MICHIGAN STATE UNIVERSITY

Alpha Presentation
Android Exploit Fuzzing Analysis

The Capstone Experience

Team Google

Karan Singh
Romario Rranza
Shubham Chandna
Anurag Kompalli
Michael Umanskiy
Catherine Xu

Department of Computer Science and Engineering
Michigan State University

Fall 2022

From Students…
…to Professionals

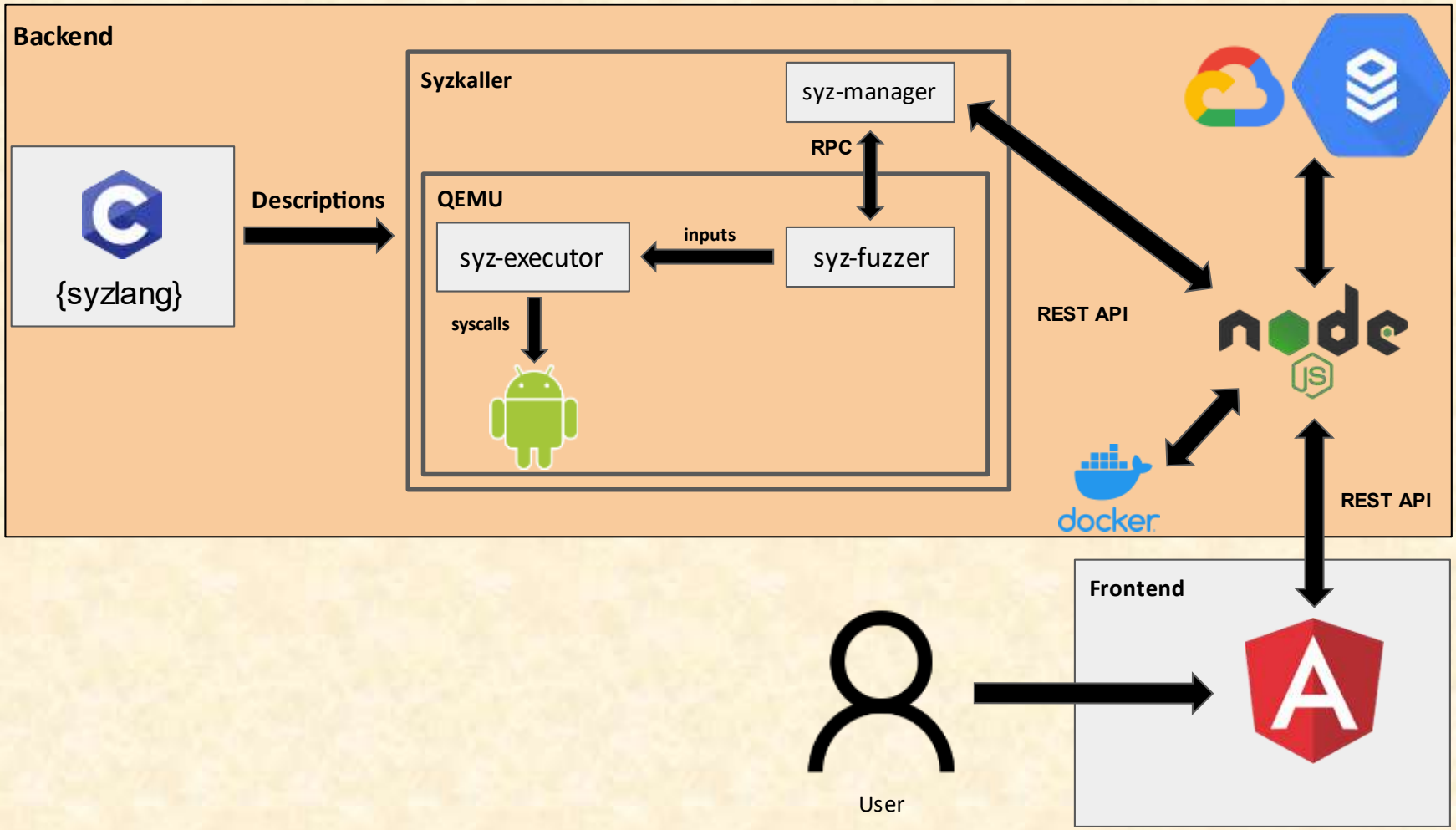
Preface

- Fuzzing: Black box software testing technique
  - Inputs malformed data to find implementation bugs
  - State-of-the-art-tool: Syzkaller
- Descriptions: Interface that uses syzkaller fuzzing to detect bugs by passing inputs to the kernel.

