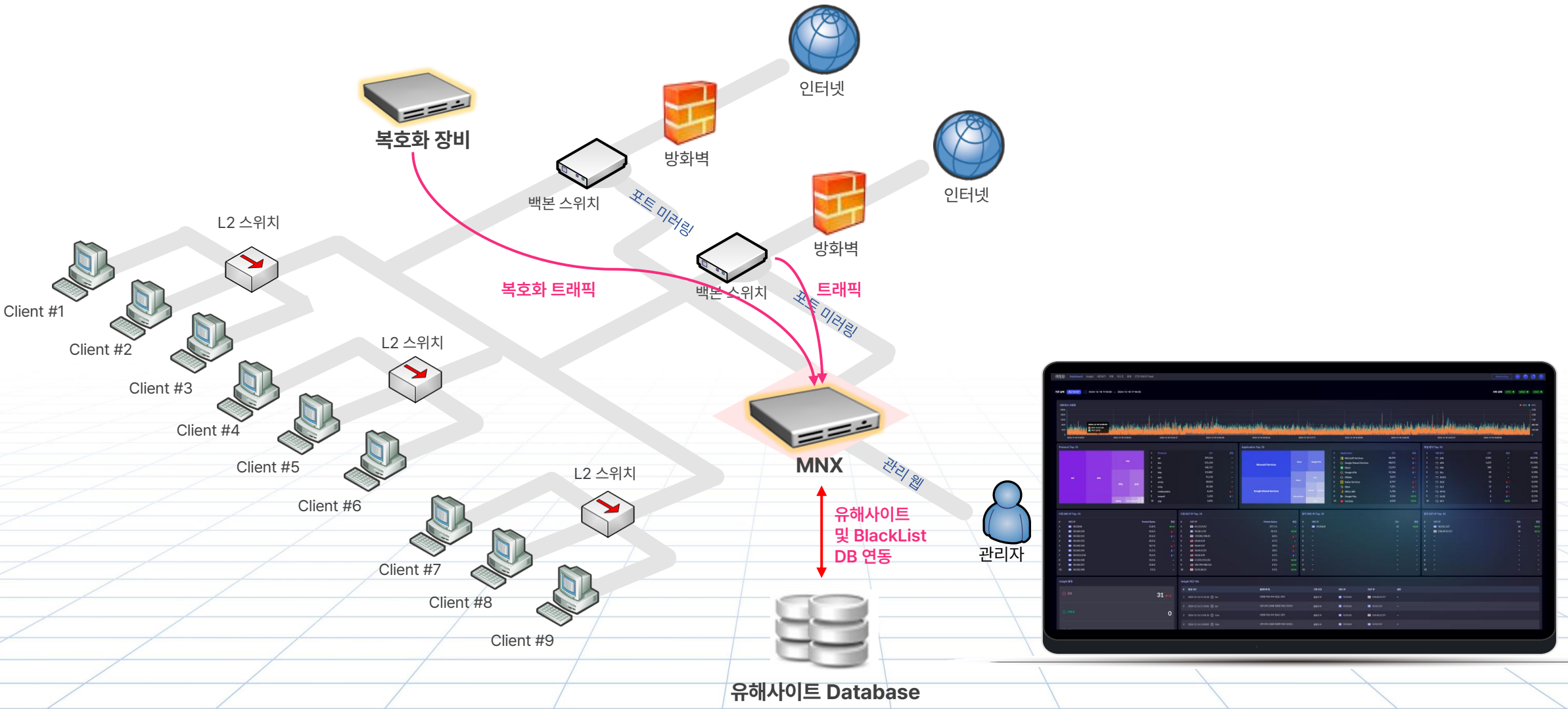
THE #1
MNX DPI
제품 / 아키텍처 소개 자료

SANDS Lab

개요

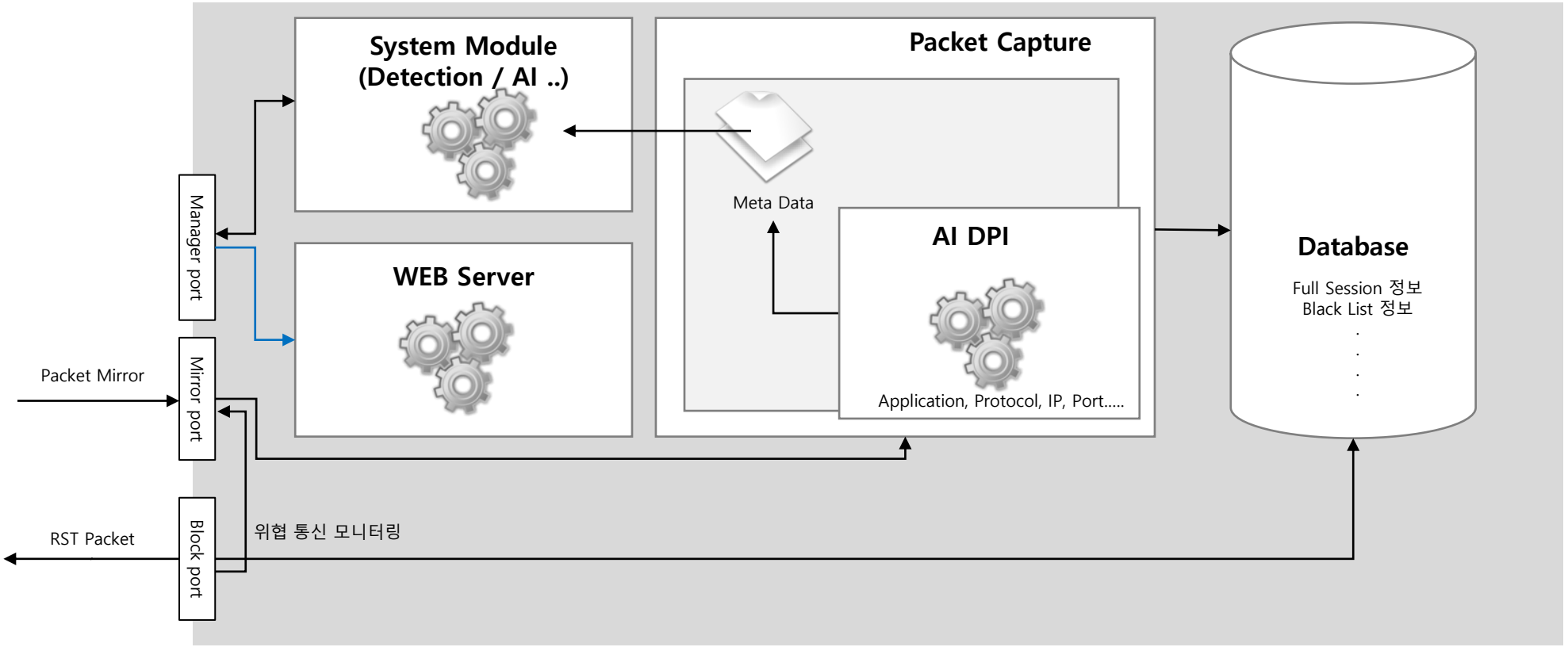
1. 구성도
- Mirror 방식 구성



2. 시스템 구성도


Internet
트래픽 미러링
HTTP MAIL FTP
SSL SSH DNS
Protocol
Application
AI DPI 식별
HTTP, SMTP, FTP 등
523개의 프로토콜과
2,555개의 어플리케이션 식별 및 분석
Application
Metadata Flow
메타데이터 분석
AI 모델 분석
CTX
Threat Intelligence
자사 TI 연동
Insight
위협 이슈 트래킹
차단
RST 기반 차단
위협 식별, 대응
API
Syslog
SNS
mail
대응

