OFFENSIVE security

Entry-Level Cybersecurity Job Description Template: How to Write a Great One (and Get More Qualified Applicants)

Author: Heather Monthie, PhD

BRIEF

One of the most critical aspects of recruiting and hiring entry-level cybersecurity employees is creating a job description that attracts qualified applicants. A job description that does not provide adequate information about the entry-level role or has education and experience requirements that do not align with an entry-level position are often barriers to finding qualified entry-level candidates. The global cybersecurity workforce shortage has made it challenging to find suitable candidates for the right roles; therefore, creating an accurate job posting is an essential first step in attracting well-qualified entry-level candidates.

For more information contact **sales@offensive-security.com**

UNDERSTANDING THE CYBERSECURITY SKILLS GAP

Cybersecurity is a top concern for technology and business leaders today. With so many data breaches and cyberattacks happening every day, it's evident that cybersecurity is a significant issue and continues to be a top concern. Due to the increase of connected devices, the amount of data stored on devices, and the ubiquitous nature of mobile and IoT devices, the demand for top cybersecurity talent continues to increase. Experienced cybersecurity professionals are in high demand but are also hard to recruit. Many are happily employed, and many require top salaries to remain competitive. This is a burgeoning industry where every employer wants an experienced professional but there is not a long history of employers hiring in this profession resulting in a shortage of mid to senior-level candidates. To be more competitive in hiring cybersecurity talent, employers can build an internal cybersecurity talent pipeline in their organizations, starting with attracting and recruiting top entry-level cybersecurity candidates.

Experienced cybersecurity professionals are in high demand but are also hard to recruit.

Entry-level candidates frequently find it difficult to land their first position since there are a plethora of entry-level job postings that require the skills and qualifications of a mid to senior-level person. When scanning job sites, it is not difficult to find entry-level cybersecurity job postings that require a long list of experience in many different technologies, certifications that require five years of experience, or even ten years of experience in a technology that's been around for only five. Inadequate job postings result in qualified candidates self-selecting out of the application process, and those who do apply may not have the skills required to do the job. This mismatch is one contributor to the skills gap in the cybersecurity industry. When job postings do not include the correct information for an applicant to determine their fit for the position, the employer will lose top applicants who self-select out of the recruiting process before they even apply.[1]

[1]Schmidt, J. A., Chapman, D. S., & Jones, D. A. (2015). Does emphasizing different types of person–environment fit in online job ads influence application behavior and applicant quality? Evidence from a field experiment. Journal of Business and Psychology, 30(2), 267-282.

WHAT DOES THE CYBERSECURITY SKILLS GAP LOOK LIKE?

There's no shortage of studies available that describe the numbers behind the cybersecurity skills gap. The purpose of this paper is not to conduct a cybersecurity workforce analysis. Instead, it describes the current state of the workforce and offers one potential solution to increase the number of qualified candidates entering the cybersecurity profession: writing effective entry-level job descriptions to attract qualified applicants.

The cybersecurity workforce shortage can be succinctly defined as "...not enough people with the skills required to meet the cybersecurity needs of organizations".[2] Other industries have widely-publicized workforce shortages, such as airline pilots and nurses. So how does the cybersecurity workforce shortage compare?

As of January 2022, Cyberseek.org reports about 600,000 open cybersecurity positions in the United States alone.[3] ISC2 reports an estimated 3 million cybersecurity positions open worldwide.[4] By comparison, the widely publicized nursing shortage in the United States is expected to be roughly 194,500 average openings each year until 2030.[5] [6] In the airline industry, there is expected to be a shortage of approximately 15,000 regional pilots in the US by 2026.[7] By comparison, the numbers show the enormity of the demand for qualified cybersecurity professionals at all levels.

