WASHINGTON STATE UNIVERSITY

AN ANALYSIS OF CYBERSECURITY EDUCATION IN THE UNITED STATES

JAMES CRABB

5/20/2024

Overview

- Motivation
- Important Frameworks
- Analysis of Top U.S. Cybersecurity Programs
- Analysis of Cybersecurity Education Research
- Analysis of Cybersecurity Curricular Frameworks
- Analysis & Mapping of WSU’s Cybersecurity Program

Motivation

- Cybersecurity protects the **technologies** we rely on daily.
- It is a constantly **evolving** landscape.
- There appears to be a **skill gap** between college graduates and cybersecurity professionals.
- This highlights a need for periodic **reviews** of cybersecurity education AND more fundamental **research**.

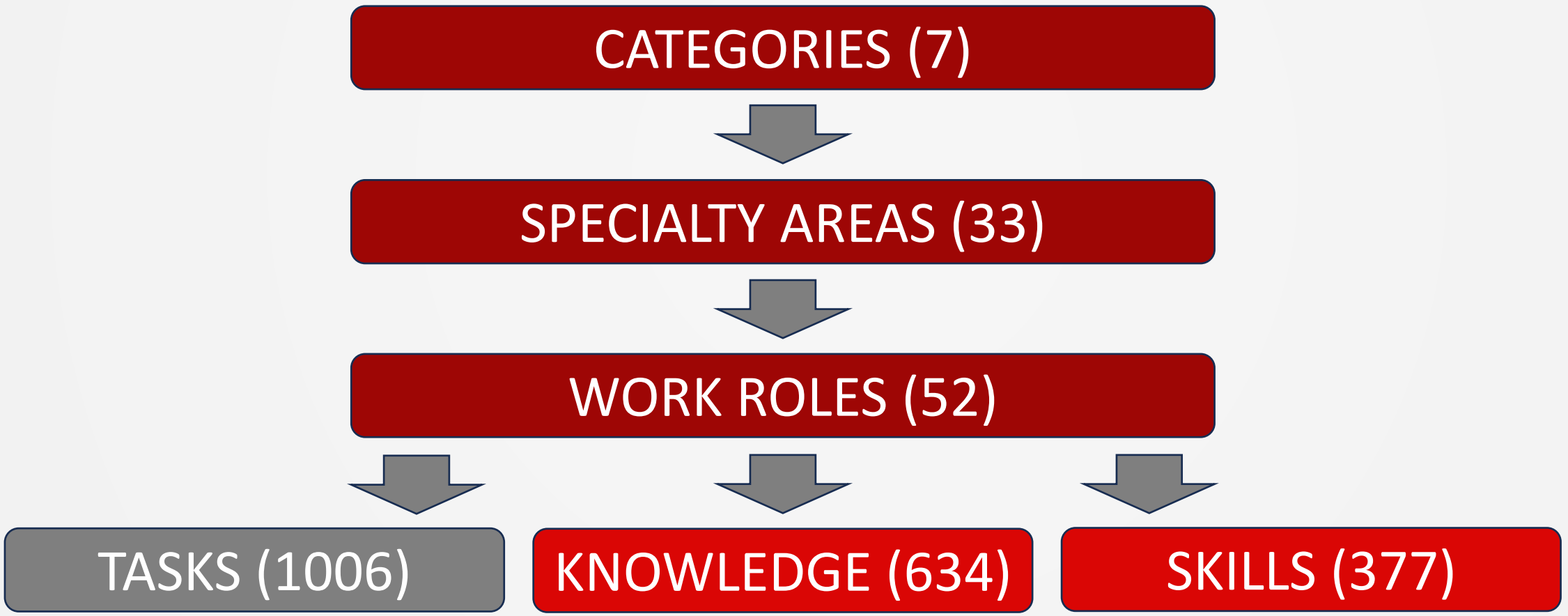
Frameworks

- NICE Framework
- CAE-C
- CSEC2017

NICE Framework

- National Initiative for Cybersecurity Education (NICE).
- Run by National Institute for Standards and Technology (NIST) .
- Published the Workforce Framework for Cybersecurity referred to as the NICE Framework.
- Reference Spreadsheet enumerating many important jobs.

NICE Framework



NICE Framework

Task Descriptions:

- Perform security reviews, identify gaps in security architecture, and develop a security risk management plan.
- Verify and update security documentation reflecting the application/system security design features.
- Analyze candidate architectures, allocate security services, and select security mechanisms.
- Develop threat model based on customer interviews and requirements.

Centers for Academic Excellence in Cybersecurity

- Operated by the NSA and DHS, includes partnerships with various other government bodies such as the NSF, FBI, NICE, and DoD.
- Goal is to help academic institutions in the United States provide training and education in cybersecurity at a high level and meet workforce needs.
- Designations
  - CAE Cyber Defense
  - CAE Cyber Operations
  - CAE Research

CAE-C

Cyber Defense (CAE-CD) Knowledge Units

- Foundational (all req.)
  - Cybersecurity Foundations
  - Cybersecurity Principles
  - IT Systems Components
- Technical Core (all req. or)
  - Basic Cryptography
  - Basic Networking
  - Basic Scripting and Programming
  - Network Defense
- Non-Technical Core (all req. or)
  - Cyber Threats
  - Cybersecurity Planning & Mgmt
  - Policy, Legal, Ethics, Compliance
  - Security Program Mgmt
  - Security Risk Analysis
- Optional (56 total, 14 or 3 req.)
  - Cloud Computing
  - Supply Chain Security

CAE-C

Cyber Defense (CAE-CD) Knowledge Unit Outcomes

- Foundational
  - Cybersecurity Foundations
    - Describe the fundamental concepts of the cybersecurity discipline and use to provide system security.
    - Describe potential system attacks and the actors that might perform them.
    - Describe cyber defense tools, methods and components and apply cyber defense methods to prepare a system to repel attacks.
    - Describe appropriate measures to be taken should a system compromise occur.
    - Properly use the Vocabulary associated with cybersecurity.

