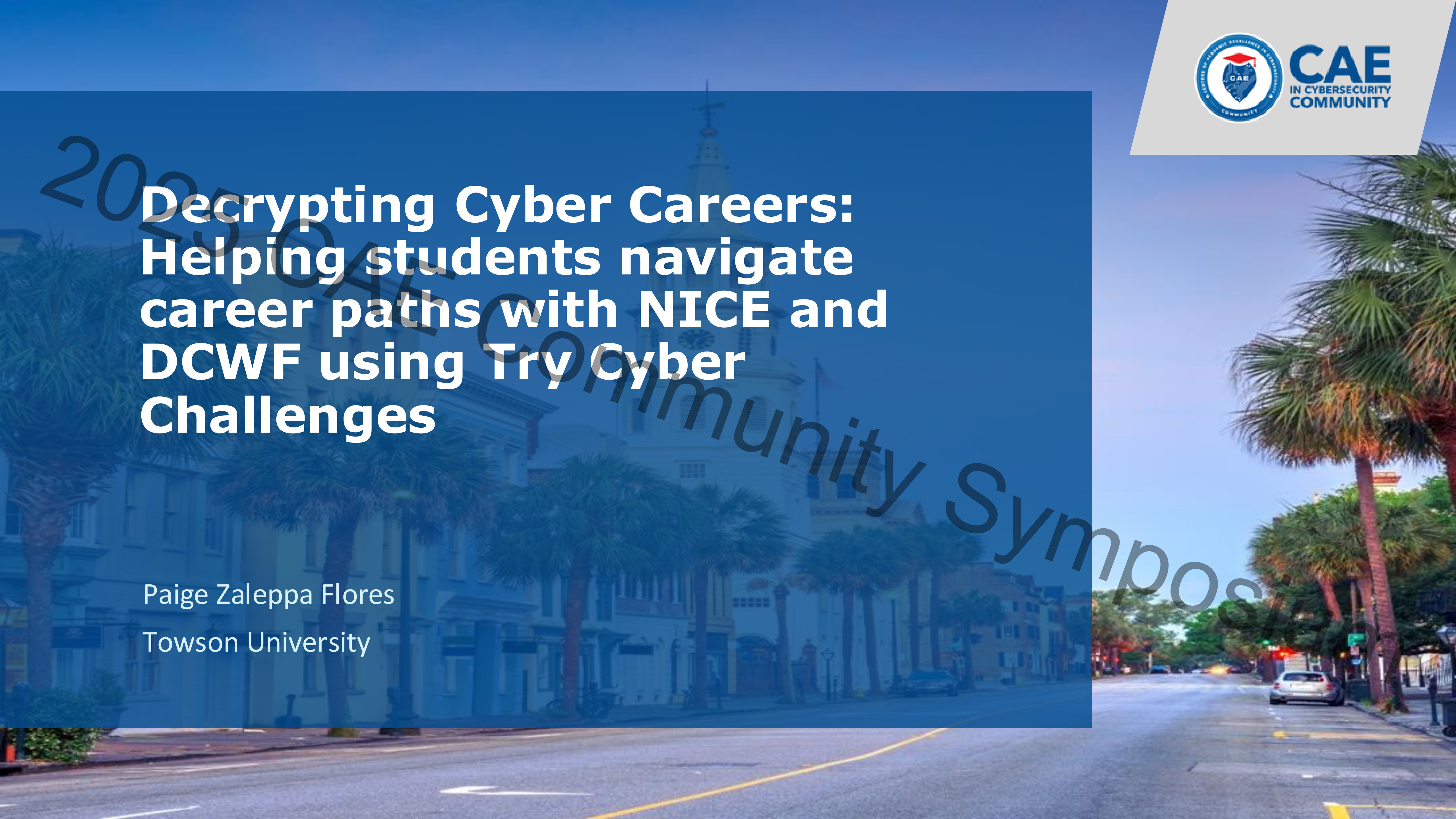


Decrypting Cyber Careers: Helping students navigate career paths with NICE and DCWF using Try Cyber Challenges

