UNMASKED

CYBRARY.IT

TAKING THE MYSTERY OUT OF CYBER SECURITY

MARCH 2018 | EDITION 4

IN THIS ISSUE

EDITOR'S NOTE

I want to thank each and every one of you for not only reading UNMASKED, but for dedicating yourselves to learning and career advancement. As you'll read in the Cybrary Declassified Report, it's individuals like yourselves who are the hope for not just our industry, but our future. We need qualified professionals now more than ever.

That said, I must also share that I have received a new career opportunity and will be discontinuing UNMASKED after this week. But, do not despair, Cybrary and their Alliance partners will continue to share industry news each week. Visit the **Alliances** page to hear from companies like Cylance, Carbon Black, Alien Vault, and Cisco.

Olivia Lynch **(@Cybrary_Olivia)** is the Marketing Manager at Cybrary. Like many of you, she is just getting her toes wet in the field of cyber security. A firm believer that the pen is mightier than the sword, Olivia considers corny puns and an honest voice essential to any worthwhile blog.

CYBER SECURITY NEWS

#PRIVACY

It seems Facebook 'unfriended' privacy as news surfaced that consulting firm Cambridge Analytica used the platform to harvest the data of 50 million users and use it without their consent.

Cambridge Analytica has worked on many political campaigns, most notably that of Donald Trump. In 2015, "an app developer violated the company's platform policies by collecting data via an app under the pretense of using it for psychological research – and instead passing users' personal information to Cambridge Analytica and its parent company SCL," recent news reports. While Facebook denies a data 'breach,' their ignorance of these happenings has the security community is questioning how Facebook handles the privacy of their

customers. Threatpost writes, "Up to 270,000 Facebook users downloaded the app – giving Kogan consent to access data, such as the city they live in or content they “Liked” on Facebook. However, in 2015, Facebook also enabled developers to collect data on the Facebook Friend networks for users – meaning that when users agreed to show their data to Kogan, he could also access data about their Friends."

Since an article from The Guardian first published this news, Facebook, politicians, cyber security experts, and Facebook users have expressed their distrust in the company, even encouraging others to delete the app. While it wasn't a technical breach, most agree it was a breach in trust.

Test the security of your social accounts with help from Cybrarian Jaden Turner.

#HACKED

Third party vendors strike again. At least, that's what it appears as Expedia owned Orbitz announces they've experienced a breach which may have led to the disclosure of 880,000 credit cards.

Reports indicate that adversaries had access to Orbitz business and consumer partner platforms and stole information during 2016 but that parent company Expedia was unaware until March 1st. Of the data compromised, the news indicates it may have included payment card information such as names, phone numbers, email and billing addresses,

“People are shocked this happened, but I’m shocked it didn’t happen sooner… it’s so easy to penetrate this kind of thing with social media providers. The real issue here is Facebook… not the people who collected the data or those who used it. Facebook knew it happened and didn’t say anything to the public.”
-Joseph Steinberg, founder of SecureMySocia

but not passwords. In response, Expedia said "To date, we do not have direct evidence that this personal information was actually taken from the platform and there has been no evidence of access to other types of personal information, including passport and travel itinerary information."

Since the initial discovery of the breach, details of how it occurred have not been disclosed, but reports indicated that it took place on a legacy system. It's interesting to mention that Orbitz was acquired by Expedia four months prior to the breach. While some have indicated the breach may have been caused by a misconfigured storage container that allowed 3rd party access. Others speculate that Carbanak cyber gang is to blame. In recent news, Carbanak allegedly stole $1 billion from financial institutions and have begun targeting hospitality industries with new techniques. Affected customers are advised to monitor their credit card statements and report suspicious activity.

"Ensuring the safety and security of the personal data of our customers and our partners' customers is very important to us. We deeply regret the incident, and we are committed to doing everything we can to maintain the trust of our customers and partners."
-Expedia

New Carabanak attack prevented by Minerva. Read the blog post to learn the details.

#BUGBOUNTY

And now, for some positive news in the cyber community. Netflix recently announced they've launched a public bug bounty program that pays $100 to $15,00 per discovery.

Previously, Netflix has had a responsible vulnerability disclosure program which transformed into a

private program through Bugcrowd. Now, they've taken things a step further. In a recent blog post, Netflix stated "We started our program with a more limited scope and 100 of Bugcrowd's top researchers. In preparation for our public launch, we have increased our scope dramatically over the last year and have now invited over 700 researchers."

