UofL COLLEGE OF EDUCATION & HUMAN DEVELOPMENT

C4 PROJECT

CYBERSECURITY CERTIFICATIONS, CAREERS AND COMMUNITIES PROJECT

The University of Louisville
Louisville, Kentucky

In partnership with:
KENTUCKY COMMISSION ON MILITARY AFFAIRS KCMA

Cybersecurity, Certifications, Career and Communities Training Program

Gap Analysis Report

June 2020

Dr. Jeffrey Sun, Principal Investigator
Dr. Jason Gainous, Lead Researcher

This study was prepared under contract with the Commonwealth of Kentucky, with financial support from the Office of Economic Adjustment, Department of Defense. The content reflects the views of the Commonwealth of Kentucky, and does not necessarily reflect the views of the Office of Economic Adjustment.

Image by Joseph Eddins via dvidshub.net

Cybersecurity, Certifications, Career and Communities Training Program Gap Analysis Report. June 2020. By Dr. Jeffrey C. Sun and Dr. Jason Gainous

College of Education & Human Development
University of Louisville © 2020
Louisville, Kentucky

Cover designed by Sarah Gossett, Kentucky Commission on Military Affairs
Cover image by Joseph Eddins via dvidshub.net

This report was made possible through grant funding of the Office of Economic Adjustment, Department of Defense. This work was supported under Federal Award HQ00052110003 and OEA award ST0924-20-03.

The authors would like to express their gratitude to the Kentucky Commission on Military Affairs for sponsoring this project and to the following collaborators whose insight made this report possible (in alphabetical order):

Brig. Gen. Steven P. Bullard, USAF Retired
Dr. Adel Elmaghraby
Jana Godwin
Dr. Jeffrey Hieb
Dr. Dallas Kratzer (Lt. Col., USAF Retired)
Lt. Col. Thomas Krupp, USA Retired
Dr. Adrian Lauf
Prof. Michael Losavio
Ms. Stacey Shane

C4: Cybersecurity, Certifications, Career and Communities Training Program Gap Analysis Report

Contents

1 Introduction to the Report - Motivation, Data and Design, and Summary Results

1.1 Motivation

In partnership with the Kentucky Commission on Military Affairs (KCMA), the University of Louisville (UofL) presents this Gap Analysis Report, commissioned by the Office of Economic Adjustment (OEA) in the Department of Defense (DoD) as part of its Phase III grant that funds the Cybersecurity, Certifications, Career and Communities (C4) Project. The primary purpose of the grant is to help develop industry-legitimized learning into DoD career pathways drawing heavily on service members, veterans, and their dependents. The purpose of the analyses in this report is to inform the development of a training program aimed at achieving this primary purpose.

We collected data to identify where other regionally based cybersecurity training programs may fall short of offering the requisite training for the types of cybersecurity certifications that most potential regional employers are seeking. Additionally, with the goal of offering a more holistic training program that offers participants more than just certification training, we use machine coding to examine cybersecurity job postings to identify skills additional to those included in common certifications that we could incorporate in our curricular design. The scope for this report includes the majority of employers in the Ohio Valley region, and every comparable online cybersecurity training program that we could find. The results here are being used to inform and legitimize our curricular design. Specifically, these results are shaping the content, preparation, and certifications that will define our program.

It is important to be clear here that this entire gap analysis was guided with some prior assumptions about our target market of students. Most importantly, we are confident that the bulk of our students will be beginners to cybersecurity, or at the least, early in their careers with limited training. All of the analysis that follows views the results through that lens. This means that, while the data may show that the highest levels of experience, education, training, and certification may be the most common requirements sought by potential employers, the aim of this gap analysis is to identify those certifications and skill sets that will most benefit students earlier in their careers. Of course, ultimately, we also seek to help them build the requisite foundation to attain the highest level of qualifications.

1.2 Data and Design

The data collection involved stages and multiple sources. Before collecting the data, we started out by determining which certifications fit within the scope of those approved by the DoD directive for which this grant is a part (DoD Directive 8570), and then the team winnowed that list to those certifications known to be the most relevant in the profession currently. This process yielded a total of ten certifications. They are as follows:

- CompTIA Advanced Security Practitioner (CASP+)
- Cisco Certified Network Associate (CCNA)
- Certified Ethical Hacker (CEH)
- Certified Information Systems Auditor (CISA)
- Certified Information Security Manager (CISM)
- Certified Information Systems Security Professional (CISSP)
- Cybersecurity Analyst Certification (CySA+)
- GIAC Certified Incident Handler (GCIH)
- Network+
- Security+

Then we used the most popular employment site and search engine, Indeed.com, to identify cybersecurity job postings in Illinois, Indiana, Kentucky, Ohio, and Tennessee (the Ohio Valley Region). This search in late April/early May identified 1097 unique job postings. We collected the job title, the company name, the job description, the job requirements, and the job location. From there, we created dummy variables for of the certifications above (0 = not included in the job requirements, 1 = included in the job requirements). We also created a dummy variable representing whether a college degree was required (0 = not required, 1 = required). Next, we constructed an ordinal indicator of the required experience (0 = less than one year, 1 = one to two years, 2 = three to four years, 3 = five years or more). Finally, we created a dummy variable flagging those job postings that mentioned the DoD assuming that these jobs are most likely DoD contractors (although this does not mean that those postings not explicitly mentioning the DoD are not defense contractors).

We begin by offering a descriptive picture of the job postings to offer a general sense of the market/climate. Much of the analysis in this report is based on subsample comparisons of those data mentioning the DoD or security clearance (assuming these are also DoD contractors) in their job postings and those that do not. The presumption is that DoD contractors may seek different qualifications and skill sets than those organizations primarily servicing the private sector. The initial description includes counts of the number of jobs by state in our data, the number of jobs by required levels of experience, and a count of the number of jobs by the expected level of education. This initial analysis is intended to provide background context to frame the inferential analyses that follow. Next, we examine the distribution of required certifications across these job postings. Here, too, we look at the conditional distributions of these certifications across required experience and education. Given that our target market is mostly beginners and early career cybersecurity specialists, these conditional distributions give us information on which certifications are most frequently required for this target market. Again, we execute all of these analyses for subsets of the data (those data where the DoD is mentioned in the job posting, and those data where it is not).

We follow this descriptive analysis by examining the bivariate correlations between certification postings. This gives us information on which certifications tend to be paired together in singular job postings. This is particularly helpful for making strategic curricular choices when viewing these results through the lens of those preceding conditional distributions. Simply, we can determine which certifications are most frequently requested first, especially for entry level positions, and then narrow that down by seeing which ones pair together. This would give our students the best competitive edge. We extend this bivariate analysis by estimating a multivariate model of inclusion of Security+ (the most commonly requested entry-level certification) as a function of the other most commonly requested entry level certifications (CCNA and CEH), experience requested, education requested, the total number of certs requested, and whether the posting was coming explicitly from a DoD contractor.

Because our intent here is to offer a more holistic training program than that offered by those competitors who simply offer certification training, we decided to take the inferential analysis a step further looking beyond certifications. We do so by using machine coding to analyze the words used in the job postings. Here we performed two types of content analysis. The first is descriptive, where we measure the most common words used in the job *requirements* after eliminating "stop words" (commonly used words such as "the", "is", "and", etc.). This allows us to pick up on requirements additional to standard certification, experience, and education that employers may seek. Here, to dig down even further, we look for differences across those postings mentioning the DoD or security clearance and those that did not.

The second type of content analysis, and perhaps most nuanced analysis we execute in this report, we turn to latent variable models capable of capturing topical structure across observed words. More specifically, we use Latent Dirichlet Allocation (LDA), a method of latent topic analysis, to identify sets of words that characterize different "topics" within the corpus of job *requirements* in the job postings. Latent topics from a topic analysis are akin, in analytical spirit, to latent dimensions from a factor analysis or principal components analysis. Given that these job descriptions are all centered on cybersecurity jobs, we expect a small number of latent dimensions – systematic sources of variance – to underwrite these postings. Capturing the general substantive topics that come up in these postings, though, allows us to employ more of our data than word-level analyses, and in a more parsimonious way. It is important to note here that the corpus we use here is based on the job descriptions, not the job requirements we used to measure expected certification, education, and experience. Our aim here was to pick up on some of the skills sought that go beyond the certifications. This way we can integrate learning on these skills into the curriculum while also giving training for those certifications we identify as important.

Next, we looked at certification pass rates to assure that those we identified above were good strategic choices for our program focus. These data are difficult to come by, but we were able to identify multiple reliable sources.

Finally, we performed an exhaustive internet search to identify all online cybersecurity training programs that would potentially be competitors to our program. We identified 111 programs nationally. We collected data on each coding for which certifications they offer training, cost for their program, whether the course is taught by an instructor or it is self-guided, and we searched for whether they explicitly offered training as part of their certification program for the more holistic and nuanced skill sets we identify in the above described analysis.

1.3 Summary Results

We detail the results of all of the analysis in the sections that follow, but before doing so, the following key takeaways are summarized here. They are as follows:

- Most cybersecurity job postings do not explicitly mention the DoD or the requirement for a security clearance.
- The jobs are concentrated in populous states and those with military bases.
- Most jobs require significant experience but there are many entry-level positions. There are fewer entry-level positions, though, in those jobs from DoD contractors.
- While CISSP (an advanced certification) is the overall most requested certification, Security+ is a close second. This is especially true for those postings from DoD contractors.
- Security+ is requested by DoD contactors very frequently for entry-level positions, and at a higher proportion than employers that are not explicitly DoD contractors.
- Security+ is requested by DoD contactors very frequently for those jobs not requiring a bachelor's degree, and at a much higher proportion than employers that are not explicitly DoD contractors.
- CCNA and CEH are generally second and third most commonly requested certifications and tend to conform to the same conditional patterns described for Security+.
- Postings requesting CCNA and CEH are considerably more likely than not to also ask for Security+. This relationship holds up in a controlled model among those postings coming from DoD contractors.
- The bulk of the competitor training programs come from a few private sector programs and the duration of the courses ranges from 3-7 days.
- There are many training program offerings for Security+ and CEH, but we only identified one online (non-open source) program offering CCNA.

- The average price for all programs is $2610, for Security+ it is $2177 (but the distribution is skewed a bit toward the less expensive side), for CEH the average is $3007, and the CCNA program costs $4223.

- Most Security+ and CEH programs are offered by a live instructor versus self-guided, a few offer both, and the CCNA program has a live instructor.

- Self-guided programs are significantly less expensive than those with live instructors, but are still costly ($1556 on average).

- Over 60 percent of the total programs offer a voucher to take the associated certification exam, less than half of the Security+ programs offer a voucher, nearly 80 percent of the CEH programs offer a voucher, and the CCNA program does offer a voucher.

- The descriptive content analysis suggests that familiarity with the NIST and RMF cybersecurity frameworks is commonly expected in DoD contractor jobs.

- An understanding of Microsoft, Microsoft Azure, and Python is commonly preferred among DoD contractor job postings.

