O24Sec

(**O**bject **O**riented Clustering **for Sec**urity Monitoring)

부제 : 객체 중심 보안관제 오탐제거

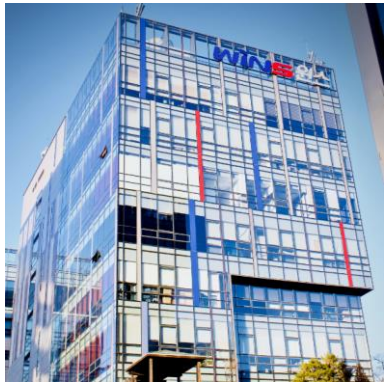
팀 (18조) : 맬러리를 찾아서

팀 소개 (맬러리를 찾아서)

김민송

장우혁

산학 담당
윤명근 교수님



㈜윈스
최병환 팀장님

Contents

산학 기관 소개

〈Wins〉

윈스는 **세계적으로 인정받은 기술력**을 가진 국가대표 정보보호기업 입니다.

Sniper® BD1

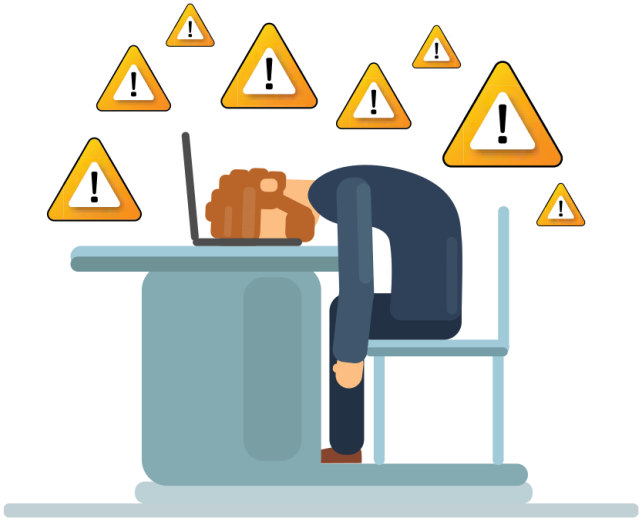
Sniper® IPS

산학 기관 요구 사항

자사 정보보안 솔루션 : “**SNIPER BD1 오탐(False Positive)** 제거”

〈Sniper IPS〉

〈Sniper BD1〉



〈Alert fatigue〉

제안 기술 (배경)

데이터 전처리의 중요성

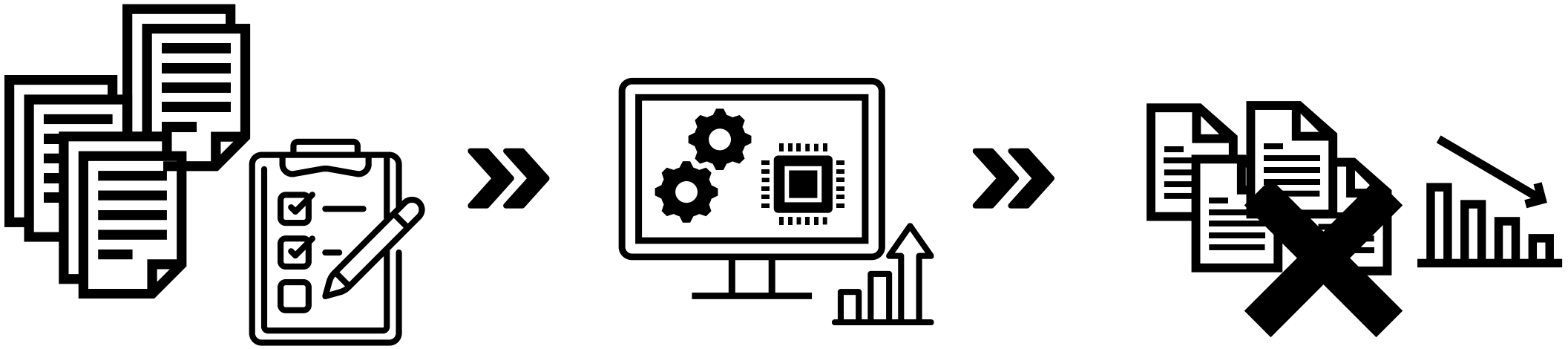
〈“Garbage in Garbage out”〉

모델	정확도	정밀도	재현율	F1-score
정합 전	98.02%	93.76%	59.6%	72.8%
정합 후	98.23%	96%	95.42%	94.3%

〈“데이터 정합 후 성능 향상” , NetSec2020 송중석 박사〉

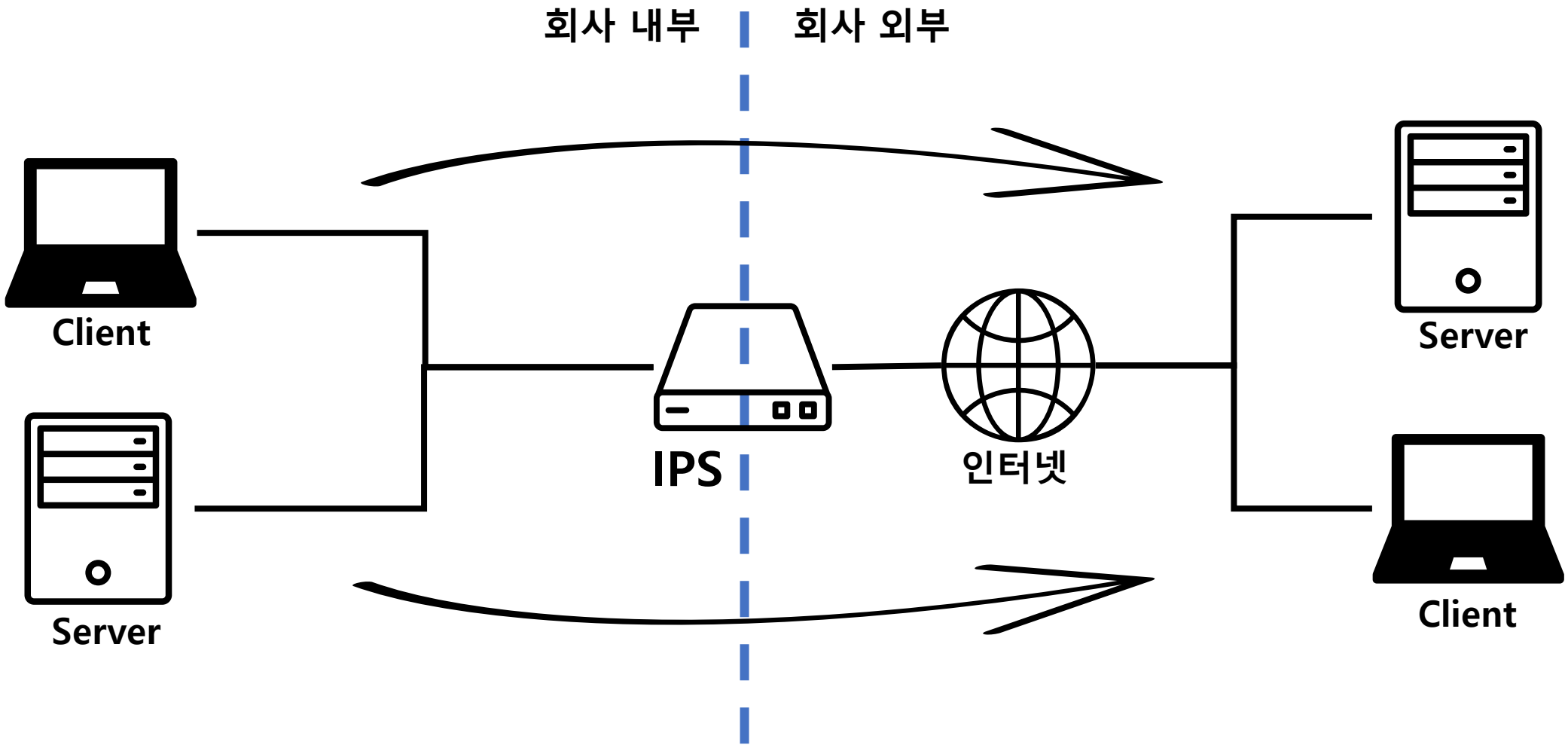
제안 기술 (배경)

