National Security Agency (NSA)

NCAE-C Cyber Curriculum and Research 2020 Program

NCAEC-003-2020

"Cyber Security Pathways Coalition (CPC)"

Adel Elmagrhraby, PhD – Co-PI & Andrew Wright, PhD –Co-PI

Sharon A. Kerrick, PhD – PI

Assistant VP Digital Transformation Center

Cyber Security Pathways Coalition (CPC) Collaboration team

- Recognizing the significant need for cybersecurity healthcare systems talent in the workforce, the University of Louisville (UofL) formed a coalition with four partner schools:
- **University of Arkansas Little Rock**
- **University of North Florida**
- **Kentucky Community Technical College Systems** – (16 colleges specifically partnered w/Bluegrass Technical & Owensboro Technical)
- **City U of Seattle** – partner school Coalition liaison (we will add more of these)

- ALL hold current NCAE-C designations and whose interests, experience, and complementary skills are aligned with cybersecurity healthcare systems.

Our team will develop and pilot a certificate-based workforce-development program, focusing on cybersecurity for the healthcare industry.

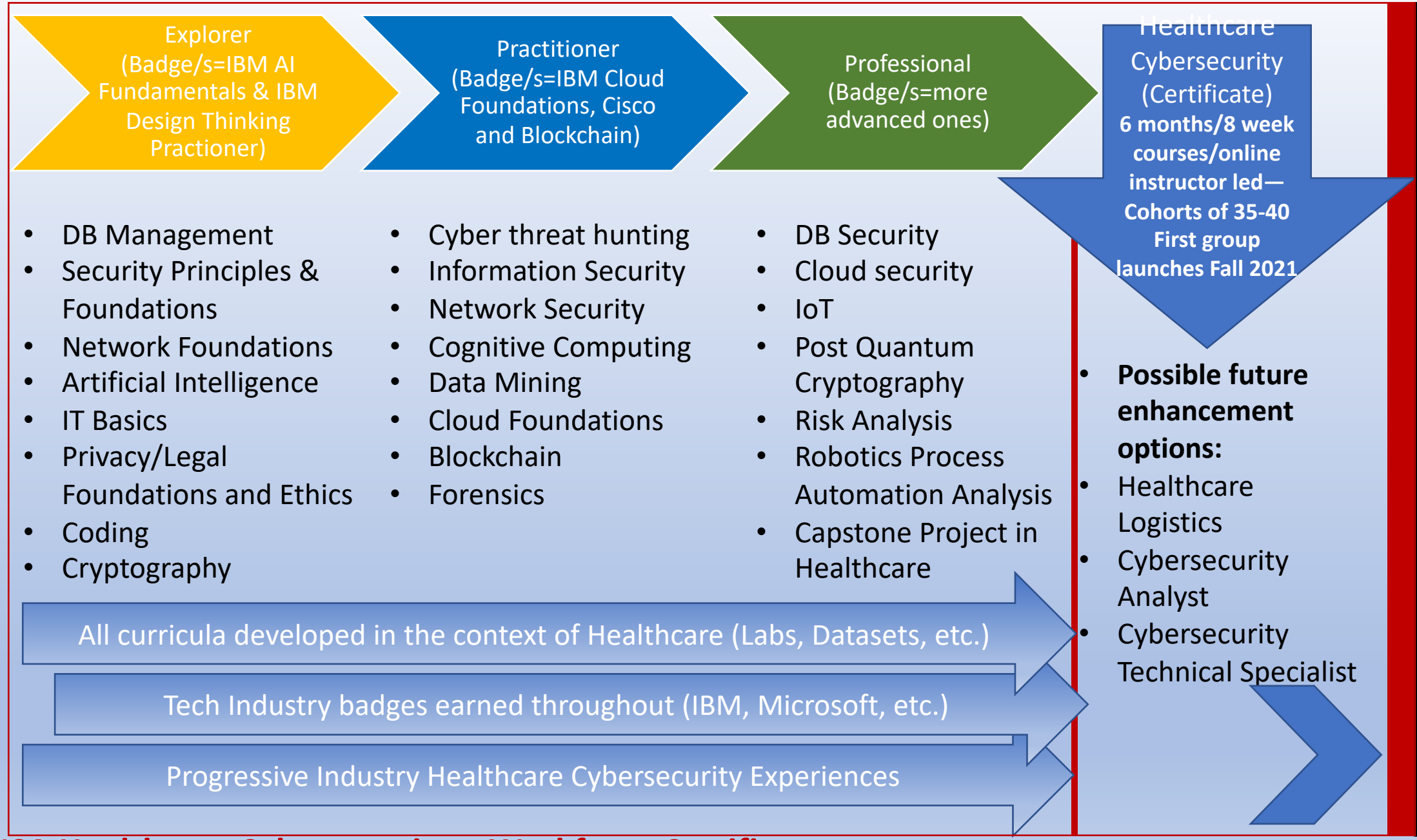
*UofL is the lead institution of this newly formed coalition called the “Cyber Security Pathways Coalition” (CPC). We operate through our Digital Transformation Center to coordinate, develop, manage, and monitor this effort.

*Certificate will take 6 months for participants to complete 3 levels (Explorer, Practitioner and Professional). Online/instructor led. Working labs w/partner data and case studies.
*Team teaching with industry professionals. Competency based modules.

* Train the trainer spots for HBC’s (Simmons College and Kentucky State)

*Pilot program – targets First responders and Military Veterans participants
Pilot participant goal =200

*2 Years Grant $6M with option for third year + Research Grant $300K over two years.



