CONNECTING O*NET® DATABASE TO CYBERSECURITY WORKFORCE PROFESSIONAL CERTIFICATIONS

Micheline Al Harrack

Department of Data Science, Information Technology, and Cybersecurity College of Business, Innovation, Leadership, and Technology Marymount University, Virginia, USA

ABSTRACT

*The Occupational Information Network O*NET is considered the primary source of occupational information in the U.S. I explore here possible uses of O*NET data to inform cybersecurity workforce readiness certification programs. The O*NET database is used to map out education requirements and how they relate to professional certifications as required by employers and job designers in accordance with the National Initiative for Cybersecurity Careers and Studies (NICCS). The search focuses on the "Information Security Analysts" occupation as listed on O*NET, Careeronestop, U.S. Bureau of Labor Statistics (BLS), and finally tied back to NICCS source work role to identify certifications requirements. I found that no site has listed any certification as required, desirable or mandatory. NICCS offered general guidance to potential topics and areas of certification. Careeronestop site provided the ultimate guidance for this role certification. Professional certifications are still not integrated in the Cybersecurity Workforce Framework official guidance.*

KEYWORDS

*Occupational Information Network O*NET, NICE Framework, NICCS, Cybersecurity Certification & Information Security Analyst*

1. INTRODUCTION

The Occupational Information Network (O*NET) is sponsored by the U.S. Department of Labor and the Employment and Training Administration (USDOL/ETA). It is considered a reliable source for occupational information for employers, job seekers, recruiters, and learners alike. The O*NET website was launched in 1998 by the U.S. Department of Labor (DOL). In this study, I consider the three major instruments in O*NET®: The Content Model that breaks down the anatomy of each occupation, the Standard Occupational Classification O*NET-SOC taxonomy that covers a wide set of work occupations, and finally the publicly available O*NET® database listing hundreds of occupations with standardized descriptions across all sectors of the U.S. economy. The O*NET® database is updated primarily in the third quarter of each year to reflect relevant changes as introduced by job incumbents and experts [1]. At the heart of this Content Model is the framework organizing the characteristics of occupational data into what is referred to as hierarchically structured taxonomy comprised of six categories or "domains" [2]. The O*NET® project revolves essentially around the valuable electronic database containing information designed to help students, educators, job seekers, employers, and workforce trainers and developers, among others. This data collection system organized job titles into more than 1,102 occupations as of July 2020 and down to 1016 occupational listings as of June 2021[3]. As more workers seek to enter the cybersecurity labor force or think of themselves as cybersecurity

professionals based on their roles, experience, and specific expertise, some seek activities related to professionalization leading to certifications [4]. Certifications can be driven by an employer's needs and requirements or by the government objectives to manage the workforce and establish a baseline for technical skills verifying federal workforce knowledge through standard certification [5] or to incorporate specific activities, occupations, and work roles into its operations [6]. I ask if O*NET explores possible uses of O*NET® data to inform workforce readiness certification programs. To answer this question in this research, I use the O*NET database to map out education requirements and how they relate to professional certifications as required by the employers and job designers in accordance with the National Initiative for Cybersecurity Careers and Studies NICCS. The search focuses on the "Information Security Analysts" occupation as listed on O*NET® with all related job titles, cross-referenced with Information Security Analysts on the U.S. Bureau of Labor Statistics site, on Careeronestop, the site sponsored by the Department of Labor (DOL), and mapped back to the NICCS work role titles "All-Source Analyst", and "Information Systems Security Manager". The study aims to establish a simple guide for professionals to align education requirements to potential certifications based on an occupation role for a clear pathway to a successful and sustainable career in cybersecurity.

2. BACKGROUND AND METHOD

The O*NET® foundational framework is based on a content model that integrates the most important components and type of information about work into a structured system. The occupational information is broken down into six areas: Worker characteristics, worker requirements, experience requirements, occupation-specific information, workforce characteristics, and occupational requirements. The worker-oriented attributes are the worker characteristics, worker requirements, and experience requirements. The job-oriented attributes are the occupational requirements, workforce characteristics, and occupation-specific information (see Figure 1, O*NET® Content Model). The model encompasses cross-occupational information that can be applied across different sectors, businesses, and industries while the occupational-specific descriptors are focused on each specific occupation. Prior to November 2020, the O*NET occupational listings of occupations in the data collection plan were categorized and coded based on the 2010 Standard Occupational Classification (SOC) which is a federal system used to classify workers into categories for data collection and analysis [7]. The current O*NET-SOC 2019 Taxonomy is based on the 2018 Standard Occupational Classification with 1016 occupations with 867 detailed SOC occupations broken down into 459 broad occupations with 98 minor groups and 23 major groups. Jobs with similar duties and skills or education requirements are grouped together. Out of 1,016 occupations, titles and data were provided for 923 while 93 had titles only listed. The O*NET-SOC 2019 updated content includes four cybersecurity-related emerging occupations: Penetration testers, information security engineers, digital forensics analysts, and blockchain engineers. The O*NET data dictionary provides a reference to relevant aspects of the listings of commodities in the United Nations Standard Products and Services Code (UNSPSC) as listed in the United Nations Development Programme (UNDP).