[2]Cobb, S. (2016). Mind this gap: Criminal hacking and the global cybersecurity skills shortage, a critical analysis. In Virus Bulletin Conference (pp. 1-8).
[3]https://www.cyberseek.org/heatmap.html
[4]https://www.isc2.org//-/media/ISC2/Research/2021/ISC2-Cybersecurity-Workforce-Study-2021.ashx
[5]https://www.bls.gov/ooh/healthcare/registered-nurses.htm
[6]https://nursing.jnj.com/
[7]Klapper, E. S., & Ruff-Stahl, H. J. K. (2019). Effects of the pilot shortage on the regional airline industry: A 2023 Forecast. International Journal of Aviation, Aeronautics, and Aerospace, 6(3), 2.

WHY THE INCREASED DEMAND?

There are many reasons why the demand for cybersecurity professionals continues to rise. As technology continues to become even more ubiquitous, there is exponential growth in the amount of data that are stored on devices and transmitted over the internet. Apps collect personal information, organizations collect valuable data about their customer's behaviors, and most of this data are stored on devices that are connected to the internet. As attackers have realized the value of this data, there is a global rise in the number and frequency of attacks. The risk of cyber-attacks increases sharply as the amount of data an organization is trying to secure increases.

Software used for web applications, mobile devices, and embedded systems may not have been developed with secure software development principles in mind. Historically, secure software development was not part of the development process, and security was (and often still is) an after-thought.

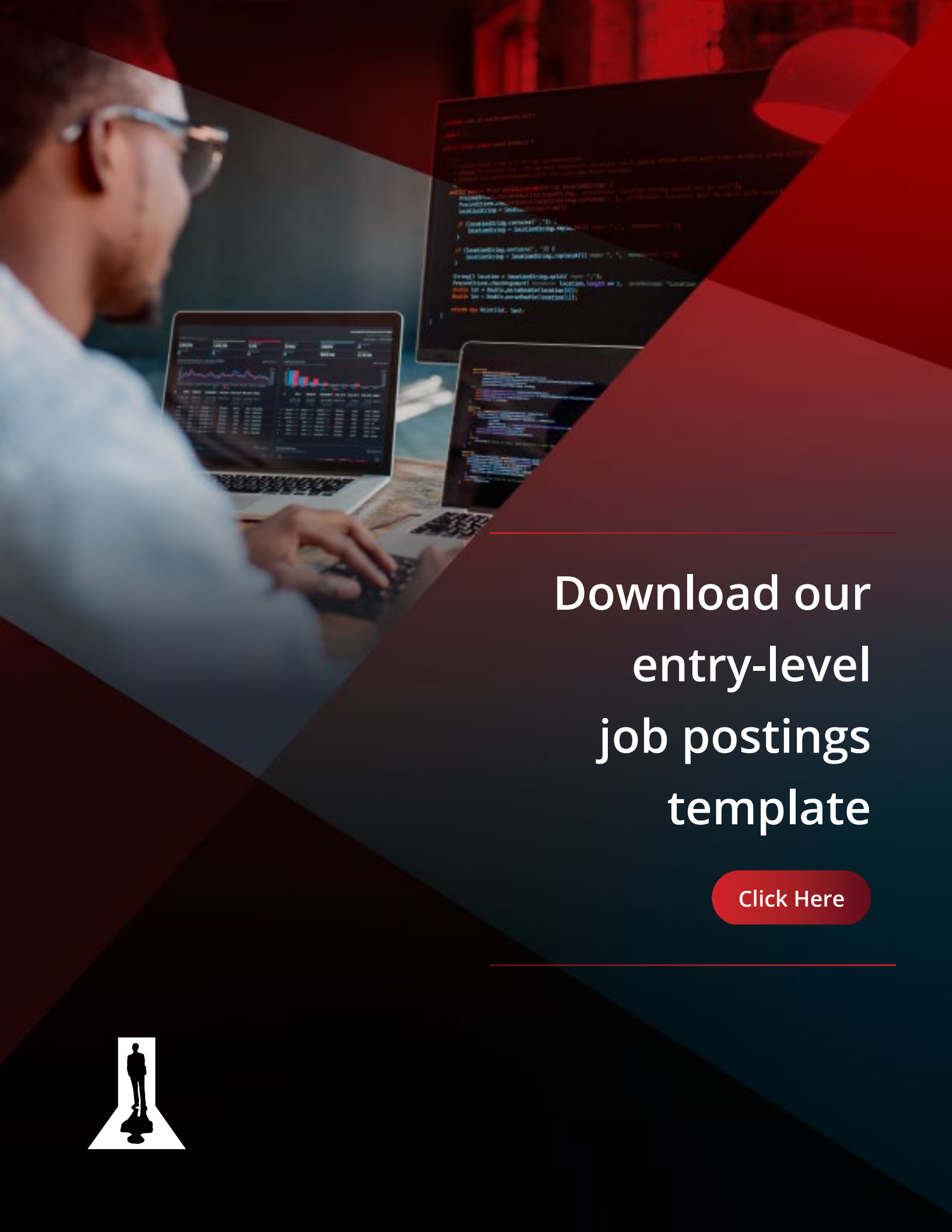
The ability to detect cyber threats either through security awareness for all employees, training for the cybersecurity team, or technology such as intrusion detection systems has made cyber defenders much more aware of cyber attacks happening every day. The increased visibility of cyber attacks has contributed to the increase in demand for top cybersecurity talent.[8]

