Toni Huhtakangas

XAMK CYBER RANGE

Design of concept for cyber training environment

Master's thesis

Master of Engineering

Cybersecurity

2022

Kaakkois-Suomen ammattikorkeakoulu

Tutkintonimike	Insinööri (Ylempi AMK)
Tekijä/Tekijät	Toni Huhtakangas
Työn nimi	Xamk kyberharjoitusympäristö - kyberharjoitteluympäristön konseptin suunnittelu
Toimeksiantaja	Kaakkois-Suomen ammattikorkeakoulu
Vuosi	helmikuu 2022
Sivu	114 sivua, liitteitä 3 sivua
Työn ohjaaja(t)	Vesa Kankare

TIIVISTELMÄ

Tämän harjoitustyön tavoitteena oli suunnitella konsepti Kaakkois-Suomen ammattikorkeakoulun (Xamk) virtuaalisesta kyberturvallisuuden harjoitteluympäristöstä. Kyberharjoitteluympäristön konsepti on tarkoitus toteuttaa vaiheittain osana Kotkan yrityspuiston kehitysprojektia, jonka avulla Kotkaan kehitetään kokonaisturvallisuuden ja satamalogistiikan turvapuistoa (turvallisuuden harjoitus- ja koulutusympäristöä). Hanke on valmistelussa Xamkissa ja sille on haettu REACT-EU rahoitusta vuonna 2021. Turvapuiston kehittämisessä oli mukana vuonna 2021 Kotkan kaupunki, Xamk, Ekami, muutamia muita yksityisiä yrityksiä sekä viranomaistahoja.

Kyberharjoituksia voidaan pitää joko pöytälaatikkoharjoituksina, virtuaalisessa suljetussa ympäristössä tai yhdistelemällä molempia harjoitustapoja. Virtuaalisen harjoitusympäristön tarkoituksena on kehittää osallistujien taitoja kyber toiminnassa. Virtuaalinen ympäristö voidaan muokata vastaamaan erityistarpeita tai normaalia käyttöympäristöä erilaisten skenaarioiden avulla. Kohderyhminä harjoitusympäristölle ovat Xamkin opiskelijat sekä yritykset, jotka haluavat toteuttaa kyberharjoituksia suljetussa ympäristössä. Virtuaalista harjoitusympäristöä voidaan käyttää harjoitteluun reaaliaikaisen tilannekuvan ylläpitämisestä tai sen avulla voidaan testata erilaisia laitteita ja niiden ominaisuuksia. Harjoitusten avulla osallistujat saavat harjoitusympäristön avulla kokemusta poikkeavien tilanteiden hallintaan sekä laitteiden toiminnallisuuksien testaukseen. Harjoituksista on mahdollista saada lisätietoa erilaisten mittareiden avulla.

Opinnäytetyön tutkimusmenetelmänä käytettiin laadullista tutkimusmenetelmää sekä toimintatutkimusmallia, joiden muodostama yhdistelmä sopii hyvin tutkimuksessa esiin nousseisiin ongelmiin sekä ratkaisuihin. Tutkimus alkoi aiheen hyväksyttämisellä sekä valitsemalla sopiva tutkimusmenetelmä. Tutkimus eteni vaiheittain keräten tietoja tieteellisistä tutkimuksista. Tutkimuksen toisessa vaiheessa vertailtiin saatua ja analysoitua tietoa. Tutkimuksen viimeisessä vaiheessa luotiin konsepti Xamkin virtuaaliselle harjoitusalustalle.

Yhteenvetona voidaan todeta, että tulokset ja johtopäätökset mahdollistavat virtuaalisen harjoitusympäristön kehittämisen tulevaisuudessa, jonka avulla voidaan toteuttaa todellisiin tapahtumiin perustuvia virtuaalisia harjoituksia. Virtuaalisen harjoitusympäristön avulla voidaan tulevaisuudessa kehittää opiskelijoiden sekä ulkopuolisen yrityksen henkilöstön tietoturvaosaamista sekä harjoitella menettelyjä poikkeamatilanteissa.

Asiasanat: Kyberturvallisuus, SOC, kyberharjoitus, dokumentointi, tilannekuva

Degree	Master of Engineering
Author (authors)	Toni Huhtakangas
Thesis title	Xamk cyber range - Design of concept for cyber training environment
Commissioned by	South-Eastern Finland University of Applied Sciences
Time	February 2022
Pages	114 pages, 3 pages of appendices
Supervisor	Vesa Kankare

ABSTRACT

The purpose for this study was to develop virtual cyber range concept for the use of South-Eastern Finland University of Applied Sciences (Xamk). The cyber range is meant to be implemented step by step as a part of City of Kotka's business park development project. The project is being prepared by Xamk, and it has applied for REACT-EU funding in 2021. In 2021, the city of Kotka, Xamk, Ekami, a few other private companies and the authorities were involved in the development of the safety park.

Cyber exercises can be considered either as tabletop exercises, or a virtual closed environment exercises, which are used in the so-called cyber range environment. The purpose of the virtual cyber range environment is to be developing the skills of the participants. The virtual training environment can be modified for fitting the special need, or it can suit the normal operating environment with different kinds of scenarios as needed. The target groups for the virtual exercises in the environment are students at Xamk and companies that are meant to carry out cyber exercise in a closed environment. Capabilities of the virtual training environment enable real-time snapshot of the events and incidents, and possible modifications and changes can be tested before implementation. Participants gain experience of managing situations in the training environment. It is possible for companies to gain more information about the exercise using various metrics.

This study used qualitative research methods with action research method. This combination of methods is suitable for projects which include incident and problem-solving procedures. The study progressed by phases with collecting information for the study. The second phase of the study was based on benchmarking received information and analyzing the collected data. The last phase of the study created the concept for Xamk cyber range.

In summary, the results and conclusions will allow the development of a virtual training environment in the future, which will allow the implementation of virtual exercises based on real events. The up-coming virtual platform enables flexible training environment for cyber exercises. Information of data collection focused on special features which provide possibility to perform different kind of realistic cyber scenarios. Virtual training platform provides possibilities to develop students' individual skills and team skills in the field of information security. The virtual platform gives an opportunity to perform exercises in a standby situation as well as test security products, and it includes the model of continuous improvement.

Keywords: Cybersecurity; SOC; Cyber-range; training; documentation; cyber-situation awareness

Contents

TERMS AND ABBREVIATIONS

AAR (After action review)	a document examining actions and results in cyber exercise
Bot, botnet	an independent machine of program capable of operating in accordance with its programming
Blue team (bt)	team of defensive actions which maintains security in training the infrastructure
CTF	capture the flag competition played by teams or individuals
CVSS	common vulnerability scoring system
Cyber	computer security
Cyber exercise	an event which simulates cyber-attacks or incidents
Cyber range	virtual platform for cyber exercises
DFIR	digital forensics and incident response
DDOS	distributed denial of service attack
Exercise	a virtually designed single operation which include training and is evaluated
Event	a selected activity which is set as part of exercise.
ICT	information and communication technology
OT	operational technology
Kill chain	concept of attackers' execution of certain tasks at certain point of task list
MSEL	master scenario event list for cyber exercise
Red team (rt)	team of players who are concentrating offensive actions
Scenario	operational environment where it is possible to achieve virtually set exercises and one or more training objectives
Situation awareness	helps for decision-making and keep track processes for operational planning
Threat	an event which is causing impact in simulation
Vulnerability	weakness in software of information systems or devices

1 INTRODUCTION

Increased services in Internet and grown usage of cloud services has brought solid ground for worldwide cyber-attacks. An attacker has an unlimited amount of time for preparation with actions of reconnaissance. Government and companies need more preparation with training for possible cyber-attacks. The quality of malware has evolved over the past decade, with malware increasingly finding module-based features and even features that the malware seeks to protect itself from (Love, 2018). Malware can be roughly divided into five different categories according to the malware evolution curve 1. Basic malware 2. Windows malware 3. worms 4. ransomware 5. advanced malware (APT) (Patten, 2017). The trend of advanced malware seems to be increasingly directed at computer and server memory, which means for example that malware may not have a physical file on your hard drive (Patten, 2017). In this case, malware running through the memory can infect, for example, the flash memory on the computer's motherboard, as was detected in reports in the first half of 2022. Antivirus programs may not immediately detect malware automatically if they are located outside the hard disk. Also, reinstalling the operating system or erasing the hard drive may not remove the malware itself from the device (Kan, 2022). The number of malwares detected on the Internet has remained high from year to year. A report submitted by Comodo for the second quarter of 2017 shows that approximately 97 million malware detections were made in the three-month follow-up period, and this data is already a few years old (Poremba, 2017).

