



Example of Incident Response Analyst Job Description

Powered by www.VelvetJobs.com

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

Responsibilities for incident response analyst

- Support the planning, coordination, and execution of crisis management exercises and/or actual events
- Engage in functional integration discussion/coordination between technical and non-technical groups that may have involvement in Incident Response activities
- Develop and Update operational playbook DDOS, ransomware
- Triage and lead escalated Security events and incident
- Responsible for the technical execution of incident handling functions directly responding to severe network incidents
- Manage and integrate threat intelligence received from a variety of sources into the security monitoring framework
- Responsible for identification, analysis, and correlation of events of interest, escalation and continued monitoring of cybersecurity events on an enterprise-wide basis
- Understanding of common network services (TCP/IP web, mail, FTP, DNS), vulnerabilities, and attack patterns is a must
- Review, triage, escalate, and respond to security events and incidents while Managing global security incidents and provides support to global security teams
- Analyze various log, network, malware, forensic, and open source information to validate security threats, recommend appropriate countermeasures, and assess impact of incidents

-
- Bilingual speaking and writing skills (Japanese, Chinese, Spanish)
 - Degree in Computer Science, Engineering or equivalent with a minimum of 6 years working experience in Information Security
 - In-depth knowledge of network and host security technologies
 - Bachelor's degree (in field mathematics, telecommunications, electrical engineering, computer engineering, computer science) or equivalent five to seven year's experience with information security
 - Bachelor's degree in and 5 years of experience in incident response or IT risk management or an equivalent combination of education and work experience
 - In-depth knowledge in incident response concepts and practices and the ability to identify, apply, and implement best practices