NICE | community coordinating council

THE CYBER RANGE

A GUIDE

Guidance Document for the Use Cases, Features, and Types of Cyber Ranges in Cybersecurity Education, Certification, and Training

Prepared by the Cyber Range Project Team and the NICE Community Coordinating Council, Cybersecurity Skills Competitions Community of Interest

September 2023

Table of Contents

SUMMARY

Cybersecurity is a twenty first century challenge requiring a twenty first century workforce. The current cybersecurity workforce lacks sufficient professionals with the skills, training, and credentials to meet this cutting edge challenge. Market studies predict that this talent and skills gap will continue to widen among current and prospective cyber professionals over the coming years, creating a tremendous risk to business, government, and society.

A proven tool for reducing this skills gap and securing society is the cyber range. Cyber ranges are interactive, simulated platforms and representations of networks, systems, tools, and applications. Cyber ranges can:

- Provide performance based learning and assessment
- Provide a simulated environment where individuals can work together to solve complex problems, improving teamwork and team capabilities
- Provide real time feedback
- Simulate on the job experience
- Provide an environment where new ideas can be tested and refined

This document first defines what a cyber range is and explores key use cases. This includes identifying key cyber range audiences, capabilities, and features. Finally, the paper describes several types of cyber ranges and summarizes a criteria checklist for selecting a cyber range for different use cases.

PURPOSE

Cybersecurity professionals require specialized education and hands-on training. The cyber range serves as a valuable tool and catalyst in these endeavors. This document aims to describe the capabilities and features found in different cyber range models and implementations.

The purpose of providing these descriptions of cyber range platforms is to facilitate an informed comparison of available options. Educators, users, or organizations can confidently explore and select a cyber range that best suits their needs. It is important to note that this document does not propose a scoring or ranking system for the features described, nor does this document provide recommendations relative to a particular platform, product, or vendor.

The value of this document centers on the exploration and analysis of the various technologies and methodologies deployed by cyber ranges. As the ecosystem of cybersecurity training, education, and workforce development continues to expand, this resource serves as a reference for the diverse uses and specifications found in cyber ranges. Its goal is to provide information about the key capabilities and features associated with these ranges.

APPROACH

The Cyber Range Project Team initiated their efforts by updating the existing Cyber Range One Pager to further define a taxonomy that describes cyber ranges. Through extensive discussions, this task evolved into the development of a guidance document. The purpose of this document is to offer cyber range users a detailed overview of the diverse features and capabilities that ranges can offer, enabling them to evaluate and determine the most suitable range type and functionality for their specific requirements. Additionally, the working group has expanded their task to include the creation of a formal checklist. This checklist will assist potential users in their search and selection process of a cyber range, aiding them in their efforts to deploy an appropriate range for their needs.

AUDIENCE

The primary objective of this document is to offer practical guidance to individuals and organizations, including governments, for-profit and non-profit entities. Its aim is to assist them in addressing the cybersecurity workforce gap by engaging, implementing, or utilizing a cyber range. The following are potential audiences for cyber ranges and users of this document:

- Educators in search of curricula and/or infrastructure for hands-on exercises.
- Individuals seeking workforce training and continuing education.
- Organizations in need of training, skills validation, or range exercises.

While the above list is not exhaustive, it serves as a fundamental framework to understand the issues that cyber ranges aim to resolve and the valuable use cases they offer to stakeholders.

PROBLEM DEFINITION

WHY ARE CYBER RANGES NECESSARY?

Organizations and individuals who seek cybersecurity education, workforce development, or training encounter a shortage of simulated environments similar to those found in professional fields like aerospace, business, or medicine. The cybersecurity profession faces multiple challenges, including factors such as the realism of training, the legality of training exercises, the capabilities of training platforms, the flexibility of training methods, the accessibility of training environments, and the scalability of training models.

Cyber ranges are interactive and simulated platforms that replicate networks, systems, tools, and applications. They provide a safe and legal environment for acquiring hands-on cyber skills and offer a secure setting for product development and security posture testing. Cyber ranges have a crucial role to play in facilitating and promoting cybersecurity education, training, and certification. These vital tools may consist of actual hardware and software or a combination of physical and virtual components. This document will outline the function and usefulness of cyber ranges in academia, business, and government, addressing the prevalent cybersecurity workforce gap they face.

WHO NEEDS A CYBER RANGE?