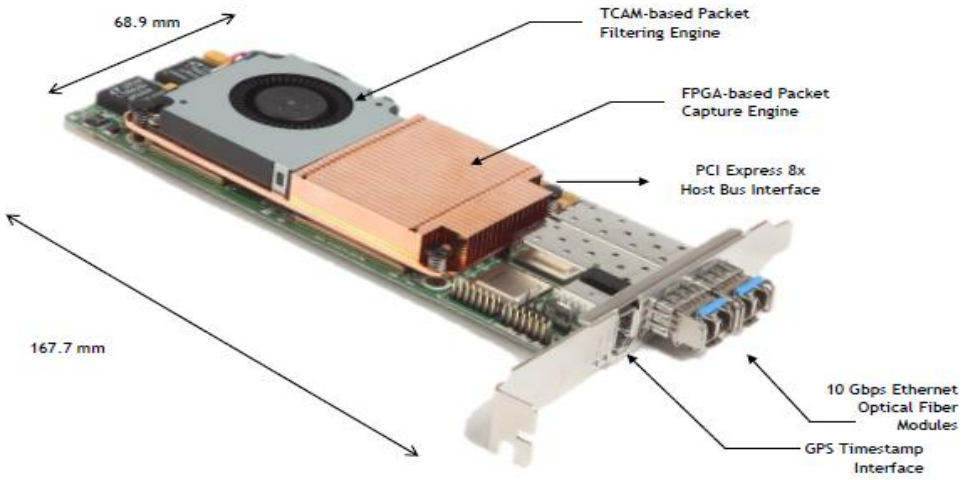
3. 시스템 아키텍처

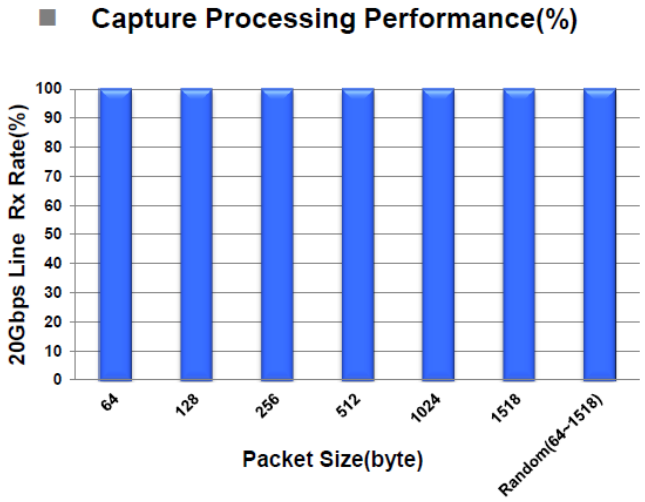


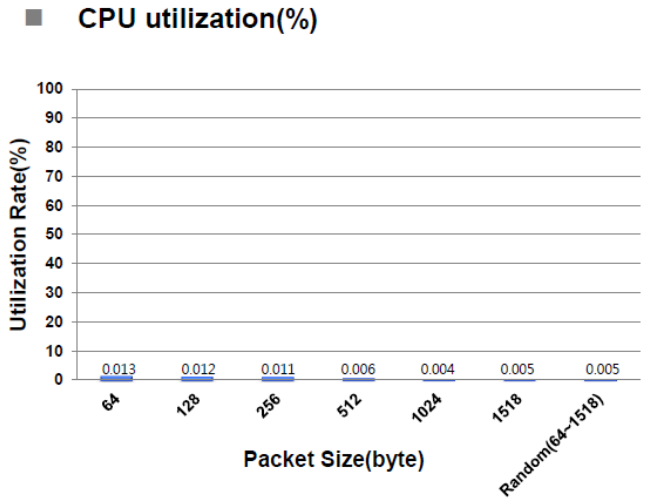
※ 공개 가능 일부 부분

기능

1. 수집
- 수집 전용 Network 카드







각종 신호를 H/W 레벨에서 처리하여 Packet 손실 0% 로 제공. 10Gbps 대역대 무손실 수집 지원

1. 수집
- WEB

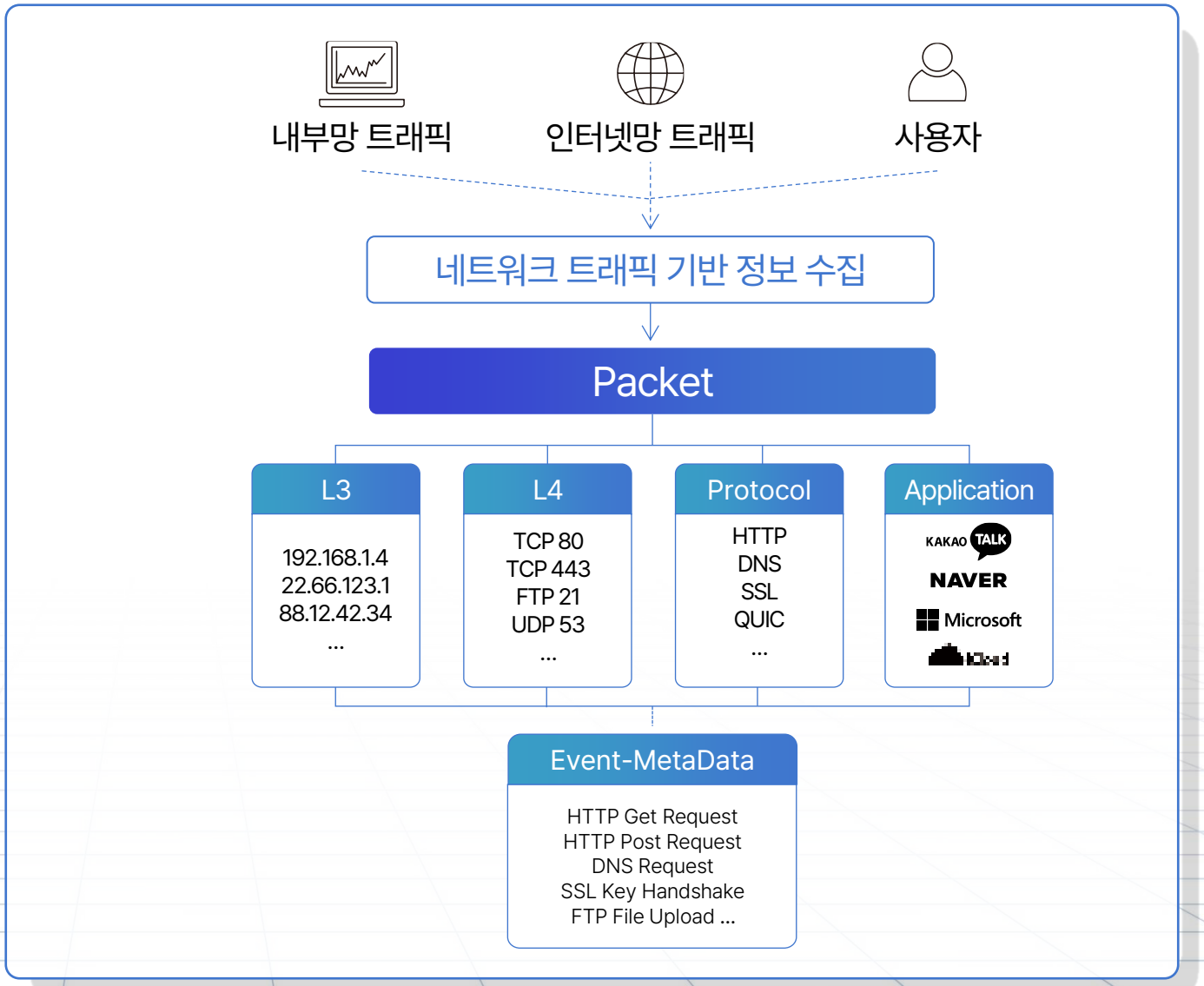

서울 구로구
Traffic Live Chart
250 Mbps
200 Mbps
150 Mbps
100 Mbps
50 Mbps
0
2025-02-20 17:59:00
2025-02-20 18:45:00
2025-02-20 19:31:00
2025-02-20 20:17:00
2025-02-20 21:03:00
2025-02-20 21:49:00
2025-02-20 22:35:00
2025-02-20 23:21:00
트래픽 수집 차트
Sensor List
Fault Sensor Count
Sensor Count
1
1
연동 센서
Sensor ID
라이선스 기간
CPU(%)
MEM(%)
HDD(%)
상태
서울 구로구
62.7
70.0
13.6
오류
Total Session Count
1,824,023
Protocol
35
Application
273
Detection Protocol
3
Detection Application
3
Detection Private IP
5
Detection Public IP
3,292
AI 분석 결과, 2025-02-20 18:00:00 ~ 2025-02-20 23:59:59 기간 동안 총 1,824,023 세션이 수집되었습니다.
수집된 총 Protocol은 35개 Application은 273개로 분석되었으며, 탐지된 총 Protocol은 3개, Application은 3개로 분석됩니다.
식별된 Application중 Top 5는 Amazon Web Services, Google Shared Services, Microsoft Services, Google APIs, Slack로 분석됩니다.
Top 50 Application을 분석하여 아래 대시보드에 출력하였습니다.
AI 어시스턴트
전체 통신에 대한 현황 설명
10.10.0.80
10.10.0.60
10.10.0.92
20.194.120.194
20.200.245.247
111.17.26.12
119.34.14.193
74.208.60.253
116.120.220.13
112.162.8.141
123.171.17.27

2. AI DPI 분석
- AI DPI 개요