CAE-C

Cyber Operations (CAE-CO) Knowledge Units

- Mandatory (all 10 req.)
  - Low Level Prog. Languages
  - Software Rev. Engineering
  - OS Theory
  - Networking
  - Cellular/Mobile Tech
  - Discrete Math & Algs.
  - Overview of Cyber Defense
  - Security Fund. Principles
  - Vulnerabilities
  - Legal & Ethics
- Optional (17 total, 10 offered, 4 taken)
  - Applied Cryptography
  - Cloud Security/Computing
  - Computer Architecture
  - Digital Forensics
  - Embedded Systems
  - Hardware Rev. Engineering
  - Industrial Control Systems
  - Microcontroller Design

Cybersecurity Curricula 2017

- Joint effort between ACM, IEEE, others.
- Additional funding from NSF, NSA, Intel
- Global Advisory Board: academic
- Industrial Advisory Board: Google, Microsoft, IBM, others
- Knowledge Area Working Groups: academia, industry, military
- Goal of providing curricular guidance for cybersecurity programs.
- Lists NICE Framework as a major source in its development.
- Used by ABET to set curricular requirements

CSEC2017

Cross-Cutting Concepts

- Confidentiality
- Integrity
- Availability
- Risk
- Adversarial Thinking
- Systems Thinking

Knowledge Areas

- Data Security
- Software Security
- Component Security
- Connection Security
- System Security
- Human Security
- Organizational Security
- Societal Security

CSEC2017

Learning Outcomes: Data Security

- Describe the purpose of cryptography and list ways it is used in data communications.
- Describe the following terms: cipher, cryptanalysis, cryptographic algorithm, and cryptology, and describe the two basic methods (ciphers) for transforming plaintext in ciphertext.
- Explain how public key infrastructure supports digital signing and encryption and discuss the limitations/vulnerabilities.
- Discuss the dangers of inventing one's own cryptographic methods.
- Describe which cryptographic protocols, tools and techniques are appropriate for a given situation.

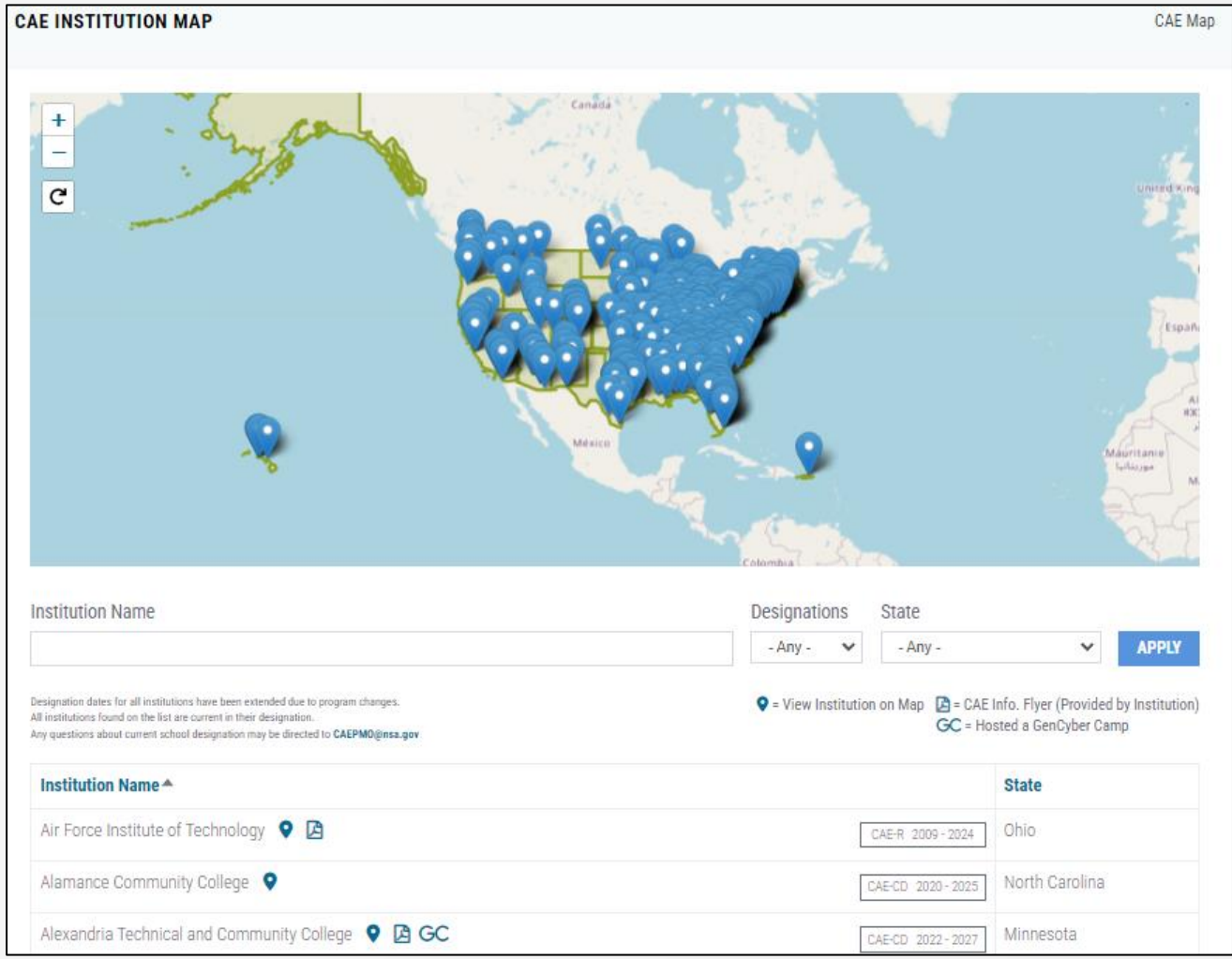
Analysis of Top U.S. Cybersecurity Programs

