STUDENT EMPLOYEE JOB DESCRIPTION JD# 623 LCDI

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

Job #: 623 LCDI
Job Level: Level
3 Rate: $11.10

Posted Job Title: LCDI Security Operations Analyst Tier 2 for The Senator Leahy Center for Digital Investigation (LCDI)

Job Description: A Security Operations Analyst Tier 2 will work at the Leahy Center for Digital Investigation and provide proactive and reactive services for internal and external clients. They will help create/build/maintain monitoring services, analyze data for threats and respond with digital forensic techniques when needed. The analyst must also be able to develop solutions while maintaining a high level of confidentially related to their work.

In order to ensure these systems are running in a manner that consistent with our mission, the Security Operations Analyst Tier 2 will conduct some of the following tasks:

- Monitor data for inconsistencies and report on potential threats or inconsistencies
- Assist with or make suggestions for increased visibility within client/partner networks
- Research latest technologies with relation to the LCDI mission
- Build and implement network equipment solutions as needed
- All other duties as assigned by the Security Operations Analyst Team Lead and/or LCDI Leadership

Required Qualifications:

- 2-3 years of experience as an undergraduate student in the ITS division and/or relevant work experience.
- Proficient in Microsoft Windows, Mac OS and Linux based operating systems
- Working knowledge of Active Directory, DHCP, DNS, Group Policy, and other Windows Server based processes
- Knowledgeable or experience with UNIX, LINUX, routers, switches, and firewalls
- Ability to program/script in at least one language
- Comfortable with the interpretation and analysis of Windows, Linux, and other OS based event/security logs
- Working knowledge of Vmware
- Understanding of network based incident responses and how they should be applied/conducted
- Working knowledge of networks, to include TCP/IP protocols
- Working knowledge in digital forensic tools and techniques
- Working knowledge in malware analysis techniques
- Attend the weekly Security Operations Analysts meeting
- All other duties as assigned by the Security Operations Analyst Team Lead and/or LCDI Leadership

Additional Desired Qualifications:

- Experience with log aggregation services such as ELK, GrayLog, or Splunk
- Experience with digital forensic analysis tools and investigations.
- **All sophomore applicants will be required to submit one recommendation from a professor or employer to jwilliams@champlain.edu before an interview will be given.**

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).

Job Location: Miller Center at Lakeside Avenue Campus – 175 Lakeside Ave, Burlington VT 05401