Evaluation of Hands-On Cybersecurity Skill Development

August 2021

Team :wq!

Marie Phelan, Boise State University

Sean Devine, University of Idaho

Morgan Aiken, Western Governors University

Joel Orban, Idaho State University

INL Mentor

Robert Beason

Abstract

Cybersecurity is a relatively new and quickly advancing industry, though there is a deficit in industry professionals throughout the world. This deficit is a result of the inability of education to keep up with the continuously changing cyber-threat landscape. A lack of effective, accessible, hands-on training platforms is a barrier for students and professionals who seek to gain the skills and abilities necessary to enter the workforce. Additionally, the lack of adequate training makes it difficult for industry experts to upskill or stay up to date on new advancements within the field of cybersecurity. The goal of this cohort is to discover what makes an effective or ineffective training platform, what platforms are currently available, and to determine the next steps for hands-on learning.

Hands-on experience is necessary to create workforce ready professionals, yet it is underutilized by students and professionals of cybersecurity due to costs, availability, and ease of use. This cohort has uncovered hands-on training solutions, identified many effective training solutions, and explored potential improvement to cybersecurity training. These findings resulted in the cohort moving beyond research to test the resources that currently exist or are in development, and to apply that knowledge to discovering and developing engaging hands-on training.

Table of Contents

Introduction

The most acute shortage of cybersecurity experts is highly technically skilled professionals. Students require test environments and instruction to acquire the knowledge, skills, and abilities necessary to make them highly proficient practitioners of cybersecurity. Hands-on experience, which is necessary to create workforce ready performers, is not readily available to students and professionals for cybersecurity due to costs, availability, and ease of use. The shortage of experts in the field results in professional burn-out and understaffed organizations. By unclogging the academia to industry pipeline, students, professionals, and organizations will benefit. Though the Idaho Cyber Research Project (ICRP) is focused on local organizations and academic institutions, the problem is international. The solution is to create more effective hands-on training to fit the needs of the industry, while mitigating the stress caused by barriers to education.

The ICRP consists of five cohorts of interns, an INL team of experts, partners in industry and academia, and the Industrial Cybersecurity Community of Practice (ICSCOP). In the future, the ICRP could be expanded to a national cybersecurity project. The Idaho National Laboratory has immense resources and is dedicated to securing critical infrastructure, which is necessary for the advancement of cybersecurity. The lab's resources allow for the development of tools designed for industry, academia, and learners such as Cyber-CHAMP, which will be used to map knowledge, skills, and abilities (KSAs) to ease stress caused by the hiring process and provide clarity of expectations between organizations and candidates.

Current Trends in Cybersecurity Education

In the cybersecurity discipline, there are multiple pathways an individual can take to gain an education. It is common for people to attend college and receive a degree, but a non-traditional route through self-teaching is also an option (Maennel, 2020). Regardless of which path is taken, having hands-on training resources is vital to becoming a productive worker in the cybersecurity field. Due to the everchanging nature of cybersecurity, professionals need access to resources to keep their skills up to date. Hands-on labs and courses need to be readily accessible for anyone interested in maintaining their skillset. A commonly brought up issue in meetings with the ICSCOP was that college programs focus on theory instead of hands-on experience. Cybersecurity graduates generally lack practical experience, which is particularly important to employers. There is a need to expand hands-on learning opportunities that can offer students a chance to gain and apply skills necessary to be effective in the cybersecurity workforce.

While the phrase "hands-on" might lead one to assume the training can only be offered in person, there are alternatives that can effectively train students outside of the physical classroom setting. Virtual labs through cloud platforms are becoming increasingly common because they allow students to access labs at any time, making training more accessible to students who are unable to attend a lab at a specific time during the day. Virtual labs are often the best option due to easy accessibility and scalability, leading to reduced costs.

There is a multitude of free training platforms available online students can take advantage of in their spare time. For example, the Naval Postgraduate School developed a game called CyberCIEGE that places the player in charge of an office with the role of protecting it from

various cyber-attacks. Although the content is free, the platforms generally have some restrictions on what can be accessed. Oftentimes, the goal of restrictions is push people to buy additional content or purchase a subscription. There is a definitive need for free, hands-on training platforms that offer complete access to the content necessary to become a cybersecurity professional. The gamification of learning is a useful way to keep students engaged in the material while also teaching them the necessary skills they need to be successful (Maennel, 2020). Courses that actively engage students increase retention and are more effective.

