



□ **일반현황**

| **아이템명** | | | *생성형 AI 및 RPA 기술이 적용된 개인정보 관리실태 자동 진단·보고 기능의 클라우드 SaaS 서비스* | | | | |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **산출물**  (협약기간 내 목표) | | | *웹사이트(1개), 관리자 콘솔(1개), AI 진단모델(1식), API 모듈(3종), 기술보고서(1식)* | | | | |
| **직업**  (직장명 기재 불가) | | | *연구원* | | **기업(예정)명** | *컴엔휴먼* | |
| **팀 구성 현황**(대표자 본인 제외) | | | | | | | |
| **순번** | **직위** | **담당 업무** | | **보유 역량**(경력 및 학력 등) | | | **구성 상태** |
| *1* | *기술이사* | *S/W 개발 총괄 및 AI 모델 아키텍처 설계* | | *컴퓨터공학 석사, AI 모델 개발·배포 경력(7년 이상)* | | | *완료* |
| *2* | *선임연구원* | *데이터 엔지니어링 및 MLOps 구축* | | *데이터 파이프라인 구축 경력(5년 이상), 클라우드(AWS) 활용 능력* | | | *예정* |
| *3* | *PM* | *프로덕트 기획·운영, 고객사 요구사항 분석* | | *보안 컨설팅 및 ISMS-P 대응 경력(6년 이상)* | | | *완료* |
| *4* | *대리* | *홍보 및 마케팅* | | *B2B 마케팅 경력(4년 이상), 디지털 마케팅 운영* | | | *예정* |

□ 아이템 개요(요약)

