Example of Incident Response Analyst Job Description

Our company is looking for an incident response analyst. 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 response analyst

- Investigate potential identity theft and/or intrusions to/from client facing systems and resources
- Produce monthly and quarterly incident reports
- Document actions taken for audit, regulatory and legal purposes within approved incident tracking system
- Collaborate with business unit technical teams for issue resolution and mitigation control implementation
- Additional responsibilities will include performing documentation review and improvement, attending meetings as needed
- Incident Response Process – Owns the critical process steps – detection, validation, containment, remediation, and communication – for computer-based security events and incidents such as malware infections, potential compromise, Distributed Denial of Service (DDoS)
- CITSIRT Team Member – Respond to critical security incidents and lead escalation teams to close with response, containment and remediation
- Security Operations Playbooks – Create, maintain and promote a set of security operation playbooks with Agilent's IT teams to effectively trigger and execute the security incident response process
- Logging and Monitoring Across infrastructure & Applications – Manages the current state of logging and monitoring through Splunk and Syslog, maintains a vision of ideal state of logging and monitoring, and drives a prioritized

- Internal / External Engagements – Act as Information Security & Risk consultant to various IT and business driven projects and operations

Qualifications for incident response analyst

- Bachelor's Degree in Business, Management Information Systems, or a related field
- Associate’s Degree or equivalent from two-year College or technical school in Information Technology, Information Security/Assurance, Engineering or related field of study
- Experience with scripting languages such as Perl, Python and PowerShell required
- This position requires on-call work in a 24/7/365 environment
- Advanced knowledge of information systems security concepts and technologies
- At least 2 years relevant working experience preferred