codio

Bridging the Cybersecurity Skills Gap: Aligning Educational Programs with Industry Needs

Bridging the Gap Between Cybersecurity Education and Industry Expectations

Cyber Field

- Current professionals find a career in cybersecurity to be increasingly more difficult as the landscape becomes more complex and the work becomes more challenging
- Dissatisfaction with their career choices

- The cybersecurity skill gap has been defined in previous research as the gap between what college graduates are capable of and what industry employers expect of them

- We widen this understanding to refer more broadly to the disparity between the demand for skilled cybersecurity professionals and the availability of qualified individuals, thereby including those who are already employed in cybersecurity but may be lacking the necessary skills to manage the current landscape

Potential Causes of the Gap

- Universities overweighting less critical areas of study
- Lack of “soft” skills in recent graduates and workers
- Insufficient diversity
- Culture within the field
- Insufficient salaries, overworked employees

codio

Respondents

- Eligibility requirements were being a senior executive responsible for an organization's cybersecurity strategy, operations, and workforce development
- 200 complete, eligible responses were received
- 71.5% male and 28.5% female
- 63% of participants were 30-44 years of age
- Average professional and skills development spend per organizational employee was $1765.73

codio

Survey Design

- The survey was designed to capture multiple themes:
  - what skills are most important in the skills gap,
  - how hiring managers perceive new hires,
  - how organizations act to close the gap
- Sought to reinforce and extend results that emphasize the importance of hands-on experience and industry-academia collaboration and the widespread impact of the skills gap on an organization, its employees, and the skills it implies
- 16 main questions, 11 demographic questions, and 1 qualification question

Question Examples

- Rank the following technical skills in order of importance when evaluating new hires
- Select the top 3 most valued technical skills in your organization.

- Hands-on experience (e.g., internships, practical projects) is important for new hires in my organization.

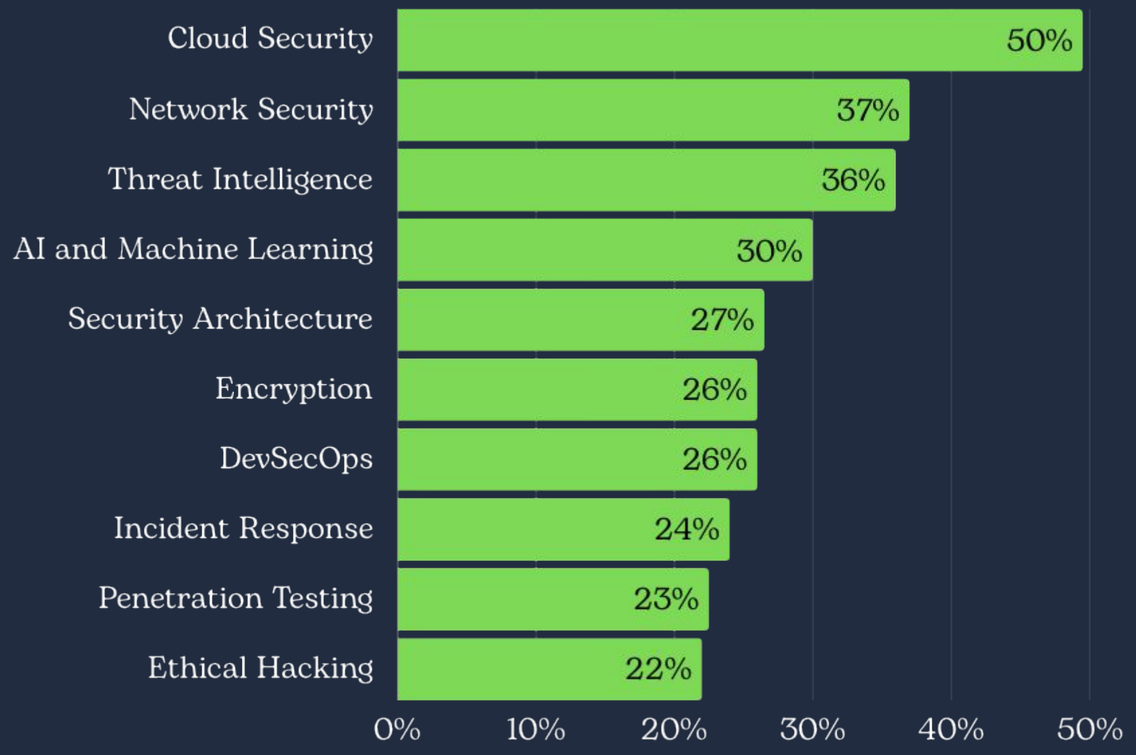
- What types of practical experiences do you value most when evaluating new hires?

