">

Seekers

PUBLIC

SEEKERSLAB · 제품 카탈로그

# 씨커스랩 제품 카탈로그

AI 보안, 보안 운영, 클라우드 보안, AI 개발 제품과 서비스 총괄 안내

| 문서 | 구분 | 발행 | 문의 |
| --- | --- | --- | --- |
| 제품 카탈로그 | 공개용 | 2026. 11 | contact@seekerslab.com |

02 · 목차

# 목차


| | |
|---|---|
| 제품 구성도 | 3 |
| 회사 소개 | 4–5 |
| 제품 선택 가이드: 과제별, 규모·환경별 | 6–7 |
| KYRA: AI 보안 및 AI 에이전트 | 8–15 |
| Seekurity: 보안 운영 | 16–20 |
| FRIIM: 클라우드 보안 | 21–24 |
| Crux: AI 개발 | 25–26 |
| 서비스: 보안관제, 클라우드, 보안 SI | 27–29 |
| 산업별 안내: 금융, 공공, 제조, 중견·중소 | 30–33 |
| 도입 및 지원 | 34–35 |
| 자료 목록, 용어 정리 | 36–37 |


## 본 카탈로그의 구성 원칙

- **수록 기준:** 구현이 확인된 제품과 기능만 수록
- **수치 기준:** 규칙 수, 점검 항목 수 등 제품 사양만 기재. 측정되지 않은 성능·효과 수치 미기재
- **가격 기준:** 공개 가격이 있는 KYRA MDR만 가격 기재, 그 외 제품은 별도 문의
- **상세 자료:** 제품별 제품소개서는 각 제품 쪽의 QR 코드 또는 웹사이트에서 제공

**KYRA**
AI 보안 및 AI 에이전트 제품군. 생성형 AI 통제, AI 기반 보안관제, 업무용 AI 에이전트와 지식 검색

**Seekurity**
보안 운영 제품군. 로그 수집·탐지·대응(SIEM)과 IT 자산관리

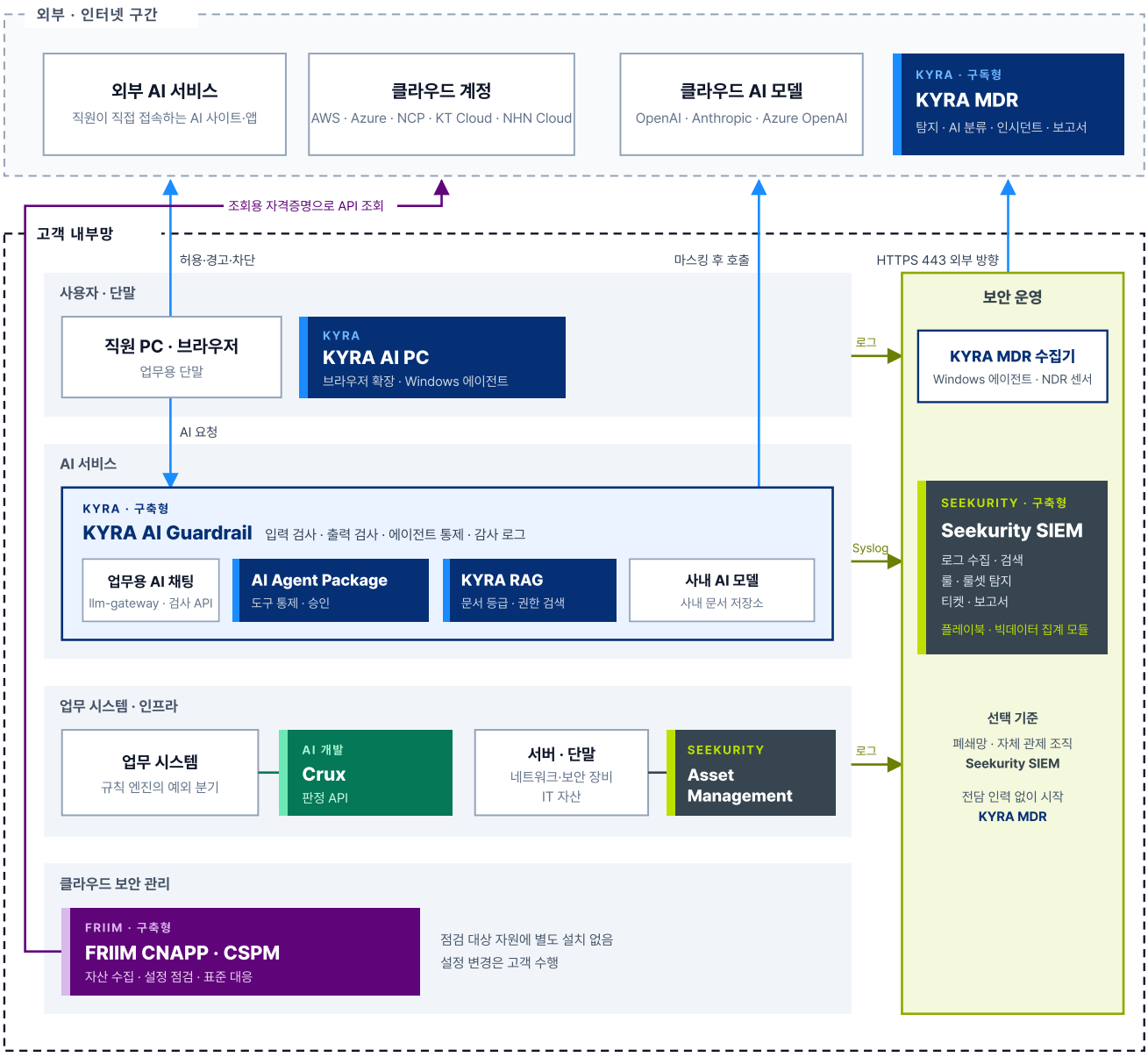
**FRIIM**
클라우드 보안 제품군. 멀티클라우드 설정 점검과 컴플라이언스 관리

**Crux**
AI 개발 제품. 기존 룰 엔진에 AI 판정을 연결하는 AI 활성화 레이어

**문의:** contact@seekerslab.com · 02-2039-8160 · seekerslab.com

03 · 제품 구성도

# 제품 구성도: 고객 인프라 기준 제품 배치




제품 상자 선택 시 해당 제품 쪽으로 이동. 화살표는 요청·조회·로그의 방향이며 각 제품은 단독 도입 가능

04 · 회사 소개

# 회사 소개 ①: 씨커스랩

씨커스랩(주식회사 씨커스): 2015년 설립, 보안관제와 SIEM 기술을 기반으로 성장한 보안 전문 기업

## 회사 개요

| 항목 | 내용 |
|---|---|
| **상호** | 주식회사 씨커스 (브랜드: 씨커스랩, SeekersLab) |
| **설립** | 2015년 3월 |
| **소재지** | 서울특별시 구로구 디지털로33길 28 우림이비지센터1차 |
| **사업 분야** | 정보보안 소프트웨어 개발, IT 보안 서비스 |
| **대표 연락처** | 02-2039-8160 · contact@seekerslab.com |
| **웹사이트** | seekerslab.com |

## 사업 영역

**제품 개발**
클라우드 보안 플랫폼 FRIIM, 보안 운영 솔루션 Seekurity, AI 보안 및 AI 에이전트 제품군 KYRA 자체 개발

**보안 서비스**
보안관제, 클라우드 보안 진단, 보안 시스템 구축

**클라우드·개발 서비스**
클라우드 전환, 플랫폼 엔지니어링, 마이크로서비스 전환, 맞춤 개발

**기술 공급**
자사 기술 기반 OEM/ODM 공급

## 기술 기반

- **출발점:** 보안관제와 SIEM(통합 로그 분석) 기술
- **확장 방향:** 클라우드 보안, 생성형 AI 보안, AI 에이전트 순으로 제품군 확장
- **연구 조직:** 기업부설연구소 운영(2015년 설립)
- **수행 분야:** 공공, 금융, 제조 분야 보안 프로젝트 수행

## 제품군별 대응 과제

| 제품군 | 고객 과제 | 대표 제품 |
|---|---|---|
| **KYRA** | 생성형 AI의 안전한 사용, 보안 인력 부족, 업무 자동화 | AI Guardrail, MDR, AI Agent Package, RAG |
| **Seekurity** | 로그 통합 관리와 탐지·대응, 자산 현황 관리 | SIEM, Asset Management |
| **FRIIM** | 클라우드 설정 오류와 컴플라이언스 점검 | CNAPP, CSPM |
| **Crux** | 룰로 처리되지 않는 예외 업무의 AI 판정 | Crux |

05 · 회사 소개

# 회사 소개 ②: 인증, 특허, 연혁

## 인증 및 등록

| 연도 | 항목 |
|---|---|
| 2015 | 기업부설연구소 설립 |
| 2016 | 벤처기업 인증 |
| 2016 | CC 인증 |
| 2019 | ISO/IEC 27001 인증 취득 |
| 2020 | KRX KSM 등록 |
| 2021 | 이노비즈협회 회원 |
| 2025 | ISO/IEC 27001:2022 전환 |

## 보유 특허 3건

**시간기반 보안위협 분석기법**
시간 축 기준의 보안 위협 분석 기술

**보안위협분석 시나리오 자동생성**
위협 분석 시나리오의 자동 생성 기술

**전산 자산 정보 자동 분석**
전산 자산 정보의 자동 수집·분석 기술

## 제품 전개 순서

1 **보안관제·SIEM**
Seekurity SIEM, 로그 수집과 상관분석

› 2 **클라우드 보안**
FRIIM, 멀티클라우드 설정 점검

› 3 **AI 기반 관제**
KYRA MDR, 구독형 탐지·대응

› 4 **생성형 AI 보안**
KYRA AI Guardrail, AI 사용 통제

› 5 **AI 에이전트**
Agent Package, RAG, Crux

## 정보보호 관리 체계

- **인증 유지:** ISO/IEC 27001 인증 유지(2019년 취득, 2025년 2022 개정판 전환)
- **적용 의미:** 제품 개발과 서비스 운영 조직의 정보보호 관리 체계 운영

## 고객 지원 창구

| 구분 | 창구 |
|---|---|
| 제품·도입 상담 | contact@seekerslab.com, 02-2039-8160 |
| 온라인 문의 | seekerslab.com/ko/company/contact |
| KYRA MDR 가입 | kyramdr.com |