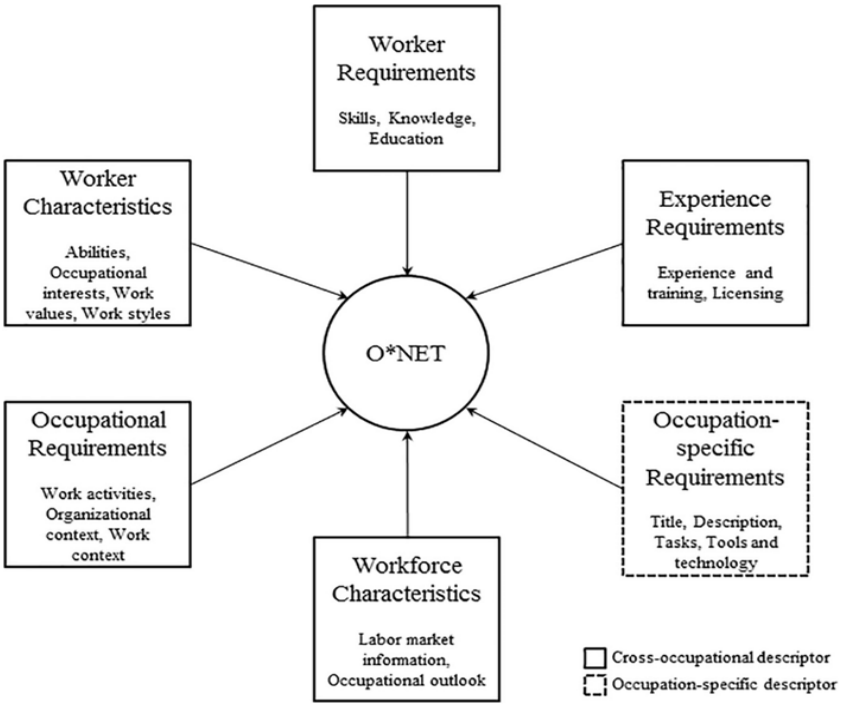

Figure 1. O*NET® Content Model [8]

2.1. O*NET® Content Model Analysis

The Content Model is comprised of six domains focused on information related to occupations. Three of these six domains are worker-oriented with the other three job-oriented. The first domain is worker characteristics which includes qualities on how to approach work and acquire relevant knowledge. These abilities are the most common criteria in job comparison, however occupational interests have been included to highlight work environment preferences in accordance with Holland's occupational personality types and career choices [9] to develop Occupational Interest Profiles (OIP). The first domain also covers work values comprised of work needs important for one's satisfaction based on the Theory of Work Adjustment (TWA) [10]. Finally, work styles are depicted based on personal characteristics impacting how well a job is approached and performed to develop Occupational Reinforcer Patterns (ORP). The second domain refers to worker requirements which are work-related attributes representing developed capacities to learn or acquire knowledge either in the form of basic skills like reading and writing or cross-functional skills, such as problem-solving or critical thinking, necessary to perform activities across jobs. Worker requirements include knowledge as an organized set of factors, facts, and principles that can be applied in different domains in addition to prior educational acquisition required for a job. The third domain covers previous work-activities such as experience and training required for a specific job, basic skills needed for entry requirements, cross-functional skills for activities performance across multiple job, and finally licenses, certifications, or training to document that a worker has gained certain relevant skills. This specifies the requirements for such credentials and the organization requesting their possession. In the job-oriented area, the first domain covers occupational requirements with information about activities across occupations. This section includes Generalized Work Activities (GWA) performed across all job families and industries, as well as intermediate work activities, and Detailed Work Activities (DWA) that are performed within a specific number of occupations within a job family. Social, physical, or organizational context that would influence how people do their work or the nature of the work are also included in this domain. The fifth domain covers the workforce characteristics that impact occupational