Results - General Trends

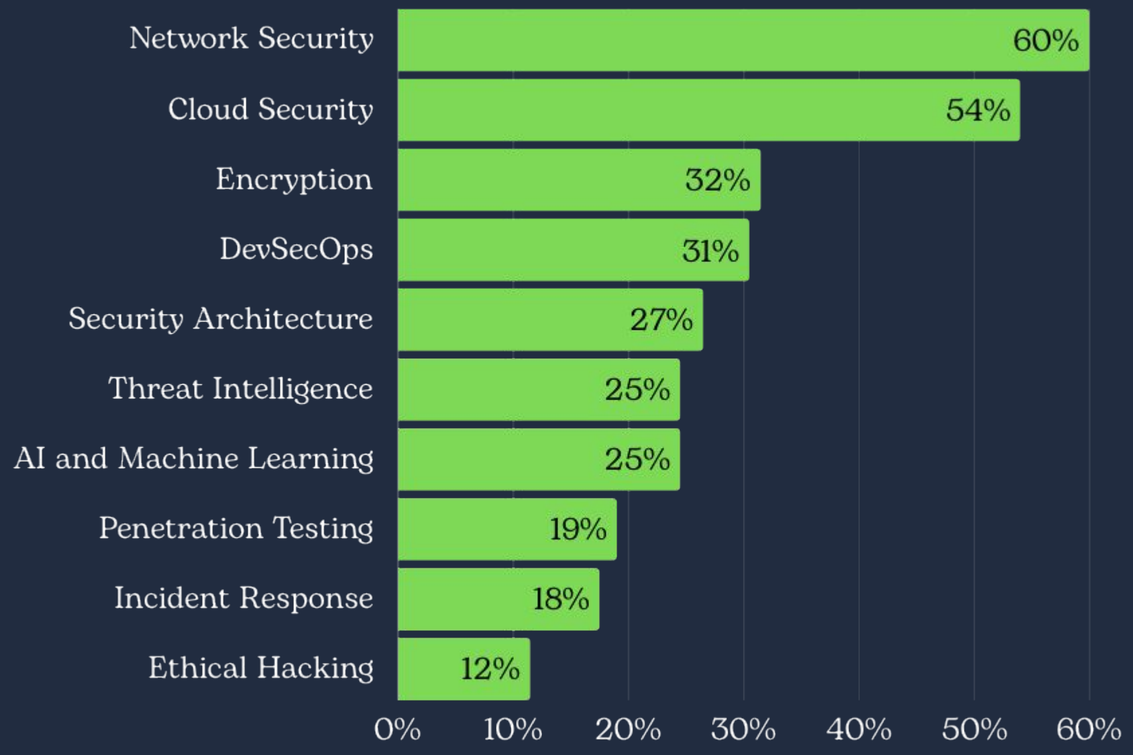
- Cloud security, and network security are both highly valued and in demand
- Problem solving/critical thinking is the most important non-technical skill
- General satisfaction with new hires
- Hands-on, practical experience is highly important and also deficient
- Many organizations collaborate with educational programs & institutions

