Journal of Cybersecurity Education, Research and Practice

Volume 2024 | Number 1 Article 6

October 2023

Building the Operational Technology (OT) Cybersecurity Workforce: What are Employers Looking for?

Christopher A. Ramezan
West Virginia University, cramezan@mail.wvu.edu

Paul M. Coffy
Civil Military Innovation Institute (CMI2), pcoffy@cmi2.org

Jared Lemons
Civil-Military Innovation Institute (CMI2), jlemons@cmi2.org

Recommended Citation

Ramezan, Christopher A.; Coffy, Paul M.; and Lemons, Jared (2023) "Building the Operational Technology (OT) Cybersecurity Workforce: What are Employers Looking for?," *Journal of Cybersecurity Education, Research and Practice*: Vol. 2024: No. 1, Article 6.
DOI: 10.32727/8.2023.31
Available at: https://digitalcommons.kennesaw.edu/jcerp/vol2024/iss1/6

Building the Operational Technology (OT) Cybersecurity Workforce: What are Employers Looking for?

Abstract

A trained workforce is needed to protect operational technology (OT) and industrial control systems (ICS) within national critical infrastructure and critical industries. However, what knowledge, skills, and credentials are employers looking for in OT cybersecurity professionals? To best train the next generation of OT cybersecurity professionals, an understanding of current OT cybersecurity position requirements is needed. Thus, this work analyzes 100 OT cybersecurity positions to provide insights on key prerequisite requirements such as prior professional experience, education, industry certifications, security clearances, programming expertise, soft verbal and written communication skills, knowledge of OT frameworks, standards, and network communication protocols, and position travel. We found that OT cybersecurity roles are typically non-entry level, as experience was the most common requirement, and was required on 95% of analyzed positions. Possession of a bachelor's degree or higher was required for 82% of positions, while industry certifications such as the Certified Information Systems Security Professional (CISSP) or the Global Information Assurance Certification (GIAC) Global Industrial Cyber Security Professional (GICSP) were listed on 64% of positions. Knowledge of OT or IT frameworks and standards and strong communication skills were listed on 48% of positions, while programming expertise, possession of the United States security clearance, and knowledge of OT or IT networking protocols were required for 18%, 24%, and 27% of positions, respectively. A work travel requirement was listed on 29% of positions. Individuals seeking to enter the OT cybersecurity field, and educational programs focusing on training OT cybersecurity professionals should prioritize obtaining experience, education, and certification, possessing strong communication skills, and knowledge of relevant OT and IT industry standards and frameworks.

Keywords

Cybersecurity, Operational Technology, Workforce Development, Cybersecurity Education

Building the Operational Technology (OT) Cybersecurity Workforce: What are Employers Looking for?

Christopher A. Ramezan
Dept. of Management Information Systems
West Virginia University
Morgantown, West Virginia, USA
cramezan@mail.wvu.edu
https://orcid.org/0000-0001-9580-9213

Paul M. Coffy
Civil-Military Innovation Institute (CMI2)
Morgantown, West Virginia, USA
pcoffy@cmi2.org
https://orcid.org/0009-0007-1766-5219

Jared Lemons
Civil-Military Innovation Institute (CMI2)
Morgantown, West Virginia, USA
jlemons@cmi2.org
http://orcid.org/0009-0000-9520-4804

***Abstract*—A trained workforce is needed to protect operational technology (OT) and industrial control systems (ICS) within national critical infrastructure and critical industries. However, what knowledge, skills, and credentials are employers looking for in OT cybersecurity professionals? To best train the next generation of OT cybersecurity professionals, an understanding of current OT cybersecurity position requirements is needed. Thus, this work analyzes 100 OT cybersecurity positions to provide insights on key prerequisite requirements such as prior professional experience, education, industry certifications, security clearances, programming expertise, soft verbal and written communication skills, knowledge of OT frameworks, standards, and network communication protocols, and position travel. We found that OT cybersecurity roles are typically non-entry level, as experience was the most common requirement, and was required on 95% of analyzed positions. Possession of a bachelor's degree or higher was required for 82% of positions, while industry certifications such as the Certified Information Systems Security Professional (CISSP) or the Global Information Assurance Certification (GIAC) Global Industrial Cyber Security Professional (GICSP) were listed on 64% of positions. Knowledge of OT or IT frameworks and standards and strong communication skills were listed on 48% of positions, while programming expertise, possession of a United States security clearance, and knowledge of OT or IT networking protocols were required for 18%, 24%, and 27% of positions, respectively. A work travel requirement was listed on 29% of positions. Individuals seeking to enter the OT cybersecurity field, and educational programs focusing on training OT cybersecurity professionals should prioritize obtaining experience, education, and certification, possessing strong communication skills, and knowledge of relevant OT and IT industry standards and frameworks.**

Keywords— Cybersecurity, Operational Technology, Workforce Development, Cybersecurity Education

I. Introduction

Operational technology (OT) is essential to the functionality of many critical infrastructures such as transportation and traffic control systems, electrical grids, water and wastewater treatment, dams, and gas pipelines as well as the infrastructure of critical industries such as the chemical, agricultural, mining, energy, and communications sectors. The consequences of a successful cyberattack on industrial control systems (ICS), supervisory control and data acquisition (SCADA) networks, programmable logic controllers (PLC) or other components of an OT enterprise can be severe, ranging from damage to physical infrastructure and operational downtime to disaster situations which could lead to hazardous safety conditions and potential loss of life. As disruptions to OT environments in critical industries could potentially cause economic, social, and political instability [1], the security of OT environments in critical industry sectors are often considered of vital importance to national security [2].

While industrial systems have been historically targeted by hackers, with famous examples such as Stuxnet [3] and Industroryer/Crashoverride [4], cyberattacks on OT are far less common than attacks on information technology (IT) systems. However, recent trends within Industry 4.0 have fueled the increasing convergence of OT and IT systems, which have created new challenges for OT security [5], [6]. The introduction of smart digital sensors, industrial internet of things (IIoT), remote access control systems, and other IT, or internet-facing devices in industrial environments may potentially increase the attack surface and risk profile of OT environments [5], [7], [8]. Although security automation and detection methods and platforms have substantially advanced in recent years, largely due to innovations in machine learning and deep learning applications [9]–[12], the need for human capital in the OT cybersecurity space remains prevalent.

As of 2023 the cybersecurity field in general is currently facing a massive skills gap, with millions of cybersecurity jobs unfilled across the world. [13] and [14] suggest that the current cybersecurity skills gap also extends to OT, however given the lack of available data and analysis on the OT cybersecurity workforce, it's unclear if the current cyber skills gap truly extends into the OT cybersecurity sector. Nevertheless, a trained cybersecurity workforce which specializes in securing OT infrastructure, processes, networks, and technologies

continues to be needed to protect critical infrastructure and industries. Given the need for a trained OT cyber workforce, this begs the question, what are the desired expertise and qualifications for OT cybersecurity professionals?

