xygeni.

# Your SCM logs every change. Nobody is watching.

*Catch a supply-chain breach while it is happening.*

**Xygeni Anomaly Detection monitors activity across your SCM and CI/CD platforms, detects tampering with critical files, and alerts your team in real time with the context to act.**

**Real time** detection of suspicious activity and code tampering across GitHub, GitLab, Bitbucket, Azure DevOps and Jenkins.

xygeni.

THE PROBLEM

# A stolen token does not trigger a vulnerability scanner.

When an attacker gets a maintainer account, a token or a CI job, they do not need a vulnerability. They clone a repository from an unusual location, remove a branch protection, merge around a review or change a build script, and every step looks like normal work. SCM and CI platforms record it, but raw audit logs are rarely monitored, correlated or tied to the code that changed.

Xygeni Anomaly Detection watches that activity continuously, protects the files that must not change outside a procedure, flags drift between repository, build and production, and raises an alert with the full context the moment it happens.

## FIVE QUESTIONS MOST TEAMS CANNOT ANSWER TODAY

**Access**
Who cloned this repository, and from where?

**Protections**
Would we notice a branch protection being deleted?

**Reviews**
Which merges bypassed review or failed checks?

**Critical files**
Who changed this workflow or CODEOWNERS file?

**Drift**
Does production still match what is in the repository?

### Context
in every alert: who, what, where and when, by email, webhook, Slack or Teams.

### Every level
organization, repository, branch and Jenkins activity, plus custom rulesets.

### Air-gapped
Code Tamper scanning also runs in disconnected environments.

ONE PRODUCT, THREE STEPS

# Monitor. Detect. Respond.

MONITOR
### Sensors
Sensors stream activity from GitHub, including its audit log, GitLab, Bitbucket, Azure DevOps and Jenkins.

→

DETECT
### Anomalies + tampering
Behaviour detectors, custom rules, Code Tamper on critical files and drift across the pipeline.

→

RESPOND
### Alerts + audit trail
Real-time alerts with context, Shield correlation and findings in the ASPM audit trail.

**Monitor every change. Detect what is not normal. Respond in real time.**

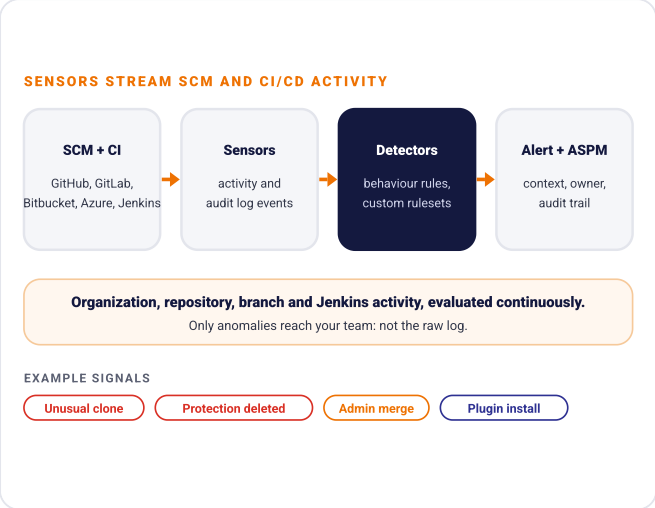
| Without Xygeni | With Xygeni |
|---|---|
| Raw audit logs nobody monitors | **Continuous detection of suspicious activity** |
| Critical files change silently | **Tampering detected, with commit and file detail** |
| Drift found during an incident | **Repository, build and production compared** |
| Alerts without context | **Who, what, where and when in every alert** |

MONITOR · SENSORS

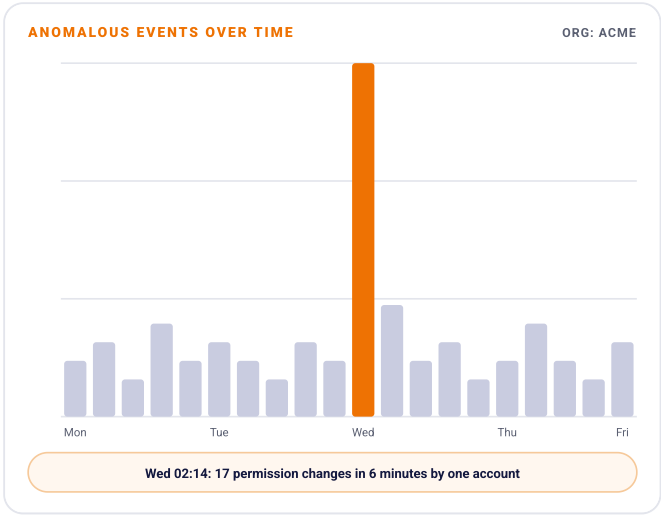
# See every change to your source code and pipelines, as it happens