| **명 칭** | | 프라이버시가드 AI | | --- | | **범 주** | | | 프라이버시테크 B2B SaaS(개인정보 컴플라이언스 자동화) | | --- | |
| --- | --- | --- | --- | --- | --- | --- |
| **아이템 개요** | | 생성형 AI와 RPA가 결합된 클라우드형 개인정보 관리실태 자동 진단·보고 솔루션. 사용 용도: ISMS-P/개인정보보호법/GDPR 등 규제 요구사항을 상시 점검하고 증적을 자동 수집·정리해 감사 대응 리포트를 생성. 가격: Basic 99만원/월(최대 3커넥터), Pro 299만원/월(최대 10커넥터·워크플로우), Enterprise 견적제(무제한 커넥터·온프레/하이브리드 옵션). 핵심 기능·성능: 규제 지식그래프 기반 자동 진단, LLM+RAG 설명가능 리포트, 모듈형 커넥터·노코드 RPA로 증적 수집/정규화, 무결성(해시·타임스탬프·WORM) 및 감사추적, 역할기반 대시보드·KPI, 한/영 리포트. 고객 혜택: 점검·보고 기간 50% 이상 단축, 인건비·컨설팅 비용 절감, 상시 모니터링으로 리스크 조기 발견, 감사 신뢰성 제고 및 재인증 성공률 향상. | | --- | | | | |
| **문제 인식 (Problem)** | | 국내 ISMS-P와 개인정보보호법 점검 강화, 공공·금융의 상시 준수 요구 확대, 해외 GDPR/CCPA 등 다중 규제 동시 대응 필요성이 증가하고 있음. 현업은 엑셀·이메일 중심 수작업 점검으로 오류/누락과 리드타임 증가 문제가 상존하며, 온프레·클라우드·SaaS로 분산된 환경 탓에 통합 가시성 확보가 어려움. 기존 도구는 설문·룰베이스 위주로 맥락 이해와 증적 자동화가 제한적이고, SMB는 전문인력·예산 부족으로 도입 장벽이 높음. 생성형 AI를 활용하더라도 정확성·근거 제시·데이터 보안에 대한 우려가 남아 실무 적용이 더딘 상황으로, 설명가능성·무결성·보안성을 갖춘 자동 진단·보고 SaaS가 요구됨. | | --- | | | | |
| **실현 가능성 (Solution)** | | 사업기간 내 규제 지식그래프와 LLM+RAG 진단엔진을 탑재한 MVP(4개월) → 커넥터·RPA 엔진 확장(8~10개월) → 무결성·감사추적·대시보드 제품화(12개월)로 단계 개발. 차별성: 규제 요구사항–통제–증적 간 그래프 매핑과 설명가능 AI를 결합해 정확도·근거 제시를 강화, 모듈형 커넥터 SDK로 생태계 확장, WORM·전자서명으로 외부 감사 신뢰 확보. 경쟁력 확보: 멀티테넌트 보안 설계(데이터 격리·KMS·프롬프트 가드), 온프레/하이브리드 옵션, 산업별 플레이북 제공. 파일럿/베타를 통해 실제 데이터로 성능 지표(정확도, 근거제시율, 오탐/미탐율) 검증 및 고도화. | | --- | | | | |
| **성장전략 (Scale-up)** | | 경쟁사: 글로벌(OneTrust, TrustArc)은 범용 프라이버시 관리 강점이나 한국 규제·언어 맥락 적합성이 낮고, 국내 솔루션은 설문·룰 중심으로 자동 증적·설명가능 AI가 제한적. 진입 전략: SMB 타깃 구독모델로 빠른 온보딩, 보안컨설팅사 번들 패키지와 클라우드 마켓플레이스(AWS/Azure) 등재로 채널 확장. 사업 모델: 월 구독(기본)+커넥터 애드온+온보딩/교육 서비스+엔터프라이즈 옵션. 로드맵: 1.0(국내 ISMS-P 중심) → 1.5(GDPR/CCPA 템플릿·영문화) → 2.0(파트너 생태계·마켓플레이스 확장). 투자 전략: 정부과제 성과로 기술 검증 후 Seed 유치(채널·커넥터 확장) → Series A(해외 진출·제품 고도화). 인증 전략: ISMS-P 준비 및 ISO 27001/27701 준수 체계로 신뢰도 제고. | | --- | | | | |
| **팀 구성 (Team)** | | 컴엔휴먼이 총괄. 대표자는 개인정보 관리실태 컨설팅 및 ISMS-P 대응 경험을 보유하고 PM을 수행. 핵심 팀: 기술이사(아키텍처/AI 총괄), 선임연구원-데이터(MLOps/파이프라인), 보안리드(클라우드 보안·접근통제·감사추적), 프론트엔드 리드(콘솔·대시보드), RPA 엔지니어(커넥터/플로우), QA/DevOps(CI/CD·테스트·관측성), 마케팅 대리(B2B 디지털 마케팅). 협력 파트너: 보안컨설팅사(산업별 플레이북·PoC 자문), 클라우드 MSP(AWS 아키텍처/마켓플레이스), 법률사무소(국내·GDPR 규제 자문), 대학 연구실(NLP/RAG·지식그래프 공동연구), 인증심사기관(ISMS-P 사전진단). 역할 배분: 내부는 핵심 기술·제품화와 고객 성공, 파트너는 규제 자문·검증·채널 확장에 집중하여 사업화 속도와 신뢰성을 동시에 확보. | | --- | | | | |
| **이미지** | |  | | --- | | | |  | | --- | | |
|  | |  | |



ㅇ 강화되는 국내·외 개인정보 규제와 제재 리스크 확대

* 국내 ISMS-P, 개인정보보호법 고시 개정·점검 강화, 공공·금융의 상시 준수 요구가 증가하고 있으며, 해외 GDPR/CCPA 등 다중 규제 동시 대응이 필요함. 위반 시 과징금·제재 리스크가 커져 상시 모니터링 체계가 요구됨.

ㅇ 수작업 중심 진단·증적 수집의 비효율

* 엑셀 체크리스트·이메일·스크린샷에 의존한 점검은 시간이 오래 걸리고 오류·누락이 잦음. 최신 상태 반영이 지연되어 실제 운영 리스크를 선제적으로 발견하기 어려움.

ㅇ 분산된 시스템 환경과 데이터 사일로

* 온프레미스·클라우드·SaaS가 혼재하고 자산관리, 접근제어, 로그, DLP, ITSM 등 솔루션이 분절되어 통합 가시성 확보가 어려움. 표준화된 인터페이스 부재로 자동 수집·연계가 제한됨.

ㅇ 현존 규정관리·점검 도구의 한계(룰베이스/설문형)

* 맥락 이해가 부족하고 규정 변경 반영이 느림. 복수 규제 간 요구사항 매핑이 미흡하며 실시간 대응·증적 자동화 기능이 제한적임.

