

NSA/DHS CAE
Special Interest Group (SIG) on:

Professional Cybersecurity Certifications

SIG-CyCERTs

Yair Levy, Nova Southeastern University, Florida

Eric Berkowitz, Roosevelt University, Illinois

Overview

- The role of certifications in a profession
- Professional certifications in cybersecurity
- Professional certifications in academic programs
- Why professional certifications in CAE Schools?
- Value of professional certifications for students and organizations
- Professional certifications costs, support, platforms
- Conflicting information for hiring
- Case 1: Nova Southeastern University
- Case 2: Roosevelt University
- SIG-CyCERTs initiative ideas? (Google Form? Signup sheet)



Role of Certifications in a Profession



*“While billions of dollars are being spent on new technologies to secure the U.S. Government in cyberspace, it is the **people with the right knowledge, skills, and abilities** to implement those technologies who will determine success”*

(U.S. National Security Council, 2011)

Role of Certifications in a Profession (Cont.)



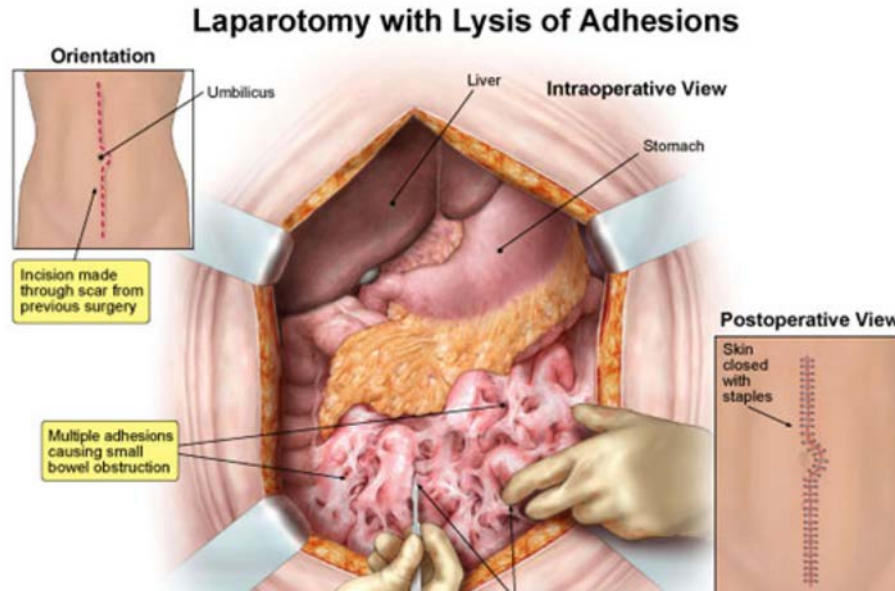
Role of Certifications in a Profession (Cont.)

Up until early 1840s most doctors learned through apprenticeships, and many did not attend medical school. Anyone could work as a doctor, or perform surgeries.



Role of Certifications in a Profession (Cont.)

In May 1847 about 250 delegates from across the country gathered in Philadelphia, Pennsylvania, and created the American Medical Association (AMA) to create structure in the medical field and mitigate potential risks to public health.

