



MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

CyberSecurity
MALAYSIA

CYBER RANGE FRAMEWORK: A REVIEW FOR GLOBAL ACE CERTIFICATION



CONTENTS

1.	INTRODUCTION	1
2.	ACRONYMS	2
3.	DEFINITIONS	3
4.	BACKGROUND AND CONTEXT	4
5.	CYBER RANGE	6
5.1	Cyber Range Use Cases	7
5.1.1	Competence Building	7
5.1.2	Competence Assessment	7
5.1.3	Security Education	8
5.1.4	Recruitment	8
5.1.5	Development of Cyber Capabilities	8
5.1.6	Development of Cyber Resilience	8
5.1.7	National and International Cybersecurity Competitions	9
5.1.8	Security Testing	9
5.1.9	Security Research	9
5.1.10	Digital Dexterity	9
5.2	Functionalities & Capabilities	10
5.2.1	Orchestration	10
5.2.2	Internet Services Simulation	11
5.2.3	Attack Simulation	11
5.2.4	User Activity Simulation	11
5.2.5	Scenarios and Content Development	12
5.2.6	Competency Management	12
5.2.7	Data Collection and Analysis	12
5.2.8	Scoring and Reporting	13
5.2.9	Instructor Tools	13
5.3	Cyber Range Functionalities & Use Case Mapping	13
5.4	Delivery Models	14
5.4.1	Cyber Range as a Service	14
5.4.2	On-Premise Cyber Range	15
5.5	International Frameworks	15
5.5.1	NIST NICE Framework	16
5.5.2	MITRE ATT&CK Framework	18
5.5.3	Global ACE Certification Scheme	20
6.	GLOBAL ACE CERTIFICATION CYBER RANGE FRAMEWORK	21
6.1	Global ACE – NICE Cyber Range Framework Mapping	23
6.2	Global ACE – MITRE ATT&CK Framework Cyber Range Mapping	24
6.3	Cloud Cyber Range Functional and Technical Requirement	25
6.4	On-Premise Cyber Range Functional and Technical Requirement	32
	REFERENCES	42

1. INTRODUCTION

This document aims to provide an overview of cyber ranges, beginning from their definition, use cases and functionalities while also looking at the international standards mapping, and different types of technologies and business models that can be implemented under the Global Accredited Cybersecurity Education (ACE) Certification (www.globalace.org).

Besides that, this framework document provides with a set of criteria that can be used to better identify and select suitable cyber ranges to meet specific needs and requirements under the Global ACE Certification scheme.

Global ACE Certification is developed by CyberSecurity Malaysia (www.cybersecurity.my). It is a holistic framework of cybersecurity professional certification that outlines the overall approach, independent assessments, impartiality of examinations, competencies of trainers, identification and classification of cyber security domains and the requirements of professional memberships. The scheme is a large-scale systematic plan of actions to certify and recognise cybersecurity workforce. It is industry driven and vendor neutral, developed in collaboration with government agencies, industry partners and academia.

2. ACRONYMS

APT	Advanced Persistent Threat
API	Application Programming Interface
Bins	Binaries or Executables
CDX	Cyber Defense Exercise
CNCI	Comprehensive National Cybersecurity Initiative
CNO	Computer Network Operations
CR	Cyber Range
CRP	Cyber Range Platform
CTF	Capture The Flag
DDOS	Distributed Denial of Service
ICT	Information and Communication technology
IoT	Internet of Things
Libs	Libraries
OS	Operating System
OT	Operational Technology
UI	User Interface
VM	Virtual Machine
SOC	Security Operations Center

3. DEFINITIONS

Capture the Flag (CTF) – In the context of computer security, a CTF is a type of cyber war game, which can be played either in teams or as individuals. A popular type of CTF is attack and defense where participants compete to compromise other participants' systems while at the same time trying to defend their own.

Competence – Competence is a set of attributes such as knowledge, skills and abilities required to successfully perform specific tasks.

Cyber Defense Exercises – Also more commonly referred to as CDX, a cyber defense exercise is a special type of cyber exercise focused on testing cyber defense capabilities.

Cyber Exercise – A cyber exercise is a planned event during which an organization simulates cyber-attacks or information security incidents or other types of disruptions in order to test the organization's cyber capabilities, from being able to detect a security incident to the ability to respond appropriately and minimize any related impact.

Cyber Resilience – Cyber resilience is the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that include cyber resources.

Orchestration – Orchestration is the automated configuration, coordination, and management of computer systems and software.

Platform – A platform is a group of technologies that are used as a base upon which other applications, processes or technologies are developed.

Scenario – A scenario is content that is used on a cyber range. A scenario may contain only a virtual environment for users to interact with or it may also include a storyline with specific objectives, some practical or theoretical challenges, or different types of questions.

Self-provisioning – Self-provisioning, commonly known as the cloud self-service, is a feature among many cloud service providers which allows their end users to provision resources by themselves and set up or launch a service or application without the intervention of dedicated IT personnel or the service providers themselves.

Virtual Machine – A virtual machine (VM) is a software program simulating the behavior of a physical computer.

Hypervisor – A hypervisor is the software layer between the hardware and the virtual machines (VMs). It coordinates the VMs ensuring they don't interfere with each other and that each has access to the physical resources it needs to execute.

4. BACKGROUND AND CONTEXT

Every 39 seconds, a cyberattack occurs somewhere in the world. These attacks cost organisations an average of \$13 million, and the cumulative global value at risk from being destroyed amounts to approximately \$5.2 trillion in the period from 2019 to 2023 [1].

Every single day, the news headlines scream out about new attacks on the financial industry, financial fraud, credit card fraud, identity theft, data leakage of corporate secrets, defense contractors being bombarded by penetration attempts, public power and water network intrusions, and politically or ideologically motivated cyber-attacks. The simple fact is that no industry is immune to this new and prevalent attack culture.

As cybercriminals and state actors become increasingly sophisticated in their cyberattacks, it's critical for companies and the public sector to ramp up their response capabilities. This includes a skilled cyber workforce. Unfortunately, **businesses globally are facing a mounting shortage of cybersecurity professionals.**

According to a study by the Enterprise Strategy Group (ESG) and the Information Systems Security Association (ISSA), the most significant factors behind data breaches are the lack of proper training for non-technical employees and the lack of highly skilled cybersecurity professionals. The study found that the current cybersecurity skills shortage can be seen as a key factor in the exacerbation of the number of data breaches today [2].

Just how big is this estimated shortage? The International Information System Security Certification Consortium (ISC)2 Cybersecurity Workforce Study 2020 estimates that the gap between the currently employed 2.8 million cyber professionals in 11 major world economies and the total number needed in the public and the private sector is estimated to be around 3.1 million [3].

Currently, the active cybersecurity workforce in the US amounts to 800,000, in the UK to 289,000 and in Germany to 133,000. **The demand for additional professionals in the field is the highest in the Asia Pacific region, which may need a staggering 2 million trained employees in the coming years.** North and South America are close seconds with over 1 million, and Europe has a demand of nearly 300,000 [4].

Cybersecurity was only included into company strategy once they realized their infrastructure, data, and brand were under attack. Suddenly, these businesses needed to train employees to defend their technology and data but were unsure how to do so accurately and efficiently – and all the while the bad guys were evolving their tactics.

There's been an interesting set of discussions going on for years with competing viewpoints as to how to solve these security issues in both the short term and the long term. There are discussions about the benefits of zero-trust architecture, open architectures, benefits of closed architectures, “secure from the ground up” network and competing architectures, use of firewall, intrusion and prevention systems, zero-day attack recognition, unified threat management systems (UMTS), and a plethora of other security architectures and discussions.

Those discussions are necessary, but most neglect something that has been very true since the beginning of recorded human history – education and training are what makes human beings good at something

and provide a means for us to adapt to new surroundings. You cannot expect your IT team to be able to defend against a complex cyber-attack that occurs if you are not adequately training them. It's like sending someone who has never thrown a punch in their life into a fight against the championship boxer. The novice doesn't stand a chance. He'll lose every single time. Yet, that is precisely the situation that most organizations find themselves in today with regard to securing their critical infrastructure.

We, at CyberSecurity Malaysia, are not going to fill the cybersecurity skills gap in a classroom-based theoretical slides, but rather with hands-on cybersecurity training, using a combination of

- simulated labs and
- end-to-end attack real-time simulations
- Performance based assessments

using our Cyber Range Framework based capacity building pathway certifications.

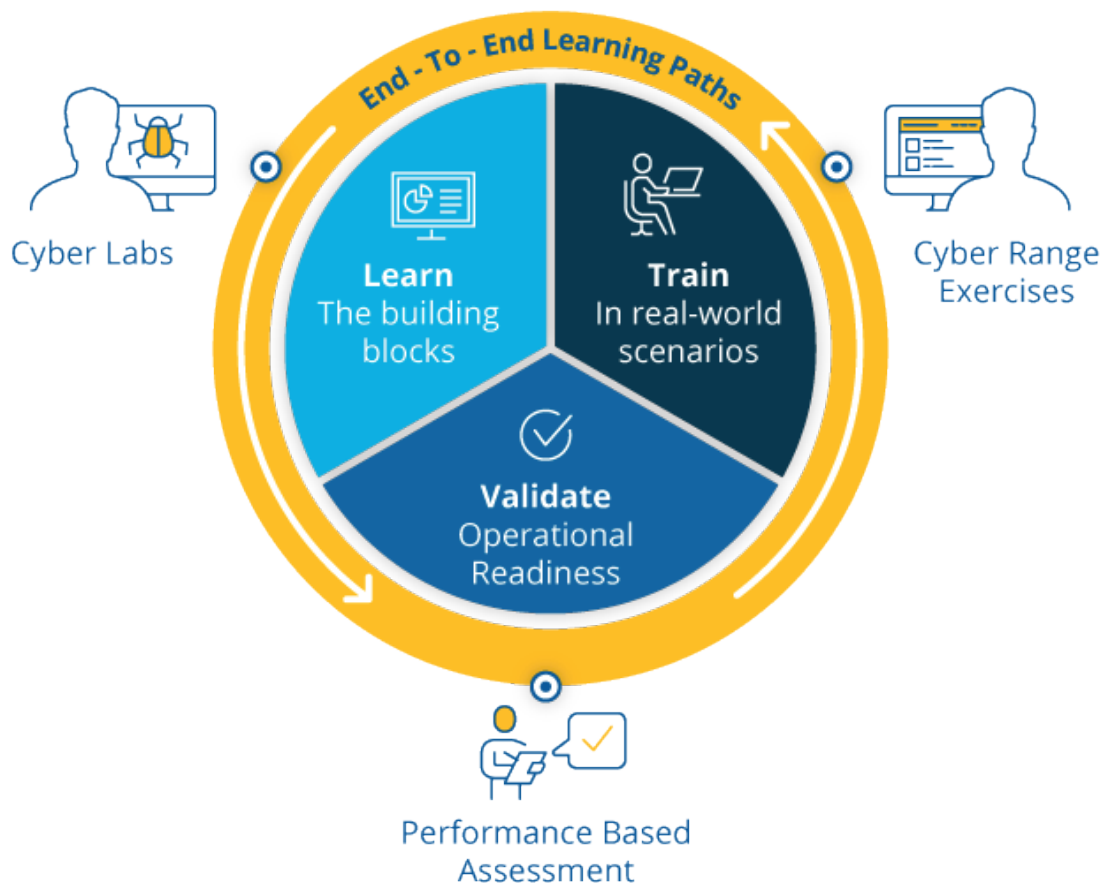


Diagram 1 : End to End Learning Path Lifecycle

5. CYBER RANGE

The meaning of cyber ranges has changed over the years and so has the way they have been defined. A review of currently existing definitions and interpretations from around the world from both private and public sector cyber range initiatives broadly identifies two possible ways of defining a cyber range:

A simulation environment – This view of the cyber range focuses on what cyber ranges have traditionally provided, which is a simulation of ICT and/or OT environments to be used for a wide set of purposes. Some definitions look at cyber ranges as inclusive of the Internet services, which are connected to the simulated environment. This way of defining cyber ranges is somewhat static as it usually refers to a simulation environment which is designed once to meet specific use cases and requirements and where any change in the environment requires considerable time and effort.