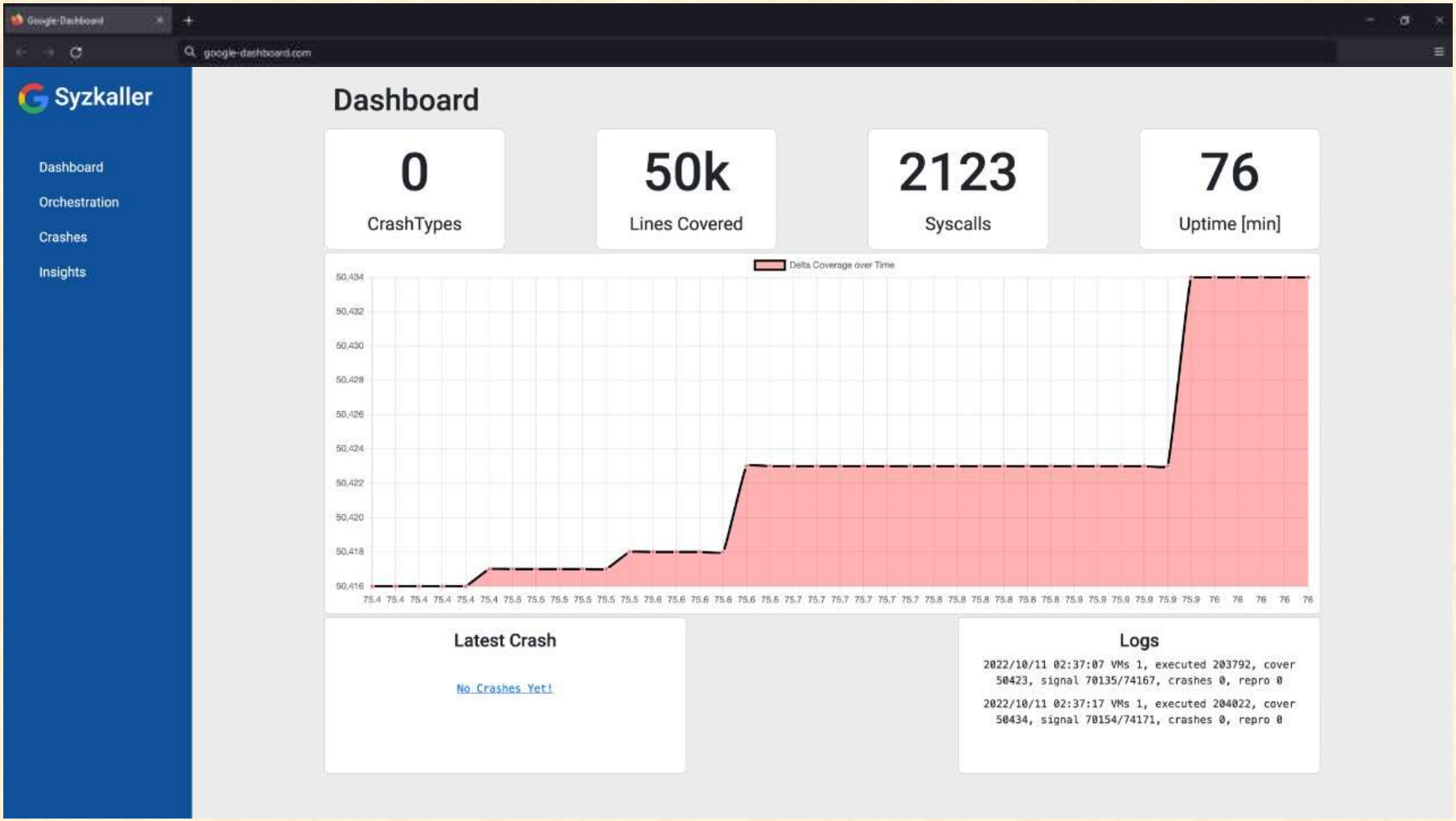
Project Overview

- Problems:
  1. While syzkaller detects bugs in Android OS, the software is constantly evolving and needs improvement
  2. Fuzzing performance can be variable, depending on the configuration
- Solutions:
  - Visualize bugs in the Android kernel intuitively
  - Extending syzkaller descriptions
  - Running multiple syzkaller instances with custom configuration

