Example of Cyber Incident Response Job Description

Powered by www.VelvetJobs.com

Our innovative and growing company is looking for a cyber incident response. Please review the list of responsibilities and qualifications. While this is our ideal list, we will consider candidates that do not necessarily have all of the qualifications, but have sufficient experience and talent.

Responsibilities for cyber incident response

- Facilitate the integration of threat and data feeds for the purposes of incident response
- Assist Incident Response coordination efforts with internal (ITS) and external organizations (law enforcement or Inspector General)
- Assist with all phases of research maintenance and support of digital forensics lab infrastructure, including evidence handling, tracking evidence inventory, configuring network equipment, updating software, and other related activities
- Assist with other Incident Response and Forensic activities related to computer security incidents for NYS, as assigned
- Work with the Firm's SOC to respond to emerging incidents in a timely manner
- Response to security incidents across a wide array of technologies
- Evaluate and/or Implement IS solutions and controls to ensure data security and integrity for CDK clients
- Protects computer assets by developing security strategies
- Review new IR tickets and perform initial analysis
- Review daily reports from security tools and respond as necessary

Qualifications for cyber incident response

- Deploy, install, manage, and operate Intrusion Detection/Prevention Systems

- Perform daily vulnerability check using multiple intelligence gathering sources and provide written summaries of threat and vulnerability information
- Coordinate with Client team to ensure all devices and components report all logs to the Security Information Event Manager and perform troubleshooting and maintenance of assets
- Update and/or assist the hosted system's personnel in updating artifacts of the Risk Management Framework (RMF)
- Will possess both Baseline and Computing Environment certification as defined in DoD Instruction 8570.01M