There is a global rise in the number and frequency of attacks.

SOLUTION

The goal for this paper is to outline a specific resource for cybersecurity hiring managers and human resources managers on how to write clear, concise, and effective entry-level cybersecurity job postings to attract the most-qualified talent as one potential solution for filling open cybersecurity roles. This paper is intended as a tool to support the process of developing a pipeline of cybersecurity talent in your organization as an effective long-term strategy for decreasing the cybersecurity skills gap as well as keeping employees motivated, happy, and satisfied in their work.

[8]Libicki, Martin C., David Senty, and Julia Pollak, Hackers Wanted: An Examination of the Cybersecurity Labor Market. Santa Monica, CA: RAND Corporation, 2014. https://www.rand.org/pubs/research_reports/RR430.html. Also available in print form.



Download our entry-level job postings template

Click Here

WRITING EFFECTIVE ENTRY-LEVEL CYBERSECURITY JOB POSTINGS

Poorly-written job postings can be a major obstacle to receiving resumes from qualified candidates. Candidates will often self-select out of the application process when an inaccurate portrayal of skills and experience is required, such as requiring mid to senior level education and experience for an entry-level role. It is often reported that women will only apply to job postings when they meet 100 percent of the requirements, while men will apply if they meet 60 percent of the requirements. If a woman does not meet 100 percent of the requirements in the job posting, it is highly likely she will self-select out of the application process.[9] Writing an effective job posting can increase the gender diversity of your applicant pool.

Candidates want to know that your organization can provide them what's needed to be successful in the entry-level role as well as how that might help their own careers grow in a meaningful way. Entry-level candidates want to know that they will have a chance at growth and success within your company.

The business goal for posting an open position is to identify qualified applicants to interview for the role. Cybersecurity and Human Resources managers should work alongside each other to craft a job posting that results in receiving resumes from cybersecurity talent that closely meets the realistic needs for the role. Applicants' needs should also be considered when writing the job posting.

An applicant's goal for their resume is to secure them a job interview.

A hiring manager's goal for a job posting is to secure interviews with qualified candidates.

[9] Desvaux, G., Devillard-Hoellinger, S., & Meaney, M. C. (2008). A business case for women. The McKinsey Quarterly, 4(4), 26-33.

