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.

Users & Uses

Users

Implementation



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

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

Uses

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

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

Design Approach

Design Structur OR AND LEAF Draw Apply for Pass employment screening procedures Analyze Ð **Backlog Tending** Sprint Retro Define Requirements Create Backlog of Weekly Sprint Developer Tickets Planning molementation orint Demo / Advisor **Developer Testing** Meeting

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

safe and secure manner

Technical Details

Client	Server
 TypeScript Angular Go.js Ant Design 	PythonDjangoNash.py
ntend ipt	Djang



Testing

Backend	API	Frontend
 Unit tests Manual script tests 	 Postman calls 	 Unit tests Manual testing
POST • http://127.0.0.1:8000/api/attack/		Send V Save V
Params Authorization Headers (10) Body •	Pre-request Script Tests Settings	Cookies Code
none form-data x-www-form-urlencoded	🖲 raw 🔍 binary 🔍 GraphQL 🛛 JSON 🔻	Beautify
<pre>1* [2 "selectedEngine": "attackTree", 3 "acceptableRiskThreshold": 1, 4 "defenseBudget": 0, 5* "nodeData": [6* { 7</pre>		
Body Cookies Headers (9) Test Results		Status: 200 OK Time: 7 ms Size: 411 B Save Response 👻
Pretty Raw Preview Visualize		