BLACKSWAN
CYBERSECURITY

Cyber Workforce Development / Alignment: Results of a Qualitative Study

Dr. Michael Saylor

March 2024

OUR PEOPLE MAKE THE DIFFERENCE.

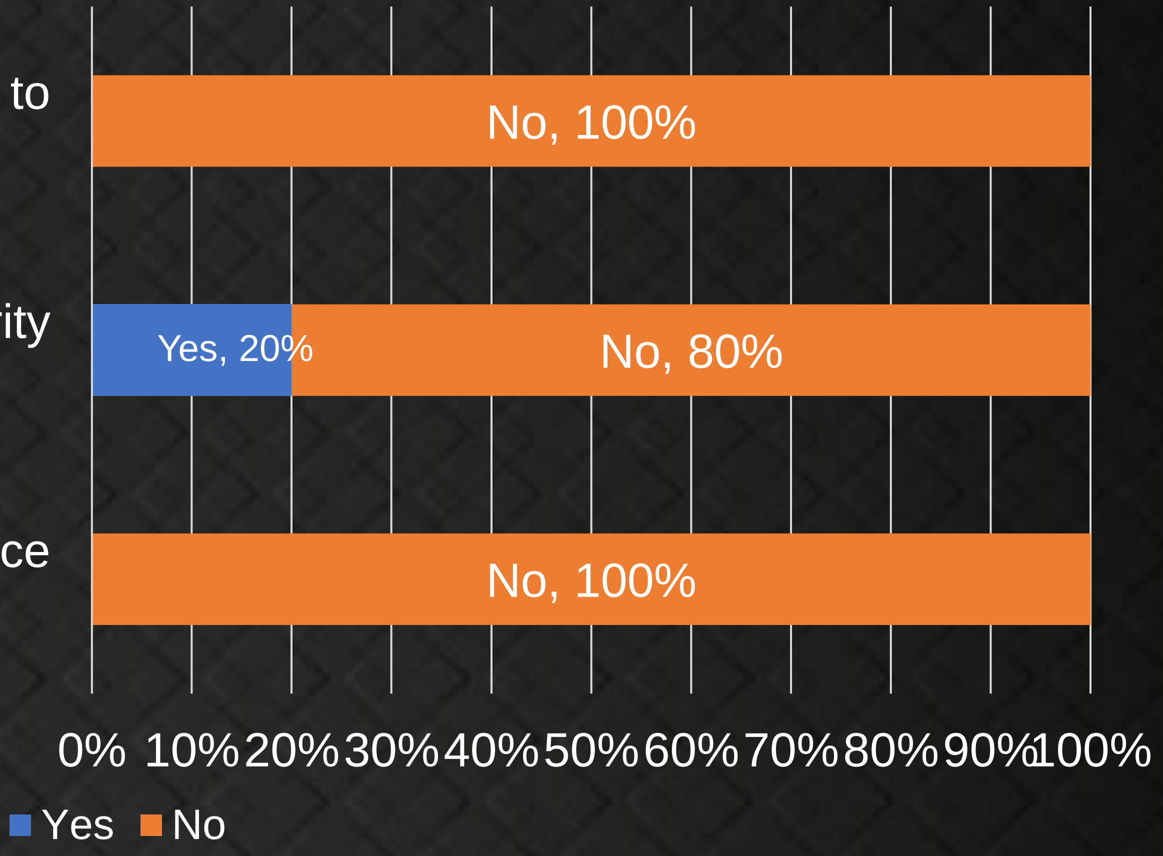
Get in Touch
855-BLK-SWAN
Contact@BlackswanCybersecurity.com
www.blackswancybersecurity.com

Mike Saylor

- 30 years in IT/Cyber, CISA, CISM, BS InfoSys, MS CJ, Doctorate Business/Cyber
- 25 years as a University Professor of Cyber and DFIR – currently at the UTSA
- North Texas FBI Infragard
- North Texas Crime Commission’s Cyber Crime Committee
- Fusion Liaison officer for the North Texas Fusion Center
- CEO and incident response lead for BlackSwan Cybersecurity
- Exec. Director for the U.S. Cyber Defense Center

