

# 연세의료원 정보보안 강화 사업

엄재호

연세의료원 디지털헬스실 디지털헬스전략팀

# 목차

---

01 의료원 정보보안 강화 사업 배경

---

02 정보보안 강화 사업 목표

---

03 구축 시 주요 사항

---

04 정보보안 강화 사업 후기(소감)

---

# 의료원 정보보안 강화 사업 배경

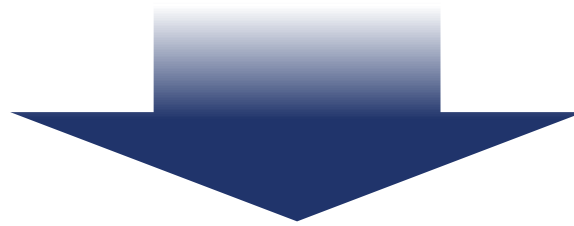
# 01. 의료원 정보보안 강화 사업 배경

## 자주적인 보안 강화 프로세스 구축

- 전방위적 사이버 위협 대응의 필요성
- 환자정보에 대한 선제적 보호 프로세스 마련

## 전사적 공통된 정보보안 품질 확보

- 의료원에 집중된 보안 전담 인원
- 보안장비의 일관된 룰 적용 필요



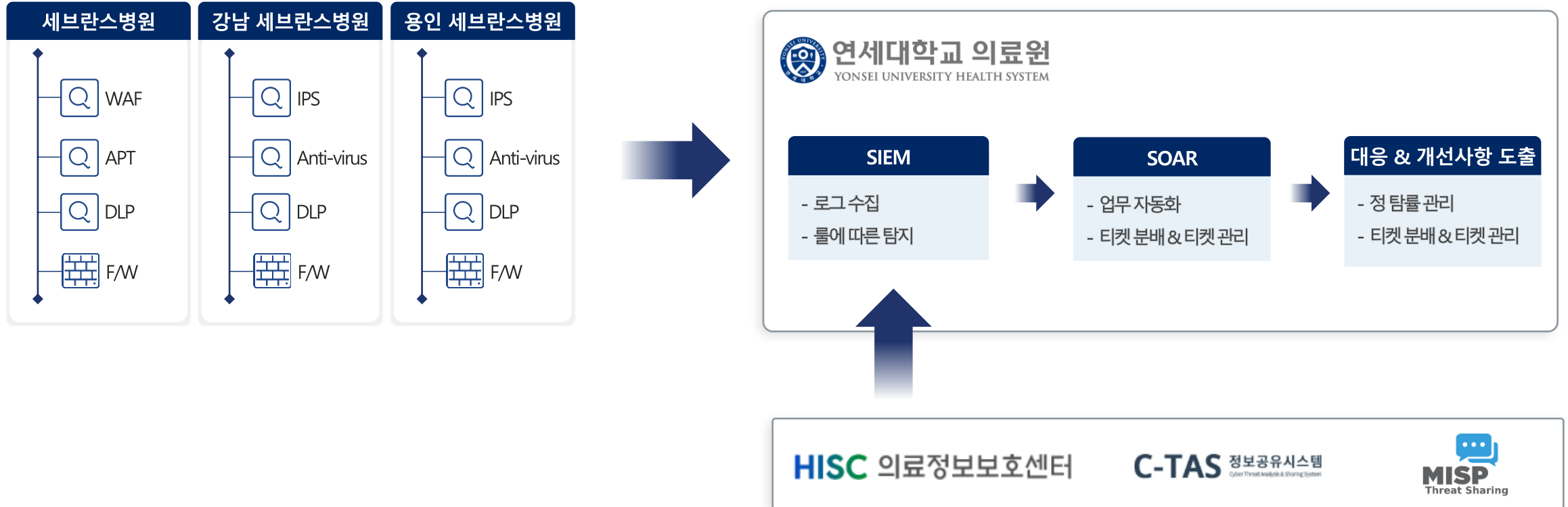
## 연세의료원 보안 강화 사업



# 정보보안 강화 사업 목표

## 02. 정보보안 강화 사업의 목표(상세)

- 통합 SOC(Security Operation Center)의 구성



진행중  
(20년 ~ 23년)

