Customer Disclosure Statement

B2C / USER FACING | ONBOARDING

User-facing copy explaining when AI is analysing your systems and your rights — CyberPlug DevSecOps Security AI

> *This statement is displayed to all users on first login and is accessible at any time via Settings > AI Transparency. CyberPlug uses artificial intelligence to identify security vulnerabilities in your code, APIs, and infrastructure faster and more thoroughly than manual review alone. Here is what that means for you.*

1. When AI Is Analysing Your Systems

CyberPlug's AI is active whenever you run or schedule a security scan. During a scan, the AI:

- Inspects your APIs, web application endpoints, and code dependencies for known and emerging vulnerabilities
- Compares detected patterns against vulnerability databases (CVE, OWASP, and CWE) to classify findings by type and severity
- Generates a written summary of each finding in plain language, explaining what was found and where
- Produces a recommended remediation action — a concrete, actionable fix — alongside a confidence indicator

You will see an **AI indicator badge** in the CyberPlug interface whenever you are viewing AI-generated content. This badge distinguishes AI-produced summaries and recommendations from raw scan output or human-authored guidance.

2. What AI Does Not Do

- CyberPlug AI does not automatically fix your code, modify your systems, or deploy changes on your behalf — unless you have explicitly enabled an automated remediation workflow.
- CyberPlug AI does not access, read, or transmit the actual source code of your application. It analyses observable behaviour, API responses, dependency manifests, and configuration metadata only.
- CyberPlug AI does not make final decisions about whether a vulnerability is real or critical. It provides recommendations. You and your team decide what action to take.

3. Understanding AI Confidence Levels

Confidence Level	What It Means	What Happens Next
HIGH	The AI has matched this finding to well-established vulnerability patterns with strong corroborating evidence	Recommendation displayed for your review; automated actions may proceed if configured
MEDIUM	The AI has identified a likely issue but contextual factors mean some uncertainty remains	Recommendation displayed with a note to verify context before acting
LOW	The AI has flagged a potential concern but cannot confirm it with high confidence	A qualified human reviewer is automatically assigned — no automated action is taken

4. Human-in-the-Loop: When a Human Reviews Before Action

A qualified human reviewer from your team will be assigned and must approve the action before CyberPlug proceeds in the following situations:

Situation	Why Human Review Applies	Who Reviews
Critical vulnerability (CVSS 9.0+)	Potential impact is too severe for automated response without human judgement	Security Engineer + Asset Owner

AI recommendation confidence rated Low	The AI itself is not sufficiently certain; human expertise required to validate	Security Engineer
Deployment block triggered	Preventing a deployment is a high-impact action requiring human authorisation	Asset Owner + Compliance Officer
Risk acceptance selected	Formally accepting a known risk requires documented human sign-off	Asset Owner (CISO countersigns for Critical)
Payment or authentication system scan	Highest regulatory exposure; any finding warrants direct human attention	Security Engineer + Compliance Officer

5. Your Rights

OVERRIDE: Override or dismiss any AI-generated recommendation with a documented reason at any time

EXPLANATION: Request a detailed explanation of why the AI produced a specific finding — provided within 5 business days

MANUAL MODE: Configure CyberPlug to operate in manual review mode — all recommendations require explicit human approval

DATA DELETION: Request deletion of all your data by contacting privacy@CyberPlug.cc — completed within 30 days

APPEAL: Raise any governance query via your Customer Success Manager or at compliance@CyberPlug.cc

6. Contact

Purpose	Contact
AI Transparency & Explanations	ai-governance@CyberPlug.cc
Data Privacy & Deletion	privacy@CyberPlug.cc
Platform Support (24/7)	support@CyberPlug.cc | In-app chat
Governance & Compliance	compliance@CyberPlug.cc