Descriptive Results

Top 3 most lacking technical skills in your organization



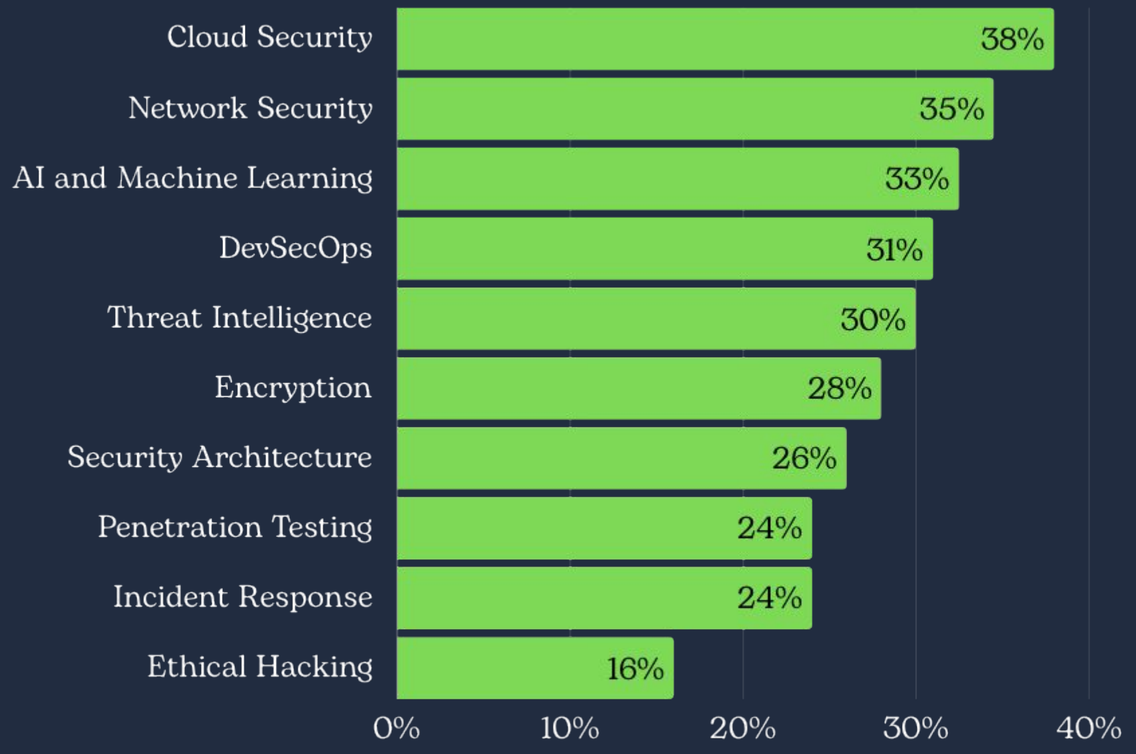
Top 3 most valued technical skills in your organization



