

보안 아키텍처 기술 개요

NxPortrait 보안 아키텍처

개발 · 검증 · 연동 · 보관 단계별 통제

기준일

2026. 10. 23.

발행

(주)엘로이큐브

보안성 인증

GS 인증 1등급 획득

인증번호 25-0021

문의

sales@eloicube.com

서울특별시 서초구

NxPortrait 보안 아키텍처 기술 개요

NxPortrait는 방화벽 정책을 수집·분석·적용하는 NSPM 솔루션입니다. 본 문서는 소스코드 개발, 배포 파이프라인 검증, 방화벽 연동, 데이터 암호화 각 단계에 적용된 DevSecOps 보안 통제를 기술합니다.

핵심 사양

항목	적용 내용
저장소 접근	ID·패스워드 + 2FA 필수
배포 검증	Semgrep · Artex · Trivy · FossLight 결과를 DefectDojo에서 통합 관리
방화벽 연동	Collector(Read) · Pylon(Write) 역할 및 구동 환경 분리
데이터 보호	접속 정보 AES-256 · 민감 정보 Salted Hash
보안성 인증	GS 인증 1등급 획득 (인증번호 25-0021)

문서 구성

구분	내용
01	소스코드 개발 보안: 저장소 접근 및 코드 반영 통제
02	소스코드 운영 보안: DefectDojo 기반 배포 파이프라인 검증
03	방화벽 수집·적용 아키텍처: 에이전트 분리 구조
04	통제된 플레이북: 수집·적용 통신 방식
05	주요 데이터 암호화 수준
06	단계별 통제 요약
07	보안 진단 도구 및 점검 기준 출처

저장소 접근 및 코드 반영 통제

저장소 접근, 코드 반영, 품질 검증, 접속 정보 관리 4개 항목에 통제를 적용해 소스코드의 **무결성**과 **기밀성**을 유지합니다.

통제 항목	내용	효과
코드 서버 2FA 인증	소스코드 저장소와 형상관리 서버 접근 시 아이디·패스워드에 더해 2단계 인증을 필수로 요구합니다.	계정 탈취로 인한 소스코드 유출과 변조를 차단합니다.
소스코드 무단 커밋 금지	승인되지 않은 작업자나 비정상 경로를 통한 Commit·Merge를 시스템 차원에서 막습니다.	백도어 삽입과 검증되지 않은 코드의 운영 유입을 방지합니다.
AI QC · Code Review 결과 강제 기록	반영 전 AI 기반 품질 관리와 동료 코드 리뷰를 의무화하고, 이력을 시스템에 영구 기록합니다.	취약점과 로직 오류를 조기에 발견하고 문제 발생 시 추적성을 확보합니다.
커넥션 문자열 암호화 관리	DB·외부 API 연결 정보를 소스코드에 평문으로 두지 않고 Vault 또는 암호화된 형태로 관리합니다.	소스코드가 유출되더라도 인프라 접근 권한은 탈취되지 않습니다.

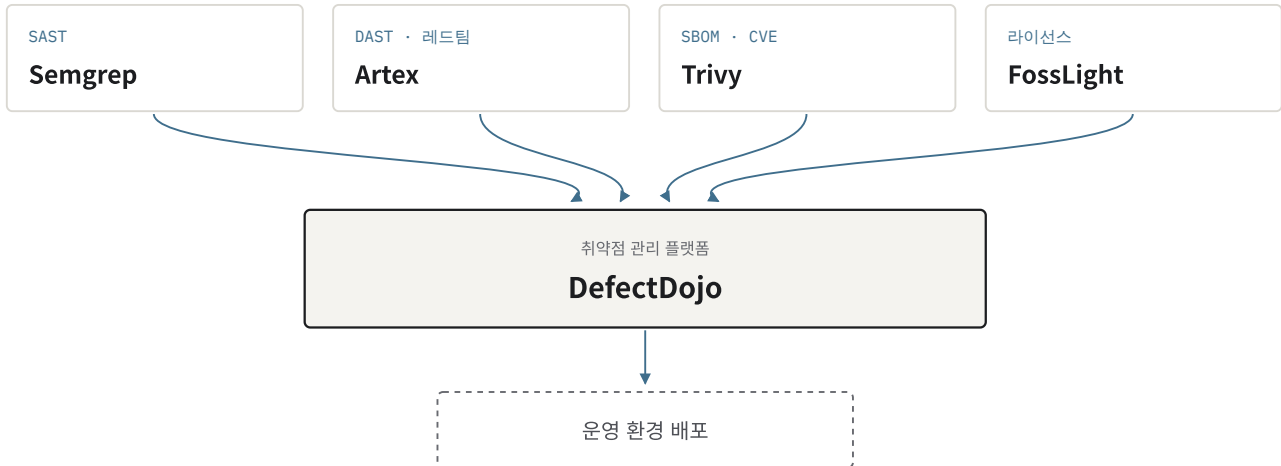
커밋 반영 절차

Commit부터 Merge까지 6단계 검증을 통과한 코드만 반영되며, AI QC·Code Review 이력은 시스템에 저장됩니다.