requirements. The descriptive occupational informational is tied to statistical labor data such as compensation, and industry size through collaboration with other governmental organizations such as Bureau of Labor Statistics (BLS), The Department of Commerce, The Department of Defense, the Bureau of the Census, and the Employment and Training Administration. Finally, the sixth domain covers occupation-specific information with the set of variables and elements to apply to each occupation or a specific job family. This domain includes work-related knowledge, occupation-specific tasks, technology, and software kills essential to the performance of this occupation, as well as tools, machines and equipment needed to perform this role. The title and the description are catalogued as per the O*NET -SOC taxonomy. Worker characteristics and occupational requirement are cross occupations descriptors while experience requirements and occupation-specific information are occupation-specific descriptors as can be inferred [11].

2.2. O*NET® Electronic Database

The second instrument in the O*NET model consists of a valuable electronic database containing information designed to help students, educators, job seekers, employers, workforce trainers, and workforce developers, among others. This data collection system organizes job titles into more than 1,102 occupations. The National Center for O*NET development continually collects data related to these occupations and identifies ways to improve data collection, use, efficacy, and efficiency. With the ever-evolving technology and new job titles, positions, and duties being added constantly to the workplace and workforce, the need to create a standard common description and acknowledged skills, abilities, and other related factors is crucial to stay current and relevant to the users for career and employment guidance as well as workforce development and human resource management. After exploring the site for cyber-related occupations, it appears that O*NET® framework does not explicitly list professional certifications required or recommended for cybersecurity jobs.

2.3. O*NET® Information Security Analyst Work Role Analysis

On the O*NET® site, the search is focused on the occupation "Information Security Analyst" to compare with the outcomes of All-Source Analyst, Information Systems Security Developer, and Information Systems Security Manager and draw connections for certificates recommended or required on the NICSS site. The summary report of Information Security Analyst contained a list of activities undertaken by an information security analyst each starting with a specific action verb: "Plan, implement, upgrade, or monitor security measures for the protection of computer networks and information. May ensure appropriate security controls are in place that will safeguard digital files and vital electronic infrastructure. May respond to computer security breaches and viruses" [12]. The Information Security Analyst work role includes a sample of related job titles: Data Security Administrator, Information Security Officer, Information Security Specialist, Information Systems Security Analyst, Information Systems Security Officer, Information Technology Security Analyst (IT Security Analyst), Information Technology Specialist, Network Security Analyst, Security Analyst, Systems Analyst. It lists 12 tasks, 51 technology skills, 8 knowledge areas, 15 related skills, 17 abilities, 21 work activities, 10 detailed work activities, 22 work context criteria. The education lists four-year degree for some jobs but not for all, some job-related skills, knowledge and experience, job training, with job zone examples. 53% of subjects surveyed reportedly hold a bachelor's degree, 23% a post –baccalaureate certification, and 13% an associate degree. The report is available in a detailed fashion with a customized option. The page provides a link to the International Information System Security Certification Consortium (ISC)2, the Computing Technology Industry Association (COMPTIA), Information Systems Audit and Control Association (ISACA), and National Initiative for Cybersecurity Education (NICE) among others as resources for additional information. O*NET® provides a crucial design for employers

and human resource professionals to employ job descriptions and selection tools pursuant to Americans with Disabilities Act (ADA) and Equal Employment Opportunity (EEO) requirements [13]. Recruitment officers and human resource personnel employ these detailed descriptions to design job titles, duties, and requirements to attract the needed workforce. Furthermore, the detailed skills, education requirements, experience, and other qualifications provide a framework for standard job description, requirements, and qualifications. An equally important function is to show that the knowledge, skills, abilities, and other characteristics (KSAO) employees need to do their work effectively are related to critical tasks to document the adequacy of hiring and the need for training and workforce development [14]. No certification requirement is listed. Under Credentials, Find Certifications link redirects to Careeronestop.

2.4. U.S Bureau of Labor Statistics: Information Security Analyst

The Bureau of Labor Statistics (BLS) estimates a faster-than-average growth rate in employment of information security analysts, a labor category that represents a significant subset of the cybersecurity workforce. The U.S. Bureau of Labor Statistics in its Occupational Outlook Handbook under Computer and Information Technology, summarizes the job outlook for an Information Security Analyst with quick facts, lists and bachelor's degree as a requirement for most related positions and links back to the O*NET® site for additional resources and information [15]. However, it is noted that, on how to become one, under Licenses, Certifications, and Registrations, BLS states that most employers prefer that employees hold certifications which validate knowledge required for an Information Security Analyst. It distinguishes between more generic certifications such as Certified Information Systems Security Professional (CISSP), and more specific ones like penetration testing and systems auditors specifically.

