IGLOO

S.O.A.R 활용의 핵심!!

PlayBook에서 찾다!

이글루코퍼레이션 손보형

IGLOO

Contents.

Cyber Attack Response Problem

[IGLOO I²SOC Monthly Event Statistics]

Limitations of Cyber Attack Response

| 01 | 증가하는 보안위협

| 02 | 고도화 되는 해킹기술

| 03 | 공격대응의 한계

증가하는 보안위협

- IT 발달에 따른 공격 POINT 증가로 대응 수준 가능 범위 한계
- 기존 공격도 지속적으로 증가하고 있지만, 신규 공격까지 추가로 발생

고도화 되는 해킹기술

- 신기술에 발달에 따른 보안위협 증가
- 공격기술의 고도화/지능화, 사회공학기법 등 및 복합 공격 형태 발생

공격대응의 한계

- 사이버 침해 대응을 위한 높은 기술의 전문인력 부족화
- 대량의 공격 이벤트 처리에 대한 인당 처리량의 한계점
- 신규로 발생 되는 공격 기법에 대해 분석하는 인력으로의 대체 필요

보안관제 공격 분석 방법 – 수동 분석

공격 이벤트에 대한 보안관제 방법

탐지 공격명을 **확인**하고 **RAW Data문자열**을 통해
분석하여 공격 여부를 판단

CTI를 통한 위협지표 평판 조사를 통해
공격성 여부를 판단

과거 공격 이력 및 **최근 공격**
(타 고객사 및 기관에 대한 공격) 이력에 대한 판단

방화벽을 통한 주요 서비스 포트로의
비정상 접근 시도 및 **순식간에 다량 공격 발생 탐지**

고객사 연관 이벤트인지 확인 절차
- 고객사 업무적으로 연관되어 있는 통신인지 여부 확인

S.O.A.R

IGLOO

It is a platform that automatically classifies the level of response to various cyber threats and supports organic cooperation between security personnel and solutions according to standardized work processes. It introduces an automated process to overcome the limitations of attack response, thereby improving attack response. Upgrades efficiency to the next level.

SOA
(Security Orchestration Automaiton)

- 이기종 솔루션과의 연계를 통해 보안 운영 자동화
- 즉각적인 대응으로 공격 피해 최소화 및 신속한 인지 가능

SIRP
(Security Incident Response Platforms)

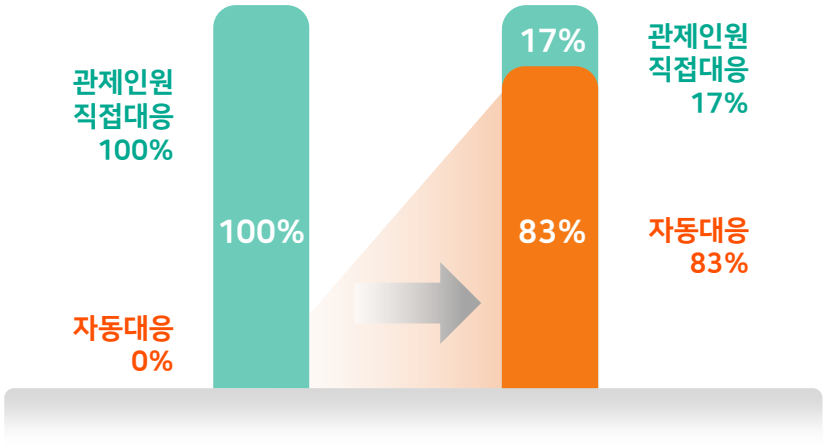
- 침해사고 대응 프로세스의 자동화 정립
- 침해사고 발생 시 각 담당에 대한 대응을 표준화 하여 신속한 대응 가능

TIP
(Threat Intelligence Platforms)

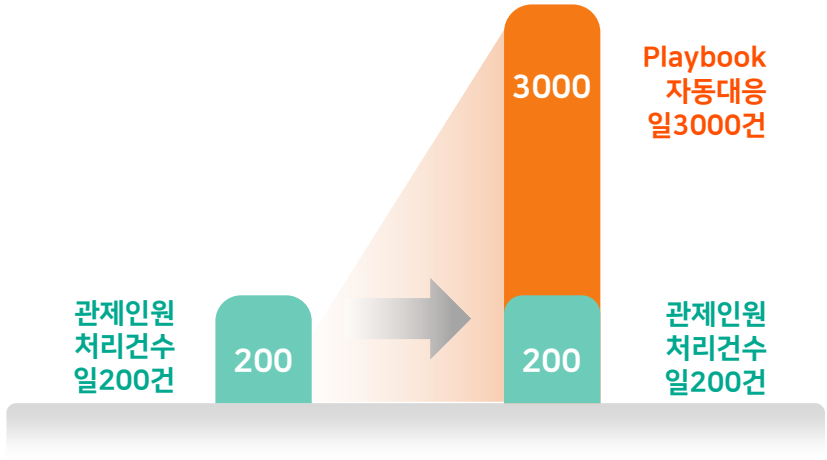
- 국내/국외 에서 발생되는 모든 보안 위협에 대해 수집/분석 자동화
- 위협에 대해 사전에 인지하고 대응 가능

