Example of Incident Response Analyst Job Description

Powered by www.VelvetJobs.com

Our company is growing rapidly and is looking for an incident response analyst. If you are looking for an exciting place to work, please take a look at the list of qualifications below.

Responsibilities for incident response analyst

- Conduct host based forensics and analysis to determine root cause and impact
- Continuously monitor changes to computing infrastructure
- Analyze a large volume of security event data from a variety of sources with the goal of identifying suspicious and malicious activity
- Identify, track and report network intrusions using multiple cyber technologies
- Triage and analysis of real-time data feeds (such as system logs and alerts) for potential intrusions
- Create documentation regarding the identification, analysis and remediation of security threats and incidents
- Perform follow-up analysis throughout the incident lifecycle, and complete projects and tasks associated with security monitoring, detection, and incident response
- Authoring and implementation of original detection rules for various monitoring systems on the basis of current threats and vulnerabilities
- Build and maintain custom security detection logic to analyze and correlate information to produce meaningful and actionable results
- Participation in on-call rotation to provide 24x7 incident response coverage

Qualifications for incident response analyst

- Excellent technical presentation skills, both written and verbal, with the ability to communicate the impact and importance of detailed technical information to a non-technical audience
- Experience leading complex and varied investigations and managing several incident analysts• Experience managing a team of analysts and investigators
- Operating System internals and security (Essential to have Windows experience, other operating systems are desirable)
- Host forensics / intrusion analysis