

# 위협정보 공유 및 관리 시스템 TARGOS

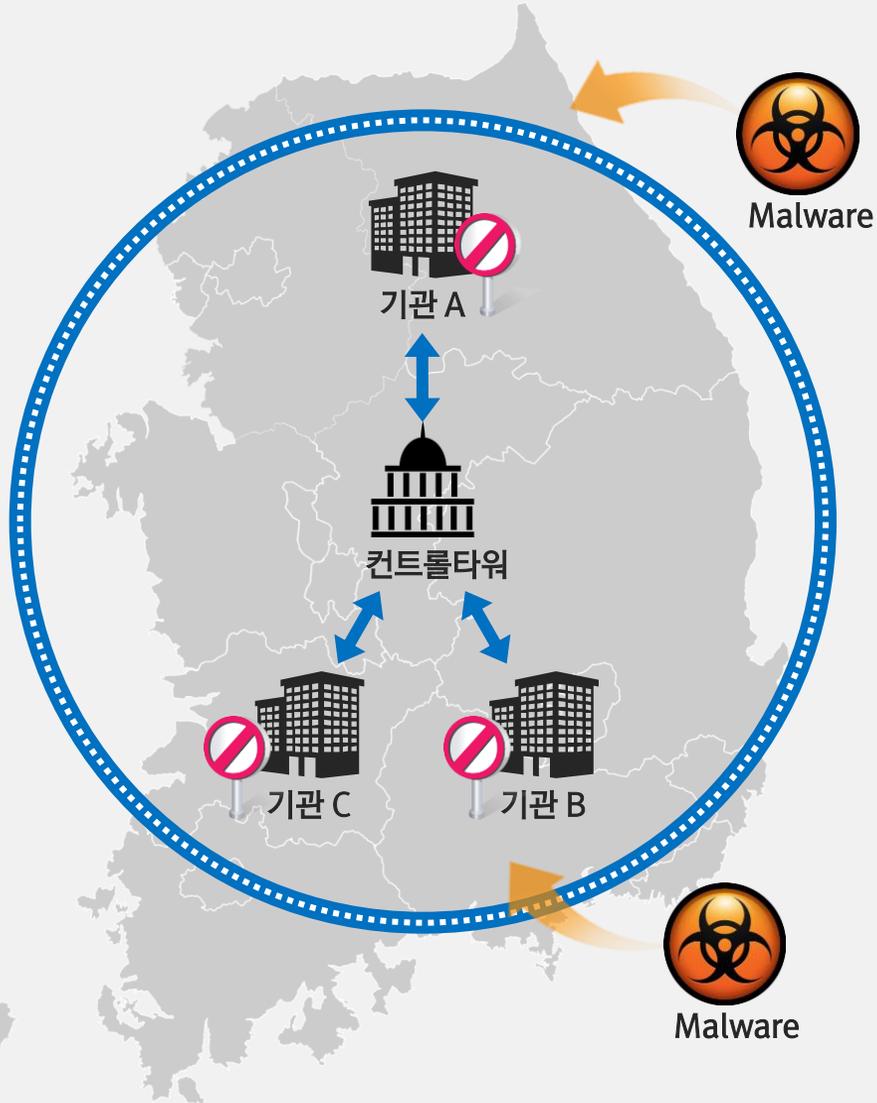
2023.03

오픈베이스 보안기술본부

# Agenda

1. 위협정보 공유 및 관리 시스템 소개
2. TARGOS 구성
3. TARGOS 운영사례
4. TARGOS 도입효과

# 위협정보 공유 개념도



## 위협정보 공유 이전의 문제점

- 각 기관은 자체 보유한 보안 솔루션에 의존  
**한정된 비용, 운영 인력의 부족, 전문성 결여**
- 기관A에 침입한 악성코드에 대한 정보를 다른 기관에서 알 수가 없음  
**동일한 공격에 의한 피해 발생 가능**
- 기관 특성에 따른 공통된 보안 정책 적용 불가  
**기 구축된 보안 장비에 의존**