One malware may impact the organization’s network’s computer and infect organization’s systems in the network. As a result of the effectiveness of cyber-attacks, the United States Defense Department introduced cyber as a fifth military dimension in 2011. NATO included cyberspace as an operational domain in 2016. NATO has developed suitable cyber range platforms which are used in allied countries (Graziano 2021). The virtual training platform cyber range is a virtual platform where cyber related scenarios can be planned and executed safely in a closed environment.

According to National Institute of Standards and Technology (NIST)-publication cyber range guide (NIST 2021), cyber ranges are “interactive, simulated platforms and representations of networks, systems, tools and applications”. Cyber ranges are focusing to enable possibilities for virtual training in different type of realistic scenarios where organizations can learn and improve situational performance. During the scenario, the teams are improving their individual skills and teamwork abilities.

1.1 Cyber ranges in the past, present, and future

Cyber range development from a cybersecurity learning perspective started in the late 2010s. It aimed for building private and public cyber ranges with the development of technologies and with initiatives of nationwide cybersecurity programs. Cyber range’s intended use is like traditional firing ranges, but physical battles are fought in cyberspace (ECSO 2020c). Cyber ranges are places for virtual exercises where individuals or teams can go through scenarios of cyberattacks and defense at their own pace.

One of the early research projects related to cyber ranges was called Deter-project, which was established in 2004 (Mirkovic et al. 2010). Deter aimed to support cybersecurity research and education by creating realistic ICT infrastructure, facilities, tools, and processes for providing resources for experimentation in cybersecurity (Mirkovic et al. 2010). Nowadays, Deter-project is the organization which is called company as “Cyber defense technology experimental laboratory” (Deter Lab). Deter Lab is a computing facility focused on researching cybersecurity and testing environment. Deter Lab is providing information for the user community, industries, and for government (Deter-project 2021). One of the latest cyber range implementations was related to Debatty and Mee’s study titled as: “The cyber range for cyber defense situation awareness” which focused on the increase of support for decision-making by training with investigated for real incidents (Debatty and Mees 2019).

Cyber training was activated in the USA when Michigan cyber range was built in 2012 to teach cybersecurity and to provide services relating to the studies of cybersecurity. After developing its operation, the Michigan cyber range has operating services from four different locations in the USA (Turčaník 2020). IBM

claimed that it opened the first commercial cyber range (X-force command) in 2016 which is in Cambridge, Maryland, USA. In the beginning, the facility contained seats for 36 participants, which was one of the largest facilities at that time. X-force cyber range's platform included a data center where the IT infrastructure was located and maintained as part of the training. The cyber range is developed for training of cyber exercises which contains actual cyber events and training of how to minimize effects of the offensive actions (Miller 2016).

Secretariat of the Security Committee of Finland introduced in 2013 publication titled "Finland's Cybersecurity Strategy", which aims for secured coordinated functions of Finland against cyber threats in all situations (Secretariat of the security committee 2019, 8). Currently, planning of minimizing the cyber threats is scoped as the part of the goal of Finnish critical infrastructure. The main threats identified are a failure of an electricity supply, telecommunications, logistics, community infrastructure, food supply, finance and payment systems, public health and well-being and information systems. Disruptions of critical infrastructure among the physical threats that are affecting security are identified as accidents, weather conditions and environmental threats, terrorism, border management disturbances, political, financial, and military pressure and use of military forces (Turvallisuuskomitea 2021). In Finland there are two regularly organized major cybersecurity-related exercises which are called TAISTO and KYHA. The state administration (Digital and population data services agency) organizes a cyber exercise called "TAISTO", which started annually in November 2018 (DVV 2021). The second cyber exercise in the Finland is called a "KYHA" which is organized by a JYVSECTEC. Kyha exercise is designed for Finnish security authorities and for health care industry. Security authorities of Finland are the police and the emergency response center (Turvallisuuskomitea 2019). Cyber exercises increase the skills of preparedness and incident response lifecycle (observation, reaction, and recovery) which include the use of resources and ICT-process understanding with supply chain (Traficom 2021).

The cyber ranges are constantly developing, with integrated systems in the future. In 2021 Canadian armed forces started to develop an infrastructure called "connected battle space" (CB). CB aims for utilizing new technologies for example low orbit satellites, Internet of Things (IoT), cloud computing, and artificial intelligence (AI) to collect and process large amounts of data. As a result, CB

has planned to give faster indicators for decision-making (Budning et al. 2021). Eventually, CB might start co-operation with North American Aerospace Defense Command (NORAD). CB will support all six domains air, land, maritime, space, information, and cyber. The United Kingdom (UK) and Australia are currently developing their own CB platforms. As a result, these variables will align intention, programming, resources, and know-how. Intention contains political declaration which gives mandates, authorities programming promote organizations and co-operative control, and innovations provided by engineers. Targeted program involves resources provided by authorized personnel. Know-how selects innovative methods for creating CB (Budning et al. 2021).

1.2 Models for cyber exercises

In Europe, the use of cyber ranges is identified as important tool set for training activities. European Cybersecurity Organization (ECSO) has started “call the action” for the European cyber range community to collaborate cyber ranges for different functions, which aims for evaluating approaches such as services, exercise types and different concepts in six different working groups (WG). Working groups were WG1 on standardization, certification, and supply chain management; WG2 on market deployment, investments, and international collaboration; WG3 on cyber resilience of economy, infrastructure & services; WG4 on support to SMES, coordination with countries and regions; WG5 on education, training, awareness, cyber ranges, and WG6 on SRIA and cybersecurity technologies (ECSO 2020b). The study is aside on results of overview of cyber ranges and their functionalities with the publications of WG5 and WG6.

In Finland, companies have been supported to start cyber exercises, and various materials have also been published for cyber training. National Cyber Security Centre of Finland (NCSC-FI) has published examples of different cybersecurity scenarios, which can help form the cyber scenarios and -exercises. The services which are offered by NCSC-FI are 1. consulting services provided for choosing the suitable partner for exercise, 2. cyber exercise planning support and situation awareness services, 3. feedback during exercise simulation services, 4. observations during the exercise, and 5. assistance during analysis after exercise (Traficom 2021). The development of cyber-related exercises needs competence, experience, and resources. Cyber range platform requires

modularity and automated features which make actions of maintenance and scenario building procedures faster and more reliable. Cyber range scenarios are used a limited amount of time, which requires balance between resources and used time frame (Parsons 2021).

Virtual cyber exercises are usually performed in three different ways, as a tabletop exercise, as an exercise in a virtual environment, or a combination of these. Exercise aims for evaluation of organization's playbooks and procedures and cyber range trainings aims for developing skills of the persons of the organizations (Parsons 2021). Instruction and training by organizations are currently scheduled on organizations daily jobs. Incident based training for cybersecurity issues is implemented also in Finland. Those trainings contain countermeasures against intrusion attempts and data thefts. The purpose of the training is to improve an organization's cyber-resilience. For achieving cyber-resilience, the organizations need to identify and utilize key resources. At the moment, cybersecurity exercises have gained popularity in operations of security operations center (SOC), instrumentation & control systems (ICS), and in maritime industry (harbor, logistics, ship industry). According to a maritime survey, the cyber-attacks have been increased by 9 % in 2020, which may indicate increase of need for cyber training in the future (Macola 2020).

1.3 Background of study

Universities are known for creativeness, knowledge, and public interaction that usually pioneers of technology with students. Knowledge is based on cycle of learning and its results are ideas and experiences which is the key element for absorption of information. Finnish universities and business industries have supported each other and connection between them is interactive. South-Eastern Finland University of Applied Sciences (Xamk) published study titled: "XAMK Beyond 2020 – At your service – Business Development, Co-operation, and Sustainability" which encourages Xamk personnel to be open and creative for publishing material for international studies and cybersecurity related publications, that some students and personnel has already done in Xamk (Neuvonen-Rauhala 2020).

