cytix

Use Case:

Identify Risky Development Changes

The Challenge

Traditional Testing Is Too Slow For AppSec

1 AI-Assisted Development = Faster Output

As development teams accelerate into AI-assisted coding, CISOs are losing visibility over what's actually being shipped.

Greater velocity means security must keep pace without sacrificing coverage.

Scanners and native AI pentesting tools add a layer of protection, but miss business logic flaws. Manual pentests are thorough, but slow and point-in-time.

So how can AppSec teams find every vulnerability at the speed of a scanner and the depth of a pentest?

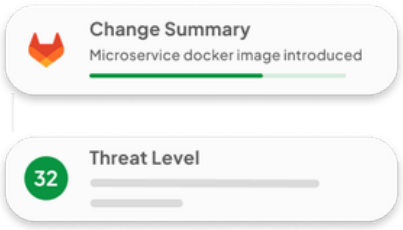
2 Manual Triage = Human Error

Testing decisions are based on the completion of developer questionnaires that are often unreliable and inaccurate.

Understanding which changes are high-risk becomes a subjective, slow and expensive process.

The Solution

Threat Model Every Change & Test In Line With Development

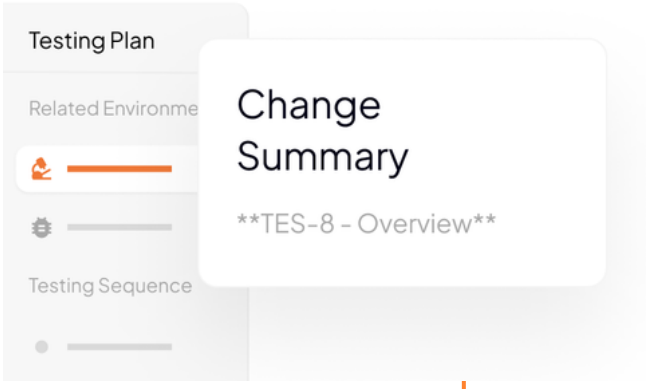


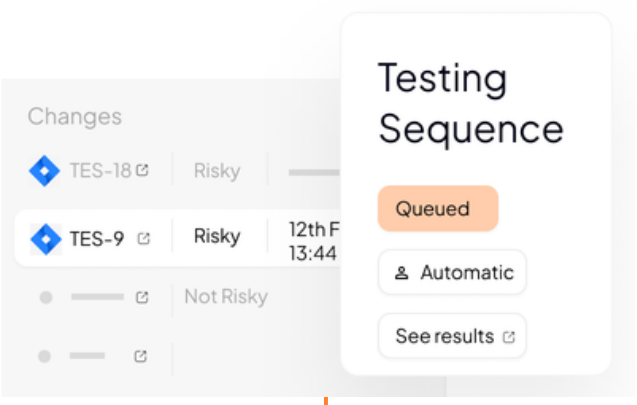
cytix

Full Security Review in 13 Seconds

Architect-Grade Analysis

Cytix ingests tickets, PRs, code diffs and system context to produce a true description of what changed, where it sits in the architecture and what it talks to.





AI Threat Modelling With Human Sign-Off

Cytix automatically generates a targeted threat mode and concreate testing plan for a security architect to review and approve.

High-risk changes are flagged immediately so it's clear exactly where to focus testing.

Correct Testing Method Every Time

Every testing plan includes the exact testing method guaranteed to find the predicted vulnerability.

Focussed micro pentests mean critical vulnerabilities typically missed by scanners, like business logic flaws, are identified instantly.