## Sensors across your SCM and CI/CD platforms, from the organization down to the branch.

Xygeni Sensors ingest activity from GitHub, including audit log processing, GitLab, Bitbucket, Azure DevOps and Jenkins. Detectors evaluate that stream against what normal looks like for your organization, at every level that matters: organization, repository, branch and build.




Schematic: sensors stream SCM and CI/CD activity into the detectors and the ASPM.




Schematic: anomalous events over time, with a burst of permission changes flagged.

- **Organization:** configuration, compliance framework and admin-privilege changes.
- **Branch:** commits that bypass protections, and changes to branch settings.
- **Behavioural signals:** clones from unusual users or locations, rapid permission churn, admin merges around review.
- **Repository:** anomalous merges, deletions and permission changes.
- **Jenkins:** suspicious logins, unusual plugin installs and build-duration anomalies.
- **Custom rulesets:** tune sensitivity and scope to your organization's risk profile.

GitHub · GitLab · Bitbucket · Azure DevOps · Jenkins

**Detection, not log archaeology.** The platform records the event. Xygeni decides whether it is anomalous, and tells you while it still matters.

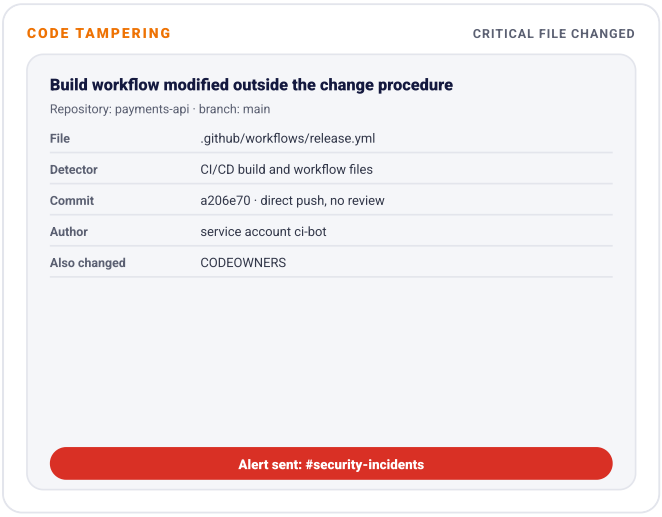
**For security operations: curated supply-chain anomalies instead of raw platform logs.**

DETECT · CODE TAMPERING

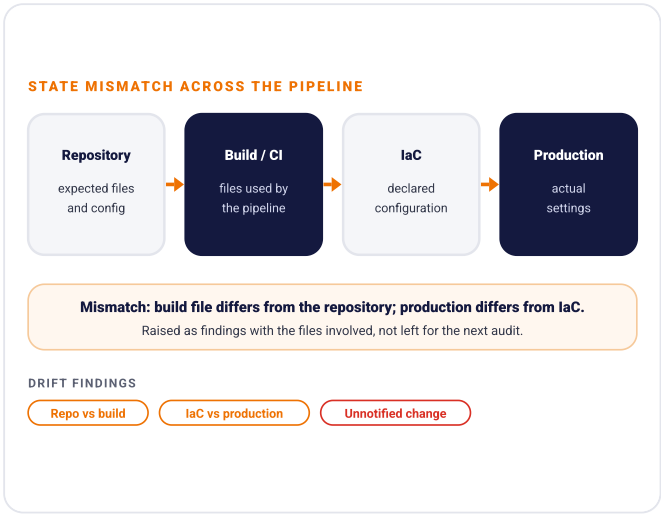
# Protect the files that must never change silently

## Code Tamper scanning for critical files, and drift detection across the pipeline.

Some files decide what your pipeline builds and who can approve it. The Code Tamper Scanner detects unauthorized changes to them, with the commit and the affected files, so you can run a "blocked by default, strict change procedure" model for critical code. Drift detection compares what should match across tools: repository versus build, IaC versus production.