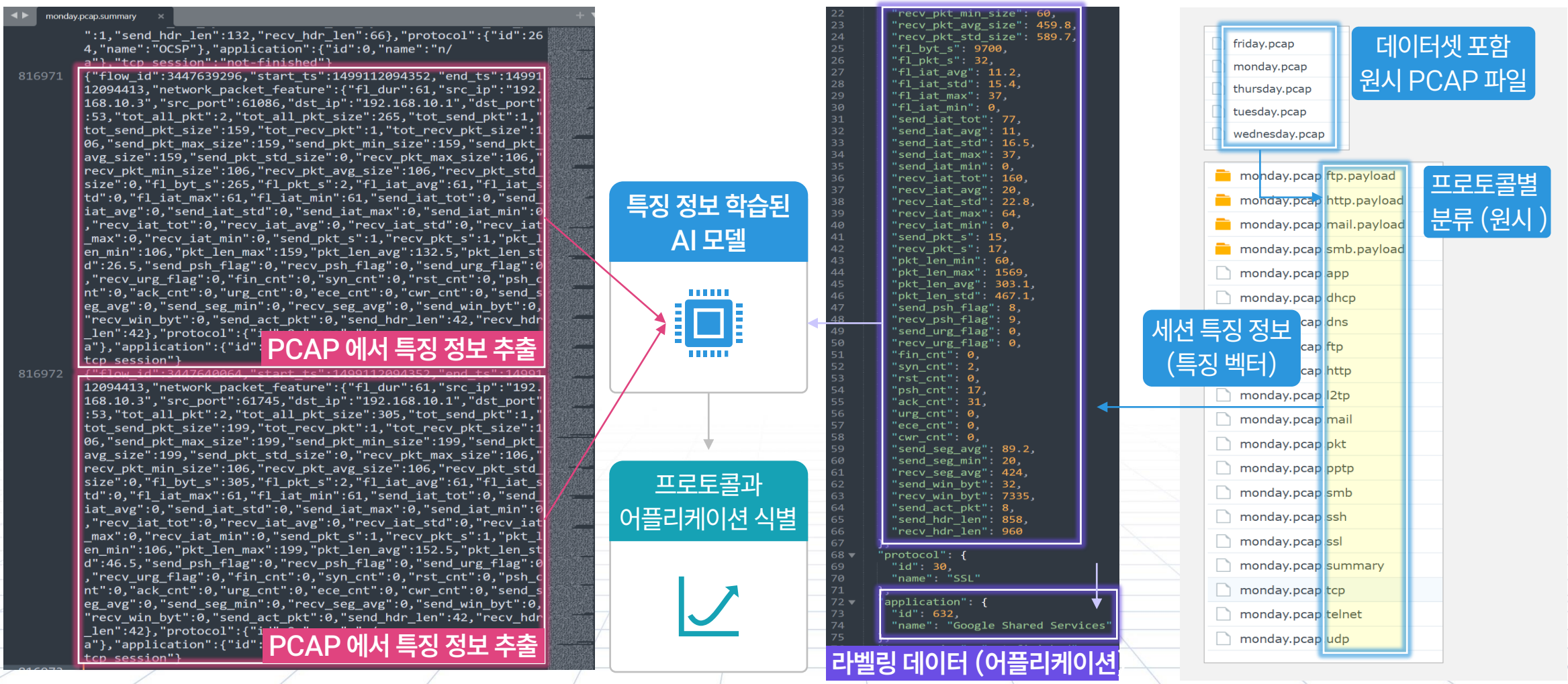
AI 기반 DPI(Deep Packet Inspection)을 통한 가시성 확보와 상세한 메타데이터 추출 및 분석

네트워크 레이어의 최상위에 있는
L7 패킷 전체에 대한 검사를 수행,
500종 이상의 L7 프로토콜을 식별

세션 별 SRC IP, DST IP, Protocol, Application 정보를 제공하여 상세한 트래픽 정보를 확인



2. AI DPI 분석
- AI DPI 학습 모델

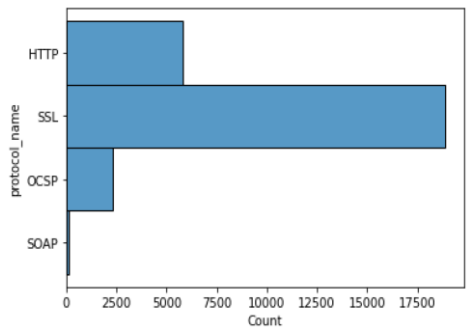


2. AI DPI 분석
- AI DPI 모델 검증 결과

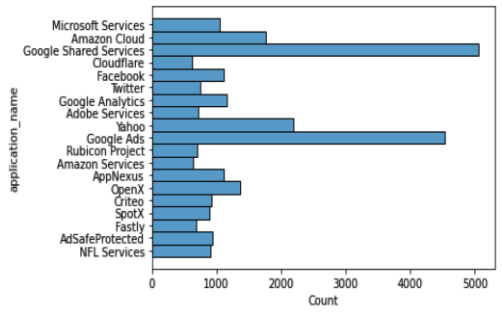
원시 데이터 (pcap) 으로 부터 특징 추출

	target	src_ip	src_port	dst_ip	dst_port	l4_protocol	fl_dur	tot_all_pkt	tot_all_pkt_size	tot_send_pkt	...	send_seg_avg	send_seg_
166	0	192.168.10.5	49176	134.170.115.55	443	6.0	139.0	5.0	495.0	3.0	...	87.0	
199	0	192.168.10.14	49433	131.253.61.80	80	6.0	140.0	8.0	1293.0	5.0	...	82.8	
222	0	192.168.10.14	49434	131.253.61.80	443	6.0	0.0	7.0	6149.0	3.0	...	83.7	
228	0	192.168.10.14	49435	65.152.202.208	80	6.0	133.0	7.0	948.0	4.0	...	94.8	
275	0	192.168.10.14	49441	23.50.75.27	80	6.0	47.0	7.0	2773.0	4.0	...	81.8	
...	...	...	...	...	...	...	...	...	...	...	...	...	
1054732	0	192.168.10.3	55166	23.211.102.137	80	6.0	76.0	15.0	3496.0	7.0	...	365.4	
1055143	0	192.168.10.14	59152	64.4.54.254	443	6.0	549.0	19.0	9040.0	10.0	...	361.6	
1055299	0	192.168.10.14	59153	23.21.84.138	443	6.0	152.0	13.0	4789.0	7.0	...	144.6	
1055343	0	192.168.10.12	48284	23.63.226.81	80	6.0	77.0	7.0	1158.0	4.0	...	108.0	
1055467	0	192.168.10.8	10399	184.84.243.218	80	6.0	249.0	7.0	1096.0	4.0	...	96.0	

