NET
ARGOS
Threat Hunting의 새로운 표준
(ZDR, Zero-day intrusion Detection & Response)
ABYSS

1. 보안 패러다임 진화의 필요성
2. ZDR : A New Threat Hunting
3. NetArgos 개요

01. 보안 패러다임 진화의 필요성

사이버보안에서 답을 하지 못하는 질문이 존재 : 보안사각(NSBS, Network Security Blind Spot)

매일 신규 탐지 정보의 추가를 결재 받을 때

이미 침투해 있지는 않을까요?

새로운 보안 취약점을 발견했을 때

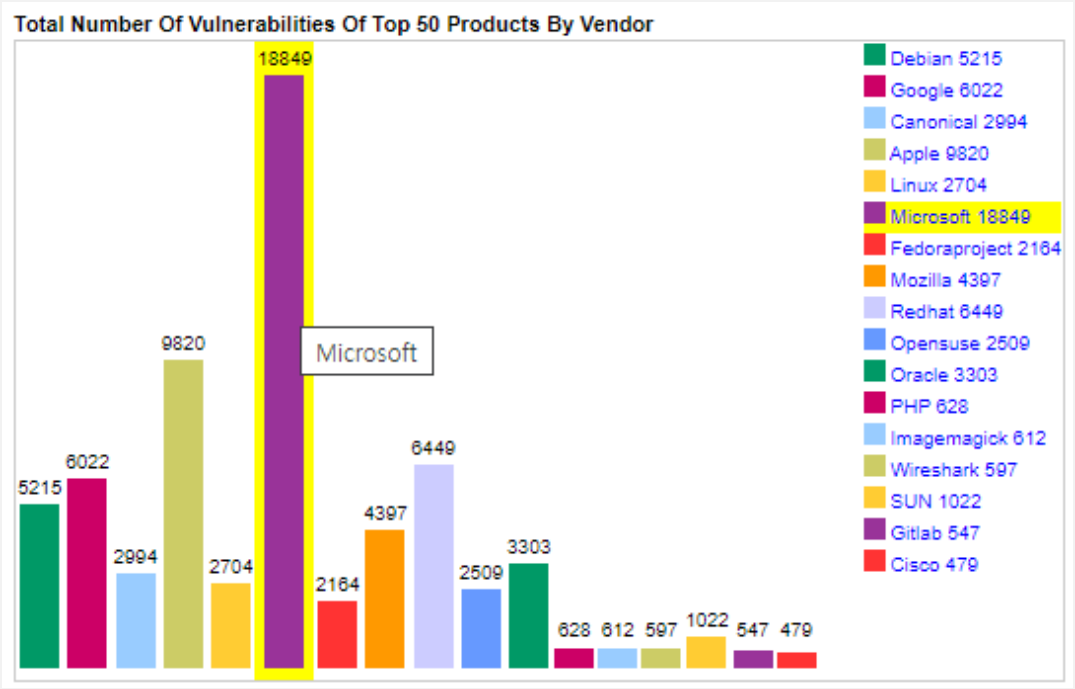
이미 이곳으로 공격을 당하지는 않았을까?

이상한 통신 행위를 발견했을 때

언제, 어디로, 어떻게 들어왔지?

01. 보안 패러다임 진화의 필요성

2021년 현재까지 발견된 CVE 카운트는 68,311건, 하루에 약 253건의 취약점이 보고



68,311 건 매년 증가 추세

253건/Day 발표 즉시 공격 시작

01. 보안 패러다임 진화의 필요성 : Threat Hunting

미탐지 된 보안 위협 침투는 Threat Hunting을 통해 능동적으로 대응해야 함

정의 (from Wikipedia)

" 기존의 보안 체계를 우회하는 위협을 탐지하고 격리하기 위하여 네트워크를 능동적이고 반복적으로 검색하는 프로세스"

- 잠재적인 위협이나 침해사고가 발생한 후에 조사/분석을 하는 기존 위협 관리 시스템(방화벽, IDS, SIEM 등)과 차별화

기존 위협 관리 시스템	사이버 위협 헌팅(Cyber Threat Hunting)
모든 위협을 막을 수 있다.	모든 위협을 차단할 수는 없다.
알려진 위협에 대한 관리	차단되지 않은 위협에 대한 관리
방어 & 사후 분석	탐지/ 분석 / 추적 후 대응

