ENTRY LEVEL INCIDENT RESPONSE

Posting ID: EM17B1243D

Company: The International Association of Computer Investigative Specialists

Company Website: https://www.iacis.com/

Work Location: Los Angeles, CA. Houston, TX. New York, NY. Vienna, VA

Salary:

College Major(s): Computer Science (CS)

College Level(s): Undergraduate-Senior, Graduate Student, PhD. Student

OVERVIEW

Over its vibrant and colorful history, IACIS has emerged as a premiere international organization specializing in training and certification in the field of computer forensics. As a testimony to its continual pursuit of excellence in the scientific discipline of computer forensics, in 2012 IACIS was accredited by the Forensic Specialties Accreditation Board (FSAB) and is recognized as the first computer forensics organization accredited for its certification program (CFCE). Later that same year IACIS began offering certification as a part of the Certified Advanced Windows Forensic Examiner’s program. Today IACIS is governed by an 11-person Board of Directors and consists of approximately 2,200 members and 1,800 CFCE’s located around the world.

For those with some forensic experience that want to expand to the incident response field, we will have a few positions opening. These will be Lab/Office positions in any one of the following areas: Vienna Va. New York City, Houston, and Los Angeles.

Navigant’s Information Security (IS) Services Practice is a rapidly growing part of the Legal Technology Solutions Segment of our business. Our professionals help our clients address their critical information security challenges, including incident investigation/response, as well as assessing and reducing information security risks.

Roles and Responsibilities

Participate in security incident investigations that involve computer crimes and require log, forensic and malware analysis
Collect and analyze intrusion detection system alerts, firewall logs, network traffic logs and host system logs to evaluate whether unauthorized access or information ex-filtration occurred
Perform forensic analysis to identify the presence of any malware, malware capabilities/actions and what actions the malware took
Conduct security investigations in Linux and/or Windows environments
Provide input into client communications, both written and oral, related to analyses performed for senior level review
**Education and Qualifications**
Approximately 0-4 years of experience working in the Incident Response space
Understanding of how to communicate effectively and concisely with high level management and C-suite clients
Ability to approach projects both from a long-range and immediate view
Experience working with non-Windows programs (such as Linux, Unix, Mac)
Scripting/programming experience (specifically Python, C#, VBA, or Shell)
Experience working on projects in an investigatory capacity – either law enforcement or incident response
Strong desire to work on a team in a collaborative environment to achieve common goals
Ability to correlate events from multiple sources to create a timeline analysis across end points of an incident
Exceptional organizational skills, to include detailed note taking abilities
Passion for the sport of Incident Response, and a desire for continuous improvement in expertise

**Preferred Skills**
Understanding of how to leverage existing security applications and appliances to address a compromise or malware/ransomware outbreak
Experience working with Enterprise networks (specifically CCNA/CCNP security)
Understanding of how to take malware apart from a virtual machine, dynamic malware analysis, and reverse engineering perspective
Memory analysis skills a plus
Understanding of mitigation and clean-up strategies
Proficient in log analysis of multiple types
Ability to analyze complex network packet captures
Undergrad or Master’s Degree in Computer Science/Cyber Security/MSIS or equivalent work experience

**How to Apply**
If interested send resume and desired location to jc.blankenship@verizon.net or John.Blankenship@navigant.com