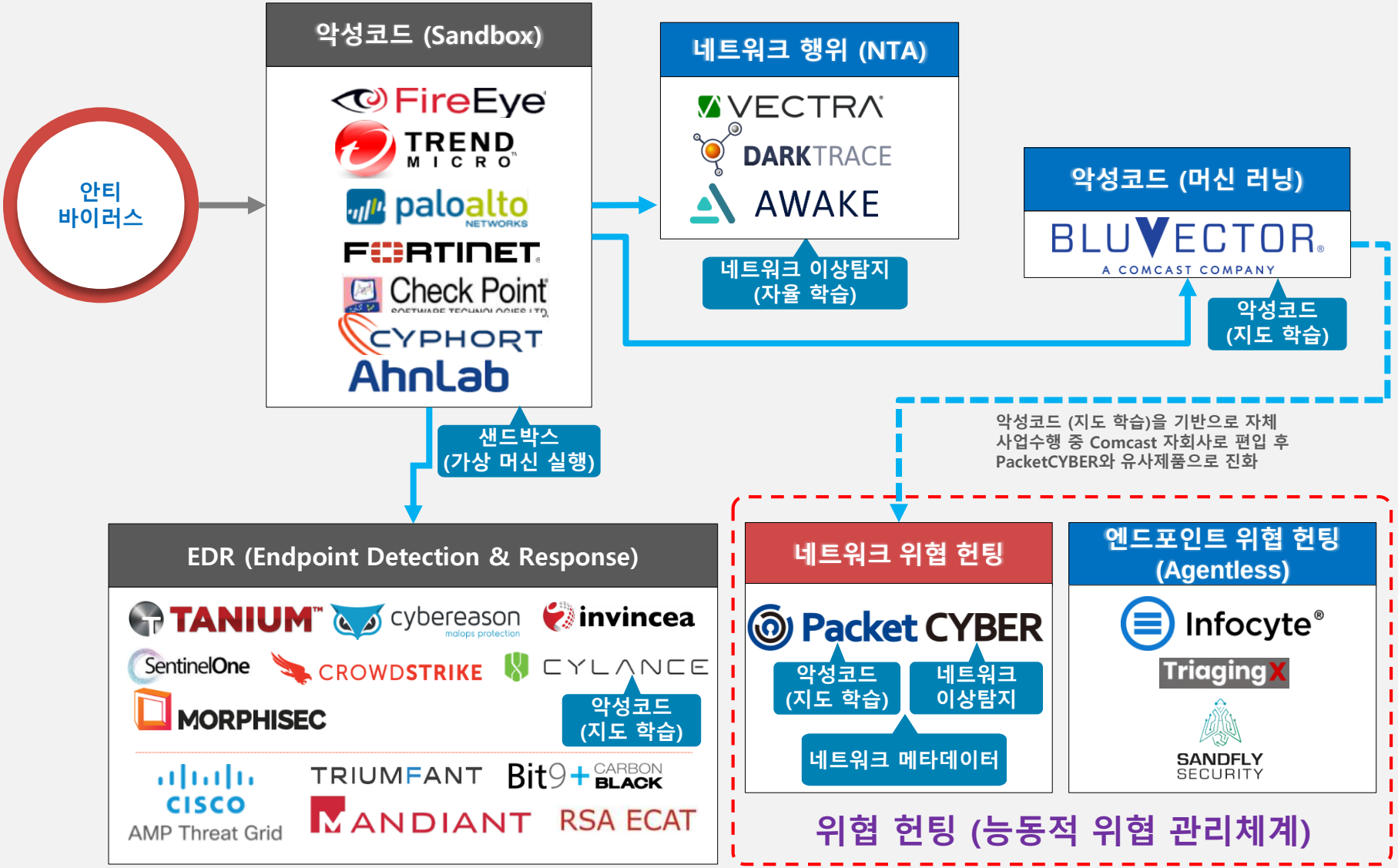
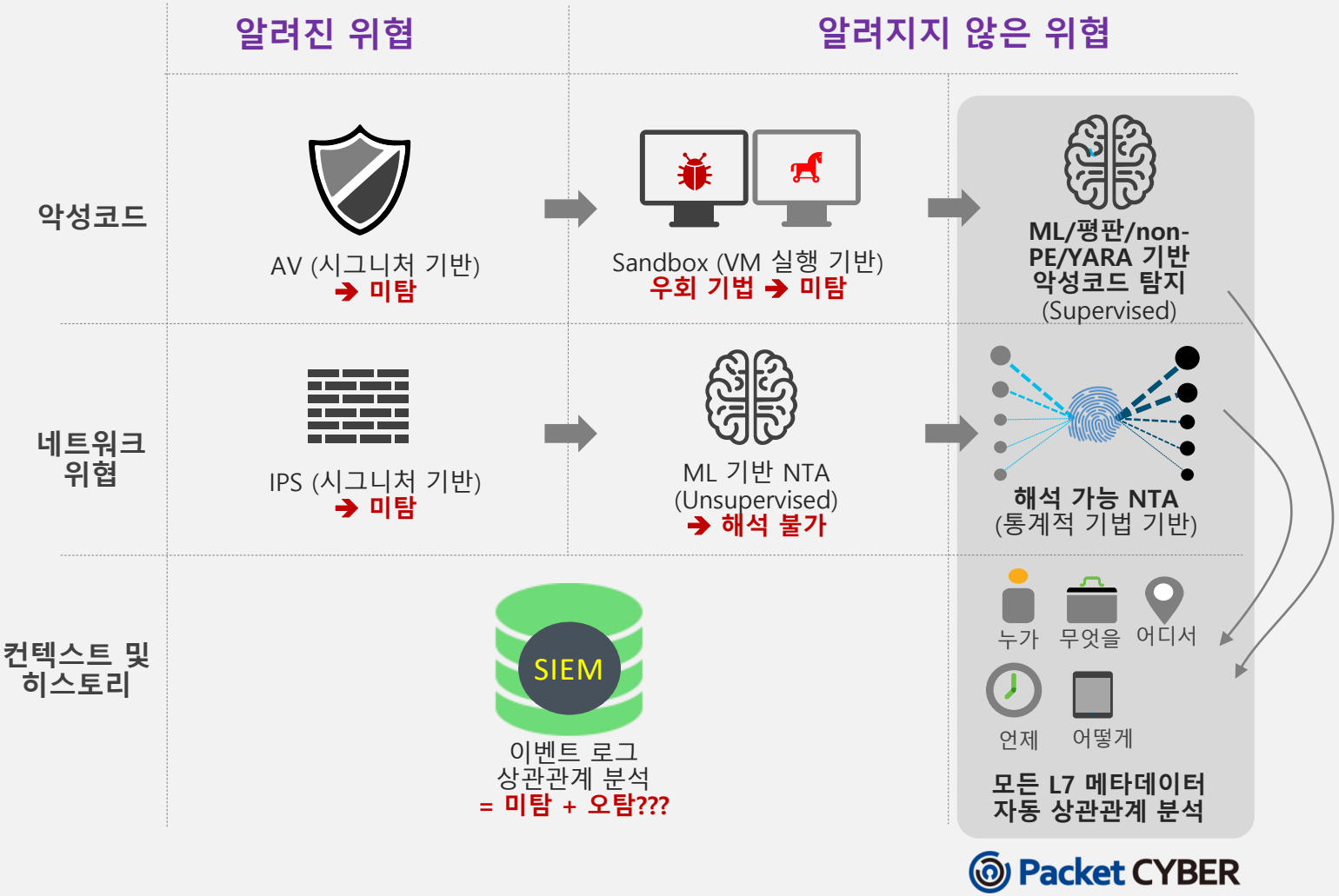
보안 기술의 진화 : 제안 배경



Our Solution: PacketCYBER 포지셔닝



공격은 방어보다 더 교묘합니다

44%의 위협은 자동화된 보안 도구로는 탐지되지 않음 [1]

1 2017 Threat Hunting Report, Crowd Research Partners

- ✓ 데이터 침해사고의 **> 90%** : 익스플로잇 사용
- ✓ **> 70%** 회사가 침해됨

- 이상 탐지
- 보안관제 센터
- 포렌식 침해 평가 팀

SIEM, EDR, UEBA

47%의 악성코드는 자체적으로 탐지하지 못하고 외부 기관에 의해 탐지 [2]

2 2017 M-trends, Mandiant

- ✓ **400,000 신종 악성코드**가 매일 출현

- 블랙/화이트 리스트
- 시그니처 (AV)
- 샌드박싱

- 파일 분석
- 휴리스틱
- URL 차단

Anti-Malware

왜 PacketCYBER인가?

