NCyTE Cybersecurity Alumni Workforce Study 2025

National Centers of Academic Excellence in Cybersecurity

NCyTE CENTER

National Cybersecurity Training & Education Center

NSF National Science Foundation

This material is based upon work supported by the National Science Foundation under award #2054724. Any opinions, findings, conclusions, or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

CTW CyberTech West

Tobi West, Ph.D., CISSP

Abstract

This report presents the findings of a ten-month study evaluating the effectiveness of National Centers of Academic Excellence in Cybersecurity (NCAE-C) in preparing individuals for careers in cybersecurity. The study involved 281 students from 36 colleges and universities across the United States. The National Institute for Standards and Technology completed an update to the NICE Workforce Framework for Cybersecurity that included the definition of 52 work roles. This study involved identifying the types of jobs CAE alumni found after graduation and the alignment of these jobs to the work roles.

Table of Contents

List of Tables

List of Figures

Introduction

Since 1999, universities and community colleges across the nation have developed rigorous cybersecurity programs designated by the National Security Agency as Centers of Academic Excellence in Cyber Defense (CAE-CD). The National Centers of Academic Excellence in Cybersecurity (NCAE-C) program now directed by the Department of Defense (DoD) Office of the Chief Information Officer (CIO), Cyber Academic Engagement Office (CAEO), includes over 480 higher education institutions with one or more cybersecurity program designations addressing the nation's cybersecurity workforce shortage (CAE in Cybersecurity Community, 2025). As the shortfall of cybersecurity professionals flatlines, the number of ransomware attacks continues to rise, up 3% over the prior year at 5,263 reported in 2024 further signifying the need for workforce development (Symantec, 2025). This study of 281 cybersecurity program alumni from 36 higher education institutions from across the United States highlights current trends and identifies potential opportunities.

According to the Identity Theft Resource Center, in 2024 there were 1.3 billion data breach notices sent to victims (ITRC, 2025). With soaring costs of cyberattacks reaching $16.6 billion in the U.S. last year, organizations seek skilled individuals to protect critical systems and mitigate the risks of cyberattacks to prevent data breaches (FBI IC3, 2025). For every 100 cybersecurity jobs, there are just 83 cybersecurity workers available. As of May 2025, the cybersecurity workforce gap persists with CyberSeek (2025) indicating that there are 457,398 cybersecurity job openings and 1,251,007 employed nationally in cybersecurity positions. The demand for skilled cybersecurity professionals remains strong, and NCAE-C programs play a vital role in advancing workforce development.

There has been a longstanding gender gap both in the technology field and among graduates of technology-focused education programs. Including a balance of genders strengthens the field with broader perspectives and a wider range of problem-solving approaches to increasingly complex cybersecurity challenges. In 2019, the workforce study of community college cybersecurity alumni called *Where Are They Now?* noted the gender imbalance with 56% women enrolled in community colleges and only 20% women in the cybersecurity workforce globally (Sands & Sande). ISC2's Survey reported that the U.S. cybersecurity workforce is made up of 19.2% women as of 2024, further highlighting that the gender imbalance has not improved in recent years (ISC2, 2025).

In addition to education, industry-recognized certification continues to be valuable and relevant to securing employment in cybersecurity. Career changers seeking to upskill and reskill may demonstrate their cybersecurity knowledge and skills to enhance their job prospects. As noted by ISC2, 65% of respondents agree that certification is a way to prove cybersecurity knowledge and 90% of respondents found their pre-employment certification to be valuable for their job (ISC2, 2024).

This follow-on study sponsored by NCyTE Center examines the career outcomes of alumni from CAE-CD designated cybersecurity programs to assess how well these programs are preparing graduates for the evolving demands of the cybersecurity workforce. There are 52 cybersecurity work roles in the NICE Workforce Framework for Cybersecurity (NICE Framework) developed by the National Institute of Standards and Technology (NIST) which aligns cybersecurity education, hiring, and career development (NICE, 2025). The NICE Framework is widely used by government, academia, and industry to support training and workforce development. NCAE-C programs support curriculum development by aligning materials with work roles in the NICE Framework. In this study, participants were asked to indicate which work roles from the NICE Framework best aligned with their daily responsibilities.

Key data on employment status, job roles, industry sectors, certifications, and the perceived impact of academic preparation on career success were captured in this study. The influence of internships, extracurricular activities, and mentorship opportunities on workforce readiness are also explored. Findings from the study will help CAE-CD institutions strengthen curriculum, align with industry needs, and better support current and future students pursuing cybersecurity careers. The insights gained will also highlight trends, skills gaps, and opportunities for continuous improvement in cybersecurity education.

Research Methodology

Study Design

A narrative inquiry approach was used for the design of this study. The target population for this study was alumni of cybersecurity degree and certificate programs ranging from associate degree to doctorate at CAE-CD designated institutions. To reach the alumni of these programs, the Points of Contact (POC) were asked to contact the graduates of their programs. Post-graduation and employment data were collected from CAE-CD alumni through an online survey and remote interviews conducted by the researcher over a span of 10 months from April 2024 to February 2025. The POCs of 36 CAE-CD institutions reportedly contacted 4,869 alumni with 281 alumni participating in the study. Among the 36 institutions, there were 22 two-year colleges and 14 universities. The participating institutions are sorted alphabetically by state in Table 1 below.