CAE-C Institutions

WASHINGTON STATE UNIVERSITY

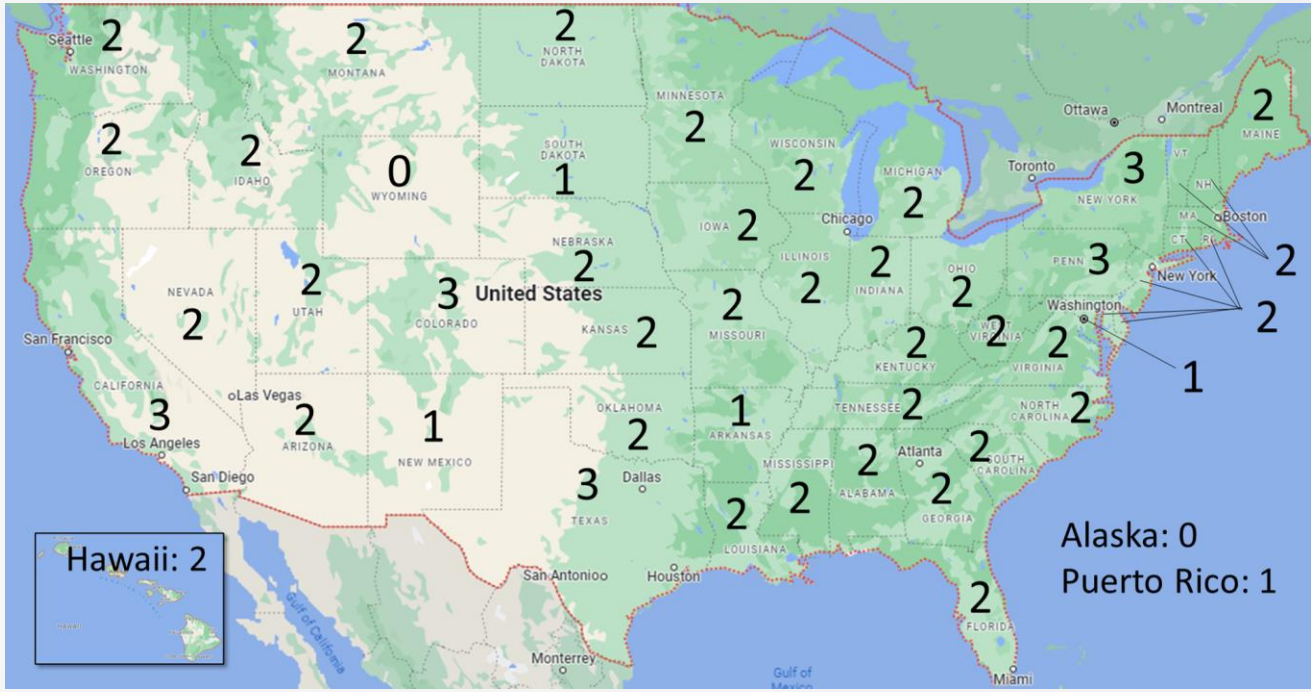
CAE-C Programs

- CAE Community manages a CAE Institution Map
- https://caecommunity.org/cae-map
- 377 institutions with current designations



Samples Used in This Study

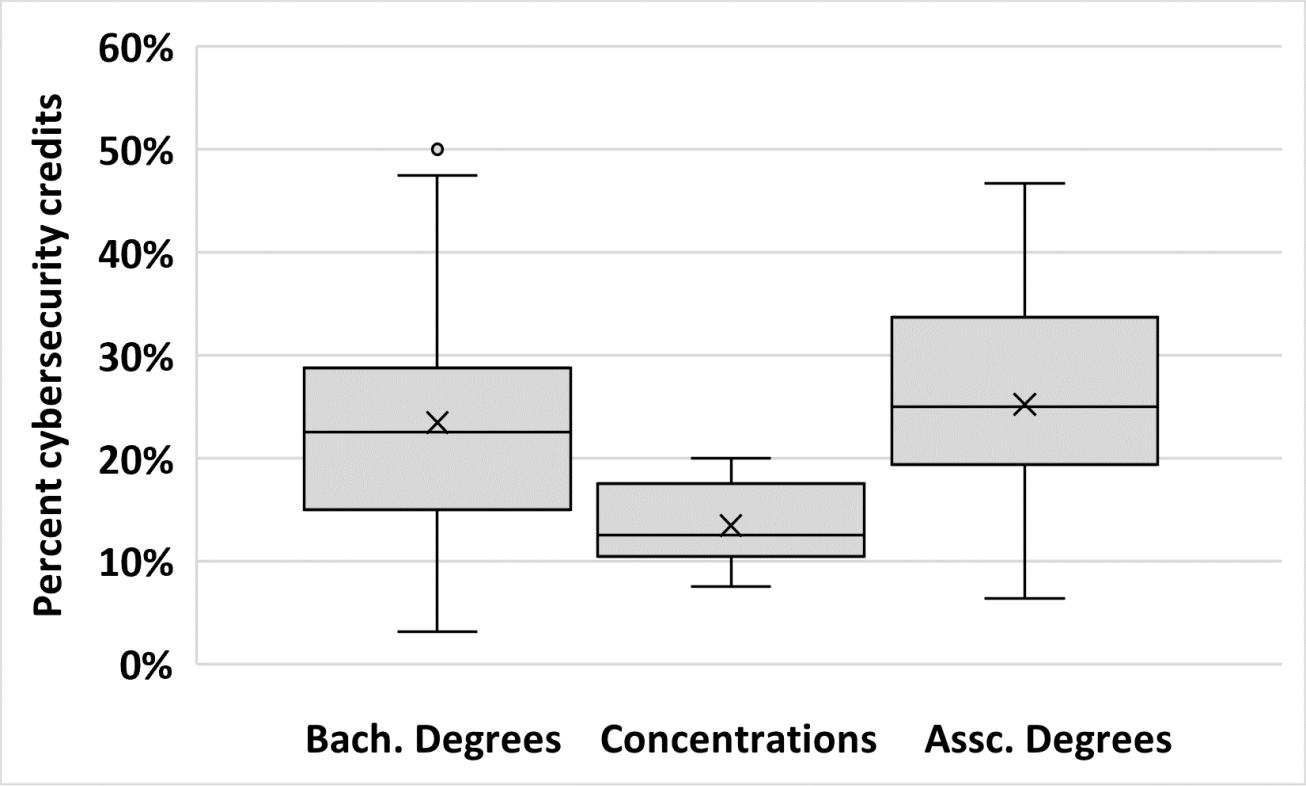
- Nation-wide view
- 100 institutions total
- 2 from each state/region



Number of sampled CAE-C institutions in each state/area. Background map credit: Google Maps.

