

Cysec Game - Risk Analysis Tool

Team: sdmay21-50

Members: Nick Battani, Jonathan Greazel, Harrison Majerus, Stefan Peng, Hayden Sellars, Joseph Strobel
Faculty Advisors/Client: Manimaran Govindarasu, Burhan Hyder

Introduction

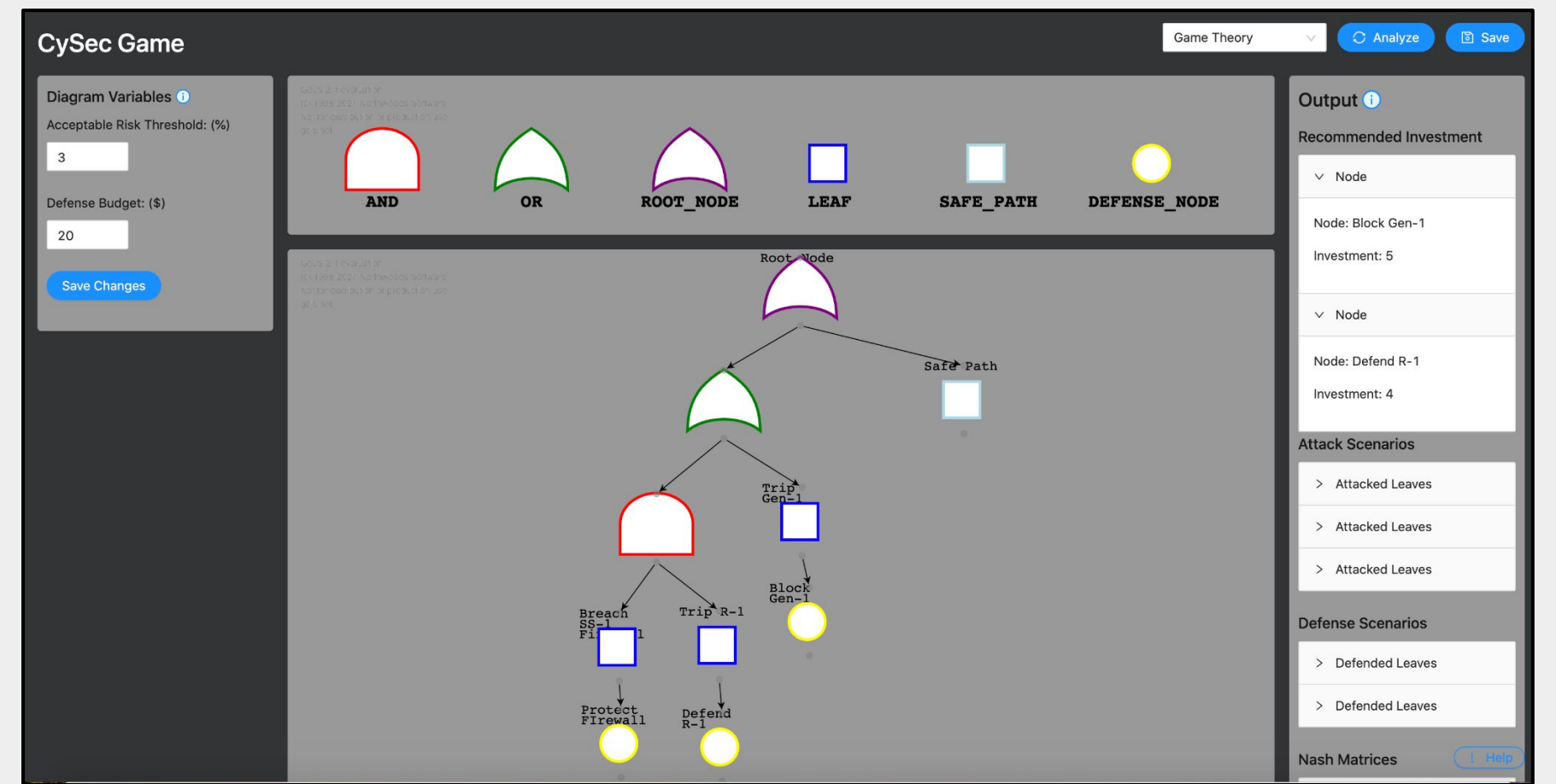
Problem

- Cyber Security Administrators have a difficult job to evaluate the risk their systems face and where to invest in defenses.

Solution

- The CySec tool allows a user to input attacks on their system and any defenses. In return the user will receive an optimal investment strategy for their system.

Implementation



Shown in the figure is an example use of the game theoretic engine with output on the right hand side.

