ASM Educational Center (ASM)

How to Fix the CyberSecurity Skills Gap

Despite the availability of a large amount of certification courses and certification standards, we continue to see organizations unprepared to deal with the increasing threat to cyber security. This is true even for large corporations with the resources to train their teams. When it comes to the small and mid-size businesses then the problem is even more exasperated.

The problem with the certification mindset is the fact that these certifications cannot provide the skills required for someone to perform in their job; furthermore, most of the certifications are based on rote memorizations and as such there is no way this can prepare an individual for the requirements that come with being in an IT security position. This is evident where the estimates are that 90% of the attacks that continue to dominate the news could be prevented with the most basics of security controls. This is another reason why despite an increasing number, the certification courses while important have not solved the problem. To solve this problem the training needs to be customized to meet the job skill requirements for that particular job. This can only be accomplished with customized training, and this training needs to be recurring. It can and has been done. The reality is certifications are helpful, but the skill specific training needs to be conducted to build the expert cyber warrior team.

The way forward is to identify the skills required, and this can use the NIST NICE format as a start, and then build a curriculum that meets the strategic needs for the organization to not only build talent, but also maintain currency in the skills set.

An example that has been used to build teams for a Security Operations Center (SoC) is as follows:

1. Identify the required skills needed for the organization
2. Interview the staff and conduct a skills analysis
3. Develop a skills gap chart
4. Design a custom curriculum to meet the requirements to fill the gaps
5. Conduct recurring training to maintain the skill proficiency
6. Gather feedback and enhance and improve the curriculum as required

This strategic model draws attention to two different levels at which the strategy needs to work:

• ***Foundation knowledge and core security skills*** – This is important as the facts, the knowledge and information about procedures and processes is very critical to the ability to continuous growth and learning.

• ***Process Centric Training*** - What individuals need to be able to do to implement the process and methodology is to follow a systematic method that emulates the threat mind set. It includes technical skills and tactical skills in identifying vectors of attacks and hence having the capability to secure against those threats regardless of the technology used.

By adopting this approach, an organization can not only provide the skills required to their personnel, but also maintain those skills with the recurring strategy.

Need more information? Please contact Azita at azitam@asmed.com .