Example of Security Operations Center Analyst Job Description

Our growing company is looking to fill the role of security operations center analyst. Thank you in advance for taking a look at the list of responsibilities and qualifications. We look forward to reviewing your resume.

Responsibilities for security operations center analyst

- Provide guidance and support to all SOC personnel and ensure that each individual has a clear understanding of SOC policies and procedures their individual responsibilities
- Assist Analysts in monitoring network traffic and security alerts for potential events/incidents trending and historical analysis and complete ticket audits and reviews
- Mentor and guide personnel growth into roles which align with the needs of the SOC
- Provide support to security operational teams on escalated incidents including troubleshooting, analysis and resolution
- Stay informed of current events in the security industry including the latest exploits and threats preventative measures, remediation, and restoration techniques
- Provide continuous Security Threat Analysis for Antivirus, Malware, and Ransomware attacks across multiple platforms
- Research security threats in our customer environments
- Update rules and use cases to ensure proactive protection of our customer's IT environments
- Ensure quality service delivery and professional service management is provided to our customer
- Produce standard and custom reports to meet service level and operational level agreements

- Experience on a Computer Incident Response Team (CIRT)
- At lease one year of experience with security operations, computer network defense or intelligence analysis
- Passion for IT security
- General IT background (networking, OS, applications)
- 6 days at work (2 mornings, 2 afternoons, 2 nights)
- 4 days off afterwards