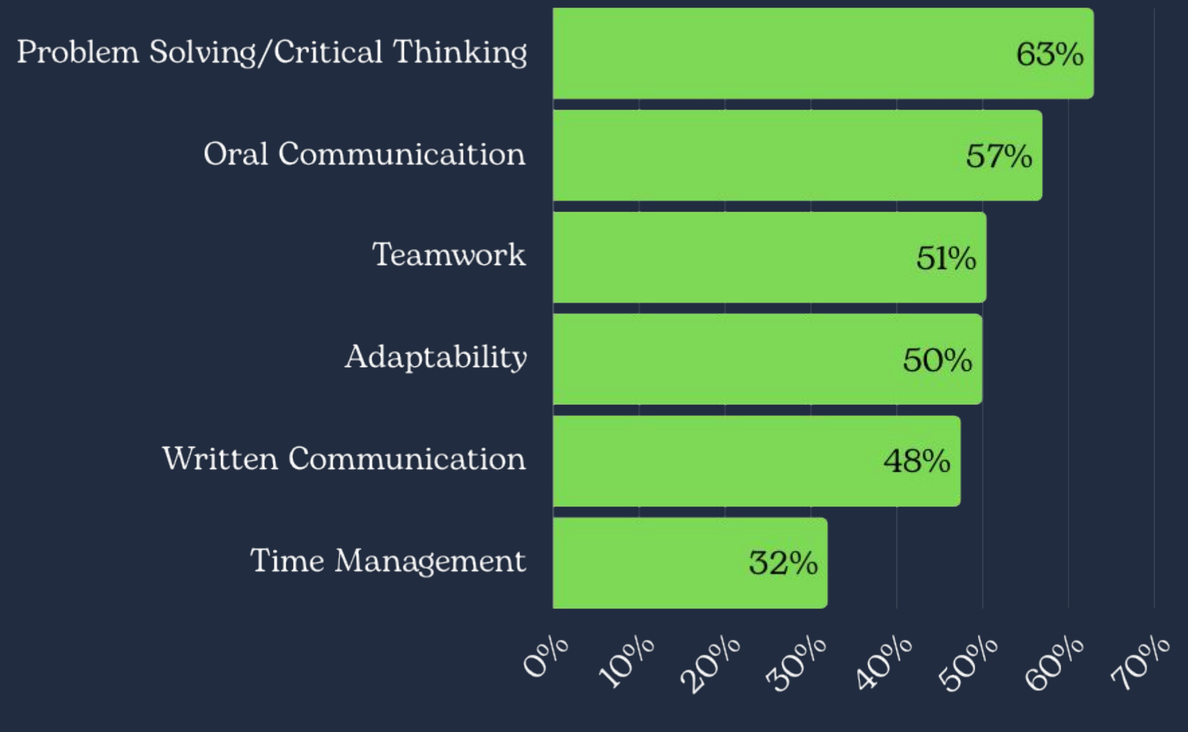
codio

Descriptive Results

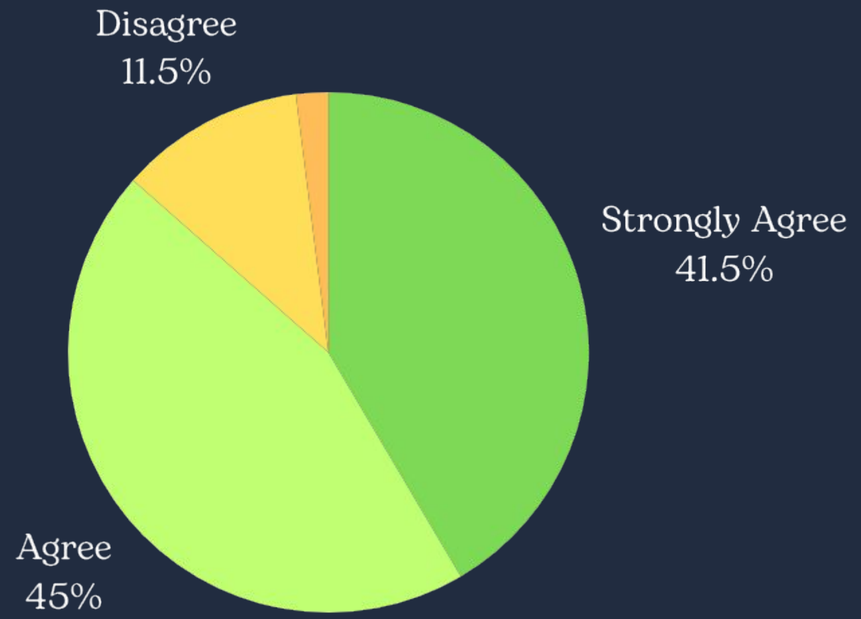
What areas of expertise are you having the most challenges hiring in?



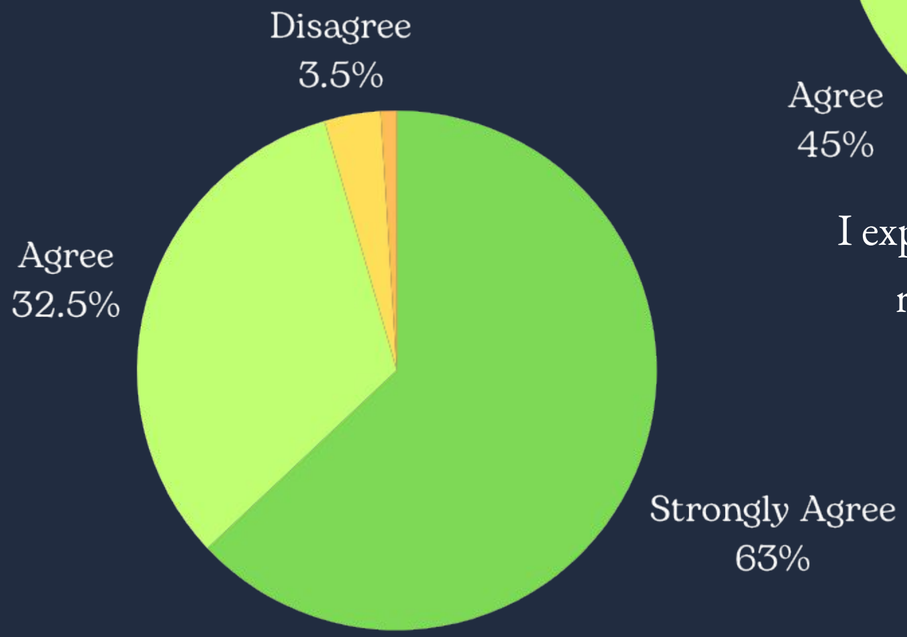
What 3 non-technical skills do you find most lacking in your organization?