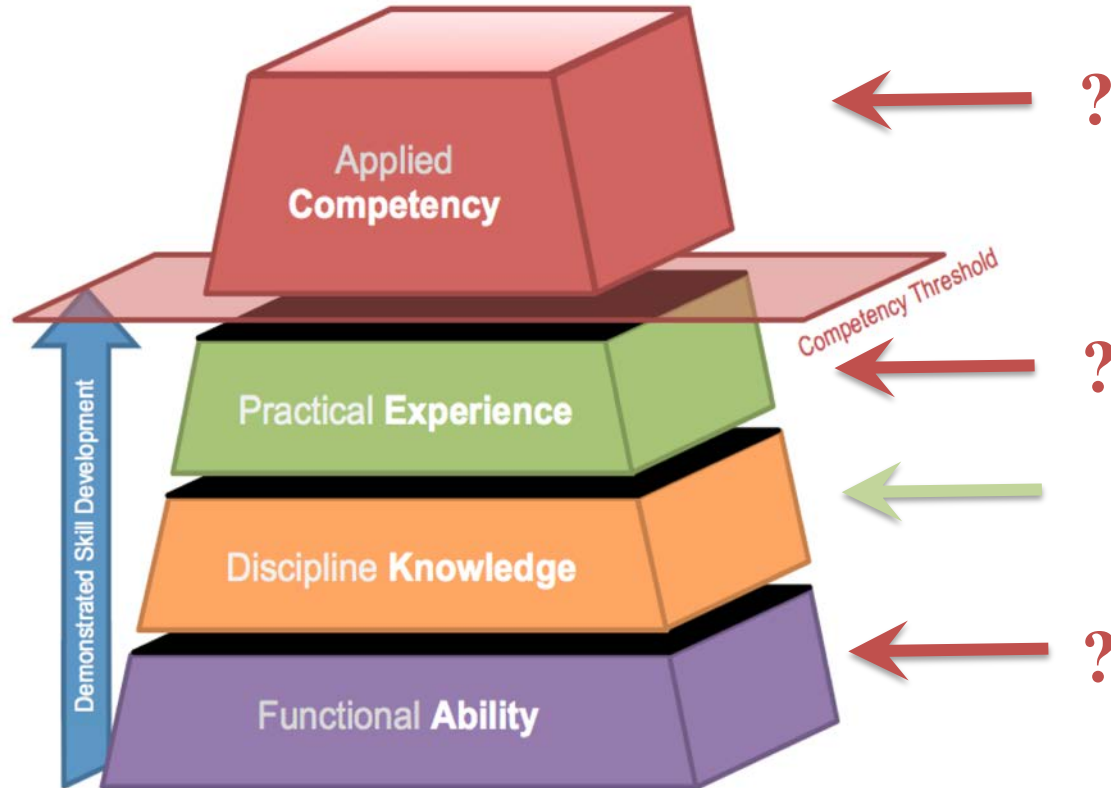


Role of Certifications in a Profession (Cont.)

AMA developed a solid set of processes to build and assess the *knowledge, skills, and abilities (KSAs)* of medical professionals, before they are licensed to practice medicine.



Role of Certifications in a Profession (Cont.)



Professional Certifications in Cybersecurity



Certified
Information
Systems Security
Professional



Systems
Security
Certified
Practitioner



Certified
Cloud
Security
Professional



Certified
Cyber
Forensics
Professional



Certified
Secure
Software Lifecycle
Professional



Professional Certifications in Cybersecurity (Cont.)

