CYBER
TALENT
INSTITUTE

HOW GOOGLE AND BLOOMBERG ARE HELPING WOMEN GET INTO CYBERSECURITY

Bridging the gap between the 'boys club' of cybersecurity and the historically overlooked but equally qualified young women in our communities is a new scholarship program created expressly to close that gap.

In early 2020, Women in Cybersecurity (WiCyS) and the SANS Institute partnered with Google to create the Security Training Scholarship for women interested in cybersecurity. The competition encourages women to pursue an interest in cyber by allowing them to learn and collaborate in a supportive, inclusive environment. That made all the difference to scholarship winner Aimee Reyes. "The men in my school were very competitive, and so am I. But I never before knew that cybersecurity was a safe space to learn, and it was wonderful to feel immersed in that," says Reyes, who has since achieved multiple certifications and now works as a security engineer at Amazon.

Last year's pilot program attracted more than 900 applicants, with more than 440 applicants participating in the initial stage of the competition. Those who chose not to compete (or had already worked in the field) did not participate. This year, the scholarship is also partnering with Bloomberg, after leaders at the business media giant saw the positive impact the pilot program was having on a historically marginalized population.

"I still can't believe I'm an undergrad with real certifications. I feel this will help with my job hunt, as will the connections I made through the program."

– Luiza Machado

Applicants came a wide array of backgrounds and from all over the world. In its pilot phase, the 15 full scholarship winners represented 5 countries: the U.S, India, Kenya, Brazil, and Mauritius. Applicants also came from unique places in their lives, some using the program resources to change their careers for the better. For example, Melinda Bigger, a former chemical engineer from Los Angeles, recently decided she might be interested in cybersecurity. She applied to the scholarship program and won. "It's [given] me huge confidence that this was something I could do, something that was worth changing careers for," she says. Others haven't launched their careers yet, such as Luiza Machado, a young woman from Brazil who is still pursuing her undergraduate degree. "I still can't believe I'm an undergrad with real certifications. I feel this will help with my job hunt, as will the connections I made through the program."

The Security Training Scholarship builds on the momentum of the CyberStart America game, which also launched its U.S. pilot program in 2020. The game turns real world cybersecurity tasks into fun, hands-on challenges for students who enjoy solving puzzles. The scholarship program gamified the early stages of its competition using CyberStart, and many applicants discovered how much they enjoyed the technical aspects of learning to solve the content challenges in the game. "The CyberStart game was the most fun part. It was the best and most fun way to learn concepts and apply them hands on," says Harsha Deepa, who now works as a Junior Solution Analyst at Deloitte and an event coordinator for WiCyS India.

"The CyberStart game was the most fun part. It was the best and most fun way to learn concepts and apply them hands on,"

– Harsha Deepa

"I was hooked, and I will never forget command injections because I had to spend hours trying to exploit a webpage that was vulnerable to it," adds Reyes, the Amazon security engineer. "It was an invaluable experience."

For those who win, the program can be life changing by opening up entirely new career paths. The Security Training Scholarship aims to ensure the employment of its winners in the field within a year and a half of completion. One recent winner, Colleen Campbell, reported receiving an offer for a cybersecurity position "less than four months after applying to the program." Today, Campbell works for Raytheon as a Senior Systems Administrator.

For many participants, the program's benefits do not stop once the competition ends. The connections they make and the community they join become just as important to their future success. "Knowing other women that are doing the same things I'm doing and going through the same things as me – and having the same doubts – was amazing," adds Bigger, the former chemical engineer. "We encouraged each other to keep going."

The program applicants all join a Slack group chat, where participants can discuss the challenges and share information. "The Slack channel was super helpful and having someone to give me a little hint was huge," adds Bigger. Applicants are also assigned a program mentor to further their experience and offer career and learning advice. As Deepa points out, "the amount of support I received from my mentor and the cohort makes the scholarship program very different from others."

To find the strongest candidates, the program takes a multi-tiered approach, consisting of five progressively more difficult, more selective stages.

STAGE ONE

Stage 1 was a beginner-Level CTF (capture the flag) game. With more than 28 content packs and a variety of challenges, this stage allowed participants to solve simple cybersecurity challenges which helps assess a candidate's potential later in the challenge. This stage took approximately one month to complete. The pilot program candidates' responses were overwhelmingly positive. As one put it: "It's very tough, but something you'll have to do research for, and research is something you'll have to do within your cybersecurity career almost every day, so it's really good practice."

STAGE TWO

Stage 2 began with 250 participants and lasted about seven weeks. Recipients were given a chance to show their passion for the field by participating in the CyberStart Game, where they completed challenges that required persistence and research skills. In this stage, participants were also introduced to key technical skills such as Linux, Web Attacks, Programming and Forensics, among others. Players used these skills and others to defend against mock attackers. Once they displayed a combination of CyberStart performance and community engagement, they could then move on to Stage 3.

STAGE THREE

By Stage 3, 100 participants were chosen to move into the SANS CyberTalent Assessment, which measures each individual's technical aptitude for cybersecurity learning potential. This stage is even more competitive, so only 38 applicants qualified to move forward. Performance in the assessment, as well as community engagement levels, were the criteria used to winnow the candidates in this stage.

As the Security Training Scholarship continues to grow, so does the potential to enable more women to join the cybersecurity workforce; a crucial sector in ensuring our country's safe online future.

STAGE FOUR

In Stage 4, rather than playing training games, participants receive real certification training. They were given the chance to complete the SEC275/Foundations Course + the GFACT Certification exam. Both courses are considered difficult and focus on foundational material concerning devices and networks. Recipients also received training in the fundamentals of Windows and Linux, two of the most popular cybersecurity languages. Exam two, the GFACT exam, validates a participant's knowledge of essential cybersecurity concepts. "SANS Foundations is essential to a cybersecurity career because it touches on so many portions of cybersecurity that you will encounter" says Christine Morency, a candidate from last year from the Washington D.C. area.

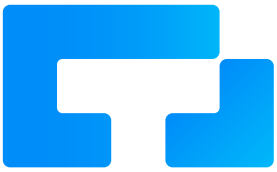
STAGE FIVE

Upon reaching the final Stage 5, recipients took a deeper dive into cybersecurity concepts, along with additional certification opportunities. The first course of Stage 5 is SEC401: an interactive, hands-on lab. Participants learned how to set up a virtual lab, crack passwords, and use hashing technology, among other skills. After finishing the course, students received the GIAC Security Essentials Certification (GSEC), which tests a participant's knowledge of cybersecurity concepts beyond basic terminology. From Linux security to cryptography, the GSEC tells an employer that participants are ready for hands-on IT security roles.

"Knowing other women that are doing the same things I'm doing and going through the same things as me – and having the same doubts – was amazing..."

– Melinda Bigger

Finally, the scholarship winners were offered the SEC504 Course + GIAC Certified Incident Handler certification. This in-depth course delves into how to design, build, and operate systems to thwart attacks. During this portion of the program, applicants can choose a facet of cybersecurity to focus on. "I decided I wanted to take a course on web-app security. It by far exceeded my expectations," says Hema Pillay, who recently received an offer as an Identity Access Management (IAM) Analyst in San Francisco. "I'm done with the exam, but my books have stayed open because I'm spending the summer doing hands-on projects using the knowledge I gained." Once certified, applicants will have proven their ability to detect, respond, and resolve security incidents using many different types of tools.



CYBER
TALENT
INSTITUTE

www.cybertalentinstitute.org

info@cybertalentinstitute.org