Example of Incident Handler Job Description

Our innovative and growing company is looking for an incident handler. 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 incident handler

- Perform additional analysis of escalations from Incident Triage Analyst and review Level 2 tickets
- Provide an effective and comprehensive response that includes the recovery of any affected systems and the return to a fully functioning, secure, operational state for all services and systems
- Understand patterns of activity and trends to characterize the threat and direct protective and defensive strategies
- Sometimes intelligence and technical information may come from sources unique to the CND environment, including sources outside the AO
- Document all findings and coordinating activities through the Judicial ticket tracking system HEAT
- Collaborate with Threat Monitoring event handlers and to improve prevention and detection methods
- Conducting digital forensics examinations utilizing a variety of tools
- Assessing and reporting on the nature and scope of compromises
- Supporting information security compliance efforts
- Processing security-related help tickets via the Remedy “Request for Service” application

Qualifications for incident handler

- Computer proficiency with MS Office application experience including Word,

- Familiarity with core concepts of security incident response, , the typical phases of response, vulnerabilities vs threats vs actors, Indicators of Compromise (IoCs)
- Incident Handler will maintain twenty four (24) hours a day, seven (7) days a week, three hundred sixty five (365) days per year, incident handling capability
- Working with other members of the IT Security team, researches, designs, and advocates new technologies, architectures, and security products that will support security requirements for the enterprise and its customers, business partners and vendors
- Research and analyze potential impact of new threats and exploits and communicate risks to relevant business units
- Relevant technical security certifications (GIAC, OSCP, EC-Council, ISC-2)