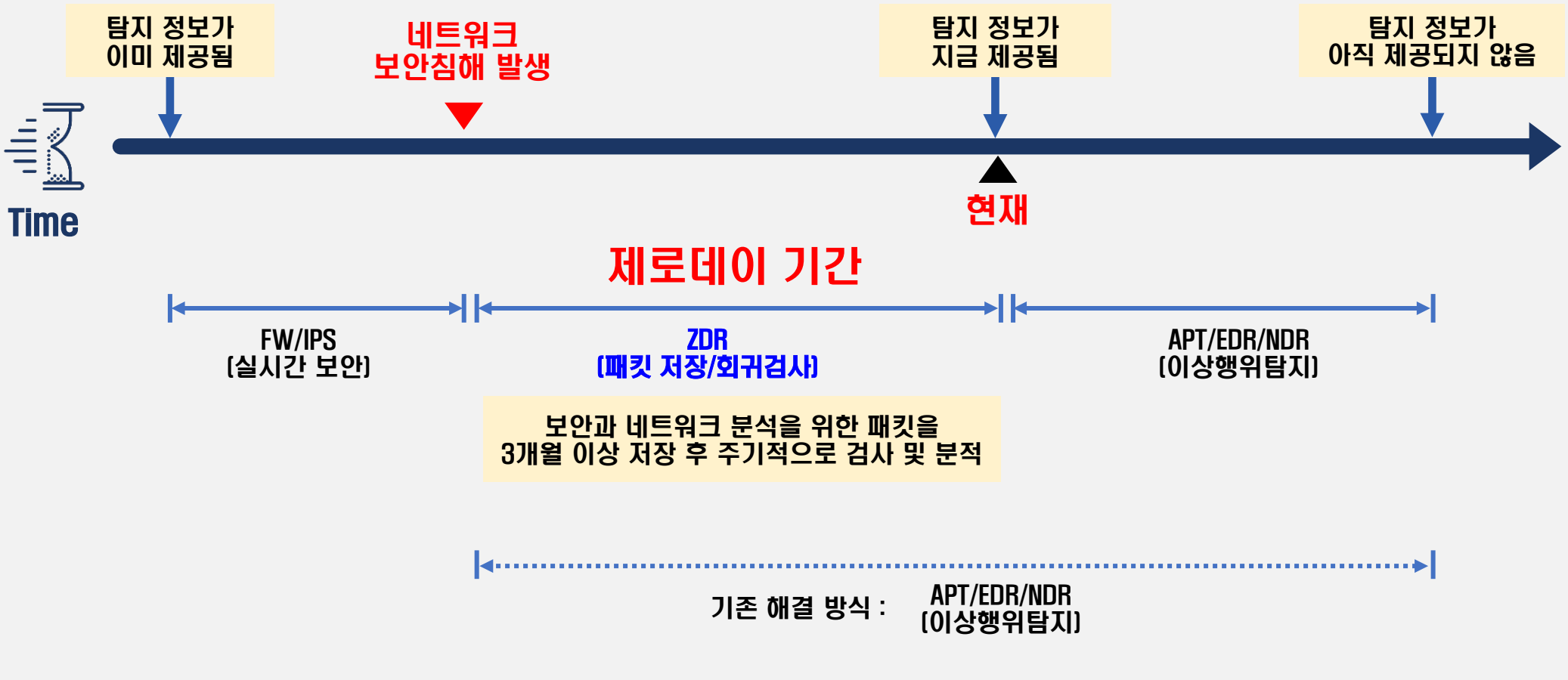

TIGER
CNS
ZDR(Zero- day intrusion Detection & Response)
NetArgos®

01. 제로데이 침투 대응방안

/ ,



01. 제로데이 침투 대응방안 – SUNBURST 공격검출 및 대응사례

데일리시큐 2021년 1월 25일 기사

- 엑사비스, 솔라윈즈 SUNBURST 보안위협 시간상 보안사각 정밀분석
- 의료기관, 대학, 연구기관 대상 SUNBURST 제로데이 스캔 발견돼