This research was aimed to develop a concept of Xamk cyber range virtual training environment, which is under continuous development by Xamk. Xamk also provides studies for Bachelor and Master of Engineering in the field of cybersecurity in the city of Kotka, Finland. At the moment, Xamk uses a virtual laboratory system (Virtual Lab) only for cyber studies. With the help of the Xamk Virtual Lab system, Xamk implements virtual laboratory exercises for ICT, cyber and gaming studies. The first version of Virtual Lab system was introduced in early 2016. The latest update was released in June 2021.

The purpose of a virtual laboratory environment is to provide cyber exercises to the students and organizations. Virtual laboratory environment with cyber related aspects gives student a holistic view to the cybersecurity and for the teacher the environment gives tools to evaluate students skills. The cyber related aspects contain interactive cyber-attack simulations which can be gene rated with scratch, from known issue, or it can be customized to the need of customer. The users of virtual laboratory environment are students of Xamk or customers of Xamk. The virtual environment is built and used in a closed network, which enables cybersecurity training safely. The research investigated theories, which included reports of common parts for concepting a suitable cyber range virtual environment. The suitable modules for the cyber range founded in the study catalog of South-Eastern Finland University of Applied Sciences (Xamk 2021). At the moment in 2021 Xamk organizes professional lectures and individual exercises in Xamk's virtual training environment. In a current virtual environment, it is possible for Xamk to provide individual training which can be created by using real life simulated cyber-attacks. Currently, organizations from area of Kotka organize cyber training at Xamk and use Xamk's virtual environment. Virtual exercises contain limited number of documentations. Teachers give instructions and documentations in the classes when needed.

Xamk cyber range needs proper concept but also more knowledge about the functionalities behind virtual environment. The concept is part of the Xamk's quality management procedures, which the school is maintaining. Quality procedures are included also with the cybersecurity degree program's "lesson by lesson" feedback from students, which ensures that only all best practices would be in use of the class. Continuous improvement by quality management

aids the students with learning and thinking. The chance for reflection (learned) of studies are given to the students after each lesson, which aims for personal growth and evaluation of self-learning. It provides feedback about the lessons which the teacher can use as a tool to of best practices developing the material and assignments for next lessons.

Xamk's organizational structure (figure 1) contains a board with chief executive officer (CEO), vice president, financial and human resource services and education administration with education services and the areas of the field of studies. The school operates between four cities: Kouvola, Mikkeli, Kotka and Savonlinna. Xamk offers studies for information technology, cybersecurity, and computer game design. The school also offers studies such as Master of Business Administration Programs (MBA) and Environmental Engineering. Xamk also provides possibility to study degrees in Humanities, Social Services, Health Care, and Maritime Technology. The Maritime Industry studies contain also electrical engineering and logistics operations studies. Xamk offers education also for Health Care and Wellbeing Management (Xamk 2021). Along the studies, the city of Kotka offers a special field of internships in the port of Kotka and on local shipping companies. As is presented in figure 1. Xamk offers in the field of study degrees in five areas (Xamk, 2021):

- business, safety, and security
- game industry and ICT
- design and restoration
- health, rehabilitation, and physical education and
- technology and forestry

As presented in figure 1, the cyber range virtual environment was planned to be in organization chart under the School of Technology. Xamk's cyber range project is a part of a project which was aimed for city of Kotka's entrepreneur park's development design venture. The project included functions of total security and harbor logistics, Instrumentation & Control (ICS) infrastructure among the cybersecurity. The project was under preparation in Xamk and waiting for EU funding. The participants of the project are city of Kotka, Ekami vocational education (Ekami 2021) and several independent organizations of the area.

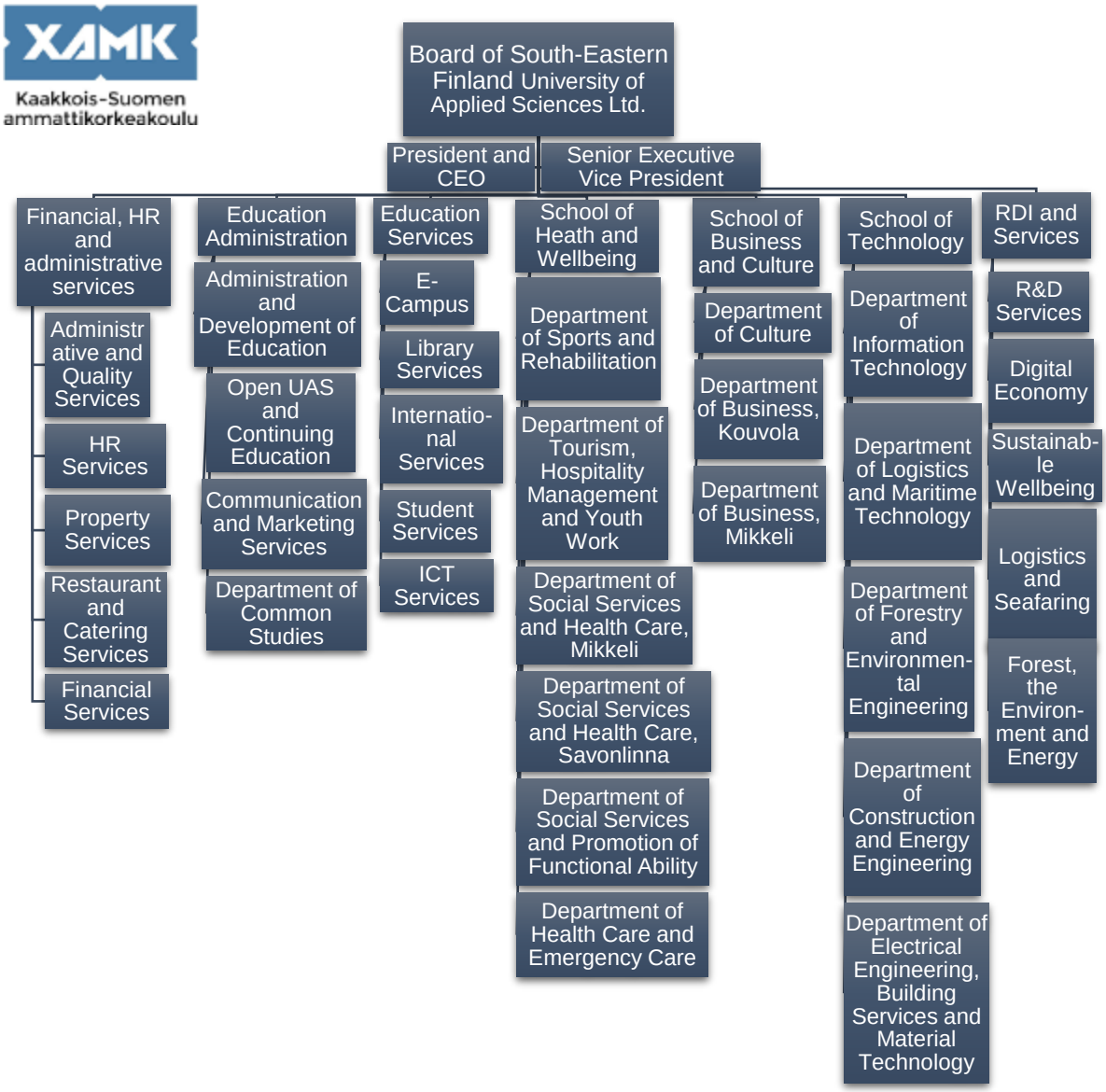


Figure 1. Organization of Xamk (Xamk 2021)

1.4 Delimitation of research

This study focuses only on the concept of Xamk virtual cyber range platform and only for its purposes of cyber training. The virtual platform can be applied for the use of common studies and other projects which are going on currently at Xamk, and they may mislead this study in the wrong direction. For example, methods of risk management and financial aspects are not included in this study. However, there is need for brief discussion on financial aspects, but no detailed information is given on that topic. During the development process of the study, the focus was set on features of the cyber range environment, and the use of the cyber range, and how these both could be improved in the future. At the end of the study, the question arises “how to start training in Xamk’s cyber

range", which eventually was included in the study as a conclusion as cogitation level.