There are also physical courses students can attend in person. Currently the SANS Institute and InfoSec are two of the top providers of hands-on cyber training. SANS provides courses and ranges that can be attended remotely or in person in a few major cities in North America, Europe, and Asia (SANS Institute). These opportunities focus on a wide array of topics from penetration testing to forensic analysis. The quality of these courses is well recognized throughout the industry. However, many students can find it difficult to attend the ranges provided by either group mainly due to the range's accessibility. Geography presents a significant obstacle for Idaho residents as these courses are not offered in the area. Overall, current existing forms of cyber education consist mainly of college courses, paid training outside of college, and online content. Within these forms, barriers to learning can arise, which could present problems to students.

Barriers to Learning

Barriers to learning exist in every field, but there are additional challenges in the field of cybersecurity especially in relation to hands-on learning options. One of the most impactful and least avoidable barriers is cost. Creation and maintenance of material must be paid for, so hands-on training can be expensive for the creators, sponsors, colleges, and students. Support can also be costly but is necessary to ensure assistance is available if any problems arise. While there is no full solution to the barrier of cost, there are different options that ease this burden for students.

Consistent and convenient access to labs is critical for learning. Though not every student can access physical labs, virtualization, especially cloud-based lab platforms, can ease this struggle. Virtual labs are readily available, provided the user has a computer and reliable access to the Internet. Some students do not have access to these necessary materials, to work around this financial barrier, students can utilize school computer labs and computers at public libraries. Different organizations, including NETLAB, provide equipment for potential students who need aid.

Labs lacking realism and flexibility create barriers for learning. Students should be encouraged to make mistakes, and approach problems with a creative perspective. As students develop their skills, they will be less likely to cause similar errors that would result in more extreme consequences upon entering industry. Since hands-on skills can be dangerous, such as penetration testing or malware injection, it is essential, both practically and legally, that training does not affect the host or the network (Topham). Well-designed virtual labs are a useful option for this type of hands-on training. These labs are improved by allowing the student to find multiple solutions to a problem or to learn by making mistakes as they attempt to navigate the system.

Certain factors of hands-on labs can either create or remove barriers to learning. Varying difficulty can make labs useful for people of different skill levels and allow for sequential and diverse labs. The tools used in labs should reflect those used in the cybersecurity industry to prepare students entering the workforce and give them the ability to transition easily into similar tools. Real-time connection should exist in labs when possible, especially in red / blue team exercises, so students can experience realistic scenarios (Topham). Labs should be updated and well-maintained to ensure that users are learning rather than troubleshooting a misconfiguration. Creativity and continuous work in the process of hands-on lab design can resolve many obstacles.

Scalability Challenges and Pathways

An issue faced when trying to create hands-on learning opportunities is the scalability of the training. As a training platform grows, so do the issues associated with maintaining it. Costs and fluctuation present challenges for scalability. Implementing hardware for training is a massive expense. Renting server space, while less costly, requires significant investment. Therefore cloud-based services, such as AWS, are a useful tool. Cloud-based services allow companies to pay for use rather than buying servers or paying a flat rate for usage they may not need (Topham).

Another problem with large-scale training programs is managing trainees. Personal information, proficiency, and user experience must be tracked for each participant. One solution is to assign four different types of users to hands-on training exercises:

1. Exercise Admin
   - Enters details of the trainees into a database and keeps track of any issues that arise.
2. Exercise Controller
   - Creates, assigns, and schedules the exercises for the trainees, and works with the exercise conductor to analyze the results.
3. Exercise Conductor
   - Moderates the training exercise. They will help trainees set up any virtual environments needed to participate in the exercise. The exercise conductor will also work with the controller to analyze the results and provide feedback to the trainees.
4. Trainees
   - Completes the training exercise. They will participate in the exercise and provide feedback about the experience to the exercise conductor.

Using this system is a great way to help mitigate the challenges of large-scale hands-on learning. When everybody knows what their role is and what is expected of them, it creates a better experience for everybody involved. This also leads to higher quality, more efficient training, and less frustrations for the trainees. Resulting in a positive experience where participants are less likely to lose motivation to continue their education until they are ready to join the cybersecurity workforce.

