LEVEL 3 · 심화 | AI 에이전트 | 기업·단체 출강교육

AI 에이전트 실무 구축

코드 템플릿으로 만드는 업무 에이전트 — 로우코드 심화

2일	16시간	8개	23개
교육 일수	총 교육 시간	단원 구성	실습 과제

1 과정 개요

목표를 주면 스스로 도구를 골라 여러 단계를 수행하는 AI 에이전트를 설계부터 운영 준비까지 직접 만드는 2일 실습 과정입니다. 1일차에는 에이전트가 맞는 업무를 가려 설계서를 쓰고, 함수 도구와 MCP(Model Context Protocol) 서버를 연결한 에이전트를 완성합니다. 2일차에는 멀티스텝·멀티 에이전트 구성, 입력·출력 가드레일, 되돌리기 어려운 작업 전 사람 승인 단계, 평가 세트와 실행 추적(트레이싱)을 다루고 참가자 조직 업무로 에이전트를 완성해 시연합니다. 강사가 제공하는 코드 템플릿과 AI 코딩 도우미를 함께 써서 코딩 경험이 적어도 따라올 수 있게 진행합니다.

교육 기간	2일 · 16시간
교육 수준	LEVEL 3 · 심화
교육 대상	실무 담당자·도입 기획자(로우코드)
교육 형태	집체(출강) · 실습 중심(약 73%) · 1인 1노트북 · 설계서 검토·토론 · 참가자 업무 과제 프로젝트
활용 도구	에이전트 프레임워크 (OpenAI Agents SDK 기반 강사 템플릿 — 도구·핸드오프·가드레일·사람 승인·트레이싱) MCP 서버·MCP Inspector · MCP 지원 AI 앱(Claude Desktop 등) LLM API (기관 정책에 맞는 서비스) · AI 코딩 도우미 (Claude Code·Cursor 등)
권장 인원	1인 1노트북 실습과 설계서 코칭이 가능한 소규모~중규모 운영 권장 (협의)

이런 분께 적합합니다

- 리서치→정리→보고·발송처럼 여러 단계로 이뤄진 업무를 AI에게 맡기려는 실무 담당자·도입 기획자에게 맞춘 과정입니다.
- 노코드 자동화(n8n·Make 등)나 프롬프트 작성 경험이 있으면 좋습니다. Python·Node.js를 설치해 강사 코드 템플릿을 고쳐 쓰는 로우코드 과정이며, AI 코딩 도우미의 도움을 받아 진행하므로 개발자가 아니어도 따라올 수 있습니다.
- 에이전트로 만들고 싶은 업무 1건과 그 업무에 쓰는 시스템·자료(시트·문서·메일 등)를 정리해 오시면 종합 프로젝트 과제가 됩니다.

2 교육 목표

1. 에이전트 설계와 도구 연결

- 정해진 순서로 충분한 업무(자동화·워크플로우)와 단계 수를 미리 정할 수 없는 업무(에이전트)를 구분해 과제를 고릅니다.
- 목표·입력·도구·해도 되는 일과 안 되는 일·사람 확인 지점·완료 기준을 담은 에이전트 설계서를 작성합니다.
- 이름·설명·입력 형식이 명확한 함수 도구를 만들고, MCP 서버를 직접 만들어 에이전트와 MCP 지원 앱에 연결합니다.

2. 멀티스텝과 통제

- 체이닝·라우팅·병렬화·오케스트레이터-워커·평가자-개선자 패턴 중 업무에 맞는 구성을 골라 구현하고 비용·품질을 비교합니다.
- 입력·출력 가드레일, 읽기/쓰기 도구 분리, 최대 반복 횟수, 메일 발송·등록 전 사람 승인으로 과도한 권한 위임을 막습니다.
- 문서·웹 페이지에 숨긴 지시문으로 에이전트를 직접 공격해 보고 방어가 작동하는지 확인합니다.

3. 평가와 운영

- 기대 결과·허용 도구·금지 행동을 적은 평가 시나리오로 성공률과 실패 유형을 기록합니다.
- 실행 추적(트레이싱)으로 에이전트가 어떤 도구를 왜 불렀는지 확인하고 지시문·도구 설명을 고쳐 재평가합니다.
- 로그 보관·비용 상한·실패 시 사람에게 넘기기·버전 관리를 담은 도입 계획서를 작성합니다.

