Agentic AppSec Unleashed '26
by Checkmarx

Remediation at AI Speed

From AI Vibe Coding to Verified, Governed Code

Harshil Parikh
Vice President, Checkmarx

Femi Oyesanya
Application Security Engineer, PatientPoint

Lily Leith
Application Security Risk Analyst, PatientPoint

Agentic AppSec Unleashed '26
by Checkmarx

Agenda

Why AI-generated code changes the risk equation

Backlogs, vibe coding, and hallucinated/slop code

Why accuracy needs deterministic AppSec controls

How Checkmarx findings can be orchestrated with AI

AI-Assisted Remediation with Deterministic Security Controls

Operating model: automation with human oversight

AI Vibe Coding Speeds Delivery—and Risk

What Changed

Developers can generate features, tests, and fixes in minutes

Small UI changes can touch data collection, consent state, APIs, dependencies, and infrastructure

Attackers can also use AI to discover and exploit weak patterns faster

What Did Not Change

Code still needs to compile, behave correctly, and comply with privacy expectations

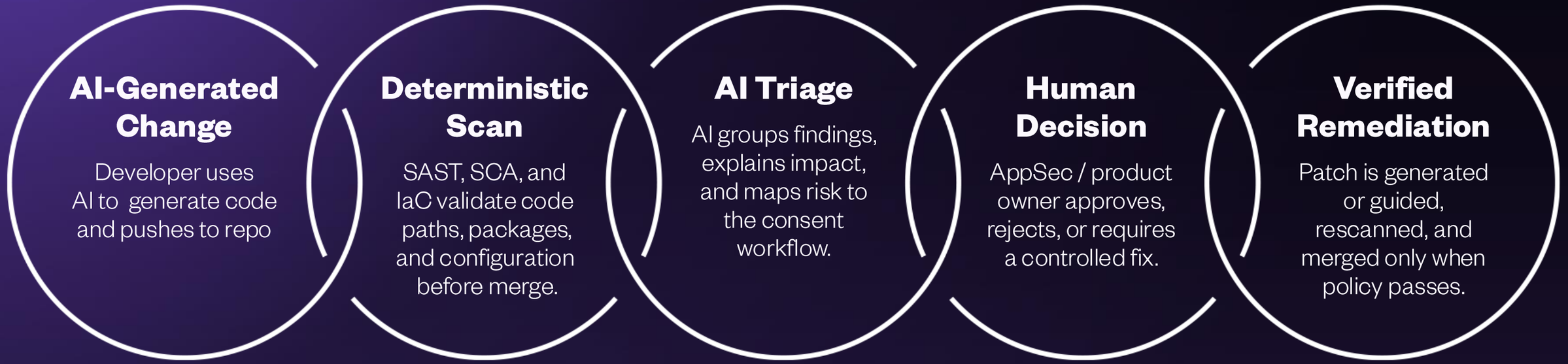
Open-source dependencies still introduce supply-chain risk

Infrastructure definitions still need least privilege, encryption, and safe defaults

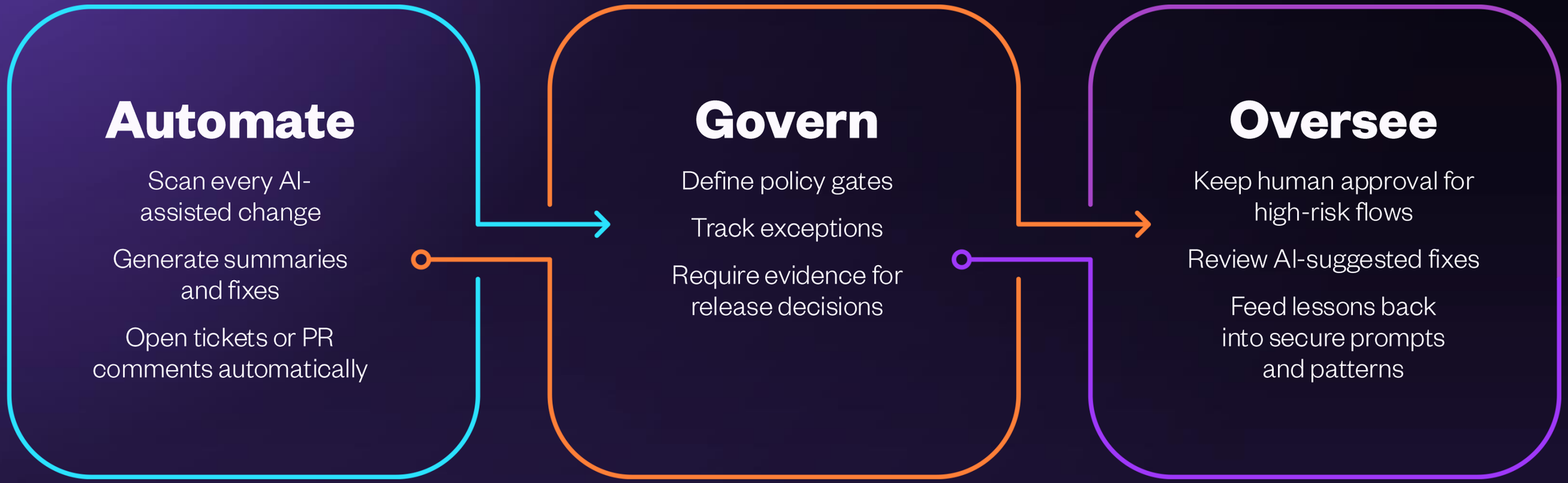
The Backlog Problem:
More Code, Same Capacity