Schematic: a code-tampering finding with the commit, the author and the affected files.




Schematic: drift detection compares repository, build, IaC and production state.

- **CI/CD files:** build and workflow definitions.
- **Dependencies:** unauthorized changes to dependency descriptors.
- **Security controls:** security policy files and the configuration of security tools.
- **Access and configuration:** CODEOWNERS, configuration and environment files, shell scripts.
- **Infrastructure as code:** changes to IaC templates.
- **Your own critical files:** any file you designate as critical.

**Blocked-by-default model** | **Commit and file detail** | **Air-gapped support** | **In CI or as a dedicated scanner**

**Drift is a signal, not a report.** Files that change without notification, IaC that no longer matches production and build files that diverge from the repository are raised as findings, not left for the next audit.

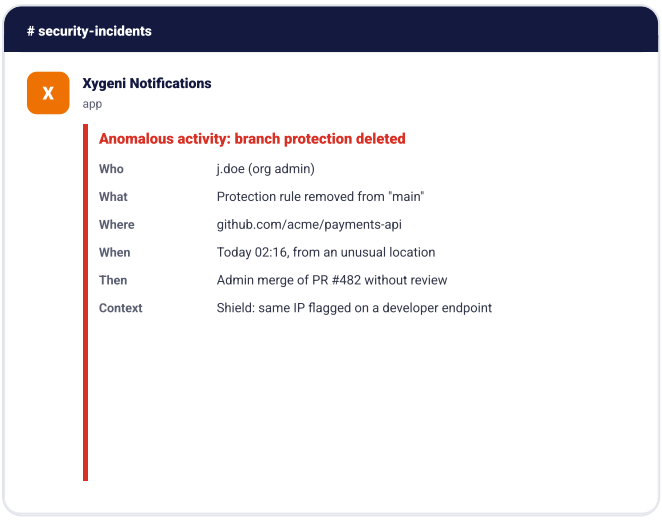
**For the CISO: evidence that critical code only changes through the procedure you defined.**

RESPOND · REAL TIME

# Alert the right people with the context to act

## Real-time alerts, Shield correlation and a per-asset audit trail in the ASPM.

Every anomaly is raised with who, what, where and when, and delivered by email, webhook, Slack or Teams. The activity detail includes Xygeni Shield artifact and IP data, so an endpoint event and a pipeline anomaly appear in one view. Findings feed the ASPM, its notifications and its per-asset audit trail.




Schematic: a real-time alert with the incident context, delivered to a team channel.




Schematic: an endpoint event from Shield and a pipeline anomaly joined in one activity view.

- **Real-time alerts:** email, webhook, Slack and Teams.
- **Shield correlation:** artifact and IP details from developer endpoints in the activity detail.
- **Audit trail:** findings in the ASPM per-asset audit trail and notifications.
- **Incident context:** actor, action, resource, location and time in every alert.
- **SIEM-ready:** curated anomalies forwarded through webhooks.
- **Deploy your way:** SaaS, on-premise or air-gapped.

### CI/CD Security
Prevents the pipeline and SCM misconfigurations that make an attack possible.

### Shield
Blocks malicious packages, IDE extensions and plugins on developer endpoints.

### Build Security
Proves each artifact was built from the expected source, untampered.

**For incident response:** an alert you can act on, not a log to reconstruct.

xygeni.

WHY XYGENI FOR ANOMALY DETECTION

## Monitor every change. Detect what is not normal. Respond in real time.

Xygeni Anomaly Detection is the detective layer of your software supply chain: it watches SCM and CI/CD activity, protects critical files and tells your team the moment something changes that should not.

### SCM and CI/CD in one view

GitHub, GitLab, Bitbucket, Azure DevOps and Jenkins activity in one place.

### Code tampering protection

Critical files monitored, with commit and file detail on every change.

### Endpoint to pipeline

Shield artifact and IP data correlated with SCM and CI/CD anomalies.

### Air-gapped ready

Code Tamper scanning runs in disconnected environments.

## Why security leaders choose Xygeni

### Proven in production

Banco Serfinanza reports around 90% less time identifying, prioritizing and assigning findings; Fintonic, a 90% reduction in prioritization time.

### 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.

## Know the moment your supply chain changes in a way it should not

**Monitor. Detect. Respond. One platform.**

Request a PoC | Book a demo

- The detective layer next to CI/CD Security and Shield
- SaaS, on-premise or air-gapped
- 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.