3 세부 시간표 (2일 · 16시간)

1일차	8시간
에이전트가 맞는 업무 고르기와 설계서 작성 2시간	• 워크플로우와 에이전트의 차이: 정해진 경로로 충분한 업무 vs 단계 수를 예측할 수 없어 AI가 스스로 판단해야 하는 업무 • 에이전트 구성 요소: 지시문·모델·도구·세션 메모리·종료 조건(최대 반복), 단순한 구성부터 시작하는 원칙 실습 내 업무 1건으로 에이전트 설계서 작성 — 목표, 입력, 사용할 도구, 해도 되는 일/안 되는 일, 사람 확인 지점, 완료 기준 실습 2인 1조 설계서 상호 검토 — 「에이전트 대신 단순 자동화로 충분한가」 판정 포함 • 결과물: 에이전트 설계서 1부

첫 에이전트 실행과 함수 도구 만들기 2시간	• 실습 환경 준비: 강사 템플릿 실행, API 키를 코드가 아닌 환경 변수로 넣기 실습 지시문만 있는 에이전트 실행 → 함수 도구 1개(사내 시트·목록 조회) 추가 후 도구 호출 과정 관찰 • 도구 설계 원칙: 명확한 이름·설명·입력 형식, 도구끼리 역할 겹치지 않기, 잘못 쓰기 어려운 입력 형식 실습 트레이싱 화면에서 모델이 어떤 도구를 어떤 값으로 불렀는지 단계별 확인 실습 AI 코딩 도우미에게 요청해 도구 함수 2개 추가·수정하고 직접 실행으로 검증
MCP로 외부 도구 연결하기 3시간	• MCP 구조: 호스트·클라이언트·서버, 서버가 제공하는 도구·리소스·프롬프트, 로컬(stdio)과 원격(Streamable HTTP) 연결 실습 공개 참조 MCP 서버(파일 시스템 등)를 MCP Inspector로 열어 도구 목록 조회·도구 호출 결과 확인 실습 템플릿으로 업무용 MCP 서버 만들기 — 조회 도구 1개·등록 도구 1개, 도구 설명과 입력 형식 작성 실습 만든 MCP 서버를 에이전트 코드와 MCP 지원 AI 앱(Claude Desktop 등)에 각각 연결해 동작 비교 • MCP 보안 기본: 출처를 확인할 수 없는 서버 설치 금지, 최소 권한 토큰, 원격 서버 인증(OAuth 권장) • 결과물: 함수 도구 + MCP 서버가 연결된 단일 에이전트
1일차 시험 운행과 개선 1시간	실습 정상 요청·모호한 요청·도구 오류 상황을 각 3건씩 실행하고 실패 사례 기록 실습 지시문과 도구 설명을 고쳐 같은 9건을 다시 실행하고 전후 비교 실습 트레이스에서 도구 호출 횟수·소요 시간을 확인해 불필요한 반복 호출 찾기 • 소그룹 공유: 에이전트가 엉뚱한 도구를 고르거나 멈추지 않은 사례와 원인

2일차 — 8시간

멀티스텝·멀티 에이전트 구성 2시간	• 업무 패턴 고르기: 프롬프트 체이닝·라우팅·병렬화·오케스트레이터-워커·평가자-개선자, 복잡도를 늘릴 근거가 있을 때만 확장 실습 자료 조사 → 분석 → 보고서 초안 흐름을 역할별 에이전트로 나누고 핸드오프로 연결 실습 평가자 에이전트가 기준표로 보고서를 검토해 수정 요청하는 루프 만들기 — 최대 반복 횟수 제한 실습 단일 에이전트 구성과 분할 구성을 같은 과제로 실행해 품질·소요 시간·토큰 사용량 비교