OO시 CCTV 폐쇄망 침해

- ✓ 폐쇄망으로 운영되는 CCTV 네트워크에 이상 현상이 발생
- ✓ 어떠한 보안 솔루션으로도 원인 규명 불가능

➔ 업계 선도 샌드박스: Callback (X)
➔ 업계 선도 AI 기반 네트워크 이상 (X)

Packet CYBER

- ✓ 네트워크 이상 탐지에 대한 원인 규명 (자동)
- ✓ DPI 기반 모든 통신 기록 기반 헌팅으로 알려지지 않은 공격 요소들을 찾아냄 (수동)

왜 PacketCYBER인가?

OO시 데이터센터 침해

✓ 데이터 센터 네트워크에 침해사고 발생
✓ 잔여 위협 및 알려지지 않은 위협 파악 필요

➔ 외산 APT 등 다수의 보안 솔루션 사용
➔ 관제 센터 요원 29명이 보안 관제 중

✓ 외산 이메일 APT로 찾을 수 없었던 다양한 **이메일 위협 헌팅**
✓ 다양한 보안 솔루션 및 관제 인력으로도 **인지하지 못한 위협 헌팅**

왜 PacketCYBER인가?

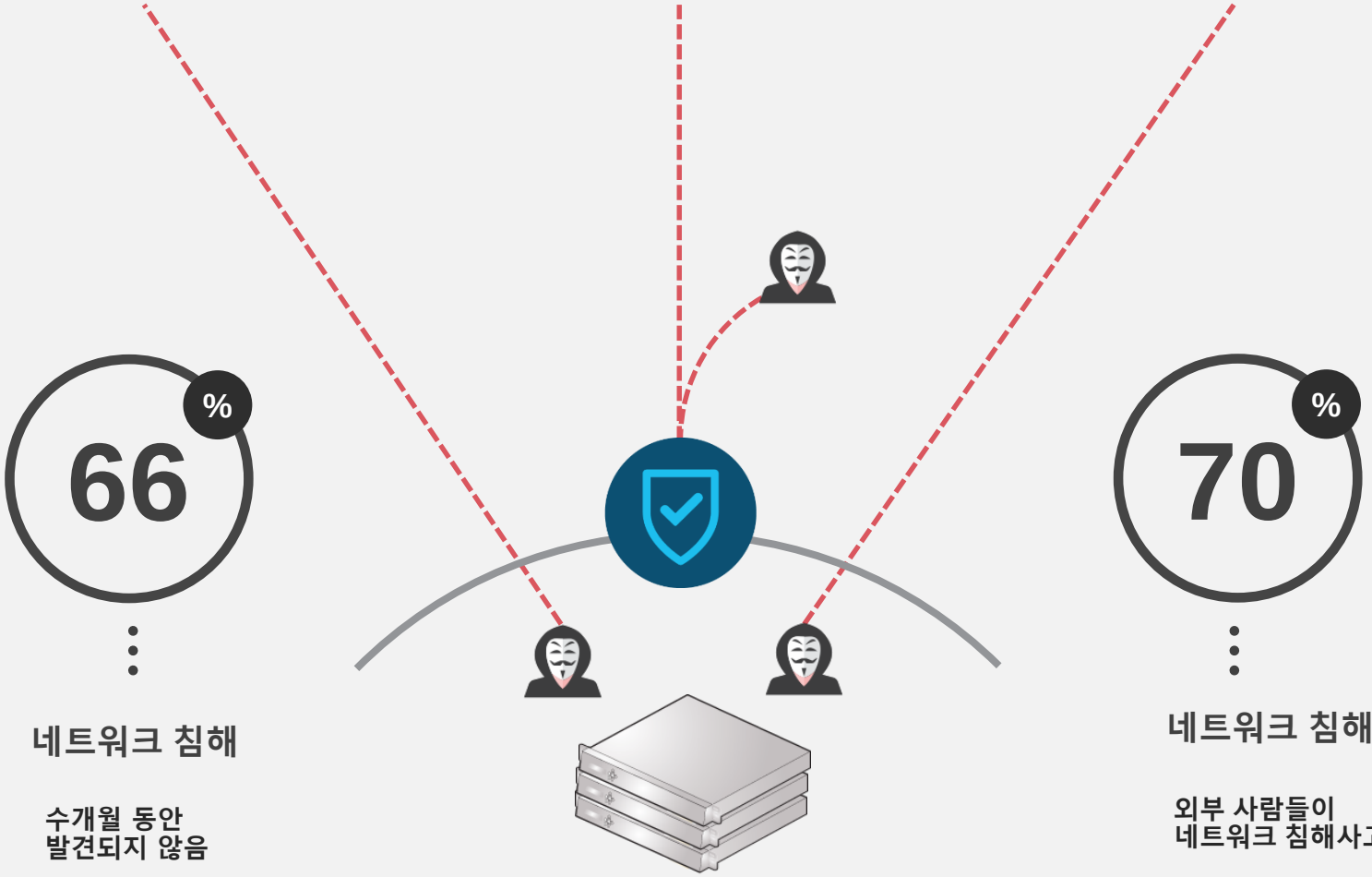
OO 중앙부처 사이버 안전센터

상급 기관으로부터 해킹 사고를 일으킨 IP 주소를 통보 받아 보안관제솔루션에서 탐색

➔ SIEM에서 탐색 실패
➔ 수개월간 보고서 제출 불가

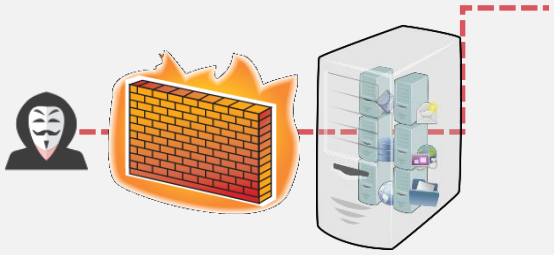
✓ DPI기반 모든 통신 기록 및 파일 다운로드 기록 및 고속 검색 지원 (정상/비정상 통신 여부와 무관)
✓ 수분~수십 분만에 해결

Problems: 모두가 침해되고 있다



Problems: 침해사고 이유는?

침입방지, 웹방화벽, 방화벽, 네트워크 샌드박싱(APT)



너무 정적이며 심각한 탐지 사각 지대가 있음
(※ 오탐 및 미탐)

SIEM(통합보안관제)

본질적으로 신뢰할 수 없는 데이터의 수집 및 분석
(※ 오탐 및 미탐)

트래픽 캡처 도구

너무 느리거나 분석가들에게 올바른 데이터를 제공하지 못함

Problems: 보안 및 위협 동향

44%

44%의 위협은 자동화된 보안 도구로는 탐지되지 않음 [1]

1 2017 Threat Hunting Report, Crowd Research Partners

47%

47%의 악성코드는 자체적으로 탐지하지 못하고 외부 기관에 의해 탐지 [2]

2 2017 M-trends, Mandiant

SOC: Big Data SIEM / AI기반 보안관제

가시광선 파장 중 380nm~780nm 사이의 스펙트럼

위협 헌팅: Detection & Response를 능동적으로 수행

사이버 위협 헌팅이란?