1 Write job postings in a way that applicants can imagine themselves in that position.

To identify more qualified applicants for entry-level cybersecurity roles, hiring managers should write job postings in a way that applicants can imagine themselves working in that position.[10] When job postings are written in a way that focuses on the needs of the candidate versus what the organization needs from the candidate, an organization can receive up to three times as many qualified applicants. [11] [12]

2 Entry-level job postings should address the resources and opportunities your organization has to offer candidates.

Statements in job postings that address the resources that your organization has to offer to meet the needs, desires, and preferences of the candidate have shown to be effective in successful recruiting. These statements identify the aspects of a position that provide an employee a sense of meaning and satisfaction, which is critical in employee motivation, well-being, and happiness.[13] [14]

A study conducted by the University of Saskatchewan, University of Calgary, and the University of Vermont provides some example statements that focus on applicants' needs. These statements should be customized for your organization and the specific role for which you are recruiting. These examples provide your organization a place to start as hiring managers develop entry-level cybersecurity job postings.

Example Statements:

"You will have the opportunity to work on a variety of tasks and develop your skills in many areas."

"The job will provide you with autonomy as you will be required to complete tasks with minimal supervision."

"Employees are given many opportunities for advancements within the organization."

"This position is on an important project, so the successful applicant will have the opportunity to make a valuable contribution to the organization and see the project through to its completion."

"We seek to provide employees with constructive feedback to foster their career growth."

"You will have many opportunities to collaborate with talented people."[15]

[10] Smith,E.Writing Cybersecurity position descriptions for greatest impact. https://www.nist.gov/video/nice-webinar-writing-cybersecurity-position-descriptions-greatest-impact
[11] Stephan, M. & Erickson, R. (2017). Deloitte 2017 Global Human Capital Trends. https://www2.deloitte.com/us/en/insights/focus/human-capital-trends/2017/predictive-hiring-talent-acquisition.html?icid=interactive:spin:hct17:feb17
[12] Schmidt, J. A., Chapman, D. S., & Jones, D. A. (2015). Does emphasizing different types of person–environment fit in online job ads influence application behavior and applicant quality? Evidence from a field experiment. Journal of Business and Psychology, 30(2), 267-282.
[13] Schmidt, J. A., Chapman, D. S., & Jones, D. A. (2015). Does emphasizing different types of person–environment fit in online job ads influence application behavior and applicant quality? Evidence from a field experiment. Journal of Business and Psychology, 30(2), 267-282.
[14] Deci, E. L., & Ryan, R. M. (2000). The" what" and" why" of goal pursuits: Human needs and the self-determination of behavior. Psychological inquiry, 11(4), 227-268.
[15]Schmidt, J. A., Chapman, D. S., & Jones, D. A. (2015). Does emphasizing different types of person–environment fit in online job ads influence application behavior and applicant quality? Evidence from a field experiment. Journal of Business and Psychology, 30(2), 267-282.

3 Keep it Short, Sweet, Brief, and Informative.

Keep entry-level cybersecurity job postings short and sweet rather than overwhelming with technical details with which candidates probably have not yet had any experiences. While it is essential to convey all functions of entry-level opportunities within your company, it is best to focus on the entry-level skill set necessary for success in the role. Asking for experience and education that does not align with entry-level talent will likely drive away qualified candidates, leading to less qualified candidates applying for entry-level positions.