시간적  
범위

공간적  
범위

의료원 내 주요 보안장비 전체 연동  
(신촌, 강남, 용인)

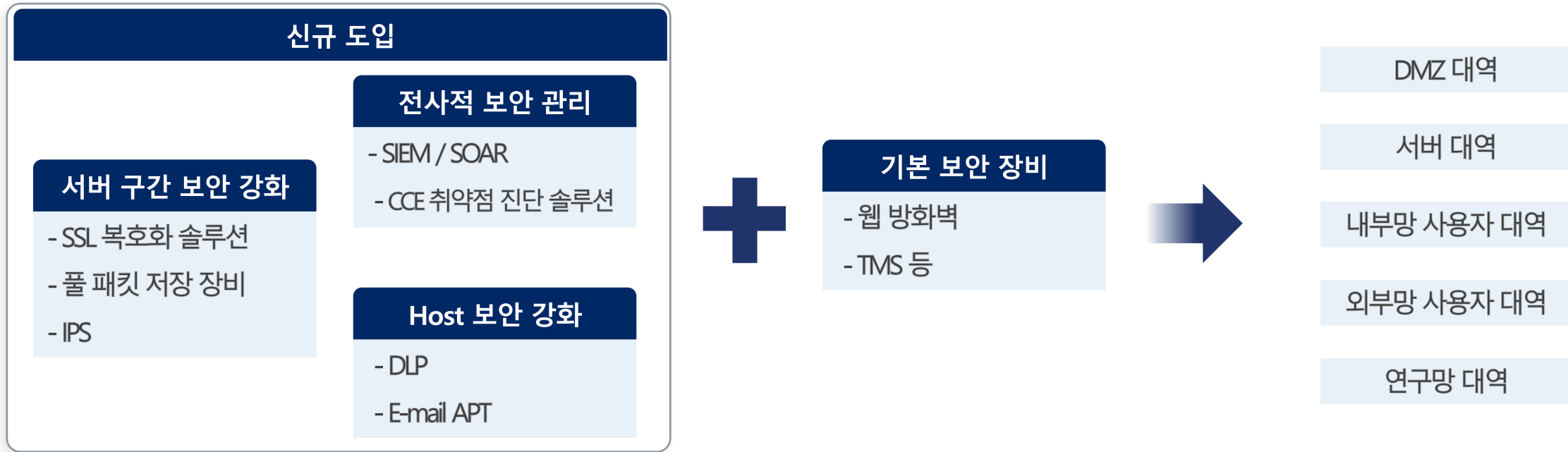
---

# 구축 시 주요 사항

---

### 03. 구축 시 주요 사항

- 보고자 하는 곳에 보안장비 배치



- ✓ 경험적인 측면을 중시하여, 필요한 구간에 대한 식별
- ✓ 충분한 PoC를 통한 장비의 특성 확인

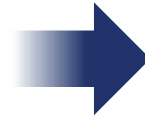


# 03. 구축 시 주요 사항

- 로그 정의서(명세서)와 비교를 통한 수집되는 로그 검토
  - > 대충 연동하면, 결과가 대충 / 시나리오까지 생각하며 로그 검토

114		
116		
118		
119		
120		
121		
122		
123		
124		
130		
131		
132		
133		
134		
140		
300		
401		
402		
451		
452		
501		
551		

Log Field Name	Description	Data Type	Length
	The status of the session: blocked - Blocked infected file by AV engine passthrough - Allowed by AV engine monitored - Log, but do NOT block infected file analytics - Submitted to Sandbox for analysis	string	18
	User agent - eg. agent="Mozilla/5.0"	string	64
	The checksum of the file submitted for analytics	string	64
	The flag for analytics submission	string	10
		string	3
	Server used to authenticate the involved user	string	64
		string	512
		string	256
	The checksum of the scanned file	string	16
	Content Disarm action- eg. disarmed, detected	string	13
	Threat Weight action	uint32	10
	Threat Weight Level	string	10
	Threat Weight Score	uint32	10
	Date	string	10
		string	16
	Message/packets direction	string	8
		string	64
	Destination Interface	string	32
	Destination Interface's assigned role (LAN, WAN, etc.)	string	10
	Destination IP Address	ip	39
	Destination Port	uint16	5



무엇이 문제 인가?