Users & Uses

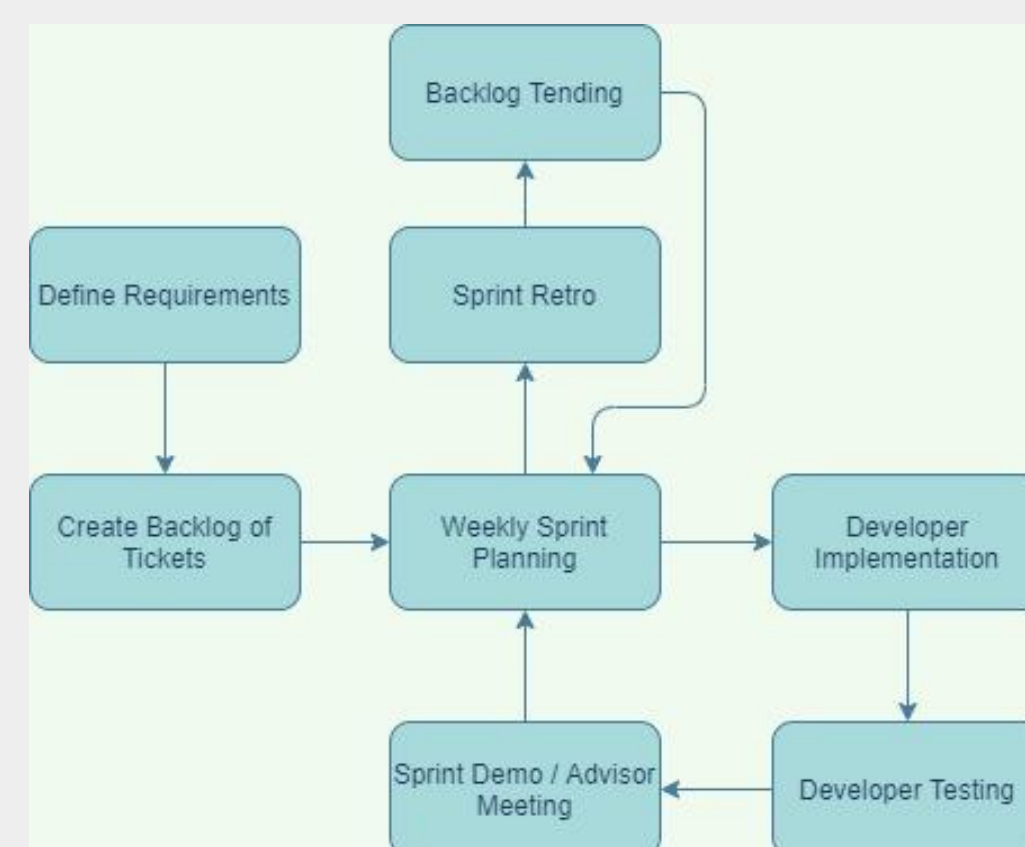
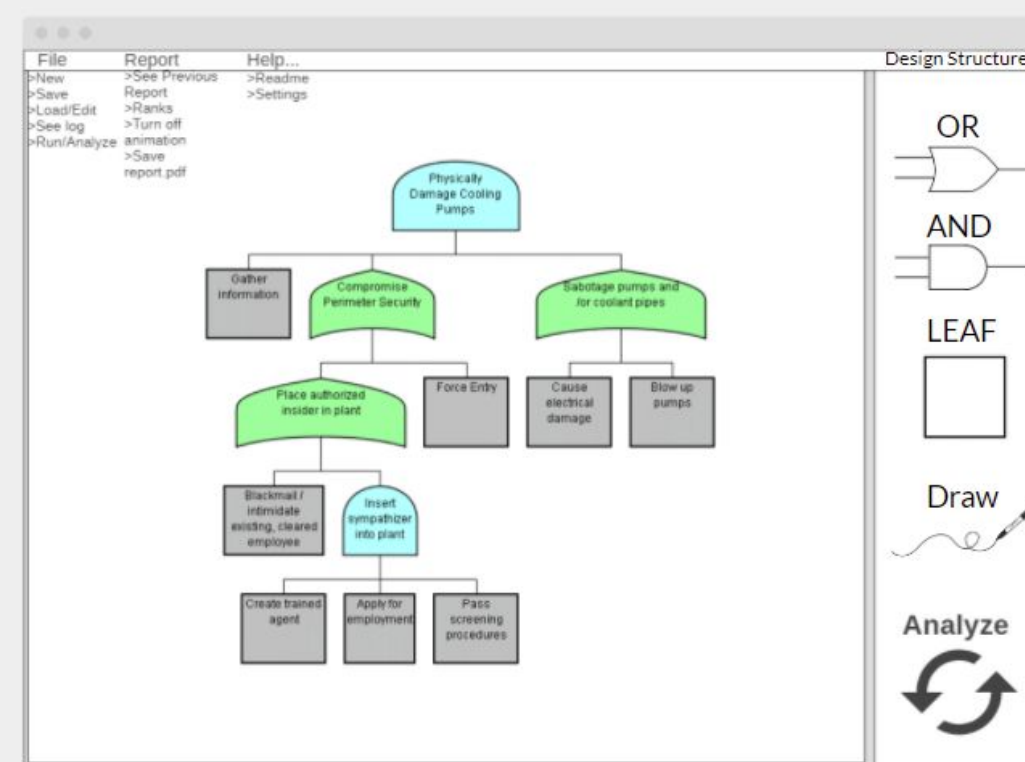
Users

