CHRISCOMPANY
architecting in Integrity

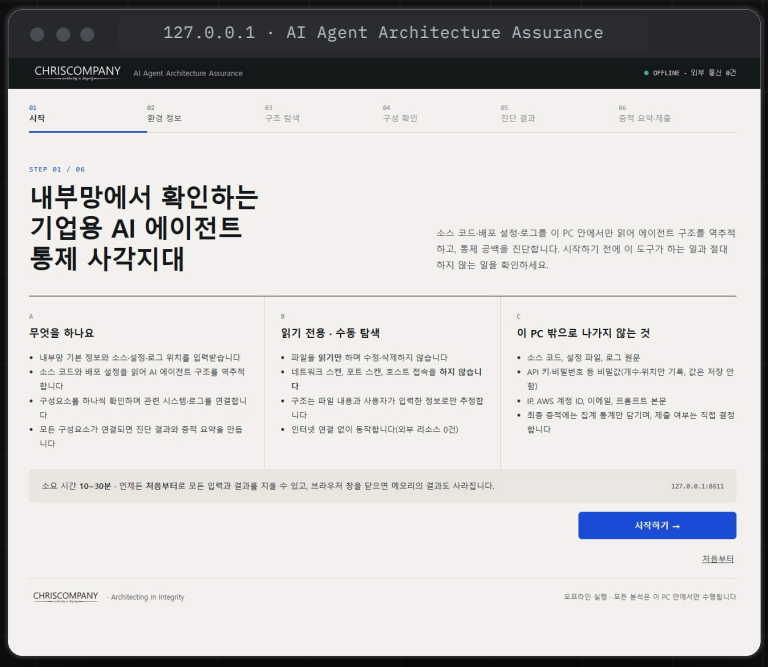
● OFFLINE · 외부 통신 0건
SERVICE GUIDE · 2026

ENTERPRISE AI AGENT CONTROL DIAGNOSTICS

AI Agent Architecture Assurance

기업용 AI 에이전트 아키텍처 진단 프로그램 & Architecture Review 서비스 안내서

기업용 AI 에이전트, 보안을 넘어 통제권을 잃지 마십시오.



RUNS ON

귀사 PC·내부망

MODE

읽기 전용·수동 탐색

OUTPUT

마스킹된 증적

(주)크리스컴퍼니 CHRISCOMPANY
Architecting in Integrity · chris.company

WHY NOW

기업용 AI 에이전트,
보안을 넘어 통제권을 잃지 마십시오.

AI 에이전트는 사람 대신 권한을 위임받아 내부 DB를 조회하고, 외부 LLM을 호출하고, 도구를 실행합니다. 도입 속도가 빨라질수록 “누가 무엇을 할 수 있고, 데이터가 어디로 가는가”는 설계 문서가 아니라 코드와 설정, 로그 속에 흩어집니다.

DELEGATED AUTHORITY

위임된 권한

에이전트 역할에 붙은 IAM 와일드카드·관리자 정책, DB 관리자 계정 접속처럼 업무에 필요한 범위를 넘는 권한이 조용히 쌓입니다.

EXECUTION PATH

실행 경로

사람의 승인(HITL) 없이 외부 LLM을 호출하거나, 에이전트가 내부 DB에 직접 접근하는 경로, 선언되지 않은 통신 대상이 생깁니다.

DATA FLOW

데이터 흐름

마스킹 근거 없이 외부 LLM으로 나가는 데이터, 로그에 남는 개인정보와 프롬프트 원문, 코드에 하드코딩된 비밀값.

감독·감사는 설명이 아니라 증적을 요구합니다.

감독기관과 감사인은 AI 에이전트가 어떤 권한으로, 어떤 경로를 거쳐, 어떤 데이터를 다뤘는지 묻습니다. 답하려면 실제 코드·설정·로그에 근거한 구조도와, 외부에 내보내도 안전한 형태로 정리된 증적이 필요합니다. 그러나 그 근거가 되는 소스 코드와 로그는 대개 외부로 반출할 수 없습니다.

WHAT WE OFFER

반출할 수 없는 자료는 귀사 안에서 분석하고, 마스킹된 증적만으로 아키텍처를 검토합니다.

귀사 내부에서 실행

AI Agent Architecture Assurance 진단 프로그램

귀사 PC·내부망에서 오프라인으로 실행되는 읽기 전용·수동(passive) 진단 프로그램. 코드·설정·로그에서 에이전트 구조를 역추적하고, 담당자가 확인한 구조를 진단해 마스킹된 증적 패키지를 만듭니다.

크리스컴퍼니가 수행

Architecture Review (유료)

제출된 증적 요약을 크리스컴퍼니가 검토해, 영역별 글로벌 선도 사례 기준 비교와 격차, 우선순위가 정해진 개선 로드맵을 담은 Architecture Review 보고서를 전달합니다.

HOW IT WORKS

코드·설정·로그에서 구조를 역추적하고, 담당자가 확인한 구조만 진단합니다.

설치가 필요 없는 Windows 실행 파일 하나로 동작합니다. 실행하면 이 PC 안(127.0.0.1)에서만 열리는 브라우저 화면이 뜨고, 6단계 안내에 따라 진행합니다.