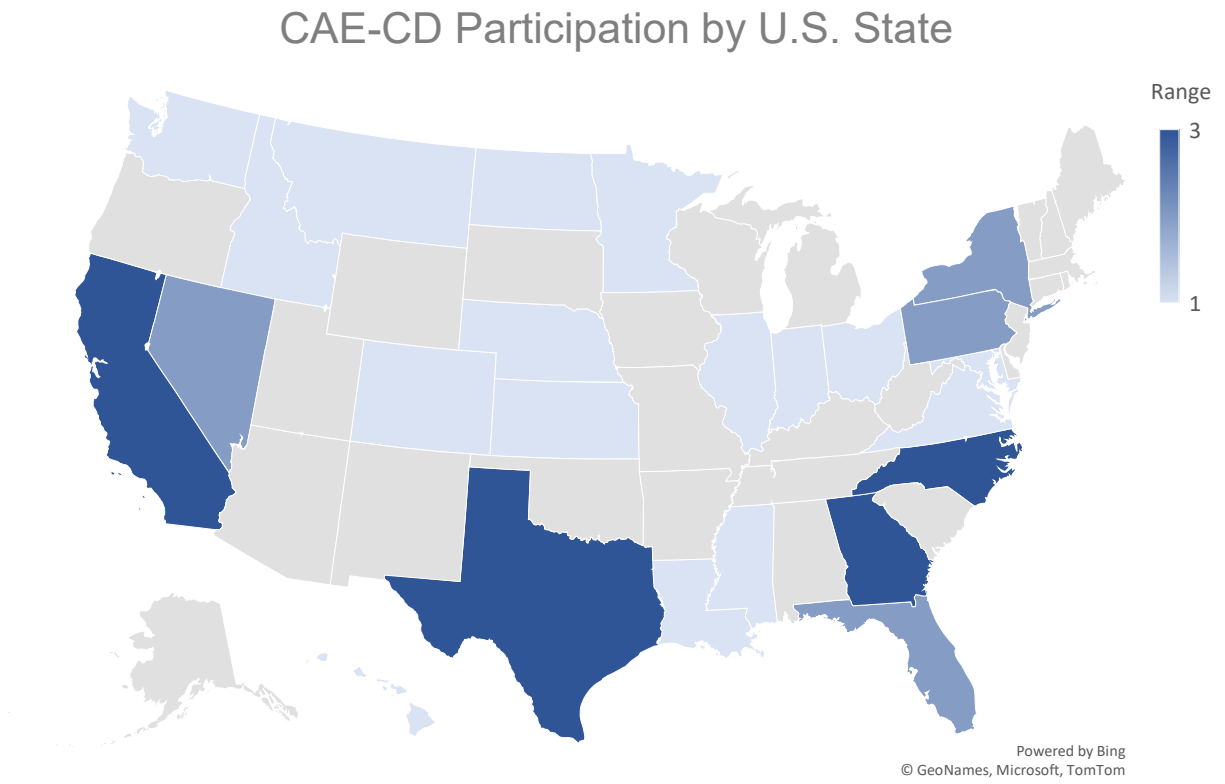
Table 1. Participating CAE-CD Institutions

CAE-CD Institution Name	CAE-CD Institution State
Coastline College	CA
Long Beach City College	CA
Riverside City College	CA
Metropolitan State University of Denver	CO
Embry-Riddle Aeronautical University	FL
St. Petersburg College	FL
Augusta Technical College	GA

CAE-CD Institution Name	CAE-CD Institution State
Gwinnett Technical College	GA
Middle Georgia State University	GA
University of Hawaii Kapiolani Community College	HI
Boise State University	ID
Loyola University, Chicago	IL
Anderson University	IN
Wichita State University	KS
Bossier Parish Community College	LA
Montgomery College, Maryland	MD
St. Cloud Technical and Community College	MN
Hinds Community College	MS
Gallatin College Montana State University	MT
Alamance Community College	NC
Blue Ridge Community College	NC
Fayetteville Technical Community College	NC
Bismarck State College	ND
Metropolitan Community College	NE
College of Southern Nevada	NV
University of Nevada, Reno	NV
University at Albany	NY
University at Buffalo	NY
Xavier University, Cincinnati	OH
Northampton Community College	PA
Temple University	PA
Collin College	TX
Hill College	TX
Sam Houston State University	TX
Virginia Commonwealth University	VA
Whatcom Community College	WA

The alumni contacted for this study reflected a broad range of cybersecurity and related programs in higher education, including three (3) certificate programs, 20 associate degree programs, 10 bachelor's degree programs, and three (3) graduate level programs. This diversity highlights the various educational pathways that lead into the cybersecurity workforce, from short-term certificate programs to advanced degrees. The national reach of cybersecurity workforce development is highlighted by the participation of CAE-CD institutions from 24 states in the U.S. as visually represented in the heat map in Figure 1 below.

Figure 1. Heat Map of CAE-CD Participation by U.S. State



Study Limitations

Limitations of the study included non-response bias, self-reported data, and potential selection bias. A concern of non-response bias is the possibility that the individuals that were less engaged in their education programs and/or that had less-positive experiences may be underrepresented due to lack of response. The study includes self-reported data which may be influenced by participant emotions or social desirability bias. The sample for this study may not be generalizable to all cybersecurity programs and alumni due to the rigorous nature of the CAE-CD program criteria.

U.S. Higher Education Enrollment Demographics

The Fall 2023 IPEDS data enrollment report highlights the enrollment demographics shaping U.S. higher education. With over 19 million students enrolled, the composition of the student body reflects both continuity and change. Women had the most enrollments at 57.6%, continuing a long-standing trend. Racial and ethnic diversity remains a defining characteristic, with White students representing 46.0% of the total population, followed by Hispanic or Latino students at 20.1%, Black or African American students at 12.0%, and Asian students at 7.1%. Smaller yet meaningful student populations, such as American Indian or Alaska Native, Native Hawaiian or Other Pacific Islander, multiracial individuals, and international nonresidents, contribute to the growing diversity in higher education (NCES, 2025).

The age distribution of enrolled students shows that higher education serves people across different generations. Approximately 68% of students were under the age of 25 in Fall 2023, reflecting traditional college enrollment patterns, while over 6 million students (more than 30%) are age 25 and older, highlighting that college remains important for adult learners as well. The enrollment status data shows the majority are balancing a full course load with 60.8% of students attending full-time and 39.2% enrolled part-time (NCES, 2025). This mix is reflective of the educational pathways that students pursue based on their work, family, and financial responsibilities. These national student demographics from IPEDS help to demonstrate that the U.S. higher education system is adapting to support a wide range of students from various backgrounds and age groups.

Alumni Demographics

Participants of this study were geographically distributed across 24 states from 36 higher education institutions. To gather sociodemographic characteristics, alumni were asked to optionally indicate their gender identity and racial/ethnic identity. More than one-fourth of the study participants selected that they preferred not to answer, or they provided no response at all for these questions. Participants were also asked about their highest level of education completed and the city of their current employer.

Gender Identity

Female participants represented 15.3% of the responses while male participants represented 57.3%. Non-binary was indicated by 0.4% of the participants. Some of the participants selected that they preferred not to answer (1.8%) and others skipped the question entirely (25.3%). The gender identities of participants are shown in Table 2 below.

