MICHIGAN STATE UNIVERSITY

Beta Presentation

AI Cyberattack Early Warning System

The Capstone Experience

Team Vectra AI

Alex Fortsch
Graham Holley
Ajay Kumar
Morghane McAnelly
Aleksa Popovic
Jacob Sock

Department of Computer Science and Engineering
Michigan State University

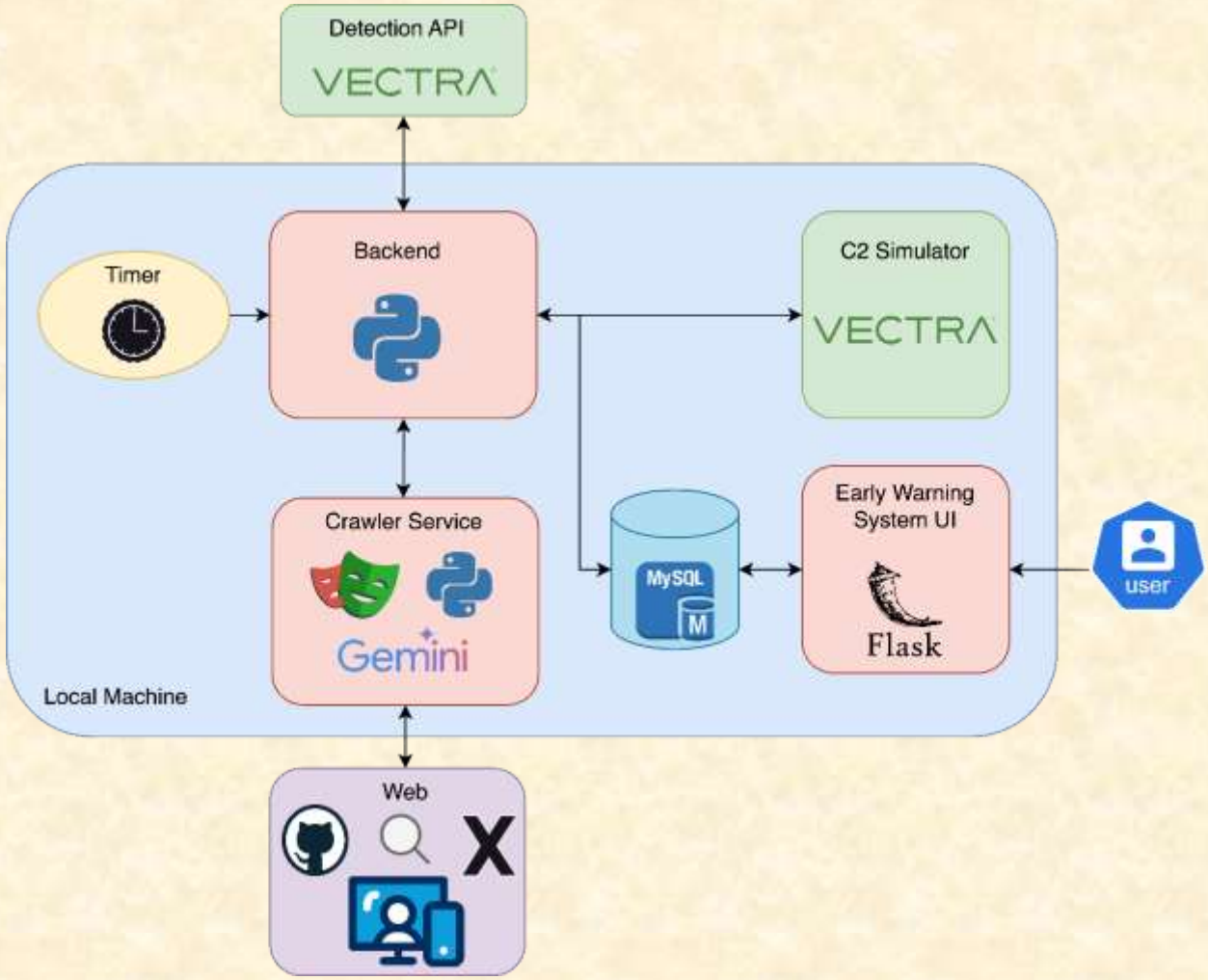
Fall 2024

From Students…
