[과제 계획서 피드백 받은 내용]

F1) 시스템 구조도에는 Python, AWS, DB 등과 같이 일반적인 tool을 명시하는게 아니라, 과제의 핵심 모듈이 잘 나타나도록 그림을 그리는 게 좋습니다.
A1) Elasticsearch, Logstash, Kibana, Django 등을 추가해 핵심 모듈이 잘 드러나도록 시스템 구조도 수정
F2) 시스템 구조도에는 입력과 출력이 명시되어야 하고,
A2) 입력(IPS 장비에서 나온 로그 파일)과 출력(시각화 된 웹 플랫폼) 이 잘 드러나도록 명시
F3) 각 모듈들의 이름이 간단명료하게 표현되어야 하며,
F4) 각 핵심 모듈들의 입출력을 명확하게 하여 다음 단계로 전달되는 흐름이 잘 나타나야 합니다. 즉, "시스템 구조" 그림 1장만 보면 프로젝트의 주요 내용을 쉽게 알 수 있도록 그림을 그리는 게 좋습니다.
F5) 시스템 구조도의 각 핵심 모듈들에 대한 기능 설명이 필요합니다. 각 모듈의 기능 설명과 더불어 구현 방법으로 여러가지 구현 기법 중에서 어떤 방법을 사용할지 등에 대해 각 모듈에 대한 설명이 필요합니다.
A3) Elasticsearch, Logstash, Kibana, Django 등을 추가해 핵심 모듈이 잘 드러나도록 시스템 구조도를 수정 했으며 A4) 시스템을 I/O, Web Service, DataBase, Model 등으로 구조화 하고 각 구조에 따른 모듈을 세부화해 시스템의 흐름을 명확히 알 수 있도록 수정했습니다. A5) 시스템 이해도를 높이기 위해 각 흐름에 따른 모듈들의 역할을 추가했습니다.
F6) 개발하고자 하는 시스템의 구체적인 목표를 명확하게 제시해야 함. (이상환 교수님)
A6) 개발목표(2.1)에서 각 단계별 세부목표를 추가하였습니다.

F7) 보안관제서비스에서 하고자 하는 오탐의 내용을 payload 부분 분석 feature 들이 모호합니다. 기업데이터 분석에 들어가는 내용이 무엇인지 정의를 하면 좋겠습니다. (최은미 교수님)

A7) 계획서 2.2.1.2에 데이터 Feature 필드 설명을 추가하였습니다.

F8) 페이로드를 바로 사용하면 정확도가 90%이상이라 것을 검증해야할 듯 해보임. (이재구 교수님)

A8) 이전 답변에서 라이트한 모델을 사용한다고 대답을 했는데, 제가 잘못 대답했던 부분이였습니다. 따라서 페이로드 임베딩에 대한 실험을 진행하였습니다. 페이로드 raw 값을 0~1로 정규화 시킨뒤 진행한 실험에서 임베딩 또는 인코딩이 중요하다는 점을 알았고, 이후 One-hot 인코딩으로 실험해본 결과 앞서 진행한 실험보다는 학습과 검증이 안정적으로 수렴하는것을 확인했습니다. 그러나 인코딩만으로는 구조가 무겁기 때문에 케라스의 임베딩 레이어를 만들어 진행한결과 One-hot 인코딩보다 더욱 가볍고 빠르게 수렴하는 것을 확인했습니다. 좋은 지적 감사합니다.

F9) 11페이지 개발 목표에서 계획서의 다른 부분을 읽지 않고도 개발 목표가 무엇인지 알 수 있게 목적어를 명확히 써서 다시 써 보세요.

F10) 로그데이타가 무엇을 로그 데이타인지 학습된 모델이 무슨 모델인지 정오탐 판별이 무엇의 정오탐 판별인지 분석 결과는 무엇을 분석한 것을 보여주는지 등. 결과물 목록도 구체적으로 기술해 주세요.

F11) "2.3.3절 시스템 구조"의 그림을 전체적인 시스템의 구조를 잘 나타낼 수 있도록 수정하기 바랍니다.

A9) 시스템 흐름에 따른 각 단계별 세부목표를 추가하였습니다.

A10) 어떻게 생성된 로그데이터인지를 기술하고 2.2.1.2 에 로그데이터 피처에 대한 구체적인 설명도 추가하였습니다.

A11) 전체적인 흐름을 구체화하고 시스템 이해도를 높이기 위해 세부적인 모듈명을 기술하였습니다.