정상 동작인가?

해당 기능을 비활성화 하는 이유는 무엇인가?

<로그 정의서>

- ✓ SIEM 구축 시 유용한 값 또는 기능을 찾을 수 있음
- ✓ 로그 정의서는 Syslog와 비교를 통해 특이사항 확인
  - :기능 비활성화 및 정상 동작 여부를 확인

### 03. 구축 시 주요 사항

- 기본 탐지 룰 이외에도 상호 보완적인 룰 생성

공격 탐지 / 대응 장비	구분	자산등록 필요 여부	차단 정책 가능 여부	탐지 기반	비고
DDoS	DDoS	X	O	패턴	내부에서 보완 장비 없음 → 외부 ISP 업체와 협력
WAF	WAF	O	O	패턴	IPS와 상호 보완 → 자산 등록
IPS	IPS	X	O	패턴	WAF와 상호 보완 → 패턴 업데이트
플 패킷 저장 장비	플 패킷 저장 장비	X	O	-	패턴 기반 장비를 보완 → 미탐 패턴 업데이트

✓ **WAF 자산 등록 누락 시** 주요 보안 위협이 발생 할 수 있음

> WAF 자산 누락 시 경보 발생

✓ WAF와 IPS는 패턴 기반의 보안장비로, **패턴 누락 시** 주요 보안 위협이 발생 할 수 있음

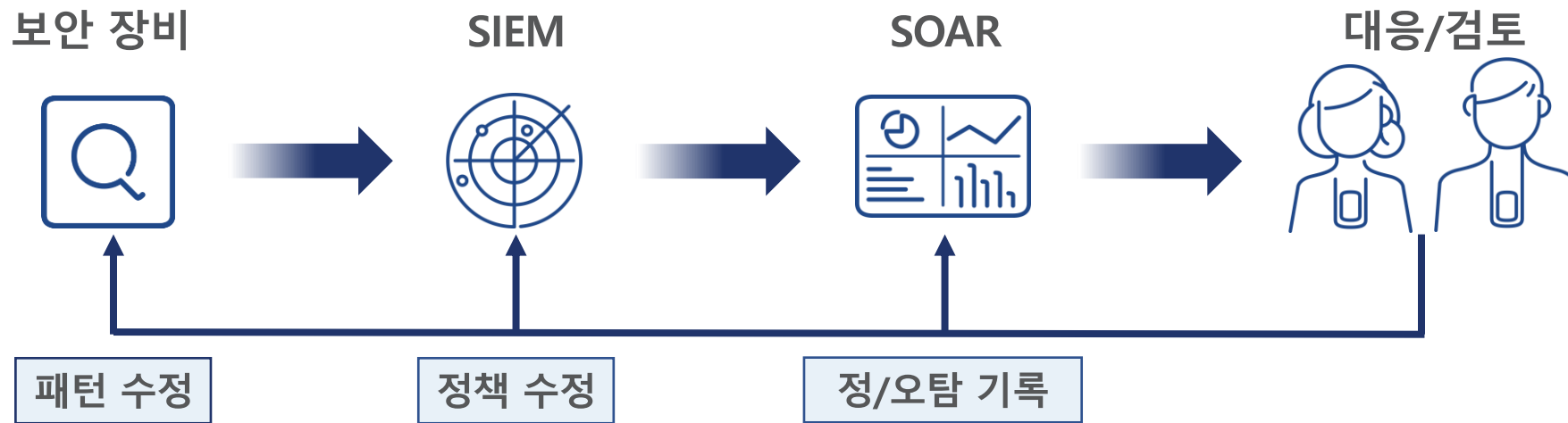
> 보안장비(WAF, IPS) 하단에 모든 패킷을 저장 하는 보완 장비를 구축하여 상호 보완할 수 있도록 구현