Paige Zaleppa Flores

Towson University

CIS 377: Introduction to Cybersecurity

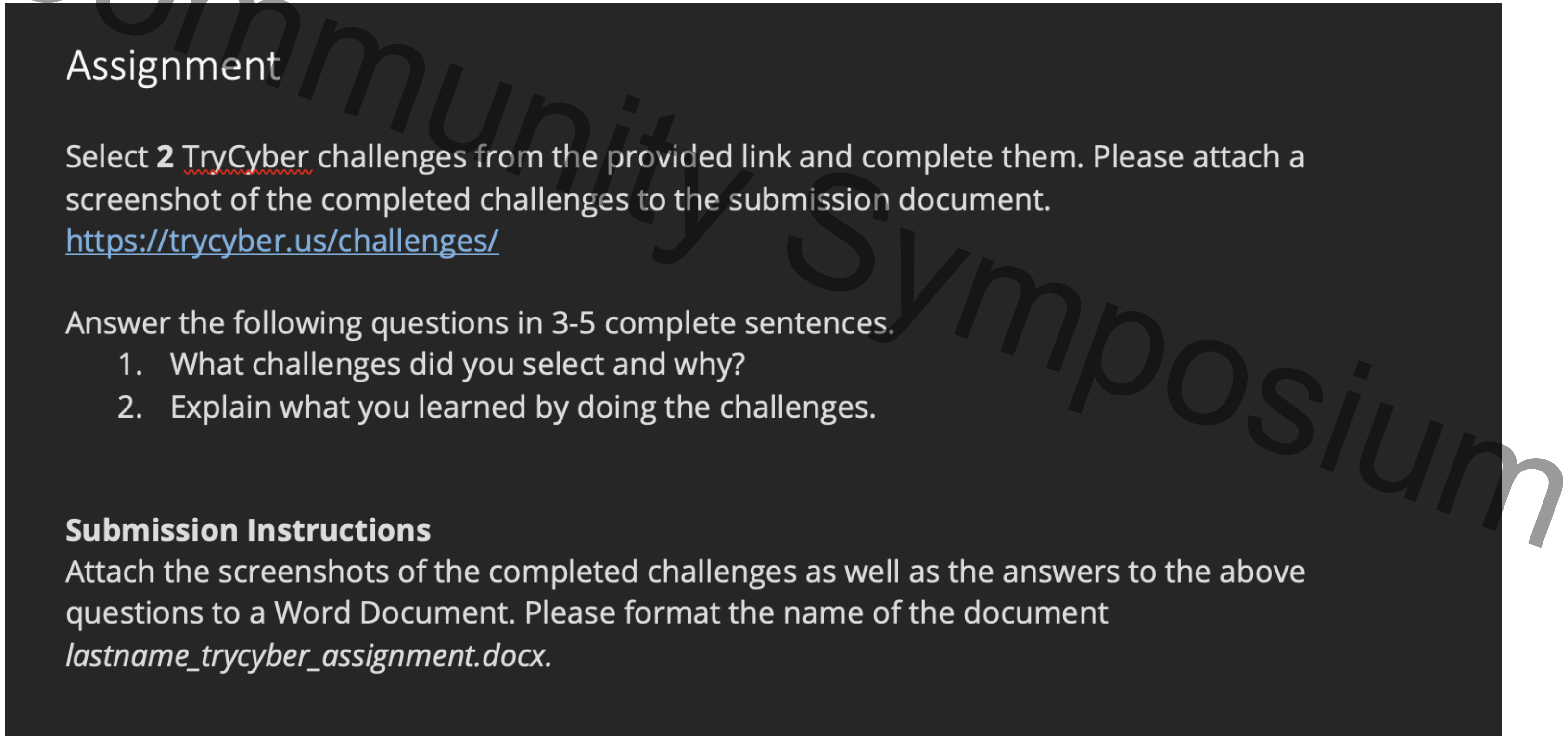
- Towson University Department of Computer and Information Sciences
- Required Course for:
  - Computer Science
    - Cyber Operations Track (CAE-CD and CAE-CO)
    - Software Engineering Track
  - Information Systems
    - Business Track
    - Data Analytics Track
    - Interface Design Track
    - Systems Track
  - Information Technology
    - Network Security Track
    - Data Management and Analytics Track