"**인공지능 학습데이터 셋에 대한 라벨의 정확도**를 높여 모델의 오탐률을 낮추는 것"

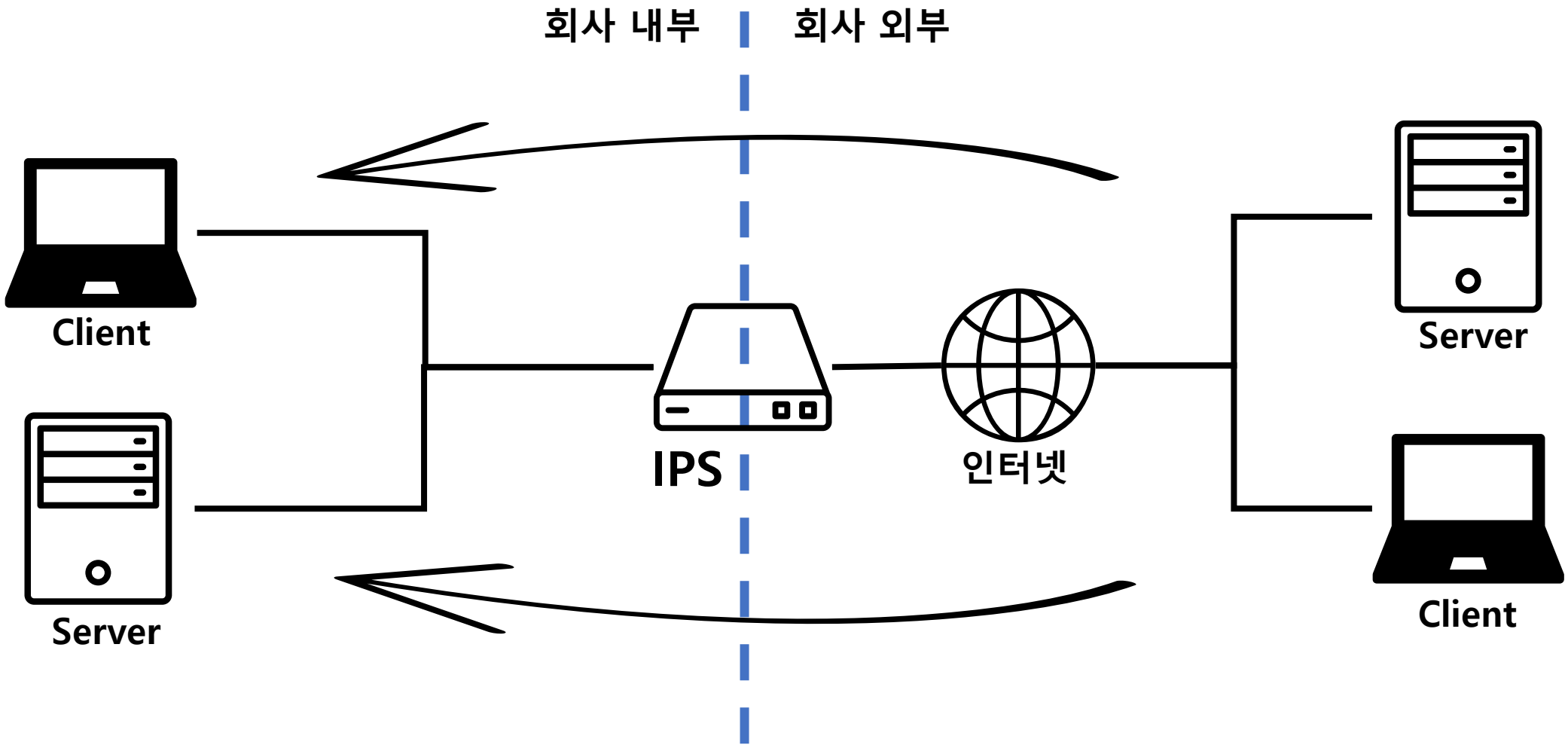


재라벨링 **모델 성능 향상** **오탐 제거**