✓ DDoS 공격 유입 시, **자체적인 대응이 불가능한 공격 패턴이 다수 있음**

> 자체 모니터링하되, 대응은 ISP 업체와 협력 체계 마련

### 03. 구축 시 주요 사항

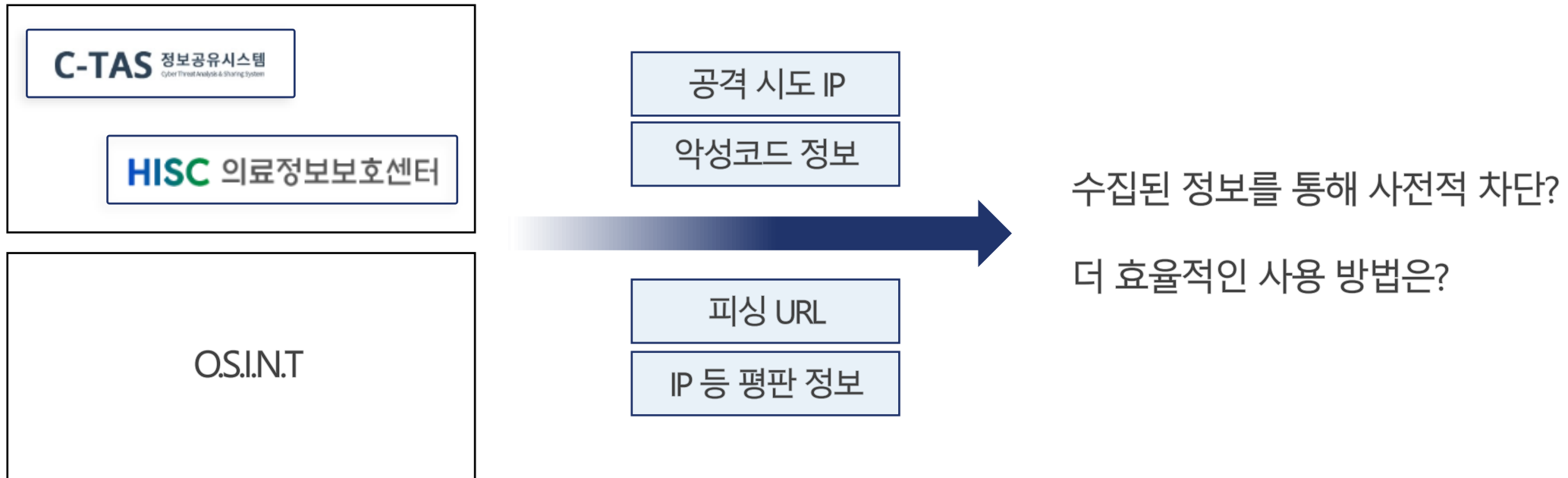
- 관리자의 관심만 있다면 지속 발전 할 수 있는 모니터링 프로세스 마련
  - > 경험이 아닌 데이터를 통해 룰 수정



- ✓ SOAR에 정탐/오탐을 기록하는 별도의 프로세스를 만들고, 정탐 및 오탐률에 대한 통계치를 자동으로 작성
- ✓ SOAR의 정오탐 기록을 통해 SIEM의 룰 또는 보안 장비의 패턴을 수정

