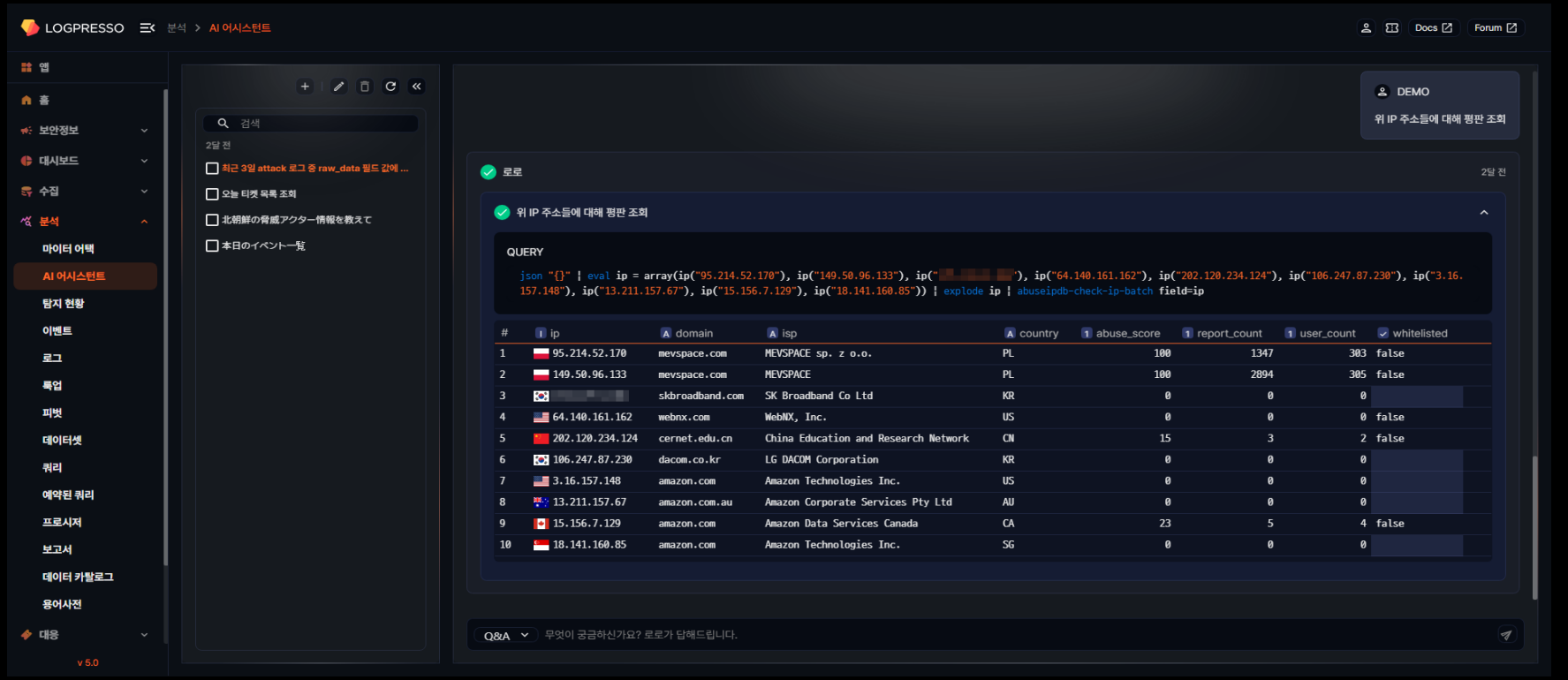
AI가 바꾸는 XDR의 풍경

OWASP Seoul
Chapter Night@SF

LOGPRESSO

XDR 운영을 위한 AI 어시스턴트

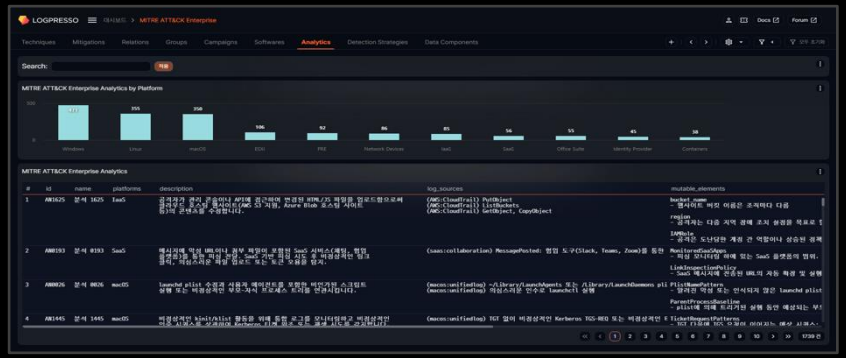
우리는 보안 업무의 전문가가 되어야 하지, XDR "제품"의 전문가가 될 필요가 없습니다