ㅇ 중소기업의 전문인력·예산 부족

* 프라이버시·보안 전담 인력 확보가 어려워 외부 컨설팅 의존도가 높고 비용 부담이 큼. 반복적 정기점검 업무 자동화 수요가 있으나 적합한 경량 솔루션이 부족함.

ㅇ LLM 활용 시 정확성·보안 우려

* 할루시네이션과 근거 미제시로 감사 대응 신뢰성이 낮을 수 있고, PII 처리 시 데이터 유출·프롬프트 주입 등 보안 리스크가 존재. 엔터프라이즈 수준의 통제 장치가 필요함.

ㅇ 증적의 무결성·감사추적성 부족

* 자동 수집 증적의 위·변조 방지, 타임스탬프, 워크플로우 이력 관리가 미흡해 외부 감사 시 신뢰 확보가 어려움.

ㅇ 통합 규제 매핑과 성숙도 지표 부재

* ISMS-P, 개인정보보호법, GDPR, ISO/IEC 27001·27701 간 교차 매핑과 산업별 컨트롤 표준이 부족해 경영진 관점의 성숙도 지표·KPI 대시보드 제공이 어려움.

ㅇ API·RPA 연계 생태계 미성숙

* 주요 클라우드·SaaS·보안솔루션에 대한 커넥터가 제한적이며, RPA는 비정형 증적·로그 수집에 취약. 운영환경 변화에 유연하게 대응하는 모듈형 커넥터가 필요함.

ㅇ 국제 확장 시 언어·현지 규제 대응의 어려움

* 국내 특화 도구는 멀티언어 처리·현지 규제 템플릿이 부족하고, 글로벌 도구는 한국어 문서·시스템 맥락 이해도가 낮아 현업 적용성이 떨어짐.

ㅇ 도입 초기 비용·시간 장벽

* 온프레 구축·커스터마이징·교육 비용이 높아 빠른 PoC와 단계적 확장이 어려움. 클라우드 기반의 즉시 사용형 모델 수요가 큼.

ㅇ 시장 성장 대비 SMB 적합 솔루션 공백

* 글로벌 프라이버시테크가 성장하는 반면, 국내 중소기업이 감당 가능한 비용·기능 구성을 갖춘 경량 자동화 솔루션이 부족해 도입이 지연됨.

ㅇ 해결방향 및 아이템 개발 필요성: 생성형 AI+RPA 기반 자동 진단·보고 SaaS

* 국내·외 규제를 구조화하여 요구사항-통제항목-증적 간 그래프 매핑을 수행하고, RPA·커넥터로 증적을 자동 수집·정규화. LLM은 근거 문서와 함께 설명가능한 진단 리포트를 생성하며, 프롬프트 가드·PII 비식별화·온프레/하이브리드 옵션으로 보안성을 확보함.

ㅇ 기대효과 및 타당성

* 진단·준비 기간 단축, 인건비 절감, 상시 모니터링으로 리스크 조기 발견, 감사 통과율·재인증 성공률 향상. 컴엔휴먼의 컨설팅 도메인 지식을 학습 데이터·룰로 전환해 산업별 플레이북을 제공함으로써 시장 적용 가능성이 높음.



ㅇ 프로토타입(MVP) 개발 및 핵심 기능 구현(협약 1~4개월 완료)

* 규제 요구사항-통제항목-증적 간 그래프 모델 설계 및 초기 지식베이스 구축, LLM+RAG 기반 자동 진단 엔진과 기본 관리자 콘솔 구현, 우선 커넥터 5종(API·로그·자산관리 계열) 개발. 차별성: 규제 그래프+설명가능형 LLM 결합으로 정확도·근거 제시 강화. 경쟁전략: 기존 컨설팅 레퍼런스 룰을 반영해 현업 적용성 확보. 예산: 정부지원사업비(인건비 중심)와 클라우드 인프라 초기 구축에 배정, 자기부담사업비는 PoC 고객 지원 및 테스트 장비에 사용.

