Packet CYBER™

실시간 네트워크 기반 위협 헌팅 플랫폼
(차세대 Real-time NDR)

[NDR 업계 최대 MITRE ATT&CK Coverage]

(주) 씨큐비스타 | sales@cqvista.com | www.cqvista.com

cq vista
Advanced Network Threat Hunting

Why threat hunting is important

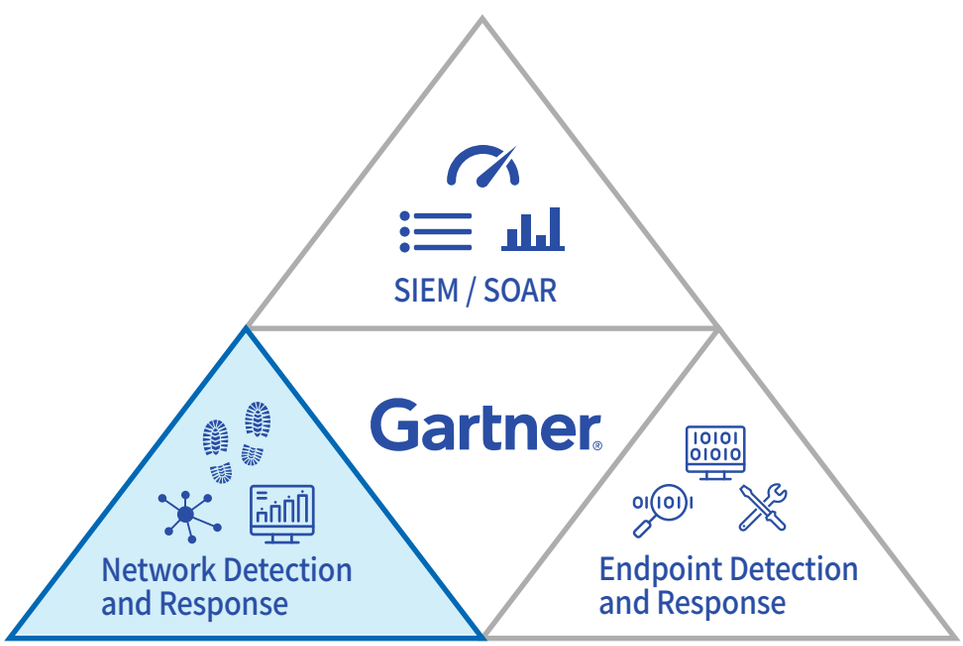
교묘한 위협은 자동화된 사이버보안을 우회할 수 있기 때문에 위협 헌팅이 매우 중요합니다.

자동화된 보안 도구와 1, 2단계 보안 운영 센터(SOC) 분석가들이 대략 80%의 위협을 처리할 수 있지만, 여전히 나머지 20%의 위협을 처리할 수 없습니다.

나머지 20%의 위협은 상당한 피해를 줄 수 있는 교묘한 위협이 포함되어 있을 가능성이 높습니다. 충분한 시간과 자원이 주어지면, 이러한 교묘한 위협은 어떤 네트워크라도 침입하여 평균적으로 280 일 동안 탐지를 회피할 수 있습니다. 효과적인 위협 헌팅은 침입에서 발견까지의 시간 갭(Gap)을 줄여 공격자에 의한 피해 규모를 줄이는 데 도움이 됩니다.

공격자들은 흔히 발견되기 전에 수 주일에서 심지어 수개월 동안 잠복합니다. 그들은 데이터를 빼돌리고 기밀 정보나 자격증명을 찾아내서 추가 접근을 가능하도록 설정하는데, 이는 중대한 데이터 유출로 이어질 수 있습니다.