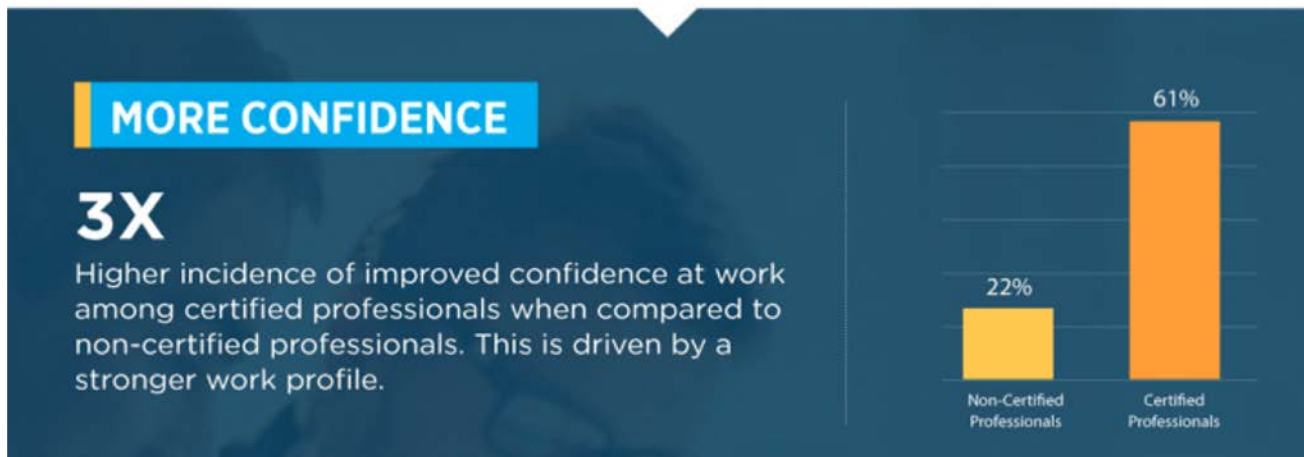


**79% of certified professionals see a
tangible impact on their career**

Professional Certifications in Cybersecurity (Cont.)

**80% of certified professionals see a
qualitative improvement in career**

Confidence, quality of work & improved work environment




Professional Certifications in Cybersecurity (Cont.)


According to Business Wire


- Certified personnel get first in line in hiring processes, getting jobs **2.7x faster** than those without certification
- Certified personnel have in average **10%+ better income**.




Professional Certifications in Cybersecurity (Cont.)




Account



[Find Jobs](#) [Career Resources](#) [Company Profiles](#) [Salary](#) [Post a Resume](#)


 Filter [Recent searches](#) **Comptia security+ Jobs (6581 Jobs Found)**

Sr. Director, Cyber Security Architecture
Vaco - Charlotte
Jupiter, FL
8 days ago



Security Specialist
Collabera
St. Petersburg, FL
2 days ago

Principle Data Loss Prevention Consultant - Public Sector
Job Juncture
Raleigh, NC
2 days ago

Principle Data Loss Prevention Consultant - Public Sector
3 days ago



Sr. Director, Cyber Security Architecture at Vaco, LLC
Jupiter, FL

 Save  Email

[Details](#) [Highlights](#) [Company](#) [Reviews](#)

Vaco is a private-equity backed solutions company that provides consulting, managed

Professional Certifications in Cybersecurity (Cont.)

The screenshot shows the Monster job search interface. At the top, the Monster logo is on the left, and search filters for 'Comptia security+', 'Location', and 'Search' are in the center. On the right, there are links for 'Account' and 'Post a Resume'. Below the search bar, navigation links include 'Find Jobs', 'Career Resources', 'Company Profiles', 'Salary', and 'Post a Resume'. The main search results section shows 'Comptia security+ Jobs (6581 Jobs Found)' with a 'Create job alert' button. A red box highlights this search result, and a red arrow points from it to a detailed job listing for 'Sr. Director, Cyber Security Architecture' at Vaco, LLC in Jupiter, FL. The job listing includes a photo of a man, the Vaco logo, and an 'Apply' button. Below the job listing, there are tabs for 'Details', 'Highlights', 'Company', and 'Reviews'. A red box at the bottom of the page also highlights the text 'Comptia security+ Jobs (6581 Jobs Found)'.

MONSTER

Comptia security+ Location Search

Account

Find Jobs Career Resources Company Profiles Salary Post a Resume

Filter Recent searches **Comptia security+ Jobs (6581 Jobs Found)** Create job alert

Sr. Director, Cyber Security Architecture 8 days ago
Vaco - Charlotte
Jupiter, FL

Security Specialist 2 days ago
Collabera
St. Petersburg, FL

Principle Data Loss Prevention Consultant - Public Sector 2 days ago
Job Juncture
Raleigh, NC

Sr. Director, Cyber Security Architecture at Vaco, LLC
Jupiter, FL

Apply

Save Email

Details Highlights Company Reviews

Comptia security+ Jobs (6581 Jobs Found)

Professional Certifications in Academic Programs

- Curriculum - in what academic level?
 - 2YR
 - 4YR
 - Graduate
- Costs
- Time
- Requirements
 - Significant KSAs
 - Years of work experience
 - Personal recommendations



Professional Certifications in Academic Programs

Are professional *certifications*

= or ≠

professional *licenses*

???