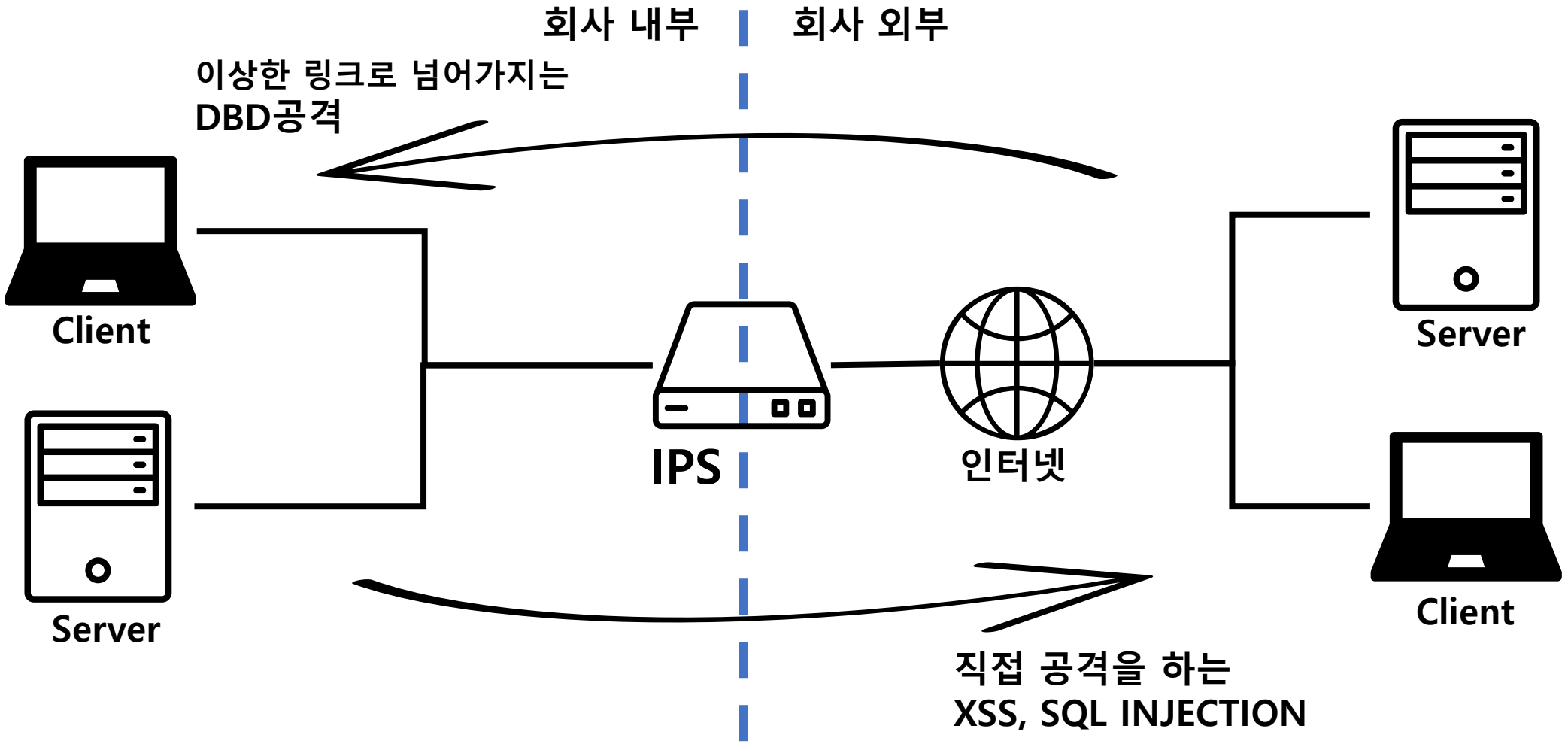
제안 기술(배경 : 네트워크 흐름)



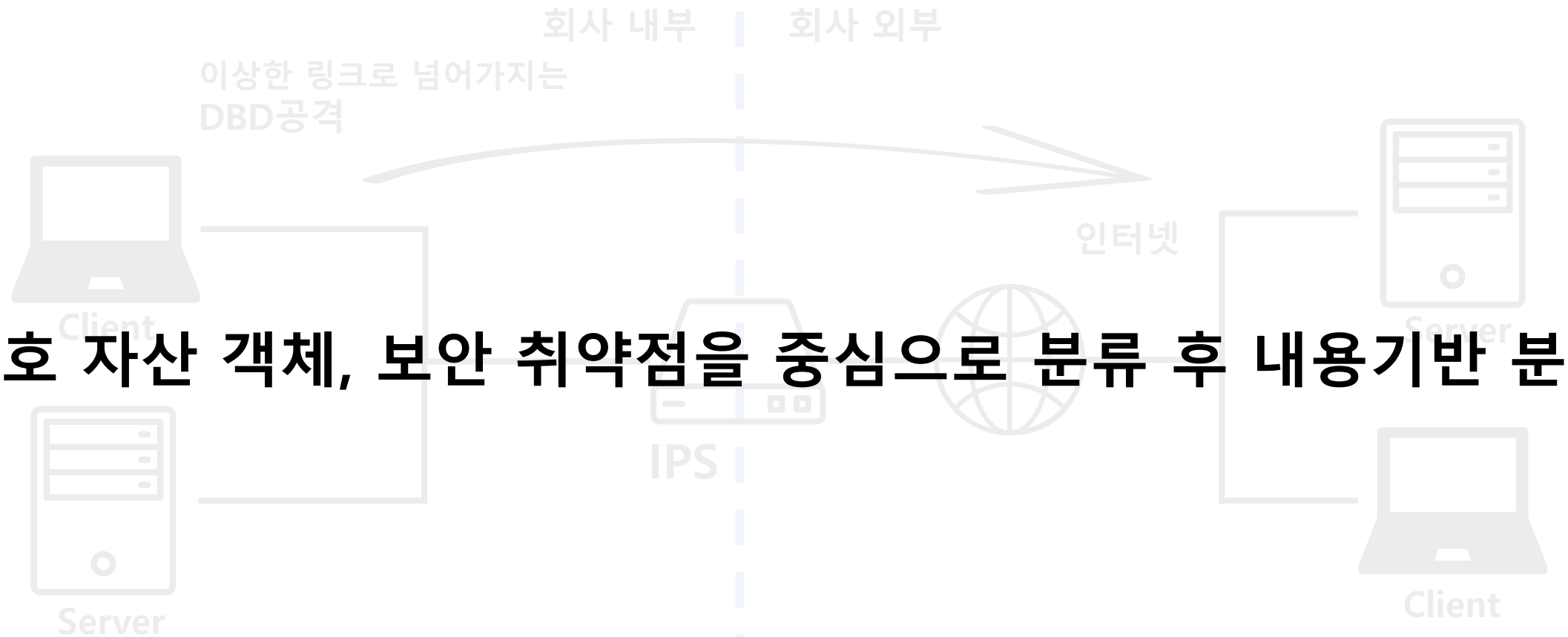
제안 기술(배경 : 네트워크 흐름)



제안 기술(배경 : 네트워크 흐름)