데일리시큐

이슈 | 산업 | 정책 | 해외 | IT&생활 | 자료실 | 전체기사 기사제보 | 뉴스레터신청 검색어를 입력해 주세요

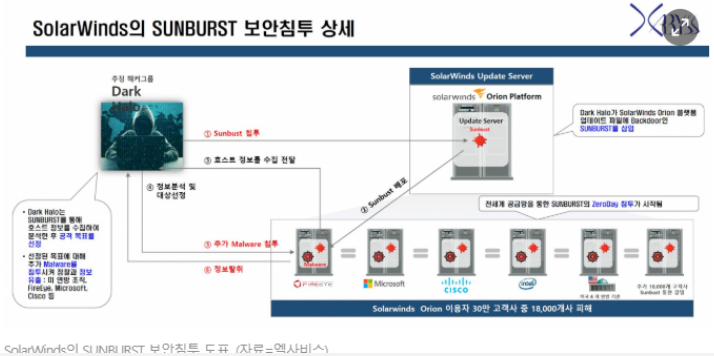
최종편집 : 2021-02-03 10:35 (수) 처음으로 | 로그인 | 회원가입

HOME > 이슈 > 긴급속보

[솔라윈즈 SUNBURST 보안위협 총정리] "한국 병원·대학·기관 등에서도 공격 스캔 발견"

길민권 기자 | 승인 2021.01.25 02:03

엑사비스, 솔라윈즈 SUNBURST 보안 위협 시간상 보안사각 정밀 분석
의료기관, 대학, 연구기관 대상 SUNBURST 제로데이 스캔 발견돼...주의
국내 조사 확대되면 더 많은 SUNBURST 피해 조직 드러날 것



SolarWinds의 SUNBURST 보안침투 도표 (자료=엑사비스)