위협 차단 (Prevention) + 피해 최소화 (Detection & Response)

- 기존의 도구에 의한 탐색을 회피한 위협을 탐색하는 적극적인 보안 탐색으로 수동적인 접근을 하는 Cyber detection과 다르다.
- 아직 탐지되지 않은 것을 찾는 것, 이미 위협은 침투되었을 것을 가정하고 이를 찾아내는 Aggressive Detection
- 포렌식 분석과 위협 추적(hunting)을 위한 과거 이벤트 분석을 위해 몇 주 이상의 저장된 패킷을 검사/분석

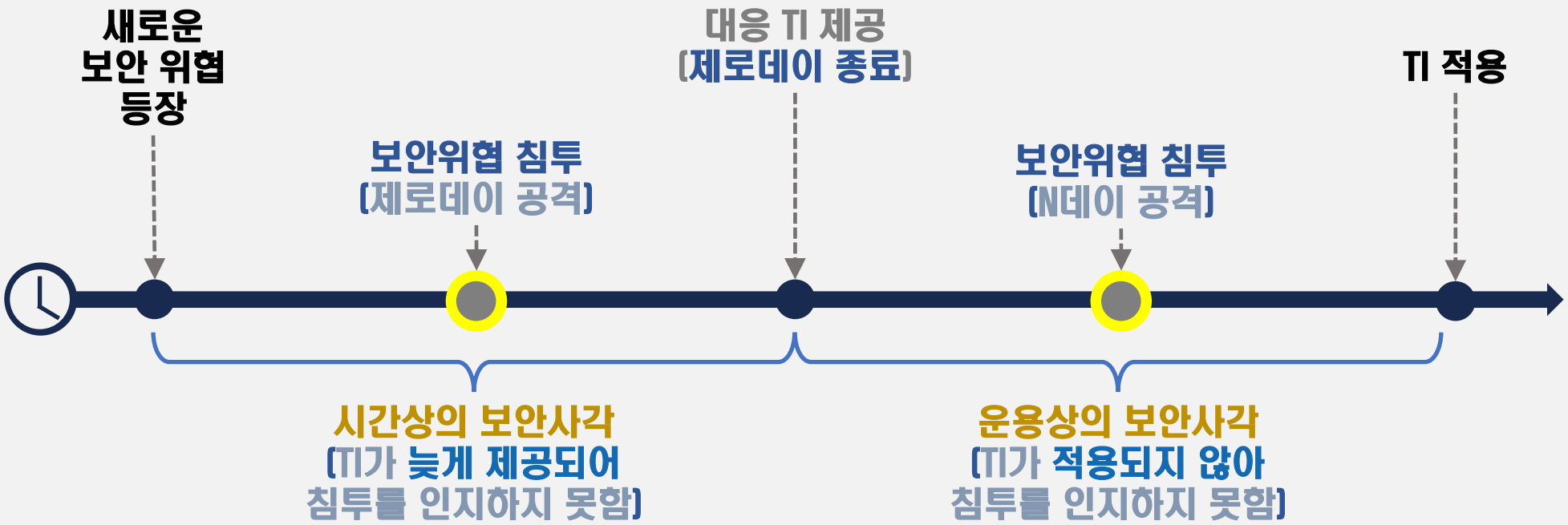
01. 보안 패러다임 진화의 필요성 : 보안사각의 세분화와 대응 체계

정확한 문제 영역의 구분과 적합한 대응을 통한 보안의 사각지대를 없애는 것이 중요

이상적인 보안 대응 절차	대응 영역 구분	기존 대응 체계
대응 절차 ↓		
알려진 TI를 기반으로 실시간 침투를 방어	실시간 침투 대응 : 위협 방지 및 검출	Firewall, IPS, WAF, Vaccine EMS, SIEM, SOAR
신규 TI 나오면 빨리 적용하여 앞으로의 침투 방어	Threat Hunting — 운용상의 보안사각	✕
과거 트래픽의 재검사를 통해 제로데이 침투를 검출하여 대응	Threat Hunting — 시간상의 보안사각	✕
아직 TI가 없는 보안 위협을 이상행위탐지를 통해 모니터링	Threat Hunting — 언노운 보안사각	ATP / EDR / NDR