프로토콜 분포



어플리케이션 분포



AI 모델 검증 (프로토콜)

Model	Accuracy	AUC	Recall	Prec.	F1	Kappa	MCC	TT (Sec)
	0.9922	0.9993	0.9558	0.9922	0.9922	0.9830	0.9831	1.0990
	0.9856							0.1210
	0.9514							0.8040
	0.9431							0.9010
	0.9267	0.0000	0.7393	0.9262	0.9240	0.8390	0.8401	0.1490
	0.8310	0.8374	0.6035	0.8356	0.8244	0.6348	0.6436	0.5730
	0.8309	0.0000	0.4878	0.8318	0.8080	0.5630	0.6027	0.0230
s	0.7029	0.5194	0.2906	0.6370				
	0.5198	0.8679	0.7102	0.7837				

[비공개] 가
가장 좋은 결과 도출 (99%)

9종 AI 모델 검증

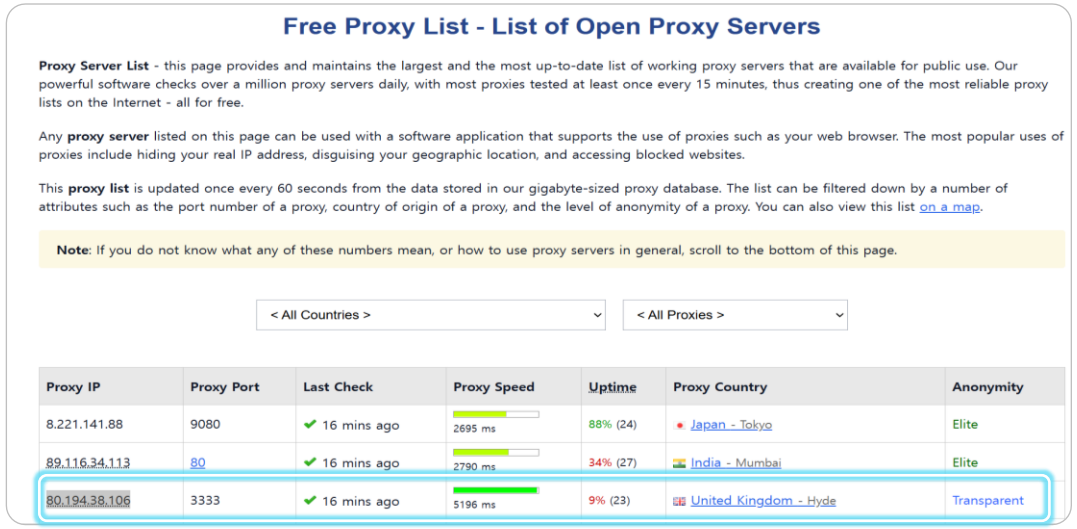
AI 모델 검증 (어플리케이션)

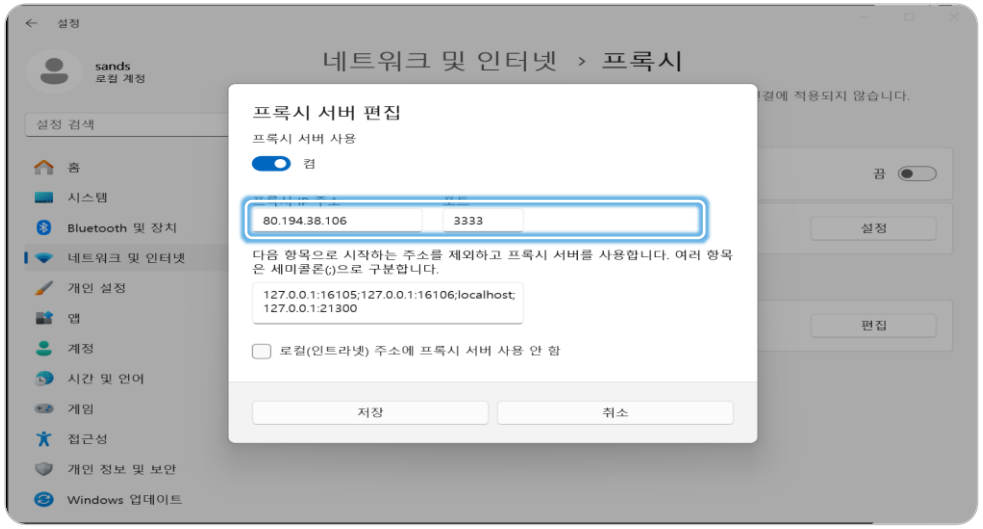
Model	Accuracy	AUC	Recall	Prec.	F1	Kappa	MCC	TT (Sec)
	0.8814	0.9898	0.8816	0.8845	0.8806	0.8692	0.8697	1.3380
	0.8251							
	0.671							
	0.512							
	0.442							
	0.3982							
	0.3479	0.7958	0.3280	0.4015	0.3472	0.2877	0.2931	0.7780
	0.2249	0.7526	0.2940	0.4058				
	0.1186	0.6166	0.1900	0.1600				

[비공개] 가 가장 좋은 결과 도출 (88%)
→ 어플리케이션의 경우 좀 더 복잡한 통신 구조를 가지고 있어 탐지율 낮음

9종 AI 모델 검증

2. AI DPI 분석
- AI DPI 식별 결과





프록시로 포트 변경해도, 트래픽 특징으로 식별하기 때문에
어플리케이션 (YouTube) 정확하게 식별 가능

2. AI DPI 분석
- AI DPI TTA 검증 결과

시험성적서

한국정보통신기술협회 소프트웨어시험인증연구소 주소: 경기도 성남시 분당구 분당로 47 전화: 031-780-9137, Fax: 031-724-0189	성적서번호: BT-A-21-0498	TTA

1. 의 뢰 자
   · 회사(기관)명 : ㈜샌즈랩
   · 주 소 : (06143) 서울특별시 강남구 선릉로 577 조선내화빌딩 4층, 샌즈랩
   · 계약일자 : 2021.12.27.
2. 시험성적서의 용도 : 과제 산출물 검증용
3. 제 품 명 : AI 기반 사이버 위협 탐지 및 유형 분류 도구
4. 버 전 : v1.0
5. 시험장소 : □ 고정시험실, ■ 현장시험
   · 시험수행주소 : ㈜샌즈랩, 서울특별시 강남구 선릉로 577 조선내화빌딩 4층
6. 시험기간 : 2021. 12. 28. ~ 2022. 1. 4.
7. 시험방법 :
   - 상세 내용은 "<3.시험항목 및 방법>" 참고
8. 시험환경 : 실온, 실습
9. 시험결과 : BT-A-21-0498-GR 참조

비 고 : 1. 이 성적서의 시험결과는 의뢰자에 의해 제공된 시험품에 한하며 용도 이외의 사용을 금합니다.
2. 이 성적서는 KS Q ISO/IEC 17025 및 KOLAS 인정 분야와 관련 없습니다.
3. 이 성적서의 진위여부는 기업지원플러스(www.g4b.go.kr)에서 진위확인코드로 확인 가능합니다.