Course Structure

- Hybrid 15-week Course
  - 75 minutes of synchronous instruction per week
  - 75 minutes of asynchronous instruction per week
- Prerequisites
  - Sophomore standing in major or minor
- Topics Covered
  - Cyber Law and Policy
  - Cyber Warfare
  - Network Security
  - Social Engineering
  - Software Supply Chain
  - Risk Management
  - Incident Response
  - Digital Forensics
  - Cryptography
  - Cyber Careers

Cyber Careers Lesson

- Learning Outcomes:
  - Compare various work roles within cybersecurity.
  - Analyze the tasks expected of a work role and align those with your own skills.
  - Explain the skills and knowledge required of a specific cybersecurity work role.



Assignment

Select **2** TryCyber challenges from the provided link and complete them. Please attach a screenshot of the completed challenges to the submission document.
https://trycyber.us/challenges/

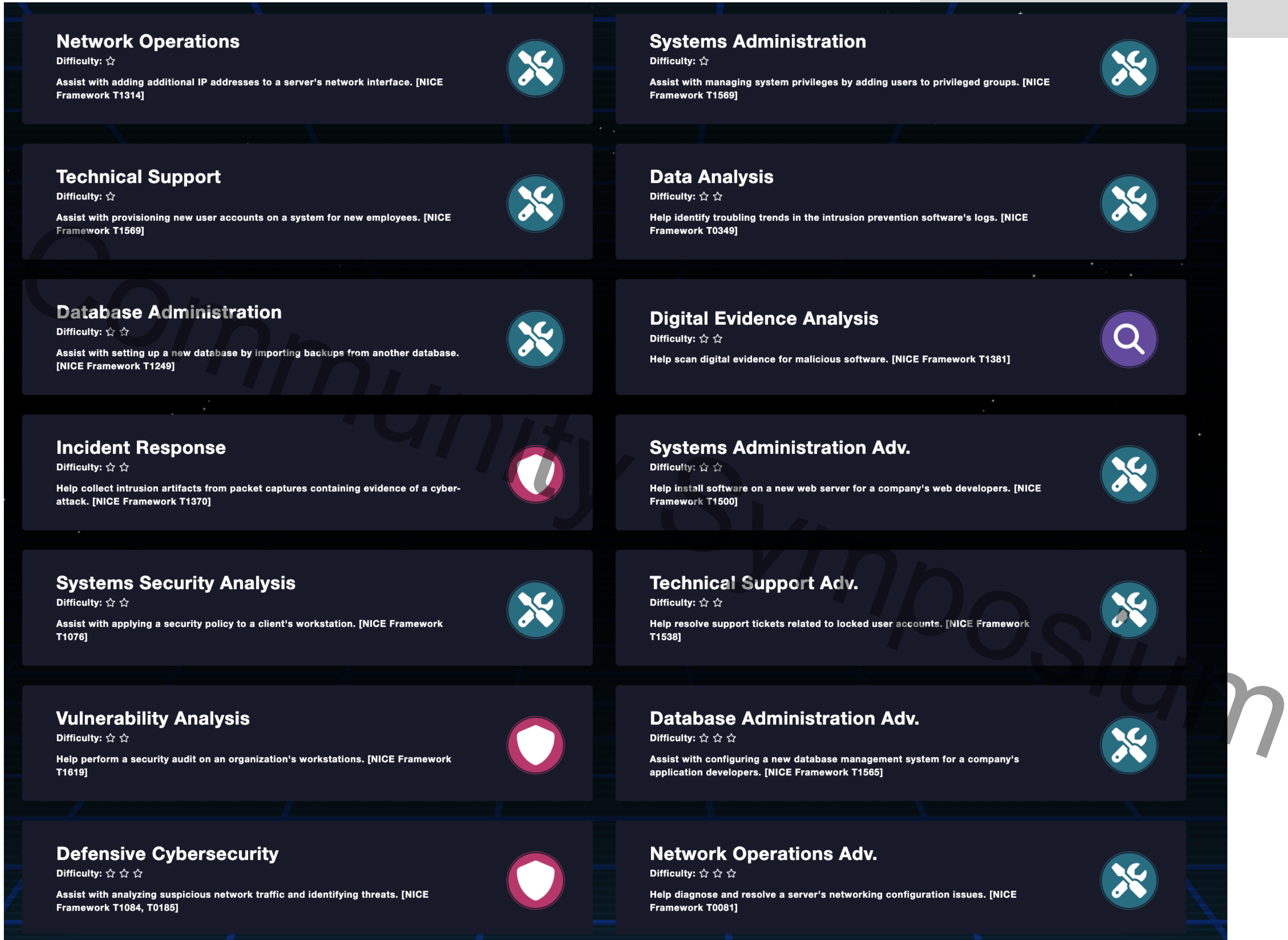
Answer the following questions in 3-5 complete sentences.

