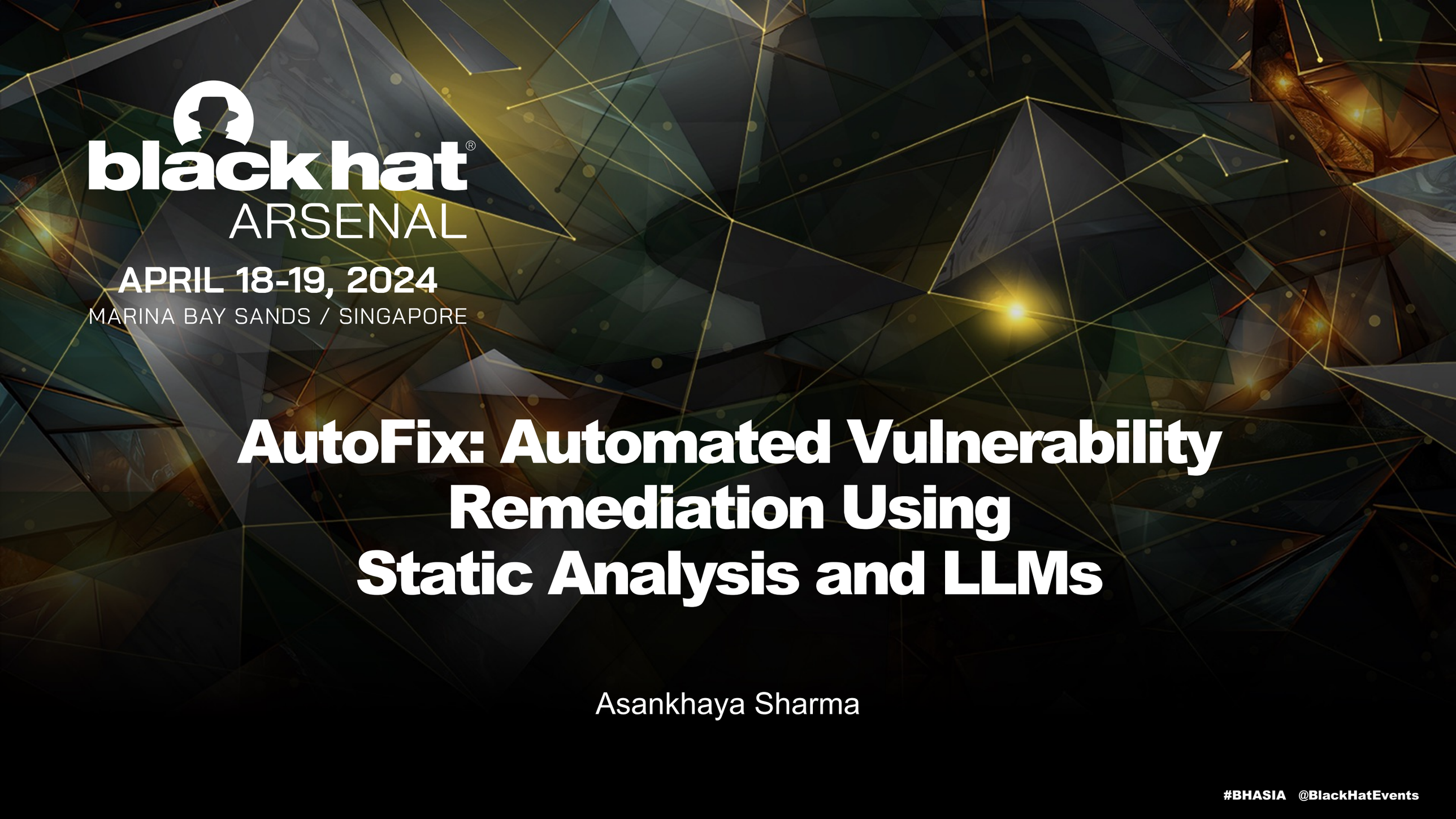



# AutoFix: Automated Vulnerability Remediation Using Static Analysis and LLMs

Asankhaya Sharma

Asankhaya Sharma, Co-Founder & CTO, https://patched.codes

2003 — Microsoft — Code Analysis Tool for .NET v2.0

2007 — INSTITUTE OF TECHNOLOGY NATIONAL WARANGAL — DIDAR – Database Intrusion Detection with Automated Recovery