Professional Certifications in Academic Programs



The Movement to License Software Engineers

In recent years, the definition of engineering has broadened to include design of intangible structures as well as tangible ones. At issue is computer software. Computer programs may be nonphysical, but they are often embedded in machines that are tangible – and where proper functioning is crucial to safety.

More than 60% of IEEE Computer Society members supported a professional engineering exam for software engineers. – 2008 IEEE Survey

There has been discussion of licensing software developers since the 1990's, and indeed Texas has been issuing licenses for more than a decade. Only in recent years, though, has there been progress on a national level.

Recent Developments

In 2008, the IEEE Computer Society, in cooperation with several other organizations, sent out a survey to its U.S.

Professional Certifications in Academic Programs

The screenshot shows the Florida Senate website. The browser address bar displays [flsenate.gov/Laws/Statutes/2011/Chapter471/All](https://www.flsenate.gov/Laws/Statutes/2011/Chapter471/All). The page header includes "MyFloridaHouse.gov | Mobile Site" and a search bar with "Go to Bill: Bill # 2020" and a "Go" button. The main navigation bar features the Florida Senate logo and links for "Home", "Senators", and "Committees". Below this, a breadcrumb trail reads: "Home > Laws > 2011 Florida Statutes > Title XXXII > Chapter 471". The main content area is titled "2011 Florida Statutes" and includes a link for "Title XXXII REGULATION OF PROFESSIONS AND OCCUPATIONS". On the right side, a box labeled "CHAPTER 471 ENGINEERING" is visible.

<https://www.flsenate.gov/Laws/Statutes/2011/Chapter471/All>

The screenshot shows the Florida Department of Business and Professional Regulation (DBPR) Online Services website. The browser address bar displays myfloridalicense.com/examSchedule.asp?SID=&val=09&SSN=&LastName=. The page header includes the "Florida dbpr" logo and a "DBPR ONLINE SERVICES" banner. A "Log On" button is visible. The main content area is titled "Exam Information (*Indicates required field)" and includes a section for "Searching for Exam Information?". A list of exam categories is displayed on the right, with "Proctored Exam Software" highlighted in blue. A red arrow points to this highlighted option. The footer contains contact information for the DBPR and a disclaimer regarding the use of email addresses.

Professional Certifications Costs, Support, Platforms

- Costs of preparation/studying for certification
- Support for “messing up”, especially in the hands-on labs
- Platforms:
 - Vendor specific (CompTIA, (ISC)2, Microsoft, CISCO NetCad, etc.)
 - TestOut LabSim
 - US ARMY SkillPort
 - CyBrary
 - Udemy, YouTube, etc.



Conflicting Information for Hiring

- Invited speakers give conflicting information from single perspective
- Hiring managers filter candidates based on “Alphabet of Certs”
- Team leaders look for hard skills and problem solving
- Business leaders look for blend of hard and soft skills
- Professors often stress foundation and theory not practice, skills and outcomes
- Students: Is the cybersecurity job shortage a *HOAX*?



Case 1: Nova Southeastern University

- CAE since 2005
- Two designated MS programs
 - MS in IA & Cybersecurity (Tech)
 - MS in Cybersecurity Management (Managerial)
- ISEC615 - Fundamentals of Cybersecurity
 - Virtual lab: LabSim - Security Pro



<http://infosec.nova.edu/>

Case 1: Nova Southeastern University (Cont.)



Teaching Aids

TestOut Security Pro *English 6.0.7*

ISBN: 978-1-935080-44-2 | Expires on 8/28/2021

Prepares you for

- ▶ TestOut Security Pro
- ▶ CompTIA Security+ SY0-501

Associated Classes

- ▶ Lab for ISEC615 (Fall 2019) -
Fundamentals of Cybersecurity w/Dr.
Levy

Case 1: Nova Southeastern University (Cont.)