1. What challenges did you select and why?
2. Explain what you learned by doing the challenges.

Submission Instructions

Attach the screenshots of the completed challenges as well as the answers to the above questions to a Word Document. Please format the name of the document *lastname_trycyber_assignment.docx.*

Try Cyber Challenges



Network Operations
Difficulty: ☆
Assist with adding additional IP addresses to a server's network interface. [NICE Framework T1314]

Systems Administration
Difficulty: ☆
Assist with managing system privileges by adding users to privileged groups. [NICE Framework T1569]

Technical Support
Difficulty: ☆
Assist with provisioning new user accounts on a system for new employees. [NICE Framework T1569]

Data Analysis
Difficulty: ☆ ☆
Help identify troubling trends in the intrusion prevention software's logs. [NICE Framework T0349]

Database Administration
Difficulty: ☆ ☆
Assist with setting up a new database by importing backups from another database. [NICE Framework T1249]

Digital Evidence Analysis
Difficulty: ☆ ☆
Help scan digital evidence for malicious software. [NICE Framework T1381]

Incident Response
Difficulty: ☆ ☆
Help collect intrusion artifacts from packet captures containing evidence of a cyber-attack. [NICE Framework T1370]

Systems Administration Adv.
Difficulty: ☆ ☆
Help install software on a new web server for a company's web developers. [NICE Framework T1500]

Systems Security Analysis
Difficulty: ☆ ☆
Assist with applying a security policy to a client's workstation. [NICE Framework T1076]

Technical Support Adv.
Difficulty: ☆ ☆
Help resolve support tickets related to locked user accounts. [NICE Framework T1538]