To provide insights on this question, we investigate numerous position requirements of a variety of OT-focused cybersecurity positions. Results of such an analysis could in turn be used as a roadmap for aspiring OT cybersecurity professionals but also as a guide for higher education and training institutions to develop pathways to train the next generation of OT security professionals to assist with protecting national critical infrastructure and critical industries. Insights on desired skills and knowledge requirements for OT cybersecurity positions would also be beneficial for organizations seeking to train and re-skill their IT security personnel to defend OT systems within converging IT-OT environments. While numerous studies have investigated qualification and skills requirements for IT cybersecurity positions [15]–[18], relatively little attention has been given to examining the job requirements of OT cybersecurity roles, with the notable exception of a 2022 study by [19] which examined 10 ICS job types to identify curriculum gaps in ICS cybersecurity within the Workforce Framework for Cybersecurity, commonly known as the NICE framework. To our knowledge, this investigation is the first of its kind to solely focus on desired qualifications for OT security positions through an examination of a wide variety of OT cybersecurity roles.

In this paper, we analyze 100 OT cybersecurity job descriptions to identify the skills, knowledge, qualifications desired for OT cybersecurity roles in industry. We first provide a brief background on OT cybersecurity followed by a literature review on job description analysis and an overview of cybersecurity job requirements. Data collection and processing methods are then presented, followed by results and discussion of findings.

II. Background

Operational Technology (OT) can be defined as a wide range of programmable systems and devices, from sensors and actuators to programmable logic controllers (PLCs), and supervisory control and data acquisition (SCADA) systems which are designed to control, monitor, and automate physical processes and equipment in real time [20]. OT systems are often used for tasks such as managing the flow of electricity within the power grid [21] or regulating temperature and pressures of varying equipment within manufacturing facilities [22]. As OT systems have a direct impact upon devices in the physical world, attacks on, or failures of OT systems often have more serious consequences than attacks on IT systems, particularly regarding human safety.

OT security has been a traditionally separate paradigm from IT security, with notable differences in knowledge areas, priorities [23], methods [24], and culture [23], [25]. For example, in the traditional CIA triad of confidentiality, integrity and availability, IT security tends to prioritize and focus on protecting the confidentiality and integrity of organizational data stored and processed on information systems and networks through the implementation of security controls such as firewalls, antivirus software, and encryption [26]. In contrast, OT security, prioritizes the availability, safety [23], [27], and resilience [26] of physical infrastructure assets and industrial processes of an organization. Organizations utilize access control, process monitoring, safety instrumented systems, event logging, and intrusion detection methods to identify and detect malicious or accidental events which may disrupt or damage industrial equipment and processes [28]. Some of the key differences between IT and OT security priorities are shown in Fig. 1.

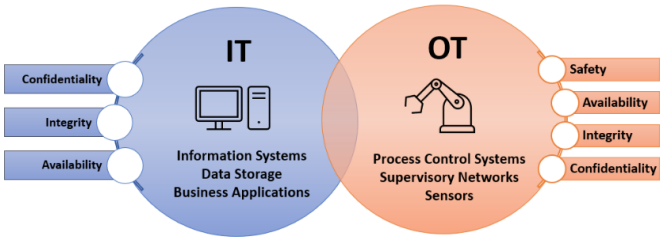

Fig. 1. IT and OT security paradigms

Until recently, IT and OT systems and networks were traditionally isolated from each other, however trends within Industry 4.0 are leading to increasing convergence between IT and OT environments, particularly through the introduction of industrial internet of things (IIoT) devices within industrial environments [29]. While the implementation of data centric IIoT systems, devices, and sensors provide competitive advantages through increased real-time insights on industrial and manufacturing processes, the interconnectedness of traditionally disparate IT and OT systems and networks through IIoT and other smart devices presents a significant challenge for IT and OT cybersecurity professionals [23].

The convergence of IT and OT systems will require a shift in organizational culture and mindset for both IT and OT security professionals. As IT and OT security teams often have different priorities and approaches to security, bringing these teams together can present a significant challenge for organizations [23]. Training security professionals in both IT and OT paradigms is highly advantageous for organizations undergoing IT-OT convergence and could potentially reduce barriers and increase cooperation between IT and OT security teams [25]. Increased understanding of IT and OT security paradigms benefits both IT and OT professionals. Thus, an in-depth analysis of the pre-requisite requirements for OT security positions would be a useful guide for IT security professionals to better understand the desired knowledge, skills, and requirements of positions within the OT security domain.

III. Literature Review and Aims

Analyses of job postings can provide valuable insights on the desired knowledge, skills, and qualifications, as well as evolving employment trends within a particular industry. Numerous analyses have been conducted on a variety of fields including human resources management [30], data analytics [31], [32], artificial intelligence and machine learning [33], and cybersecurity [17], [34], [35]. While insights from such

analyses can be advantageous for individuals seeking to enter a specific field or industry, they can also be beneficial developing and fine-tuning curriculum within higher education and training programs to maintain relevance and ensure education and training are in alignment with industry needs to continue to develop the next generation workforce. For continually evolving fields such as cybersecurity, such insights can be particularly advantageous for keeping abreast of developments and trends within a rapidly advancing and dynamic discipline.

Prior investigations on cybersecurity job postings [17], [34]–[36] have found several key prerequisite requirements were typically required for cybersecurity positions. In an analysis of 487 cybersecurity analyst positions, [34] found that general technical skills, industry certifications, higher education degrees, and prior professional experience were frequent prerequisites for employment. In addition to these pre-requisite requirements, a similar but more extensive study by [35] found that programming skills were also frequently desired among entry level cybersecurity jobs. Ramezan [17] further expanded upon this topic through examining cybersecurity positions within different cybersecurity sub-fields and found that security clearances were another frequent requirement for cybersecurity positions within the United States. Parker and Brown [36] and [37] found that these position requirements were also common internationally through their analyses of cybersecurity positions in South Africa and Morocco, respectively. Although these analyses primarily examined IT-focused cybersecurity roles, their results suggest several key position requirements to examine for an analysis on OT cybersecurity roles.

Additionally, it is notable that many prior investigations tend to focus on long-term position requirements such as education and experience, rather than ephemeral trends such as specific software platforms, vendors, or technologies which may change more rapidly, and thus reduce the usefulness of insights for long-term strategic planning. Therefore, we focus our investigation on position requirements such as education, experience, and certifications, but also expand upon those traditional requirements to focus on several OT specific areas such as knowledge of OT frameworks and communications protocols. In total, our analysis primarily focuses on nine prerequisite or desired requirements for OT cybersecurity positions (Table 1).