Before individuals or organizations consider implementing, purchasing, or utilizing a cyber range, it is essential for them to have a clear understanding of their own purpose and objectives. The table provided below presents a non-exhaustive list of potential use cases for cyber ranges.

CYBER RANGE USE CASES	
1	Educators seeking to implement basic and advanced cybersecurity education courses and curricula
2	Organizations or individuals seeking training and continuing education for security operations, analysis, and forensic specialists
3	Organizations seeking “situational operations” testing for new products, software releases, and organizational restructuring
4	Organizations or individuals seeking cybersecurity skills validation to evaluate candidates for cybersecurity positions
5	Individuals seeking workforce training for people moving into cybersecurity related fields and positions

These use cases can serve various objectives, including:

- Enhancing individual and team knowledge and capabilities across diverse groups.
- Applying knowledge in a simulated network environment to develop cyber skills.
- Collaborating as teams to solve cyber problems.
- Preparing for cyber credentialing examinations or assessments.
- Evaluating cyber capabilities and testing new procedures.
- Training teams on new organizational and technical environments and protocols.

It's important to note that these objectives are not exhaustive, but they represent common goals that can be achieved through the use of cyber ranges.

FEATURES OF A CYBER RANGE

Traditional education and training models fall short in addressing the cybersecurity skills gap. Cyber ranges offer the necessary technology to effectively implement, assess, and track the training and performance of cybersecurity professionals. They instill confidence in both job seekers and employers by providing training that accurately predicts job success. This section of the guide highlights the key features of cyber ranges that play a crucial role in bridging the cybersecurity skills gap. These features include technical components, realism and fidelity, accessibility and usability, scalability and elasticity, as well as curriculum and learning outcomes.

