위협정보 공유 및 관리 시스템
TARGOS

2023.03

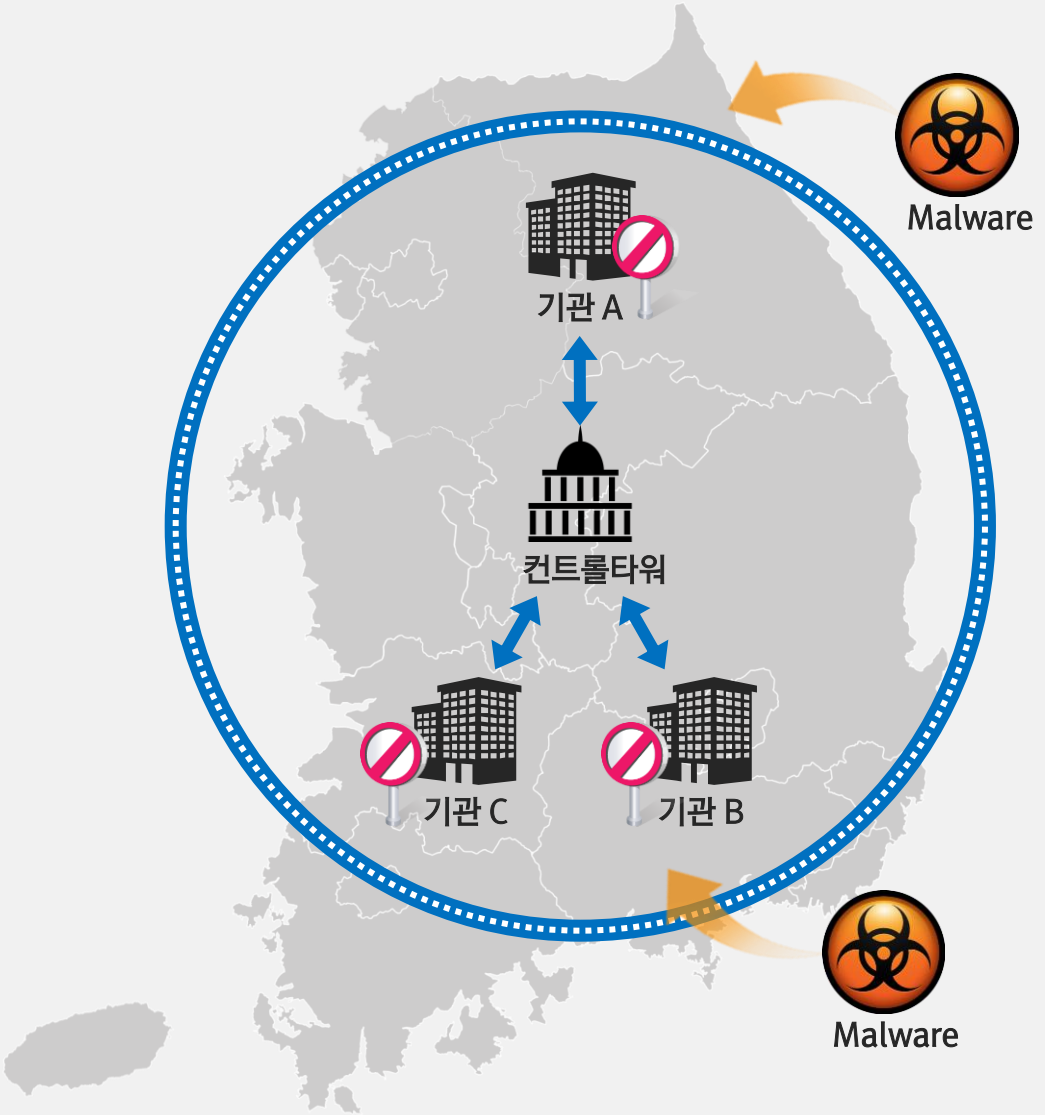
오픈베이스 보안기술본부

openbase
where the intelligence works

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 관리 시스템 필요성

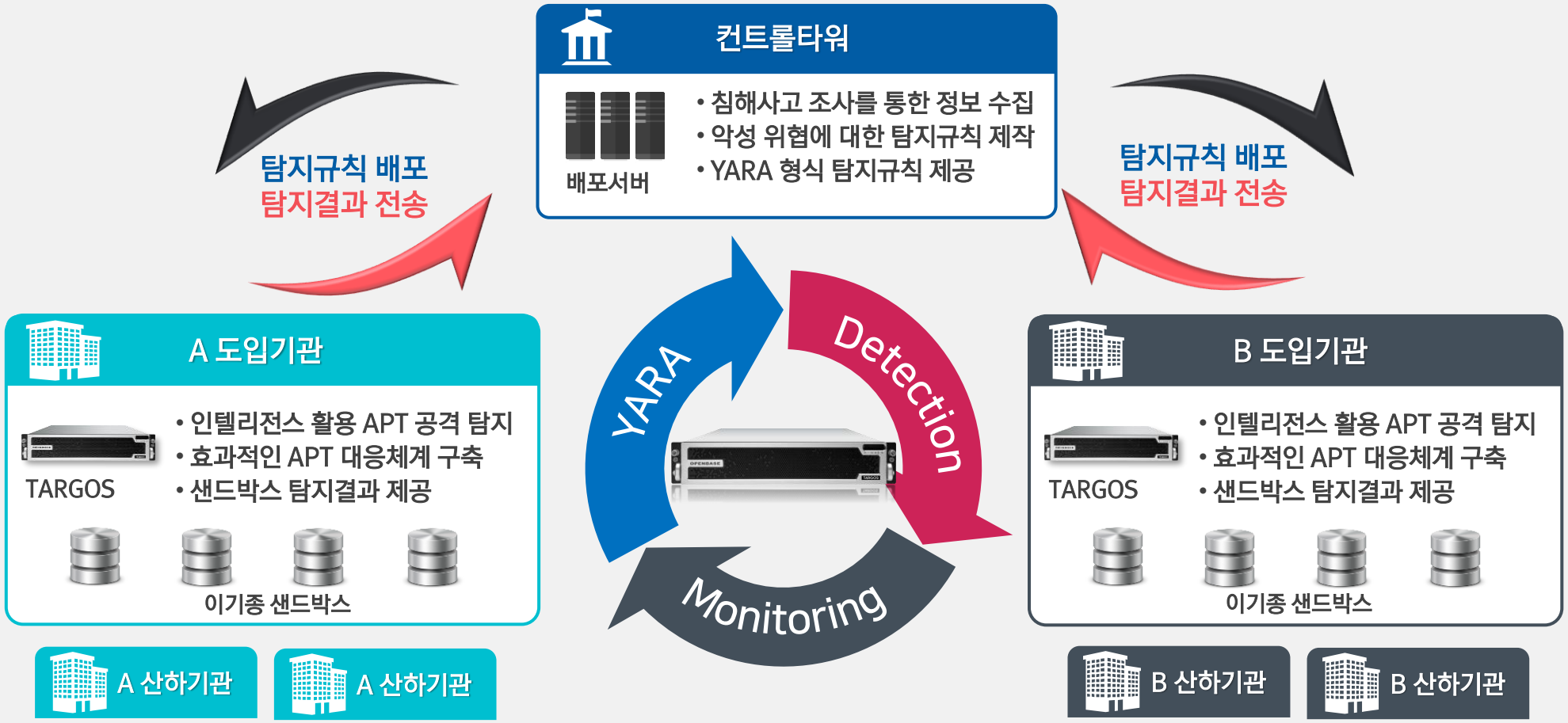
위협정보 공유 시 고려 사항

- 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

TARGOS 기관 도입 현황(21)

KPX 전력거래소 POWER EXCHANGE
한국전력공사 KOREA ELECTRIC POWER CORPORATION
KWP 한국서부발전|주| KOREA WESTERN POWER CO., Ltd.
보건복지부
KPFIS 한국재정정보원 Korea Public Finance Information Service