Responses

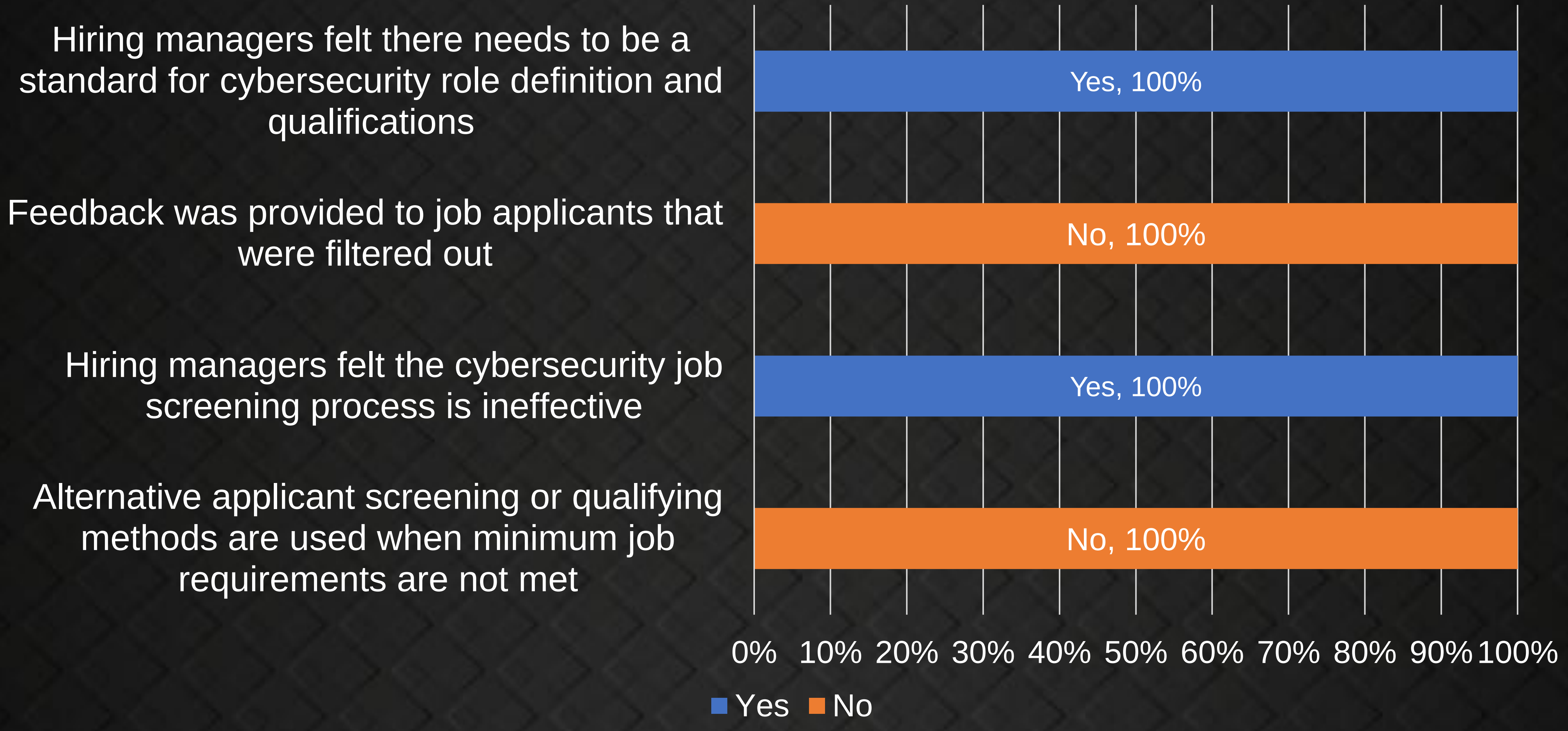
BLACKSWAN
CYBERSECURITY



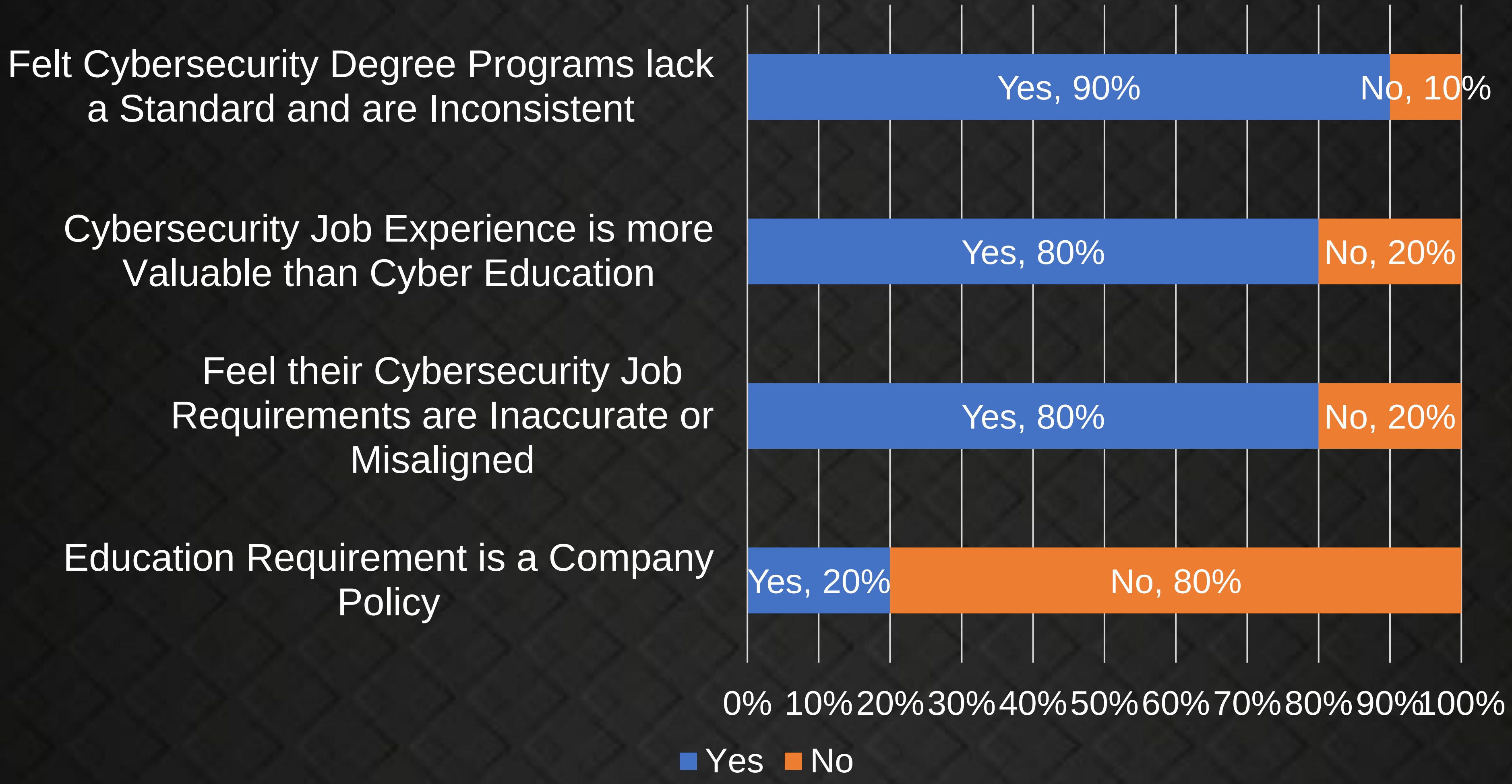
OUR PEOPLE MAKE THE DIFFERENCE.

Get in Touch
855-BLK-SWAN
Contact@BlackswanCybersecurity.com
www.blackswancybersecurity.com

Responses


Hiring managers felt there needs to be a standard for cybersecurity role definition and qualifications
Yes, 100%
Feedback was provided to job applicants that were filtered out
No, 100%
Hiring managers felt the cybersecurity job screening process is ineffective
Yes, 100%
Alternative applicant screening or qualifying methods are used when minimum job requirements are not met
No, 100%
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
🟦 Yes
🟧 No

