Example of Cyber Incident Response Job Description

Powered by www.VelvetJobs.com

Our company is growing rapidly and is searching for experienced candidates for the position of cyber incident response. To join our growing team, please review the list of responsibilities and qualifications.

Responsibilities for cyber incident response

- Direct global delivery of 24/7 cyber security incident response services and resources
- Oversee the development and maintenance of incident response standards, processes, and guidelines
- Coordinate incident response scenarios and routine exercises to ensure operational readiness
- Improve security monitoring efficiency and incident response tasks through automation and scripting
- Record and document security incidents, including analysis results, the timeline of events and incident response activities
- Develop and maintain incident response standards, processes, and guidelines
- Lead the delivery of incident response scenarios and routine exercises
- Participate in the analysis and development of improved standardized operating processes and procedures for the Cyber Command Center
- Coordinate with CyCom staff to validate network alerts
- Perform analysis of log files from individual host logs, network traffic logs, firewall logs, and intrusion detection system logs

Qualifications for cyber incident response

- An ability to build relationships and liaise with clients
- The ability to manage and prioritize workload
- Experience of delivering projects as part of a team

- Experience in Malware analysis and using analysis tools such as Splunk, Elastic search, RSA Analytics/NetWitness or similar
- Experience of performing computer forensic analysis in support of litigation and/or investigation