UFIT Information Security

Cybersecurity Detection & Response Internship

Hiring Manager Name & Title: Derrius Marlin, Cybersecurity Engineer, Team Lead
Department: Information Security
Title of Internship: Cybersecurity Engineer Intern

Brief Description of Internship (please include physical location of the job):

This internship position will support the Cybersecurity Detection and Response (CDR) team by assisting staff in one or more of these areas, threat management, vulnerability management, incident management, or the processing of eDiscovery, litigation, and investigative support service requests.

Specific Duties:

- Monitor the CDR's intrusion detection and prevention systems to identify and escalate identified threats to the institution.
- Working with CDR's enterprise vulnerability management system to identify vulnerabilities in university IT assets.
- Shadow CDR staff to learn about daily threat and vulnerability detection and response tasks and assist in related activities as needed.
- Triage email sent to abuse@ufl.edu to identify email threats and compromised accounts. Validate the legitimacy of email reported to abuse@ufl.edu and respond to recipient's inquiries.
- Contribute to UF's phishing awareness training program.
- Contribute to the CDR team's technical documentation.
- Other duties as assigned

Hours Per Week: 10 -20 hours per week. Shifts must be in increments of 3 or more consecutive hours
Location: Ayers building at 720 SW 2nd Avenue
Hourly Rate: $13.00

Qualifications Needed:

- Basic knowledge of various software, operating systems, networking, database, and hardware.
- Basic knowledge of Internet network addressing (IP addresses, routing, TCP/UDP port numbering) and network security concepts (encryption, firewalls, perimeter protection).
- Basic knowledge of current cybersecurity threats and vulnerabilities
- Technical certifications a plus
- Level 2 background check required.

Learning Objectives:

- Develop an understanding of their career field of interest, including the skills, responsibilities, and career trajectory of professionals. This includes the importance of Confidentiality, Integrity, and Availability in an enterprise system.
- Develop and demonstrate effective work habits, including time management, punctuality, and personal accountability related to the work and its function in the economy.
- Demonstrate openness, inclusiveness, sensitivity, and the ability to interact respectfully with all people and understand individuals' differences.
- Identify, document, and carry out performance objectives (mutually agreed upon by the employer, the UFIT experiential learning supervisor, and the student) related to the practical experience in their internship.
- Develop a fundamental understanding of cyber-attack stages, methods, and techniques.
- Develop a fundamental understanding of intrusion detection methodologies and techniques for detecting host and network-based intrusions.
- Develop a fundamental understanding of the function and use of a Security information and event management (SIEM) and log management platform.
- Develop a fundamental understanding of system and application security vulnerabilities.
- Develop a fundamental understanding of established incident management protocols, processes, and procedures.