
NET
ARGOS
제로트러스트를 구현하는 네트워크 보안 솔루션
넷아르고스
ABYSS

NET ARGOS

01. 개요 : 사이버 공격의 증가

금융권을 대상으로 한 지속적인 사이버 공격

금융

매일 600건씩 사이버 공격 국내 은행, 대체 왜?

Editor. 김준철 기자 | 입력 2022.02.16 08:53 | 댓글

급증하는 금융권 사이버 공격...보안 투자&공조·협력 강화해야

이성노 기자 | 입력 2024.02.25 21:17

올 상반기 금융권 사이버 공격 가장 많아…비트코인 노렸다

발행일 : 2024-07-02 12:00 지면 : 2024-07-03 11면

국제

日 곳곳 사이버 테러…항공·은행 혼란

이승훈 기자 thoth@mk.co.kr

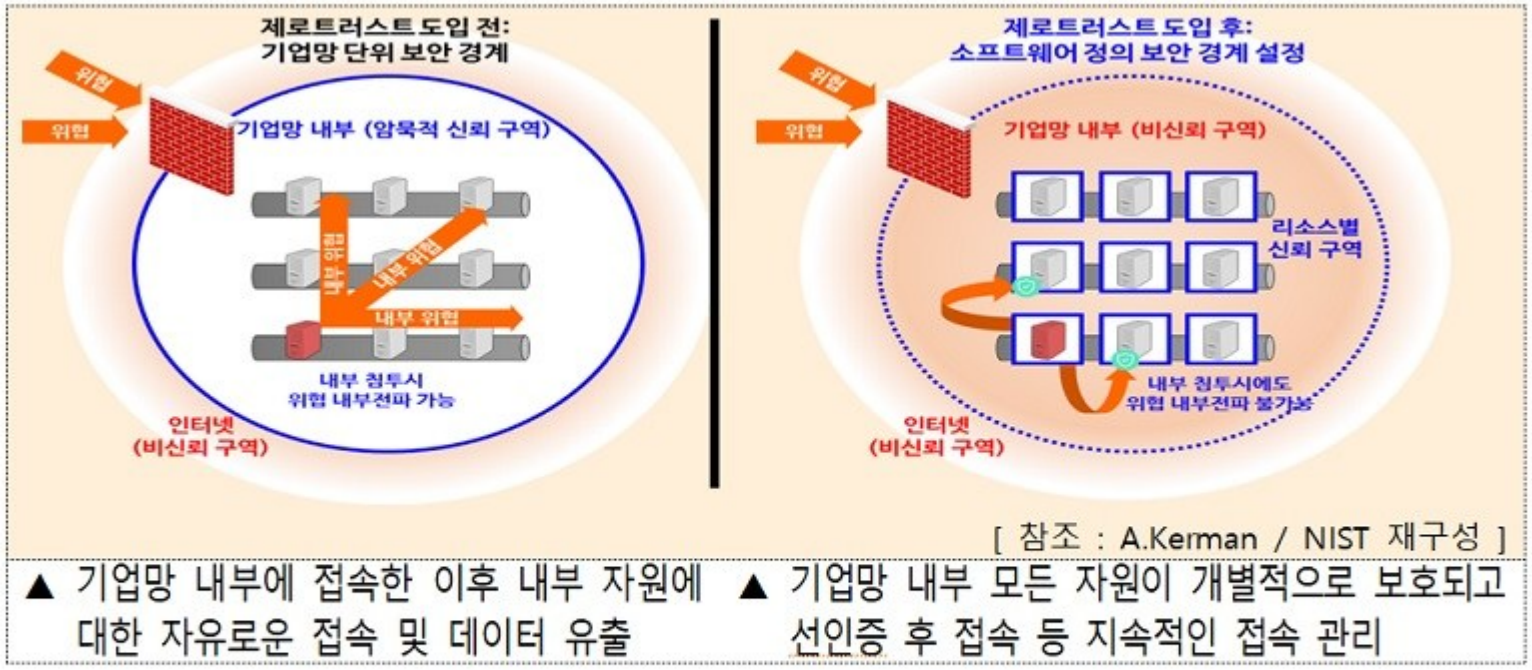
입력 : 2025-02-04 17:24:59

연말연시 피해 158건 달해

01. 개요 : 보안의 패러다임 변화 (제로트러스트)

"보안의 경계를 신뢰하지 않는다, 모든 대상을 확인하고 검증해야 한다."

< 기존 경계기반 보안과 제로트러스트 개념 비교 >



[참조 : A.Kerman / NIST 재구성]

▲ 기업망 내부에 접속한 이후 내부 자원에 대한 자유로운 접속 및 데이터 유출

▲ 기업망 내부 모든 자원이 개별적으로 보호되고 선인증 후 접속 등 지속적인 접속 관리

※ 제로트러스트는 ①Enhanced Identity Governance, ②Micro-Segmentation, ③SW Defined Perimeter에 기반을 두며, 각각의 자원에 대한 접속요구에 **동적인증**을 통한 **선인증 후 접속**, 이후에도 **가시성 확보**를 통한 **지속적 모니터링**으로 보안 수준을 높임

"송수신 데이터를 검사하고 또 검사해야 된다."

02. 제품 컨셉

네트워크 보안에서 제로트러스트의 의미는?

매일 신규 탐지/차단 정책을 추가할 때

이미 침투해 있지는 않을까?

새로운 보안 취약점이 공개 되었을 때

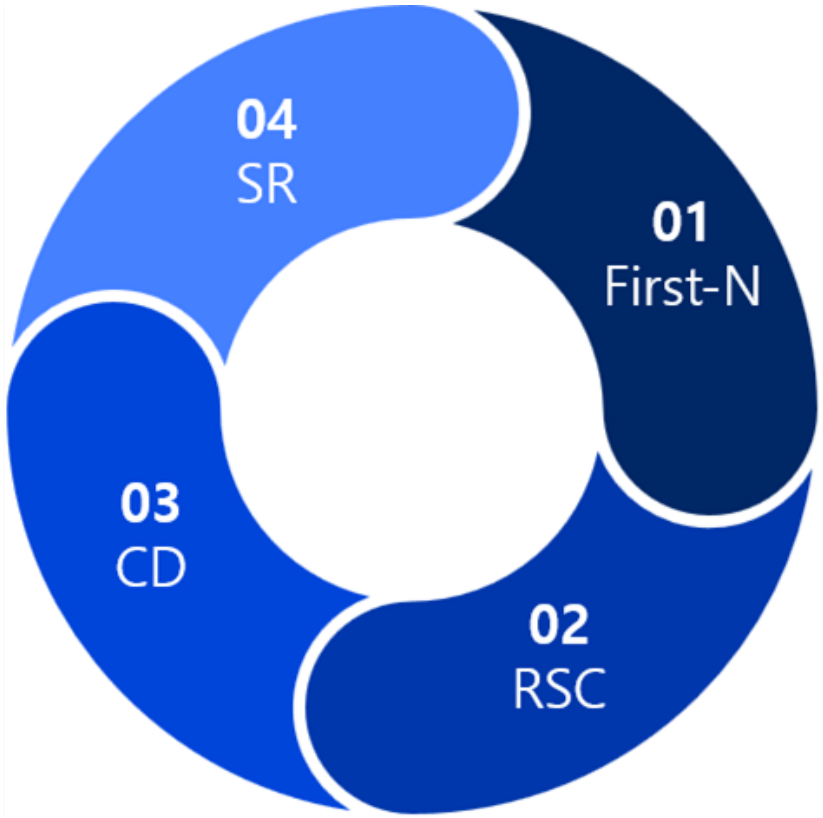
이곳에도 동일한 취약점이 있는 게 아닐까?