# 위협정보 공유 및 관리시스템 필요성

## 위협정보 공유 시 고려 사항

악성코드 표현체계 불일치

악성코드 탐지엔진 불일치

악성코드 탐지결과 불일치

악성코드 공유체계 불일치

악성코드 대응체계 불일치



국가 위협정보 공유체계 지원

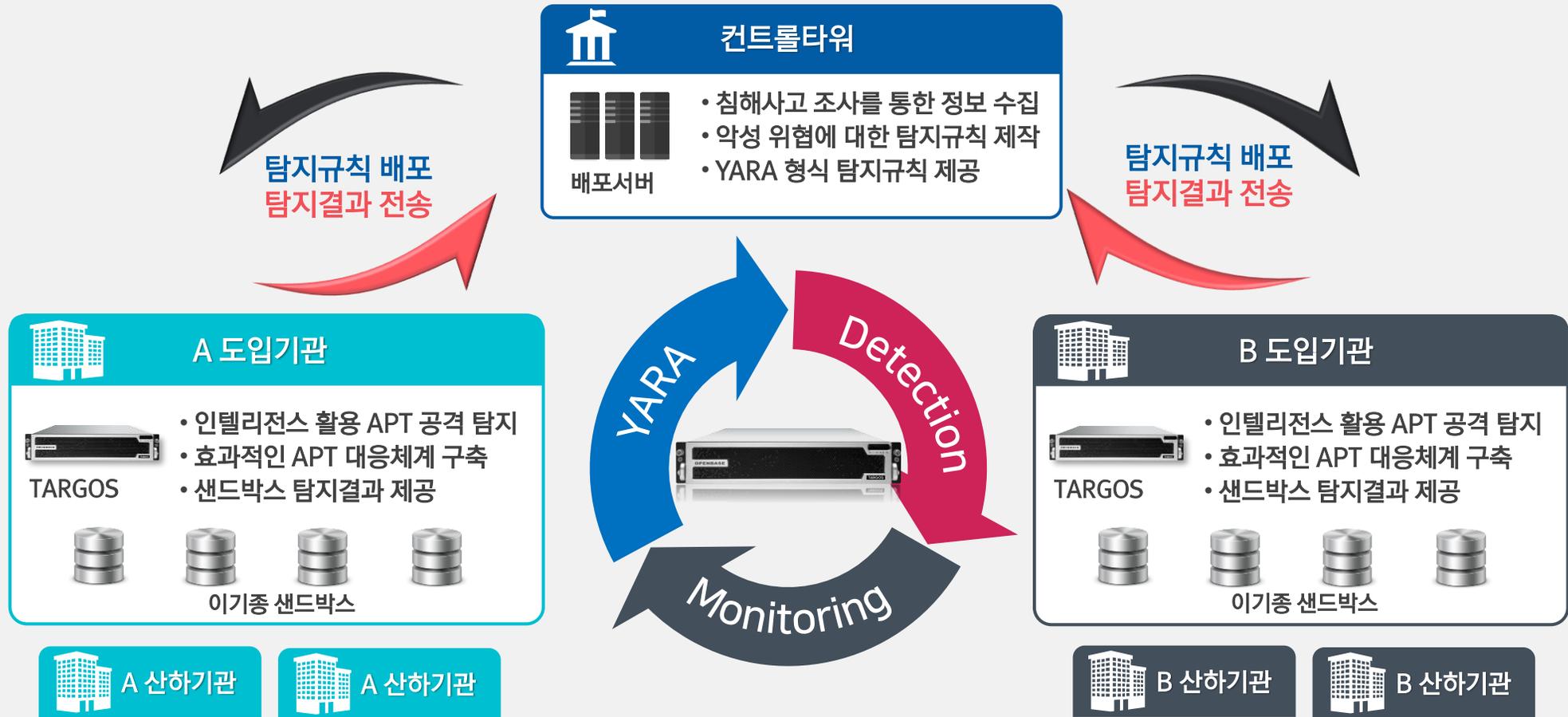
탐지규칙(YARA, STIX 등) 배포

탐지결과 전송

위협정보 공유 모니터링

# TARGOS 개요

❖ 다양한 샌드박스와 연동되는 악성파일 표준 판별 체계를 통해, 컨트롤타워와 도입 기관 간의 긴밀한 APT 대응체계 구축



# 고객 현황 & 연동 샌드박스

❖ 총 21개 고객사 납품 및 11개의 보안제품 연동

## TARGOS기관도입현황(21)

KPX 전력거래소  
 한국전력공사  
 wp 한국서부발전|주  
 KOREA WESTERN POWER CO., Ltd.  
 보건복지부  
 KP FIS 한국재정정보원  
 Korea Public Finance Information Service  
 한국보건복지인력개발원  
 SSIS 사회보장정보원  
 한국수력원자력|주  
 EWP 한국동서발전|주  
 KOREA EAST-WEST POWER CO., LTD.  
 산림청  
 국토교통부  
 KISA 한국인터넷진흥원  
 KOREA INTERNET & SECURITY AGENCY  
 금융보안원  
 FINANCIAL SECURITY INSTITUTE  
 문화체육관광부  
 NPS 국민연금  
 HYUNDAI 현대 HCN  
 한국지역난방공사  
 h-well 국민건강보험  
 National Health Insurance Service  
 KANGWON LAND  
 KOICA 한국국제협력단  
 Incheon Airport 인천국제공항공사

## TARGOS 연동 샌드박스 현황(11)

- FireEye
  - FireEye NX / EX / AX
- Trend Micro
  - Trend Micro DDA
- paloalto NETWORKS
  - Paloalto WildFire
- CISCO
  - CISCO Threat Grid
- BaileyTech
  - BaileyTech ZBlock
- KORNIC GLORY
  - KonicGlory TMS
- AhnLab
  - AhnLab MDS
- ANY RUN
  - ANY.RUN
- wINS
  - Wins Sniper APTX
- SECU LETTER
  - SecuLetter
- CROWDSTRIKE
  - CrowdStrike Falcon

## TARGOS 제품 라인업

구분		TARGOS Software	TARGOS Appliance	
제품사양	제품 외관			
	모델	나라장터 종합쇼핑몰 등록 (Appliance 제공가능)	TSX2000	TSX5000
	보안제품 연동 대수	별도협의를	5	10
	다계층 연동 대수	별도협의를	10	20
	탐지 이벤트 처리 성능	별도협의를	8000/일	15000/일
Hardware	CPU	Intel 4Core x 1	Intel 4Core x 1	Intel 10Core x 2
	Memory	32GB	32GB	128 GB
	HDD	SATA 1 TB x 1	SSD 240 GB x 1 SATA 1 TB x 1	SSD 240 GB x 2 SATA 2 TB x 2
	RAID	-	-	RAID 1(HW)
	NIC	Intel 10/100/1000 x 1	Intel 10GB x 2	Intel 10GB x 2
	Size(H*W*D In)	-	1.75" x 17.24" x 21.8"	3.44" x 16.93" x 27.95"
	Stack	-	1 U	2 U
	Power	-	AC/DC 1100W x 2	AC/DC 1300W x 2