Having a system in place to ensure large-scale, hands-on training programs are available will benefit the cybersecurity world. Large-scale training programs will be able to use more resources to provide better training, while also training more people. Leading to a more competent and robust cybersecurity workforce.

Measuring Skill Progression

An effective hands-on lab requires a measurement of skill progression to demonstrate what the participant has learned as well as the overall value of the lab. Improvement can be quantified through a pre-lab and post-lab assessment to accurately measure changes in competency. An assessment would demonstrate learning for the participant and highlight areas of the course that need to be refined for maximum learning. Surveys are also helpful for refining courses, though they may not accurately reflect an improvement of skills due to their subjectivity.

Badging and certifications are another way to measure a person's progression in cybersecurity. Badges and certifications are often grouped together because of their similarities. Though a badge is awarded for the mastery of a single skill, while a certification is awarded for the mastery of an entire subject. As students improve their skills, they can obtain certifications to represent the knowledge and skills they possess. As mentioned in meetings with the ICSCOP, badges and certifications are valuable because they present proof of knowledge and skills for an individual that can increase marketability and ease the hiring process for businesses that require certain skillsets. Badges and certifications can also be used as a method of continuing education. The effectiveness of badges and certifications can vary between organizations. They may be seen as critical proof of understanding, or they could be overlooked in preference of a degree and experience as was mentioned in a meeting with INL's HR. National standards for badges and certifications in cybersecurity could greatly increase their effectiveness and ease both learning for individuals and the hiring process for organizations.

Motivation

Idaho National Laboratory's academia partners believe a balance of lecture and experience, along with a strong desire to learn are the most conducive aspects of a positive learning experience. College students often have hectic schedules and responsibilities beyond the heavy workload of their classes, but they also have access to resources such as professors, student discounts, scholarships, and vast amounts of knowledge and learning materials. While independent students face similar challenges, they do not typically have access to the same resources as traditional students. These students need more access and awareness of free, easy-to-use, hands-on training that can advance their skills and motivate them to continue learning. While there are options available, they are not always well-known. With tools such as Cyber-CHAMP and CyberKnights, as well as the training catalog that Cohort 5 is working on, students can be matched to courses for specific KSAs, and employers can look for candidates with a specific skill set, which is why these types of resources are incredibly valuable. Experts in the field of cybersecurity must remain motivated to continue their education to stay up to date with the latest advancements or else risk becoming uninformed. It is critical for labs to replace unused KSAs with the most recent advancements, supplying students with important, relevant training that keeps students curious and wanting to learn more.

Even after obtaining a degree, badges, and certifications, cybersecurity can be a difficult field to enter. Though people are motivated by the opportunities in the field, they may be discouraged by challenges they face. Despite the surplus of jobs and shortage of workers, entry-level jobs with are difficult to find. Most organizations need experts and may not have the budget to train a new employee. Fortunately, after two to five years of experience, a great number of new opportunities arise. If hands-on training were standardized and readily available, the stress of the training process and entry to industry would be eased.

Hands-on training has the potential to address lapses in motivation commonly seen in cybersecurity as it is proven to provide an increase in confidence levels, a healthy social learning environment, and increased engagement. Studies confirm hands-on training boosts confidence, which emboldens student learning (Tulane.edu). Cybersecurity professionals benefit from developing their problem solving skills. Simulations are often the most effective method for this development.

Most conventional education emphasizes singular effort with some inclusion to teamwork, while the professional environment often necessitates the opposite approach. Cybersecurity practitioners and students can enhance the effectiveness of their work by including associates with different skills and backgrounds. Depending upon a team is the realistic alternative to depending on an instructor which encourages students to engage in cooperation. A simulation that depends on teamwork also mandates leadership.

Participants in hands-on learning show that retention of information is up to six times greater than that of lectures. (cnd.zspace.com) Whether visual, auditory, or kinesthetic, there is the ability to generate a conducive environment adapted to each participant.