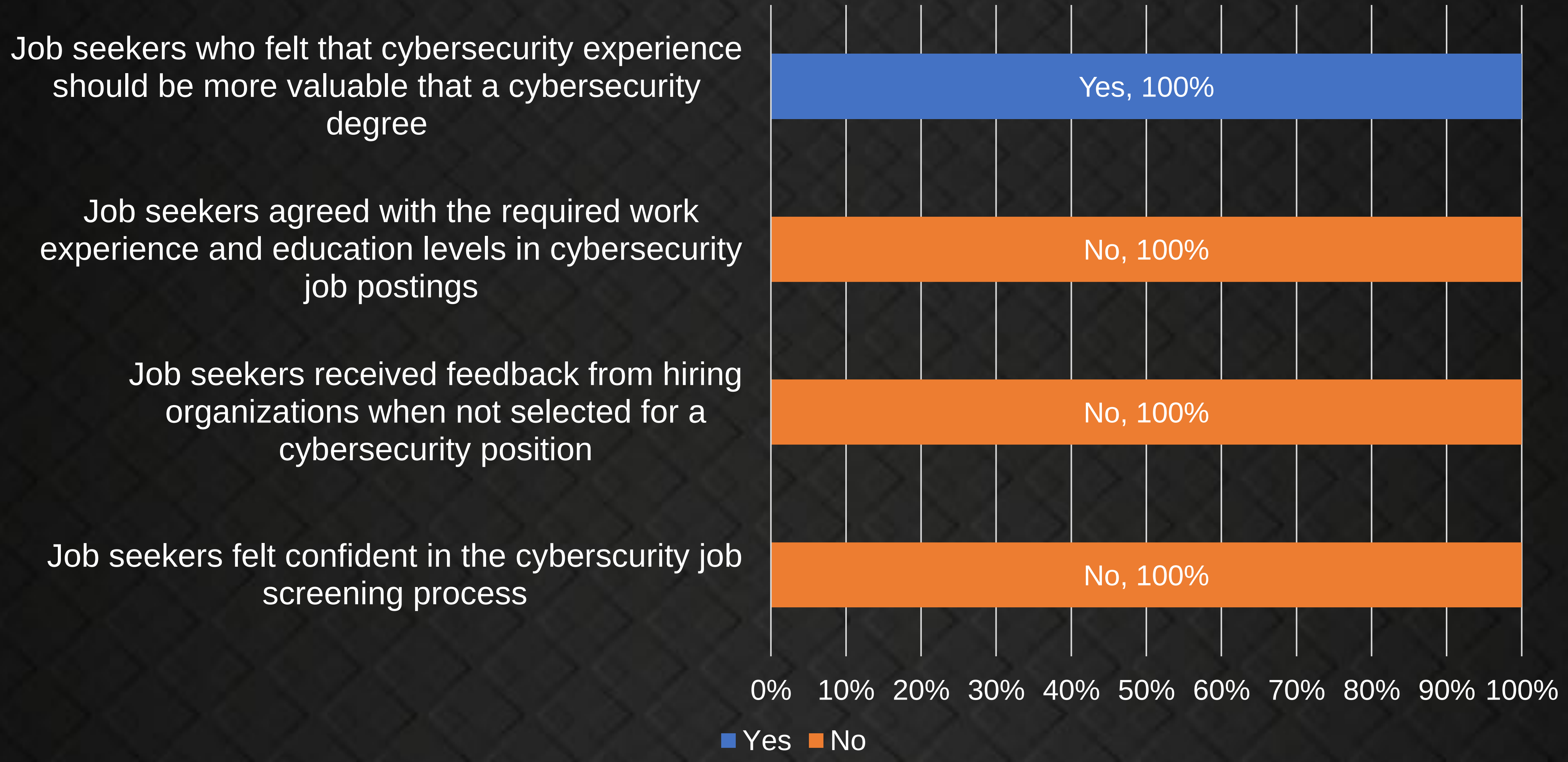
Responses



OUR PEOPLE MAKE THE DIFFERENCE.