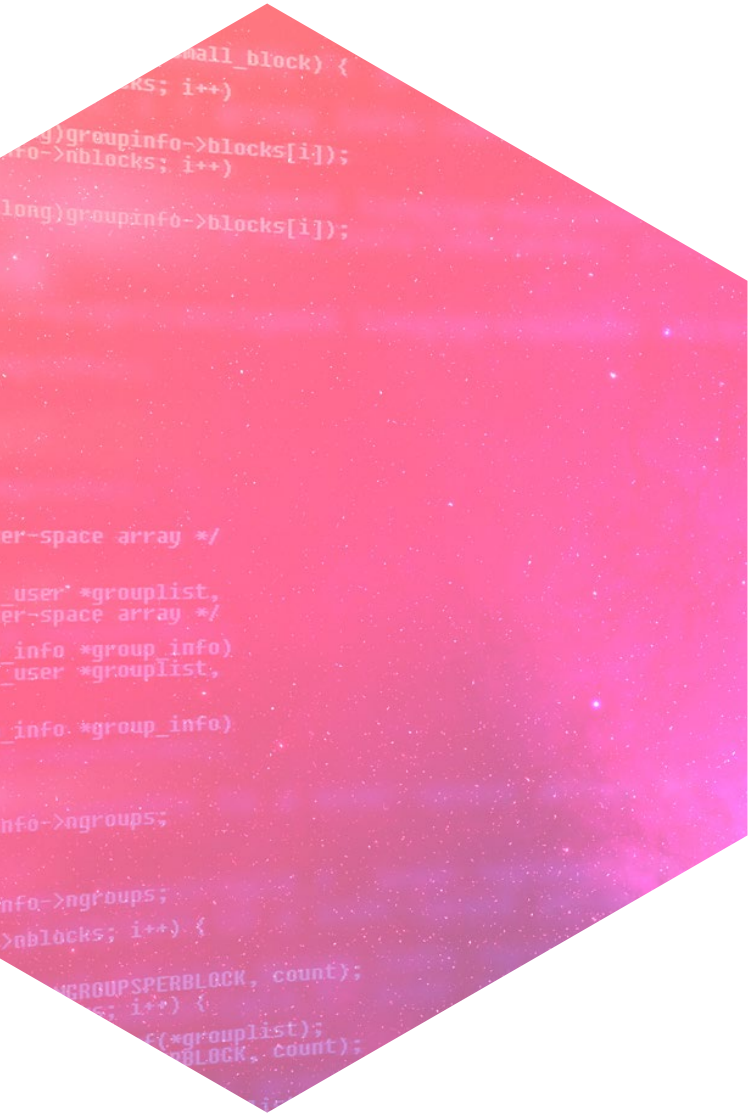
The job posting should be clear and concise, yet should include all pertinent information about the entry-level cybersecurity position. Try to be as specific as possible with entry-level candidate requirements, yet not turn away any applicants by making it too high level. Some examples of areas to include would be: technical skills, project responsibility, and working with others. Always make sure to leave room for flexibility in duties and responsibilities based on each entry-level employee's skill set and abilities. These tips will help ensure that you create a detailed entry-level job description that will attract qualified candidates with interest in a particular entry-level cybersecurity position.

4 Be realistic about the expectations of an entry-level role

Entry-level position descriptions should be a realistic representation of both the entry-level candidate and the entry-level employee role. Be realistic about what you are looking for in an entry-level employee. Adding a long list of required experience in 20 different technologies will likely result in candidates overlooking your position. Academic programs cannot possibly teach to every single piece of technology that is out there. Rather than requiring experience with a specific vendor's product, asking for some experience with any SIEM, IDS, IPS or other technology will attract more candidates. Academic programs generally teach one specific tool along with the mindset needed that can be transferred to another vendor's product. Experience with your organization's specific vendor can be learned on the job. Entry-level candidates are hoping to gain this valuable experience by working within your organization.

5 Job postings should be dynamic and evolving

The job posting should be adapted over time to continue attracting entry-level talent, even after sharing the initial job posting. As the modern workforce moves into a new way of working, remote work opportunities greatly benefit attracting qualified cybersecurity talent. Candidates who are still in an undergraduate program or training program have the opportunity to expand their skillset with your organization, regardless of where they currently live.



6 Ensure you are using the best practices when writing an entry-level cybersecurity job description

Offensive Security has developed two different templates for you to use to attract qualified entry-level candidates: Junior Penetration Tester and Junior SOC Analyst. These templates provide example statements that you can use in your own job postings. There are some areas on the templates where you can customize for your own organization.

