Here's a template for you to use in attracting qualified entry-level information security candidates. The template will give your hiring managers and HR leaders a great starting point when creating job postings.

Customize the information security job posting template to fit your company's specific needs.

1. Company Background - The template provides an opportunity for you to share your company's background with potential applicants. A well-written company background helps convey your organization's culture, allowing the candidate to determine if it is a good fit for their values.

2. Overview - Update the "overview" section to match the entry-level role in your business. You may add in the title for the position, the titles of those this role interacts with on a regular basis and a description of what daily duties are. You could include an example tool that will be utilized in this job, but listing too many technologies might eliminate a suitable applicant from the application process.

3. Salary - Depending on the geographic area of where your applicants live, it might be required by law to share a salary range. This is also an opportunity to give a competitive wage while enticing potential employees with other benefits your company offers. Even if it's not required by law to include the salary range, many applicants find it helpful in the decision-making process. Remember that entry-level salaries for cybersecurity positions tend to be higher than in other industries, so make sure you're paying a competitive wage.

4. Education - Consider the fact that you're creating an entry-level opportunity when writing the education and experience sections. A recent college graduate from a cybersecurity, IT, or engineering program might be educated for an entry-level position. It could also be a seasoned professional in another field who wishes to change careers to pursue a career in cybersecurity and has completed certifications or a boot camp or certificate program.

5. Experience - The experience section should, like the education section, reflect what is needed for an entry-level position. If you require 2-5 years of cybersecurity or IT experience, this is not an entry-level role! You might get more qualified applicants if you list several technologies used in the job and look for candidates who have gained exposure to three of them through classes, projects, and security competitions.

6. Preferred experience: In addition, you can add a "preferred experience" section to highlight the qualities of an outstanding applicant. Nevertheless, keep in mind that this is an entry-level job posting, so including certifications such as the CISSP which calls for five years of experience or a master’s degree does not correspond with an entry-level role.

© 2019 Heather Monthie, PhD
7. Responsibilities - In the responsibilities section, list the duties that are relevant to your definition of success for this position. Avoid making a lengthy list of activities that aren't necessary for the candidate to succeed on your team.

8. What you will learn in this position - This section is designed to inform the candidate about the resources and opportunities your organization offers to help entry-level employees grow in their cybersecurity careers. It should include what the candidate can expect to learn from this role, which will aid them in determining if the position represents a good fit for their future goals.
Cloud Security Analyst Job Posting - TEMPLATE

Overview
Cloud Security Analysts work with Cloud Architects and DevOps teams to ensure the security of cloud-based systems and data. They are responsible for identifying risks, implementing security controls, and monitoring for compliance with security policies.

Example Titles
Cloud Security Analyst I, Security Analyst, Cybersecurity Analyst - Cloud, Cloud Security Engineer

Salary
The average salary is approximately $87,000 annually

Education
Current student or recent graduate,

Experience
Minimum
1 year of experience through course projects, classes, training, or internships in at least three of the following:
- AWS, GCP, Azure
- Producing technical documentation
- Conducting vulnerability scans and recognizing vulnerabilities in systems
- Security Information and Event Management tools (SIEM) tools
- MITRE ATT&CK Framework
- Lockheed Martin Cyber Kill-Chain
- Conducting Privacy Impact Assessments (PIA)
- Knowledge of database systems
- Knowledge of resiliency and redundancy
- Knowledge of Windows or Linux operating systems
- Knowledge of secure configuration management techniques
- Agile project management tools, such as Jira
- [Add or delete tools here as necessary for the position]

Preferred
Experience in one or more of the following:
- Prior experience in a security internship
- Experience in security competitions, CTFs

Responsibilities
- Conduct risk assessments of cloud-based systems and recommend security controls to mitigate risks

© 2019 Heather Monthie, PhD
● Implement security controls in cloud-based systems
● Monitor compliance with security policies
● Respond to incidents involving data breaches or unauthorized access to systems

What you will learn in this position
The Cloud Security Analyst position offers the opportunity to learn about:
● cloud security architecture and controls
● how to implement security in a variety of cloud-based systems.
● incident response procedures in the event of a data breach or unauthorized access to systems.
● make recommendations to improve existing processes and procedures