2.5. National Initiative for Cybersecurity Careers and Studies NICCS: All-Source Analyst

For validation purposes, I searched for this work role on the National Initiative for Cybersecurity Careers and Studies NICCS website under the NICE Cybersecurity Workforce Framework Work Role [16]. The Information Security Analyst is not listed independently rather it must be searched under All-Source Analyst work role title and any work role ID. This search resulted in the following description: "Analyzes data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and production requirements in support of planning and operations." [17]. The role description listed 18 abilities, 56 knowledge areas, 18 related skills, and 42 related tasks for all-source analyst. The capabilities indicators were listed by certification/credentials, education, continuous learning, and experiential learning and divided into three categories: entry level, intermediate, and advanced. Education was not essential for entry level with bachelor's as an example. For intermediate level, a Bachelor's degree was recommended. For advanced level, a Master's or Doctorate degree was recommended. As for certifications, for an entry level they were labeled as not essential but may be beneficial with potential areas covering new attack vectors such cloud computing and mobile platforms. Other areas included vulnerabilities, threats, audit, IT governance and management and information systems related topics without specifying designated commercial certificates. At the intermediate level, a certificate was recommended with topics covering security and risk management, security engineering, communications and network security, software development security, and identity and access management security among very defined security topics. At the advanced level, certifications were deemed not necessary but might be beneficial with focus on project management areas, other topics listed at the entry and intermediate level in addition to specific topics focusing on U.S. privacy laws and practice areas. For this work role, it is obvious that the O*NET® framework provides a valid context to generate KSAO and other related job requirements to compile job descriptions, roles, qualifications and

attract qualified workforce looking for a common standard in a more increasingly non-conventional world and workplace. However, the guidance is very generic, and the language is not authoritative as it relates to certifications. For comparison purposes, the Information Security Systems Manager had education recommended for all three levels starting with a bachelor's degree for the first two up to a Master's and Doctorate for an advanced level. However, certifications ere not essential for entry level but provided an extensive list of potential beneficial areas of certifications. Certificates were recommended for the other two levels with areas of focus identical on the intermediate level to the all-source analyst topics area, and more focused on security, risk, and management areas on the advanced level. The NICCS in its 2020 cybersecurity workforce toolkit stated "Earning certifications enables staff to stay current on in-demand skills and become leaders in the cybersecurity field" [18]. The three certifications listed were COMPTIA+, Certified Information Security Specialist CISSP, and GIAC Security Essentials (GSEC).

Work Role Name: All-Source Analyst - Work Role ID: AN-ASA-001 - Specialty Area: All-Source Analysis (ASA) - Category: Analyze (AN)

Work Role Description: Analyzes data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and production requirements in support of planning and operations.

Tasks: T0569, T0582, T0583, T0584, T0585, T0586, T0589, T0593, T0597, T0615, T0617, T0642, T0660, T0678, T0685, T0686, T0687, T0707, T0708, T0710, T0713, T0718, T0748, T0749, T0751, T0752, T0758, T0761, T0771, T0782, T0783, T0785, T0786, T0788, T0789, T0792, T0797, T0800, T0805, T0834

Knowledge: K0001, K0002, K0003, K0004, K0005, K0006, K0036, K0058, K0108, K0109, K0177, K0221, K0349, K0362, K0444, K0471, K0560, K0377, K0392, K0395, K0405, K0409, K0427, K0431, K0436, K0437, K0440, K0445, K0446, K0449, K0458, K0460, K0464, K0469, K0480, K0511, K0516, K0556, K0561, K0565, K0603, K0604, K0610, K0612, K0614, K0357, K0410, K0457, K0465, K0507, K0533, K0542, K0549, K0551, K0577, K0598
Skills: S0194, S0203, S0211, S0218, S0227, S0229, S0249, S0256, S0278, S0285, S0288, S0289, S0296, S0297, S0303, S0189, S0254, S0360

Abilities: A0013, A0066, A0080, A0084, A0072, A0082, A0083, A0085, A0087, A0088, A0089, A0091, A0101, A0102, A0106, A0107, A0108, A0109

The search in NICCS Education and Training Catalog for Information Security Analyst yielded 40 different training courses that had any combination of these keywords [19]

2.6. Careeronestop Certification Finder

Using the toolkit on the Careeronestop site and searching for "Information Security Analysts", the results included 116 certifications from 26 providers. These certifications are available by providers in a downloadable excel file. The providers included: Broadcom Inc., Amazon.com Web Services, Cisco Systems, EC-Council, IBM Corporation, Dell, Oracle, Microsoft, Wireshark, Global Information Assurance Certification, Hewlett Packard Certification and Learning, COMPTIA, International Information Systems Security Certification Consortium, Inc., and several other specific ones. The 116 certifications focused on different areas of information security and topics listed on NICCS site under the NICE Cybersecurity Framework roles for all-source analyst.