본 카탈로그는 고객사명, 고객 수, 도입 효과 수치를 수록하지 않음. 도입 사례 확인이 필요한 경우 상담 시 별도 안내

06 · 선택 가이드

# 제품 선택 가이드 ①: 과제별

현재 과제에서 출발하여 검토 대상 제품 확인

| 현재 과제 | 검토 제품 | 쪽 |
|---|---|---|
| **사내 챗봇·AI 에이전트의 민감정보 입력과 인젝션 통제** | KYRA AI Guardrail | 9–10 |
| **직원의 외부 AI 서비스 사용 현황 파악과 통제** | KYRA AI PC (Shadow AI 관리) | 15 |
| **보안 인력 없이 관제 시작** | KYRA MDR | 11–12 |
| **사내 문서 기반 AI 질의응답 구축** | KYRA RAG | 14 |
| **승인 절차를 갖춘 업무용 AI 에이전트 운영** | KYRA AI Agent Package | 13 |
| **폐쇄망 내 로그 통합, 탐지, 감사 대응** | Seekurity SIEM | 17–18 |
| **실제 자산과 자산 대장의 불일치 해소** | Seekurity Asset Management | 19–20 |
| **멀티클라우드 설정 오류와 컴플라이언스 점검** | FRIIM CNAPP, FRIIM CSPM | 22–24 |
| **룰로 처리되지 않는 예외 업무의 자동 판정** | Crux | 25–26 |
| **클라우드 보안 현황의 외부 전문가 진단** | 클라우드 보안 진단 서비스 | 28 |

## 구매 계기별 출발점

**인증 심사·감사 대응**
ISMS-P 등 심사 준비 단계. 로그 보관과 증적은 Seekurity SIEM 또는 KYRA MDR, 클라우드 점검은 FRIIM

**생성형 AI 도입 결정**
사내 AI 개방 전후 단계. KYRA AI Guardrail로 입력·출력·에이전트 통제, KYRA RAG로 문서 권한 통제

**침해 사고 우려**
탐지·대응 체계 부재 단계. KYRA MDR 무료 플랜으로 시작 후 확장

**클라우드 전환**
전환 전후 단계. 클라우드 보안 진단 서비스 후 FRIIM 상시 점검

## 제품 간 연결

1 **KYRA AI Guardrail** — AI 사용 이벤트 생성
› 2 **Syslog 전송** — CEF 또는 JSON 형식
› 3 **Seekurity SIEM** — 타 보안 이벤트와 통합 분석
› 4 **대응** — 티켓, 플레이북

- **연결 기준:** 위 연결은 KYRA AI Guardrail의 Syslog 전송 기능 기준
- **단독 도입:** 모든 제품은 단독 도입 가능, 제품 간 연결은 선택 사항

07 · 선택 가이드

# 제품 선택 가이드 ②: 규모·환경별

## 조직 규모별

| 조직 유형 | 일반적 상황 | 출발 제품 |
|---|---|---|
| **중소기업 (보안 담당 겸직)** | 전담 인력 부재, 구축 여력 제한 | KYRA MDR (구독형, 무료 플랜 보유) |
| **중견기업 (보안 담당 1–3명)** | 인증 심사 대응, AI 도입 병행 | KYRA MDR, KYRA AI Guardrail |
| **대기업·그룹사** | 자체 관제 조직, 다수 시스템 연동 | Seekurity SIEM, KYRA AI Guardrail, FRIIM CNAPP |
| **공공·금융** | 망분리, 감사 증적, 구축형 선호 | Seekurity SIEM, KYRA AI Guardrail (폐쇄망 구성) |

## 운영 환경별

| 폐쇄망·구축형 | 구독형 | 혼합 환경 |
|---|---|---|
| Seekurity SIEM: 고객 환경 설치 | KYRA MDR: kyramdr.com 가입 후 수집기 설치 | 사내 시스템은 SIEM, 클라우드 계정은 FRIIM(구축형, 자격증명 등록) |
| KYRA AI Guardrail: 사내 모델 연결 구성 | 무료 플랜으로 사전 확인 | AI 서비스는 Guardrail로 단일 정책 적용 |
| KYRA RAG, AI Agent Package: Guardrail 플랫폼 내 구성 | 수집기의 외부 방향 통신 필요 | 단말의 AI 사용은 브라우저 확장과 에이전트 |
| Seekurity Asset Management: 고객 환경 설치 | | |

## 도입 방식 요약

| 제품 | 도입 방식 | 가격 안내 |
|---|---|---|
| **KYRA MDR** | 구독형(SaaS) | 공개 가격 (12쪽) |
| **KYRA AI Guardrail, RAG, AI Agent Package** | 구축형 (Docker Compose, 쿠버네티스) | 별도 문의 |
| **KYRA AI PC** | Guardrail의 단말 구성 요소 | 별도 문의 |
| **Seekurity SIEM** | 구축형 | 별도 문의 |
| **Seekurity Asset Management** | 구축형 | 별도 문의 |
| **FRIIM CNAPP, CSPM** | 구축형 (클라우드 자격증명 등록) | 별도 문의 |
| **Crux** | 프로젝트형 (API 연동) | 별도 문의 |

**선택이 어려운 경우:** 현재 운영 중인 시스템, 망 환경, 당면 과제(심사 일정, AI 도입 계획)를 정리하여 문의 시 적합 제품과 도입 순서 안내

08 · KYRA

KYRA

# KYRA: AI 보안 및 AI 에이전트 제품군

기업의 생성형 AI·AI 에이전트 사용을 통제하고, AI로 보안관제와 업무를 자동화하는 제품군

## 제품 구성

| | |
|---|---|
| **AI 사용 통제** | KYRA AI Guardrail · KYRA AI PC (Shadow AI 관리) |
| **AI 기반 보안관제** | KYRA MDR |
| **업무용 AI** | KYRA AI Agent Package · KYRA RAG |
| **공통 기반** | 인증·권한 · 민감정보 검사 · 감사 로그 |

## 제품별 역할

| 제품 | 해결 과제 | 도입 방식 | 쪽 |
|---|---|---|---|
| **KYRA AI Guardrail** | 사내 AI의 입력·출력·에이전트 실행 통제 | 구축형 | 9–10 |
| **KYRA MDR** | 보안 인력 없이 탐지·대응 시작 | 구독형 | 11–12 |
| **KYRA AI Agent Package** | 승인 절차를 갖춘 업무용 에이전트 운영 | 구축형 | 13 |
| **KYRA RAG** | 권한을 반영한 사내 문서 질의응답 | 구축형 | 14 |
| **KYRA AI PC** | 직원 PC의 외부 AI 서비스 사용 관리 | 단말 배포 | 15 |

## 제품 간 관계

- **동일 플랫폼:** AI Guardrail, AI Agent Package, RAG, AI PC는 동일 플랫폼의 구성 요소로 동일한 정책과 감사 로그 사용
- **독립 서비스:** KYRA MDR은 kyramdr.com에서 제공하는 독립 구독 서비스
- **연결:** Guardrail의 보안 이벤트는 Syslog로 관제 시스템에 전송 가능

## 도입 순서 예시

**1 현황 파악** — AI PC로 외부 AI 사용 현황 확인 ›

**2 사내 AI 개방** — Guardrail로 입력·출력 통제 ›

**3 문서 연결** — RAG로 등급별 검색 권한 적용 ›

**4 에이전트 확대** — Agent Package로 도구·승인 통제

위 순서는 예시이며 각 제품은 단독 도입 가능. 사내 챗봇을 이미 운영 중인 경우 Guardrail의 llm-gateway 연결부터 시작

09 · KYRA

KYRA

# KYRA AI Guardrail ①: 개요와 구조

사내 생성형 AI의 입력, 출력, 에이전트 실행을 단일 지점에서 통제하는 구축형 AI 보안 게이트웨이

**대상**
사내 챗봇·AI 에이전트를 운영 중이거나 도입 예정인 기업·기관

**도입 방식**
고객 환경 설치형(Docker Compose, 쿠버네티스), 폐쇄망 운영 가능

**연결 모델**
OpenAI, Anthropic, Azure OpenAI, Ollama 기반 사내 모델

## 대응 과제

- **민감정보 입력:** 고객 명단, 접속 비밀번호가 포함된 로그 등의 AI 입력
- **숨은 지시:** 업로드 문서와 검색 결과에 포함된 인젝션 문구
- **에이전트 실행:** 승인 없는 도구 호출, 조회, 발송
- **감사 대응:** AI 사용 기록의 증적 요구

## 구조

| | |
|---|---|
| **접점** | 업무용 AI 채팅 · 관리 콘솔 · 외부 AI 서비스·에이전트 |
| **연동** | api-gateway · llm-gateway (선택) |
| **가드레일 검사** | 인젝션 탐지 · 민감정보 검사 · 정책 평가 · 위험 점수 |
| **AI 서비스** | 채팅 · 지식 검색 · 에이전트 · 워크플로 |
| **기록·운영** | 감사 로그 · 알림 · Syslog 전송 · 보고서 |

## 연결 방식 3종

| 방식 | 적용 상황 | 변경 사항 |
|---|---|---|
| **업무용 AI 채팅** | 사내 AI 채팅 신규 개설 | 없음 |
| **llm-gateway** | 운영 중인 AI 서비스·에이전트 보유 | 모델 호출 주소와 키 변경 |
| **검사 API** | 자체 파이프라인의 개별 단계 검사 | 검사 지점에 API 호출 추가 |

## 질문 1건의 처리 순서

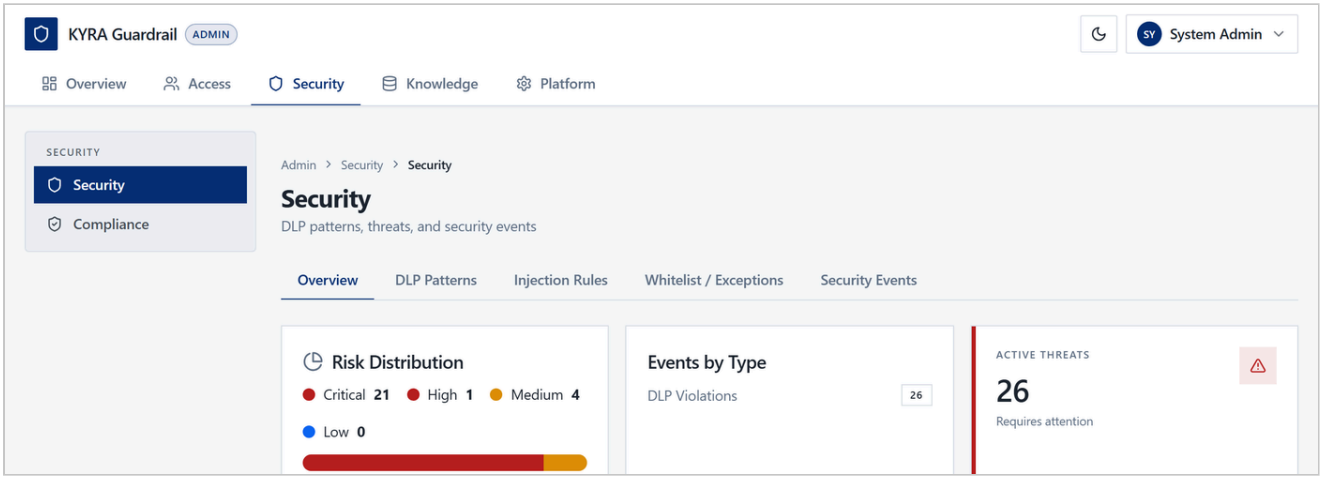
1. **입력 검사** — 인젝션, 민감정보
2. **지식 검색** — 권한 내 문서, 조각 검사
3. **모델 호출** — 마스킹된 문장 전달
4. **출력 검사** — 스트리밍 조각 단위
5. **기록** — 판정과 사유

