CAE Program Updates and Support

National CyberWatch Center
Prince George’s Community College
Room 129B
301 Largo Road
Largo, MD 20774

www.nationalcyberwatch.org
Webinar Protocol

:: Mute your phone/mic when not talking
:: Questions during the webinar?
:: Technical problems
About the 2015 Webinar Series

:: Last Friday each month, 1 hour long, 11am ET
:: Great topics
:: Recorder & archived on National CyberWatch Center YouTube channel
CAE Program Updates and Support

:: Produced May 29, 2015
:: 11am EST
Dr. Vera Zdravkovich

- Senior Advisor
- Past Director and PI of CyberWatch
- Championed the Center of Academic Excellence Two Year Designation
Denisha Jackson

- CAE Program Manager, NSA
Professor Michael Burt

- National CyberWatch Program Manager
- Author of one of the first six CAE2Y proposals
- Author of the first CAE2Y re-designation proposal
Professor Tony Coulson

• Director Cyber Security Center at Cal State San Bernardino
• Chair CAE Community
• Co-PI CyberWatch West Faculty Development
Important Facts

• CAE is an INSTITUTIONAL designation

• National Security Agency (NSA) and Department of Homeland Security (DHS) award the CAE designation

• CAE awarded ceremony held at a June event and at NICE Workshop in the fall

• CAE designation is awarded based on successful application
Why CAE?

• Internal Recognition and Support

• External Recognition and Support

• CAE program graduates have better job opportunities

• Collaboration and funding opportunities
CAE Program Criteria

0. Letter of Intent
1. Program Outreach and Collaboration
2. Student Development/Student Curriculum Path and Recognition
3. IA/CD Center Establishment and Maintenance
4. IA/CD Multidisciplinary Efforts
5. Practice of IA/CD at the Institution Level
6. IA/CD Faculty
7. KU Mapping

* Please note: CAE2Y and CAE-CDE criteria varies slightly
Letter of Intent

- Institution must include an official letter stating the institution’s intent to apply for CAE IA/CD designation
- Must be on official institution letterhead, signed by a collegiate official at an appropriate level (Dean or higher)
- To be uploaded to web application (hard copy should not be mailed)
Program Outreach and Collaboration

- Shared curriculum and faculty
- Articulation agreements with high schools and 4 year institutions
- Sponsorship/participation in cyber competitions
- Community outreach
- Providing cybersecurity practitioners to students
IA/CD Center Establishment and Maintenance

- Formal organization for use as a resource for faculty and students (does not have to be a physical space)
- “Center” website should be operational, dynamic and current: contains up-to-date links to key IA/CD resources such as other academic institutions, government sites, conferences, workshops, IA/CD news, center POCs, IA/CD courses, etc.
- Website must be easy to find and easily accessible
Student Development/Student Curriculum
Path and Recognition

• Hands-on labs

• IA/Cybersecurity degrees/areas of study/track or certificates available to students

• Certificate for students to recognize completion of a KU mapped and CAE approved program

• Must demonstrate that courses used to map to KUs are within a path that students can take towards degree/certificate; Path must be attainable
IA/CD Multidisciplinary Efforts

- Internal dissemination of cybersecurity
- Review other department programs for the integration of cybersecurity
- Presentation to disciplinary groups of faculty on infusion of cybersecurity
- Development of cybersecurity modules for other disciplines
Practice of IA/CD at the Institution Level

- Review and describe the institutional policies for IA/CD applications and practices
- Discuss practices with the CTO for additional information
IA/CD Faculty

- Identify all full-time and adjunct faculty teaching in the program
- Describe credentials and experience of the IA/CD faculty
- Describe internal and external professional development opportunities for these faculty
- Describe planned future developments
Mapping to Knowledge Units (KUs)

- 70 Knowledge Units
- KUs - targeted technology areas composed of Topics and expected Outcomes

3 KU categories: Core, Mandatory, and Optional
KU Breakdown and Minimum Requirements

• Core 2Y: 11 Mandatory KUs
  – 2 year institutions must map to all 11

• Core 4Y: 6 Additional Mandatory KUs
  – 4 year institutions must map to the 11 Mandatory Core 2Y KUs
  – Plus map additional 6 KUs

• Optional KUs: 51 Elective KUs
  – 4 year institutions must select 5

• Summary of Minimums: 2Y – 11 KUs; 4Y – 22 KUs
Mapping Resources

- KUs - Download reference materials: www.iad.gov/NIETP/CAERequirements.cfm
- National CyberWatch Mapping Guide: https://scout.wisc.edu/cyberwatch/r131
- Content experts: Faculty who teach topics
- Course materials: Syllabi, detailed course outlines, textbooks, lab exercises, handouts.
Sample Mapping Resource

