vista Preventive Network Security

BAYTECH

차세대 NDR 기술동향 및 적용사례

Introduction to NDR
(Technical Trends and Use Cases Perspective)

2023.03

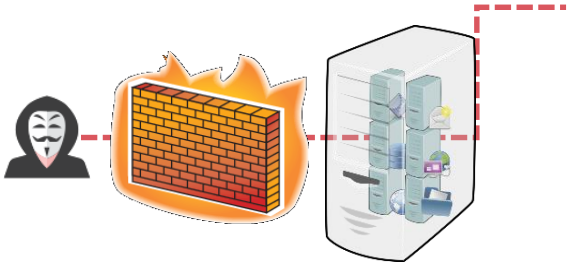
발표자: ㈜ 씨큐비스타 전덕조

Go beyond NDR, SIEM
& Network Forensics...

1 보안 위협 관리 실태와 NDR 기술

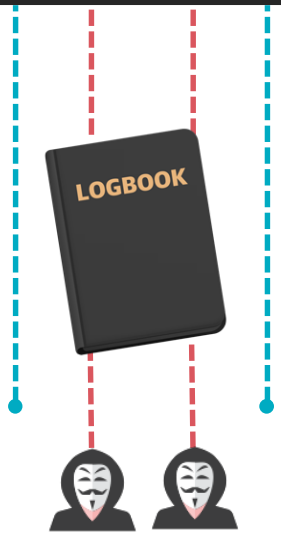
오탐 및 미탐

침입방지, 침입탐지, 방화벽, 네트워크 샌드박싱(APT)...



너무 정적이며 심각한 탐지 사각 지대가 있음
(※ 오탐 및 미탐)

SIEM(통합보안관제)