이상행위를 탐지했는데 분석할 데이터가 필요할 때

분석할 패킷을 최소 2~3개월 이상 저장해야 되지 않을까?

03. 핵심기능 : 회귀보안검사(검증 또 검증)

보안검사에 필요한 패킷만 저장하고 신규 TI가 배포될 때마다 저장된 패킷 재검사



01 장기 저장

응용별 First-N 패킷 저장(ZDR을 위한 최적화된 네트워크 트래픽 저장 기술)

02 재검사

1일 1회이상 주기적/자동적 회귀보안검사(Retroactive Security Check)

03 분석

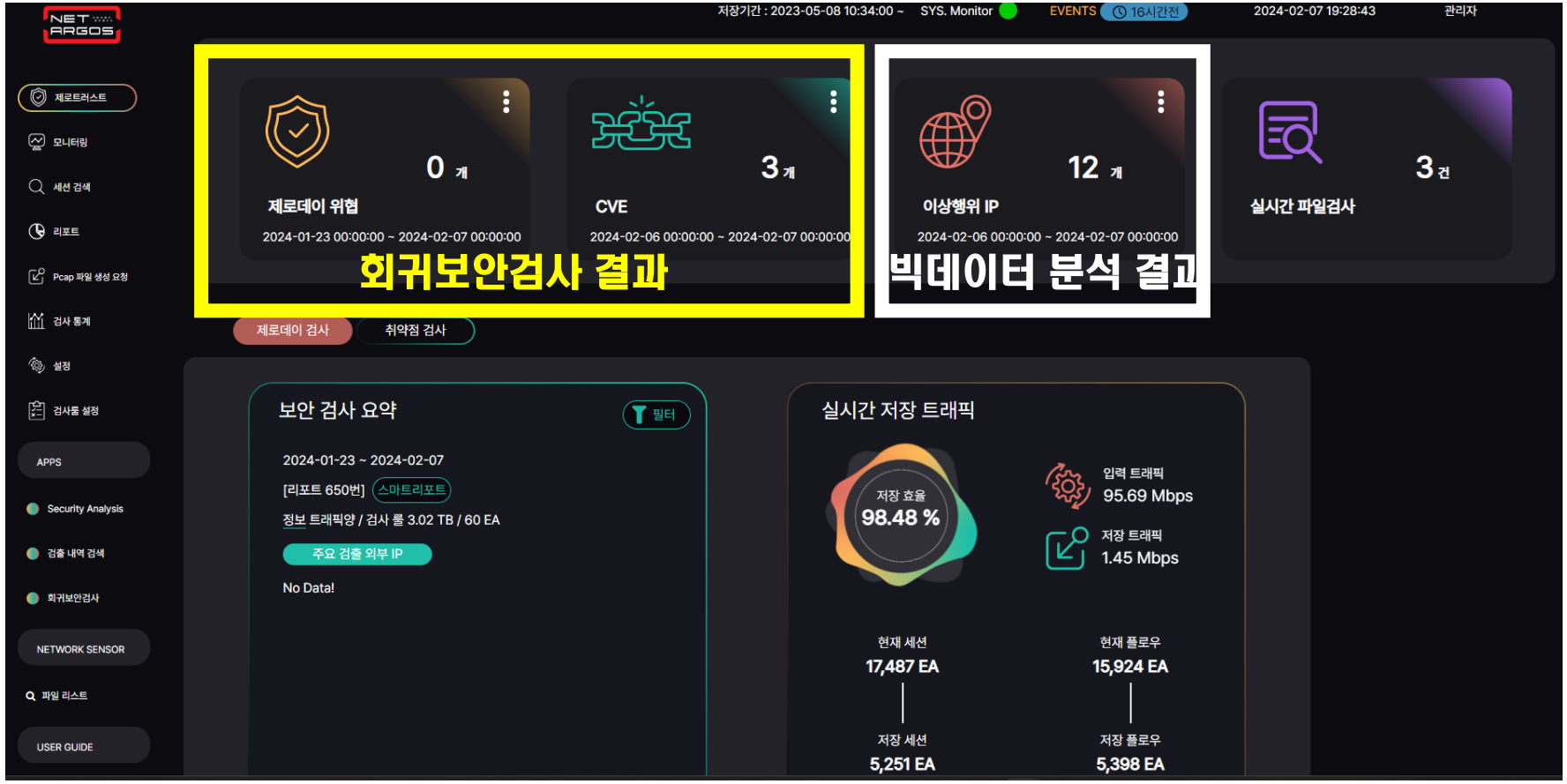
미탐 위협 후보군 추출(Candidate Detection) – AI / BigData 분석

04 보고

스마트 리포트(Smart Report) – 핵심 위협 / 위협 가시성 정보 제공

03. 핵심기능 : 회귀보안검사 & 이상행위 분석

- 회귀보안검사를 통한 **이미 침투에 성공한 위협 탐지, 취약점 검증**
- 빅데이터 분석을 통한 **이상행위 IP 탐지**



04. 넷아르고스 대응 영역

제로트러스트에 기반하여 알려지지 않은 위협 탐지

네트워크 보안 대응 체계		대응 솔루션	
N-Day	경계 보안 ▪ 보안 위협의 침해 발생 시에 TI 또는 IoC가 있음	Firewall, IPS, WAF EMS, SIEM, SOAR	
Zero-Day	제로데이 대응 ▪ 보안 위협의 침해 발생 시에 TI 또는 IoC가 없음	Threat Hunting	▪ Not Yet ▪ 이상행위탐지
		Retro Hunting	▪ Now ▪ 과거 재검사

05. 넷아르고스 활용

제로데이공격 탐지 솔루션

네트워크 취약점 진단 솔루션

네트워크 포렌식솔루션

(넷아르고스)