1.5 Cyber- and computer security

Cybersecurity, which is also called computer security by International Atomic Energy Agency (IAEA), is used for controlled use and protection of ICS/ICT-systems and electrical equipment. Cybersecurity controls increase resilience of computer devices (IAEA 2011). Protective controls are used against various forms of attacks such as theft, unauthorized use of devices, networks, servers, services, and electronic systems (Kaspersky 2021). Information security refers to protecting confidentiality, integrity, and availability (CIA) of data with storage and transit. Cybersecurity actions refer to principles which aim for actions where computer devices are improved with their security and system health (Kaspersky 2021). Preparedness is needed for today's work environment (organizations' private network) for abnormal situations, and it will require constant attention and resources for maintaining and updating the network's services. Whenever the network's protection measures are required for actions, the reaction of resources are crucial for defending the organization's network. This leads to continuous improvement of the organization's maturity level of cybersecurity.

In the area of computer security, IAEA has established an IAEA graded approach, where implemented security controls are measured against potential impact of threats. The graded approach categorizes systems in different zones, where each zone includes certain requirements based to its security level. Each security level includes a set of protective security controls and as security classifications increase, security controls will become more stringent. The hardware and software (ICS/ICT) can be protected on a zone-by-zone basis according to the possible security classification (IAEA 2011, 29).

1.6 Definition for cyber range

The following areas of cybersecurity are best suited for virtual cyber training: application security, information security, network security, disaster recovery, operational security, and user education) which can be trained in virtual simulations (Touhid 2019). The cyber range is meant to be similar as "firing range"

but it is instead meant for training skills of cybersecurity in virtual simulation environment. Cyber ranges consist of ICT-systems in network in its own platform, which is mainly isolated from other networks, and it contains applications, processes, and technologies, which are used by virtual environment (ECSO 2020a). These cyber ranges are used for security-oriented events, which includes training, testing skills and evaluates new ICT-systems (Roque et al. 2020).

Cyber range virtual environment supports modularity, which helps to test procedures, emulations and simulations including related hardware- and software tools (Roque et al. 2020). An operating environment for cyber events and exercises may have a complex structure, which is required to be described in documentation. The presented structure needs to be intuitive including scientific concepts with evaluation, testing and training approaches (Roque et al. 2020). The virtual cyber range platform is needed for practicing the skills of individual and teams which are needed daily basis. The cyber range utilizes its virtual environment to support functions in the training area, server room and other facilities for activity. The main functionality for cyber range is, however, the virtuality where the specific scenario can be loaded in the memory. The scenario is written before the actual exercises. The cyber range environment is suitable for use in the situations as presented in figure 2 below. Cyber range activities can be set in different areas, which are 1. Classroom teaching, 2. Virtual exercises 3. Virtual ongoing threat exercises 4. Cyber-attack exercises, 5. Testing and research (ECSO 2020c). Those activities include educative and development capabilities for cyber resilience.

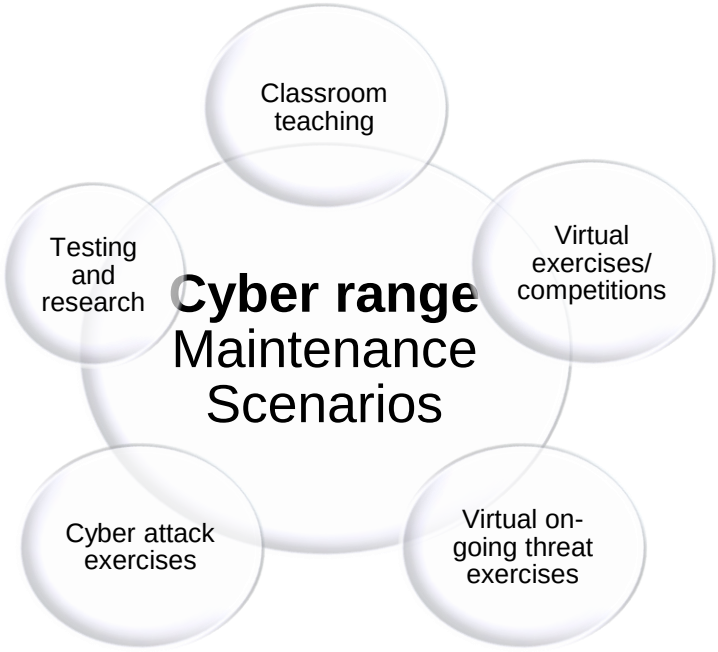


Figure 2. Cyber range – capabilities of usage (NIST 2021)

According to figure 2, the virtual cyber training platform can be utilized in various virtual cyber exercises and competitions. In addition, the platform can be used for software testing and scientific research. Classroom teaching contains regular teaching and homework, which are possible to create in the cyber range environment. Virtual exercises in cyber range environment are related to maintain ICT-infrastructure in closed environment. Virtual ongoing threat exercises include a selected scenario which the participant is going to solve. Cyber-attack exercises are team-based offensive and defensive scenarios which could be for example capture the flag (CTF) type of competitions or exercises. The technical aspect in the cyber range environment includes virtual servers in clustered environment. Although servers maintenance is set by a group of automated processes, the scenario-side automation logic requires a human for controlling the devices in cyber exercises. It is possible to automatize some cyber range's manual procedures for reduction of manual work, which may help to safely deploy automation support tools for cyber range. For example, a tool called Pandora may help work of maintenance (Jiang et al. 2020).

Evaluation of cyber threats may include cloud computers for incidents and testing methods against autonomous offensive cyber tools. For defensive use there are automated tools available for SQL injection detections, penetration testing

and for man-in-the-middle attacks. For testing environments, it would also include tools for automated binary exploits (Jiang et al. 2020). Although the cyber range platform is a closed system, it still needs to take consideration possibilities of platform vulnerabilities such as Venom (CVE-2015-3456) and VMware (VM) Fusion's vulnerability (VMSA-2015-0004, CVE-2015-2337). Vulnerabilities allows malicious code execution between virtual machine (VM) and host which could exploit the system (Jiang et al. 2020).

Table 1. Cyber range architecture and functionalities (Jiang et al. 2020)

function	**role**	**function**	**role**
portal	user, admin, client	management	cyber range, scenario, exercise or test
training and education module	scoring, tutoring, after action analysis	testing module	test case definition, analysis & verification
scenario	creation/edit, deployment, generation, execution, controlling, deletion	monitoring	collection, analysis, logging
runtime environment	emulate, simulate, traffic generation, attack generation, hardware, generate user behavior	data storage	simulate parameters, scenario definition, games rules, information index, replica, date, tools

Table 1 presents the cyber range's different categories of how the cyber range could be maintained and presents the desired features of the cyber range. As far as functions are concerned, the portal contains user access levels for cyber range. The training and education module contains the ability for scoring the action points of the scenario. Tutoring help before and during the scenario with the analysis services after the scenario helps the user to use tools of cyber range and to analyze the users' performance. The purpose of the testing module is to set validated test case definitions and verify executed tests with analysis of the scenario. Scenarios contain selected features, including the lifecycle of created the scenario. The platform's monitoring module increase awareness of the scenario, and it provides statistics of the scenario. Platform's runtime environment module activates scenarios by pre-selected incidents. The data storage module contains parameters for the scenarios which are included with definitions, documentations, rules, and backups. The source code of the platform

can be used as open source with end user license agreement (EULA) which are used for example KYPO cyber range, or platform may use closed code (KYPO 2021). Cyber range platform software has been used in virtualized environment, which might also be used as open-source software.

Cyber range platform might use scalable modules as well as adapts which are needed features to the purpose of the exercise, for example:

- cyber range training is suitable for critical infrastructure because of virtual environment is flexible for use of different designs. For example, energy industry is modernizing its equipment in digital form and case colonial pipeline, USA (Turton and Mehrotra 2021)
- case Vastaamo in Finland introduced vulnerabilities of medical care industry. Cyber exercises for students of medical care will be reality in the future (Harris 2021)
- maritime industry technology (including port and ship industry) will be activated for the cyber training in the future. Electronical equipment in the port and ships are being also modernized which will increase need of digitalization

Cybersecurity exercises in cyber range environment contain planned scenarios, which are meant for testing organizations' preparedness against for selected type of cyber incidents (NCSC-FI 2020). Cyber incidents or disruptions are identified as irregular situations in the operational environment which have an impact on the organization functions. Learning from threats and impacts are an asset. Cyber exercise training for protective methods usually requires to be closed network and reality with resources. Actions during exercise typically contain tasks with device hardening, segmentation, and routing which must be done also in real life. Cyber trainings are meant to help to determine of how and where the authenticated users' networks data is stored and what defensive methods will be used (Kaspersky 2021).