AI는 XDR의 복잡성을 대신합니다

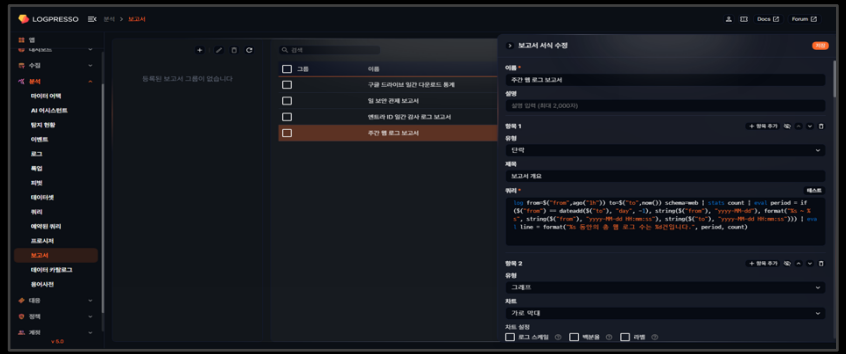
우리가 업무를 정의하면 보고서, 탐지 룰, 파서, 대시보드까지 AI가 알아서 만듭니다

<대시보드 자동 생성>



<탐지 규칙 자동 생성>

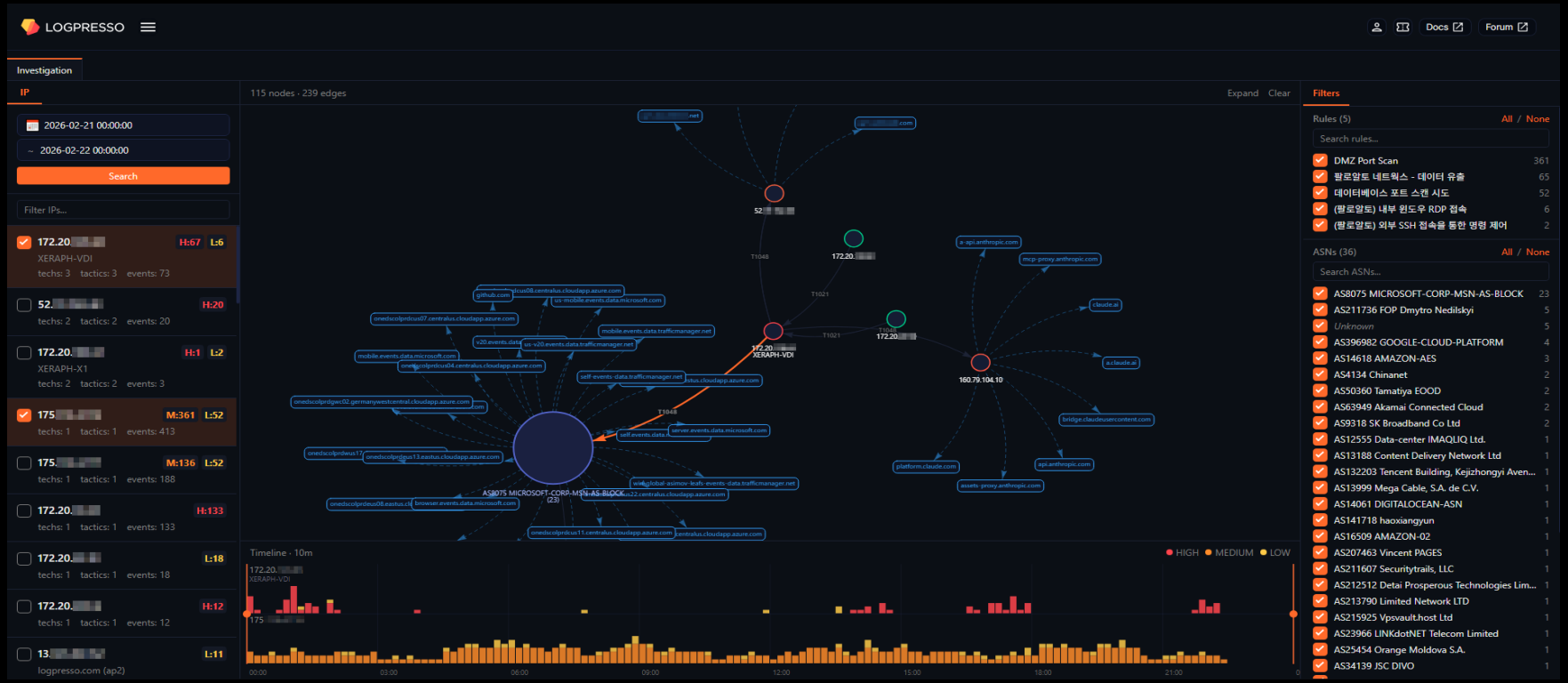
<파서 자동 생성>



<보고서 자동 생성>

AI로 고객의 요구사항에 빠르게 대응합니다

전통적인 개발 사이클이 아니라, 빠르게 개발하고 고객의 피드백을 수용합니다



생성형 AI를 활용한 다양한 기능을 제공합니다

탐지 이벤트의 맥락을 분석하고, 맥락을 고려한 리포트를 생성합니다

자산, 계정별 TTP 탐지 이벤트 조회

↓

공격 전술(Tactic) 전이 상태 판단

↓

공격 전이도 및 연결 그래프 생성

↓

티켓 제목 및 요약문 생성

↓

증적 포함한 티켓 생성

LOGPRESSO

감사합니다