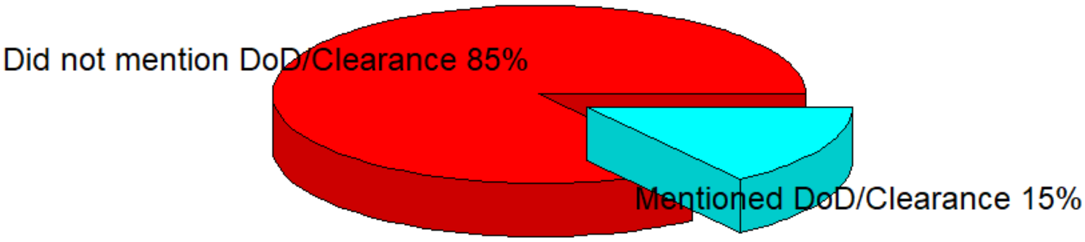
- The inferential content analysis (topic modeling) consistently highlights a set of common general expectations among applicants that DoD contractors expect including an understanding of infrastructure, network security, risk management, and they clearly expect certifications.

Based on these results, the report recommends that we focus the C4 training program on Security+, CCNA, CEH, with layered training in Microsoft tools including Azure, Python, and the soft skills identified in the inferential topic models.

2 A Description of the Cybersecurity Job Postings

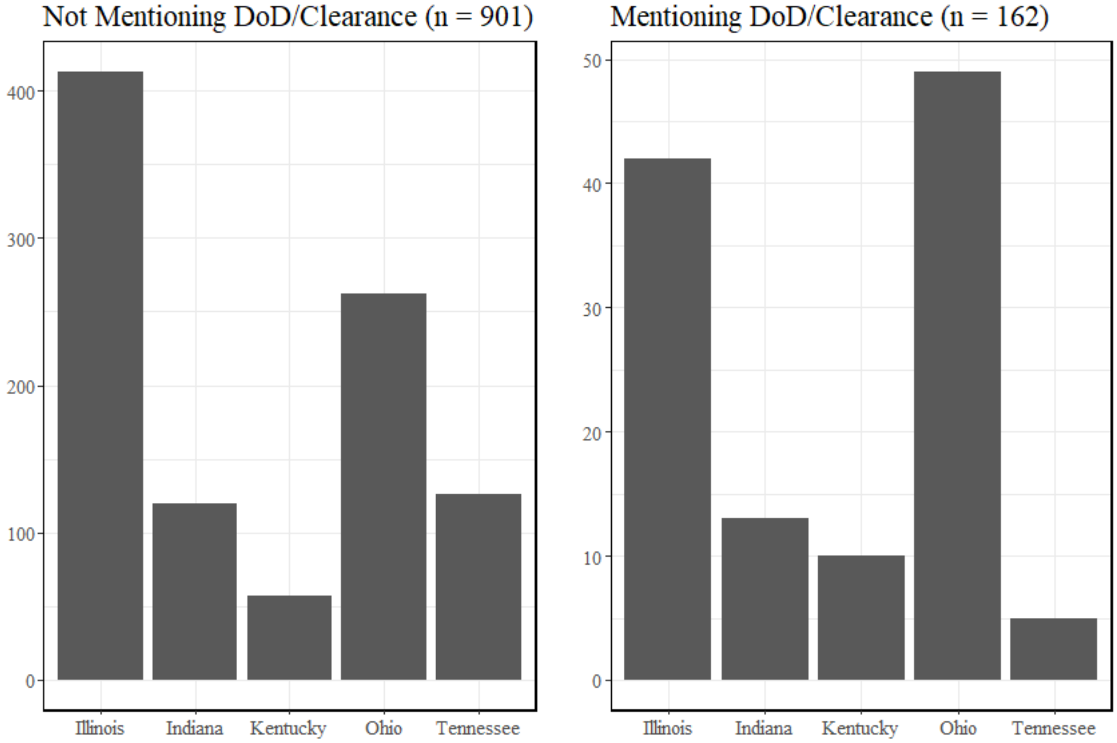
2.1 DoD Contractors versus Private Sector Jobs

Figure 1: Percentage of Jobs mentioning the DoD in their Posting



Clearly, most job postings do not mention the DoD or security clearance (again we are assuming that including either of these indicates that the employer is most likely a DoD contractor) in their job description or requirements - 85% (see Figure 1). That said, it is important to note here that exclusion of DoD mention does not necessarily mean that the company is not a DoD contractor. On the other hand, mention of the DoD essentially guarantees that they are. Here, the 15% represented in Figure 1 is nothing to scoff at. Remember that the data include 1097 job postings. As such, around 162 jobs mentioned the DoD.

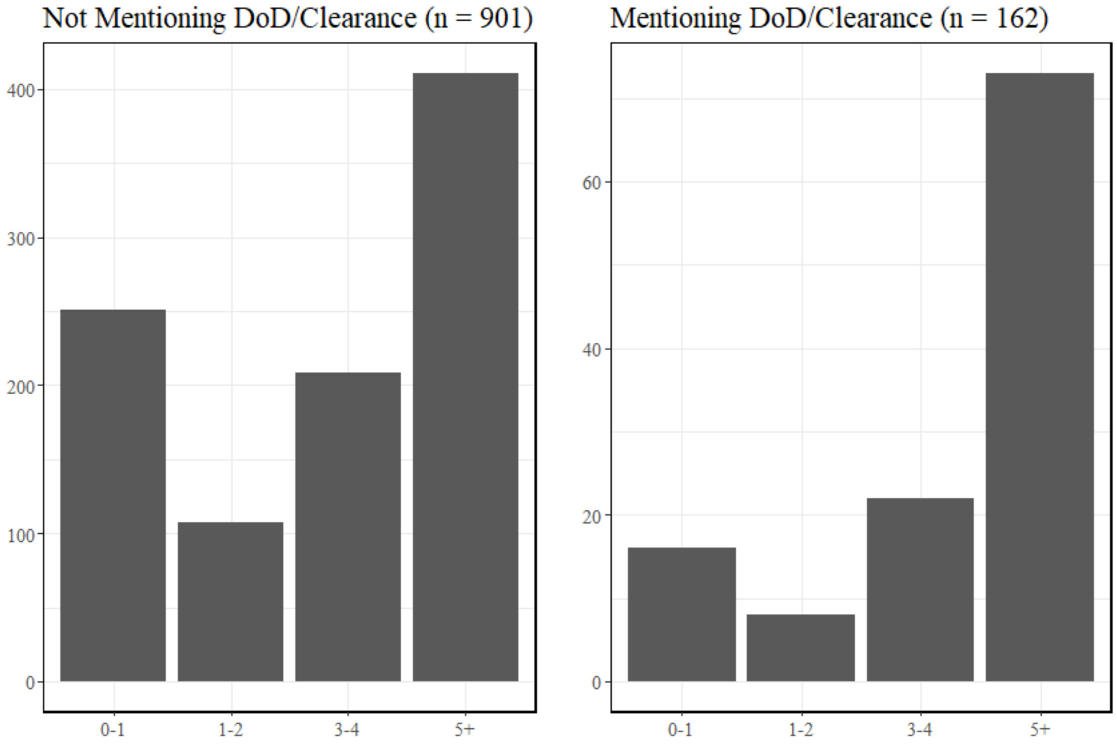
Figure 2: Number of Cybersecurity Job Postings by State across DoD/Clearance Mention



2.2 Jobs by State

There are several inferences that can be drawn from the conditional distributions presented in Figure 2. To begin, the majority of jobs overall are in Illinois. This is not surprising given the population of the state, and in Chicago particularly. That said, there are actually more jobs in Ohio than in Illinois among those jobs mentioning the DoD or security clearance which is not surprising given that Wright-Patterson Air Force Base is there. Given that we will likely draw many of our students from Kentucky, and many of those jobs in Ohio are closer to Kentucky than most of the jobs in Illinois, this could be advantageous for the placement of our students. The only other distributional difference across jobs mentioning or not mentioning the DoD or security is it seems that, proportionally speaking, there are many fewer job posting in Tennessee for those posting mentioning the DoD/clearance relative to those not mentioning the DoD or security clearance.

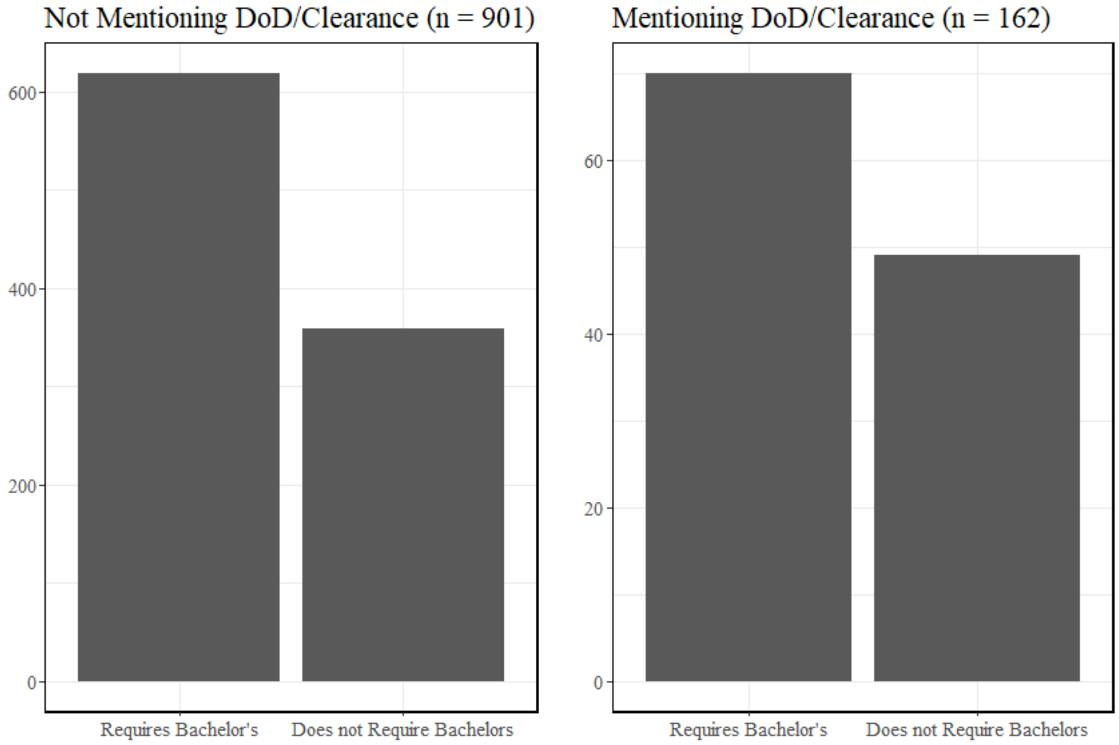
Figure 3: Number of Cybersecurity Job Postings by Expected Years Experience across DoD/Clearance Mention



2.3 Jobs by Expected Experience

The distinction between the graphs in Figure 3 show data discrepancies in terms of prior years of experience. When comparing the conditional distributions of job postings by expected years experience, it is clear that proportionally speaking there are significantly more entry level positions for those jobs not mentioning the DoD or security clearance. This is something that we definitely need to consider, both when shaping our curriculum and when recruiting students.