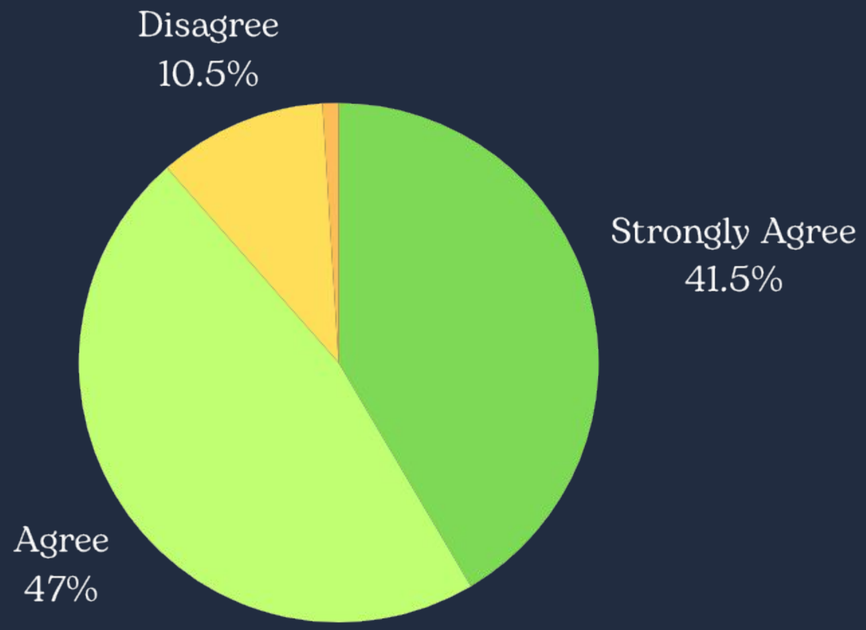
codio



I expect new hires to be immediately ready to work once they start.



Hands-on experience (e.g., internships, practical projects) is important for new hires in my organization.



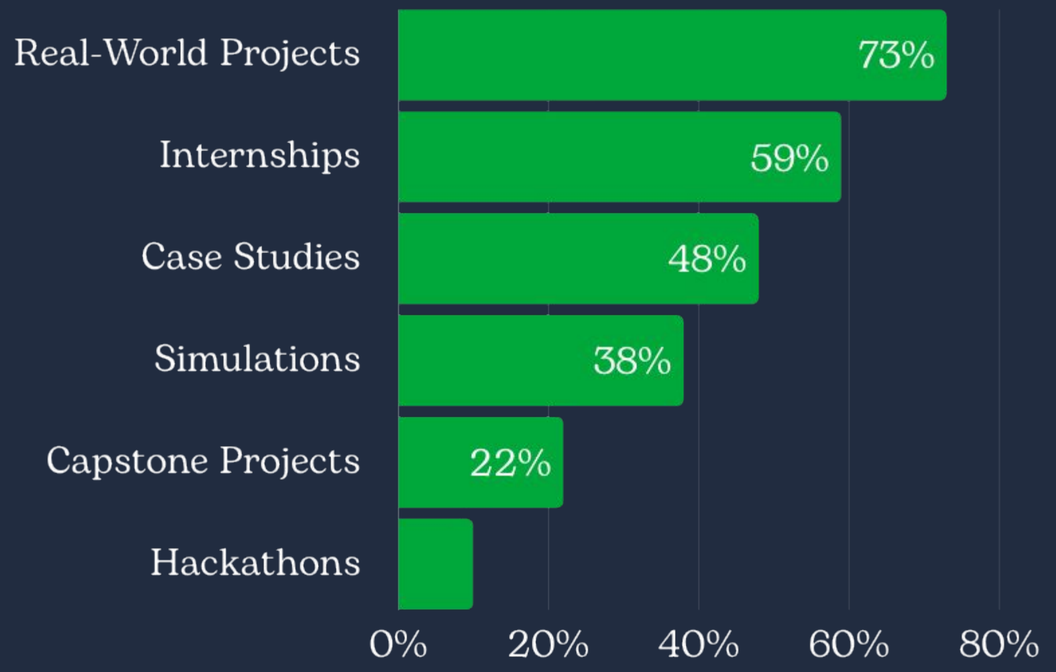
I am generally satisfied with the performance of new hires within 30 days of employment.

