Example of Security Operations Engineer Job Description

Powered by www.VelvetJobs.com

Our company is growing rapidly and is hiring for a security operations engineer. 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 engineer

- May lead projects and provide guidance
- Provide technical assistance in the validation and evaluation of security alerts or incidents
- Engineer, implement, administer, and monitor security measures for the protection of computer systems, networks and information
- Work across team boundaries to share information and to collaborate when solving complex problems
- Monitor and analyze potential infrastructure security events to determine if it qualifies as a legitimate security incident / breach
- Monitor and review network, system, and security events to identify potential security incidents in IT infrastructure
- Triage events, attempt to remediate, and initiate escalation procedures to appropriately inform and advise management on incidents and incident prevention
- Document, communicate, and conform to processes related to security monitoring
- Be able to analyze malicious files through use of static and dynamic analysis and provide expertise in cyber forensics for identifying malicious viruses, worms, Trojans, and backdoors
- Identify security exposures

- Experience with Splunk, Linux, Apache web server, Snort, Tomcat, nginx, mysql and postgresql is a major advantage
- Experience with cloud technologies and platforms
- Advanced technical knowledge in technology methodologies, design, and implementation
- Information Security Certification highly desirable
- Bachelor’s degree and 3+ years of relevant career experience
- Proficiency in at least one scripting languages