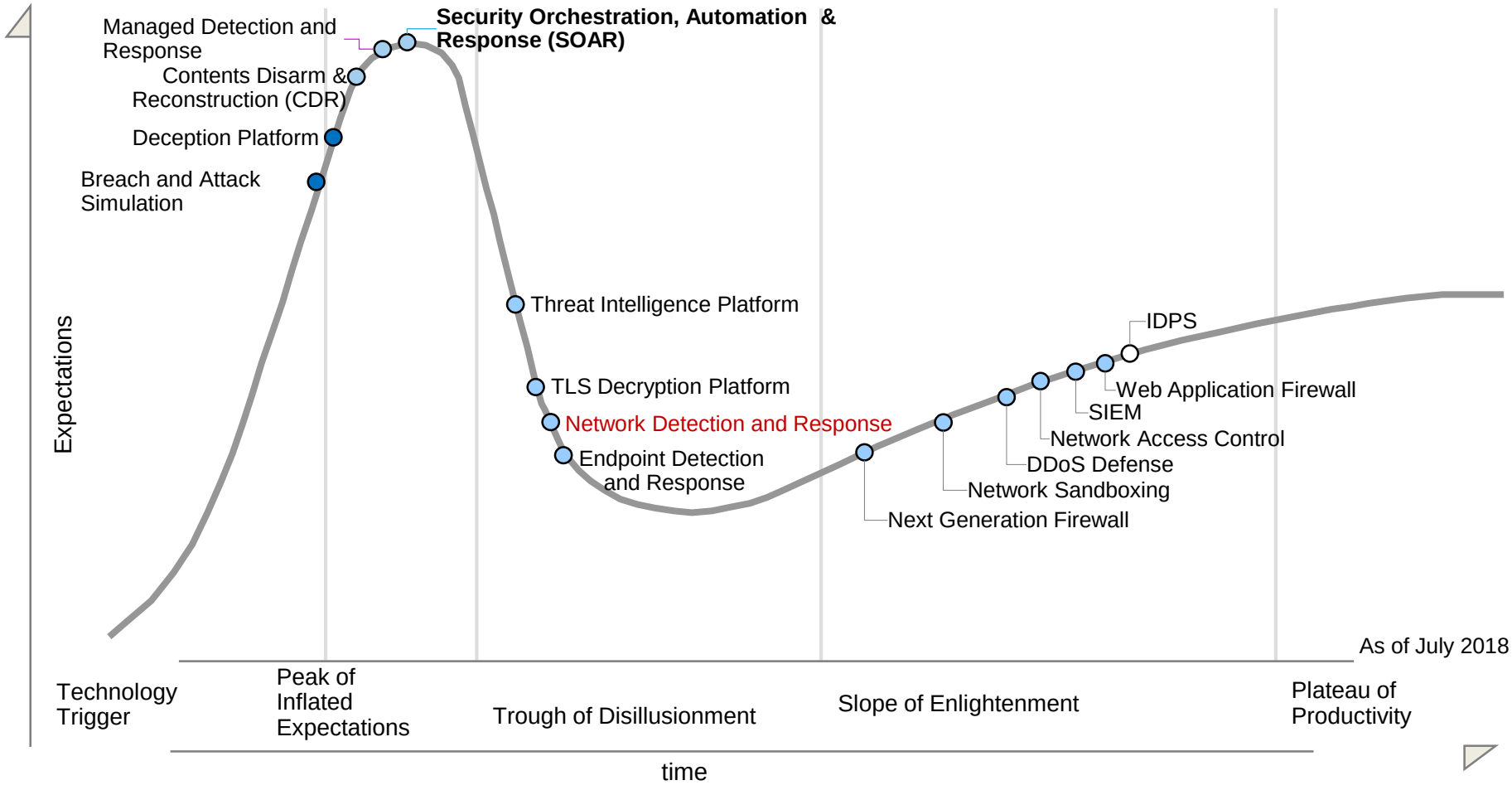


본질적으로 신뢰할 수 없는 데이터의 수집 및 분석
(※ 대량 경보)
(※ 오탐 및 미탐 포함)

네트워크 패킷 캡쳐 도구

너무 느리거나 분석가들에게 올바른 데이터를 제공하지 못함

Hype Cycle for Threat-Facing Technologies, 2019 - Gartner



Gartner : 새로운 솔루션 NDR 권고 (2019)

기존 보안솔루션 문제점

시그니처 기반 보안솔루션 (IPS, 웹방화벽 등)

"시그니처에 정의되어 있지 않은 위협 : 미탐 문제"
"시그니처 매칭 : 오탐 문제"

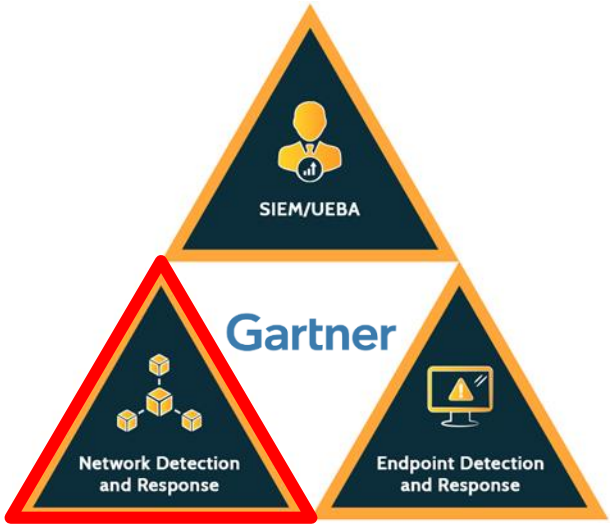
네트워크 샌드박스 (APT)

"수 많은 우회 기술의 발달 : 미탐 문제"
대량 파일 발생 시 : 일부 분석 안함

통합보안관제 (SIEM)

미탐과 오탐이 포함된 로그간의 이벤트 상관관계 분석
(보안관리 56% 효율성)

새로운 솔루션 범주 NDR 권고 (기존 보안솔루션 보완)



다른 보안 도구(예: 방화벽, EDR, SIEM 등)가 놓치는 위협을 찾기 위해
네트워크 머신러닝 또는 고급 분석 기술을 사용하여 분석

방화벽, EDR 및 SIEM 을 보완하는
새로운 솔루션 범주 NDR(Network Detection and Response) 권고

Hacking / Malware

44% 44%의 위협은 자동화된 보안 도구로는 탐지되지 않음 [1]

미탐

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

미탐

1 Threat Hunting Report, Crowd Research Partners

- 이상 탐지
- 보안관제 센터
- 포렌식 침해 평가 팀

ANOMALY DETECTION,
SIEM/SOAR,
FORENSICS

2 M-trends, Mandiant

- 블랙/화이트 리스트
- 시그니처 (AV)
- 샌드박싱
- 파일 분석
- 휴리스틱
- URL 차단

Anti-APT
AV
URL 차단...

✓ 기존 보안 도구로 놓치는 위협(미탐) 문제는 보안사고를 유발하는 핵심 원인 임

✓ Anti-APT(Sandbox) 등 다양한 보안 기술에도 불구하고 악성코드는 여전히 주요한 보안 문제임

미탐: Malware

#1 Sandbox Industry Leader - Network Sandboxing

✓ 실시간에 악성코드를 탐지하지 못함.

✓ 24 시간 후 57 % 탐지.

#1 NGFW Industry Leader with Cloud Sandbox

✓ 실시간에 악성코드를 42.2% 탐지.

✓ 24 시간 후 86.4 % 탐지.

#1 Firewall Price Leader:

✓ 실시간에 악성코드를 1/5 이상 탐지하지 못함.

✓ 24 시간 후 77.1 % 탐지.