SOAR 자동화 분석/대응 적용 효과

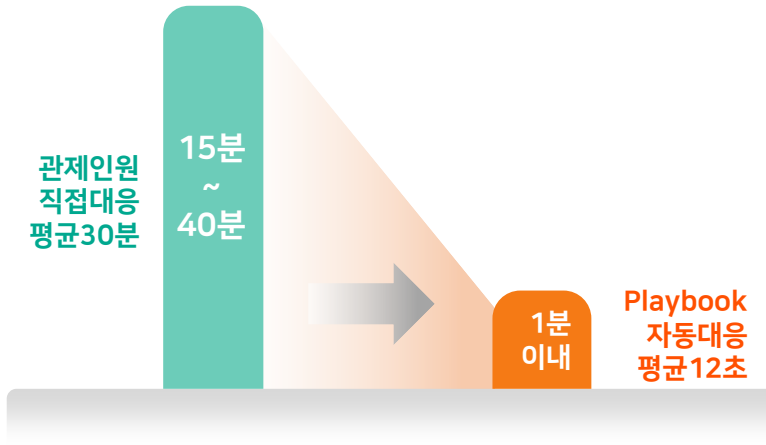
위협 분석 및 대응 자동화



대응 건수 비교

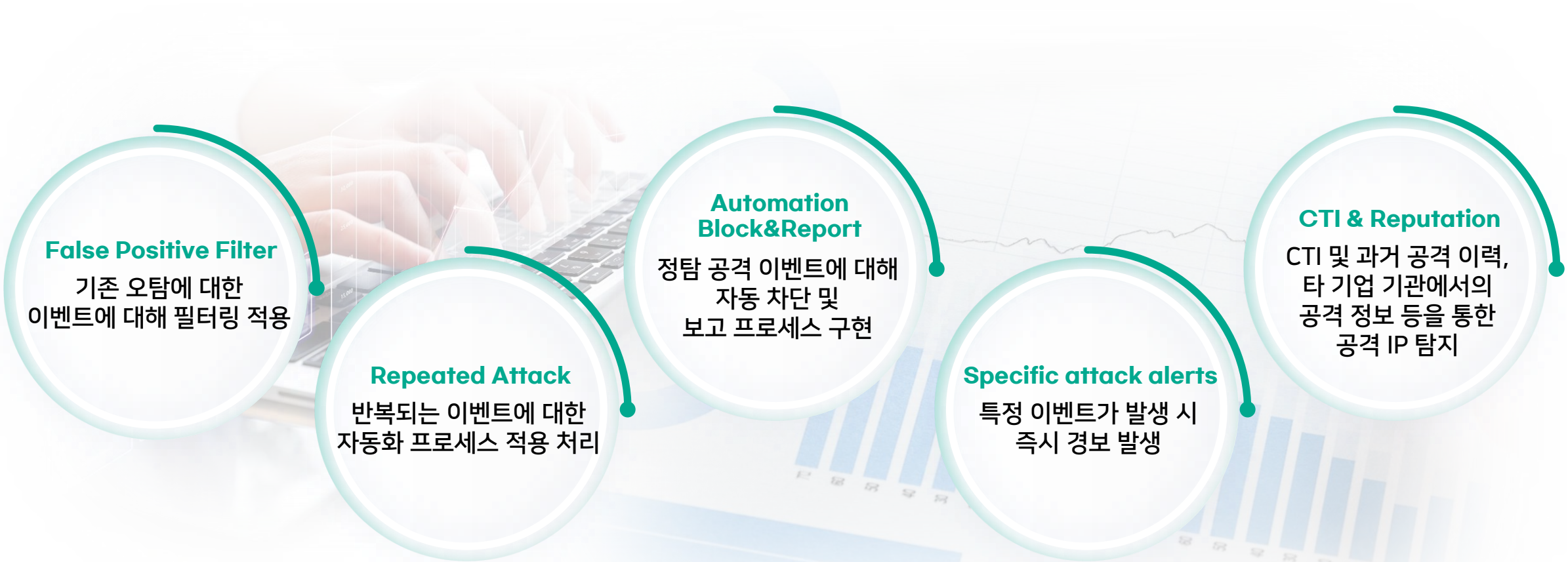


위협 대응 시간
(탐지→분석→보고서 발송 시간)