Cyber training for disaster recovery and business continuity is part of the regular training, which includes actions of forensics. Cyber threat is an action enabler for protective countermeasures for cyber-attacks. Virtual training may include indicators which could be related to cybercrime, cyber-attack, and cyberterrorism as a result the attention may be focused on attack phases (kill chains) which includes active reconnaissance and scouting for network vulnerabilities (Kaspersky 2021).

1.7 Design of research

This research was done by interviewing personnel of Xamk and comparing academic research documents and their analysis methods. Theoretical framework of reference and concept included are part of this research study. This study contains six chapters. Chapter one describes the research and gives an introduction for the reader of this study. The second chapter describes used methodology and material in the research. Chapter two includes the research plan, which utilizes an action research approach, and which is also included in the action learning sequence. This research utilizes best practices from other cyber ranges, which also implements qualitative research methods for this study. Chapter three is formed to gather relevant research material for the study. Chapter four contains benchmarks for received information of the study. The fifth chapter describes the proposal of concept for the study. The Sixth chapter represents the results of the study and is the closing chapter for the research. Chapter six also contains conclusions and discussions for the study, including proposals for actions and continuing the research after this study.

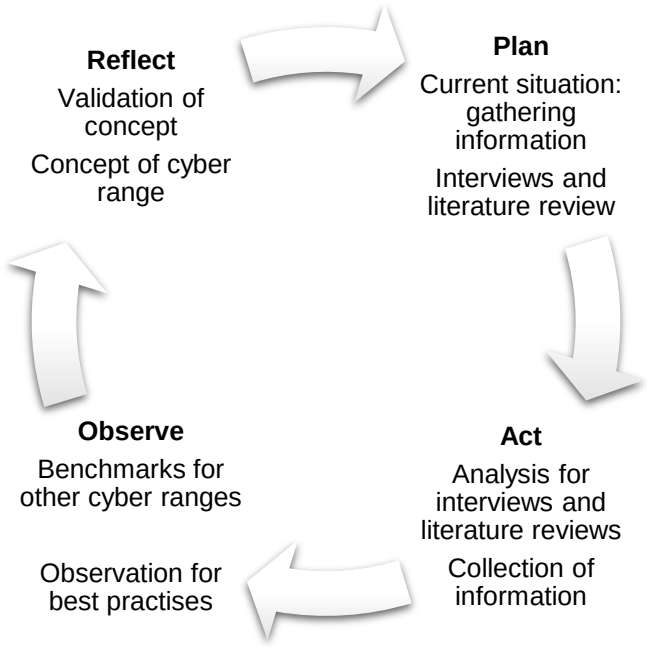


Figure 3. Learning cycle for this study (Watson et al. 2019)

This study follows the pattern of the learning cycle. The study's learning cycle has been described in the figure 3. The learning cycle in figure 3 includes the following steps: 1. Planning is a phase where problems and analysis are identified and defined, and which enable creation of a strategic plan, 2. Acting is a

phase which implements strategic planning, 3. Observing phase refers to evaluation of findings and to detection of the actions in the study with selected research method, 4. Reflecting phase is used for thinking critically past actions, not just planning, evaluation and results. The proposal of concept aims to improve understanding the outcome of research (Zuber-Skerritt & Wood, 2019, 5). Whenever it is needed, the learning cycle procedures can be viewed from the study and learning cycle results can be reflected and verified.

2 OBJECTIVES, METHODS AND MATERIALS FOR RESEARCH

This chapter contains an overview of the study by detailing the research approach and how the interviews were conducted and what was the outcome. Research methods which used in the study are qualitative research methods. Used research methods are based on the need to collect precise information. This study is built on the qualitative research principles, and action research was chosen as a research approach for this study.

2.1 Research approach

The purpose of the thesis was to study which features are most useful for the use of a virtual cyber training platform. According to teachers and staff, Xamk's virtual platform for cybersecurity studies is also suitable for large-scale cyber exercises. From the point of view of the thesis, the best results come from utilizing suitable research methods. The method of qualitative research was chosen as the research method because a lot of information can be found on the topic to be researched, but the materials suitable for Xamk's virtual training environment must be filtered from the available materials. Various studies on virtual cyber training platforms and the technologies used in them have begun to be published around the world. With the help of a qualitative research method, it was possible to collect research materials related to virtual cyber learning environments published around the world, as well as to gather information about other virtual cyber learning environments. The data collected using the qualitative research method formed a data collection that complemented the data collected using the action research method.

In order to ensure the results of the thesis, it was necessary to obtain information about the current Virtual Lab - a virtual training platform used by Xamk, for which an action research method was used. With the help of the action research method research, it was possible to find out the issues related to the use of the current virtual training platform. Questions regarding the maintenance, use, features, and types of exercises currently included in the system were clearly raised. Utilizing the action research method, two rounds of interviews were conducted to gather information about the features related to the virtual training environment. With the help of the action research method, the researcher was able to practice the completed exercises on a virtual cyber training

platform and form a description of the training environment. Combining several research methods provides more information to support the outcome of the thesis.

2.1.1 Qualitative research methodology

Qualitative research (QR) is based on people's experiences to better understand the things that are important to people (Silverman, 2020, 4). QR methodology works around a theoretical frame of reference, whereby scientific research serves as a source of background information. QR methodology complements volume-based research by supplementing missing information and complementing practices and experiences. QR methodology produces credible and accurate descriptions of theoretical insights. With the help of QR methodology, information can be searched in different places and by combining the retrieved information can be converted into knowledge. In addition to qualitative research methods, QR methodology also enables other research methods that support research. Data analysis with the help of QR methodology enables the collection, evaluation, and data definition of data for the evaluation of research results (Silverman, 2020, 8).

2.1.2 Action learning approach

The research was conducted by using the action research approach (AR). AR is used with Action learning (AL). AL was introduced back in the 1940s by Reg Revans in the coalmines of Wales when miners started solving problems themselves without consultants (Zuber-Skerritt & Wood 2019, 19). According to AL, the basic instructions are not enough if the learning is needed, but learning is voluntary. AL is reflecting the experience of action and its results. The learning is coming from each other which includes different kind of problems major, complex, and practical etc. (Zuber-Skerritt & Wood 2019, 4). Questions related to the research concern are required to solve problems. Action must be taken to solve the problem, but it also requires the feedback, which is important for learning experience (Zuber-Skerritt & Wood 2019, 22).

Researchers are examining the beliefs, values and focuses for understanding better the behaviors of other participants (Zuber-Skerritt & Wood 2019, 24). In-

vestors are seeking companies in technology, which are trying to find more effective ways to utilize modern technology, which can be called action research methodology. Action research (AR) build the foundation from the past and notices it in today's environment and foresees it to the future (Zuber-Skerritt & Wood 2019, 87). The differences between AR and AL are learning and research. The research must be organized, exact, verified, and public document (Zuber-Skerritt & Wood 2019, 13).

2.1.3 Action research approach

Action research (AR) was introduced by Kurt Lewin in 1951 and David Kolb was developed the theory further in 1984 and 1985 Curr and Kemmis (Zuber-Skerritt & Wood 2019, 5). AR method gives an assumption that people can create knowledge and learn continuously. With forming through analysis and test concepts in all situations there is possibility to make contribution to create knowledge with ability to create experience and afterwards start process once again. AR contains four variables in cyclic pattern, which are: 1. Plan, 2. Act, 3. Observe and 4. Reflect (Zuber-Skerritt & Wood 2019, 5).

AR method can be used in practical, participative, emancipatory, interpretative, and critical research because its framework is used to improve development of organization (including personal and team) (Zuber-Skerritt & Wood 2019, 3). Action is used to describe actions in the past, to the present and into the future (Zuber-Skerritt & Wood 2019, 4). AR is used for suitable collaborative actions combining both theory and practice. As an AR, the researcher will most likely find AR from academic research (Zuber-Skerritt & Wood 2019, 3).