✓ Top Global 업체의 Anti-APT(Sandbox) 및 NGFW의 악성코드 대응 능력은 마케팅과는 달리 매우 제한적!!!

기존 NDR 기술 특징

경쟁 기술 특징

AI 기반 네트워크 이상 탐지기술 특징

- 수 주일간의 정상 트래픽 학습 필요
- 의심스러운 트래픽은 쉽게 해석되지 않을 수 있음
- 악성코드 탐지 기능 없음
- **많은 경험 필요 (별도 전문가 필요)**

► **문제점**

- 이미 유입(감염)된 위협 환경 적용 불가
- 이동 설치 불가 (재 학습 필요)

Full Packet 수집 기반 네트워크 이상 탐지기술 특징

- 보안요원이 무엇을 분석할지를 사전에 알고 사용하여야 함
- 하나의 사실을 확인하는 데 상당한 분석 시간 소요
- 벤더가 제공하는 위협 인텔 기반 악성코드 및 이상 징후 탐지는 매우 제한적
- **많은 경험 필요 (별도 전문가 필요)**

► **문제점**

- 이미 유입(감염)된 위협 환경 적용이 매우 어려움
- 이동 설치가 매우 어려움 (수작업에 의한 분석)

2 차세대 NDR 기술동향

미국 국가안보국(NSA) : 포괄적인 위협 헌팅 가설 설정 및 위협 헌팅

National Security Agency

	NSA 해커 조직 지능형 공격 기법	NSA 지능형 공격 대응 권고사항
1	초기 정찰 (Initial Reconnaissance) • 스캐닝 : 운영 체제 식별, 취약점 조사	초기 정찰 (Initial Reconnaissance) • 스캐닝 탐지 • 중요 자산 접속 감시 • 내부 네트워크 감시
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
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
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

악성코드 탐지

통신 이상 탐지 및 분석 기능

FDR (File Detection and Response): 미국 DoD JIE (Joint Information Environment)

✓ EDR(Endpoint Detection and Response), NDR(Network Detection and Response), XDR(Extended Detection and Response)과 같은 다른 탐지 및 대응 솔루션과 차별화된 **파일 탐지 및 대응 솔루션 - FDR(File Detection and Response)**

✓ **FDR(File Detection and Response) :** 네트워크 트래픽에서 파일을 추출하여 압축을 해제하여 APT (Sandbox)의 문제점을 파일 평판, 멀티 백신 등을 이용하여 고속 파일 탐지 및 대응하는 기술

✓ **FDR(File Detection and Response)** 현재 미 국방부 공유 글로벌 네트워크인 **JIE(Joint Information Environment) 에서 채택 사용 중**인 솔루션 중 하나임

미국 국방부 산하
보안정보체계국(DISA)
(Defense Information Systems Agency)

미국 국방부 산하
육군부 (Department of the Army)

미국 국방부 (펜타곤 PENTCIRT)
(Pentagon CIRT)
Computer Incident Response Team

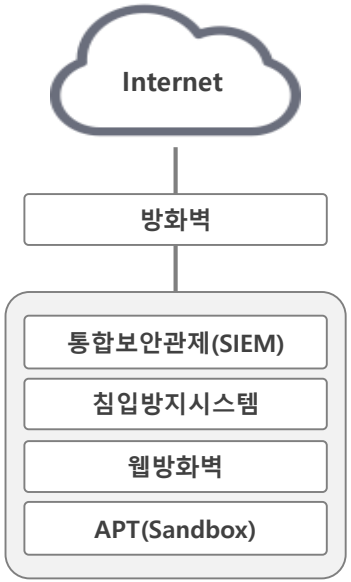
미국 국방부 산하
국방위협감축국(DTRA)
(Defense Threat Reduction Agency)

미국 국방부 소속 정보부대
국가 정찰국 (NRO)
(National Reconnaissance Office)

미국 방위산업체

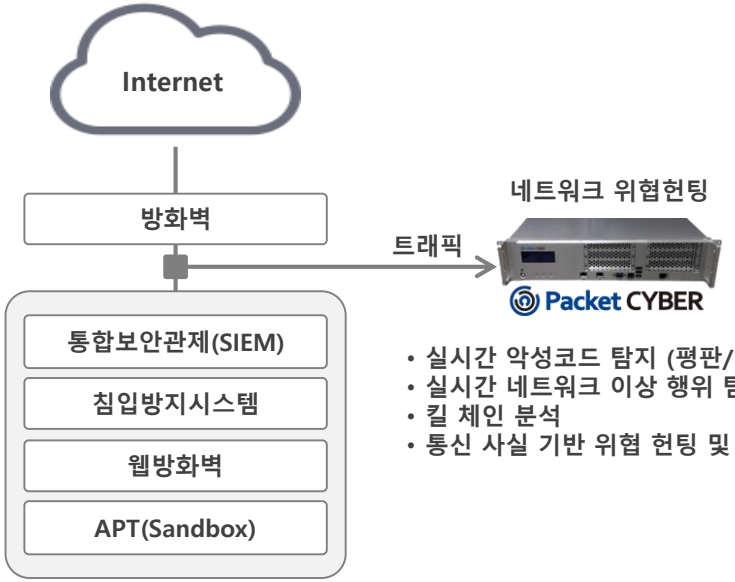
PacketCYBER : 기존 보안 운영관리 문제점을 개선

기존 보안솔루션 (예시)



