Titles: Incident Response Analyst (Incident Response Engineer, Incident Responder)

Experience: 3 – 5+ years related work experience

Education: Bachelor’s degree in Computer Science; Master’s degree preferred for some positions

Certifications: GCFA, GCIH, GCFE, GNFA, GREM, GCCC

Overview: Seeking an experienced Incident Response Analyst. The analyst will be responsible for incident response, threat hunting, and data analysis to protect and maintain the overall security of the enterprise.

Responsibilities:

- Protecting enterprise systems and information by promptly responding to security threats and incidents, acting individually and as part of a team to resolve issues
- Proactively hunting for threats and enacting identification, containment, and eradication measures while supporting recovery efforts.
- Act as subject matter expert to provide insight and guidance to colleagues engaging in prevention measures.
- Analyzing cyber security incidents to solve issues and improve incident handling procedures
- Receive Tier 2/3 incident escalation from detection operations and assist with real-time, continuous (24x7) security event monitoring, response, and reporting
- Proactive coordination with appropriate departments during a security incident – management, legal, security, operations, and others.
- Conducting research regarding the latest methods, tools, and trends in digital forensics analysis
- Creating thorough reports and documentation of all incidents and procedures; presenting findings to team and leadership on a routine basis

Requirements:

- Must have a deep understanding of computer intrusion activities, incident response techniques, tools, and procedures
- Thorough knowledge of digital forensics methodology as well as security architecture, system administration, and networking (including TCP/IP, DNS, HTTP, SMTP)
- Knowledge of operating systems including Linux/Unix and Windows
- Experience with programming languages such as Python, Perl, C/C++, PowerShell, etc.
- Experience with security assessment tools such as NMAP, Netcat, Nessus, and Metasploit is a plus.
- Excellent written and verbal communication skills

- Excellent organization, time management, and attention to detail
- Must be action-oriented and have a proactive approach to solving issues
- Ability to work individually and as part of a team
- May need to have or obtain a security clearance