한국보건복지인력개발원
SSiS 사회보장정보원 SOCIAL SECURITY INFORMATION SERVICE
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	별도협의	5	10
	다계층 연동 대수	별도협의	10	20
	탐지 이벤트 처리 성능	별도협의	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

TAXII
STIX
CybOX

특징

- 다양한 APT탐지시스템 연동
- 다계층 구성 지원
- 모니터링 통계 데이터 제공
- 빅데이터 플랫폼 기술 적용

TARGOS 주요 기능

탐지규칙 수신 및 배포

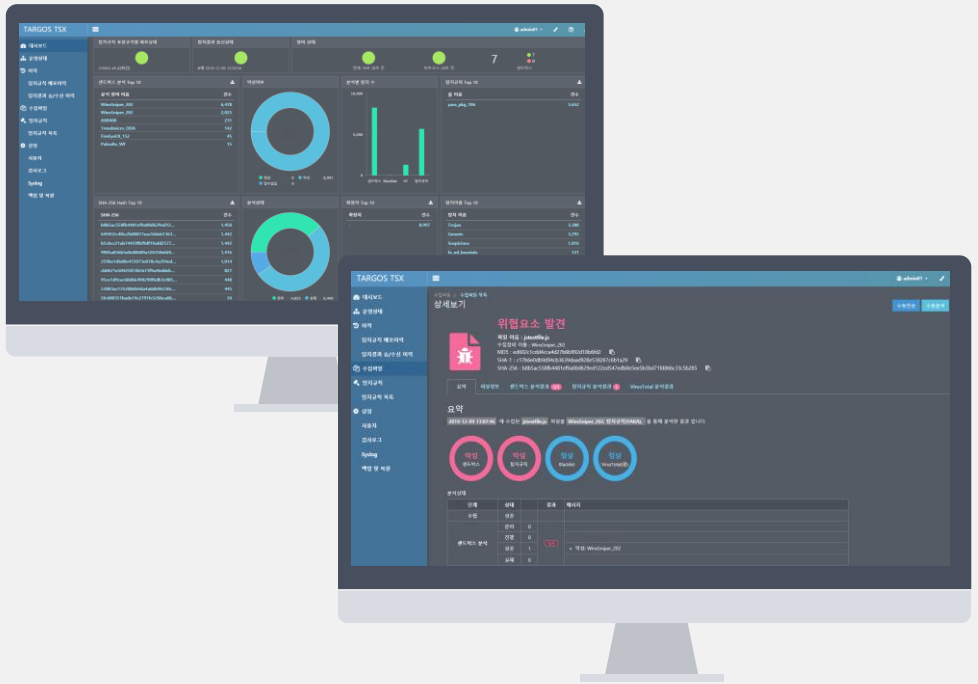
- 배포기관(상위기관) → TARGOS → 샌드박스
- 배포기관으로부터 탐지규칙 자동 동기화 및 샌드박스에 탐지규칙 배포