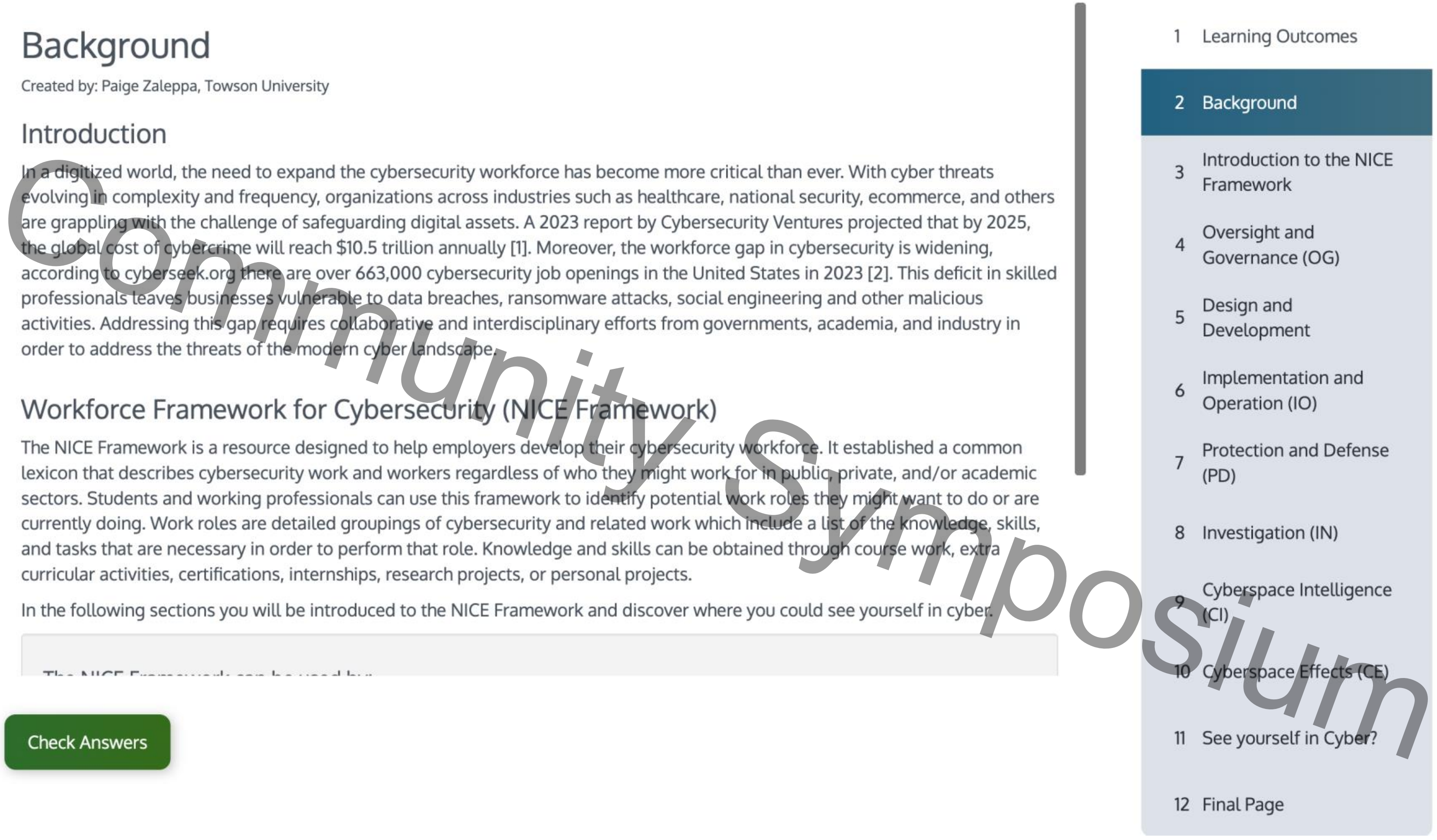
Vulnerability Analysis
Difficulty: ☆ ☆
Help perform a security audit on an organization's workstations. [NICE Framework T1619]

Database Administration Adv.
Difficulty: ☆ ☆ ☆
Assist with configuring a new database management system for a company's application developers. [NICE Framework T1565]

Defensive Cybersecurity
Difficulty: ☆ ☆ ☆
Assist with analyzing suspicious network traffic and identifying threats. [NICE Framework T1084, T0185]

Network Operations Adv.
Difficulty: ☆ ☆ ☆
Help diagnose and resolve a server's networking configuration issues. [NICE Framework T0081]

Additional Resources



Background

Created by: Paige Zaleppa, Towson University

Introduction

In a digitized world, the need to expand the cybersecurity workforce has become more critical than ever. With cyber threats evolving in complexity and frequency, organizations across industries such as healthcare, national security, ecommerce, and others are grappling with the challenge of safeguarding digital assets. A 2023 report by Cybersecurity Ventures projected that by 2025, the global cost of cybercrime will reach $10.5 trillion annually [1]. Moreover, the workforce gap in cybersecurity is widening, according to cyberseek.org there are over 663,000 cybersecurity job openings in the United States in 2023 [2]. This deficit in skilled professionals leaves businesses vulnerable to data breaches, ransomware attacks, social engineering and other malicious activities. Addressing this gap requires collaborative and interdisciplinary efforts from governments, academia, and industry in order to address the threats of the modern cyber landscape.