HOW TO CUSTOMIZE THE ENTRY-LEVEL CYBERSECURITY JOB POSTING TEMPLATES

1. Determine which template is suitable for your open position. You can use the "Junior Penetration Tester" template on the Offensive side. You can use the "Junior SOC Analyst" template on the defensive side. You can change the titles to fit within your organization chart. Each template provides example titles, such as "Tier 1 SOC Analyst."

2. Organization Background - Add your organization's background to the template. This section is an opportunity for you to share more about your company as a whole 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.

3. Overview - Customize the "overview" section so that it is aligned with the entry-level role within your organization. You can add in the title for the position, the titles of those this role frequently interacts with, and a description of what the day-to-day activities are for the position. You may want to include example tools that will be used in the role, keeping in mind that listing too many technologies may cause a qualified candidate to select-out of the application process. An example overview is provided in the template. You are free to use as much of this example as you would like.

4. Salary - Depending on your organization's policies, salary information can be included in the job posting. Depending on the geographic area of where your applicants live, it might be required by law. Make sure you research to ensure that you're offering a competitive entry-level cybersecurity salary, as entry-level pay in cybersecurity is oftentimes higher than other industries.

5. Education - Remember that you're posting an entry-level job, so consider this when writing the education and experience sections. Education for an entry-level position might be a recent college graduate from a cybersecurity, IT, or engineering program. It could also be an experienced professional in another field who is interested in transitioning to a career in cybersecurity and has completed certifications or a boot camp or certificate program.

6. Experience - As with the education section, the experience section should reflect the requirements of an entry-level position. Requiring 2-5 years of cybersecurity or IT experience here is not an entry-level position! You may receive more qualified applicants if you list a few different technologies used in the role and ask for candidates to have experience in three of them through classes, projects, and security competitions. Candidates who have degrees and experiences in other disciplines often have highly-valuable transferable skills. Entry-level candidates have a work-harder mindset knowing that they have a lot to learn and are keen to prove their capabilities. Keep these candidates in mind as you write this section.

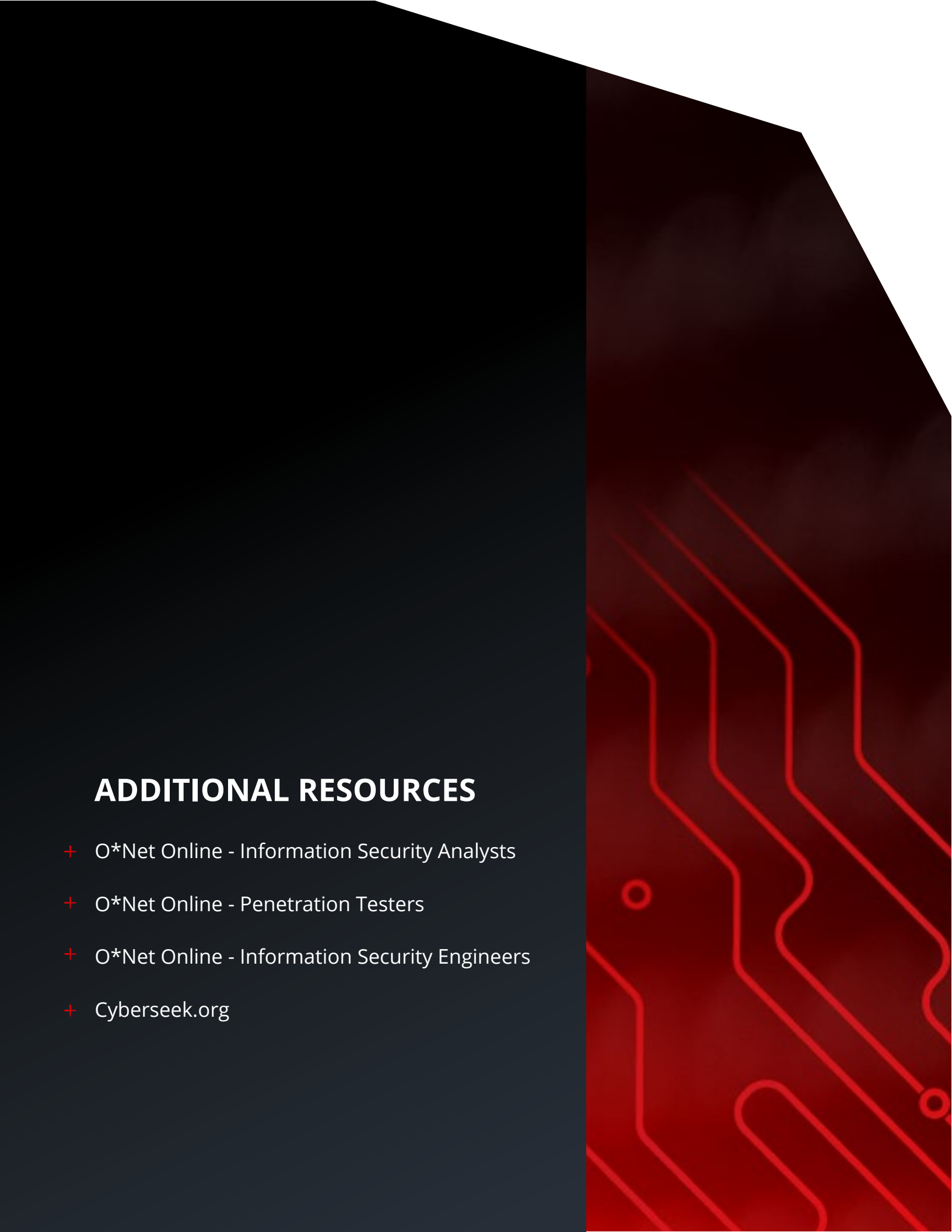
You can add a "preferred experience" section as well to highlight the characteristics of a highly qualified applicant. Remember, this is an entry-level position, so adding certifications here, such as the CISSP which requires five years of experience or a master's degree does not align with an entry-level role.