codio

Descriptive Results

What specific areas do you believe are most deficient in new hires?

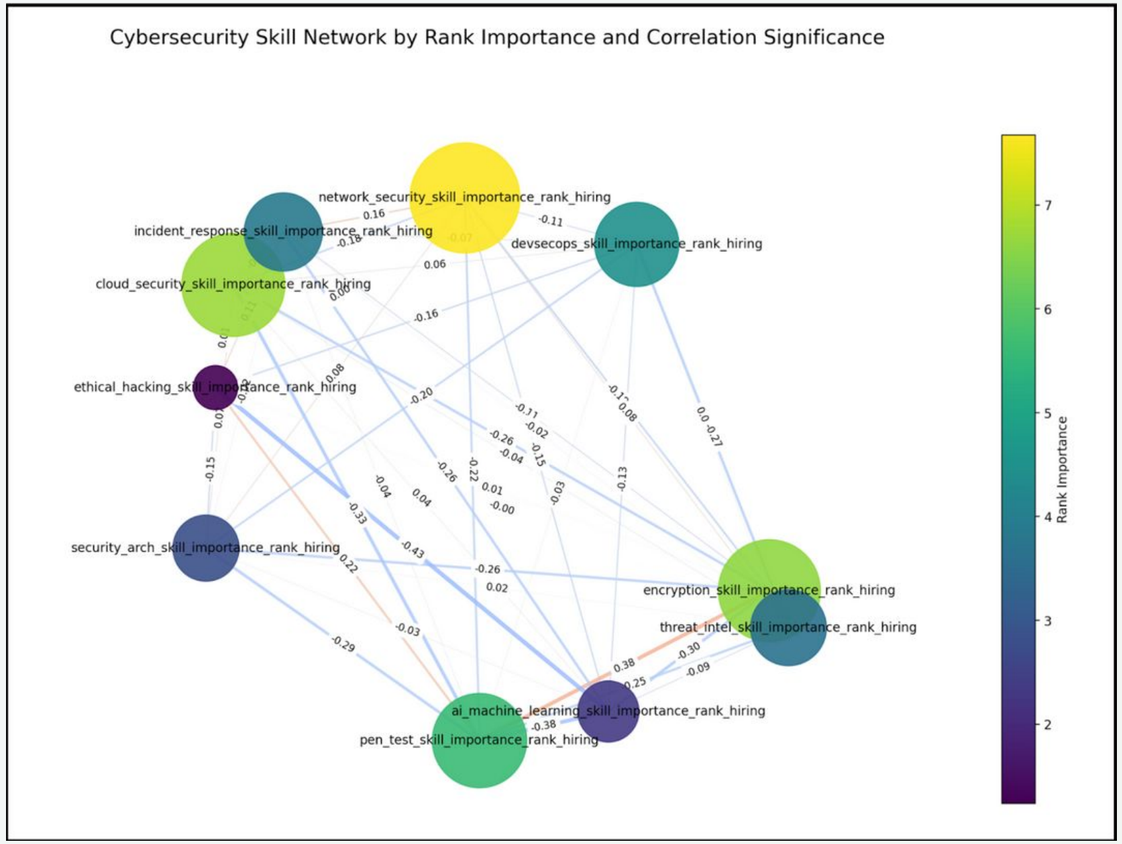
What types of practical experiences do you value most when evaluating new hires?