A platform – A platform is usually defined as a group of technologies that are used as a base upon which other applications, processes or technologies are developed. In the context of cyber ranges, a platform can be intended to be a group of technologies that are used to create and use a simulation environment. The emphasis here is on the word “use” since for a cyber range to be used for specific purposes, the cyber range must have additional capabilities and expose specific functionalities to the end user. This view of the cyber range is clearly more dynamic as it implies that different environments can be more easily created and that functionalities are provided to help in the use of the simulation environment. How easy it is to dynamically create different simulation environments and the breadth of functionalities offered will then vary across different cyber ranges.

NIST’s definition, for instance, falls into the first interpretation of what a cyber range is, making no reference to services and/or functionalities to be provided by a cyber range other than the simulation environment [5]:

“interactive, simulated representations of an organization’s local network, system, tools, and applications that are connected to a simulated Internet level environment. They provide a safe, legal environment to gain hands-on cyberskills and a secure environment for product development and security posture testing. A cyber range may include actual hardware and software or may be a combination of actual and virtual components. Ranges may be interoperable with other cyber range environments. The Internet level piece of the range environment includes not only simulated traffic, but also replicates network services such as webpages, browsers, and email as needed by the customer.”

The challenge in defining cyber ranges purely from the point of view of the simulation environments can be compared to the challenge of defining a car in terms of its generic technical characteristic such as having 4 wheels, an engine, a gear box, a seat for the driver and for other passengers etc. The Cambridge dictionary defines a car as:

“a road vehicle with an engine, four wheels, and seats for a small number of people”

When it comes to cars though, we have nearly 200 years of experience and we can easily differentiate between sport cars, F1 cars, SUVs, cabrio, 4x4. We can, to a varying degree of ease, look for and select the right car based on our specific needs. The same cannot be said for cyber ranges which have only been around for a few years. Just like cars, cyber ranges can be used for different purposes and by different

types of users. However, unlike cars, cyber ranges have evolved to be highly configurable to the point that while we cannot easily convert a F1 car to a family car, we can much more easily use a cyber range for multiple purposes such as security research, security training, assessing cyber resilience and more.

The great majority of existing cyber ranges from both the public and private sector do offer additional capabilities beyond the mere simulation environment. Furthermore, most cyber range use cases require one or more capabilities beyond the simulation environment. Therefore, it is logical to infer that a cyber range would be better defined as a platform rather than a simulation environment.

On that basis, this **document defines a cyber range as follows:**

A cyber range is a platform for the development, delivery and use of interactive simulation environments. A simulation environment is a representation of an organization's ICT, OT, mobile and physical systems, applications, and infrastructures, including the simulation of attacks, users and their activities and of any other Internet, public or third-party services which the simulated environment may depend upon. A cyber range includes a combination of core technologies for the realization and use of the simulation environment and of additional components which are, in turn, desirable or required for achieving specific cyber range use cases.

5.1 Cyber Range Use Cases

This section of the document focuses on what a cyber range can be used for and not on the specific cyber range functionalities, capabilities or even technologies that would be best suited for each use case. The following is a list of possible use cases of Cyber Range.

5.1.1 Competence Building

Most of the security training today is done through online and face to face training courses with little time spent on hands-on learning. The use of cyber range changes that, as it can provide a convenient and **more cost-effective way of delivering hands-on training, as well as the associated training assessment and certification.** According to Gartner, by 2022, 15% of large enterprises will be using cyber ranges to develop the skills of their security teams, up from less than 1% in 2019 [6].

5.1.2 Competence Assessment

Competence is a set of attributes such as knowledge, skills and abilities required to successfully perform specific tasks. **As the security skills gap increases, organizations need an efficient way of assessing and selecting the right personnel.** Using cyber ranges can allow organizations to perform competence assessment beyond the traditional tests, based on multiple choice questions or theoretical simulations. Cyber ranges allow the assessment to be practical and based on the successful completion of practical tasks and/or on the observation of user behavior and choices made in the execution of practical tasks or assignments.

5.1.3 Security Education

Security education specifically refers to academia as opposed to the lifelong learning and training that professionals undergo after they leave university. **One of the recurring complaints from industry is the lack of hands-on experience by young graduates as their curriculum is not updated and doesn't have hands-on learning.** The root cause of such a gap is the cost and complexity of providing students with hands-on experience while at the same time not diluting the educational value of university degrees. Universities around the world have begun looking at cyber ranges as a means of improving teaching and learning.

5.1.4 Recruitment

As cyber ranges are used for competence assessment, it is also to be expected that they will change hiring practices allowing organizations to better identify, validate and hire suitable candidates.

5.1.5 Development of Cyber Capabilities

Cyber capabilities are the resources and assets available to a state to resist or project influence through cyberspace. At a human level, cyber capabilities coincide with the competences of security professionals across a wide range of cyber-attack and defense domains. In such context, cyber ranges are part of a country's cyber capabilities and can be used for developing the capabilities of security professionals, for the research and development of cyber tools and other assets, and for the continuous delivery of cyber exercises to test those cyber capabilities. Also, within the context of cyber capability development, cyber ranges can be used to organize large scale cyber exercises involving government agencies and private organizations.

5.1.6 Development of Cyber Resilience

Cyber resilience refers to the capability of an organization to respond and be able to sustain a security incident or cyber-attack while maintaining its ability to deliver its core business services. NIST defines cyber resilience as *"the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that include cyber resources"* [7]. Gartner defines it as *"... the degree of adaptiveness and responsiveness to a threat to or failure of digital business ecosystems"* [8]. Overall, cyber resilience applies to any process, system, business and organization where there is a reliance on IT, OT, IoT which pretty much covers the majority of organizations, including critical infrastructure. In the context of cyber resilience, cyber exercises provide opportunities for organizations to demonstrate critical capabilities and reveal how effectively they integrate people, processes, and technology to protect their critical information, services, and assets. Cyber exercises can be divided into 'Capture the Flag' (CTF) and live-fire exercises. CTF are usually organized in attack and defense style where individuals or teams must find and fix vulnerabilities in their own systems while simultaneously attacking systems that belong to other participants. Live-fire cyber exercises enable teams to train cyber professionals to detect and mitigate large-scale cyber-attacks while being constantly attacked by a "red team" of hackers.

Cyber exercises provide the opportunity to test an organization's capability to handle complex cyber incidents involving several organizations at the same time, thus simulating the interaction with subcontractors, service providers, customers, etc. upon which modern organizations depend. Cyber exercises also enable organizations to find gaps and areas for development in their processes, procedures,

and technologies. By addressing the findings from exercises, organizations can greatly enhance their cyber resilience against modern cyber-attacks.

5.1.7 National and International Cybersecurity Competitions

More and more countries are organizing national cyber security competitions and participating in international ones as a way of discovering new cybersecurity talents and to help fill the security skills gap. Such competitions are typically delivered as CTFs involving a combination of practical challenges. Cyber ranges are changing the way such competitions have been organized allowing for more large-scale events and more realistic simulations. Notable examples include the European Cyber Security Challenge organized by ENISA [9], the Word Skills [10], and the CyberStars competition [11].

5.1.8 Security Testing

This is the most traditional use case of cyber ranges where system and application are tested with security attacks carried out against them, in a controlled way, to identify potential vulnerabilities before deployment and use. Example: the IBM X-Force Command Centre, is a situational operations simulator that enables testers to see how systems will withstand malware attacks on new products, software releases, protocols, and organizational restructuring. Security Testing with Cyber ranges can be used as an attack simulator on the software products developed in Malaysia and to provide a security Trustmark validation framework.

5.1.9 Security Research

Cyber ranges are a fundamental means to carry out security research across a wide range of security domains. By their very nature, cyber ranges are themselves being developed by researchers around the world in order to research new attack detection and mitigation methods, malware emulation, and much more. Research demands for environments that are fully controlled and isolated but at the same time complex to develop and test a new tool, or to design new attack techniques or methods. Cyber ranges can be used in Security research with the scope of cyber-security experimentation, machine learning, special malware detection, and 5G cellular IoT security features. Cyber range allows to collect and store data while ensuring their confidentiality and integrity, both logically and physically, while offering a safe environment for researchers to work.

5.1.10 Digital Dexterity

Digital dexterity, as defined by Gartner, is “the ability and desire to exploit existing and emerging technologies for business outcomes” [12]. Traditional software development methodologies and security best practices recommend the use of different environments such as developing, staging and production. With the ongoing digital transformation and the requirements to support multiple communication and business challenges, organizations are being challenged to project those very same traditional best practices across different channels while at the same time supporting faster development lifecycles. Terms like DevSecOps have become engrained into the fiber of modern organizations and cyber ranges are being looked at to provide organizations with the ability to improve the organization’s digital dexterity.

5.2 Functionalities & Capabilities

The emphasis in this section of the framework is on the technical capabilities embedded into the cyber range itself available either to the cyber range end users or its administrators. The following figure illustrates the common architectural components and associated functionalities of a cyber range.