### 03. 구축 시 주요 사항

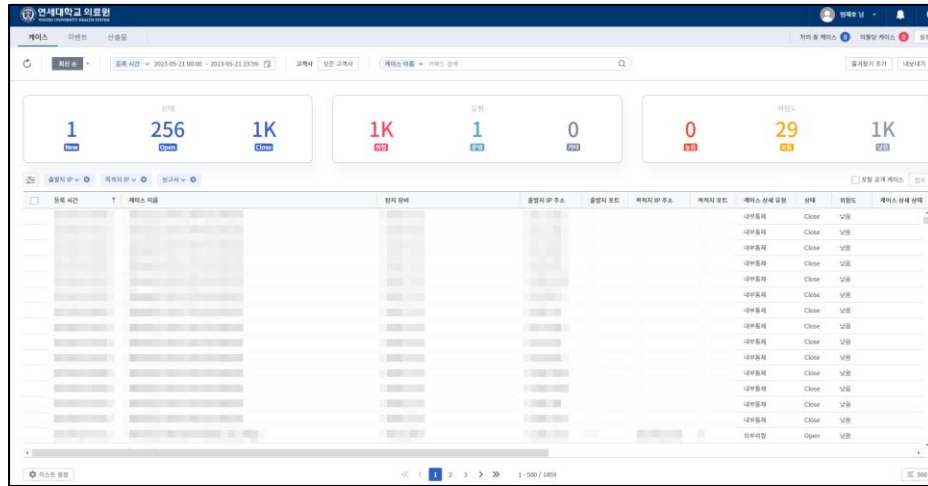
- **T.I(Threat Intelligence)정보와 OSINT(Open Source Intelligence)의 활용**  
 > 의료 HISAC의 관제 결과는 적극적 활용 / C-TAS 및 기타 OSINT는 보조적 수단으로 활용



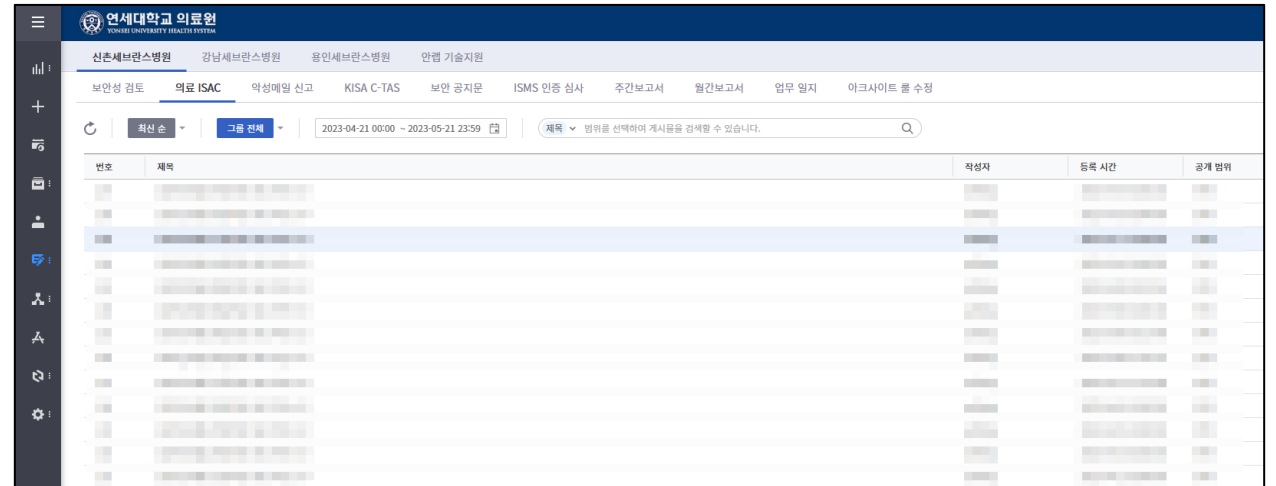
- ✓ C-TAS 가입을 통한 T.I 정보를 한번 확인해 볼 필요는 있다고 판단함
- ✓ 이후 참고용으로 미탐 된 로그 검색 등 보완의 개념으로 활용

# 03. 구축 시 주요 사항

- SOAR의 활용 방안
  - > SIEM에서 발생 된 티켓을 각 담당자에게 자동 분류
  - > 통합된 정보보안팀 포탈 개념(데이터 업로드, 인수인계사항 기입 등)



The screenshot shows a dashboard with several key performance indicators (KPIs) at the top: 1, 256, 1K, 1K, 1, 0, 0, 29, 1K. Below these are several data tables with columns for '등록 시간' (Registration Time), '카테고리' (Category), '발생 일자' (Occurrence Date), '종료 일자' (End Date), '처리 일자' (Processing Date), '처리 상태' (Processing Status), and '담당자' (Responsible Person). The table contains multiple rows of data, with some rows highlighted in blue.