7. Responsibilities - In the responsibilities section, include the responsibilities of the role that align to your definition of success for the role. Try to avoid this becoming a long list of responsibilities that are not necessarily required for the candidate to become a successful employee on your team. Remember that a job posting is an advertisement and not an internal job description. By focusing on what means success in the role you will increase your chances of attracting candidates who seek to be successful. Use the example statements listed on page 6 as a template for some of the statements in this section.

8. What you will learn in this position - In this section, you can highlight the resources and offerings your organization has in place to help the entry-level employee grow as a cybersecurity professional. This section should also highlight what the candidate can expect to learn in this role. This helps candidates determine if the position is aligned to their future goals. Use the example statements listed on page 6 as a template for some of the statements in this section.

CONCLUSION

The cybersecurity workforce shortage continues to be a top concern for business leaders and is also a matter of national security. We've outlined some tips and provided templates that you can use to write an effective job posting that will attract qualified entry-level candidates. By highlighting responsibilities and what the candidate can expect to learn, you can create a job post that is attractive to entry-level cybersecurity candidates. Sharing with candidates that your organization is willing to offer on-the-job training or provide certifications to new hires is attractive to candidates, as this shows that you are invested in their success.



ADDITIONAL RESOURCES

- O*Net Online - Information Security Analysts
- O*Net Online - Penetration Testers
- O*Net Online - Information Security Engineers
- Cyberseek.org

ABOUT OFFENSIVE SECURITY

Offensive Security is the world's leading provider of hands-on cybersecurity training and certifications for the cybersecurity professionals. Created by the community for the community, Offensive Security's one-of-a-kind mix of practical, hands-on training and certification programs, virtual labs and open source projects provide practitioners with the highly-desired offensive and defensive skills required to advance their careers and better protect their organizations. Offensive Security is committed to funding and growing Kali Linux, the leading operating system for penetration testing, ethical hacking and network security assessments.

For more information, visit
www.offensive-security.com
and follow @offsectraining and @kalilinux