…to Professionals

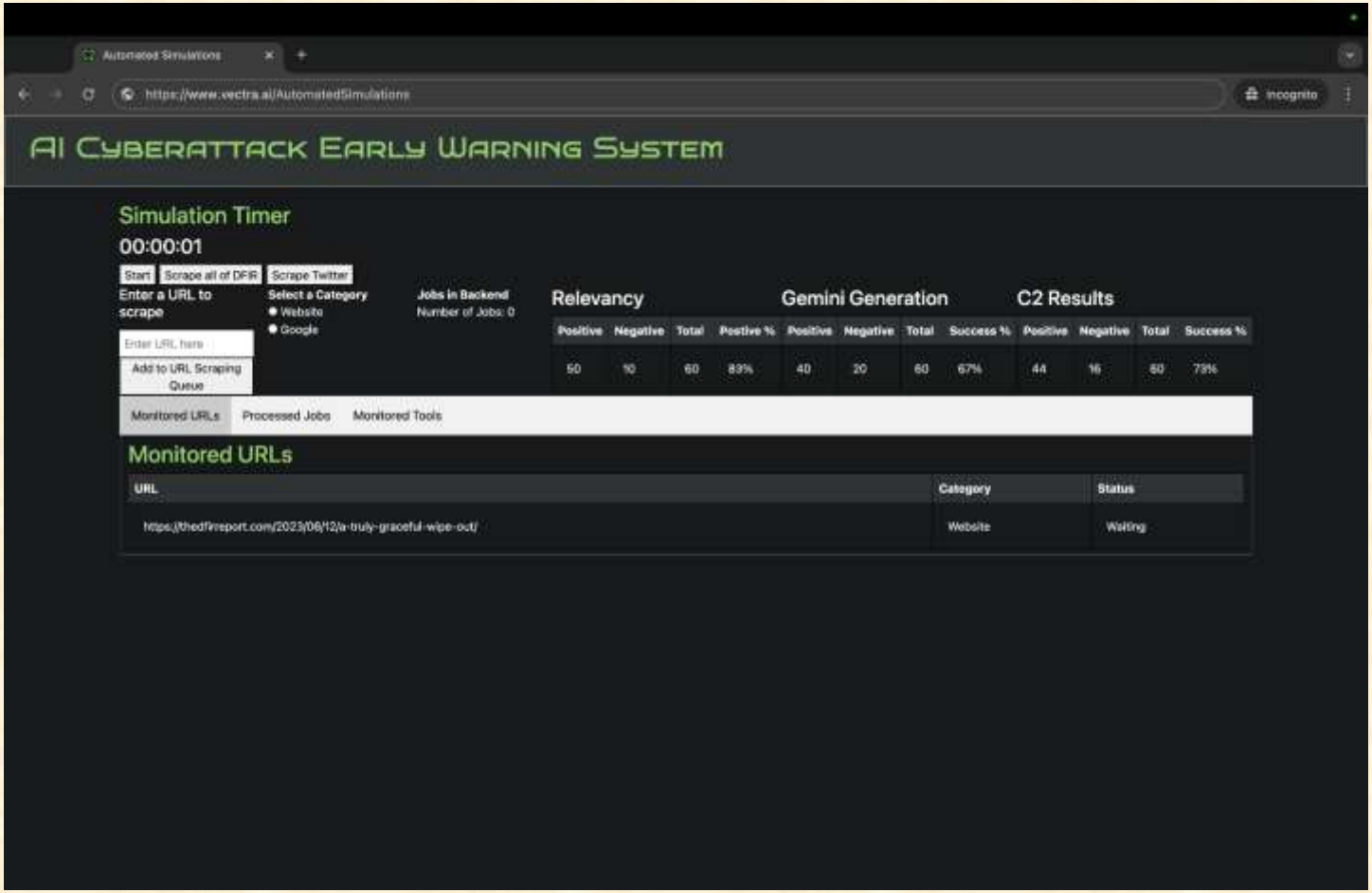
Project Overview

- Problem
  - Data scientists have to manually read reports and configure the C2 simulator
- Solution
  - Automate the process by web scraping threat intel resources, extrapolating C2 configs, and generate PCAP samples
- Result
  - Human intervention in the process is eliminated