codio

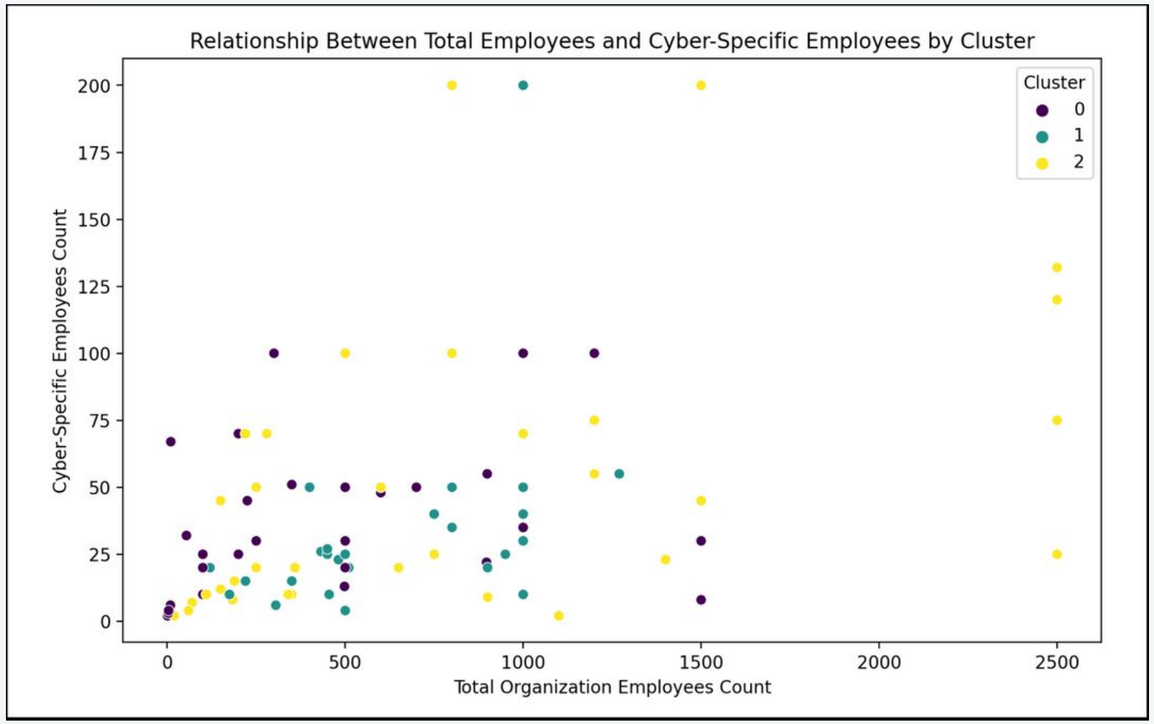
Key Correlations

- Ethical Hacking and AI/Machine Learning
- Penetration Testing and AI/Machine Learning
- Cloud Security and Penetration Testing
- Security Architecture and Penetration Testing
- Encryption and Penetration Testing



codio

Cluster Analyses



Cluster 0 orgs allocate a substantial budget to cybersecurity education & emphasize a broad range of skills such as network security, encryption, and cloud security.

Cluster 1 orgs spend moderately on cybersecurity education and focus on specialized areas like AI and machine learning. This cluster is more common in specific industries, including transportation, advertising, government, and nonprofits.

Cluster 2 is defined by a lower overall spend on cybersecurity education, with a strategic focus on core skills such as network security and encryption. This cluster maintains a balanced distribution of cyber-specific employees, emphasizing foundational cybersecurity skills.

Conclusions & Implications

Industry Specific Best Practices:

1. Educational programs should integrate more hands- on, experiential learning opportunities such as internships, real-world projects, simulations, and case studies to address employer perceptions of new hires lacking practical experience.
2. Despite being lower in current priority, skills like AI and machine learning should still be incorporated to prepare students for future industry shifts and advancements.
3. Educational institutions should actively seek partnerships with industry players to keep curricula up to date with industry needs, provide practical experiences, and continuously refine educational content based on feedback from the field.

Going Forward:

- Future studies could explore the long-term impacts of different types of practical experience on job performance and career progression in cybersecurity
- Investigate the specific mechanisms by which industry-academia collaborations can most effectively address skills gaps

codio

codio

codio.com