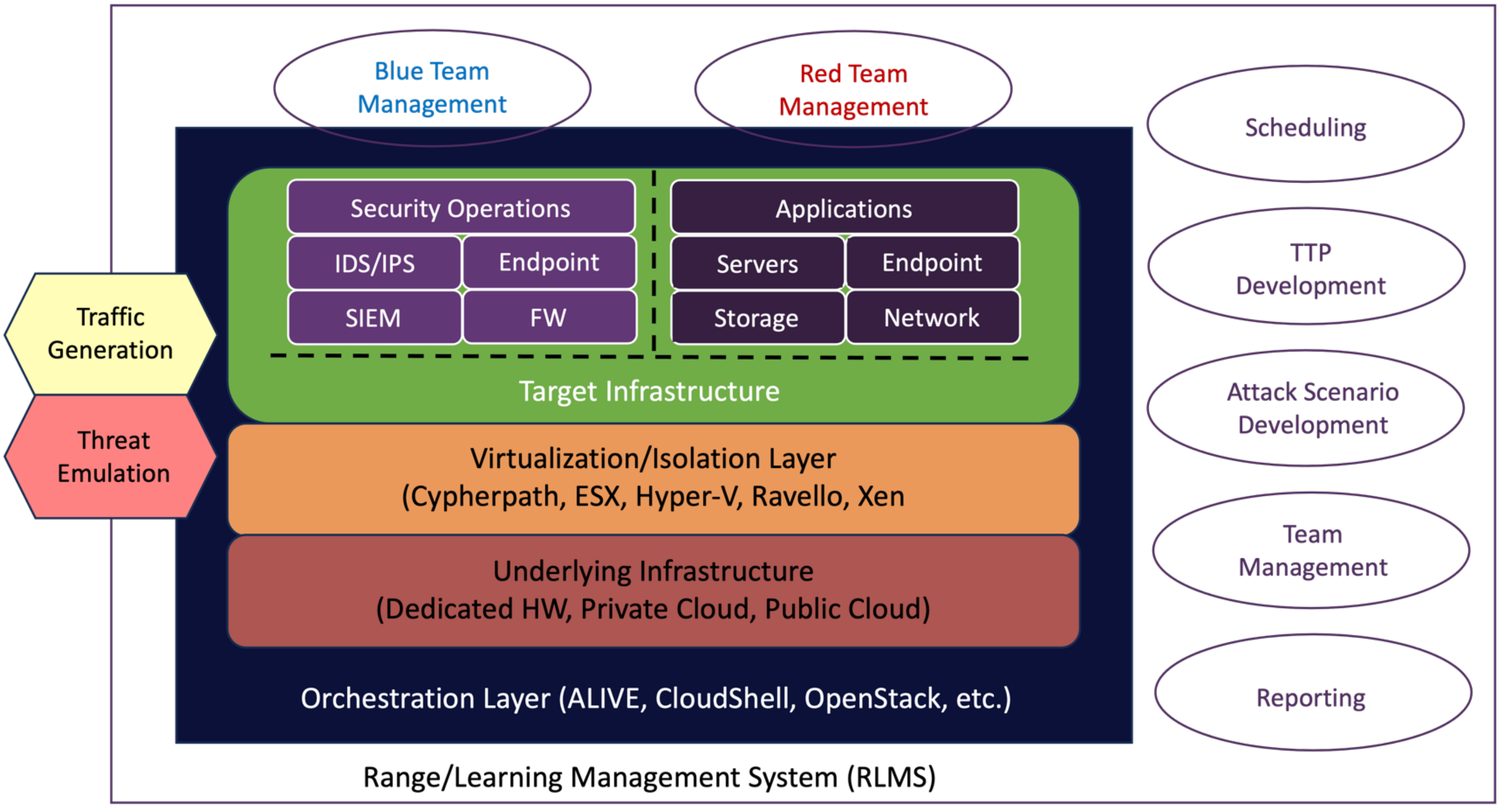
TECHNICAL COMPONENTS

Cyber ranges have many moving parts, but the essential core technological components include:

Range Learning Management System

A key component found in many cyber ranges is the range learning management system (RLMS). As the name implies, the RLMS encompasses the standard features of a learning management system (LMS) along with the distinct characteristics specific to a cyber range.

The diagram provided below depicts the technical components of a range and highlights various features of an RLMS.


Blue Team Management
Red Team Management
Scheduling
TTP Development
Attack Scenario Development
Team Management
Reporting
Traffic Generation
Threat Emulation
Security Operations
IDS/IPS
Endpoint
SIEM
FW
Applications
Servers
Endpoint
Storage
Network
Target Infrastructure
Virtualization/Isolation Layer (Cypherpath, ESX, Hyper-V, Ravello, Xen
Underlying Infrastructure (Dedicated HW, Private Cloud, Public Cloud)
Orchestration Layer (ALIVE, CloudShell, OpenStack, etc.)
Range/Learning Management System (RLMS)

Orchestration Layer

The orchestration layer, fueled by input from the RLMS, brings together the various technology and service components of a cyber range. While some cyber ranges rely on an in-house developed orchestration layer, others opt for a commercial product. The orchestration layer plays a crucial role in the effectiveness of cyber ranges, as it enables the integration of the underlying infrastructure, virtualization or isolation layer, and the target infrastructure. Moreover, this layer facilitates dynamic cyber range extensibility, supporting public cloud, private cloud, and dedicated hard-wired infrastructures.

Underlying Infrastructure

Every cyber range relies on an underlying infrastructure consisting of networks, servers, and storage. While some dedicated ranges are directly built on physical infrastructure (such as switches, routers, firewalls, endpoints) within a rack, this approach is often expensive and lacks scalability. To address scalability, cost, and extensibility concerns, many range providers are transitioning to software-defined virtual infrastructure. The infrastructure chosen significantly impacts the realism and fidelity of the cyber range.

When selecting and utilizing the infrastructure, an important consideration revolves around the level of support required for legacy hardware or software to meet the client's specific use cases. It is worth noting that although not strictly part of the underlying infrastructure, many cyber ranges incorporate use cases that involve traffic generation and attack emulation.

Virtualization Layer

The majority of cyber ranges employ virtualization to reduce their physical footprint. There are two common approaches: hypervisor-based solutions and software-defined infrastructure. Regardless of the virtualization method chosen, the degree of disintermediation between the underlying physical infrastructure and the target infrastructure has an impact on the realism of the cyber range, as it can introduce undesirable and unpredictable jitter and latency. However, virtualization is essential for creating economically viable cyber ranges. It also serves as a protective barrier between the target infrastructure, which may contain potential attack vectors, and the underlying infrastructure, which can be dedicated, public cloud, or private cloud-based.

Target Infrastructure

The target infrastructure refers to the simulated environment in which students are trained. Depending on the specific use case, the target infrastructure can sometimes replicate the student's actual IT and security infrastructure in the real world. Advanced cyber ranges include profiles of commercially available servers, storage systems, endpoints, applications, and firewalls. When students interact with the range, the RLMS generates scripts that guide the orchestration layer in creating the target infrastructure. These scripts may include client-specific configuration details such as IP address ranges, routing information, server stacks, and endpoint software.

