eSENTIRE

Filling Positions Despite the Cybersecurity Skills Shortage

Five things cybersecurity professionals wish recruiters and companies knew.

Eighty-seven percent of organizations feel their cybersecurity staffing levels are adequate, while 78 percent also feel they have a skills gap, according to a 451 Research study commissioned by eSentire in June 2019. This indicates that companies have the people, but they do not think these people possess the necessary expertise.

ISACA's 2019 State of Cybersecurity survey shows that 32 percent of organizations say it takes more than six months to fill cybersecurity positions. Further, 29 percent say fewer than one-quarter of job candidates are qualified for the cybersecurity position for which they applied. Organizations are definitely having a hard time finding qualified candidates to fill open cybersecurity roles.

In July 2019, eSentire surveyed 300 cybersecurity professionals to get their take on the skills shortage, what organizations can do to alleviate it and what motivates them in their career. Topics range from job security and satisfaction to career growth and issues with the recruiting process. The complete white paper with the results of that survey can be found here. The perception of the recruiting process these professionals have is a key takeaway from this research. It is not good.

Cybersecurity is a complex animal and organizations looking to fill a particular role with a specific skill set are facing challenges beyond the lack of candidates. Anecdotal information collected during the research phase of the white paper suggests that some of the skills gap problem may be compounded by issues in the recruiting process. The cybersecurity professionals surveyed have five pieces of advice they would offer to cybersecurity recruiters.

1 Understand that skill sets can vary widely within the same security job title.

While the basic purpose of the job may be universal, all security analysts, for example, are not created equal. The specific skills and certifications organizations want may vary within a job title. If the individuals doing the recruiting are pulling all "security analyst" resumes when the company is specifically looking for a security analyst with Security+ or CISSP certifications, that would explain why organizations feel only one-quarter of the candidates they source are qualified.

2 Spamming candidates through LinkedIn does not work.

Cybersecurity professionals are not likely to respond to recruiter inquiries, making it even more difficult to fill open positions. Forty-six percent of survey respondents report being approached by recruiters between one and three times per month, while 34 percent say they rarely respond to recruiter inquiries. A total of 17 percent never respond to recruiters at all.

3 Understand the job requirements.

In one anecdote on a Reddit thread, a cybersecurity professional shared a story about having a recruiter ask if they had any SIEM experience. When the candidate replied that they had experience with Splunk, the recruiter repeated, “Yes, but do you have any SIEM experience?”

The individuals doing the recruiting often lack cybersecurity knowledge, which contributes to the inability to find candidates with the right skill set. Employers need to make sure the job description matches the skills required, and recruiters need to understand the abilities that match the role.

4 Matching cybersecurity skills requires a conversation with potential candidates.

Weeding through resumes collected from job boards is a great start, but without a deep understanding of cybersecurity, it is difficult to understand how the candidate’s skill set matches (or doesn’t match) the job requirements. Cybersecurity professionals agree that having a conversation with a candidate is the best way to clarify their expertise and how it may match up to the requirements of the position without missing out on a good match due to the next item on the list.

5 Relying on keyword searches will result in overlooking good candidates.

Just like the anecdotal story above, recruiters who rely on keyword searches to pull resumes of potential candidates will miss qualified candidates. They may search for “SIEM” and miss a potentially great candidate whose resume lists “Splunk.”

Final Thoughts

The five categories listed share a common theme. Cybersecurity skill sets are complex, and successful recruiting when there is a known skills shortage requires a deep understanding of the complexities of cybersecurity qualifications. Much like the different roles in cybersecurity require certain certifications, organizations would be wise to ensure that recruiters they use are well-versed in the nuances of the field.

The ever-changing cybersecurity landscape means that the demand for highly skilled cybersecurity professionals will not wane in the foreseeable future. The shortage will always be there, but it is manageable. With improved recruiting practices organizations may be able to cut down that six-month timeframe to fill roles.

However, cybercriminals are knocking on your doors every day. So, while your organization is working to staff up, hiring a security provider like eSentire to fill the gap is an excellent idea. We can quickly provide you with the tools you need, while also supplying the highly skilled individuals you currently lack. Our services are designed to remove the staffing burden with human expertise at machine scale, accelerating response times and minimizing threat actor dwell time and the risk of business disruption.

eSENTIRE

eSentire, Inc., the global leader in Managed Detection and Response (MDR), keeps organizations safe from constantly evolving cyberattacks that technology alone cannot prevent. Its 24x7 Security Operations Center (SOC), staffed by elite security analysts, hunts, investigates and responds in real-time to known and unknown threats before they become business disrupting events. Protecting more than $5.7 trillion AUM in the financial sector alone, eSentire absorbs the complexity of cybersecurity, delivering enterprise-grade protection and the ability to comply with growing regulatory requirements. For more information, visit www.esentire.com and follow @eSentire.