설치 0	127.0.0.1	0건	Read-only
실행 파일 하나	**이 PC 안에서만**	**외부 통신**	**읽기 전용·수동 탐색**
더블클릭하면 콘솔 창과 기본 브라우저가 열립니다.	서버는 로컬 주소에만 열리고, 창을 닫으면 종료됩니다.	네트워크 코드·웹 폰트·CDN 없음, 사용 통계 전송 끔.	파일 수정·삭제 없음. 네트워크·포트 스캔, 호스트 접속 없음.

진행 6단계

4단계의 진행 조건을 통과해야 진단 결과가 열립니다.

01	02	03	04	05	06
시작	**환경 정보**	**구조 탐색**	**구성 확인**	**진단 결과**	**증적 요약·제출**
프로그램이 하는 일과 절대 하지 않는 일을 먼저 확인합니다.	기관·시스템, 망 구역, 허용된 외부 통신 대상, 분석할 폴더.	소스·설정 파일을 읽기 전용으로 정적 분석합니다.	구성요소를 하나씩 확인하고 로그·설정을 연결합니다.	5개 영역 점수, 발견 항목과 권고, 로그 토폴로지.	미리보기와 확인 후 증적 zip을 저장합니다.

이런 조직에 맞습니다

망분리·폐쇄망 환경
인터넷이 끊긴 PC에서도 그대로 동작합니다.

소스·로그 반출이 어려운 조직
원문은 귀사 안에 두고 집계·마스킹된 통계만 제출합니다.

감독·감사 대응이 필요한 조직
코드·설정·로그에 근거한 구조도와 증적을 남깁니다.

STEP 02 – 03

알려 주신 위치의 파일만, 읽기만 합니다.

STEP 02

환경 정보

진단 대상과 분석할 자료의 위치를 입력합니다.

- 대상 기관·조직명과 시스템명
- 내부망 구역(업무망·DMZ·설비망 등)별 CIDR 대역·호스트·도메인
- 허용된 외부 통신 대상 (예: api.openai.com)
- 에이전트 소스 코드, 배포·설정 파일, 로그 폴더 경로 (폴더 찾아보기 지원)

수동(passive) 탐색만 합니다. 입력한 대역·호스트로 접속하거나 스캔하지 않으며, 코드·로그에서 찾은 통신 대상이 허용 범위 안인지 비교하는 데만 씁니다.

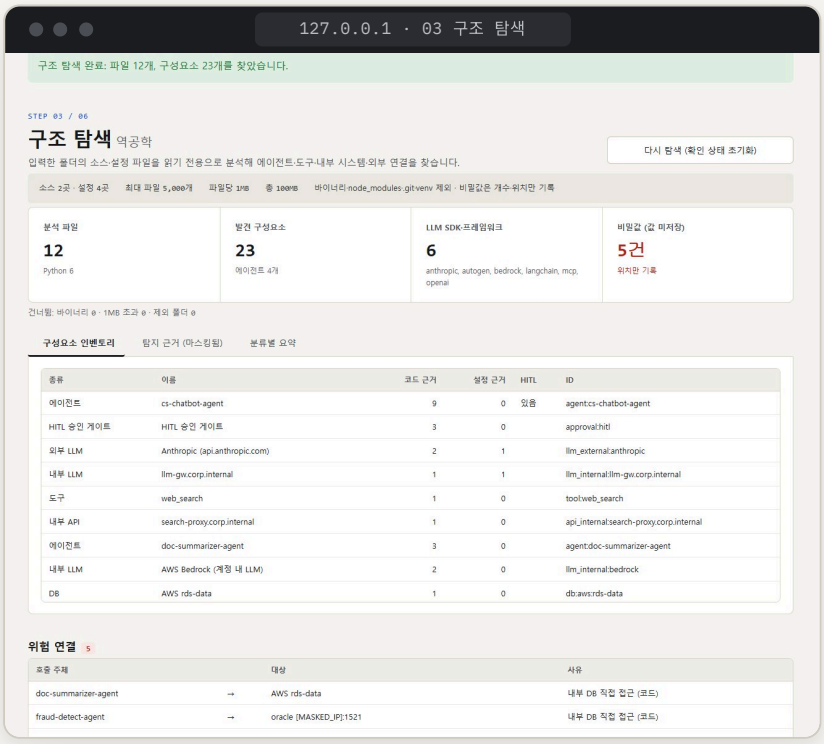
STEP 03

구조 탐색

입력한 폴더의 소스·설정 파일을 정적 분석해 다음을 찾습니다.

- 언어·진입점, LLM SDK (openai·azure openai·anthropic·google·bedrock)
- 에이전트 프레임워크 (langchain·llamaindex·autogen·crewai·semantic-kernel·mcp)와 에이전트 도구
- 외부·내부 통신 대상, DB 드라이버·접속 문자열(계정·비밀번호 마스킹), 큐, S3·boto3
- HITL 승인 훅, 마스킹·DLP, 로깅, 셸 실행, IAM 와일드카드