KYRA

# KYRA AI Guardrail ②: 주요 기능과 도입

## 주요 기능

| 구분 | 내용 |
|---|---|
| **인젝션·탈옥 탐지** | 규칙 25종, 7개 언어. 문자 변형 정규화와 인코딩 해독 후 검사 |
| **민감정보 검사** | 기본 규칙 37종. 주민등록번호·보안 등급 표시 차단, 전화번호·계좌번호 등 마스킹 |
| **사용자 정의 규칙** | 정규식·키워드 등록, 예문 시험 기능, 재시작 없이 반영 |
| **에이전트 통제** | 허용 도구, 단계 수 제한, 실행 시간 제한, 요청자 외 관리자 승인 |
| **지식 검색 권한** | 문서 4등급, 역할별 열람 권한, 원본 시스템 권한 동기화 |
| **출력 통제** | 응답 민감정보 마스킹, 주제 제한, 출처 필수 설정 |
| **감사** | SHA-256 해시 체인 감사 로그, 기본 7년 보관, 법적 보존 |
| **컴플라이언스** | ISMS-P, 개인정보보호법 등 5개 기준 37개 점검 항목 |
| **연동** | SSO(SAML, OIDC), SCIM, Syslog(CEF, JSON), Slack, Teams, 이메일 |




관리 콘솔 [Security] 화면(시연용 데이터). 콘솔 언어는 영문

## 도입 절차

**1** 요구사항 확인
모델, 사용자 규모, 연동 시스템

›

**2** 설치·연동
SSO, Syslog, 기본 정책

›

**3** AI 서비스 연결
호출 경로 전환

›

**4** 검증
시나리오 기반 확인

›

**5** 운영 이관
교육, 운영 자료

## 추가적으로 확인해야 되는 부분

- **사내 모델:** 폐쇄망은 사내 모델과 구동 서버 별도 준비 필요(가드레일은 모델 미내장)
- **문서 등급:** 지식 검색 권한 통제는 문서 등급 부여가 전제
- **화면 언어:** 관리 콘솔과 업무용 채팅은 영문

> **상세 자료:** KYRA AI Guardrail 제품소개서(18쪽) · seekerslab.com/ko/ai/guardrail

KYRA

# KYRA MDR ①: 개요와 구성

수집기 설치로 로그 수집, 탐지, AI 1차 분류, 인시던트 관리, 보고서를 단일 콘솔에서 제공하는 구독형 보안관제 서비스

**대상**
보안 전담 조직이 없는 중소·중견기업의 IT 담당자, 로그 보존과 모니터링 증적이 필요한 감사 대응 담당자

**도입 방식**
kyramdr.com 가입 후 사내 Linux 서버에 수집기 설치. 무료 플랜으로 시작

**구성**
로그 수집·검색, 규칙 기반 탐지, AI 경보 분류, 인시던트, 플레이북, EASM, NDR(선택)

## 구성 요소

| | |
|---|---|
| **로그 발생원** | 방화벽 · 스위치 · Linux 서버 · Windows PC·서버 |
| **고객 환경 수집** | 수집기 · Windows 에이전트 · NDR 센서 (선택) |
| **전송** | 외부 방향 HTTPS(443) · 연결 단절 시 로컬 디스크 버퍼 |
| **플랫폼** | 탐지 규칙 실행 · AI 분류 · 인시던트 · 플레이북 · 로그 검색 · EASM |
| **알림** | 이메일 · Slack · 웹훅 · 카카오톡 알림톡 · 모바일 푸시 |

## 주요 기능

| 구분 | 내용 |
|---|---|
| **탐지** | 규칙 4종(SIGMA, 상관 분석, 이상 탐지, 클라우드), 1분 주기 실행, ATT&CK 14개 전술 표시 |
| **AI 분류** | 경보별 분류 5종과 신뢰도 표시, 최종 판정은 고객 담당자 수행 |
| **대응** | 경보 상태 5종, 인시던트 5단계, 플레이북 조치와 원복 |
| **조사** | 필드 검색, 심각도별 히스토그램, 엔티티 피벗, CSV·JSON 내보내기 |
| **확장** | EASM(하위 도메인, DNS 레코드, 인증서 점검), NDR 센서 8개 프로토콜 분석 |
| **보고** | 보고서 4종(경영진 요약, 인시던트, 컴플라이언스, 위협 동향) |

## 역할 구분

| AI | 고객 담당자 | 씨커스랩 |
|---|---|---|
| 경보 분류와 신뢰도 산정 | 정탐·오탐 최종 판정 | 서비스 플랫폼 운영 |
| 판단 근거 요약 | 인시던트 전환과 단계 관리 | 탐지 기능 제공 |
| | 플레이북 조치 승인 | 플랜별 기술지원 |

- **네트워크 요건:** 수집기는 외부 방향 HTTPS(443)만 사용, 외부에서 사내로의 포트 개방 불필요
- **기존 장비:** 방화벽과 백신 교체 불필요, 로그 전송 주소를 수집기로 지정

KYRA

# KYRA MDR ②: 요금제와 도입

요금은 kyramdr.com 공개 기준(2026년 11월 19일 확인). 최신 조건은 웹사이트에서 확인

| 구분 | FREE | MDR | PRO | CUSTOM |
|---|---|---|---|---|
| **월 요금** | ₩0 | ₩300,000 | ₩800,000 | 협의 |
| **초당 이벤트(EPS)** | 50 | 500 | 1,500 | 무제한 |
| **일 수집량** | 500MB | 5GB | 20GB | 무제한 |
| **로그 보존** | 7일 | 90일 | 180일 | 365일 |
| **엔드포인트** | 40 | 120 | 350 | 무제한 |
| **기술지원** | - | 이메일(영업시간) | 전담 | 전담 |

## 플랜 선택 기준

**FREE**
자사 장비 로그의 수집 여부와 콘솔 적합성 확인 단계. 보존 7일

**MDR**
담당자 1명이 경보와 인시던트를 처리하는 중소 규모 조직. 보존 90일

**PRO**
여러 사용자가 함께 운영하거나 ISMS-P 준비에 컴플라이언스 화면이 필요한 조직

**CUSTOM**
수집량이 크거나 보존 365일, 현장 온보딩이 필요한 조직

## 시작 절차

1. **가입** — kyramdr.com 계정 생성
2. **수집기 설치** — 사내 Linux 서버에 설치
3. **로그 연결** — 장비의 로그 전송 주소 지정
4. **탐지 확인** — 콘솔에서 경보 확인
5. **운영** — 판정, 인시던트, 보고서

## 추가적으로 확인해야 되는 부분

- ☑ **로그 발생량:** 초당 이벤트와 일 수집량 추정 후 플랜 선택
- ☑ **외부 전송:** 수집기의 외부 방향 통신 허용 여부. 외부 전송이 불가한 폐쇄망은 Seekurity SIEM 검토
- ☑ **판정 주체:** 경보의 최종 판정과 야간·휴일 수신 담당자 지정
- ☑ **Windows 에이전트:** 이벤트 로그 전달 도구이며 단말 차단 기능을 포함한 EDR 제품과 구분

**상세 자료:** KYRA MDR 제품소개서(16쪽) · kyramdr.com

13 · KYRA

KYRA

# KYRA AI Agent Package: 통제된 에이전트 실행 환경

계획 검증, 도구 입출력 검사, 승인, 감사 기록을 거쳐 실행되는 에이전트·워크플로 실행 환경

**대상**
에이전트 시범 운영이 보안 심의에서 멈춘 조직, 문서 검색·요약·보고서 업무를 AI에 맡기려는 부서

**도입 방식**
KYRA AI Guardrail 플랫폼에 포함된 기능. 고객 환경 설치형, 화면은 영문

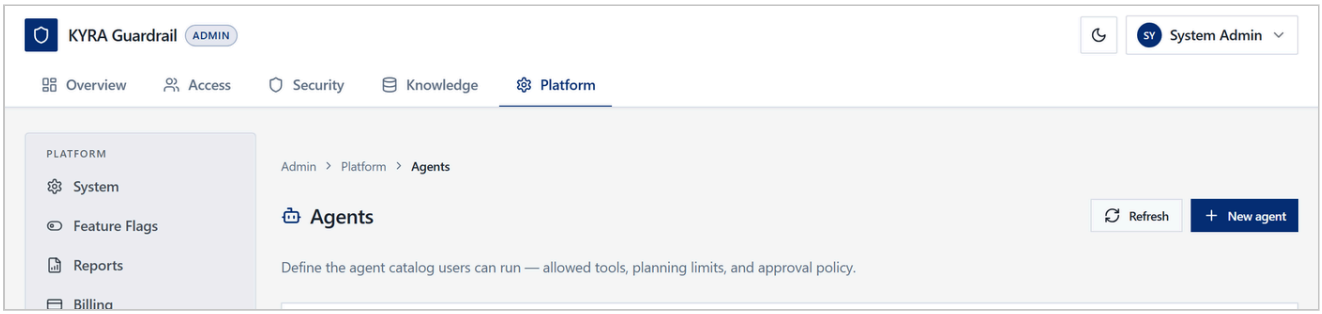
**구성**
에이전트 카탈로그, 기본 도구 10종, 워크플로, 모델 등록부, 페르소나 12종

## 실행 순서와 통제 지점

1 **요청** — 에이전트 선택, 과업 입력
2 **과업 검사** — 인젝션·민감정보 검사
3 **계획 수립** — 허용 도구 범위 내 단계 구성
4 **계획 검증** — 도구·입력값·의존 관계 확인
5 **도구 호출** — 입력 검사, 실행, 결과 검사
6 **승인** — 대상 단계에서 정지
7 **결과** — 단계별 결과 취합
8 **감사 기록** — 실행·단계·승인 이벤트