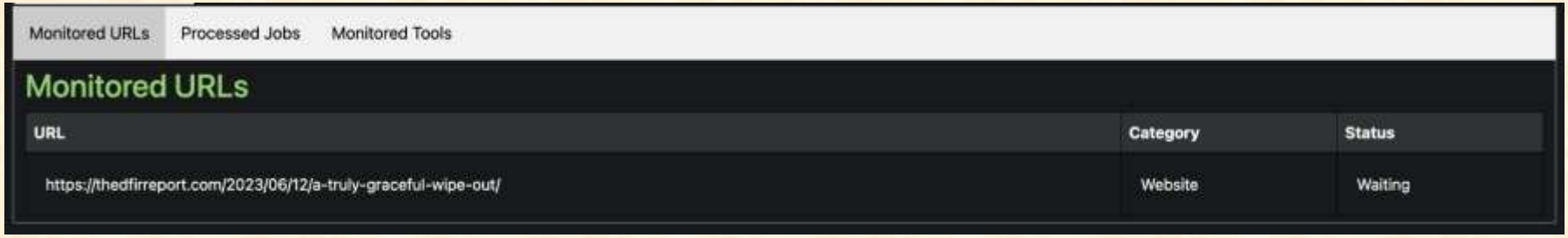
System Architecture

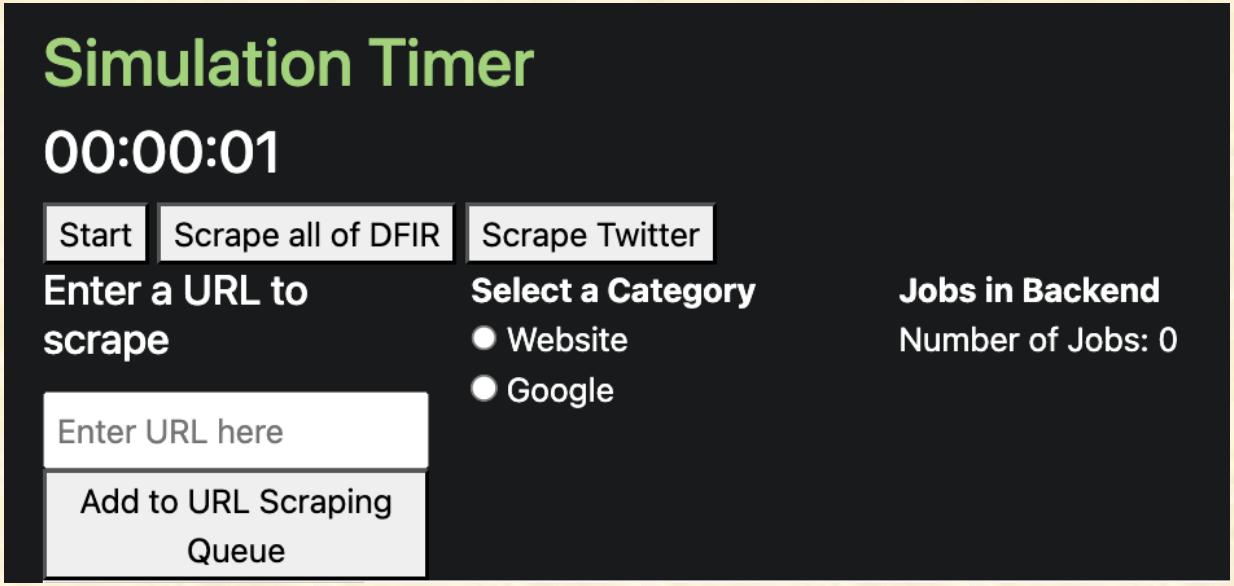


User Interface

