Example of Incident Response Analyst Job Description

Powered by www.VelvetJobs.com

Our growing company is searching for experienced candidates for the position of 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

- Acts as Incident Commander for high impact cyber breaches and advanced attack methods through using the Cyber Kill Chain methodology the TMC playbook based on NIST methods and procedures
- Detailed analyses of various security event sources (FW, IDS, PROXY, AD) Acts as the interface with other IT and business departments regarding IT security incidents
- Follow documented workflows and procedures during information security incident response and remediation
- Stay abreast of the latest information security controls, practices, techniques and capabilities in the marketplace
- Monitor intrusion detection systems and create/monitor IDS signatures
- Provides project support related tasks to integrate security platforms ongoing tuning support for existing technology
- Apply technical acumen and analytical capabilities to improve efficiency and effectiveness of response
- Develop and enhance capabilities of digital and computer forensics
- Knowledge sharing of threat intelligence/ management during weekly meetings
- Interface with different departments to increase security awareness for the business

- Conduct root cause analysis to identify gaps and recommendations ultimately
- Experience with forensic analysis, using EnCase or FTK-Experience with performing static and dynamic analyses of suspect malware-Knowledge of Microsoft Windows, including registry, logs, and common forensic artifacts-Knowledge of TCP/IP and networking fundamentals, network architecture, and security infrastructure's best practices-Ability to document technical analyses and generate reports-Ability to obtain a security clearance-BS degree
- 1-2 years of hands on incident response
- 1-2 years of virtual threat tracking
- 1-2 years of exploit / hack tool research and/or development
- Incident and Forensic Security certifications