SOC Visibility Triad vs. NDR (Network Detection & Response)



SIEM/SOAR로 관리 가능한 위협: 최대 80%

20% 위협을 놓침 (※ 위협 헌팅의 중요성 - IBM)

새로운 솔루션 범주 NDR : EDR 및 SIEM/SOAR 보완

MITRE ATT&CK Introduction

개요

MITRE ATT&CK(어택, Adversarial Tactics, Techniques & Common Knowledge)는**"해커가 어떻게 침투하고, 무엇을 하고, 어떤 도구를 쓰는지"를 표준화된 목록으로 정리한 공개 프레임워크.**

- 해커의 행위(전술·기술)를 표준 코드로 정리한 공개 프레임워크 — 갭 분석, 탐지 설계, 훈련·검증에 즉시 활용

왜 중요한가 (Why it matters)

- **공통 언어(Shared Language):** 공격 행위를 전술·기술·하위기술(TTP, TID) 코드로 표준화해 보안팀·경영진·벤더가 같은 용어로 대화합니다.
- **갭 분석(Gap Analysis):** 우리 조직 탐지·차단이 어떤 기술은 커버하고, 어떤 기술은 비어 있는지를 표로 즉시 파악합니다.
- **리스크 기반 우선순위(Risk-Based Prioritization):** 업종/환경에서 자주 쓰이는 TTP부터 투자·탐지·운영을 집중합니다.
- **측정 가능한 성숙도(Measure & Mature):** "탐지 커버리지, 탐지 지연, 재현율/정밀도" 등 지표로 성과를 관리합니다.
- **벤더/솔루션 비교(Eval & Procurement):** 제품 비교 시 ATT&CK 매핑으로 기능 격차를 객관적으로 평가합니다.

Tactics (전술)	Techniques (기술)	Sub-techniques (하위 기술)	Software (소프트웨어)
적대 행위자가 달성하려는 주요 목표 ※ Kill-Chain과 유사 (14 공격 단계)	전술을 달성하기 위해 사용되는 방법 ※ Techniques 개수: 211개	더 넓은 기술(Technique)의 구체적 변형/세분화된 방법	기술(Techniques)과 연관된 도구 또는 악성코드

2025-04-22 기준 MITRE ATT&CK Enterprise의 Techniques 개수: 211개

MITRE ATT&CK 활용 Example

침해사고 상황(Story)

- 한 직원이 **"인사평가.xlsx"**로 위장한 첨부파일을 열자, 숨겨진 매크로가 **PowerShell**을 호출해 외부에서 페이로드를 다운로드 함.
- 이후 악성 프로그램이 주기적 **(예: 60±5초)**으로 **HTTPS**로 비콘(주기적 통신)을 보내며 명령을 대기함.

ATT&CK TID 매핑 (핵심 3개)

- **T1566.001** Spearphishing Attachment (초기 침투)
- **T1059.001** Command and Scripting Interpreter: PowerShell (실행)
- **T1071.001** Application Layer Protocol: Web Protocols (HTTPS) (명령·제어)

탐지 포인트 (Detection Point)

- **네트워크(NDR):** 희귀 SNI/JA3 조합, 규칙적 비콘 주기(=간격 분산이 낮음), 소용량 주기 통신 + 간헐적 급증
- **이메일 보안 게이트웨이:** 유사 도메인(look-alike), 신규 등록 도메인, 매크로 포함 문서 첨부
- **엔드포인트/EDR:** winword.exe → powershell.exe 자식 프로세스 생성, -EncodedCommand, -w hidden, IEX 등 스위치