ㅇ 클라우드 멀티테넌트 아키텍처 및 보안 설계(협약 1~3개월)

* VPC 분리·데이터 격리·키관리(KMS)·비식별화 파이프라인 설계, 하이브리드/온프레 연동 옵션 제공. 차별성: 엔터프라이즈 통제(접근통제·감사로그·비밀관리) 내장. 경쟁전략: 공공·금융 도입 대응을 위한 보안 가이드 준수 체크리스트 포함. 예산: 정부지원사업비로 보안 설계/테스트 도구, 자기부담사업비로 보안 컨설팅 일부 및 침투테스트 비용 배정.

ㅇ 모듈형 커넥터·RPA 엔진 개발(협약 2~8개월)

* AWS/Azure/Google, AD/Okta, O365/Google Workspace, EDR/DLP, WAF/로그 등 12종 이상 커넥터 단계적 확장, 노코드 RPA 플로우 디자이너 제공. 차별성: 커넥터 SDK 제공으로 파트너·고객 자가 확장. 경쟁전략: 주요 솔루션 벤더와 기술제휴·마켓플레이스 등재. 예산: 정부지원사업비로 커넥터 개발 인건비와 테스트 환경, 자기부담사업비로 제휴·검증 비용.

ㅇ AI 진단모델 고도화 및 정확성 보증(협약 4~10개월)

* 도메인 RAG, 프롬프트 가드, 팩트체크 루프, 근거문서 하이라이트와 신뢰도 점수 제공. 내부 벤치마크(정확도, 근거제시율, 오탐·미탐율) 운영. 차별성: 설명가능 리포트와 감사 대응용 근거 자동 패키징. 경쟁전략: 컨설턴트 생산성 지표로 효과 입증. 예산: 정부지원사업비로 학습·평가 데이터 가공/툴, 자기부담사업비로 모델 서빙 최적화 및 라이선스.

ㅇ 증적 무결성·감사추적 기능 구현(협약 3~9개월)

* 증적 해시·타임스탬프·WORM 스토리지, 워크플로우 이력/전자서명, 변경불가 감사로그 제공. 차별성: 외부 감사 대응 신뢰성 확보. 경쟁전략: ISMS-P/ISO 27001 준비 기업에 특화 패키지. 예산: 정부지원사업비로 스토리지·개발, 자기부담사업비로 외부 검증.

ㅇ 제품화 UI/UX 및 경영 대시보드(협약 5~10개월)

* 역할기반 콘솔, KPI/성숙도 지표, 교차규제 매핑 기반 리포팅, 멀티언어(한/영) 초도 지원. 차별성: CxO 관점의 리스크·비용절감 효과 가시화. 경쟁전략: 의사결정자 데모 시나리오 제공. 예산: 정부지원사업비로 프론트엔드 개발, 자기부담사업비로 디자인·사용성 테스트.

ㅇ 베타테스트 및 파일럿 운영(협약 7~11개월)

* 산업별 3개 시범기업과 PoC 수행, SLA·보안성·정확도 검증 및 기능 개선. 차별성: 실데이터 기반 성능 입증. 경쟁전략: 레퍼런스 확보와 케이스 스터디 발간. 예산: 정부지원사업비로 PoC 인건비·클라우드 비용, 자기부담사업비로 사용자 교육·현장 대응.

ㅇ 사업화 준비 및 1.0 출시(협약 10~12개월)

* 가격정책(월 구독+커넥터 애드온), 판매채널(파트너/직판) 정립, 약관·계약서·보안백서 준비, 기술지원 체계 구축. 차별성: SMB 친화 요금제와 빠른 온보딩. 경쟁전략: 컨설팅 번들 상품 출시. 예산: 정부지원사업비로 매뉴얼·문서화, 자기부담사업비로 마케팅·홍보.

ㅇ 지식재산·인증 및 규제 대응 확대(협약 8~12개월, 차년도 연계)

* 커넥터 SDK·증적 무결성 관련 특허·상표 출원, ISMS-P 사전진단·준비, 해외 규제 템플릿(GDPR/CCPA) 초기 버전 작성. 경쟁전략: IP로 진입장벽 강화, 인증으로 신뢰도 제고. 예산: 정부지원사업비 일부를 시험·검증에, 자기부담사업비로 특허·상표·인증 수수료.