NSA Healthcare Cybersecurity – Workforce Certificate – will be available for one year per RFP requirement

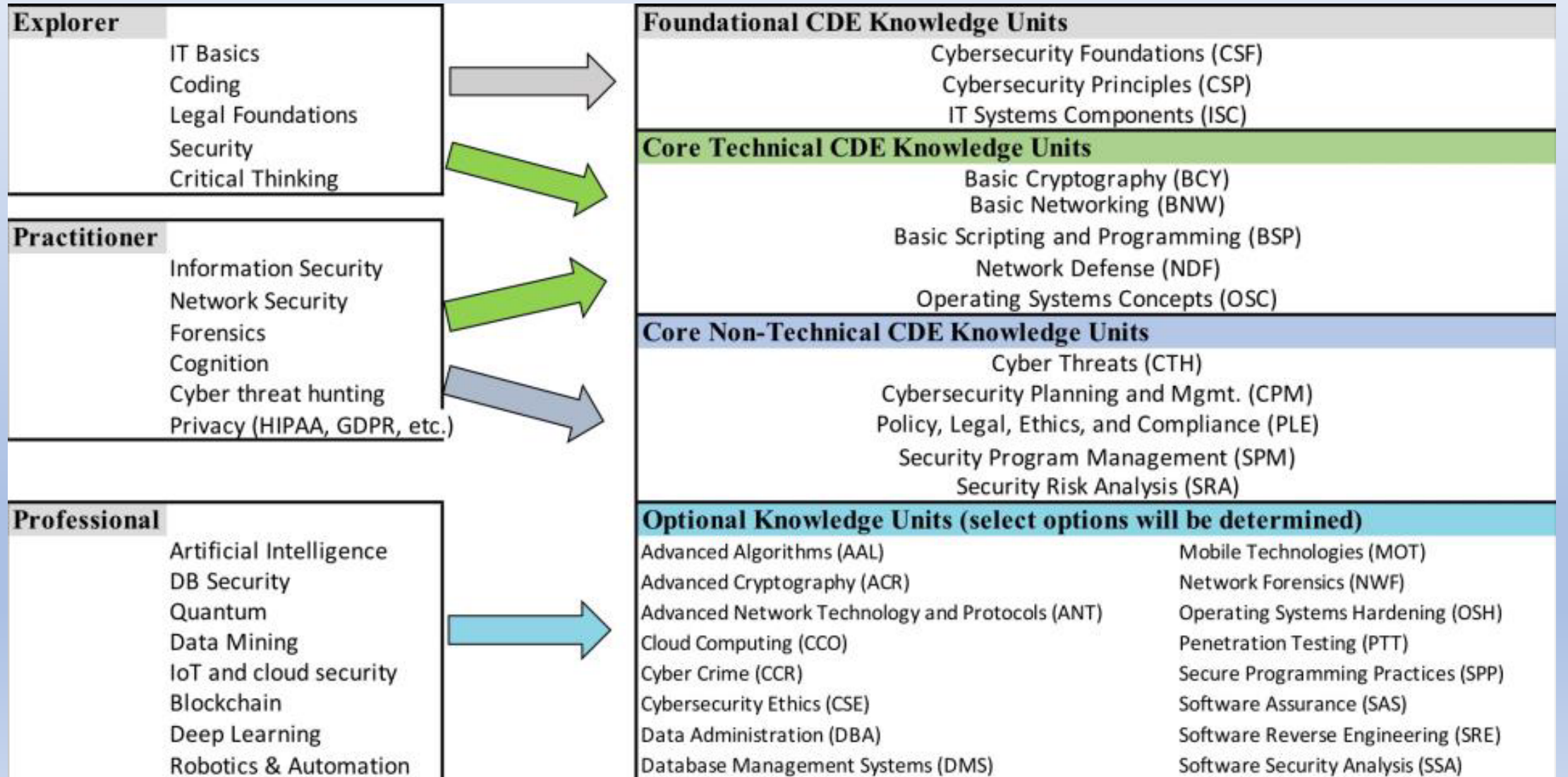
Innovations:

*Technology industry badges (Artificial Intelligence, Blockchain, developer, Machine Learning etc.) embedded throughout the Certificate

* Utilization of Gamification, Industry subject matter experts as co-instructors using data-sets (anonymous) and Use Cases from current industry, IoT Medical

*Certificate may be used toward “for credit”at U of L specific programs or stand alone “non-credit” certificate

Aligned with National Standards



Summary & Questions

Research Component Dr. Adel Elmagraby - PI lead
Partnering with Alcorn State University (HBU) located in Mississippi we will research biometric sources to detect sources of breaches related to cybersecurity.

*the Research goals require development of a set of neural network (NN) models to detect and utilize multiple biometric sources to enhance cybersecurity. Multi-factor authentication is the known to as a basis for cybersecurity enhancement but may have the limitations of being a static approach and therefore we propose to integrate keystroke and mouse dynamics as additional biometric features for an enhanced layer of cybersecurity.

*The objectives are to develop a set of neural network (NN) models of utilizing user interaction behavior as ones' biometrics to enhance cybersecurity, and to involve students in all research activities and various applications of Cybersecurity. Three-factor authentication is the best available option for cybersecurity enhancement, which includes 'know' (password), 'have' (username, token, or card) and 'are' (biometrics). Each one makes this process stronger and more secure. **We propose to utilize keystroke and mouse dynamics as users' biometrics in cyberspace.** In case of username and password are compromised, these dynamics still function as a layer of protection from intrusion.