Since 2016, Netflix has received 145 valid bug bounty submissions out of 275 total. “What’s unique about Netflix and makes this program so exciting is the enormous amount of traffic that the company transmits around the globe. That traffic is now being protected by the broader white hat community,” Casey Ellis, CTO of Bugcrowd said. The scope of the program is fairly large, including Netflix.com, and the Android and iOS apps, which are used by over 117 million users. What is restricted, however, is customer and employee information and pre-release Netflix content, as well as client applications and third-party websites. Many other big names in tech, including

Samsung and Microsoft, use bug bounties as a more cost-effective way of identifying vulnerabilities. "We have attempted to fine tune things like triage quality, response time and researcher interactions to build a quality program that researchers like to participate in," Netflix added. A focus on cross-site scripting (XSS) bugs, SQL injections and API vulnerabilities, among others, is encouraged.

For those unfamiliar with Bugcrowd, check out their page on the site.

"Engineers at Netflix have a high degree of ownership for the security of their products and this helps us address reports quickly. Our security engineers also have the autonomy and freedom to make reward decisions quickly based on the reward matrix and bug severity. This ultimately helps create an efficient and seamless experience for researchers which is important for engagement in the program."
-Netflix

FACT BYTE

80% OF RESPONDENTS DO NOT FEEL ADEQUATELY PREPARED TO DEFEND THEIR ORGANIZATION

-2018 Cybrary Declassified Report

MEET THE CYBRARIAN

MAGDA CHELLY

Magda is the Managing Director of Responsible Cyber Pte. by day, and a cyber feminist hacker by night, and is the course creator of the **Advanced Social Engineering Tactics course.**

“I believe everyone is entitled to learn. Knowledge should be shared and free. This is definitely the best way to change the world and make it a better place. Education should be accessible to people wherever they are and without spending huge budgets creating constraints for the rest of their lives."

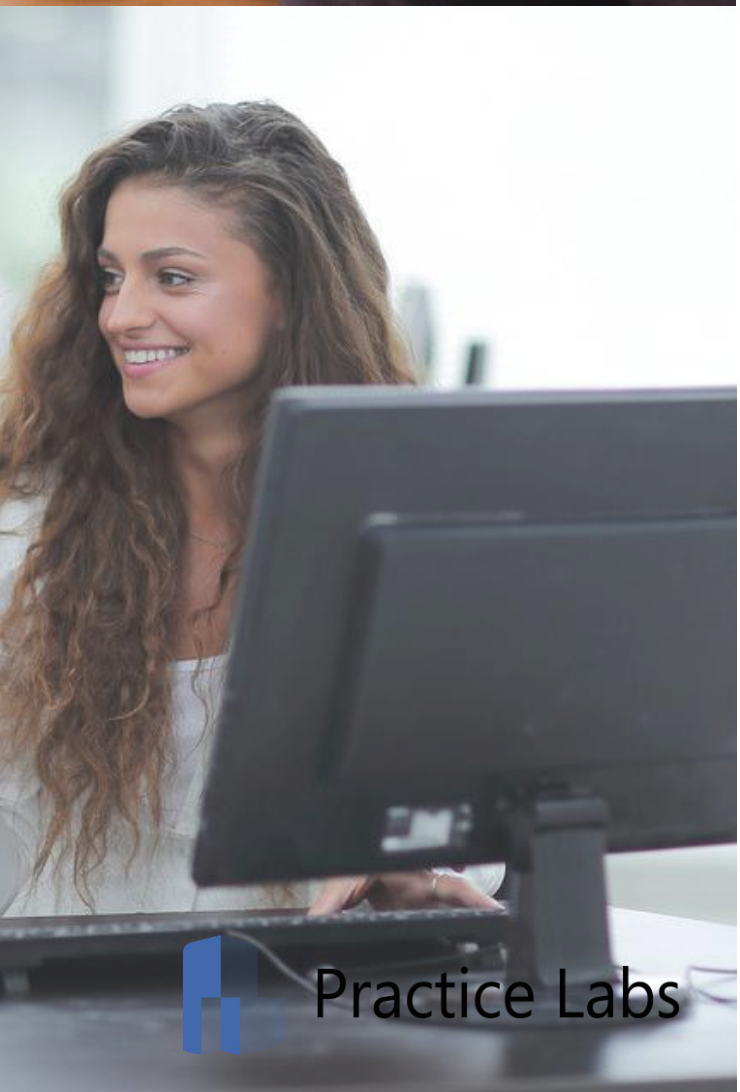
START COURSE

TEACH ON CYBRARY

PMP Practice Test

Professionals seeking a comprehensive understanding of the project management process will greatly benefit from the PMI PMP Practice Test. This practice test will prepare you to ace the PMI PMP certification exam. Obtaining your certification signifies that you possess the fundamental knowledge to initiate, plan and manage a project.