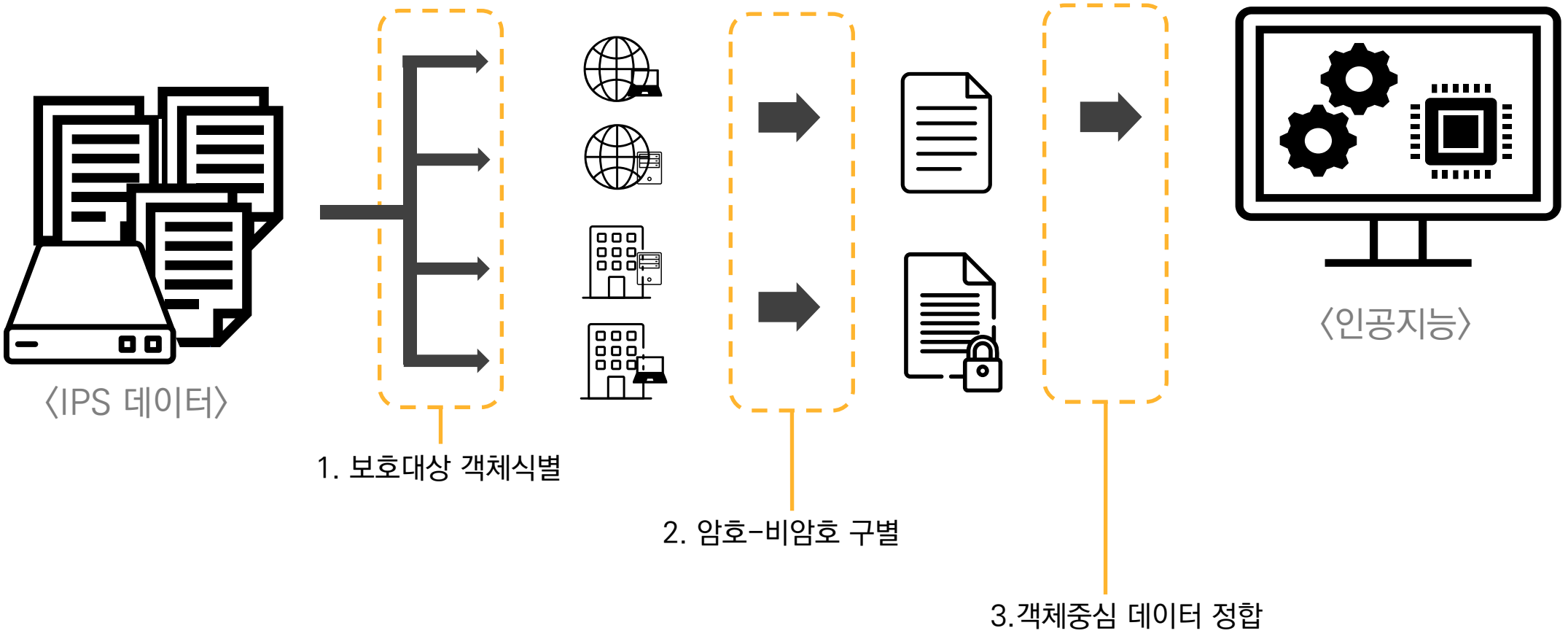


제안 기술 (배경 : 네트워크 흐름)



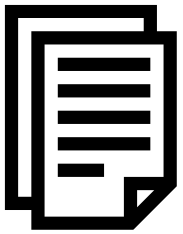
보호 자산 객체, 보안 취약점을 중심으로 분류 후 내용기반 분석

제안 기술



프로젝트 진행상황 (1. 보호대상 객체식별)

- 사용데이터: IPS 이벤트 약 2000만건(1년)



- **Source IP**
- **Destination IP**
- **Source Port**
- **Destination Port**
- **Protocol**

〈5-Tuple〉

From 외부 클라이언트 To 내부 서버

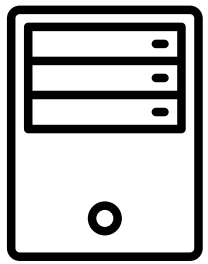
From 외부 서버 To 내부 클라이언트

From 내부 서버 To 외부 클라이언트

From 내부 클라이언트 To 외부 서버

프로젝트 진행상황 (1. 보호대상 객체식별)

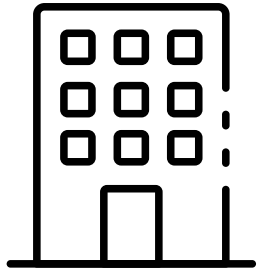
Step1



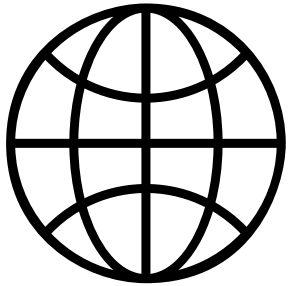
Server

Client

Step2



회사 내부



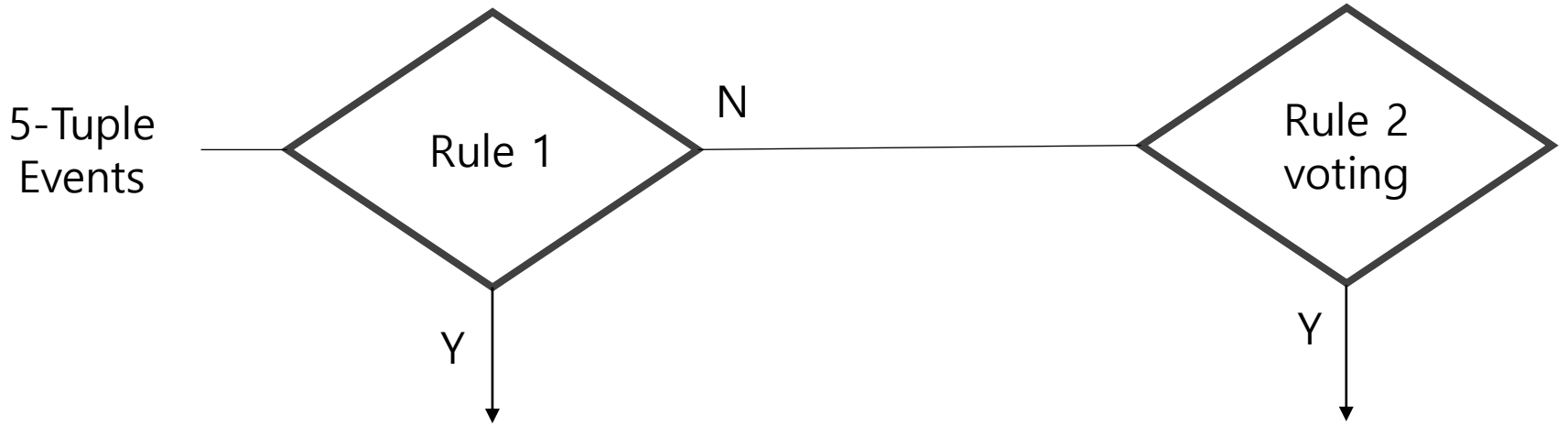
회사 외부

프로젝트 진행상황 (1. 보호대상 객체식별)