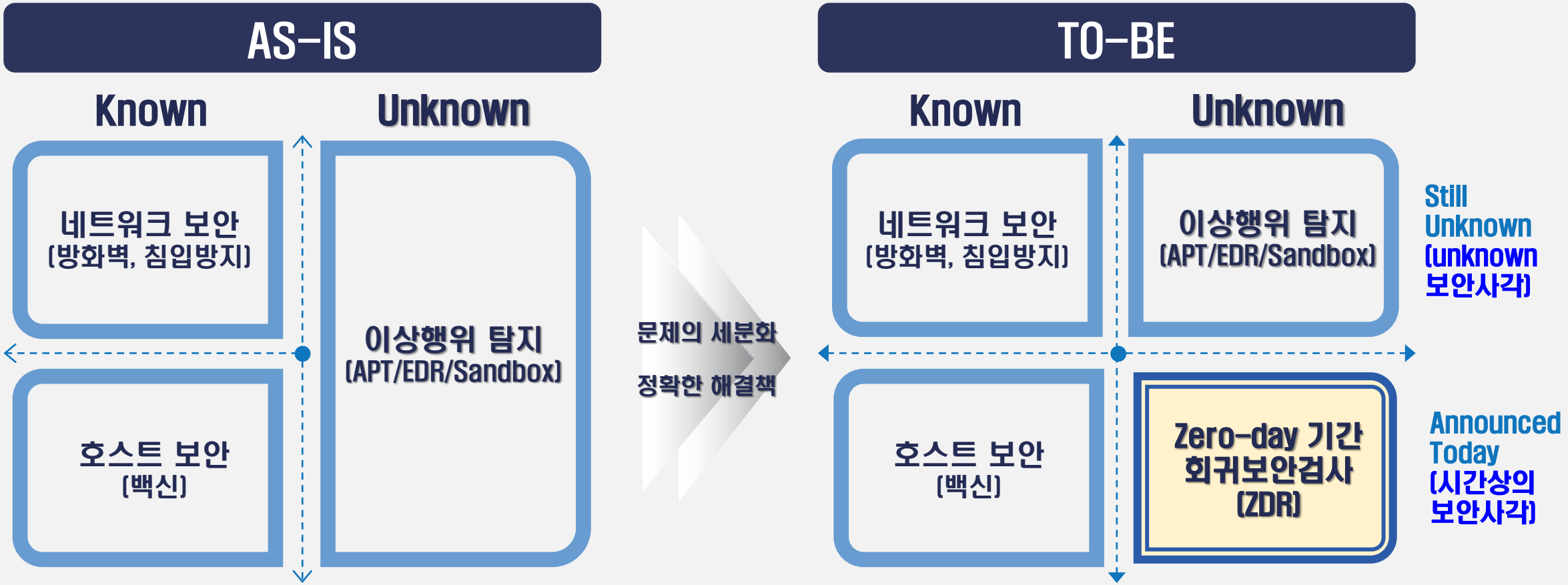
많이 본뉴스

1 [솔라윈즈 SUNBURST 보안위