Lab Design

Labs must be generated to allow diverse yet assessable learning for a broad audience. Ideal environments foster confidence, teamwork, leadership, competition, exposure to expertise, demand creativity, and cross training. Each of these qualities is necessary to provide an opportunity for participants to find edification at their level. Diversity of experience is best provided through a series of sequentially building tasks comprising individual simulations, in a team environment, with the addition of a competitive enterprise. The most popular providers of simulated training position their participants in opposition to each other within an attacking group and a defending group. As cybersecurity experts engage in penetration testing, they can understand the realistic vulnerabilities accessed.

If participants in simulations are assumed to be compiled into a well-balanced team, these simulations present a variety of cybersecurity challenges. The NIST cybersecurity framework identifies the five phases of cybersecurity as identify, protect, detect, respond, and recover (Nist.gov). The use of these phases can be seen throughout an organization. People, processes, and information must be defended from cyber threats.

Implementing secure operational processes is the broadly painted method by which threat vectors are decreased. Cybersecurity students trained in policy design and enforcement must consider the possibility of potential loss as present in every operation and action that is related to the organization. Attention called to the modalities of operation can mitigate or avoid unsafe behaviors, which can lead to compromise. While phishing campaigns and password requirements are often seen as an annoyance, the skillful deployment of these and similar practices can provide robust protection against a variety of threats. Much of the utilization of these practices involves proper configuration of software and infrastructure provided or hosted by third parties. Any email services, cloud systems, et cetera can be configured to increase the integrity of an organization. Properly configuring the products of the most popular technology service providers hardens one part of the system. Still more concern is to be directed to securing operations on the premise, or exclusively within an organization. This security can be enforced through the proper administration of host machines, physical access, internal auditing, and more. There are many

disciplines parcel to this concept. Realistic and diverse training with platforms and systems concerned is essential. Vulnerability testing will be fruitfully undertaken herewith (Compact.nl). Such can provide continuous improvement through verification where flaws can be found and overcome.

The value of informationally concerned cybersecurity is often framed by the CIA Triad, Confidentiality, Integrity, and Availability of information must be maintained (NIST 2). The priority of information assurance is known to employ technological methods and may see the most significant arms race between attacking and defending parties. Any component of the triad being compromised results significant loss. The importance of these values calls for substantial investment to their preservation. The training in methods of protecting information compromises the bulk of cybersecurity education for most practitioners. While each constituent of the CIA Triad is justified, one or another may call for special emphasis due to particular circumstances.

Risk of loss of confidentiality of information is centered in the improper disclosure of protected data. This information may be proprietary, financial, medical, or personally identifiable information (PII). Encryption, access restriction, and secure communication protocols aim to fulfill confidentiality requirements. Flaws in these technologies are continually discovered and patched by professionals. Education to accomplish this goal can be achieved by securely configuring storage and communications. Hands-on lab design involves implementing and testing security methods. Encrypting storage or setting an encryption standard on communications is simply done (Cisco), yet the ability to deliver an enterprise-ready solution must be honed. Many environments comprise dozens or hundreds of hosts with diverse auxiliary technology, which brings an example of a condition under which a study has limited value. Issuing a realistic solution that maintains proper resource segmentation and prevents proliferation of protected information while preserving its utility must be exercised in a simulation.

Conclusion

Cybersecurity is a constantly evolving field. New threats arise every day and there is a need for cybersecurity workers to secure systems against these threats. However, the absence of effective hands-on training opportunities leads to cybersecurity workers entering the workforce without the skill set they need to succeed. A lack of competent cybersecurity workers results in nation's computer systems being more vulnerable than ever. Everything, from industrial control systems to the biggest corporations in Silicon Valley has a need for properly trained cybersecurity professionals.

There are many barriers to creating a useful hands-on training exercise. The more these barriers are analyzed, the easier it will be to come up with solutions. The most important part of the process is initiating continuous improvements over time. Creating engaging and meaningful hands-on training exercises will help prepare industry professionals to prevent cyber attackers from accessing the nation's computer systems.

Ultimately, the continual development of accessible and engaging hands-on labs will be necessary to create a cyber-ready workforce. The cohort focused on hands-on learning should continue to develop new, engaging opportunities, and advocate for the use of resources designed to advancement in the field of cybersecurity. Cybersecurity is not a regulated profession, as it lacks a uniform set of ethical standards and disciplined codes. Compared to certified public

accountants who must train under a CPA for years, pass an exam, continue education throughout their career. Cybersecurity lacks these regulations, so the future of this field depends on the development of national standards, which will improve the quality of hands-on skills, training, and cybersecurity readiness.