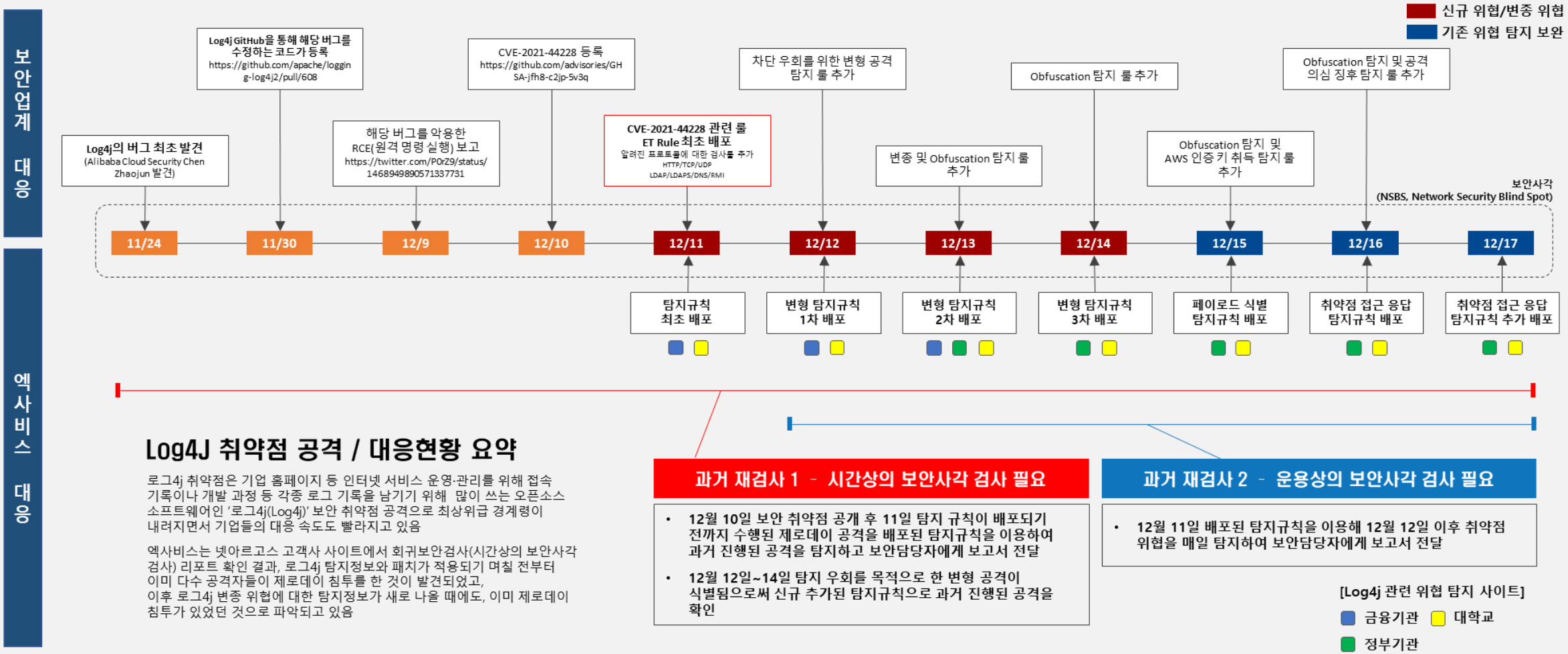
01. 보안 패러다임 진화의 필요성 : 시간 및 운용상의 보안사각

보안사각을 통한 제로데이 침투는 100% 성공하며, 침투 여부가 인지되지 않음



01. 보안 패러다임 진화의 필요성 : Log4j 사례 분석

신속한 TI의 설정과 패치의 적용은 더 이상 안전하지 않음 : 잠재적인 위험에 대한 대응이 전무



Log4J 취약점 공격 / 대응현황 요약

로그4j 취약점은 기업 홈페이지 등 인터넷 서비스 운영·관리를 위해 접속 기록이나 개발 과정 등 각종 로그 기록을 남기기 위해 많이 쓰는 오픈소스 소프트웨어인 '로그4j(Log4j)' 보안 취약점 공격으로 최상위급 경계령이 내려지면서 기업들의 대응 속도도 빨라지고 있음

엑사비스는 넷아르고스 고객사 사이트에서 회귀보안검사(시간상의 보안사각 검사) 리포트 확인 결과, 로그4j 탐지정보와 패치가 적용되기 며칠 전부터 이미 다수 공격자들이 제로데이 침투를 한 것이 발견되었고, 이후 로그4j 변종 위협에 대한 탐지정보가 새로 나올 때에도, 이미 제로데이 침투가 있었던 것으로 파악되고 있음

