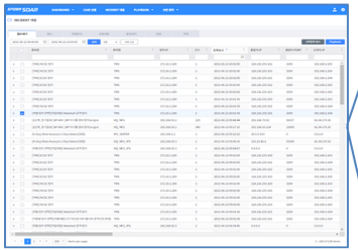
Ⅳ. 보안관제 대응 자동화의 핵심 SOAR (Security Orchestration, Automation and Response)

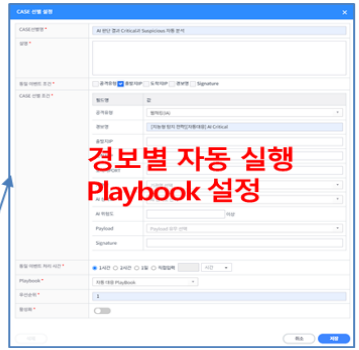


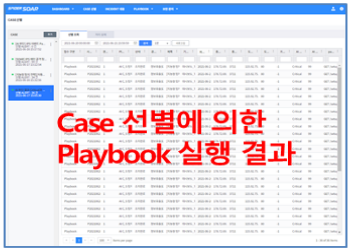
Ⅳ. 보안관제 대응 자동화의 핵심 SOAR (Security Orchestration, Automation and Response)

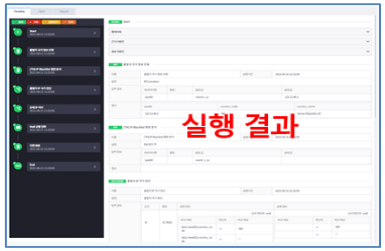
Case 선별에 의한 Playbook 자동 실행

Incident 접수 리스트

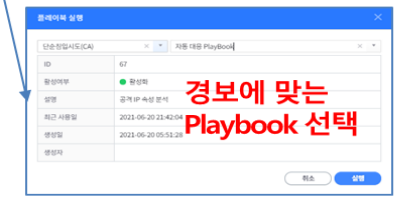


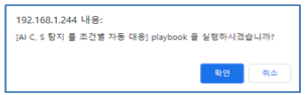


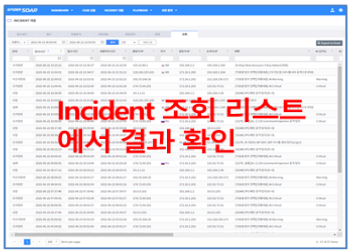


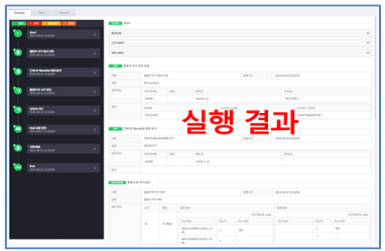


Playbook 수동으로 경보 처리하기



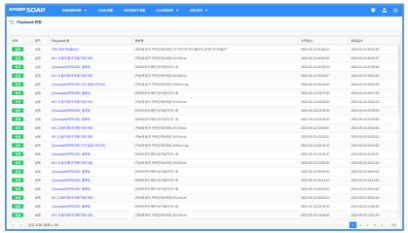




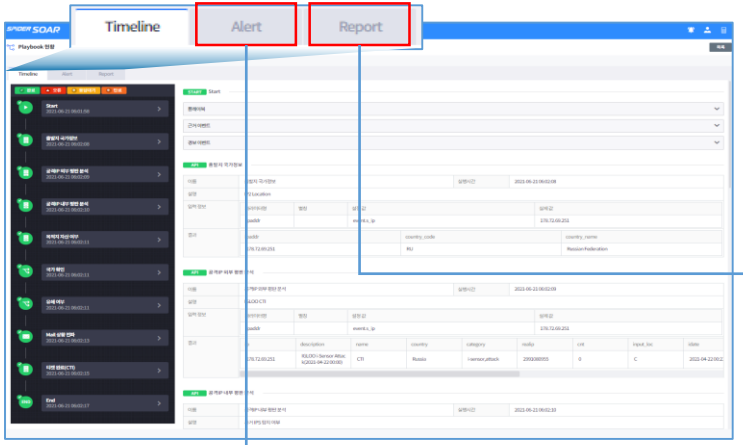


Ⅳ. 보안관제 대응 자동화의 핵심 SOAR (Security Orchestration, Automation and Response)