확 인	작성자 성 명 : 조 경 우	승인자 직 책 : 기 술 책 임 자 성 명 : 신 준 호 (서명)

2022년 1월 4일

한국정보통신기술협회 회장

TPS-0071-3(01)

5. 시험결과

시험 항목별 시험 결과는 아래와 같다. (상세 시험 결과는 "<6. 시험기록>" 참고)

ID	시험항목	시험목표 및 기준	결과	비고
TC1	침해사고 예·탐지 데이터셋 메타데이터 생성 정확도	<시험목표> 수집된 http 프로토콜 원천데이터에 대한 메타데이터 생성 정확도 확인 <시험기준> o 기준: 원천데이터에 포함된 http request 주소와 시험의뢰기업이 사전에 생성한 메타데이터의 http request 주소의 일치 여부 확인 o 산정식: $X = \frac{A}{B}$ - A: 원천데이터와 메타데이터의 http request 주소 일치 수량 - B: 원천데이터 총 수량	$X = 1$	-
TC2	침해사고 예·탐지 데이터셋 기반 프로토콜 및 어플리케이션 식별 정확도	<시험목표> TC1의 메타데이터와 레이블을 기반으로 학습한 시험대상 제품(모델)의 프로토콜 및 어플리케이션 식별 정확도 확인 <시험기준> o 기준: 프로토콜 및 어플리케이션 식별모델별 다중 분류 성능 o 산정식: Accuracy(%) = $\frac{\text{결과일치 샘플수}}{\text{전체 샘플수}} \times 100$	프로토콜 식별모델 98.10% 어플리케이션 식별모델 91.80%	-
TC3	침해사고 예·탐지 데이터셋 기반 공격, 정상 이벤트 구분 정확도	<시험목표> TC1의 메타데이터와 레이블을 기반으로 학습한 시험대상 제품(모델)의 이벤트 분류 정확도 확인 <시험기준> o 기준: 이벤트(공격/정상) 이진 분류 성능 o 산정식: Accuracy(%) = $\frac{\text{결과일치 샘플수}}{\text{전체 샘플수}} \times 100$	93.40%	-

ID	TC5

* System event log: 원천데이터-12,199건 / 학습데이터-12,199건

No.	속성명	유형	전처리 후 특성 수
1	action	범주형	10
2	event_id	범주형	10
3	event_time	텍스트(연속형)	5
4	host	범주형	3
5	level	범주형	5
6	logtype	범주형	4
7	payload	텍스트(연속형)	10
8	source	범주형	10
	계		57

※ 성능 결괏값은 시험 로그, 코드 및 모델링 결과 파일(.csv)을 통해 확인함

ID	TC6

상세 시험결과

- 시험대상 제품(모델)의 분류 성능은 평균 99.90%로 확인됨

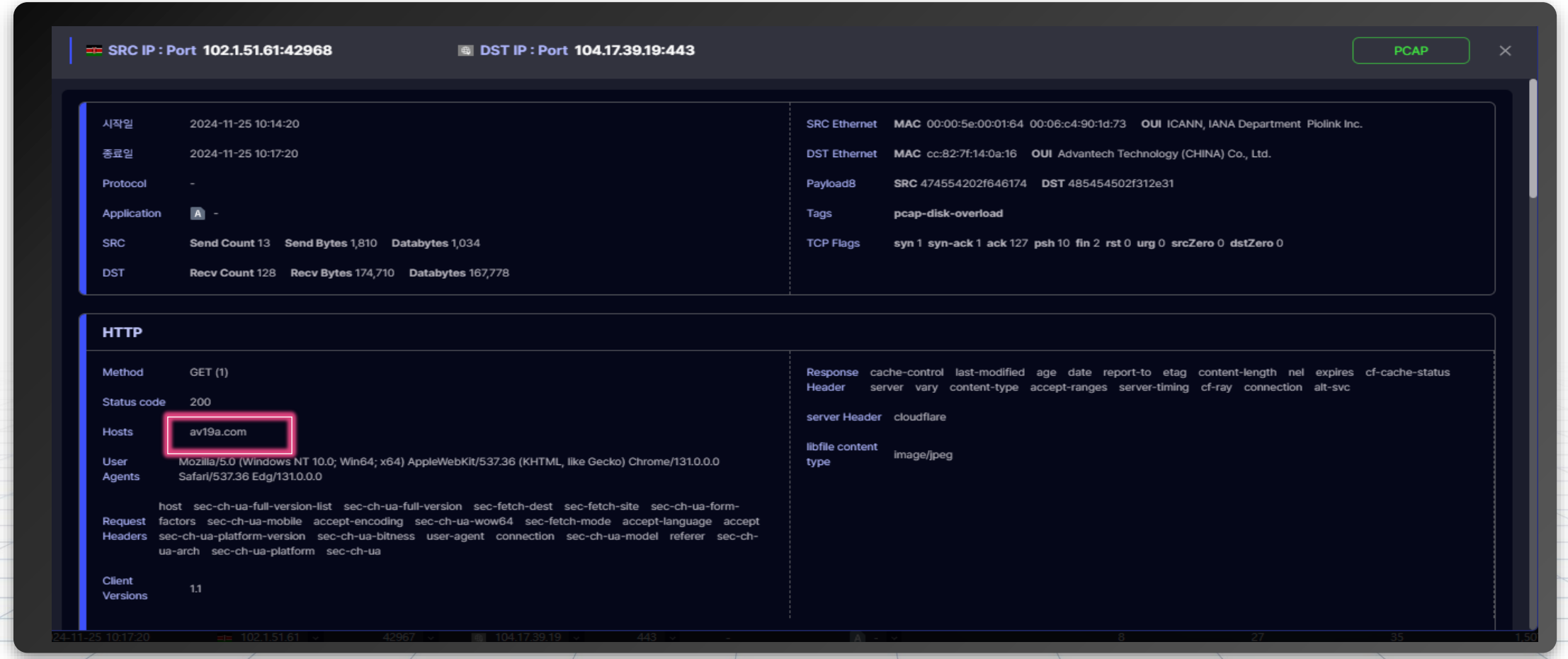
공격 탐지 분류 성능				
장비 유형		측정결과		
		Precision	Recall	F1-Score
FW (Firewall)	RF	99.92%	99.98%	99.95%
	XG	99.95%	99.98%	99.97%
IPS (Intrusion Detection System)	RF	98.87%	100%	99.43%
	XG	99.43%	100%	99.72%
IDS (Intrusion Detection System)	RF	100%	100%	100%
	XG	100%	100%	100%
WAF (Web Application Firewall)	RF	100%	100%	100%
	XG	100%	100%	100%
WEB Access log	RF	100%	100%	100%
	XG	100%	100%	100%
System event log	RF	99.81%	99.62%	99.71%
	XG	100%	100%	100%
평균 (F1-Score)				99.90%