※ TARGOS S/W : H/W 최소사양

# TARGOS 특징



## 인증 및 수상



GS(Good Software) 인증  
인증번호 : 17-0130



2018년  
TARGOS 신SW상품대상  
과기정통부 장관상

## 국내/해외 공유체계 표준 지원

HTTPS JSON

행위분석 리포트

YARA



## 특징



다양한 APT탐지시스템 연동



다계층 구성 지원



모니터링 통계 데이터 제공



빅데이터 플랫폼 기술 적용

# TARGOS 주요 기능

## ❖ 탐지규칙 수신 및 배포

- 배포기관(상위기관) → TARGOS → 샌드박스
- 배포기관으로부터 탐지규칙 자동 동기화 및 샌드박스에 탐지규칙 배포

## ❖ 탐지결과 수집 및 송신

- 배포기관(상위기관) ← TARGOS ← 샌드박스
- 샌드박스 탐지결과를 수집하여 상위로 해당 탐지결과를 전송

## ❖ 연결장비 상태 및 탐지결과 모니터링

- 다양한 분석 방식 활용을 위한 대시보드 제공
- 연동된 장비현황 및 장애상황을 파악할 수 있는 운영상태 정보 제공



# TARGOS 주요 화면 - 대시보드

❖ 장비 상태 및 데이터 수집 현황을 파악할 수 있는 대시보드 제공

TARGOS TSX
admin01

대시보드

» Summary

운영상태

이력

탐지규칙 배포이력

탐지결과 송/수신 이력

수집파일

탐지규칙

탐지규칙 목록

설정

사용자

감사로그

Syslog

백업 및 복원

대시보드

Summary 2021-02-25 16:53:10 - 2021-02-26 16:53:10 새로고침 수정

YARA 배포

Y

v2.10(최신)

탐지결과 송신상태

0개

2021-02-26 16:45:43

타르코스

타

54초 전

연계 서버

연

54초 전

파일저장소

저

54초 전

샌드박스

2 1

하위매니저

1 1

샌드박스 분석 Top 10

분석 장비 이름	건수
FireEyeNX	15

악성여부

15

수집 파일수

● 정상 0
● 악성 15
● 알수없음 0

분석별 탐지 수

탐지규칙 Top 10

조회기간 내 데이터가 없습니다.

SHA-256 Hash Top 10

SHA-256	건수
4535d19558108c23e59535eb6d5b90f1c707e365e87bc3340fe5e17973c70b0c	2
72b986ce3762a9388148c768c316e47afc3199059a8a42be209b7ebd813e118f	2
e3d54db34b40b2dd0e11ecaf92058dc099abb2ebe675e0961b7ccfca0b1f16de	2
137ddff1ee508f0b0d59bd3c25cc80717a00116902ff657b58dc7df8cd32fb21	1

분석상태

15

수집 파일수

확장자 Top 10

확장자	건수
zip	13
exe	2

탐지이름 Top 10

탐지 이름	건수
FEK_JS_IN_ZIP	8
fe_ml_heuristic	7
PASSWORD_EXTRACTION_FAILED	5
Malware.Binary.exe	2
PUP.Win32.Puamson.FEC2	2
Trojan.Win32.Caspio.FEC2	2

10

# TARGOS 주요 화면 - 운영상태

❖ 연동된 장비현황 및 장애상황을 파악할 수 있는 운영 상태 화면 제공

**TARGOS TSX**

- 대시보드
- Summary
- 운영상태**
- 이력
- 탐지규칙 배포이력
- 탐지결과 송/수신 이력
- 수집파일
- 탐지규칙
- 탐지규칙 목록
- 설정
- 사용자
- 감사로그
- Syslog
- 백업 및 복원

운영상태
admin01

### 운영상태 목록

추가
새로고침

장비 이름	연결상태	탐지규칙 버전 상태	탐지결과 송신/수신 상태
연계서버 192.168.2.119	정상 48초 전	YARA v2.10 18분 전	0 8분 전
targos CPU : 54.10% Memory : 31.53% Disk : 37.14%	-	YARA v2.10 (최신) 2020-11-12 16:40:41	0 48초 전
Targos_MID(5.72) 192.168.5.72 CPU : 2.02% Memory : 80.26% Disk : 5.72%	정상 46초 전	YARA v10.21 2020-12-28 13:39:43	3 6분 전
FireEyeAX 192.168.5.240	정상 45초 전	YARA v10.21 2020-12-28 13:39:51	3 6분 전
Targos_Bottom(17.88) 192.168.17.88 CPU : 3.79% Memory : 47.40% Disk : 50.38%	정상 45초 전	YARA v21.22 2021-01-04 15:16:44	11분 전
FireEyeEX 61.82.88.136	정상 45초 전	YARA v21.22 2021-01-04 15:16:49	0 2분 전
FireEyeNX 61.82.88.140	정상 44초 전	YARA v21.22 2021-01-04 15:16:49	11분 전

※ 현재시간 기준 최종시간 단, 샌드박스 처리 상태는 현재시간 기준 최종 1분

# TARGOS 주요 화면 – 탐지규칙 배포 및 탐지결과 송신 이력

❖ 탐지규칙 배포 및 탐지결과 송신 상태를 한눈에 파악할 수 있는 이력 화면 제공

The screenshot displays the TARGOS TSX interface. The left sidebar contains navigation options such as 대시보드, 운영상태, 이력, 탐지규칙, and 설정. The main content area is titled '탐지결과 송신 이력' (Transmission History of Detection Results). It features two large statistics: '송신 이력 수' (Transmission History Count) at 2,013 and '송신 탐지 수' (Transmission Detection Count) at 2,638. A bar chart shows the '송신 탐지수 추이' (Transmission Detection Count Trend) over time, with data points for Jan 31, Feb, Feb 06, Feb 09, Feb 12, Feb 15, Feb 18, Feb 21, and Feb 24. Below the chart is a table of transmission records with columns for '송신시간' (Transmission Time), '송신상태' (Transmission Status), '메시지' (Message), '송신 탐지수' (Transmission Detection Count), and '대상별 송신 탐지수' (Transmission Detection Count by Target). The table shows two records: one from 2021-02-24 at 12:35:44 with 1 detection, and another from 2021-02-09 at 07:14:04 with 35 detections. At the bottom, a network diagram shows a '연계서버' (Link Server) connected to a 'targos' node, which is in turn connected to 'FireEyeAX' and 'FireEyeNX' nodes. Arrows indicate the direction and count of data flow: 35 from targos to 연계서버, 28 from FireEyeAX to targos, and 7 from FireEyeNX to targos.