사이버 위협 헌팅은 능동적인 사이버 방어 활동으로서 **기존 보안 솔루션을 회피하는 지능형 위협을 탐지하고 격리하기 위해 네트워크를 통해 사전 및 반복적으로 검색하는 프로세스**임.
잠재적 위협에 대한 경고가 발생한 후 증거 기반 데이터를 조사하는 방화벽, 침입 탐지 시스템 (IDS), 맬웨어 샌드 박스 및 SIEM 시스템과 같은 기존의 위협 관리 조치와 대조됨.

공격 모델 (예: 킬 체인 관점의 ATT&CK, NSA ...)

- ✓ 기본 소양(Programming, Data Science, 지식...)
- ✓ 무엇을 찾을 것인가?
  - 위협 모델 및 프레임 워크
  - 공격자 활동 (TTP) 모델
  - Post-Compromise 행위 목록
  - Post-ATT & CK (MITRE)

사이버 위협 헌터

기본 소양(C-Programming, 스크립팅, Data Science, 보안 전문지식...)

위협 헌팅: 네트워크 POST-EXPLOIT 증거 확인

- ✓ C&C (레이어 7 필요)
- ✓ 예상하지 않은 내부 ←→ 내부 트래픽
- ✓ 실행 파일
- ✓ SSL 인증서
- ✓ 패스워드 스프레이, 추측, 무차별 대입
- ✓ 네트워크 공유 및 사용자 검색

통신 및 파일 메타데이터

- ✓ DNS
- ✓ HTTP
- ✓ SSL Certs
- ✓ SMTP
- ✓ SMB
- ✓ TCP/UDP/ICMP/IP
- ✓ 파일...

네트워크 포렌식 vs. 사이버 위협 헌팅

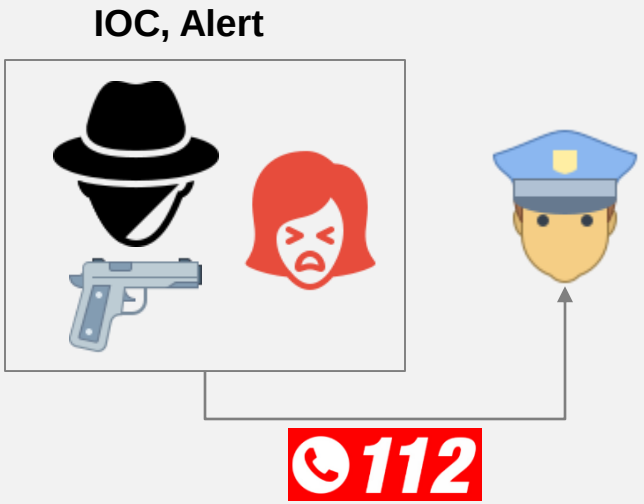
DFIR

DFIR (Dee-Fur로 발음)은 Digital Forensics & Incident Response (디지털 포렌식 및 침해사고 대응)은 사이버 악성 행위에 대한 대응을 의미함.

DIFR은 일반적으로 IOC (Indication of Indicator) 가 알려 지거나 네트워크 / 호스트 침입 탐지 시스템에서 이벤트 / 경고가 트리거 될 때 수행됨.

➔ **수동적**

범죄 발생 신고



CYBER THREAT HUNTING

Cyber Threat Hunting (Hunting)은 "기존 보안 솔루션을 회피하는 지능형 위협을 탐지하고 격리하기 위해 네트워크를 통해 사전에 능동적이고 반복적으로 탐색하는 프로세스"

Cyber Threat Hunting (Hunting)은 IOC (Indication of Indicator) 와 관계없이 네트워크 / 호스트에 대한 위협을 선제적이고 지속적으로 탐색함.

➔ **능동적**

우범 지대 순찰 강화

Solution: Gartner : 차세대 보안

44%의 위협은 자동화된 보안 도구로는 탐지되지 않음 [1]

1 2017 Threat Hunting Report, Crowd Research Partners

사이버 위협 헌팅?

3.5M
Openings
5 년 동안 채워지지 않은 사이버 보안 직원 (Cybersecurity Ventures 2017)

Gartner.

자동화된 보안

Prevent
공격 표면 최소화

위협 헌팅

Response
분석 및 조치

Detection
침해사고/위협 인지

알려진 위협 대응

- ✓ Firewall, IPS, NGFW, WAF…

알려지지 않은 위협 대응

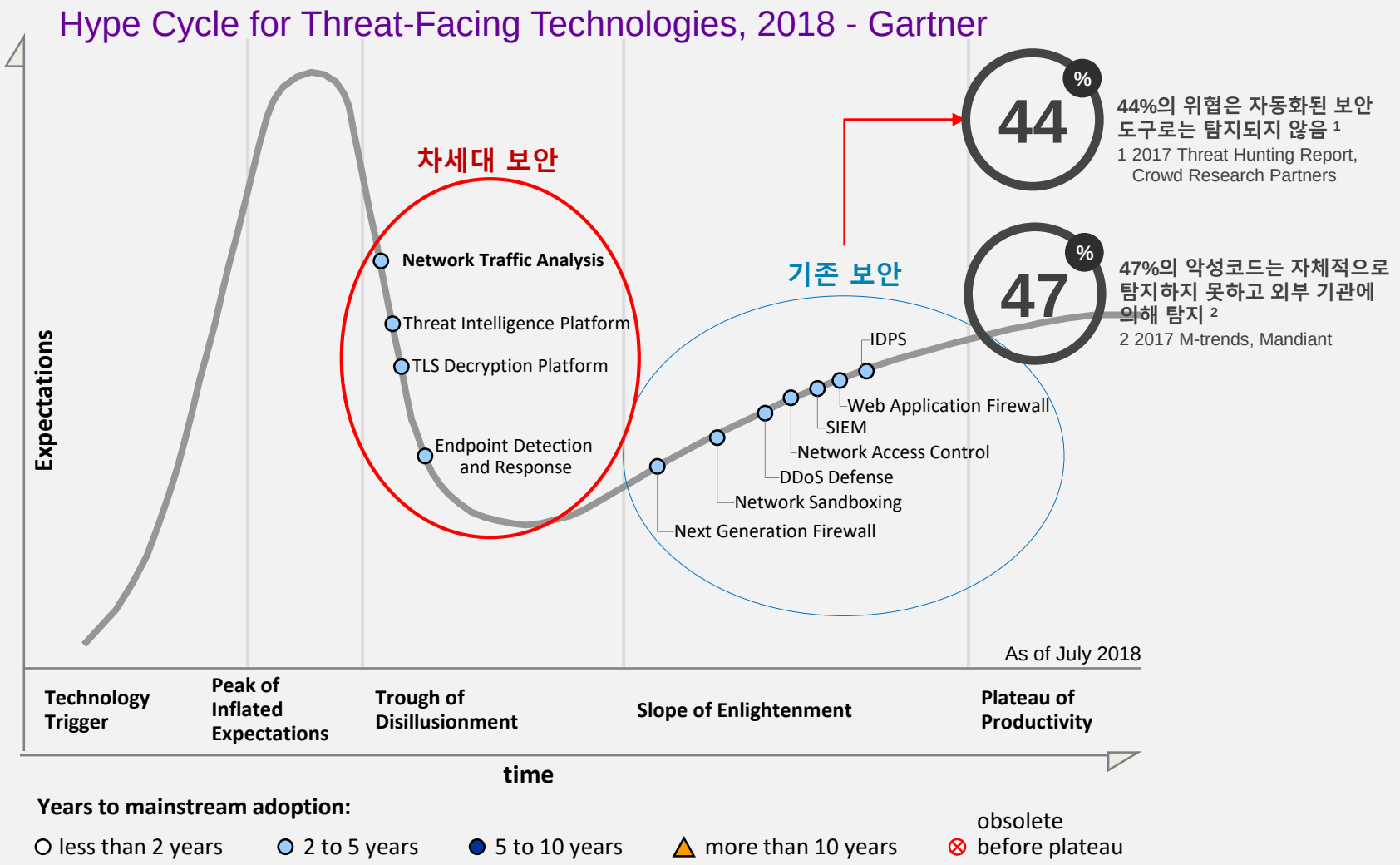
- ✓ NTA (Network Traffic Analysis, NDR)
- ✓ EDR (Endpoint Detection & Response)