탐지결과 수집 및 송신

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

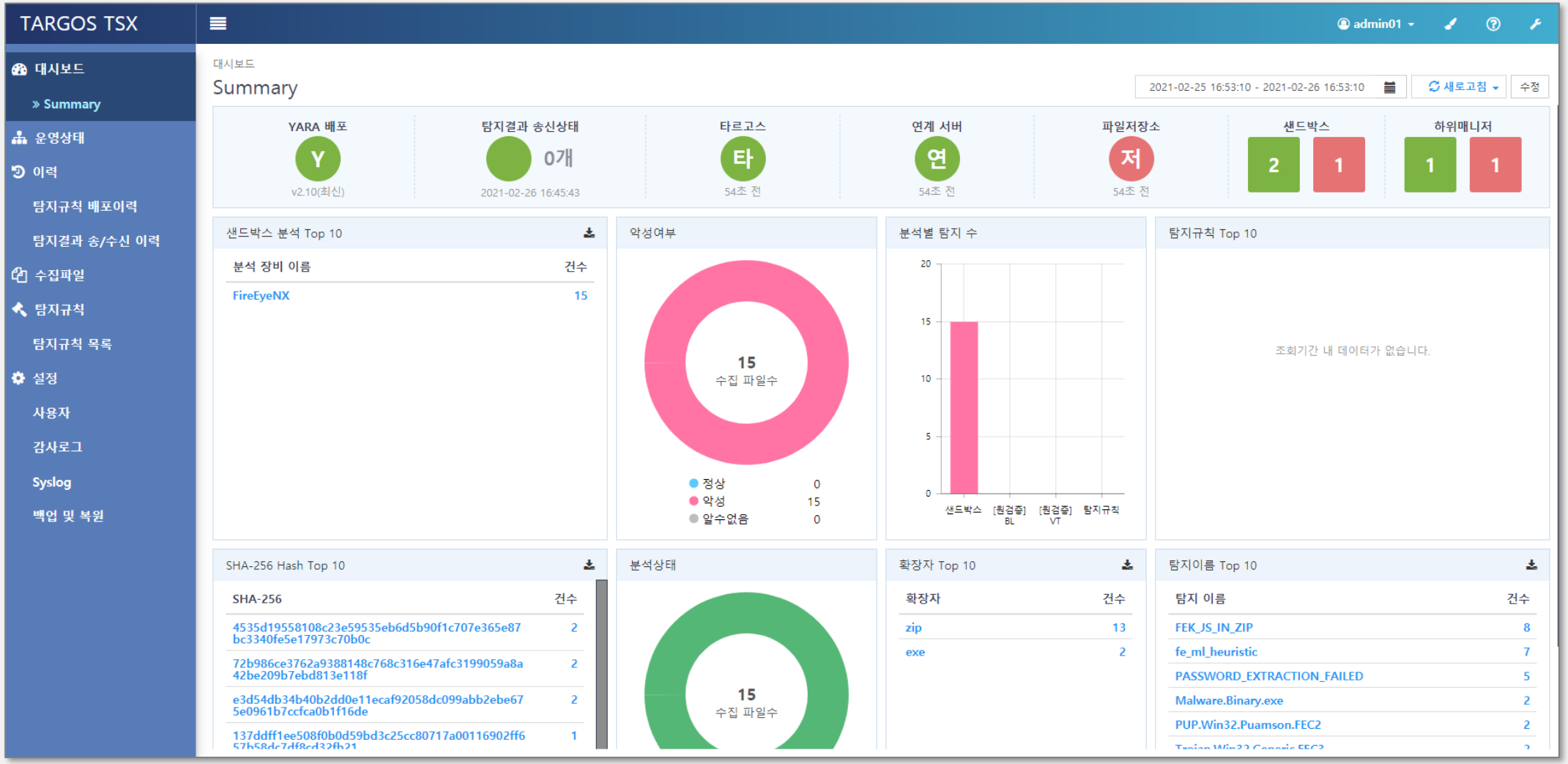
연결장비 상태 및 탐지결과 모니터링

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



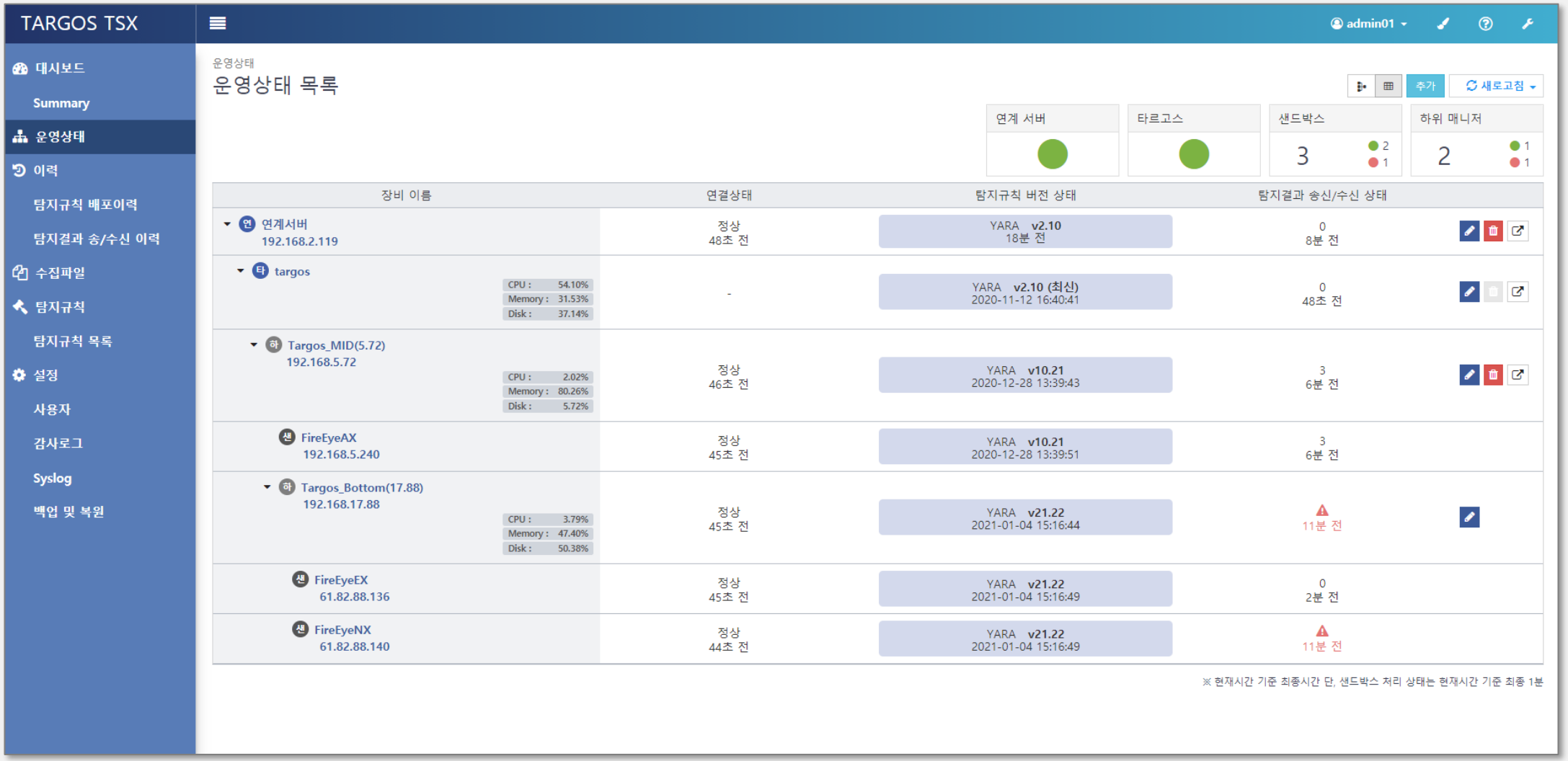
