캡스톤 18 조 회의록

<table>
<tr><td>프로젝트명</td><td>O24Sec</td><td>팀 명</td><td>맬러리를 찾아서</td></tr>
<tr><td>회의 시간</td><td colspan="3">3 월 26 일 18:00 - 21:00</td></tr>
<tr><td>장소</td><td colspan="3">국민대학교 미래관 7 층 K 랩</td></tr>
<tr><td>참석자</td><td>김민송, 장우혁</td><td>서기</td><td>김민송</td></tr>
<tr><td>안건</td><td colspan="3">• 현재까지 진행 사항 확인
• 내부/외부 객체 분리 임계치 확정시키기
• 중간 발표 준비(발표자, 피피티 내용), 중간 보고서 역할 분담</td></tr>
<tr><td rowspan="2">회의 내용</td><td colspan="3">☞ 현재까지 진행 사항 확인
1. 객체 별 이벤트 분리: 임계 값만 찾으면 됨
- 임계 값에 대한 규칙만 어느 상황이든 상대적으로 사용가능 한 것 찾기

2. 암호화 패킷 분리: 코드, 수식, 임계 값 등 실험에 필요한 내용 모두 완료
- 임계 값까지 수학적 근거로 보여줄 수 있는 식을 만들어서 완전히 끝난 상태

3. 이벤트 클러스터링: AE 청킹 + 클러스터링 알고리즘 종류별로 실험 중
- 가지고 있는 이벤트 데이터 중 애플리케이션 데이터만 사용해서 어느 정도 결과를 만들어 낼 수 있을지 여러 클러스터링 알고리즘을 이용해서 실험 결과 확인 중</td></tr>
<tr><td colspan="3">☞ 내부/외부 객체 분리 임계치 확정시키기

1. 머신러닝을 통한 각 기관별 임계치 구하기
- 많은 데이터를 학습시킨 뒤 회귀를 통해 새로운 기관이 나왔을 때 임계치를 출력한다
- 데이터를 학습시켜 본 뒤 머신러닝 모델이 출력해주는 가중치 값을 이용한다.
⇨ 두개 다 결국 처음에 라벨이 있어야 모델을 학습 시킬 수 있기 때문에 중단

2. 통용될 수 있는 절대값을 임계치로 정하기
- 18 을 그대로 이용한다.
⇨ 데이터가 적은 기업이나 다른 기관이 나올 때 무조건 사용 가능 하다는 보장이 없기 때문에 중단

3. 수학적 통계를 통한 임계치 구하기
- Log_2(Event Count / IP Cardinality) => 로그에 대한 근거가 없음, 안 맞는 기관도 일부 있음
- 제일 Event Count 가 많은 순으로 나열하여 Top-k 만 이용하기 => k 에 대한 임계치를 다시 정해야 하기 때문에 중단</td></tr>
</table>

<table>
<tr><td></td><td>4. 피처의 특성을 이용한 임계치 구하기
⇨ B 클래스 대역에서 통신한 상대 B-class IP Cardinality 를 기준으로 새로 생각한 알고리즘을 통해 분리.

결과: 4 번 항목이 가장 타당하고 전체 데이터에서 적용도 잘되고 효율적이어서 4 번 규칙을 통해 내부/외부 분리 임계치를 정하기로 함.</td></tr>
<tr><td></td><td>☞ 중간 발표 준비
- 장우혁은 팀장을 맡고 있고 여러가지 문서 작업 중이니 발표자는 김민송이 하도록 함.
- 발표 대본은 내일 아침에 같이 만나서 흐름을 짜도록 함.
- 발표 피피티는 장우혁이 만들되 자료나 필요 내용 같은 걸 김민송이 보내주고 마지막 검토를 진행하도록 함.

☞ 중간 보고서 역할 분담
- 현재 해야 할 것: Github page, 중간 보고서 작성
- Github page 는 장우혁이 다뤄 보고 양식을 만들고 있으므로 그대로 진행하도록 함.
- 중간 보고서 작성은 같이 진행하면서 서로 필요할 거 같은 부분에 대한 자료를 보냄.

발표 준비는 다음 주 화요일 이내에 어느정도 완료해서 윤명근 교수님께 피드백을 받도록 함.</td></tr>
<tr><td>프로젝트 진행사항</td><td> 
</td></tr>
<tr><td>서기의 의견</td><td>계획한 타임테이블 대로 잘 흘러가고 있는 것 같아서 상당히 안정적이다. 힘든 부분에 대해서는 같이 고민해서 결과를 내는 부분에서 팀이라는 걸 다시 한번 생각해낼 수 있었고 둘 다 적극적으로 참여를 하고 있어 프로젝트 목표에 대해 잘 도달할 수 있을 거 같다는 확신이 든다.</td></tr>
</table>