The screenshot shows a web portal interface with a navigation menu on the left and a main content area. The main content area displays a table with columns for '번호' (Number), '제목' (Subject), '작성자' (Author), '등록 시간' (Registration Time), and '공개 범위' (Access Scope). The table contains multiple rows of data, with some rows highlighted in blue.

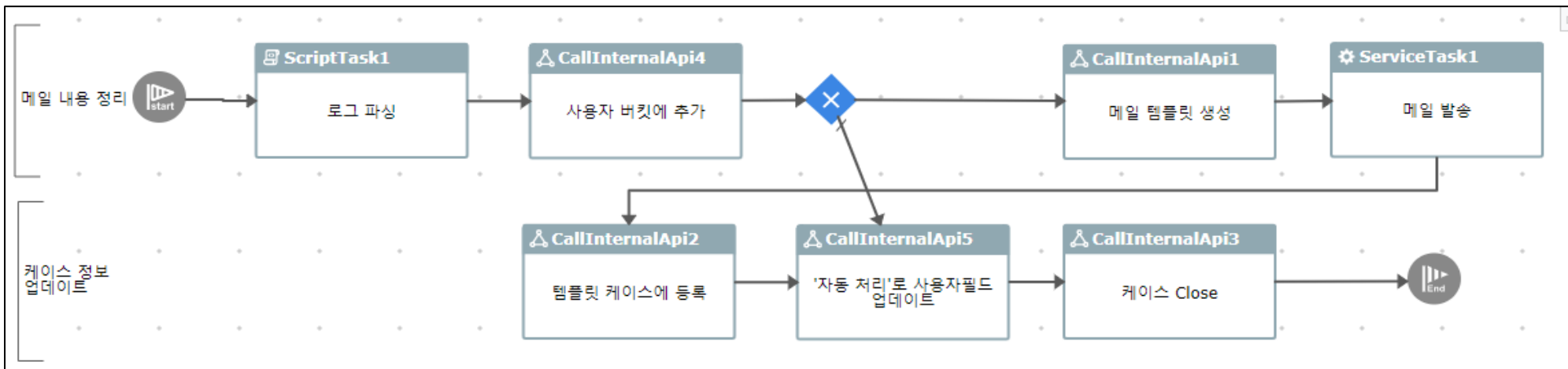
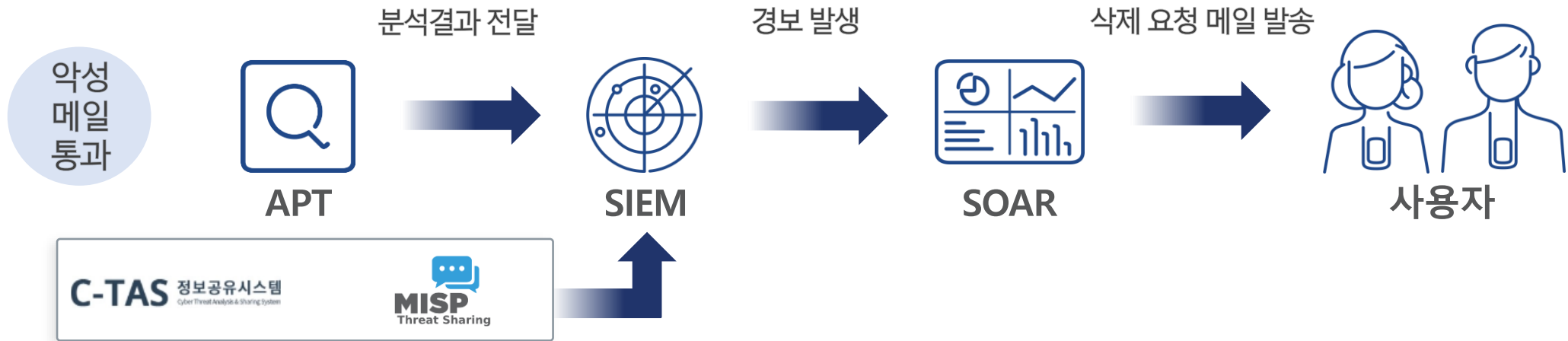
> 추가