# TARGOS 주요 화면 - 수집 파일

## ❖ 샌드박스에서 수집된 악성 파일에 대한 분석 상태 및 상세 정보 제공

The screenshot displays the TARGOS TSX interface. On the left is a navigation menu with options like 대시보드, Summary, 운영상태, 이력, 탐지규칙, and 설정. The main area is divided into two panels. The top-left panel shows a summary of collected files: '수집파일 목록' with a total of 6,305 files. The top-right panel shows a detailed view of a file named 'bin.sh', including its MD5, SHA-1, and SHA-256 hashes. Below this, there are analysis results from SandBox, VirusTotal, and other engines. A table at the bottom shows the analysis status for the file.

단계	상태	결과	메시지
수집	성공		
샌드박스 분석	준비	0	
	진행	0	
	성공	2	> 악성: FireEyeAX(winxp-sp3m), FireEyeNX
	실패	0	
	준비	0	
	진행	0	

# TARGOS 주요 화면 - 탐지규칙 목록

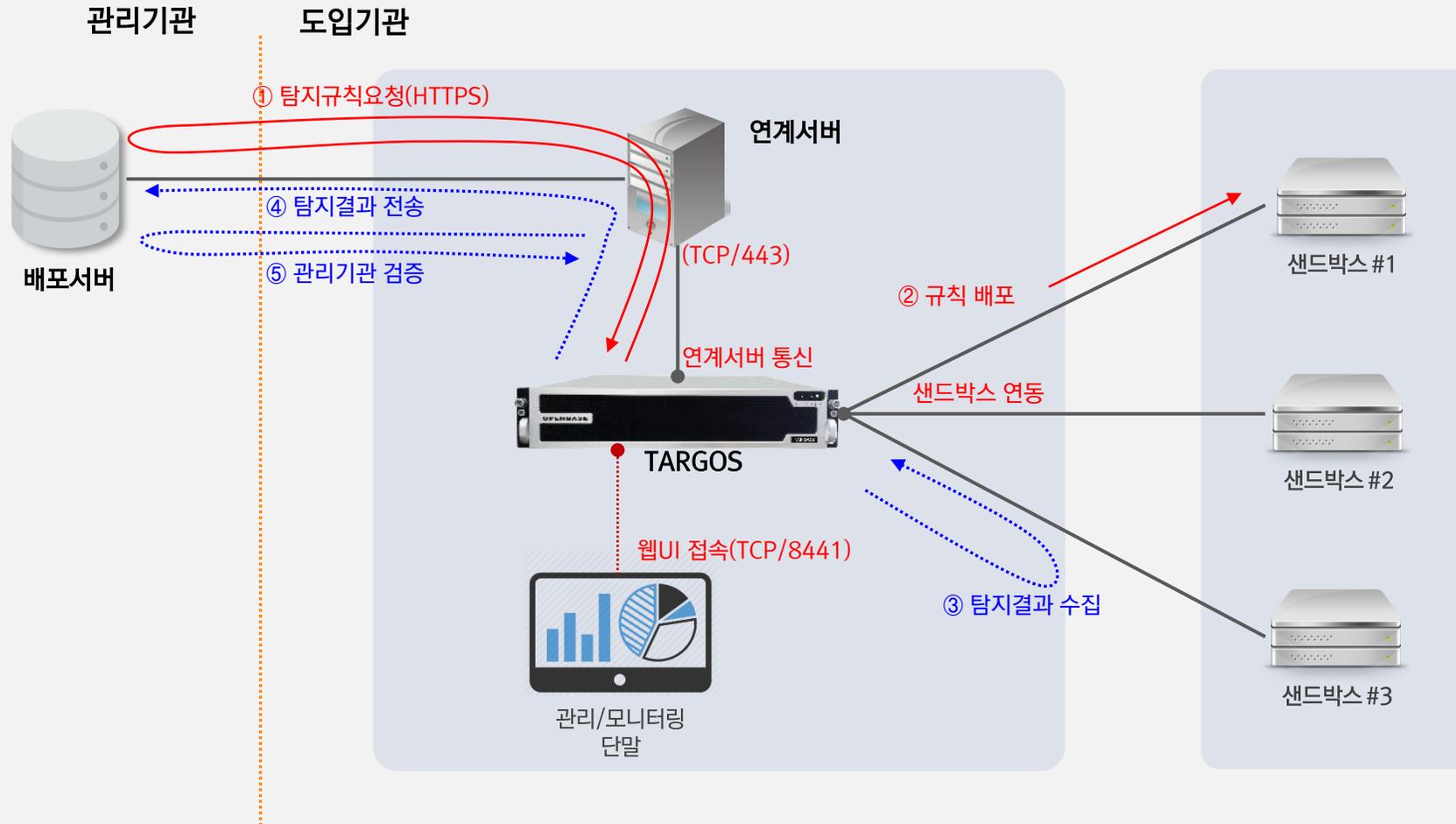
❖ 상위기관으로부터 받은 탐지규칙 현황 및 각 규칙에 대한 활성화/비활성화 설정, 사용자 정의 규칙 생성 제공

The screenshot displays the TARGOS TSX interface. On the left is a navigation menu with options like '대시보드', 'Summary', '운영상태', '이력', '탐지규칙 배포이력', '탐지결과 송/수신 이력', '수집파일', '탐지규칙', '설정', '사용자', '감사로그', 'Syslog', and '백업 및 복원'. The main area shows the '탐지규칙 목록' (Detection Rule List) with a summary card for 'YARA v10 배포버전' and three donut charts for '장비이름', '상태', and '다계층 지원여부'. A table below lists 15 rules with columns for checkboxes, '장비이름', '상태', '다계층 지원여부', and '수신버전'. An overlay window titled '탐지규칙 수정' (Edit Detection Rule) shows details for a rule named '연계서버' (YARA), including its ID, creator, status (Enable), weight (100), and strings/condition definitions.