ㅇ 정부지원사업비 및 자기부담사업비 집행 계획(요약)

* 정부지원사업비: 인건비 70%, 장비·클라우드/개발도구 15%, 시험·검증·외주 10%, 기타/간접 5%. 자기부담사업비: 마케팅·고객 PoC 40%, 인증·법률·특허 30%, 운영비(서버·모니터링) 20%, 교육·파트너십 10%. 월별 집행·분기별 점검으로 집행률 95% 이상 목표.

< 사업추진 일정(협약기간 내) >

| **구분** | **추진 내용** | **추진 기간** | **세부 내용** |
| --- | --- | --- | --- |
| *1* | *핵심 인력 채용 및 조직 구축* | *2025.10 ~ 2025.11* | *AI/백엔드/프런트/데이터/보안 등 5명 충원, 개발·품질·PM 체계 수립* |
| *2* | *규제 지식그래프 및 스키마 설계* | *2025.10 ~ 2025.12* | *ISMS-P/개인정보보호법/GDPR 요구사항 구조화, 온톨로지·매핑 규칙 정의* |
| *3* | *클라우드 아키텍처 구축(멀티테넌트/보안)* | *2025.10 ~ 2025.12* | *VPC·서브넷·IAM·KMS·모니터링 구성, 데이터 격리·로그 수집 체계 마련* |
| *4* | *커넥터 SDK 설계 및 1차 커넥터 6종 개발* | *2025.11 ~ 2026.02* | *AWS, Azure, Google Cloud, AD/Okta, O365, EDR 연동 모듈 구현 및 테스트* |
| *5* | *RPA 플로우 템플릿 1차 개발* | *2025.12 ~ 2026.02* | *증적 수집·검증·정규화 자동화 시나리오 10종 설계/개발* |
| *6* | *LLM 기반 진단엔진 MVP 완성* | *2025.12 ~ 2026.03* | *RAG 파이프라인 구축, 프롬프트 가드·근거 하이라이트 기능 포함* |
| *7* | *학습/평가 데이터셋 구축* | *2025.11 ~ 2026.04* | *도메인 문서 크롤링 및 정제, 벤치마크 지표·테스트 케이스 수립* |
| *8* | *증적 무결성·감사추적 모듈 개발* | *2026.01 ~ 2026.04* | *해시·타임스탬프·WORM 스토리지·감사로그 API 구현* |
| *9* | *관리자 콘솔 UI/UX 및 리포팅 개발* | *2026.02 ~ 2026.06* | *역할기반 접근, 대시보드·교차규제 리포트, 다국어(한/영) 지원* |
| *10* | *보안성 점검 및 침투테스트* | *2026.03 ~ 2026.06* | *소스 보안 점검, 취약점 진단·침투테스트, 개선 조치 반영* |
| *11* | *커넥터 2차 확장(추가 6종)* | *2026.03 ~ 2026.06* | *WAF/로그, DLP, Git, SIEM 등 확장 및 마켓플레이스 등록 준비* |
| *12* | *베타테스트/PoC 운영(3개 기업)* | *2026.05 ~ 2026.08* | *성능·정확도·SLA 검증, 사용자 피드백 수집 및 개선 스프린트 수행* |
| *13* | *성능 고도화 및 안정화* | *2026.06 ~ 2026.08* | *오탐/미탐 저감, 모델 서빙 최적화, 비용/성능 튜닝* |
| *14* | *지식재산권 출원 및 상표 등록* | *2026.04 ~ 2026.08* | *커넥터 SDK·증적 무결성 기술 관련 특허 2건, 서비스명 상표 1건 출원* |
| *15* | *사업화 준비(가격/계약/파트너)* | *2026.07 ~ 2026.09* | *가격정책·계약서·보안백서 완성, 리셀러/컨설팅 파트너 계약 체결* |
| *16* | *해외 규제 템플릿 초안 작성* | *2026.06 ~ 2026.09* | *GDPR/CCPA 요구사항 매핑 초안 및 영문 리포트 템플릿 제작* |
| *17* | *ISMS-P 사전진단 및 인증 준비* | *2026.05 ~ 2026.09* | *격차분석·보완계획 수립, 문서화·운영증적 정비* |
| *18* | *시제품 1.0 완성 및 최종 보고* | *협약기간 말* | *버전 1.0 출시 후보 빌드, 사용자 매뉴얼·기술보고서 제출* |
| *19* | *정부지원·자부담 집행 및 정산* | *협약기간 전기간* | *월별 집행·분기 점검·최종 정산, 집행률 95% 이상 달성* |