Results: Cyber Credits

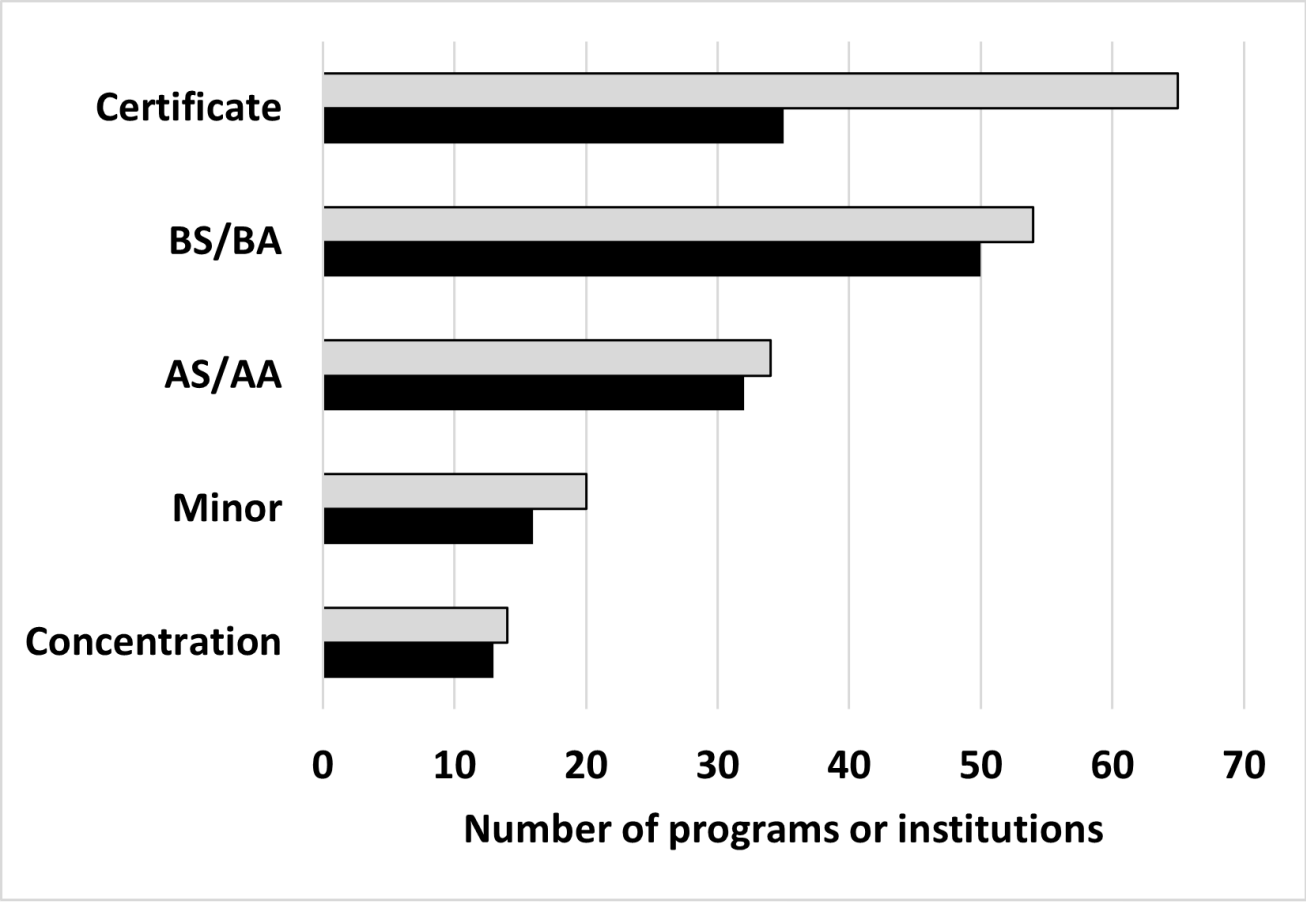
- Lots of variation between programs in terms of cybersecurity-specific courses required by the curricula.
- High flexibility in CAE-CD required Knowledge Units.



Percent of total required credits from cybersecurity courses.