최초 침투 행위 방어 위주
→ 수동적 위협관리체계

개선방안



- 실시간 악성코드 탐지 (평판/머신러닝)
- 실시간 네트워크 이상 행위 탐지
- 킬 체인 분석
- 통신 사실 기반 위협 헌팅 및 분석

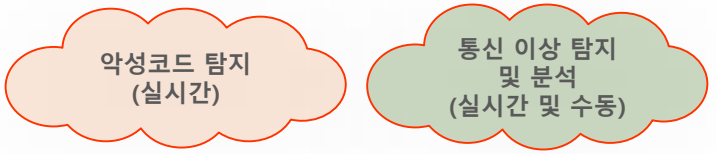
악성코드 | 네트워크 이상 행위 | 킬 체인 분석 | 통신 사실 기반 위협 헌팅

해커 공격 지속 과정에서 위협을 적기에 식별하고 대응
→ 능동적 보안관리체계로 개선

PacketCYBER : 실시간, 자동화 기반 차세대 NDR 솔루션

차세대 NDR: 실시간 탐지, 헌트 및 대응

Real-time DETECT. HUNT. RESPOND.



- **별도 전담인력 없이 !!!**
- 공격자의 Dwell 타임을 줄이는 것이 핵심 !!!

타 솔루션 대비 차별성

실시간, 자동화 기반의 진정한 차세대 NDR(Network Detection and Response) 솔루션

경쟁사 대비 차별화된 장점

유사 제품은 "감염 후 활동 단계"에서 발생할 수 있는 네트워크 이상 위주의 탐지만 제공하는 반면,
PacketCYBER는 "감염 단계" + "감염 후 활동 단계"에 걸쳐 지능형 위협이 형성하는 공격 단계 전반에서 위협을 탐지, 분석, 대응

경쟁사 기술 특징

AI 기반 네트워크 이상 탐지기술 특징

- 수 주일간의 정상 트래픽 학습 필요
- 많은 경험 필요 (전문가 필요)
- 의심스러운 트래픽은 쉽게 해석되지 않을 수 있음
- 악성코드 탐지 기능 없음

▶ **문제점**

- 이미 유입(감염)된 위협 환경 적용 불가
- 이동 설치 불가 (재 학습 필요)

Full Packet 수집 기반 네트워크 이상 탐지기술 특징

- 보안요원이 무엇을 분석할지를 사전에 알고 사용해야 됨
- 하나의 사실을 확인하는 데 상당한 분석 시간 소요
- 벤더가 제공하는 위협 인텔 기반 악성코드 및 이상 징후 탐지는 매우 제한적

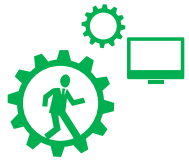
▶ **문제점**

- 이미 유입(감염)된 위협 환경 적용이 매우 어려움
- 이동 설치가 매우 어려움 (수작업에 의한 분석)

타사 대비 차별성

경쟁우위 사항

- 보안요원의 사전지식 불필요
- 실시간 위협 탐지 및 분석 (자동)
- FDR: 실시간 파일 추출 및 악성 여부 판별 (평판, ML)
- 메타데이터 추출을 위한 패킷 디코딩
- NDR: 통계적 기법 기반 네트워크 이상 행위 탐지
- 사이버 킬 체인 분석 및 크로스 세션 분석
- 탐지된 위협과 위협 원인 데이터간 자동상관관계 분석
- 모든 통신 세션 메타데이터의 고속 검색 (수동)
- 이미 유입(감염)된 위협 환경 적용 가능
- 이동 설치 가능 (학습 불필요)



타 솔루션 대비 차별성

미국 국가안보국 NSA(National Security Agency)의 권고 사항을 만족하는 차세대 NDR(Network Detection and Response) 솔루션

기존 솔루션의 트래픽 분석 절차 및 문제점

기존 솔루션의 트래픽 분석 절차

① 트래픽에서 통신 세션 추출,
② 통신 세션을 기반으로 정상 통신 세션 특징 학습
③ 정상에서 벗어나는 의심스러운 통신 세션 경고
④ 의심 세션을 전체 통신세션과 비교, 원인 파악