Step1: 서버-클라이언트 분류

1. IP:PORT 카운트가 높은 쪽
2. IP의 PORT 종류가 적은 쪽
3. IP에서 해당 PORT 점유율이 높은 쪽

한 쪽만 1024 미만의 포트를 가짐



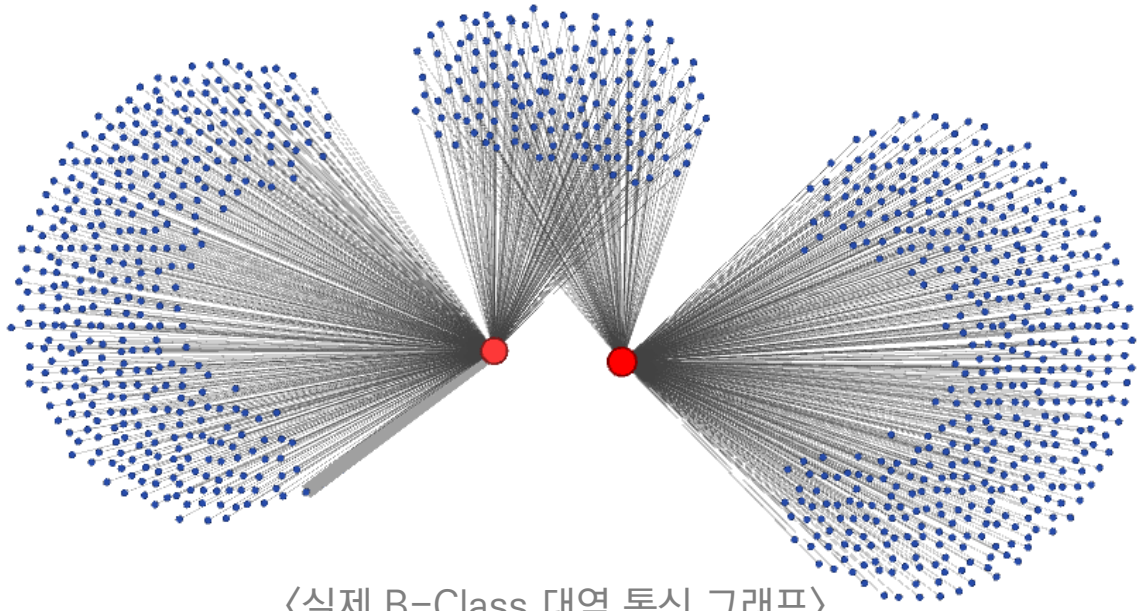
1024 미만: 서버
1024 이상: 클라이언트

과반수쪽: 서버
반대쪽 : 클라이언트

프로젝트 진행상황 (1. 보호대상 객체식별)

Step2: 내부-외부 분류

- IP를 B-Class대역으로 묶었을 때 통신한 상대 B-Class대역이 많으면 내부로 판별



〈실제 B-Class 대역 통신 그래프〉

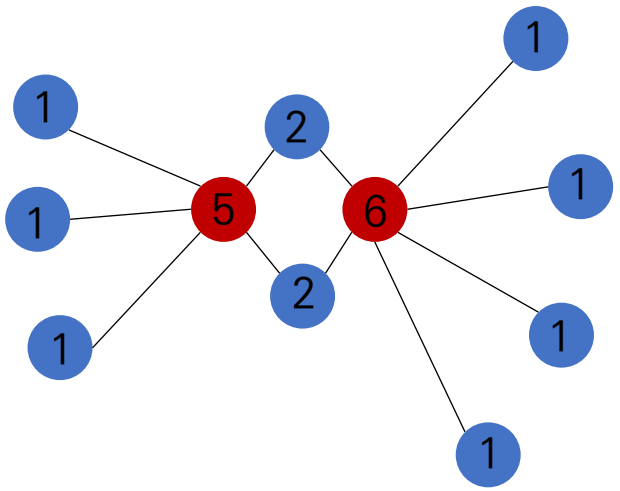
빨간 노드: 내부
파란 노드: 외부
엣지 : 통신

프로젝트 진행상황 (1. 보호대상 객체식별)

Step2: 내부-외부 분류

- 통신한 상대 B-Class대역이 많은 순으로 내림차순 정렬 후 임계점까지 내부로 분류

내부
외부



〈IPS이벤트 B-Class IP 예시 그래프〉

내림차순 정렬

B-Class	상대방 종류	내부 개수(가정)
내부1	6	1
내부2	5	2
외부1	2	3
외부2	2	
외부3	1	
외부4	1	
외부5	1	
외부6	1	
외부7	1	
외부8	1	
외부9	1	

외부

내부 개수를 1씩 추가,

상대방 종류가 내부 개수보다 작은 B-Class 부터 외부

프로젝트 진행상황 (암호화 분리)

Entropy(복잡도)

페이로드에 Byte가 얼마나 여러 종류(최대 256가지)로 들어가 있는지

<Byte Stream>

일반적으로 암호화 되었을 경우 Entropy값이 높음
Ex) SSH, TLS

ADDEB79218960CA907EE9907EABCFGDD4
8CE1WGN5T4RGHER1D2FQ5VRNY4NUM

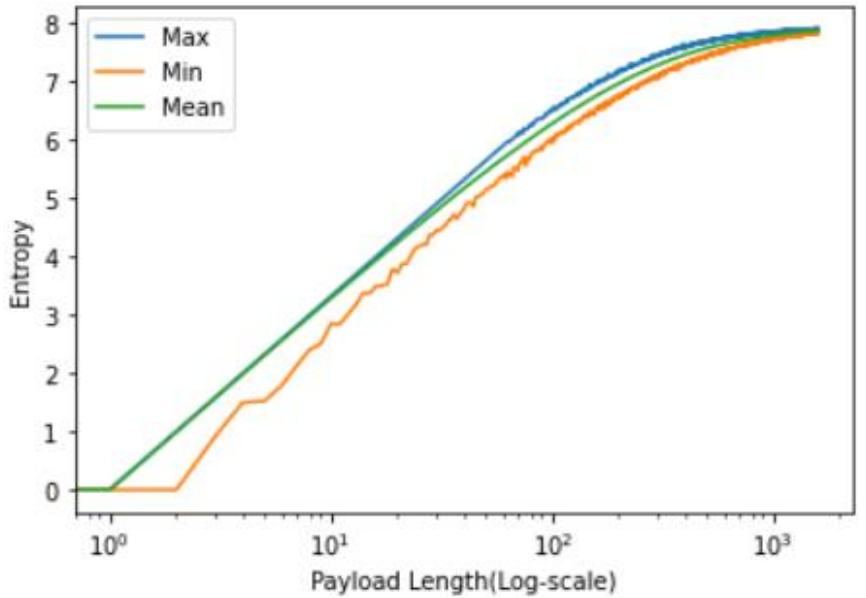
일반적으로 암호화 되지 않았을 경우 Entropy값이 낮음
비슷한 범위의 Byte 값이 계속 쓰이기 때문
Ex) HTTP, FTP