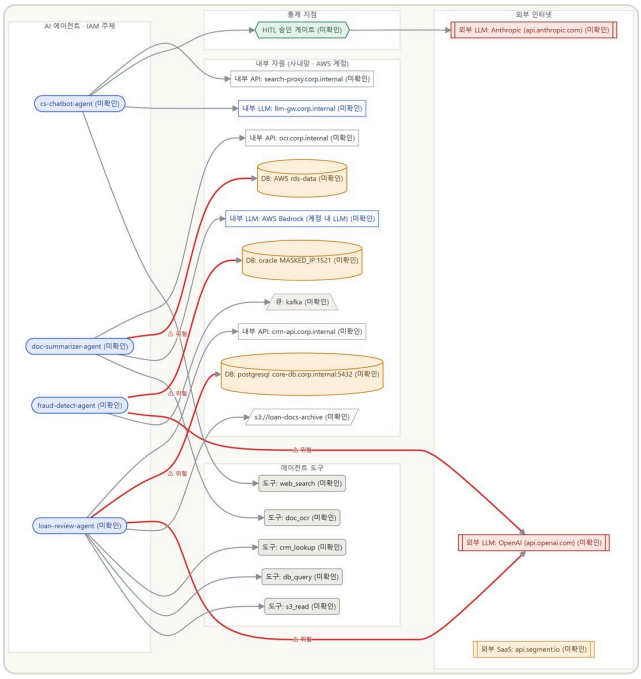
비밀값은 값을 남기지 않습니다. API 키·비밀번호·토큰은 종류와 위치(파일:줄)만 기록합니다.



STEP 04 · CONFIRM

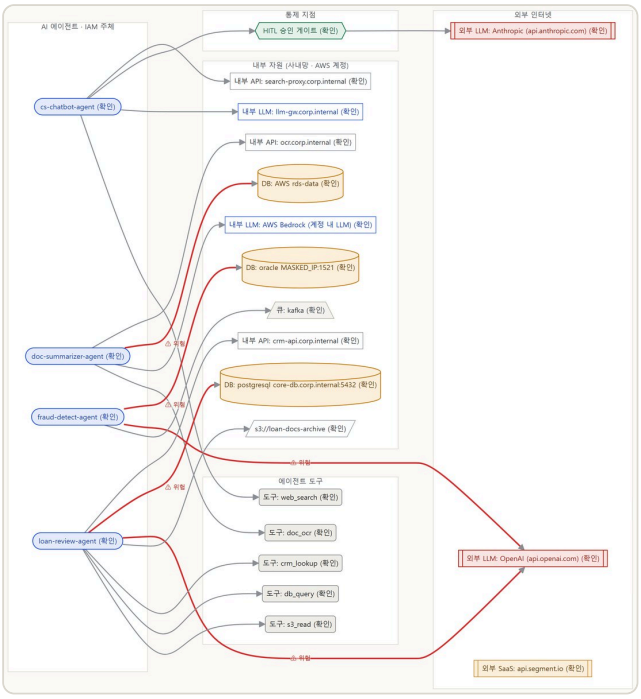
코드에서 역추적한 구조를,
담당자가 하나씩 확인해 완성합니다.

FIG. A 코드에서 역추적한 구조 미확인



3단계 직후. 소스·설정에서 찾은 구성요소가 모두 **(미확인)** 상태로 표시됩니다.

FIG. B 담당자 확인 완료 확인

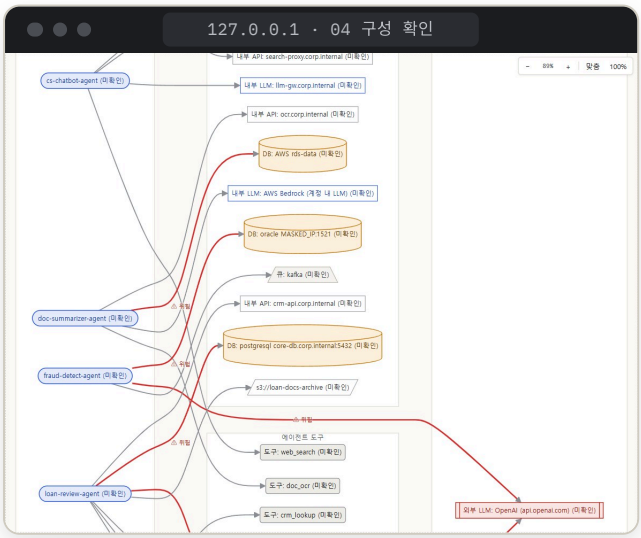


모든 구성요소에 근거가 연결되어 **(확인)**으로 바뀐 구조. 이 구조가 진단의 기준이 됩니다.

빨간 굵은 선 = 위험 연결. 에이전트의 내부 DB 직접 접근, HITL 승인 게이트를 거치지 않는 외부 LLM 호출.

회색 선 = 코드에서 찾은 호출 관계 · 영역 — AI 에이전트 · IAM 주체 / 통제 지점 / 내부 자원 / 에이전트 도구 / 외부 인터넷

노드 괄호 = 확인 상태. (미확인) · (확인) · (수정) · (해당 없음)



프로그램 안의 구성도. 오른쪽 위 도구 막대로 확대·축소합니다.

확인하는 방법

- 구성요소마다 **확인** · **수정**(이름 등을 고친 뒤 확인) · **해당 없음**(사유 필수)을 고릅니다.
- 로그·설정 파일을 연결해 근거를 붙입니다.
- 스캔이 놓친 구성요소는 **추가**하고, 같은 대상은 **합치기**로 정리합니다.
- − / + / 맞춤 / 100% 버튼과 Ctrl+휠로 확대·축소하고, 끌어서 이동합니다.

진행 조건. 모든 구성요소가 확인(근거 1개 이상) 또는 해당 없음(사유)이 되어야 5단계가 열립니다.