TARGOS 주요 화면 – 대시보드

❖ 장비 상태 및 데이터 수집 현황을 파악할 수 있는 대시보드 제공



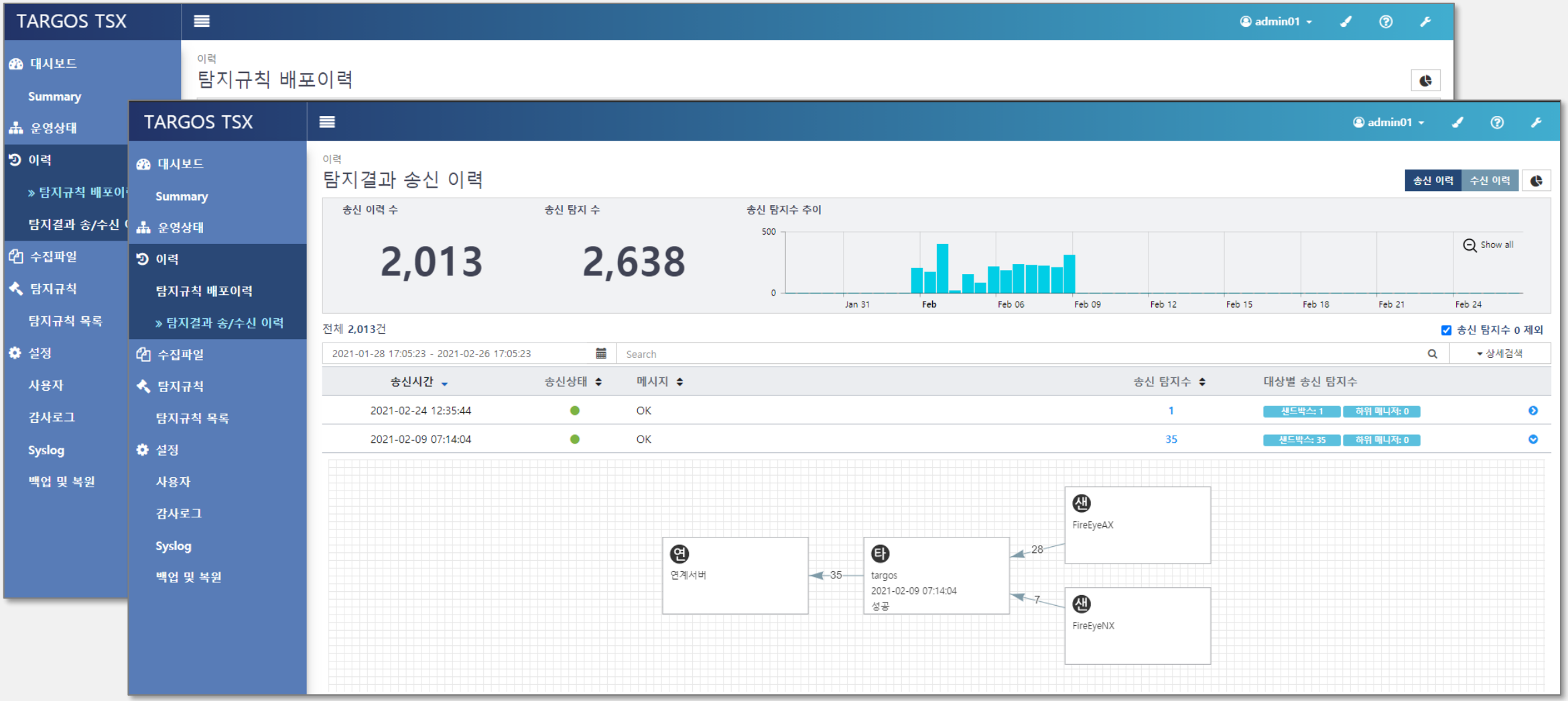
TARGOS 주요 화면 – 운영상태

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



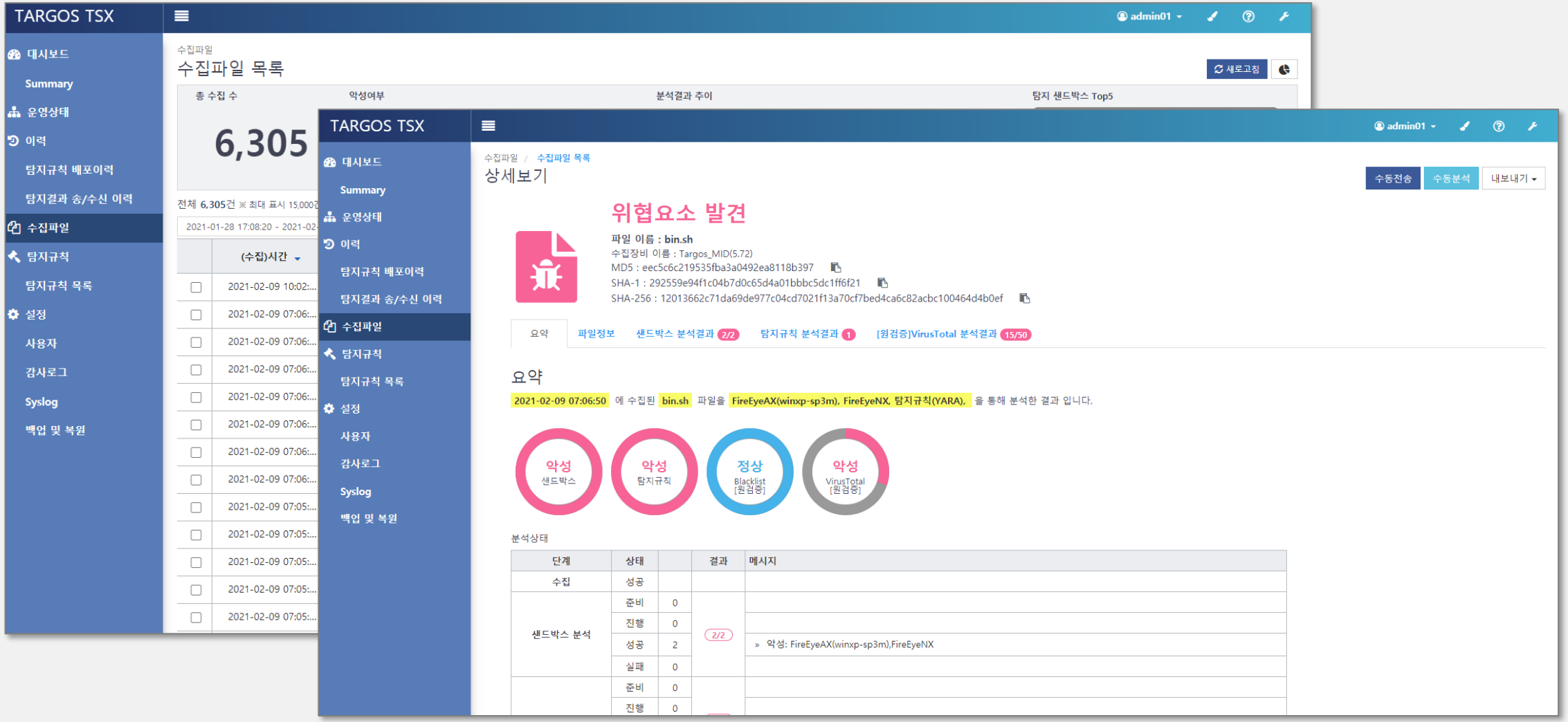
TARGOS 주요 화면 – 탐지규칙 배포 및 탐지결과 송신 이력