Workforce Framework for Cybersecurity (NICE Framework)

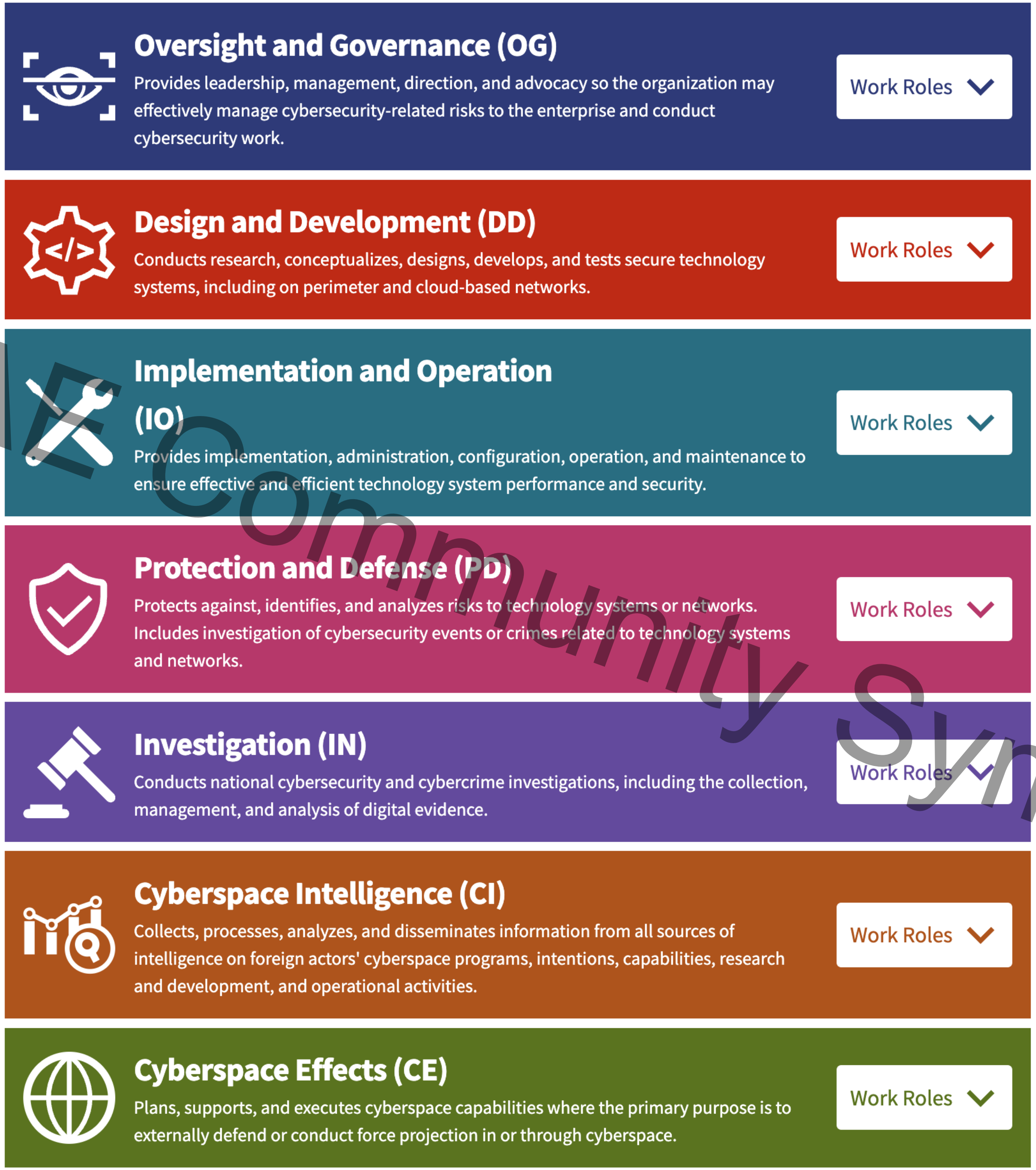
The NICE Framework is a resource designed to help employers develop their cybersecurity workforce. It established a common lexicon that describes cybersecurity work and workers regardless of who they might work for in public, private, and/or academic sectors. Students and working professionals can use this framework to identify potential work roles they might want to do or are currently doing. Work roles are detailed groupings of cybersecurity and related work which include a list of the knowledge, skills, and tasks that are necessary in order to perform that role. Knowledge and skills can be obtained through course work, extra curricular activities, certifications, internships, research projects, or personal projects.