▼

기존 솔루션의 트래픽 분석 문제점

① 수 주일간의 정상 트래픽 학습 기간 필요
② 많은 경험 필요 (보안 전문가 필요)
③ 의심스러운 탐지 트래픽 해석의 어려움
④ 악성코드 탐지 기능 없음

차세대 NDR의 조건 (NSA 권고 사항)

	NSA 해커조직의 APT 공격 기법	NSA APT 공격 대응 권고사항
1	초기 정찰 (Initial Reconnaissance) • 스캐닝 : 운영 체제 식별, 취약점 조사	초기 정찰 (Initial Reconnaissance) • 스캐닝 탐지 • 중요 자산 접속 감시 • 내부 네트워크 감시
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
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
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

National Security Agency

악성코드 탐지 (자동)
통신이상 탐지 및 분석 (자동)

차세대 NDR - PacketCYBER

추출 ▸ 탐지 ▸ 분석 ▸ 대응 ▸

악성코드 (Malware) 네트워크 이상 (Anomaly) 킬 체인 (Kill-Chain) 분석 (Analysis)

- 머신러닝 / 평판 기반 악성코드 탐지 (실시간)
- 통계적 분석 기반 네트워크 이상 탐지 (실시간)
- 탐지된 위협에 대한 킬 체인 및 크로스 세션 분석 (자동)
- 모든 통신 세션 기록 및 실시간 검색 (수동)

주요 특징

- 실시간 네트워크 트래픽 분석
- 파일 추출 및 악성 여부 판별
- 네트워크 이상 통신 여부 판별
- 킬 체인 분석
- 모든 통신 기록과의 자동 상관관계 분석

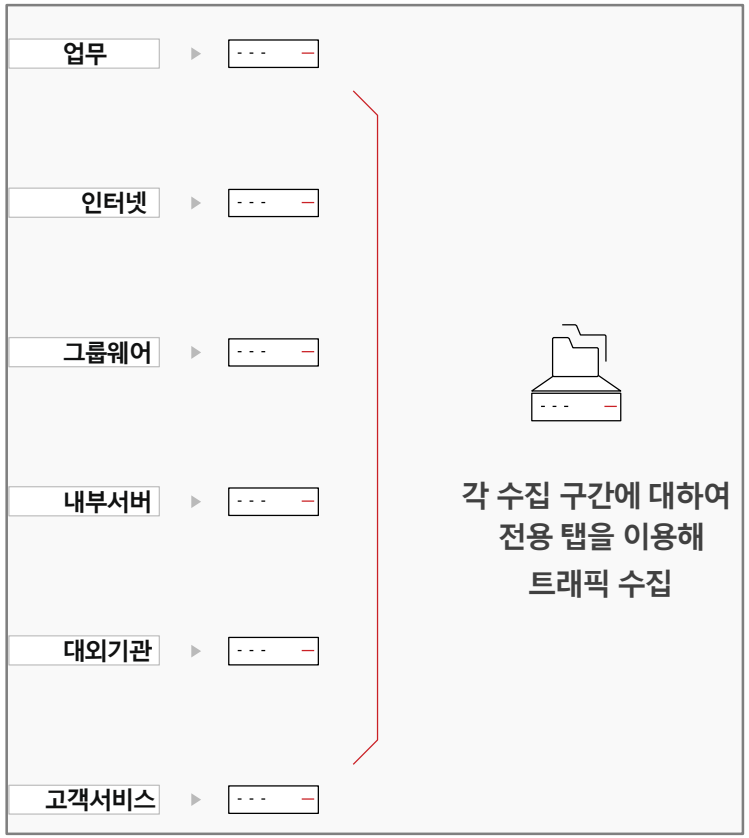
▼

차세대 NDR

기존 솔루션의 트래픽 분석기법의 문제점으로 완전한 정보보호가 어려움 (한계점 내포) → 미국 국가안보국 NSA 해커조직(TAO)에서 APT 공격 기법을 분류하고, 이에 대한 APT 공격 대응 권고사항을 정의함 → 미국 국가안보국 NSA의 APT 공격 대응 권고사항을 만족하는 차세대 NDR 솔루션(PacketCYBER)을 제안 ✓