474554202F434F4E54454E542E7068702048
5454502F312E31
("GET /CONTENT.php HTTP/1.1")

프로젝트 진행상황 (암호화 분리)

```
[ 92 ] Byte MAX entropy :  6.39312717344833
[ 92 ] Byte Mean entropy :  6.192444540067714
Packet Entropy :  6.240953260404848
ASCII :  b'5W!₩xf3₩xed₩x189₩xf4y₩x12₩xf8OfHu₩xOfo₩xff₩xdf^₩x81₩x1a~m₩xafo₩x17₩xd9₩x8e₩xcc₩xe7₩xdb₩xf6₩xd1₩xf71₩xfa_₩x8b₩x9b₩xd
f₩x85₩x1ae<7₩xa2₩x87^₩x1b*₩xa9₩xe8₩x10₩x9d₩x82₩x94₩x19₩xd8f*₩xbf₩x9b/₩xe4₩x8b₩x07%₩xf4j₩n₩x85₩x83|₩xe9₩xc7[₩xab7₩xd1q₩xc8N₩x9
c,₩x0b₩x7fdOn₩r₩n'
```

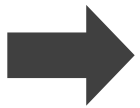
〈Payload 길이에 따른 암호화된 페이로드의 Entropy 최대/평균/최솟값〉



256 미만의 길이를 가진 Payload의 경우 256바이트를 모두 표현하지 못하기 때문에 암호화 되었더라도 최대 Entropy 값인 8에 비해 값이 작다.

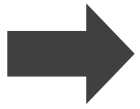
프로젝트 진행상황 (2. 암호화 분리)

1. Entropy가 높지만 식별 가능한 정보가 담겨져 있는 경우



White List

2. 길이가 짧아서 엔트로피가 낮게 측정되지만 불필요한 정보를 담고 있는 경우



Black List

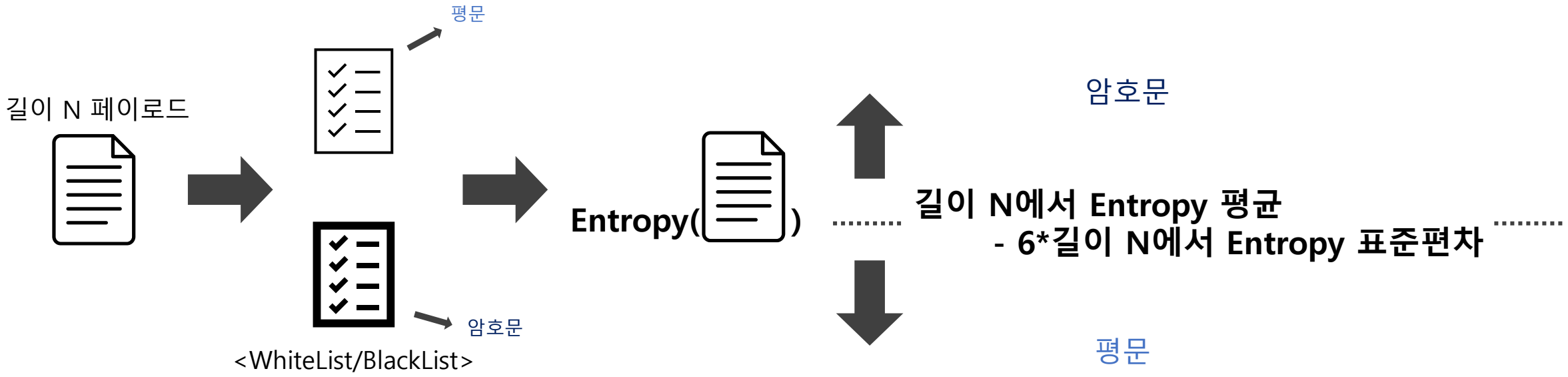
프로젝트 진행상황 (암호화 분리)

최종 Rule :