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



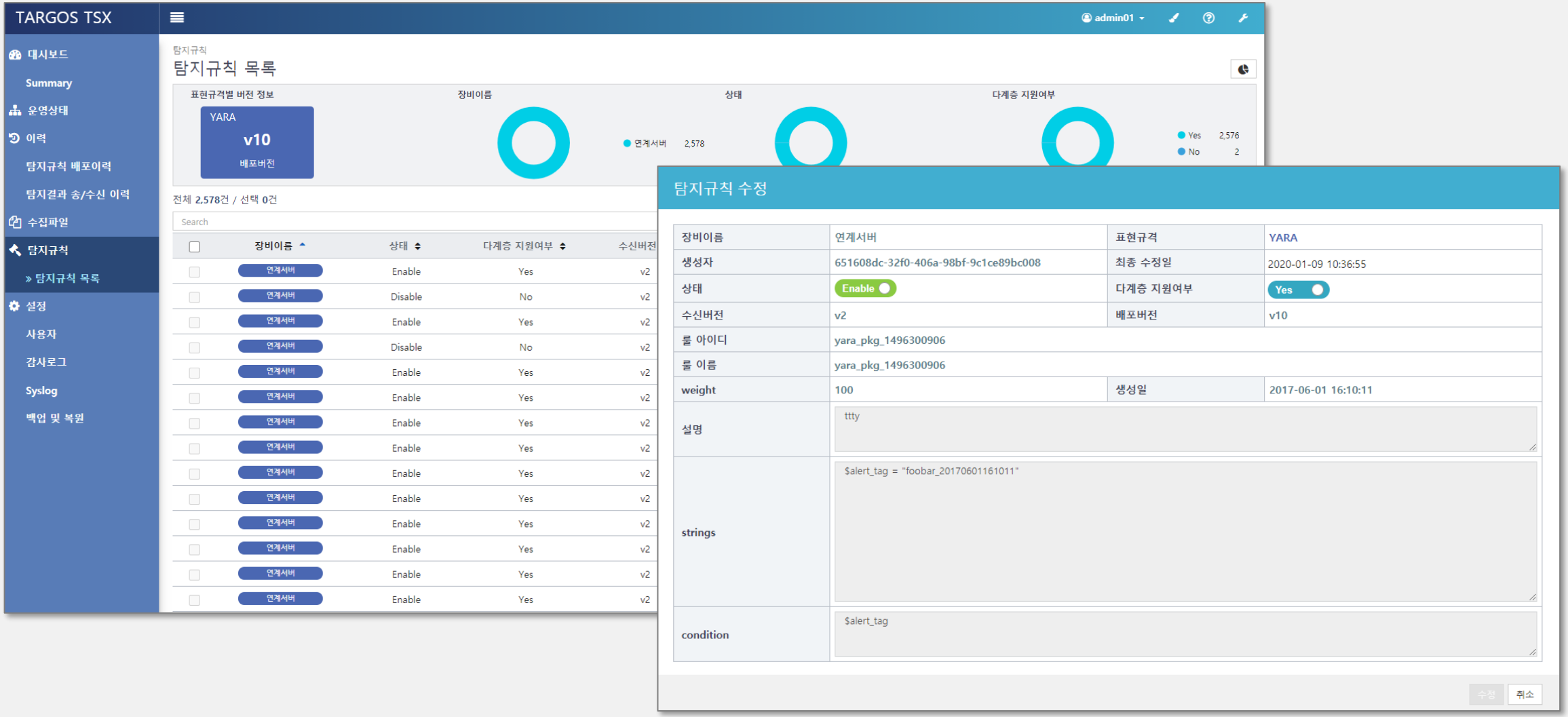
TARGOS 주요 화면 – 수집 파일

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

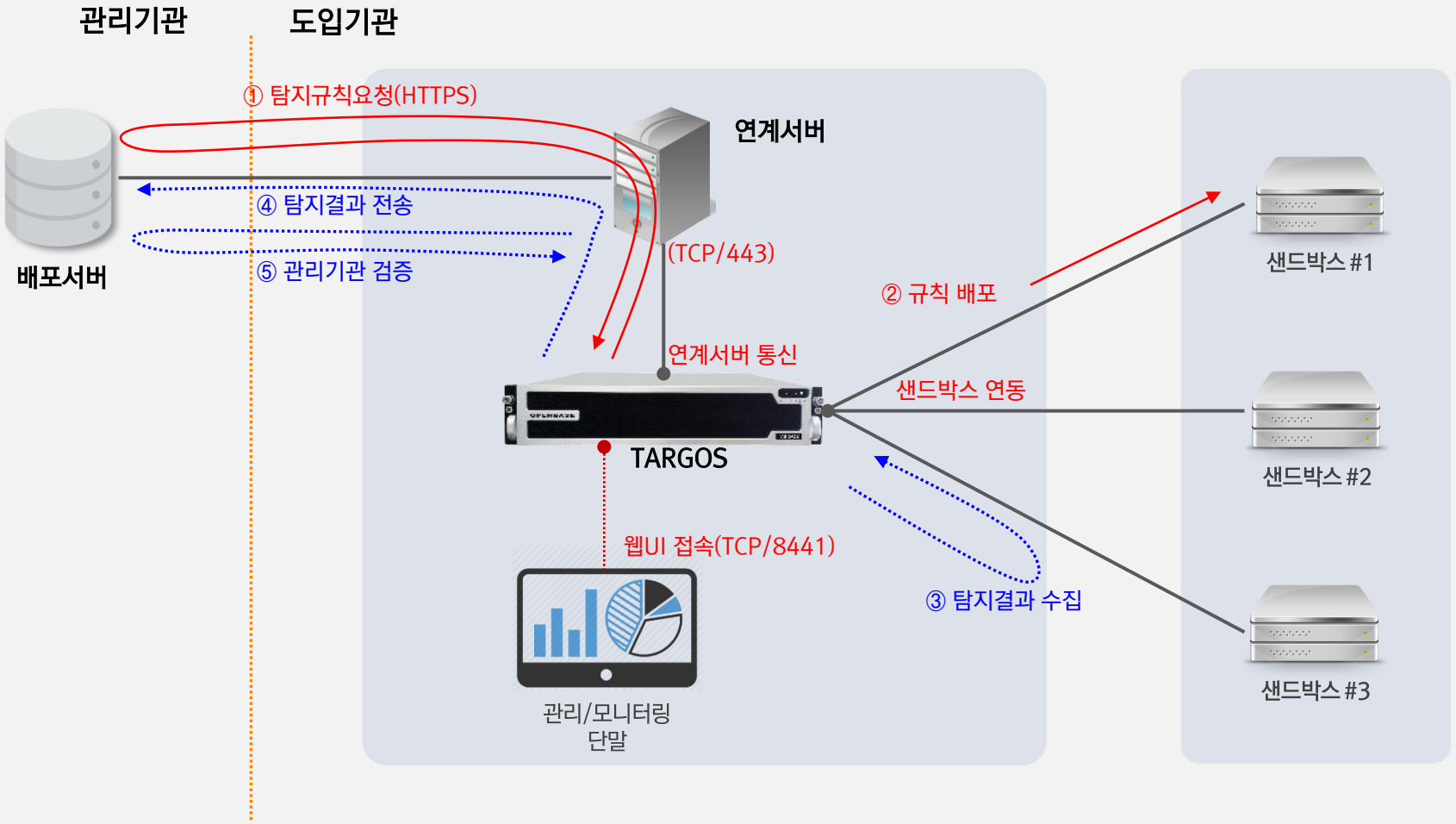