가드레일과 사람 승인 단계 2시간	• OWASP LLM Top 10으로 보는 에이전트 위험: 프롬프트 인젝션(LLM01), 부적절한 출력 처리(LLM05), 과도한 권한 위임(LLM06), 무제한 소비(LLM10) 실습 입력 가드레일(업무 범위 밖·개인정보 포함 요청 차단)과 출력 가드레일(민감정보·형식 위반 검사) 붙이기 실습 메일 발송·데이터 등록 도구에 승인 필요 설정 → 실행 중 멈춤 → 승인/거절 후 이어서 실행 실습 도구 권한 줄이기 — 읽기 도구와 쓰기 도구 분리, 금액·건수 한도, 호출 횟수 상한 실습 문서·웹 페이지에 숨긴 지시문으로 공격해 보고 가드레일·승인 단계가 막는지 확인
평가와 운영 준비 2시간	• 평가 시나리오 설계: 업무 사례 15~20건마다 기대 결과·허용 도구·금지 행동 명시 실습 평가 시나리오 일괄 실행 → 성공률·도구 오선택·승인 요청 발생 건수 기록, 트레이스로 실패 원인 확인 실습 지시문·도구 변경 후 같은 시나리오 재실행으로 다른 사례가 나빠지지 않았는지 회귀 확인 • 운영 설계: 실행 로그 보관, 비용 상한, 실패 시 사람에게 넘기는 기준, 지시문·도구 버전 관리 • 결과물: 평가 결과표와 운영 체크리스트
종합 프로젝트: 우리 조직 업무 에이전트 완성·시연·피드백 2시간	실습 1일차 설계서의 조직 과제로 에이전트 완성 — 함수/MCP 도구, 멀티스텝, 가드레일, 사람 승인 단계 포함 실습 평가 시나리오 결과와 남은 위험 목록 정리 실습 도입 계획서 1장 — 사용자·권한·운영 담당·확대 조건·중단 기준 • 시연·피드백: 정상 사례와 위험 사례를 함께 시연하고 강사·동료 피드백으로 보완 목록 확정

4 교육 후 손에 남는 산출물

- ✓ **우리 조직 업무로 완성한 AI 에이전트 1개(도구·가드레일·사람 승인 단계 포함)**
- ✓ **직접 만든 업무용 MCP 서버 1개**
- ✓ **에이전트 설계서와 평가 시나리오·결과표**
- ✓ **운영 체크리스트와 도입 계획서**

5 수료 후 이렇게 달라집니다

항목	수강 전	수강 후
작업 방식	단계마다 사람이 지시하고 복사	목표를 주면 에이전트가 도구를 골라 수행
도구 연결	AI 앱마다 따로 연동	MCP 서버 하나로 여러 앱에 연결
위험 관리	AI가 무엇을 할지 예측 어려움	가드레일·권한 한도·사람 승인으로 통제
품질 확인	몇 번 써 보고 판단	평가 시나리오와 실행 추적으로 반복 측정

6 운영 안내

참가자 준비사항

- 노트북 지참 (필수, 프로그램 설치 권한 필요 — 사내 PC는 사전 확인)
- LLM API 계정·키 (사전 안내에 따라 준비, 기관 정책상 사용 가능한 서비스 확인)
- 실습 환경 설치 (사전 안내: Python·Node.js·AI 코딩 도우미, 설치 점검 체크리스트 제공)
- 에이전트로 만들 업무 1건과 연결할 자료·시스템 목록 (개인정보 가린 샘플 데이터)

교육장 요건

- 프로젝터 또는 대형 스크린
- 고속 인터넷(Wi-Fi) — 외부 AI API·패키지 설치 접속이 사내 방화벽에서 허용되는지 사전 확인
- 2인 1조 설계서 검토·토론이 가능한 좌석 배치

맞춤 구성 옵션

- 주 1일씩 나눠 2회 운영 (사이 기간에 설계서 과제를 현업 자료로 보완)
- 사내 시스템·문서로 실습 — 사내 API를 MCP 서버로 감싸는 과제 (보안 승인 범위 내, 협의)
- 선행 과정 연계: 노코드 AI 자동화 (n8n·Make) 과정과 패키지 운영
- 사내 보안 정책에 맞춘 가드레일·권한 설계 심화 (협의)
- 사후 1회 기술 점검 세션 (협의)

설치 문제로 실습 시간이 줄지 않도록 교육 전 설치 점검을 꼭 진행해 주세요. 사내 PC에 설치가 어려우면 클라우드 개발 환경 사용을 협의합니다.

nuguna

기업·단체 출강교육 문의

전화 010-6395-3043 · 카카오톡 @nuguna · nugunapass@gmail.com
www.nugunapass.com/onsite — 인원·대상·희망 일정을 알려 주시면 맞춤 커리큘럼과 견적을 제안드립니다.