REALISM & FIDELITY

The level of accuracy with which a cyber range replicates the real world plays a crucial role in developing predictive operational and learning outcomes. It's important to note that high fidelity in simulation does not necessarily equate to a real-world representation. While emulation generally creates a more realistic environment with both operational and functional fidelity, simulation is often a more practical choice. In other words, individuals and organizations must strike a balance between cost, practicality, and reality when considering their options.

When teaching or training specific skills, it may even be beneficial to use a less realistic scenario. This allows the trainer and student to focus on mastering the skill itself. The integration of that skill into more realistic environments can occur at a later stage in the training cycle.

ACCESS CONSIDERATIONS

Another key consideration regarding the capabilities of a cyber range revolves around how users can access its features and engage in rage activities. Access considerations can generally be divided into two main issues: location and sophistication.

Location

A key aspect of accessibility is whether the range platform is an on-premises or cloud-based solution. It is crucial for users, instructors, and range owners to understand how and when they can access the range technology and applications. For instance, educators should be aware of the differences in access at the school, county, and state levels. Furthermore, the selected location, whether on-premises or in the cloud, can be affected by bandwidth limitations.

In the case of internet-accessible range environments, it is essential to consider the hardware and software requirements for clients. Some remote virtualization solutions necessitate the installation of client-side software, while others can be accessed through a web browser.

Sophistication

Analyzing accessibility also involves considering the users' level of sophistication. Cyber range owners need to comprehend the required effort for installation, usage, and implementation. Operators, trainers, and faculty members must have a clear understanding of the modules, levels, and tools available within each platform or system.

SCALABILITY & ELASTICITY

Scalability refers to the cyber range's capacity to accommodate the target user population effectively. Elasticity, on the other hand, relates to the time required to expand the range's capacity to accommodate additional users. Ideally, a range should be capable of supporting its entire potential user population simultaneously, and swiftly increase its capacity upon request.

Cyber ranges relying on local hardware infrastructure face limitations imposed by the available RAM and hard drive space. They can only scale up to the point where local resources are exhausted and thus lack elasticity. Increasing capacity beyond the provisioned limits requires purchasing and configuring new hardware and software, which can take weeks or even months.

In contrast, public cloud-based ranges generally exhibit excellent scalability by leveraging additional resources from cloud providers as needed. They can also be highly elastic when automation is heavily employed, relying on the underlying public-cloud infrastructure for provisioning system resources for additional users.

Apart from computer and storage infrastructure, scaling also necessitates sufficient server-side bandwidth to accommodate high user access volumes during peak periods. Limited scalability and/or elasticity can lead certain commercial range solutions to impose restrictions on simultaneous access. This may involve requiring instructors or students to reserve time slots or denying access until sufficient resources become available.

CURRICULUM & LEARNING OUTCOMES

Cyber range-based curricula and learning outcomes are central to all possible use cases and stakeholder objectives for utilizing a cyber range. Not surprisingly, this field is rapidly evolving and can be difficult to navigate. This section provides an overview of the emerging trends and models in this area.

Cyber Range Curricula

There are two primary models that encompass the majority of cyber range curricula: pre-packaged curriculum and ad hoc curriculum. The pre-packaged curriculum features a syllabus with low to medium fidelity content, testing, and gamification, providing a standardized path to completion. On the other hand, the ad hoc curriculum is highly customizable and tailored to each client, often necessitating a persistent, integrated, and high-fidelity experimentation space. The table below provides an outline of potential and probable curriculum customization for different use cases.

	CYBER RANGE USE CASES	CURRICULA
1	Educators seeking to implement basic and advanced cybersecurity education courses and curricula	Pre-Packaged Ad Hoc
2	Organizations or individuals seeking training and continuing education for security operations, analysis, and forensic specialists	Pre-Packaged Ad Hoc
3	Organizations seeking “situational operations” testing for new products, software releases, and organizational restructuring	Ad-Hoc
4	Organizations or individuals seeking cybersecurity skills validation to evaluate candidates for cybersecurity positions	Pre-Packaged
5	Individuals seeking workforce training for people moving into cybersecurity-related fields and positions	Pre-Packaged

The next important question for a range operator or user to understand is how the curricula, whether pre-packaged or ad-hoc, aligns or maps to prominent industry frameworks and standards.

