ROAT

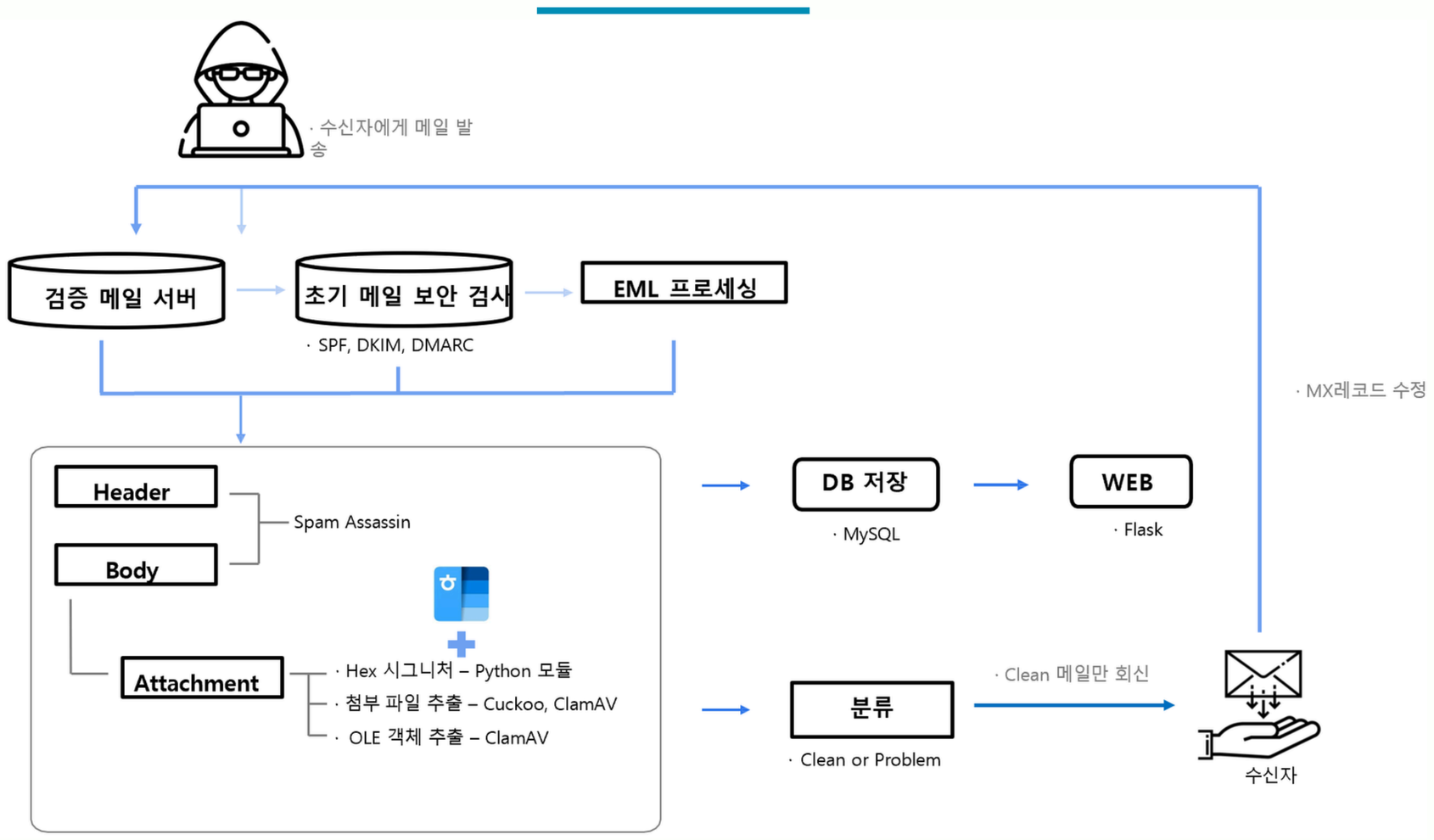
악성 문서 중심의 이메일 보안 솔루션 개발

팀원 구성 팀장 이경재, 팀원 전유병, 김근수, 김정욱, 송지현

개요

- 이 연구는 이메일을 통한 악성코드 유입 중 특히 HWP/HWPX 문서를 이용한 공격에 대응하기 위해, 문서 내부 구조를 정적으로 분석하고 SpamAssassin·ClamAV·Cuckoo 등 기존 엔진과 연동한 자동화된 이메일 보안 분석 파이프라인을 구축하는 것을 목표로 한다.
  이를 통해 악성 행위 탐지 정확도와 메일 보안 운영 효율을 향상시켰다.

구상도



기대효과

- 이메일 첨부 HWP/HWPX 문서 내 숨겨진 악성 행위를 조기에 탐지할 수 있으며, 정적·동적 분석을 결합한 자동화 파이프라인으로 보안 대응 속도와 정확도를 향상시킨다. 또한 탐지 결과의 시각화 및 데이터베이스화를 통해 운영자가 보안 현황을 직관적으로 파악할 수 있다.