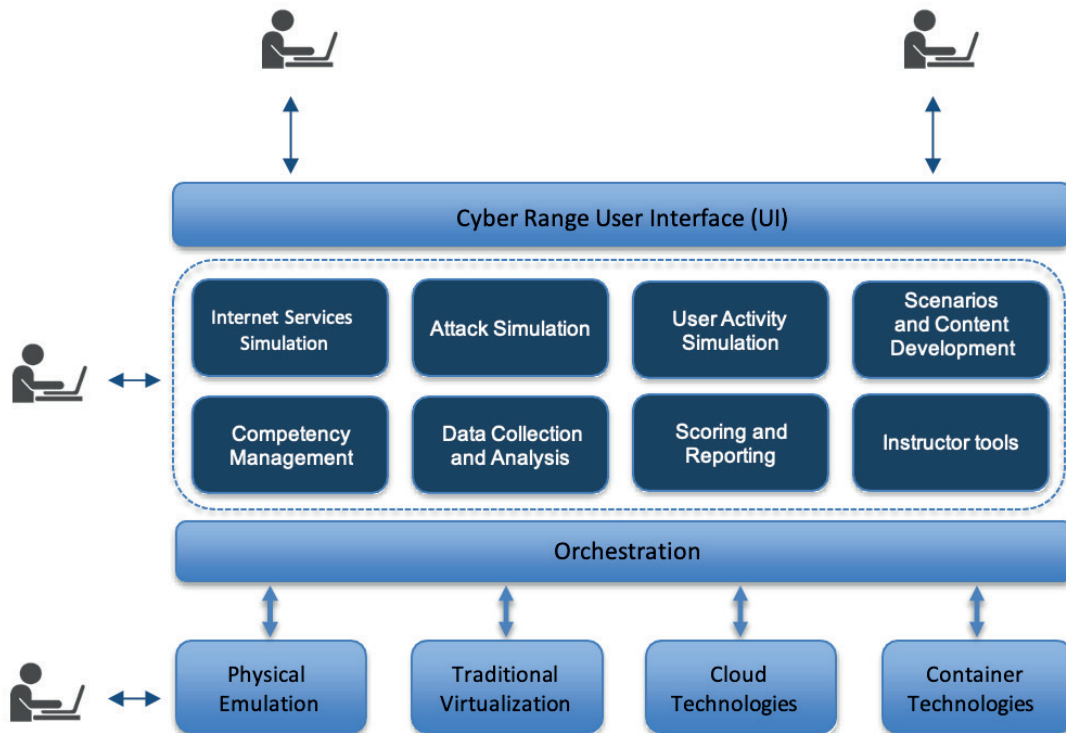


Diagram 2: Architectural Components

5.2.1 Orchestration

Orchestration is the automated configuration, coordination, and management of computer systems and software. In relation to cyber ranges and to virtualization technologies, orchestration refers to the technology responsible for the creation of automation workflows including the mass configuration, creation, modification and deletion of virtual machines, self-provisioning, and automation of tasks between the virtual infrastructure and other cyber range components or other systems interfacing with the cyber range.

Orchestration falls under the technology section of a cyber range and would be transparent to an end user accessing a cyber range. However, the use of an orchestrator can greatly affect the usability and cost of using a cyber range as well as the support for specific use cases. A cyber range with orchestration capabilities can support additional functionalities, which would otherwise require additional manual effort and coordination and hence additional costs for the cyber range users.

At its most fundamental level, orchestration includes the orchestration of the virtual environment. At its finest, orchestration may also be used to automate tasks and interactions across different components of the cyber range such as the ability to schedule attacks and user simulation, events injection to initiate the

collection of user activities and more, depending on the specific use cases.

Hence, orchestration is a mandatory component in the architecture.

5.2.2 Internet Services Simulation

Simulation of Internet Services is a broad term to describe any service outside the main simulated environment upon which the simulated environment itself depends for the realization of a specific use case. Under this category, we find the simulation of social media platforms such as Facebook, LinkedIn, Twitter, app stores, internet routing protocols and different tiers of service providers, controlled update and software repositories for various operating systems, global services such as name resolution, PKI, Pretty Good Privacy (PGP), public news sites and discussion forums.

Simulation on Internet Services adds the realism of scenarios being implemented by the cyber range. Modern attacks utilize global infrastructure and services considerably in order to avoid detection. Therefore, it is very important for cyber ranges to be able to simulate the Internet and its services realistically. However, in many cases, Internet services are not simulated due to the added complexity required to guarantee the right level of realism.

In Cyber Range implementation, we expect the cyber range to have this good-to-have component.

5.2.3 Attack Simulation

Attack simulation refers to the ability to simulate attacks within and to the cyber range simulated environment [13] and it falls under what is currently known as Breach and Attack Simulation (BAS). While traditional vulnerability scanning technology focuses on the identification of systems, networks, and application vulnerabilities, attack simulation goes the extra mile by allowing to simulate the different phases of the security kill-chain while at the same time providing recommendations on how to secure the organization.

In Cyber Range implementation, the cyber range attack simulation is recommended to focus more on the MITRE ATT&CK™ knowledge base of adversary tactics and techniques, than the traditional security kill chain model [14]. Desirable features regarding the attack simulation are the availability of an attack library, containing a list of pre-defined attacks, and the ability to import/create custom attacks.

5.2.4 User Activity Simulation

User simulation refers to the ability to simulate the presence and behavior of benign users in the cyber range environment. While the technology, tools and methods used may be similar to what is used to simulate attacks, user activity simulation is required for specific scenarios depicting real environments. Besides the actual simulation of systems and applications, user activity simulation is very important as it makes the simulated environment much more realistic. User simulation may refer to both internal users and fictitious client users of the simulated environment. For instance, if the simulated environment is a banking corporate network, user simulation may refer to the simulation of the fictitious banking organization's members of staff and to the simulation of the clients of the fictitious bank logging in to the online banking website.

Examples of user activity simulation include:

- User Internet browsing activity
- Users watching YouTube videos
- Users using P2P file sharing applications to download files
- Users sending emails
- Users interacting with cloud services such as Office 365, Dropbox etc.

In Cyber Range implementation, the desirable features for user simulation are the availability of a simulation library, containing a list of pre-defined user simulations, and the ability to import/create custom simulations.

5.2.5 Scenarios and Content Development

The usefulness of a cyber range is ultimately highly correlated to how the cyber range is used, which in turn is correlated to the scenarios the cyber range can be used to deliver. That is somewhat comparable to the experience of using a computer gaming console which is related to the number of available games and the number of third parties developing games for the console. In relation to cyber ranges, the game is represented by the scenario, and the ability to support the development of scenarios by third parties, or by the users themselves, greatly enhances the usefulness and value added of the cyber range.

In Cyber Range implementation, cyber range must include the ability to create basic simulation scenarios/ environments up to full scale custom simulation of attacks and other services.

5.2.6 Competency Management

A competence is a set of attributes such as knowledge, skills and abilities required to successfully perform specific tasks. For a long time, organizations have been using ISO17024 to certify job profiles through the execution of job task analysis which would identify the competences associated to a specific job in relation to the job-specific tasks. More recently, work has been done at national and international level to define competence frameworks which include comprehensive taxonomies of competences and models to define new job profiles or roles. Some frameworks also sample job profiles, demonstrating how the framework can be applied. Notable competence frameworks include the NIST NICE Framework [15] and the European e-Competence Framework (eCF) [16].

Competency (or competence) management systems (CMS) are systems which allow an organization to manage a competence program from skills gap analysis and user profiling up to the definition of learning paths and competence assessment.

CyberSecurity Malaysia has created Global ACE Certification Framework based on ISO 17024 standard for Competency Management. Cyber Range implementation will align to Global ACE Certification Framework together with NICE Framework and MITRE ATT&CK Framework.

5.2.7 Data Collection and Analysis

Data collection refers to the capability of the cyber range to collect users' interaction with the cyber range such as traffic generated, memory dumps, tools used, systems targeted etc. This capability may depend on the cyber range's core technologies and how the simulation environment is created.

Data analysis refers to the capability of the cyber range to more easily allow the analysis of the collected data to learn about how the cyber range is used, how users perform etc. In this regard, data analysis of both automatically collected data and of the output of user activities underpins the ability to provide meaningful feedback to the cyber range users. In addition, cyber range must have full capability of Artificial Intelligence (AI) driven data collection and analysis to provide recommendation and feedback of the cyber range users' learning and performance.

5.2.8 Scoring and Reporting

Scoring provides out of band capability to allow users of a cyber range to be scored based on their activities and interaction with the cyber range. Scoring systems can be as simple as collecting user input to questions and tasks, up to more complex functionalities such as the ability to monitor the progression of user activities and to show a timeline of individual and team performance, while emphasizing the different roles in a team.

The reporting side include a list of standard reports (e.g. per user or per team playing the scenarios) and the ability to create new custom reports that an organization can use to better visualize its cyber resilience or performance over time, etc. Reporting must also include real-time cyber situational awareness to allow to clearly visualize the use of the cyber range, the impact of tools used, and action taken by the cyber range users (especially in the context of a cyber exercise).

5.2.9 Instructor Tools

Instructor tools refer to the capabilities desired and/or required by an instructor using the cyber range for either educational and/or training purposes. Instructor tools should support the evaluation of users and their action. These data are crucial for providing feedback and evaluating objectives and goals during CDX and CTF.

Sample functionalities include:

- Communication facilities (e.g. chat, event broadcasting etc.)
- Instructor mode functionality to show sample answers
- Ability to control the workflow of the scenario (stop, pause, interrupt the execution of the scenario)
- Ability to record and replay users' screen session
- Ability to record and review users' actions (e.g. commands executed)
- Ability to analyze recorded users' actions and other collected data
- Ability to carry out user evaluation
- Ability to deliver user evaluation and feedback, and associated reports

5.3 Cyber Range Functionalities & Use Case Mapping

The following table compares cyber range functionalities to the different use cases. Each cyber range capability is marked as (“D”) Desirable. It is important to highlight that a cyber range, regardless of the offered functionalities, could potentially be used for a wide range of different use cases.

Functionality	Cyber Range Use Cases									
	Security Testing	Security Research	Competence Building	Security Education	Development of Cyber Capabilities	Development of Cyber Resilience	Competence Assessment	Recruitment	Digital Dexterity	National Cyber Security Competitions
Orchestration			D	D	D	D	D	D	D	D
Internet Services Simulation						D			D	
Attack Simulation	D	D	D	D	D	D	D	D		D
User Activity Simulation		D	D	D	D	D	D	D	D	D
Competency Management			D	D	D	D	D	D	D	D
Scenarios and Content Development			D	D	D	D	D	D		D
Data Collection and Analysis		D	D	D	D	D	D	D		D
Scoring and Reporting			D	D	D	D	D	D		D
Instructor Tools			D	D	D	D	D	D		D

Table 1 : Cyber Range Functionalities vs Use Cases

5.4 Delivery Models

Cyber ranges can be broadly accessed in one of two possible ways, which are:

1. Cyber Range as a Service
2. On-Premise Cyber Range

5.4.1 Cyber Range as a Service

In this model, the cyber range is owned and managed by a cyber range provider who makes it available to third parties with charging models based on the cyber range provider, the specific functionalities, capabilities and, ultimately, the services offered. Two main types of cyber range as a service exist:

- **Online:** In this case, the cyber range is accessed remotely by the client and is most likely deployed on the Cloud using virtualization technologies.
- **Physical:** In this case, the cyber range is hosted at a physical location that the client needs to visit to use it. The cyber range will usually provide physical training facilities, break out rooms, and debriefing rooms, which constitute part of the service offering.

