Hiring IT and Security Professionals – What really matters?

By Jason Brown, CISO, Merit Network

Your organization is at great risk for a cyber attack, and chances are, you don't have the personnel to protect you.

DDoS (distributed denial of service) attacks grew more than 160% in the last year with millions of new malware and ransomware variants each day. The growing volume and sophistication of this cybercrime is driving an estimated security workforce shortage of 1.5 million worldwide in the next two years.

While hiring cybersecurity and IT professionals isn't a "magic bullet," it can be the first line of defense in protecting your business, your customers and your revenue. How can a hiring manager wade through the myriad certifications and credentials to understand what really matters when hiring security professionals to protect their organization?

The first step is to determine the right level of security professional for your organization.

1. **Entry level cybersecurity positions,** such as risk analysts, typically require less than one year of practical experience. Certifications such as CompTIA's Security+ or ISC²'s Systems Security Certified Practitioner (SSCP) confirm that the candidate has the knowledge to evaluate risk, understands network and server security and grasps the fundamentals of identity and access management.

2. Organizations looking for **mid-level security positions,** such as secure code developers, penetration testers or cybersecurity engineers, must require a bachelor's degree in IT or computer science and that the candidate has a minimum of five years of practical experience. Individuals in this career level are responsible for ensuring that the development of applications along with company networks

and servers are configured properly. Mid-level employees may also be required to architect and deploy new systems and services, develop policies, standards and procedures and provide higher level support. In addition to a college degree, employers should look for candidates that have obtained engineering or professional level certifications. These could include EC-Council's Certified Ethical Hacker (CEH), Cisco Certified Network Associate (CCNA) or one of the many Microsoft MCSE certifications. These candidates will not only understand how systems, networks and software are built, they will also understand potential misconfigurations of IT systems, vulnerabilities and risks for exploitation.

3. **Architectural, managerial or C-level positions** require extensive education and on-the-job experience. Those in this type of role will not only drive cybersecurity strategy, they may also be required to architect new solutions, determine risk and demonstrate expertise in regulations which may impact your business. Hiring managers must look for advanced certifications such as ISC^2's Certified Information Systems Security Practitioner (CISSP) and EC-Council's CCISO certifications both which require a minimum of five years in the cybersecurity field. Management training, certification and experience are also necessary for individuals who will be supervising security teams.

Merit Network helps businesses and nonprofits improve their security posture through network and organization vulnerability assessments, workforce development and certification courses, end user training, security hardware and software solutions and more.

Our seasoned security team can develop custom programs to prevent your organization from falling victim to the millions of U.S. hacking attempts that occur each day. Contact the Merit Security Team today by visiting Merit.edu/custom-training.