과거 재검사 1 - 시간상의 보안사각 검사 필요

- 12월 10일 보안 취약점 공개 후 11일 탐지 규칙이 배포되기 전까지 수행된 제로데이 공격을 배포된 탐지규칙을 이용하여 과거 진행된 공격을 탐지하고 보안담당자에게 보고서 전달
- 12월 12일~14일 탐지 우회를 목적으로 한 변형 공격이 식별됨으로써 신규 추가된 탐지규칙으로 과거 진행된 공격을 확인

과거 재검사 2 - 운용상의 보안사각 검사 필요

- 12월 11일 배포된 탐지규칙을 이용해 12월 12일 이후 취약점 위협을 매일 탐지하여 보안담당자에게 보고서 전달

[Log4j 관련 위협 탐지 사이트]
금융기관 대학교
정부기관

01. 보안 패러다임 진화의 필요성

매일 제로데이 침투로 치명적인 위협에 무방비로 노출 : **보안 보고 체계**의 변화가 필요

3%

신규 발생

매일 3% ~ 5%의
위협정보가 업데이트

30%

보안 위협

악성코드 공격의
30% 이상이
제로데이 공격

76%

성공한 공격

성공한 침투의 76%는
제로데이 공격

3M

제로데이 기간

제로데이 기간은 평균
3개월

**보안담당 임원에게 일일 보안 업무 보고 및 결재 시에
신규 TI의 제공과 설정 보고 뿐만이 아니라 신규 TI에 대한 제로데이 침투 여부를 보고할 수 있어야 함**

02. ZDR : A New Threat Hunting

보안사각으로 인한 **제로데이 침투**를 해결하기 위해서는 과거 트래픽을 제로데이 기간 동안 저장한 후,
새로운 탐지정보가 제공될 때마다 자동으로 회귀보안검사 및 분석이 필요

02. ZDR : A New Threat Hunting

ZDR은 지금까지 통제선 밖에 있었던 **시간/운용상의 보안사각**을 통제선 안으로 인양

Z

- 시간/운용상의 보안사각에 대응하기 위해 제로데이 기간 동안의 과거 트래픽을 저장

D

- TI(Threat Information)의 업데이트 시마다 자동 회귀보안검사 및 분석을 통해 제로데이 침투와 관련된 행위를 검출

R

- 자동 분석 리포트와 보안 장비와 연동 대응을 통해 운용자의 부담을 최소화

02. ZDR : NDR과의 비교

침해 사고의 80%를 차지하는 제로데이 침투에 대응하기 위한 추가적인 Threat Hunting 솔루션이 필요

	ZDR	NDR
역할 분석	▪ 매일 보안사각에 대한 자동 회귀보안검사(조기 대응) ▪ 제로데이 침투 보고 및 대응을 위한 자동 리포팅 및 검증을 위한 과거 트래픽 제공(장기간)	▪ 네트워크 상에서 발생하는 이상행위 모니터링 ▪ 검출된 이상행위 검증을 위한 과거 트래픽 제공(단기간)
적합성 분석	▪ 시간/운용상 보안사각에 대한 새로운 Threat Hunting 능력 제공 ▪ 타 보안 솔루션이 커버할 수 없는 신규 영역(보안사각)	▪ 언노운 보안사각에 대한 Threat Hunting 능력 제공
기대효과 분석	▪ 일일 보안사각 보고 및 대응을 통해 보안 강화 ▪ 연동 검증이 완료된 기존 NAC, SIEM, EDR과의 연계를 통한 보안 위협 대응 능력 강화	▪ 탐지 결과의 오탐 및 분석을 위한 전문 인력이 필요

02. ZDR : Forensic과의 비교

Forensic ANALYTICS SOLUTION

막대한 디스크 공간 소요
10G 1회선 기준 3개월간의 트래픽 저장을 위해 4.5PB의 저장 공간이 필요하며, 64TB 스토리지 기준 서버 75대 소요

고가의 컴퓨팅 하드웨어
저장된 데이터의 1회/1일 재검사를 위해 2.4GHz/8코어 서버 50여대 소요

분석 전문 인력 필요
저장된 데이터에 대한 분석을 위해 전문 인력 별도 요구

기존 솔루션을 이용한 시간/운용상의 보안사각 탐지는
너무 많은 비용이 소모되어 **현실적으로 도입 불가**

ZDR SOLUTION

특수 패킷 저장기법
특허 받은 First-N 패킷 저장기법을 통해 1대의 시스템으로 3개월 이상 데이터 저장

50배 수준의 하드웨어 비용 절감

매일 1회 이상 주기적 자동 보안 재검사
매일 1회 이상 자동으로 새로 업데이트된 공격탐지방법으로 회귀보안 검사를 수행하고, 분석 후 리포팅

자동 분석으로 전문 인력 불필요
AI 기반의 전문가 시스템으로 별도의 전문인력 불필요.

