Healthcare Cybersecurity Pathways: Technology Badges, Certificates, and Degrees

Sharon Kerrick, PhD (PI), **Adel Elmaghraby**, PhD (Co-PI), **Andrew Wright**, PhD (Co-PI)
University of Louisville, Digital Transformation Center
https://louisville.edu/digital-transformation

Introduction

The **NCAE-C Program** has funded three **certificate-based workforce development pilots** (via NCAE-C-003-2020) to increase the number of qualified cybersecurity professionals. Each of the programs were asked to focus on a **specific workforce sector** and engage with **industry partners** when developing their programs. The developed curricula were also required to incorporate topics on **cutting edge technologies** not traditionally considered as part of the cybersecurity core areas including **artificial intelligence** and **robotic process automation**. During the pilot period, the programs were directed to focus on providing training to **transitioning military**, **first responders**, and **veterans** transitioning to cyber-oriented work roles.

Coalitions of at least three CAE-C institutions were awarded for 2-3 years in Fall 2020 and are led by **The University of West Florida**, **Purdue University Northwest**, and **The University of Louisville**.

This poster focuses on the **University of Louisville-led coalition** known as the **Healthcare Cybersecurity Pathways Coalition**.

Healthcare Cybersecurity Pathways Coalition

The initial University of Louisville-led **Healthcare Cybersecurity Pathways Coalition** two-year pilot includes the **University of Arkansas at Little Rock**, the **University of North Florida**, **Bluegrass Community and Technical College**, **Owensboro Community and Technical College**, and the **Kentucky Community and Technical College System**, with the **City University of Seattle** serving as a coalition partner liaison.

The Coalition was recently awarded third-year funding from the NCAE-C Program and is expanding to include the **City University of New York**, **Hood College**, **Kennesaw State University**, **Kentucky State University**, and **Northwest Missouri State University**. This expansion includes several **Minority Serving Institutions** that will participate in **Train-The-Trainer** sessions so that they may customize the curriculum and begin delivering the content to their constituents.

The initial workforce sector our Coalition focused on is **healthcare** and the curriculum includes real problems, data sets, challenges, and solutions directly from the healthcare industry. As part of the third-year award, the Coalition will adapt the curriculum to address the cybersecurity needs of the **logistics sector**. Faculty from the University of Louisville's **Logistics and Distribution Institute** will work with new industry partners to adapt and validate the revised curriculum.

Note: Any curricula developed as a part of this grant will be listed in the NCAE Resources Directory, made available to designated and candidate NCAE-C institutions for one year and will also be provided to the public via the Clark Project.