TARGOS 주요 화면 – 탐지규칙 목록

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



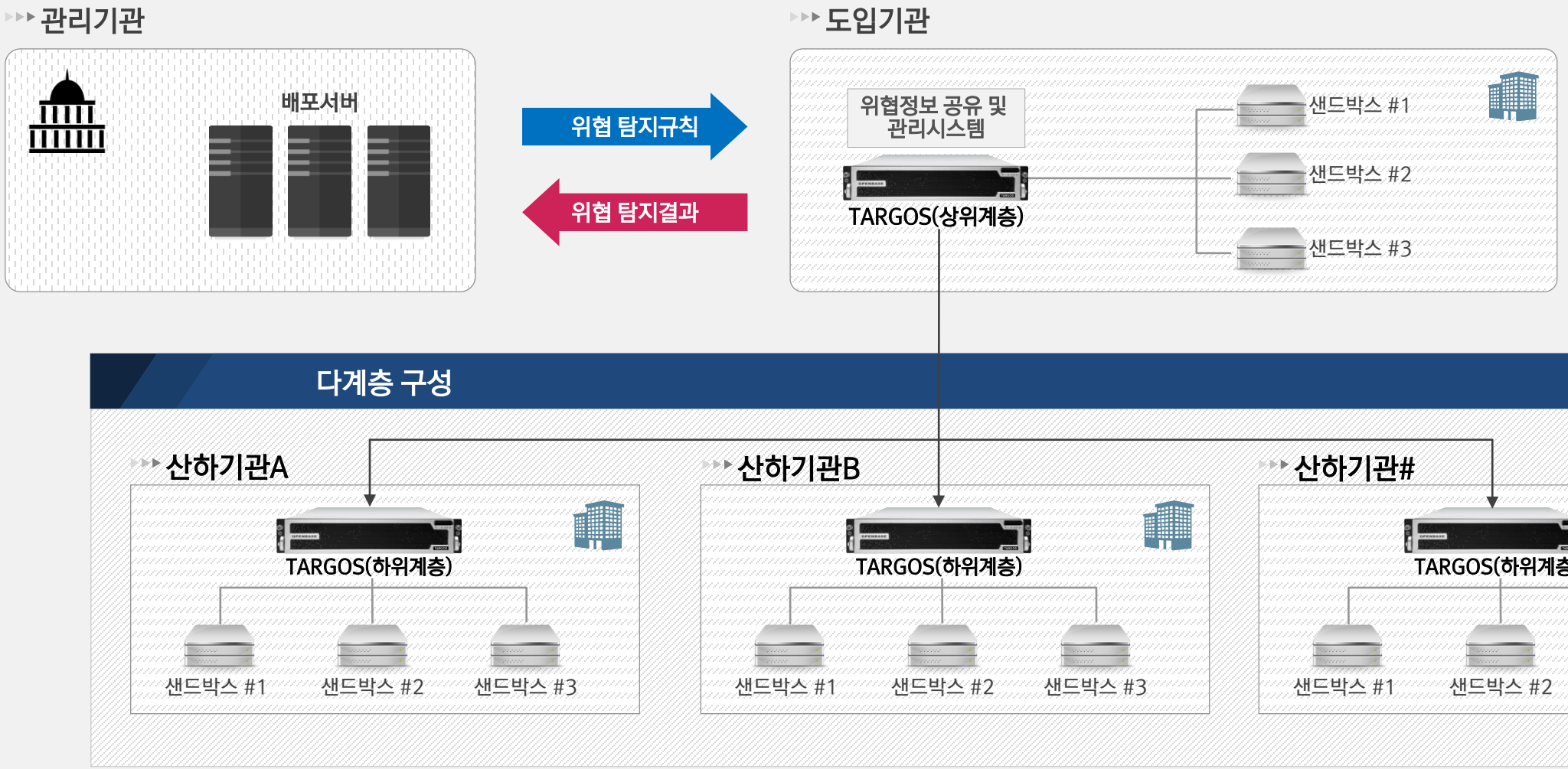
TARGOS 동작 프로세스



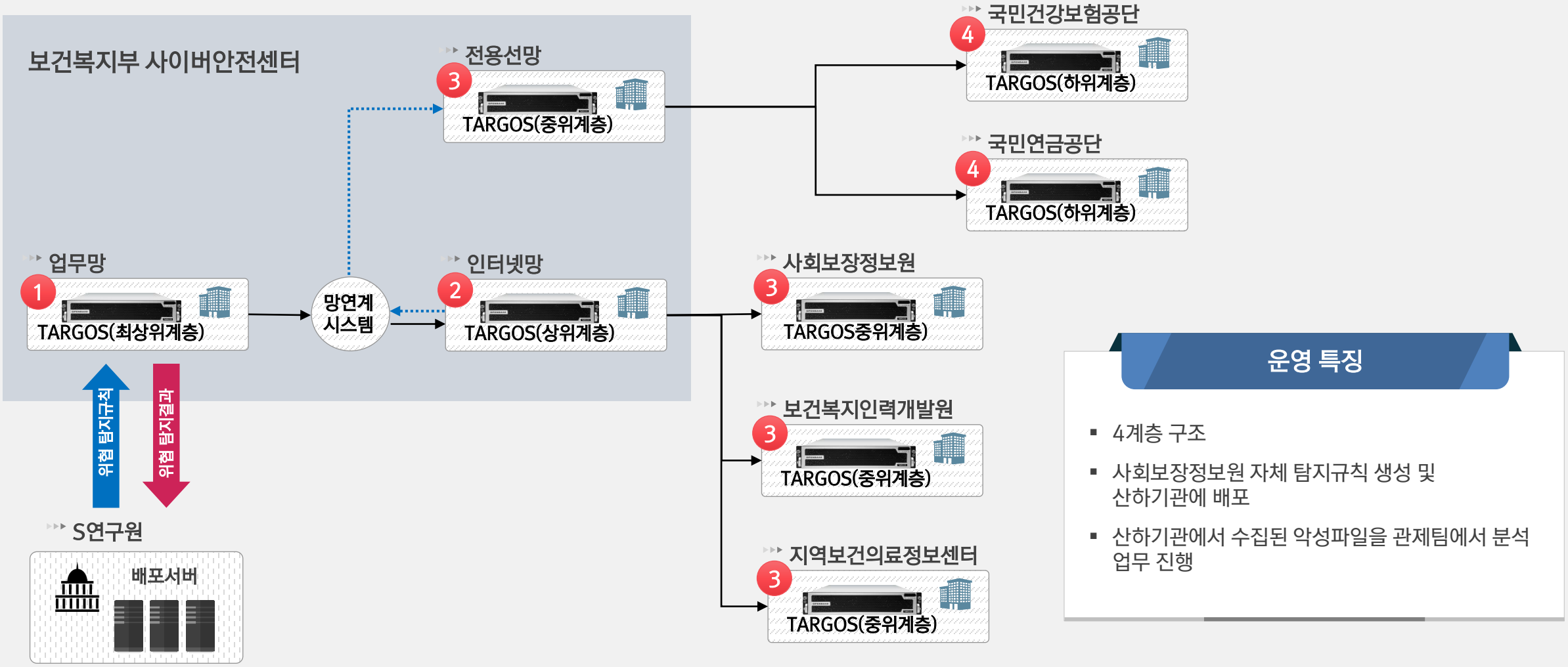
TARGOS 위협정보 관리 체계 동작

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
배포서버
위협 탐지규칙
위협 탐지결과
도입기관
위협정보 공유 및
관리시스템
TARGOS(상위계층)
샌드박스 #1
샌드박스 #2
샌드박스 #3
다계층 구성
산하기관A
TARGOS(하위계층)
샌드박스 #1
샌드박스 #2
샌드박스 #3
산하기관B
TARGOS(하위계층)
샌드박스 #1
샌드박스 #2
샌드박스 #3
산하기관#
TARGOS(하위계층)
샌드박스 #1
샌드박스 #2
샌드박스 #3