Figure 4: Number of Cybersecurity Job Postings by Expected Education across DoD/Clearance Mention



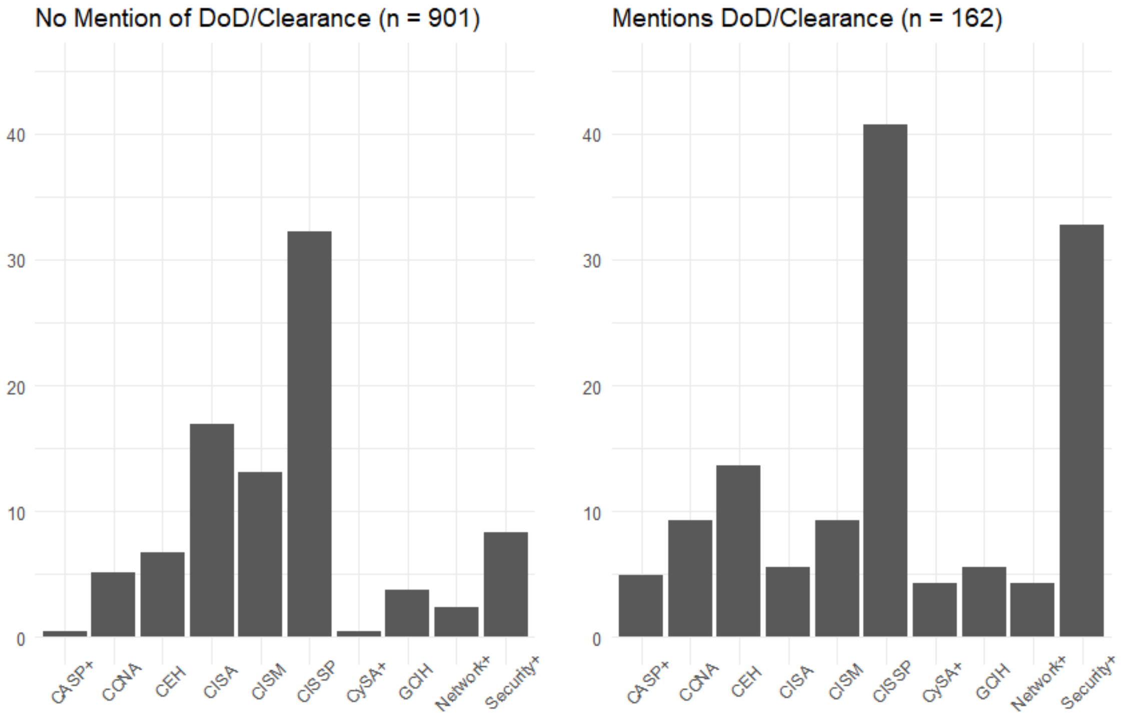
2.4 Jobs by Education

Clearly in Figure 4 most employers, regardless of whether they mention the DoD in their posting, require at least a bachelor's degree. That said, it is quite encouraging for our program that the number of jobs not requiring a bachelor's degree is quite substantial. Further, the proportional number of jobs not requiring a bachelor's degree relative to those who do is considerably closer for potential employer's mentioning the DoD/clearance in their postings.

3 Descriptive Analysis of Certifications Most Requested by Cybersecurity Employers

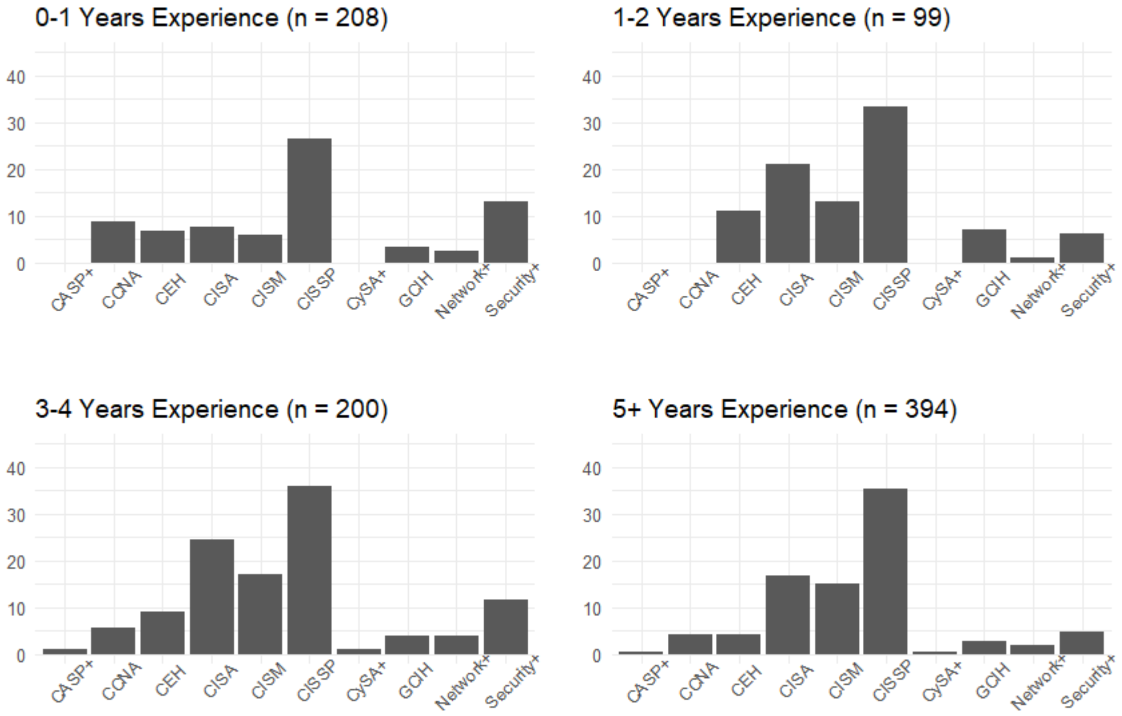
3.1 Most Common Requested Certifications

Figure 5: Full Data: Certification Mentions in Job Postings across DoD/Clearance Mention (% of Total Postings)



Moving beyond the context/background information in Section 1, the analyses presented in this section get directly at which certifications may best suit our target market. The distributions of requested certifications presented in Figure 5 paint a clear initial picture. To begin, it seems that CISSP is clearly the most requested certification across jobs postings mentioning the DoD/clearance and not. As mentioned above, and also as will become clear in the more granulated analysis that follows below, CISSP is a certification required by senior level positions and requires quite a bit of experience before even being qualified to test for it. The more interesting result for our purpose here is in the clear distributional differences across postings mentioning the DoD and those that do not. For instance, Security+ rivals CISSP in requests for those jobs mentioning the DoD/clearance while it is not even the second most requested certification for those postings not mentioning the DoD. Next, the third most frequent certification requested for postings mentioning the DoD/clearance is CEH. This is particularly promising given that it is one of the newer certifications meaning that it is likely that there will be fewer job applicants with this certification as well as fewer

Figure 6: Across Requested Experience: Certification Mentions in Job Postings for Postings not mentioning DoD/Clearance (% of Total Postings)

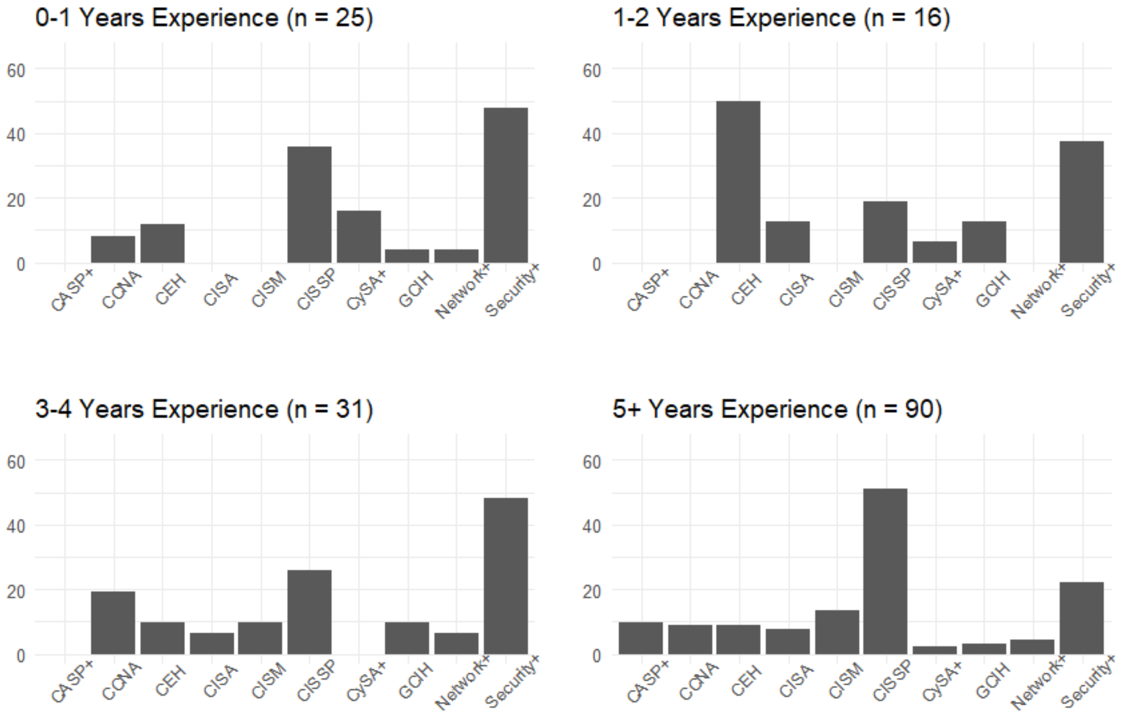


programs offering training for this certification (discussed further in Section **??**). Finally, CCNA is also commonly requested, just slightly below CEH for those postings mentioning the DoD/clearance.

Consistent with the results presented in Figure 5, CISSP is the most commonly requested certification for jobs not mentioning the DoD/clearance across levels of experience. The story here does begin to become clearer when looking at the changing frequency of requested certifications across levels of expected experience in Figure 6. Even among the jobs not mentioning the DoD, it is clear that many of the entry level jobs (0-1 year experience and 1-2 years experience) are requesting both Security+, CEH, and CCNA.