Case 1: Nova Southeastern University (Cont.)



Case 1: Nova Southeastern University (Cont.)

Scenario

You are the IT security administrator for a small corporate network. You have already configured a network security appliance (NSA) with the settings necessary to connect to the Internet. Today, you will install the NSA. The router has been disconnected and configured to connect to the NSA.

In this lab, your task is to perform the following:

- Install the NSA into the rack's top slot and make the following connections:
 - Connect the power cable to the NSA through a critical bank outlet on the UPS.
 - Use a Cat5e cable to connect the NSA's WAN port to the left Ethernet port on the wall plate. The left Ethernet port connects to the internet through a

Shelf

▼ Cables



Workspace

Front

Back



Front

Front

Back



Selected Component



Case 1: Nova Southeastern University (Cont.)

Scenario

You work as the IT security administrator for a small corporate network. The company president has received several emails that he is wary of. He has asked you to determine whether they are hazardous and handle them accordingly.

In this lab, your task is to perform the following:

- Read each email and determine if it is legitimate.
- Delete any emails that are attempts at social engineering.
- Keep any emails that are safe.

Hold your mouse over the embedded links to see the actual URL in the status bar at the bottom of the screen.

The screenshot shows a WebMail interface in a browser window. The address bar displays `http://my.webemail.com/default.aspx#` and the page title is "WebMail - jcameron@hotmail.com". The user is logged in as "Cameron Jacklin" with a "sign out" link. The interface includes a navigation bar with "New", "Reply", "Reply all", "Forward", "Delete", "Junk", "Mark as", "Move to", and "Options" buttons. The left sidebar shows the "Inbox (6)" folder selected, with other folders like "Junk", "Drafts", "Sent", "Deleted", and "New folder" listed. The main inbox area displays a list of emails:

From	Subject	Date
Microsoft Windows Update Center	New Service Pack	3:45 PM
Human Resources	Ethics Video	1:06 PM
Online Banking De...	Payment Pending	6:57 AM
Grandma Jacklin	FW: FW: Virus At...	11/7/19
Emily Smith	Web Site Update	11/7/19
Sara Goodwin	Wow!!	11/6/19
Grandma Jacklin	Free Airline Tickets	11/6/19
Joe Davis	Re: Lunch Today?	11/6/19
Human Resources		11/5/19

The selected email, "New Service Pack" from "Microsoft Windows Update Center", is displayed on the right. It includes a "Reply" and "Forward" button. The email body contains the following text:

Microsoft Windows Update Center
11/8/19

To jcameron@hotmail.com

New Service Pack v7.1.8 update is read for download.