**Syllabus Course Objectives:**

- Describe gaining confidential information or unauthorized access through human intelligence (i.e. social engineering)
- Discuss counter measures to social engineering (training and education of users, administrators and personnel)
- Describe fishing
- Define organizational policies and procedures
- Describe security policies (guidance provided by security policies, points of contact, roles and responsibilities, enterprise, issue specific, and system specific security policies)
- Describe AIS and telecommunications systems policies (points of contact, references)
- Explain change management
- Explain classification of information
- Describe documentation, logs, and journals
- Explain acceptable use of resources, internet usage policy, and e-mail usage policy
- Discuss due care, due diligence, and due process
- Describe separation of duties, need to know and least privilege
- Discuss transportation of media
- Explain monitoring of critical areas, communications centers, information systems centers (IT/data centers), protected distributed systems, stand-alone systems, peripherals, storage areas
- Describe Policies and Procedures for computers and users
### KU Mapping Matrix Main Screen

<table>
<thead>
<tr>
<th></th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>All links below take you to the datasheet for that KU.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td><strong>Core 2Y Knowledge Units</strong></td>
<td><strong>Optional Knowledge Units</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Basic Data Analysis</td>
<td>Advanced Cryptography</td>
<td>Hardware Reverse Engineering</td>
<td>Secure Programming Practices</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Basic Scripting</td>
<td>Advanced Network Technology and Protocols</td>
<td>Hardware/Firmware Security</td>
<td>Security Program Management</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Cyber Defense</td>
<td>Algorithms</td>
<td>IA Architectures</td>
<td>Security Risk Analysis</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Cyber Threats</td>
<td>Analog Telecommunications</td>
<td>IA Compliance</td>
<td>Software Assurance</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Fundamental Security Design Principles</td>
<td>Cloud Computing</td>
<td>IA Standards</td>
<td>Software Reverse Engineering</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Information Assurance Fundamentals</td>
<td>Cybersecurity Planning and Management</td>
<td>Independent/Directed Study/Research</td>
<td>Software Security Analysis</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Introduction to Cryptography</td>
<td>Data Administration</td>
<td>Industrial Control Systems</td>
<td>Supply Chain Security</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Information Technology System Components</td>
<td>Data Structures</td>
<td>Intro to Theory of Computation</td>
<td>Systems Programming</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Networking Concepts</td>
<td>Database Management Systems</td>
<td>Intrusion Detection</td>
<td>Systems Certification and Accreditation</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Policy, Legal, Ethics and Compliance</td>
<td>Digital Communications</td>
<td>Life-Cycle Security</td>
<td>Systems Security Engineering</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Systems Administration</td>
<td>Digital Forensics</td>
<td>Low Level Programming</td>
<td>Virtualization Technologies</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td></td>
<td>Device Forensics</td>
<td>Mobile Technologies</td>
<td>Vulnerability Analysis</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td><strong>Core 4Y Knowledge Units</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>16</td>
<td>Databases</td>
<td>Host Forensics</td>
<td>Network Security Administration</td>
<td>Wireless Sensor Networks</td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Network Defense</td>
<td>Media Forensics</td>
<td>Operating Systems Hardening</td>
<td></td>
<td></td>
</tr>
<tr>
<td>18</td>
<td>Network Technology and Protocols</td>
<td>Network Forensics</td>
<td>Operating Systems Theory</td>
<td></td>
<td></td>
</tr>
<tr>
<td>19</td>
<td>Operating Systems Concepts</td>
<td>Embedded Systems</td>
<td>Overview of Cyber Operations</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Probability and Statistics</td>
<td>Forensic Accounting</td>
<td>Penetration Testing</td>
<td></td>
<td></td>
</tr>
<tr>
<td>21</td>
<td>Programming</td>
<td>Formal Methods</td>
<td>QA / Functional Testing</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Fraud Prevention and Management</td>
<td>RF Principles</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Mapping Suggestions

• Enlist multiple content experts, even for same KU
• Use textbook TOC and detailed course outlines that contain Topic descriptions in creating your Master Syllabi (a well developed Master Syllabus will make your like so much easier during the mapping process)
• Specify clear testing (grading) of Outcomes expectations
• Map **fewest** number of courses required to satisfy KU
• Consolidate individual KU mapping sheets into a single document to facilitate data entry into NSA/DHS application database
Application Deadlines

• The website application is closed

• The website application re-opens around July 1, 2015

• Deadline, August 1, 2015 for NICE designation in November 2015

• Deadline January 15, 2016 for designation in June 2016
Next Step

• Data Entry
• Go to NIETP - [www.iad.gov/NIETP/](http://www.iad.gov/NIETP/)
• Login
• Select (or apply for admission to) institution
  ➢ First time: Specify institution information
• Add new or Edit existing course
NIETP Welcome Screen

WELCOME

What's New?