Through this unique and expanded analysis we seek to provide insights on position requirements for OT cybersecurity roles which could be used to develop a roadmap for individuals seeking to enter the OT cybersecurity workforce, as well as informing higher education and training institutions which have OT-focused or even IT-focused cybersecurity programs on what skills, knowledge, and expertise are currently desired by OT cybersecurity employers. The results of our analysis may also be beneficial for employers and OT cybersecurity talent acquisition managers to better understand and adapt to potential obstacles created by certain position requirements which could lead to hiring bottlenecks, or the exclusion of potential talent due to certain prerequisites. Finally, our work may also be beneficial for organizations with converging IT-OT environments seeking to re-train and skill their current IT-focused cybersecurity units on OT cybersecurity best practices, through a better understanding of the general knowledge and skills requirements currently desired for OT cybersecurity professionals.

TABLE I. EXAMINED PRE-REQUISITE OR DESIRED REQUIREMENTS FOR OT CYBERSECURITY POSITIONS

Requirement	Description
Education	Possession of a secondary education diploma, higher education degree, or other vocational training
Experience	Prior full-time or part-time professional experience acquired through previous employment, internships, consulting, or projects
Certifications	Vendor-neutral or vendor-specific cybersecurity certifications
Programming	Knowledge and experience of a specific programming language
Clearance	Active status and possession of a United States (U.S.) security clearance
Travel	Ability to travel as needed as part of the position duties
Communication Skills	Verbal and written communication skills
Frameworks & Standards	Knowledge and experience with OT or IT industry standards and frameworks
Protocols	Knowledge and experience with OT or IT networking and communications protocols and protocol stacks

IV. METHODS

Fig. 2 provides a workflow of our data acquisition, data cleaning, and information extraction methods. Similar to [33] and [17] OT security job position data were acquired from two job aggregator platforms, Indeed.com and Google jobs.

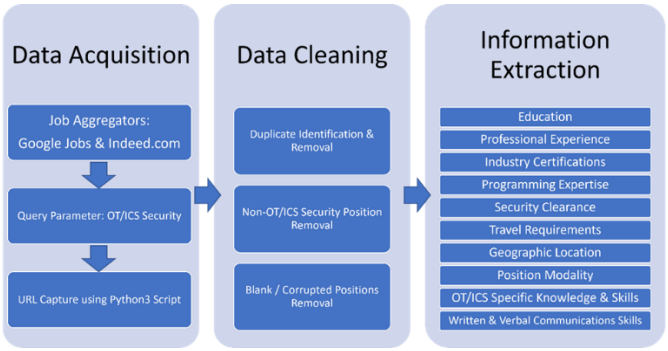

Fig. 2. Methodology workflow

Job aggregator websites can be particularly beneficial for acquiring a variety of job postings and positions within a given field of interest and are frequently used in analyses of position requirements and qualifications. Furthermore, job aggregators such as Indeed.com and Google Jobs often have standardized formats and informational fields such as qualifications and

responsibilities, which aid in the information extraction process [32].

Two job search queries were conducted on Indeed.com and Google Jobs on February 3rd, 2023 using a single search parameter: "OT/ICS Security". This search parameter was chosen as it was found to return the largest number of positions, while minimizing the number of IT or physical security related positions. Although we found that search parameters such as "ICS Security" or "industrial cybersecurity" returned a slightly larger number of positions, a pilot investigation revealed that many of the roles returned by these queries were IT, physical security, or law enforcement positions which would not be suitable for this analysis. Thus, we found that for this analysis, "OT/ICS Security" was the optimal search parameter.

To capture job positions that were not confined to a single geographic location or region, location information was not specified in the Indeed.com query, and the location range in the Google Jobs was set to "anywhere". It should be mentioned however, that it is possible that IP address localization or language preferences were used by both websites, as all positions returned by the query were located within the United States or the United Kingdom. Employer requirements, job type (e.g. Full-time, part-time, contract, internship), company type, and employer name were set to "All", so as not to limit the query search results to any pre-set criteria.

A Python3 script was written to capture the unique URL to each job posting from the results of both queries. In total, 175 positions were returned between both queries. Postings were inspected by the authors over the course of several weeks to avoid issues with analyst fatigue. 12 of the 175 positions were determined to be non-OT security positions such as a Business Development Manager for ICS, or a Senior Corporate Counsel which contained the terms OT or ICS within the job posting but would not be considered OT or ICS cybersecurity roles. One role was a cybersecurity internship for an undergraduate university program and was removed. Another role that was removed was an IT security role that contained only one OT security function within the position responsibilities. Furthermore, 61 positions were identified to be duplicates between both queries, resulting in 100 unique positions.

Multiple information fields were extracted, including the position title, company name, city, state, modality (in-person, remote, hybrid), type (full-time, part-time, contract, etc), compensation, prior professional experience, educational degree level, degree field/major, industry certification, programming language, security clearance, travel requirement, travel percentage, as well as the full position responsibilities, and the full position qualifications.

Due to small variations in language and formatting between different job posts, a series of rules were set up to guide and standardize the information extraction process. For example, as several positions listed a range of professional experience requirements (i.e. 4-5 years), experience was recorded at the minimum required years of experience to obtain the position. Furthermore, if the experience requirement varied depending on educational level (e.g. High school diploma with 5 years' experience, or Bachelors degree with 3 years' experience), the experience requirement was listed at the Bachelors degree level. In addition, positions were assumed to be full-time and in-person unless explicitly stated otherwise in the job posting.

It should also be mentioned that while automated text analysis approaches such as machine learning classifiers and natural language processing were considered, given the size of the dataset, a manual analysis was determined to be feasible. However, automated approaches may be warranted in similar analyses incorporating larger datasets.

V. Results

Fig. 3 provides a summary of the percentage of positions listing a specific position requirement. Out of the 100 analyzed job postings, 95 postings listed either an educational, professional experience, certification, programming expertise, or security clearance as a prerequisite for employment. The other five postings included a description of the position and various job responsibilities but did not include any pre-requisite qualifications or requirements for employment. Despite part-time and contract positions being included in both queries, almost all positions were full-time, except for one position, an OT/ICS Security Architect which was specifically listed as a contract-based position.