CYBERSECURITY WORKFORCE CERTIFICATE PROGRAM

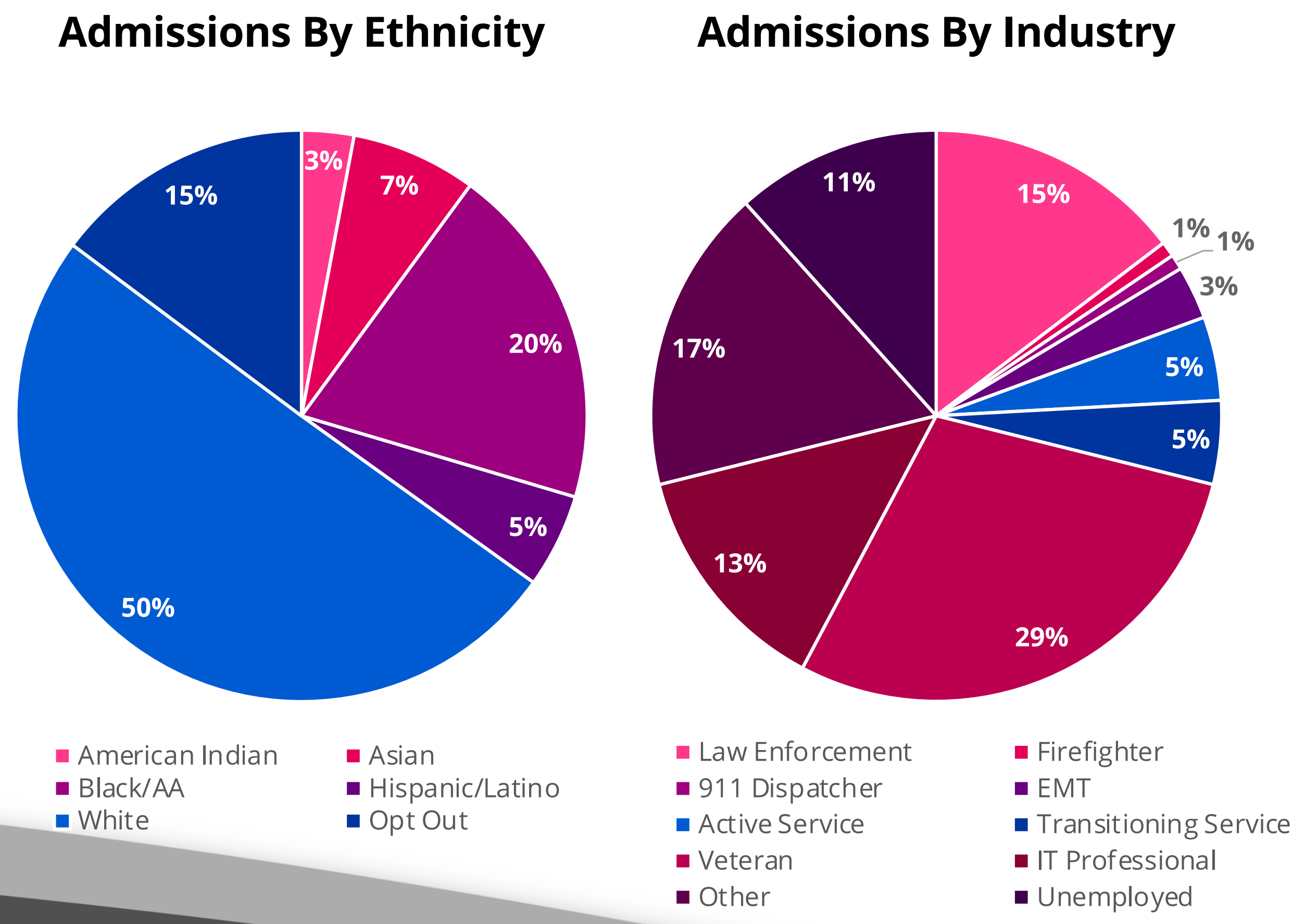
Program Overview

The **6-month** Healthcare Cybersecurity Pathways program is divided into three **8-week** levels (**Explorer**, **Practitioner**, and **Professional**) delivered fully **online** (asynchronously). Participants only need a **GED** and **4+ years of work experience** (that may be offset by additional education). Each begins the program by completing a **World of Work Inventory**, the world's first empirically-based, fully integrated, multidimensional career assessment and reviewing it with our cybersecurity career specialist.

Instructors provide support for each module, including regular office hours, focusing on hands-on labs and applied learning activities and assessment (both formative and summative). In addition, **success coaches** are engaged to connect learners to wrap-around services that they need to be successful academically, personally, and professionally. These coaches act as the primary points of contact that learners can count on throughout their entire program experience. Participants are also encouraged to engage in some friendly cohort competition through **gamification** in our smartphone **app**. Learners compete by answer questions related to our curriculum content. Cybersecurity **tutors**, including service-learning undergraduate students and other individuals recruited from the Coalition partner schools' faculty and industry partners provide additional support for the modules' hands-on labs as needed.

The first group of **35-40** participant **cohorts** launched in Fall 2021 and our fifth cohort of the initial pilot began in March 2022 and is scheduled to complete late summer. **~200** military veterans and first responders received **scholarships** to **fully support** their participation in the initial pilot with over 75 on a **waiting list** for our third-year offerings.

Admissions



Curriculum Design

Explorer (Badges = AI Fundamentals & Enterprise Design Thinking)

- IT Basics
- Network Foundations
- Coding
- DB Management
- Privacy/Legal Foundations and Ethics
- Security Principles & Foundations
- Cryptography
- Artificial Intelligence*

Practitioner (Badges = Cloud Security, Cisco Cybersecurity & Blockchain)

- Cloud Foundations
- Network Security
- Information Security
- Cyber Threat Hunting*
- Forensics
- Cognitive Computing*
- Data Mining*
- Blockchain*

Professional (Badges = Azure IoT, RPA and Power Automate & Threat Modeling)