There are no current notices posted.

IA National Centers of Academic Excellence

NSA and the Department of Homeland Security (DHS) jointly sponsor the National Centers of Academic Excellence in IA/CD programs. The goal of these programs is to reduce vulnerability in our national information infrastructure by promoting higher education and research in IA/CD and producing a growing number of professionals with IA/CD expertise in various disciplines. Students attending CAE IA/CD-E and CAE IA/CD-R schools are eligible to apply for scholarships and grants through the Department of Defense Information Assurance Scholarship Program and the Federal Cyber Service Scholarship for Service Program. Designation as a Center does not carry a commitment for funding from NSA or DHS.

CAE IA/CD institutions receive formal recognition from the U.S. Government as well as opportunities for prestige and publicity for their role in securing our Nation's information systems.
NIETP Login

Returning Users Login
Note: Bold* items below are required.

Login
All returning users: always login here once your registration is approved.

Login Name *
Password *
Login

New User / Institution
To use this site, you must first add your institution and apply for an account using the "New Registration" button.

Forgot Password
Forgot your password? We can't reset your password; to reset your password click on the "Forgot Password" button.

Forgot Username
Forgot your username? We'll send it to you by email; to receive your username click on the "Forgot Username" button.
Add or Edit Course
### Course Topic and Objective

<table>
<thead>
<tr>
<th>Course Number</th>
<th>COSC 3365</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title</td>
<td>Cyber Defense I</td>
</tr>
<tr>
<td>Course Created</td>
<td>01/15/2013</td>
</tr>
<tr>
<td>Course Last Reviewed</td>
<td>01/15/2014</td>
</tr>
<tr>
<td>Course Link</td>
<td><a href="http://sandboxU.edu">http://sandboxU.edu</a></td>
</tr>
<tr>
<td>Description</td>
<td>This course introduces the student to the identification of vulnerabilities, forms of attack, appropriate countermeasures, and the detection and defense of the same. Tools and techniques for the securing of hardware, software and data, including physical security are covered. The issues and facilities available to both the intruder and administrator will be examined and evaluated with appropriate exercises to illustrate their effect.</td>
</tr>
<tr>
<td>Is Currently Taught</td>
<td>Yes</td>
</tr>
<tr>
<td>Course Length</td>
<td>45 hours for 15 weeks; 2 one-and-a-half hour meetings per week</td>
</tr>
<tr>
<td>Current Enrollment</td>
<td>35</td>
</tr>
<tr>
<td>Past Enrollment</td>
<td>35</td>
</tr>
<tr>
<td>Instruction Methods</td>
<td>Lecture, Demonstrations, Labs, Projects</td>
</tr>
<tr>
<td>Evaluation Methods</td>
<td>Lab Projects, Exams</td>
</tr>
<tr>
<td>Syllabus</td>
<td>Sandbox Univ Syllabus-CyberDef</td>
</tr>
<tr>
<td>Outline</td>
<td>Sandbox Univ Syllabus-CyberDef</td>
</tr>
<tr>
<td>Is Active</td>
<td>Yes</td>
</tr>
</tbody>
</table>

#### Major Topics for COSC 3365

| 1 | Potential Attack Methods |

#### Objectives for COSC 3365

| 1 | Student will identify various potential system attack methods including social engineering, denial of service, Trojans, logic bombs, database inference, man-in-the-middle, etc. Graded written exams will assess their understanding of ability to recognize attack methods. | Yes | Yes |  |

Return to Edit Course Select List
CAE Resources

Resources such as mapping consultation, KU Mapping Guide, sample applications, and personal assistance is listed on these websites:

- NSA website: www.iad.gov/NIETP/CAERequirements.cfm
- National CyberWatch Center website: www.nationalcyberwatch.org
- CyberWatch West website: www.cyberwatchwest.org
- CAE website: www.caecommunity.org

Email: askCAEIAscE@nsa.gov

Additional Questions: info@nationalcyberwatch.org
UPCOMING EVENTS

• The Colloquium for Information Systems Security Education (CISSE) Annual Conference, June 14-17, 2015, JW Marriott Las Vegas Resort and Spa, Las Vegas, Nevada

• 2015 Community College Cyber Summit (3CS), June 17-19, 2015, Las Vegas, Nevada (same location as CISSE)

• National Initiative for Cybersecurity Education (NICE) – 3-4 November 2015, San Diego, CA
Next Webinar

:: August 28, 11am EDT
:: Q&A with Advanced Cyberforensics Education (ACE) consortium
Thank You!