Results: Program Types

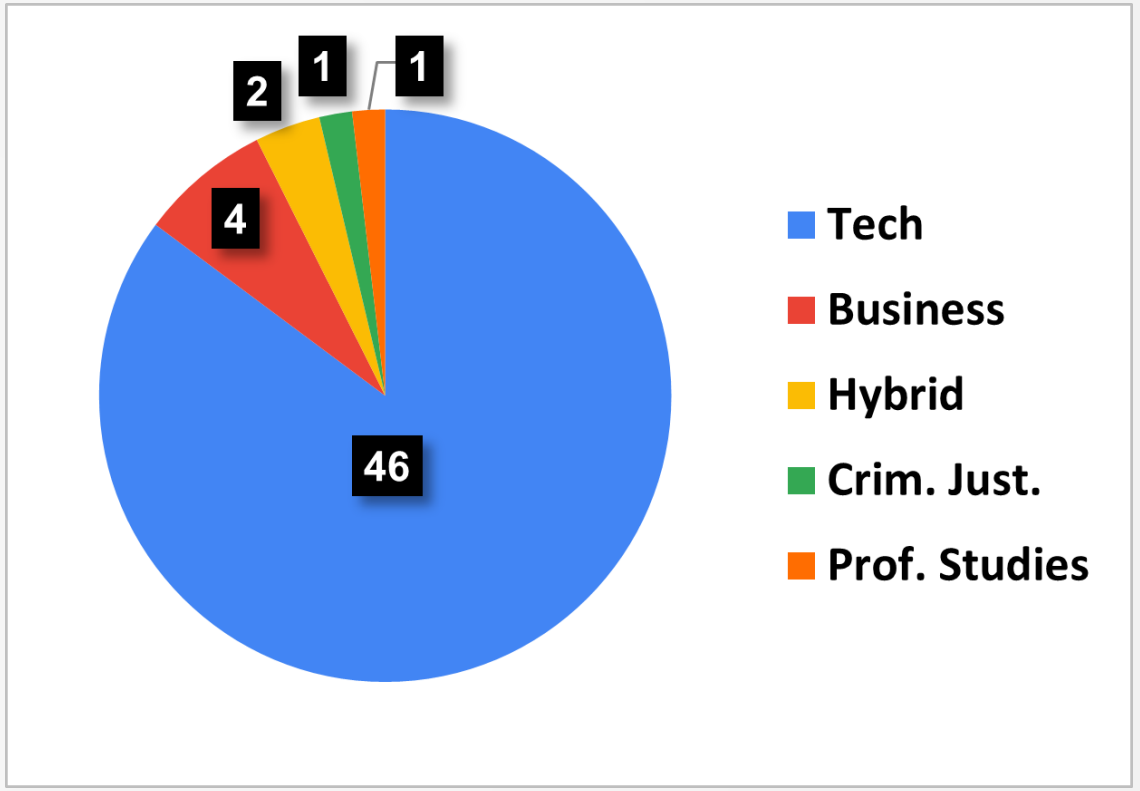
- 50 institutions offered Bachelor's Degrees
- 35 offered certificates
- 32 offered Associate Degrees
- 16 offered minors
- 14 offered concentrations



Number of programs offered by sampled CAE-C institutions. Gray bars: number of programs. Black bars: number of institutions.

Results: Organization

- Most programs are housed in Computer Science-, Technology-, or Engineering-type organizations (a college, school or department).
- Couldn't always tell a program's organization.
- "Hybrid" = Tech + Business



Number of programs housed by college/school.

Results: Program "Promotion"

- Most program titles are, or include the word, "Cybersecurity"
- 46 programs advertise their CAE designation.
- 8 refer to the NICE Framework.
- 2 refer to the CSEC2017.
- 26 list overall program learning outcomes.
- 20 list appropriate job titles.

Analysis of Cybersecurity Education Research

Content, Tools, Methods

WASHINGTON STATE UNIVERSITY

Samples

- Limited to last ten years (2014 - 2023)
- “cyber*” AND “educat*”
- Sorted by relevance
- Inclusion requires reporting on content, tool, or method
- ACM Digital Libraries: screened 51 papers to find 25
- IEEE Xplore: screened 80 papers to find 25