3 차세대 NDR 적용 사례

구성: NDR + 네트워크 포렌직 구성



각 장비로
미러링

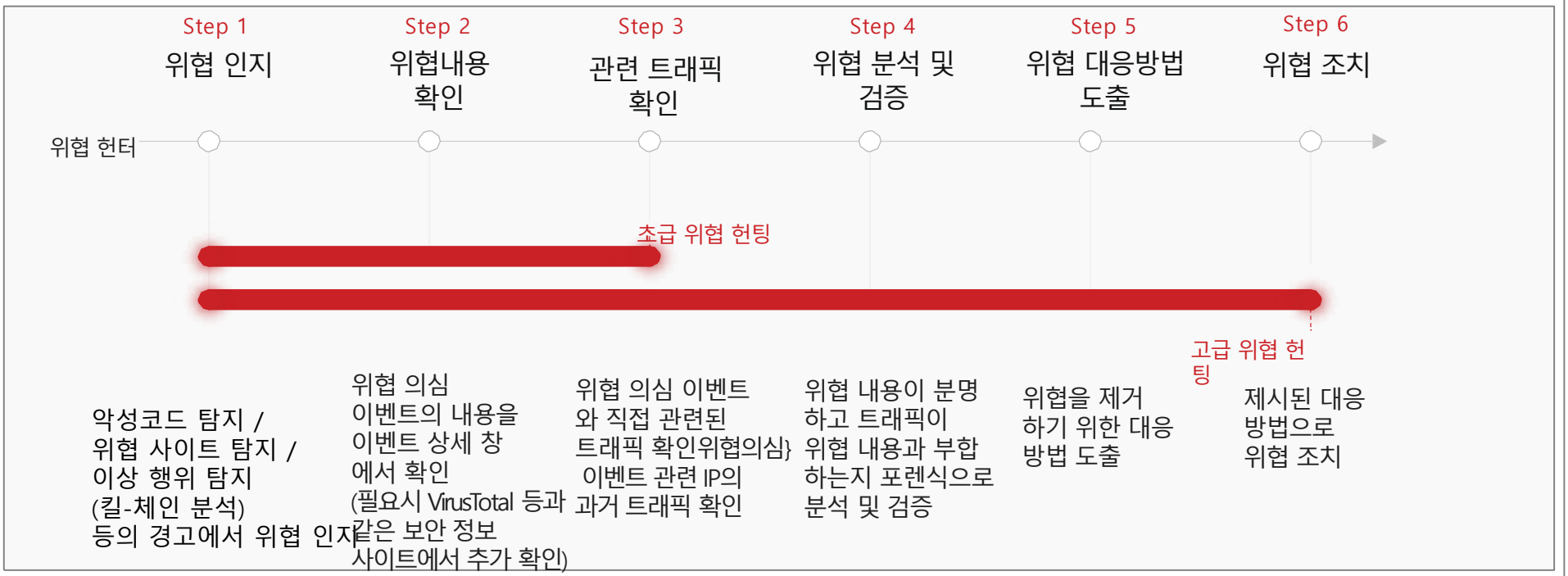
차세대 NDR

- ✓ 위협인지
- ✓ 위협 내용 확인
- ✓ 관련 트래픽 확인

네트워크 포렌식

- ✓ 위협 확정
- ✓ 1차 대응
- ✓ 위협 2차 분석 및 검증
- ✓ 위협 대응 방법 도출
- ✓ 2차 위협 조치

구성: NDR + 네트워크 포렌직 구성



보안 담당자 솔루션 도입 후기

위협 헌팅은 "공격의 가장 기본이 되는 위협 행위를 찾는다"는 면에서 정보보호 활동의 중심이다.

위협 헌팅을 통해 취약점을 발견 및 조치하고 위험을 줄이는 활동이 상호 보완적인 관계를 이룬다면 최적화된 인력과 솔루션을 바탕으로 효과적인 공격 방어가 가능할 것이다.

글로벌 APT, 글로벌 AI 기반 NDR 실패!!! ➔ 적용 보안 가능 솔루션 없음

사례1 OO 시청 (2016년 10월)

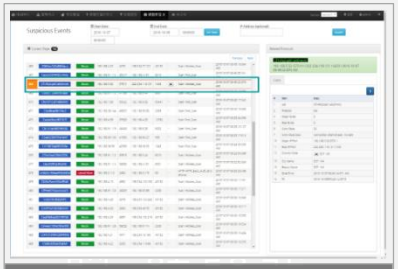
- 폐쇄망으로 운영되는 CCTV 네트워크에 이상 현상을 감지하였으나, 어떠한 보안 솔루션 및 네트워크 관리 솔루션으로도 원인 규명이 불가능한 상태
- 침해사고 대응에 필요한 위협 가시성 및 악의적인 행위를 찾을 수가 없음

	적용 솔루션	수행 내용	결과
1	업계 최고 외산 샌드박스	Call Back기반 탐지 시도	실패
2	AI 기반 네트워크 이상탐지	네트워크 이상 탐지 시도	학습 기간 필요로 실패
3	EDR	-	임베디드 디바이스 환경으로 적용 불가