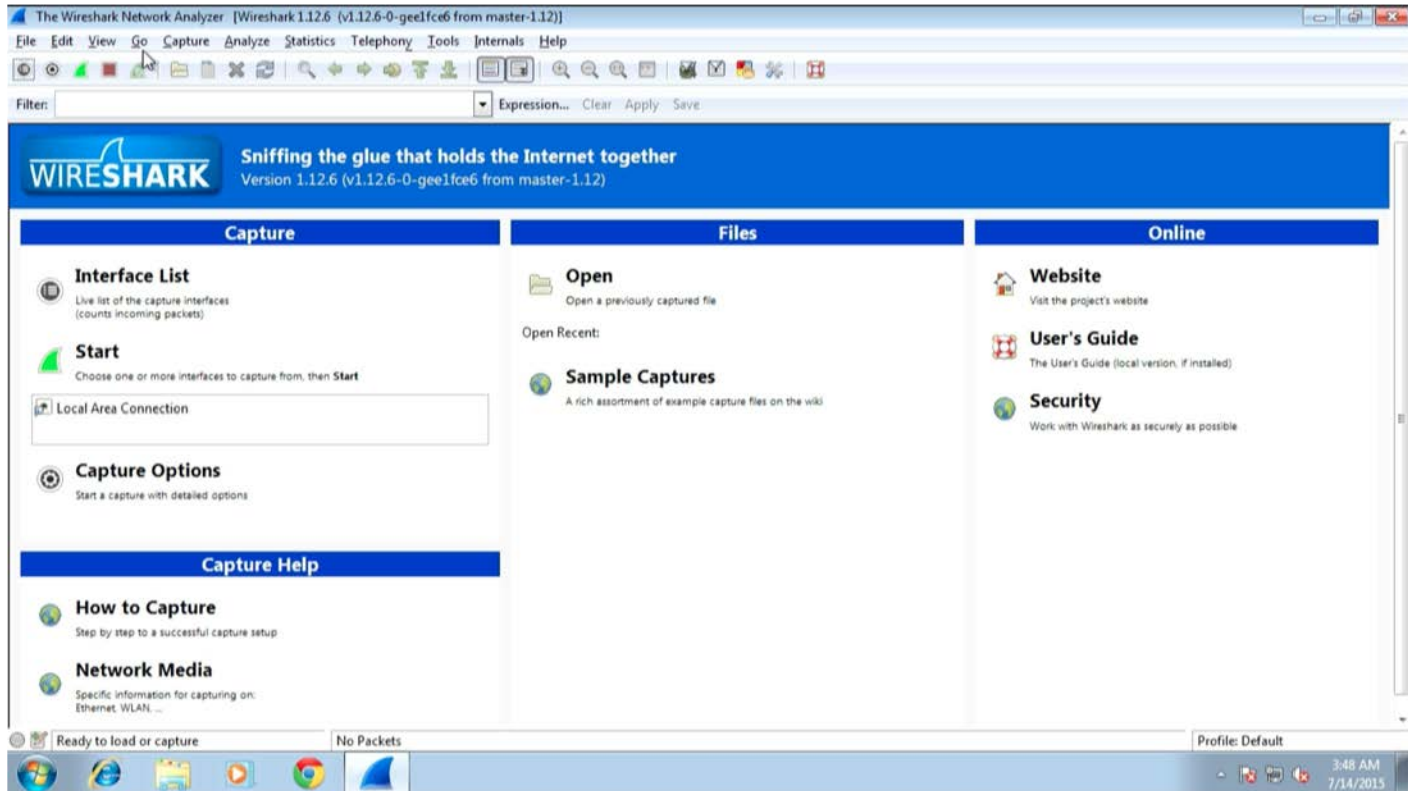
*Stay secure with the new Microsoft AntiVirus and AntiMalware system.
*Some security flows were fixed and new features were added by this Service Pack Update.
*This update is available by clicking the following link:

<http://www.microsoft.com/windowsupdate/v7/update-all/>

*No more SPAM / Viruses / Safe Web Navigation

Sincerely,
Microsoft Update Team

Case 1: Nova Southeastern University (Cont.)



Case 1: Nova Southeastern University (Cont.)

Professor,

I took the certification exam today and passed on the first attempt. I only used your class and the test out material to prepare and have no previous experience in IT.

Dear Professor....

I hope this email finds you well. I know how busy you must be at this time of year so I want to thank you beforehand to read this email. I'm writing you to let you know that I took the CompTIA Security + exam last Friday, and I successfully passed it. I also want you to know that a few

Dr. Levy,

I wanted to let you know I took your class last semester and I took my CompTIA security+ yesterday and passed. You had said to let you know as you like to keep track. I really think the TestOut course was an amazing study tool. I redid some of the modules to help study for the certification exam.

Regards,

Dr. Levy,

Just wanted to let you know I took my CompTIA this morning and passed.

Hope all is well.

Case 1: Nova Southeastern University (Cont.)