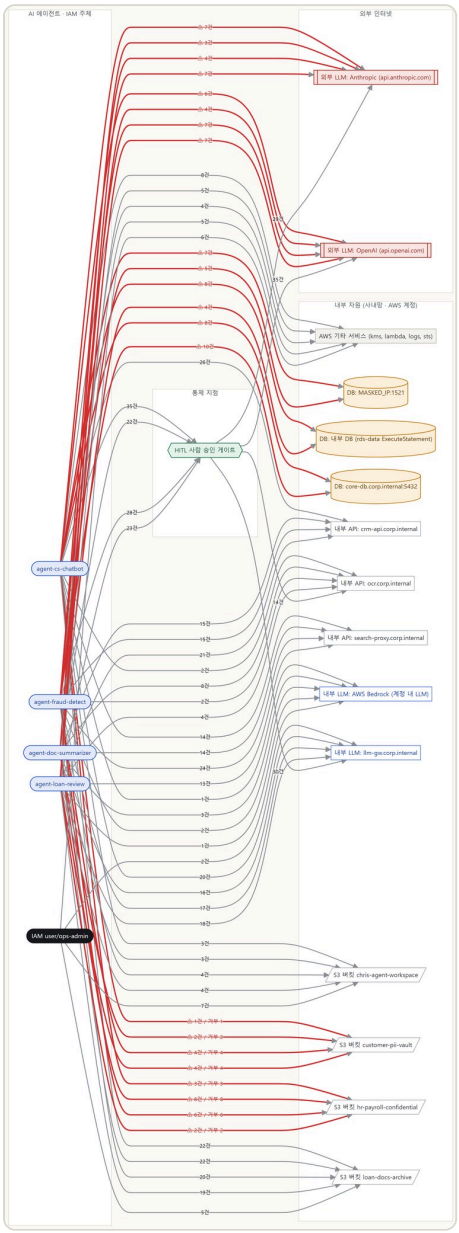
구성도는 프로그램이 실제로 만든 출력입니다. 샘플 환경 예시 — 가상의 기관 '데모은행'과 가상 데이터를 사용했습니다.

LOG-BASED TOPOLOGY

로그로 다시 그린 실제 통신은 설계도와 다를 수 있습니다.

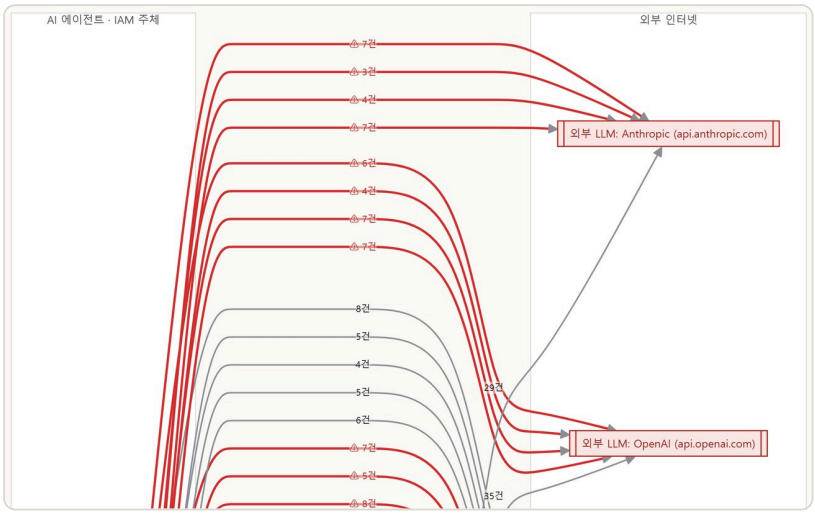
연결한 CloudTrail·API Gateway 로그를 마스킹한 뒤 호출 주체와 대상을 집계해, 실제로 오간 통신을 구성도로 다시 그립니다. 선마다 로그에 기록된 호출 건수가 붙습니다.

FIG. C 로그 기반 전체 통신



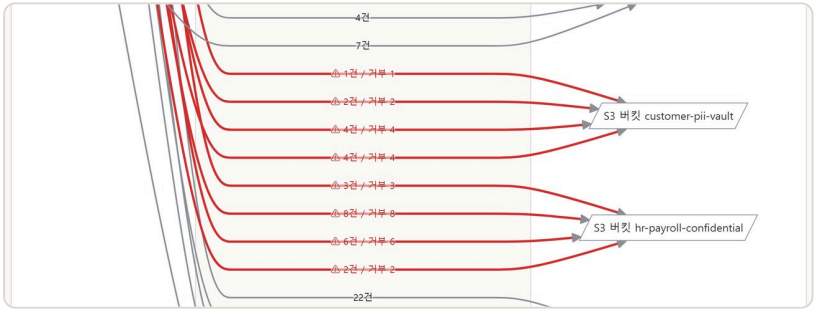
전체 모습. 왼쪽 에이전트·IAM 주체에서 뻗는 빨간 선 다발이 위험 연결입니다.

C-1 승인 없는 외부 LLM 호출 위험



HITL 승인 게이트를 거치지 않고 외부 LLM(Anthropic·OpenAI)으로 간 호출. ⚠ **N건**은 로그상 호출 수입니다.

C-2 권한 밖 S3 버킷 접근 시도 위험



N건 / 거부 N — 권한 거부(AccessDenied·403)된 접근. 에이전트가 권한 밖 자원을 탐색한 신호입니다.