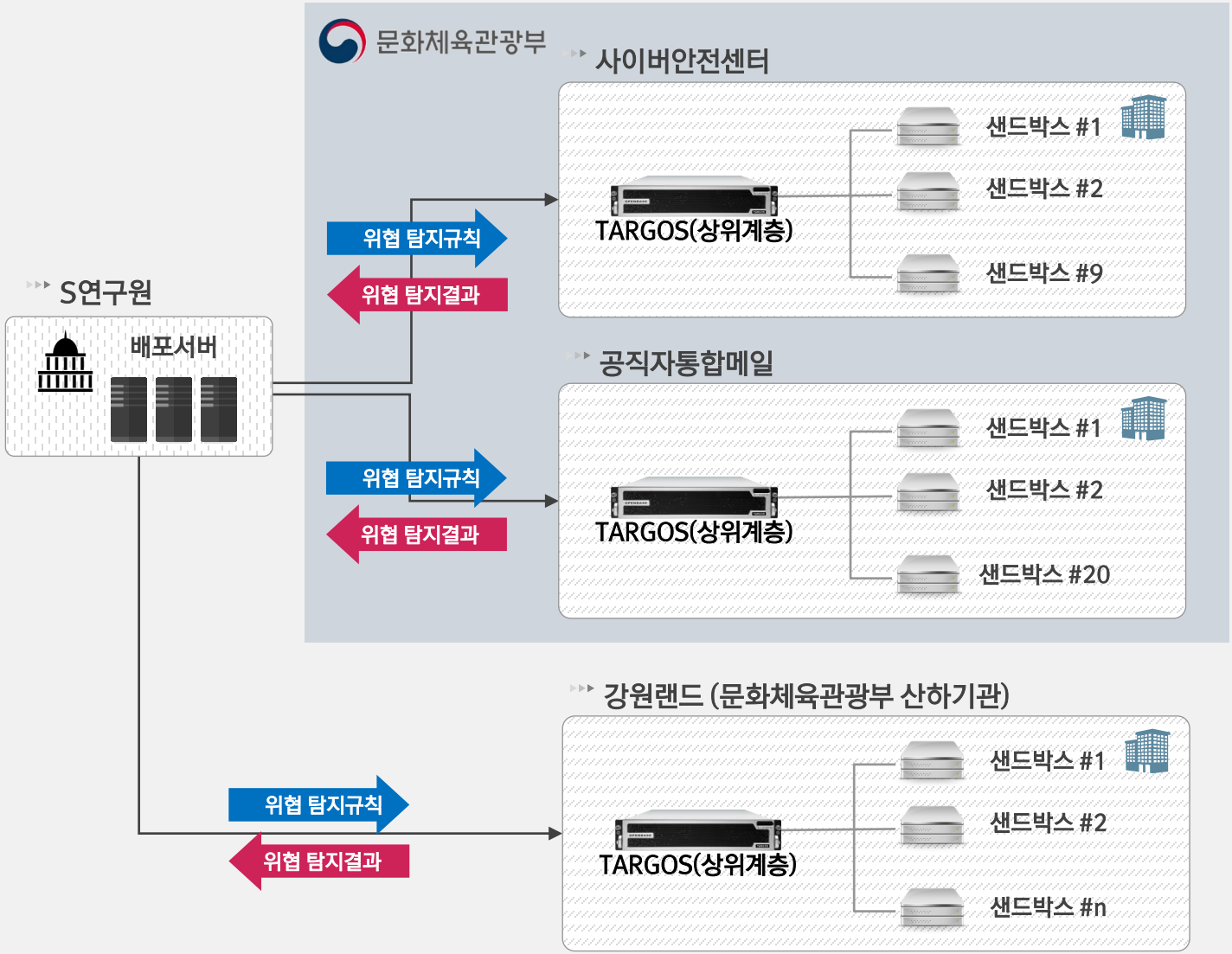
TARGOS 운영 사례 – 사회보장정보원



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

국가사이버안전센터(상위기관) & 고객사 | **고객사 & 오픈베이스** | **오픈베이스**

상위 기관 확인/승인

- 국가사이버안전센터/ 상위기관에게 TARGOS 연동관련 문의 및 승인

연계서버 준비

- 리눅스 계열의 OS 서버
- 국가사이버안전센터와 연계서버 연동 준비(전용망 회선 사용)
- 국가사이버안전센터 연계 API 설치

상위 기관 연동 협의 및 환경 구성

- 상위 기관과 연동 준비(인터넷망/업무망 사용)

운영 환경 파악 (네트워크/샌드박스)

- 연계서버/TARGOS/샌드박스 네트워크 구성 확인
- TARGOS 설치 위치 확인
- 연계서버 및 샌드박스 정보 확인(모델명, 버전, 계정, API 등)

TARGOS 설치

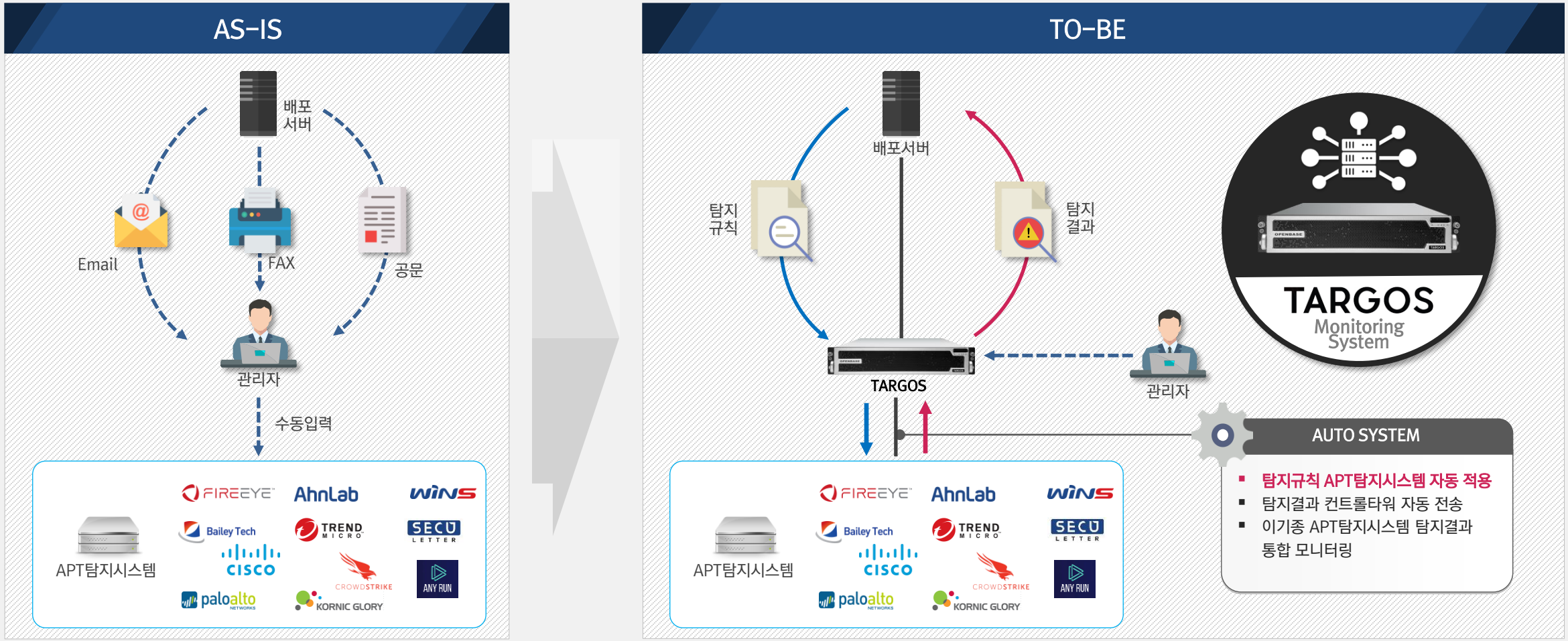
- TARGOS 랙 마운트
- TARGOS 네트워크 설정

상위 기관/샌드박스 연동 및 운영 설정

- 연계서버 또는 상위기관 연동
- 샌드박스 연동
- Syslog 등 운영 설정

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.

openbase
where the intelligence works