- 1) 메일 발송 등 **상황 전파**가 필요한 곳에 SOAR를 **적극 활용**
- 2) 특정 이벤트에 대한 대응
- 3) 방화벽 차단 시 자동화

# 03. 구축 시 주요 사항

- SOAR 구축

> APT에서 미탐지 메일 식별하는 PlayBook의 구현



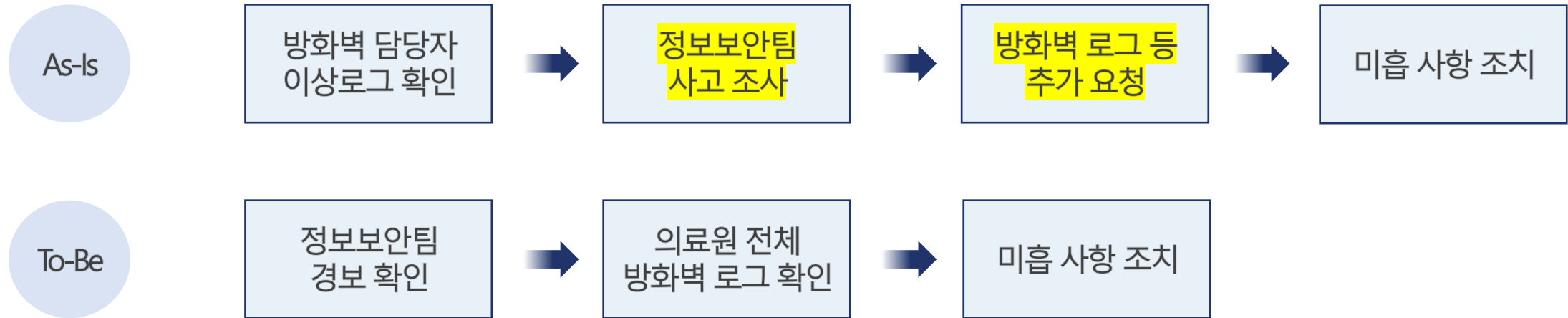
---

# 정보보안 강화 사업 후기

---

# 04. 정보보안 강화 사업 후기

- 효율적인 모니터링 및 사고 조사
  - > 장비 간의 지역적 한계를 뛰어 넘어, 사고 조사가 가능함



조사 시간은 짧게 / 품질은 높게



# 04. 정보보안 강화 사업 후기

- SOAR

> 기존 정보보안 인력이 접근하기 힘든 영역, 즉 SOAR 구축 엔지니어에 의존도가 높음

```

1 import re, json
2
3 caseObj = execution.getParam('case')
4 eventList = execution.getParam('events')
5
6 caseName = caseObj.get('name')
7 caseId = caseObj.get('id')
8 ruleName = caseName.split('-')[1]
9 customData = caseObj.get('customData')
10 deviceZoneURI = customData.get('deviceZoneURI')
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28
29
30
31
32
33
34
35
36
37
38
39
40
41
42
43
44
45
46
47
48
49
50
51
52
53
54
55
56
57
58
59
60
61
62
63
64
65
66
67
68
69
70
71
72
73
74
75
76
77
78
79
80
81
82
83
84
85
86
87
88
89
90
91
92
93
94
95
96
97
98
99
100

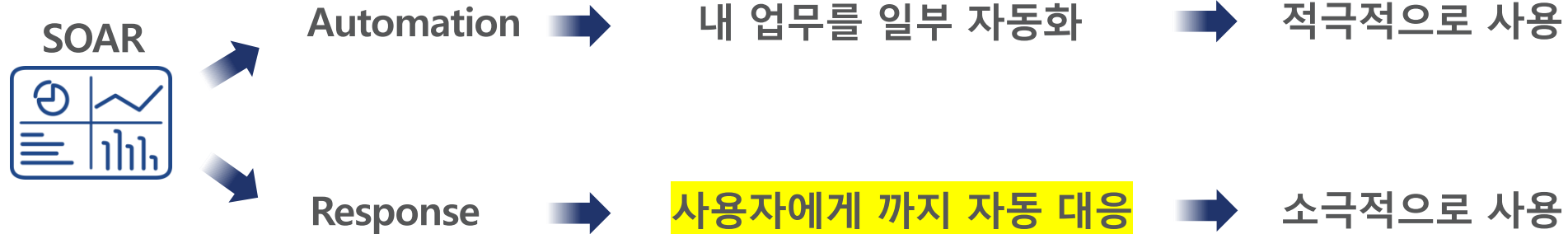
```



