Improving Security Operations and Leveraging SIEM

Aleika Chery, DigITs Intern – Information Security (Security Threat Incident Management)

SOC (Security Operations Center): Centralized team responsible for monitoring, detecting, analyzing, & responding to security events

SOC-CCM Methodology:
- ○ Plan scope
- ○ Assess capabilities
- ○ Find gaps
- ○ Recommend improvements

SIEM
- ○ Security Incident and Event Management
- ○ Splunk: A SIEM Tool used to monitor security logs

Internal SOC Assessment:
- ○ Identify security gaps
- ○ Evaluate SOC effectiveness
- ○ Improve threat response
- ○ Ensure compliance

Examples of Questions:
- ○ Alerts prioritized correctly?
- ○ Incident response process documented?
- ○ Are tools regularly updated and tuned?

Goals:
- ✓ Complete Intro to Splunk Courses
- ✓ Learn how to conduct searches & create dashboards in Splunk