Security Padawans?

By Keith Posner

A few years back someone proposed moving a few security-related accountabilities to my team. My comment was along the lines…
'my staff were not hired for that. They will need training, or I need new hires'

The response… *'don't worry, you can hire, that won't be difficult'*

My inner monologue… *'Huh?'* (think Scobby Doo)

My response…something like *'if I had access to unlimited resources, absolutely'*

By unlimited resources I had meant both the monetary kind along with the available talent pool. From my experience and I presume for most us, resources are finite. Budget constraints and well-defined salary ranges are most of our realities. Now add in other factors that could make the hunt for skilled individuals more challenging. Have you ever wondered…

- How is your organization viewed by the broader security community?
- Is what you are doing cutting edge or thought of as interesting?
- How have others spoken about past experiences at your organization?

The answers to these questions can impact our ability to attract qualified candidates. If we were able to consistently exceed candidate salary expectations by thirty percent, I am sure the focus of our discussions might change.

Before we proceed, I will stop and share one of my primary assumptions, and that is as readers, you have an interest in technical skills and capability. I am talking about candidates with a genuine interest in security. Those who, keep current with changes in technology and take the time to understand security implications, monitor developments in the broader security landscape, conduct their own research and maintain technical currency through hands-on work, can offer experience supported guidance and solutions based on what they know to be possible. To offer value in security, I am going to suggest that you need to understand the subject from both a theoretical and practical perspective. Hands on experience in invaluable.

On the opposite end of the spectrum, you might have a need for individuals who can manage the complicated world of checklists or those who are experts negotiation or business-speak. If this is your focus the remainder of this document may not be all that interesting or informative. Let me be clear, I am a supporter of relationship building, business knowledge, and other non-technical skills; but not at the expense of technical skills and capability. A colleague recently provided me with an example for comparative purposes. I will preface it by acknowledging that most of us are not savings lives day to day.

A surgeon has a certain technical skillset. They perform surgery using hands on experience refined over years. They keep up to date with new techniques and approaches. These skills are maintained and for good reason. Now if my surgeon had unparalleled bed-side manner and could walk me through a five-page checklist, but had a 70% mortality rate for tonsil surgery, I might raise an eyebrow and seek a new surgeon.

Technical skills are crucial for information security professionals just like doctors (or civil engineers, pilots, plumbers). The non-technical skills sit atop the technical and are used to communicate issues, concerns, approaches, plans etc. It is my belief that at a certain point in our lives, primary interests are well established and our willingness to step outside of our comfort zone decreases. What this means is that a typical candidate is far more likely to learn and/or fine-tune non-technical skills as opposed to becoming technical. For that reason, I am going to suggest two things…
1. It is unlikely that you will find a candidate who excels at every aspect of a role (the prized unicorn)
2. Knowing that, prioritize technical

With that… the question remains….what next?

Your objective
What is it you are looking for? Do you need someone to hit the ground running? Someone who can come in and short of knowing process and people, understands the world of security in all its glory? Or do you have time to allow on-the-job training? A well-defined ramp up? Someone who can shadow more senior members of your team? Or still, are you looking to develop a talent pipeline (think farm team) where the focus is fundamentals, hoping to one day have a team of highly skilled staff to draw from.? Each is valid, each has its own pros and cons.

And onto assumption #2. You are looking for the first example above. Someone who knows the world of information security, having technical hands on experience and the ability to hit the ground running with minimal effort.

Laying the groundwork
Speak with HR. If possible reach out to external recruiters to get a sense of what the local market is paying for comparable experience and skillsets. If there are online resources you can also reference (e.g., payscale.com) it can only help support general conclusions. The goal is to identify potential issues and determine if you have any means to deal with them. During a round of hiring I was doing in 2017, I had somehow missed the mark on salary by almost 25% in the market I was looking at. I only discovered this useful bit of knowledge when a recruiter seemed to be laughing at me through email. This is ultimately about managing your own expectations. Your future may involve your head meeting a wall in frustration. Knowing you are off the mark and knowing you can't doing anything about it may allow you to change your approach. Can you work with someone less senior?

Acknowledge that people are by far your most important asset. People are the foundation on which process and tools must be built. Without skilled people, process and tools with fail. Tools cannot solve process issues. Processes cannot solve issues with staff capability and skill. When a process fails, or a tool fails to live up to expectations, then some questions should come to mind. Did you have the right people? Did they understand the technology? Were they capable? I would be surprised if the answer is yes.

Next, focus on organizational values. I don't mean corporate values, I mean what behaviors are rewarded, and what skillsets are perceived as relevant by management.

- Is there genuine interest in core enterprise security capabilities and maturity?
- Does your organization value technical competency?
- How is it rewarded?
- Are there proven examples of employees advancing into senior roles as technically focused individual contributors?
- Does your organization value certifications and memberships?
- Do your information security staff have access to tools and environments to keep their skills current
- Is transparency into gaps and obstacles encouraged and rewarded?
- Does your organization value collaboration and providing opportunities to explore areas of interest in the information security field?