* RF: Random Forest, XG: XGBoost

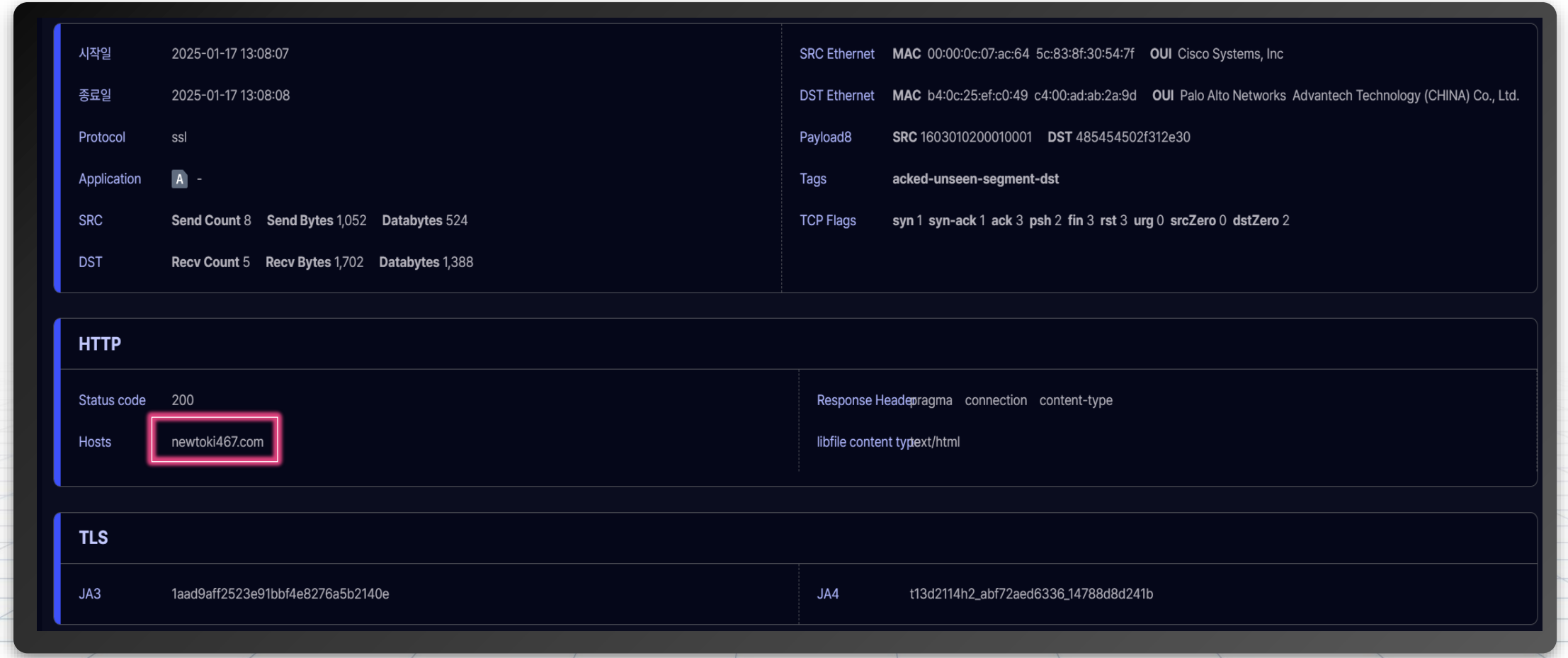
※ 성능 결괏값은 시험대상 제품의 로그 및 모델링 결과 파일(.csv)를 통해 확인함