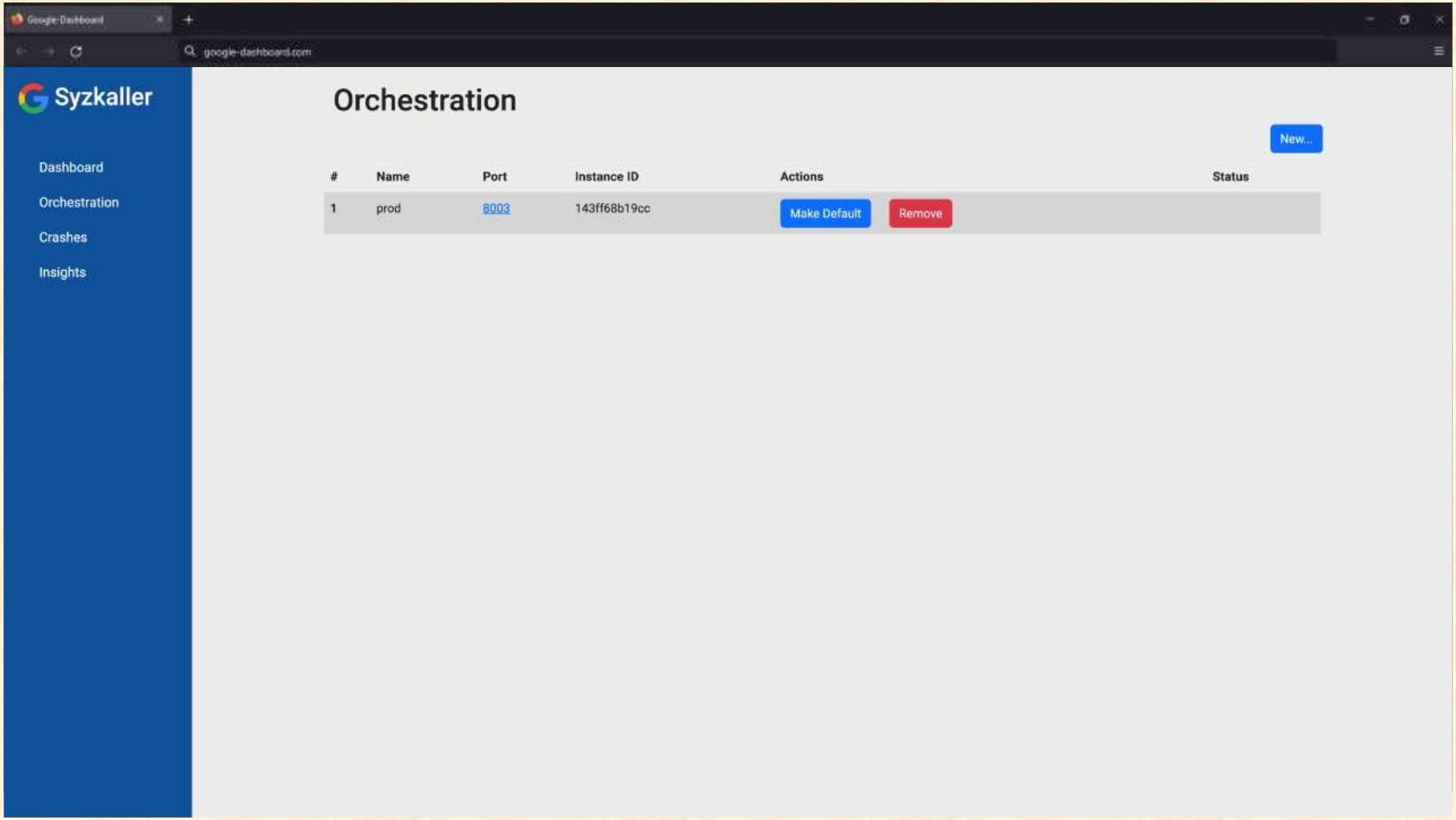
System Architecture



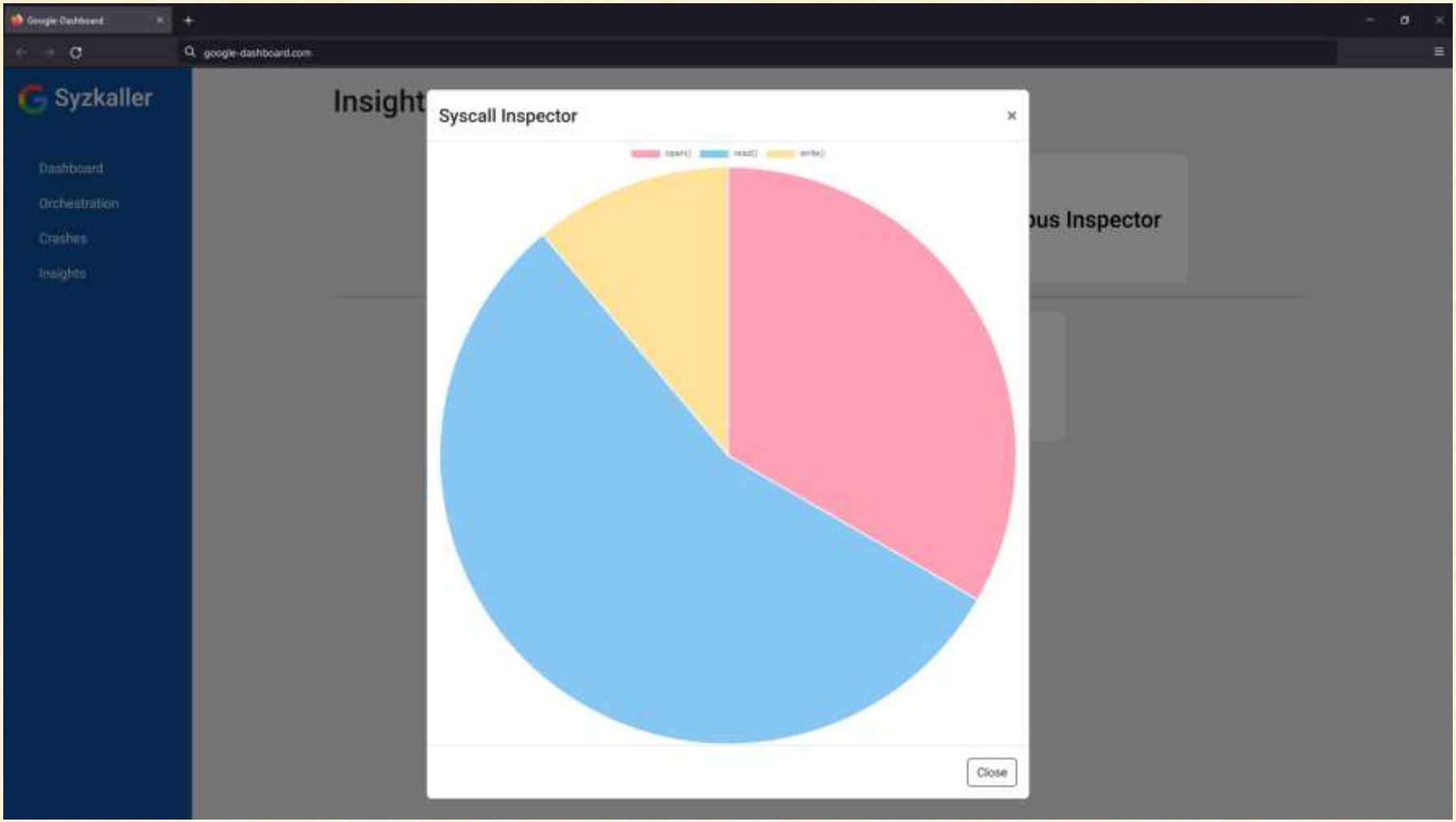
Dashboard Page



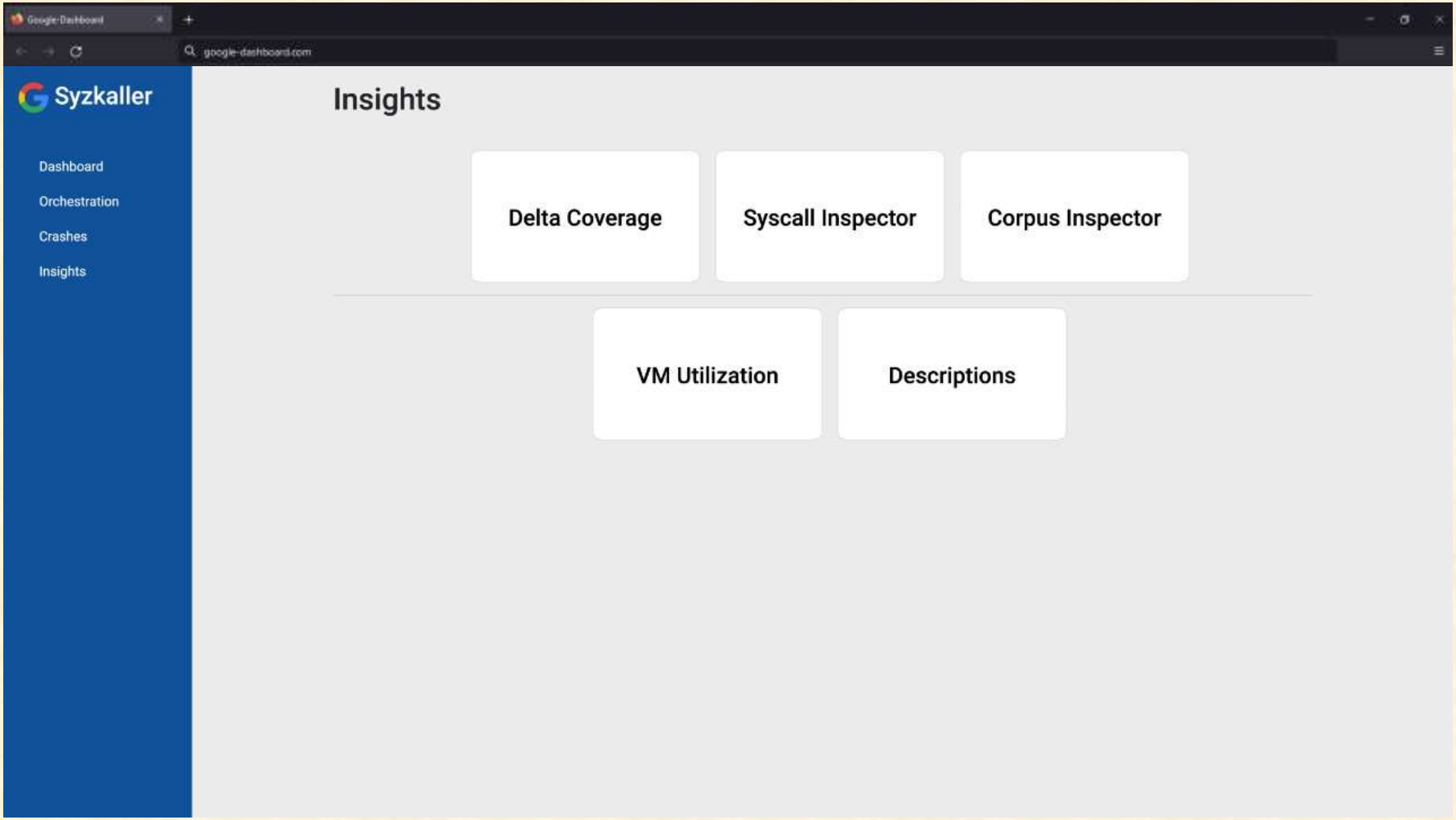
Orchestration Tab



Insights Tab: Syscall Inspector



Insights Tab



What's left to do?

- Work on the Crashes tab to display the latest crashes and their reports
- Write more descriptions for syzkaller
- Enable custom configurations for syzkaller in the Orchestration tab
- Add more visualizations to the Insights tab relating to the Corpus and VM Utilization

Questions?