References

Ase-gsw.tulane.edu. (n.d.). Building Confidence Through Hands-on Activities. http://asee-gsw.tulane.edu/pdf/building-confidence-through-hands-on-activities.pdf.

Cisco. (n.d.). 2021 Data Privacy Benchmark. https://www.cisco.com/c/dam/global/en_hk/products/security/security-reports/2019_cisco_cybersecurityseries_data_privacy_benchmark_study_en.pdf.

Cyber Security Courses and Certifications. (n.d.). SANS Institute. https://www.sans.org/cyber-security-courses/.

Danielle.santos@nistgov. (2021, July 20). *Free and low cost online cybersecurity learning content.* NIST. https://www.nist.gov/itl/applied-cybersecurity/nice/resources/online-learning-content.

Data integrity: Identifying and Protecting Assets Against Ransomware and Other Destructive Events. Executive Summary - NIST SP 1800-25 documentation. (n.d.). https://www.nccoe.nist.gov/publication/1800-25/VolA/index.html.

Maennel, K. (2020). *Learning Analytics Perspective: Evidencing Learning from Digital Datasets in Cybersecurity Exercises*. 2020 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). https://ieeexplore.ieee.org/abstract/document/9229751.

National Initiative for Cybersecurity Education (NICE) Cybersecurity WORKFORCE FRAMEWORK. Cybersecurity and Infrastructure Security Agency CISA. (n.d). https://www.cisa.gov/nice-cybersecurity-workforce-framework.

Navigation. Naval Postgraduate School. (n.d.). https://nps.edu/web/c3o/cyberciege.

Nicole.keller@nist.gov. (2021, July 21). *Cybersecurity framework.* NIST. https://www.nist.gov/cyberframework.

Purple team: Drive defense with offense. Compact. (2020, April 23). https://www.compact.nl/en/articles/purple-team-drive-defense-with-offense/.

A scalable model for implementing cyber security exercises. IEEE Xplore. (n.d.). https://ieeexplore.ieee.org/abstract/document/6828048.

Topham, L., Kifayat, K., Younis, Y. A., Shi, Q., & Askwith, B. (n.d.). *Cyber Security Teaching and Learning Laboratories: A Survey*. Google Books. https://books.google.com/books?hl=en&lr=&id=ZKDYDwAAQBAJ&oi=fnd&pg=PA135&dq=cybersecurity%2Bskills%2Bmeasurement&ots=RuEvo4EgPm&sig=qWoNo2l2aWMbhQKNFpX_hRPdLv0#v=onepage&q=cybersecurity%20skills%20measurement&f=false.

Appendix A

Co*Star

Customer

- Who
  - Students, independent professionals, cybersecurity experts
  - Anyone with a desire to learn more about cybersecurity
  - Industry and Academia
- Unmet Needs
  - Scalable platforms and cost-effective solutions
  - Engagement and competition
  - Accessible hands-on learning opportunities
  - Improvements in the academia / industry pipeline

Opportunity

- The scale of the problem is worldwide
- Currently working within Idaho to research and find solutions, but national expansion may occur in the future

Solution

- Virtualization and cloud-based resources
- Gamification
- Accurate skill measurements
- National standards

Team

- Current
  - ICRP, ICSCOP, INL
  - College partners
- Future
  - Congress / elected legislatures / governmental agencies
  - Other national labs

Advantage of Hands-on Training over Theoretical Learning

- Increased engagement and retention
- Teamwork and leadership opportunity
- Real-world KSAs

Results

- Cybersecurity readiness / industry preparedness
- Ease of transitioning from learning to industry
- Marketability and Confidence in their KSAs

Ask

- National standards and regulations
- Continued development of out-of-the-box hands-on learning opportunities
- More collaboration between experts in industry and academia to meet the needs of students

Appendix B

Additional Tasks

Throughout the course of this internship, the cohort had opportunities to work on additional projects and conducted research into different municipalities throughout Idaho as well as major cybersecurity incidents, such as the Colonial Pipeline attack. As the cohort reached out to different organizations, free use of the Cyber-CHAMP tool, which has been in development, was offered. The cohort aided in design that would provide clarity to users and had the opportunity to view the process of web development. This process was also seen in the splash page set up for the ICRP, for which the cohort provided input.