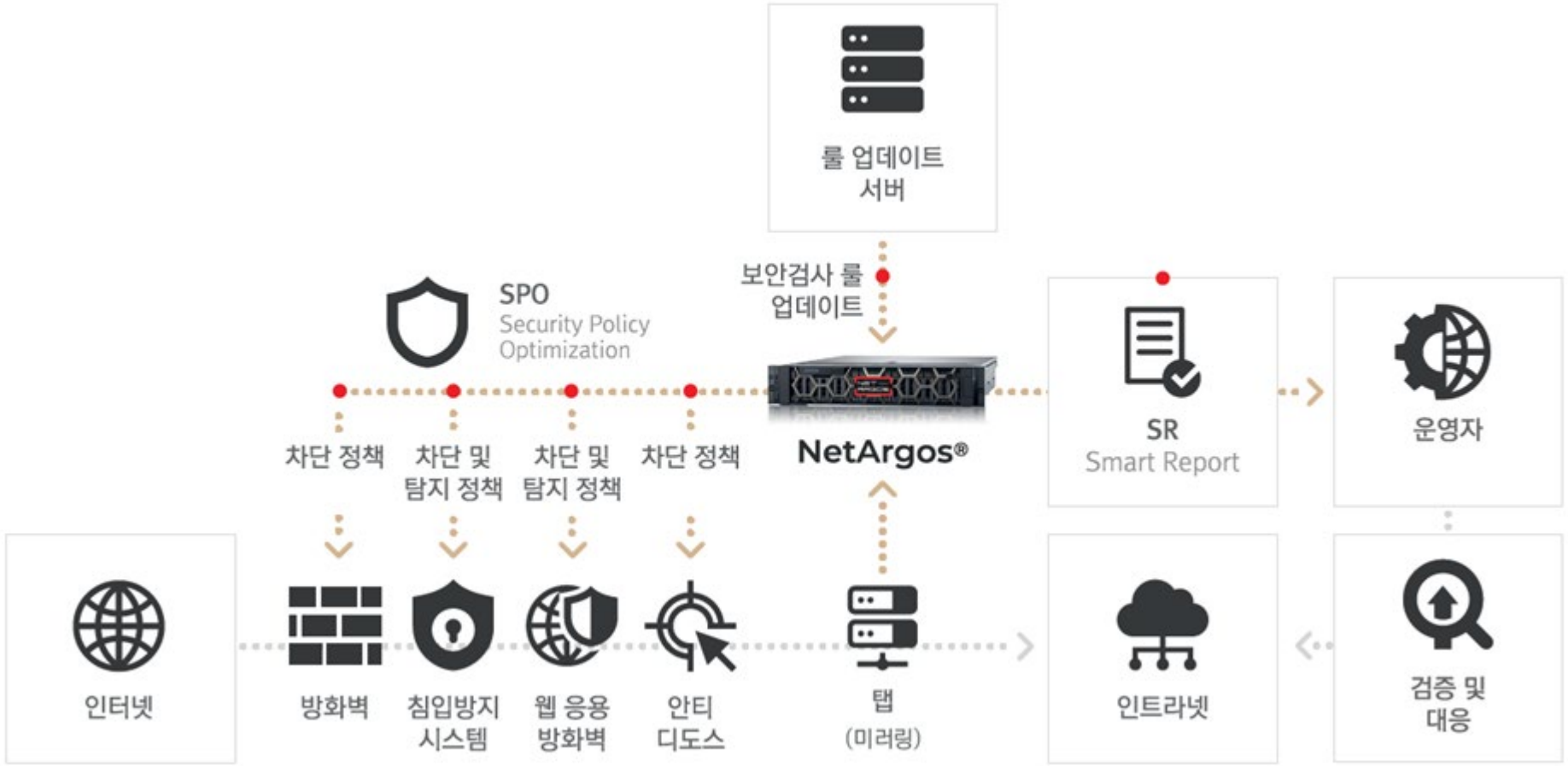
2 북한 해킹그룹 추정,

02. 제로데이 대응을 위한 새로운 보안 영역

( )
/ ZDR .