## 핵심 기능

| 구분 | 내용 |
|---|---|
| **실행 통제** | 과업 검사, 계획 검증, 도구 입력·결과 검사, 실행 시간·단계 수 제한 |
| **기본 도구** | 문서 검색·요약, 웹 검색, 보고서 생성, 알림, 번역 등 10종 |
| **카탈로그** | 에이전트별 허용 도구, 단계 수, 승인 방식 지정 |
| **승인·감사** | 요청자 외 관리자 승인, 실행·단계·승인 이벤트 기록 |
| **워크플로** | 모델 호출, 지식 검색, 조건 분기, API 호출 단계 조합 |
| **모델·페르소나** | 모델 등록부, 사내 모델 추가, 역할별 페르소나 12종 |




관리 콘솔 [Platform] > Agents: 에이전트별 허용 도구 수, 단계 제한, 승인 방식(시연용 데이터)

## 추가적으로 확인해야 되는 부분

- **도구 범위:** 기본 도구 10종은 제품 내장. 신규 도구 추가는 별도 협의 대상
- **데이터 조회 도구:** 사용자 본인의 이용 현황 조회용이며 업무 데이터 조회 용도와 구분
- **알림 도구:** 제품 내 알림 전용. 이메일 발송과 구분

**상세 자료:** KYRA AI Agent Package 제품소개서(14쪽) · seekerslab.com/ko/products/ai-agent

14 · KYRA

KYRA

# KYRA RAG: 권한을 반영하는 사내 지식 검색

사내 문서 저장소를 연결하여 문서 등급과 원본 권한을 유지한 채 검색하고, 출처와 함께 답변 근거를 제공하는 지식 검색 서비스

**대상**
사내 문서 기반 질의응답을 준비하는 IT 운영 책임자, 보안·개인정보 담당자, 문서 관리 부서

**도입 방식**
KYRA AI Guardrail 플랫폼의 지식 검색 서비스. 고객 환경 설치형

**구성**
커넥터 10종, 문서 변환과 문자 인식, 색인, 권한 필터 검색, 재순위화, 출처 표기

## 수집부터 답변까지

1 **저장소 연결** — 커넥터 동기화, 파일 업로드
2 **문서 변환** — 본문 추출, 문자 인식
3 **조각 분할** — 문단·문장 경계 기준
4 **색인** — 벡터 색인, 전문 검색 색인
5 **권한 필터 검색** — 열람 가능 문서만 대상
6 **재순위화** — 관련도 재평가
7 **출처 구성** — 번호형 출처

## 핵심 기능

| 구분 | 내용 |
|---|---|
| **저장소 연결** | 커넥터 10종, 변경분 동기화, 삭제 반영 |
| **문서 처리** | PDF·Word·Excel·HTML 변환, 스캔 문서 문자 인식, 조각 분할 |
| **권한** | 문서 4등급, 역할별 열람 범위, 원본 권한 동기화, 검색 전후 확인 |
| **검색 품질** | 하이브리드 검색, 재순위화, 질의 보강, 사전 설정 3종 |
| **출처** | 문서명, 쪽 번호, 절 제목이 포함된 번호형 출처 |
| **가드레일 연계** | 검색된 문서 조각별 검사, 출처 필수 페르소나 |

## 추가적으로 확인해야 되는 부분

- ☑ **커넥터 설정:** 콘솔 설정 화면 제공은 5종(S3, REST, Confluence, SharePoint, Google Drive), 그 외 5종은 API 설정
- ☑ **동기화 실행:** 내장 일정 기능 없음. 관리자 실행 또는 외부 스케줄러로 동기화 시작
- ☑ **원본 권한:** 원본 권한 반영은 Confluence, SharePoint, Google Drive 대상. 그 외는 동기화 시 지정한 등급 적용
- ☑ **문서 형식:** HWP, PPTX는 변환 대상 외

**상세 자료:** KYRA RAG 제품소개서(14쪽) · seekerslab.com/ko/products/kyra-rag

15 · KYRA

KYRA

# KYRA AI PC: 직원 PC의 AI 사용 관리

직원 PC의 AI 서비스 사용을 파악하고 서비스별 정책을 적용하는 KYRA AI Guardrail의 단말 구성 요소

**대상**
직원의 외부 AI 서비스 사용 현황을 파악하려는 보안·IT 운영·개인정보 담당자

**도입 방식**
브라우저 정책과 단말 관리 도구로 일괄 배포. Guardrail 관리 콘솔에서 관리

**구성**
브라우저 확장(Chrome, Edge), Windows 엔드포인트 에이전트, 네트워크 센서

## 구조

| | | | | |
|---|---|---|---|---|
| **직원 PC (브라우저)** | 브라우저 확장 | 서비스별 정책 적용 | 입력·파일 검사 | |
| **직원 PC (운영체제)** | Windows 엔드포인트 에이전트 | 접속 탐지 | 차단 (선택) | |
| **네트워크** | 네트워크 센서(SPAN·TAP) | 관찰 전용 | | |
| **KYRA AI Guardrail 서버** | AI 서비스 목록 | 서비스별 정책 | 민감정보 규칙 | 감사 로그 |

## 수집 지점별 비교

| 항목 | 브라우저 확장 | Windows 에이전트 | 네트워크 센서 |
|---|---|---|---|
| **관찰 대상** | 브라우저의 AI 사이트 접속 | PC 내 프로그램의 AI 접속 | 네트워크상의 AI 접속 |
| **통제** | 허용·경고·차단, 입력 검사 | 차단(선택) | 관찰 전용 |
| **주된 역할** | 사용자 안내, 사유 기록 | 브라우저 외 사용 파악 | 미설치 구간 보완 |

## 서비스별 정책 3단계

| 정책 | 동작 |
|---|---|
| **허용** | 제한 없이 사용 |
| **경고** | 경고 화면 표시, 사유 입력 후 60분 사용, 사유 기록 |
| **차단** | 차단 안내 화면으로 이동 |

- **AI 서비스 목록:** 51종 기본 제공, 기관별 추가 가능. 미지정 서비스의 기본값은 경고
- **입력 검사(선택):** 전송 직전 입력 문장과 첨부 문서(Word, Excel, PowerPoint, 텍스트)를 민감정보 규칙으로 검사
- **수집 범위:** 에이전트는 프로그램명, 사용자명, AI 도메인, 횟수만 전송. 화면 내용과 프롬프트 미전송

## 추가적으로 확인해야 되는 부분

- **서버 필요:** KYRA AI Guardrail 서버 없이 단독 동작 불가
- **범위 외:** PC에서 직접 구동하는 모델의 탐지와 PC 하드웨어 사양은 본 제품 범위 외
- **임직원 안내:** 수집 항목 안내문과 개인정보 처리 근거를 기관 규정에 맞게 준비

**상세 자료:** KYRA AI PC 소개서(10쪽) · seekerslab.com/ko/products/ai-pc

16 · SEEKURITY

# Seekurity: 보안 운영 제품군

로그 수집·탐지·대응과 IT 자산 관리를 위한 구축형 보안 운영 제품군

## 제품 구성

| | |
|---|---|
| **로그 통합·탐지** | Seekurity SIEM |
| **SIEM 모듈** | 플레이북 (Seekurity SOAR) · 빅데이터 집계 (Seekurity BigData) |
| **자산 관리** | Seekurity Asset Management |

## 제품별 역할

| 제품 | 해결 과제 | 도입 방식 | 쪽 |
|---|---|---|---|
| **Seekurity SIEM** | 폐쇄망 내 로그 통합, 탐지, 티켓 처리, 감사 대응 | 구축형 | 17–18 |
| **플레이북 모듈** | 탐지 이후 알림, 티켓 생성 등 후속 절차 자동화 | SIEM 선택 서비스 | 18 |
| **빅데이터 집계 모듈** | 수집 로그의 집계 분석 | SIEM 메뉴 | 18 |
| **Seekurity Asset Management** | 자산 발견, 대장 대조, 수명주기 이력 관리 | 구축형 | 19–20 |

## 모듈 안내 기준

- **플레이북(Seekurity SOAR):** 독립 제품이 아닌 Seekurity SIEM의 선택 서비스로 제공
- **빅데이터 집계(Seekurity BigData):** Seekurity SIEM 내 집계 메뉴로 제공

## 적합 환경

**폐쇄망 운영 기관**
인터넷 연결 없는 환경의 오프라인 설치, 로그의 내부 보관

**감사 증적 요구 기관**
정기 보고서, 감사 로그, 로그 무결성 검증

**자체 관제 조직 보유**
룰·룰셋 직접 운영, 티켓 기반 처리 절차

**자산 현황 정비 필요**
대장과 실제 자산의 불일치 해소, 정기 재물조사

## KYRA MDR과의 구분

| Seekurity SIEM | KYRA MDR |
|---|---|
| 고객 서버 설치형 | 구독형 서비스 |
| 폐쇄망 운영 | 수집기의 외부 방향 통신 필요 |
| 고객 관제 조직이 룰과 티켓 운영 | 전담 조직이 없는 조직에 적합 |
| 로그 내부 보관 | 무료 플랜으로 시작 |

17 · SEEKURITY

# Seekurity SIEM ①: 개요와 구조

폐쇄망 내부에 설치하여 보안 장비·서버의 로그를 수집하고, 룰로 탐지하며, 티켓으로 처리하는 구축형 SIEM

**대상**
폐쇄망을 운영하는 공공·금융·제조 기관의 보안 관제 책임자, 감사 담당자

**도입 방식**
고객 서버 설치형, 오프라인 설치. 단일 서버 구성이 기본

**구성**
로그 수집·검색, 룰·룰셋 탐지, 티켓, 정기 보고서, 로그 무결성 검증

## 구조

| | |
|---|---|
| **로그 발생원** | 보안 장비 · 네트워크 장비 · 서버 · 업무 DB |
| **수신** | Syslog 수신 · SNMP 수집 · DB 수집(JDBC) · 전용 Agent 수신 (선택) |
| **전달·파싱** | Kafka(내부 메시지 브로커) · 정규표현식 파싱 · 인덱스 저장 |
| **저장** | OpenSearch(로그 인덱스) · PostgreSQL(설정, 룰, 티켓, 계정) |
| **화면** | 웹 콘솔(HTTPS) |
| **통지** | 이메일(SMTP) · Syslog 전송 · Slack · SNMP Trap |




기본 대시보드: 등급별 룰 탐지 현황, 시스템 상태, 보안로그 수집 현황(시험 환경 데이터)

