xygeni.

Your pipeline ships every release.
Who secures the pipeline?

Harden the path every release travels.

Xygeni CI/CD Security scans your pipeline definitions and the settings of the DevOps platforms themselves, enforces a secure baseline with guardrails, and fixes what it finds with AI.

OWASP CI/CD Top 10 risks covered by dedicated detectors, across GitHub, GitLab, Azure DevOps, Bitbucket, CircleCI and Jenkins.

xygeni.

THE PROBLEM

The pipeline is a production system. Most teams do not secure it like one.

Recent supply-chain attacks did not need a vulnerable application. A compromised third-party GitHub Action, a hijacked maintainer account or an over-permissioned workflow token was enough. The pipeline holds credentials, builds artifacts and pushes to production, yet its configuration is scattered across SCM and CI tools, with no single control plane and no posture an auditor can check.

Xygeni CI/CD Security reads both the pipeline as code and the platform settings, maps findings to the OWASP CI/CD Top 10, blocks risky changes before they merge and gives each finding a fix or a remediation guide.

FIVE QUESTIONS MOST TEAMS CANNOT ANSWER TODAY

Branches
Can anyone push to the delivery branch without review?

Identity
Which workflows still use long-lived tokens instead of OIDC?

Actions
Are third-party actions pinned, or do they follow a mutable tag?

Runners
Who can run code on our self-hosted runners?

Audit
Can we prove our pipeline posture to an auditor?

Two views

of every pipeline: the files in the repository and the platform's own organization, repository and branch settings.

Guardrails

that block risky changes in CI and pull requests, with posture against CIS, OpenSSF Scorecard and NIST.

AI

triage, explanation and a proposed change or remediation guide for every misconfiguration.

ONE PRODUCT, THREE STEPS

Detect. Enforce. Remediate.

DETECT

Code + platform

Pipeline files, build scripts and CI jobs, plus the organization, repository and branch settings of each platform.

→

ENFORCE

Guardrails + compliance

Guardrails fail builds and PR checks on risky changes. Posture measured against CIS, OpenSSF and OWASP.

→

REMEDIATE

AI + guided fixes

AI Triage and AI Explanation, plus a proposed change or a remediation guide in the Remediation View.

Detect every misconfiguration. Enforce the baseline. Remediate with AI.

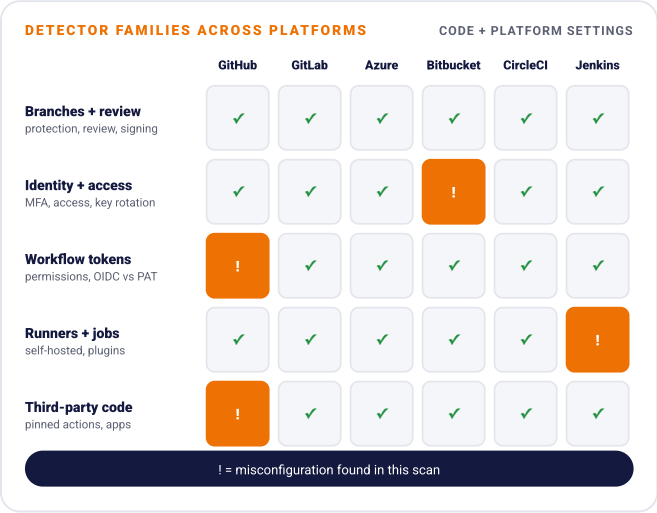
Without Xygeni	With Xygeni
Pipeline settings checked by hand, once	**Continuous scans of files and platform settings**
A different console per CI/CD tool	**Every CI/CD and SCM platform in one posture view**
No answer to "how do you secure your pipeline?"	**Posture mapped to OWASP CI/CD Top 10, CIS and OpenSSF**
A policy violation with no clear fix	**AI explanation, proposed change or remediation guide**