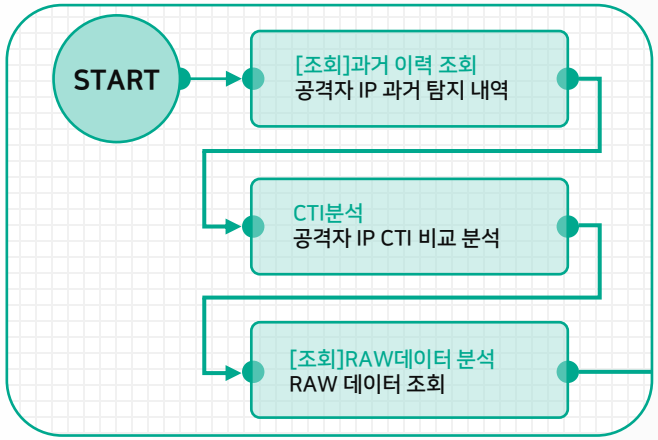
SOAR 적용을 통한 자동화 사례

SOAR 적용을 통한 보안관제 자동화 예시



공격 이벤트에 대한 SOAR Response Process - 자동화 분석

공격 IP 위협 비교 및 RAWDATA 추출



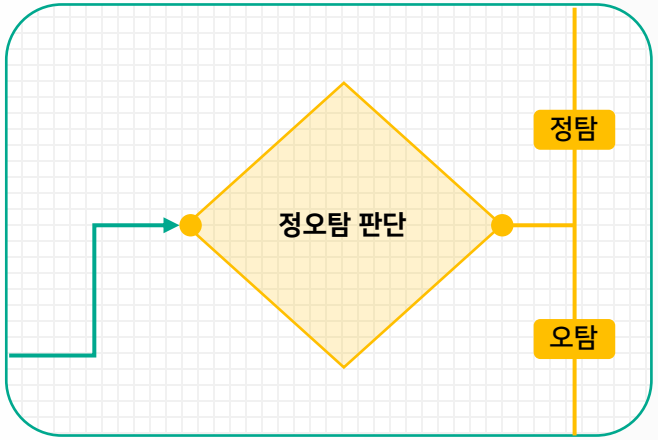
SIEM에서 발생된 경보 이벤트를 바탕으로

01 출발지(공격IP) IP에 대한 과거 공격 이력 분석

02 CTI 정보 비교 조회 하여 유해 IP 여부 판단

03 RAW 데이터를 조회하여 공격 시그니처 패턴 추출

정· 오탐 공격 분석



비교 분석 된 데이터에 대한 정· 오탐 분석

01 과거 공격 이력 분석에 대한 조건 여부를 판단

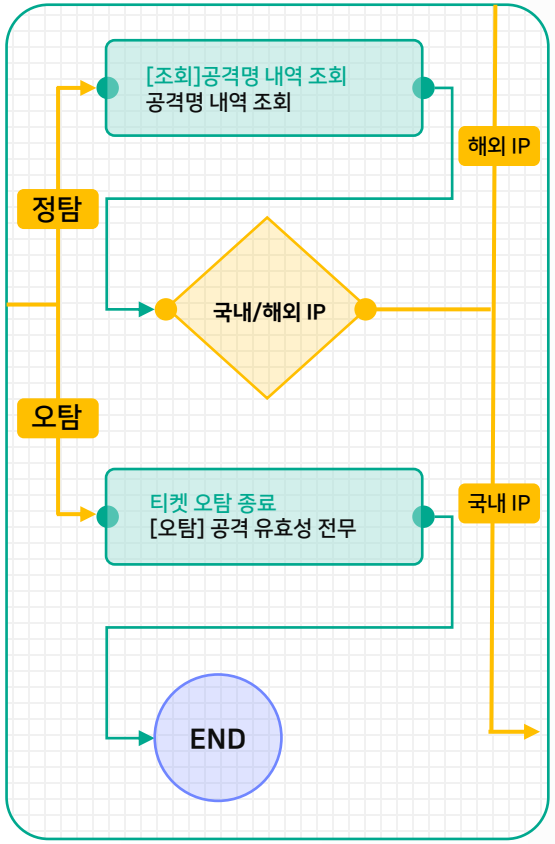
02 공격 IP에 대한 CTI 정보 이력의 존재 여부 판단

03 추출 된 공격 패턴 과 탐지 룰 패턴과 일치 여부 분석

04 정탐 및 오탐으로 구분

공격 이벤트에 대한 SOAR Response Process - 자동화 분석

분석 이벤트에 대한 결과 종합



이벤트 보고서 작성
정보 수집 및
오탐 이벤트 티켓 종료

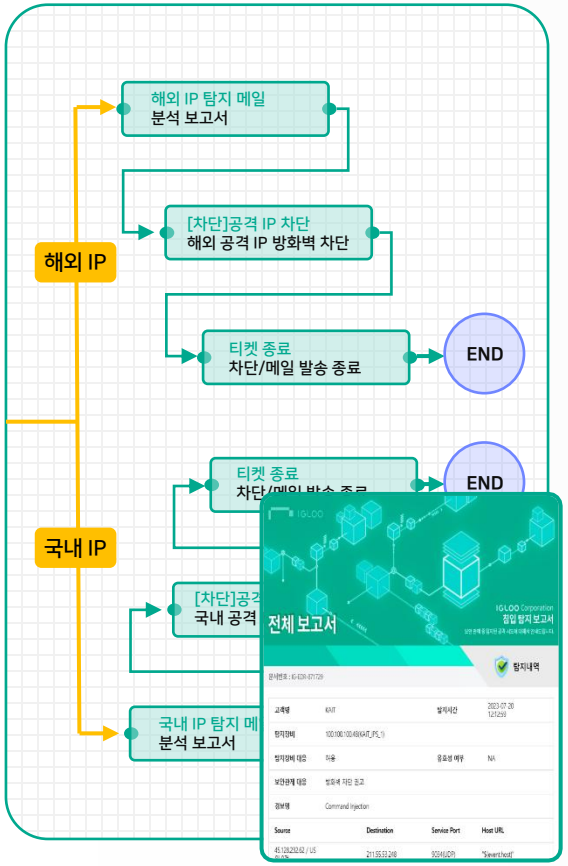
01

분석 된 이벤트에 대한
보고서 작성을 위한
탐지 솔루션 정보 수집

02

오탐 분석 결과에 대한
티켓팅 종료

분석 보고서 작성/송부 및 공격 IP 차단



공격 이벤트 분석
보고서 작성 및
공격 IP 차단

01