장비이름	상태	다계층 지원여부	수신버전
연계서버	Enable	Yes	v2
연계서버	Disable	No	v2
연계서버	Enable	Yes	v2
연계서버	Disable	No	v2
연계서버	Enable	Yes	v2
연계서버	Enable	Yes	v2
연계서버	Enable	Yes	v2
연계서버	Enable	Yes	v2
연계서버	Enable	Yes	v2
연계서버	Enable	Yes	v2
연계서버	Enable	Yes	v2
연계서버	Enable	Yes	v2
연계서버	Enable	Yes	v2
연계서버	Enable	Yes	v2
연계서버	Enable	Yes	v2

장비이름	연계서버	표현규격	YARA
생성자	651608dc-32f0-406a-98bf-9c1ce89bc008	최종 수정일	2020-01-09 10:36:55
상태	Enable	다계층 지원여부	Yes
수신버전	v2	배포버전	v10
룰 아이디	yara_pkg_1496300906		
룰 이름	yara_pkg_1496300906		
weight	100	생성일	2017-06-01 16:10:11
설명	tty		
strings	Salert_tag = "foobar_20170601161011"		
condition	Salert_tag		

# TARGOS 동작 프로세스



## TARGOS 위협정보 관리 체계 동작

1. 관리기관에 탐지규칙 요청 및 수신
2. 샌드박스 및 하위 기관 TARGOS에 규칙 배포
3. 샌드박스에서 탐지결과 수집
4. 상위 기관으로 탐지결과 전송
5. 관리기관의 탐지결과 검증 업데이트

