CYBERSECURITY ANALYTICS AND OPERATIONS, B.S. (INFORMATION SCIENCES AND TECHNOLOGY)

Begin Campus: Any Penn State Campus

End Campus: University Park, World Campus

Program Learning Objectives

- **Knowledge/Application:** Understand and apply the interdisciplinary knowledge of information sciences in a security context to recognize, analyze, defend against, and manage cyber risks.
  - Understand the components and interoperability of computer hardware, operating systems, networks and databases.
  - Demonstrate proficiency in programming and scripting to perform Cybersecurity automation and analysis.
  - Understand Cyber threats and appropriate defensive designs and tools to mitigate the risk of attack.
  - Understand the procedures for Cybersecurity Incident Handling and Response.
  - Understand the static and dynamic analysis of malware.
- **Problem-Solving:** Understand, apply and adapt various problem solving strategies, using appropriate technology and methods.
  - Identify Cybersecurity threats and implement complementary defensive measures to mitigate risk.
  - Apply data analytics in a security context to analyze, predict and prevent cyberattacks.
  - Perform malware analysis and forensics to understand the nature and origin of attacks.
  - Evaluate several Cybersecurity frameworks and provide analysis that culminates in a high level executive briefing exercise.
- **Evaluation and Communication (Individual and Team):** Communicate and work effectively (both individually and in teams) with a range of perspectives and audiences through a variety of media.
  - Synthesize data from multiple sources to help make informed decisions.
  - Communicate effectively to a variety of audiences through writing and the spoken word.
- **Professional Responsibilities:** Understand professional responsibilities in terms of the ethical, legal and security policy aspects of information assurance and security.
  - Understand the rules, regulations and issues related to compliance with applicable laws and regulations related to Information Security and Privacy.
  - Understand the legal and ethical ramifications of violating the trust that organizations will place in you as a Cybersecurity professional.
- **Lifelong Learning:** Commit to the continuous acquisition of relevant knowledge for professional development by self-teaching and/or on-going education and certification.
  - Employ information-seeking strategies and self-directed learning in pursuit of current knowledge.
  - Enroll in professional development and pursue industry certifications to enhance your career and the profession.