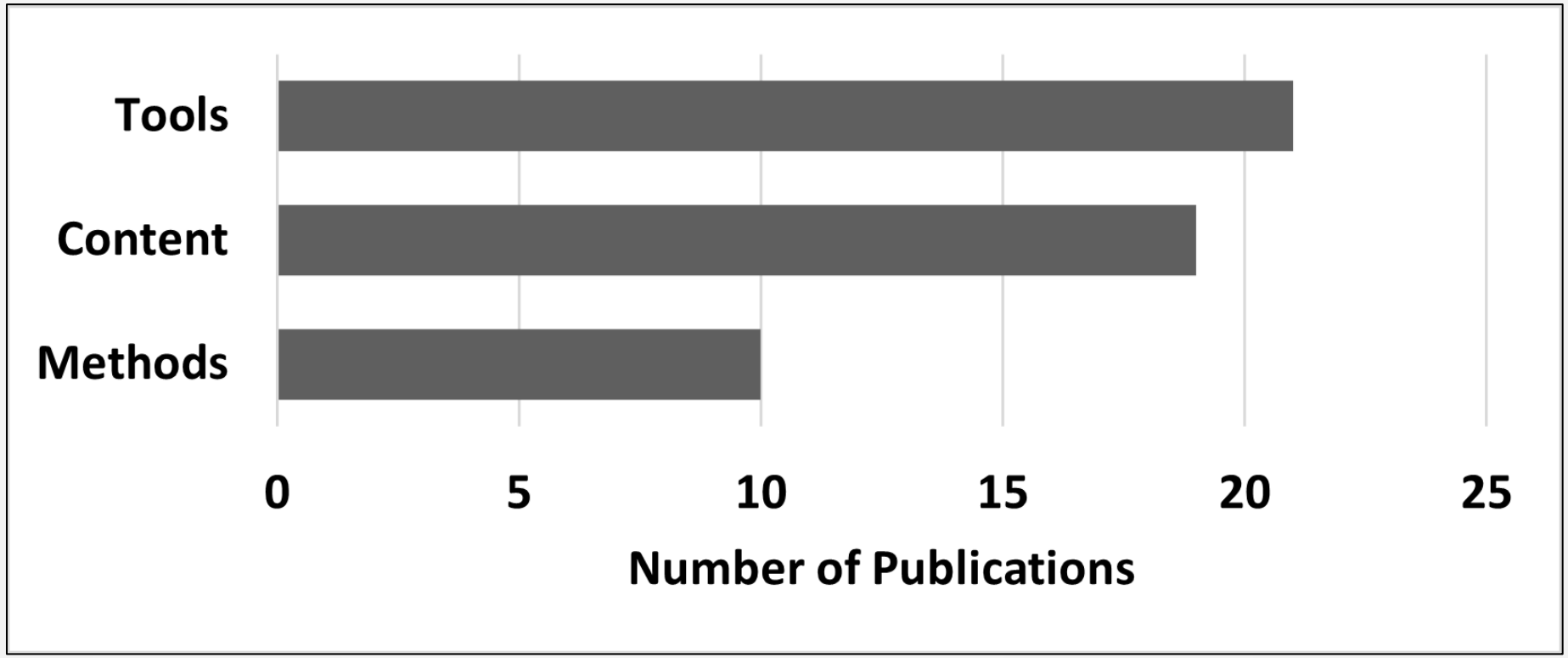
Results

21

19

10

8*



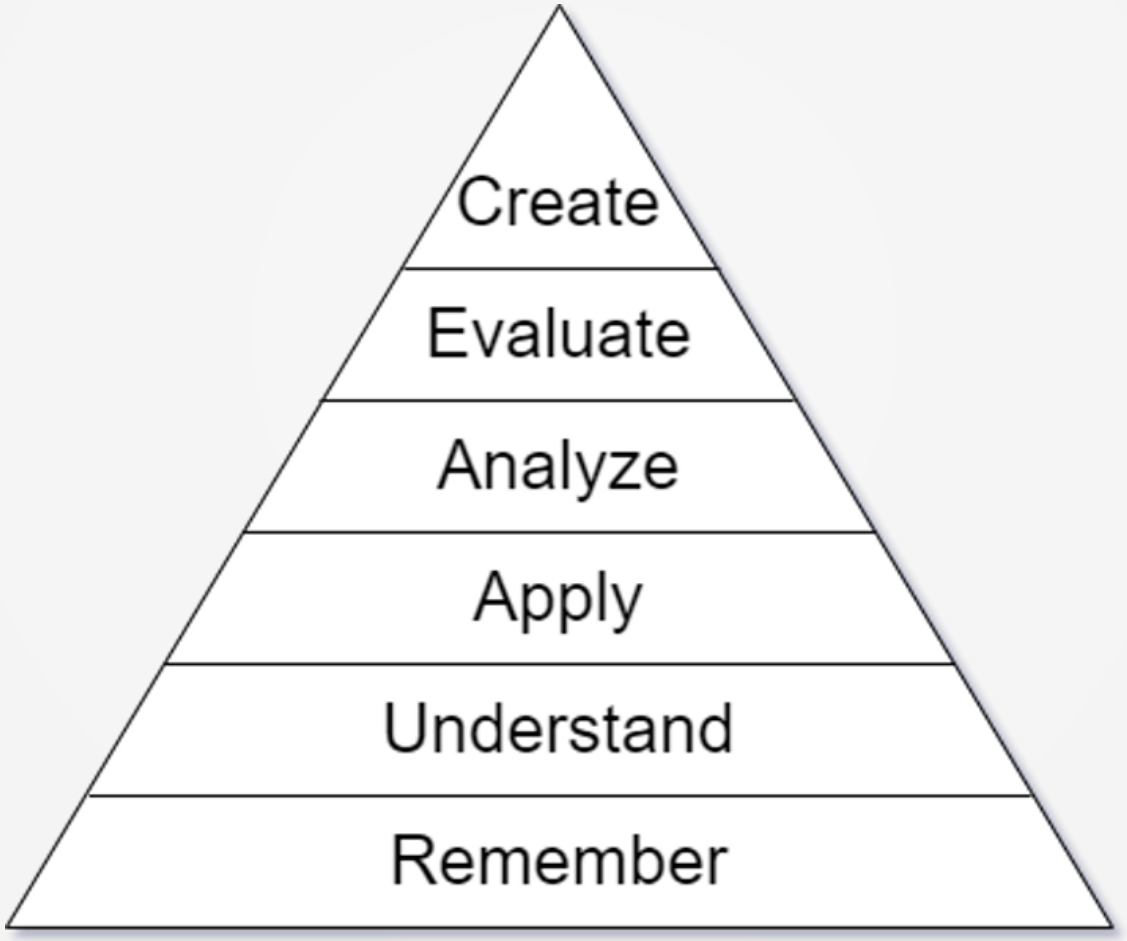
*: empirical studies (Methods - 6, Tools - 2)

