YUPRO PLACEMENT
PART OF YEAR UP UNITED

This is a skills-based job posting example for a Security Operations Center (SOC) Analyst. It puts skills and capabilities front and center and does not include any unnecessary obstacles that could discourage excellent candidates from applying. Moreover, it is presented in an inclusive and welcoming way to all potential candidates. You can use this as a template: Select "File" and "Make a copy" and then edit the document to meet your needs.

SKILLS-BASED JOB POSTING: SECURITY OPERATIONS CENTER (SOC) ANALYST

Job Title: Security Operations Center (SOC) Analyst

Company Overview: *(Describe what makes your company unique and the impact of its cybersecurity team.)*

Security Operations Center (SOC) Analyst Job Description: *(Please describe why the role is being filled and how it fits into the organization and the team.)*

We are seeking a **SOC Analyst** to join our security operations team, where you will play a frontline role in detecting, analyzing, and responding to cybersecurity threats. This position is ideal for individuals who thrive in high-stakes environments, enjoy problem-solving, and are passionate about protecting enterprise systems from cyber threats.

Security Operations Center (SOC) Analyst Job Responsibilities:

- Monitor security alerts and investigate potential cybersecurity incidents in real-time.
- Conduct threat analysis using SIEM tools and network monitoring technologies.
- Respond to security events, escalating incidents and executing remediation plans.

- Correlate threat intelligence with internal security data to proactively mitigate risks.
- Maintain and improve security documentation, including incident response reports and threat assessments.
- Continuously enhance security detection and response capabilities by researching emerging threats.

Preferred Skills:

- Hands-on experience with SIEM platforms (e.g., Splunk, IBM QRadar, Microsoft Sentinel).
- Knowledge of network security principles, firewall management, and intrusion detection systems (IDS/IPS).
- Understanding of common attack techniques (MITRE ATT&CK framework) and incident response methodologies.
- Proficiency in log analysis, malware analysis, and security forensics.
- Ability to communicate technical security findings to stakeholders effectively.
- Analytical skills with the ability to work under pressure in fast-paced environments.

Preferred Certifications *(Certifications are highly regarded but not mandatory. Candidates with equivalent experience or a strong willingness to obtain certifications are encouraged to apply.)***:**

- CompTIA Security+
- Certified SOC Analyst (CSA)
- GIAC Security Essentials Certification (GSEC)
- Certified Incident Handler (GCIH)

Valuing Transferable and Diverse Skillsets: We recognize that valuable skills can be developed through a variety of experiences. We encourage applicants with transferable skills from diverse backgrounds, including those transitioning from non-traditional careers, to apply.