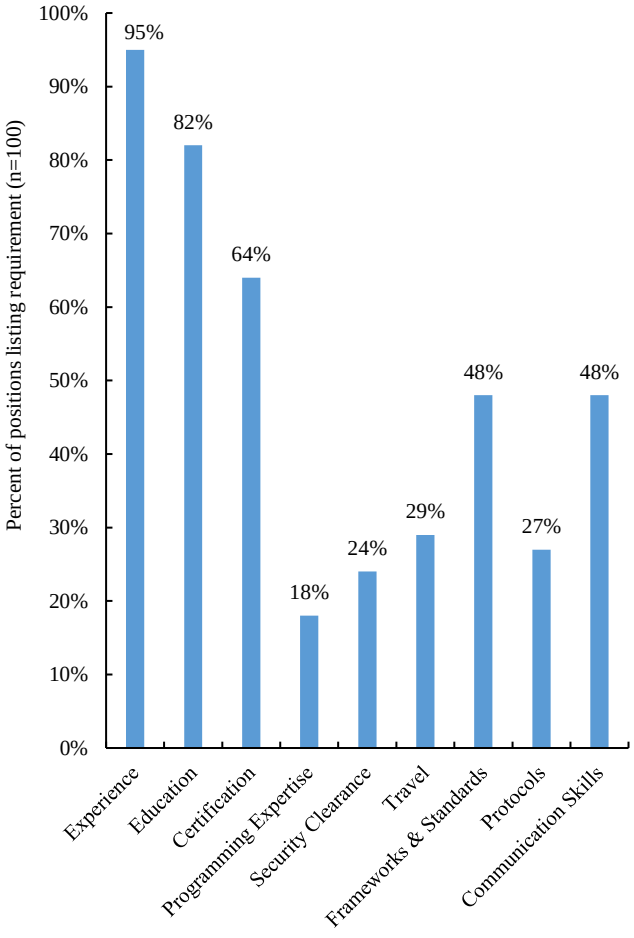

Fig. 3. Percent of positions listing a specific type of position requirement

Experience, education, and industry certifications were the most frequently listed requirements. 57% of positions required a combination of experience, education, and possession of an industry certification as a prerequisite for employment, while 24% of positions had listed an education and experience requirement (Fig. 4).

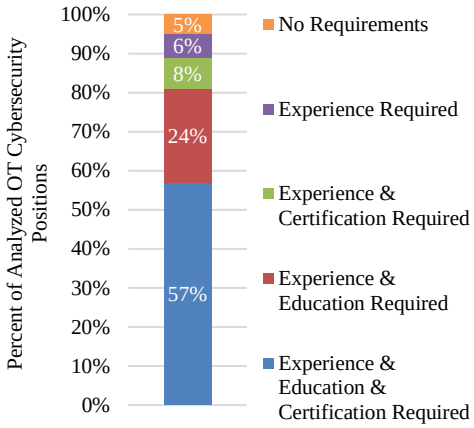

Fig. 4. Percent of positions listing experience, education, and certification requirements

Some level of prior professional experience was universally required on all positions which listed pre-requisite requirements. Interestingly, knowledge of OT frameworks and either strong verbal or written communication skills were required on 48% of all analyzed positions. Knowledge of OT protocols were listed on 27% of positions, while possession of an active U.S. security clearance and programming expertise were listed on 24% and 18% of positions, respectively. Additionally, 29% of analyzed OT cybersecurity postings required some form of regular travel as part of the position responsibilities.

Before diving into specifics on each job requirement category, it's notable that job titles in our dataset were highly diverse, with positions ranging from senior-level management focused roles such as a Deputy Chief Information Security Officer for Operational Technology, to highly technical roles such as a Sr. Systems Engineer - Principal ICS/SCADA Cyber Engineer or a Senior OT Penetration Tester.

Industrial Control Systems Cybersecurity Engineer was the most frequent common job title, consisting of 10% of analyzed positions. 40 out of 100 position titles contained the term "Engineer", while 11 out of 100 titles contained the word "Analyst". "Consultant" and "Specialist" were also frequent occurrences, appearing on 8 positions each.

While engineer was the most common job title for OT cybersecurity positions, there was considerable variation even within OT cybersecurity engineer titles, which suggests a lack of standardization and consistency of job titles within the OT cybersecurity field. Similar inconsistencies have been found in job postings in other fields such as IT cybersecurity [38], and nursing [39], which can lead to confusion about position expectations and responsibilities. Fig. 5 visualizes the top 50 most common terms used in OT job titles in a word cloud scaled by frequency of listing.

Fig. 5. Word cloud of OT cybersecurity job titles scaled by frequency of appearance

A. *Experience*

Prior professional experience was the most frequently requested prerequisite requirement for OT cybersecurity positions. 95 out of 100 analyzed positions required some form of professional experience. Of the 95 positions which did list an experience requirement, 8 positions required experience but did not provide a specific number of required years of experience. As for the 87 positions which did list a numeric experience requirement, desired years of experience ranged from 1 to 15 years, with an average of 7.9 years of experience required. The median experience requirement of all analyzed positions was 5 years. Over a quarter of positions required 5 years of professional experience, while 77% of positions required 3 years or more experience. This is notable as it suggests entry-level positions in OT security are uncommon, which could present an obstacle for college graduates or individuals with minimal experience seeking to transition into an OT security role. Obtaining several years of prior professional experience in either IT security, engineering, systems administration, or a related field before transitioning into an OT cybersecurity role also seems to be a viable pathway for employment in the OT cybersecurity sector. Fig. 6 provides the distribution of professional experience requirements among analyzed OT cybersecurity positions.

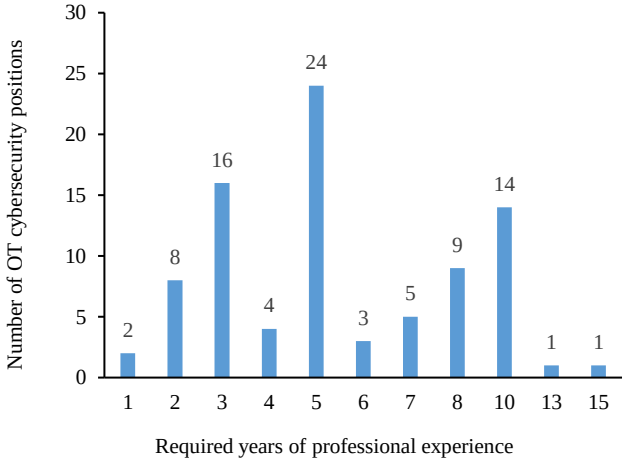

Fig. 6. Experience requirements for analyzed OT cybersecurity roles.