- ✓ 탐지 및 대응(Detection & Response)과 결합되지 않은 방어(Prevention)는 효과가 없다".
- ✓ 2017년 탐지 및 대응(Detection & Response)이 조직 보안의 최상위 우선 순위!
- ✓ 향후 5년 동안 보안 시장 성장을 주도

https://www.gartner.com/newsroom/id/3638017

Solution: 글로벌 동향: Gartner : Hype Cycle

– 위협 대응 관련 기술



[1] 2017 Threat Hunting Report, Crowd Research Partners
[2] 2017 M-trends, Mandiant

Solution: 외산 AI 기반 NTA (Network Traffic Analysis) 벤더

제품

벤더	제품명	투자현황	기타
DarkTrace/영국	Enterprise Immune System	• Enterprise Immune System • 2013년 창업 • 2,766 억 원 이상 투자유치	국내진출
Vectra AI/미국	Cognito Detect	• AI-driven threat detection and response • 2010년 창업 • 2,670억 원 이상 투자유치,	국내진출
Awake Security/미국	Awake Security Platform	• Advanced Network Traffic Analysis Solution • 2014년 창업 • 360억 원 이상 투자유치,	국내진출

『보안에서 '인공 지능' 이라는 표현이 붙을 만한 기술은 아직 존재하지 않는다.
현 시점에서 인류가 보유한 기술을 가장 정직하게 표현하는 말은 *'머신 러닝'* 이라고 생각한다.』

『 자율학습 기반 머신 러닝을 적용한 NTA는 **비정상 행위나 공격을 탐지해내는 데 있어서는 매우 제한적이다.**
물론 클러스터링(clustering)이라는 데이터 '묶어 내기' 기술로 이를 보완하는 방법을 개발 중에 있으나,
아직 도착점에서는 상당히 멀어 보인다. 특히 알고리즘의 '클러스터링' 기준을 아직 아무도 설명할 수 없기에,
이를 상용화하려는 시도는 먼 훗날의 얘기다.』

- RAFFAEL MARTY, 보안 및 인공지능 전문가, black hat USA, 2018

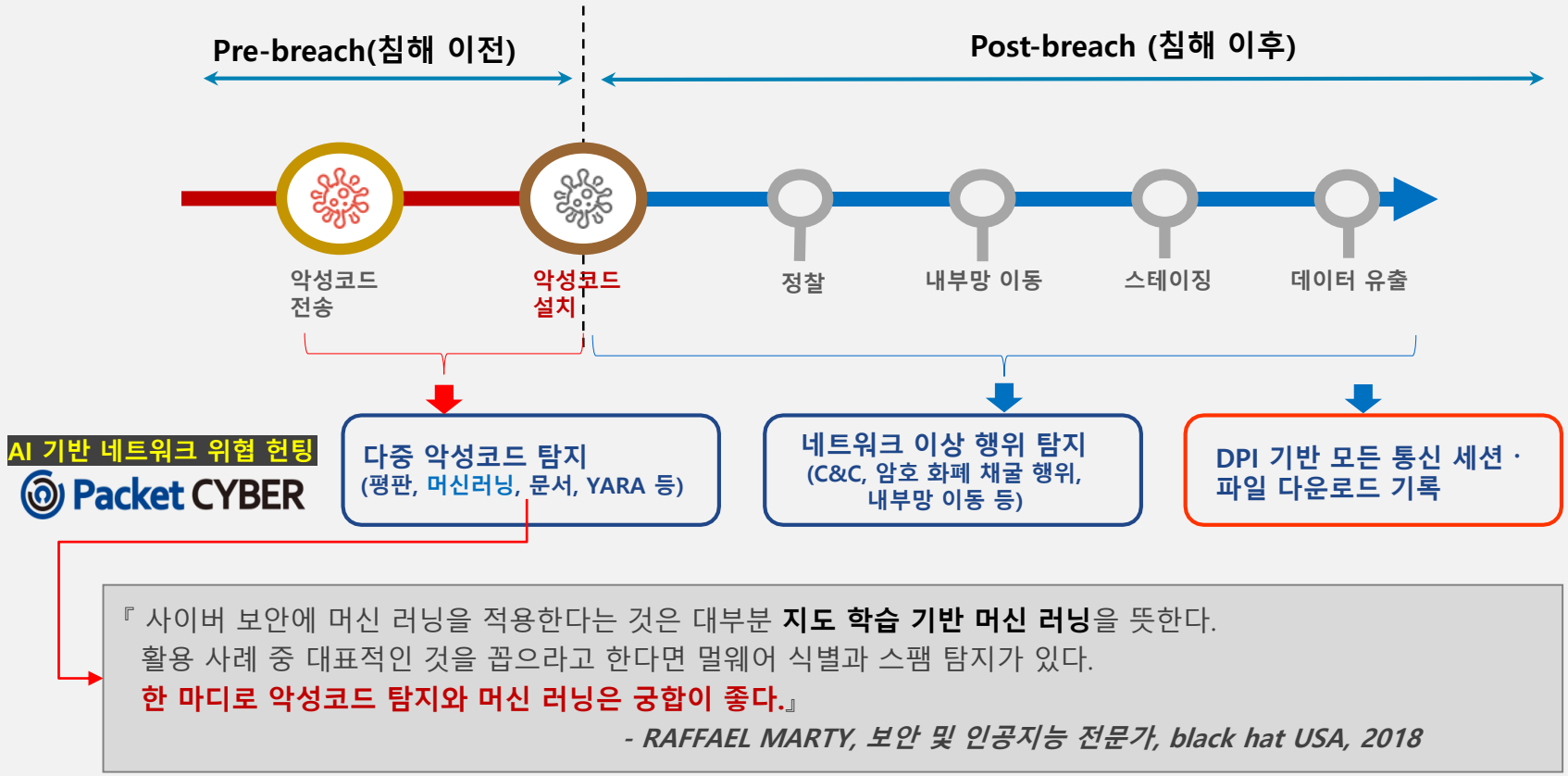
Problem: 외산 AI기반 NTA(Network Traffic Analysis) 솔루션

✓ 네트워크 보안 분석가: "신뢰할 수 있지만 검증은 필수 "

✓블랙 박스(Black-Box) 머신 러닝은 이해하기 어렵기로 악명이 높다!!!

✓실행 및 설명 가능한 NTA 메커니즘을 제공 할 수 있을 것인가?