긴급보안이슈 점검 솔루션

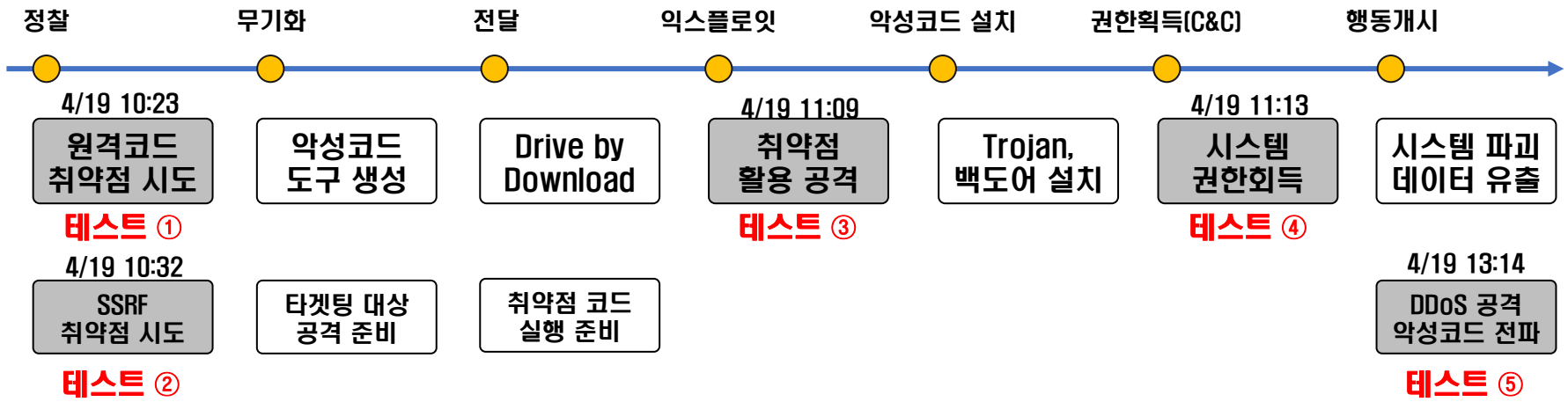
통신 트랙킹 툴

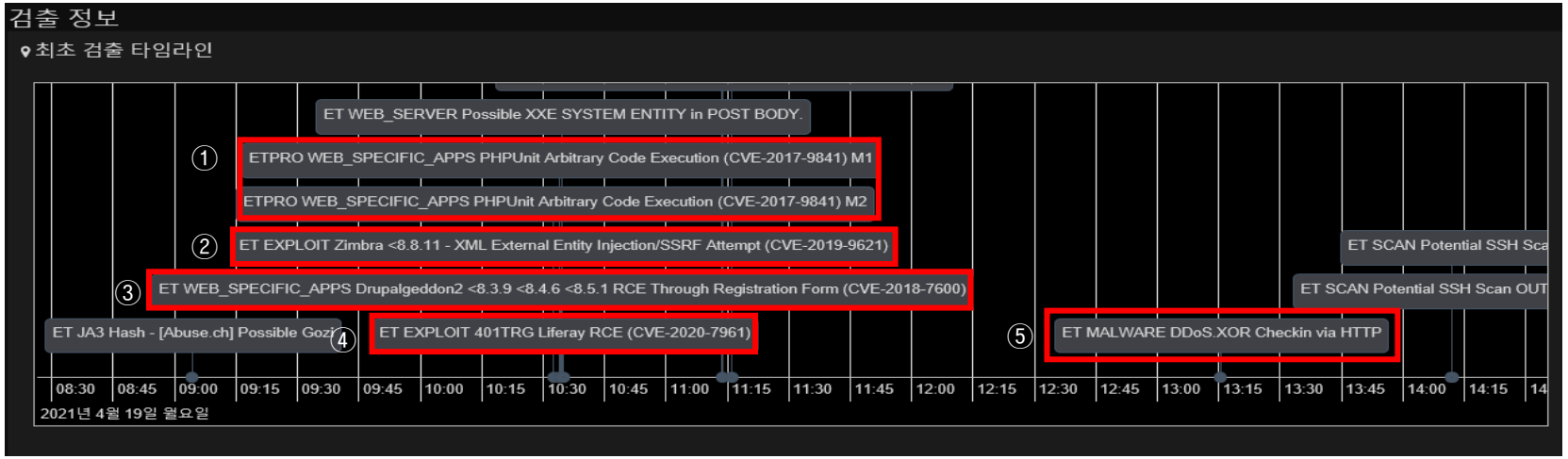
패킷 검색 툴

주요 기능	설명
제로데이공격 탐지 솔루션	이미 침투한 위협이 있는지 없는지 탐지
네트워크 취약점 진단 솔루션	네트워크 관리상 취약한 부분이 있는지 진단
네트워크 포렌식 솔루션	사이버 공격 또는 이상행위 분석을 위한 데이터 제공
긴급보안이슈 점검 솔루션	국내외 긴급 사이버 보안이슈 발생 시 침투여부 점검
패킷 검색 툴	특정패턴이 포함된 패킷을 검색
통신 트래픽 툴	과거 통신행위에 대한 데이터 제공

05. 넷아르고스 활용 : 제로데이 공격 탐지 솔루션

신규 TI를 이용한 회귀보안검사 실시(이미 침투한 위협 탐지)

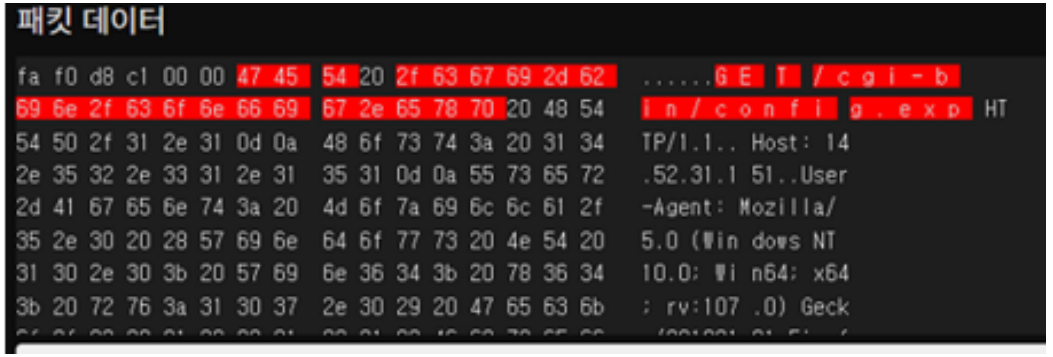




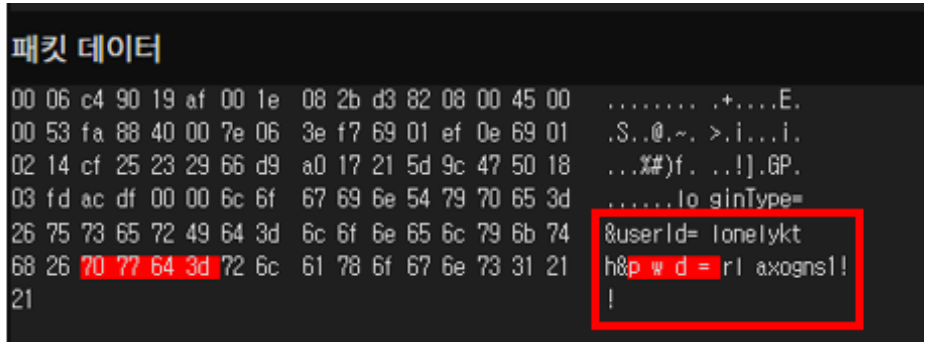
05. 넷아르고스 활용 : 취약점 점검 솔루션

- 네트워크 측면에서 보안 취약점이 있는지 점검
  - 웹서비스 , 네트워크 장비 및 응용 서비스의 취약점 점검
  - 개인정보관리 취약점 점검
  - 내트워크 관리 정책상 취약점 점검