Table 1. Careeronestop certification finder

Certification	**Organization**
Administration of Data Center Security: Server Advanced 6.7	Broadcom Inc.
Administration of Symantec Client Management Suite 8.5	Broadcom Inc.
Administration of Symantec Cloud Workload Protection - R1	Broadcom Inc.
Administration of Symantec Data Loss Prevention 15.5	Broadcom Inc.
Administration of Symantec Email Security.cloud - v1	Broadcom Inc.
Administration of Symantec ProxySG 6.7	Broadcom Inc.
Administration of Symantic Security Analytics 8.0	Broadcom Inc.
Associate of International Information Systems Security Certification Consortium	International Information Systems Security Certification Consortium, Inc.
AWS Certified Security Specialty	Amazon.com Web Services
CCNA Cyber Ops Certification	Cisco Systems, Inc.
Certification Authorization Professional	International Information Systems Security Certification Consortium, Inc.
Certification in Risk and Information Systems Control	Information Systems Audit and Control Association
Certified Advanced Windows Forensic Examiner	International Association of Computer Investigative Specialists
Certified Application Security Engineer	EC-Council
Certified Cloud Security Professional	International Information Systems Security Certification Consortium, Inc.
Certified Computer Crime Investigator - Advanced	High Tech Crime Network
Certified Computer Crime Investigator - Basic	High Tech Crime Network
Certified Computer Forensic Technician - Basic	High Tech Crime Network
Certified Confidentiality Officer	Business Espionage Controls and Countermeasures Association
Certified Encryption Specialist	EC-Council
Certified Ethical Hacker	EC-Council
Certified Expert Penetration Tester	Global Information Assurance Certification
Certified Forensic Computer Examiner	International Association of Computer Investigative Specialists
Certified Healthcare Protection Administrator	International Association of Healthcare Security and Safety
Certified in Healthcare Privacy and Security	American Health Information Management Association
Certified Information Privacy Professional	International Association of Privacy Professionals
Certified Information Privacy Technologist	International Association of Privacy Professionals
Certified Information Security Manager	Information Systems Audit and Control Association
Certified Information Systems Auditor	Information Systems Audit and Control Association
Certified Information Systems Security Professional	International Information Systems Security Certification Consortium, Inc.

Certified Information Systems Security Professional - Architecture	International Information Systems Security Certification Consortium, Inc.
Certified Information Systems Security Professional - Management	International Information Systems Security Certification Consortium, Inc.
Certified Network Defense Architect	EC-Council
Certified Secure Computer User	EC-Council
Certified Secure Software Lifecycle Professional	International Information Systems Security Certification Consortium, Inc.
Certified Security Specialist	EC-Council
Certified Threat Intelligence Analyst	EC-Council
Certified Wireless Security Professional	Certified Wireless Network Professional
Cisco Certified Internetwork Expert Security	Cisco Systems, Inc.
Cisco Certified Network Associate Security	Cisco Systems, Inc.
Cisco Certified Network Associate Security Certification	Cisco Systems, Inc.
Cisco Certified Network Professional Security	Cisco Systems, Inc.
CIW Web Security Associate	Certified Internet Web Professionals
CIW Web Security Professional	Certified Internet Web Professionals
CIW Web Security Specialist	Certified Internet Web Professionals
Cloud Technology Associate+ Certification	Cloud Credential Council
CompTIA Advanced Security Practitioner	Computing Technology Industry Association (CompTIA)
CompTIA Security+	Computing Technology Industry Association (CompTIA)
Computer Hacking Forensic Investigator	EC-Council
CSX Cybersecurity Practitioner	Information Systems Audit and Control Association
CyberSec First Responder	CertNexus
EC Council Certified Chief Information Security Officer	EC-Council
EC-Council Certified Security Analyst	EC-Council
Electronic Security Networking Technician	ETA International
GIAC Assessing and Auditing Wireless Networks	Global Information Assurance Certification
GIAC Certified Enterprise Defender	Global Information Assurance Certification
GIAC Certified Firewall Analyst	Global Information Assurance Certification
GIAC Certified Forensics Analyst	Global Information Assurance Certification
GIAC Certified Forensics Examiner	Global Information Assurance Certification
GIAC Certified Incident Handler	Global Information Assurance Certification
GIAC Certified Intrusion Analyst	Global Information Assurance Certification
GIAC Certified ISO-27000 Specialist	Global Information Assurance Certification
GIAC Certified Penetration Tester	Global Information Assurance Certification
GIAC Certified Perimeter Protection Analyst	Global Information Assurance Certification
GIAC Certified UNIX Security Administrator	Global Information Assurance Certification
GIAC Certified Windows Security Administrator	Global Information Assurance Certification
GIAC Continuous Monitoring Certification	Global Information Assurance Certification
GIAC Continuous Monitoring Certification	Global Information Assurance Certification
GIAC Cyber Threat Intelligence	Global Information Assurance Certification
GIAC Cyber Threat Intelligence	Global Information Assurance Certification
GIAC Exploit Researcher and Advanced Penetration Tester	Global Information Assurance Certification
GIAC Information Security Fundamentals	Global Information Assurance Certification