< 사업비 집행 계획 >

| **비 목** | **집행 계획** | **총사업비**(**원**) (ⓐ+ⓑ) | | | |
| --- | --- | --- | --- | --- | --- |
| **정부지원사업비**  (ⓐ) | **자기부담사업비**(ⓑ) | | **합계**  (ⓐ+ⓑ) |
| **현금** | **현물** |
| *재료비* | *▪ DMD소켓 구입(00개×0000원)* | *3,448,000* |  |  | *3,448,000* |
| *▪ 전원IC류 구입(00개×000원)* | *7,652,000* |  |  | *7,652,000* |
| *외주용역비* | *▪ 시금형제작 외주용역* | *3,000,000* | *7,000,000* |  | *10,000,000* |
| *…* |  |  |  |  |  |
| **합 계** | | *...* | *...* | *...* | *...* |



ㅇ 제품 성능 고도화

* LLM+RAG 기반 진단정확도 향상, 팩트체크 루프·근거 하이라이트 제공, 오탐/미탐 최소화 벤치마크 운용

ㅇ 규제 지식그래프 기반 정합성 확보

* ISMS-P/개인정보보호법/GDPR/ISO 27001·27701 교차 매핑 온톨로지 설계, 규정 변경 자동 반영 파이프라인 구축

ㅇ 보안·프라이버시 강화 설계

* 데이터 비식별화, KMS 키관리, 네트워크 격리, 프롬프트 가드·정책기반 접근통제, 온프레/하이브리드 옵션 제공

ㅇ 증적 무결성·감사추적성 확보

* 증적 해시·타임스탬프·WORM 스토리지·전자서명·감사로그로 외부 감사 신뢰성 강화

ㅇ 모듈형 커넥터·RPA 생태계 구축

* 커넥터 SDK 공개, 주요 솔루션(클라우드/IDP/EDR/DLP/로그) 순차 연동, 마켓플레이스 등재로 확산 가속

ㅇ 품질·보안 인증 취득

* ISMS-P 준비 및 사전진단, ISO 27001·27701 준수 체계 수립, 클라우드 보안 가이드 적합성 점검

ㅇ 지식재산권 확보

* 커넥터 SDK·증적 무결성·규제 매핑 기술 특허 출원, 서비스명 상표 등록, 데이터셋·모델 라이선스 전략 수립

ㅇ 고객가치 중심 GTM 전략

* SMB 친화 구독요금제+커넥터 애드온, 컨설팅 번들 상품, 산업별 플레이북·대시보드로 의사결정 지원

ㅇ 해외 시장 진출

* 한·영 UI/리포트 지원, GDPR/CCPA 템플릿 제공, 현지 파트너 협력·가격 현지화·지원문서 영문화

ㅇ 지속적 업데이트를 통한 경쟁력 유지

* 월간 릴리즈 캘린더, A/B 테스트·사용성 지표 기반 개선, Observability로 비용/성능 최적화

ㅇ 데이터 거버넌스·Responsible AI

* AI 윤리 가이드라인·평가지표 운영, 근거 기반 리포트 기본값 제공, 고객 데이터 주권 보호 정책 수립

ㅇ 정부과제·투자 연계 스케일업

* 정부지원사업 결과물 사업화 연계, Seed 투자로 마케팅·채널 확장 및 기술 고도화 재투자

< 사업추진 일정(전체 사업단계) >

| **구분** | **추진 내용** | **추진 기간** | **세부 내용** |
| --- | --- | --- | --- |
| *1* | *필수 개발 인력 채용* | *2025.10 ~ 2025.11* | *AI/백엔드/프런트/데이터/보안 등 핵심 인력 5명 채용 완료* |
| *2* | *홍보용 웹사이트 제작* | *2025.11 ~ 2025.12* | *서비스 소개·데모 영상·문의 연동 포함 웹사이트 자체 제작* |
| *3* | *지식재산권 출원* | *2026.04 ~ 2026.08* | *특허 2건·상표 1건 우선 출원 및 심사 대응* |