In the following sections you will be introduced to the NICE Framework and discover where you could see yourself in cyber.

The NICE Framework can be used by:

https://security-injections.clark.center/Interdisciplinary-Intro_to_Cyber.html

Additional Resources



Oversight and Governance (OG)

Provides leadership, management, direction, and advocacy so the organization may effectively manage cybersecurity-related risks to the enterprise and conduct cybersecurity work.

Design and Development (DD)

Conducts research, conceptualizes, designs, develops, and tests secure technology systems, including on perimeter and cloud-based networks.

Implementation and Operation (IO)

Provides implementation, administration, configuration, operation, and maintenance to ensure effective and efficient technology system performance and security.

Protection and Defense (PD)

Protects against, identifies, and analyzes risks to technology systems or networks. Includes investigation of cybersecurity events or crimes related to technology systems and networks.

Investigation (IN)

Conducts national cybersecurity and cybercrime investigations, including the collection, management, and analysis of digital evidence.

Cyberspace Intelligence (CI)

Collects, processes, analyzes, and disseminates information from all sources of intelligence on foreign actors' cyberspace programs, intentions, capabilities, research and development, and operational activities.

Cyberspace Effects (CE)

Plans, supports, and executes cyberspace capabilities where the primary purpose is to externally defend or conduct force projection in or through cyberspace.

