ST. JOHN'S
UNIVERSITY

Exploring NCAE cyber competencies under ABET student outcomes framework

ABET | Computing Accreditation Commission

What is a Cybersecurity competency?

Cybersecurity competency is defined as the **ability of a student to perform a Cybersecurity task within the context of Cybersecurity work role**!

Why are Cybersecurity competencies important?

New regulations in NCAE designation require all NSA validated programs, in our case UG/GR, to define and implement 10 competencies by 2026!

After 2026 we MUST also measure the defined 10 competencies.

Where and how will 10 Cybersecurity competencies be defined, implemented, measured?

5 competencies must be defined, implemented, measured in the classroom

5 competencies must be defined, implemented, measured either through internships or through cybersecurity competitions

NSA won't allow all 10 to be defined, implemented, measured in the classroom!

Anatomy of a Cybersecurity competency through ABCDE framework

A Actor Who is involved in this competency? What background knowledge/ experience/previous learning are necessary for this competency?

Anatomy of a Cybersecurity competency through ABCDE framework

B Behavior/task What is being done? Maps directly onto tasks from either the DoD's DCWF or the NICE framework.

Anatomy of a Cybersecurity competency through ABCDE framework

C Context How is this task being done? With what resources, affordances and constraints?

Anatomy of a Cybersecurity competency through ABCDE framework

D Degree How long should this task take to complete? How accurate does it need to be? What degree of completion would be acceptable to an employer?

Anatomy of a Cybersecurity competency through ABCDE framework

E Employability What professional skills are also embedded in this practice (e.g. team work, collaboration, ethics etc.)?

ABET / Cybersecurity competencies interaction

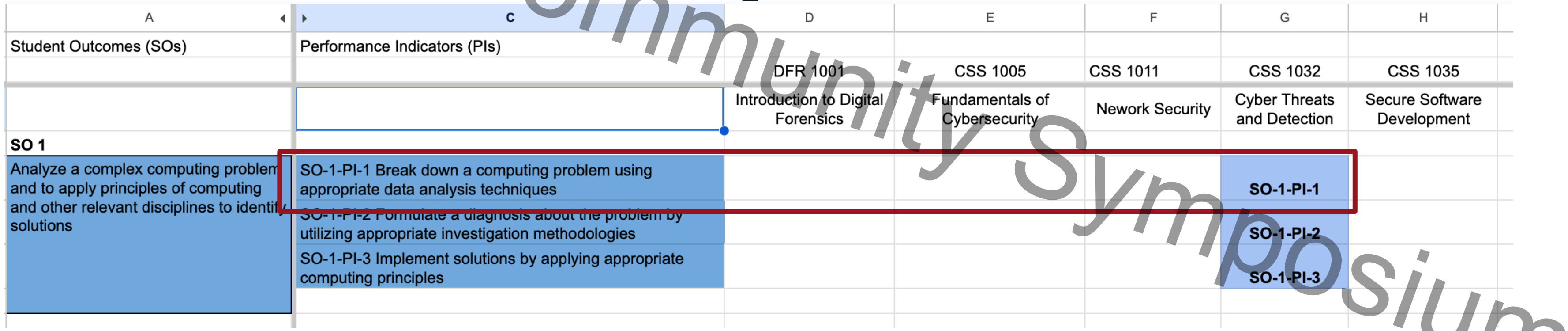
Worst case scenario: PDs tasked with performing ABET Performance Indicator measurement AND performing Cybersecurity competencies measurement = analysis paralysis!

ABET / Cybersecurity competencies interaction

Best case scenario: Chance to be **clever** and use ABET Performance Indicators as the basis for defining, implementing, measuring Cybersecurity competencies in the classroom!

ABET / Cybersecurity competencies interaction

UG first Cybersecurity competency defined, implemented, and assessed based on current re-aligned ABET PI measurement:



A	C	D	E	F	G	H
Student Outcomes (SOs)	Performance Indicators (PIs)					
		DFR 1001	CSS 1005	CSS 1011	CSS 1032	CSS 1035
		Introduction to Digital Forensics	Fundamentals of Cybersecurity	Nework Security	Cyber Threats and Detection	Secure Software Development
SO 1						
Analyze a complex computing problem and to apply principles of computing and other relevant disciplines to identify solutions	SO-1-PI-1 Break down a computing problem using appropriate data analysis techniques				**SO-1-PI-1**	
	SO-1-PI-2 Formulate a diagnosis about the problem by utilizing appropriate investigation methodologies				**SO-1-PI-2**	
	SO-1-PI-3 Implement solutions by applying appropriate computing principles				**SO-1-PI-3**	

SO1-PI-1-Vulnerability Analysis-Penetration Testing

Type of Activity: Classroom

Actor: A fourth year student majoring in Cyber Security Systems enrolled in CSS 1032 Cyber Threats and Defense course.

SO1-PI-1-Vulnerability Analysis-Penetration Testing

Behavior:

Workforce Framework: NICE WORKFORCE FRAMEWORK FOR CYBERSECURITY

Work Role: Vulnerability Assessment Analyst

Task: T0028 - Conduct and/or support authorized penetration testing on enterprise network assets.

SO1-PI-1-Vulnerability Analysis-Penetration Testing

Context: The students are assumed to be working on relatively small groups of maximum 3 team members. The students are introduced to a fictitious network environment which contains multiple vulnerable devices attached to it. The students are assumed to be "gifted" terminal access onto the network from where they will start their enumeration process and vulnerability assessment.

Technology: Linux terminal access, Nmap port discovery, Nessus vulnerability finder, Armitage/Metasploit

Documentation: Lab manual

Limitations: Students should be in the confines of the Cybercurity lab without access to any other tools expect as specified on the lab guidelines.

SO1-PI-1-Vulnerability Analysis-Penetration Testing

Degree: The student should score at least 80% on the activity which will be measured through various metrics such as the degree to identify vulnerable hosts, vulnerable services, and the student's ability to summarize how to ethically disclose any reconnaissance findings according to the principles of ethical hacking.

SO1-PI-1-Vulnerability Analysis-Penetration Testing

Employability: The professional soft skills of this competency are: Critical thinking, Communication, Teamwork as follows.

Critical thinking: Students are expected to utilize critical thinking during the network mapping and enumeration process

Communication: Students are expected to be effective communicators and relay any vulnerability findings to the concerned stakeholders based on ethical principles

Teamwork: Students are expected to rotate tasks during the duration of the activity ranging from note takers, to technical leads, to research leads within the team