The story could not be clearer than it is in Figure 7. Security+ is, on average, the most requested certification for those postings that are certainly DoD contractors. This is especially true for the entry level positions where it is requested in over 60% of the posting asking for 0-1 years experience, and nearly 40% of the postings asking for 1-2 years experience request Security+. Also, there is quite a bit of evidence suggesting that CCNA and CEH are strong candidates for our curriculum as well. They are commonly requested in entry level and senior level positions. Here, though, we also see that CySA+ is quite common. In fact, on average, more than CEH. That said, CySA+ is almost never requested among the most senior postings (5+ years) while CEH is the third most requested certification among these senior-level postings. This suggests that CEH may have more legs across time. CCNA

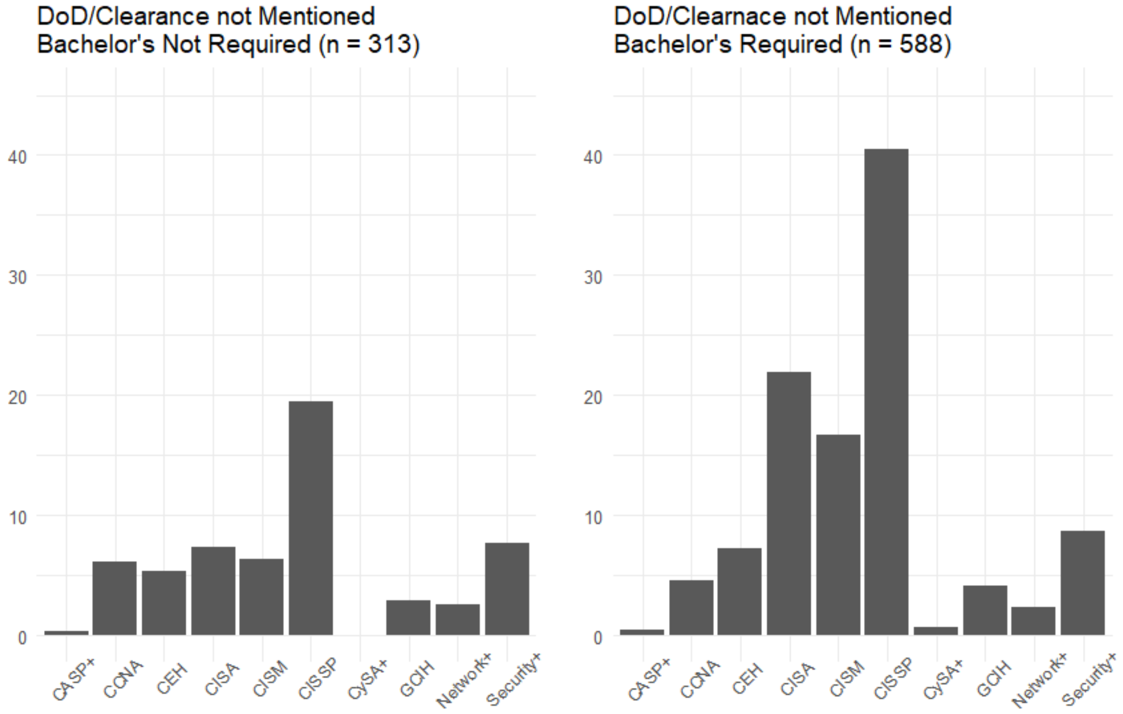
Figure 7: Across Requested Experience: Certification Mentions in Job Postings for Postings mentioning DoD/Clearance (% of Total Postings)



is also common among the more senior level posting (3-4 years and 5+ years), but on the other hand is absent in those postings expecting 1-2 years experience.

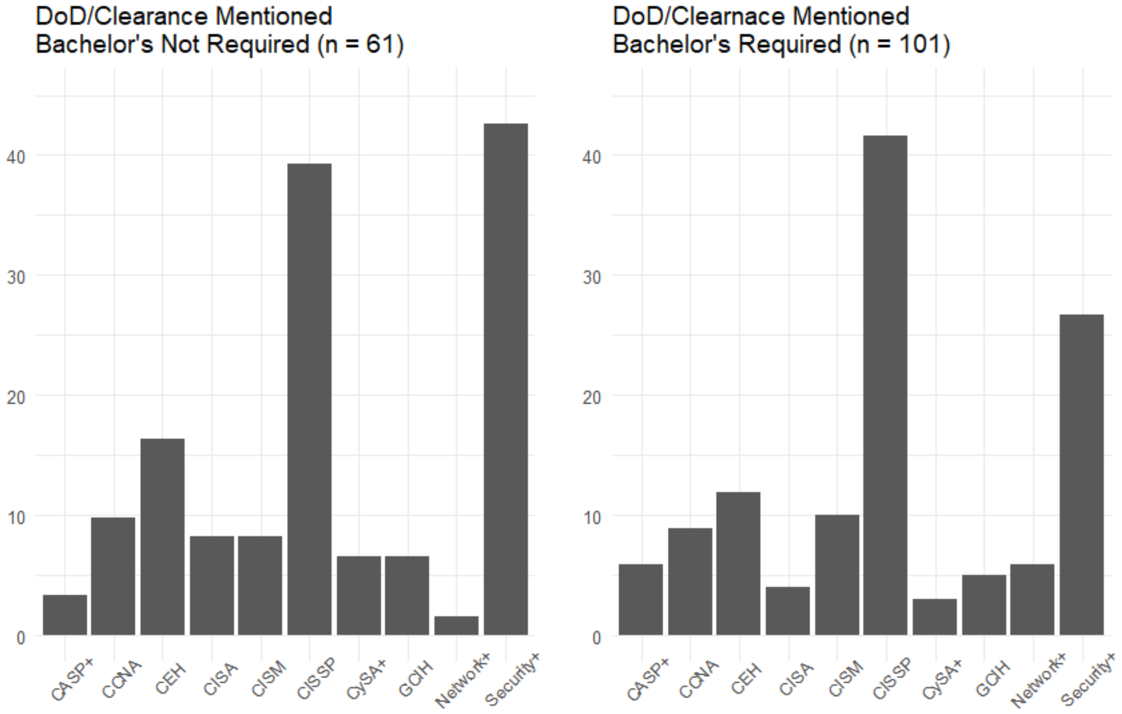
Figure 8 presents the comparative distributions of certification requests for job postings not mentioning the DoD/clearance for those jobs not requiring at least a bachelor's degree and those requiring a bachelor's degree. Again, CISSP is the most requested certification and this is especially true for those jobs requiring a bachelor's degree. This is not surprising given the degree of experience required for that certification, not to mention that it is aimed at certifying management-level qualifications. Here, again though, we see that Security+ is frequently requested particularly for those jobs not requiring a bachelor's degree.

Figure 8: Across Education: Certification Mentions in Job Postings when the DoD/clearance is not Mentioned (% of Total Postings)



The comparative distributions of certification requests for for those jobs not requiring at least a bachelor's degree and those requiring a bachelor's degree for job postings mentioning the DoD or security clearance are presented in Figure 9. Here the evidence that Security+ is frequently requested is glaring. Again it rivals CISSP, particularly for those postings not requiring a bachelor's degree. Further, CEH is toward the middle of the pack of most requested certification for both postings requesting a bachelor's degree and those that do not. CCNA follows relatively closely behind.

Figure 9: Across Education: Certification Mentions in Job Postings when the DoD/Clearance is Mentioned (% of Total Postings)



3.2 Which Certifications are Paired with Security+

At this point it is clear that Security+ is a commonly requested certification especially for jobs that do not require extensive experience or education. The data also suggest that CCNA and CEH may also be a good candidates for our program. The evidence on this latter possibility is definitely less clear at this point. Given that Security+ is overwhelmingly the most common beginning level certification requested, we can go ahead and accept that the evidence suggests it is good baseline certification for us to focus on regardless of the yet to come analysis of the programs with which we would compete. The intention of this next set of analyses is to determine which certifications might pair well with Security+ based on the frequency with which potential employers ask for it with other certifications. It is here where we can fill a gap.

Table 1: Tetrachoric Correlations between Mentions of Expected Certifications in Job Postings for Postings Not Mentioning the DoD

	Security+	CEH	CISA	CISM	CCNA	GCIH	Network+	CASP+	CySA+	CISSP
Security+	1									
CEH	0.24	1								
CISA	-0.03	0.11	1							
CISM	-0.02	0.15	0.58	1						
CCNA	0.37	0.06	-0.05	-0.05	1					
GCIH	0.16	0.18	0.02	-0.04	0.01	1				
Network+	0.42	0.16	-0.01	-0.02	0.13	0.08	1			
CASP+	0.10	-0.02	0.01	0.02	-0.02	0.08	0.21	1		
CySA+	0.16	0.05	0.03	-0.03	-0.02	0.16	0.31	0.25	1	
CISSP	0.22	0.25	0.52	0.54	0.14	0.11	0.13	0.06	0.06	1

Table 2: Tetrachoric Correlations between Mentions of Expected Certifications in Job Postings for Postings Mentioning the DoD

	Security+	CEH	CISA	CISM	CCNA	GCIH	Network+	CASP+	CySA+	CISSP
Security+	1									
CEH	0.18	1								
CISA	0.06	0.22	1							
CISM	-0.18	-0.06	0.29	1						
CCNA	0.37	0.06	0.29	0.04	1					
GCIH	0.18	0.30	0.65	0.02	0.48	1				
Network+	0.24	0.00	0.21	0.14	0.56	0.08	1			
CASP+	-0.10	-0.09	0.19	0.62	0.12	0.19	0.09	1		
CySA+	0.24	0.27	0.21	0.04	0.25	0.35	-0.10	0.23	1	
CISSP	0.14	0.15	0.29	0.39	0.21	0.29	0.26	0.27	0.19	1

The bivariate correlations between all of the certification requests for those job postings not mentioning the DoD or security clearacne are presented in Table 1 (tetrachoric correlations because the indicators are dichotomous). Both CEH and CCNA are the most correlated with Security+ requests relative to all other certifications with the relationship being modestly stronger between CCNA and Security+ requests with the exception of Network+ which did not appear as commonly in the preceding analyses.

The bivariate correlations between all of the certification requests for those job postings that do mention the DoD or security are presented in Table 2. Excluding the negative relationship between CISM and CASP+ requests and Security+ requests as well as CISSP and Security+, the strongest relationships with Security+ in order from strongest to weakest are CCNA, Network+, CySA+, and then CEH and GCIH equally. The differences between these correlations are not that great.

Given that CCNA and CEH were the most commonly requested certifications for entry level positions as evidenced in the conditional distributions presented graphically above, the overall results suggest that Security+ combined with CCNA and CEH make the most sense. That said, given the level of funding, it may make more sense for us to focus on both of these along with those more holistic skill sets we aim to cover as well. Looking at the pass rates of the exams for these certifications does not suggest that either CEH or CCNA is strategically better. Based on a small sample of data gathered by the team, we can estimate that the pass rates for Security+ is around 60%, for CCNA it is around 22%, and for CEH it is about 23%. Again, though these estimates are based on small samples, and there is very little publicly and verifiable data on pass rates out there.

Before examining the competing programs to see if that can help provide data to make this determination that we should proceed with Security+, CCNA, and CEH, though, it is prudent to estimate multivariate models gauging the likelihood employers ask for Security+ as a function of both requests for CCNA and CEH while holding constant other factors to determine which is most related.

3.3 Multivariate Models of the Probability of Requesting Security+

Table 3: Ordered Logit Estimates of Inclusion of Security+

	Estimate	**S.E.**	**P-Value**	**Odds Ratio**
CEH	1.38	0.30	0.00	3.96
CCNA	2.44	0.34	0.00	11.52
Bachelor's	-0.04	0.24	0.00	0.96
Master's	-0.65	1.02	0.52	–
Experience	-0.33	0.09	0.00	0.72
Cert Index	0.35	0.11	0.00	1.42
DoD	1.94	0.25	0.00	6.93

Here we estimate a logit regression model of the inclusion of Security+ in the job requirements posting. We also include odds ratios so as to provide us a sense of the magnitude of the relationship. The results presented in Table 3 are clear, and quite stark. The mention of both CEH and CCNA is strongly related to also requesting Security+ even when holding constant (at their means) education, experience, the total number of certifications requested, and whether the job mentions the DoD or security clearance. The model suggests that postings including CEH are nearly 4 times more likely to also include Security+ than not. While this relationship is quite strong, the relationship between inclusion of CCNA and Security+ in the job requirements is even stronger. Here the model indicates the the odds of mentioning Security+ are increased by 11.52 times when CCNA is also mentioned.

