MONTREAT COLLEGE

Montreat College's award-winning, cutting-edge and visionary cybersecurity program prepares students to solve the cybersecurity issues and concerns faced today in many corporate and government environments. Montreat College is actively engaged in developing government, industry, and educational partnerships in the field of cybersecurity. In addition to a traditional on-campus program, and a global on-line program, Montreat College established the Carolina Cyber Center to focus on continuing education training, an innovative workforce development "Academy" program, providing regional cybersecurity services, and developing public/private partnerships to advance the "state of practice" in cybersecurity.

The Carolina Cyber Center (C^3) of Montreat College has an open position to lead a series of cybersecurity classes in our Academy program to develop entry-level cybersecurity professionals of character. We expect to invest heavily in this individual to learn and apply leading practices in pedagogy, andragogy, virtual labs, new cybersecurity technologies, teaching tools, etc.

Position: Full-time Cybersecurity Instructor, Technical Mentor, and Course Developer

Location: Montreat, North Carolina, or remote/virtual

Start Date: Negotiable, but 1st classes start in early May 2021

Summary: Carolina Cyber Center seeks a qualified candidate to serve in a highly diverse, demanding, and critical role:

- Cybersecurity course developer and instructional designer
- Instructor for live and online cybersecurity education and leadership, and
- Serve as a technical and professional mentor to staff and students.

This position will support the C^3 training and workforce development programs. As such, this is a dynamic opportunity to impact the lives of youth, to grow in your own cybersecurity skills and to develop a unique "non-profit" cybersecurity services business. This is a full-time position with commensurate compensation and benefits, which also has the opportunity for additional income via teaching assignments at Montreat College.

A qualified candidate will have a personal commitment to Jesus Christ and affirm and support the vision, mission, statement of faith, and community life covenant of Montreat College. https://www.montreat.edu/about/mission/

Duties and Responsibilities:

This position will have multiple roles, providing a wonderful opportunity to teach, support and mentor cybersecurity students, while going beyond the technical cybersecurity topics to include the whole person – what we term "Essential Life Skills" proven to be critical a successful career in cybersecurity (curriculum for these areas is already either developed or underway):

- Curiosity
- Collaboration
- Discipline
- Grit
- Critical Thinking

The successful candidate will work closely with our team of professionals who are committed to measure ourselves and our programs in order to continually improve and grow. This role will support C^3 by developing, updating, and teaching cybersecurity courses in various media and modalities and will coordinate with and support the Montreat College Cybersecurity program (e.g., 4- year degree education) as well as the Adult and Graduate Studies department (additional on-line courses).

The position will entail leading and mentoring young adults into cybersecurity careers. The role includes leading and working with our curriculum developers and instructional designers to design, write and produce courses and then manage the "virtual" classroom, conduct labs (e.g., NDG, Cisco CyberOps, TryHackMe, RangeForce or Cyberbit, and Immersive Labs, are examples of virtual labs we are considering), and assist students with learning objectives.

Our goal is to help close the cybersecurity skills and employee gap through scalable training. Specifically, the education lead by this position will focus on helping young adults and professionals with their entry-level skills and certifications, such as, but not limited to CompTIA ITF+, A+, Network+, Linux+, Security+, CCNA, Ethical Hacking, SOC Analyst I courses, and like-kind entry-level certifications. Existing materials are available for all courses – but we are ever striving to keep the content current and to explore more opportunities for hands-on/real-world experience.

The position will require a strong knowledge of cybersecurity, IT fundamentals and a willingness for continuous learning. This position will entail both periodic in-person training (e.g., travel to Charlotte or Atlanta once per month) and online training for distance learning. The position will also require some evening and weekend work, though generally will be regular work hours.

Additional responsibilities:

- Research, Evaluate, and prescribe cybersecurity labs, cyber ranges, and/or 3rd party videos/programs that educate and teach practical skills to cybersecurity students.
- Lead/coach students as a team and individuals to compete in CTF (capture the flag) events.
- Stay up to date on the latest information security threats to enterprise networks.