03. NetArgos제 품개요



03. NetArgos 제품개요

NetArgos® NDR(Network Detection & Response)
/ ,
FORENSIC (, ,) 1/50

네트워크 트래픽 데이터의 2% 저장

시간/운용상의 보안 사각 99.6% 대응

- 40Gbps
-

- 1 /1 /3
- AI(Expert System) /
-

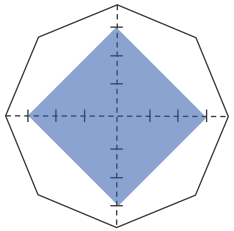
- First- N +FPC
- FORENSIC 50
(10G 3)

- DPI(Deep Packet Inspection)
- Drill- down
-

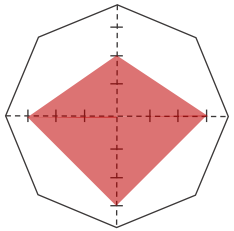
04. 핵심기술

ZDR

Theoretical

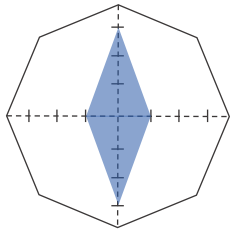


First- N

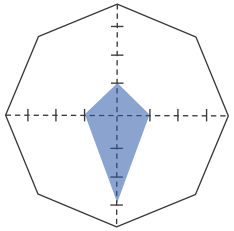


FPC

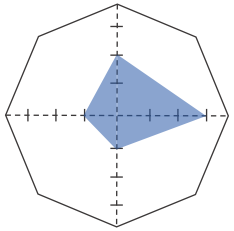
[Full Packet Capture]



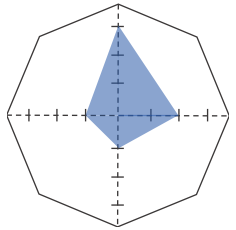
Packet Compression



Event- Driven



Packet Slicing



장기간First- N 방식 Packet 저장후 검사

- 1.8% 패킷 저장
- 99.6% 검출

"NetArgos 1대 = Forensic 50대"

매일제로데이에대한자동회귀보안검사 사전대응

VS

보안사고인지후 원인분석: 사후대응

짧은기간Full packet 저장후 검사(Forensic)

- 100%
- 100%

시험결과서

ETRI 한국전자통신연구원

연월일	문서번호	버전코드	페이지
2019.05.24.	NSQT-19-RNDT-0058	1.0	1/(54)

작성자	승인자	검토자	문서종류
이재정	남기동	류함양	TDP

NetArgos Public v1.0 시험결과서

2019. 07. 29.

통 신 미 디 어 연 구 소

I C T 시 험 연 구 실

ETRI 한국전자통신연구원

무단 전재/복사 금지 (ETRI Proprietary) ICT시험연구실

04. 핵심기술

5 접 /

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

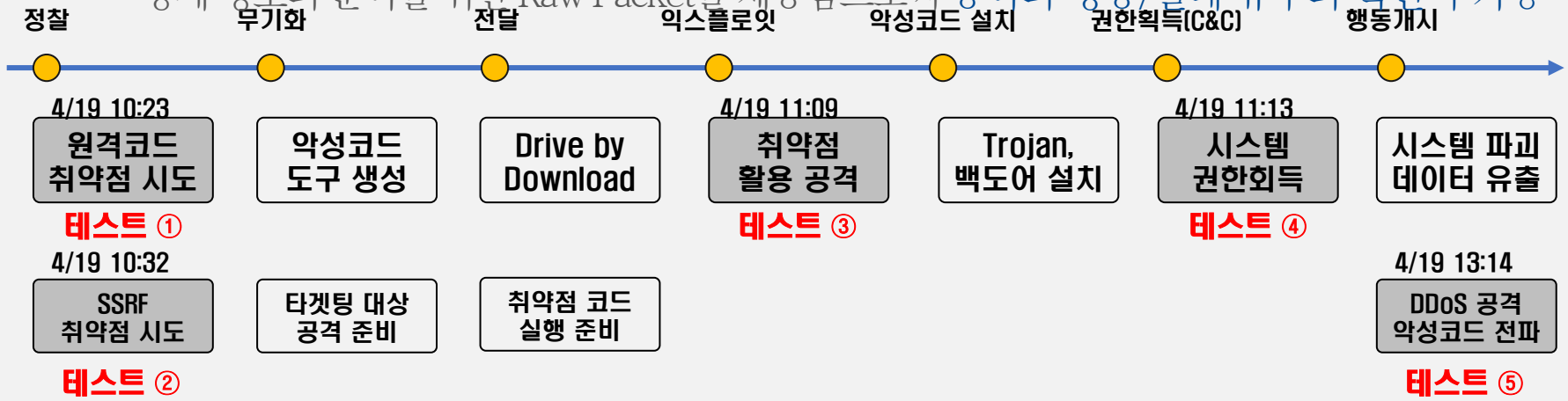
스마트 리포트(Smart Report)
보안 비전문가도 이해가 가능한 수준의 정보 정리 및 통계적 분석