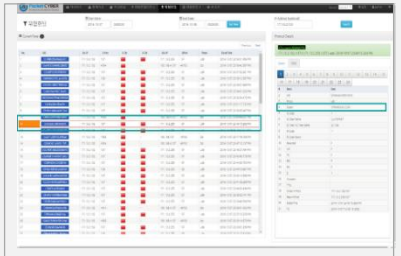
1. DB 공격 이상 징후
2. 드로퍼 공격 이상 징후
3. C&C 접속 이상 징후
4. 이상 접속 시도 1
5. 이상 접속 시도 2

해결책 : PacketCYBER

- **네트워크 이상에 대한 원인 규명 및 알려지지 않은 공격 요소들을 찾아냄**
- **보안 담당 주무관의 호평:**
  "이미 감염되어 있는 Endpoint들을 찾을 수 있는 유일한 솔루션"

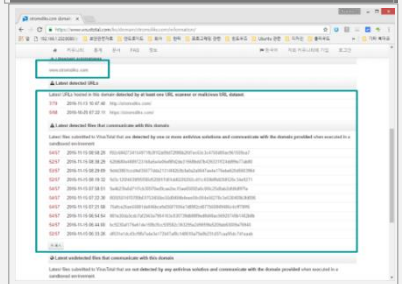


탐지 – 경고 발생 확인



이상 DNS 쿼리 탐지

다양한 IP의 1433포트(MS-SQL Port)로의 접속 시도 확인



드로퍼 악성코드 감염 확인

최신 보안 솔루션 + 관제 요원 29명 ➔ 실패!!!

사례2 OO 시청 (2019년 6월)

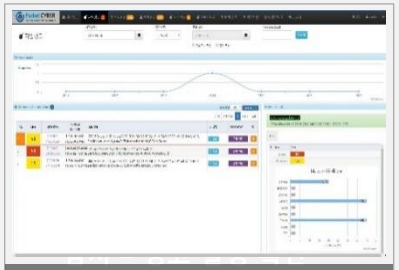
- 다양한 보안 솔루션 운영 중이나 네트워크가 안전한지 분석이 불가능한 상황
- 알려지지 않은 위협에 의한 악의적인 행위를 찾을 수 없음

	적용 솔루션
1	다수 보안 솔루션 및 악성코드 샌드박싱 운용
2	보안관제 팀 운영

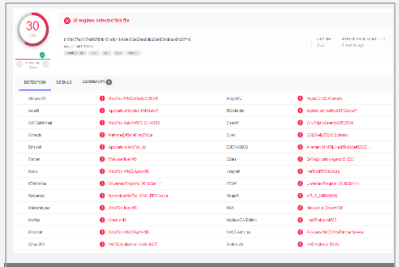
1. SMTP 메일에 악성 파일이 포함되어 외부로 전송
2. kSign 툴로 위장한 악성코드와 접속 기록이 있는 IP가 HTTP 프로토콜에 포함
3. ftp.aiub.unibe.ch로 FTP 접속을 계속 시도
4. 악성코드와 통신 기록이 있는 의심 IP가 HTTP 프로토콜에 포함
5. 스캐닝 탐지

해결책 : PacketCYBER

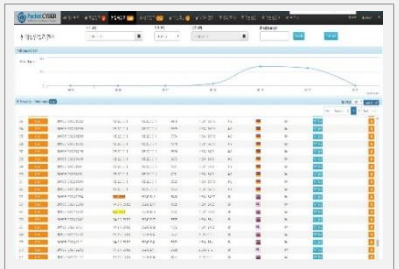
- 네트워크 이상에 대한 원인 규명 및 알려지지 않은 공격 요소들을 찾아냄



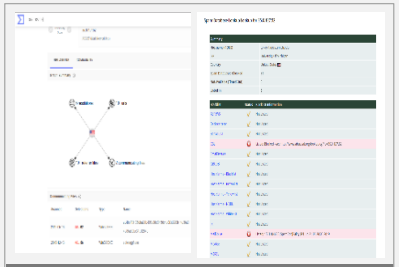
탐지 – 악성코드 유입 경고가 발생했음을 파일경고에서 확인함



위험 경고가 발생한 악성코드가 KMSpico (MS우회 인증 툴) 임을 확인함



위협 의심 IP(35.0.127.52)가 탐지되었음을 접속경고에서 탐지



위협 의심 IP 헌팅 - 6개의 Spam DB에 등록되어 있음을 확인함

적용 가능 보안 솔루션 없음!!!