5.4.2 On-Premise Cyber Range

An on-premises cyber range is physically deployed at an organization. This is usually the most expensive cyber range option as it requires a larger upfront capital investment associated to the cyber range hardware and software. While on-premises deployment is more expensive, it is better suited to meet the security requirements of an organization which can better exercise control over the data associated to the use of the cyber range.

5.5 International Frameworks

Cyber range is designed to be utilized by different users with different roles. Usually, a cyber range has three leading roles.

- **White Team:** created for instructors, moderators, and administrators; it allows content management, designing, managing, and scenario configuration to prepare offensive operations and defensive operations and to evaluate the participants and the teams.
- **Red Team:** members of the red team play the role of attacker, pentesters, security consultants, and ethical hackers that want to train their attack techniques.
- **Blue Team:** it plays the role of a defensive team member such as an organization's security team, internal or outsourced SOC team - that allows improving and learning about attack techniques that are being used by hackers to improve their defensive capacity and sharpen their incident response skills.

Although there is no formal framework for the development of Cyber Range scenarios, we can use, implement, and rely on recognized frameworks such as MITRE or NIST NICE.

These frameworks allow the development of the challenges and training scenarios of a Cyber Range. The use cases, based on an impact point of view, should be balanced between defensive technology versus cyber-attacks, depending on if they are used and implemented in a corporate or a government environment.

The process and design of the use cases and challenges are based on different approaches maintaining the following priorities:

- Develop and expand cybersecurity skills
- Measure knowledge and capabilities of cybersecurity teams
- Raise awareness on companies and C-Suite executives
- Improve overall cybersecurity education

A cyber range should be designed to implement challenges with the objective that the participants can develop, improve their capabilities, develop their skills, or build new ones based on experiences acquired on their own cyber security experiences.

5.5.1 NIST NICE Framework

National Initiative for Cybersecurity Education (NICE)[15] is a partnership between government, academia, and the private sector to address cybersecurity education, like Malaysia’s very own Global ACE Certification Scheme. NICE is led by the National Institute of Standards and Technology (NIST).

In May 2019, the President of the United States signed an Executive Order to grow America’s cybersecurity workforce and strengthen the nation’s cybersecurity. This encourages widespread adoption of this framework.

The NICE Framework is a common taxonomy and lexicon that categorizes and describes cybersecurity work and workers regardless of organization or industry. This national resource aims to standardize cybersecurity workforce definitions across the public, private, and academic sectors so that the entire cybersecurity industry speaks a common language and shares common goals.

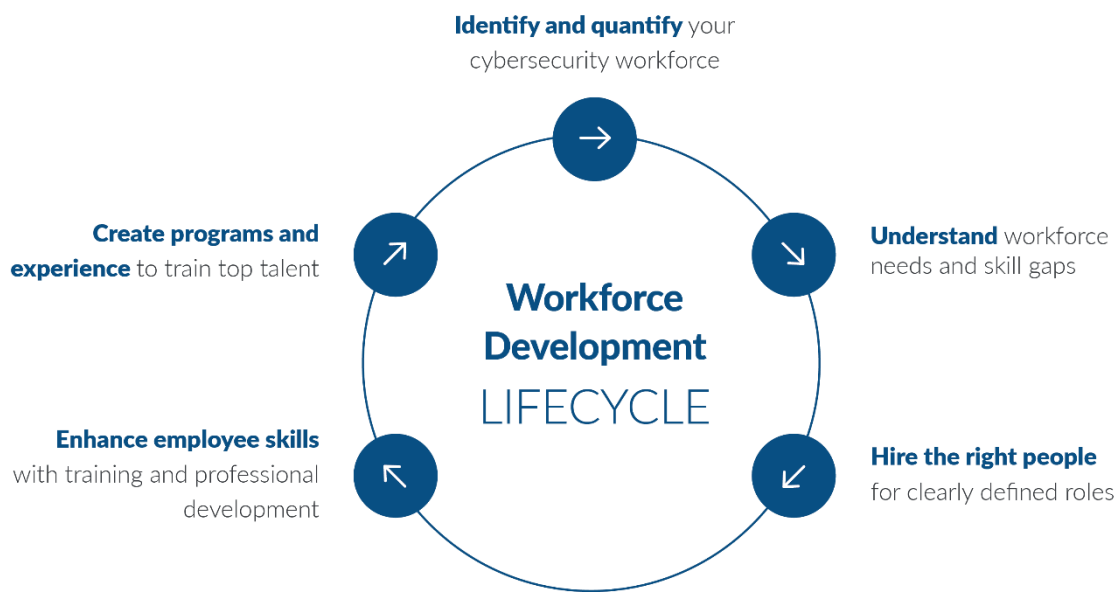


Diagram 3: Workforce Development Lifecycle

The NICE Framework includes the following components:



7 Categories defining high-level cybersecurity functions.



33 Specialty Areas defining distinct areas of cybersecurity work.



52 Work Roles defining detailed groupings of cybersecurity work comprised of specific knowledge, skills, and abilities (KSA) required to perform tasks in a work role.

NICE Framework Components and Relationships	
Categories	Categories provide the overarching organizational structure of the NICE Framework. There are seven categories, and all are composed of Specialty Areas and work roles.
Specialty Areas	Each specialty area represents an area of concentrated work, or function, within cybersecurity and related work.
Work Roles	Work roles are the most detailed groupings of cybersecurity and related work, which include a list of attributes required to perform that role in the form of knowledge, skills, and abilities (KSAs) and tasks performed in that role.
Knowledge, Skills, and Abilities (KSAs)	KSAs are the attributes required to perform work roles and are generally demonstrated through relevant experience, education, or training.

Source: NIST Special Publication 800-181

Table 2: NICE Framework Components

Why Map Training and Education Programs to NICE Framework?

For Educators

Ensuring students are armed with the required knowledge for them to be successful in their careers is one of the key values in the education system. The NICE Framework is a reference to develop curriculum, courses, seminars, and research that cover the KSAs for students to select roles that they want to be in their future career in cybersecurity. For example: for a student to be a successful Tier-2 SOC analyst, the NICE Framework details exactly which skills they will need to have to fill this role. This will make it easier for educators to build out curriculum, classwork, and home assignments to provide the information that students need for future success.

For SOC managers and CISOs

Preventing a critical attack is one of the primary responsibilities of any SOC. It is imperative that your team possess the required skills to prevent this attack. Given that most SOC Managers or CISOs believe their team to be under skilled and under qualified to prevent a critical attack, having a framework in place provides a road map to skill training and qualification. By using the NICE Cybersecurity Framework, SOC managers can detail exactly which role the members of the team are taking, which skills are required for the assigned role, and what training needs to take place for them to be successful.

For Recruiters and HR Managers

It is becoming increasingly difficult and competitive to hire qualified candidates to work on the cybersecurity team. Aligning with NICE KSAs allows HR managers to compare candidates more easily from diverse backgrounds. This will allow an additional tool in the arsenal with the ability to run prospective candidates through exercises that will test if they have the required skills to fill the specified role. Using NICE Work Roles and Skills will also help recruiters to determine accurate and applicable training programs, leading to better qualified employees and higher employee retention.

5.5.2 MITRE ATT&CK Framework

When an organization is breached, attackers will remain on networks for weeks/months before being detected. Once the attacker has been detected, there are a myriad of questions to answer:

- How did the attacker enter the network?
- How is the attacker moving around on the network?
- What action is the attacker taking while on the network?

For an experienced professional, many of the questions are second nature. However, mapping your training to the MITRE ATT&CK (Adversarial Tactics, Techniques, & Common Knowledge) Framework [14] ensures that not only are these questions asked; they are answered as well.

MITRE's ATT&CK Framework is defined as globally accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community. This framework describes how attackers penetrate networks and then move laterally, escalate privileges, create a persistent state, or generally evade your defenses. ATT&CK looks at the "problem" from the perspective of the attacker, helping cybersecurity professionals determine what goals the attacker is aiming to achieve and what methods the attacker will use to achieve their goals. The Framework organizes attacker behaviors into a series of tactics, specific technical objectives that an attacker wants to achieve. For example, an attacker may perform lateral movement to move to a different part of the network where the specific data they are looking for is waiting to be exfiltrated.

Within each tactic category ATT&CK defines a series of techniques. Each technique describes one way an attacker may attempt to achieve their objective. Each tactic contains multiple techniques because different attackers may deploy different attack methodologies based on their own knowledge or circumstance (availability of tools, system configuration, etc.). Each technique defined in ATT&CK includes a description of the method deployed by the attacker, the systems, or platforms the methodologies apply to, and, where known, which attackers or attack groups have been associated with the defined technique. Techniques also provide the process by which the SOC team can mitigate attacker behavior along with any published references to the technique being deployed.

Another important use of ATT&CK is to help you learn how to detect an attacker's actions on your network. The ATT&CK Framework includes resources that are purpose built to help you develop analytics that detect the techniques used by attackers as they attempt to breach, explore, and exfiltrate data from your databases. ATT&CK will also provide information on hacking collectives or groups and the campaigns they've conducted, allowing you to be as prepared as possible for a future attack.

ATT&CK helps you understand how attackers might operate so that you can plan and build response playbooks to mitigate attacker incidents. Armed with this knowledge and "attack playbooks" you are now better prepared to understand how your adversaries prepare for, launches, and execute their attacks to achieve specific desired objectives.

ATT&CK Enterprise and PRE-ATT&CK combine to form the full list of tactics that align with the [Cyber Kill Chain](#). While PRE-ATT&CK mostly aligns with the first three phases the Cyber Kill Chain, ATT&CK Enterprise aligns with the final four phases.



The Enterprise Matrix included in the ATT&CK Framework consists of 12 tactics that attackers may use to breach and exfiltrate data from your network. The Matrix includes techniques spanning Windows, macOS, Linux, AWS, GCP, Azure, Azure AD, Office365 and SaaS tools. You can use the [MITRE ATT&CK Navigator](#) to filter through the different tactics and their assigned MITRE ATT&CK Techniques. This framework is on the MITRE Git and makes navigating attack techniques significantly easier.