The NICE Framework

The National Institute of Standards and Technology (NIST), located within the United States Department of Commerce, is one of the federal government's primary agencies responsible for creating and establishing cybersecurity frameworks. Within NIST, there is a dedicated cybersecurity education and workforce initiative known as NICE. This essential initiative “is a partnership between government, academia and the private sector” with a mission to “energize and promote a robust network and an integrated ecosystem of cybersecurity education, training, and workforce development.” The NICE mission seeks to “coordinat[e] with government, academic, and industry partners to build on existing successful programs, facilitate change and innovation, and bring leadership and vision to increase the number of skilled cybersecurity professionals helping to keep our nation secure.” [1]

As a part of this mission, NICE engaged its various stakeholders in order to create a comprehensive workforce framework for cybersecurity, known as the NICE Framework, in order to establish a taxonomy and common lexicon to describe cybersecurity work and workers.[2] The NICE Framework is intended to be applied in the public, private, and academic sectors. To serve the needs of these stakeholders, the Framework outlines the

[1] See the NICE Strategic Plan, available at: https://www.nist.gov/itl/applied-cybersecurity/nice/about/strategic-plan

[2] See the NICE Workforce Framework for Cybersecurity, available at: https://www.nist.gov/itl/appliedcybersecurity/nice/resources/nice-cybersecurity-workforce-framework

following core components: Work Role Categories, Work Roles, Competency Areas, and Task, Knowledge, and Skills (TKS) statements.

The NICE Framework holds significant potential as an essential tool for integrating with Cyber Ranges. Cyber Range administrators can leverage the core components of the Framework to effectively align their curricula and activities. For instance, curricula and activities can be linked to specific Work Role Categories, such as Securely Provision, Operate and Maintain, Oversee and Govern, Protect and Defend, Analyze, Collect and Operate, and Investigate. To ensure consistency and industry relevance, the programming of cyber ranges can prioritize education and training related to Task, Knowledge, and Skills (TKS) within these categories. This approach benefits both the consistency of cyber ranges and the industry as a whole. For more on the NICE Framework, visit -- https://www.nist.gov/nice/framework.

TYPES OF CYBER RANGES

Cyber ranges have evolved into various types, each encompassing a range of features and capabilities as discussed earlier. Broadly speaking, there are four main types of cyber ranges: simulations, overlay, emulation, and hybrid ranges. While these distinctions may seem subtle, they become significant when aligning the type of cyber range with the specific use case of an individual or organization. It is crucial to consider these differences to ensure the optimal match between the cyber range type and the intended objectives of the user or organization.

SIMULATION RANGES

Simulations emerged as the preferred cyber range type for many environments, particularly after being introduced by the United States Air Force in 2002. Simulations involve creating a synthetic network environment that replicates the behavior of real network components. These simulations are executed within virtual instances, eliminating the need for physical network equipment. In a typical simulation setup, virtual machines (VMs) are used to mimic specific servers, networks, and storage configurations found in various IT infrastructures (small, medium, large, etc.).

It's important to note that VM templates used in simulations are standardized, which means they may have limitations in accurately reproducing real-world IT infrastructures. The fidelity of the exercise within the cyber range increases as the simulation closely matches the target exercise infrastructure. Achieving a higher level of granularity in simulating the target environment requires a robust orchestration layer, which plays a critical role in coordinating the simulation activities.

Simulations offer the advantage of quick reconfiguration and the ability to utilize generic server and storage equipment. However, a drawback of simulated networks is the potential for unpredictable and unrealistic latency and jitter in network performance. These factors can impact the overall realism and effectiveness of the simulation.

OVERLAY RANGES

Overlay ranges are cyber ranges that operate on top of existing real networks, servers, and storage systems. Unlike simulations, overlay ranges provide a higher level of fidelity as they directly utilize the actual network infrastructure. However, this increased fidelity comes with notable costs, including the expense of hardware and the potential risk of compromising the underlying network infrastructure. Overlay networks are often established as global testbeds, with one prominent example being the Global Environment for Network Innovations (GENI), which is sponsored by the National Science Foundation. GENI serves as one of the largest overlay networks designed for research and experimentation.

EMULATION RANGES

Emulation involves deploying the cyber range on dedicated network infrastructure, where the actual network, server, and storage infrastructure is mapped onto physical infrastructure. This approach transforms the physical infrastructure into the cyber range itself. Emulation provides closed-network environments that consist of multiple interconnected components. Emulation goes beyond simulating network behavior and includes traffic generation that emulates various protocols, source patterns, traffic flows, attacks, and even the underlying internet connectivity. When executed effectively, emulation delivers authentic and true-to-life experiences, rather than pre-programmed actions and responses.