Analysis of Cybersecurity Curricular Frameworks

NICE, CAE-C, CSEC2017

WASHINGTON STATE UNIVERSITY

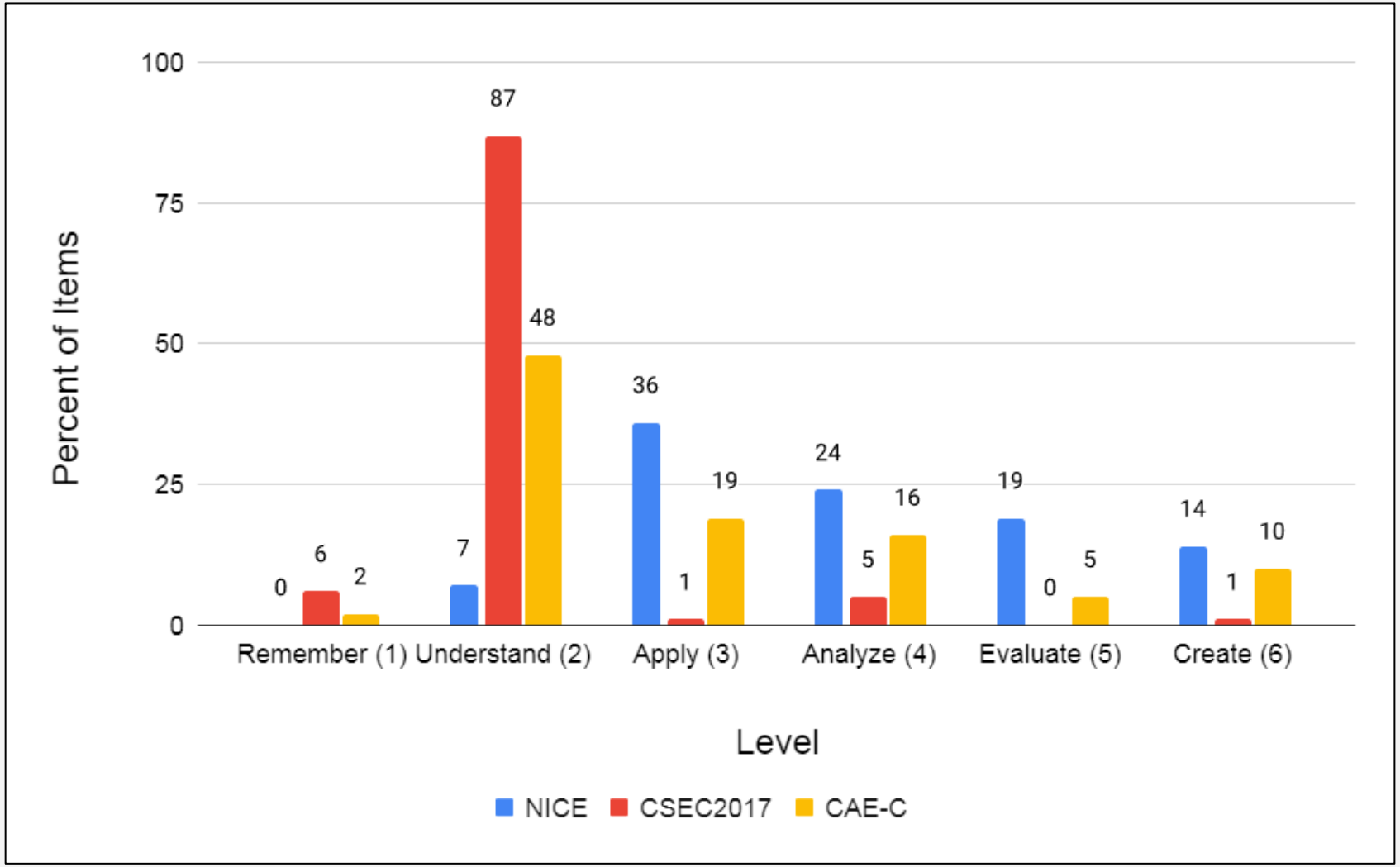
Bloom's Revised Taxonomy



Samples

- NICE Framework
  - 270 out of 1006 Task Descriptions
  - All TDs for 10 Work Roles, at least 1 from each Category
- CSEC2017
  - All 140 Learning Outcomes from all Knowledge Areas
- CAE-C
  - All 269 Learning Outcomes from all Knowledge Units (CD & CO)

Results


100
75
50
25
0
Percent of Items
0
6
2
7
87
48
36
1
19
24
5
16
19
0
5
14
1
10
Remember (1)
Understand (2)
Apply (3)
Analyze (4)
Evaluate (5)
Create (6)
Level
NICE
CSEC2017
CAE-C

Analysis & Mapping of WSU's Cybersecurity Program

NICE, CSEC2017, ABET, CAE-CO

WASHINGTON STATE UNIVERSITY

NICE Alignment

Course syllabi

- Student Learning Outcomes
- Course topics

NICE Framework

- Task Descriptions
- Securely Provision, Collect & Operate, Investigate

	327	424	425	426	427	428	429	431	432	439	455	Gen
All Source-Collection Mgr.	0	1	0	0	0	0	5	1	0	0	0	2
All Source-Collection Req. Mgr.	0	0	0	0	0	0	6	0	1	0	0	4
Cyber Intel Planner	0	0	0	0	0	1	3	0	0	1	0	4
Cyber Ops Planner	0	1	0	0	0	0	5	0	0	1	0	3
Partner Integration Planner	0	3	0	0	0	0	1	0	0	0	0	4
Cyber Operator	0	0	2	0	4	4	0	0	0	0	8	2
Authorization Official	0	0	0	0	0	0	0	0	0	0	0	0
Security Control Assessor	0	0	0	0	0	1	0	7	0	0	0	0
Software Developer	3	0	0	1	0	6	0	4	5	0	0	5
Secure Software Assessor	2	0	0	1	0	5	0	2	3	0	0	1
Enterprise Architect	0	0	0	0	0	0	0	2	5	0	0	0
Security Architect	0	0	0	0	0	1	0	3	5	0	0	0
R&D Specialist	0	0	0	0	0	3	1	0	3	0	1	1
Systems Req.Planner	0	0	0	0	0	0	0	2	3	0	0	0
System Testing and Evaluation Specialist	0	0	0	0	1	0	0	1	3	0	0	2
Information Systems Security Developer	3	0	0	0	1	8	0	3	1	2	0	0
Systems Developer	0	0	0	0	0	3	0	3	7	2	0	1
Cyber Crime Investigator	1	1	11	0	0	1	0	0	0	0	0	0
Law Enf./Counterint. Forensics Analyst	0	0	20	0	0	3	0	0	0	0	1	1
Cyber Defense Forensics Analyst	1	0	21	0	0	4	0	0	0	0	1	2

NICE Alignment

Table 5.1 Cybersecurity courses included in WSU's B.S. in Cybersecurity

CptS 327	Fundamentals of Cybersecurity and Cryptograph
CptS 424	Cyber Law, Ethics, Rights, and Policies
CptS 425	Cyber Forensics and Anti-forensics
CptS 426	Hardware, Firmware Security and Reverse Engineering
CptS 427	Cybersecurity of Wireless and Distributed Systems
CptS 428	Software Security and Reverse Engineering
CptS 429	Virtualization and Offensive Cyber Operations
CptS 431	Security Analytics and DevSecOps
CptS 432	Cybersecurity Capstone Project
CptS 439	Cybersecurity of Critical Infrastructure Systems
CptS 455	Introduction to Computer Networks and Security