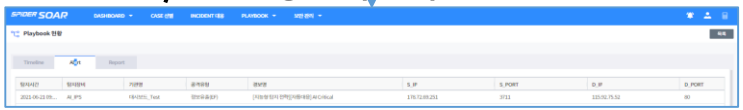
* Playbook 실행 목록에서 선택



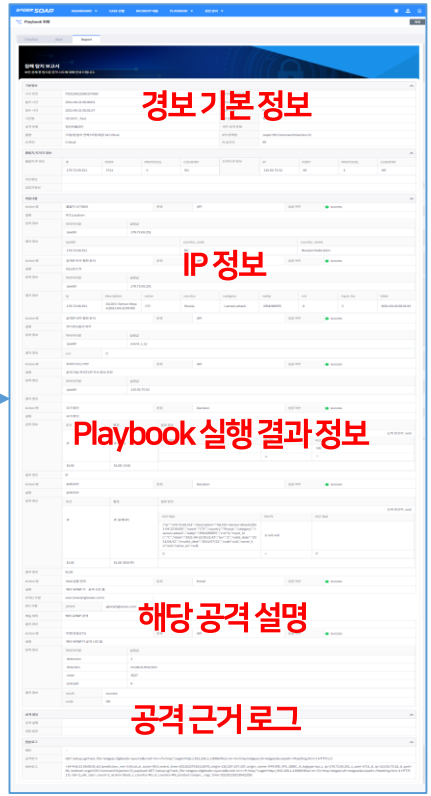
* Playbook 실행 결과(TimeLine)



* Playbook 실행 결과(Alert)

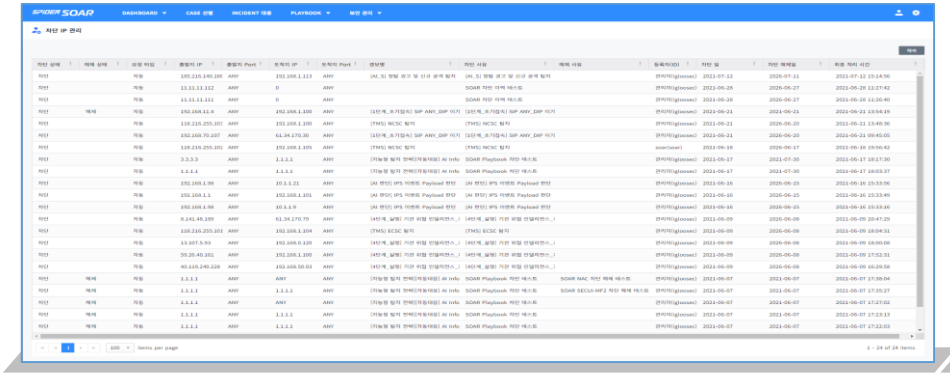


* 분석 보고서 (Report)