Our Solution: PacketCYBER – 네트워크 위협 헌팅



『 사이버 보안에 머신 러닝을 적용한다는 것은 대부분 **지도 학습 기반 머신 러닝**을 뜻한다.
활용 사례 중 대표적인 것을 꼽으라고 한다면 멀웨어 식별과 스팸 탐지가 있다.
한 마디로 악성코드 탐지와 머신 러닝은 궁합이 좋다.』

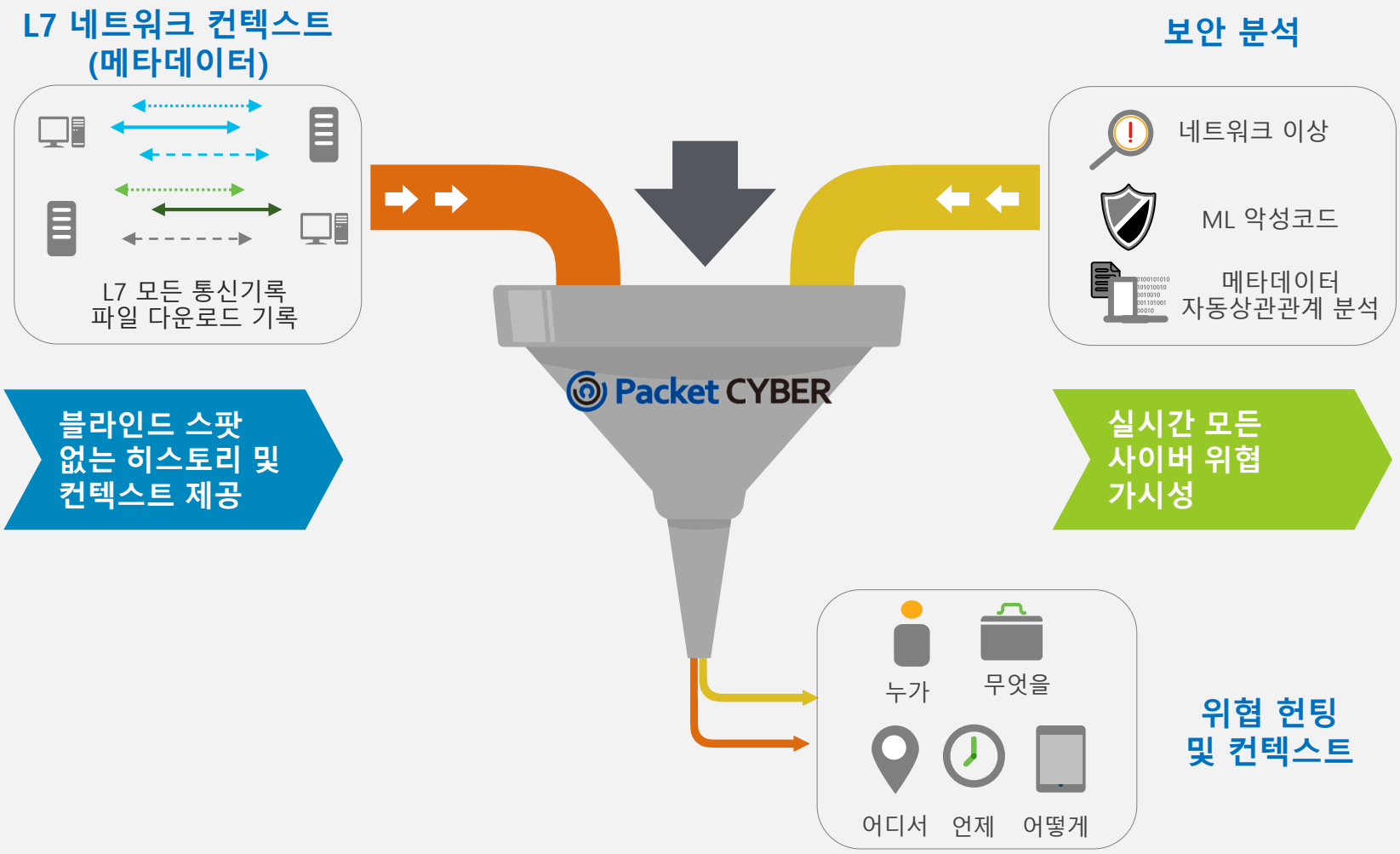
- RAFFAEL MARTY, 보안 및 인공지능 전문가, black hat USA, 2018

2019년 7월 과학기술정보통신부 권고

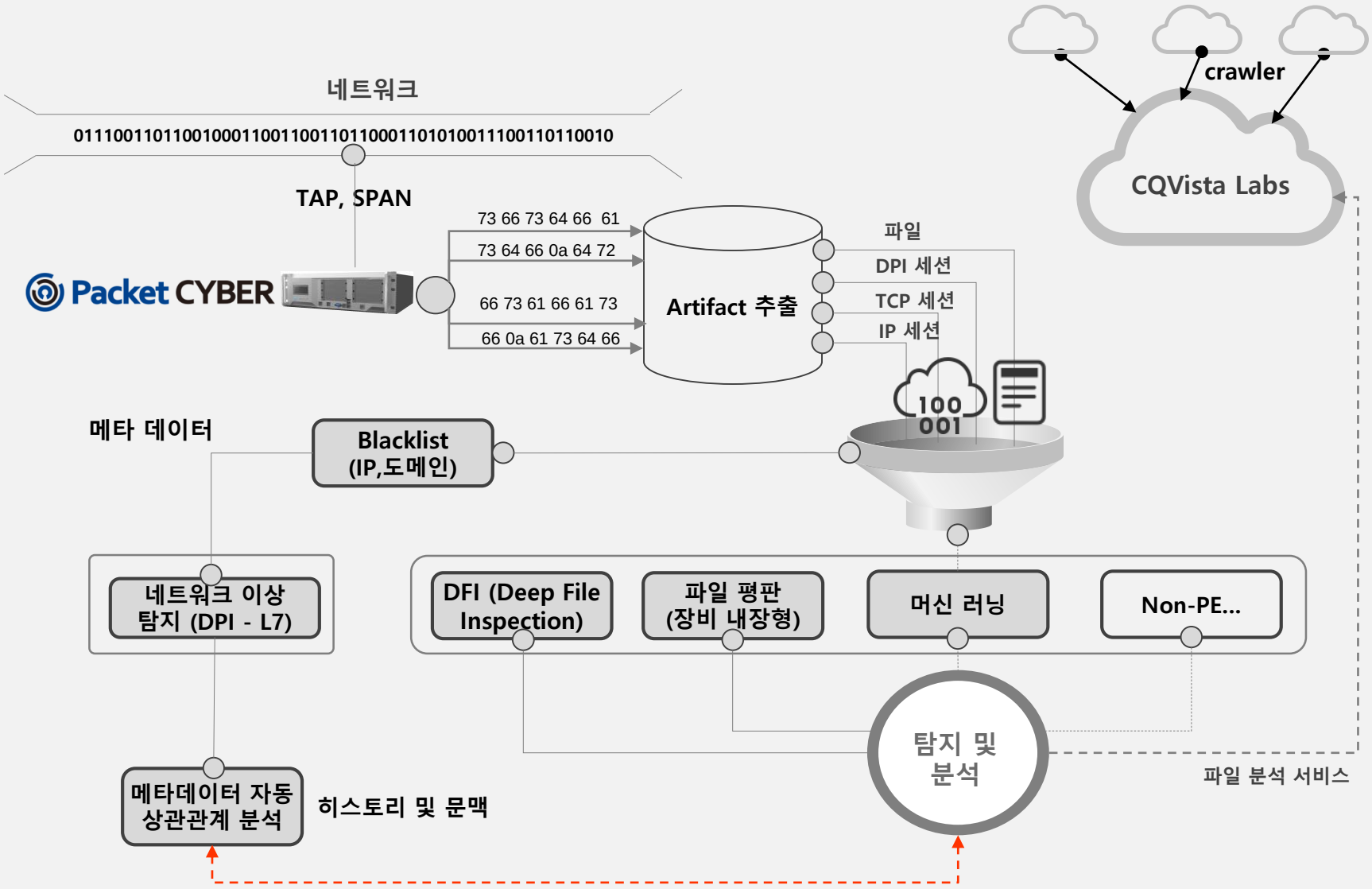
최초 침투 행위 방어 뿐만 아니라 "해커의 공격이 계속되는 과정" 에서 위협을 적기에 식별하고 대응할 필요