| *4* | *베타테스트/PoC 운영* | *2026.05 ~ 2026.08* | *시범기업 3곳 대상 성능·정확도·SLA 검증 및 개선 스프린트* |
| *5* | *ISMS-P 인증 준비* | *2026.05 ~ 2026.09* | *격차분석·보완·문서화·운영증적 정비 및 심사 신청* |
| *6* | *제품 패키지·요금제 확정* | *2026.07 ~ 2026.08* | *구독형(기본+커넥터 애드온) 가격 및 약관·계약서 확정* |
| *7* | *파트너 영업 채널 구축* | *2026.07 ~ 2026.10* | *리셀러/컨설팅 파트너 5개사 계약 및 기술 세미나 진행* |
| *8* | *클라우드 마켓플레이스 등재* | *2026.08 ~ 2026.09* | *AWS/Azure 마켓플레이스 리스팅 및 결제 연동* |
| *9* | *정식 출시(Commercial Launch)* | *2026.09 ~ 2026.09* | *버전 1.0 공개, 온보딩 가이드·보안 백서 배포* |
| *10* | *초기 고객 확보 캠페인* | *2026.09 ~ 2026.12* | *산업별 웨비나·사례집 배포, 파일럿 할인 및 레퍼런스 계약* |
| *11* | *고객성공(CSM) 체계 구축* | *2026.08 ~ 2026.10* | *온보딩·교육·헬프센터·SLA 운영 프로세스 수립* |
| *12* | *커넥터 2차·3차 확장* | *2026.10 ~ 2027.02* | *WAF/로그·DLP·SIEM·Git 등 추가 12종 개발·검증·배포* |
| *13* | *해외 진출 준비(영문화·GDPR)* | *2026.10 ~ 2027.03* | *영문 콘솔/리포트 완성, GDPR/CCPA 규제 템플릿 론칭* |
| *14* | *투자 유치(Seed)* | *2026.11 ~ 2027.02* | *핵심 KPI 제시로 투자유치, 자금은 채널 확장·R 고도화에 배분* |
| *15* | *레퍼런스 고도화 및 사례집 발간* | *2026.12 ~ 2027.03* | *도입 사례 5건 확보, 산업별 성공사례집/백서 발간* |
| *16* | *규정 업데이트·제품 릴리즈 운영* | *2026.09 ~ 2027.12* | *월간 규제 업데이트 반영, 분기 릴리즈·성능 튜닝 지속* |



ㅇ 대표자의 경력과 전문성

* 개인정보 관리실태 컨설팅 다년간 수행, ISMS-P 대응 및 보안 거버넌스 구축 경험 보유. 정부지원사업 총괄(PM) 수행 경험을 기반으로 일정·품질·예산 관리 체계 확립

ㅇ AI·데이터·보안 융합 역량

* 생성형 AI(RAG)·MLOps·데이터 엔지니어링과 클라우드 보안 설계를 융합할 수 있는 핵심 인력 확보 계획. 규제 지식그래프/증적 자동수집 등 핵심 기술 내재화

ㅇ 사업화 및 SaaS 운영 능력

* B2B SaaS 기획·가격정책·파트너 영업·CSM 체계를 갖춘 사업화 경험 보유(또는 보완 채용 계획). 멀티테넌트/구독형 과금/마켓플레이스 등재 준비

ㅇ 정부과제 수행·정산 경험

* IRIS 접수·평가 대응·중간점검·최종 정산 등 공공과제 전 과정의 경험을 축적하여 집행률 및 성과관리 리스크 최소화

ㅇ 인프라·장비 및 품질체계

* 클라우드(AWS/Azure) 기반 개발·테스트 환경과 보안/성능 모니터링 체계 구축, 표준 개발 프로세스(코드리뷰·CI/CD·테스트) 운영

ㅇ 외부 자문·협력 네트워크

* 보안컨설팅사·인증심사기관·법률자문·대학 연구실 등과의 협력망으로 기술검증·규제 대응·인재 파이프라인 확보

팀 구성(안)