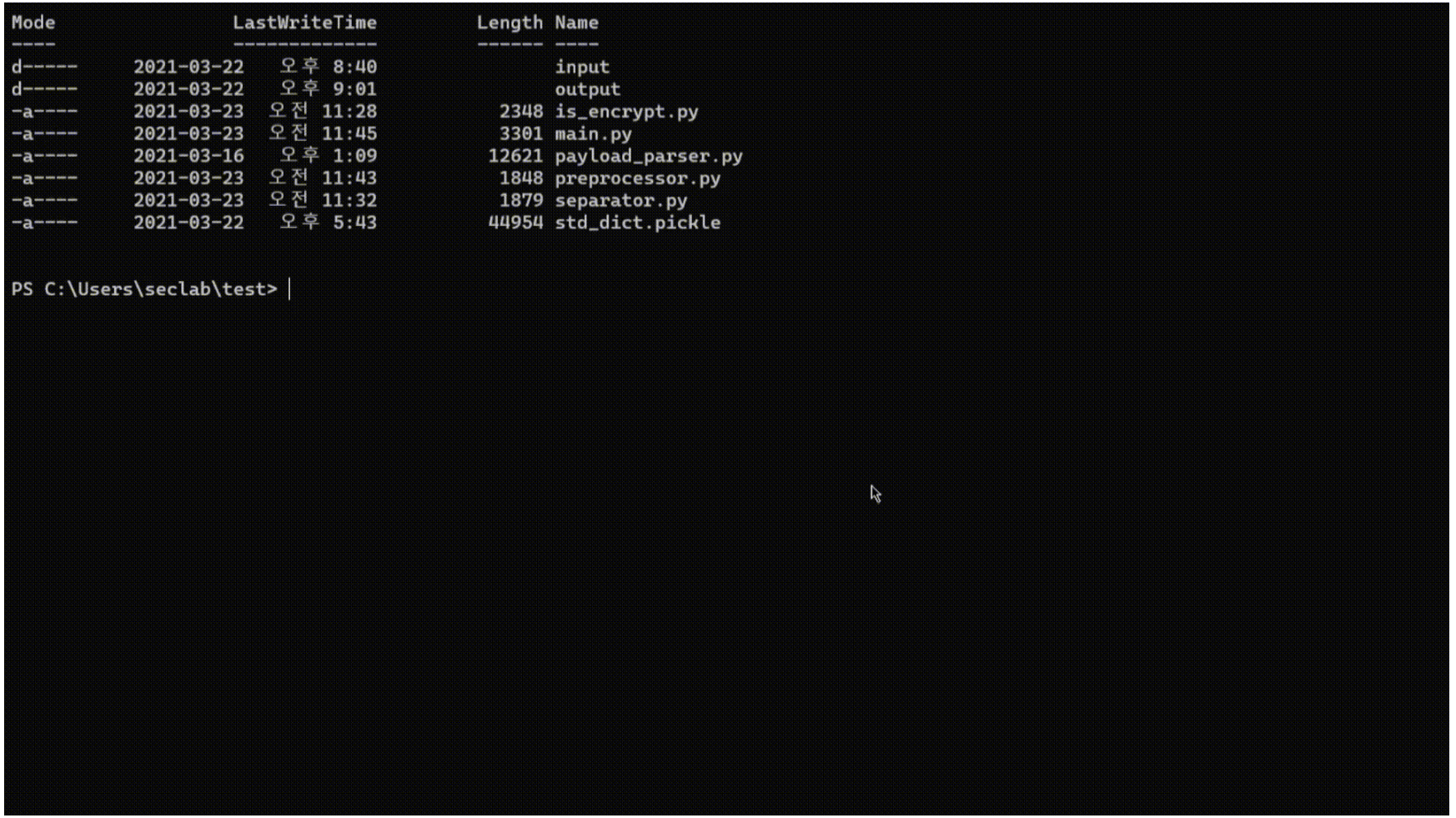
각 페이로드의 길이에 대해 Entropy값이 정규분포 하기 때문에

그 길이에 해당하는 Entropy 평균값에 6*표준편차 값을 뺀 것 보다 Entropy가 클 경우 암호화 된 페이로드 이다.

단, 특정 케이스에 대해 블랙리스트와 화이트리스트로 우선 처리한다.



프로젝트 진행상황 (목표 1, 2 실행 화면)



프로젝트 진행상황 (3. 유사도 기반 클러스터링)

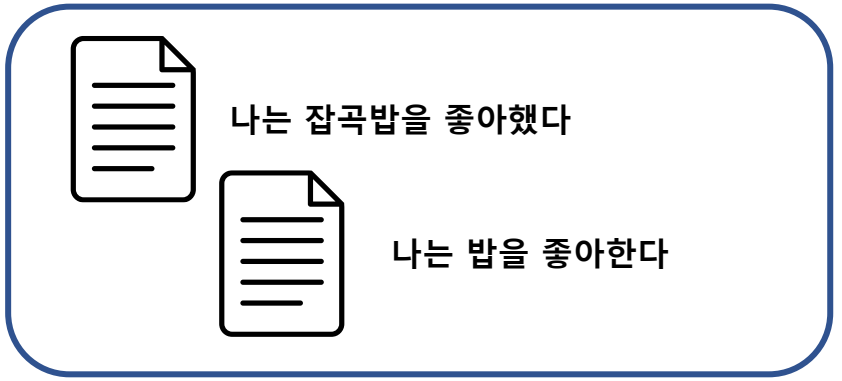
나는 밥을 좋아한다

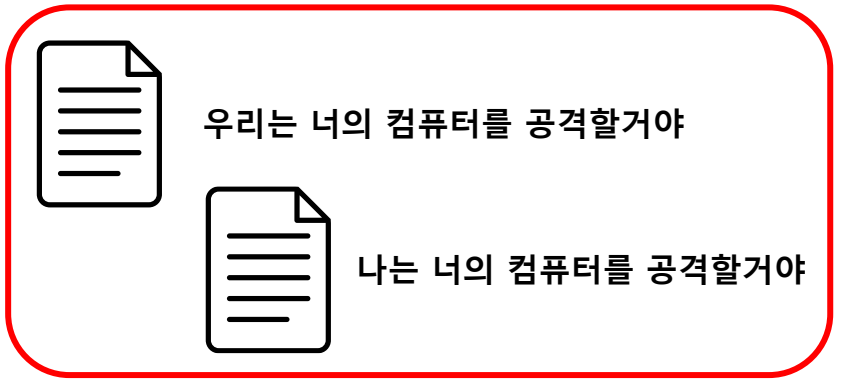
우리는 너의 컴퓨터를 공격할거야

나는 잡곡밥을 좋아했다

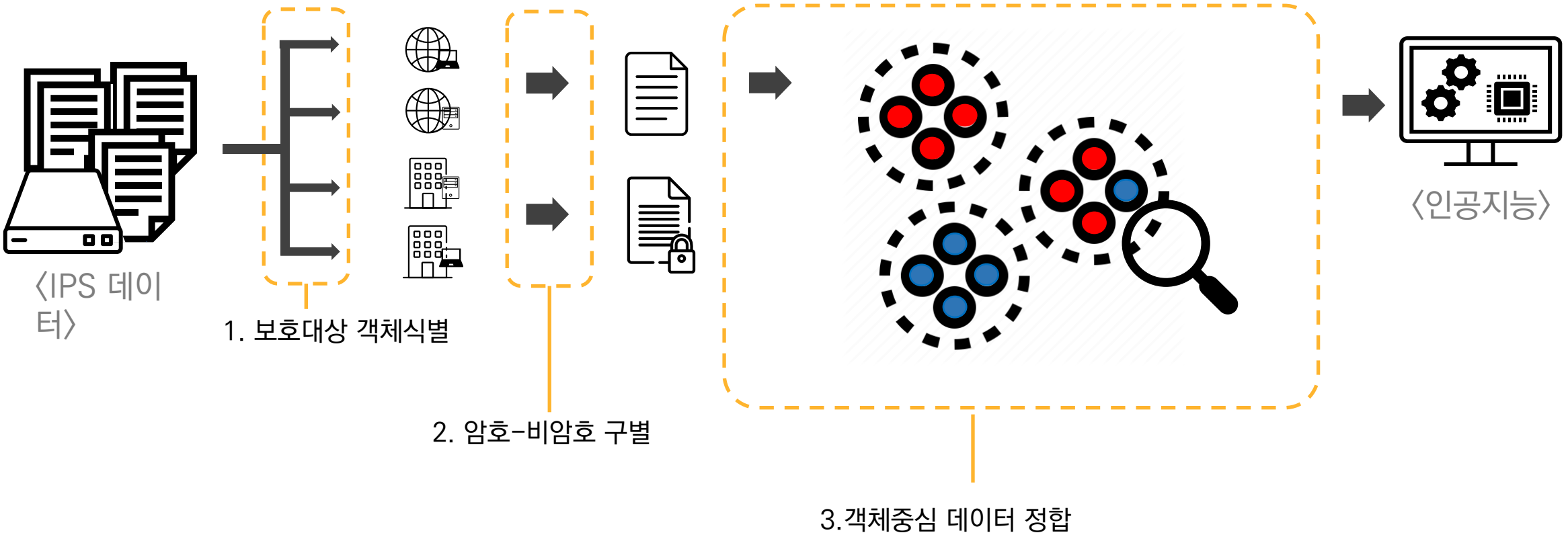
나는 너의 컴퓨터를 공격할거야

유사한 이벤트 끼리 군집화





프로젝트 진행상황 (3. 클러스터링 진행 중)