Why Map Training and Education Programs to MITRE ATT&CK Framework?

For Educators

Ensuring students are armed with the “attacker playbook” will ensure their success while working in a SOC. MITRE ATT&CK is a valuable reference tool to develop curriculums, coursework, seminars, and research of different combinations of attack techniques. Knowledge of attacker behavior is vital to the success of students who plan to have a bright future in cybersecurity. For example: if a student is knowledgeable enough to understand that attackers who use certain entry techniques will usually also perform lateral movement as their next step and be familiar with the different techniques that can be used by attackers to achieve this goal, they can mitigate the lateral movement, and thus the attack itself. Taking the next step and allowing students to experience the technique on a cyber range will give them the experience to identify the technique in the real-world, giving students a leg up on the malicious actor.

For SOC Managers and CISOs

Preventing a critical attack is one of the primary responsibilities of any SOC. Critical to achieving this goal is advance knowledge of how your attacker will behave when attempting or after they successfully breach a network. Since a lack of skilled staff is the top issue facing a SOC for the past two years (SANS SOC Survey 2019), arming your team with the knowledge of attacker behavior and allowing them to train against these known behaviors gives your SOC team an advantage when attempting to expel and lock out an attacker from your network. Building your training plan with MITRE ATT&CK at the forefront ensures that you can expose your team to many of the techniques outlined in ATT&CK, ensuring true preparation in the face of any attack. Training your team on a cyber range allows them to mitigate the techniques being used, ensuring that your team will be able to perform when they see a malicious attacker on the network they’ve been tasked with protecting.

For Recruiters and HR Managers

It is becoming increasingly difficult and competitive to hire candidates who are truly qualified to be a member of the SOC team in your organization. Recruiters can refer to the MITRE ATT&CK knowledge base to effectively assess pentester job applicants on the skills that they may claim to have. Additionally, blue team members should also have intimate knowledge of MITRE ATT&CK to ensure they know how attacker behave. Possessing this knowledge will allow potential job candidates to perform more effectively and efficiently in their role. Testing incoming blue and red Team members on a cyber range against live attacks can provide evidence to their knowledge of MITRE ATT&CK and prove their strategic ability to mitigate incidents while they are occurring on a network.

5.5.3 Global ACE Certification Scheme

The Global ACE Certification Scheme is a holistic framework of cybersecurity professional certification that outlines the overall approach, independent assessments, impartiality of examinations, competencies of trainers, identification and classification of cyber security domains and the requirements of professional memberships. The scheme is a large-scale systematic plan of actions to certify and recognise the cybersecurity workforce. It is industry driven and vendor-neutral, developed in collaboration with government agencies, industry partners and academia.

The establishment of the scheme is in tandem with international standards such as ISO 9001 on processes, ISO/IEC 17024 on certification of persons and ISO/IEC 27001 on security management, which is vital to:

- Assure workforce capability and experience
- Secure and validate core skills, knowledge, attitude and experience
- Assure trustworthiness, ethical conduct, and responsibility

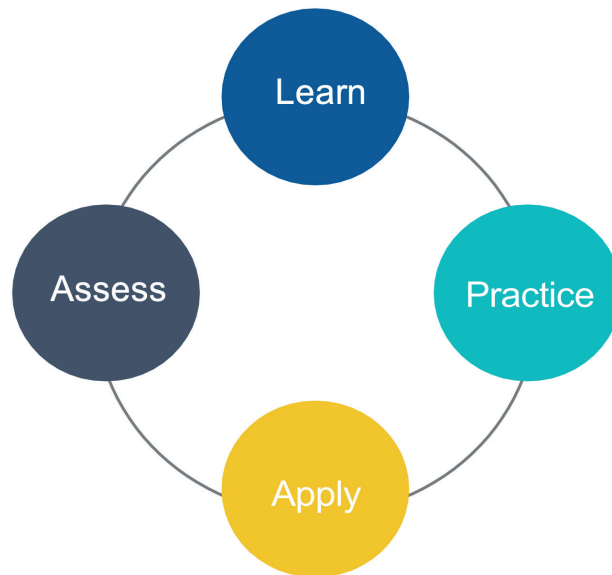
The Global ACE Certification aims to enhance the skill sets of the cybersecurity workforce congruent with local and international requirements. The Global ACE Certification Recognition Arrangement permits mutual recognition of certified cybersecurity workforce across the country boundaries. It creates value for the cybersecurity industry and elevates the security-facet of participating countries.

The heart of the Global ACE Certification is the framework that provides a standard base and means of acknowledging the “knowledge, skills and attitudes” for the workforce in the cyber security sector. The framework will be the base for impartial examinations and guideline for certifications. The framework encompasses two broad categories of domains as below:



6. GLOBAL ACE CERTIFICATION CYBER RANGE FRAMEWORK

In a normal learning cycle for technical skills there are four steps that work together to build long lasting skills. Each stage of the learning cycle focuses on a different area of knowledge and learning ensuring that your cybersecurity professionals have the building blocks, foundation, and skills to be successful



Learn: Ensure cybersecurity professional has a strong base in cybersecurity theory, attacker tactics, and theoretical mitigation techniques. Understand why attackers behave the way they do, how they achieve their goals, and how incidents can be resolved on a theoretical level.

Practice: Combine theoretical knowledge with hands on skills in a smaller environment, focusing on effectively building cybersecurity skills in small environments to ensure the appropriate skill can be applied when required

Apply: Combine theory and practice in a complete, end to end, cyberattack simulation to create muscle-memory like responses to cybersecurity incidents. Cybersecurity professionals need to map their newly learned skills together to complete entire incident response playbooks, effectively reinforcing their cybersecurity skills and building critical soft skills.

Assess: Actionable feedback is key in the development of cybersecurity skills. With a rapidly evolving attacker landscape, cybersecurity professionals need to receive feedback to help them to better apply their knowledge and skills in a real-world environment. Additionally, actionable and constructive feedback helps cybersecurity professionals address key gaps in their skills and knowledge, ensuring that which training comes next is apparent to all involved.

Global ACE Certification Cyber Range framework is built on these basics to build cybersecurity skills that are actionable and immediately applicable in the real-world scenarios where Mean Time To Detect (MTTD) and Mean Time To Respond (MTTR) is a paramount metric in saving an organization from a breach or a ransomware.

A cyber range platform complying to Global ACE Certification Cyber Range framework must provide all the following four elements for an effective cybersecurity skill building program that last for a lifetime, reducing time to response, reducing onboarding time, and helping to solve the growing global cybersecurity skills shortage:

1. Build Foundational Elements of Cybersecurity with Theoretical Labs

Providing the foundation for all cybersecurity skills, theoretical knowledge is key to understanding how to effectively mitigate an incident. Having a strong foundation will also arm cybersecurity professionals with the knowledge to identify unknown attacks, identify attacker objectives, and mitigate incidents prior to critical damage. Conversely, without a strong base in cybersecurity theory, a cybersecurity professional will have major gaps in their knowledge, significantly hindering their ability to perform at critical times.

A cyber range platform complying to Global ACE Certification Cyber Range framework must provide a wide variety of theoretical labs, ensuring that cybersecurity professionals possess the base knowledge to be successful in their roles.

2. Transform Knowledge into Skill with Practical Labs

To be a contributing member of a security operations center (SOC) team, cybersecurity professionals must possess the required skills for their work role. For example, without skill in remote command line and Graphic User Interface (GUI) tool usage, detecting a fileless attack like NotPetya would be significantly more challenging, leading to a decrease in time to detection and increased cybercrime costs for an organization.

A cyber range platform complying to Global ACE Certification Cyber Range framework must include smaller environments where cybersecurity professionals can practice individual skills, perfecting them in isolation before applying them in a real- world environment

3. Apply Knowledge and Skills in Real World Attack Scenarios

To be truly successful as a contributing member of a SOC team, cybersecurity professionals must be able to turn their knowledge and isolated skills into a complete skillset, mapping multiple technical skills together along with their teammates to mitigate incidents. Additionally, for a team member to be truly effective, they must possess the soft skills to work as a team, ensuring they perform their required tasks in a timely manner, effectively communicating forensic evidence to team members, and building the emotional IQ to realize that a teammate is in distress. Building both technical skills and soft skills together ensures that a team has the experience required to be successful when an attack occurs in the real world.

A cyber range platform complying to Global ACE Cyber Range framework must include complete attack scenarios across the entire cyber-attack lifecycle to provide trainees with the environment to map together the knowledge and skills built in earlier training. Complete attack scenarios induce the stress associated with a real attack, providing a real-world experience that ensures cybersecurity professionals are prepared to mitigate any incident that comes their way. Like the real world, trainees will have to mitigate incidents according to the NIST Incident Response Framework, ensuring that the team is training, as well as acting, according to industry standards.

4. Provide Actionable Feedback to Optimize Skills Development

To ensure that a team improves, the platform must provide constructive feedback. Let them know where they have missed important steps in attack mitigation, where they can improve their intra-team communication, and where they are lacking the required knowledge to build a skill. Using the information relayed during a training session, next training steps become clear. If a member of the team displays a missing skill or a lack of theoretical knowledge in a specific area, the platform must assign them to the related theoretical or practical exercise to ensure they build their missing foundation, better preparing them for the real-world scenarios.

A cyber range platform complying to Global ACE Cyber Range framework must include a complete debriefing suite, providing critical feedback to trainees and must include a dashboard with goals and milestones achieved based on the NIST Incident Response Framework, Time to Response measurement, where trainees required hints, and how they performed in post exercise quizzes. Each point of measured data included in the debriefing suite must correlate allowing the team to focus training on problem areas and transforming the aforementioned areas into strengths.

5. Align Cybersecurity Training with Global ACE Certification KSAs

A cyber range platform complying to Global ACE Cyber Range framework must map its components/functions/features to Global ACE KSAs to ensure that cybersecurity professionals are training to the highest standard. Global ACE KSAs perfectly align with the learning cycle since KSAs are aligned to a building blocks methodology. Knowledge equals theoretical cybersecurity knowledge, ensuring that cybersecurity professionals have the required knowledge for their required role. Skills align to practice, ensuring that individual skills are built to perfection in isolation, without the stress of an ongoing attack. Abilities are the combination of theoretical knowledge and practical skills ensuring that cybersecurity professionals can handle the continued evolution of cybersecurity incidents across the kill chain. In this way, the learning cycle, Global ACE KSAs, and the Cyber Range platform are all focused on the same learning path, educational theory, and all working towards the same goal of solving the global cybersecurity skills shortage with effective cybersecurity education.