- ✓ 수집된 로그를 통해 엔지니어에게 설명
- ✓ SIEM에서 최대한 경보로 발생하고, 발생한 내용을 메일로 전달 되는 패턴으로 구축

## 04. 정보보안 강화 사업 후기

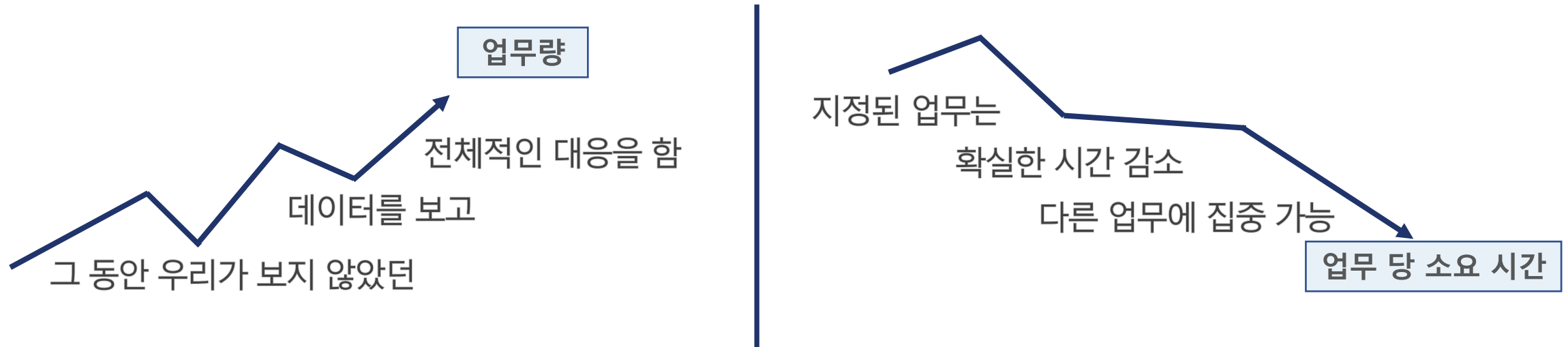
- SOAR의 Input에 거짓이 있으면, Output이 거짓이다.  
 > 대응은 전수 담당자의 확인을 통해 반자동 개념으로 적용



- ✓ 자동화의 경우 일정 예상 범위 안의 효과 입증
- ✓ 대응의 경우 최종 판단 단계의 개입이 반드시 필요로 판단

# 04. 정보보안 강화 사업 후기

- 업무량 변화 / 기존 업무의 소요 시간 변화
  - > 업무량은 증가하였지만, 각 단위 별 업무 소요시간은 단축



- ✓ SIEM과 SOAR의 기능으로 목적인 바가 이루어지고 있음을 확인
  - 백데이터가 없으므로, 업무량이 구체적으로 얼마나 증가하였는지는 객관적으로 표현 불가능
  - 향후 개선이 필요한 사항은 SOAR로 정량적 평가의 시도



YONSEI UNIVERSITY  
HEALTH SYSTEM