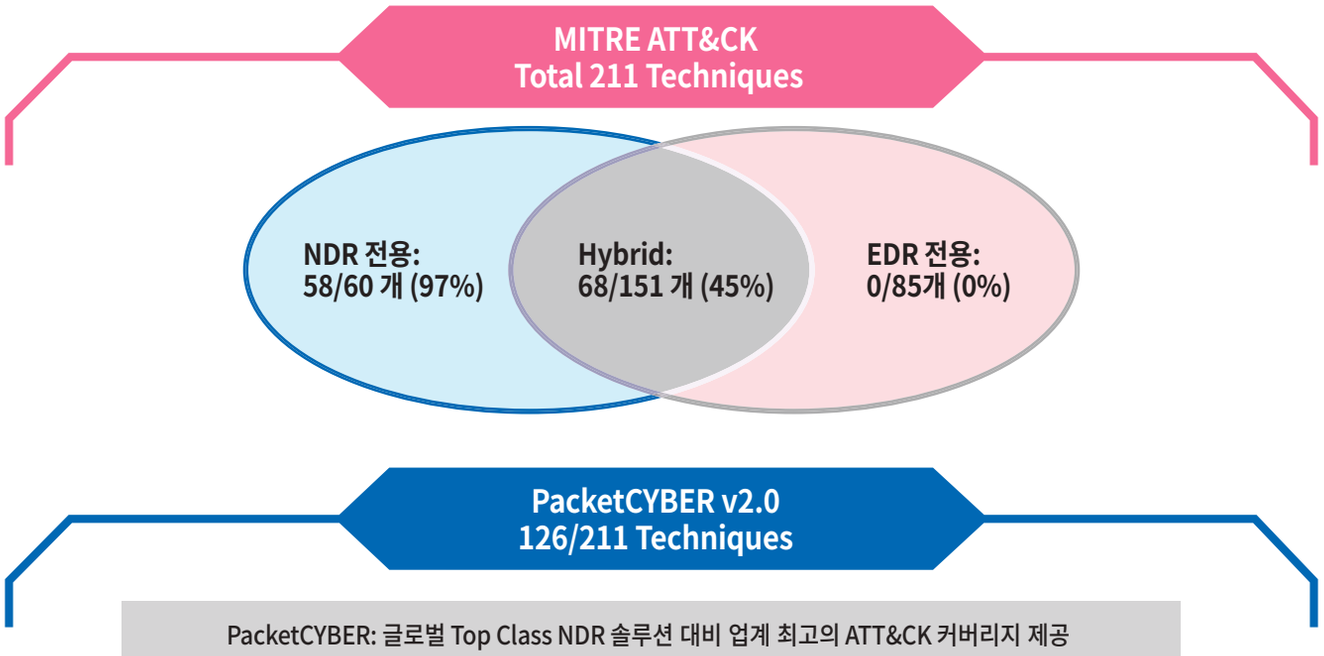
PacketCYBER internal 랜섬웨어 탐지

	Case 1 (기본)	Case 2 (도구 다운로드)	Case3 (대체 유출)	Case 4 (초기 침투 포함)
1.초기 확산	T1046	T1105 → T1046	T1046	1190 → T1105 → T1046
2. 측면 이동	T1021.002 → T1570	T1021.002 → T1570	T1021.002 → T1570	T1021.002
3, 암호화 활동	T1486	T1486	T1486	T1486
4. C2 통신	T1071	T1090	T1571	T1071/T1571/T1090
5. C2 통신 (병렬)	-	-	-	다른 C2 기법 동시
6. 데이터 유출	T1041	T1041	T1048	T1041 또는 T1048

PacketCYBER internal BPFdoor 탐지

단계	TID	탐지 모듈
1. 대기	T1595 (선택적)	**부분 탐지•** 네트워크 활동 거의 없음: BPF 필터만 활성 / 수동 대기 상태
2. Magic Packet 수신	T1205.002	**완전 탐지:** BPFDoor 모듈 핵심 / 가장 강력한 탐지지점
3. 백도어 활성화	T1014	**탐지:** Phase 3 + BPFDoor / Rootkit 행동 추정
4. C2 세션 구축	T1095 T1571 T1573	**탐지:** 코버트 채널 / 비표준 포트 / 암호화 통신
5. 명령 실행 & 데이터 수집	T1041	**부분 탐지:** 네트워크 지표만 / 실제 내용 불명