사례3 OO 시 (2020년 12월)

- 공공Wi-Fi를 구축하여 시범 운영하고 있으나 공공 Wi-Fi 네트워크 위협 상황이 궁금하나 해결책이 없음

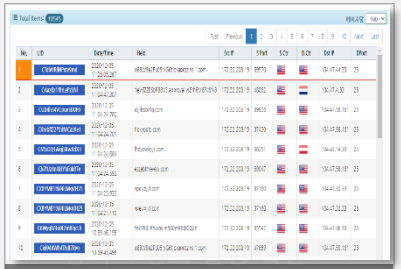
적용 솔루션
적용 가능 솔루션 없음

1. Wi-Fi라우터에 할당된 공인 IP를 이용하여 10,545건의 SPAM 메일 발송
2. 특정 사설 IP에서 외부에 있는 66개 IP의 80번 포트로 1,286회 접속 시도
3. 영리 사업자의 POS단말기가 Wi-Fi 서비스 사용
4. 중국 IP를 포함한 다수의 외부 IP에서 공인 IP의 22번 포트(SSH)로 접속 시도

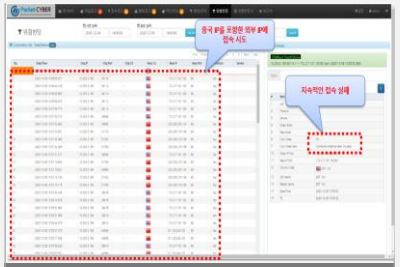
...

해결책 : PacketCYBER

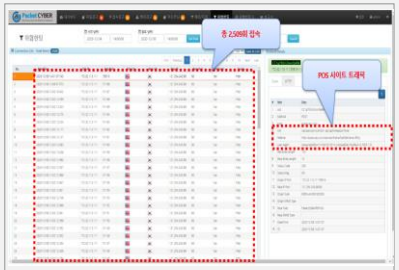
- 공공 Wi-Fi 네트워크 위협 상황 분석



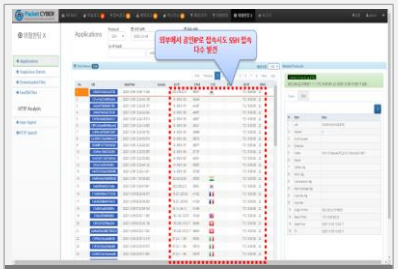
25 Perfect Gifts For Those You Love
25 Gadgets That Will Make 2020 A Lot Better
25 Best Gifts Under $60 In 2020 등



내부 IP가 중국을 포함한 66개 외부 IP의 80번 포트로 지속적인 접속을 시도하나 실패함



영리 사업자의 POS 단말기가 공공 Wi-Fi망에 접속해 트래픽 사용



중국 포함 다수의 외부 IP에서 공인 IP의 22번 포트(SSH)로 접속 시도

※ 차세대 NDR PacketCYBER 도입 기대효과

PacketCYBER 도입 기대효과

Pain Points	Technical Solution	PacketCYBER
상급 기관에서 IP 주소를 주고 해커 IP라고 하며 해당 IP가 어디를 어떻게 접속했는지 보고서를 요구한다. SIEM을 검색해보니 해당 IP에 대한 기록이 전혀 없다. !!!	모든 통신 기록과 파일 아티팩트 저장 (~40日) 및 고속 검색 지원	**차세대 네트워크 보안 패러다임 → 네트워크 기반 위협 헌팅** Packet CYBER 패킷 캡쳐(PCAP) 스토리지 일부 비용으로 신속한 위협 헌팅 및 대응이 가능
언제들어왔는지,언제 유출됐는지도 모르는 보안사고는 어떻게 확인해야하는가?	다양한 악성코드 탐지, 네트워크 이상 탐지, 모든 통신 기록과의 자동 상관관계 분석	 **기존 보안으로 확인할 수 없는 위협 탐지/헌팅/대응 능력 강화**
폐쇄망으로 운영되는 CCTV망이 이상하다. 모르는 위협이 존재하는 것 같은데... 업계 선도 샌드박스와 AI 기반 NDR로도 아무것도 검출되지 않는다. !!!	사전 학습없이 네트워크 이상 통신 탐지 및 모든 통신 기록과의 상관관계 분석으로 증거 확인	

실시간, 자동화 기반의 차세대 NDR 플랫폼

- 기존 보안 수단으로 **탐지할 수 없는 악성코드 실시간 탐지**
- 악성코드 이외의 **실시간 네트워크 행위 기반 위협 탐지** (예: C&C 행위, 내부망 이동 행위 등)
- 탐지된 위협의 **침입 킬 체인(Intrusion Kill Chain) 분석**
- 탐지된 위협과 DPI 기반 통신 **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)
- 로그에 누락된 컨텐츠와 문맥을 DPI 기반 통신 메타데이터를 통하여 **누가, 언제, 어디서, 무엇을 , 어떻게 파악**

감사합니다.

Let the Hunt Begin!

(제조사) 씨큐비스타 / (총판) 이베이테크