로그상 위험 연결 — 무승인 외부 LLM 호출, 내부 DB 직접 접근, 권한 거부(403) 접근.

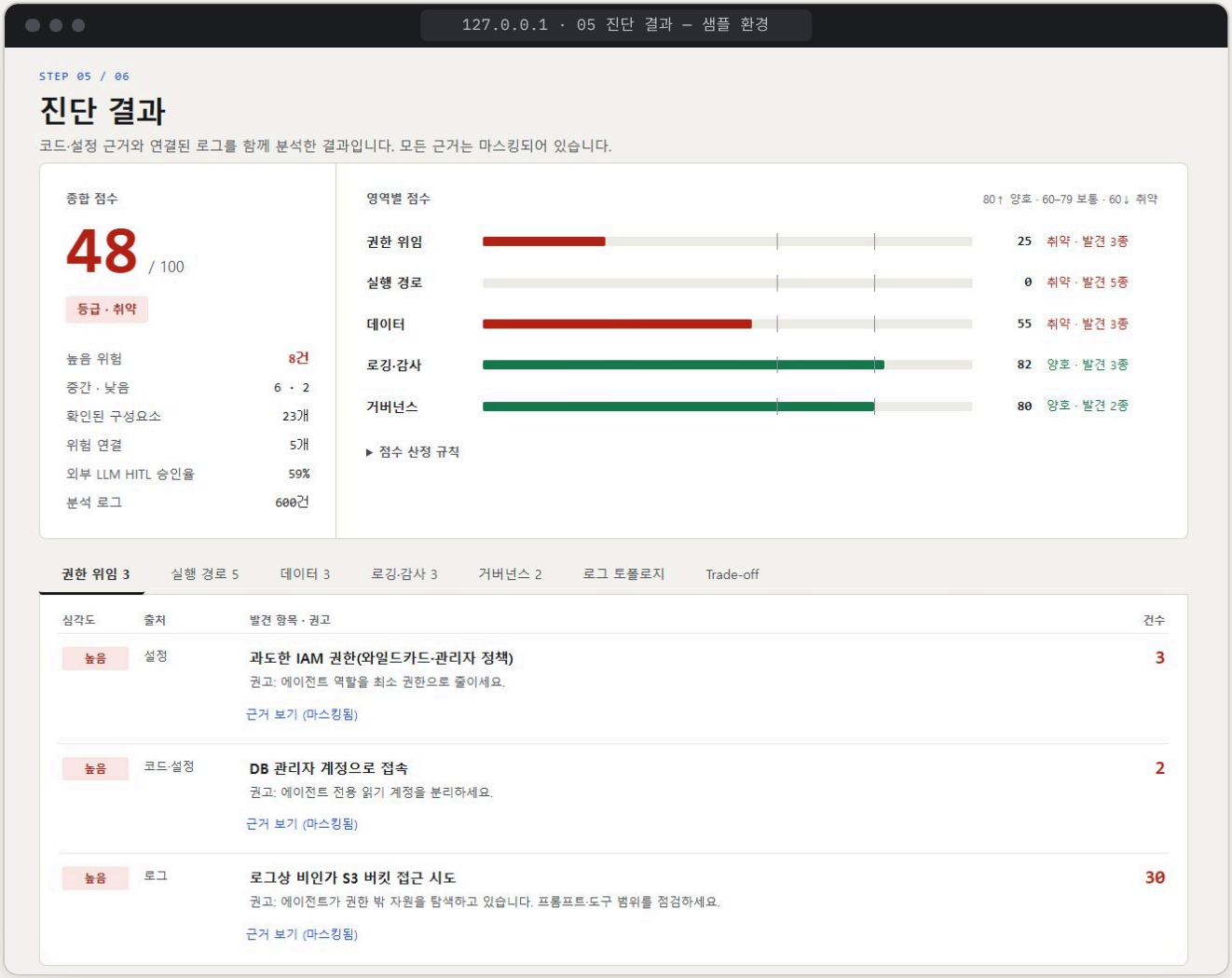
사람 계정도 IAM 주체로 나타납니다 (예: IAM user/ops-admin).

샘플 환경 예시 — 가상의 기관 '데모은행'과 프로그램에 동봉된 가상 로그로 만든 실제 출력입니다. IP는 MASKED_IP로 마스킹되어 있습니다.

STEP 05 · DIAGNOSIS

5개 통제 영역을 근거와 함께 점수로 보여 줍니다.

확인된 구조의 코드·설정 근거와 연결된 로그를 합쳐 진단합니다. 발견 항목마다 출처(코드·설정·로그), 권고, 마스킹된 근거가 함께 표시됩니다.



진단 영역과 주요 판정

영역	주요 판정
권한 위임	IAM 와일드카드·관리자 정책, DB 관리자 계정, 비인가 S3 접근, 도구 과다 노출
실행 경로	승인 없는 외부 LLM 호출, 에이전트의 내부 DB 직접 접근, 셸 실행, 선언되지 않은 통신 대상
데이터	하드코딩된 비밀값, 외부 LLM 전송 전 마스킹 근거 없음, 로그의 개인정보·프롬프트 원문
로깅·감사	로그 근거 없는 구성요소, CloudTrail·호출 로그 미연결, 로깅 코드 없는 에이전트, 5xx 비율
거버넌스	외부 LLM 승인율 90% 미만, 승인 게이트 없는 에이전트, 문서화 누락, 망 구역 미선언

점수 산정 규칙

영역 점수 = 100 − 감점 합계 (최저 0). 같은 종류의 발견은 한 번만 감점합니다. 종합 점수는 5개 영역의 평균입니다.