2.1.4 Relationship between selected research methods

As illustrated in figure 3, this thesis is based on a learning cycle model, which includes planning, action, review, and reflection on the action before starting the perimeter measures again. Chapter 2.3 describes the data collection collected through qualitative research, which has been used in two different interviews using the methods of action research. Additional information obtained through the interviews has been added to the data collection for the analysis phase. The AR method as a whole describes learning, which includes studies published worldwide and Xamk's own virtual cyber training platform and the exercises

used in it. Chapter 5.2 describes the results obtained using the AR method when considering the burden on the participant in the cyber exercise in relation to the benefits of the exercise, which should also be considered in the cyber exercise. Taken as a whole, this thesis includes learning through doing and research, in which case the thesis includes qualitative research, research methods in accordance with AR and AL.

2.2 Timeframe for the research

This study used a qualitative method including action research as the research method. The part one of the study contains illustration of the structure for the research. Part two contains gathering information collection, including interviews. Part three contains literature review and observations of interviews.

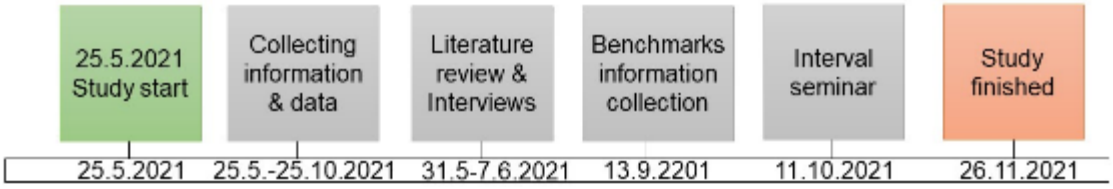


Figure 4. Timeframe for this study

The thesis is divided into different stages according to figure 4:

- start of the study with selecting topic for the study
- phase 1: 31 May - 7 June 2021 collecting information and data. Selecting suitable research methodology.
- phase 2: 8 June 2021 - 28 October 2021 literature review and interviews included in this phase.
- phase 3: 8 June 2021 - 28 October 2021 literature review and observation of collected information
- phase 4: 21 June 2021 - 28 August 2021 literature review and benchmarking
- phase 5: 28 August 2021 - 28 October 2021 additional information collected, and supplementary interviews held
- phase 6: Acceptance of study and seminar

The research process was scheduled by the need of South-Eastern Finland University of Applied Sciences. Study schedule is described in the above figure 4. The study was built in phases, where the first two phases included received idea for the study and was the reason to start building data collection. Phase three consisted of analysis with selected academic research methodology and phase four included research of benchmarks for different cyber range platforms.

Phase five was about to gathering the knowledge for concept of proposal and finalizing the findings. Sixth phase is the last chapter in the study and includes answers to the research question and provides guidance for post-study actions.

2.3 Research question and -objectives

A suitable research question has been formulated for this study, which helped to focus and narrowing the scope in the field of study, and it gives suitable objective for study. The research question limits the scope, so that the research is conducted more effectively. Research question was formed in the beginning after the suitable research topic was given. The research question focus was targeted for maximizing user experience in cyber range platform's cyber exercise, which is the key element for having satisfied customers.

Research question for this study:

What functionalities will be most beneficial for the concept of cyber range?

The study also has four sub-questions which are related to the main research question:

- what are the key functions for the cyber range (maximizing its effects and getting influence)?
- what features are needed to maximize the benefits of the cyber range?
- what are the key resources required for the cyber range?
- what are cyber range training evaluation and measurements of performance?

The purpose of the sub-questions was to give focus on details which may benefit the participant of the cyber exercise and Xamk. The design of the Xamk cyber range will be having its shape when all these questions have their answers. Key functions of the cyber range will help to give the focus on these operational principles which have direct impact for customer experience in the cyber range training. The features of information systems that can be used to implement more automated measures help to save time and resources. The resources for the training are a key element which may have human or financial effect, but without resources there would be lack of knowledge in the cyber

range training. The last but not least, the evaluation of the cyber range cyber exercises. Are they required and if they are then what they would be?

2.4 Data collection and analysis methods

This study's research method utilized data collection for concept of proposal. The data collection was formed by using analysis method called as qualitative analysis method which aimed for background and environment research for understanding the needs, aspects and meaning for research subject. Qualitative research approach included narrative analysis with interviews, observations, and content analysis. Qualitative research approach utilizes both internalizing and learning (Hennink et al. 2020, 10).

Data flow for data collection was formed from academic research literature and information from cyber exercise platforms (cyber range and different platforms) around the world. Information of data collection obtained for the study based on interviews, benchmarks, and observations. Data collection enabled information analyses and forming knowledge for the result of the study. The study was conducted with action research approach which utilizes literature review and interviews with the teachers in the Xamk and with combination of received information of benchmarks it provided concept of proposal for this study.

2.4.1 Interviews of Xamk personnel

Interviews are part of the selected research approach. Interviews are used to gather information for data collection. Teachers and one maintenance person volunteered to answer my questions during the interview period in study phase 2. Academic information search based on results of interviews. The questions for the interview were based on some knowledge on the current Virtual Lab environment. Information received from the interviews gave a holistic view of the current virtual environment and the needed features for the cyber range environment, which were identified during study phase three in observation analysis. Observation phase needed data collection based on gathered information.

Interviews were conducted in two parts and collected information of current Virtual Lab -system and its features. Interviews were an important method to collect required information on current Virtual Lab system and the challenges which new cyber range concept may be encountered during its development process. Contacts for interviews were scheduled on 7 June 2021 and 8 October 2021. The interviews from the teachers showed the need to increase the use of this Virtual Lab system to the cyber range platform. The interviewed persons are using weekly basis this current Virtual Lab system. The outcome of the interviews revealed the current state of the Xamk virtual environment, and it also introduced the Xamk roadmap in the future. The interviews resulted in data that could be used to collect missing information from the current ICT-system. Interviews were scheduled before the literature review and benchmarking, which were done in phase four. Phase five included additional information collection via 2nd interview and the study ends in the phase six which would be acceptance of study and seminar.

2.4.2 Benchmarks of the study

Benchmarks of the study analyzes, compares, and gives holistic view of cyber range documentation and measures from globally used cyber ranges and what they would offer for Xamk and for end users of cyber range. Benchmarks were used as evaluative measurements collected through literature reviews and Internet publications. Literature reviews focused on available features that are used in cyber range environments. Benchmarks included also cyber range -related published guidance from authorities from EU, USA, and Finland.

The inspected benchmarks measured and compared existing Virtual Lab environment's features and existing documentation. This study is all about receiving the latest features and documentation from similar cyber ranges all over the world, with knowledge transfer from the existing platforms for maximizing the usability of Xamk cyber range. Some features of the existing cyber ranges are unique, so copying is not desirable, but instead it makes thinking to "outside the box" how Xamk should develop its unique services with features of its specialties. Eventually, the benchmarks of the study will give the direction for study and the reasonable path to follow and possibility to complete the study as planned.

2.4.3 Analysis session

Analysis for the study required reading the documentation and academic researchers from literature reviews and benchmarks. Collected information was added to data collection which included changeable information in visible form, so it could be processed into knowledge, which is the proposal of the concept. Analysis of the cyber range noticed related guidance from authorities from EU, USA, and Finland. As a result of analysis, the information of literature reviews, interviews were reflected against benchmarks which conducted data collection and enabled the creation of knowledge. After analysis the observation phase was finished, the selection of required information and knowledge was formed for the use of the study.

2.4.4 Observations

Observations gathered input for this study’s concept of proposal. During observations phase, the researcher has used the current Virtual Lab system for evaluation purposes. The purpose of the observation was to determine how the environment is suitable for the usage of cyber range environment specifications. In observation phase, the data analysis was reflected for the experience of evaluation of Virtual Lab use. The findings were carried out by teachers, students, Xamk employees and the researcher's own colleagues for the thesis. Findings were collected for observations to facilitate data analysis.

The purpose of observations helped to collect information about how the Virtual Lab environment works at a moment. Information was needed to support the research in order to get the right kind of information through questions. What kind of measurements cyber range might need for value added features to the participants and customers of the cyber exercises? What kind of user experience researcher got at a moment? Cyber range platform and its virtual scenario types for users might get similarities about customer experience.

3 CYBER TRAINING IN VIRTUAL LAB PLATFORM OF XAMK

This chapter examines how the current virtual lab environment specification of requirements meets the cyber range requirements. The data required for the current state analysis used in this study, as well as the data collection methods, are described in this chapter. A fully functional cyber range environment needs suitable network components with scalable environment and with the latest technical innovations.