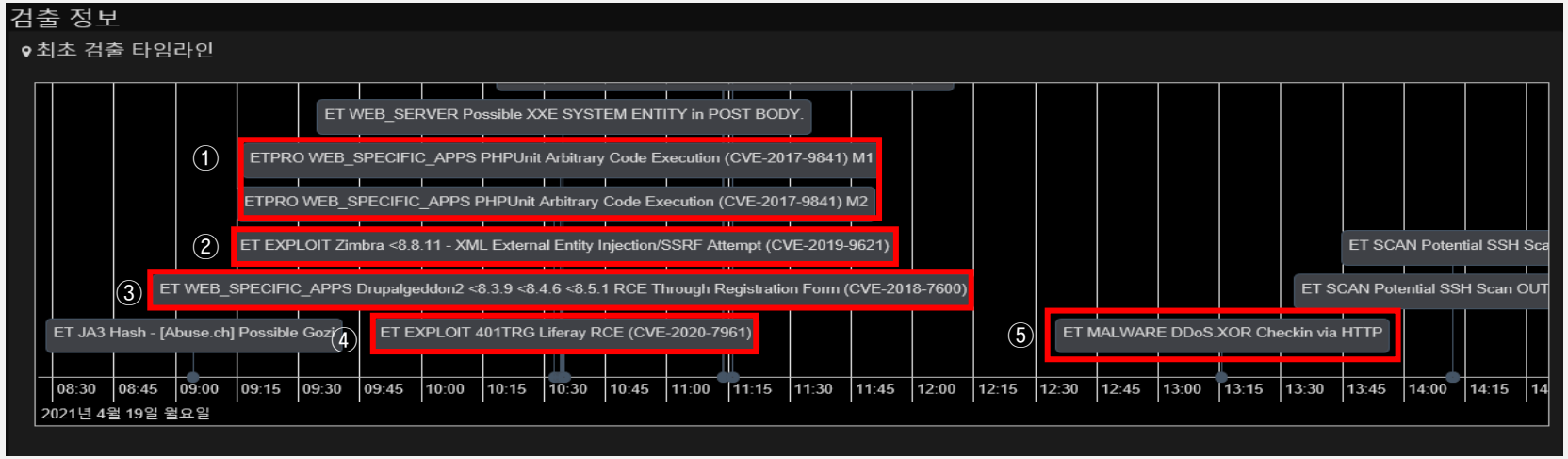
05 대응

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

04. 핵심기술: 신한DS 내부 모의테스트 및 증명 결과

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





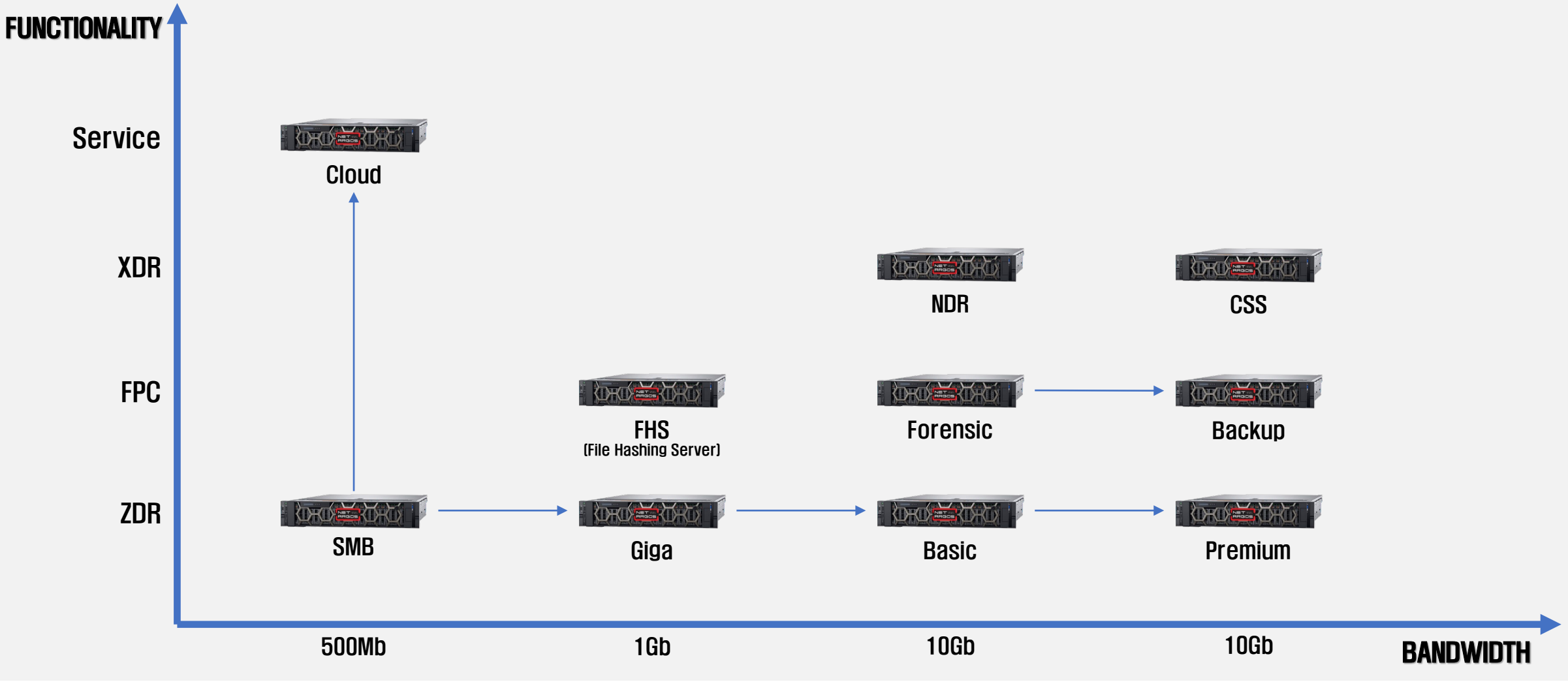
[공격 탐지 이벤트 시계열 정보 제공]

05. 제품및모델

처리성능 저장기간

상품구분	상품명	제품 형태	적용방식
독립형 어플라이언스	NetArgos		• 오프라인 형태로 패킷을 미러링 받아 분석 • 저장된 패킷을 회귀분석하여 과거 위협에 대한 재탐지 • 탐지된 결과에 기반하여 IN-LINE 보안툴에 제어정책 업데이트 • 처리용량에 따라 라이선스 구분
클라우드	NetArgos CLOUD		• 다양한 클라우드 환경내에 VM형태로 제공 • vSwitch에서 미러링 받은 패킷을 분석 후 리포팅

05. 제품및모델


FUNCTIONALITY
Service
XDR
FPC
ZDR
Cloud
NDR
CSS
FHS
(File Hashing Server)
Forensic
Backup
SMB
Giga
Basic
Premium
500Mb
1Gb
10Gb
10Gb
BANDWIDTH

