



# Example of Cyber Incident Response Job Description

Powered by [www.VelvetJobs.com](http://www.VelvetJobs.com)

Our company is looking to fill the role of cyber incident response. Thank you in advance for taking a look at the list of responsibilities and qualifications. We look forward to reviewing your resume.

## Responsibilities for cyber incident response

- Developing a role within the Forensic Technology team as a whole, supporting internal development opportunities and helping to grow the practice
- Analyze forensic evidence for security incidents and disciplinary or criminal investigations
- Conduct network packet analysis using commercial and open source tools
- Analyze malware and system forensics to determine level of impact
- In conjunction with the Sr
- Initiate computer incident handling procedures as needed to identify, contain and remediate actual or potential security-related compromises
- Conduct analysis of computer security advisories, vulnerability scans, and cyber intelligence threat reports in order to improve the company IT security posture
- Proactively study and detect threats to the corporation
- Perform phishing, spam, malware or forensic analysis as part of the incident management process
- Perform sensitive security investigations in a manner consistent with industry standards with regards to computer and network forensics services

## Qualifications for cyber incident response

- Experience in leading a team with a proven ability in developing talent, including identifying and attracting talent and creating an organization that is

- Previous experience in effectively utilizing intel driven defense
- Eligibility for and willingness to obtain a US Secret or higher clearance, if required
- Deploy, install, manage, and operate McAfee ESM Security Information Event Manager
- Deploy, install, manage, and operate file integrity monitoring systems