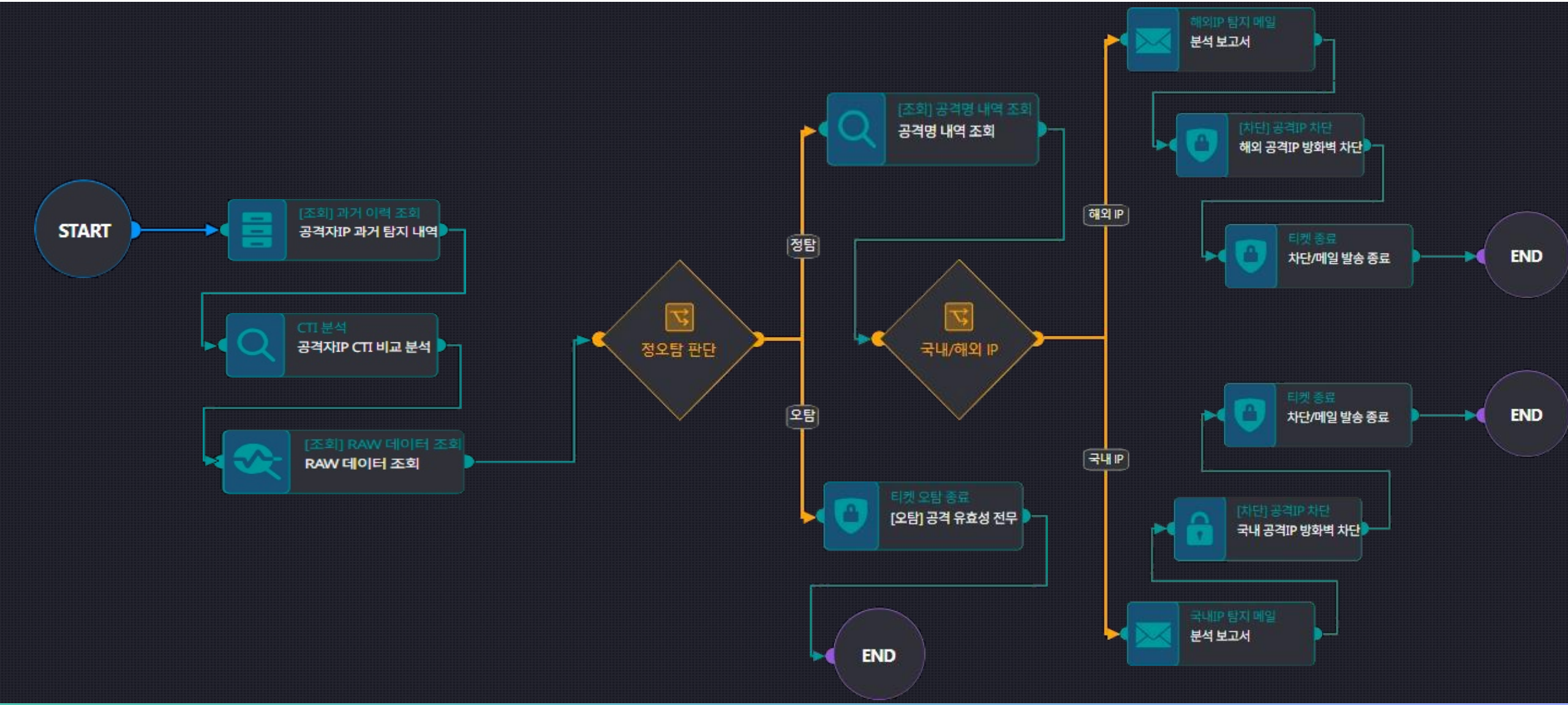
해외/국내 IP 에 대해 조회하고 최
종 분석 보고서 작성 및 발송

02

공격 IP 에 대한 자동 차단 수행

공격 이벤트에 대한 SOAR Response Process - 자동화 분석

SOAR를 통한 자동화 분석



SOAR의 핵심은

Playbook!!

IGLOO

About SOAR Community...

| Q1 |

SOAR를 사용하고 싶은데 Playbook을 어떻게 만들어야 하나요?

| Q2 |

수많은 공격에 대한 Playbook을 생성해야 할 Process를 모르겠습니다

| Q3 |

공격별 Plabybook을 볼 수 없을까요?

| Q4 |

Playbook을 참고 할 수 있는 정보가 없을까요?

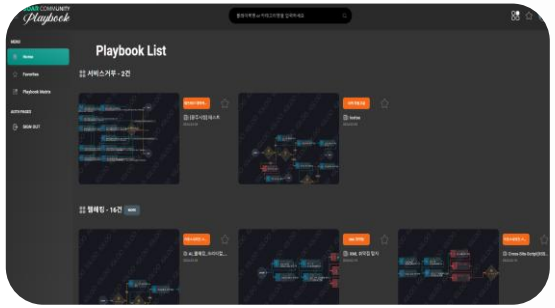
Q&A

SOAR Community

The core of SOAR is Playbook. However, people who are new to SOAR find it difficult to create playbooks due to a lack of understanding of them. To solve this problem, we created the SOAR COMMUNITY. SOAR COMMUNITY collects playbooks for various cyber attacks in one place and provides them easily and conveniently, so the playbook can be easily applied based on this.