Table 2. Participants' Gender Identities

Gender Identity	Count	Percentage
Female	43	15.3%
Male	161	57.3%
Non-Binary	1	0.4%
Prefer not to answer	5	1.8%
Unreported	71	25.3%

Racial and Ethnic Identity

Like that of the cybersecurity workforce, the dominant racial identity indicated by study participants was White at 37%. Followed by Black or African American at 13.9%, Asian at 7.5%, Hispanic at 6.0%, Two or More Races at 5.7%, and American at 0.4%. The remaining racial/ethnic identities had no responses. Some of the participants selected that they preferred

not to answer (3.6%) and others skipped the question entirely (26.0%). The racial and ethnic identities of participants is shown in Table 3 below.

Table 3. Participants' Racial/Ethnic Identities

Racial/Ethnic Identity	Count	Percentage
American Indian or Alaska Native	0	0.0%
Asian	21	7.5%
Black or African American	39	13.9%
Hispanic or Latino	17	6.0%
Native Hawaiian or Other Pacific Islander	0	0.0%
White	104	37.0%
Two or More Races	16	5.7%
Other (American)	1	0.4%
Prefer not to answer	10	3.6%
Unreported	73	26.0%

Level of Education Achieved

The largest portion of participants indicated that their highest level of education achieved was a bachelor's degree at 33.8%. Followed by associate degree earners at 22.1%, master's degree at 16.4%, and doctoral degrees at 0.7%. Over one-fourth of the participants did not indicate their highest level of education. The highest level of education earned by participants is shown in Table 4 below.

Table 4. Participants' Education Levels

Highest Education Level	Count	Percentage
Associate degree	62	22.1%
Bachelor's degree	95	33.8%
Master's degree	46	16.4%
Doctoral degree	2	0.7%
Unreported	76	27.0%

Employment Outcomes

A key indicator of program effectiveness and workforce readiness is the employment status of alumni from cybersecurity education programs. Information technology is known to be a traditional pathway into cybersecurity roles (ISC2, 2024). To understand the employment outcomes of cybersecurity alumni, participants were asked about their employment status prior to and after the completion of their academic programs. Study participants were also asked to identify the name of their employer and work roles based on the NICE Framework.

Employment Status

CAE-CD institutions develop programs to prepare students for employment in cybersecurity and technology-related fields. Participants in the study were asked to indicate their current employment status and, if employed, whether their role is in the technology field. Most of the participants, 76% indicated that they are currently employed in a technology role. Another 7.5% indicated that they are employed in another field. The remaining participants indicated that they are not currently employed, were never employed, or that they preferred not to answer. The current employment status of participants is shown below in Table 5.

Table 5. Current Employment Status of Participants

Current Employment Status	Count	Percentage
Currently Employed in a Technology Role (Yes)	204	72.6%
Employed in another field (No)	21	7.5%
Not currently working but previously employed	17	6.0%
Never employed	36	12.8%
Prefer not to answer	3	1.1%

Individuals already in the workforce may choose to update or expand their skills to advance their careers. Others may choose to gain new skills to enter the workforce. Participants in the study were asked to indicate whether they were previously employed in the technology field. Most of the participants, 53.4% indicated that they were not previously employed in a technology role. While 22% indicated that they were employed in a technology role prior to starting their academic program. The remaining participants did not indicate whether they were previously employed in any role. The prior employment status of participants is shown below in Table 6.

Table 6. Participants' Employment Status Prior to Academic Program

Prior Employment Status	Count	Percentage
Employed in technology or cybersecurity prior to academic program	62	22.0%
Not previously employed in technology or cybersecurity	150	53.4%
Unreported	69	24.6%

Current Job Titles

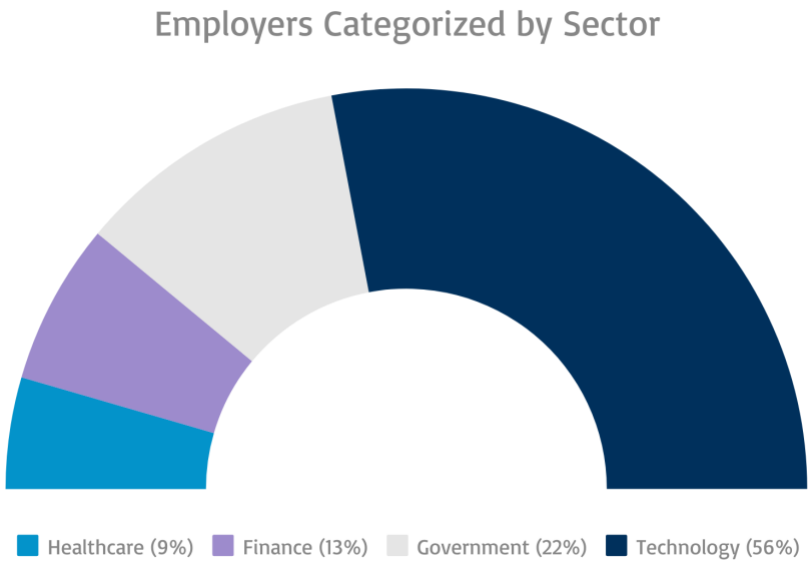
The cybersecurity workforce is comprised of a wide array of jobs, including technical, analytical, strategic, and operational roles that address various aspects of protecting digital assets, information systems, and networks. Study participants reported a wide range of technology-related job titles which were grouped into five categories: Cybersecurity Roles; Information Technology (IT) Roles; Software Development & Engineering Roles; Data Analysis, Cyber Risk, and Business Intelligence Roles; and Other Specialized Roles. The variety of categories is visually represented in the word cloud in Figure 2 below. A list of the job titles is in Appendix A.

Figure 2. Participants' Job Categories

Industry Sectors

In workforce development, classifying organizations by industry sector can help to highlight trends and skill needs by industry. This can provide context to education to help align academic programs and certifications with industry demands. Different sectors require different skill sets, such as cybersecurity in healthcare, where there may be an emphasis on compliance, or finance where there may be more emphasis on fraud prevention and data integrity. Each employer has been classified into sectors of healthcare (9%), finance (13%), government (22%), and technology (56%). The sectors are visually represented in Figure 3 below.

Figure 3. Employers of Participants Categorized by Sector



NICE Work Roles

Job titles and responsibilities can vary across organizations, which can make it challenging to understand the cybersecurity workforce. The NICE work roles help bring clarity and consistency through a list of 52 standardized work roles developed collaboratively by government, industry, academia, with community feedback (NICE, 2025). The top 10 work roles most frequently selected by alumni participants employed in technology are represented in Table 7 below.