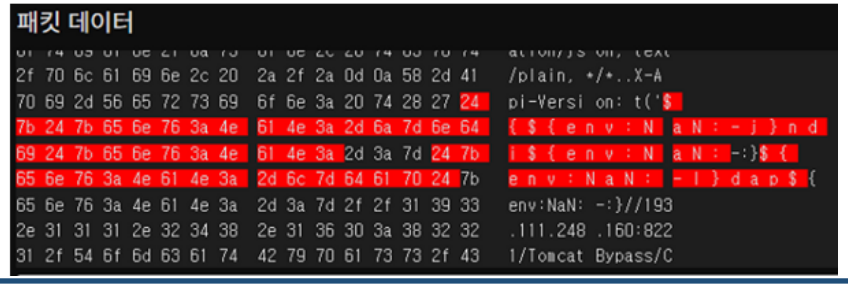
[네트워크 장비 취약점 탐지 : CISCO 라우터(cve-2019-1653)]



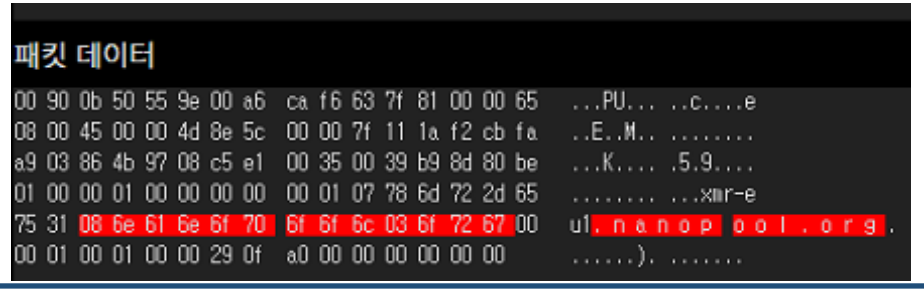
[개인정보 취약점 탐지 : ID/PWD 노출]



[웹서비스 취약점 탐지 : Log4j 취약점]



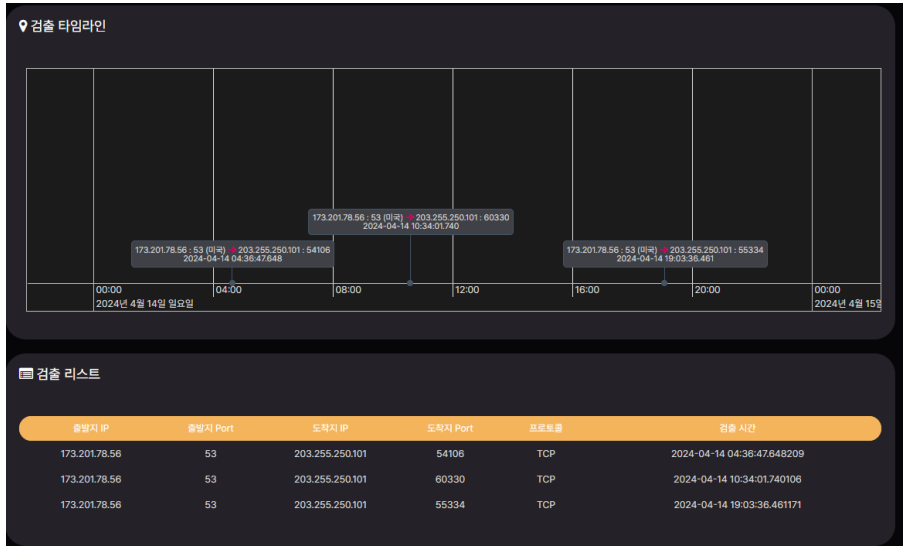
[네트워크 관리 정책 취약점 탐지 : 암호화폐 채굴, snmp public access 접근]



05. 넷아르고스 활용 : 네트워크 포렌식 솔루션

- **탐지된 위협에 대한 분석/증거 자료 제공**
  - 타 솔루션이 탐지한 위협에 대한 **raw packet 제공**
  - 정보 유출 시 **유출 자료(파일) 제공**
  - **최소 2개월 이상** raw packet 저장, **최소 6개월이상** 원본 파일 저장

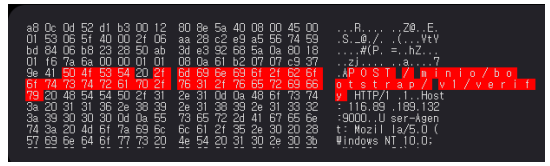
[탐지정보 제공: 타임라인 및 탐지 세션]



[추출된 파일리스트]

[세션간 송수신 패킷 재현]

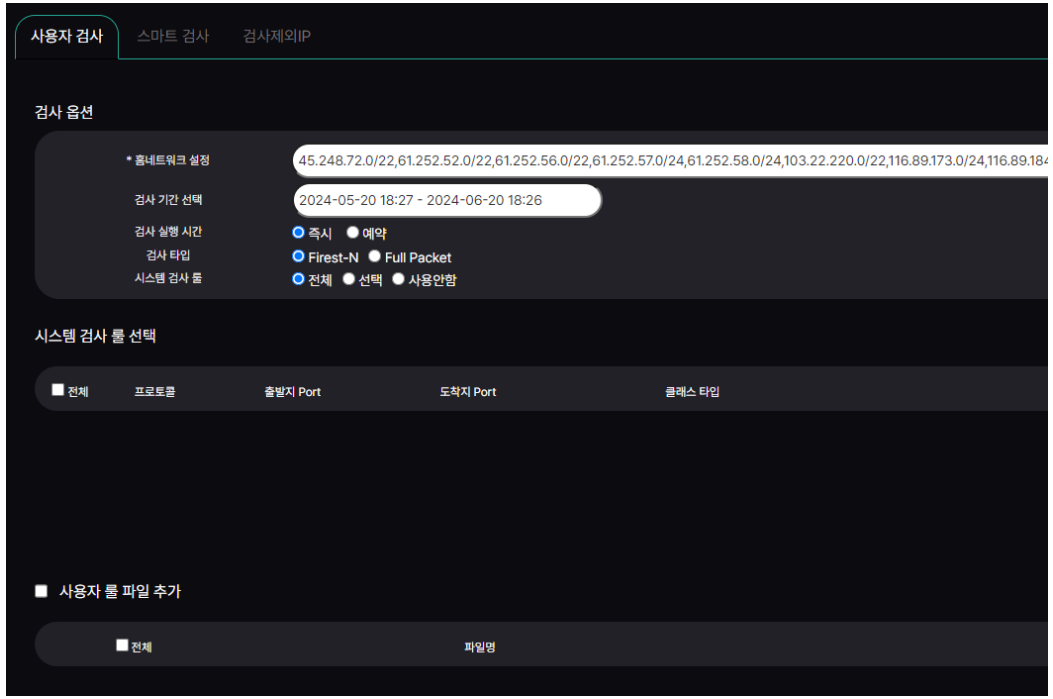
[패킷내 위협 표시]