B. *Education*

Possession of a higher education degree or other academic credential was also a common requirement for OT cybersecurity positions. 82% of positions listed an educational requirement. A bachelor's degree was the most frequently requested academic credential, listed on 77 out of 100 positions. Master's degrees were listed on 16% of analyzed positions. Positions requesting doctoral degrees were relatively rare, with only 5 out of 100 positions listing a doctoral degree as a desired educational requirement. One position required a high school diploma, while 4 other positions required an academic degree, but did not specify the level of degree required. Computer science was by far the most frequently listed major, listed on half of all positions, followed by engineering, and cybersecurity, which were listed on 28% and 23% of positions, respectively. The top 10 most frequently listed majors are shown in Table 2.

TABLE II. FREQUENTLY LISTED DEGREE MAJORS

Major	Number of positions (*n*=100)
Computer Science	50
Engineering (non-specific)	28
Cybersecurity	23
Electrical Engineering	19
Information Systems	18
Computer Engineering	12
Information Technology	11
Information Assurance	6
Information Security	4
Systems Engineering	3

C. *Certifications*

We found that industry certifications were also frequently listed as a prerequisite requirement for OT cybersecurity roles, as 64% of analyzed positions included a certification as a requirement for employment. In total we identified 52 unique certifications listed among the 100 analyzed positions. While the number of certifications is seemingly large, this is unsurprising given the number and variety of cybersecurity certifications currently offered within industry. Fig. 7 visualizes the various certifications in a word cloud, scaled by frequency of appearance. It should also be mentioned that several positions also listed non-specific certifications from hardware and software vendors (i.e. Microsoft, Cisco, Splunk, Palo Alto, Amazon Web Services), or vendor-neutral certification associations such as CompTIA, ISACA or ISC2 along with requesting specific certifications.

Fig. 7. Word cloud of industry certifications scaled by frequency of appearance

We found that the Certified Information Systems Security Professional (CISSP) and the GIAC Global Industrial Cyber Security Professional (GICSP) certifications were by far the most frequently requested certification and were listed on 38% and 29% of analyzed positions, respectively. Aside from the GICSP, and the Certified SCADA Security Architect (CSSA), which was listed on 9 positions, most of the desired certifications are IT-focused cybersecurity certifications. While unsurprising given the relative rarity of OT-focused certifications, the prevalence of traditional IT-focused certifications in OT jobs could be advantageous for individuals seeking to transition from IT to OT security who already possess IT security certifications such as college graduates or IT security professionals. Certifications which were listed on five or more positions are included in Table 3.

TABLE III. FREQUENTLY LISTED INDUSTRY CERTIFICATIONS

Certification	Positions (*n*=100)
Certified Information Systems Security Professional (CISSP)	38
GIAC Global Industrial Cyber Security Professional (GICSP)	29
Certified Information Security Manager (CISM)	18
Certified Ethical Hacker (CEH)	17
Certified Information Systems Auditor (CISA)	12
CompTIA Security+	10
Global Information Assurance Certification (GIAC)	9
Certified SCADA Security Architect (CSSA)	9
Cisco Certified Network Associate (CCNA)	7
Offensive Security Certified Professional (OSCP)	5
GIAC Security Essentials (GSEC)	5
GIAC Certified Incident Handler (GCIH)	5

D. Programming Skills

Programming skills were listed on 18 out of 100 analyzed positions as prerequisites for employment. We identified 19 unique programming languages that were requested for OT cybersecurity roles, including Python, PowerShell, C++, bash, C, Java, SQL, Perl, assembly, go, JavaScript, C#, Visual Basic, .NET, HTML, MATLAB, Rust, PHP, and Ruby. Python was the most frequently requested language and was listed on 13 out of the 18 positions with a programming requirement. PowerShell and C++ were the second and third most frequently desired languages, listed on 6 and 5 positions, respectively. All of the other languages were mentioned on less than 5 positions each. Despite the variety of languages listed, it is surprising that programming skills were not a frequently desired prerequisite for OT cybersecurity positions.

E. Security Clearances

Security clearances were required for 24% of analyzed positions. Top Secret / Sensitive Compartmented Information (TS/SCI) clearance was the most frequently requested clearance level and was listed on 9 positions. Other clearance levels such as Department of Energy Q clearance, Secret, and Department of Energy L clearance were listed on 6, 3, and 1 position, respectively. Seven positions curiously listed a clearance requirement but did not specify the level of security clearance. Finally, two positions listed a Department of Homeland Security (DHS) clearance but did not provide any further details.

F. Travel Requirements

Work travel was required on 29% of positions, however only 18 out of 29 positions listed an actual percentage of responsibilities dedicated to travel. Travel percentages tended to widely vary, from the lowest at 5% to a high of 51-75% of an OT cybersecurity position dedicated to travel. Notably, there did not seem to be any work travel percentage that seemed to be frequent, which suggests that travel expectations for OT positions are not standardized and are highly dependent upon the nature of the position.

G. Communication Skills

Written and verbal communication skills were frequently listed as a desired pre-requisite for OT cybersecurity roles. In total, 48% of analyzed positions listed verbal communication skills among desired job qualifications, while 41% of positions included written communication skills as a desired qualification for employment. Nearly all roles specifically included the term "strong" when requesting written or verbal communication skills. Given the technical nature of the analyzed positions, the prevalence of verbal and written communication skills among OT cybersecurity roles was unexpected and suggests that good soft communication skills are important within the OT cybersecurity field. Given the need for communications between professionals with engineering backgrounds versus professionals with cybersecurity backgrounds, soft skills can be seen to be an important requirement for a holistic approach to realistic usability and cybersecurity practice within an OT enterprise.

H. Frameworks, Standards, and Protocols

Knowledge of several OT industry standards and frameworks were frequently listed as part of the requirements for OT cybersecurity positions. Out of the 100 analyzed positions, 48 listed one or more industry standard or framework within the job posting. The International Electrotechnical Commission (IEC)-62443 standard was listed on 30 positions and was the most frequently requested standard. As the IEC-62443 series is considered one of the major global standards for OT and is often the foundation for many industry specific standards, it's unsurprising that it's the most frequently listed standard on OT positions. There also seems to be a lack of standardization of the nomenclature of IEC 62443, as several positions also listed the International Society of Automation (ISA)-99 standard either in place of, or alongside IEC-62443. It should be noted that these terms are essentially referring to the same series of standards. As the ISA-99 committee developed many of the foundations of what would eventually become IEC 62443, it's understandable how these terms are used interchangeably, although IEC 62443 is the correct nomenclature for the standard.

In addition to IEC 62443, the National Institute of Standards and Technology Special Publication 800-82 (NIST 800-82), Guide to Industrial Control Systems Security, and the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) standards were also listed on 22% and 17% of analyzed positions, respectively. Several IT cybersecurity standards and frameworks such as the NIST Cybersecurity Framework (NIST CSF) and International Standards Organization (ISO) 27001 and 27002 were also listed on several positions. Table 4 lists the following standards and frameworks by frequency of appearance on OT job postings.