GIAC Information Security Professional	Global Information Assurance Certification
GIAC Mobile Device Security Analyst	Global Information Assurance Certification
GIAC Network Forensic Analyst	Global Information Assurance Certification
GIAC Reverse Engineering Malware	Global Information Assurance Certification
GIAC Secure Software Programmer - Java	Global Information Assurance Certification
GIAC Secure Software Programmer.NET	Global Information Assurance Certification
GIAC Security Essentials Certification	Global Information Assurance Certification
GIAC Security Leadership Certification	Global Information Assurance Certification
GIAC Strategic Planning, Policy, and Leadership	Global Information Assurance Certification
GIAC Systems and Network Auditor	Global Information Assurance Certification
GIAC Web Application Penetration Tester	Global Information Assurance Certification
Global Industrial Cyber Security Professional	Global Information Assurance Certification
HP ASE - ArcSight Administrator V1	Hewlett Packard Certification and Learning
HP ASE - ArcSight Analyst V1	Hewlett Packard Certification and Learning
HP ASE - ArcSight Logger V1	Hewlett Packard Certification and Learning
HP ASE - Fortify Security V1	Hewlett Packard Certification and Learning
HP ATP - ArcSight Security V1	Hewlett Packard Certification and Learning
HP ATP - Fortify Security V1	Hewlett Packard Certification and Learning
IBM Certified Administrator - Security Guardium V10.0	IBM Corporation
IBM Certified Administrator - Spectrum Protect V8.1	IBM Corporation
IBM Certified Analyst - i2 Analysts Notebook V9	IBM Corporation
IBM Certified Associate - Security AppScan DAST V9.0.1	IBM Corporation
IBM Certified Associate - Security Trusteer Fraud Protection	IBM Corporation
IBM Certified Associate Administrator - Security Guardium Data Protection V10.1.2	IBM Corporation
IBM Certified Associate Administrator - Security QRadar SIEM V7.2.8	IBM Corporation
IBM Certified Associate Analyst - Security QRadar SIEM V7.2.6	IBM Corporation
IBM Certified Deployment Professional - Identity Governance and Intelligence V5.2	IBM Corporation
IBM Certified Deployment Professional - Security Access Manager V9.0	IBM Corporation
IBM Certified Deployment Professional - Security AppScan Source Edition V9.0.3	IBM Corporation
IBM Certified Deployment Professional - Security Directory Integrator V7.2	IBM Corporation
IBM Certified Deployment Professional - Security Privileged Identity Manager V2.0.2	IBM Corporation
IBM Certified Deployment Professional - Security QRadar SIEM V7.2.7	IBM Corporation
Licensed Penetration Tester	EC-Council
Microsoft Security Fundamentals	Microsoft Corporation
Oracle Identity Governance Suite PS3 Implementation Essentials	Oracle Corporation
Professional Cloud Security Manager Certification	Cloud Credential Council

SAP Certified Application Associate - SAP BusinessObjects Access Control 10.0	SAP America, Inc.
Specialist - Infrastructure Security, Version 1.0	Dell Corporation
Specialist - Infrastructure Security, Version 1.0	Dell Corporation
Systems Security Certified Practitioner	International Information Systems Security Certification Consortium, Inc.
The Certified Information Privacy Professional	International Association of Privacy Professionals
The Certified Information Privacy Professional/Information Technology	International Association of Privacy Professionals
Wireshark Certified Network Analyst	Wireshark
Wireshark Certified Network Analyst	Wireshark