## 핵심 기능

| 구분 | 내용 |
|---|---|
| **수집** | Syslog, SNMP, 전용 Agent, DB(JDBC) 4개 방식과 정규표현식 파서 |
| **탐지** | 조건 룰, 횟수 기준 탐지, 룰을 Step으로 조합한 룰셋 |
| **현황** | 기본 대시보드, 위젯 기반 커스텀 대시보드 |
| **처리** | 탐지 연계 티켓, 칸반 보드, 4개 상태 관리, 티켓 리포트 |
| **관리** | 위협·내부 인텔리전스, 보안정책 배포, 상면 관리 |
| **감사** | 정기 보고서, 감사 로그, 인덱스 해시 기반 무결성 검증 |

# Seekurity SIEM ②: 모듈, 사양, 도입

## 모듈

| 플레이북 (Seekurity SOAR) |
|---|
| SIEM의 선택 서비스 |
| 탐지 이후 후속 절차 자동화 |
| 제공 동작: 알림, SNMP Trap 전달, 티켓 생성 |
| 장비 차단·격리 동작은 제공 범위 별도 확인 |

| 빅데이터 집계 (Seekurity BigData) |
|---|
| SIEM 내 집계 메뉴 |
| 수집 로그의 집계 분석 |
| 집계 결과의 보고서·대시보드 연계는 도입 시 확인 |

## 설치 환경

| 항목 | 내용 |
|---|---|
| **운영체제** | Rocky Linux 9.x, RHEL 9.x |
| **설치 방식** | 오프라인 설치 패키지와 설치 스크립트 |
| **사전 설치 대상** | Java, PostgreSQL, Nginx, Kafka, OpenSearch |
| **라이선스** | 고객별 서명 라이선스 파일. 만료일과 최대 로그 소스 수 포함 |

## 하드웨어 기준

| 구분 | CPU | 메모리 | 디스크 |
|---|---|---|---|
| **최소** | 8코어 | 16GB | 500GB(SSD) |
| **권장** | 16코어 | 32GB | 2TB |

- **최종 사양:** 일일 로그 수집량과 보관 기간을 기준으로 설계 단계에서 산정

## 구성 형태

**단일 서버 구성**
수집, 저장, 분석, 탐지, 화면을 서버 1대에 설치하는 기본 구성

**역할 분리 구성**
수집, 저장, 분석 역할을 서버별로 분리. 로그량과 망 구조에 따라 설계 단계에서 협의

## 추가적으로 확인해야 되는 부분

- ☑ **일일 로그량:** 장비별 일일 로그 발생량과 증가 추세. 서버 사양과 디스크 용량 산정의 기준
- ☑ **연동 장비:** 수집 대상 장비의 로그 형식. 신규 형식은 정규표현식 파서 작성 대상
- ☑ **플레이북:** 등록·수정 방식과 제공 동작 범위를 시연에서 확인
- ☑ **보관 기간:** 기관 규정상의 로그 보관 기간과 저장 용량

**상세 자료:** Seekurity SIEM 제품소개서(18쪽) · seekerslab.com/ko/products/siem

Seekers

# Seekurity Asset Management ①: 개요와 구조

발견된 자산을 대장과 대조하여 결재로 편입·격리하고, 수명주기 전 과정의 이력을 남기는 IT 자산관리 플랫폼

**대상**
실제 보유 자산 현황을 답해야 하는 IT 자산 담당자, 보안 담당자, 감사 담당자

**도입 방식**
고객 환경 설치형(컨테이너 기반), 웹 브라우저 접속

**구성**
8개 업무 영역, 30개 화면, 권한그룹 4종

## 대응 과제

- **대장 불일치:** 표 형식 대장과 실제 자산의 차이, 반납되지 않은 PC
- **미등록 자산:** 대장에 없는 서버·단말의 네트워크 접속
- **미승인 SaaS:** 승인 절차 없이 사용 중인 SaaS 구독
- **이력 부재:** 도입부터 폐기까지의 변경 이력 추적 곤란

## 구조

| | |
|---|---|
| **사용자** | 웹 브라우저 · 권한그룹 4종(사용자, 자산담당, 보안담당, Admin) |
| **업무 화면** | Main · 자산관리 · 재고·계약 · Discovery · AI 인텔리전스 · 워크플로 |
| **처리** | 자산 지문 병합 · 대장 대사 · 결재선 집행 · 알림 발송 · 리포트 산출 |
| **통제** | 화면 접근 제어 · 기능 권한 · 탐지 정책 · AI 정책 |
| **기록** | 자산 대장 · 발견 자산 · 관측 이력 · 결재 이력 · 감사 로그 |

## 8개 업무 영역

| 영역 | 주요 기능 |
|---|---|
| **Main** | 대시보드, 역할별 처리 대기 목록, 공지사항, QnA |
| **자산관리** | 자산 대장, 도입·검수, 불출·이동, 반납·유휴, 폐기 |
| **재고·계약** | 재고 현황, 재물조사 계획·수행, 계약, SW 라이선스 대사 |
| **Discovery** | 6개 탐지 채널, 자산 지문 병합, 대장 대사, Shadow SaaS, 외부 공격표면 |
| **워크플로** | 신청·결재, 다단계 결재선 |
| **AI 인텔리전스** | AI 어시스턴트, 분석·예측, 리포트 자동 생성 |
| **환경설정** | 메뉴·권한, 사용자·결재선, 공통코드, 탐지 정책, AI 정책 |
| **연동·인프라** | 커넥터 관리, 알림 발송 이력, 감사 로그 |

# Seekurity Asset Management ②: Discovery와 도입

## 발견부터 처리까지

**1 관측 적재**
채널별 관측 기록 저장

›

**2 지문 병합**
동일 장비 관측을 1건으로 통합

›

**3 대장 대사**
대장과 대조, 4개 상태 판정

›

**4 위험도 분류**
높음, 중간, 낮음

›

**5 소유자 확인**
추정 부서에 확인 요청

## 6개 탐지 채널

| 채널 | 발견 대상 |
|---|---|
| **네트워크 능동 스캔** | 미등록 단말·서버·IoT 장비 |
| **패시브 트래픽** | 스캔이 도달하지 않는 구간의 활성 장비 |
| **DNS·프록시 로그** | 미인가 SaaS 사용 |
| **EDR·엔드포인트** | 설치 SW, USB 저장매체, 로컬 가상머신 |
| **클라우드 API** | 미관리 클라우드 리소스·계정 |
| **AD/IdP·SSO 로그** | 미인가 OAuth 앱, 휴면 계정 |

## 대사 결과 4개 상태

| 대사 결과 | 후속 처리 |
|---|---|
| **등록·일치** | 최종 확인 일시 갱신 |
| **등록·불일치** | 대장 보정 후 대사 확인으로 종결 |
| **미등록** | 소유자 확인 요청, 편입 결재 또는 격리 요청 |
| **미확인** | 유휴·분실 후보, 수시 재물조사 편성 |

## 추가적으로 확인해야 되는 부분

- ☑ **보유 제품 연동:** NAC, EDR, 프록시, 계정 관리 제품과의 연동은 도입 단계에서 제품별로 구성·검증
- ☑ **허용 채널:** 망 정책상 허용되는 수집 채널 범위(능동 스캔, 트래픽 관측, 로그 수집, 클라우드 API)
- ☑ **AI 모델:** 사용 모델과 구동 서버는 도입 단계에서 확정. 모델 미연결 시 규칙 기반 동작
- ☑ **인증과 저장소:** 통합 인증(SSO) 방식, 데이터베이스 구성, 백업 기준
- ☑ **기존 대장:** 이관할 대장의 형식과 필수 항목 정리 상태

**상세 자료:** 제품소개서(18쪽) · seekerslab.com/ko/products/asset-management

21 · FRIIM

FRIIM

# FRIIM: 클라우드 보안 제품군

여러 클라우드 계정의 자산과 보안 설정을 점검하고 표준 기준으로 결과를 정리하는 클라우드 보안 플랫폼

## 제품 구성

| | |
|---|---|
| **통합 플랫폼** | FRIIM CNAPP: 계정 연결과 자산 수집과 형상 점검과 표준 대응과 결재·보고 |
| **형상 점검 구성** | FRIIM CSPM: 보안 설정 점검과 표준 팩 기준 결과 정리 |

## 제품별 역할

| 제품 | 해결 과제 | 도입 방식 | 쪽 |
|---|---|---|---|
| **FRIIM CNAPP** | 다수 클라우드·계정의 자산과 설정 통합 관리, 심사 대응 | 구축형 | 22–23 |
| **FRIIM CSPM** | 클라우드 설정 상태의 정기 점검과 증적 준비 | 구축형 | 24 |

## 일반적 과제

**계정별 상이한 콘솔**
클라우드마다 다른 콘솔과 용어로 인한 통합 현황 파악 곤란

**설정 오류**
공개 설정된 저장소, 과도하게 열린 네트워크 규칙 등 설정 상태의 상시 확인 필요

**심사 대응**
표준별 점검 결과를 증적으로 정리하는 반복 작업

**조치 추적**
미준수 항목의 조치 담당과 승인 이력 관리

## 동작 방식

1. **계정 등록** — 클라우드별 자격증명 등록
2. **자산 수집** — 자원 목록과 설정 조회
3. **형상 점검** — 항목별 Pass/Fail 판정
4. **표준 매핑** — 표준 팩 단위 결과 정리
5. **결과·결재** — 대시보드, Excel, 기안·결재

- **설치 범위:** 점검 대상 자원에 별도 설치 없음. 등록된 자격증명으로 클라우드 API 조회
- **조치 주체:** 설정 변경은 고객 수행. FRIIM은 점검과 결과 정리 담당

## 수록 범위

본 카탈로그는 현재 제공 중인 계정 연결, 자산 수집, 형상 점검, 표준 대응 기능만 수록. 워크로드 실행 보호와 권한 분석은 수록 범위 외이며 문의 시 개별 안내

FRIIM

# FRIIM CNAPP ①: 개요와 구조

여러 클라우드 계정의 자산을 수집하고 보안 설정을 점검하여 국내외 표준 기준으로 결과를 정리하는 구축형 플랫폼

**대상**
2개 이상의 클라우드 또는 다수 계정을 운영하는 기업·기관의 클라우드 운영 책임자, 보안 담당자

**도입 방식**
고객 인프라 설치형. 클라우드별 조회용 자격증명 등록으로 연결

**구성**
계정 연결, 자산 수집, 형상 점검 204개 항목, 표준 팩 9종, 결재와 Excel 내보내기

## 구성도

| | |
|---|---|
| **웹 콘솔** | 대시보드 · 통합계정 관리 · 점검 항목·팩 관리 · 리소스 목록 · 기안함 |
| **진입·인증** | API 게이트웨이 · 인증(OAuth2/JWT, OTP) |
| **클라우드 연동** | 프로바이더 등록 · 키 관리 |
| **자산 수집** | 컴퓨트 · 오브젝트 스토리지 · 자원 검색 |
| **점검·분석** | 정책 · 형상 점검 · 분석 |
| **운영 지원** | 사용자·계정 · 알림 · 대시보드 데이터 |