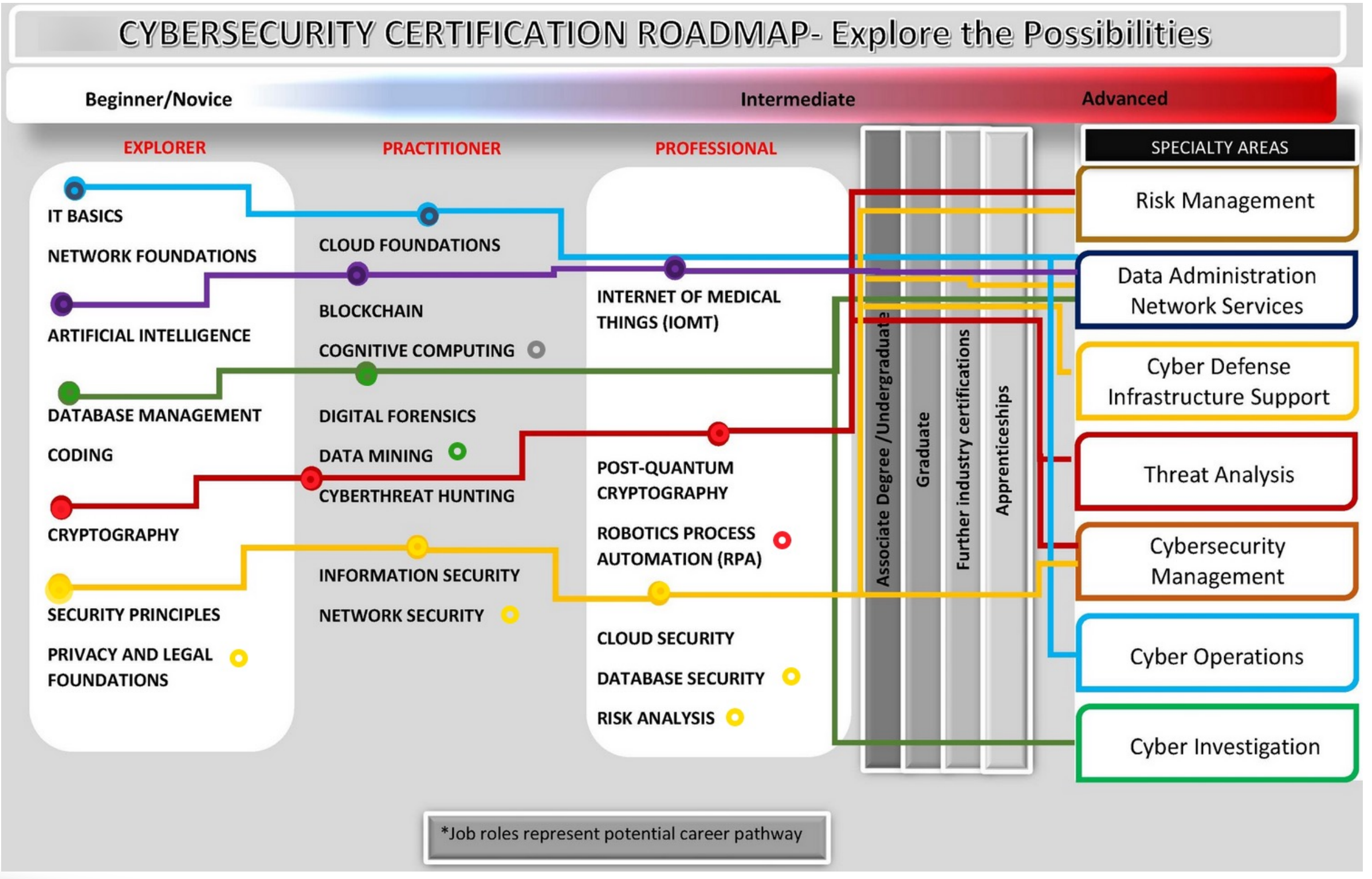
- DB Security
- Cloud security
- IoT
- Post Quantum Cryptography*
- Risk Analysis
- Robotic Process Automation Analysis*
- Healthcare Capstone Project

*Cutting Edge Topic

The program's learning design includes a **competency-based approach** with industry partners co-constructing the competency domains, as well as validating the competency achievements to ensure the learning is systematic, industry-relevant, and evidence-based. In addition to the purpose-built learning activities of the Coalition, the curriculum also builds technical skills by assigning **technology industry certificates & badges** that complement the course materials as homework exercises within each level of the program. These **microcredentials** from top technology vendors such as **Google**, **IBM**, and **Microsoft** include:

- **Cisco Intro to Cybersecurity**
- **Google Analytics for Beginners**
- **IBM Blockchain Essentials**
- **IBM Enterprise Design Thinking**
- **IBM Introduction to Cloud**
- **IBM Watson Studio Essentials**
- **MS Analyze Data with Power BI**
- **MS Intro to Azure IoT**
- **MS Cloud Security**
- **MS Fundamentals of Network Security**
- **MS Get Started with AI on Azure**
- **MS Automate Processes with RPA and Power Automate Desktop**

Interactive Competency Mapping



https://bit.ly/ULCompMap1

Digital Badge & Degree Pathways

Digital badges are awarded throughout the program from top technology vendors to develop knowledge, skills, and experience as well as build credentials demonstrating workforce skills to employers. Upon completion of the program students earn a **Cybersecurity Workforce Development certificate** (non-academic) and are issued a Coalition badge. This concluding digital badge demonstrates that earners have achieved foundational cybersecurity knowledge, skills, and abilities. Interested students may then continue their studies through our **Coalition Pathways to Success** that offer cybersecurity-related degrees from the Associate's level all the way up to a doctorate from our Coalition partner schools.

CYBERSECURITY PATHWAYS COALITION
WANT THIS BADGE? CLICK HERE!
UL
UL
CYBERSECURITY CERTIFICATE
UALR | CITY U | UNF | BCTC | OCTC

https://bit.ly/ULCyberBadge

Acknowledgments

As the Coalition nears the end of the initial curriculum pilot, we are excited to begin seeing the success of our first certificate earners and wish to acknowledge the support of our first cohorts. The feedback they provided during the pilot has been invaluable in assisting us with better aligning the content to the needs of workforce learners. Our entire **Industry Advisory Board** has also been critical to the success of our pilot program, but special thanks go to the following organizations for sharing so generously of their time and expertise:

Baptist Health
Humana
IBM
Knox Regional Development Alliance

The Healthcare Capstone Project, especially, benefited from the gracious participation of **Michael Erickson**, Chief Information Security Officer for Baptist Health.

Contact Us

For more information about the **Healthcare Cybersecurity Pathways** program , please visit:

https://bit.ly/ULWorkCyber