AI-Assisted Remediation with Deterministic Security Controls

AI Can Accelerate the Workflow, But Deterministic Controls Decide Whether the Change is Safe Enough to Ship



Operating Model: Automate the Work, Not the Judgment



AUTOMATED APPSEC WORKFLOW

From vulnerability detected to fix merged — fully automated

- Zero manual triage steps
- Noise filtered automatically
- Loops until the PR is clean

PHASE 1

Scan

Checkmarx scans the PR and surfaces all findings

PHASE 2

Triage

Filters out noise — only real, fixable issues move forward

PHASE 3

Remediate

Posts fix requests to @Checkmarx, which generates fix PRs

PHASE 4

Verify

Waits for fix PRs to pass their scan, then auto-merges

PHASE 5

Loop

Re-scans the base PR and repeats until no issues remain

Returns to Scan until the PR is clean

CX Checkmarx

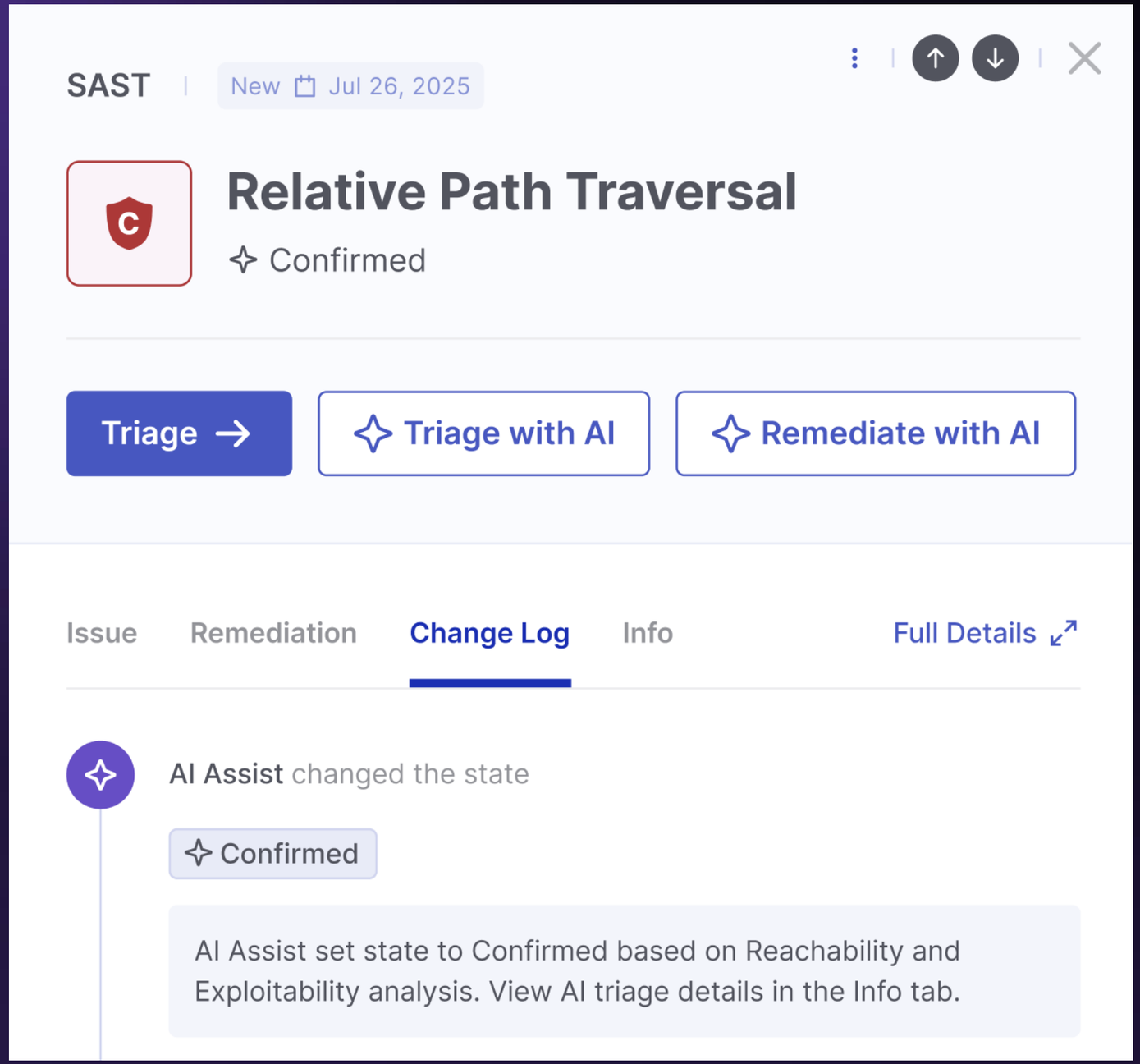
Checkmarx Triage Assist | Remediation Assist | Fully Automated