Get in Touch
855-BLK-SWAN
Contact@BlackswanCybersecurity.com
www.blackswancybersecurity.com

Responses


Job seekers who felt that cybersecurity experience should be more valuable that a cybersecurity degree
Yes, 100%
Job seekers agreed with the required work experience and education levels in cybersecurity job postings
No, 100%
Job seekers received feedback from hiring organizations when not selected for a cybersecurity position
No, 100%
Job seekers felt confident in the cyberscurity job screening process
No, 100%
0%
10%
20%
30%
40%
50%
60%
70%
80%
90%
100%
🟦 Yes
🟧 No

Findings (1 thru 4)

1. Absence of a standard for defining cybersecurity job role descriptions and KSA criteria found in 100% of the responses from participants.
2. Lack of a standard for defining job roles is also complicit in the misalignment of job-related qualifications, specifically years of job-related experience - 80% of participants.
3. 100% of participating hiring organizations’ entry-level job postings required at least two years of experience, reportedly because they thought it was standard not because it was an accurate qualification.
4. 0% of participants were familiar with a cybersecurity workforce standard or framework.

Quotes - “We don’t have a good process for how to define cybersecurity job descriptions or qualifying requirements. We usually just Google it to see what’s out there that we can use and if it sounds similar, we just go with it.” & “Using standard definitions for the different jobs would help me better understand which jobs I qualify for, some companies post an analyst job but it’s really an engineer job that they just want to pay less for.”

Findings (5 thru 7)

5. 80% of hiring organization felt their education and experience requirements were inaccurate or misaligned due to improper role definition.
6. 80% of hiring organizations felt that cybersecurity job experience was more valuable and qualifying than education and certification. (ISC2 study found that < 30% found value in Cyber degrees)
7. 90% of all participants felt that cybersecurity degree programs are inconsistent in design and lack a standard for ensuring consistent requirements for fundamentals that apply to cybersecurity in general.

Quotes - "… hiring manager stressed the need for experience over education, but a lot of the applicants…are just out of school…and applied despite the requirement for both education and experience." and "The trick and the problem are figuring out what the basic minimum level of experience is necessary for the job, which translates into finding the right person, with the right skills, at the right price." "Experience in cyber is important for the role, ensuring we are giving the responsibility to someone that isn't seeing it for the first time." and "We used to be very particular about requiring a degree, but with the inconsistencies among cyber degrees from different schools, we can't count on the degree to provide candidates the basic skills…"

Findings (8 thru 11)

8. 0% of hiring organizations used an alternate method for screening applicants that do not match posted qualifications.
9. 100% of hiring organizations felt the screening process for cybersecurity jobs in their organization was ineffective at finding the right resource for the job.
10. 80% of hiring organizations felt their cybersecurity job postings contained inaccurate and or misaligned job role descriptions and qualifications, resulting in overlooking an otherwise qualified candidate.
11. 100% of hiring organizations stated that they primarily rely on automated filters to screen applicants.

Quotes - “It is frustrating to see the volumes of resumes submitted for a job, sometimes more than 100, and none of them meet the minimum requirements, the requirements that you’d expect to be standard across the board…We do not currently consider applicants that don’t meet the requirements, and as a result our positions are still unfilled.” and “We don’t have an alternative method for screening applicants that aren’t a match.” and “We don’t have an alternative way to determine if someone that gets filtered out is a good fit, their resume never gets to a person.”

Findings (12 thru 16)

12. 0% of hiring organizations used an alternate method for screening applicants that do not match posted qualifications.
13. 100% of hiring organizations felt the screening process for cybersecurity jobs in their organization was ineffective at finding the right resource for the job.
14. 80% of hiring organizations felt their cybersecurity job postings contained inaccurate and or misaligned job role descriptions and qualifications, resulting in overlooking an otherwise qualified candidate.
15. 100% of hiring organizations stated that they primarily rely on automated filters to screen applicants.
16. 100% of job applicants stated they did not receive feedback from hiring organizations with regard to their application to a cybersecurity position.

Quotes - "It is frustrating to see the volumes of resumes submitted for a job, sometimes more than 100, and none of them meet the minimum requirements, the requirements that you'd expect to be standard across the board…We do not currently consider applicants that don't meet the requirements, and as a result our positions are still unfilled." and "We don't have an alternative method for screening applicants that aren't a match." and "We don't have an alternative way to determine if someone that gets filtered out is a good fit, their resume never gets to a person."

Findings (12 thru 16)

Addition Quotes: “I’ve been an analyst for over 2 years and have a total of 4 years of experience in cyber, but they never called me.” and “I’ve applied for a lot of jobs over the years and never heard any feedback, but it would have been nice to know…what needs improvement or what I could have done or said differently, maybe something on my resume.”