➔ **능동적 위협 관리체계로 개선**

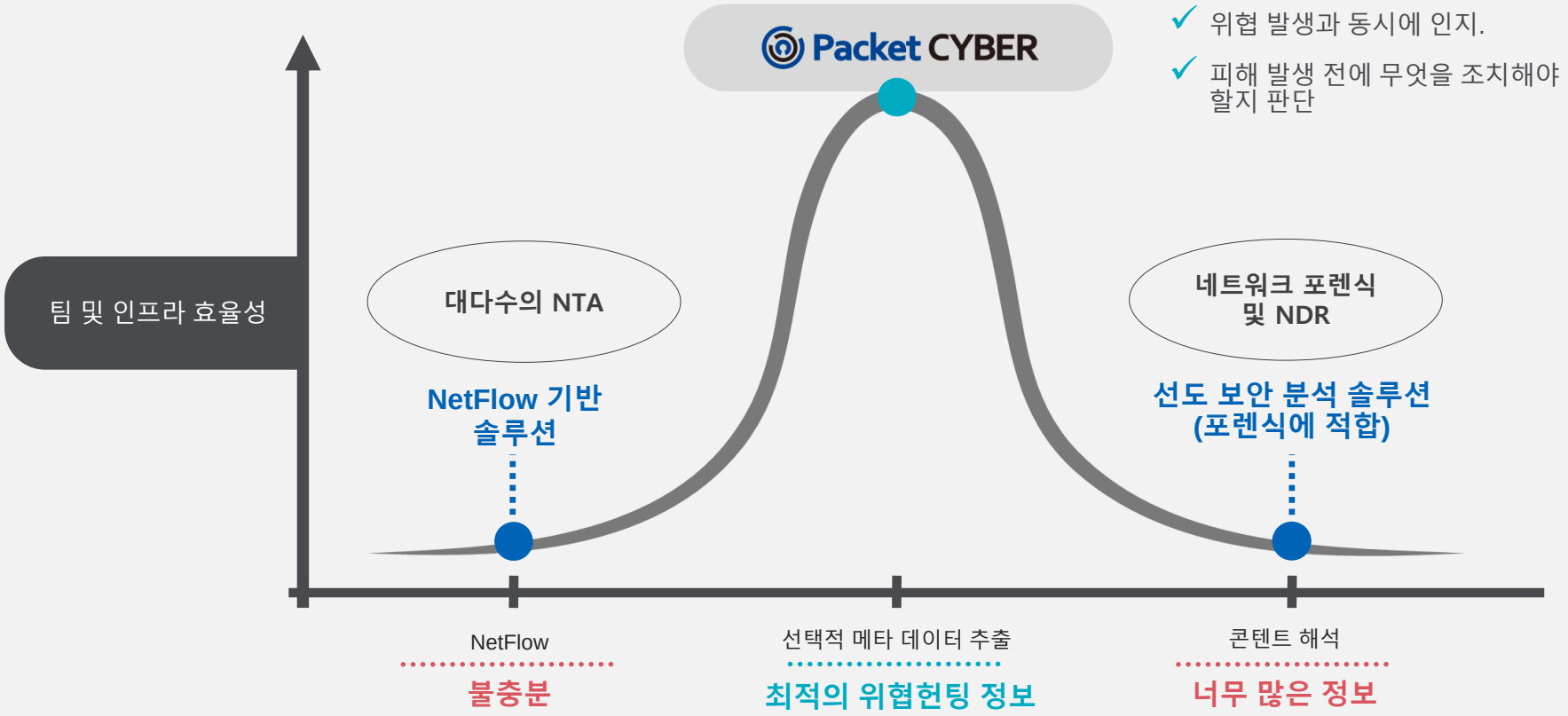
Our Solution: PacketCYBER 아키텍처



Our Solution: PacketCYBER 아키텍처



차별화 : 유사 실시간 이내에 완전한 분석정보 제공



타사 NTA 솔루션 비교

외산 NTA는 위협 의심 트래픽을 탐지하여 이를 관리자에게 보고하는 기능을 제공합니다.
PacketCYBER는 다중분석 및 모든 통신 사실 분석을 통하여 위협 여부를 판정하고 헌팅 할 수 있습니다.
또 위협의 유입 경로를 정확히 확인하고 분석할 수 있습니다.