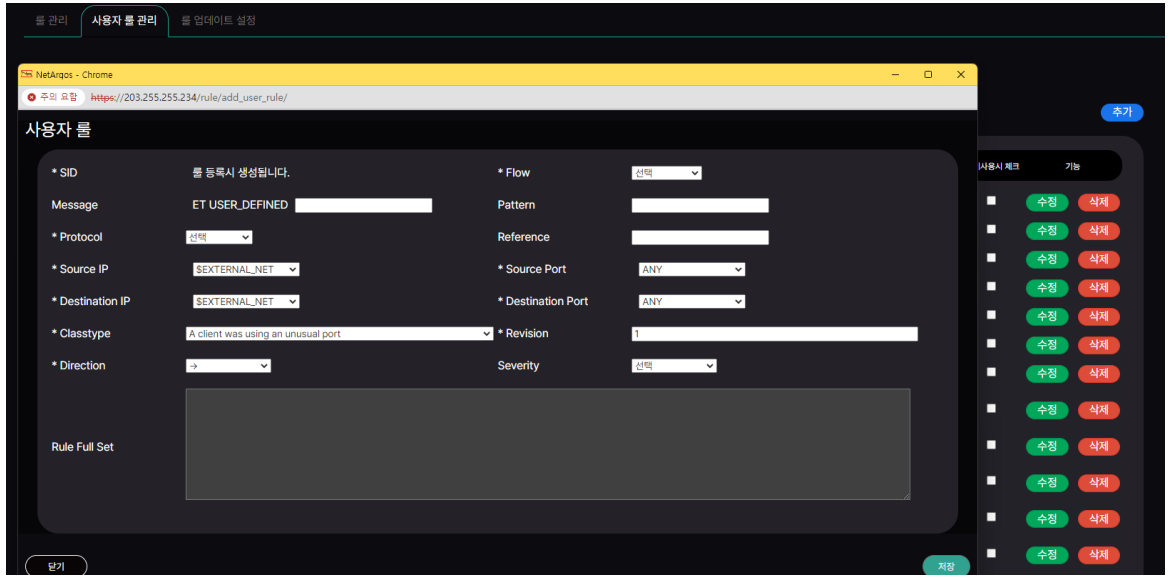
05. 넷아르고스 활용 : 긴급 보안이슈 점검 솔루션

- Log4j 처럼 글로벌 보안이슈 발생 시 긴급 점검
  - 긴급 배포되는 탐지룰을 이용한 회귀보안 검사 실시
  - 기업 내 분석팀이 생성한 탐지룰을 이용한 회귀보안 검사 실시
  - 원하는 기간, 원하는 탐지룰을 이용하여 검사

[사용자가 원하는 기간, 원하는 탐지룰을 적용하여 검사]



[긴급 배포 룰을 추가하여 회귀보안검사 실시]



06. 도입효과 : 기존 보안제품과의 시너지

탐지는 넷아르고스, 차단은 기존 솔루션 활용

제로데이 침투 및 통신 정보
검증 및 분석을 위한 트래픽 정보

SIEM　SOAR

언노운 보안사각 검증 및 분석을 위한
트래픽 정보

APT　NDR　EDR

ZDR

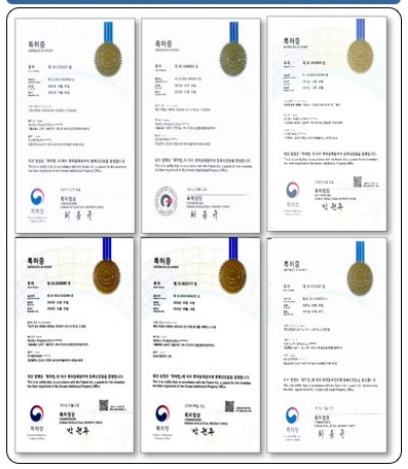
Packet / Network Meta data / Zero-day Event

Firewall　IPS　WAF

제로데이 침투 및 데이터 유출 위협의 차단
정책 생성 및 전달

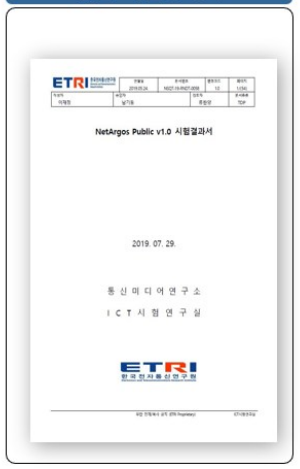
07 : 넷아르고스의 효용성 및 기술가치 검증

특허증 : 국내 6건, 미국 1건(2건 출원)



GS 1등급 인증서

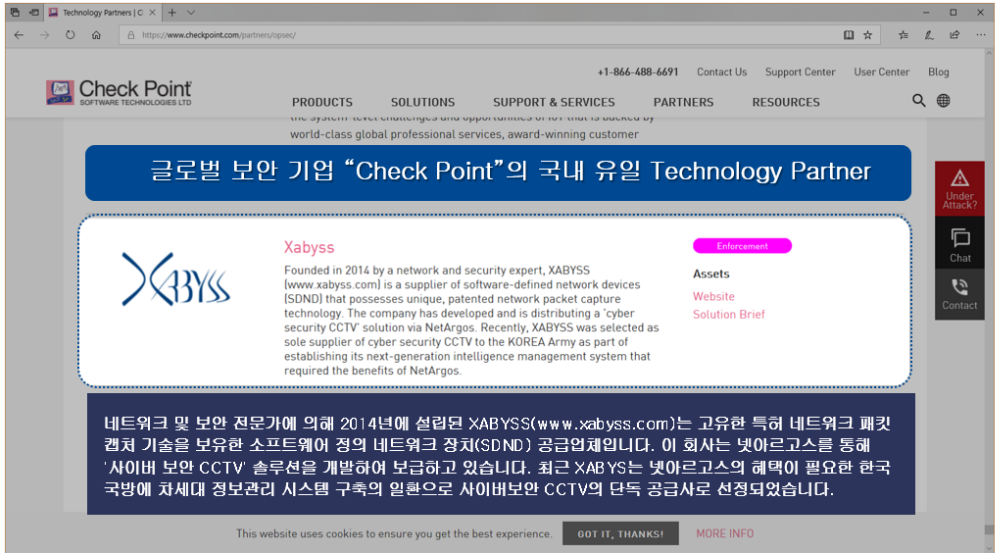
공인 시험결과서



SCI 논문

[기술적 가치 검증]