IGLOO SOAR COMMUNITY 구성

SOAR COMMUNITY



HOME

SOAR Playbook을 한 눈에 확인 할 수 있도록
구성 하였으며, 각 Playbook을 선택 시
상세한 설명, Playbook 정보, 공격 유형까지 제공

spiderSOAR & SOAR COMMUNITY

Favorite

즐겨찾기 기능을 통해
특정 Playbook을
저장 할 수 있는 기능

Playbook View

Playbook과 상세한
설명, 정보, 공격 유형까지 제공

Playbook Metrix

각 공격별 Playbook을 쉽게 찾을 수 있도록 구성

SOAR & SOAR Community

SOAR & SOAR COMMUNITY 활용 방안

"악성코드 관련 Playbook을 찾고 싶은데요?"

SOAR 커뮤니티

'악성코드 IP' 관련 Playbook을 찾는 방법?

- 최신 Playbook 목록
- Playbook Metirx
  - "경유지악용" 선택
- Playbook 검색
  - "악성코드 " 입력

관심 대상 Playbook을 관리하는 방법?

- Playbook 즐겨찾기 등록

Playbook 세부적인 내용 확인 및 적용 방법?

- Playbook 상세확인
- Playbook 다운로드
  - 악성코드 IP CTI 탐지

SPiDER SOAR

SPiDER SOAR에서 해당 Playbook을 적용하는 방법?

- 다운로드 Playbook 적용
  - 악성코드 IP CTI 탐지

IGLOO

THANK YOU