정해진 시간동안 자동으로 분석이 이루어지며 운영자에게 자동 리포트 전송

최소의 비용으로 시간/운용상의 보안사각 제거

03. NetArgos 개요

NetArgos®는 기존 NDR(Network Detection & Response) 기술이 해결하지 못했던 제로데이 침투가 발생하는
시간/ 운용상의 보안사각을 특허 받은 데이터 저장기술과 회귀보안검사 및 분석 기술로 해소 .
기존 FORENSIC 기술에 비해 전체 비용(도입, 운용, 상면)을 1/50 이하로 절약.

네트워크 트래픽 데이터의 2% 저장

- 40Gbps 실시간 패킷 수집 및 저장
- 실시간 네트워크 메타 데이터 생성

- 1일/1회/3개월 이상 주기적 자동 회귀보안검사
- AI(Expert System) 기반 시간/운용상 보안사각 분석
- 외부 보안장비 연동을 통한 자동 대응

시간/운용상의 보안사각 99.6% 대응

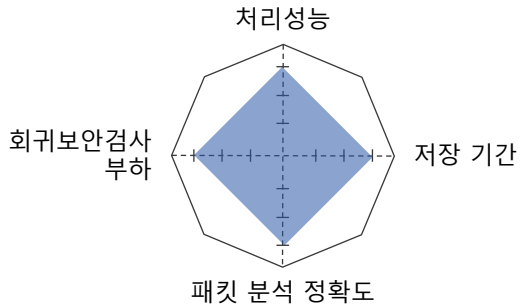
- First-N 패킷 저장 + FPC
- 기본 FORENSIC 대비 50배의 저장 효율성 (10G 환경에서 3개월 이상 저장)

- DPI(Deep Packet Inspection)
- Drill-down 네트워크 정보 검색
- 표준화된 네트워크 정보 추출 및 전달

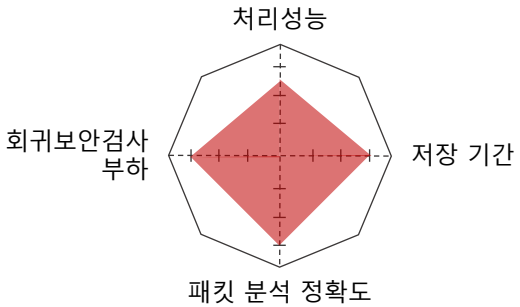
03. NetArgos 개요

이상적인 ZDR의 조건을 만족시킬 수 있는 **유일한 저장 및 분석 기술**

Theoretical

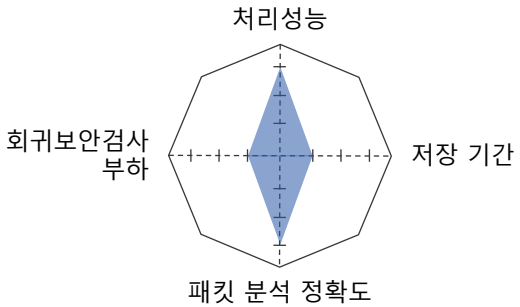


First-N

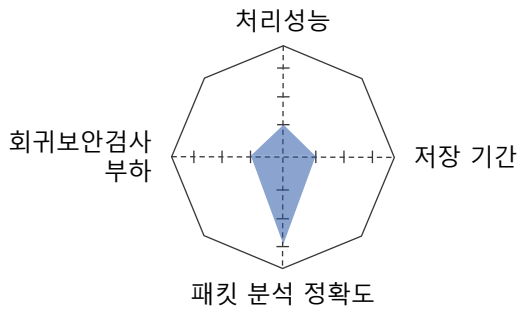


FPC

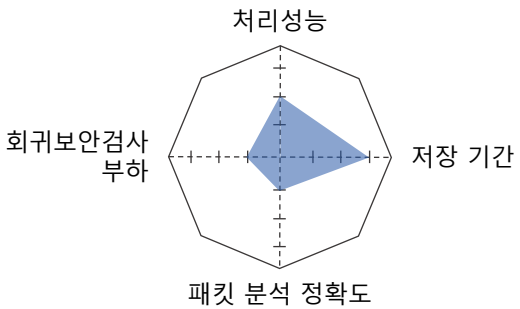
[Full Packet Capture]