	327	424	425	426	427	428	429	431	432	439	455	Gen
All Source-Collection Mgr.	0	1	0	0	0	0	5	1	0	0	0	2
All Source-Collection Req. Mgr.	0	0	0	0	0	0	6	0	1	0	0	4
Cyber Intel Planner	0	0	0	0	0	1	3	0	0	1	0	4
Cyber Ops Planner	0	1	0	0	0	0	5	0	0	1	0	3
Partner Integration Planner	0	3	0	0	0	0	1	0	0	0	0	4
Cyber Operator	0	0	2	0	4	4	0	0	0	0	8	2
Authorization Official	0	0	0	0	0	0	0	0	0	0	0	0
Security Control Assessor	0	0	0	0	0	1	0	7	0	0	0	0
Software Developer	3	0	0	1	0	6	0	4	5	0	0	5
Secure Software Assessor	2	0	0	1	0	5	0	2	3	0	0	1
Enterprise Architect	0	0	0	0	0	0	0	2	5	0	0	0
Security Architect	0	0	0	0	0	1	0	3	5	0	0	0
R&D Specialist	0	0	0	0	0	3	1	0	3	0	1	1
Systems Req.Planner	0	0	0	0	0	0	0	2	3	0	0	0
System Testing and Evaluation Specialist	0	0	0	0	1	0	0	1	3	0	0	2
Information Systems Security Developer	3	0	0	0	1	8	0	3	1	2	0	0
Systems Developer	0	0	0	0	0	3	0	3	7	2	0	1
Cyber Crime Investigator	1	1	11	0	0	1	0	0	0	0	0	0
Law Enf./Counterint. Forensics Analyst	0	0	20	0	0	3	0	0	0	0	1	1
Cyber Defense Forensics Analyst	1	0	21	0	0	4	0	0	0	0	1	2

NICE Alignment

Work Role Alignments

- Cyber Operator: 77%
- Research & Development Specialist: 75%
- Software Developer: 71%
- System Testing and Evaluation Specialist: 54%

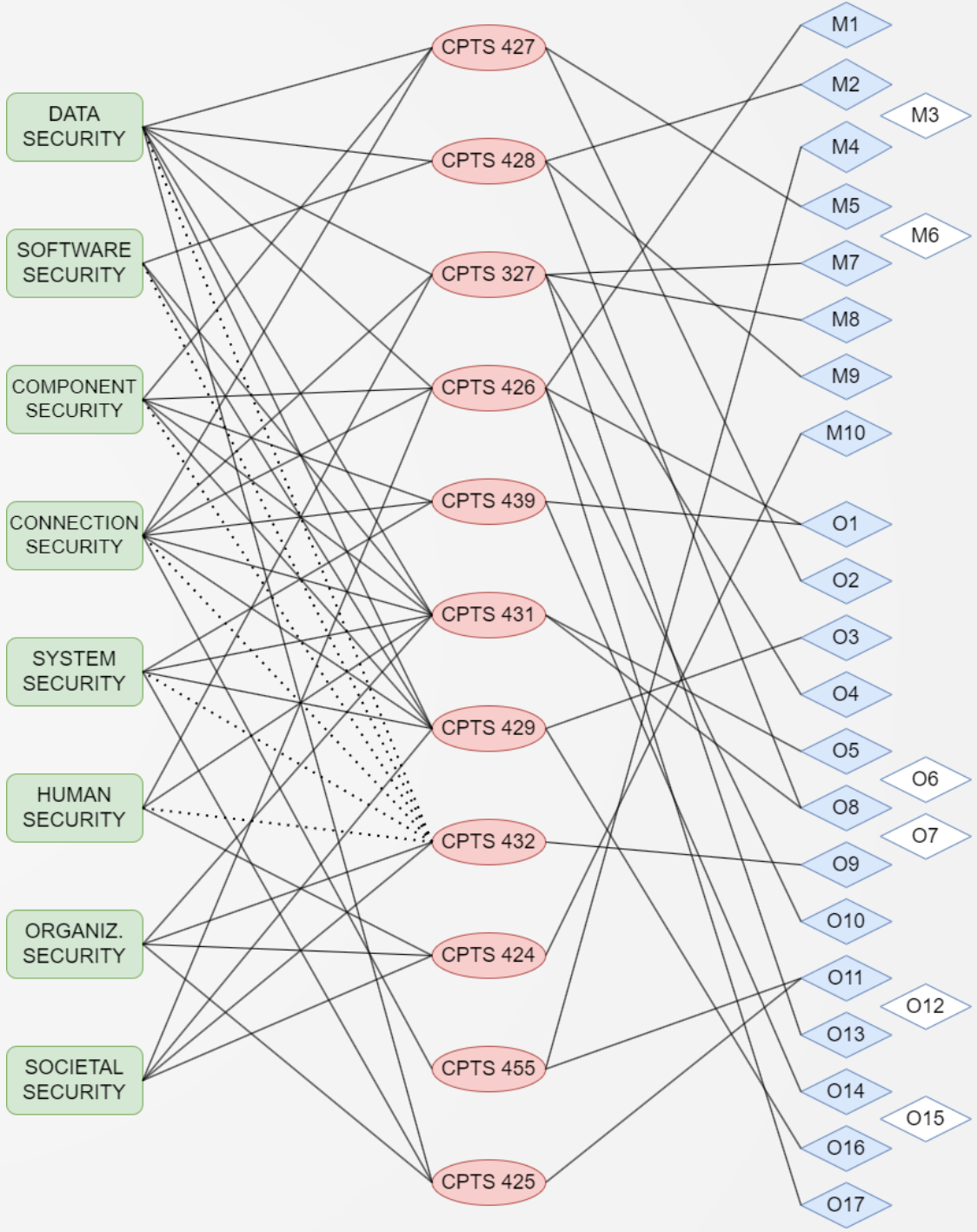
Course Mapping to ABET/CSEC2017 & CAE-CO

Course syllabi

- Student Learning Outcomes
- Course topics

ABET, CSEC2017, CAE-CO

- Fundamental Topics
- Knowledge Areas
- Knowledge Units



Questions & Discussion