Answers to questions such as these will help shape your approach in attracting and retaining a team of skilled information security professionals.

On your way…
Job description… avoid buzzwords and jargon. Be clear, concise and honest. There is nothing worse than someone joining your organization and realizing that it is not the job they applied for. There will always be some aspects of the job not clearly called out on in the job description, but the candidate should never wonder if they have gone crazy and taken a job without understanding it. The phrases, 'I think they lied to me in the interview' and 'I am really glad I took this job' are likely not going to go hand in hand.

Candidate screening…If you have an opportunity to use up front screening questions great. Make them specific and if possible, limit candidate research and response times. I have had success with initial phone screening conducted by members of my team or external recruiters (with a technical skillset). It is critical that whomever is screening candidates understands the material and can take relevant and meaningful notes. One of the more interesting experiences I had here

was working with an external recruiter who used a video interview platform. I was able to provide questions that were flashed in front of candidates who were then given a defined time limit for their response. In these instances, responses came directly from the candidates which was a bonus.

Now, in terms of questions focus on fundamentals. Test candidate understanding of security principles and the ability to articulate opinions. If a candidate…

- explains that SSL and HTTPS are identical, consider another candidate
- believes that an NMAP scan is a penetration test, it is safe to assume they will not be terribly effective in a penetration testing role.
- doesn't understand operational, security, or legal aspects of open-source software, they may not be suited to conduct risk assessments.
- thinks that DDoS protection is enabled through IDS, you may not want them monitoring your networks
- understands MFA to be UserIDs and passwords provided at different stages of the authentication process, keep them away from PCI and regulatory work.

With a quick google search, you will find a host of similar questions already pulled together with expected answers.

The interview…Understand that behavioral interviews on their own, assumptions based on listed experience and reliance on listed certifications will not end positively. I have seen instances of these approaches in action and the long-term impact. Interviews must be balanced in terms of:

- understanding candidate technical capabilities
- how comfortable and capable a candidate is expressing thoughts and ideas
- understanding how a candidate may fit into the team dynamic

I will stress the importance of the technical capabilities. It is here where you should spend a chunk of time working through specific open-ended questions based on listed experience and desired capabilities. If part of the role you are filling involves certain aspects, then your questions should reflect that…

Knowledge of firewall function and an understanding of associated rules?

Your IT client approaches you, indicating they would like to open TCP port 22 to an external vendor to share information. What is your thought process? What questions would you ask? What would you do if a client asked for TCP/UDP port 53 for DNS queries?

Aspects of vendor security assessment?

An IT partner is looking to sign a contract for a SaaS product. The vendor (ABC) uses an external hosting provider. The vendor (ABC) has indicated that they are PCI-certified. What questions would you ask?

Penet*ration testing and vulnerability management?*

You have completed a web application penetration test for a public facing site, and now you have scheduled a walkthrough of the results with the Project team. How would you describe cross site request forgery and its associated risks. What about CSRF?

Working with the development community on secure coding practices?

W*hat are your thoughts on static code analysis vs dynamic code analysis? Where does RASP fit in?*

Rolling out logging and monitoring?

What logs would you look at if you were interested in WPAD and pass-the-hash attacks? What alerts would you set up for apache web-server logs?

Creating / updating Information Security Policy or Standards

What is your definition and view of end-to-end encryption? How would you approach implementation in a corporate environment using a variety of vendor based infrastructure servies?

These are high level examples. Be specific…question experience….dig into the use of terms such as expert and advanced. If you are not comfortable with the subject matter, bring in a member of your team or subject matter expert. Ensure you can identify both insightful and concerning responses.

Be clear as to what you are interested in. It is here you may discover overstated or dated skillsets. In my experience one of the paths most travelled in information security begins with hands on technical experience and shifts overtime into the realm of governance and risk. In some cases, technical skills are left behind in the pursuit of advancement. This is directly related to what skills are valued and rewarded in the industry and what opportunities are available. Think of it in terms of existing career paths for technical staff.

You should be looking for individuals who are genuinely interested in information security beyond a 9-5 job. They should be able to speak to interests, how they keep up to date, what they think of current events in information security, what their personal goals are in terms of development and learning, how they have contributed to the broader information security community, how they take their expertise and apply it to their personal lives. I have had the opportunity to ask related questions during recent interviews. I think the responses below underscore why it is so important to find candidates with a genuine interest in security. Keep in mind the responses from interview over the past few years are the beginning and end of how some candidates protect their home networks.

- 'I make my router password really long'
- "I tell my parents and significant other to make their passwords really long'
- 'I put a firewall in front of my ISP's modem'
- 'I have anti-virus running'

As with anything in life, the most challenging path often is the most rewarding. There are obvious shortcuts. Hire contractors, loosen internal standards, focus on checklists, create snappy colorful dashboards that are more subjective in nature. Ultimately the lack of technical skill and capability will become apparent.

And there you have it…. decision time. But your job is not quite over. There are other considerations to ponder. If I am feeling ambitious I will offer some thoughts soon.

- How do you approach technical self-assessment
- How can you build an engaged information security team
- How can automation make your life easier

..stay tuned