Table 7. Top 10 NICE Work Roles for those Employed in Technology

Count	NICE Work Role
74	**Technical Support** IO-WRL-007 Responsible for providing technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational policies and processes.
62	**System Administration** IO-WRL-005 Responsible for setting up and maintaining a system or specific components of a system in adherence with organizational security policies and procedures. Includes hardware and software installation, configuration, and updates; user account management; backup and recovery management; and security control implementation.
54	**Incident Response** PD-WRL-003 Responsible for investigating, analyzing, and responding to network cybersecurity incidents.
45	**Cybersecurity Policy and Planning** OG-WRL-002 Responsible for developing and maintaining cybersecurity plans, strategy, and policy to support and align with organizational cybersecurity initiatives and regulatory compliance.
44	**Network Operations** IO-WRL-004 Responsible for planning, implementing, and operating network services and systems, including hardware and virtual environments.
42	**Vulnerability Analysis** PD-WRL-007 Responsible for assessing systems and networks to identify deviations from acceptable configurations, enclave policy, or local policy. Measure effectiveness of defense-in-depth architecture against known vulnerabilities.
41	**Defensive Cybersecurity** PD-WRL-001 Responsible for analyzing data collected from various cybersecurity defense tools to mitigate risks.
38	**Systems Testing and Evaluation** DD-WRL-007 Responsible for planning, preparing, and executing system tests; evaluating test results against specifications and requirements; and reporting test results and findings.
36	**Cybersecurity Instruction** OG-WRL-005 Responsible for developing and conducting cybersecurity awareness, training, or education.
34	**Threat Analysis** PD-WRL-006 Responsible for collecting, processing, analyzing, and disseminating cybersecurity threat assessments. Develops cybersecurity indicators to maintain awareness of the status of the highly dynamic operating environment.
470	*Total*

Professional Development and Certifications

Preparing to enter the workforce and maintaining employment requires professional development. CAE-CD institutions provide students with professional development opportunities in the form of curriculum, hands-on practical assignments, extra-curricular activities, and preparation for industry-recognized certification exams. Participants were asked about the activities they participated in during their academic program and after graduation.

The field of cybersecurity is continually evolving, and job seekers can validate their knowledge and experience through industry-recognized certifications. Certifications are typically developed in collaboration with industry representatives to ensure that the exams and objectives meet industry expectations for knowledge and skills. Career changers and early-career job seekers may use industry-recognized certifications to break into the cybersecurity workforce. Study participants were asked about the certifications that they had achieved both during and after their academic program.

Participation in Extracurricular Activities

CAE-CD institutions offer a variety of extra-curricular activities to help students prepare for entry into the cybersecurity workforce or advancement in their careers. Study participants indicated that they had experienced a variety of extra-curricular activities during their academic programs. Those employed in technology roles were asked which of the activities contributed to their employment. The majority identified hands-on lab assignments (110) as a top contributor to employment in a cybersecurity role. Course preparation for industry certification was the second most contributing activity (73). Mentor/advising (64) was the third most contributing activity while internships (53) were fourth. Networking and social events (49) ranked as the fifth most contributing activity towards employment in cybersecurity.

Also with mid-range rankings were part-time employment (39), cybersecurity competitions (36), industry certification exam vouchers (36), student clubs (35), capture-the-flag competitions (32), and industry speakers (28). Apprenticeship (11), fellowship (11), dual enrollment (8), and summer camps (3) ranked much lower than the other extra-curricular activities in their contribution towards aiding the participants in becoming employed in a cybersecurity role. The extra-curricular activities experienced by participants is shown in Table 8 below.

Table 8. Extra-curricular Activities Experienced by Participants

Activity	Count
Hands-on labs and/or practical assignments	110
Course preparation for industry certification	73
Mentor/advising	64
Internship	53
Networking and social events	49
Part-time employment/on-the-job training while in school	39

Activity	Count
Cybersecurity competition(s)	36
Industry certification exam voucher	36
Student Club	35
Capture the flag (CTF) competition	32
Industry speakers	28
Apprenticeship	11
Fellowship	11
Pathways/dual enrollment	8
Summer Camp	3

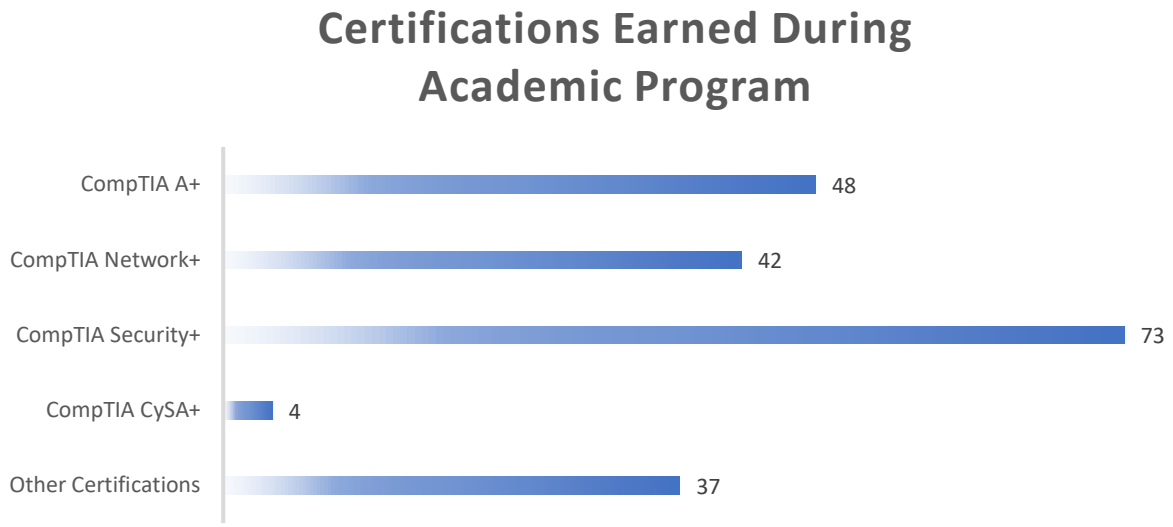
Certifications Earned

Industry-recognized certifications can enhance employability in the field of cybersecurity. Job seekers can demonstrate their readiness for roles and validate their skills beyond education by earning a certification. As noted by CyberSeek (2025), top certifications desired by employers serve as gateways to entry-level, mid-level, and advanced roles within the cybersecurity field. The top certifications highlighted by CyberSeek include ISC2 Certified Information Systems Security Professional (CISSP), ISACA Certified Information Systems Auditor (CISA), IAPP Certified Information Privacy Professional (CIPP), ISACA Certified Information Security Manager (CISM), SANS Global Information Assurance Certification (GIAC), and CompTIA Security+.

