Status | Complete

The final goal of this program is to prepare learners to be job-ready, with an ultimate career outcome of gaining employment in the cyber security field. This doesn't mean you will finish the program knowing everything about cyber security. Rather, you will have the foundation and skills to meet work challenges, problem solve issues, and, most importantly, continue to learn and develop on the job.

Program Outcomes

After completing the Cyber Security Bootcamp Program, learners will be able to:

- Demonstrate a foundational understanding of Cybersecurity principles and roles, Computers & Operating Systems, and Networks
- Design, configure, implement and troubleshoot a single-site network
- Implement the confidentiality, integrity and availability (CIA) triad, adjusting an existing network to meet specific scenario requirements
- Create and maintain batch and BASH files, and write basic Python scripts for cybersecurity-specific scenarios
- Develop an effective blue team, an optimized organizational chart, and a functional security operations center (SOC) to organize and monitor the security of an organization
- Create a report typical of a blue team communication to C Level Executives as a result of a new or updated compliance requirement that would be made to a specific industry at a specific location
- Conduct a complete vulnerability assessment to highlight where vulnerabilities exist, assess vulnerabilities, identify risks to a business, and effectively communicate the results
- Create a response report that shows the categorization and prioritization of incidents, the use of escalation and the NIST incident response lifecycle
- Build a work case on encryption by researching, comparing, assessing, and recommending encryption tools and protocols.
- Effectively communicate the relevance of the MITRE ATT&CK Framework, Lockheed Martin Cyber Kill Chain and dwell times to a business audience
- Examine, prepare for, and discover indicators of compromise on networks and systems, using network forensics tools
- Perform threat modelling which will inform clearly communicated mitigation plans and reviews for network architecture.
- Work collaboratively within a cyber security team to assess risk and develop a security process that meets a specific set of objectives.
- Employ specific learning strategies and frameworks to continue to build their skill set while on the job.
- Identify knowledge gaps, growth path, and specialization pathways, and develop actionable next steps for themselves immediately after completing the program.

✕ Cancel Submission