높음	중간	낮음
−25	−10	−4

이 밖에 로그 토폴로지와, HITL 승인율 대비 승인·미승인 호출의 지연 중앙값(보안과 자동화 속도의 trade-off)을 보여 줍니다.

STEP 06 · EVIDENCE

집계·마스킹된 통계만으로 증적을 만들고, 저장 전에 전부 보여 드립니다.

evidence_summary.csv

웹사이트 제출 파일 · 4MB 이하

영역 점수, 발견 항목 종류별 건수·심각도, 구성요소 상태, HITL 승인율, 로그 집계 통계, 마스킹 건수.

evidence_summary.json

같은 내용 + 익명화 구성 그래프

구성요소는 `agent-1`, `db-1`, `external-llm:openai`처럼 익명화됩니다.

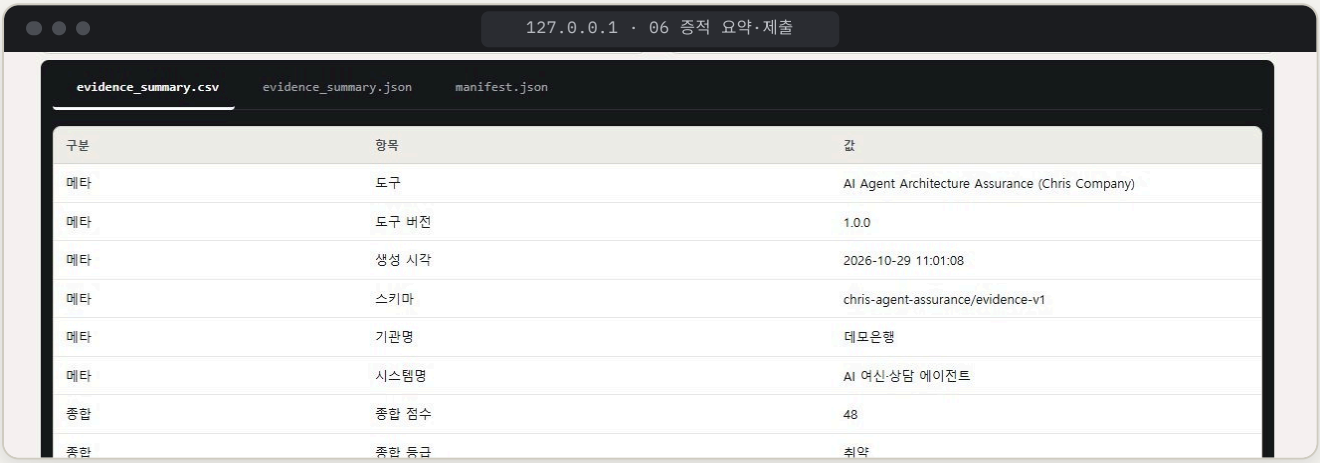
manifest.json

무결성 확인

각 파일의 SHA-256, 도구 버전, 생성 시각. 제출 후 변경 여부를 확인할 수 있습니다.

저장 전 미리보기

세 파일을 탭으로 넘겨 가며 실제 내용을 확인합니다 — 샘플 환경



● 포함되는 것

- 영역별 점수·등급, 발견 항목 종류별 건수·심각도
- 구성요소 종류별 수, 확인 상태, 근거 범위
- LLM SDK·프레임워크 이름, 비밀값 탐지 **건수**
- HITL 승인율·지연, 로그 집계 통계, 마스킹 건수

● 절대 포함되지 않는 것

- 소스 코드·설정·로그 원문, 개별 로그 행
- 비밀값, 근거 스니펫, 파일 경로
- IP, AWS 계정 ID, 이메일, 프롬프트
- 내부 시스템 호스트명 (허용한 경우만 포함, 기본은 마스킹)

미리보기에서 세 파일의 내용을 모두 본 뒤 **"위 세 파일의 내용을 모두 확인했습니다. 이 내용만 크리스컴퍼니에 제출됩니다."**에 체크해야 zip(`ChrisAgentAssurance_evidence_YYYYMMDD.zip`)을 저장할 수 있습니다.

WHAT LEAVES, AND HOW

귀사가 확인하기 전에는 아무것도 나가지 않습니다.

귀사 PC
분석·마스킹
원문은 이 PC 안에서만 읽고, 결과는 집계·마스킹합니다.

→

담당자
미리보기·확인
세 파일의 전체 내용을 보고 확인해야 저장됩니다.

→

귀사 절차
자료 반출
귀사의 반출 절차에 따라 담당자가 직접 옮깁니다.

→

CHRIS.COMPANY
CSV 제출
evidence_summary.csv (4MB 이하)만 올립니다.

SECURITY & PRIVACY

원문은 귀사 밖으로 나가지 않습니다. 무엇이 나갈지는 귀사가 결정합니다.

진단 프로그램에는 네트워크 통신 코드가 없습니다. 증적 파일은 담당자가 내용을 확인한 뒤, 귀사의 자료 반출 절차에 따라 직접 옮겨 제출합니다.