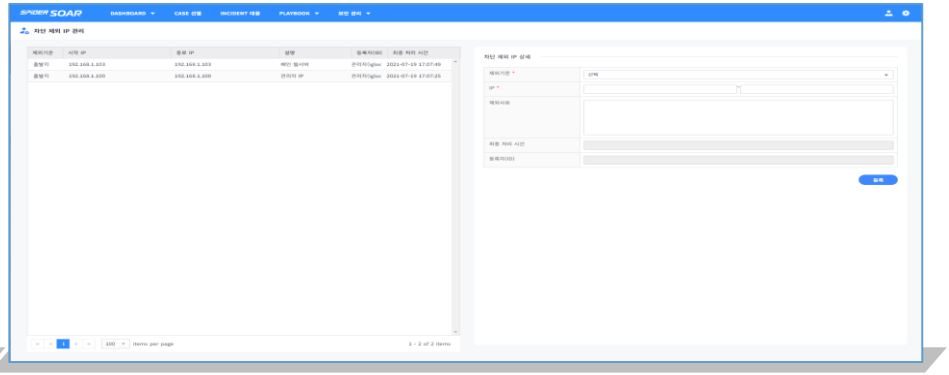


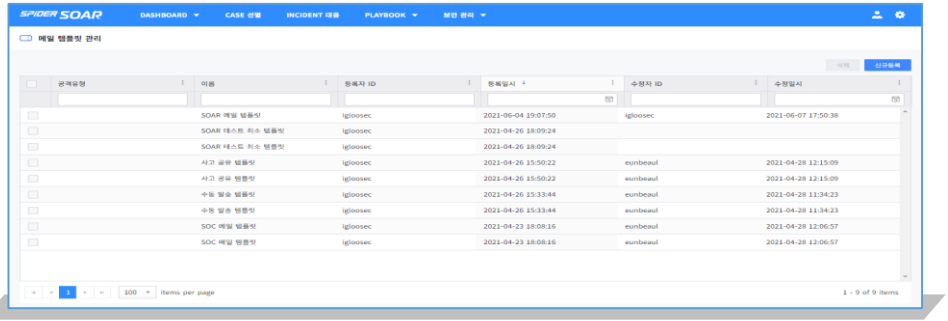
Ⅳ. 보안관제 대응 자동화의 핵심 SOAR (Security Orchestration, Automation and Response)

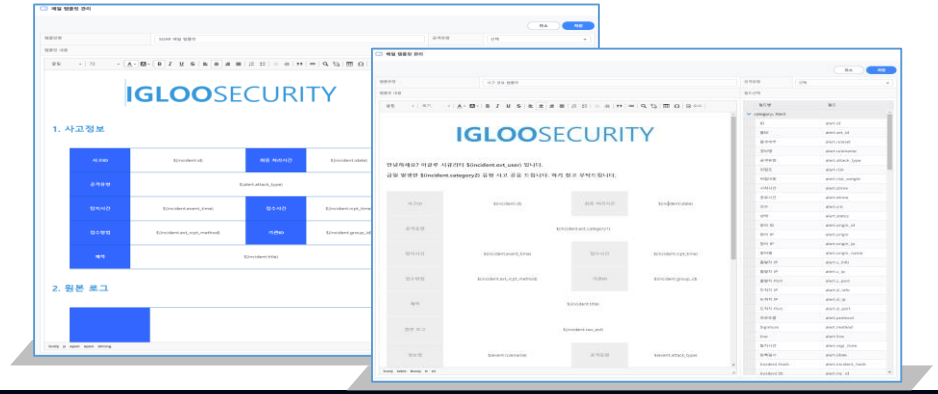
차단 IP 관리 : 자동 차단된 IP 리스트 > 즉시 해제



차단 제외 IP 관리 : 휴먼 장애 관리







AI Leader in Cyber Security
IGLOOSECURITY

V. SOAR 도입 시 고려사항

V. SOAR 도입 시 고려사항

SOAR 도입 시 고려사항

01 국내 환경
- 국내 보안관제센터 환경과 보안관제를 가장 잘 아는 업체가 제공하는 SOAR 솔루션인지?

02 노하우
- 보안관제를 경험해 본 업체만이 제공할 수 있는 보안관제 노하우가 반영 된 Playbook을 제공하는지?

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

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

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

06 효율화
- 효율적인 관제업무를 위한 Incident Management, Case Management, 수동 대응 기능을 모두 제공하는지?

07 품질 향상
- SOAR 솔루션 도입 후 기존 관제 업무의 업무량 증가가 아닌, 관제 편의 증가 및 관제 품질 향상이 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?

THANK YOU

AI Leader in **Cyber Security**