Again, it is important that we include all of these controls to assure that these observed relationships are not spurious, but also just to determine their relationship to the inclusion of Security+. The only statistically insignificant variable in the model is requiring a master's degree. This requirement was just not that common. That said, we see that there is a modest negative relationship (odds ratio = 0.96) between requiring a bachelor's degree and asking for Security+. This bodes well for us operating under the assumption that many of our students will not have a degree. The same is true for the relationship between the experience required and asking for Security+. Those postings asking for Security+ are less likely to require high levels of experience.

Perhaps our most important control variable just for the sake of diminishing the probability of spuriousness is the total number of certifications required (we summed all certification dummy variables excluding Security+, CCNA, and CEH). This helps us be sure that the relationship between CEH, CCNA, and Security+ is not simply a product of potential employers listing out all the common certifications in their postings. Clearly, that is not the case here, as the relationship holds up even with the inclusion of this contol.

Finally, is quite encouraging for our plan to focus on Security+ that mentioning the DoD or security clearance is stongly, and positively, related to the inclusion of Security+ in the job posting. In fact, the odds of mentioning Security+ is nearly 7 times higher when the posting also mentions the DoD or security clearance. This suggests that Security+ is extremely commonly requested by DoD contractors.

4 A Quantitative Description of Comparable Online Training Programs

Here, using Google, we searched using all of the specific certification acronyms described above (CISSP, CEH, CISA, CISM, etc.) with some combination of either "certification online" or "online training camp" (CEH certification online, Security + online training camp). We went through every possible combination to identify the population. Generally, we would go about 5-7 pages deep on Google for each set of search terms when saturation was reached (when all the results were either websites we already visited or they were irrelevant). This search identified 111 programs. We checked each website to make sure the criteria were there (actually offered an online training course that was not free tutorial). Every website had either a search functionality or a tab that showed a list of all of the training courses they offered. We coded each training course for which certification they offered, the provider, whether the course was live with an instructor or asynchronous and self-guided, the price, the time required to complete the course, and whether they offered vouchers to cover the cost of the certification exam. Finally, we recorded whether they also offered training in azure and python courses since our analysis above identified these additional skills as high in demand.

4.1 Comparable Online Training Programs

Table 4: Major Online Cybersecurity Certificate Training Programs

Providers	Counts
LearningTree	13
TheKnowledgeAcademy	12
TestPass Academy	8
TrainingCamp	8
Infosec	7
PhoenixTS	7
Alpine Security	6
Global Knowledge	6
CyberProtex	5
Intense School	5
New Horizons	5
ASMED	4
CyberVista	4
EC-Council	4
ASPE Training	3
IntelliPaat	3
CertificationCamps	2
CompTIA	2
EndpointLearning	2
ISC2	2
CyberTraining365	1
Simplilearn	1
TheCyberAcademy	1

Surprisingly, there are not that many competitors who offer online training. As presented in Table 4, there are only 23 organizations offering training programs identified in our search. Further, it is clear that the majority of the different programs offered are done so by limited number of organizations. For instance, LearningTree accounts for 13 of the total programs offered and TheKnowledgeAcademy accounts for 12. Given that there are only 11 total programs, that means that just two organizations are responsible for about 23 percent of the online offerings. This, at the least, suggests that we do not have that much competition.

4.2 Common Certification Types

As evidenced in Table 5, there are clearly many training program offerings for Security+ and CEH, but we only identified one online (non-open source) program offering CCNA. This

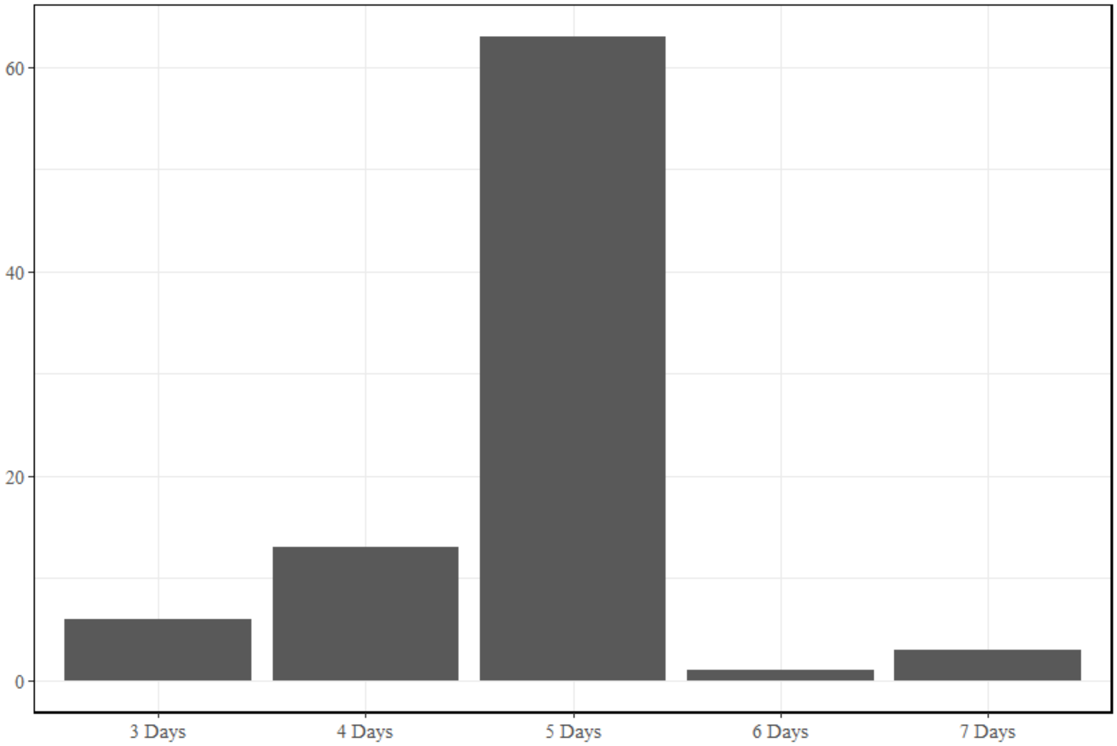
Table 5: Distribution of Types of Certification Training Programs.

Type	Counts
CISSP	18
CEH	18
Security+	18
CASP+	13
CISM	13
CySA+	12
CISA	11
CCISO	7
CCNA	1

latter observation suggests we have a real opportunity to increase the odds of success for those students we train for CCNA certification. This is especially true for those DoD contractor employment opportunities where CCNA was a quite commonly requested certification. Also, pairing CCNA with those other commonly requested certifications (Security+ and CCNA) bodes well for our model too given that these other programs do not offer both.

4.3 Duration

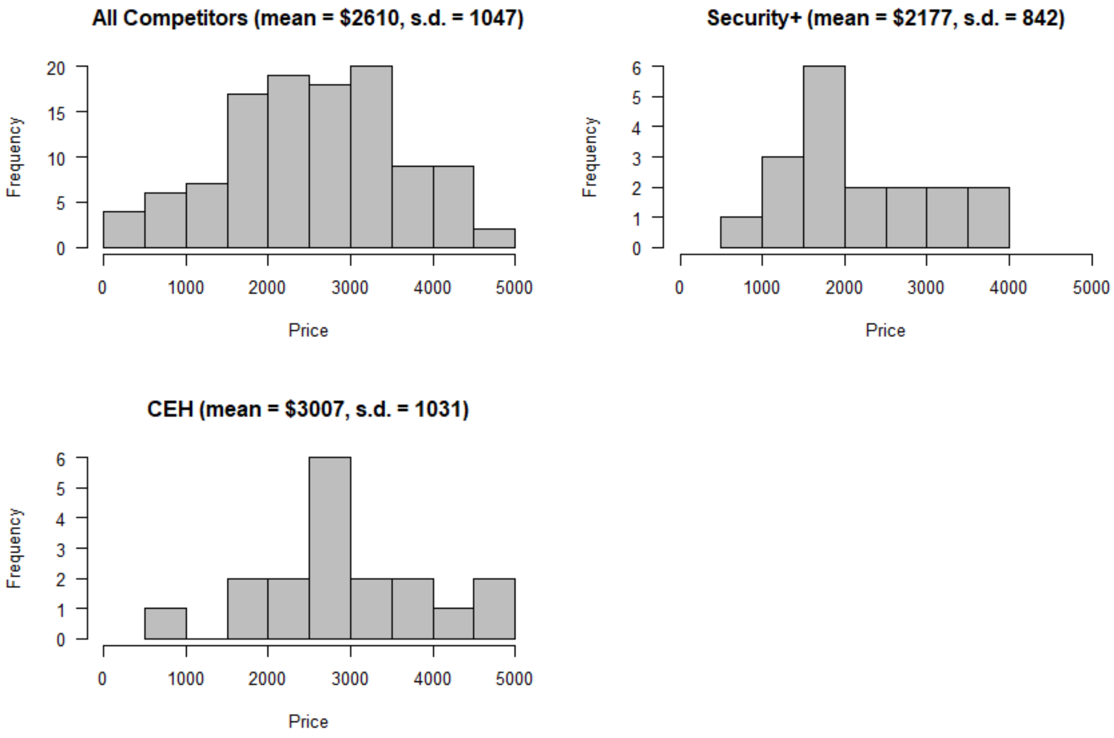
Figure 10: Distribution of Duration of Programs



The results presented in Figure 10 indicate that the the competitor training programs range from 3-7 days, and that overwhelmingly the modal duration here is 5 days. As such, we should shoot for a 5 day program to be comparable should potential recruits be weighing this as part of their choice in program.

