Polk State College Apprenticeship Partnership in Information Technology (MAP IT)

Cybersecurity Analyst

Eight-week course; Online self-paced independent study
Total Course Cost: $336
Cost Breakdown: Credit Cost: $336
Cost covered by the Grant: Books $149, Lab Fees: $60, and One-time exam fee: $250

This course covers the information and skillsets necessary for responding to cybersecurity threats and attacks, including the application of environmental reconnaissance techniques such as OS fingerprinting, e-mail harvesting, and social media profiling using various tools (e.g., Nmap, netstat, and Syslog). Training enables the participant to analyze the results of network reconnaissance, recommend or implement countermeasures, and secure a corporate environment by scanning for vulnerabilities. The course incorporates response strategies for cyber incidents such as using a forensics toolkit, maintaining the chain of custody, and analyzing the severity of an incident.

OJT Competencies: This training develops the student's ability to:

Security Operations Center (SOC)
- Recognize the role and responsibilities of each individual involved in a Security Operations Center.
- Create basic incident response processes for a functioning SOC.
- Deploy technology to aid a Security Operations Center.

Network Monitoring
- Demonstrate fluency with Network Security Monitoring (NSM) concepts.
- Configure event collection for devices on a network.
- Identify ways to increase visibility when monitoring different network layers.
- Develop the ability to centralize network logs.

Incident Lifecycle
- Monitor events across devices on a network.
- Trigger alerts for suspicious activity while reducing the noise of false-positives.
- Detect anomalous behavior and activity effectively while monitoring devices throughout a network.
- Determine when to escalate into an incident and respond appropriately.

The Role of Threat Intelligence
- Assess the value a strong threat-intelligence feed brings to an organization.
- Introduce a threat platform and threat intelligence successfully into Security Operations Center.

Polk State College Apprenticeship Partnership in Information Technology (MAP IT)

This page left blank.