**Cybersecurity Scenario Generator**

**Project Plan**

**Team DHJM**

**Table of Contents**

[**Project Summary 3**](#_2w5kvmyasnn0)

[**Points of Contact & Organization 4**](#_azsuf7drji2)

[**Project Charter 5**](#_njpkpbayiaqs)

[**Activity List 6**](#_t7yqgcdo5gg5)

[**Work Breakdown Structure 7**](#_cy562bjtfgce)

[**Work Products 8**](#_4jcrfl9wa4w)

[**Schedule 9**](#_kbfe36kdf3m3)

[**Gantt Chart 9**](#_o5t8z7z7w36m)

[**Risks 10**](#_w5j3efkjw24a)

[**Quality 11**](#_eb0blbmcfbd9)

[**Issues and Action Items 12**](#_k8xmf9o94ujw)

# Project Summary

The Cybersecurity scenario generator project will involve the development of a customizable scenario generator for both high school and middle school students. This will enable the creation of interactive investigative scenarios, where students must engage in solving mysteries by analyzing clues that are embedded in digital artifacts. With inputs from the teacher such as the school mascot, a location, and a rival team, the project would automate the generation of scenario specific learning materials. This would include the generation of a PowerPoint presentation, disk images with digital clues, and a quiz. This would enhance student engagement through hands-on problem-solving activities. The project’s aim is to save teachers time by automating content creation, allowing them to focus on tailoring the materials to their specific teaching goals. A user-friendly interface will be provided to accommodate teachers with varying levels of technical expertise. The success of this project will be measured by its ease of use and the positive feedback from educators who implement it in their classrooms.

# Points of Contact & Organization

# Sponsor, David Hochstetler, [jacob.hochstetler@unt.edu](mailto:jacob.hochstetler@unt.edu)

# Project Manager, Michael Hoover, [michaelhoover@my.unt.edu](mailto:michaelhoover@my.unt.edu)

# Project Scribe, Stephanie Molina, [stephaniemolina@my.unt.edu](mailto:stephaniemolina@my.unt.edu)

# Project Developer Jared Diosdado, [jareddiosdado@my.unt.edu](mailto:jareddiosdado@my.unt.edu)

# Project Developer, Zachary Jones, [zacharyjones4@my.unt.edu](mailto:zacharyjones4@my.unt.edu)

# Points of contact are either through email and the project’s discord server where the team has access to real-time instant messaging with the sponsor and the group members.

# Activity List

# See Schedule

# Work Breakdown Structure

# See Schedule

# Work Products

# The product of the project will be a hosted website and server that allows users to generate educational powerpoints surrounding common cybersecurity concepts

# Schedule

# [Gantt Chart](https://docs.google.com/spreadsheets/d/1VRNlGZxkUmGccDn1DIbFMUHy9tPjTqeO573sLhSDDng/edit?usp=sharing)

# 

# Risks

# **Scope Creep:** This is where the project objectives are not clearly stated and the team is confused on who should do each objective.

1. **Low Performance:** Someone or the whole group is being lazy and not participating in the project will lead to disaster.
2. **Time Crunch:** This ties in with scope creep, but this is the risk when the project will take longer than expected.
3. **Stretched Resources:** Resource risk occurs if you don’t have enough resources to complete the project. Resources may include time, skills, money, or tools.
4. **Lack of Clarity:** Some examples of this would bemiscommunication from stakeholders, vague project scopes, or unclear deadlines.
5. **Project Quality Risk:** Project might not have the quality that the client was looking for.
6. **Client Risk:** The project team and client might not have the same views on the project and might disagree with each other.
7. **Programming Language:** Some people might try to code without the proper training for the programming language and mess up the project.

# 

# 

# 

# 

# 

# 

# 

# Quality

# Issues and Action Items