Example of Security Operations Center Job Description

Powered by www.VelvetJobs.com

Our company is growing rapidly and is looking for a security operations center. We appreciate you taking the time to review the list of qualifications and to apply for the position. If you don’t fill all of the qualifications, you may still be considered depending on your level of experience.

Responsibilities for security operations center

- Adhere to THR incident response workflow establishing impact and urgency of detected events and follow through the triage, escalation, remediation and documentation
- Updates incident response scenarios and procedures to adapt to changing organization/cultural/system configuration updates
- Executes established procedures as it relates to incident response
- Interpersonal skills to interact with team members, management, and CSOC stakeholders
- Ability to think outside of the box when the need arises
- Perform technical analysis of security alerts from all sources (automated tool alerts, employee reported alerts, fraud investigation related alerts)
- Provide ongoing security tool optimization using aggregation, filters, correlation rules
- Provide analysis and trending of security log data from a large number of heterogeneous security devices and develop processes that analyze data and produce accurate, meaningful, easily interpreted results based on user requirements and use cases
- Make recommendations to management appropriate to an organizations needs and requirements
- Provide first and second level troubleshooting support for security applications and appliances

- Must possess strong computer skills and demonstrate the ability to effectively operate and manage security tools and processes
- 4+ years of experience in management of a global SOC
- Demonstrated ability to manage geographically distributed SOC teams
- Experience within pharmaceutical or healthcare industries
- Able to gather all relevant incident information (e.g., affected systems, asset information, vulnerability information, system configurations, logs, console reviews, memory dumps, forensic analysis,) in accordance with incident management and response processes
- Has responded to current security incident types, such as DDOS attacks, anomalous activity, malware infections, APT activity, unauthorized access, data extraction