An important aspect of accurate emulation is the resolution of URLs to the cyber range's DNS and virtualized Internet IP addresses, which are aligned with real-world geo-IP addresses. This ensures a high level of fidelity in the emulation process. A notable example of the use of emulation is the National Cyber Range (NCR), which provides a comprehensive platform for advanced cyber range capabilities.

HYBRID RANGES

As the name suggests, hybrid ranges are formed through a customized combination of any of the previously mentioned types. These ranges integrate various features and capabilities from simulations, overlay ranges, and emulation, creating a hybrid environment that suits specific requirements. The Virginia Cyber Range is an example of a hybrid range that incorporates multiple features discussed throughout this document to provide a comprehensive cyber range experience. Another instance of a hybrid range is the European Future Internet Research & Experimentation (FIRE) initiative, which started in 2008. These hybrid ranges demonstrate the flexibility and adaptability of cyber range implementations, leveraging a combination of range types to meet diverse needs and objectives.

CONCLUSION

Closing the cybersecurity workforce gap and mitigating cyber threats to industry and enterprises necessitates innovative and practical approaches to educate and train both current and aspiring cybersecurity professionals. While traditional academic methods and on-the-job training remain important, they are no longer sufficient to meet the increasing demand for qualified workers in the cybersecurity field.

In this rapidly evolving landscape, the cyber range emerges as a vital tool and platform to bridge the skills gap and enhance societal security.

This document provides actionable guidance to individuals and organizations seeking to address the cybersecurity workforce gap by engaging with, implementing, or utilizing a cyber range. By leveraging the capabilities of cyber ranges, stakeholders can enhance their training and educational initiatives, thereby fostering a well-prepared cybersecurity workforce.

APPENDIX A –
THE CYBER RANGE: A CHECKLIST

This Checklist outlines key features, considerations and options and can be used by an individual or an organization in evaluating the various vendors and providers of Cyber Range platforms, tools and technologies.

FEATURES	CONSIDERATIONS & OPTIONS
Use Case(s) of the Cyber Range	The Cyber Range is focused on the following audiences and/or use cases (more than one selection is possible) – ▪ Educators seeking to implement basic and advanced cybersecurity education courses and curricula ▪ Organizations or individuals seeking training and continuing education for security operations, analysis, and forensic specialists ▪ Organizations seeking "situational operations" testing for new products, software releases, and organizational restructuring ▪ Organizations or individuals seeking cybersecurity skills validation to evaluate candidates for cybersecurity positions ▪ Individuals seeking workforce training for people moving into cybersecurity-related fields and positions
Location of the Range	The Cyber Range is located – ▪ On-Premises (fixed or limited users) ▪ On-Premises (with cloud capability) ▪ Cloud-Based ▪ Hybrid (blend of on-premises and cloud-based)
Curriculum Type	The activities and assessments of the Cyber Range are – ▪ Pre-Packaged (no customization) ▪ Pre-Packaged with Options (some customization) ▪ Ad-Hoc (full and significant customization)
Learning Outcomes & Standard Alignment	The Cyber Range aligns with or utilizes the following standards or certifications – ▪ The NICE Framework ▪ Other ______________________________________
Assessment & Debriefing Tools	The Cyber Range utilizes the following functions to aid in assessment and debriefing of users – ▪ Recording and Replay Functionality ▪ Assessment or Rating/Scoring Functionality ▪ Assessment of Team Performance Functionality ▪ Assessment of Individual Performance Functionality
Scalability & Elasticity	The Cyber Range is able to support – ▪ Limited Number of Users for a Limited Time Period ▪ Limited Number of Users for an Unlimited Time Period ▪ Unlimited Number of Users for a Limited Time Period

	▪ Unlimited Number of Users for an Unlimited Time Period
Training & Support	The Cyber Range operator or vendor provides – ▪ Initial Support and Training ▪ Periodic Support and Training ▪ On-Call Support and Training
The Special Sauce	The Cyber Range includes other features and capabilities such as – ▪ Industry-Specific Customization ▪ A Scheduling Component ▪ Specialized LMS or RLMS ▪ Other ____ ▪ Other ____ ▪ Other ____ ▪ Other ____ ▪ Other ____