Example of Security Operations Center Job Description

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

- Report and investigate potential security incidents
- Provide recommendations to clients for containment and eradication of threats
- Maintain Intrusion Detection/Prevention signatures
- Update security operations processes and procedures
- Assist in IT security investigations, exercises and tests
- Research, consultation with colleagues and training to maintain awareness of trends in new security threats, technologies and regulations
- Execute security monitoring through an intimate knowledge of SIEM technologies and the security threat landscape
- Establishing and executing a multi-year strategic plan to improve SOC services and operations
- Building and developing an effective and engaged global team
- Troubleshoot customer-facing issues and communicate with customers as needed

Qualifications for security operations center

- Experience performing security analysis utilizing Security Incident and Event Management (SIEM) technologies
- Demonstrated experience managing Tier 1-3SOC Teams, including

- Knowledge of security technologies (encryption, data protection, design, privilege access)
- Abide by and enhance runbooks and documentation associated with SOC actions
- A minimum of 2 years' experience as a security analyst within a SOC / NOC role or with an MSS provider