# TARGOS 구성도

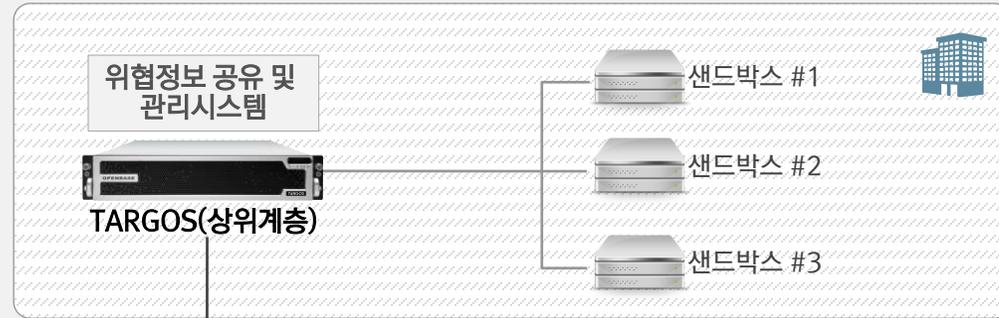
## ▶▶ 관리기관



위협 탐지규칙

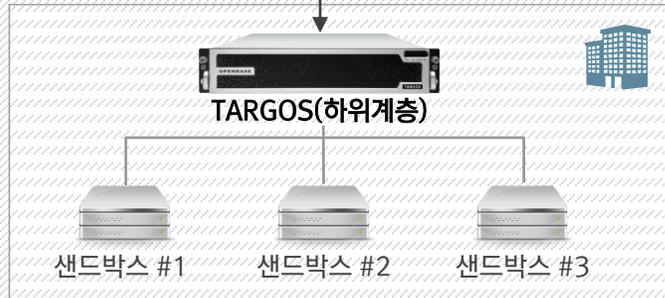
위협 탐지결과

## ▶▶ 도입기관

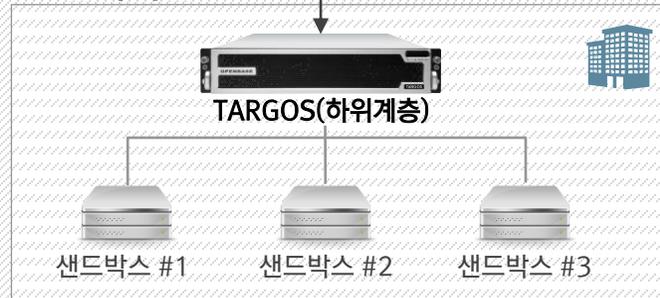


## 다계층 구성

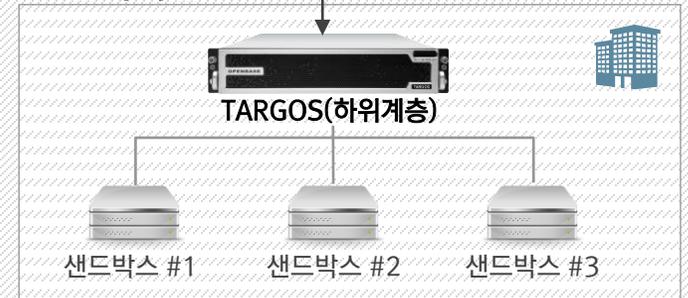
### ▶▶ 산하기관A



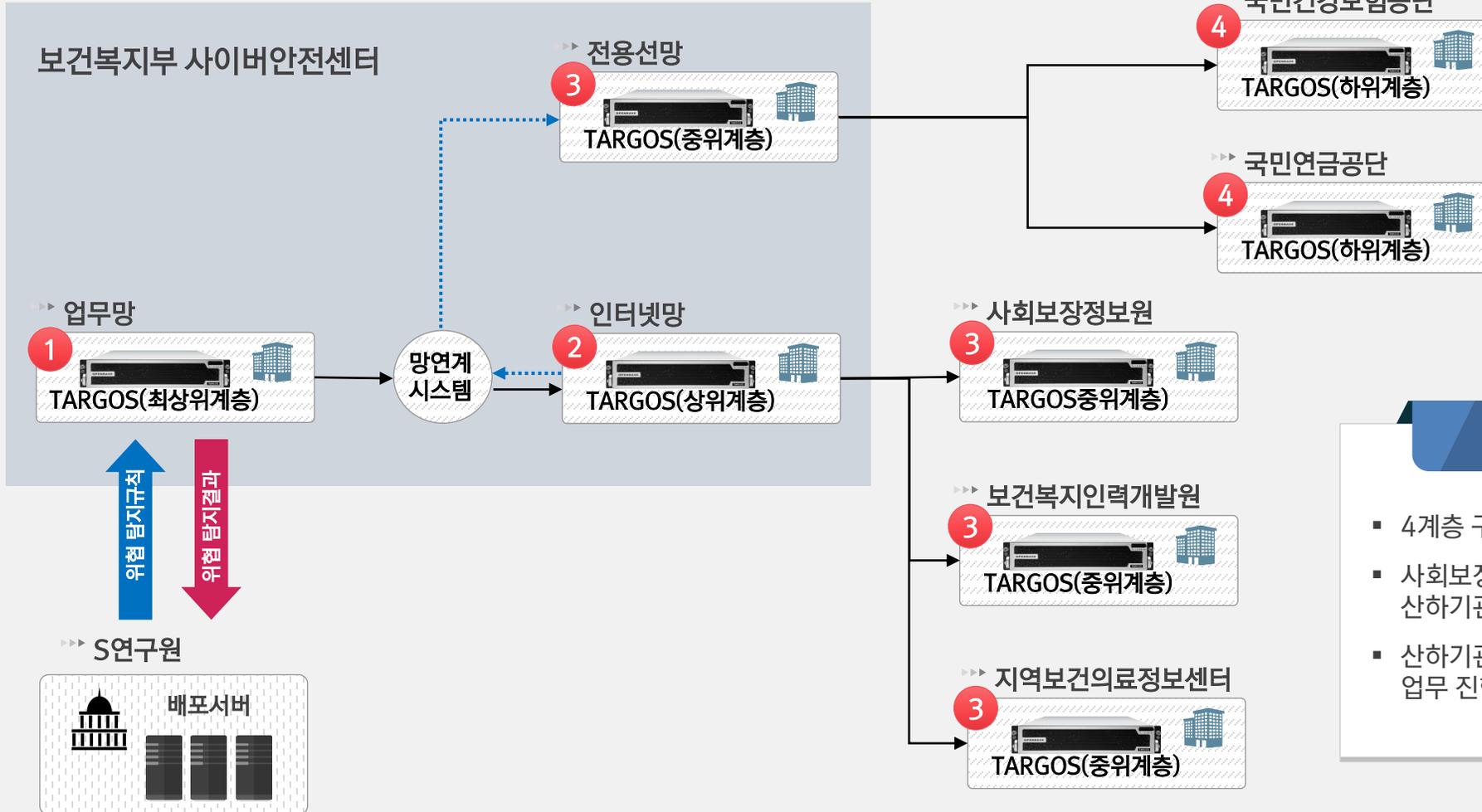
### ▶▶ 산하기관B



### ▶▶ 산하기관#



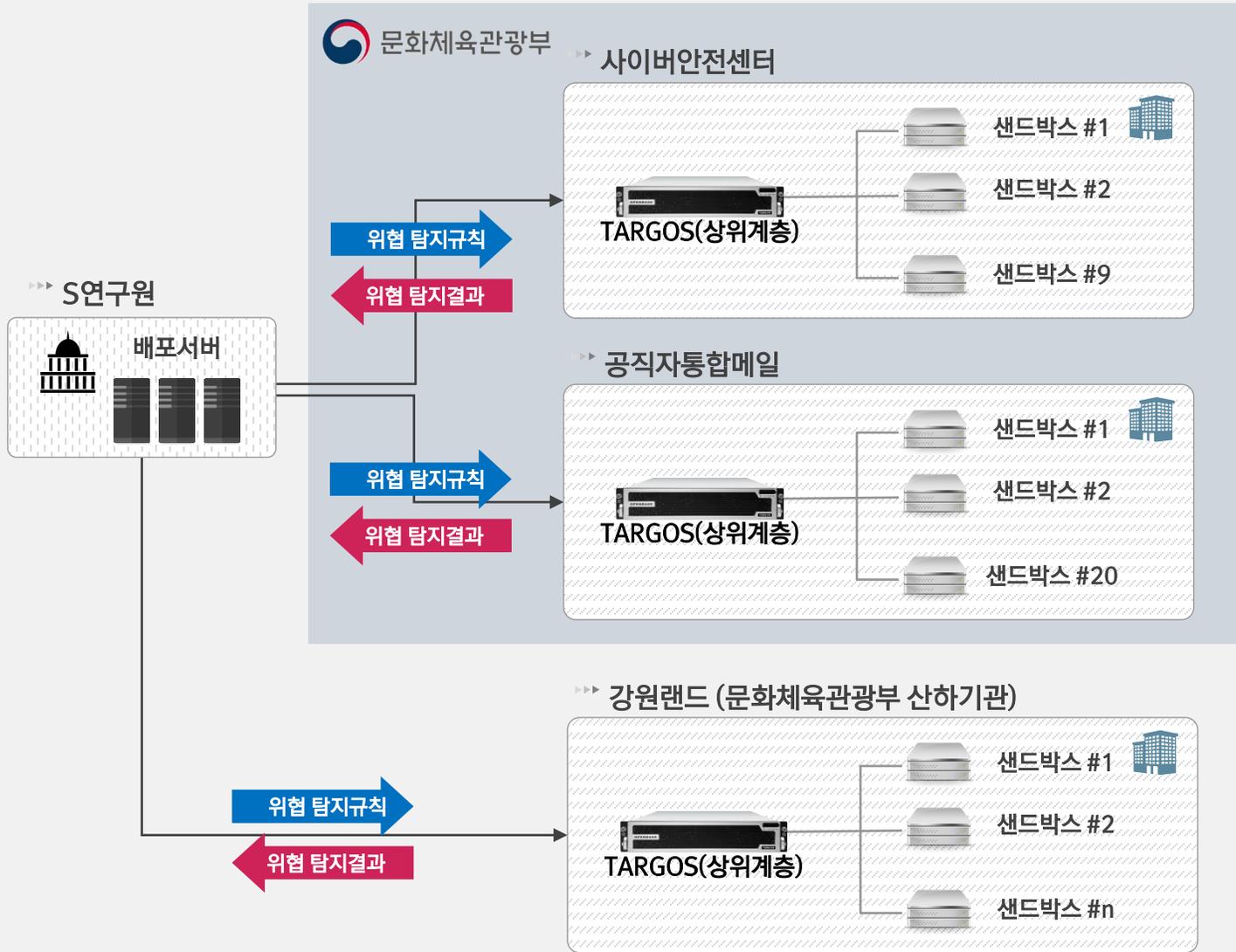