4.4 Pricing

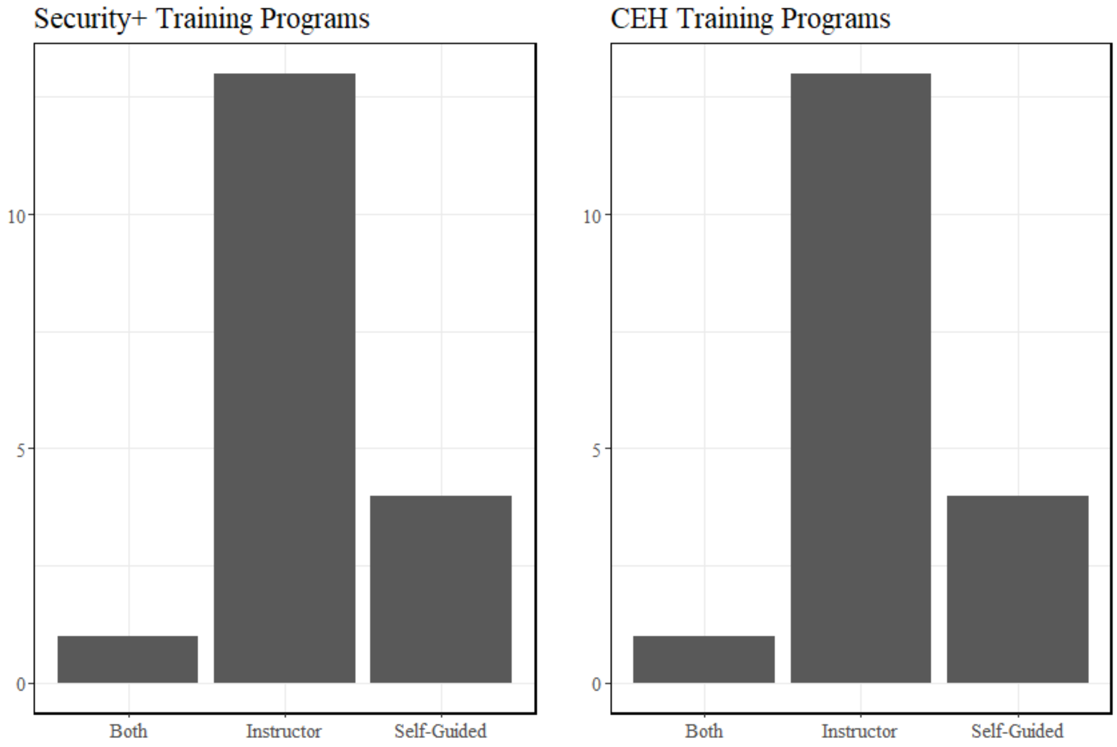
Figure 11: Distribution of Pricing across Certification Type



The average prices for all programs, and across certification offered, are presented in Figure 11. The data indicate that the average price for all programs, collectively, is $2610. The average price for Security+ is $2177 (but the distribution is skewed a bit toward the less expensive side), for CEH the average is $3007, and the CCNA program costs $4223. You'll see here that the standard deviation is significantly smaller than the mean in each instance confirming as we can see in Figure 11, that the price largely distributes normally around the mean without a great amount of variation. As such, pricing for us could safely hover around those means without pushing off too many likely recruits.

4.5 Types of Instruction

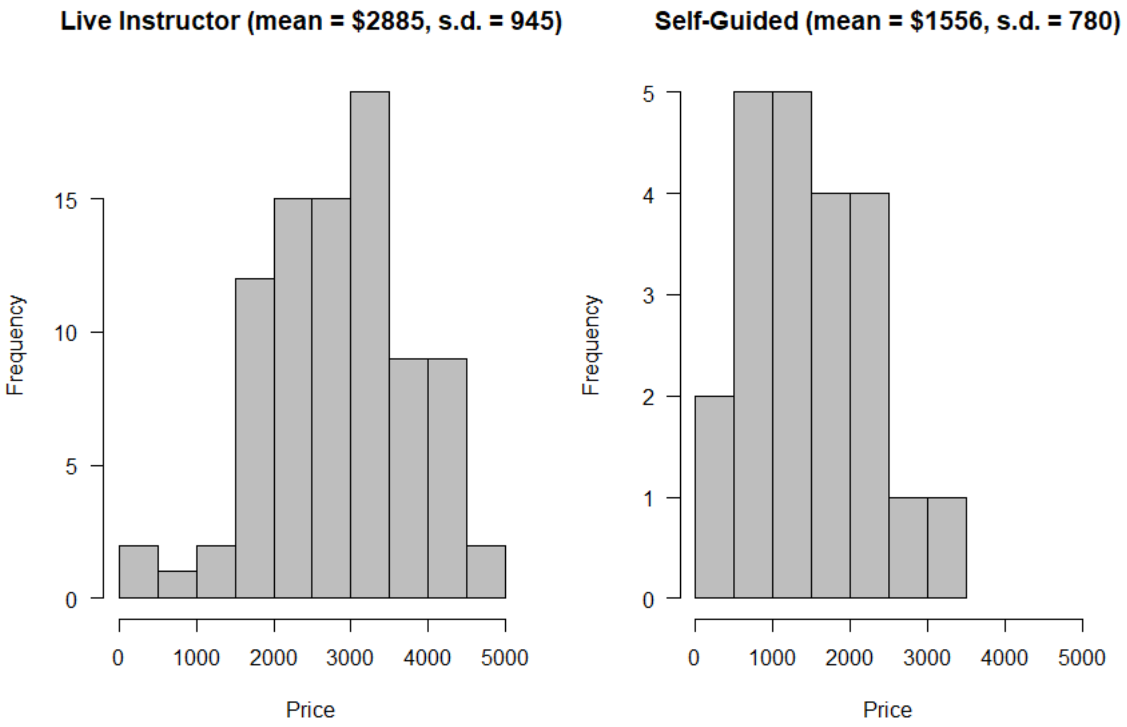
Figure 12: Distribution of Type of Instruction across Certification Type



As clear in Figure 12, most Security+ and CEH programs are offered by a live instructor versus self-guided and only a few offer both, and the CCNA program has a live instructor.

4.6 Price and Types of Instruction

Figure 13: Distribution of Pricing across Instruction Type



As should be expected, self-guided programs are significantly less expensive than those with live instructors, but are still costly ($1556 on average). Not only is the mean price higher for courses with live instructors ($2885), but the distribution is skewed toward the more expensive range (see Figure 13). Thus, when potential recruits research the competitors most of the comparable courses with live instructors will be above the average. This could be a good reason for our program to be near or lower than the average.

4.7 Vouchers

When it comes to cost, it is also important to consider whether the student tuition includes with it a voucher to cover the cost of the associated certificate exam. Over 60 percent of the total programs offer a voucher to take the associated certification exam (see Figure 14), less than half of the Security+ programs offer a voucher (see Figure 15), nearly 80 percent of the CEH programs offer a voucher (see Figure 16), and the CCNA program does offer a voucher. Given that not all programs offer a voucher, and Security+ vouchers are actually only at 45 percent, it seems a prudent strategic recruiting tool to offer a voucher.

Figure 14: Frequency Programs offer Vouchers - All Programs

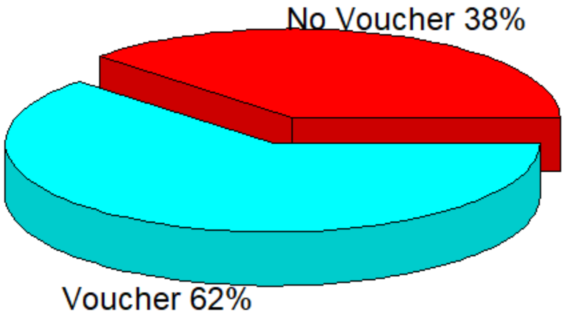


Figure 15: Frequency Programs offer Vouchers - Security+

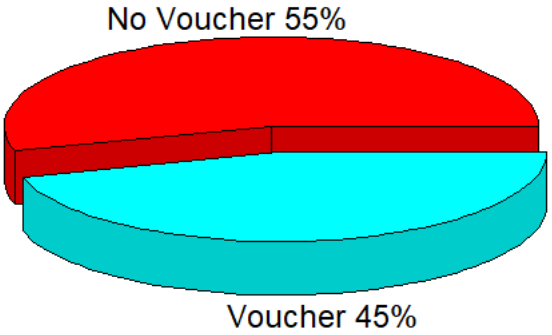
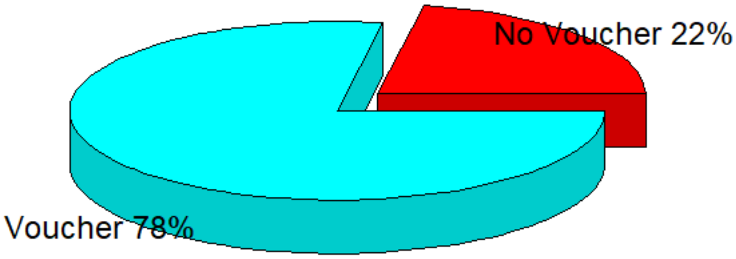


Figure 16: Frequency Programs offer Vouchers - CEH



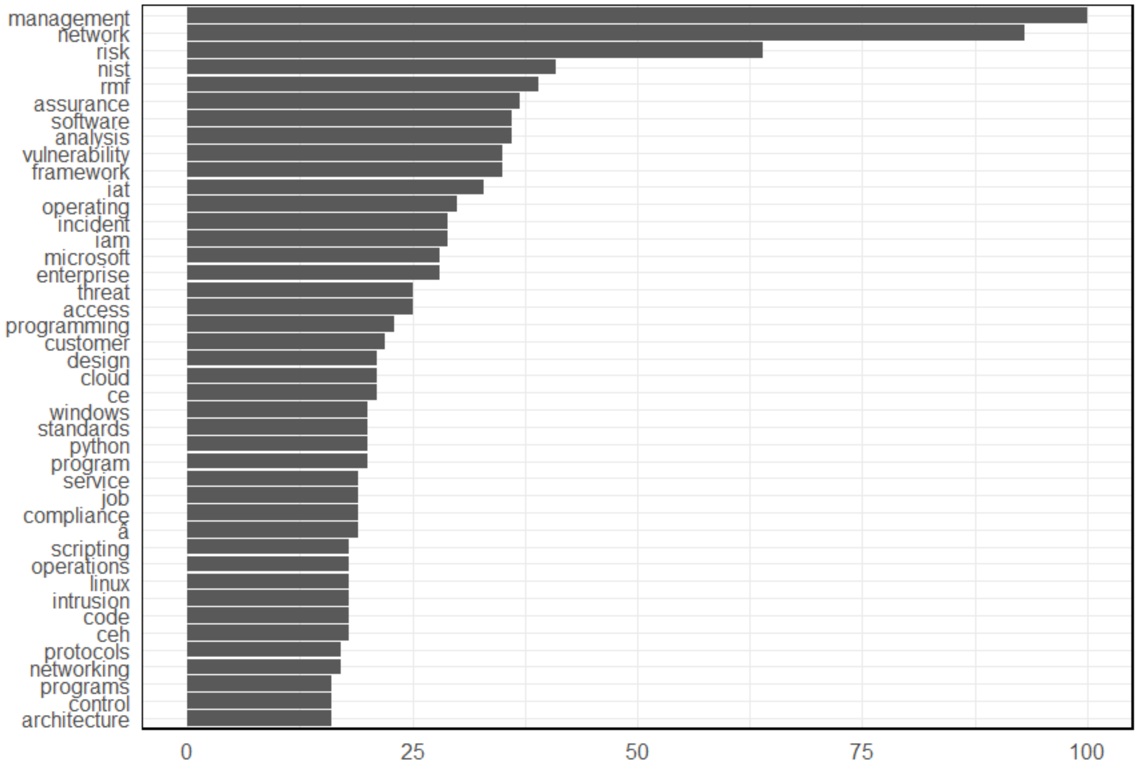
5 A Machine Coding Based Content Analysis of Cybersecurity Job Postings

5.1 Descriptive Content Analysis of Job Requirements

Figure 17 displays the most common words showing up in the job requirements section of the postings from explicit DoD contractors (see the Appendix in Section 7 for graphs displaying the most common words for those postings not mention the DoD or security clearance). It is important to note here that we eliminated all “stop words” from the corpus (a, if, the, but, etc.), but also went a step further by eliminating words that did not give us information directly informative to shaping our curriculum (e.g. information, knowledge, internet, skills, required, etc.). In total we eliminated 95 words from the corpus in addition to the standard stop words.

