Description of Cybersecurity AAS Program experience

This AAS degree prepares students for entry-level positions in careers in the fast-growing field of cybersecurity. Practical skills in cybersecurity are learned from industry professionals.

The program emphasizes computer security and information assurance concepts augmented with current industry standard techniques. Topics cover threats and vulnerabilities, prevention at the technical (hardware and software) and human levels, detection, response, and management aspects of security.

Our Cybersecurity Center and Lab provides significant virtual computing and networking capabilities. The Cyber Lab is used for academic competitions and research activities and can host 100-plus virtual servers, 250-plus virtual desktops, isolated networks, and wireless and forensic technologies. It is available for customized, short, intensive training.

The program prepares entry-level employees with cybersecurity expertise and also offers students a transfer option to four-year institutions. The proposed program of study is designed to address the need for increasing the talent pool of highly qualified employees to work in cybersecurity in the homeland security industry.

As a member of CyberWatch, the Montgomery College curriculum follows National Security Telecommunications and Systems Security Instruction (NSTISSI) 4011 and 4013 standards. Also, the courseware is certified as mapping 100% to the Committee on National Security Systems (CNSS) National Standard 4011.

It will also help prepare students to sit for a variety of industry certifications, including the Computing Technology Industry Association's (CompTIA) A+, Network+ and Security+ certifications; Cisco Certified Network Associate (CCNA) certification; and the Security Certified Network Professional certification.

A new transfer option exists as of September 25, 2020. MC, in partnership with SANS Technology Institute (STI) will offer the first two years of STI's Bachelor of Professional Studies in Applied Cybersecurity (BACS) program. This new degree was approved by the Maryland Higher Education Commission (MHEC) Sept. 25. The BACS creates a cost-effective academic pipeline that supplies highly skilled cybersecurity professionals qualified for elite positions with employers in Maryland and across the nation. In addition to all degree requirements, graduates will have seven advanced immersion cybersecurity courses. For the graduates, the BACS will provide credentials that demonstrate hands-on cybersecurity skills and knowledge far beyond those offered in most graduate cybersecurity degree programs.

Program Outcomes

Upon completion of this program a student will be able to:

- Apply software patches to operating systems and applications.

- Evaluate a system for security vulnerabilities using appropriate resources.
- Use standard software tools to detect attempted security breaches in networks.
- Implement network security defenses.
- Describe a professional's responsibility in the areas of individual privacy, intellectual property rights, and ethics and codes of conduct.
- Examine legal, social, and ethical concerns related to securing information systems and networks.
- Explain how to use current forensic tools.
- Demonstrate critical thinking and problem-solving skills on issues related to cybersecurity.
- Describe the differences between internal and external threats and how to defend against each.
- Propose cybersecurity solutions based on real-world problem scenarios.
- Demonstrate the skills necessary to be successful in passing at least 2 of the following certification exams: CCNA (Cisco Certified Network Administrator), CompTIA Network+, CompTIA Security+, and/or ISC2 Professional Security certification(s).

Required Courses. Courses descriptions available at https://www.montgomerycollege.edu/offices/elite/navy/

CMSC 135 Introduction to Scripting

CMSC 253 UNIX/LINUX System Administration

NWIT 127 Microcomputer Essentials - prepares students for the Essential exam for the CompTIA A+ Certificate.

NWIT 151 Introduction to Networking

NWIT 173 Network Security - prepares students for the CompTIA Security+ certification exam.

NWIT 230 Intro to Cyber Ops

NWIT 245 Defending the Network

NWIT 246 Attacker Tools and Techniques

NWIT 247 Introduction to Incident Response

NWIT 252 CISCO Networking - equivalent to CyberWATCH course CW 151

NWIT 263 Intro to Digital Forensics - equivalent to Cyber WATCH course CW 170.

NWIT 275 Wireless Security

NWIT 291 Cybersecurity Capstone - prepares students for the ISC2 Professional Security Certification(s).