# TARGOS 운영 사례 - 사회보장정보원



### 운영 특징

- 4계층 구조
- 사회보장정보원 자체 탐지규칙 생성 및 산하기관에 배포
- 산하기관에서 수집된 악성파일을 관제팀에서 분석 업무 진행

# TARGOS 운영 사례 - 문화체육관광부



## 운영 특징

### 사이버안전센터

- 산하기관별 다양한 샌드박스 사용
- 2차 분석을 활용하여 위협탐지 결과 재 검증
- TARGOS에서 각 샌드박스에 탐지규칙 일괄 배포
- 통계 및 탐지결과를 관제 업무에 활용

### 공직자통합메일

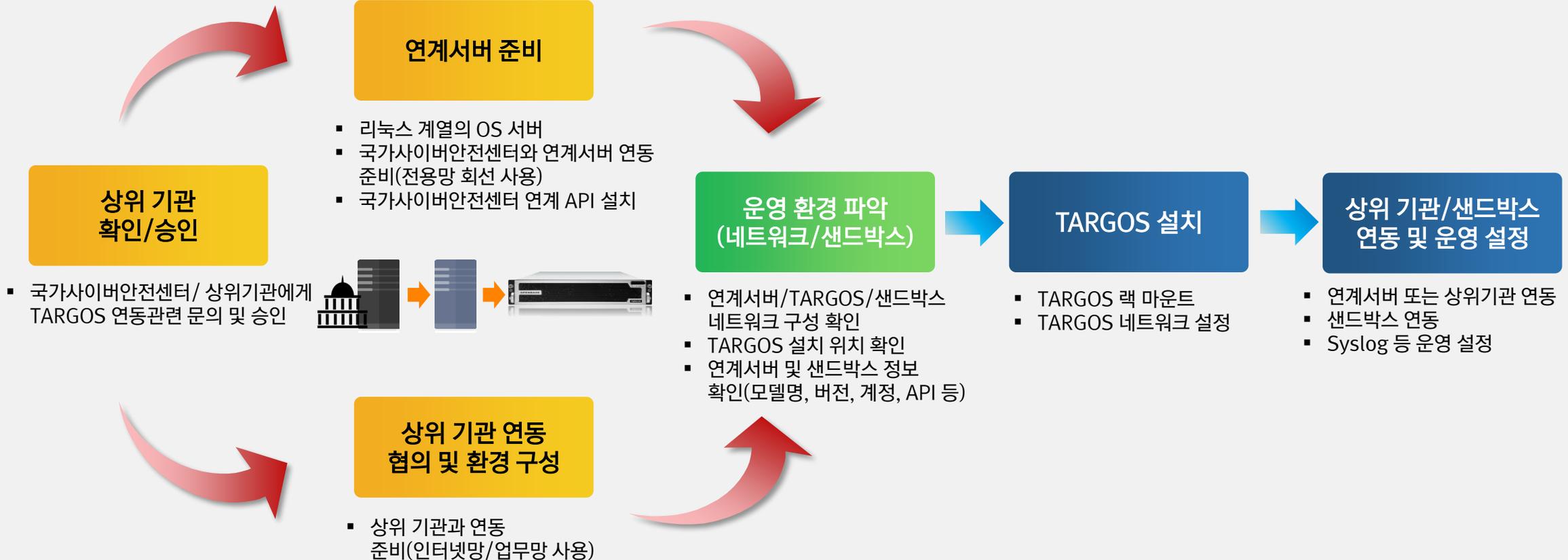
- 산하기관별 동일한 제조사의 샌드박스 20대 연동
- 다수의 샌드박스에 탐지규칙 일괄 배포
- 통계 및 탐지결과를 관제 업무에 활용

