CEN 6940 Project Proposal

Project Title: CyberSphere

Project Category: Innovative Product

Team Name: VR Cyber Educators

Submitted By: Thang, Taiwo, and Zoe'

Problem Statement:

Conventional cybersecurity precepts in schools often need help engaging students and effectively training them for real-world challenges. This issue stems from the archaic practice of teaching methods needing to be more theoretical and sparsely intertwined with practical applications. Many existing programs rely largely on abstract concepts, creating a less user-friendly experience by limiting hands-on practice and real-world problem-solving opportunities. It is also through this that many students find it difficult to translate their classroom knowledge into practical skills needed in their respective fields, and with cybersecurity being heavily reliant on practical application, poses a major hindrance to the student's real-world growth.

The nature of this issue is born from the disparity between the structure of academic teaching and the ever-dynamic and changing requirements in the cybersecurity field. Many school modules/curricula may not effectively adapt to the ever-evolving nature and practical needs of this field, leading to many graduates feeling unprepared to enter the workforce as such, creating individuals who may have the theoretical knowledge, but lack the on-the-job training skills needed to tackle various security challenges.

This problem relates to our cybersecurity degree because effective and efficient training in this field will develop us as more than adequate professionals who can confidently address present day-to-day security issues. Our project serves to enhance and build upon the learning

provided to students by placing them in scenarios similar to on-the-job environments where they have to understand and tackle issues that they could encounter.

The significance of this project is its possibility to enhance cybersecurity education by providing a more practical and engaging learning method. Our project will better link the space between theoretical knowledge and real-world practical use through its provision of a more effective educational structure thus improving student's engagement, knowledge retention, and confidence to face real-world challenges in the present digital terrain.

Opportunities to explore:

Based on our project, there are multiple opportunities we could explore to address and reduce the issue of effectively preparing students such as:

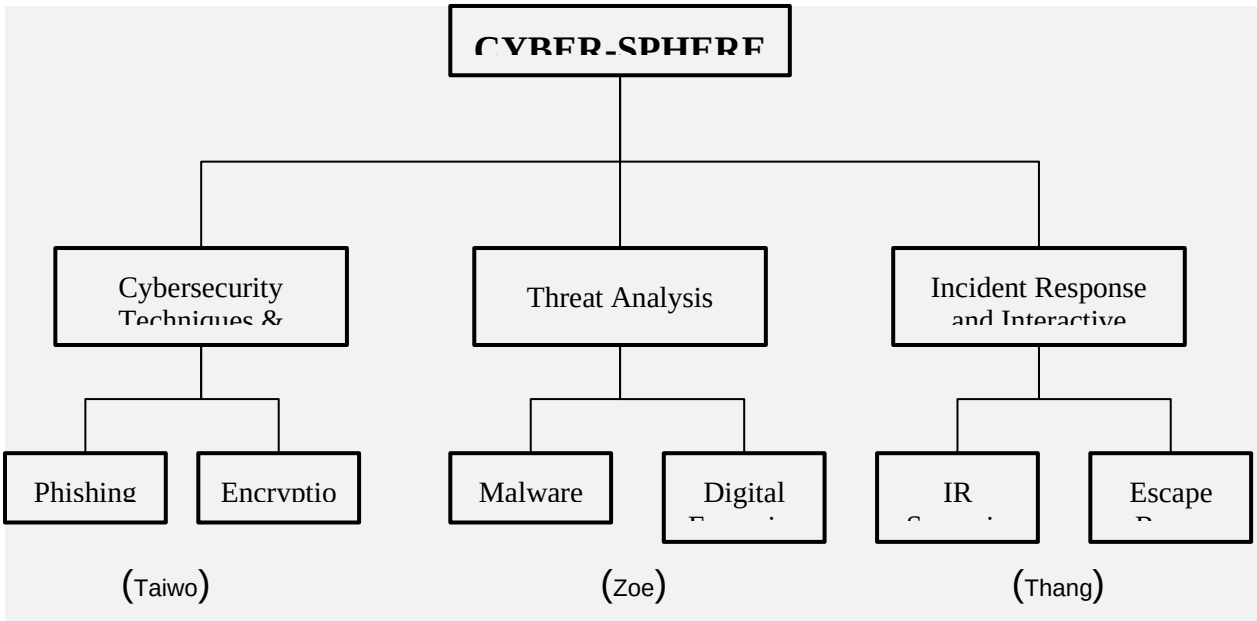
- Enhancing the current curriculum by incorporating real-world case studies and threat simulations could provide students with an investigative learning experience through the analysis of recent cybersecurity breaches whereby they could incorporate their theoretical knowledge to further solidify their understanding.
    - Research Outcome: Increased student engagement during classes as well as Improved Learning.
- Development of realistic incident response events through a fun and interactive game training environment which would bring in a fun and dynamic way of engaging students and polishing their skills (i.e. the use of an escape room that will be modeled after various cyber security concepts would challenge the user to perform various tasks such as solving puzzles related to digital forensics, encryption, and malware analysis thus providing a fun, hands-on, and practical experience in addressing and organizing incidents).