6.1 Global ACE – NICE Cyber Range Framework Mapping

Since industries worldwide are still in the process of aligning its terminologies and training programs with NICE Work Roles, the job titles we will find in security organizations and on job seeking boards will often not correlate with NICE Work Roles. For example, the conventional job title of a Tier-1 analyst would be aligned with the NICE Work Role of a Cyber Defense Analyst. To complicate things further NICE roles may overlap across conventional titles. For example, what we call a Tier-2 Analyst would need to have the combined skills of a NICE Cyber Defense Analyst and of a NICE Cyber Defense Incident Responder. When mapping training programs and definitions to the NICE Framework it is important to understand how the job titles map to NICE work roles.

Global ACE Certification Cyber Range Framework acknowledges that to develop skills across multiple roles require more intense training because there are more skills required. While certain skills do reach across multiple roles, the sheer number of non-concurrent skills required across several roles means that training must be more intense, in-depth, and simulation oriented.

There are certain job titles in a SOC that do not fall under one specific role or do not have a perfect alignment to a specific role. Thus, Global ACE Certification Cyber Range Framework have identified relevant skills from different roles and put them together to fit a current job in a cyber security red team to ensure relevant training that maps to Global ACE KSAs as well as NICE KSAs.

Example of a Global ACE Certification Cyber Range Course with NICE KSA mapping:

Global ACE Certified Red Team Professional

<p>NICE Category:</p> <ul style="list-style-type: none"> • Protect & Defend • Analyze 	<p>NICE Specialty Areas:</p> <ul style="list-style-type: none"> • Cyber Defense Analysis, • Exploitation Analysis, • Incident Response, and 	<p>NICE Work Roles:</p> <ul style="list-style-type: none"> • Cyber Defense Analyst/Tier 1 Analyst • Exploitation Analyst • Cyber Defense Incident Responder/Tier 2 Analyst
--	---	--

Global ACE Certified Blue Team Professional

<p>NICE Category:</p> <ul style="list-style-type: none"> • Collect & Operate • Analyze • Investigate 	<p>NICE Specialty Areas:</p> <ul style="list-style-type: none"> • Cyber Operations, • Threat Analysis, • Cyber Investigations, and • Digital Forensics. 	<p>NICE Work Roles:</p> <ul style="list-style-type: none"> • Cyber Defense Operator • Threat Analyst • Cyber Crime Investigator • Cyber Defense Forensics Analyst
--	--	--

6.2 Global ACE – MITRE ATT&CK Framework Cyber Range Mapping

Global ACE Cyber Range Courses and all scenarios included within the course must be mapped to the techniques and methodologies used by attackers as set out by MITRE ATT&CK. This will allow trainees to break down the cyber range exercises, in real time, to the different techniques and methodologies outlined by ATT&CK, ensuring that the attendees will be prepared for the inevitable attack when it happens.

Sample Attack Scenario mapped to MITRE ATT&CK: Dragonfly

Today, more than ever, the human factor is the focus of attacks over the internet - targeting users as the weakest link in the security chain. In this attack scenario, a seemingly innocent email can be the source of a sophisticated cyber-attack. While closely monitoring the attacker’s steps, trainees will get a close look at different attack techniques for lateral movement, privilege escalation and data exfiltration using web vulnerability.

MITRE Techniques in Scenario:

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Lateral Movement	Collection	Command and Control
Spear phishing Link (T1192)	Command-Line Interface (T1059)	Hidden Files and Directories (T1158)	Web Shell (T1100)	Hidden Files and Directories (T1158)	Exploitation of Remote Services (T1210)	Data from Local System (T1005)	Fallback Channels (T1008)
	Exploitation for Client Execution (T1203)	Redundant Access (T1108)		Redundant Access (T1108)		Data Staged (T1074)	Web Service (T1102)
	PowerShell (T1086)	Web Shell (T1100)		Scripting (T1064)		Screen Capture (T1113)	
	Scripting (T1064)			Template Injection (T1221)			
	User Execution (T1204)			Web Service (T1102)			

6.3 Cloud Cyber Range Functional and Technical Requirement

#	Requirements
A	High Level Requirements
A-1	The system will simulate networks, traffic and attack scenarios, to train and test trainees, security practitioners, procedures and technologies in a safe and controllable environment.
A-2	The system training environment will be available as a SaaS hosted on a public cloud and will not require any on-site installation of hardware or software to operate.
A-3	The system training environment is automatically reverted to default "clean" state prior to a new training session.
A-4	The system will provide a realistic cyber training and simulation platform.
A-5	The system will provide a rich and diverse virtual network, with leading commercial security tools, which emulates a corporate network.
A-6	The system will provide a virtualization and emulation of network devices and protocols, including: <ul style="list-style-type: none"> • Security components • Network appliances • Servers and applications • User computer endpoints
A-7	The system will include a catalogue of pre-scripted, out-of-the-box, IT attack scenarios. Part of the scenarios shall be for individuals and adapt micro out-of-the-box networks, and some of scenarios shall adapt team training running on a full network.

A-8 The system will include a catalogue of pre-scripted, out-of-the-box, Pen-testing/Red scenarios.

B Virtual Network

B-1 The system will include multiple segments of IP subnets, VLANS, and a DMZ - in order to realistically represent an operational corporate network.

B-2 The system will include a perimeter firewall and an internal firewall. Fully operational and licensed (not open source/community edition).

B-3 The system will include a server to monitor the status of server services of all servers

B-4 The system will include a commercially licensed SIEM (Security Information and Event Management) product. The SIEM included in the system will not be open source/community edition, but a commercial product, to emulate a real-life SOC environment.

B-5 The SIEM will be pre-configured to include rule sets that will support the attack scenarios, so that SIEM alerts will be triggered according to the training scenario.

B-6 The system will include a mail relay server.

B-7 The system will include a Domain Controller server.

B-8 The system will include a DHCP server.

B-9 The system will include a server segment including SQL, DC, DHCP, File server etc.

B-10 The system will include a User segment, and will include workstations running Ubuntu OS, and Windows OS.

B-11 The system will include a Web segment including an FTP application server, an Apache web server and a Microsoft Internet Information Services (IIS) web server.

B-12 The system will include a VPN Segment. Trainee stations will connect to the training network by means of the VPN Server residing in this segment.

B-13 The system will support remote training by means of a browser-based application, without having to install a client on the trainee machine.

B-14 The system will include an ISP Segment to simulate an internet network, and will include Domain Naming Services (DNS), IIS Web Server and WebMail - SendMail-based mail server.

B-15 The system will include VLAN and IP segmentation of the various segments (e.g. Users segment, SIEM segment, ISP, VPN, SCADA etc.) in order to maintain a network structure resembling a real-life corporate network.

B-18 The out of the box networks shall include "detectors" which detect the trainee's activity and impact the final score.

C Traffic Generator

C-1 The system will include a traffic generator that will simulate real-life, benign traffic, to maximize the effectiveness of the training sessions. The traffic generator will simulate traffic in multiple protocols including IP, HTTP, SMTP, POP, FTP, and ICMP.

C-2 The system will allow to configure the source and destination of the traffic generated by the traffic generator.

C-3 The system will allow to configure the traffic type and protocol of the traffic generated by the traffic generator.

C-4 The system will allow to configure the duration of the traffic generated by the traffic generator.

C-5 The system will allow to configure the amount of network traffic generated by the traffic generator, by allowing the creation of flow groups.

D Attack Generator

D-1 The system will include an attack generator that will simulate cyber-attack scenarios.

D-2 The attack generator will simulate attack scenarios and will inject malware into the simulated network, originated in various network segments, according to the attack scenario configuration. Attack origins may be:

- External – simulating an external threat.
- Internal – simulating user misconfigurations, user errors, or malicious insiders.

E Trainer Management Console

E-18 The Trainer Management Console will provide a view of the training network info via the trainer and trainee interface (in a format such as JPEG, CSV etc.)

E-19 The Trainer Management Console will display a session timeline, displaying attack progress, milestones, and session events including milestones achieved and notes.

E-20 The Trainer Management Console timeline will monitor and display SIEM events.

E-21	The Trainer Management Console timeline will provide a summary of all the training events at the timeline.
E-22	The Trainer Management Console will allow the trainer to add textual comments which will appear on the timeline.
E-24	The Trainer Management Console will provide the option to zoom into the trainee's screen during the session and will allow zooming to full screen size for improved viewing quality.
E-26	The Trainer Management Console will provide an option to view the timeline progress as absolute or relative, during a training.
E-33	The trainer can configure the training to run in self training mode. This mode means that the trainees can start the training by themselves.
F	Trainee Interface
F-1	Trainees can train over commercial, best of breed security tools, investigation and monitoring tools including: SIEM, Firewall, station logs, server logs, Zenoss, Putty, and Wireshark for investigation. The system should include best of breed security products including QRadar SIEM, Palo Alto Network Security, Splunk and more.
F-3	The trainee interface will display session time progression and score as an overlay without interfering with security product UI.
F-5	The trainee interface will provide an RDP connection to all Windows machines in the network.
F-6	The trainee interface will include an interactive investigation tool for the trainees, where they can capture their insights and evidence for the investigated attack scenario.
F-7	The investigation tool on the trainees' interface provides an indication whether the evidences added by the trainee during the training are correct or not, so the trainee can use it for learning, fix it, and get real-time feedback. This tool is helpful for self-learning and deep understanding.
F-8	The trainee interface will include a quiz, that aims to test and verify the trainee's understanding.
F-9	The trainees will be able to initialize the network and start the training session by themselves.
F-10	The trainee will be able to request hints in case of self-training. The hints shall help the trainee to solve the training.
F-11	The trainee will be able to open a full solution of the scenario in case of self-training.

F-12	The trainee interface will include an on-boarding process to guide the trainee on how to use the system.
F-13	The trainee interface will provide introduction videos for the main tools available on the network.
F-14	The trainee interface will show the result of the training at the end, when running in training mode.
G	Attack Scenarios
G-1	The system will include an attack generator that will simulate pre-scripted attack scenarios. The system will not require human resources or red teams to operate and run the attacks, ensuring the attacks are consistent and repeatable, and minimizing the need for additional resources.
G-2	The system will provide a catalogue of IT attacks.
G-3	The system will provide a scenario market-place on the web, allowing users to filter scenarios based on different criteria, like: NICE roles, firewall vendor, SIEM vendor, duration, etc.
G-4	The system will support varying levels of scenario difficulty and complexity.
G-5	The simulated attack scenarios will include a wide set of attack vectors including Web, Email, infected CD, FTP, and VPN.
G-6	The system will simulate multiple exploit scenarios such as: data theft, web crawling, SQL injection, port scanning, ping sweep, password brute force, backdoor scripting, website spoofing, spear phishing, SSH protocol fuzzing, and DNS poisoning.
G-8	The system will provide attack scenarios with high tangible impact on the network including Denial of Service (DOS), information theft, and website defacement,
G-9	The system will provide attack scenarios utilizing Linux logs, Windows PC and server logs, SIEM logs, firewall logs, Zenoss logs, mail relay logs, reverse engineering and web and networking forensics, MSSQL server logs, SCADA IDS logs, network forensics, VPN log forensics
G-11	The system will provide a module for customization of attacks - Setting security tools alerts to silent or active, to impact diagnostics difficulty.
G-12	The system will provide a module for customization of attacks - Deleting logs created during the attack, to impact diagnostics difficulty.