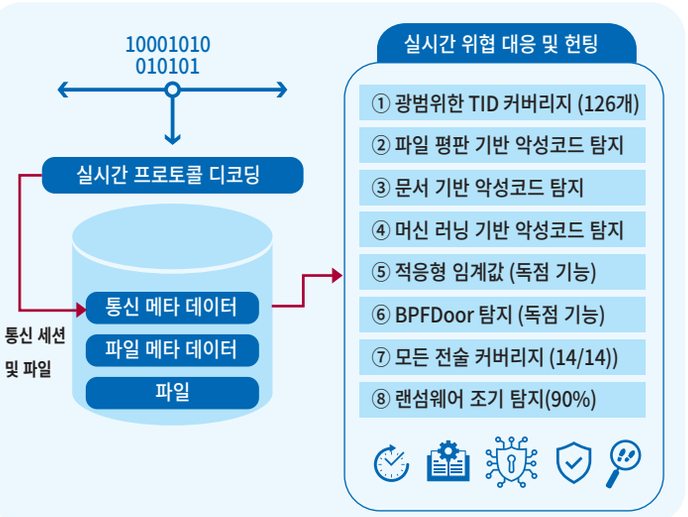
PacketCYBER MITRE ATT&CK Coverage



PacketCYBER: 글로벌 Top Class NDR 솔루션 대비 업계 최고의 ATT&CK 커버리지 제공

PacketCYBER's Benefits (28.6% Broader ATT&CK Coverage)

Real-time – *실시간 위협 탐지 및 대응 / 위협 헌팅*



Why Speed Matters in Decision Making? (Seconds)

