    - 예를 들어 Microsoft는 “제품 카탈로그 정보를 모두 학습해 고객 질문에 상세히 답변”하는 에이전트를 언급했다.

- **직원 에이전트**: 조직 내부 직원을 지원하는 역할로,
    - 예를 들면 영업사원의 목표 달성을 돕기 위해 “영업 리드 생성” 같은 업무를 자동화하는 에이전트가 해당한다.

- **데이터 에이전트**: 회사의 내부 데이터를 수집·전처리·분석하여 RAG 등에 활용 가능한 지식을 제공한다.
    - 예를 들어 사내 문서나 DB를 정기적으로 인덱싱해 임베딩하고, 엔티티 추출·정합성 검증 등을 수행한다.

- **시큐리티 에이전트**: AI 시스템 전체의 보안·권한 관리를 담당한다.
    - 사용자 인증, 문서 접근 제어, 활동 로그 모니터링 등을 통해 시스템 안전성을 강화한다.

13. Agentic RAG란 무엇인가? LLM과 유연하게 연계되는 방식은?

Agentic RAG는 RAG 파이프라인에 AI 에이전트를 도입한 개념으로, 에이전트가 여러 검색/도구를 유연히 사용하도록 확장한 방식이다.

즉, 단순히 벡터 검색만 하는 것이 아니라 LLM 기반 에이전트가 웹 검색·계산기·API 호출 등 여러 도구를 필요에 따라 활용해 정보를 조회한다.

에이전트는 쿼리 내용을 분석해 최적의 검색 수단을 선택하고, 필요 시 여러 단계를 거쳐 정보를 보충한다.

이렇게 하면 한 번에 하나의 지식원만 참조하는 기존 RAG의 한계를 넘어 보다 정교하고 유연한 정보 검색·통합이 가능하다.

14. AI 컨설팅은 누가 수행하며, 어떤 내용이 포함되는가?

→ 이부분은 별도 설명 필요

15. 효과 중 환경 보안 강화의 의미는?

‘환경 보안 강화’는 AI 솔루션이 구축되는 시스템 환경의 보안 수준을 높이는 것을 의미한다.

예를 들어 AI를 온프레미스 환경에 배치하면 데이터와 시스템을 외부 인터넷으로부터 완전히 격리할 수 있어 보안성이 극대화된다.

이렇게 하면 데이터 유출 위험을 줄이고, 네트워크 접근 제어와 침입 탐지 등의 보안 정책을 강화하여 전반적인 시스템 안전성을 높일 수 있다.