All INL employees are required to go through certain training, and the cohort was fortunate enough to gain access to additional training specific to ICS cybersecurity. Each cohort took the CISA training course. Due to the nature of the cohort, access to additional resources including NETLAB and VMware training was provided. This cohort also developed at-home virtual ranges and labs. The ranges consisted of security monitoring, penetration testing, and victim hosts, allowing for attack and defense on a single host. The labs developed employ these same principals. Participants in these labs will be guided to use state-of-the-art attacking and defensive technologies and methods.

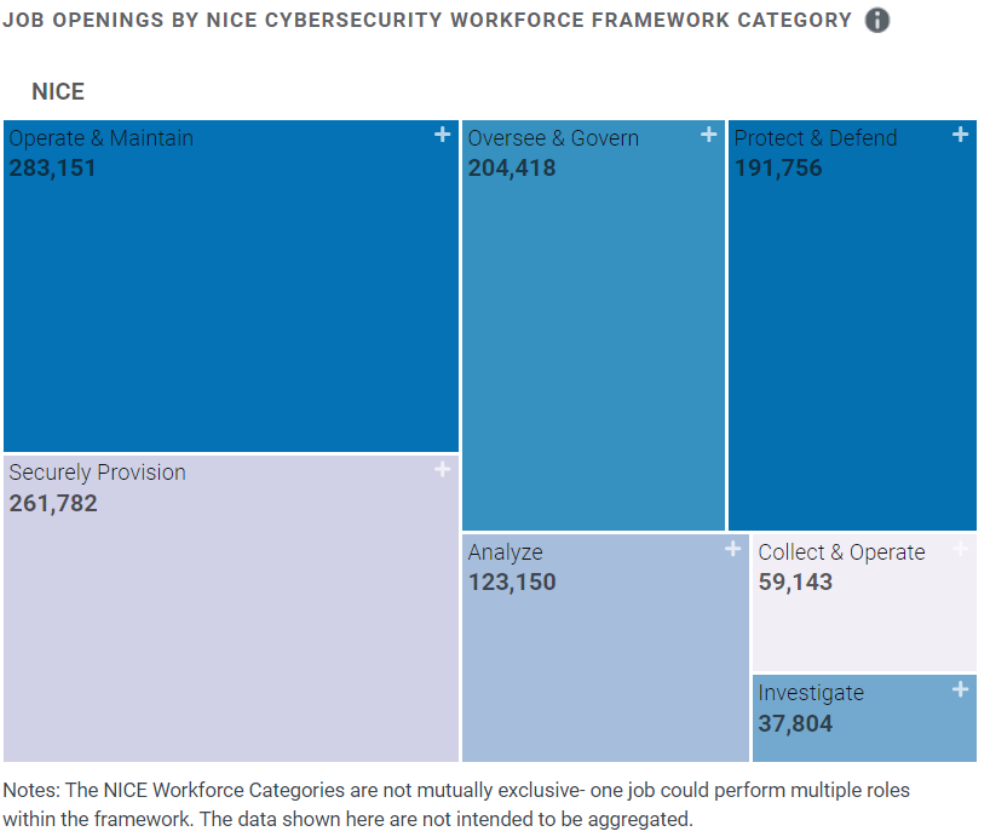
The cohort presented the idea of an escape room that could potentially be included as the hands-on section of the CISA 301 training. The cohort developed an escape room focused on incident response that employed the use of ICS kits. The escape room immerses the trainee into the middle of a cyber-attack with the objective to secure their systems and ensure everything running properly. This training bridges a gap between IT and OT as the student must secure both the networks and the physical systems. The simulation provides opportunities for learning to people with different skill levels and experiences. The escape room has a speed run option and a maximum points option. Users can see how quickly they can expel the attacker and mitigate the main problem, or they can harden their systems to be less likely to be compromised again in the future.

