**10 Most Desired Traits for Cyber Security Job Candidates**

Finding a good candidate, or possibly any candidate, to fill one of the thousands of open cybersecurity positions available is one of the greatest challenges facing security executives today.

So with that in mind, we asked some of the top names in the industry what traits they look for in a job applicant. **Here are the top ten most desired cybersecurity traits:**

**1. Continuous Learner**

**Shamla Naidoo, Chief Information Security Officer, IBM**

“The cybersecurity landscape is evolving continuously and rapidly, and therefore the most important quality I look for in a security hire is someone who can do the same – someone with a natural curiosity that will lead to continual learning.  The security workforce needs people who will be a part of inventing the solutions that will keep us safe not only today but in the future.

For me, it’s about hiring someone who has intellectual depth but is willing to learn from others, without ego – not just experience to perform the role.  I look for demonstrable willingness to learn new things and think outside of the box, with specific examples of where they’ve done this successfully in the past.”

**2. Persistence**

**Reg Harnish, CEO of GreyCastle Security**

“The most important quality I look for when hiring new talent is persistence. Are they determined? Do they have the gumption to do the job right? In the cybersecurity world, the problems people face are not only ever-changing, but also very difficult to start with, so persistence is key.

Additionally, a certain level of persistence requires confidence, which is a must in this industry, as security consultants have to deal with the full gamut of employees, from CEOs and board-level executives to end users. There’s no time to second guess yourself.”

**3. Curious and Perceptive**

**Renee Walrath, Founder of Walrath Recruiting**

“To work in cybersecurity, curiosity is an absolutely essential trait. Anyone who gets comfortable in fighting off threats in the same fashion will quickly be outdated, and subject to breaches. To be successful you have to be curious, and seek out new weaknesses before they become weaknesses. A cybersecurity professional needs to be a continuous learner to stay one step ahead of external threats. Proactively learning and updating systems is the only way to stay ahead.”

Perceptive- “A good cyber security professional needs to see problems from both sides. They have to be in the mindset of the company, thinking of what they want to protect. They also have to look through the lens of an external threat and perceive any weaknesses or places to attack. Having both perspectives will make it easier to build a strategy to defend against an external threat.”

**4. Cerebral, Instinctive and Emotional**

**Chris Drake, CEO Armor**

“The dynamic nature of cybersecurity dictates that a person will need to wear a variety of hats and excel in diverse areas to be successful. While tangible skills like these are critical, there are several intangible characteristics that can serve as the foundation for rising above the crowd, including:

* Cerebral – intelligence, process and reason
* Instinctive – innate desire, awareness, quick thinking
* Emotional – heart, passion, sense of duty, pride, morality, justice

It doesn’t stop there, however. Working in cybersecurity is different from other sectors of IT. There is a tremendous amount of collaboration across various disciplines, which requires qualities that might not be as significant in other IT roles. This includes attributes such as creativity, confidence, focus, reliability and humility. Interestingly, we’ve found that those with musical talent have an innate ability to synchronize these skills and emerge as a solid security expert.”

**5. Having a well-rounded skillset**

**Scott Laliberte, managing director, Protiviti**

“These skills range from cyber governance and related soft skills to technical skills, such as penetration testing, hardware/ IOT security, industrial control system security, secure development and code review, network security, identity and access management, etc. The ability to communicate issues in non-technical terms that business people can understand. This is a key attribute in attaining leadership positions in this field.

Finding a candidate that has a balance of strong technical skills, business acumen and communication aptitude is extremely rare, but those candidates will go very far.”

**6. Can work under the gun, attention to detail**

**Michael Potters (right), the CEO of Glenmont Group**

“The ability to work at speed, under pressure, to make decisions in real time and with reliable accuracy and to be able to work in a global environment and drive change.”

**7. Think like a black hat**

**Domini Clark, principal, Blackmere Consulting**

“The ability to think like a ‘bad guy’ enables security professionals to anticipate what hackers might try, and to identify weak points in system defenses. This ability is sometimes lovingly referred to as the ‘evil bit’ (as in bits and bytes) which seems to be coded into the personalities of many industry superstars.”

**8. Analytical**

**Tim Erlin, VP, Tripwire**

“Being analytical, curious and a good communicator are just some of the attributes that make a good cybersecurity professional. If you have the right systems in place, there is no reason not to hire someone who has these skills and teach them the technical skills later. There is an abundance of IT talent that wants to break into this sector and there are many diamonds in the rough that can be mentored and nurtured into future stars. Moving forward, we need a change in mindset quickly otherwise this issue will scale out of hand.”

We know that companies are seeking the perfect candidate who has 5-10 years’ experience and several certifications for an entry-level position. This is an impractical and damaging approach to hiring as we are substantially restricting the pool of potential candidates.

**9. Military veteran**

**Stephan Tallent, senior director of managed security service providers, Fortinet**

“They have the proven ability to learn new skills and concepts, which makes them ideal candidates. And many have been trained in the use of some of the most advanced technologies in the world. Performance under pressure is another big differentiator for veterans. They have a capacity to accomplish priorities on time and they know the critical importance of staying with a task until it is done right. And like active military duty, cybersecurity is detail- and process-oriented, often with extreme consequences for failure.

Additionally, military duties involve a blend of individual and group productivity, they can function as both a highly effective team operator as well as an individual contributor. As a bonus, many veterans come with highly sought-after security clearances already in place.”

**10. Willingness to continuously develop skills**

**Rob Clyde, ISACA Board Member**

“About 70 percent of organizations require cyber-security applicants to have a cyber-security certification. Therefore, an increased emphasis on and investment in training and professional development is a must. Hiring personnel and giving them the chance to develop that experience would go a long way toward raising cyber capabilities across all industries. While having a realistic sense of cyber professionals’ market value is a must, investment in professional development opportunities and job rotation to help round out skills and minimize frustration with repetitive tasks also can incentivize employees to stay for longer periods.

Retaining and providing professional development to employees help organizations be prepared to meet cyber-security challenges head-on.”