Project Proposal

- Research Outcome: Student's professional skill development and hands-on experience.

- Interactive Learning to enhance theoretical knowledge would prove invaluable and highly effective to the student. Using virtual reality to strengthen the topics/concepts covered such as simulated phishing attacks or cryptographic encryption techniques will aid students in identifying potential threats in a controlled environment as well as having a better grasp on data security.
    - Research Outcome: Curriculum and Learning Improvement.

Project goals (contributions of each team member):



- Incident Response and Iterative Training: This section will be covered by Thang. The user/student will be introduced to IR (Incident Response) scenarios and the Escape room offers an interactive way of simulating a real-world environment and teaches how to handle cybersecurity challenges.

Project Proposal

- Threat Analysis: This section will be covered by Zoe'. It offers an introduction to malware (Malicious Software) and in conjunction with digital forensics, digital evidence (i.e. an infected image) can be analyzed by the user/student to identify the tactics used by cybercriminals and help create an effective counter. The user/student will also learn about steganography by analyzing the infected image.
- Cybersecurity Techniques and Threats: This section will be covered by Taiwo. Phishing and Encryption are opposing sides of a coin. The user/student will learn about ways in which criminals use social engineering to steal data while also learning about techniques to protect data from such threats.

Value proposition (Why will the project outcomes matter?):

- Incident Response and Iterative Training will provide enhanced practical skills through user/student engagement in realistic incident response scenarios and escape room simulations. Thang's contribution will further develop the user/student and better prepare them for handling real-world challenges effectively creating more than adequate employees for employers while boosting the university's educational quality.
- Threat Analysis will strengthen a user/student's understanding of malware and forensics which is a crucial area in the field. Zoe's contribution will give the user/student the needed skills to analyze, address, and counter threats posed. Through the understanding of malware and threat analysis, companies will gain employees who can strengthen their overall security through data protection by detecting vulnerabilities/unknown access points.
- Cybersecurity Techniques and Threats: Taiwos contribution gives a stable balance of offense and defense by assisting the user/student in identifying phishing attacks as well as