[기능적 가치 검증]

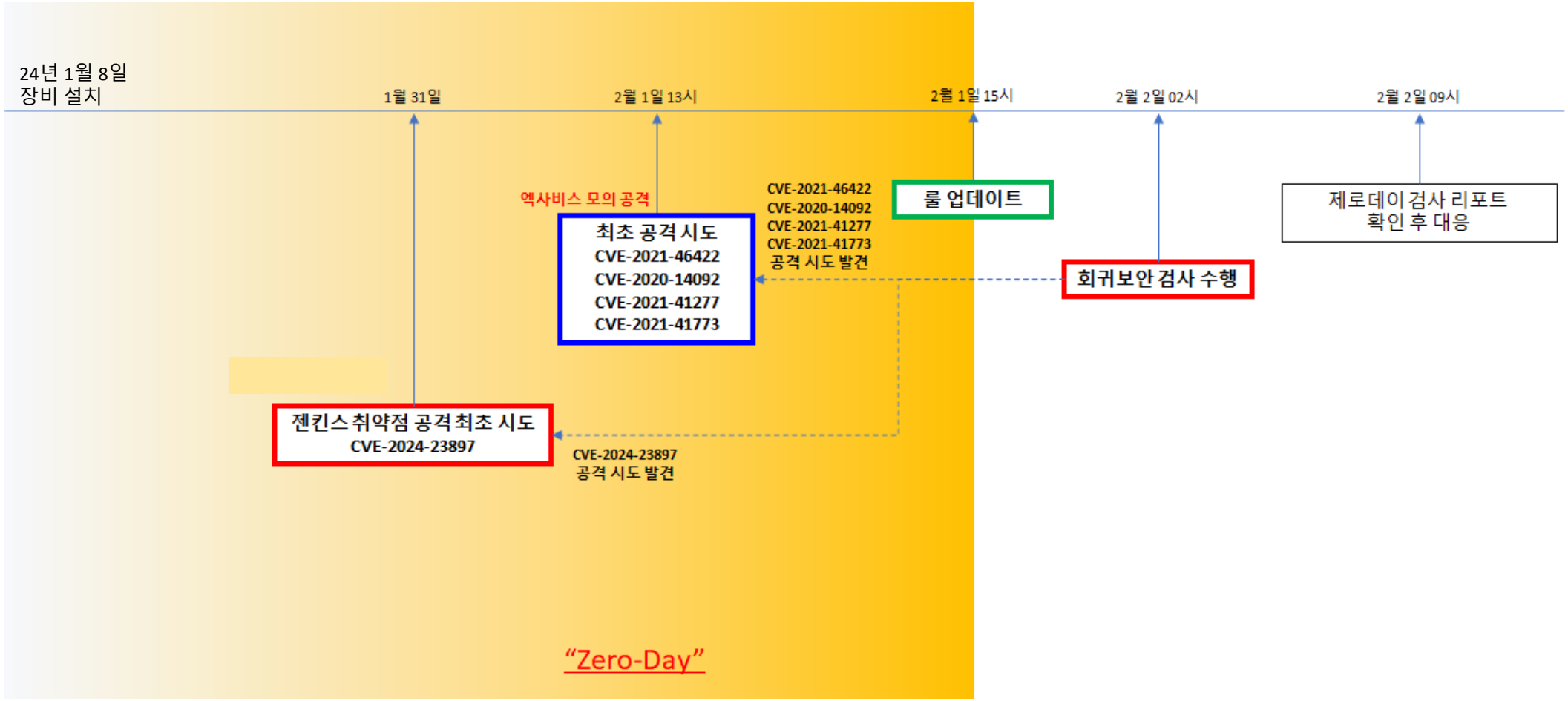


08. 주요 레퍼런스

2023년 12월 6일 : 금융감독원, "최근 5년간 제로데이 공격 사례, 대응 시스템 및 예방 방안에 대해 현황 파악 요청 "

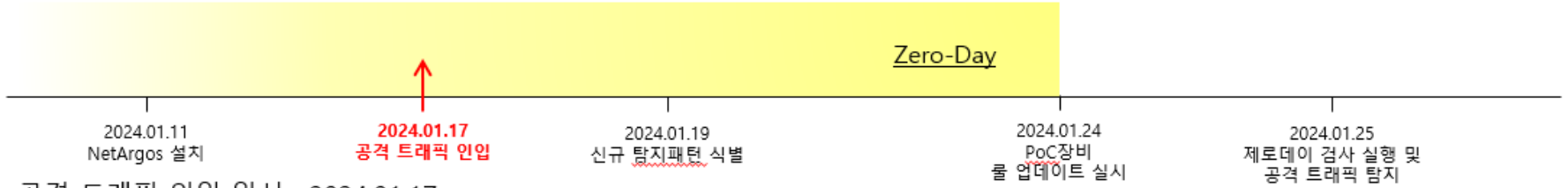
고객 구분	고객 레퍼런스
금융	우리에프아이에스, 하나금융그룹, BNK 금융그룹, NH Bank
국방	Ministry of National Defense Republic of Korea MIMS(Military Intelligence Management System) 군사정보 통합처리체계
공공	대한민국 국가정보원, pohang 포항시, DAEGU 대구광역시 DAEGU METROPOLITAN CITY, 강남구도시관리공단 Gangnam-gu city management corp.
기업	kt, Dongwon 동원산업, LAPP KOREA, HJ 중공업
연구 / 교육	ETRI, 국립한국교통대학교 KOREA NATIONAL UNIVERSITY OF TRANSPORTATION, 충북대학교 CHUNGBUK NATIONAL UNIVERSITY

APPENDIX : 탐지 사례 (1금융 은행, 23년 12월)



APPENDIX : 탐지 사례 (증권사, 24년 2월)

1. 타임라인



·공격 트래픽 인입 일시 : 2024.01.17

·신규 탐지패턴 식별 : 2024.01.19

·룰 업데이트 일시 : 2024.01.24

·제로데이 검사 일시 : 2024.01.25

2. 탐지결과

·제로데이 검사 결과

- 외부 IP 149.56.15.116, 149.56.13.248 로부터 취약점이 존재하는 것으로 알려진 URL 접근 시도 (/mifs/aad/api/v2/)
- 대응 세션 확인 결과 302 Found 반환 및 error404.html 페이지로 리다이렉션, API 응답 발생하지 않음
- 취약점이 존재하지 않는 환경으로 확인, 악의적 접근은 확인되었으나 공격 시도는 실패