NO NETWORK

외부 통신 없음

서버는 127.0.0.1에만 열립니다. 웹 폰트·CDN을 쓰지 않고, 사용 통계(텔레메트리) 전송을 끕니다.

READ-ONLY

읽기 전용

파일을 읽기만 하며 수정·삭제하지 않습니다. 심볼릭 링크는 따라가지 않습니다.

PASSIVE

수동(passive) 탐색

네트워크 스캔, 포트 스캔, 호스트 접속을 하지 않습니다. 입력한 대역·호스트는 비교에만 씁니다.

BOUNDED

범위 제한

파일 5,000개, 파일당 1MB, 총 100MB까지. `.git` · `node_modules` · `venv` · `build` 등과 바이너리는 건너뜁니다.

NO SECRETS KEPT

비밀값 미저장

API 키·비밀번호·토큰은 종류와 위치(파일:줄)만 기록하고, 값은 어디에도 저장하지 않습니다.

LOCAL RENDERING

구성도는 로컬에서

Mermaid 구성도는 프로그램에 동봉된 라이브러리로, 엄격한 콘텐츠 보안 정책(CSP) 아래에서 그립니다.

읽는 즉시 마스킹

로그와 근거 스니펫은 읽는 즉시 마스킹되고, 화면에는 마스킹된 데이터만 남습니다. 일반 텍스트 로그는 원문 줄을 보관하지 않고 통계만 남깁니다.

IP 주소	`[MASKED_IP]`
12자리 AWS 계정 ID	`[MASKED_ACCOUNT]`
이메일	`[MASKED_EMAIL]`
프롬프트·본문·SQL	`[MASKED]`
접속 문자열의 계정·비밀번호	`[MASKED_USER]:[MASKED_SECRET]`
내부 시스템 호스트명 (증적, 기본값)	`[MASKED_HOST]`

OUR IMPACT

이 서비스는 크리스컴퍼니의 아키텍처 자문 경험 위에 만들어졌습니다.

크리스컴퍼니는 도메인 주도 설계(DDD), 클라우드 네이티브 아키텍처, 기술 부채 감사 및 iSAQB® 국제 공인 교육을 제공하는 글로벌 IT 컨설팅 및 아키텍처 전문 기업입니다. Architecture Review는 그동안의 소프트웨어 아키텍처 진단과 IT 감리 자문 방식을 AI 에이전트에 적용한 서비스입니다.

엔터프라이즈 아키텍처 및 AI 통합

South Korea

국내 1금융권, 대형 증권사 및 보험사의 기간계 시스템 재구축(Next-generation) 자문. 보수적인 금융 레거시 환경을 해체하고, 가장 안전하고 규제 순응적인 방식으로 AI를 이식하는 아키텍처 전환 전략을 제공합니다.

글로벌 물류 및 레거시 현대화

Singapore

싱가포르 HQ 선사의 벙커 텐더링(Bunker Tendering) 솔루션 전면 재설계. 3개의 레거시 시스템과 70여 개의 파편화된 화면을 서비스 워크숍을 통해 통합하고, 베트남 개발 센터를 활용한 글로벌 딜리버리 파이프라인을 아키텍팅하여 벙커링 비용을 혁신적으로 절감했습니다.

크로스보더 AX 전략

Azerbaijan / USA

국경을 넘나드는 AI 비즈니스 스케일업. 국내 SW 기업의 Global Market Fit을 설계해 아제르바이잔 AI 관제 시스템 수출을 성사시켰으며, 실리콘밸리 AI 스타트업의 아시아(APAC) 마켓 확장 전략을 주도했습니다.

글로벌 AI 데이터 아키텍처

New York, USA

뉴욕 소재 뷰티 브랜드의 초개인화 AI 추천 플랫폼 구축 자문. 글로벌 소비자의 피부톤 맞춤형 화장품 추천을 위한 한국 내 고품질 AI 학습 데이터 소싱 및 모델링 기반을 설계했습니다.

"

무거운 금융 기간계 시스템을 재구축하면서 동시에 AI를 도입해야 하는 막막한 상황이었습니다. IT 감리와 아키텍처를 아우르는 그들의 통찰은 뜬구름 잡는 기술적 환상이 아닌, 현실의 규제와 레거시를 돌파하는 가장 정확한 나침반이었습니다.

국내 대형 금융사

IT 기획 본부장

"

수십 개의 화면과 3개의 낡은 레거시가 얽힌 복잡한 비즈니스 로직을 단번에 꿰뚫어 보았습니다. 크리스컴퍼니의 명확한 아키텍처 설계와 크로스보더 개발 조직 안정화 리드 덕분에, 우리는 시스템 복잡도를 줄이고 벙커링 비용을 획기적으로 절감할 수 있었습니다.

싱가포르 HQ 선사

디지털 전환 프로젝트 총괄

"

글로벌 시장을 타겟으로 한 AI 추천 모델을 위해 어떤 데이터를 어떻게 소싱해야 할지 막막할 때, 국경을 넘나드는 크리스컴퍼니의 데이터 설계 자문은 우리 프로덕트의 핵심 경쟁력이 되었습니다.