| **구분** | **직위** | **담당 업무** | **보유 역량**(**경력 및 학력 등**) | **구성 상태** |
| --- | --- | --- | --- | --- |
| *1* | *기술이사* | *S/W 개발 총괄 및 AI 아키텍처 설계* | *컴퓨터공학 석사, 대규모 분산 백엔드·AI 서빙 경력(7년 이상)* | *예정(25.11)* |
| *2* | *선임연구원(데이터)* | *데이터 파이프라인 설계 및 MLOps 구축* | *Python/SQL, ETL·피처스토어·모델 배포 경력(5년 이상), AWS 활용 능력* | *예정(25.11)* |
| *3* | *PM* | *프로덕트 로드맵·요구사항·일정/예산 관리* | *보안 컨설팅 및 ISMS-P 대응 경력(6년 이상), 애자일 운영 경험* | *완료(25.10)* |
| *4* | *보안리드* | *클라우드 보안 아키텍처·접근통제·감사추적 설계* | *정보보안기사, ISO 27001/27701·ISMS-P 실무(7년 이상)* | *예정(25.11)* |
| *5* | *프론트엔드 리드* | *관리자 콘솔·대시보드 UI/UX 개발* | *React/TypeScript·데이터 시각화 경험(6년 이상)* | *예정(25.11)* |
| *6* | *RPA 엔지니어* | *커넥터 개발 및 RPA 플로우 설계/구현* | *API 연계·UiPath/Power Automate 경험(5년 이상)* | *예정(25.12)* |
| *7* | *QA/DevOps* | *테스트 전략 수립·CI/CD·모니터링·성능 튜닝* | *Jenkins/GitHub Actions·IaC(Terraform)·Observability 경험(5년 이상)* | *예정(25.12)* |
| *8* | *마케팅 대리* | *B2B 디지털 마케팅·세일즈 자료 제작·리드 운영* | *콘텐츠·퍼포먼스 마케팅 경력(4년 이상), 보안/SaaS 분야 이해* | *예정(25.12)* |

협력 기관 현황 및 협업 방안

| **구분** | **파트너명** | **보유 역량** | **협업 방안** | **협력 시기** |
| --- | --- | --- | --- | --- |
| *1* | *A보안컨설팅(협의중)* | *ISMS-P/개인정보보호 컨설팅 및 갭분석·실사 노하우* | *산업별 컴플라이언스 플레이북 공동 개발, PoC 자문 및 초기 레퍼런스 지원* | *협약기간 내* |
| *2* | *B클라우드파트너스(AWS 파트너, 협의중)* | *멀티테넌트 아키텍처 설계·KMS/네트워크 보안·마켓플레이스 등재 지원* | *VPC/KMS/모니터링 아키텍처 검토 및 비용 최적화, AWS 마켓플레이스 리스팅 지원* | *25.10 ~ 26.09* |
| *3* | *C법률사무소(개인정보 전문, 협의중)* | *개인정보보호법·GDPR 규제 자문, 약관/계약서 법률 검토* | *규제 템플릿·자동 진단 결과 법률 리스크 검토, 약관·DPA 자문* | *26.06 ~ 26.09* |
| *4* | *D대학 산학협력단/데이터AI 연구실(협의중)* | *NLP·RAG·지식그래프 연구 및 석·박사급 인재 풀* | *알고리즘 공동연구·성능 벤치마크·인턴십 연계* | *25.12 ~ 26.08* |
| *5* | *E보안솔루션사(협의중)* | *EDR/DLP/로그 플랫폼 API 제공 및 기술지원* | *모듈형 커넥터 공동 개발·호환성 검증·공동 마케팅* | *26.03 ~ 26.06* |
| *6* | *F인증심사기관(ISMS-P, 협의중)* | *ISMS-P 인증 심사·사전진단 수행 경험* | *사전진단·운영증적 점검 및 인증 준비 컨설팅* | *26.05 ~ 26.09* |
| *7* | *G디자인에이전시(협의중)* | *B2B SaaS UI/UX·브랜딩·디자인 시스템 구축* | *관리자 콘솔 UX 고도화·디자인 가이드 제작* | *26.02 ~ 26.05* |