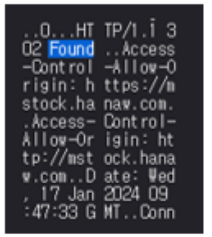
·대응 권고사항

- 공격자 **외부 IP (149.56.15.116, 149.56.13.248) 차단 권고**

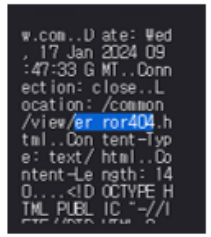
·조치 사항 (관제센터 조치 내역)

- 모증권 웹방화벽 탐지 결과 해당 공격 IP에서 SQL Injection 공격이 동시 발생
  차단 조치 됨 (조치 시간 : 2024년 01월 17일 18시 51분)

공격 시도 패킷



대응 패킷(1)

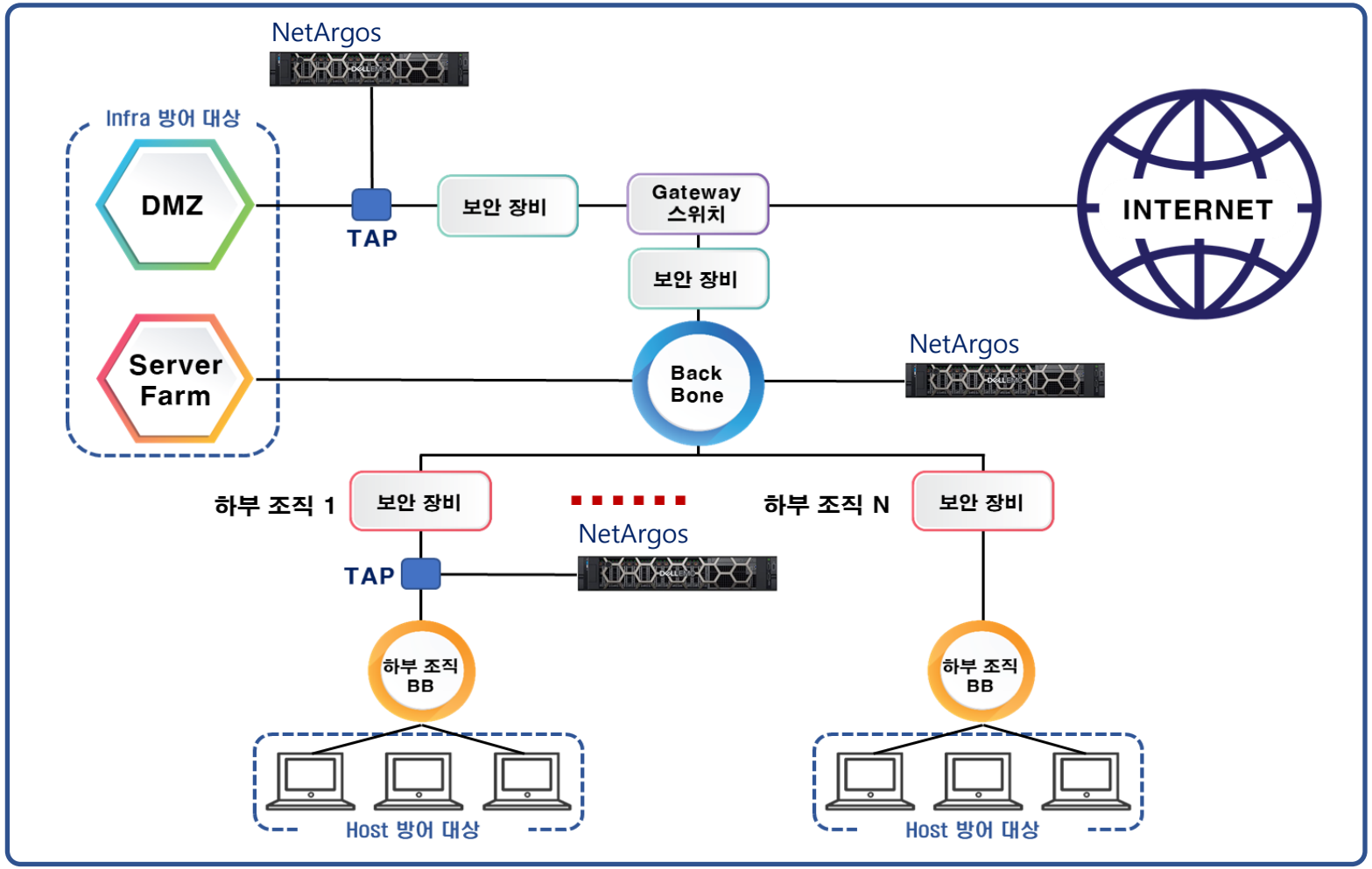


대응 패킷(2)

APPENDIX : 구축사례(All-in One)

저장 / 검사 / 분석 / 관리를 하나의 장비에서

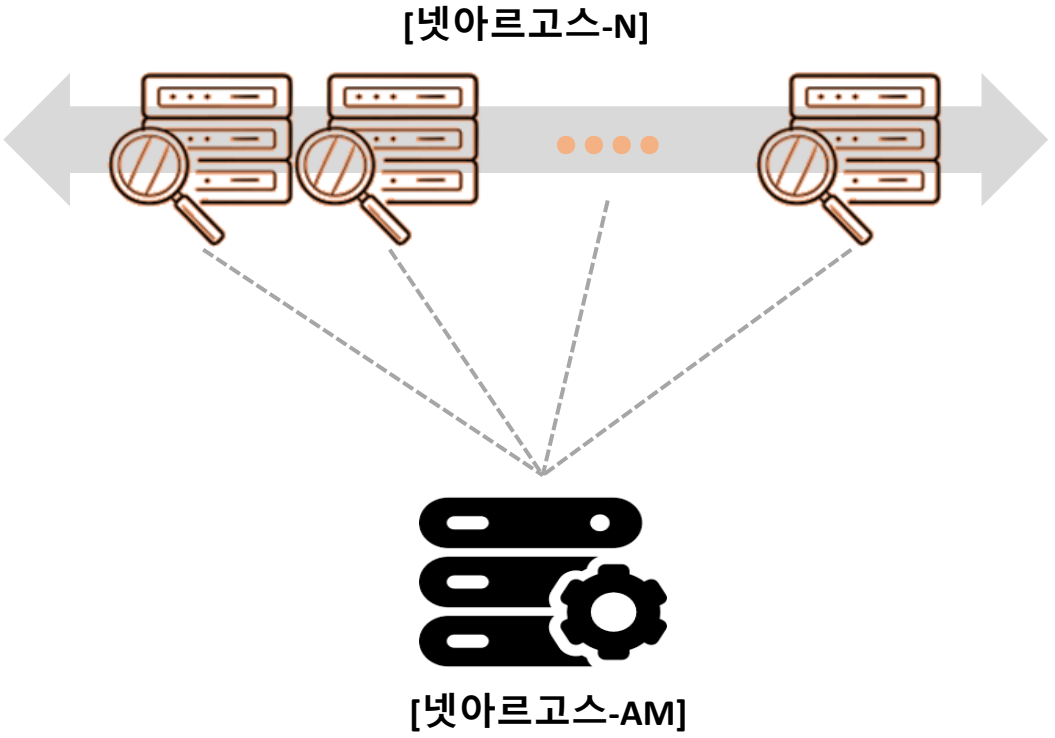
- 기본적인 구성 : 손쉬운 설치와 관리, 사용
- 필요 지점에 설치(예: B/B, DMZ, 망분리된 곳 등)
- 최대 4개 링크 input 가능



