Downloaded from <https://www.velvetjobs.com/job-descriptions/incident-analyst>

# Example of Incident Analyst Job Description

Our company is growing rapidly and is looking for an incident analyst. Thank you in advance for taking a look at the list of responsibilities and qualifications. We look forward to reviewing your resume.

## Responsibilities for incident analyst

* Maintain and continuously improve the process, toolkits, and systems for managing business incidents
* Monitor business incidents to confirm they are promptly contained, remediated, analysed and corrected for root cause, recorded, and reported to senior management as needed
* Periodically monitor incident records to confirm documentation is appropriate and trends or systemic issues are identified
* Develop and deliver training to relevant employees on incident management including root cause analysis
* Develop and deliver reports to oversight functions and the Statutory Board to provide insight on incidents
* Partner with process, assurance, change, and incident managers to drive focus on incident identification and implementation of controls to prevent recurrence of incidents
* Escalate and facilitate incident response as needed to ensure that service operations are restored as quickly as possible
* Collect incident response metrics and recommends process improvement measures to drive efficiencies and effectiveness in responding to issues
* Coordinate with technical and business teams during incident response
* Coordinate post incident resolution process and reporting

## Qualifications for incident analyst

* Knowledge of security applications or processes in of the following platforms SCADA and Industrial Control Embedded systems CEH, CISSP, Encase, scripting
* Processes, Train dispatching, and understanding of general code of operating rules preferred
* Must demonstrate a general understanding of information technology, networking concepts, cyber security incident and forensics analysis principles, theories, concepts and techniques
* Of the following certifications are preferred CISSP, GIAC Certifications - GCIA, GCIH
* Knowledge of malware behavior and techniques employed by attackers to evade existing security controls
* Experience in penetration testing, threat intelligence and detection of incidents/network monitoring - Knowledge of security applications or processes in of the following platforms SCADA and Industrial Control Embedded systems CEH, CISSP, Encase, scripting