STUDENT EMPLOYEE JOB DESCRIPTION JD# 648 LCDI

Supervisor: Joseph Williams
Department: Leahy Center for Digital Forensics (LCDI)
Position Type: Federal Work-Study Program __X__ Part-Time Student Employment __X___

Job #: 648 LCDI
Job Level: 2
Pay Rate: $10.98
Workday Job Title: LCDI Security Operations Analyst – Tier 1

Posted Job Title: Security Operations Analyst – Tier 1 for The Senator Leahy Center for Digital Investigation (LCDI)

Job Description: Security Operations Analyst Tier 1 will conduct routine inspections of security logs, install, manage, and configure security software, and monitor for security events and indicators of compromise on the LCDI's network. This position is considered entry level. Student(s) in this position will all assist the Tier 2 Analysts with proactive and reactive security services for both the LCDI and its external clients.

The Security Operations Analyst Tier 1 duties will include but not limited to the following tasks:

- Track, maintain, and respond to service tickets from LCDI users.
- Analyze data for inconsistencies and report on potential threats or inconsistencies
- Utilize the LCDI's SIEM system to perform log analysis and correlation.
- Monitor the LCDI's network for security alerts and promptly respond to those alerts.
- Prepare technical reports based off of security investigations.
- Research and deploy new technologies that will help the LCDI advance its mission goals.
- All other duties as assigned by the Security Operations Analyst Team Lead and/or LCDI Leadership

Required Qualifications:

- Proficient in Microsoft Windows based operating systems
- Practical understanding of computer hardware and software
- Basic understanding of computer networks and network configurations
- Basic troubleshooting skills
- Ability to collaborate with the team
- Strong written and verbal communication and social skills
- Attend the weekly Security Operations Analysts meeting
- All other duties as assigned by the Security Operations Analyst Team Lead and/or LCDI Leadership

Additional Preferred Qualifications:

- Knowledgeable or experienced with UNIX, LINUX, and firewalls
- Working knowledge of virtual environments
- Understanding of Active Directory
- Basic knowledge of Windows Domain environments
- Working knowledge of log aggregation services such as ELK, GrayLog, or Splunk
- Working knowledge of digital forensic analysis tools and investigations

How to Apply: Interested applicants should complete an application online: http://bit.ly/LCDIapplication
Approximate Hours per Week: ~6/8 hr/week
Job Location: Miller Center at Lakeside Avenue Campus

Qualified candidates will also be expected to attend a mandatory LCDI Town Hall and staff one LCDI event (i.e. Open Houses, Tech Jam, etc). In order to successfully accomplish the goals of this position, it may be necessary for the student to adjust his/her schedule to accommodate meetings with team members (i.e. monthly training and/or meetings).