3.1 Current Xamk Virtual Lab environment

Xamk's Virtual Lab environment is in the city of Kotka. Virtual Lab environment is separated from other networks, but Virtual Lab is usable through Internet. Virtual Lab offers a virtual environment where it is possible to create an ICT environment with needed components from a scratch. The virtual training environment can be used to simulate network traffic using active network devices (e.g., routers, switches, firewalls) that can also be used to implement network segmentation. The training environment also supports Domain Name System (DNS), Network Time Protocol (NTP), and other services available on the Internet. Currently, about 50% of the virtual platform's capacity is in use.

As shown in figure 5, the first version of the virtual laboratory system (Virtual Lab) was released in early 2016 at Xamk. Following the release, with the popularity of the virtual environment, its performance had to be increased twice, in 2016 and 2017. System upgrades performed during 2017 reduced maintenance costs, but at the same time optimized server performance. Virtual laboratory system upgrades made in 2020 optimized server response time and smoothed out traffic. During 2020-2021, the backend of the servers has been updated and, as the most visible change for users, the time spent booting virtual laboratories has been reduced. During 2021, the user interface has been updated to allow the user to build their own virtual laboratories and, at the same time, the response time of the user interface has been reduced. At a moment, the current redundant architecture model is cost-effective, and its performance is possible to optimize between optimized resources and speed. The last section of figure 5 describes the future and development of the Virtual Lab system.

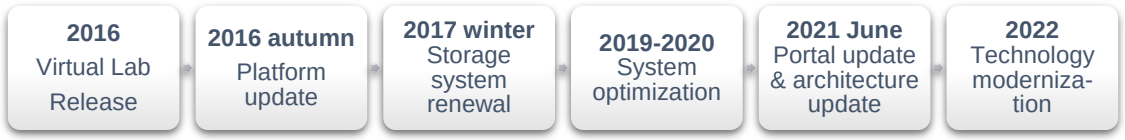


Figure 5. Virtual Lab version history

Although the architecture has been improved and the technology updated over time, the current architecture is based on virtual technology. Currently, Virtual Lab is running with three clusters (n+2), which has five nodes each. User training labs are automatically run with the four least used nodes. Redundancy keeps Virtual Lab running with one cluster. If one node is down, it affects approximately 7.14 % of all virtual labs which are offline. Virtual lab (VLAB) backend collects information from these nodes and sends the information through a portal to the DC Frontend (figure 6). Virtual Lab environment is behind the demilitarized zone (DMZ) which separated the Internet-connections as described in figure 6 below. With Virtual Lab architecture design, the number of running virtual images in laboratory server can be more than a thousand at a same time and there can be hundreds of virtual laboratory instances running at once. The virtual platform architecture model allows the system to be maintained and upgraded without the need for downtime and no maintenance to the end user.

Virtual Lab environment platform capacity is calculated at a moment with estimated of 6124 virtual devices on eight servers on traffic load testing. Testing ensures that the resources required for user-created exercises do not appear as a slowdown in system response time. Virtual Lab will respond users request under 200ms even during in maximum load. Xamk requires response time and minimum bandwidth 10/1-megabit connection with latency with under 100ms, but connection to the Virtual Lab is possible even with mobile connection.

The reliability of the Virtual Lab environment is based on three clusters, which make it possible to implement various maintenance measures and tests on the system, even during live cyber training. A single virtual laboratory instance can be disconnected from the Internet due to maintenance or classified cyber exercises as needed. All data is saved in the storage network, so if the Virtual Lab

environment is down, the cyber exercises and configuration files can be restored (figure 6). If there is need for model in cyber exercise's classified environment and its behavior, then it is possible to erase cyber exercise after the exercise, and it can be confirmed by maintenance. With careful design, the suitable background noise can be generated for an exercise with Internet connection. Student needs to be cautious in laboratories if Internet connection is enabled for outside Virtual Lab for avoiding external incidents and impacts.

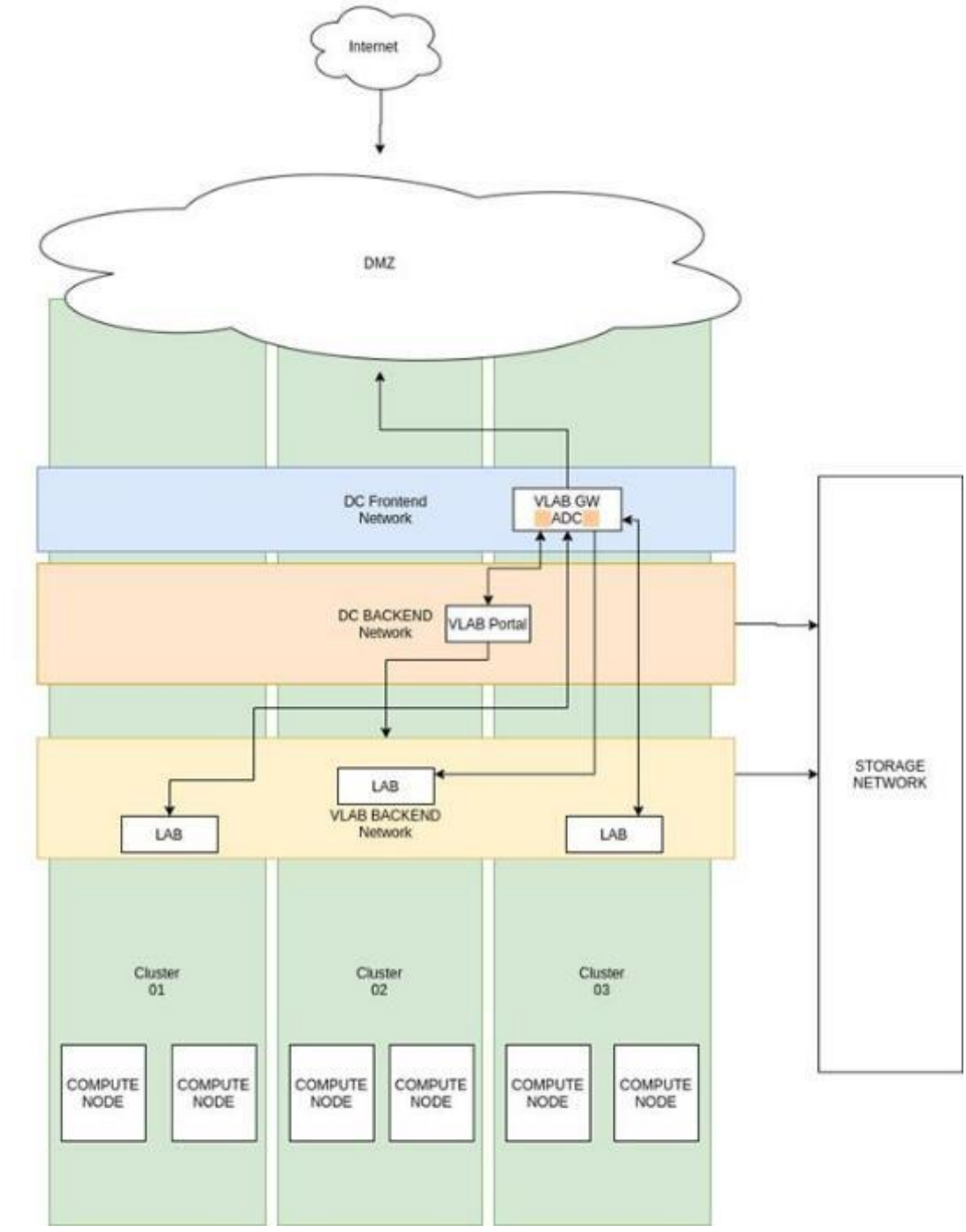


Figure 6. Topology of virtual laboratory (Virtual Lab 2021)

As shown in figure 6 Virtual Lab contains 400 cores but the laboratory limit is currently over 7000 laboratory cores. At a moment there is available about 5.6 TB RAM which will be increased in the future if more memory is needed.