TABLE IV. FREQUENTLY LISTED OT, IT FRAMEWORKS AND STANDARDS

Framework or standard	Number of positions (*n*=100)
IEC 62443	30
NIST 800-82	22
NERC CIP	17
NIST CSF	10
CIS	7
ISO 27001	7
NIST 800-53	6
ISO 27002	5

Knowledge of OT and IT networking standards and protocols were listed on 27 out of 100 analyzed positions. The most requested standards and protocols were the Transmission Control Protocol / Internet Protocol (TCP/IP) suite, Modbus, and Open Platform Communications (OPC), listed on 19, 18, and 16 positions, respectively. Ethernet, Distributed Network Protocol 3 (DNP3), and IEC 61850 were each listed on less than 10 positions. Although Modbus, OPC, and DNP3, specific to process engineering environments, are outdated from a security perspective, knowledge of these protocols was frequently

requested on positions which required knowledge of OT and IT networking standards and protocols, which suggests that working many OT positions may require knowledge of and ability to work with legacy protocols and equipment. In general, knowledge of protocols and frameworks specific to engineering environments for an OT-focused cybersecurity role is valuable.

VI. Discussion

In our analysis of OT cybersecurity job postings, we found experience, education, and possession of an industry cybersecurity certification were common prerequisite requirements for OT cybersecurity positions. The possession of prior professional experience is considered particularly valuable as some level of experience was almost universally requested for OT cybersecurity roles. As over three out of four analyzed positions required 3 years or more of prior professional experience, positions requiring entry levels of experience were relatively rare, which could present a challenge for recent college graduates or individuals seeking to transition into OT security roles with minimal levels of experience. Steep experience requirements were also found by prior analyses on IT security job descriptions [17], [34]. While entry level OT cybersecurity positions do exist, given the average years of experience of analyzed OT cybersecurity positions in this analysis was 7.9 years, it can be argued that the typical OT cybersecurity position is not entry level, with employers often seeking individuals with advanced years of experience in OT or IT security.

Possession of a bachelors degree or higher in related areas such as computer science, engineering, cybersecurity, or information systems would be advantageous for obtaining or transitioning into an OT cybersecurity role. While not as frequently requested as professional experience or education, the possession of an industry certification was also a common requirement for OT cybersecurity positions. Certifications such as the CISSP, GICSP, CISM, and CEH are often required for OT security roles. The prevalence of more traditional IT-focused cybersecurity certifications such as the CISSP and CISM in OT cybersecurity roles in notable, however this may be due in part to the small number of OT or ICS focused cybersecurity certifications currently in industry, when compared to the large number of IT cybersecurity certifications. Additionally, while there are distinct differences between OT and IT security practices, much of the content in vendor-neutral certifications such as the CISSP or CISM focus on general cybersecurity concepts which could be applied to both IT and OT security paradigms.

Knowledge of OT or IT frameworks and verbal or written communications skills were listed on nearly half of all analyzed positions. While the knowledge of industry frameworks such as IEC 62443 and NERC CIP were expected, given the widespread adoption of such frameworks in numerous sectors, the prevalence of positions which listed strong verbal or written communication skills was quite surprising, given the technical nature of most of the analyzed positions. This suggests that written and verbal skills are highly valuable in OT cybersecurity roles, and such soft skills should be included in education and training programs which focus on OT or ICS security. Conversely, we also found that knowledge of OT or IT communications protocols and security clearances were slightly less common and were listed on roughly one out of every four analyzed positions. Programming expertise was listed on less than one out of five analyzed positions, while a travel requirement was listed on nearly three out of ten analyzed job postings.

Based upon the results of our analysis, we recommend for early career aspiring OT security professionals to obtain a degree in cybersecurity or a related technical field, preferably computer science, engineering, or information systems, while obtaining an industry certification such as the CISSP or GICSP. As the CISSP requires 5 years of prior related experience before certification, a more entry level certification such as the CEH, Security+, GIAC, or CSSA would also be advisable. Additionally, obtaining prior IT or OT cybersecurity experience whether through internships, co-ops, or full-time positions would be highly advisable. Finally, good verbal and communication skills, as well as knowledge of industry frameworks would also be advantageous.

For more experienced individuals with IT security or ICS engineering backgrounds, experience may be less of a barrier for obtaining an OT security role, so obtaining a more senior certification such as the CISSP, CISM, CISA, or an OT or ICS focused certification such as the GICSP or CSSA would be advisable. Furthermore, knowledge of OT industry standards and frameworks such as IEC 62443, NERC CIP, and NIST 800-82 would be advantageous for transitioning into an OT security role. Also, for organizations that are seeking to retrain their IT security personnel, additional education, whether through training programs which familiarize personnel with OT frameworks and protocols, OT or ICS focused certifications, or formal degree programs such as a graduate degree in OT-focused cybersecurity programs, engineering, computer science, or information systems may be worthwhile.

As prior research [19] has suggested that major cybersecurity curriculum guidance documents such as the NICE framework or the National Security Agency Centers of Academic Excellence Knowledge Units (NSA-CAE KU), do not adequately address OT or industrial cybersecurity to the levels desired by industry, higher education program must think beyond these current frameworks and assess what knowledge and skills are currently needed to defend OT environments.

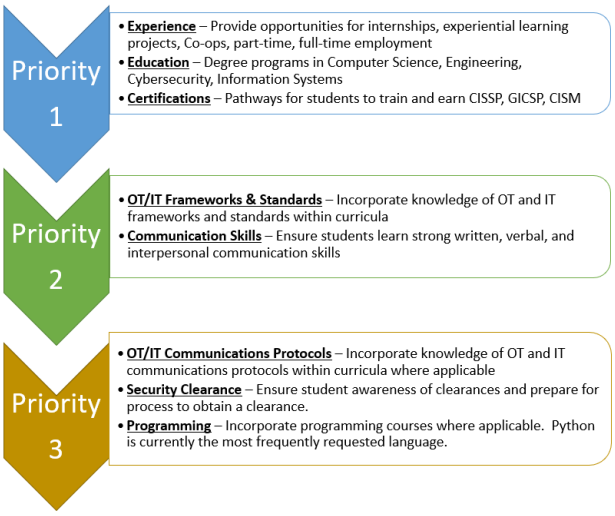

Fig. 8. Higher education roadmap of priorities for OT cybersecurity positions requirements

Summarized in Fig. 8, based on the results of this analysis we suggest that if cybersecurity programs in higher education want to produce the next generation of OT cybersecurity professionals, they should in-part structure their curriculum to include major OT frameworks and protocols, and align courses to train students for industry certifications such as the CISSP or GICSP. Development of communications skills should also be an integral part of the curriculum. A major priority of OT cybersecurity education programs should be to focus on the importance of hands-on experiential learning, internships, and employment opportunities in OT or IT cybersecurity to enable students to obtain professional experience as early as possible. Ensuring students have a strong knowledge of OT and IT communication protocols would also be beneficial, even though this was not as frequently listed as other requirements. Courses in programming, as well as preparing students for the security clearance process, can also be beneficial, but are less of a priority.