- Cyber security advisors
- Power grid administrators
- Other critical infrastructure administrators

Uses

- Model network threats
- Analyze attack and defense scenarios
- Suggest security investments

Design Approach



- Angular Framework
- GoJS library
 - HTML Graph Element
 - HTML Palette Element
- UI Components from Ant

Requirements

Functional

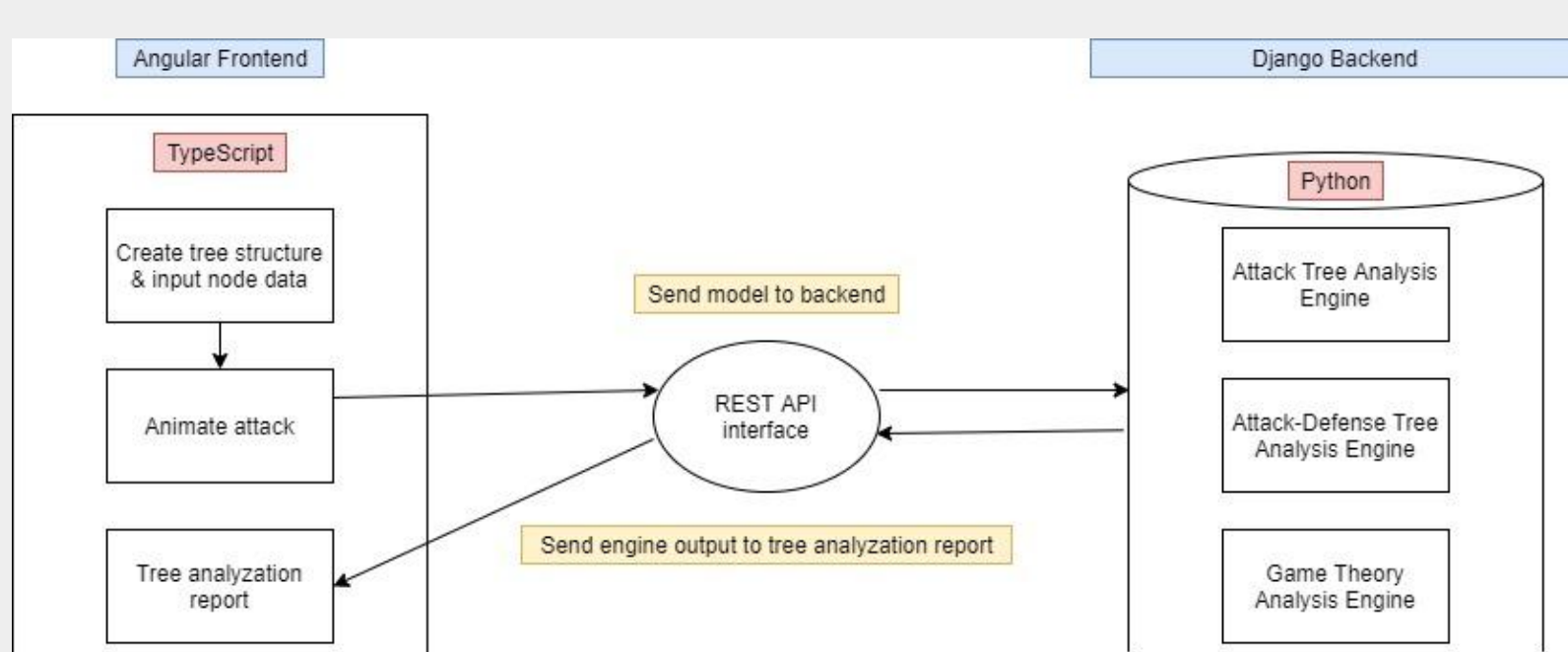
- The software shall be remotely accessible through a web application
- The software shall utilize Game Theory and attack-tree analysis algorithms for risk assessment and provide strategies to mitigate risk
- The software's UI design shall encourage ease of use and work to minimize clicks per action

Non-Functional

- Different environments (Windows, Linux, etc.) shall have no effect on software usability
- The software shall cost no more than \$0
- Any sensitive user information shall be stored in a safe and secure manner

Technical Details

Client	Server
<ul style="list-style-type: none"> TypeScript Angular Go.js Ant Design 	<ul style="list-style-type: none"> Python Django Nash.py



Testing

Backend	API	Frontend
<ul style="list-style-type: none"> Unit tests Manual script tests 	<ul style="list-style-type: none"> Postman calls 	<ul style="list-style-type: none"> Unit tests Manual testing