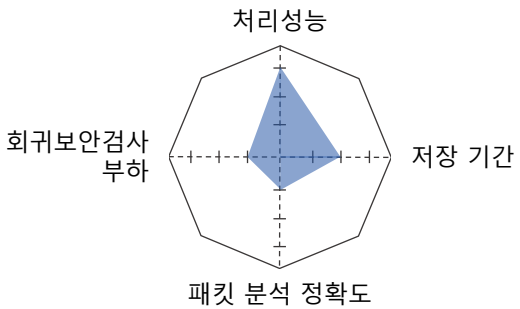
Packet Compression



Event-Driven



Packet Slicing



03. NetArgos 개요

시간/운용상 보안사각 대응을 위한 5단계 원형접근방법을 제공

01 장기 저장

응용별 First-N 패킷 저장(ZDR을 위한 최적화된 네트워크 트래픽 저장 기술)
FPC 대비 50배의 저장 공간 축소와 99% 이상의 정확도 유지

02 재검사

주기적/자동적 회귀보안검사(Retroactive Security Check)
1회/1일 이상 고속으로 제로데이 기간을 재검사

03 분석

미탐 위협 후보군 추출(Candidate Detection)
행위기반분석과 시계열 상관관계 분석을 위한 인공지능 및 빅데이터 분석

04 보고

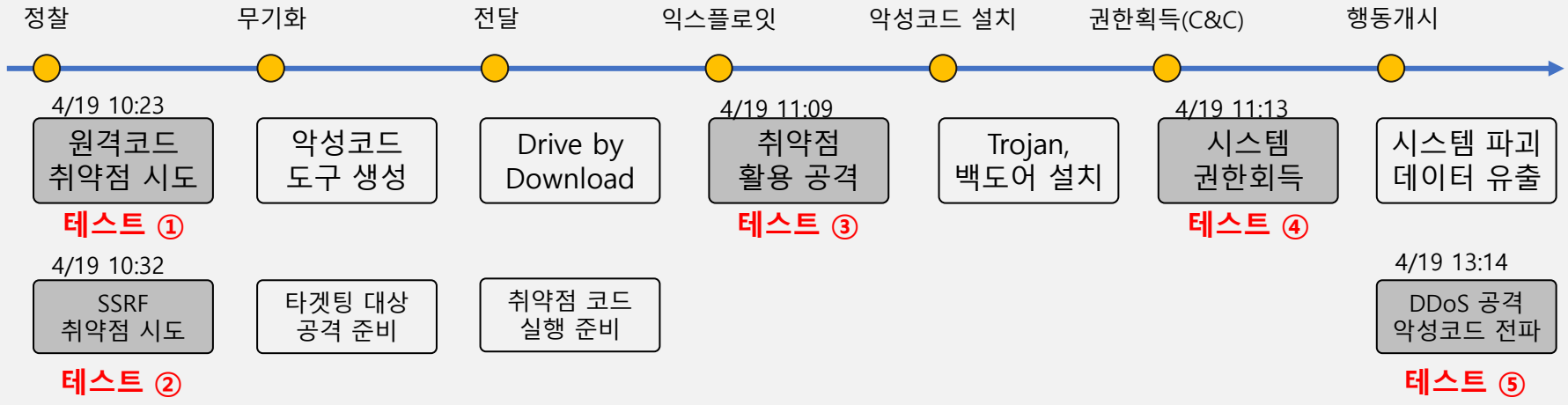
스마트 리포트(Smart Report)
보안 비전문가도 이해가 가능한 수준의 정보 정리 및 통계적 분석