프로젝트 향후 계획

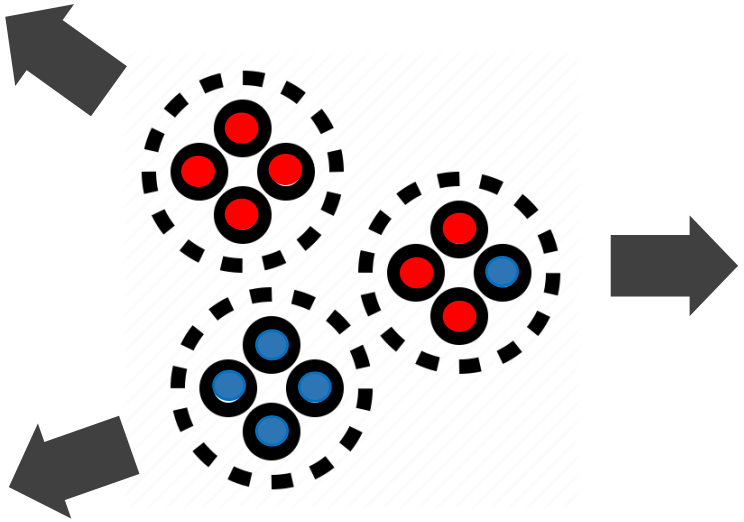
공통적으로 나온 내용 :
Ddos (실제 공격)

1번 IPS 이벤트 : 정탐
2번 IPS 이벤트 : 정탐
3번 IPS 이벤트 : 정탐
4번 IPS 이벤트 : 정탐

공통적으로 나온 내용 :
Download JPG (공격 아님)

1번 IPS 이벤트 : 오탐
2번 IPS 이벤트 : 오탐
3번 IPS 이벤트 : 오탐
4번 IPS 이벤트 : 오탐

각 군집에서의 공통적 내용과 각 이벤트의 정보를 보여줌



공통적으로 나온 내용 :
CMD

1번 IPS 이벤트 : 공격(정탐)
2번 IPS 이벤트 : 공격(정탐)
3번 IPS 이벤트 : 정상(오탐)
4번 IPS 이벤트 : 공격(정탐)

감사합니다.

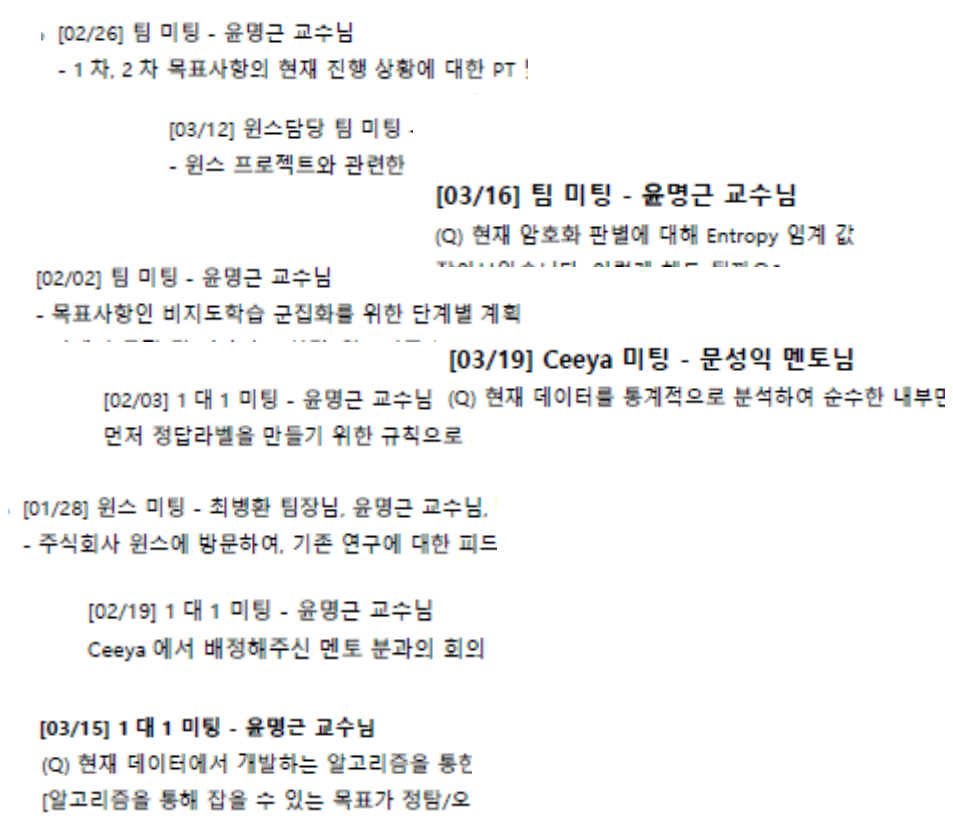
멘토링을 통한 배움

멘티의 질문 및 토론

- 클러스터링 feature / distance measure 를 어떻게 정하면 좋을까?
- 네트웍 구성에 대한 정보가 없는 상태에서 내부/외부 객체를 어떻게 구분 할 수 있을까?
- 위 질문에서 NAT 이 포함된 경우에는?
- 세션을 재구성 할 수 있나? 할 필요가 있나?
- 패킷 암호화 여부를 판별할 방법은?
- 학습된 클러스터로 Classification 을 어떻게 할 수 있을까?

이론적으로 학습된 학부생 입장에서
현업에서의 기술을 통해 좀 더 완성도 있는 결론을 낼 수 있었고, 프로젝트의 도입과 완성부분에 대해 노하우를 배울 수 있었음

멘토링을 통한 배움



주기 적인 미팅을 통해 현재 진행상황을 점검하고 다음 아이디어에 대해 피드백을 받으며
정해진 시간 내에 구현해내야 하는 기술에 대해 차질 없이 단계를 진행 할 수 있게 도와 주셨고, 더 넓은 시야에서 문제에 대한 해결방법을 어느 정도 줄여 주 실 수 있었다.

예를 들어 암호화 판별할 때는 엔트로피를 사용해 보는 것이나, 유사도 검사를 한때 기본적인 문자열 청킹 방법을 n-gram으로 하고, 클러스터링을 할 때도 알고리즘 보다는 데이터 전처리에 신경 써야 하는 부분 등 학부생 입장에서 놓치거나 오래 찾아봐야 할 기술을 빨리 알 수 있어 그에 대해 깊게 공부할 시간을 확보 할 수 있었다.

멘토링을 통한 배움(향후)

- 진행 된 프로젝트를 기술로서 밖에 선보일 때 주의해야 할 점
- 네트워크 프로토콜들의 헤더나 규격을 전수조사 해서 일반화 시킬 수 있을지
- 클러스터링 실험 과정에서 하이퍼파라미터관련 기준
- 등등