Columbia University Medical Center

Information Security Incident Specialist

COMPANY: Columbia University Medical Center

LOCATION: Washington Heights, New York, NY

GRADE: Officer 105

JOB DESCRIPTION

The Security Operations team is a part of the Information Security Office (ISO) of Columbia University Medical Center. The Information Security Incident Specialist is a member of the Information Security Operation Manager's team, primarily as a resource to the Lead Incident Handler, but may also be allocated to projects and tasks as required by the Information Security Engineer.

This is intended to be an entry-level position with a recent 4-year undergraduate degree in a computer science related area of, with some experience to evidence an interest in an information security career. The ideal candidate will be a motivated self-starter and a team player with superior analytic skills, the ability to write clearly about technical issues to a variety of audiences, and a strong work ethic.

PRINCIPAL DUTIES AND RESPONSIBILITIES

- Monitor and evaluate data from sources of security event information in order to promptly identify, evaluate, and respond appropriately to information security incidents which impact the information infrastructure of Columbia University Medical Center. May be called upon to mobilize and participate in incident handling on short notice during off-shift hours.
- Draft formal incident reports. Contribute to the preparation of vulnerability reporting metrics, threat intelligence, and other analysis.
- Interface with I.T. resources and other key stakeholders in order to facilitate coordinated security operations. Critically the execution of this function should be carried out in a manner which promotes a collegial environment.
- Assist in security thought leadership activities which promote greater awareness of information security leading practices.
- Other duties as required.

REQUIREMENTS

- Four-year undergraduate degree in computer science or related field. Transcript must show sufficient course work related to information security.

- Some relevant work experience either in applications development, I.T. operations, incident management, health care, research, institutes of higher learning, and/or technical writing. Additional evidence that technical skills are current is strongly favored.
- Education, training, or working experience with data forensics is highly desireable.
- Writing ability demonstrated through outstanding cover letter and technical writing sample.

ESSENTIAL FUNCTIONS

- Monitor and evaluate data from sources of security event information in order to promptly identify, evaluate, and respond appropriately to information security incidents which impact the information infrastructure of Columbia University Medical Center. May be called upon to mobilize and participate in incident handling on short notice during off-shift hours. 30%
- Draft formal incident reports. Contribute to the preparation of vulnerability reporting metrics, threat intelligence, and other analysis. 25%
- Interface with I.T. resources and other key stakeholders in order to facilitate coordinated security operations. Critically the execution of this function should be carried out in a manner which promotes a collegial environment.25%
- Assist in security thought leadership activities which promote greater awareness of information security leading practices. 5%
- Other duties as required. 15%