미국 뉴욕 뷰티 기업

AI 프로덕트 총괄(CPO)

TRAINING

Licensed iSAQB® Accredited Training Provider

iSAQB® 공인 CPSA-Foundation(CPSA-F) 교육

ASSESSMENT

소프트웨어 아키텍처 진단 및 IT 감리 자문

기술 부채 분석, 성능 병목 진단, 규제 준수 및 아키텍처 품질 속성(QA) 종합 평가

ARCHITECTING

DDD · 클라우드 네이티브 · 엔터프라이즈 AI 통합

LLM 에이전트 오케스트레이션, RAG 파이프라인, AI 워크플로우 안정화 설계

사례와 고객 인용은 chris.company에 게시된 내용 그대로이며, 고객사명은 웹사이트와 같이 익명으로 표기합니다.

ARCHITECTURE REVIEW

신청부터 보고서까지

01	**무료 자가진단** 선택 · chris.company	업종별 15문항에 답하면 5개 영역 통제 점수와 업종별 보고서(금융·공공·의료·제조·일반)를 바로 받습니다.
02	**Review 신청** chris.company	로그인 → **내 진단 결과** → **Architecture Review**에서 기업 규모를 고르고 주문합니다.
03	**결제** 계좌이체	안내된 계좌로 이체합니다.
04	**프로그램 다운로드**	진단 프로그램(Windows 실행 파일)을 받아 내부망 PC로 옮깁니다.
05	**내부 실행** 귀사 PC·내부망	6단계를 진행해 증적 zip을 저장합니다. 이 과정에서 외부 통신은 없습니다.
06	**증적 제출** chris.company	귀사 반출 절차에 따라 옮긴 **evidence_summary.csv**(4MB 이하)를 Architecture Review → 증적 제출에 올립니다. zip은 담당자가 요청한 경우에만 admin@chris.company로 보냅니다.
07	**검토·보고서 전달** 크리스컴퍼니	크리스컴퍼니가 증적을 검토해 Architecture Review 보고서를 전달합니다.

BENCHMARK

영역별 선도 사례 비교

5개 영역마다 글로벌 선도 사례(leading practice) 기준과 비교합니다.

GAPS

통제 격차

증적에서 드러난 격차를 영역별로 정리합니다.

ROADMAP

우선순위 로드맵

무엇부터 보완할지 우선순위를 정한 개선 로드맵을 제시합니다.

PRICING

기업 규모별 요금

부가가치세(VAT) 별도
결제는 계좌이체로 진행합니다.

소기업	직원 50명 미만	**250** 만원
중소기업	직원 50~299명	**500** 만원
중견기업	직원 300~999명	**1,000** 만원
대기업	직원 1,000명 이상	**2,000** 만원
공공기관·공기업	국가·지자체·공공기관	**500** 만원

REQUIREMENTS & FAQ

실행 환경

운영체제	디스크	브라우저	설치·인터넷
Windows 10 / 11 (x64)	**약 200MB 여유 공간**	**Edge · Chrome 등 최신 브라우저**	**설치 불필요 · 인터넷 불필요**

코드 서명이 되지 않은 실행 파일이라 Windows SmartScreen이 경고할 수 있습니다. **추가 정보 → 실행**을 누르면 됩니다. 처음 실행은 압축 해제 때문에 수십 초 걸릴 수 있습니다.

Q 우리 데이터가 외부로 나가나요?

아니요. 프로그램에는 통신 기능이 없고 이 PC 안에서만 동작합니다. 제출하는 것은 집계·마스킹된 통계(evidence_summary.csv) 뿐이며, 저장 전에 전체 내용을 미리보기로 확인하고, 반출 여부와 방법도 귀사 절차로 직접 결정합니다.

Q 프로그램이 구성요소를 놓치면요?

정적 패턴 기반이라 동적으로 만들어지는 호출은 놓칠 수 있습니다. 4단계에서 구성요소를 직접 추가하거나 합치고, 이름을 수정하거나, 해당 없음(사유)으로 처리해 실제 구조에 맞춥니다.

Q Architecture Review 보고서에는 무엇이 담기나요?

5개 영역별 글로벌 선도 사례 기준 비교, 증적에서 드러난 격차, 우선순위가 정해진 개선 로드맵입니다.

Q 도입 전에 먼저 체험해 볼 수 있나요?

2단계의 **샘플 환경으로 채우기**를 누르면 프로그램에 동봉된 가상 프로젝트와 가상 로그로 6단계 전 과정을 볼 수 있습니다. 이 안내서의 화면이 그 예시입니다.

Q 어떤 로그를 연결할 수 있나요?

CloudTrail JSON, API Gateway CSV, 앱 로그(JSON-lines·CSV·텍스트)를 연결할 수 있습니다. 설정 파일은 yaml, .env 샘플, tf, properties 등을 추가로 연결할 수 있습니다.

Q 진단 결과는 어디에 남나요?

진행 중의 결과는 메모리에만 있고 브라우저 창을 닫으면 사라집니다. 남는 것은 담당자가 확인 후 직접 저장한 증적 zip뿐이며, 언제든 '처음부터'로 모든 입력과 결과를 지울 수 있습니다.

Q 얼마나 걸리나요?

프로그램 진행은 자료 위치만 알고 있으면 한자리에서 마칠 수 있는 분량입니다. 자료 준비와 검토 일정은 대상 시스템의 규모와 범위에 따라 달라 신청 후 안내해 드립니다.

CHRISCOMPANY
architecting in integrity

(주)크리스컴퍼니 · Architecting in Integrity

WEB
chris.company

CONTACT
admin@chris.company