06. 연동

NetArgos

- (/ /)
- /
-

- /
-

SIEM / SOAR

-
- , ,

APT / NDR / EDR

- /
-

FW / IPS / WAF

7. ZDR vs FORENSIC

LEGACY SECURITY ANALYTICS SOLUTION

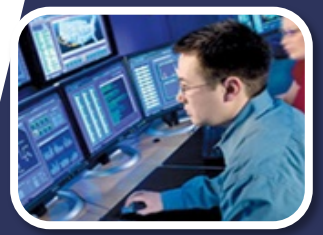
/

10G 1 3 4.5PB

, 64TB 75

1 /1

2.4GHz/8 50



XABYSS ZDRSOLUTION

/

First- N 1 3

50

1

1

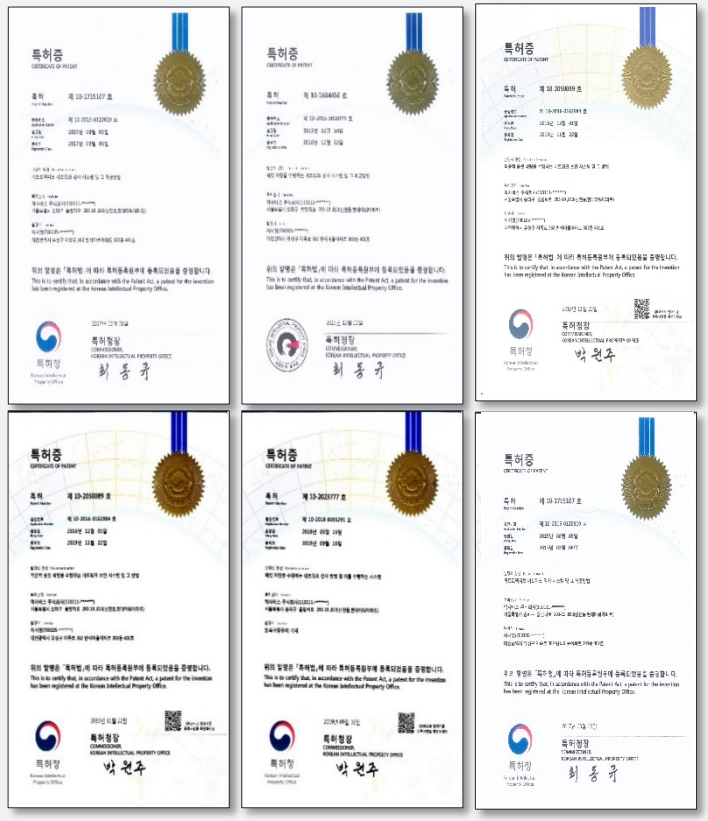
,

AI .

8. 기술검증

(1/50) (over 99%) ,

: 6 , 2



GS 1

8. 기술검증

Technology Partners | C

https://www.checkpoint.com/partners/opsec/

+1-866-488-6691 Contact Us Support Center User Center Blog

Check Point SOFTWARE TECHNOLOGIES LTD

PRODUCTS SOLUTIONS SUPPORT & SERVICES PARTNERS RESOURCES

world-class global professional services, award-winning customer

글로벌보안기업"Check Point"의 국내유일Technology Partner

Under Attack?

Chat

Contact

XABYSS

Xabyss

Enforcement

Founded in 2014 by a network and security expert, XABYSS (www.xabyss.com) is a supplier of software-defined network devices (SDND) that possesses unique, patented network packet capture technology. The company has developed and is distributing a 'cyber security CCTV' solution via NetArgos. Recently, XABYSS was selected as sole supplier of cyber security CCTV to the KOREA Army as part of establishing its next-generation intelligence management system that required the benefits of NetArgos.

Assets

Website

Solution Brief

네트워크및 보안전문가에의해2014년에설립된XABYSS(www.xabyss.com)는 고유한특허네트워크패킷캡처 기술을보유한소프트웨어정의네트워크장치(SDND) 공급업체입니다이 회사는넷아르고스를통해'사이버보안CCTV' 솔루션을개발하여보급하고있습니다최근XABYS는 넷아르고스의혜택이필요한한국국방에차세대정보관리시스템 구축의일환으로사이버보안CCTV의 단독공급사로선정되었습니다

This website uses cookies to ensure you get the best experience. GOT IT, THANKS! MORE INFO


Check Point | Xabyss

CHECK POINT + XABYSS
INTEGRATED THREAT PREVENTION

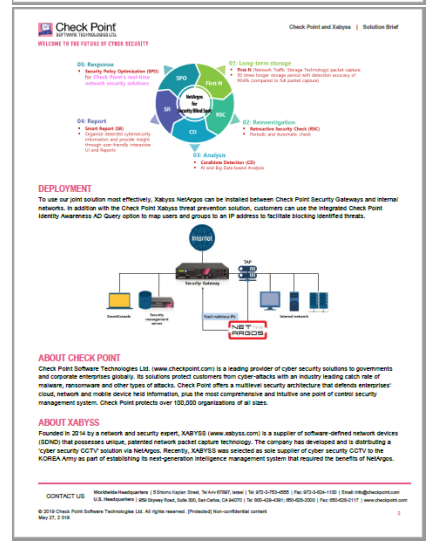
Benefits

Features

INSIGHTS

JOINT SOLUTION

INTEGRATED THREAT PREVENTION ECOSYSTEM


Check Point

DEPLOYMENT

ABOUT CHECK POINT

ABOUT XABYSS

TIGER CNS

NET ARGOS

Detect the Knife of Assassin

울

645- 2 H C615
Tel: +82- 70- 8113- 0013
Email: sales@tigercns.com