2.7. To Certify or not to Certify?

A certification is considered a measurable outcome to assess the knowledge and information acquired within academia and the workplace. Not surprisingly, conceptual knowledge would not replace practical skills and operational excellence for cybersecurity jobs. Recent research shows that holding an IT certification positively influences hiring and job retention, in addition to earning potential. However, two-to-four-year degree holders are less likely to be laid off and potentially earn higher income than non-degree holders [20]. Industry certifications help qualify that individuals possess the knowledge, skills, and abilities for work in the job field as much as one-third of cybersecurity-related jobs require some form of certification [21]. The Bureau of Labor Statistics in its current population survey (CPS) on labor force, employment, and unemployment statistics for persons with or without certifications and licenses reported answers to questions to identify persons with professional certifications and licenses after they were added to the Current Population Survey (CPS) in January 2015 [22]. Computer and mathematical occupations of 5,352 were included in the 37,237 professional and related occupations constituting a 12.5% of a population size of 45.3%. Only 5.6% had a certification but no license, 6.9% held a license and 87.5% held neither a certification nor a license. Certificates and certifications are helpful to employers to evaluate the skills and knowledge of applicant especially in small organizations where managers are not well versed in cybersecurity issues [23]. Certifications are not conclusive, but they may be given greater importance as construed as indicators of embodiment of knowledge in a specific area as well as interest and commitment in a field of work. Certifications are often pursued as an addition to an academic degree to highlight an area of interest and expertise. In a workshop conducted by the National Research Council in 2013, some workshop participants expressed that certification played a crucial role in their careers to establish credibility and competence. Others dissented and pointed out that CISSP certification is a perfect example of an over-glorified certification where highly qualified individuals do not hold it or any other certifications and lamented the hyper-emphasis on certifications which would restrict their employment prospects if required in the candidate selection process. Some participants indicated that some certifications are not viewed positively in some organizations where the experience, the practical skills, the educational attainment, and other factors were better measures and more sought after. They reported omitting certain certifications on their resumes for specific jobs. Views and perceptions on certifications differ. While some job seekers, mostly entry and intermediate levels, view certifications as an entry ticket initially and advancement as they pursue career growth, other professionals focus on gaining experience, practical skills, knowledge and furthering their educational goals. Indeed, almost all sites listed educations and degree from Associate to a Doctorate as recommended and beneficial acquisition ability, or educational achievement, were seen as better measures. A few said that they sometimes omitted listing certifications on their resumes for this reason.

3. CONCLUSIONS AND FUTURE WORK

In analyzing O*NET® database for Information Security Analyst for work role certifications, no valuable and actionable information was available. Links to other government sites were listed for additional resources. The Bureau of Labor Statistics listed general guidance while offering an example of CISSP for general certifications and cited other specific areas like pen testing or systems auditing. Similarly, NICCS under the NICE Cybersecurity Framework Work Roles offered general guidance as to potential topics and areas of certification for this work role based on the career level: entry, intermediate, and advanced. Finally, Careeronestop site under certification finder provided the ultimate guidance for certification tied to the role "Information Security Analyst". Not one site has listed any certification as required, desirable or mandatory. Certifications are still not an integral part of the Cybersecurity Workforce preparation and requirements even as they gain more momentum with job seekers and employers. Current frameworks do not integrate certifications in a prominent manner contrary to the popular belief. In the context of shortage of skilled workforce, the cybersecurity workforce dilemma is more than a solution to a staffing problem; rather it should be a competitive advantage in a proactive agile business model. With private and public sectors competing for the same assets in a time when the pipeline is still lagging in preparing adequately educated and trained cybersecurity professionals, this problem is widespread in academia, business, government, and other types of organizations [24]. Future potential work is possible exploration of adequate workforce preparation mechanisms, and avenues for investing in the human power as it is reported that 71% to 76 % of the businesses are not investing in their long-term assets of "manpower" via training, professional development, and career path development [25] but rather investing more in infrastructure and advanced technology.