## 핵심 기능

| 구분 | 내용 |
|---|---|
| **클라우드 연결** | AWS, Azure, NCP, KT Cloud, NHN Cloud 등 계정을 통합계정으로 등록 |
| **자산 수집** | 컴퓨트, 네트워크, 스토리지, 데이터베이스 등 자원 목록 수집 및 검색 |
| **형상 점검** | 5개 분류 204개 점검 항목, 자원별 Pass/Fail 판정 |
| **표준 대응** | 표준 팩 9종, 팩에 할당된 점검 항목 합계 338건 |
| **승인·보고** | 기안·결재(승인/반려) 절차, 주요 목록 Excel 내보내기 |
| **계정·접근** | 조직·그룹·서브유저, 메뉴 권한, OTP, 접속 로그 |

## 단계별 확인 화면

| 단계 | 확인 화면 |
|---|---|
| **계정 등록** | 클라우드 통합계정 관리 |
| **자산 수집** | 리소스 목록 |
| **형상 점검** | 컴플라이언스 항목 관리 |
| **표준 매핑** | 컴플라이언스 팩 관리 |
| **결과·결재** | 대시보드, 기안함 |

# FRIIM CNAPP ②: 표준 대응과 도입

## 표준 팩 9종과 할당 점검 항목 수

| 팩 | 기준 | 할당 항목 수 |
|---|---|---|
| **CSAP** | 클라우드 보안인증(CSAP) 2024 | 64 |
| **CSAP CCE 2024** | KISA 클라우드 취약점 점검 가이드 2024 | 58 |
| **ISO 27001** | ISO/IEC 27001:2022 정보보안 경영시스템 | 30 |
| **CSA CCM v4.0** | CSA Cloud Controls Matrix v4.0 | 81 |
| **CIS Benchmarks** | CIS Foundations Benchmarks(AWS, Azure, GCP) | 35 |
| **PCI DSS 4.0.1** | 결제카드 데이터 보안 표준 | 19 |
| **SOC 2** | SOC 2 Trust Services Criteria 2024 | 15 |
| **NIST 800-53** | NIST SP 800-53 Rev.5 | 21 |
| **NIST CSF 2.0** | NIST 사이버보안 프레임워크 2.0 | 15 |

- **1회 점검, 다중 표준:** 동일 점검 결과가 할당된 모든 팩의 준수 현황에 동시 반영
- **자체 팩:** 기관 자체 기준에 맞는 팩 추가 구성과 계정별 팩 할당




[컴플라이언스 팩 관리]: 표준 팩 목록과 팩별 할당 점검 항목 수(일부 정보 가림 처리)

## 추가적으로 확인해야 되는 부분

- ☑ **대상 클라우드:** 사용 중인 프로바이더의 점검 항목 제공 여부. GCP는 지원 확대 진행 중
- ☑ **필요 표준:** 심사 대상 표준의 팩 제공 여부. ISMS-P 등 9종 외 표준은 자체 팩 구성 방안 확인
- ☑ **네트워크:** 설치 서버에서 각 클라우드 API로의 접근 경로 확보 여부
- ☑ **자격증명 권한:** 조회 전용 권한 발급 절차와 키 교체 주기
- ☑ **조치 절차:** 설정 변경은 고객 수행. 미준수 항목의 조치 담당과 기한 관리 절차 준비

**상세 자료:** FRIIM CNAPP 제품소개서(14쪽) · seekerslab.com/ko/products/cnapp

# FRIIM CSPM: 클라우드 설정 점검

클라우드 계정의 보안 설정을 204개 항목으로 점검하고 표준 팩 기준으로 결과를 정리하는 FRIIM의 형상 점검 기능

**대상**
클라우드 계정의 설정 상태를 정기적으로 확인하고 심사 증적을 준비하는 운영·보안 담당자

**도입 방식**
고객 인프라 설치형. 조회용 자격증명 등록, 점검 대상 자원에 별도 설치 없음

**구성**
점검 항목 204개, 자원별 Pass/Fail 판정, 표준 팩 9종

## 점검 절차 5단계

**1 계정 등록**
클라우드별 조회용 자격증명을 통합계정으로 등록

**2 자산 수집**
등록 계정의 자원 목록과 설정 조회

**3 형상 점검**
자원 유형별 점검 항목 적용, 자원별 Pass/Fail 판정

**4 표준 매핑**
팩에 할당된 점검 항목 기준으로 결과 집계

**5 결과 확인**
준수 현황 조회, 목록 Excel 내보내기




[컴플라이언스 항목 관리]: 점검 항목 목록, 검색과 엑셀 다운로드(일부 정보 가림 처리)

## CNAPP과의 관계

| FRIIM CSPM | FRIIM CNAPP |
|---|---|
| 형상 점검과 표준 대응 중심의 구성 | 계정·자산·점검·결재·보고를 포함한 통합 구성 |
| 설정 점검과 심사 증적이 주된 목적인 조직 | 다수 클라우드와 계정을 통합 운영하는 조직 |

## 추가적으로 확인해야 되는 부분

- **점검 주기:** 수집·점검 실행 주기와 운영 시간대 협의
- **점검 범위:** OCI, OpenShift, Tanzu, Kubernetes 환경은 점검 범위 사전 확인

**상세 자료:** FRIIM CSPM 소개서(8쪽) · seekerslab.com/ko/products/cspm

25 · CRUX

# Crux ①: 개요와 구조

기존 규칙 엔진이 판단하지 못한 건만 받아 AI로 판정하고, 판정 근거와 확신도를 반환하는 판정 API

**대상**
승인, 심사, 분류 업무를 규칙 엔진으로 운영하는 기업의 개발 책임자와 아키텍트

**도입 방식**
프로젝트형. 업무 영역 1곳의 PoC 이후 단계적 확대, 파트너가 연동 구축

**제품 성격**
AI 개발 제품이며 보안 제품이 아님

## 대응 과제

- **예외 건 누적:** 규칙에 일치하지 않는 건이 담당자 수작업으로 누적
- **규칙 추가의 부담:** 예외마다 규칙을 추가하면 규칙 수와 충돌 증가
- **엔진 유지 요구:** 운영 중인 규칙 엔진의 교체 없이 예외 처리만 보완하려는 요구

## 구조

1 **기존 규칙 엔진** — 정의된 조건은 기존대로 처리 ›
2 **else 분기** — 일치 규칙이 없는 건만 전달 ›
3 **Crux 판정 API** — 건 정보와 맥락 수신 ›
4 **판정 방식 적용** — RULE, AGENT, HYBRID ›
5 **결과 반환** — 판정, 확신도, 근거 ›
6 **후속 처리** — 자동 반영 또는 검토 대기열

## 판정 방식 3종

| 방식 | 적용 대상 | 처리 |
|---|---|---|
| **RULE** | 결정론적 조건으로 표현되는 건 | 위임받은 판정 기준을 조건으로 적용 |
| **AGENT** | 맥락 판단이 필요한 건 | 건 정보와 맥락을 바탕으로 모델이 판정 |
| **HYBRID** | 두 방식의 경계에 있는 건 | 조건 적용과 맥락 판단 병행 |

## 확신도에 따른 분기

| 확신도 높음 | 확신도 낮음 |
|---|---|
| 판정 즉시 반환 | 검토 대기열로 전달 |
| 고객 시스템이 결과를 후속 절차에 반영 | 담당자가 근거 확인 후 최종 판단 |
| 판정과 근거 기록 | 판단 결과 기록 |

**기준:** 본 쪽의 기능 설명은 제품 설계 기준이며 측정 결과가 아님

26 · CRUX

# Crux ②: 주요 기능과 도입

## 주요 기능

**간편 연동**
기존 규칙 엔진 교체 없이 `else` 분기에 API 호출 추가. 규칙 이관과 데이터 이전 없음

**확신도 기반 검토 전달**
판정, 확신도, 근거 반환. 확신도가 낮은 건은 사람 검토 대기열로 전달

**규칙 제안과 승인**
판정 이력이 누적되면 AI가 규칙 전환 제안. 사람이 승인한 제안만 반영

**모델 선택**
고객 지정 모델 연결이 기본. 별도 모델 계약이 없는 경우 관리형 모델 선택

## 운영 콘솔 구성

| 구성 | 용도 |
|---|---|
| **규칙 카탈로그** | 고객사가 위임한 건 유형과 판정 기준 관리 |
| **AI 추천 대기열** | 규칙 전환 제안을 근거와 함께 검토, 승인·반려 |
| **감사 로그** | 판정 실행과 승인·반려 이력 추적 |

## 적용 업무 예시

| 업무 영역 | 규칙이 판단하지 못하는 건의 예 |
|---|---|
| **ERP·재무 승인** | 전표·지출 승인 예외, 승인 권한 대리 위임 |
| **구매·운영** | 규정에 정의되지 않은 발주, 운영 중 예외 요청 |

## 도입 3단계

**1 업무 영역 선정**
`else` 분기 건이 많고 업무 가치가 높은 영역 1곳 선정

**2 PoC 연동**
해당 영역 규칙 엔진의 `else` 분기에 판정 API 연결, 소수의 건으로 검증

**3 검증 후 확대**
판정 결과와 승인 이력을 근거로 다음 영역으로 확대

## 추가적으로 확인해야 되는 부분

- ☑ **자동 반영 범위:** 자동 반영을 허용할 판정과 반드시 사람이 결정할 판정의 구분
- ☑ **모델:** 고객 지정 모델과 관리형 모델 중 선택, 판정 데이터의 전달 대상 확인

**상세 자료:** Crux 소개서(12쪽) · seekerslab.com/ko/products/crux

27 · 서비스

# 서비스 ①: MDR·보안관제

로그 수집부터 탐지, 분석, 대응까지의 관제 체계 제공. 구독형 플랫폼과 구축형 중 선택

## 관제 수행 순서

1 **수집**
로그 수집, 이벤트 집계

› 2 **분석**
AI 1차 분류, 규칙 대조

› 3 **검증**
담당자 판정, 영향도 평가

› 4 **대응**
차단 조치, 복구 지원

## 관제 대상 영역

**네트워크**
방화벽, 침입 탐지 장비 등 네트워크 보안 장비 로그

**엔드포인트**
서버와 PC의 운영체제, 보안 에이전트 로그

**클라우드**
클라우드 계정의 감사 로그, 설정 변경 이력

**애플리케이션**
웹 서버, 업무 시스템 로그

## 제공 형태

| 형태 | 내용 | 적합 대상 |
|---|---|---|
| **구독형 플랫폼** | KYRA MDR 가입 후 수집기 설치, 플랜별 기능 제공 | 전담 인력이 없는 중소·중견기업 |
| **구축형 관제** | Seekurity SIEM 구축 후 고객 관제 조직 운영 | 자체 관제 조직 보유 기관, 폐쇄망 |
| **관제 지원** | 씨커스랩의 기술지원과 분석 지원 | 범위와 조건은 플랜 및 계약 기준 |