This study asked participants to indicate the certifications they had earned during their academic programs and after completion of their academic program. Over half of the study participants indicated that they had earned at least one certification (141 total) at some point in time. Of the participants employed in technology roles, 110 reported to have earned at least one certification. A smaller number of the study participants that were either not employed in technology or were never employed had earned at least one certification (31).

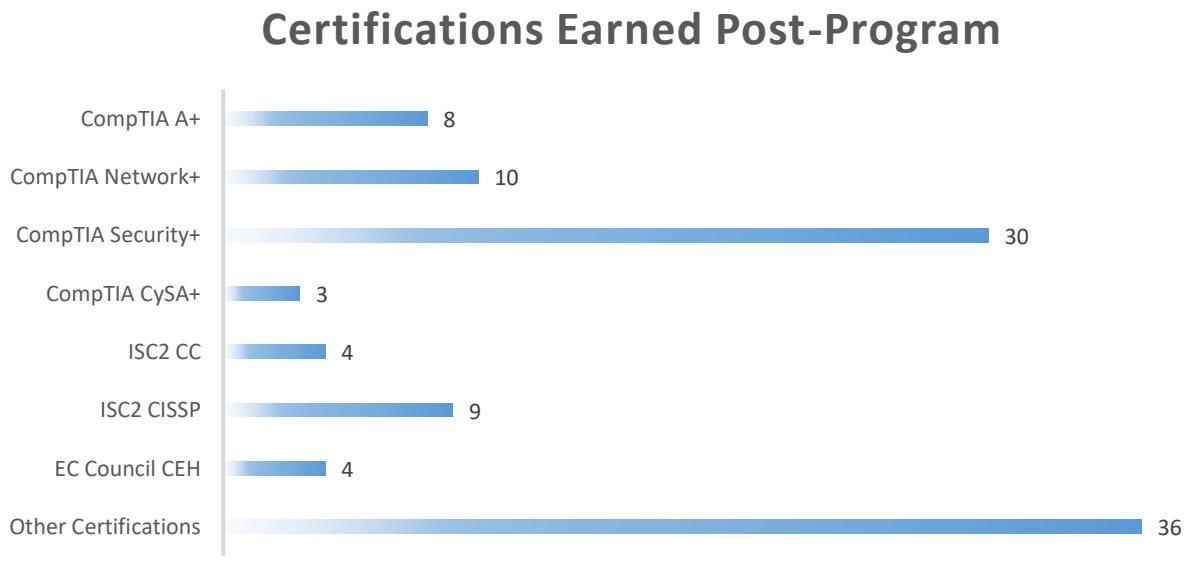
The highest number of certifications earned by study participants during the academic program was CompTIA Security+ at 73, followed by CompTIA A+ at 48, CompTIA Network+ at 42, 37 other certifications, and 4 of the CompTIA CySA+. Like other certifying bodies, CompTIA offers academic discounts to students and higher education institutions. CompTIA also provides learner pathways aligned with specific job roles to help individuals understand which careers their certifications can support. Additional certification types noted as “Other Certifications” included EC Council CEH, ISC2 Certified in Cybersecurity, ISC2 CISSP, and others from AWS and Azure in cloud computing. Alumni also commented that they studied for additional certifications after graduation. Figure 4 below shows the certifications earned by participants during their academic program.

Figure 4. Industry-Recognized Certifications Earned During Academic Program



The highest number of certifications earned by study participants after the academic program was again CompTIA Security+ at 30, followed by CompTIA Network+ at 10, CompTIA A+ at 8, 36 other certifications, and 3 CompTIA CySA+. Additional certification types noted as "Other Certifications" included cloud-based certifications from AWS and Azure, CompTIA PenTest+, Cisco CCNA, ISACA Certified Information Systems Auditor (CISA), Cisco Certified Network Associate (PMP), and a variety of SANS GIAC certifications. Figure 5 below shows the certifications earned by participants after their academic program.

Figure 5. Industry-Recognized Certifications Earned After Academic Program



Post-Program Activities

The ever-evolving nature of the cybersecurity field requires that professionals refine their skills and continue developing new skills to stay current or advance in their careers. The most common post-program activity was employer-provided training (28.8%), followed by education, training, or bootcamps (25.6%) and industry certifications (21.7%), all of which were reported to contribute meaningfully to participants' current roles or promotions in cybersecurity or technology roles. A smaller portion (6.0%) selected "other" activities, while 13.2% indicated they had not participated in any additional training or certification after completing the CAE-CD program.

Participants who selected "Other" activities after completing the CAE-CD program engaged in a diverse range of self-directed and specialized efforts to advance their cybersecurity and technology careers. These included advanced certification preparation such as ICS2 CISSP, ISACA CISA, Cisco CCNA, and CMMC CCP, as well as participation in hands-on training like the Army's Cyber Common Technical Core, DOE Cyberfire, and Tracer Fire workshops. Others enrolled in graduate programs in security, cloud computing, or computer science, while many pursued independent learning through Coursera, online research, and personal projects. Practical skills were also developed through IT support roles (e.g., helpdesk, desktop/printer repair, financial aid security) and participation in cybersecurity competitions. Several noted that internships and automation-related work helped open doors to further career advancement. Table 9 below highlights the professional development activities that participants were involved in after their academic program.

Table 9. Post-Graduation Activities of Participants

Alumni Participation in Post-Graduation Activities	Count	Percentage
Education, training, and/or bootcamps	72	25.6%
Employer-provided training	81	28.8%
Industry certification(s)	61	21.7%
None of the above	37	13.2%
Other	17	6.0%

Academic Program Impact on Employment

It is essential to evaluate the impact of academic programs, including the measurable outcomes and broader effects on students, the cybersecurity workforce, and society. Key indicators included in this section are the frequency that students experienced practical or hands-on lab assignments and the effect on their employment, the impact the academic program made overall on their current employment position, and the effects the academic program had on their employment.