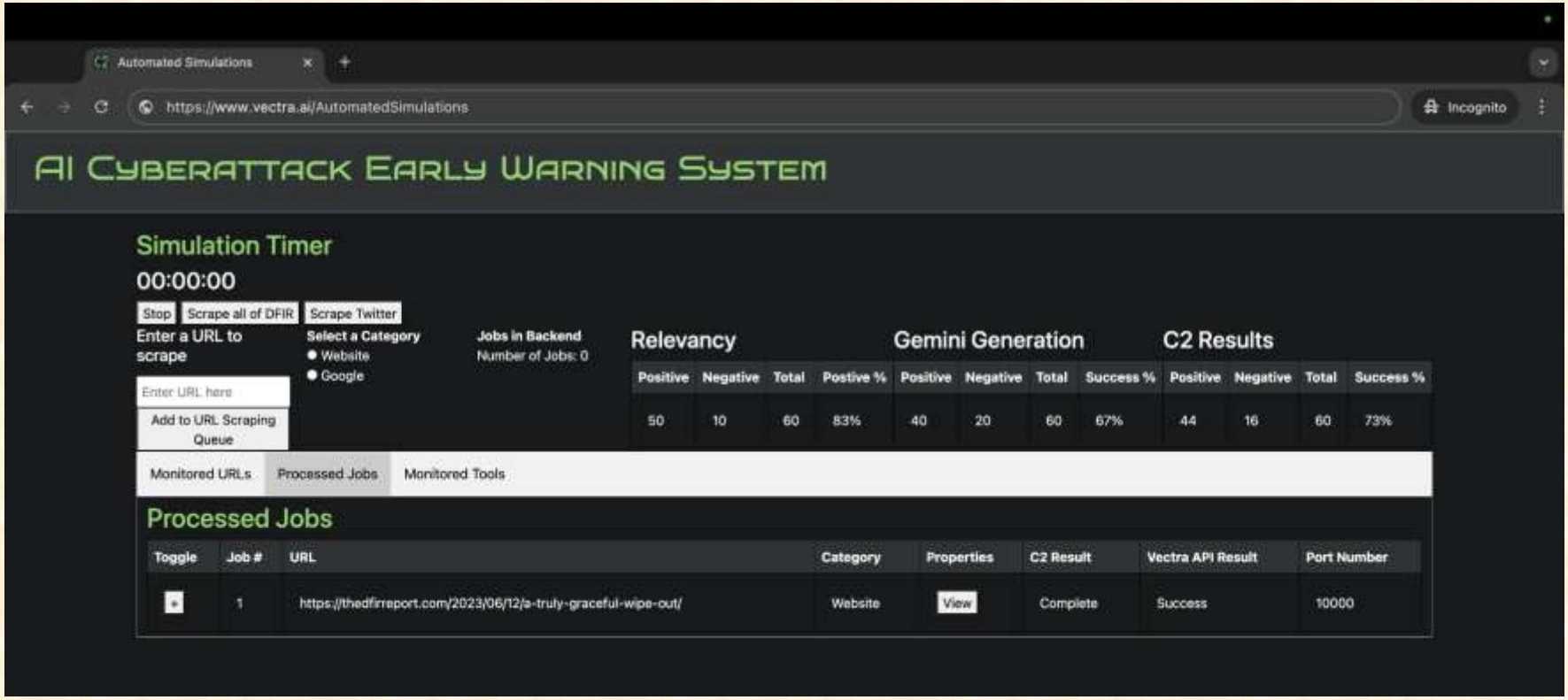


User Interface

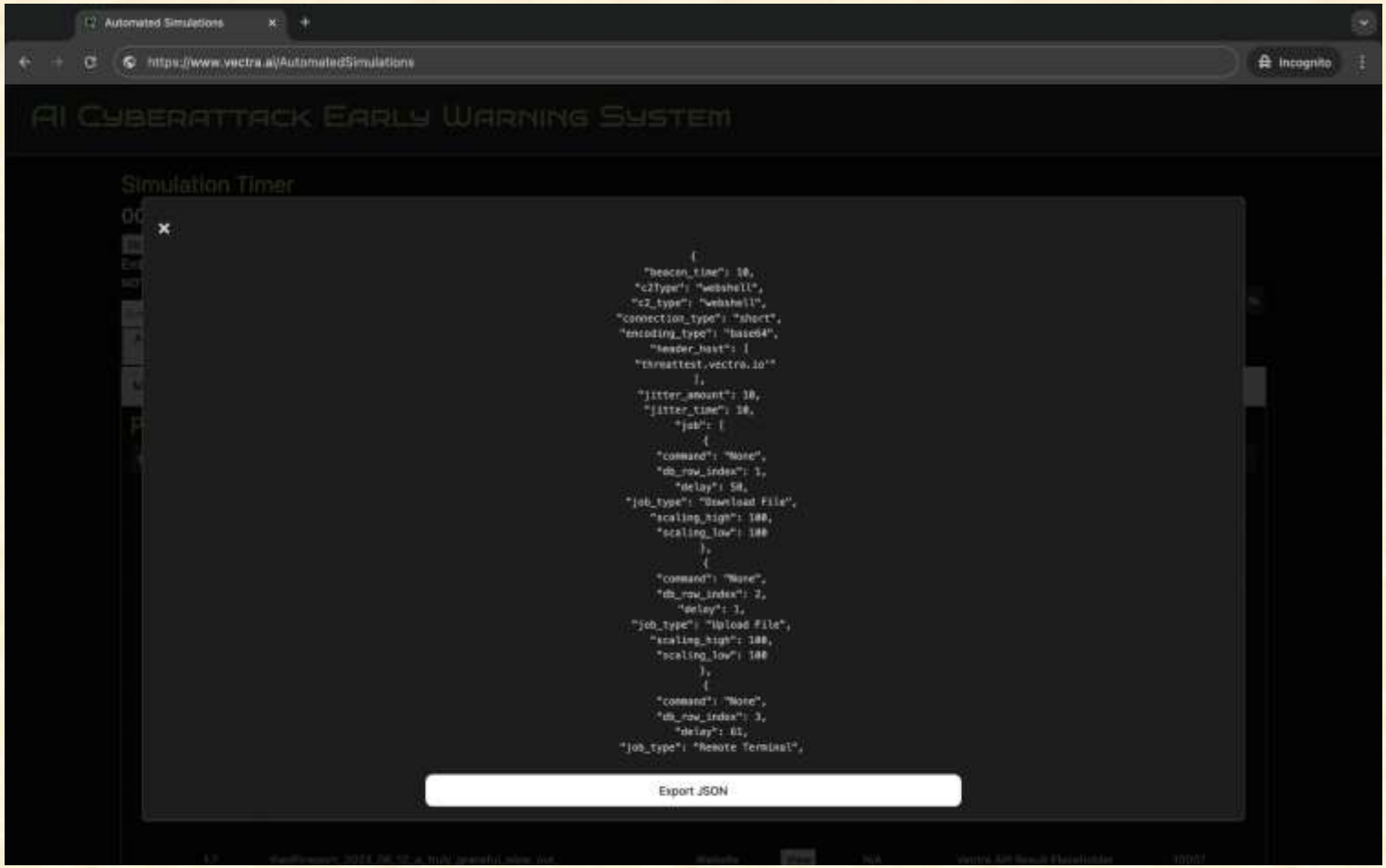




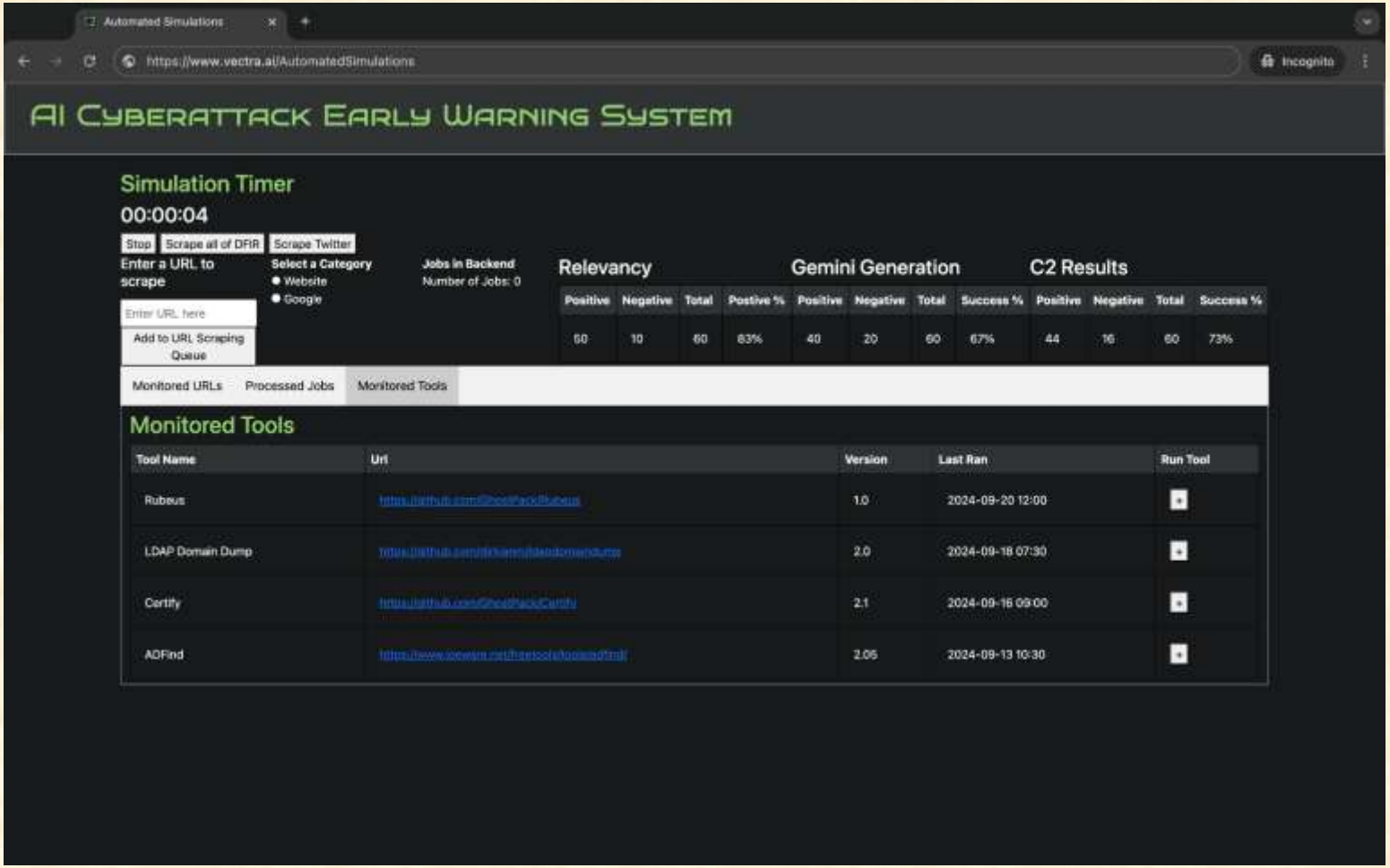
User Interface



User Interface



User Interface



What's left to do?

- Stretch Goals
  - Visualize PCAP data
  - Gemini default usage percentage
  - Add additional known tools
- Other Tasks
  - Integrate with Vectra AI's VM
  - Refactor code

Questions?