It should be noted that our study had several limitations. While our analysis included a larger sample size than previous analyses [19], our sample size of OT cybersecurity positions was limited, and only included OT cybersecurity positions within the United States, and the United Kingdom. Additionally, our dataset was a snapshot in time, as the initial queries for data acquisition were conducted on a single day. While we endeavored to avoid more ephemeral categories such as specific technologies or vendors which are subject to rapid change, given the dynamic and rapidly changing nature of the cybersecurity field, it's highly likely that certain insights, such as the popularity of programming languages, or industry certifications may change with time. Thus, we suggest that future research on this subject include an expanded dataset that was captured over a longer period, to capture more long-term qualification trends in the OT cybersecurity field, and potentially identify position requirement fields that are highly dynamic. Additionally, a comparative analysis of IT and OT position requirements would also be interesting to highlight the commonalities and differences between the fields. Furthermore, textual analysis using automated methods, and machine learning data mining techniques may also reveal further insights on OT cybersecurity position requirements that were not found in this analysis.

VII. Conclusion

In summary our analysis provided several key insights on OT cybersecurity position requirements which may serve as a barrier of entry to aspiring OT cybersecurity professionals. Prior professional experience requirements for OT cybersecurity positions tend to be steep, as OT cybersecurity positions tend not to have entry-level requirements. In addition to professional experience, a higher education degree in computer science, cybersecurity, engineering, or information systems, and possession of an industry certification such as the CISSP or GICSP are also commonly desired for OT cybersecurity positions. Knowledge of relevant OT and IT industry frameworks and protocols, as well as strong verbal and written communication skills are also frequent requirements. Work travel, and security clearances are also common, but not always required for OT cybersecurity roles. If organizations are facing an OT cybersecurity talent shortage, lowering position requirements such as years of experience, or senior-level certifications may widen the potential talent pool. Furthermore, to continue to train the next generation of OT cybersecurity professionals, higher education and training programs should note the position requirements highlighted in this analysis and adapt their curriculum to include relevant OT frameworks and protocols, soft skill communications, as well as assist students with obtaining professional experience and industry certifications to best meet the current requirements of the OT cybersecurity workforce.

References

[1] L. A. Maglaras et al., "Cyber security of critical infrastructures," ICT Express, vol. 4, no. 1, pp. 42–45, Mar. 2018, doi: 10.1016/j.icte.2018.02.001.

[2] W. Harrop and A. Matteson, "Cyber resilience: a review of critical national infrastructure and cyber security protection measures applied in the UK and USA," J Bus Contin Emer Plan, vol. 7, no. 2, pp. 149–162, 2014 Winter 2013.

[3] R. Langner, "Stuxnet: dissecting a cyberwarfare weapon," IEEE Secur. Privacy Mag., vol. 9, no. 3, pp. 49–51, May 2011, doi: 10.1109/MSP.2011.67.

[4] M. Geiger, J. Bauer, M. Masuch, and J. Franke, "An analysis of Black Energy 3, Crashoverride, and Trisis, three malware approaches targeting operational technology systems," in 2020 25th IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Vienna, Austria: IEEE, Sep. 2020, pp. 1537–1543. doi: 10.1109/ETFA46521.2020.9212128.

[5] L. L. Dhirani, E. Armstrong, and T. Newe, "Industrial IoT, cyber threats, and standards landscape: evaluation and roadmap," Sensors, vol. 21, no. 11, p. 3901, Jun. 2021, doi: 10.3390/s21113901.

[6] S. Z. Kamal, S. M. Al Mubarak, B. D. Scodova, P. . Naik, P. . Flichy, and G. . Coffin, "IT and OT convergence - opportunities and challenges," in All Days, Aberdeen, Scotland, UK: SPE, Sep. 2016, p. SPE-181087-MS. doi: 10.2118/181087-MS.

[7] I. C. Ehie and M. A. Chilton, "Understanding the influence of IT/OT convergence on the adoption of internet of things (IoT) in manufacturing organizations: An empirical investigation," Computers in Industry, vol. 115, p. 103166, Feb. 2020, doi: 10.1016/j.compind.2019.103166.

[8] P. K. Garimella, "IT-OT integration challenges in utilities," in 2018 IEEE 3rd International Conference on Computing, Communication and Security (ICCCS), Kathmandu: IEEE, Oct. 2018, pp. 199–204. doi: 10.1109/CCCS.2018.8586807.

[9] H. Alkahtani and T. H. H. Aldhyani, "Developing cybersecurity systems based on machine learning and deep learning algorithms for protecting food security systems: industrial control systems," Electronics, vol. 11, no. 11, p. 1717, May 2022, doi: 10.3390/electronics11111717.

[10] M. Sekar, "SCADA and operational technology," in Machine learning for auditors, Berkeley, CA: Apress, 2022, pp. 131–135. doi: 10.1007/978-1-4842-8051-5_12.

[11] S. Singh, H. Karimipour, H. HaddadPajouh, and A. Dehghantanha, "Artificial intelligence and security of industrial control systems," in Handbook of big data privacy, K.-K. R. Choo and A. Dehghantanha, Eds., Cham: Springer International Publishing, 2020, pp. 121–164. doi: 10.1007/978-3-030-38557-6_7.

[12] S. Mubarak, M. Hadi Habaebi, M. Rafiqul Islam, F. Diyana Abdul Rahman, and M. Tahir, "Anomaly detection in ICS datasets with machine learning algorithms," Computer Systems Science and Engineering, vol. 37, no. 1, pp. 33–46, 2021, doi: 10.32604/csse.2021.014384.

[13] S. Koelemij, "The OT security skills gap," Industrial Cyber, May 09, 2022. https://industrialcyber.co/threat-landscape/the-ot-security-skills-gap/ (accessed Jun. 13, 2023).

[14] B. Siemers et al., "Modern trends and skill gaps of cyber security in smart grid : Invited Paper," in IEEE EUROCON 2021 - 19th International Conference on Smart Technologies, Lviv, Ukraine: IEEE, Jul. 2021, pp. 565–570. doi: 10.1109/EUROCON52738.2021.9535632.

[15] T. Caldwell, "Plugging the cyber-security skills gap," Computer Fraud & Security, vol. 2013, no. 7, pp. 5–10, Jul. 2013, doi: 10.1016/S1361-3723(13)70062-9.