## 역할 구분

| 구분 | AI | 고객 담당자 | 씨커스랩 |
|---|---|---|---|
| **경보 분류** | 1차 분류, 신뢰도, 근거 요약 | 정탐·오탐 최종 판정 | 탐지 기능 제공 |
| **사고 대응** | 플레이북 실행 | 조치 승인, 내부 조치 | 플랜·계약 범위 내 기술지원 |
| **보고** | 보고서 생성 | 검토 및 내부 보고 | 플랫폼 운영 |

**확인 사항:** 관제 시간대, 대응 범위, 서비스 수준은 플랜과 계약에 따라 상이. 상담 시 요구 수준 제시 필요

28 · 서비스

# 서비스 ②: 클라우드 보안 진단 및 전환

## 클라우드 보안 진단

클라우드 환경의 보안 현황 진단과 개선 방안 제시

**보안 설정 점검**
IAM 정책, 네트워크 보안 그룹, 암호화 설정, 로깅 설정 등 핵심 보안 요소 검토

**취약점 분석**
인프라, 컨테이너, 애플리케이션 취약점과 구성 오류를 자동화 도구와 수동 점검으로 식별

**컴플라이언스 점검**
ISO 27001, SOC 2, GDPR, 개인정보보호법 등 규정 준수 현황 확인

**위험 평가**
식별된 위험의 위험도·영향도 평가, 우선순위와 개선 로드맵 제시

- **대상 환경:** AWS, Azure, GCP 등 멀티클라우드
- **산출물:** 위험도별 발견 사항 목록, 단계별 개선 로드맵
- **후속 연계:** 진단 이후 FRIIM을 이용한 상시 점검 전환 가능

## 클라우드 전환

온프레미스 시스템의 클라우드 전환 설계와 이행

1 **현황 분석** — IT 자산 및 환경 분석 › 2 **전략 수립** — 전환 전략과 로드맵 › 3 **PoC 수행** — 시범 전환 검증 › 4 **본 전환** — 단계별 클라우드 전환 › 5 **안정화** — 운영 안정화

## 플랫폼 엔지니어링 및 마이크로서비스 전환

| 서비스 | 내용 |
|---|---|
| **클라우드 플랫폼** | 클라우드 네이티브 아키텍처 설계 |
| **컨테이너 플랫폼** | 쿠버네티스 기반 컨테이너 플랫폼 구성 |
| **CI/CD 파이프라인** | 빌드·배포 자동화 구성 |
| **IaC 구현** | 인프라 구성의 코드화 |
| **마이크로서비스 전환** | 서비스 경계 정의, 단계별 전환, API Gateway·Service Mesh 구성 |

**기간 및 비용:** 대상 시스템 규모에 따라 상이하므로 현황 분석 이후 산정

29 · 서비스

# 서비스 ③: 보안 SI, 개발 SI, OEM/ODM

## 보안 SI

보안 솔루션 구축과 보안 시스템 통합

**1 보안 요구사항 분석**
대상 시스템, 규제 요구, 기존 보안 체계 확인

**2 설계**
보안 아키텍처와 연동 구조 설계

**3 개발 및 구축**
솔루션 설치, 연동 개발, 정책 설정

**4 안정화**
시험 운영, 운영 이관, 관리자 교육

- **수행 범위:** 자사 제품(SIEM, Guardrail, FRIIM) 구축과 고객 맞춤형 보안 시스템 개발
- **협업 방식:** 단계별 고객 협의와 검수

## 개발 SI

| 단계 | 내용 |
|---|---|
| **요구사항 정의** | 업무 요구와 기존 시스템 인터페이스 분석 |
| **아키텍처 설계** | 통합 아키텍처와 데이터 매핑 규칙 정의 |
| **개발 및 테스트** | 통합 레이어 개발, 단계별 테스트 |
| **배포 및 안정화** | 단계적 전환 |
| **운영 지원** | 운영 이관 이후 기술 지원 |

## OEM/ODM 기술 공급

**OEM (기술 라이선싱)**
자사 제품 기술의 라이선스 공급

**ODM (맞춤형 개발)**
파트너 요구 사양에 따른 맞춤 개발

**White Label**
파트너 브랜드로의 제품 공급

**기술 컨설팅**
제품 기획과 통합에 대한 기술 자문

- **진행 절차:** 초기 상담, 계약 체결, 개발·통합, 출시 준비, 지속 지원 순
- **대상 기술:** SIEM, CSPM, CNAPP, AI 에이전트 등 자사 보유 기술
- **조건:** 라이선스 조건과 지원 범위는 계약 기준

30 · 산업별

# 산업별 안내 ①: 금융

아래 내용은 금융권의 일반적 과제를 정리한 것이며 특정 기관의 사례가 아님

## 일반적 과제

**망분리 환경의 AI 도입**
내부망 업무에 생성형 AI 적용 시 모델 위치, 입력 정보 통제, 사용 기록 확보 필요

**감사 증적**
접근 기록과 로그의 장기 보관, 무결성 입증 요구

**클라우드 이용 확대**
클라우드 이용 시 설정 점검과 규제 기준 대응 필요

**예외 업무 처리**
심사, 분류, 승인 업무에서 룰로 처리되지 않는 예외 건의 수작업 누적

## 과제별 검토 제품

| 과제 | 제품 | 확인 포인트 |
|---|---|---|
| **내부망 AI 통제** | KYRA AI Guardrail | 폐쇄망 구성(사내 모델 연결), 민감정보 차단·마스킹, 해시 체인 감사 로그 |
| **내부 문서 질의응답** | KYRA RAG | 문서 등급별 열람 권한, 원본 시스템 권한 동기화 |
| **로그 통합과 증적** | Seekurity SIEM | 폐쇄망 구축, 로그 보관과 무결성 점검 |
| **클라우드 설정 점검** | FRIIM CNAPP | 대상 클라우드, 표준 팩 9종, 구축형 설치 |
| **예외 업무 자동 판정** | Crux | 기존 룰 엔진 유지, 낮은 신뢰도 건의 담당자 검토 |

## 도입 검토 순서 (권장 예시)

1. **규제·내규 확인**
   적용 규정과 내부 통제 기준에서 AI·클라우드 관련 요구 사항 정리
2. **대상 업무 선정**
   내부망 AI 적용 업무와 보호 대상 정보 유형 선정
3. **구성 검토**
   모델 위치, 연동 시스템(인증, 관제), 로그 보관 기준 검토
4. **시범 운영**
   제한된 부서 대상 기록 위주 운영 후 차단 기준 확정

**추가적으로 확인해야 되는 부분:** 적용 규정의 해석과 감독 기관 보고 요건은 기관의 준법 부서 확인 필요. 본 카탈로그는 규제 준수를 보증하지 않음

31 · 산업별

# 산업별 안내 ②: 공공

아래 내용은 공공 부문의 일반적 과제를 정리한 것이며 특정 기관의 사례가 아님

## 일반적 과제

**망분리와 구축형 요구**
외부 연결이 제한된 환경에서의 설치·운영 요구

**등급 문서 관리**
비밀, 대외비, 취급주의 등 보안 등급 표시 문서의 AI 입력 통제 필요

**감사 대응**
사용 기록의 장기 보관과 변조 방지 요구

**자산 현황 관리**
자산 대장과 실제 자산의 불일치, 정기 재물조사 부담

## 과제별 검토 제품

| 과제 | 제품 | 확인 포인트 |
|---|---|---|
| **내부 AI 서비스 통제** | KYRA AI Guardrail | 보안 등급 표시(I·II·III급 비밀, 대외비) 차단 규칙, 폐쇄망 구성 |
| **비인가 AI 사용 관리** | KYRA AI PC | 브라우저 확장 정책 일괄 설치, 서비스별 허용·경고·차단 |
| **로그 통합 분석** | Seekurity SIEM | 구축형, 장비 로그 수집과 탐지 규칙 |
| **자산 관리** | Seekurity Asset Management | 자산 탐지와 대장 대조, 수명주기 이력 |

## 조달 및 도입 시 확인 사항

- [x] 도입 형태(구축형) 및 설치 환경(폐쇄망 여부, 서버 준비 주체) 확인
- [x] 기관 보안 지침상의 인증·검증 요구 사항 확인 및 해당 여부 사전 문의
- [x] 사내 모델 구동 서버(GPU 포함) 준비 계획 확인
- [x] 관리 콘솔 언어 확인(KYRA AI Guardrail 관리 콘솔은 영문)
- [x] 로그 보관 기간과 저장 용량 기준 확인

**추가적으로 확인해야 되는 부분:** 제품별 인증 보유 현황과 조달 등록 여부는 시점에 따라 변동 가능하므로 도입 검토 시 문의 필요

32 · 산업별

# 산업별 안내 ③: 제조

아래 내용은 제조업의 일반적 과제를 정리한 것이며 특정 기업의 사례가 아님

## 일반적 과제

**설계·기술 자료 보호**
도면, 공정 자료, 프로젝트 코드명의 외부 AI 서비스 입력 우려

**다수 사업장**
본사와 공장별로 분산된 시스템과 자산의 현황 파악 곤란

**제한된 보안 인력**
IT 담당자의 보안 겸직, 야간·휴일 경보 대응 곤란

**협력사 접점**
협력사와의 자료 교환 과정에서의 정보 관리

## 과제별 검토 제품

| 과제 | 제품 | 확인 포인트 |
|---|---|---|
| **기술 자료의 AI 입력 통제** | KYRA AI Guardrail | 프로젝트 코드명 등 사용자 정의 규칙(정규식, 키워드) |
| **외부 AI 서비스 사용 관리** | KYRA AI PC | 사용자별·앱별 사용 현황, 서비스별 정책 |
| **관제 시작** | KYRA MDR | 구독형, 수집기 설치 후 탐지 시작 |
| **자산 현황 관리** | Seekurity Asset Management | 네트워크 내 자산 탐지, 대장 대조 |
| **사내 기술 문서 검색** | KYRA RAG | 문서 등급과 부서 단위 컬렉션 |