2010 — NUS National University of Singapore — HIP/SLEEK :Automatic Verification and Specification Inference System

2014 — [:]SourceClear — Botwall4J

2018 — ca technologies — GramTest

2019 — VERACODE — SRC CLR SCA Agent

2022 — Securade.ai — AutoFix — Static Analysis + LLM = AutoFix

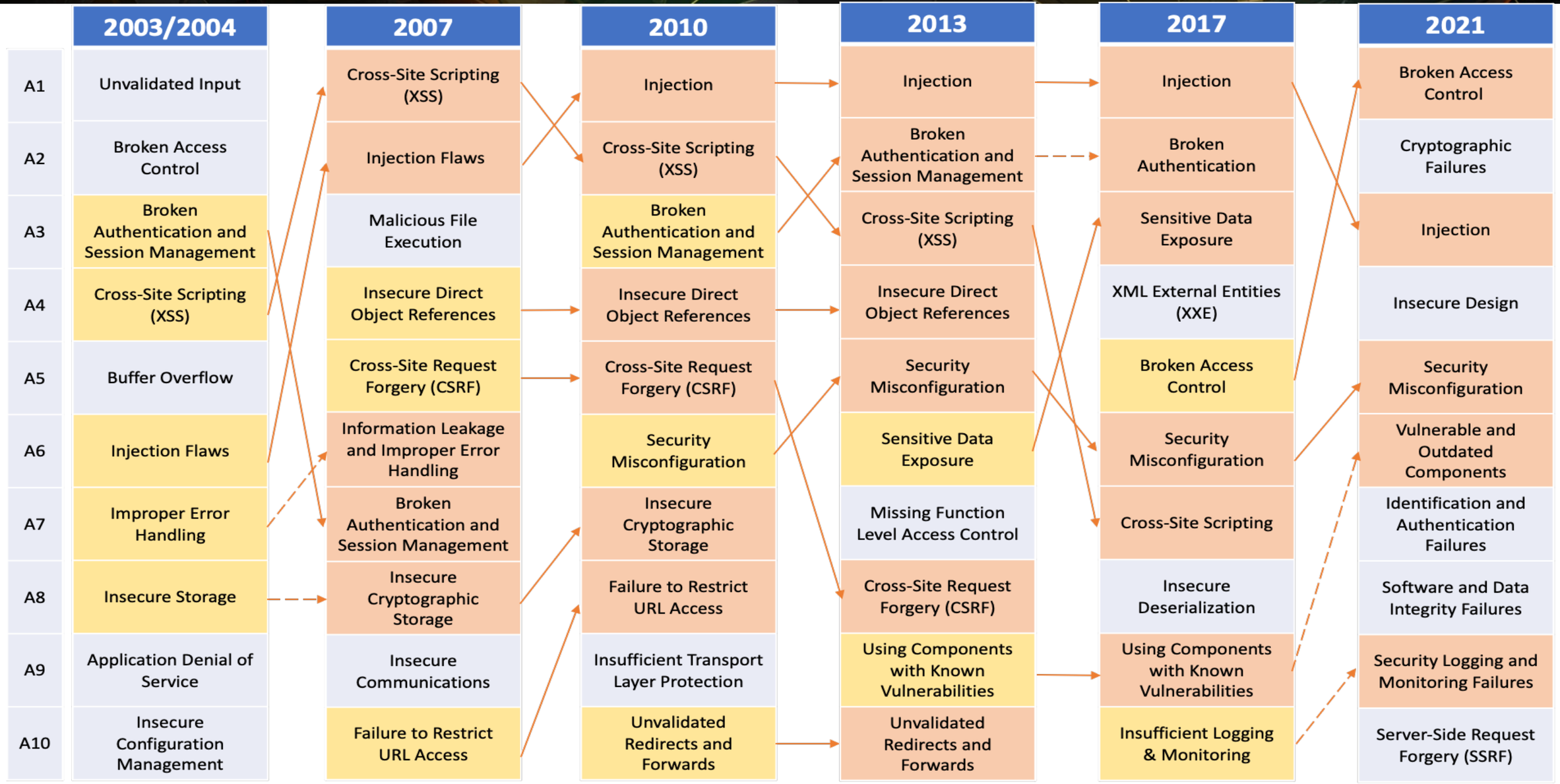
2023 — patched


*building security tools for developers*

*v/s*

*developer tools for security*

# OWASP Top Ten



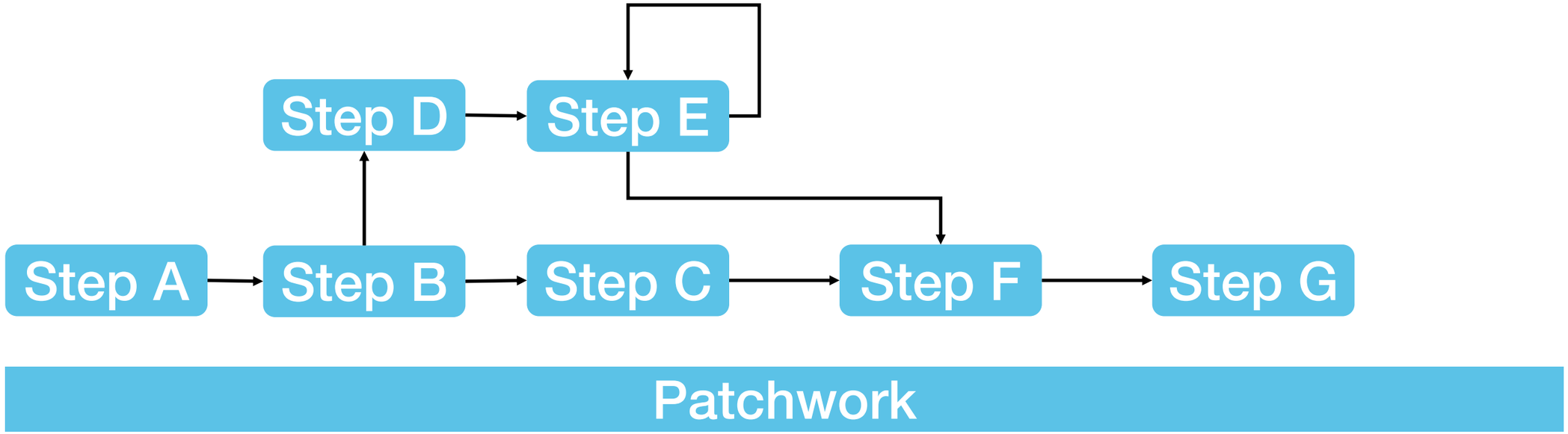
# Breaking the Cycle: Beyond Scan-and-Fix in AppSec

- Old Ways, New Challenges: Stuck in a "scan and fix" loop, traditional SAST/DAST tools leave us chasing vulnerabilities, not proactive security.
- Shift Left Illusion: Moving security earlier in the SDLC doesn't stop the cycle; it starts it sooner, overburdening developers with endless issues to fix.
- IDE Interruptions: Real-time scanning in IDEs promises security but disrupts developer workflow, compromising productivity with constant alerts and system overhead.