[16] M. J. Cobb, "Plugging the skills gap: the vital role that women should play in cyber-security," Computer Fraud & Security, vol. 2018, no. 1, pp. 5–8, Jan. 2018, doi: 10.1016/S1361-3723(18)30004-6.

[17] C. A. Ramezan, "Examining the cyber skills gap: An analysis of cybersecurity positions by sub-field," Journal of Information Systems Education, vol. 34, no. 1, pp. 94–105, 2023.

[18] R. Vogel, "Closing the cybersecurity skills gap," Salus Journal, vol. 4, no. 2, pp. 32–46, 2016.

[19] I. Ngambeki, S. McBride, and J. Slay, "Knowledge gaps in curricular guidance for ICS security," CISSE, vol. 9, no. 1, p. 6, Mar. 2022, doi: 10.53735/cisse.v9i1.149.

[20] K. Stouffer, M. Pease, C. Tang, T. Zimmerman, V. Pillitteri, and S. Lightman, "Guide to operational technology (OT) security: initial public draft," preprint, Apr. 2022. doi: 10.6028/NIST.SP.800-82r3.ipd.

[21] P. Ganguly, M. Nasipuri, and S. Dutta, "Challenges of the existing security measures deployed in the smart grid framework," in 2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE), Oshawa, ON, Canada: IEEE, Aug. 2019, pp. 1–5. doi: 10.1109/SEGE.2019.8859917.

[22] H. Wu, M. Jiang, and M. Cen, "An integrated security framework for OT system based on edge computing," in 2022 IEEE 21st International Conference on Ubiquitous Computing and Communications (IUCC/CIT/DSCI/SmartCNS), Chongqing, China: IEEE, Dec. 2022, pp. 9–16. doi: 10.1109/IUCC-CIT-DSCI-SmartCNS57392.2022.00016.

[23] G. Murray, M. N. Johnstone, and C. Valli, "The convergence of IT and OT in critical infrastructure," Australian Information Security Management Conference, 2017, doi: 10.4225/75/5A84F7B595B4E.

[24] A. Abzakh, A. A. Alkhatib, O. Rabayah, S. Elmanaseer, R. N. Albustanji, and N. Almadi, "A survey: threat junting for the OT systems," in 2023 International Conference on Information Technology (ICIT), Amman, Jordan: IEEE, Aug. 2023, pp. 130–134. doi: 10.1109/ICIT58056.2023.10225758.

[25] Y. Maleh, "IT/OT convergence and cyber security," Computer Fraud & Security, vol. 2021, no. 12, pp. 13–16, Dec. 2021, doi: 10.1016/S1361-3723(21)00129-9.

[26] Wm. A. Conklin, "IT vs. OT security: a time to consider a change in CIA to include resilience," in 2016 49th Hawaii International Conference on System Sciences (HICSS), Koloa, HI, USA: IEEE, Jan. 2016, pp. 2642–2647. doi: 10.1109/HICSS.2016.331.

[27] M. Mesbah, M. S. Elsayed, A. D. Jurcut, and M. Azer, "Analysis of ICS and SCADA systems attacks using honeypots," Future Internet, vol. 15, no. 7, p. 241, Jul. 2023, doi: 10.3390/fi15070241.

[28] S. Kropatschek et al., "Combining models for safety and security concerns in automating digital production," in 2023 IEEE 21st International Conference on Industrial Informatics (INDIN), Lemgo, Germany: IEEE, Jul. 2023, pp. 1–8. doi: 10.1109/INDIN51400.2023.10218184.

[29] O. Peter, A. Pradhan, and C. Mbohwa, "Industrial internet of things (IIoT): opportunities, challenges, and requirements in manufacturing businesses in emerging economies," Procedia Computer Science, vol. 217, pp. 856–865, 2023, doi: 10.1016/j.procs.2022.12.282.

[30] D. Goldberg and N. Zaman, "Text analytics for employee dissatisfaction in human resources management," in Advances in Management Information Systems Research (General Track), 2018.

[31] A. Ho, A. Nguyen, J. L. Pafford, and R. Slater, "A data science approach to defining a data scientist," SMU data science review, vol. 2, no. 3, 2019, [Online]. Available: https://scholar.smu.edu/datasciencereview/vol2/iss3/4

[32] A. Verma, K. M. Yurov, P. L. Lane, and Y. V. Yurova, "An investigation of skill requirements for business and data analytics positions: A content analysis of job advertisements," Journal of Education for Business, vol. 94, no. 4, pp. 243–250, May 2019, doi: 10.1080/08832323.2018.1520685.

[33] A. Verma, K. Lamsal, and P. Verma, "An investigation of skill requirements in artificial intelligence and machine learning job advertisements," Industry and Higher Education, vol. 36, no. 1, pp. 63–73, Feb. 2022, doi: 10.1177/0950422221990990.

[34] A. Peslak and S. Hunsinger D., "What is cybersecurity and what cybersecurity skills are employers seeking?," IIS, vol. 20, no. 2, pp. 62–72, 2019, doi: 10.48009/2_iis_2019_62-72.

[35] J. Marquardson and A. Elnoshokaty, "Skills, certifications, or degrees: what companies demand for entry-level cybersecurity jobs," Information Systems Education Journal, vol. 18, no. 1, pp. 22–28, 2020.

[36] A. Parker and I. Brown, "Skills requirements for cyber security professionals: a content analysis of job descriptions in South Africa," in Information Security, H. Venter, M. Loock, M. Coetzee, M. Eloff, and J. Eloff, Eds., in Communications in Computer and Information Science, vol. 973. Cham: Springer International Publishing, 2019, pp. 176–192. doi: 10.1007/978-3-030-11407-7_13.

[37] I. Rahhal, I. Makdoun, G. Mezzour, I. Khaouja, K. Carley, and I. Kassou, "Analyzing cybersecurity job market needs in Morocco by mining job ads," in 2019 IEEE Global Engineering Education Conference (EDUCON), Dubai, United Arab Emirates: IEEE, Apr. 2019, pp. 535–543. doi: 10.1109/EDUCON.2019.8725033.

[38] C. M. Graham and Y. Lu, "Skills expectations in cybersecurity: semantic network analysis of job advertisements," Journal of Computer Information Systems, pp. 1–13, Sep. 2022, doi: 10.1080/08874417.2022.2115954.

[39] A. Leary, K. Maclaine, P. Trevatt, M. Radford, and G. Punshon, "Variation in job titles within the nursing workforce," J Clin Nurs, vol. 26, no. 23–24, pp. 4945–4950, Dec. 2017, doi: 10.1111/jocn.13985.