### 강원랜드

- 문화체육관광부 산하기관
- 담당자 요청에 따라 단층구조로 구축한 사례

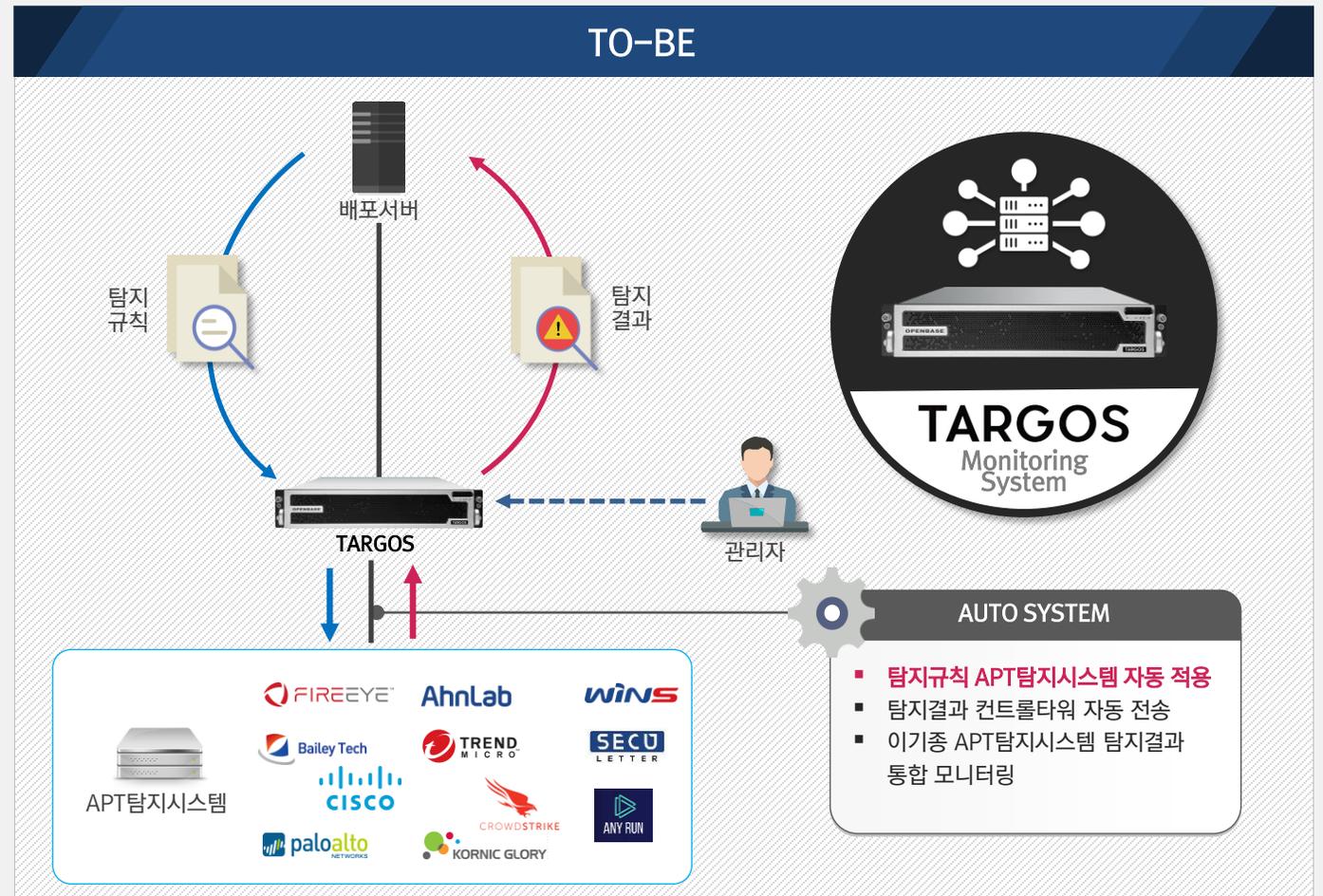
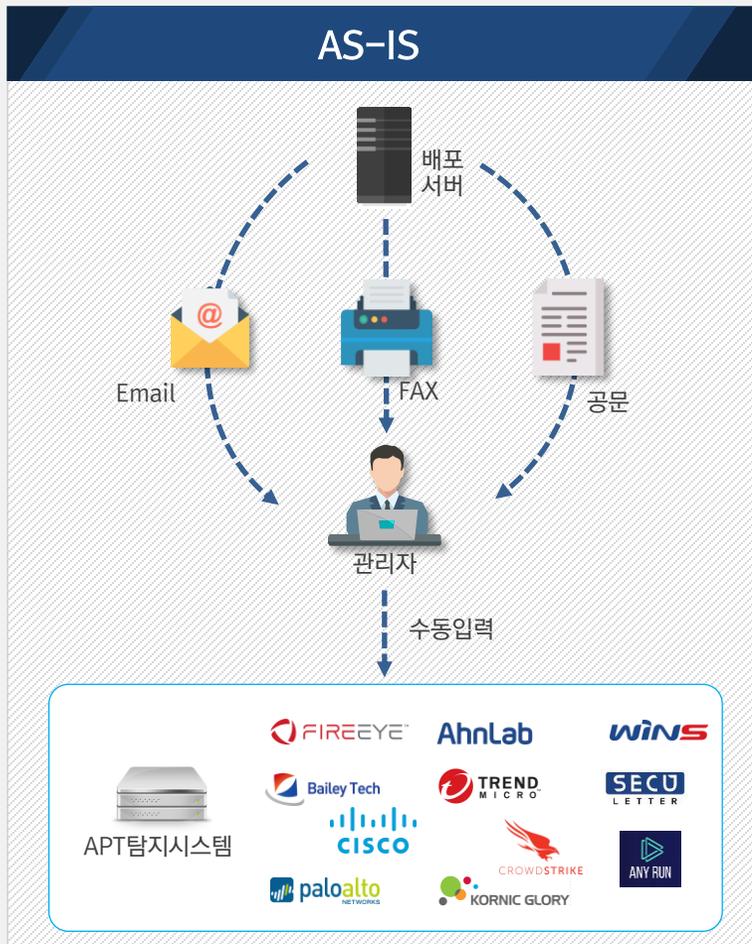
# TARGOS 구축 절차

❖ 국가사이버안전센터 또는 상위기관과의 사전 연동 협의 후, TARGOS 구축 프로세스 진행



# 도입 효과(1/2)

❖ 탐지규칙 자동적용과 모니터링을 통해 운영 효율 향상



## 도입 효과(2/2)

효율적인  
보안 위협  
대응

전문 기관의  
위협정보  
공유

변화하는  
보안 위협의  
대응

- 체계적이고 표준화된 위협정보를 공유하고 이를 기존 보안 장비에 적용
- 컨트롤타워와의 유기적인 연동으로 보안 위협 발생 시 빠른 대응 가능
- 컨트롤 타워에서 인지한 새로운 위협에 대해 신속한 대응 체계 유지

감사합니다.