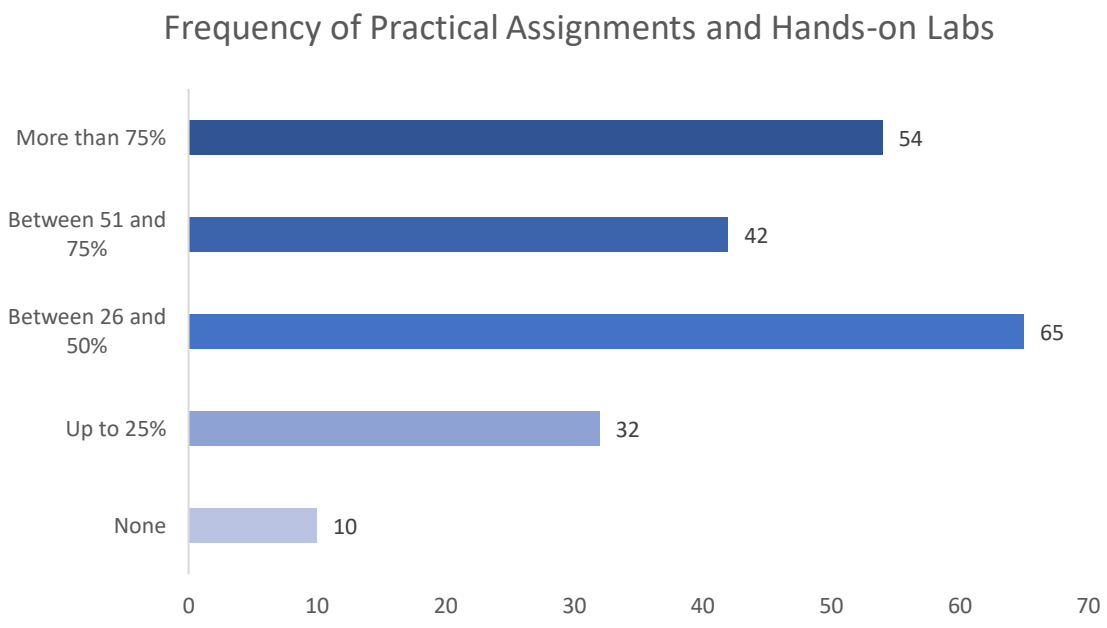
Frequency of Practical Assignments

Practical assignments are vital to any cybersecurity program to ensure job readiness and build student confidence in industry tools and methodologies. Practical assignments ensure that job seekers entering the cybersecurity workforce are ready to protect systems and contribute meaningfully on day one. There was somewhat of a balance between the groups that experienced practical assignments and hands-on labs as part of their academic program. Nearly one-third of the participants (31.1%) reported to have experienced practical assignments and/or hands-on labs 26-50% of their studies. Over one-fourth (26.9%) of the participants reported to have experienced practical assignments and/or hands-on labs in more than 75% of their studies. Other participants reported to have experienced practical assignments 51-75% of the time. While 5.2% reported not to have experienced any practical assignments in their academic program. Table 10 and Figure 6 below show the details of the frequency of practical assignments and hands-on labs.

Table 10. Frequency of Practical Assignments and Hands-on Labs

Frequency of Practical Assignments and Hands-on Labs	Count	Percentage
More than 75%	52	26.9%
Between 51 and 75%	40	20.7%
Between 26 and 50%	60	31.1%
Up to 25%	31	16.1%
None	10	5.2%

Figure 6. Frequency of Practical Assignments and Hands-on Labs



Effect of Practical Assignments on Employment Position

Practical assignments and real-world simulations play a pivotal role in influencing employment outcomes for students in cybersecurity and related technology fields. Academic programs frequently dedicate resources to prepare students for the workforce through the development of practical assignments and hands-on labs to give students the opportunity to develop skills with tools used by industry. For those employed in technology roles, the largest portion of participants (39.1%) said that the practical assignments experienced in their academic programs had a major effect on their current employment position. Next, 33.8% reported a moderate effect. While only 7.9%, 11.9%, 6.0%, and 1.3% reported a minor effect, neutral, no effect, or not applicable, respectively. Table 11 below shows the effect of practical assignments on the participants' employment positions.

Table 11. Effect of Practical Assignments on Employment Position

Effect of Practical Assignments on Employment Position	Count	Percentage
Major effect	59	39.1%
Moderate effect	51	33.8%
Minor effect	12	7.9%
Neutral	18	11.9%
No effect	9	6.0%
N/A	2	1.3%

Impact of Education on Employment Position

CAE-CD institutions play a critical role in preparing students for careers in the cybersecurity workforce by offering structured and comprehensive education pathways. These pathways are designed to include rigorous curriculum aligned with work roles, extracurricular activities, and professional development opportunities to equip students with both the technical knowledge and practical skills needed to address real-world cyber threats. Participants of the study were asked how much their education contributed to their current employment position.

Nearly half of the participants said their academic program made a very significant contribution (46.8%) to their current employment position and more than one-fourth reported it made a significant contribution (26.0%). Others noted that their academic program made some contribution (18.5%) while smaller numbers of participants reported that it made a slight contribution (4.0%) or no contribution (4.6%). Table 12 below presents a breakdown of the impact of education on the participants' employment position.

Table 12. Impact of Education on Employment Position

Impact of Education on Employment Position	Count	Percentage
Very significant contribution	81	46.8%
Significant contribution	45	26.0%
Some contribution	32	18.5%
Slight contribution	7	4.0%
No contribution	8	4.6%

Effect of Academic Contribution on Employment Position

Education can have a transformative effect on shaping individual career paths. By equipping learners with the technical knowledge and skills to be workforce-ready, education serves as a key driver of employability. Participants of the study reported that their academic programs contributed to their employment position in meaningful ways, such as receiving an increase in salary (42.2%), receiving a promotion (28.4%), being hired into a technology position (11.8%), making a career change (5.9%), moving from a lead to an expert role (2.5%), from a technician to a leadership role (6.9%), or other advancement (6.9%). Table 13 below shows the effects of academic contribution on participants' employment position.