Get Started

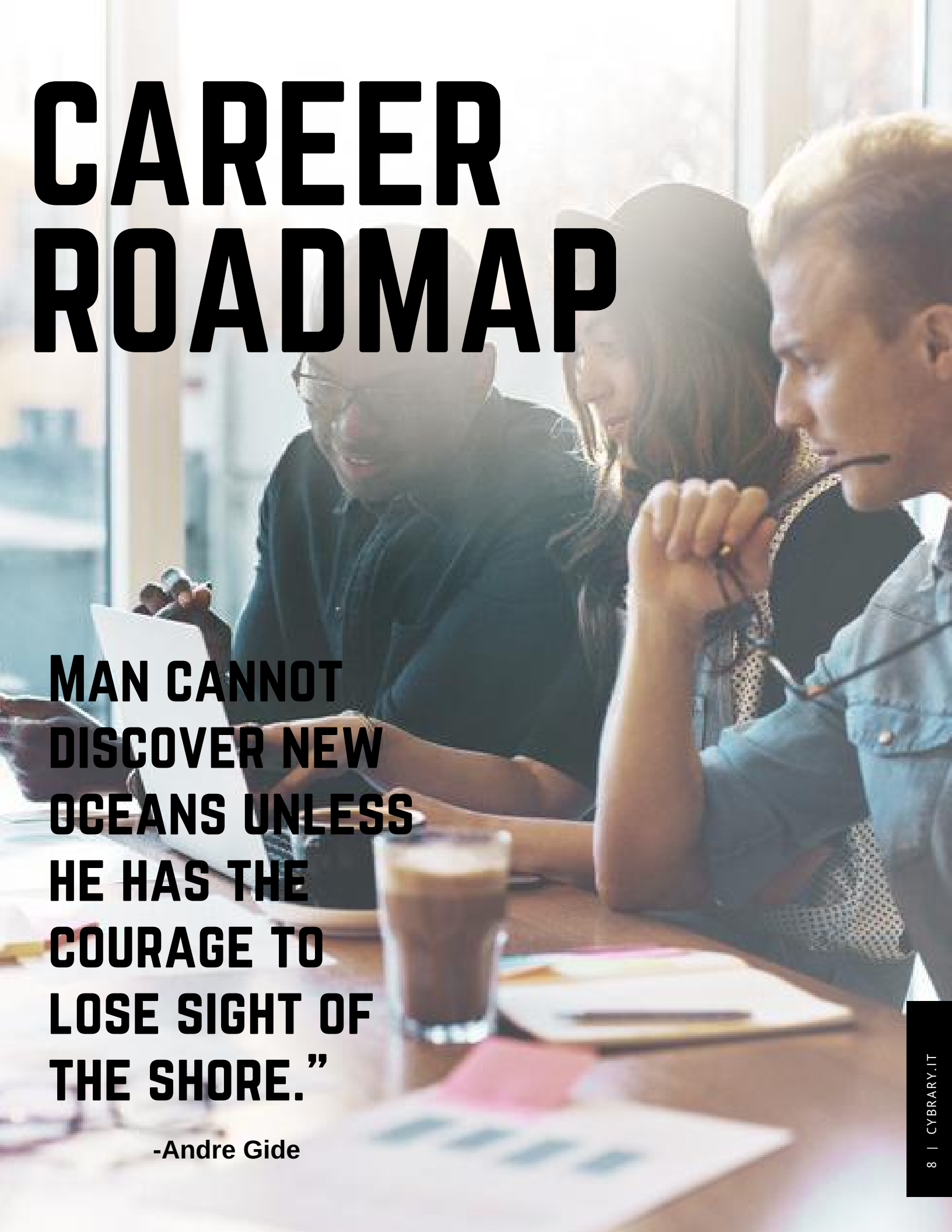


Network Security Tools Virtual Lab

With this virtual lab, you will gain hands-on skills needed as a capable network administrator, network technician, network installer, help desk technician or IT cable installer.Completion of this lab indicates that you are familiar with popular security tools, including firewalls, IDS/IPS, access control, and antivirus solutions. The topics covered in this lab will help you tackle more complex networking problems.

Dive In

CAREER ROADMAP



MAN CANNOT DISCOVER NEW OCEANS UNLESS HE HAS THE COURAGE TO LOSE SIGHT OF THE SHORE."

-Andre Gide

Cisco 2018
Annual Cybersecurity
Report

MAKING CONNECTIONS

Cisco researchers have found, “In complex security environments, organizations are more likely to deal with breaches. Of organizations using 1 to 5 vendors, 28 percent said they had to manage public scrutiny after a breach; that number rose to 80 percent of organizations using more than 50 vendors (figure 51).”

You can earn a badge and a Certificate of Completion when you pass the ACR 2018 Assessment. Simply apply code **ACR2018** to take the assessment free.

