AI Inventory List

ASSET REGISTER | SD2 SUBMISSION

Summary of all internal AI models, automated systems, and digital assets — CyberPlug DevSecOps Security AI

1. Platform Core Assets

Auto-discovered and reconciled monthly. Classification by data sensitivity, exposure level, and business criticality.

Asset ID	Asset Name	Type	Criticality	Exposure	Data Sensitivity	Owner
CP-CORE-001	Scan Orchestration Engine	Microservice	**CRITICAL**	Internal	Security metadata	Eng. Lead
CP-CORE-002	AI Remediation Model	ML Service	**CRITICAL**	Internal	Vuln. findings	AI Lead
CP-CORE-003	Vulnerability Database	Data Store	**CRITICAL**	Internal	CVE data	Sec. Eng.
CP-CORE-004	Tenant API Gateway	API	**CRITICAL**	External	API metadata	Platform Ops
CP-CORE-005	Audit Log Service	Microservice	**HIGH**	Internal	Audit records	Compliance
CP-CORE-006	RBAC & IAM Module	Service	**HIGH**	Internal	Identity data	Sec. Eng.
CP-CORE-007	Customer Dashboard (UI)	Web App	**HIGH**	External	Tenant UI data	Product
CP-CORE-008	Notification & Alerting	Microservice	**MEDIUM**	Internal	Alert metadata	Platform Ops
CP-CORE-009	Report Generation Service	Microservice	**MEDIUM**	Internal	Report data	Eng. Lead
CP-CORE-010	CI/CD Integration Hooks	Integration	**HIGH**	Third-party	Build metadata	DevOps

2. Third-Party & Open-Source Dependencies

Component	Version	Purpose	Licence	Approval Status	Last Review
OWASP ZAP	2.14.x	Web app scanning engine	Apache 2.0	Approved	Q1 2026
Nuclei	3.x	Template-based vulnerability scanning	MIT	Approved	Q1 2026
Trivy	0.50.x	Container & IaC scanning	Apache 2.0	Approved	Q1 2026
NVD / CVE Feed	Live	Vulnerability intelligence	Public Domain	Continuous	Ongoing
OSV.dev Feed	Live	OSS package vuln. data	CC BY 4.0	Approved	Q1 2026
GitHub Advisory DB	Live	Code dependency advisories	CC BY 4.0	Approved	Q1 2026
PostgreSQL	16.x	Primary data store	PostgreSQL Licence	Approved	Q4 2025
Redis	7.x	Session & queue caching	BSD 3-Clause	Approved	Q4 2025
Kafka	3.7.x	Event streaming	Apache 2.0	Approved	Q1 2026

3. Inventory Management Controls

AUTO-DISCOVERY:	API gateway inspection, DNS enumeration, CI/CD pipeline integration
RECONCILIATION:	Full monthly reconciliation; immediate reconciliation post major deployment
CLASSIFICATION:	Each asset classified by data sensitivity (PII, payment data), exposure level, and business criticality
OWNERSHIP:	Every asset has a designated owner responsible for remediation decisions and escalation sign-off
TOTAL ASSETS:	10 platform core assets | 9 third-party dependencies | Continuous discovery active