The descriptive content analysis, here, suggests several things. First, familiarity with the NIST and RMF cybersecurity frameworks is commonly expected in DoD contractor jobs. Next, an understanding of Microsoft, Microsoft Azure, and Python is commonly preferred among DoD contractor job postings. When digging a bit further into the Microsoft tools, some of the most common tools that came up were Enterprise, Microsoft Server, the Active Directory (various related components therein), Microsoft Cloud, and most frequently, Mi-

Figure 17: Most Common Words used in Job Requirements (n > 15)



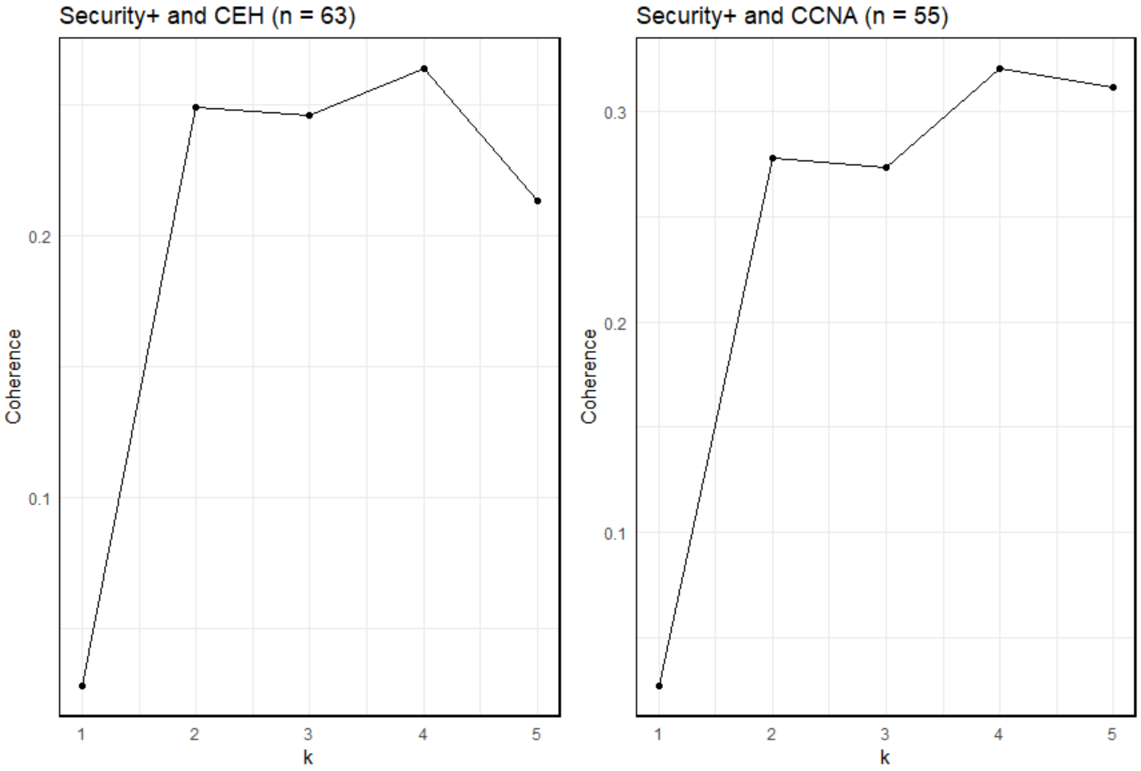
crosoft Office (86 times in the full data). That said, Microsoft Azure comes up 138 times in the full data, so we clearly would benefit from incorporating Azure training into our platform. Python also comes up 140 times in the full data. An understanding of the Python language would also greatly benefit our students' employment prospects, and as such, likely help with recruitment.

5.2 Building Topic Models

As briefly described in Section 1.2, topic models are a way to inductively identify patterns in text by identifying associational relationships between words in a corpus of text. The corpus we use here are all of the job requirements. To analyze the patterns of words, we first, take those job requirement postings, and dis-aggregate them into single words while keeping track of the case from which they came (this process is done via machine coding - not manually). We eliminate the stop words. From there we use a maximum likelihood process that identifies the underlying structure in that matrix of words by calculating the probability that each word (and two word combination) appears with every other word in the corpus in its given case.

The process is iterative in that it runs through Markov chains that fit the words in two separate factors/vectors until it identifies the number of vectors of words and two-word combinations that results in the highest possible aggregate association between the total corpus of words. We then examined the vectors of words (the top 20 on each vector) to determine if there are more words, aside from the stop words, that can be eliminated for us to specifically identify vectors of words or topics that are centered on useful skills we may include in our curriculum. After identifying the additional unhelpful words, we estimate the model again, and again, until it is distilled down to relevant and useful topics for us.

Figure 18: Using Coherence Scoring to Estimate the Most Likely Number of Topics in the Job Descriptions



The results presented in Figure 18 show the aggregated correlation for each maximized structure of the words on vectors of 1, 2, 3, 4, and 5 possible vectors. There are two graphs here because we decided to restrict the corpus first on the left to those postings that mentioned Security+ and/or CEH, and second on the right, to those postings mentioning Security+ and/or CCNA. As you can see, the combination of words into 4 possible topics maximizes the correlational structure. Thus, we extract the top 20 words from each of those 4 topics.

The top 20 words for the data restricted to postings including Security+ and/or CEH are displayed in Table 6. They are in the order from left to right in the topics that had the highest internal structure (the most correlated), and then are in the order by which each word is the most correlated with the vector/topic within which it is grouped. We simply examined the lists of words to make a qualitative assessment about what each topic is about. In this model, we decided that the first topic is infrastructure. Notice words like management, tools,

Table 6: Top 20 words representing each topic extracted via latent topic modeling procedure for Security+ & CEH

Infrastructure	Network Security	Risk Management	Accreditation
tools	incident	level	cissp
management	capture	management	practical
assessment	intrusion	risk_management	ii
implementation	packet	risk	comptia
environment	traffic	framework	accredited
microsoft	packet_capture	management_framework	andor
hbss	flow	assurance	nist
linux	full_packet	rmf	level
certified	full	ce	hacker
citizenship	ports_protocols	nist	casp
administrator	proficiency	access	travel
windows	ports	iam	networking
compliance	protocols	framework_rmf	level_ii
andor	tcpip	iat	army
risk	top	ia	scripting
cissp	engineering	sci	ccna
cisa	protocols_traffic	acas	sans
operating	traffic_flow	top_sci	gsec
software	attack	development	csa
penetration	osi	level_ii	python

Note: The unit of analysis is the word.

implementation, and compliance. These employers are expecting candidates to have a sense of the organization's infrastructure (perhaps digitally and as business). The next level of importance is network security. Here you see words such as incident, intrusion, packet, and traffic. Then there is risk management. The single words and combinations of words here are obviously talking about managing risk. Finally, the last topic is focused on expectations about certifications. Notice that Python shows up on this topic - reinforcing the results from the descriptive content analysis.

All of these topics together give us insight into content that we can include in our curriculum that will give our students an edge on the job market. It gives us a sense of the language and content we can incorporate and integrate into our certification training. This way, these students will have a stronger sense of what the market is looking for. Further, just having communicated about these topics in-depth may give them an edge when it comes time to interview. They will be more well-rounded.

The top 20 words for the data restricted to postings including Security+ and/or CCNA are displayed in Table 7. Here, again, the topics are the same, just not in the same order and with some different words. It is important here though that there is consistency. This increases our confidence that these topics generalize across employers' desired qualities of job candidates. Thus, we believe that adding to our instruction material/content that focuses

Table 7: Top 20 words representing each topic extracted via latent topic modeling procedure for Security+ & CCNA

Infrastructure	**Risk Management**	**Accreditation**	**Network Security**
practical	level	training	incident
comptia	risk	cissp	capture
management	risk_management	hbss	packet
access	assurance	compliant	traffic
andor	management	accredited	packet_capture
ce	framework	top	flow
linux	management_framework	ii	full_packet
compliance	rmf	csa	intrusion
iam	certified	army	full
acas	ii	scripting	proficiency
scap	assessment	customer	ports
development	framework_rmf	environment	protocols
level	tools	iat	tcpip
focused	nist	ticket	protocols_traffic
iam_level	ia	service	traffic_flow
nispom	implementation	casp	attack
microsoft	level_ii	level_ii	osi
operating	engineering	ce	tcpip_networking
special	iat_level	gicsp	ports_protocols
server	iat	area	model

Note: The unit of analysis is the word.

on infrastructure, network security, risk management, and of course, the certifications for which we are training our students, will create a more holistic cybersecurity specialist. It will better equip them not just for the market, but for the job.

6 A Summary Recommendation for our Curriculum

This gap analysis was intended to identify the differential between employer needs and cybersecurity programming offerings. By doing so, this team would identify curricular modifications to better prepare a workforce responding to the U.S. Department of Defense (DoD). The report raises several challenges faced by those entering or wishing to advance in the employment field of cybersecurity - including barriers to entry, conflictions in employment qualifiers, high cost of certifications coupled with low options in program choice, and the call for preferred supplemental certifications that are not directed by, nor often recognized by, the DoD. This report also clarifies the opportunities available to our joint project between the University of Louisville and the Kentucky Commission on Military Affairs. Specifically, our project seeks to bridge these identified gaps for our service members, veterans, and their dependents as they seek workforce development training and navigate employment transitions into the increasingly expanding cyber market within DoD and its contractors.

- BARRIERS TO ENTRY: The ability to obtain and maintain a security clearance is indisputably a foundational requirement to most cybersecurity positions within the DoD, yet it is rarely mentioned. The range of supports (from the absence of data points to a need for assistance in education and training) would enable graduates of our unique program to enter the labor market for DoD related jobs. Baseline certifications are required regardless of and in addition to a traditional degree; none more so than CompTIA Security+, which is a worthy note to make. This certification will form the basis of our educational program as it resonates highly throughout the market. Coupling this foundational certification with holistic and layered education in the topics of infrastructure, network security and risk management will ensure our graduates clear the hurdle presented by job application online diagnostic tools that pre-screen for minimum knowledge requirements. Also, drawing on social science research, we know that odds are high that these barriers are exacerbated for underrepresented minorities, yet if we wish to be truly responsive to our communities, we must explore strategies that tackle these barriers across the spectrum of learners.
- CONFLICTIONS IN EMPLOYMENT QUALIFIERS: Surprisingly, conflictions in employment qualifiers are permeated in the employment market. Minimum experience requirements present employment access challenges for applicants that seem insurmountable. Most cybersecurity jobs require significant experience to apply. Confusion reigns as some highly functional DoD 8750 certifications are shown to not be requested (i.e., CASP+CE) by employers. Furthermore, there are mismatched advertisements (i.e., CISSP, an advanced certification, required for entry-level positions) revealing industry-wide disconnects among certifications, position duties, and human resource requisitioning. These conflictions, when identified and revealed, uncover underlying concerns, and it is no wonder that shortages in qualified applicants appear. Culling the field to three of the most highly requested certifications (i.e., CompTIA Security+, Cisco Certified Network Associate, [EC-Council] Certified Ethical Hacker) will allow our program to focus and direct resources where they will be most valued for our

graduates. Industry recognized activities including a cyber range system and periodic capture the flag events will bridge these gaps so our learners will gain experiential hours to be utilized in meeting experience requirements for cyber positions. Success and career coaching, which integrates both the professional learning and the University of Louisville's robust career development center, will be paramount to support learner's development and decode cyber employer postings.