Packet CYBER™

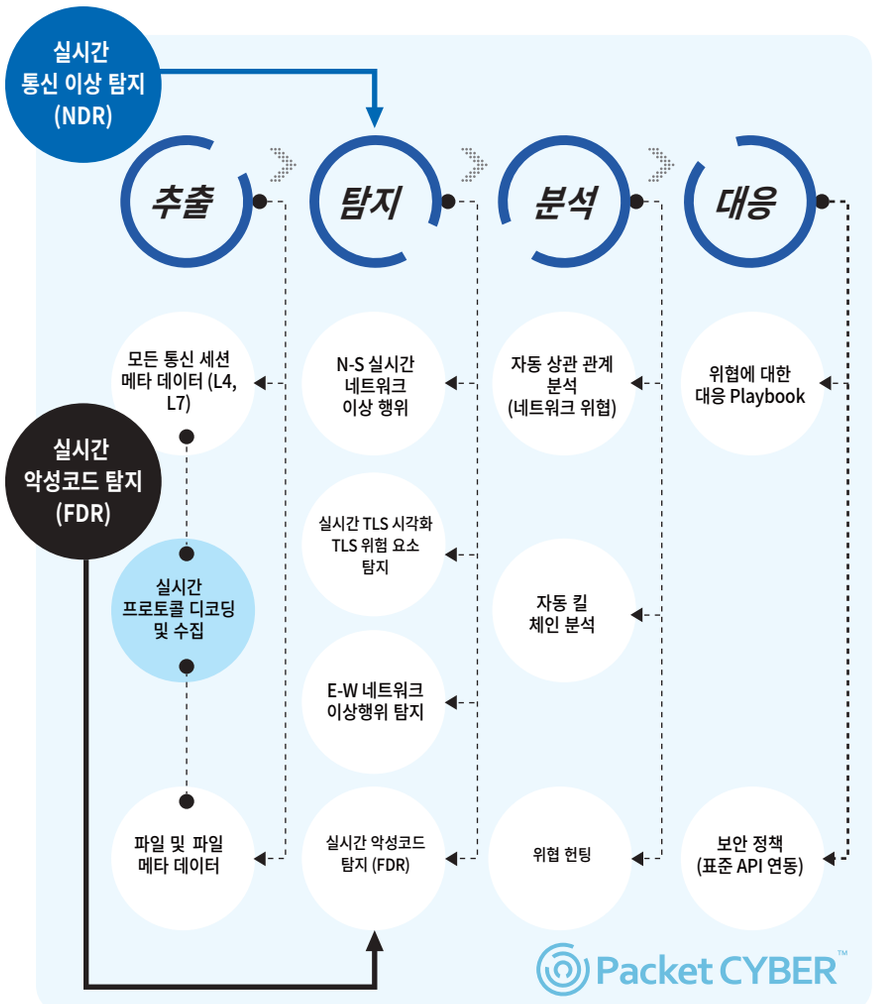
P a c k e t C Y B E R

- "실시간" 악성코드 탐지 / 위협 특정
- 광범위한 TID 커버리지 (126개: 검증됨)
- Adaptive Thresholds (독점 기능)
- Earlier Kill Chain Detection (행위 기반)
- BPFDoor 탐지 (독점 기능)
- 랜섬웨어 조기 탐지 (90%): 9X Faster
- 모든 전술 커버리지 (14/14))
- 공격자 추적 및 위협 헌팅
- 탐지된 위협에 대한 대응 가이드북 제공
- 이미 유입(감염)된 위협 환경 즉각 적용 가능
- 이동 설치가 용이하며 즉각적인 위협 탐지 및 헌팅
- 사람의 개입 최소화 운영 (SIEM/SOAR 연동 등)

- **업계 최다 126개 TID 구현 - 경쟁사 대비 28.6% 더 넓은 커버리지 제공**
- **NDR 업계 유일 14개 전술 100% 완전 지원**
- NDR 업계 유일의 Adaptive Threshold 기술로 공격 단계마다 자동으로 민감도 조정
- 전 세계 유일 BPFDoor 네트워크 기반 탐지 - 2,206개 Magic Packet 실전 검증
- 암호화 시작 전 90% 차단 - 업계 최고 랜섬웨어 조기 탐지율 제공
- 암호화 트래픽도 복호화 없이 66개 위협 시나리오 탐지 (TLS1.3, QUIC 포함)

Architecture (다계층 탐지 및 분석 아키텍처)

1	"실시간" 악성코드 탐지 / 위협 특정) ※ 평판, 머신러닝, 문서, AV, 30종 파일타입
2	Rule-based Detection (행위 규칙 기반) • MITRE ATT&CK TTP 매핑 • 530+ 탐지 규칙 및 시나리오
3	Statistical Analysis (통계 기반 분석) • 베이스라인 편차 분석 • Z-score 이상치 탐지
4	Time Series Analysis (시계열 분석) • 시간대별 트래픽 패턴 분석 • 주기성 탐지 (FFT, Autocorrelation) • 계절성 및 추세 분석 • 시간 윈도우 기반 이상 탐지
5	ML-based Prediction (머신러닝 예측) • Random Forest, Neural Network • Zero-day 예측
6	Correlation Engine (상관 분석 엔진) • Kill Chain 진행도 추적 • 다중 이벤트 연관성
7	Beacon Analyzer (비콘 분석기) • C2 통신 주기성 탐지 • 10-300초 간격 패턴
8	Adaptive Threshold (적응형 임계값) • 동적 임계값 조정 (10→5) • 환경별 자동 튜닝
9	Ensemble Voting (앙상블 투표) • 8개 모듈 가중 투표 • 최종 신뢰도 계산



Differences from Other NDR Solutions

PaketCYBER가 경쟁사 NDR 대비 우수한 이유는 무엇인가요?
PacketCYBER 고객은 침해 이후 공격을 가장 폭넓고 빠르게 탐지합니다!

28.6%+

네트워크상의 위협을 신속하고 폭넓1게 가시화 함으로써 공격자의 Dwell 타임을 줄이는 것이 핵심 !