G-13	The system will provide a module for customization of attacks - Control the scenario running speed (slow, medium, fast).
G-14	The system will provide a module for customization of attacks - Change attacker IP address between actions.
G-15	The system will provide a module for customization of attacks - Adding customized scripts and integrating user-created scripts to propagate specialized attacks into the scenario attack flow.
G-20	The system shall provide individual content including scenarios and networks, focused on specific discipline such as Malware analysis, advanced incident response, specific product practice, etc.
G-21	The system shall include dedicated scenarios for pen-testers/ethical-hackers. The scenarios include a network and a "Flag" the trainees have to achieve during the training. The trainee can use Kali Linux to execute the attack.
G-22	The system will provide all attack scenarios mapped to MITRE ATT&CK Framework
H	Automatic scoring and evaluation
H-2	The out-of-the-box networks shall include "detectors" which detect the trainee's activity and affect the training score.
H-3	Correct answers to scenario quiz questions shall affect the total score of the training.
H-4	The trainer can configure the training to run in "test mode", which means that the trainees will not see scores nor feedback in their application during the training. They will not be able to get hints or see the full solution. This mode is useful for certifications.
H-6	The system will provide the ability to export the training results to a PDF report for each trainee.
I	Deliverables and Services
I-12	The system will be provided with written material describing the scenarios for the trainers, to be used for briefing and debriefing.
I-13	The system will provide access to a simulated network with the applicable commercial tools.
I-14	The system will be provided with additional security, networking and forensics tools required to successfully complete the provided training scenarios (e.g. Wireshark, IDA Pro, SysInternals, etc.)

J-9	The system provides a cloud-based, AWS hosted, SaaS architecture.
J-10	The system cloud-based architecture supports multiple classes running simultaneously, with multiple users connecting over the internet.
K	Web Interface
K-1	The system will provide a web-based marketplace where users can book a training session.
K-2	The system will provide the ability to configure the list of trainees. These trainees can be later assigned to a training.
K-3	The system will provide the ability to filter the available scenarios based on duration, difficulty level, tools, NICE roles, and additional properties.
K-4	The system will provide the ability to view and choose the relevant network for each scenario before booking a training session.
K-5	The system will provide the ability to book multiple sessions in different configurations (guided, self, individual, team) according to the subscription license and availability of the environments.
K-6	The system will provide the ability to schedule the time for a training session. Once the training session time arrives, the environment should be available for trainees to start training.
K-7	The system will provide the ability to view the results of each completed session. The result should include the score, the achieved goals and additional information about the completed training.
K-8	The system will provide the ability to change the score by the trainer at the end of the training session.
K-9	The system will provide the ability to automatically deduct the score of the trainee in cases of using hints.

6.4 On-Premise Cyber Range Functional and Technical Requirement

#	Requirements
A	High Level Requirements
A-1	The system will simulate networks, traffic and attack scenarios, to train and test trainees, security practitioners, procedures, and technologies in a safe and controllable environment.
A-2	The system training environment will be isolated and will not require internet connectivity, or connectivity to the corporate network.
A-3	The system training environment can easily revert to default "clean" state prior to a new training session.
A-4	The system will provide a realistic cyber training and simulation platform.
A-5	The system will provide a rich and diverse virtual network, with leading commercial security tools, which emulates a corporate network.
A-6	The system will provide a virtualization and emulation of network devices and protocols, including: <ul style="list-style-type: none"> • Security components • Network appliances • Servers and applications • User computer endpoints
A-7	The system will provide an industrial control system (ICS) network segment, to enable the simulation of ICS, critical infrastructure attacks. The ICS segment will include ICS devices, including Programmable Logical Controller (PLC) and Human-Machine Interface (HMI) devices.
A-8	The system will include a catalogue of pre-scripted, out-of-the-box, IT attack scenarios. Part of the scenarios shall be for individuals and adapt micro out-of-the-box networks, and some of scenarios shall adapt team training running on a full network.
A-9	The system will include a catalogue of pre-scripted, out-of-the-box, ICS attack scenarios.
A-10	The system will include a catalogue of pre-scripted, out-of-the-box, Pen-testing/Red scenarios.
A-11	The system will support the training of multiple, independent classes (teams) simultaneously, over a single architecture, managed by a single trainer.

A-12	The system shall include a "War Game" training mode. In this mode you can have attackers vs. defenders in one training. It's a free style attack training between two groups of trainees.
A-13	The system will provide the option for remote training over VPN.
A-14	The system will provide an option to customize the existing network or create new, virtual networks.
A-15	The system will provide an intuitive GUI-based tool for customizing existing attack scenarios, and for creating new attack scenarios. (Custom Scenario builder)
A-16	The system shall include the ability to import the trainees list from an external LMS
A-17	The system shall include the ability to export training session results to an external LMS
B	Virtual Network
B-1	The system will include multiple segments of IP subnets, VLANS, and a DMZ - in order to realistically represent an operational corporate network.
B-2	The system will include a perimeter firewall and an internal firewall. Fully operational and licensed (not open source/community edition).
B-3	The system will include a Zenoss server to monitor the status of server services.
B-4	The system will include a commercially licensed SIEM (Security Information and Event Management) product. The SIEM included in the system will not be open source/community edition, but a commercial product, to emulate a real-life SOC environment.
B-5	The SIEM will be pre-configured to include rule sets that will support the attack scenarios, so that SIEM alerts will be triggered according to the training scenario.
B-6	The system will include a mail relay server.
B-7	The system will include a Domain Controller server.
B-8	The system will include a DHCP server.
B-9	The system will include a server segment including SQL, DC, DHCP, File server etc.
B-10	The system will include a User segment, and will include workstations running Ubuntu OS, and Windows OS.
B-11	The system will include a Web segment including an FTP application server, an Apache web server and a Microsoft Internet Information Services (IIS) web server.

B-12	The system will include a VPN Segment. Trainee stations will connect to the training network by means of the VPN Server residing in this segment.
B-13	The system will support remote training by means of a browser-based application, without having to install a client on the trainee machine.
B-14	The system will include an ISP Segment to simulate an internet network, and will include Domain Naming Services (DNS), IIS Web Server and WebMail - SendMail-based mail server.
B-15	The system will include VLAN and IP segmentation of the various segments (e.g. Users segment, SIEM segment, ISP, VPN, SCADA etc.) in order to maintain a network structure resembling a real-life corporate network.
B-16	The system will include an ICS (Industrial Control Systems) segment. It will include hardware to simulate operational technology (OT) processes, which are simulated in OT training scenarios.
B-17	The system will include the ICS segment with a visual Graphic Use Interface (GUI) representation of an industrial process.
B-18	The out of the box networks shall include "detectors" which detect the trainee's activity and impact the final score.

C	Traffic Generator
----------	--------------------------

C-1	The system will include a traffic generator that will simulate real-life, benign traffic, to maximize the effectiveness of the training sessions. The traffic generator will simulate traffic in multiple protocols including IP, HTTP, SMTP, POP, FTP, and ICMP.
C-2	The system will allow to configure the source and destination of the traffic generated by the traffic generator.
C-3	The system will allow to configure the traffic type and protocol of the traffic generated by the traffic generator.
C-4	The system will allow to configure the duration of the traffic generated by the traffic generator.
C-5	The system will allow to configure the amount of network traffic generated by the traffic generator, by allowing the creation of flow groups.
C-6	The system's traffic generator can utilise any traffic recorded in a PCAP file and replay it during a training session.

D Attack Generator

- D-1 The system will include an attack generator that will simulate cyber-attack scenarios.
- D-2 The attack generator will simulate attack scenarios and will inject malware into the simulated network, originated in various network segments, according to the attack scenario configuration. Attack origins may be:
- External – simulating an external threat.
 - Internal – simulating user misconfigurations, user errors, or malicious insiders.

E Trainer Management Console

- E-1 The system will provide a management console for tracking and maintaining a trainee performance card. Each trainee will be identified by ID, image, role, and additional fields as required.
- E-2 The Trainer Management console will provide an Intuitive graphical user interface (GUI) enabling trainers to configure and run training sessions.
- E-3 The Trainer Management console will provide straightforward setup of a training session including trainees assignment, network selection, and scenario selection
- E-4 The Trainer Management Console will provide the option to record and allow playback of trainee screens.
- E-5 The Trainer Management Console will provide a messaging function enabling trainer and trainees to exchange messages during the session.
- E-6 The Trainer Management Console messaging feature will record the messaging conversations and they can be played back after the session for debrief purposes.
- E-7 The Trainer Management Console will provide the option to search for previous sessions in the database.
- E-8 The Trainer Management Console will enable the instructor to initiate the attack scenario during the session.
- E-9 The Trainer Management Console will allow tracking and grading trainee performance.
- E-10 The Trainer Management Console will provide the option to execute, control and monitor the flow of the session in real time.
- E-11 The Trainer Management Console will provide an evaluation module - per individual trainee and per team. The evaluation will support a bonus mechanism.

E-12	The Trainer Management Console will provide the option to store and run previous lessons.
E-13	The Trainer Management Console will provide the option to replicate a previous lesson, including its settings, and to reuse it as a new session.
E-14	The Trainer Management Console will provide a view of training history.
E-15	The Trainer Management Console will display detailed goals for the session.
E-16	The Trainer Management Console will provide the option to edit the goals and the workflow of existing scenarios.
E-17	The Trainer Management Console will provide option to influence the level of difficulty of the scenario and simulating more sophisticated attackers, by modifying parameters such as changing attack duration, deleting logs during the attack, and performing a silent attack.
E-18	The Trainer Management Console will provide a view of the training network info via the trainer and trainee interface (in a format such as JPEG, CSV etc.)
E-19	The Trainer Management Console will display a session timeline, displaying attack progress, milestones, and session events including milestones achieved and notes.
E-20	The Trainer Management Console timeline will monitor and display SIEM events.
E-21	The Trainer Management Console timeline will provide a summary of all the training events at the timeline.
E-22	The Trainer Management Console will allow the trainer to add textual comments which will appear on the timeline.
E-23	The Trainer Management Console will allow playing back the session including video playback of trainee screens, and will recreate the timeline including session events, milestones achieved and comments. The Console will allow skipping to these events for effective playback.
E-24	The Trainer Management Console will provide the option to zoom into the trainee's screen during the session and will allow zooming to full screen size for improved viewing quality.
E-25	The Trainer Management Console will provide the option to zoom into the trainee's screen in playback during debrief and will allow zooming to full screen size for improved debrief quality.
E-26	The Trainer Management Console will provide an option to view the timeline progress as absolute or relative, during a training.