PacketCYBER vs 타사 NTA 솔루션 비교

PacketCYBER

Layer 7 NTA

- 트래픽 수집
- 악성코드 탐지
- 네트워크 이상 탐지
- 킬 체인 분석
- 통신 사실 및 기록 분석

타사 NTA (외산) 솔루션

Layer 4 NTA

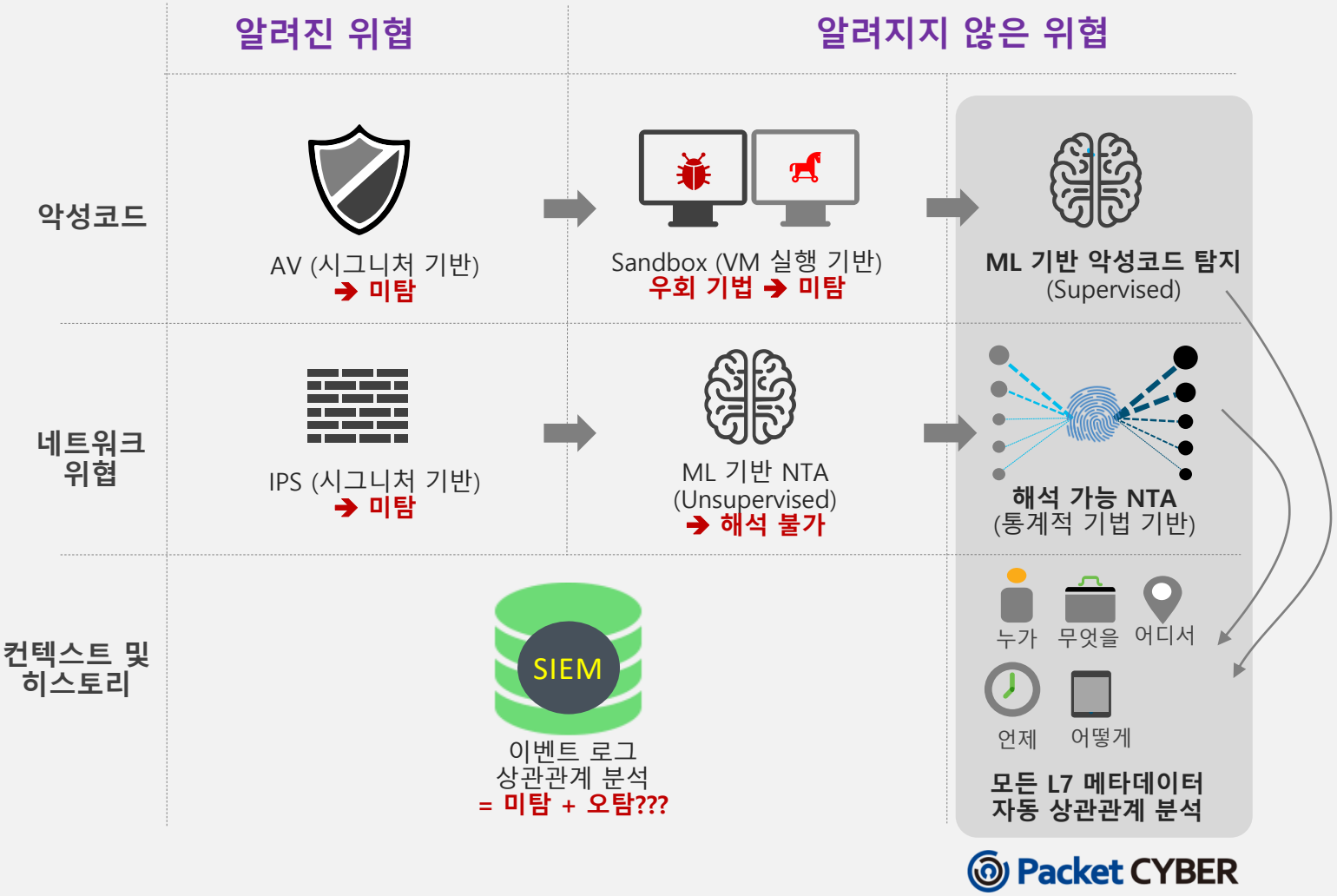
- 트래픽 수집
- 네트워크 이상 탐지

대부분의 **AI 기반 네트워크 보안 제품들은 악성행위에 대한 이해 없이 AI를 네트워크 트래픽에만 적용하고 있음.**
이러한 **통계적 접근은 많은 오탐을 유발함.** – ***결국 모든 이상은 공격의 결과로 발생하는 것은 아님.***

AI 기술을 네트워크 트래픽에 적용하면 필연적으로 네트워크 트래픽 내에서 비정상적인 동작 패턴을 탐지하게 되며 이는 AI를 사용하여 그렇게 하도록 설계된 기능임.
하지만 AI 기반 도구들은 탐지된 이상이 악성인지 정상인지 이해하는 것은 사실상 불가능함.

결과적으로 이러한 기술은 **충실도가 낮은 통계적 경보를 발생** 시키며 **여러 시간에 걸친 조사가 필요**하므로 **침해사고 대응 속도를 느리게 만듦.**

Our Solution: PacketCYBER 포지셔닝



PacketCYBER: 자동화된 네트워크 위협헌팅

위협 헌터

위협 인지

① 악성코드 탐지 / 위협 사이트 탐지 / 이상 행위 탐지 (킬-체인 분석) 등의 경고 확인

위협 내용 확인

② 위협 의심 이벤트의 내용을 이벤트 상세 창에서 확인
(필요 시 Virustotal / whois 등과 같은 정보 추가 확인)

연관 통신기록 분석

③ 위협 의심 이벤트와 직접 관련된 통신기록 확인
④ 위협 의심 이벤트 관련 IP의 과거 통신기록 확인

위협 특정

⑤ 위협 관련 사항이 분명하고 통신 기록이 위협 내용 부합 시, 위협 특정

위협 대응

⑥ 확정된 위협에 따른 대응 방법을 강구하여 조치

제품 라인업

구분	P-500XF (500Mbps)	P-1000XF (1Gbps)	P-2000XF (2Gbps)
CPU	Intel Xeon E5-2620 (6CORE) * 2	Intel Xeon E5-2620 (6CORE) * 2	Intel Xeon E5-2680 (14CORE) * 2
메모리	SAMSUNG 16G DDR4 ECC * 6	SAMSUNG 16G DDR4 ECC * 8	SAMSUNG 16G DDR4 ECC * 16
SSD	512G SSD * 4	1TB SSD * 4	1TB SSD * 6
인터페이스	1G Copper (Intel i350) * 4	1G Copper (Intel i350) * 4 (10GbE Fiber * 2 – 옵션)	1G Copper (Intel i350) * 4 10GbE Fiber * 2
전원	750W 1+1 ATX Redundant Power	750W 1+1 ATX Redundant Power	750W 1+1 ATX Redundant Power

트래픽 분석 기반 보안 관리 PacketCYBER P-500XF

88,000,000원 유사상품 검색

* 위 가격은 업체가 조달청에 제출한 견적가격입니다.

업체명	주식회사 씨큐비스타	사업자등록번호	1208688075
식별번호	23403169	단위	조
/공급	제조	창업기업	N
중기간경쟁제품	N	벤처기업	Y

벤처·창업기업 제품 전용몰 조달청 벤처나라

나라장터 종합쇼핑몰

시장 검증 (Market Validation): 경쟁 우위

네트워크 기반 위협 헌팅 솔루션 "패킷 사이버(PacketCYBER)"는 다수의 중앙 부처 사이버안전센터 등에 공급함으로써 기술력과 효과를 인정받았으며, 일부 금융권에서는 미국 및 영국 등의 글로벌 보안 업체들 대비 경쟁 우위를 확보하였습니다.

공공 기관 (최근 구축 사례)

중앙부처 사이버안전센터

민간 기업 (구축 사례)

기업 보안관제 센터

일본 @Tokyo 센터

공공 기관 (예산 확정)

지방자치단체 및 광역단체

중앙부처 사이버안전센터

금융 기관 (예산 확정)

증권사

카드사

OO 은행

사용자 검증 (User Validation): 위협 헌팅 사례

1

경기도 OO (OO시)
CCTV 폐쇄 망이 침해되어 원인을 분석하기 위해 세계최고의 APT 솔루션과 네트워크 이상탐지 솔루션으로 문제를 해결하고자 하였으나 실패하였다.

PacketCYBER를 설치하여 1주일 만에 모든 침해 현상을 분석할 수 있었다.

단연코 PacketCYBER가 세계 최고의 솔루션이다.

2

전라남도 OO (중앙부처)
국산 APT 및 외산 APT 솔루션을 고루 검토하였으나, 탐지 및 분석 기능이 마음에 들지 않아서 도입하지 못했다.

PacketCYBER는 악성코드 뿐만이 아니라 네트워크 이상 탐지를 지원하는 동시에 모든 통신 기록에 기반한 메타데이터와 자동 상관관계 분석을 제공하여 도입하게 되었다.

3

서울 OOO (중앙부처)
센터에서 다수의 국산 APT를 운영 중이나, 악성코드 탐지 효율성이 미흡하여 고심하였다.
국산 APT에서 잘 검출되는 않는 악성코드 1500개로 PacketCYBER를 테스트하였는데, 거의 완벽하게 탐지하였다.

PacketCYBER는 인공지능 기반의 지능형 위협 관리 시스템으로서 손색이 없다.

4

서울 OOO (OO 증권)
보안 관제를 고도화하기 위하여 외산 인공지능 기반 네트워크 이상탐지 솔루션들을 검토하였으나 운영이 너무 어려워서 고심하였다.

PacketCYBER는 외산 인공지능 기반 네트워크 이상탐지 대비 비교적 운영이 간편하여 선정하게 되었다.

5

서울 OOO (OO 기관)
외산 APT 및 다양한 보안 솔루션과 보안관제센터를 운영 중에 침해사고가 발생하였다. 침해사고 및 잔여 위협을 분석할 수 있는 솔루션이 없어 고심하였다.

PacketCYBER를 설치하여 1주일 만에 모든 침해 현상을 분석할 수 있었을 뿐만 아니라 어플리케이션 프로그램 오류를 확인할 수 있었다.

6

경기 OOO (OO 카드)
보안 관제를 고도화하기 위하여 외산 인공지능 기반 네트워크 이상탐지 솔루션과 네트워크 포렌식 솔루션들을 검토하였으나 운영이 너무 어려워서 고심하였다.