Findings (17 thru 18)

BLACKSWAN
CYBERSECURITY

17. 100% of job seeker participants did not feel confident in the hiring process, specifically the screening process where their credentials are scanned for alignment with what is commonly a misaligned job description and minimum qualifications.
18. 80% of participants' hiring process did not include a formal analysis of internal need and or the process did not seek to align the role objectives submitted by hiring managers with a standard cybersecurity job role definition.

Quotes - "I've applied for several … entry-level jobs that I am more than qualified for, that should only require 2 years of experience, but …required 5 years of experience and no way to discuss my background or capabilities because I was filtered out." and "…hiring organizations should … stop trying to write … elaborate description and start listing bullet points of what they need, remove the experience and degree requirements and actually put the work in to interviewing people." "…minimum requirements are understandable, but the problem is their minimum is usually too high and…doesn't line up with what's required for the job." and "I don't think there is a [cybersecurity] shortage as much as there is an industry problem with aligning the definition of what we need with what is required to be successful in that role."

Implications

1. The relationship between the level of experience required by hiring organizations and the level of experience reported by job applicants was found to be both inconsistent and misaligned, as well as overwhelmingly viewed as an inaccurate attribute of an ineffective hiring process.

2. Cybersecurity-related job experience was valued significantly higher than cybersecurity-related education, yet both were typically defined as minimum requirements for entry-level cybersecurity jobs.

3. Hiring organizations did not have an alternative screening process to further evaluate job applicants that did not meet the posted minimum qualifications for cybersecurity jobs.

4. There is a lack of confidence in the hiring process for cybersecurity jobs, beginning with a hiring organization’s understanding and definition of the needed role and associated qualifications and extending to the screening and interviewing of job seeker candidates.

Recommendations

1. Implement a standard for defining the cybersecurity workforce, using a common language to define job roles and Knowledge-Skills-Abilities (KSAs), and establishing continuity between hiring organizations and job candidates in how they describe their respective expectations and qualifications.

   A. Hiring organizations must first implement the standard within their hiring procedures to define the job role, objectives, and KSAs (the demand), resulting in:
      - i. Alignment of job needs with standard role definitions and KSAs
      - ii. Improved applicant screening process
      - iii. Support for internal career development programs
      - iv. Demand-based influence on higher education to implement a standards-based curriculum

   B. Job seekers must become familiar with the standard
      - i. Raising awareness of cybersecurity job roles and specialties and related KSAs
      - ii. Aids in career path planning and progression
      - iii. Aligns applicant KSAs with job postings

Recommendations

2. Establish an alignment of the standard among hiring organizations, education and training programs, and opportunities for internships or apprenticeships.
   - A. Higher-education degree objectives and outcomes must align with the standard for roles and KSAs that translate directly to the jobs at hiring organizations .
     - i. Creating clarity for job seekers and students regarding cybersecurity jobs and careers.
   - B. Higher-education degree programs must create opportunities for students to apply their knowledge through internships and apprenticeship programs established with community organizations.
     - i. Obtaining referenceable experience towards entry-level employment.
     - ii. Opportunities to demonstrate the application of knowledge and skills obtained.
   - C. Establish mentorship programs through cybersecurity industry associations, based on the NICE framework,
     - i. Aid job seekers in career path awareness and design, goal setting, and professional development.

