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

# Example of Incident Handler Job Description

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

## Responsibilities for incident handler

* Analyze volatile system data.Collaborate with level one event handlers and to improve prevention and detection methods
* Lead Incident Handling efforts
* Processing security-related requests via the Remedy Request for Service application
* Be an in-house subject matter expert in the Computer Emergency Response Team (CERT), who diligently handles information security incidents by leading and coordinating investigations with internal and external stakeholders a forensics team
* Create security incident reports and dashboards upon the request of management
* Analyse System, Security and Application alerts raised to CERT to recognise and respond to abnormal activity, threats, and vulnerabilities
* Support the SIEM solution, by improving the visibility of security incidents by defining and optimizing use-cases
* Research emerging technologies to design, develop and implement automated tools to increase incident response efficiency
* Report key performance indicators to management for team activities
* Help to improve the CERT process excellence by maintaining information security documentation

## Qualifications for incident handler

* Knowledge of network protocols, enterprise architecture, and common network logging functions
* Hands on experience with security tools, such as, Encase, Splunk, network forensic and capture tools, CarbonBlack, Tanium
* Ability to prioritize assignments and efforts in a complex work environment
* Direct working knowledge of enterprise incident management systems
* Industry certifications such as CEH, CISA, Security + are desirable
* Experience work as part of a SOC or CSIRT team is desirable