2. AI DPI 분석
- WEB

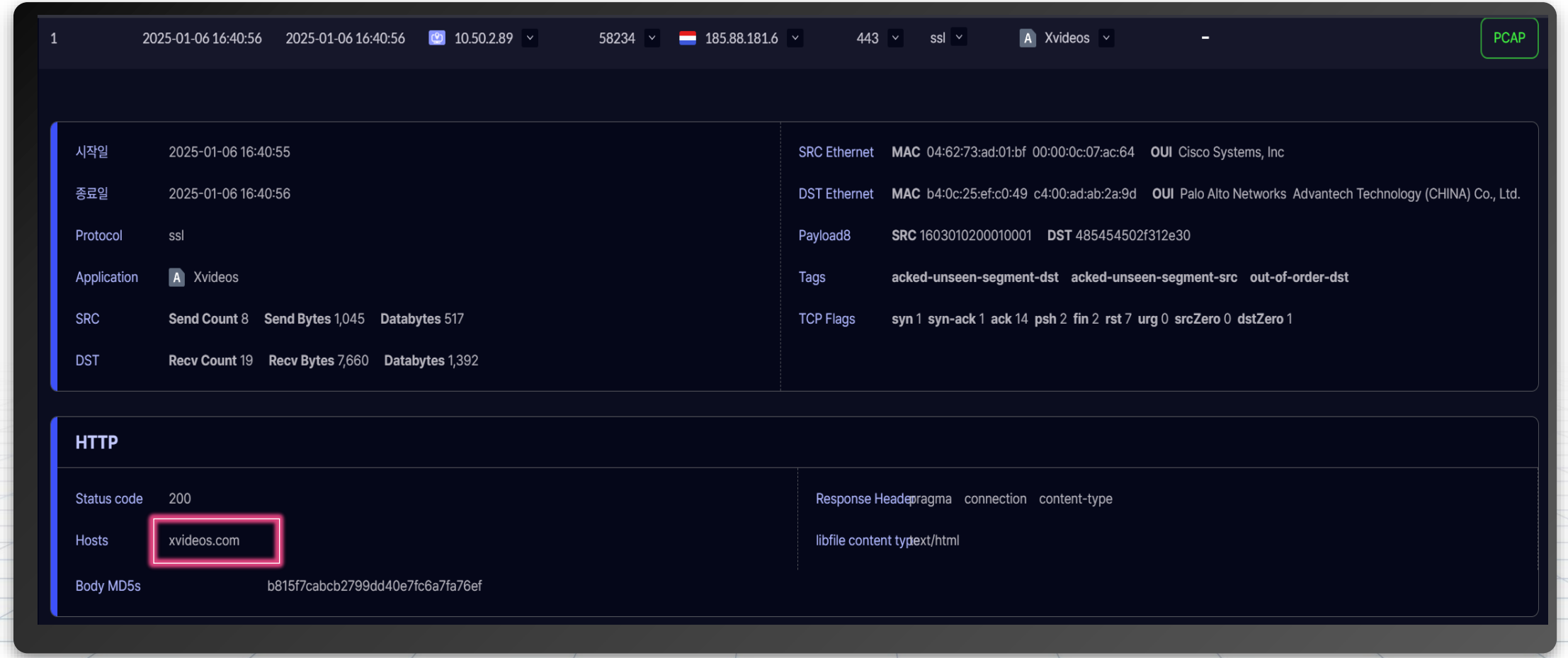
2. AI DPI 분석
- WEB



2. AI DPI 분석
- WEB



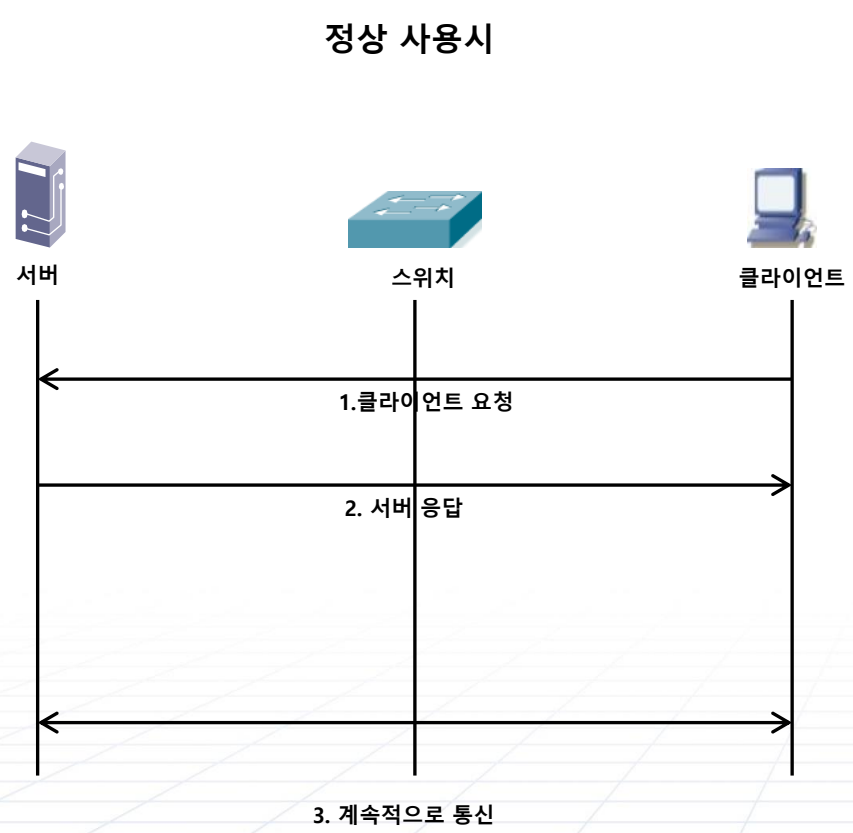
2. AI DPI 분석
- WEB

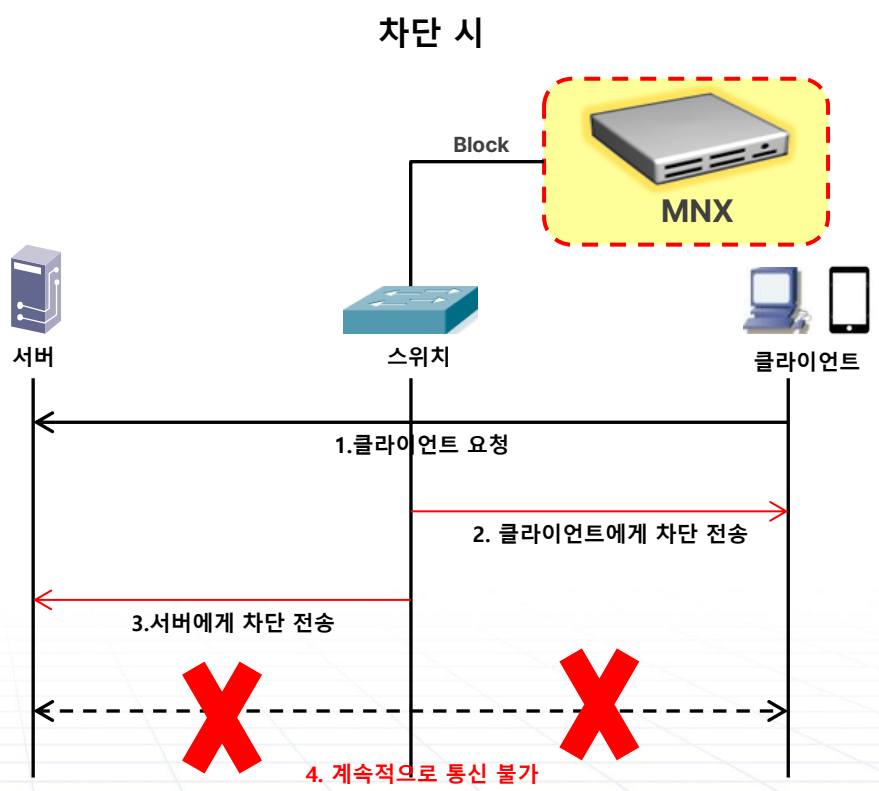


3. 탐지
- WEB

#	Ticket-ID	발생 시간 ↓↑		플레이북 명	기준 조건	위험도	SRC IP
458	1623	2025-04-25 18:16:25	2025-04-25 18:16:25	유해사이트 접속탐지(성인사이트)	출발지 IP	하	10.10.0.60
457	1622	2025-04-25 18:06:25	2025-04-25 18:06:25	유해사이트 접속탐지(성인사이트)	출발지 IP	하	10.10.0.60
456	1621	2025-04-25 17:56:25	2025-04-25 17:56:25	유해사이트 접속탐지(도박사이트)	출발지 IP	하	10.10.0.60
455	1620	2025-04-25 17:46:25	2025-04-25 17:46:25	유해사이트 접속탐지(성인사이트)	출발지 IP	하	10.10.0.60
454	1619	2025-04-25 17:36:25	2025-04-25 17:36:25	유해사이트 접속탐지(불법웹툰사이트)	출발지 IP	하	10.10.0.60
453	1618	2025-04-25 17:26:25	2025-04-25 17:26:25	[AI 위협 탐지] 내부 단일 호스트에서 다...	출발지 IP	상	10.10.0.60
452	1617	2025-04-25 17:16:25	2025-04-25 17:16:25	[AI 위협 탐지] 내부 단일 호스트에서 다...	출발지 IP	상	10.10.0.60

4. 대응
- TCP 세션 차단

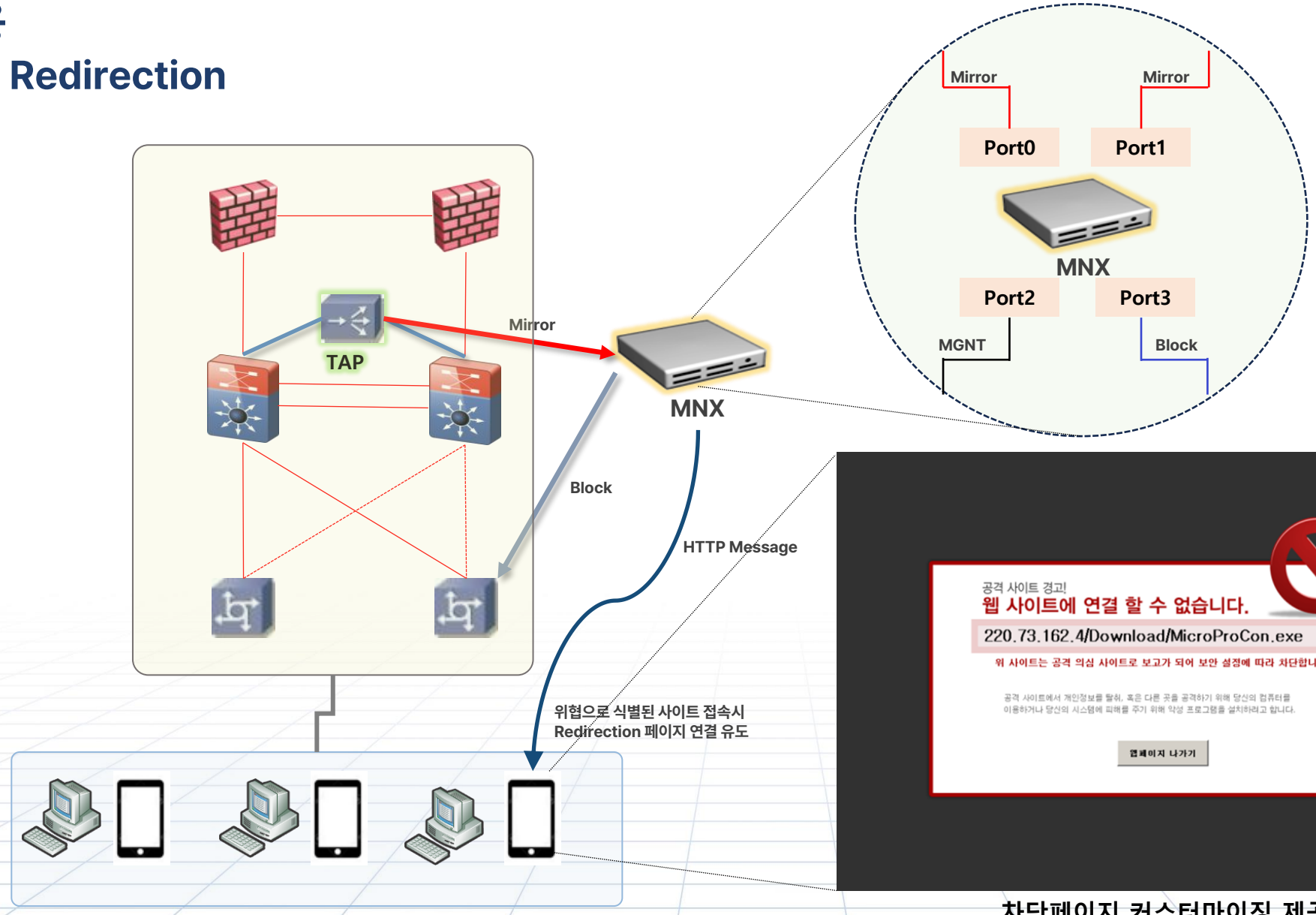




RST 기반 차단.