Continue Reading **Take Assessment**

Source and Recruit Pre-Qualified Cyber Security Professionals on Cybrary

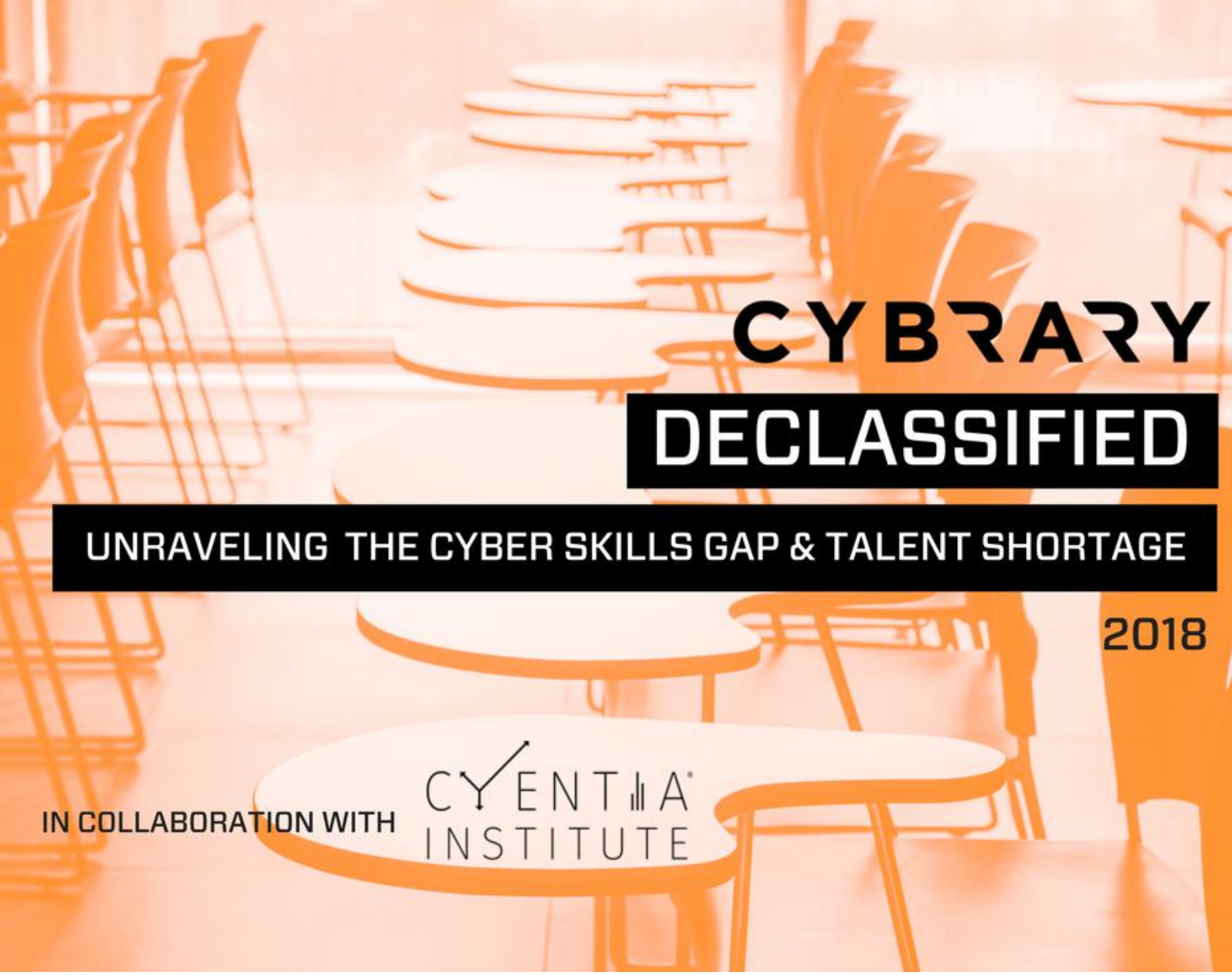
Join the waitlist today. These great companies are lowering their cost to hire and growing their pipelines on Cybrary:

Cognizant

Access the world's largest talent pool of cyber security professionals, and receive candidates with pre-assessed technical skills.

- Eliminate the pain and costs of a technical assessment
- Receive candidate skill profiles highlighting knowledge and technical proficiency
- Reach active and passive candidates; and, fill your pipeline with pre-vetted, qualified cyber professionals.

Learn More



“It is clear that the likelihood of employer-paid training increases with the respondent’s level of experience. Whether that’s a good thing or not is another question. Logic suggests that the learning needs of junior employees were at least equal to that of those with more experience—and quite possibly more. This in itself might be a contributor to the overall talent gap in IT or cybersecurity, regardless of gender or ethnicity,” writes Wade Baker of Cyentia Institute.

Read the Blog

Download Report