## 단계적 도입 예시

1 **현황 파악**
외부 AI 사용 현황, 자산 현황

› 2 **관제 시작**
KYRA MDR

› 3 **AI 사용 통제**
Guardrail, 사용자 정의 규칙

› 4 **사내 AI 확대**
RAG, 에이전트

- **출발점:** 현황 파악이 선행 과제, 사용 현황 자료를 근거로 정책 수준 결정
- **사용자 정의 규칙:** 기관 고유 코드명과 키워드는 도입 단계에서 등록

**추가적으로 확인해야 되는 부분:** 생산 설비망(OT) 대상 탐지는 본 카탈로그 수록 범위 외. 설비망 요구 사항은 상담 시 별도 확인

33 · 산업별

# 산업별 안내 ④: 중견·중소기업

## 일반적 과제

**전담 인력 부재**
IT 담당자 1명이 보안 겸직, 관제 조직 구성 곤란

**인증 심사 준비**
ISMS-P 등 심사에서 로그 관리와 탐지·대응 체계 증적 요구

**예산 제약**
구축형 장비와 운영 인력 확보 부담

**AI 사용 확산**
직원의 외부 AI 서비스 사용 증가, 현황 미파악

## 권장 출발점: KYRA MDR

- **시작 방식:** kyramdr.com 가입, 수집기 설치 후 탐지 시작
- **무료 플랜:** FREE 플랜 보유, 유료 플랜은 공개 가격(12쪽)
- **구성:** SIEM, NDR, EASM, SOAR 결합 플랫폼
- **분석 지원:** AI 기반 경보 1차 분류와 근거 요약, 최종 판정은 담당자 수행

## 단계별 확장 예시

| 단계 | 과제 | 제품 |
|---|---|---|
| 1 | 로그 수집과 탐지 시작 | KYRA MDR FREE |
| 2 | 심사 대응용 보고서와 대응 체계 | KYRA MDR 유료 플랜 |
| 3 | 직원 AI 사용 현황 파악 | KYRA AI PC |
| 4 | 사내 AI 서비스 개방 | KYRA AI Guardrail |
| 5 | 클라우드 계정 점검 | FRIIM CSPM |

## 사전 준비 사항

- [x] 수집 대상 서버와 장비 목록, 로그 발생량 추정
- [x] 외부 전송 가능 여부(수집기의 외부 통신 허용) 확인
- [x] 야간·휴일 경보 수신 담당자 지정
- [x] 인증 심사 일정과 요구 증적 목록 정리

**추가적으로 확인해야 되는 부분:** 플랜별 기능 범위와 로그 보관 기간은 kyramdr.com 게시 기준 확인. 정부 지원 사업 연계 여부는 해당 사업 공고 기준으로 고객 직접 확인 필요

34 · 도입 및 지원

# 도입 및 지원 ①: 도입 절차

## 공통 도입 절차

**1 상담**
현황과 과제 청취, 적합 제품과 도입 순서 협의

**2 시연**
제품 시연, 고객 환경 기준 질의응답

**3 PoC**
범위와 성공 기준 합의 후 고객 환경 또는 시험 환경에서 검증

**4 계약**
구성, 가격, 지원 범위 확정

**5 구축**
설치, 연동, 정책 설정

**6 운영 이관**
관리자 교육, 운영 자료 제공

## 제품 유형별 차이

| 유형 | 해당 제품 | 도입 특징 |
|---|---|---|
| **구독형** | KYRA MDR | 가입 후 수집기 설치로 시작, 무료 플랜으로 사전 확인 |
| **구축형** | Guardrail, RAG, Agent Package, SIEM, Asset Management | 고객 환경 설치, 서버 사양은 요구사항 확인 단계에서 산정 |
| **구축형 (클라우드 연결)** | FRIIM CNAPP, CSPM | 고객 인프라 설치, 클라우드별 조회용 자격증명 준비 |
| **프로젝트형** | Crux | 기존 룰 엔진 분석과 판정 기준 합의가 선행 |

## PoC 준비 자료

- [x] 대상 시스템과 범위(부서, 계정, 장비)
- [x] 성공 기준: 확인할 시나리오 목록과 통과 조건
- [x] 시험 계정, 시험용 데이터(실제 개인정보 사용 금지)
- [x] 연동 대상 정보: 인증 시스템, 관제 시스템, 모델 접속 정보
- [x] 고객 측 담당자와 일정

> **PoC 원칙:** 성능과 효과는 고객 환경에서 직접 측정한 결과로 판단. 사전 수치 약속 미제공

35 · 도입 및 지원

# 도입 및 지원 ②: 지원 체계

## 지원 범위

| 구분 | 내용 |
|---|---|
| **설치 및 연동** | 제품 설치, 인증·관제 시스템 연동, 초기 정책 설정 |
| **교육** | 관리자 교육, 운영 자료 제공 |
| **기술 지원** | 운영 중 문의 대응, 장애 지원 |
| **업데이트** | 제품 업데이트, 탐지 규칙 갱신 |

- **지원 수준:** 응답 시간과 지원 시간대는 계약 기준
- **파트너 경유 고객:** 1차 문의는 파트너, 2차 기술 지원은 씨커스랩

## 제품별 제공 자료

| 제품 | 공개 자료 | 계약 후 제공 자료 |
|---|---|---|
| **KYRA AI Guardrail** | 제품소개서 | 구축·운영 가이드 |
| **KYRA MDR** | 제품소개서, kyramdr.com 문서 | 콘솔 사용자 매뉴얼 |
| **Seekurity SIEM** | 제품소개서 | 사용자 매뉴얼, 구축 가이드 |
| **Seekurity Asset Management** | 제품소개서 | 사용자 가이드 |
| **FRIIM CNAPP** | 제품소개서 | 운영 자료 |
| **Crux** | 소개서 | API 가이드 |

## 문의 전 정리 사항

- [x] 검토 중인 제품 또는 당면 과제
- [x] 망 환경(인터넷 연결, 폐쇄망)과 운영 환경(온프레미스, 클라우드)
- [x] 사용자 또는 대상 장비 규모
- [x] 연동 대상 시스템(통합 인증, 기존 관제)
- [x] 희망 일정(심사 일정, 서비스 개시 일정)

## 문의 창구

**이메일**
contact@seekerslab.com

**전화**
02-2039-8160

**온라인 문의**
seekerslab.com/ko/company/contact

**KYRA MDR 가입**
kyramdr.com

36 · 자료

# 자료 목록

제품별 상세 자료. 공개 자료는 웹사이트 각 제품 페이지에서 제공

| 제품 | 자료 | 제공 구분 |
|---|---|---|
| **KYRA AI Guardrail** | 제품소개서 | 공개 |
| **KYRA AI Guardrail** | 구축·운영 가이드 | 파트너, 계약 고객 |
| **KYRA MDR** | 제품소개서 | 공개 |
| **KYRA MDR** | 콘솔 사용자 매뉴얼 | 가입 고객 |
| **KYRA AI Agent Package** | 제품소개서 | 공개 |
| **KYRA RAG** | 제품소개서 | 공개 |
| **KYRA AI PC** | 소개서 | 공개 |
| **Seekurity SIEM** | 제품소개서 | 공개 |
| **Seekurity SIEM** | 사용자 매뉴얼 | 계약 고객 |
| **Seekurity Asset Management** | 제품소개서 | 공개 |
| **FRIIM CNAPP** | 제품소개서 | 공개 |
| **FRIIM CSPM** | 소개서 | 공개 |
| **Crux** | 소개서 | 공개 |
| **전 제품** | 제품소개서(파트너용) | 파트너 |

## 제품 페이지

| 제품군 | 주소 |
|---|---|
| **KYRA AI Guardrail** | seekerslab.com/ko/ai/guardrail |
| **KYRA MDR** | kyramdr.com |
| **Seekurity SIEM** | seekerslab.com/ko/products/siem |
| **Seekurity Asset Management** | seekerslab.com/ko/products/asset-management |
| **FRIIM CNAPP** | seekerslab.com/ko/products/cnapp |
| **Crux** | seekerslab.com/ko/products/crux |

> **자료 요청:** 파트너용 자료와 계약 고객용 자료는 contact@seekerslab.com으로 요청

37 · 용어

# 용어 정리

| 용어 | 설명 |
|---|---|
| **가드레일** | 생성형 AI의 입력과 출력을 검사하여 정책에 따라 허용, 마스킹, 차단하는 통제 장치 |
| **프롬프트 인젝션** | AI에 전달되는 입력에 지시문을 숨겨 의도와 다른 동작을 유발하는 공격 |
| **마스킹** | 민감정보를 다른 표시로 치환하여 원본 값이 전달되지 않도록 하는 처리 |
| **RAG** | 사내 문서를 검색하여 그 내용을 근거로 AI가 답변을 생성하는 방식 |
| **AI 에이전트** | 답변 생성 외에 도구 호출, 조회, 발송 등 작업을 수행하는 AI |
| **Shadow AI** | 회사가 승인하지 않은 AI 서비스의 업무 사용 |
| **SIEM** | 여러 장비와 시스템의 로그를 수집하여 통합 분석하고 위협을 탐지하는 체계 |
| **SOAR** | 탐지 이후의 대응 절차를 플레이북으로 자동화하는 체계 |
| **MDR** | 탐지와 대응 체계를 서비스 형태로 제공받는 관리형 탐지·대응 |
| **NDR** | 네트워크 트래픽을 분석하여 위협을 탐지하는 체계 |
| **EASM** | 외부에서 확인되는 조직의 자산과 노출 지점을 점검하는 체계 |
| **CNAPP** | 클라우드 설정, 워크로드, 권한 보안을 통합 관리하는 플랫폼 범주 |
| **CSPM** | 클라우드 설정 오류와 기준 미준수를 점검하는 체계 |
| **ISMS-P** | 국내 정보보호 및 개인정보보호 관리체계 인증 |
| **폐쇄망** | 외부 인터넷과 연결되지 않은 내부 전용 네트워크 |
| **HITL** | 신뢰도가 낮은 AI 판정을 담당자가 검토하는 절차 |
| **BYOM** | 고객이 선택한 AI 모델을 연결하여 사용하는 방식 |
| **SSO** | 하나의 인증으로 여러 시스템에 로그인하는 통합 인증 |
| **Syslog** | 장비와 시스템의 이벤트를 전송하는 표준 로그 전송 방식 |

CONTACT

# 제품 상담 및 자료 요청

contact@seekerslab.com · 02-2039-8160
주식회사 씨커스 · 서울특별시 구로구 디지털로33길 28 우림이비지센터1차 (08377)

제품 페이지
**seekerslab.com/ko**

WEB
seekerslab.com

발행
2026. 11

구분
공개용

문서
제품 카탈로그