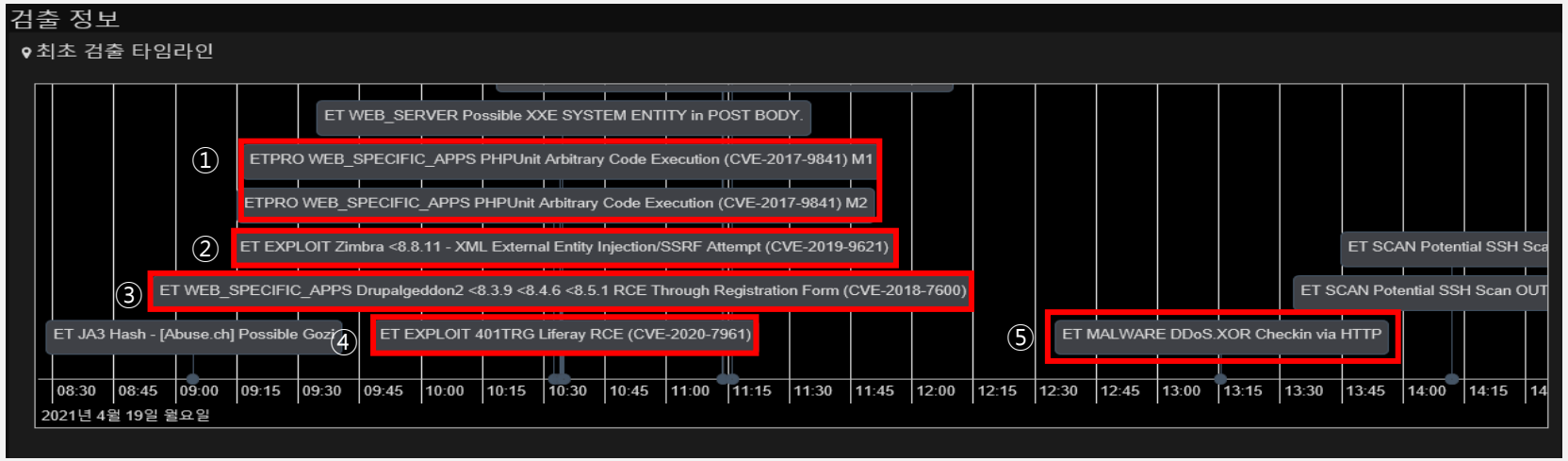
05 대응

실시간 보안장비들을 위한 보안 정책의 최적화(Security Policy Optimization)
패킷 기반의 가시화된 추적 및 검증과 보안사각 대응을 위한 보안 정책 수립 및 전달

03. NetArgos 개요

내부 모의테스트 수행(공격유형 5건, 50종) 결과 해당 공격 탐지를 회귀보안검사를 통해 시계열상 정보로 제공하고,
상세 정보의 분석을 위한 Raw Packet을 제공함으로써 공격의 성공/실패 유무의 확인이 가능





03. NetArgos 개요

Zero Trust Security Service : 기존 보안 관제 체계가 **통제하지 못하는 시간/운용상의 보안사각에 대한 대응 능력**을 제공

NetArgos

Packet
0101010101
0011001100
1001110011

네트워크 메타 데이터
/ 패킷 정보 추출

주기적 회귀보안검사로
제로데이 침투 검출

TI에 대한 회귀보안검사로 Zero-day 침투 확인

- DB or Syslog -
Zero-day Threat Event

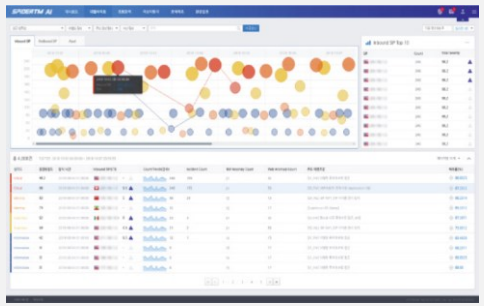
- API -
Network Meta-data and Packets

- API -
학습을 통한 위협 모델링(TI)

SIEM/SOAR

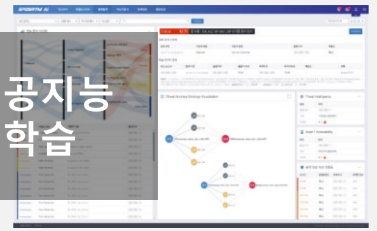
이미 침투한 위협 이벤트 수집/분석

- 회귀보안검사로 탐지된 위협 및 가시성 확보
- EDR/NDR 연동 분석을 통한 Threat Hunting



Threat Hunting
위협 모델링(TI) 생성

인공지능
학습



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