https://niccs.cisa.gov/workforce-development/nice-framework

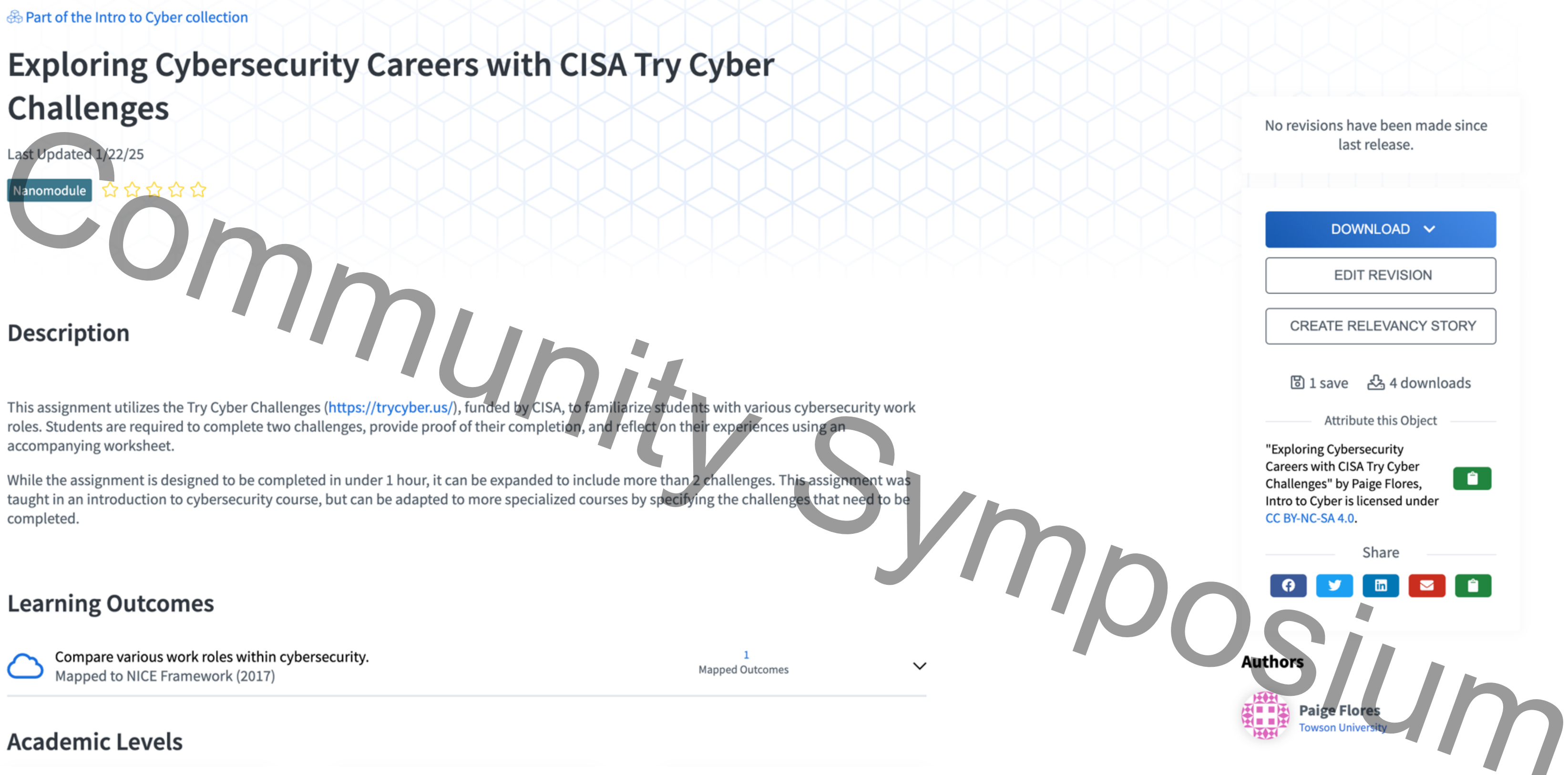
Student Feedback

TRY CYBER
https://trycyber.us/
Finish a challenge and receive a entry for the prize drawing every 20 minutes!
LOVE YOU
CUTIE PIE

- Learning Outcomes:
  - Compare various work roles within cybersecurity.
  - Analyze the tasks expected of a work role and align those with your own skills.
  - Explain the skills and knowledge required of a specific cybersecurity work role.

TRY CYBER
Finish a challenge and receive a entry for the prize drawing at 1:30PM!

Lesson Available on CLARK



Part of the Intro to Cyber collection

Exploring Cybersecurity Careers with CISA Try Cyber Challenges

Last Updated 1/22/25

Nanomodule ☆☆☆☆☆

Description

This assignment utilizes the Try Cyber Challenges (https://trycyber.us/), funded by CISA, to familiarize students with various cybersecurity work roles. Students are required to complete two challenges, provide proof of their completion, and reflect on their experiences using an accompanying worksheet.

While the assignment is designed to be completed in under 1 hour, it can be expanded to include more than 2 challenges. This assignment was taught in an introduction to cybersecurity course, but can be adapted to more specialized courses by specifying the challenges that need to be completed.

Learning Outcomes

Compare various work roles within cybersecurity.
Mapped to NICE Framework (2017)

1
Mapped Outcomes

Academic Levels

No revisions have been made since last release.

1 save 4 downloads

Attribute this Object

"Exploring Cybersecurity Careers with CISA Try Cyber Challenges" by Paige Flores, Intro to Cyber is licensed under CC BY-NC-SA 4.0.

Authors

Paige Flores
Towson University

https://clark.center/details/pzalep1/09ae8f70-4b6d-46b9-b4bf-ce4f2bbc5867/0