Example of Security Operations Center Analyst Job Description

Our growing company is looking to fill the role of security operations center 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 security operations center analyst

- Operate SEIM (Trustwave) consoles in order to monitor the environment for events of interest
- Perform analysis of security logs in an attempt to detect unauthorized access
- Participate in the creation, modification and maintenance of all SOC policies and procedures
- Tier 1 security event monitoring and device oriented activities in the SOC with guidance of short-term projects such as upgrades, migrations and implementations on the part of the tier 3 and 4 staff
- Monitor IT defense perimeter and scanning infrastructure and communicate security events and incidents to applicable Computer Emergency Response Team personnel and/or management
- Perform reviews/audits of mixed UNIX and Microsoft Windows environments, including network devices, databases, web services, and enterprise applications
- Coordinate with infrastructure support teams to maintain/trouble shoot defense perimeter and monitoring integrity
- Working rotational shifts (1st, 2nd or 3rd)
- Monitoring telephones and operating radios and computer equipment in the security operations center
- Interacting routinely with employees, executives and contractors

- Good knowledge of Windows, Linux and Unix
- Knowledge of Intrusion Detection and Prevention techniques
- Knowledge of vulnerability scanners such as Nessus, Tenable
- Demonstrated experience with access control systems such as Active Directory and Virtual Private Network (VPN)
- Working knowledge of Tivoli, IBM End Point Manager
- Strong interpersonal and communication skills (verbal and written with both technical and non-technical staff)