DETECT · COVERAGE

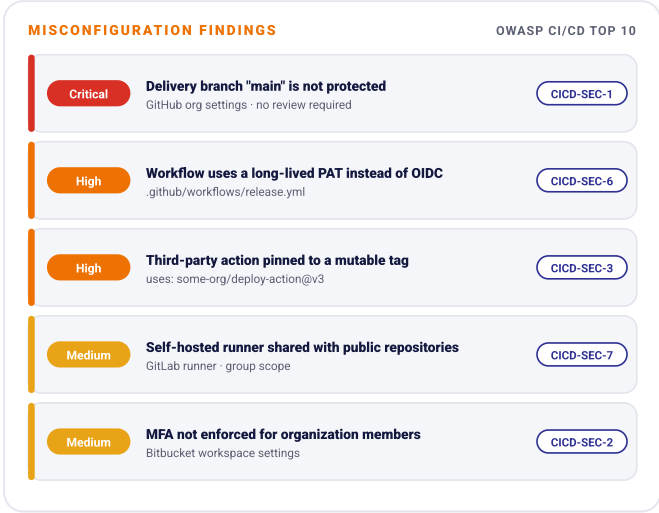
Find the misconfigurations that turn a pipeline into an attack path

Pipeline as code and the platforms' own settings, across your CI/CD and SCM platforms.

Xygeni detectors scan configuration files, build scripts and CI job definitions, and read the organization, repository and branch settings of each DevOps platform. They flag the deviations that enable supply-chain attacks: unprotected delivery branches, missing reviews and MFA, over-permissioned workflows, insecure runners and unpinned actions.



Schematic: detector families checked across the supported platforms.



Schematic: misconfiguration findings with their severity and OWASP CI/CD Top 10 category.

- **Branches and review:** unprotected delivery branches, missing code review and signed commits, insecure webhooks.
- **Workflow permissions:** over-permissioned jobs and tokens, and long-lived PATs where OIDC should be used.
- **Third-party code in CI:** unpinned actions, and installed apps and OAuth integrations as inventory risk.
- **Identity and access:** missing MFA, weak access control and password policies, keys that are never rotated.
- **Runners and jobs:** self-hosted runner posture, insecure CI jobs and risky plugins.
- **Data and transport:** public cloud storage, unencrypted data at rest, HTTPS for remote repositories, container practices in CI.

GitHub · GitLab · Azure DevOps · Bitbucket · CircleCI · Jenkins

Two views of the same pipeline. Detectors run over the files in the repository and over the platform's own settings, so a protection removed in the platform UI is visible, not only a workflow edited in code.

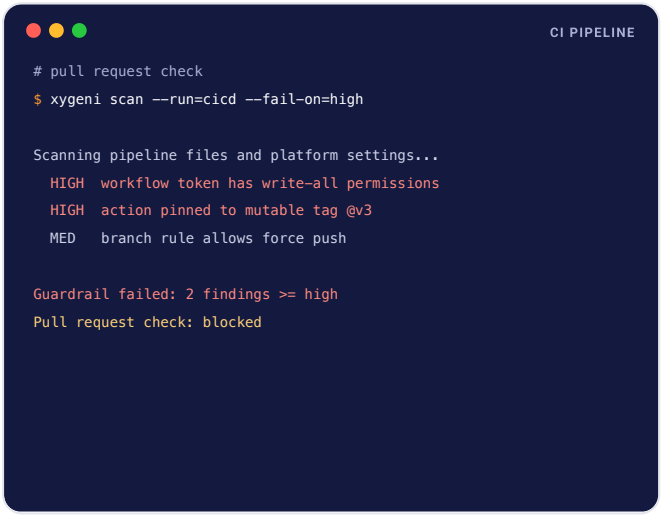
For the platform team: one posture view for every SCM and CI system you run.

ENFORCE · GUARDRAILS

Block risky pipeline changes before they merge

Guardrails, pull-request checks and compliance posture against the standards auditors ask for.

Guardrails turn the baseline into a gate: a scan in CI or a pull-request check fails when a change introduces a misconfiguration above your threshold. Compliance checkpoints measure each project against CIS Software Supply Chain Security, OpenSSF Scorecard, NIST and the OWASP CI/CD Top 10, with a compliance level per checkpoint.



Schematic: a guardrail blocks a pull request that introduces high-severity misconfigurations.