NSA Center of Academic Excellent Knowledge Units	
CAE-CD KUs	TestOut Security Pro v6
Topics and sub-Topics:	
1. Threats and Adversaries (threat actors, malware, natural phenomena)	2.1 Understanding Attacks, 2.1.1 Threat Actor Types, 2.1.2 Threat Agents Overview
2. Vulnerabilities and Risk management (include backups and recovery)	3.2 Risk management, 6.2 Network Device Vulnerabilities, 6.9 Vulnerability Assessment
3. Common Attacks	2.1 Understanding Attacks, 2.1.1 Threat Actor Types, 2.1.2 Threat Agents Overview, 3.5.4 Investigating a Social Engineering Attack, 5.1.5 DoS Attack Facts, 5.2.1 Session and Spoofing Attacks, 5.2.5 DNS Attacks, 5.11 Wireless Attacks, 6.1 Network Threats, 6.4 Switch Attacks, 7.2 Password Attacks, 8.4 Web Application attacks, 9.4 Cryptographic Attacks
4. Basic Risk Assessment	3.2 Risk Management
5. Security Life-Cycle	2.2 Defense Planning, 3.3 Business Continuity, 3.4 Manageable Network Plan
6. Applications of Cryptography and PKI	2.4 Cryptography Basics, 9.2 Advanced Cryptography, 9.3 Cryptography Implementations, 9.4 Cryptographic attacks, 9.8 Public Key Infrastructure (PKI)
7. Data Security (in transmission, at rest, in processing)	3.1.6 Data Retention, 9.1 Data Management, 9.10 Data Transmission Security, 9.11 Data Loss Prevention (DLP),
8. Security Models (Bell-La Padula, Biba, Clark Wilson, Brewer Nash, Multi-level security)	2.2 Defense Planning
9. Access Control Models (MAC, DAC, RBAC, Lattice)	8.1 Access Control Models
10. Confidentiality, Integrity, Availability, Access, Authentication, Authorization, Non-Repudiation, Privacy	2.3 Access Control, 5.9 Network Access Protection, 6.11 Remote Access, 6.12 Network Authentication, 8.2 Authentication, 8.3 Authorization, 8.13 Hardening Authentication 1, 8.14 Hardening Authentication 2, 3.1.2 Data Privacy Laws,

Case 2: Roosevelt University

- Program contains significant CS and other technical elements
- Many students minor (some dual major) in CS or Math
- Looking for a way to accentuate these achievements as credentials
- Certifications not the only way - other achievements fill a resume and trigger A.I. filters



<https://www.roosevelt.edu/centers/cyber-security>

Case 2: Roosevelt University (Cont.)

- Certifications :
 - Programming - Python
 - We offer a full programming sequence
 - Unix or Redhat
 - Linux based user and administration course
 - Cyber Operations
 - Highly enrolled elective
 - Ethical Hacking
 - Part of the required curriculum



Case 2: Roosevelt University (Cont.)

- Issues:
- How much vendor relationship is too much?
- Handling the cost.
- Perspective: are there alternatives? (portfolio projects)
- Perspective: do students seek too many?
- Academic culture and certification classes.
 - Undergraduate? Graduate?
- Who should teach them?
 - Academic faculty? Certified Adjuncts? Either? Both?



Case 2: Roosevelt University (Cont.)



- Students "vote with their feet"
 - Courses that lead to certifications are always fully enrolled
- Certifications can be "a spoon full of sugar"
 - The promise of a certification can encourage students in academically rigorous classes.
- Students want portfolios that include certs and significant experiences

SIG-CyCERTs Initiative Ideas

- Dedicated web page for the SIG: <http://caecommunity.org/SIG-CyCERTs/> ?
- Sub-committee to solicit CAE Tech Talk and Forum presentation under the SIG
- Track for SIG presentations during CAE Symposium 2020
- Research and publications opportunities related to CyCERTs?

SIG-CyCERTs Initiative Ideas (Cont.)

- Creating a SIG logo?
- Other ideas?

To take part of the SIG-CyCERTs, please register via:

<https://forms.gle/CM9ztYp9TXpNariDA>

Thank you!