DefectDojo 기반 배포 파이프라인 검증

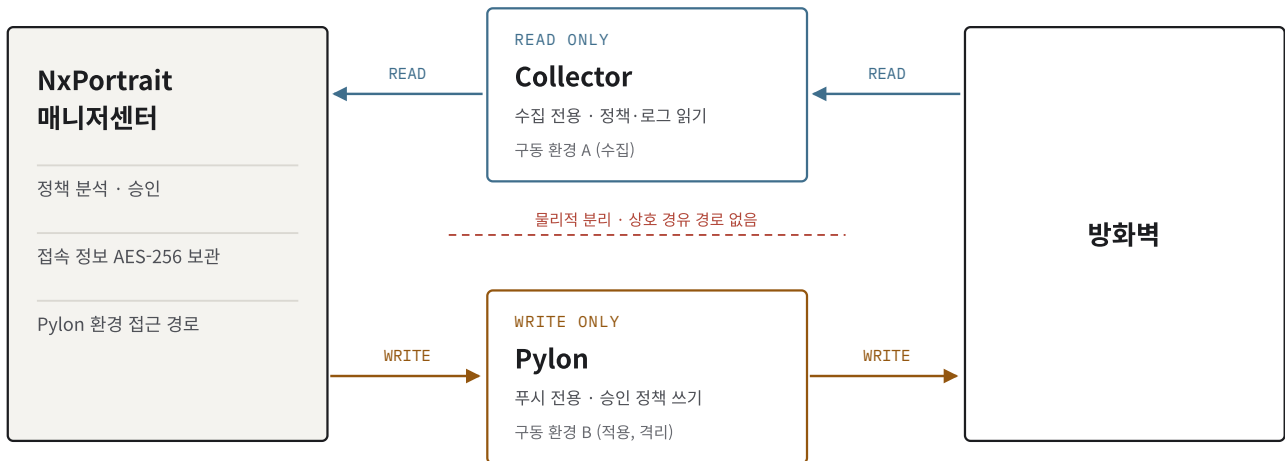
운영 배포 파이프라인의 SAST, DAST, SBOM/CVE, 라이선스 검증 결과를 취약점 관리 플랫폼 DefectDojo에서 통합 관리합니다.



도구	분류	분석 대상	탐지 항목	보안 효과
Semgrep	SAST · 정적 코드 분석	소스코드	SQL 인젝션, XSS 등 코드 수준 취약점	배포 전 코드 단계에서 취약점 식별
Artex	DAST · 동적 분석 / 모의해킹	실행 중인 애플리케이션	런타임 환경 취약점	정적 분석으로 확인할 수 없는 런타임 결함 검증
Trivy	SBOM · CVE 검증	SBOM 등재 오픈소스 라이브러리	알려진 취약점(CVE)	공급망 구성요소의 CVE 상시 모니터링
FossLight	SBOM · 라이선스 검증	오픈소스 구성요소	라이선스 준수 여부	배포 전 라이선스 위반 확인

수집·적용 에이전트 분리 구조

방화벽 연동은 읽기 전용 Collector와 쓰기 전용 Pylon으로 역할을 분리하고, 두 에이전트를 물리적으로 분리된 환경에서 구동합니다. **최소 권한 원칙(PoLP)**에 따라 단일 에이전트 탈취 시 영향 범위를 제한합니다.



경로	동작
수집 경로 (Read-only)	Collector가 방화벽 정책과 로그를 조회해 매니저센터로 전달합니다. 이 경로에는 쓰기 권한이 없습니다.
적용 경로 (Write-only)	승인된 정책은 매니저센터 → Pylon → 방화벽 순으로 적용됩니다. Pylon 구동 환경은 매니저센터 경유 접근만 허용합니다.
Collector 탈취 시	Collector 권한은 읽기로 한정되어 정책 변경이 불가능합니다. Pylon 환경과 물리적으로 분리되어 측면 이동 경로가 없으므로 무단 정책 배포로 이어지지 않습니다.

설계 원칙

원칙	구현
최소 권한 원칙	에이전트별로 읽기 또는 쓰기 권한 하나만 부여. 단일 에이전트 탈취 시 영향 범위 제한.
구동 환경 물리 분리	Collector와 Pylon은 물리적으로 분리된 환경에서 구동. 상호 경유 경로 없음.

원칙	구현
매니저센터 단일 진입점	Pylon 구동 환경은 매니저센터 경유 접근만 허용. 직접 접근 차단.
접속 정보 AES-256	방화벽 접속 정보 전체를 AES-256으로 암호화해 저장.