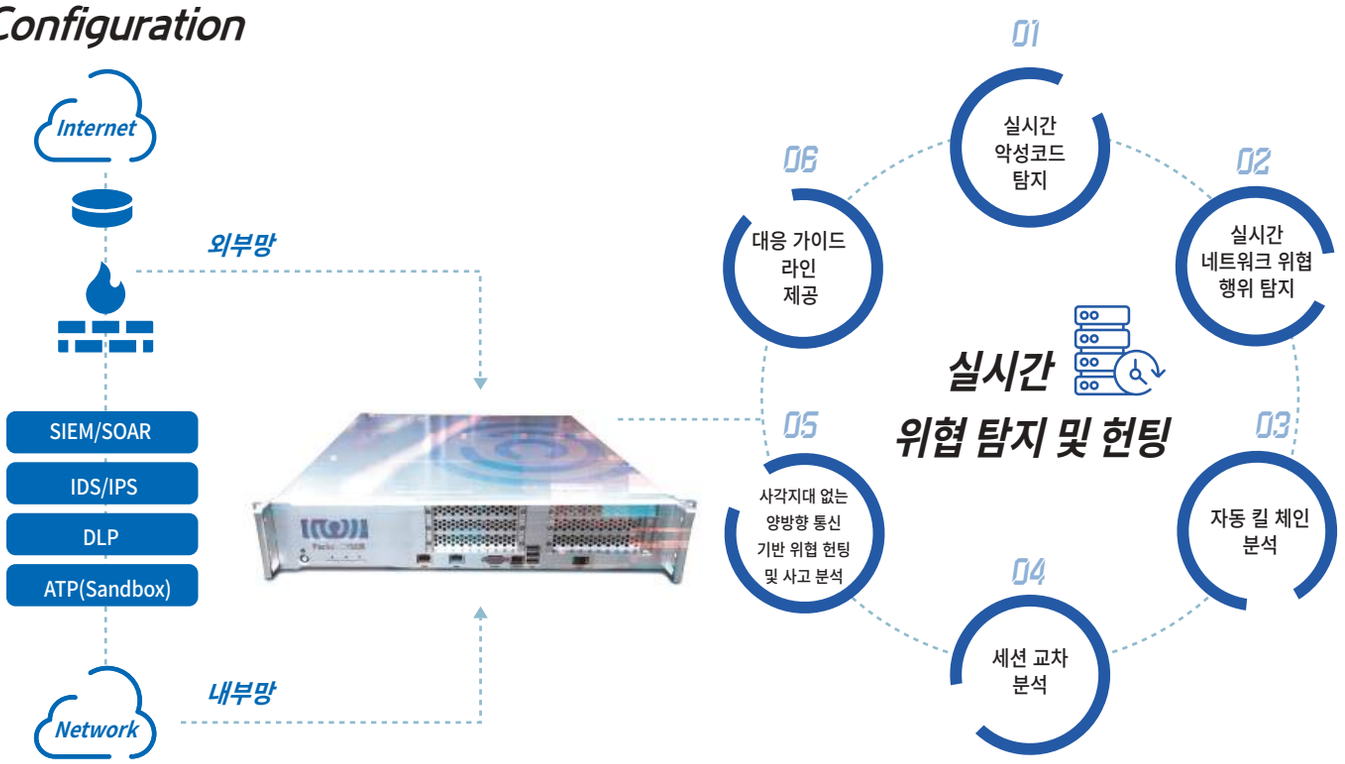
Real-time DETECT, HUNT, RESPOND

기능	PacketCYBER	Top Class NDR경쟁사	경쟁 우위 수준
BPFDoor 탐지	업계 유일	-	무한대
적응형 임계값	업계 유일	-	업계 유일
TID 커버리지	126개	98개	+28.6%
전술 커버리지	14/14	12/14	+17%
랜섬웨어 조기	90%	70%	+29%
악성코드 탐지	평판, ML, AV, 문서, 30종 파일타입	제한적	N/A
암호화 트래픽 분석	EVA: TLS/QUIC (복호화 없이)	TLS (제한적)	+QUIC /복호화 없음

1. 업계 최대 MITRE ATT&CK TID를 "실시간 탐지 및 대응"
2. 효과적이고 포괄적인 공격자 활동 추적 및 네트워크 위협 헌팅
3. 해커가 지울 수 없는 "가장 객관적인" 통신 사실을 기반으로 사각지대 없는 보안 관리 지원