E-27	The Trainer Management Console will allow the trainer to skip to interesting moments in the timeline during playback, including attack milestones, trainees' achievements, and messages sent.
E-29	The Trainer Management Console will record trainee stations in video. The instructor will be able to view all trainee screens simultaneously and enlarge any trainee screen to full screen.
E-30	The trainer application shall provide an indication if a goal was automatically detected/achieved by the trainees. The trainer can edit and override the system feedback.
E-31	The trainer can control the whole site (all trainees) from one application. The trainer can easily navigate between the trainings in the site.
E-32	The trainer can create training according to the site configuration. It means that the trainer can create multiple individual sessions simultaneously, each one with individual network and scenario.
E-33	The trainer can configure the training to run in self training mode. This mode means that the trainees can start the training by themselves.
E-34	The Trainer Management Console will provide an option to filter events on the timeline per type.
F	Trainee Interface
F-1	Trainees can train over commercial, best of breed security tools, investigation and monitoring tools including: SIEM, Firewall, station logs, server logs, Zenoss, Putty, and Wireshark for investigation. The system should include best of breed security products including QRadar SIEM, Palo Alto Network Security, Splunk and more.
F-3	The trainee interface will display session time progression and score as an overlay without interfering with security product UI.
F-4	The trainee interface will include vSphere access to all machines in the network.
F-5	The trainee interface will provide an RDP connection to all Windows machines in the network.
F-6	The trainee interface will include an interactive investigation tool for the trainees, where they can capture their insights and evidence for the investigated attack scenario.
F-7	The investigation tool on the trainees' interface provides an indication whether the evidences added by the trainee during the training are correct or not, so the trainee can use it for learning, fix it, and get real-time feedback. This tool is helpful for self-learning and deep understanding.

F-8	The trainee interface will include a quiz, that aims to test and verify the trainee's understanding.
F-9	The trainees will be able to initialize the network and start the training session by themselves.
F-10	The trainee will be able to request hints in case of self-training. The hints shall help the trainee to solve the training.
F-11	The trainee will be able to open a full solution of the scenario in case of self-training.
G	Attack Scenarios
G-1	The system will include an attack generator that will simulate pre-scripted attack scenarios. The system will not require human resources or red teams to operate and run the attacks, ensuring the attacks are consistent and repeatable, and minimizing the need for additional resources.
G-2	The system will provide a catalogue of IT attacks.
G-4	The system will support varying levels of scenario difficulty and complexity.
G-5	The simulated attack scenarios will include a wide set of attack vectors including Web, Email, infected CD, FTP, and VPN.
G-6	The system will simulate multiple exploit scenarios such as: data theft, web crawling, SQL injection, port scanning, ping sweep, password brute force, backdoor scripting, website spoofing, spear phishing, SSH protocol fuzzing, and DNS poisoning.
G-7	The system will simulate exploit scenarios such as VPN HeartBleed.
G-8	The system will provide attack scenarios with high tangible impact on the network including Denial of Service (DOS), information theft, and website defacement,
G-9	The system will provide attack scenarios utilizing Linux logs, Windows PC and server logs, SIEM logs, firewall logs, Zenoss logs, mail relay logs, reverse engineering and web and networking forensics, MSSQL server logs, SCADA IDS logs, network forensics, VPN log forensics
G-10	The system will provide attack scenarios utilizing SCADA IDS logs
G-11	The system will provide a module for customization of attacks - Setting security tools alerts to silent or active, to impact diagnostics difficulty.
G-12	The system will provide a module for customization of attacks - Deleting logs created during the attack, to impact diagnostics difficulty.

G-13	The system will provide a module for customization of attacks - Control the scenario running speed (slow, medium, fast).
G-14	The system will provide a module for customization of attacks - Change attacker IP address between actions.
G-15	The system will provide a module for customization of attacks - Adding customized scripts and integrating user-created scripts to propagate specialized attacks into the scenario attack flow.
G-16	The system will include an ICS attack scenario using site-to-site connection vulnerability.
G-17	The system will provide multiple scenarios of OT attacks.
G-18	The system will provide attack scenarios showing impact on the operational technology (OT) network as SCADA process tampering, and SCADA process disruption and downtime.
G-19	The system will provide an ICS attack scenario in which the attack vector initiates in the IT network and traverses to the OT network (IT to OT attack) simulating the evolvement of a typical OT attack.
G-20	The system shall provide individual content including scenarios and networks, focused on specific discipline such as Malware analysis, advanced incident response, specific product practice, etc.
G-21	The system shall include dedicated scenarios for pen-testers/ethical-hackers. The scenarios include a network and a "Flag" the trainees have to achieve during the training. The trainee can use Kali Linux to execute the attack.
G-22	The system will provide all attack scenarios mapped to MITRE ATT&CK Framework
H	Automatic scoring and evaluation
H-1	The system will provide an automatic scoring mechanism (self-evaluation), to automatically detect the trainees achievements.
H-2	The out-of-the-box networks shall include "detectors" which detect the trainee's activity and affect the training score.
H-3	Correct answers to scenario quiz questions shall affect the total score of the training.
H-4	The trainer can configure the training to run in "test mode", which means that the trainees will not see scores nor feedback in their application during the training. They will not be able to get hints or see the full solution. This mode is useful for certifications.

H-5 The system will provide a template-based report generator, to allow the trainer to produce a trainee report at the end of the training session.

I Deliverables and Services

I-1 The system will be supplied with all hardware components, including:

- Storage
- Servers
- Ethernet switches
- UPS
- Ethernet cables
- Power cables
- Server rack

I-2 The system will be supplied with all hardware components, including:

- SCADA cabinet including PLCs, power supply, IO points, and display panels.

I-3 The system will be supplied with all software components, including:

- Windows
- Microsoft Office
- McAfee Endpoint Security
- SIEM (ArcSight or QRadar or Splunk)
- Firewall (Check Point or Palo Alto)
- VMware vCenter Standard
- Zenoss

I-4 The system will be provided with on-site support for system installation and configuration.

I-5 The system will be provided with on-site training to authorize trainers ("train the trainer").

I-6 The system will be provided with remote support for maintenance and troubleshooting.

I-7 The system will be provided with hardware warranty.

I-8 The system will be provided with software warranty.

I-9 The system will be provided with a White Team Guide: Scenario guide with specific instructions on how to solve each scenario.

I-10 The system will be provided with an Admin Guide.

I-11 The system will be provided with a Blue Team Guide: including network overview, usernames & passwords.

I-12 The system will be provided with written material describing the scenarios for the trainers, to be used for briefing and debriefing.

I-14 The system will be provided with additional security, networking and forensics tools required to successfully complete the provided training scenarios (e.g. Wireshark, IDA Pro, SysInternals, etc.)

J Architecture

J-1 The system architecture will include a server (physical appliance) to run the solution components.

J-2 The system architecture will include Windows-based trainee stations.

J-3 The system architecture will include a trainer station.

J-4 The system architecture will include Ethernet network to connect the server, trainee and trainer stations.

J-5 The trainee stations will be grouped to 10 in each Class.

J-6 The architecture will support running multiple independent classes from a single trainer station.

J-7 The architecture will allow optional connection of trainee PC via VPN from an external network.

REFERENCES

- [1] Terrifying Cybercrime Statistics – Protect Yourself in 2021, <https://safeatlast.co/blog/cybercrime-statistics/>
- [2] Cyber Security Skills Crisis Causing Rapidly Widening Business Problem, <https://www.prweb.com/releases/2017/11/prweb14899778.htm>
- [3] Cybersecurity Professionals Stand Up to a Pandemic, (ISC)2 CYBERSECURITY WORKFORCE STUDY 2020, <https://www.isc2.org/-/media/ISC2/Research/2020/Workforce-Study/ISC2ResearchDrivenWhitepaperFINAL.ashx>
- [4] The cybersecurity skills gap: 4 million professionals needed worldwide , <https://www.hdi.global/en-za/infocenter/insights/2020/cyber-skills-gap/>
- [5] NIST (2018), Cyber Ranges, https://www.nist.gov/system/files/documents/2018/02/13/cyber_ranges.pdf
- [6] <https://cyberstartupobservatory.com/next-gen-cyber-ranges-delivering-customer-specific-repeatable-large-scale-realistic-exercises/>
- [7] NIST (2019), Developing Cyber Resilient Systems: A Systems Security Engineering Approach, <https://csrc.nist.gov/CSRC/media/Publications/sp/800-160/vol-2/draft/documents/sp800-160-vol2-draft-fpd.pdf>
- [8] Gartner (2018), Organizational Resilience Is More Than Just the Latest Trend, <https://www.gartner.com/en/documents/3875514/organizational-resilience-is-more-than-just-the-latest-trend>
- [9] ENISA (2020), European Cyber Security Challenge, <https://europeancybersecuritychallenge.eu>
- [10] WorldSkills (2019), <https://worldskills.org>
- [11] Cyber Stars (2019), <https://www.cyberstars.pro>
- [12] Gartner (2020), Digital Dexterity, At Gartner Digital Workplace Summit, <https://www.gartner.com/en/conferences/na/digital-workplace-us/featured-topics/digital-dexterity>
- [13] Geekflare (2018), 8 Cyber Attack Simulation Tools to Improve Security, <https://geekflare.com/cyberattack-simulation-tools/>
- [14] MITRE ATT&CK, <https://attack.mitre.org>
- [15] NIST, NICE CYBERSECURITY WORKFORCE FRAMEWORK RESOURCE CENTER, <https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center>
- [16] European e-Competence Framework, A common European framework for ICT Professionals in all industry sectors, <https://www.ecompetences.eu/>

Corporate Office:

CyberSecurity Malaysia

Level 7, Tower 1, Menara Cyber Axis,
Jalan Impact, 63000 Cyberjaya,
Selangor Darul Ehsan,
Malaysia.


Tel: +603 8800 7999

Fax: +603 8008 7000


Email: info@cybersecurity.my

www.cybersecurity.my

 [@cybersecuritymy](https://twitter.com/cybersecuritymy)

 [CyberSecurityMalaysia](https://www.facebook.com/CyberSecurityMalaysia)

 [cybersecurity_malaysia](https://www.instagram.com/cybersecurity_malaysia)

 [CyberSecurityMy](https://www.youtube.com/CyberSecurityMy)

© CyberSecurity Malaysia 2022 – All Rights Reserved



MINISTRY OF COMMUNICATIONS
AND MULTIMEDIA MALAYSIA