REFERENCES

[1] O*NET Resource Center (2021, June 10). O*NET® 25.3 Database. https://www.onetcenter.org/database.html#overview

[2] National Research Council (2010). A Database for a Changing Economy: Review of the Occupational Information Network (O*NET). Washington, DC: The National Academies Press. https://doi.org/10.17226/12814 https://www.nap.edu/read/12814/chapter/11

[3] O*NET Resource Center (2021). Occupational Listings. https://www.onetcenter.org/taxonomy/2019/list.html

[4] National Research Council (2013). Professionalizing the Nation's Cybersecurity Workforce?: Criteria for Decision-Making. Washington, DC: The National Academies Press. https://doi.org/10.17226/18446.

[5] DoD 8570.01-M (2005, 2014). Information Assurance Workforce Improvement Program. DoD 8570.01-M, December 19, 2005, Incorporating Change 4 on November 10, 2015 (whs.mil)

[6] DoD 8530.1 (2016, 2017). Cybersecurity Activities Support to DoD Information Network Operations. DoDI 8530.01, March 7, 2016, Incorporating Change 1, July 25, 2017 (whs.mil)

[7] Bureau of Labor Statistics, (2021). Standard Occupational Classification. https://www.bls.gov/soc/

[8] Researchgate.net (2020). https://www.researchgate.net/figure/ONET-content-model-21_fig1_317600739

[9] Spokane, A. (1985). A review of research on person-environment congruence in Holland's theory of careers, Journal of Vocational Behavior, Volume 26, Issue 3, pp. 306-343, https://doi.org/10.1016/0001-8791(85)90009-0.

[10] Dawis, R. & Lofquist, L. (1984). A psychological theory of work adjustment. Minneapolis: University of Minnesota Press

[11] www.onetcenter.org (2021). The O*NET® Content Model. https://www.onetcenter.org/content.html

[12] www.onetonline.org (2020). National Center for O*NET Development, Bureau of Labor Statistics, O*Net Online Summary Report for 15-1122.00—Information Security Analysts. https://www.onetonline.org/link/summary/15-1122.00

[13] SHRM (2020). Performing Job Analysis. https://www.shrm.org/resourcesandtools/tools-and-samples/toolkits/pages/performingjobanalysis.aspx
[14] Bauer, T., Erdogan, B., Caughlin, D., & Truxillo, D. (2019). Fundamentals of Human Resource Management. Sage Publication Inc.
[15] Bureau of Labor Statistics (2020, July 12). U.S. Department of Labor, Occupational Outlook Handbook, Information Security Analysts. https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm
[16] Newhouse, W., Keith, S., Scribner, B. & Witte, G. (2020). National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181.pdf#page21
[17] National Initiative for Cybersecurity Careers and Studies NICCS (2020). NICCS Education and Training Catalog. https://niccs.us-cert.gov/training/search
[18] NICCS (2020). https://niccs.us-cert.gov/sites/default/files/documents/pdf/cybersecurity_workforce_development_toolkit.pdf?trackDocs=cybersecurity_workforce_development_toolkit.pdf
[19] NICCS (2021). Education and Training Catalog. NICCS Education and Training Catalog | National Initiative for Cybersecurity Careers and Studies (cisa.gov)
[20] Belanich, J. & Morriosn, J. (2019, March). Impact of Professional Credentials on Employability. https://www.researchgate.net/publication/334170431. DOI: 10.13140/RG.2.2.20406.96324
[21] Stines, A. (2020, March 24). Faculty Perceptions of Open Educational Resources in Cyber Curriculum: A Pilot Study Curriculum: A Pilot Study. Beadle Scholar
[22] Bureau of Labor Statistics (2020, January 21). Labor Force Statistics from the Current Population Survey. https://www.bls.gov/cps/demographics.htm#certs_licenses
[23] National Research Council (2013). Professionalizing the Nation's Cybersecurity Workforce?: Criteria for Decision-Making. Washington, DC: The National Academies Press. https://doi.org/10.17226/18446
[24] Mailloux, L. & Grimaila, M. (2018, May/June). "Advancing Cybersecurity: The Growing Need for a Cyber-Resiliency Workforce," in IT Professional, vol. 20, no. 3, pp. 23-30. doi: 10.1109/MITP.2018.032501745.
[25] Olstik, J., (2019, April). The lives and Times of Cybersecurity Professionals. https://www.esg-global.com/hubfs/pdf/ESG-ISSA-Research-Report-Life-of-Cybersecurity-Professionals-Apr-2019.pdf

AUTHORS

Micheline Al Harrack is a Faculty at Marymount University, USA in the College of Business, Innovation, Leadership and Technology in the department of Data Science, IT, and Cybersecurity. Her research interests include Machine Learning Applications, Statistical Analysis, Function Points, Linguistics, and Cybersecurity topics.