Configuration & Key Benefits

Configuration



Benefits: Solving the Security Monitoring Gap

SIEM / SOAR / Other NDR / EDR

- 제한적 탐지
- 부족한 증거 및 문맥

Packet CYBER (실시간 OpenNDR)

- 포괄적 탐지
- 모든 증거 및 문맥

동일 타임스탬프 기반

네트워크 구간

Packet CYBER™

트래픽에서 모든 파일 추출 / 모든 통신 세션 기록 및 검색

- ✓ "실시간" 악성코드 탐지 / 위협 특정
- ✓ 광범위한 TID 커버리지 (126개: 검증됨)
- ✓ Adaptive Thresholds (독점 기능)
- ✓ Earlier Kill Chain Detection (행위 기반)
- ✓ BPFDoor 탐지 (독점 기능)
- ✓ 랜섬웨어 조기 탐지 (90%): 9X Faster
- ✓ 모든 전술 커버리지 (14/14))
- ✓ 공격자 추적 및 위협 헌팅
- ✓ 탐지된 위협에 대한 대응 가이드북 제공
- ✓ 실시간 시그니처 기반 탐지
- ✓ 자동 크로스 세션 분석
- ✓ 모든 통신 세션 • 파일 기반 위협 헌팅 및 사고 분석

동일 타임스탬프 기반(상관관계), 실시간 다중 탐지 엔진에 의한 위협 탐지, 헌팅 및 대응 프로세스 제공

PacketCYBER(**Real-time OpenNDR**)는 위협 여부와 관계없이, 모든 파일 및 세션을 수집하며, 동일타임스탬프상에서 사각지대 없는 "광범위한 위협 탐지 및 대응과 위협 헌팅"을 지원합니다.

Case Study I : OO 기관 폐쇄망

Problem: CCTV 네트워크 (폐쇄망) 이상 현상	Solution: PacketCYBER 사용
• 폐쇄망으로 운영되는 CCTV ㅋ 네트워크에 이상 현상을 감지하였으나, 어떠한 보안 솔루션 및 네트워크 관리 솔루션 (글로벌 APT, 글로벌 NDR 등)으로도 원인 규명이 불가능한 상태 • 침해사고 대응에 필요한 위협 가시성 및 악의적인 행위를 찾을 수가 없음	• 네트워크 이상에 대한 원인 규명 및 알려지지 않은 공격 요소 들을 찾아냄 • 보안 담당 주무관의 호평: "이미 감염되어 있는 임베디드 엔드포인트들을 찾아낼 수 있는 유일한 보안 솔루션"

Case Study II: OO 기관

Problem: 기존 보안이 놓치는 위협 헌팅	Solution: PacketCYBER 사용
• 다양한 보안 솔루션 운영 중이나 네트워크가 안전한지 분석이 불가능한 상황 • 보안관제센터 (SIEM), OO명의 보안 관제사, APT 등 다수의 보안 솔루션 운영	• APT를 포함한 각종 보안 솔루션, 통합 보안 관제 (SIEM) 센터 및 OO명의 보안관제사가 놓치고 있는 다수 위협 헌팅 성공 • 보안 담당 사무관의 호평

Case Study III: 제1 금융권

Problem: 기존 보안이 놓치는 위협 헌팅	Solution: PacketCYBER 사용
• APT, SIEM, SOAR 및 네트워크 포렌식 운영에서 놓치고 있는 위협 헌팅	• APT, SIEM, SOAR 및 네트워크 포렌식 운영에서 놓치고 있는 다수 위협 헌팅 성공 • 보안 담당 직원의 호평

Case Study IV: OO Wi-Fi

Problem: OO Wi-Fi망에 대한 위협 헌팅	Solution: PacketCYBER 사용
• 어떠한 보안 솔루션 (APT, NDR 등)도 적용 불가능했던 OO Wi-Fi망에 대한 성공적인 위협 헌팅	• OO Wi-Fi에 대한 다수 위협 헌팅 성공 • 보안 담당 사무관의 호평