- Serve as a mentor and provide guidance cybersecurity students, demonstrating what it means to be an ethical, critical thinking cybersecurity professional.
- Serve as an IT hardware expert to advise the C^3 Academy (cybersecurity boot camp) and professional divisions of the Carolina Cyber Center on the latest hardware and best practices in implementation.
- Contribute to profitable strategic direction of managed security service provider.

We are also interested in teachers/instructors with a passion to extend/expand their own skills and knowledge and who can bring new insights, technologies, and courses to help us expand our program (e.g., cyber range, cloud security, SOC analyst skills).

We anticipate that a successful candidate will, of course, not know all the labs, certifications, etc. but will be committed to continual learning and "staying ahead of the students" with respect to what and how to lead their learning journeys.

Qualifications:

Successful candidates will demonstrate a passion for developing cybersecurity talent – specifically, passionate about building student's capabilities in alignment with relevant IT/Cybersecurity industry demands, a passion to teach and serve "the next generation" and will have knowledge and experience in:

- Demonstrated entry-level technical skills in the areas largely provided by security services businesses (the "Customers" for our students), for example:
    - Network management
    - Backups
    - End user support
    - EDR/EDM
    - Email and other collaboration system "hardening" and triage
    - Incident Response planning and execution
    - Threat/vulnerability assessments and mitigation
    - Social engineering attacks
- Designing Cybersecurity courses for classroom, live online and asynchronous delivery (and blended)
- Familiarity in instructional design methodologies
- Performing classroom instruction and online/video instruction
- Familiarity with various courses and companies in cybersecurity, prevalent threat vectors, and awareness of leading practices and products in the cybersecurity training industry
- 3-to-5 years professional industry experience in the current state of IT and cybersecurity

Education/Experience:

The most important education/experience is the ability to enable students to be optimal learners. While a master's degree or Bachelor of Science in Computer Science, Information

Systems, Information Security, or Cybersecurity is desired, this is NOT required. We also prefer experience teaching and 5^{+} years of "hands on" industry experience. This position requires certifications (either to hold current, or that we could support you achieving within the first roughly six months) in areas such as: Linux+, A+, Network+, Server+, Security+, Cloud+, and CySA+. We also desire that the candidate could teach, or grow to teach (within 12-18 months), the skills for students to become SOC Analysts, Defense Analysts and other positions aligned to the NIST 800-181 NICE framework. We also have opportunities to teach/train on CCNA and Red Hat courses (low priority), and to earn various cloud security certifications (e.g., AWS, GCP, Azure), CISM, and GIAC.

Application Requirements/How to Apply:

Review of applicants will begin immediately and continue until the position is filled. Feel free to reach out to Adam C. Bricker (contact below) to discuss your interest, or move to directly providing the following materials:

- Complete https://www.montreat.edu/about/job-openings/application/
- Letter of Application (include passions for future personal and professional growth)
- Curriculum Vitae or Resume
- Samples of any courses developed and/or taught (videos, outlines, etc.)

Send materials electronically to:

Adam C. Bricker
Executive Director, Carolina Cyber Center
Montreat College
adam.bricker@carolinacybercenter.com

About Montreat College:

Montreat College is a Christian liberal arts college accredited by the Commission on Colleges of the Southern Association of Colleges and Schools to offer masters, bachelors, and associates degrees. The main campus is in the Blue Ridge Mountains fifteen miles east of Asheville, North Carolina, a region recognized as one of the most attractive living environments in the United States. Satellite campuses in Asheville, Charlotte, and other sites supplement the main campus. The College is committed to Christ-centered teaching and learning and is a member of the Council for Christian Colleges & Universities.

The Carolina Cyber Center began as a vision from Dr. Paul Maurer, President of Montreat College, in 2018 to leverage the tremendous progress Montreat College made with its cybersecurity education program (e.g., enrollment growth, highly qualified/experienced professors, CAE designation from NSA/DHS, MOU with the U.S. Army). Initial funding for C3 was provided by Montreat College and in 2019 the State of North Carolina provided additional funding and in late 2020 we were awarded several new grants providing multi-year funding. The Center's vison is to be a national demonstration resource for developing community cyber

awareness, ethical cybersecurity professionals, and public/private partnerships to advance the "state of practice" in cybersecurity.