Project Proposal

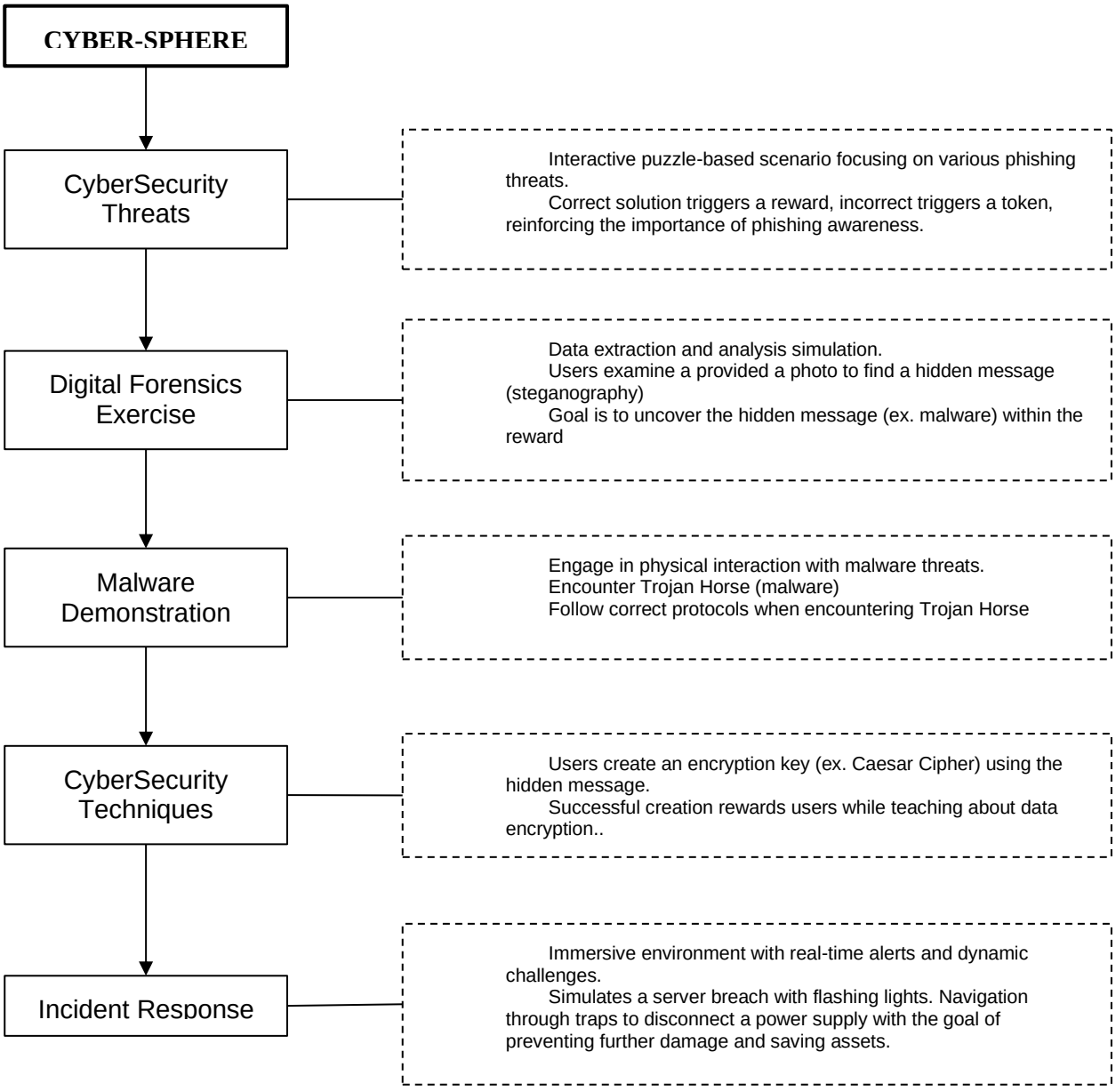
a method of countering them through data encryption which will prove invaluable to organizations as well as the student as it provides a solid foundation in the fundamentals of cybersecurity techniques.

Sample Image:

Cyber-Sphere: Our product is an immersive virtual reality training system created to improve cybersecurity education. It offers an opportunity for users to enter a simulated world where they can tackle realistic cybersecurity challenges while receiving an effective educational experience crucial in real-world scenarios.

The system will encompass a wide range of topics, including Cybersecurity Techniques for countering various Threats (Taiwo), Threat Analysis and Malware Identification (Zoe'), and Incident Response (Thang). Each of these is incorporated into an interactive virtual world to provide a comprehensive and refined summary of critical concepts.

Project Proposal



This innovative product will enhance both the educational field and students' practical knowledge and skills to ensure they are competent enough to meet current on-the-field demand.

Project Proposal

Proposed Weekly Milestones:

Week 1 (Sep 12 - Sep 18) - KickOff Meeting (Finalize Roles/Responsibilities), Setup Communication options and Project Management Tools, Role Research.

Week 2 (Sep 19 - Sep 25) - Research findings

Week 3 (Sep 26 - Oct 2) - Design Drafts for simulator, puzzle, scenario, etc.

Week 4 (Oct 3 - Oct 9) - Initial Prototype

Week 5 (Oct 10 - Oct 16) - Feedback and Iteration of prototype

Week 6 (Oct 17 - Oct 23) - Updated designs

Week 7 (Oct 24 - Oct 30) - VR Integration and testing

Week 8 (Oct 31 - Nov 6) - Controlled user testing feedback

Week 9 (Nov 7 - Nov 13) - Fine tuning and potential system enhancements

Week 10 (Nov 14 - Nov 20) - Finalized system/ quality assurance

Week 11 (Nov 21 - Nov 27) - Project documentation/Presentation

Week 12 (Nov 28 - Dec 4) - Rehearsal & Final Report