04 / 통제된 플레이북

수집·적용 플레이북 통신 방식

플레이북은 장비의 CLI/API 지원 여부에 따라 경로를 결정합니다. 수집은 **CLI 기본·API 폴백**, 적용은 **API 기본·CLI 폴백**(API 미지원 레거시 장비 한정)입니다.

정책	수행 에이전트	목적	기본 경로	폴백 경로
수집 정책	Collector	텍스트 기반 정밀 수집	CLI	API (CLI 미지원 장비)
적용 정책	Pylon	구조화된 데이터 전송	API	CLI (API 미제공 레거시 장비)

장비 유형별 경로 결정

장비 지원 방식	수집 경로	적용 경로
CLI · API 모두 지원	CLI (기본)	API (기본)
API만 지원	API (폴백)	API (기본)
CLI만 지원 (레거시)	CLI (기본)	CLI (폴백)

데이터 유형별 암호화 방식

복호화가 필요한 접속 정보는 AES-256, 복호화가 필요 없는 민감 정보는 Salted Hash로 처리합니다.

구분	방식	대상	복호화	특성
접속 정보	AES-256 (대칭키 암호화)	DB 패스워드, API 토큰, 방화벽 접속 정보 등 연동 시 복호화가 필요한 값	필요 시점에만 복호화	국제 표준 대칭키 알고리즘
민감 정보	Salted Hash (단방향 해시)	사용자 비밀번호, 주민등록번호 등 복호화가 필요 없는 값	불가 (단방향)	임의 Salt 추가 후 해시. 관리자도 원본 확인 불가

입력값이 같아도 salt가 다르면 해시값이 달라지므로, 사전 계산된 레인보우 테이블 공격이 적용되지 않습니다.

단계별 통제 요약

서비스 생애주기 각 단계에 적용된 통제와 대응 위협입니다.

단계	적용 통제	대응 위협 · 효과
개발	저장소 2FA, 무단 커밋 차단, AI QC · Code Review 이력 기록, 커넥션 문자열 암호화	계정 탈취, 백도어 삽입, 소스 유출을 통한 인프라 접근
운영	DefectDojo 중심 통합: Semgrep SAST, Artex DAST, Trivy CVE, FossLight 라이선스	코드·런타임 취약점, 오픈소스 CVE, 라이선스 위반
연동	Collector(읽기) / Pylon(쓰기) 역할·환경 분리, 매니저센터 단일 경유, 통제된 플레이북	단일 에이전트 탈취, 무단 정책 배포, 네트워크 마비
보관	접속 정보 AES-256, 민감 정보 Salted Hash	접속 정보 유출, 레인보우 테이블 공격, 내부자 원본 열람
인증	GS 인증 1등급 획득 (인증번호 25-0021)	제3자 시험 기반 품질·보안성 검증

보안 진단 도구 출처

배포 파이프라인과 레드팀 진단에 사용하는 보안 진단 도구, 그리고 준수하는 점검 기준의 개요와 공식 출처입니다.

도구	분류	개요	출처
DefectDojo	취약점 관리 플랫폼	OWASP 오픈소스 프로젝트. 보안 테스트 결과 수집, 중복 제거, 취약점 추적, 조치 및 보고를 단일 플랫폼에서 관리합니다.	OWASP 프로젝트 owasp.org/www-project-defectdojo/ GitHub github.com/DefectDojo/django-DefectDojo
Semgrep	SAST	소스코드를 실행하지 않고 취약점, 노출된 시크릿, 위험한 오픈소스 의존성을 탐지합니다. 오픈소스 Community Edition은 30개 이상 언어를 지원합니다.	공식 문서 docs.semgrep.dev
Artex	DAST · 레드팀	다중 AI 에이전트 기반 자율 모의해킹 도구. 실행 중인 애플리케이션을 대상으로 정찰, 취약점 탐지, 공격 경로 검증을 수행하며 레드팀 진단에 활용합니다.	공개 공식 출처 없음
Trivy	SBOM · CVE	Aqua Security의 오픈소스 보안 스캐너. 컨테이너 이미지, 파일시스템, 코드 저장소, SBOM을 대상으로 취약점(CVE), 설정 오류, 시크릿, 라이선스를 검사합니다.	공식 문서 trivy.dev/docs GitHub github.com/aquasecurity/trivy
FossLight	오픈소스 라이선스	LG전자가 공개한 오픈소스 컴플라이언스 도구. 소스 경로와 저장소를 분석해 오픈소스 구성요소와 라이선스 정보를 보고서로 출력합니다.	가이드 fosslight.org/fosslight-guide/scanner/ GitHub github.com/fosslight/fosslight_scanner
KISA CCE	점검 기준	한국인터넷진흥원(KISA) 「주요정보통신기반시설 기술적 취약점 분석·평가 방법 상세가이드」의 점검항목. NxPortrait의 점검 항목은 이 기준을 준수합니다.	KISA 가이드 자료실 www.kisa.or.kr/2060204