▼ Fixed Issues (5)

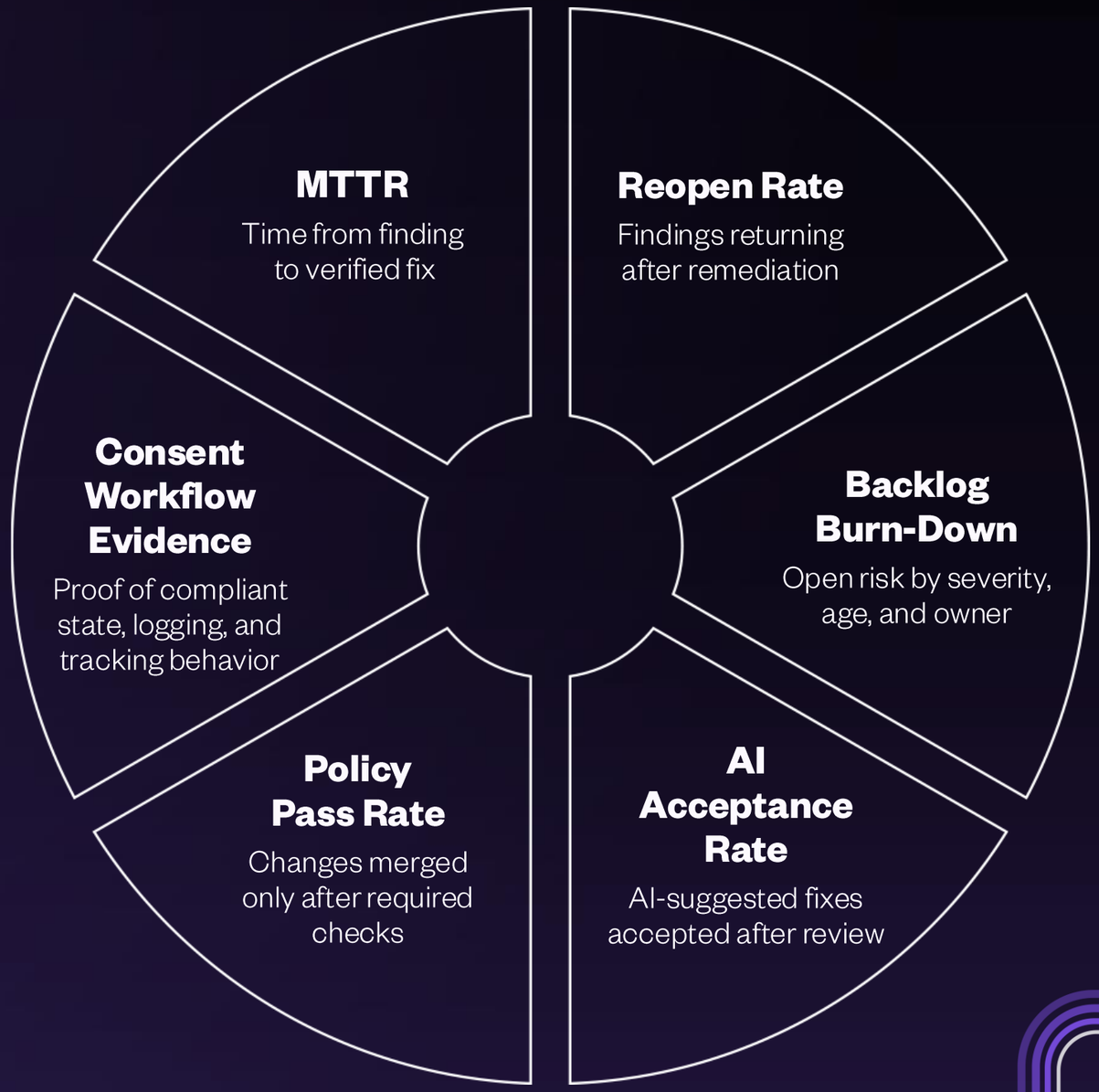
Critical: 2 · High: 3

Great job! The following issues were fixed in this Pull Request

Severity	Issue	Source File / Package
C	~~Stored_XSS~~	vuln_file_ops.php: 94
C	~~Stored_XSS~~	vuln_file_ops.php: 132
H	~~Reflected_XSS~~	vuln_file_ops.php: 132
H	~~SSRF~~	vuln_file_ops.php: 60
H	~~Unsafe_Reflection~~	vuln_file_ops.php: 102


SAST
New Jul 26, 2025
Relative Path Traversal
Confirmed
Triage
Triage with AI
Remediate with AI
Issue
Remediation
Change Log
Info
Full Details
AI Assist changed the state
Confirmed
AI Assist set state to Confirmed based on Reachability and Exploitability analysis. View AI triage details in the Info tab.

Measure Speed and Confidence Together



Agentic AppSec Unleashed '26

by Checkmarx