- HIGH COST OF CERTIFICATIONS COUPLED WITH LOW OPTIONS IN PROGRAM CHOICE: The cost of technical training remains high - both fiscally and in time requirements. At an average of over $2,600 per certificate and 3-7 days of in-person, intense workshops for baseline certifications, transitioning into cybersecurity or advancing in the field is cost and time prohibitive for many military families. Together with a lack of choice in programs and very little opportunity to pursue in regional institutes of higher education, the problems are exacerbated. This project with the DoD will help offset these significant hurdles. Our courses of action to cover this gap recognize the needs of often moving military members, transitioning service members, veterans and their families for affordable, and portable training that is, at the same time, expertly led.
- NEED FOR PREFERRED SUPPLEMENTAL CERTIFICATIONS: This analysis revealed a DoD-wide industry preference from employers expecting applicants to hold specific supplemental certifications; significantly, all of them are non-DoD Directive 8750. This expectation is as important a discovery as the baseline certification correlations: it attests to further education and training that sets applicants apart as highly marketable. These expected industry qualifications include only Microsoft certifications, particularly Windows, Azure, and Python. By including these preferred certifications as part of our base curriculum, we will ensure our learners, who complete participation at the University of Louisville, possess the most desirable credentials that employers are seeking in their employees.

The challenges of the cybersecurity job market are daunting but not insurmountable. The University of Louisville gap analysis gives a clear set of breaching tools for our learners to make it past the screening to the interview pool and beyond to meaningful employment. Certainly, there are opportunities abound to assist (a) our learners who are service members, veterans, and military dependents to navigate employment transitions into the increasingly expanding cyber market and (b) the DoD and their contractors as a major employer in this space to conduct that training and education at the University of Louisville.

7 Appendix: Supplemental Analysis using Data from Non-DoD Job Postings

Figure 19: Most Common Words used in Job Requirements (n > 199)

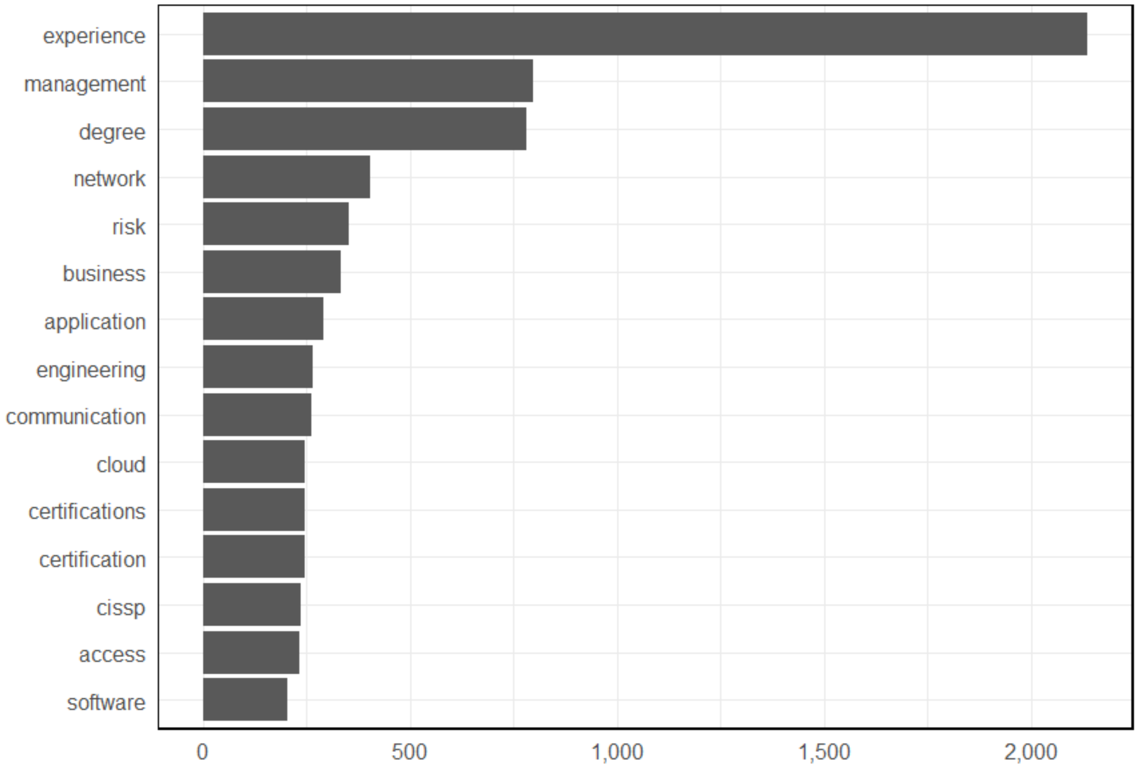


Figure 20: Most Common Words used in Job Requirements (n > 149 & < 200)

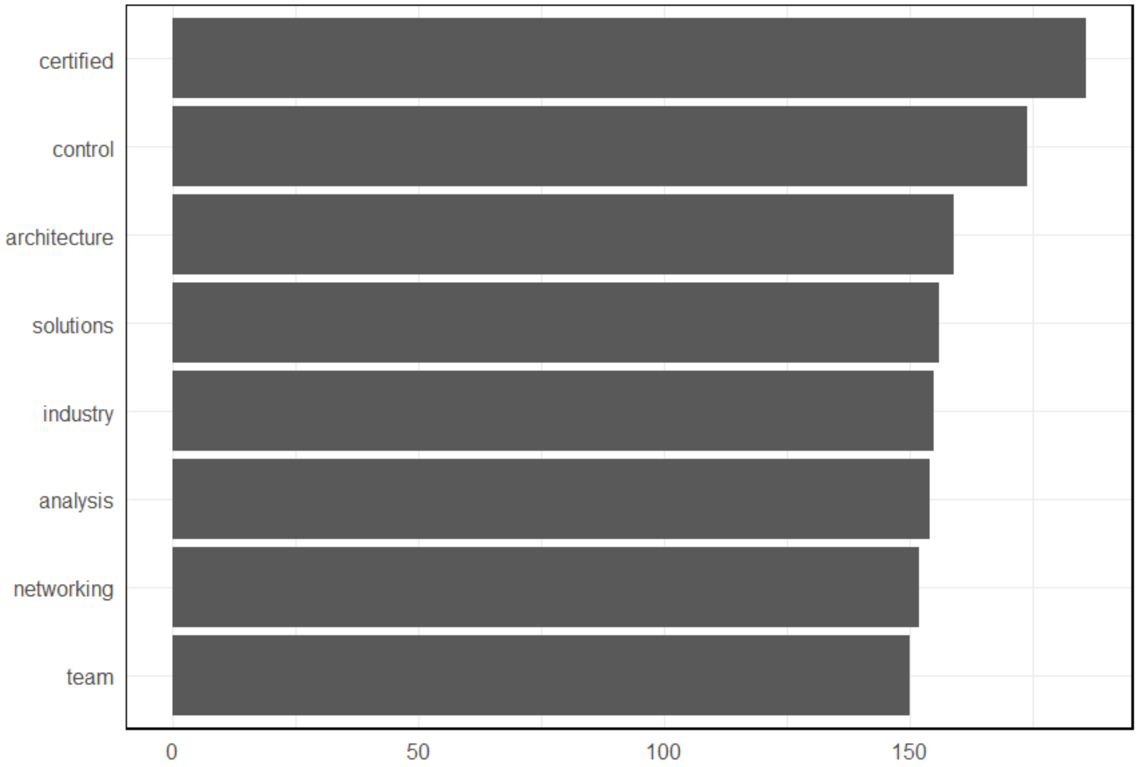
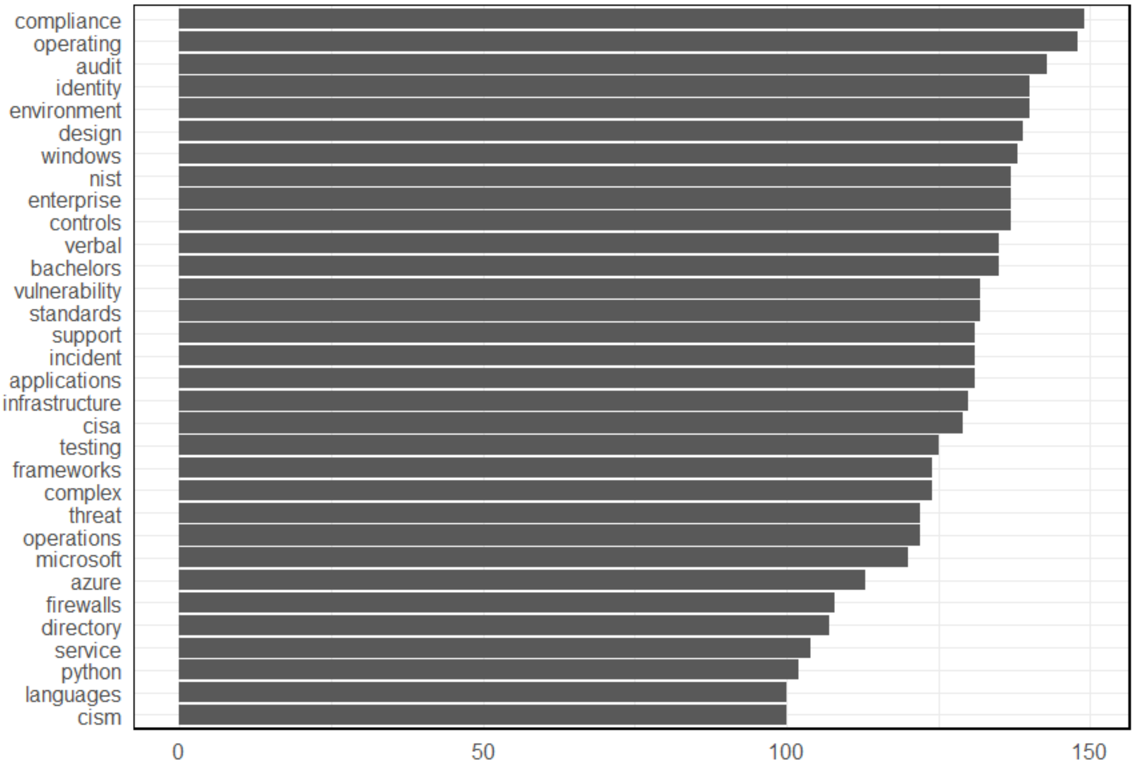


Figure 21: Most Common Words used in Job Requirements (n > 99 & <150)


compliance
operating
audit
identity
environment
design
windows
nist
enterprise
controls
verbal
bachelors
vulnerability
standards
support
incident
applications
infrastructure
cisa
testing
frameworks
complex
threat
operations
microsoft
azure
firewalls
directory
service
python
languages
cism