- RST 패킷이 클라이언트(단말기)로 도달할수 있어야하며, 네트워크 장비에 의해 드롭되지 않아야 합니다.

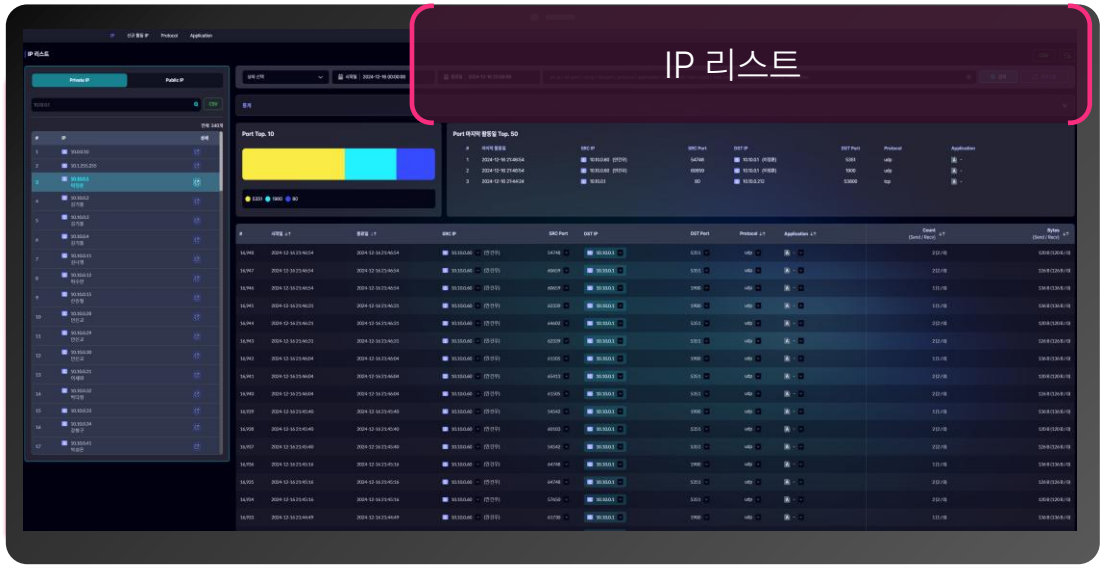
4. 대응
- HTTP Redirection

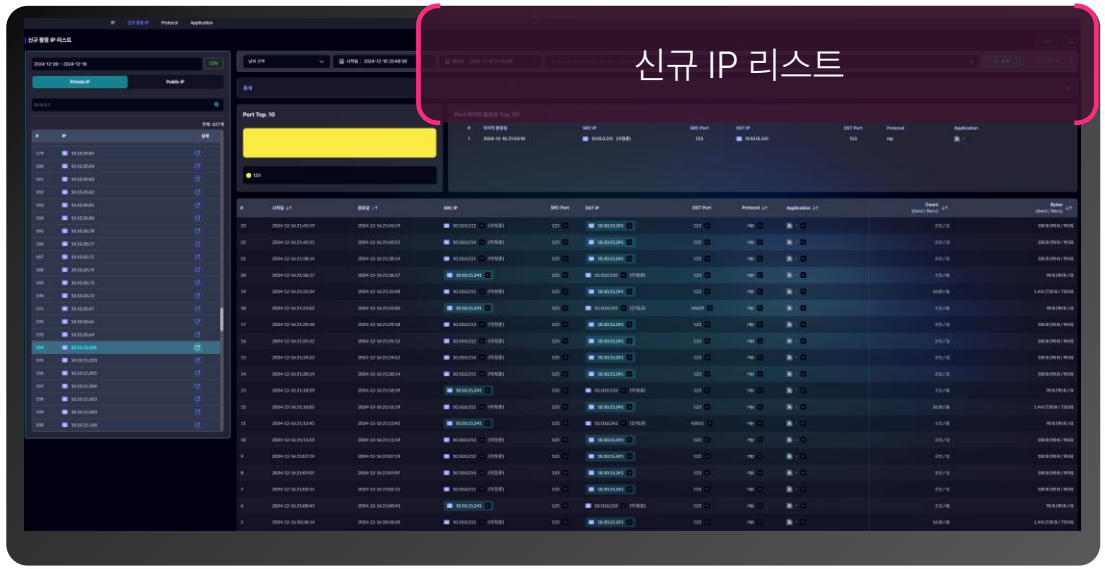


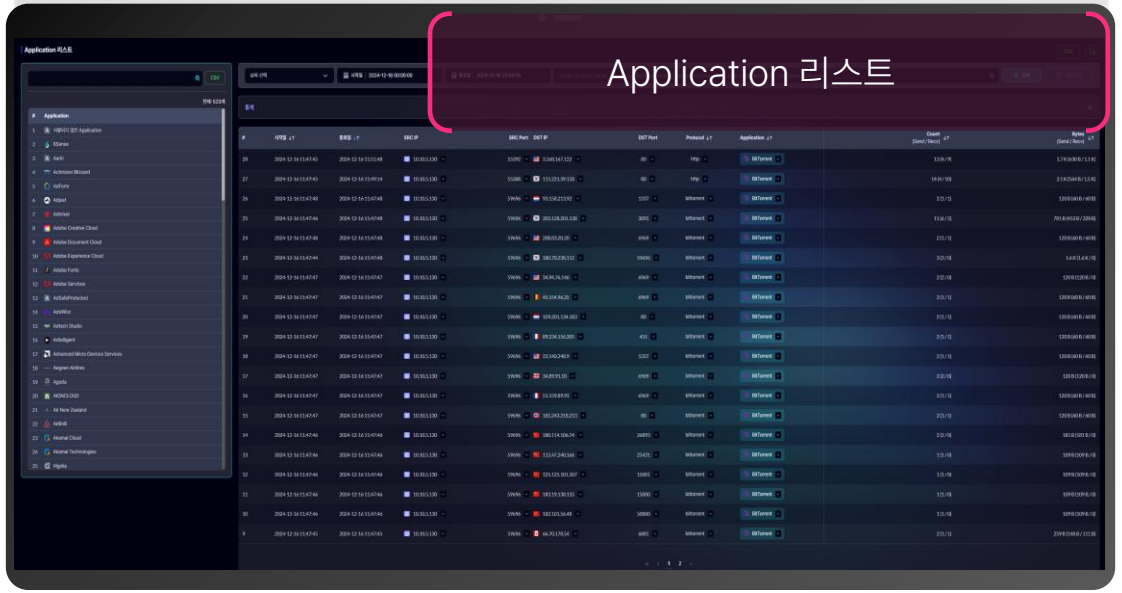
차단페이지 커스터마이징 제공

차단시 Redirection 페이지 제공
- 복호화장비를 통해 암호화 트래픽에 대해 복호화 트래픽을 받아야만 가능합니다.

5. 가시화
- 트래픽 활동







Security,
AI,
Network,
Data for
Society

SANDS Lab

경기도 과천시 과천대로7나길 25, 12F
02-704-7502
www.sandslab.io