Table 13. Effects of Academic Contribution on Employment Position

Effects of Academic Contribution on Employment Position	Count	Percentage
Increase in salary	86	42.2%
Promotion	58	28.4%
Hired into Technology Position	24	11.8%
Career Change	12	5.9%
From Lead to Expert	5	2.5%
From Technician to Leadership Role	14	6.9%
Other Advancement	14	6.9%

Concluding Remarks

Beyond individual outcomes, CAE-CD programs contribute to addressing national workforce gaps by producing qualified professionals equipped to meet the growing and evolving cybersecurity threats. Study participants emphasized the value of faculty support, extracurricular activities, and industry certifications towards their ability to gain employment in the field of cybersecurity. A few indicated that lack of work experience continues to be a barrier to entry into the workforce. Some participants indicated that internships and apprenticeships during their educational journey could help to reduce those barriers to entry while some others indicated the need for more labs and practical experiences while enrolled in higher education programs.

To build on current findings and consider the continually evolving needs of the cybersecurity workforce, it is recommended that a follow-on study be conducted every three to five years. These future studies would provide critical insights into the effectiveness of cybersecurity education, workforce alignment, and emerging talent needs. As the cybersecurity workforce continues to evolve to include career changers and those from different backgrounds and the higher education community continues to adapt to support student needs, this will likely shift the expectations and skills needed for entry into the cybersecurity workforce.

References

CAE in Cybersecurity Community. (2025, April). *2025 CAE in Cybersecurity Symposium - Refereed Proceedings – CAE in Cyber Defense (CD) Track.* Retrieved from CAE Symposium - CD Program Committee: https://caecommunity.org/sites/default/files/2025-03/20250324_2025CAESymposiumProceedingsCDTrack.pdf

CyberSeek. (2025, May). *Hack the gap*. Retrieved from CyberSeek: https://www.cyberseek.org/heatmap.html

FBI IC3. (2025, April 23). *Federal Bureau of Investigation Internet Crime Report 2024.* Retrieved from Internet Crime Complaint Center (IC3): https://www.ic3.gov/AnnualReport/Reports/2024_IC3Report.pdf

ISC2. (2024, October 31). *ISC2*. Retrieved from 2024 ISC2 Cybersecurity Workforce Study: https://www.isc2.org/Insights/2024/10/ISC2-2024-Cybersecurity-Workforce-Study

ISC2. (2025, March 6). *Survey: Women Comprise 22% of the Cybersecurity Workforce*. Retrieved from ISC2: https://www.isc2.org/Insights/2025/03/Women-Comprise-22-percent-of-the-Cybersecurity-Workforce#

ITRC. (2025, January 28). *Identity Theft Resource Center's 2024 Annual Data Breach Report Reveals Near-Record Number of Compromises and Victim Notices*. Retrieved from Identity Theft Resource Center (ITRC): https://www.idtheftcenter.org/post/2024-annual-data-breach-report-near-record-compromises/

NCES. (2025). *National Center for Education Statistics (NCES) Summary Tables*. (Institute of Education Sciences) Retrieved from Integrated Postsecondary Education Data System (IPEDS): https://nces.ed.gov/ipeds/SummaryTables/

NICE. (2025, May). *NICE Framework: Current Versions*. Retrieved from NICE Framework Resource Center: https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center

NICE. (2025, January). *Occupations, Jobs, and Work Roles*. Retrieved from NICE Framework Resource Center: https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/resources/occupations-jobs-and-work

Sands, J., & Sande, C. (2019). *2019 Workforce Study: Community College Cybersecurity Alumni.* Retrieved from NCyTE Center: https://www.ncyte.net/home/showpublisheddocument/10/637896711130970000

Symantec. (2025, February 20). *Ransomware 2025: Attacks Keep Rising as Threat Shows its Resilience*. Retrieved from Symantec Enterprise Blogs / Threat Intelligence: https://www.security.com/threat-intelligence/ransomware-trends-2025

Appendix A

Job Titles

Cybersecurity Roles

Application Security Engineer
Assistant Professor in Cybersecurity
CERT Cyber Mission Readiness Intern
Chief Information Security Officer
Cloud Security Analyst
Cloud Security Engineer
Computer Forensic Analyst 2
Cyber Defense and Readiness Consultant II
Cyber Software Engineer
Cybersecurity Administrator
Cybersecurity Analyst
Cybersecurity Analyst IV
Cybersecurity Contractor (C-SCRM)
Cybersecurity Defense Operations Analyst 2
Cybersecurity Engineer
Cybersecurity GRC Analyst
Cybersecurity Lab Assistant
Cybersecurity Network Defense Analyst
Cybersecurity Researcher
Cybersecurity SOC Analyst II
Cybersecurity Specialist
Director of Digital Forensics Services
Financial Services Specialist II (Cybersecurity)
Governance risk and compliance analyst
Information Security Administrator
Information Security Analyst
Information Security Analyst Intern
Information Security Engineer
Information Security Manager
Information Security Officer
Information System Security Officer / Cybersecurity Analyst
Instructor, Cybersecurity
Lead Cyber Security Engineer
Network Administrator / Information Security Officer
Network/Systems Supervisor - Security Officer
Operational Computer Systems Analyst
Penetration tester
Principal Cyber Systems Engineer
Risk and Security Analyst III
Security Administrator
Security Analyst
Security Analyst I
Security Engineer
Security Research Engineer
Security Resource Associate 1
Senior Cybersecurity Consultant
Senior Data Security and Compliance Engineer
Senior Incident Response Consultant
Senior Information Security Analyst (Tier 2)
Senior Security Engineer
Senior Security/Access Control Specialist
Senior Threat Intelligence Analyst
SOC Analyst
SOC Lead
Sr. IT security engineer/Project Manager
Sr. Security Engineer
Staff Product Security Engineer
Supervisor - Governance, Risk & Compliance | Global Cyber Security
Threat & Vulnerability Analyst
Threat Detection Engineer
Watch Officer

Information Technology (IT) Roles

ADC engineer
Assistant Director of Information Technology
Associate Incident Response Consultant
Associate Infrastructure Engineer
Auditor II
Boot Technician
Branch Chief
Chief Technology Officer
Cloud Engineer

