IBM Launches Cybersecurity Skills Initiative for "New Collar" Jobs

New Programs & Recommendations to Expand Cybersecurity Workforce Pipeline

IBM Security has launched an initiative to help address the cybersecurity worker shortage through programs and partnerships that promote a "new collar" cybersecurity workforce strategy.

The security workforce shortage is growing rapidly, predicted to reach 3.5 million cybersecurity job openings by 2021 according to a recent report by Cybersecurity Ventures.

To address this shortage, IBM is sponsoring alternative education models such as Hacker Highschool and Pathways in Technology Early College High School (P-TECH), while defining new workforce approaches to reach a broader pipeline of employees based on skills, experience and aptitudes as opposed to traditional hiring models which focus on degrees alone. In fact, nearly 20 percent of IBM Security professionals hired in the U.S. since 2015 fall into this category of "new collar" employees.

To help overcome the cybersecurity talent shortage and build the skills needed for the modern security workforce, IBM Security is investing in several initiatives including:

- New collaboration with the Hacker Highschool project, an open cybersecurity training program for teens and young adults.
- Continued investment in skills-based education, training & recruitment, including vocational training, coding camps, professional certification programs and innovative public/private education models like P-TECH (which IBM pioneered in 2011).
- Outlining a strategic workforce approach for the security industry with practical steps that all organizations can take to rethink their own cybersecurity talent models, via a new industry whitepaper from IBM Institute for Business Value.

"The cybercrime landscape is evolving rapidly, yet many organizations are still approaching their cybersecurity education and hiring in the same way they were 20 years ago," said Marc van Zadelhoff, General Manager of IBM Security. "The truth is that many of the critical cybersecurity roles we need to fill don't require a traditional four-year technical degree. Industry leaders need to take an active part in resolving the talent issues we're facing, by investing in new models and extending the pipeline to focus on hands-on skills and experience over degrees alone."

Rethinking Cybersecurity Training & Education: Hacker Highschool & P-TECH

More than half of security hiring managers say that practical, hands-on experience is the most important qualification for a cybersecurity candidate.[1]

Yet the majority of students are not given the opportunity to learn these security skills in a traditional classroom setting, particularly at a high school level. In fact, two out of three high schoolers say the idea of a career in cybersecurity had never been mentioned to them by a teacher, guidance or career counselor.[2]

IBM Security is investing in alternative education models that focus on bringing cybersecurity exposure and skills to students at a younger age. This includes a new initiative with ISECOM, a non-profit organization which provides Hacker Highschool, open cybersecurity courses designed specifically for teenagers to develop the critical thinking and hands-on, technical skills needed for today's security professionals.

As part of this collaboration, IBM will provide sponsorship, expert guidance and IBM Security tools for a new Hacker Highschool lesson focused on the skills needed for an entry-level security operation center (SOC) analyst – a position that is in particular demand.

---

[1] State of Cyber Security 2017, ISACA

[2] Securing our Future: Closing the Cyber Talent Gap, Raytheon

Students completing the Hacker Highschool curriculum will also have the opportunity for hands-on practice with IBM Security QRadar software, a deep security analytics technology used in thousands of security operation centers around the globe to help monitor malicious activity and detect attacks.

“A critical factor in the cybersecurity workforce challenge is the huge gap that exists in relevant security education resources at a high school level. The fact is that most schools don’t have teachers equipped on this subject, or appropriate course materials available," said Pete Herzog, co-founder of ISECOM. "With Hacker Highschool we make the courses so students can teach themselves, with an emphasis on thinking like a hacker to develop deep technical security skills, along with creativity, resourcefulness and a sense of moral responsibility to keep them on track.”

IBM is also helping students gain cybersecurity skills and training through its continued investment in the P-TECH education model, which connects high school, college and the business world to prepare students for technology jobs of the future, including cybersecurity. Through P-TECH, public high school students can earn both a high school diploma and an industry-recognized two-year postsecondary degree at no cost to them or their families, while working with industry partners like IBM on skills mapping, mentorship, workplace experiences and internships.

The P-TECH model has expanded to over 60 U.S. schools and 300 industry partners, including several new schools which are pioneering a cybersecurity-focused, IBM-sponsored degree program, such as Excelsior Academy in New York and P-TECH@Carver in Maryland. Hundreds of students are currently enrolled in these cybersecurity-focused P-TECH schools, and those who finish will earn an Associate of Applied Science (AAS) in Cybersecurity upon completion.

Redefining Hiring Tactics in Security – A “New Collar” Approach
While bringing more people with a broader set of talents into the cybersecurity workforce is critical, companies must also take a more strategic approach to how they recruit and hire talent, widening the aperture to accommodate all types of skills needed for the modern security workforce.

With the wide variety of cybersecurity roles that exist today, many of the core attributes and skills needed to succeed in this industry can be developed outside traditional four-year, university degree programs. Vocational schools, associate degree programs, military veterans programs, coding camps and skills-based certifications are all great sources of cybersecurity talent which are often overlooked in traditional hiring and recruitment programs.

A growing number of positions in cybersecurity – and the technology industry as whole – shouldn’t be defined as “blue collar” or “white collar,” but rather as “new collar” roles that prioritize capabilities and skills over degrees.

As a company with over 8,000 cybersecurity-focused professionals, IBM is helping lead the way by incorporating a “new collar” hiring approach into its own security business. In fact, nearly 1 in 5 IBM Security employees hired since 2015 fall into this “new collar” category.

To help organizations address their own security hiring challenges, IBM has outlined several steps companies can consider to get started with their own strategic talent approach, such as:

- **Redefine your hiring models;** identify the attributes and skills needed for various positions and those that can be filled by non-traditional candidates. Don’t focus solely on degrees as prerequisites.
- **Expand where you recruit;** don’t limit yourself to the select set of universities that you have always focused on; expand to community colleges, P-TECH schools and other educational programs like professional certifications.
- **Create new partnerships in your region** – with government organizations, educational institutions and programs, and other groups.

Provide a robust support program for new hires – such as mentorships, rotational assignments, shadowing and other opportunities for new cybersecurity hires to gain experience and learn. Additionally, help employees build and refine skills with classes, certifications, and conferences. Cybersecurity is a highly dynamic field, which requires a constant refreshing of skills.

To see the full whitepaper outlining tips for companies looking to expand to a “new collar” security approach, visit: ibm.biz/newcollarjobs. To get the latest insights on how IBM is helping security leaders tackle tough risk and security challenges, visit: ibm.com/security/ciso.

About IBM Security
IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research, enables organizations to effectively manage risk and defend against emerging threats. IBM operates one of the world’s broadest security research, development and delivery organizations, monitors 35 billion security events per day in more than 130 countries, and holds more than 3,000 security patents. For more information, please visit www.ibm.com/security, follow @IBMSecurity on Twitter or visit the IBM Security Intelligence blog.

###