Traditional job descriptions and specifications list the "typical" requirements for the role, including relevant work experience and the proper education.

However, they can be problematic. Not all great candidates have a relevant work history, and many lack the "expected" educational background, even when the relevant skills can be obtained through alternative paths. This means traditional job descriptions alone could be narrowing your talent pool.

A skills-based job description prioritizes and focuses on skills rather than asking for degrees and years of experience to help you access a broader audience and attract top talent. This is the aim of a skills-based job description.

This is a skills-based job posting example for a cybersecurity 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: Copy and paste the contents into an MS Word or Google Word file or edit it directly in Adobe Acrobat.

SKILLS-BASED JOB POSTING: CYBERSECURITY ANALYST

Job title: Cybersecurity analyst

Company overview: *(Describe what makes your company unique and what it would be like to work for your company)*

Cybersecurity analyst job description: *(Edit as required)*

Join our team as a Cyber Security Analyst where you will be at the forefront of protecting our organization's digital assets. In this vital role, you will identify, analyze, and manage system vulnerabilities to maintain the confidentiality, integrity, and availability of our information and systems.

Data Analyst job responsibilities: *(Edit as required)*

A brief overview of the key deliverables and day-to-day responsibilities of this role:

- Design and implement security protocols to protect network and information systems.
- Manage the application and maintenance of security measures to prevent unauthorized access and breaches.
- Actively seek out and mitigate security weaknesses to enhance system security.
- Handle and resolve incidents involving security breaches and malware effectively and efficiently.

Required skills: *(Edit as required)*

- Capability in safeguarding various operating systems, such as Windows, Linux, iOS, and Android, across different devices and environments.
- Proficiency in analyzing security logs, performing malware analysis, and engaging in proactive threat hunting.
- Experience with vulnerability assessments, including conducting scanning and penetration testing to address security vulnerabilities.
- Good understanding of network security concepts and experience in managing firewalls and orchestrating incident response.
- Familiarity with contemporary security tools and technologies like SIEM, IDS/IPS, IAM, antivirus, and IDPs.
- Analytical skills to conceptualize security solutions that balance organizational safety with business functionality.
- Commitment to continuous learning to keep abreast of the latest security threats and technological advancements.
- Flexibility to work independently on projects as well as collaborate within a team environment.

Preferred certifications *(Only add this if required - Select one or more and provide further detail. Delete the rest)*

- CompTIA Cybersecurity Analyst (CySA+)
- Global Information Assurance Certification (GIAC) Security Essentials
- CompTIA Security+
- ITIL Intermediate Level
- IBM Cybersecurity Analyst Professional Certificate

Commitment to Inclusivity

Our company is committed to diversity and inclusion. We welcome applicants from all backgrounds and experiences. We strive to create an environment that fosters growth and learning for all team members.