Conclusions

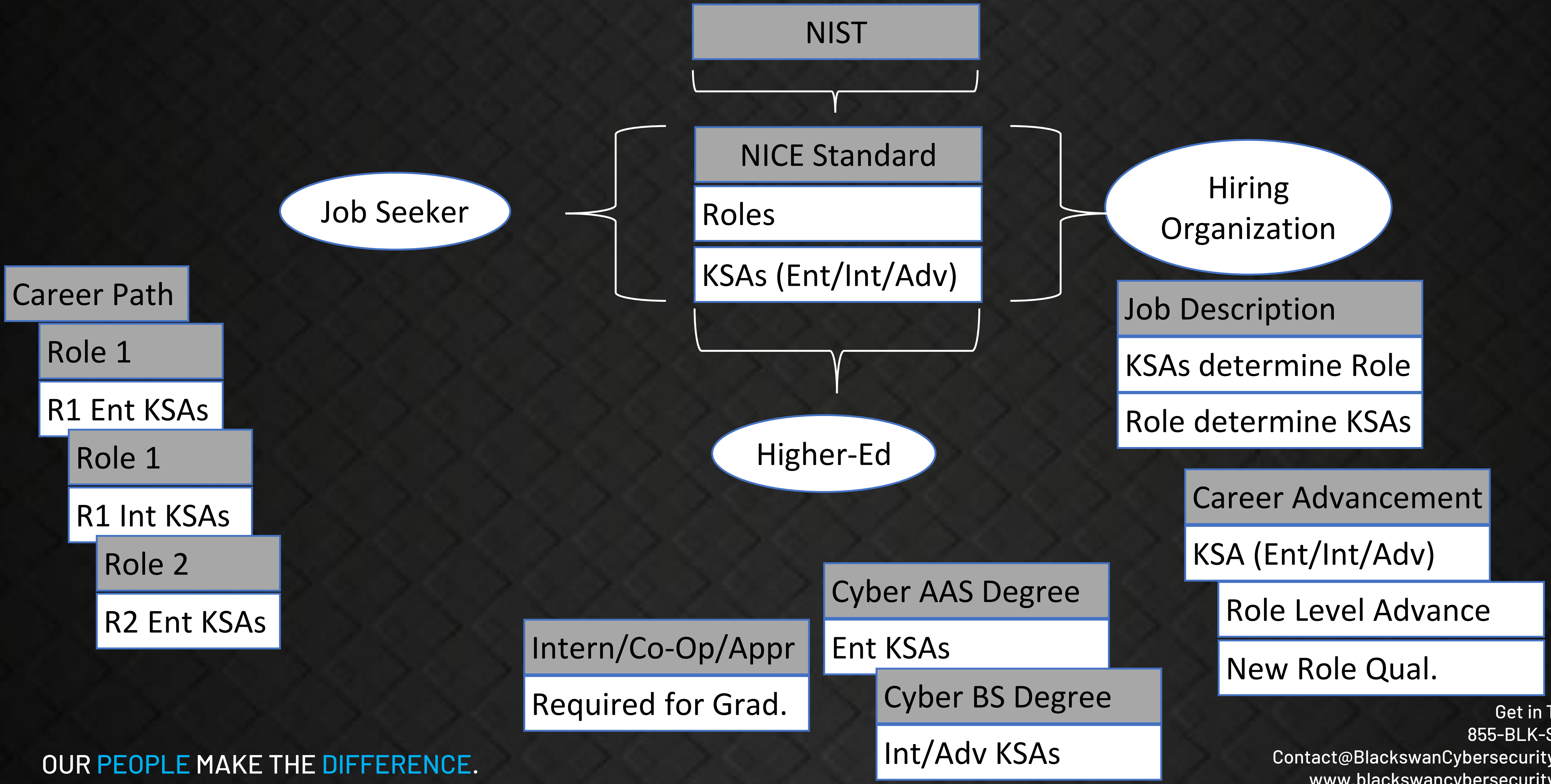
1. The primary, root cause, and most impactful factor contributing to the cybersecurity workforce deficiency was the absence of a standard from which the workforce can be consistently defined, qualified, and measured across all stakeholders.

Gaps in the literature

1. Most of the literature presented pointed solutions without recommendations or reference to an integrated approach. Studies focused on training & education, diversity staff development, competency, and hiring requirements with little observation to their interconnectedness or the application of a more holistic solution.

The takeaway message from this study is that the widely publicized message of a lack of cybersecurity talent cannot be verified because of the known and significantly misaligned, inconsistent, and inaccurate definition of job roles and qualification that discount otherwise qualified workers.

The Ecosystem



NIST

NICE Standard

Roles

KSAs (Ent/Int/Adv)

Job Seeker

Hiring Organization

Higher-Ed

Career Path

Role 1

R1 Ent KSAs

Role 1

R1 Int KSAs

Role 2

R2 Ent KSAs

Job Description

KSAs determine Role

Role determine KSAs

Career Advancement

KSA (Ent/Int/Adv)

Role Level Advance

New Role Qual.

Intern/Co-Op/Appr

Required for Grad.

Cyber AAS Degree

Ent KSAs

Cyber BS Degree

Int/Adv KSAs