PacketCYBER는 외산 인공지능 기반 네트워크 이상탐지 대비 비교적 운영이 간편하여 선정하게 되었다.

NSA TAO 표적 침입 대응 전략

National Security Agency

	NSA 해커 조직 APT 공격 기법	NSA APT 공격 대응 권고사항	네트워크 위협헌팅
1	**초기 정찰 (Initial Reconnaissance)** • 스캐닝 : 운영 체제 식별, 취약점 조사	**초기 정찰 (Initial Reconnaissance)** • 스캐닝 탐지 • 중요 자산 접속 감시 • 내부 네트워크 감시	• 모든 트래픽 메타데이터 저장 : DPI 기반 • 연관 트래픽 고속 검색 : 위협헌팅 토대 (권고사항: 전체)
2	**초기 침입 (Initial Exploitation)** • 악성코드 첨부 이메일 발송 • 감염 웹사이트 접속 유도 • 감염된 이동식 매체 발송	**초기 침입 (Initial Exploitation)** • **악성코드 탐지 : 파일 평판**	• 악성코드 탐지: 평판, 머신러닝, 문서 (권고사항: 2, 4) • 위협 의심 트래픽 탐지: 평판 도메인, 행위 (권고사항: 1, 3, 5, 6) • 침입 Kill-Chain 분석: 위협 가시성 제공 (권고사항: 전체)
3	**지속성 확보(Establish Persistence)** • 추가 백도어 설치 • 은닉	**지속성 확보(Establish Persistence)** • 사용자 행위 감시 • 악성사이트 탐지 : 도메인 평판 • 내부 네트워크 감시	
4	**공격 도구 설치 (Install Tools)** • 추가 공격 도구 다운로드	**공격 도구 설치 (Install Tools)** • **악성코드 탐지 : 파일 평판**	• 자동 상관관계 분석: 탐지된 위협과 트래픽 매칭 • 위협헌팅 컨텍스트: 트래픽 추적 제공 (권고사항: 전체)
5	**내부망 이동 (Move Laterally)** • 중요 시스템 또는 중요 데이터베이스로 이동	**내부망 이동 (Move Laterally)** • 내부 네트워크 감시 • 계정 접속 감시	
6	**수집 / 유출 (Collect, Exfil, Exploit)** • 중요 데이터 유출 • 데이터 손상, 조작 및 파괴	**수집 / 유출 (Collect, Exfil, Exploit)** • 실시간 네트워크 모니터링 • 해커가 노리는 대상 파악	

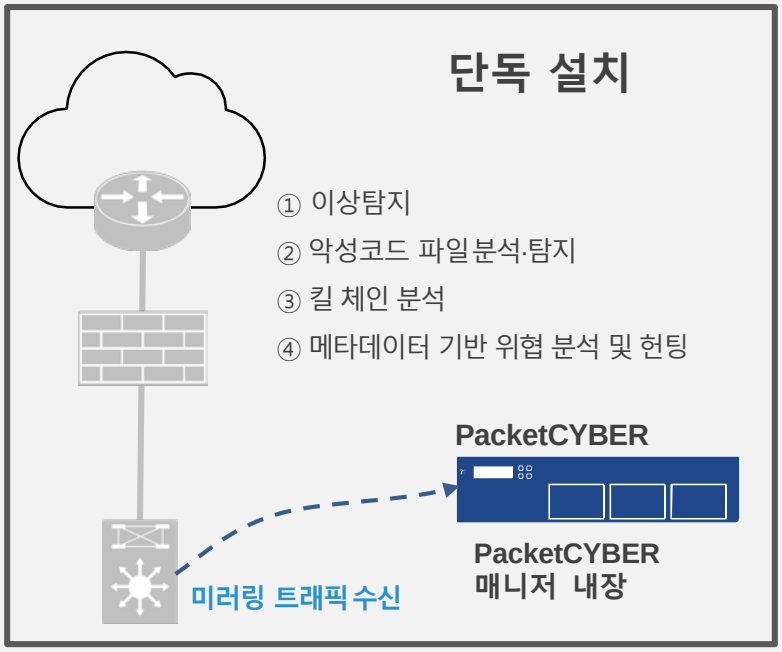
2019년 7월 과학기술정보통신부 권고

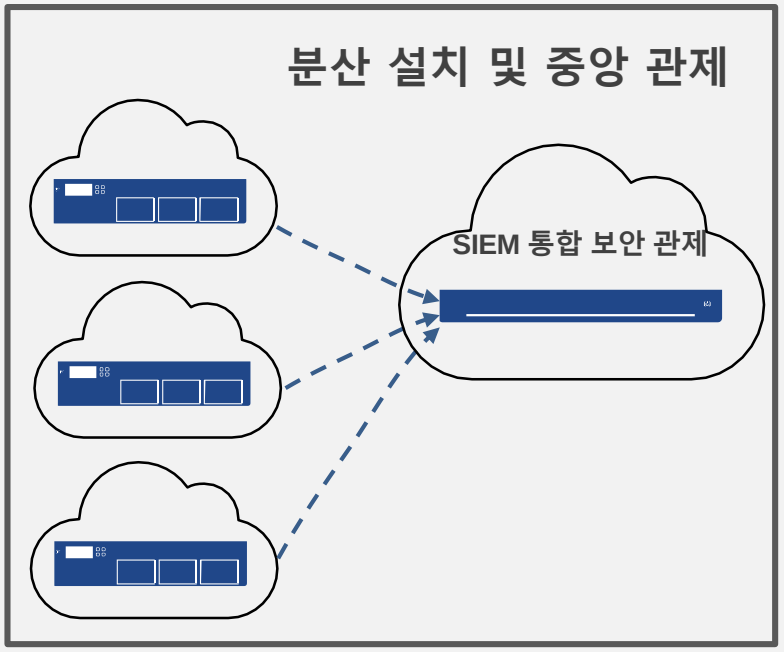
최초 침투 행위 방어 뿐만 아니라 "해커의 공격이 계속되는 과정" 에서 위협을 적기에 식별하고 대응할 필요

➔ **능동적 위협 관리체계로 개선**

도입 기대효과

- ❖ 기존 보안 수단으로 탐지할 수 없는 악성코드 탐지 (NSA 킬 체인 2,4 단계)
- ❖ 악성코드 이외의 네트워크 행위 기반 위협 탐지 (NSA 킬 체인 1,3,5,6 단계) (예: 암호 화폐 채굴 행위[2], C&C 행위, 내부망 이동 행위 등[1])
- ❖ PacketCYBER 탐지 위협의 침입 킬 체인(Intrusion Kill Chain) 분석 (NSA 킬 체인 1~6 단계)
- ❖ 탐지한 위협과 PacketCYBER DPI 기반 메타데이터와의 자동상관관계 분석을 통한 위협의 컨텍스트 및 히스토리 파악
- ❖ 최초 침투 행위 방어 뿐만 아니라 "해커의 공격이 계속되는 과정(킬 체인)"에서 위협을 적기에 식별하고 대응할 수 있는 '능동적 위협 관리체계'로 개선 (※ 과학기술정보통신부 권고 2019년 7월 7일)





㈜소울소프트
서울특별시 서초구 신반포로 315 204 (잠원동, 삼덕빌딩) (zip 06532)

제품문의: 010-8138-3415 | cyberckh@soulsoft.co.kr

㈜씨큐비스타
경기도 의왕시 성고개로 53 (포일동, 에이스청계타워) 8F 822호 (zip 16006)

구매문의: 02-565-0236 | dejeon@cqvista.com

Q & A

Let the Hunt Begin!