Schematic: compliance level per standard and per checkpoint for one project.

- **Guardrails:** fail on severity, with pull-request checks, status checks and commit comments on the SCM.
- **Compliance assessment:** automated audits with a compliance level per checkpoint.
- **Hardened bootstrap:** checksum-verified Xygeni action and GitLab component, pinned versions, signed installer.
- **Server-side audit:** audit a project from the platform, without changing its pipeline.
- **OWASP CI/CD Top 10 detectors:** runner posture, OIDC over PATs, ref-protection parity, third-party app inventory.
- **Incremental scanning:** faster scans that fit the pull-request rhythm.

OWASP CI/CD Top 10 | CIS Software Supply Chain | OpenSSF Scorecard | NIST SSDF | NIS2 | DORA | CRA

We run it on our own supply chain. Xygeni applies its OWASP CI/CD Top 10 detectors to its own organization, as auditable evidence of how it secures its own pipeline.

For the CISO: pipeline posture you can show to an auditor, not just describe.

REMEDIATE · AI

From a finding to a secure setting, with AI that explains why

AI Triage, AI Explanation, proposed changes and remediation guides in one workflow.

Every finding lands in the ASPM funnel with the rest of your application risk. AI Triage gives a verdict, an urgency and a complexity. AI Explanation describes what the misconfiguration lets an attacker do. Auto-fix proposes the change for configuration in code, or a step-by-step remediation guide for platform settings.



Schematic: AI Triage verdict, urgency and complexity on a workflow-permission finding.



Schematic: a proposed change that scopes workflow permissions and pins an action to a commit.

- **AI Triage:** verdict, remediation urgency and complexity per finding.
- **Auto-fix and guides:** a proposed change for configuration in code, a guide for platform settings.
- **Any LLM:** Xygeni's hosted model, your provider or a self-hosted model.
- **AI Explanation:** what the misconfiguration allows an attacker to do, in plain language.
- **Remediation View:** CI/CD fixes next to code, dependency and secrets fixes.
- **Into your workflow:** Jira, Slack and Teams, plus SARIF output.

Anomaly Detection

Detects suspicious activity and code tampering in SCM and CI/CD as it happens.

Build Security

Signs and verifies build provenance, so tampering after the build is caught.

Secrets Security

Finds hardcoded credentials in code and pipeline files, and blocks them.

For developers: a fix or a guide, not just a policy violation.

xygeni.

WHY XYGENI FOR CI/CD SECURITY

Detect every misconfiguration. Enforce the baseline. Remediate with AI.

Xygeni CI/CD Security treats the delivery pipeline as the production system it is: scanned in code and in platform settings, gated by guardrails and fixed with AI, in the same platform as the rest of your application risk.

Code and platform

Pipeline files and the platforms' own settings, across your CI/CD and SCM systems.

OWASP CI/CD Top 10

Dedicated detectors, applied by Xygeni to its own organization as evidence.

Gate, don't just report

Guardrails and pull-request checks stop risky changes before they merge.

AI on every finding

Triage, explanation and a proposed change or remediation guide.

Why security leaders choose Xygeni

Proven in production

Banco Serfinanza runs CI/CD Security on GitLab across 100+ repositories, with analysis on every commit and pull request.

One platform

Code, open source, secrets, IaC, pipelines, running apps and AI in one inventory, one risk model and one workflow.

Extend, don't replace

Xygeni's AI layer triages, explains and fixes findings from the security tools you already run.

Built for regulated environments

European vendor. SaaS, on-premise or air-gapped, with any LLM, including self-hosted models.

xygeni.

A delivery pipeline you can prove is secure

Detect. Enforce. Remediate. One platform.

Request a PoC | Book a demo

- SaaS, on-premise or air-gapped
- Your CI/CD and SCM platforms in one posture view
- xygeni.io

RECOGNIZED IN 2026

Hot Company in Application Security Posture Management 2026
Global InfoSec Awards · Cyber Defense Magazine

Some capabilities are in active development and may not be generally available yet; features and timelines are subject to change.

© 2026 Xygeni Security SL.
All rights reserved.