*This pattern is just wrong. It's broken. We've seen a history of the challenges following this pattern does in working with developers." —Chris Romeo*

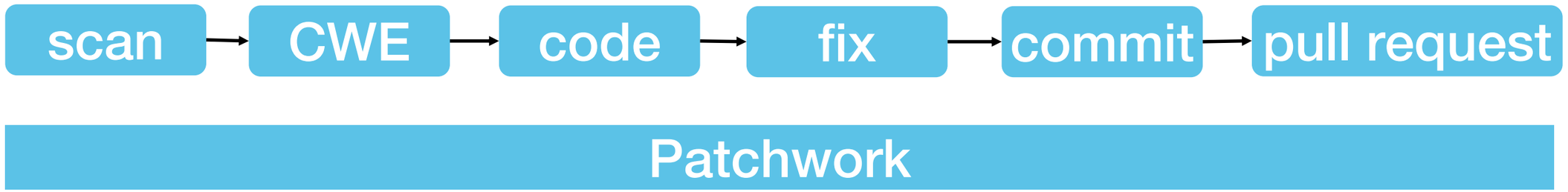
# Patchflow

patched-codes / patchwork




https://github.com/patched-codes/patchwork

# AutoFix




patchwork AutoFix -sarif=results.sarif -createBranch=patch-main -severity=critical -patch=customprompts.json

## Extensible with steps

Add, modify, or remove steps easily to extend the patchflow to suit your needs.

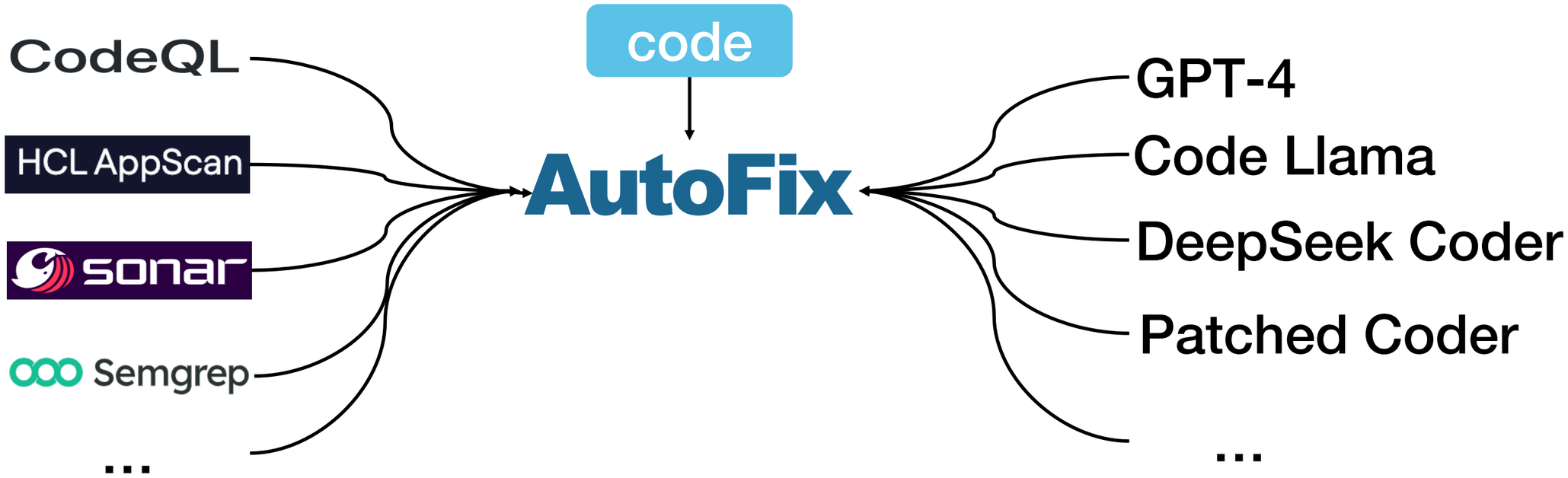
## Integrations with development tools

Run anywhere CLI, CI, IDE etc.

## Customizable with patchprompts

Use of customizable natural language prompts allows for highly tailored solutions to specific vulnerabilities or coding standards. This flexibility ensures that the automated fixes are aligned with the project's requirements and coding practices.

# SAST + LLMs


CodeQL
HCL AppScan
sonar
Semgrep
...
code
AutoFix
GPT-4
Code Llama
DeepSeek Coder
Patched Coder
...

# DEMO


# Thanks!

https://github.com/patched-codes/patchwork

asankhaya@patchedcodes.com