APPENDIX : 구축사례(유연한 시스템 확장)

제로데이 기간 확장이 필요할 때

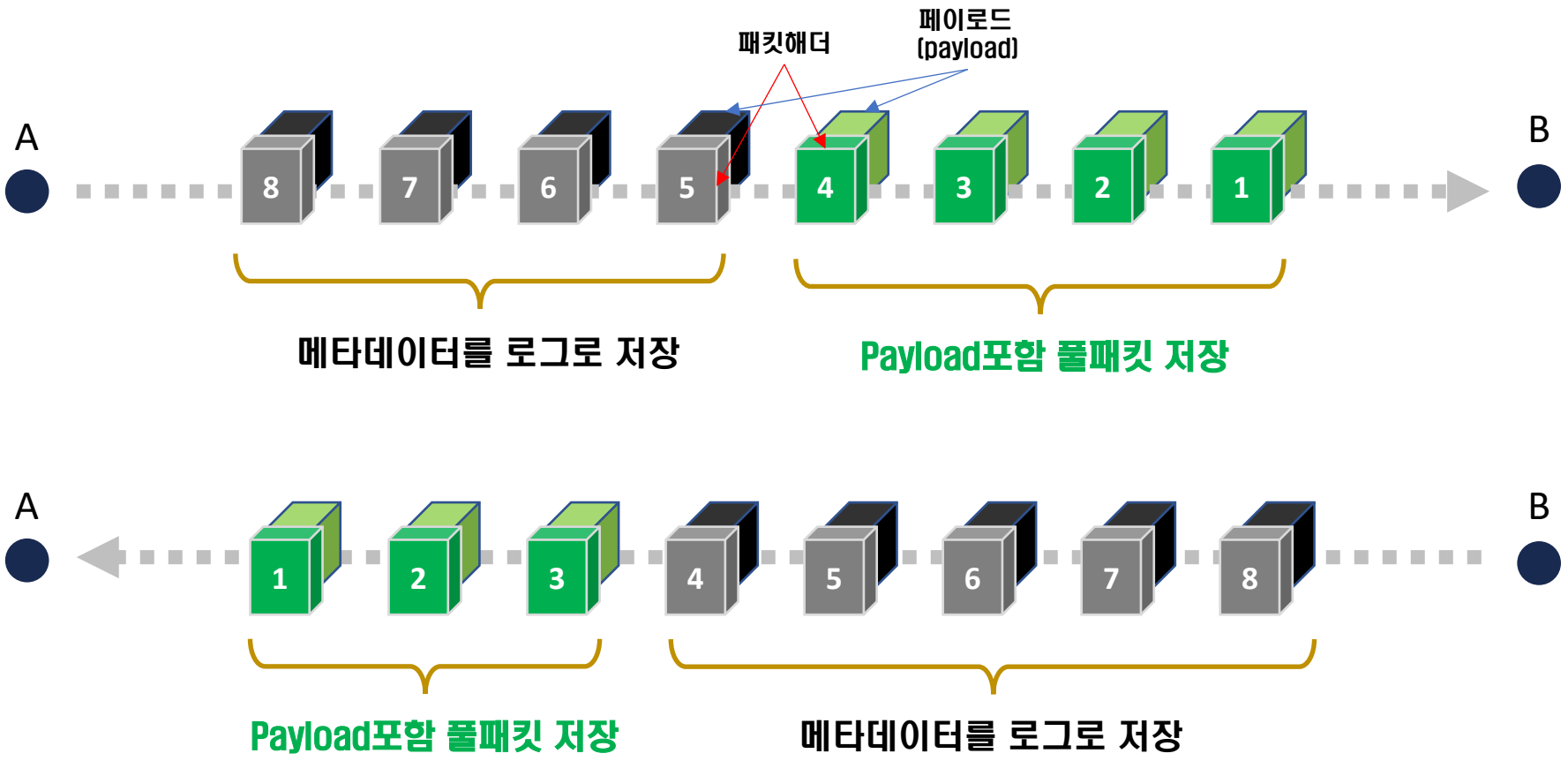
- 수집/검사용 서버를 여러 대 설치
- 1대의 서버에서 탐지위협 분석 및 관리
- 단순 연결, 유연한 설치
- 통합 분석 및 관리



APPENDIX : First-N (PCT 특허 등록)

보안검사에 필요한 패킷만 저장

(두 지점간 통신 시 단방향 세션 기준 초기 패킷만 저장)



APPENDIX : 회사 소개 및 주요 연혁

구분	내용
회사명	엑사비스㈜
설립일	2014년 2월 4일
대표이사	이시영
자본금	3.3억
임직원수	15명 (개발 9명, 영업/관리 6명)
사업	네트워크 보안 장비(SDND) 개발 및 판매 제로데이 탐지 솔루션 판매 및 클라우드 서비스
주소	경기도 수원시 영통구 영통로 237 에이스하이엔드타워 305호
홈페이지	www.xabyss.com

연월	주요 연혁
2024년 04월	(주) KTds 와 국내총판계약 체결
2024년 01월	우리금융 제로데이 공격 탐지시스템 구축
2023년 01월	우수특허기반 혁신제품 지정 (조달청)
2021년 11월	신한은행 Zero-Day 공격 역추적 시스템 납품
2021년 03월	GS 1등급 획득(조달등록 완료)
2020년 12월	2020 기술창업기업 최우수상 수상
2019년 06월	IBK기업은행으로부터 투자 유치
2019년 02월	국방 MIMS 2018 프로젝트에 납품 계약
2018년 11월	NET Challenge season 5 금상 수상
2017년 03월	특허 등록
2014년 02월	엑사비스㈜ 설립

Detect the Knife of Assassin

www.xabyss.com

경기도 수원시 영통구 영통로 237, 305호/306호
(영통 에이스하이엔드타워)
Tel: +82-70-7510-8200
Fax: +82-70-8673-8200