PacketCYBER Product Lines

국내 최초! 네트워크 위협 탐지 및 대응 **NDR** 부문 *보안기능 확인서 획득!*

250 Mbps	500 Mbps	1 Gbps	2 Gbps	5 Gbps	10 Gbps
✓ 2U Size ✓ 1Gbp x 4 Ports	✓ 2U Size ✓ 1Gbp x 4 Ports	✓ 2U Size ✓ 1Gbp x 4 Ports	✓ 2U Size ✓ 1Gbp x 4 Ports *(opt.) 10Gbp x 2 Ports	✓ 2U Size ✓ 1Gbp x 4 Ports ✓ 10Gbp x 2 Ports	✓ 2U Size ✓ 1Gbp x 4 Ports ✓ 10Gbp x 2 Ports

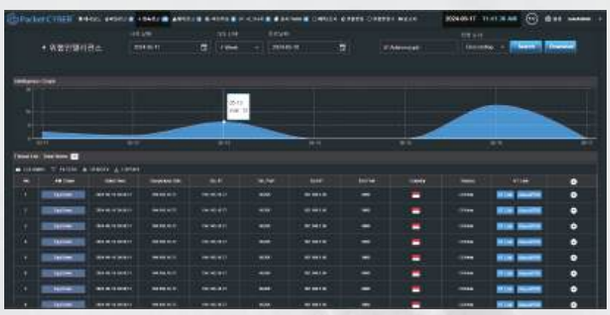
Administrator UI

Packet CYBER

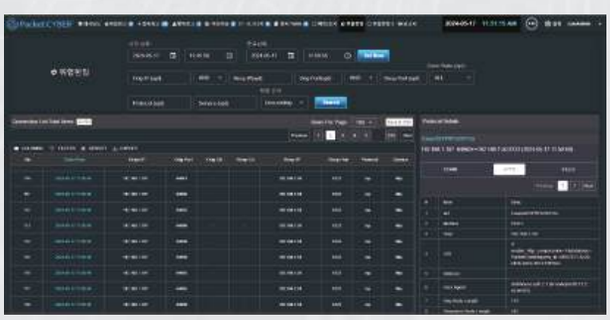
실시간 위협 탐지 정보기반 대시보드

네트워크 행위 , 악성코드, 침해징후(IOC)
탐지 결과의 통합 인텔리전스

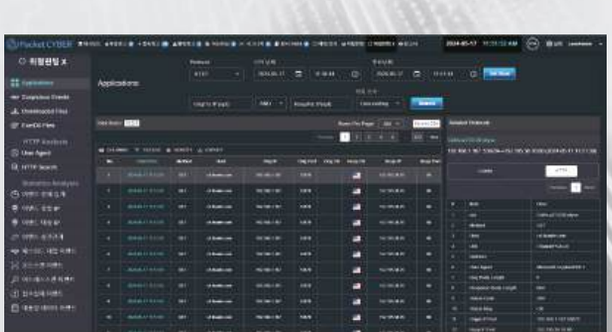
악성코드 탐지



침해징후(IOC) 탐지



탐지 위협 기반 자동 위협 헌팅(Hunting)



확장 위협 헌팅(Hunting) (수동)

Packet CYBER™ Advanced Network Threat Hunting

1등급 GOOD Software

2024 K-디지털 브랜드 대상

2024 K-디지털 브랜드 ' 대상 ' 선정
보안 솔루션 부문

조달청
Public Procurement Serv
디지털서비스몰

CERTIFIED NDR CERTIFIED

국내 최초!
네트워크 위협 탐지 및 대응 (NDR) 부문
보안기능 확인서 획득

CQ VISTA
Advanced Network | Threat Hunting

㈜씨큐비스타
경기도 성남시 분당구 판교로 255번길 9-22, 5F 511호 (우 13486)
문의 : 02-565-0236 | sales@cqvista.com