Appendix C

Relation to Other Cohorts

Cohort	Purpose	Relation
1. SS Cyberion	Building a cyber-ready workforce	By providing training that allows students to obtain badges and certifications, organizations can see how qualified candidates are as well as note what knowledge gaps need to be filled. This provides efficiency and clarity to create a more cyber-ready workforce.
2. Team Quiver	Determining need and duties for cyber jobs	By determining what is necessary for a cybersecurity position, badging and certifications can be connected to a role in an organization. This would simplify the hiring process, place people in roles suited for their KSAs, and supply organizations with necessary positions.
3. Cyber League	Solutions for the Individual in the Education / Industry Pipeline	By identifying the obstacles faced by individual students and the faults within the academia / industry pipeline, hands-on training platforms can be refined to best fit the needs of individuals. Through improvements in self-efficacy, awareness, and support, individuals will be able to focus on meaningful training in preparation to enter the workforce. Connecting students with training (using CyberKnights and Cyber-CHAMP), apprenticeships and internships can also increase hands-on skills.
5. Boilermaker	ML Development	Through the use of machine learning, cybersecurity courses can be categorized into an easily utilized, indexed catalog based upon text-based language elements used to define each course. Allowing students to be more easily matched with courses to develop specific KSAs.

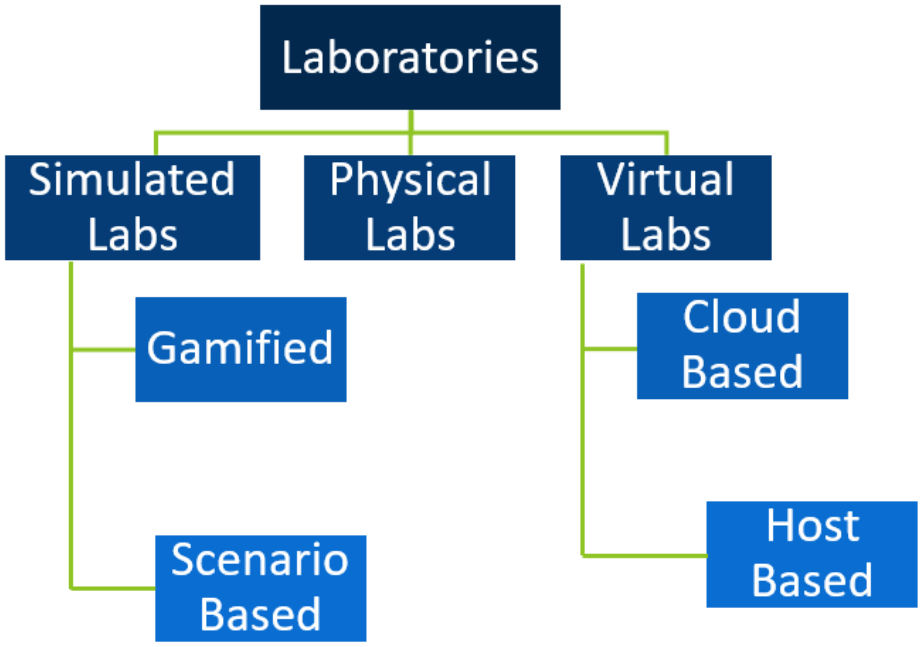
Appendix D



The NICE Cybersecurity Workforce Framework is **the foundation for increasing the size and capability of the U.S. cybersecurity workforce**. It provides a common definition of cybersecurity, a comprehensive list of cybersecurity tasks, and the knowledge, skills, and abilities required to perform those tasks. (cisa.gov)

Appendix E

Categorization of Labs



This chart was created by Cohort 4

- Simulated:
  - Gamified
    - Definition: Gamified learning includes interactive elements and aims to make education enjoyable.
    - Examples
  - Scenario Based
    - Definition: Scenario based learning simulates a historical or fictitious occurrence in which participants must solve a given set of problems.
    - Examples: The escape room this cohort designed, and many courses offered through professional cybersecurity educators are scenario based.
- Physical
- Virtual
  - Cloud-Based
    - Definition: Cloud-based labs are accessed via remote interface and operate in a virtual or hosted environment.
    - Examples: Netlabs, VMware, and educators utilize cloud-based solutions.
  - Host-Based
    - Definition: Host-based labs utilize a virtual environment local to the participant.
    - Examples: Home labs are commonly used by cybersecurity and IT professionals.