Cloud System Administrator
Computer Technician
Contractor (Network Engineer 1)
Control Lead
Critical Infrastructure Risk Analyst
Customer Service Representative
Database Administrator
DCO manager
Education IT
Engineer, Field Engineering (IGA, PAM, TPAG)
Enterprise WAN Operation Technician
Escalation Engineer
Export control analyst, cyber and semiconductors
Field Technician
Head of IT & Facilities
Help Desk Security Analyst
Ic2
Implementation Consultant
Implementation Engineer I
Incident Manager
Info Security Associate
Information Systems Worker
Information Technology Auditor
Information Technology Management
Information Technology Specialist
Information Technology Support Specialist
Integration Admin
Intelligence Analyst
Intern
IT administrator
IT Assistant
IT Auditor
IT Compliance Analyst
IT Director
IT Help Desk Employee
IT Helpdesk Support
IT intern
IT Project Manager
IT Recruit
IT Security Analyst
IT Software Engineer
IT Specialist
IT Supervisor
IT Support Analyst (Level 2)
IT Support Specialist
IT Support Technician I
IT Technical Support (internship)
IT/Facilities Specialist
Jr. Network Engineer
Lab Technician 1
Lead Microbiologist
Logistics Management Specialist III
Managed Services Engineer
Manager
MDR Analyst
NetDevOps Engineer
Network Engineer
Network Specialist
Network Specialist III
Network Tech
Owner
Paracompliance Support Specialist
PC Network Technician II
PT Computer Support Technician I (MIS)
Sales
Scenic Technician Contractor
Senior Cloud Engineer Space Systems
Senior Manager of Engineering
Senior Network Engineer
Senior Windows Administrator
Service Desk Analyst
Service Desk Analyst
Service Desk Technician
Service Manager
System Admin
System Administrator
Systems Administrator
Systems Administrator (IT Specialist)
Systems Analyst
Systems Engineer
Systems Support Analyst II
TCSR
TEAM LEAD
Technical Consultant
Technical Lab Consultant
Technical Support Associate II

Technology Support Specialist
Technology Support Technician
Windows and Linux System Administrators

Software Development & Engineering Roles
Application Developer
Artificial Intelligence (AI) Data labeling Technician
Platform Architect
Robotic Process Automation Developer
Senior Software Engineer
Software Developer
Software Engineer
Software Engineer 2
Software/Data Engineer
Tester 1
Tools & Automation Engineer

Data Analysis, Cyber Risk, and Business Intelligence Roles
Business Intelligence Data Engineer Contractor
Business Product Advisor
Data Analyst
Financial Planning & Analysis
Management and Program Analyst
Risk Examiner
Senior Analyst
Staff analyst

Other Specialized Roles
Adjunct Instructor
Biomedical Cybersecurity Analyst
Brand technical sales specialist
Conductor (not in tech role)
Credit Analyst
Director
Education IT
Grad Student (2nd masters)
Graduate Research Assistant
HR Director
Medical Receptionist
Owner
Police Sergeant
Producer/Podcast Co-Host
Professional Expert (Contract Work)
Security Engineer II
Specimen Management
Student Assistant
Student Assistant (Enterprise Network Solutions)
Substation Electrician
Substitute Teacher
Unarmed Security Guard

Appendix B

Employer Names

Government
Army
ATF
CISA
Defense Information Systems Agency
Department of Air Force
Department of Defense
Department of Transportation
DHS Cybersecurity and Infrastructure Security Agency
DOD DTSA
Federal Aviation Administration
FDIC
Naval Nuclear Laboratory
New York State Department of Financial Services
New York State Office of Information Technology Services
New York State Police
ND IT
NYS Government
Office of Inspector General, Social Security Administration
Office of Personnel Management
State Board
State of California
State of Mississippi
State of North Dakota
United States Coast Guard Cyber Command
US Department of Agriculture Food Safety & Inspection Service
USAF Civilian Service
USMC
City of Anaheim
City of Arvada
City of Atlanta
City of Dallas
City of Griffin
City of Philadelphia Controller's Office
San Bernardino County Sheriff's Department
Charlotte County Sheriff's Office
Municipality in Wyoming

Finance
Abacus LLC
ABR Employment Services / Sentry Credit Union
American Express
American Pride Bank
CitiCorp
Capital Group
Discover Financial Services
Equifax
First Citizens Bank
First International Bank & Trust
First United Bank of North Dakota
Jefferson Capital Systems, LLC
JP Morgan Chase
Navy Federal Credit Union
Citizens Business Bank
Wells Fargo
Visa
Visa Inc
Unum
Markel Corp
The Bonadio Group
Public Employee Retirement System of MS

Healthcare
Banjo Health
Evergreen Goodwill
Houston County Public Library System
Humana
Labcorp
Longeviti Neuro Solutions
PeaceHealth
Piedmont Healthcare
Progyny Inc

Protenus Inc
Puerto Rico Medical Services-Health care
local government
Rehab Therapy Partners
Temple University Health System
Wellstar MCG
ShiftMed

Technology
22halomedia
Accenture
Acorn Technology Services
ADI
Affordable Computers
Amazon
Apple
AT&T
ATOS/Eviden
AWS
Bear Technologies
BMC Software
Booz Allen
Brooksource
Buchanan Technologies
Business Communications Inc.
C Spire
CACI
Cardone Training Technologies
CCCS
CDW
Cisco Talos
Clearwater Analytics
Core Group Inc
Costco Wholesale
CrowdStrike
CSA
CSG International
Cutsforth
DAT
Engineered Transportation International
Ennovar | Spirit Aerosystems
Epic Games
EW Scripps Company
Exact Staff
Express Employment International
Five9
Fortreum, LLC
Fusion Risk Management
Gainwell Technologies
Garmin
GEA Group
General Data
General Data Tech
General Motors
Google data center
Hacker Valley Media
Halvik
IBM
Idaho National Laboratory
iVenture Solutions, Inc.
Jackson Municipal Airport Authority
JD Finish Line
Kenny's Construction
Knight Communications
Koch Industries
Kyndryl
Lawrence Livermore National Laboratory
Los Angeles County, Internal Services
Department
Mandiant, Part of Google Cloud
Mattermost
Micron Technology
NexusTek
Nordic Consulting Partners
Northrop Grumman
Oracle
Palo Alto Networks Unit 42
Peraton
Quality Technology Services
Raytheon
ReliaQuest
Rocket EMS
Rocket Lab USA
Saviynt
Seek Now
Semperis
Simpson Strongtie
Skyward IT

Software Engineering Institute | Carnegie Mellon University
Southwest Research Institute
Swan Bitcoin
Swire Coca-Cola
TekSynap
Teksystems (Radian)
Tier 2 Technologies
Unit 42 at Palo Alto Networks
WebstaurantStore
Weg Electric Corporation
Williams Consulting
XOtech, LLC
Yum! Brands
Zelis
Zillow Group
Zoll Itamar
Zoom Communication