3.2 Measurements used in Virtual Lab system

Technical measurements of the Virtual Lab contain server-side software which allows measuring virtualized hard drives speed, memory usage, chipsets and fan speed and virtual environment current capacity etc. in real time basis. In a training simulation, there are usually measurements to calculate response time and visible actions. If there is offensive simulation in exercise, for example the denial of distributed service attack (DDoS) then the indicators can show the most vulnerable devices on the network. Technical details from Virtual Lab infrastructure are available as tacit knowledge, and these received details can be categorized as a part of measurements. However, no written documentation was shown as evidence during the interviews. This might be a problem in resourcing if employees are determined to change company and there is no knowledge to maintain the infrastructure.

One observation was that the user cannot create an unlimited number of new virtual laboratories in the Virtual Lab system because the functionality has been limited by the administrator. Virtual Lab infrastructure measurements include devices in the infrastructure which are for example CPU usage, memory, fan speed, voltages etc. Virtual pool of Virtual Lab laboratories response time was measured in 2021 (under 1500 milliseconds at all the time) which is not decrease of performance and is not currently related to availability. Development of virtual laboratory utilization trends are also in visible form (running virtual labs and number of devices), and it is started from August 2017. According to figure 7, the amount of active virtual laboratories has increased from year 2017 where starting point is 100 active labs up to the years 2020 where almost 350 active labs are running simultaneously at the same time with over 5000 virtual devices. In the future the amount of running laboratories can be increased which may result with increased amount of memory and processors. However, Virtual Lab system is scalable environment, so basically increasing of performance is no problem, and it can be done whenever it is needed.

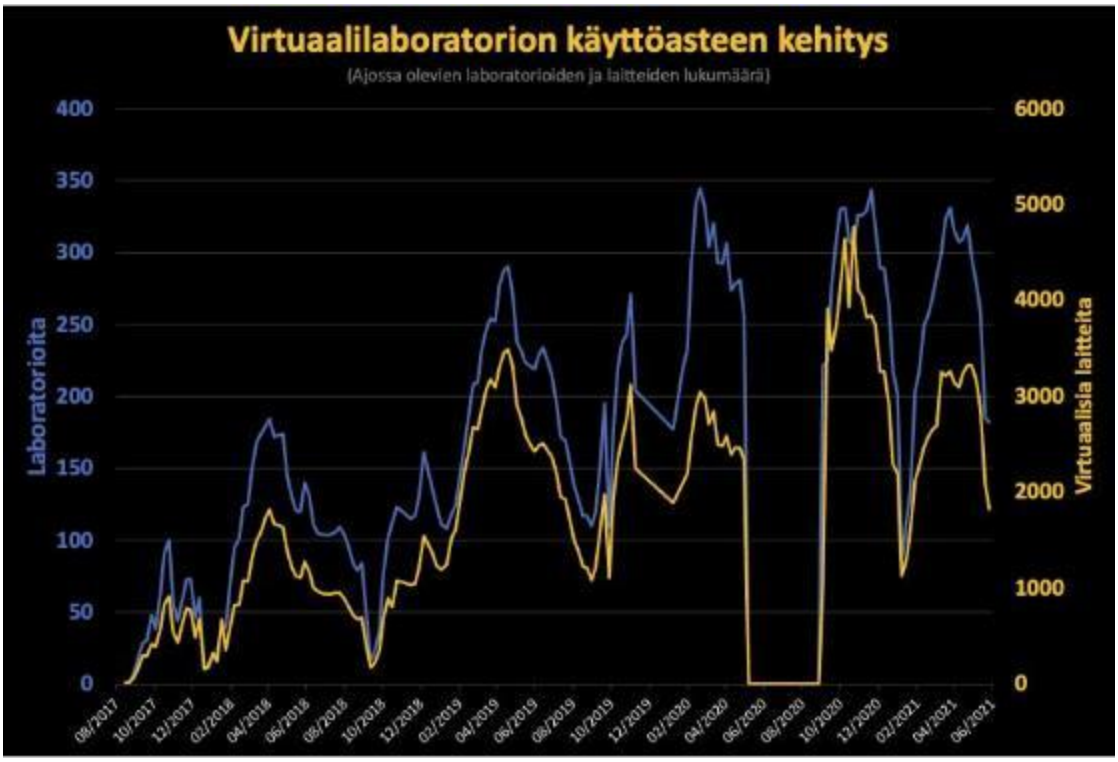


Figure 7. Development of virtual laboratory utilization trends (Virtual Lab, 2021)

As seen in figure 7, the maintenance timeframe is found on a chart in October 2020 chart, when no data is available during the maintenance period. The maintenance period was about two months. Timeframe also shows that Virtual Labs has never actual idle time because there are always at least 20 laboratories running all the time.

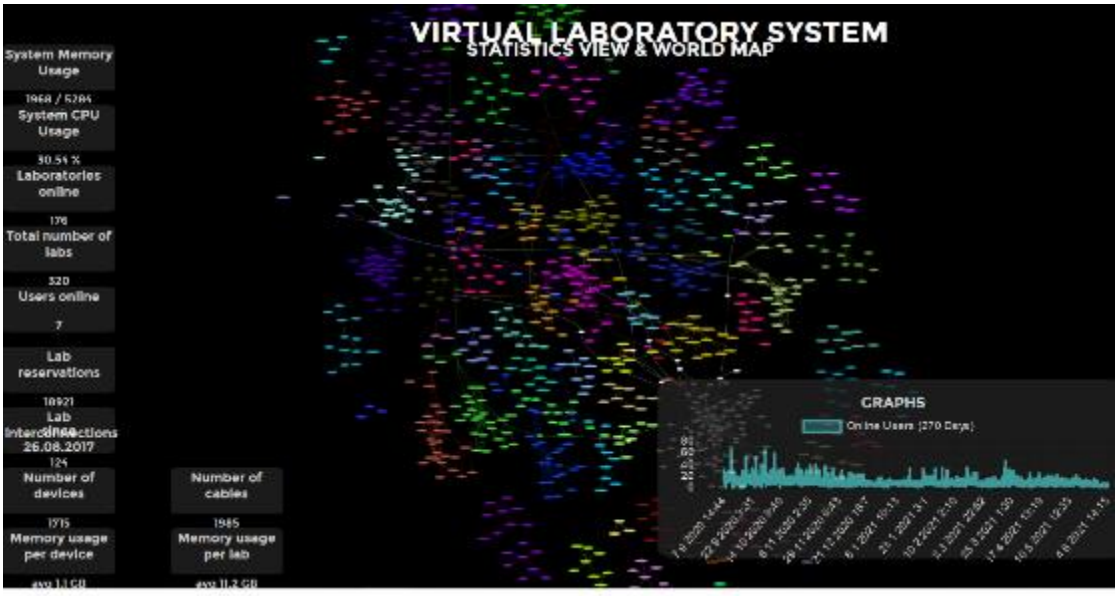


Figure 8. Statistics of Xamk Virtual Lab system (Virtual Lab 2021)

figure 8 shows statistics from the Virtual Lab system. During the observation period the statistics were clarified, and they include system memory usage, system CPU usage, laboratories online, total number of labs, users online, lab reservations, lab connections, number of devices, memory usage per device, number of cables and memory usage per lab etc. The Virtual Lab system provides the administrator with comprehensive features that can be used to monitor the use of the system, e.g., in terms of memory and storage space, so that the system can be expanded if necessary.

3.3 Analysis of interviews

During the study there were two different interviews with the teachers, the first round of interviews included general questions about Virtual Lab and its use in the cybersecurity training program. The second round of interviews included more detailed questions about the platform of the Virtual Lab system, as well as about the changes made to the system itself. The second round of interviews also reviewed future development plans related to the cybersecurity environment. The main result from the interviews is that both Virtual Lab system and Xamk are constantly evolving with the actions around cybersecurity. In the future there will be a new campus built with premises/facilities also for cybersecurity training. After the new building, the space inside the facility is totally increasing 240 square meters with classrooms of blue and red teams.

Virtual Lab system’s exercises are under development, and new components are implemented in cyber exercise projects as soon as an outcome from project called: “a public key infrastructure (PKI-architecture) with best current practices (BCP) private certificate authority (CA) in Virtual Lab system” is finished. Also, the upgrading the Virtual Lab system networks are currently as a project which aims to improve virtualization and automation features in cybersecurity laboratories with new ICT system inside Virtual Lab system.

The planning stage has also Kubernetes cluster pipeline training, which is meant to increase in a way more defensive content for Virtual Lab system in the future. The services provided by the Virtual Lab system will be enhanced in the form of a template that includes cyber exercises and modeling of various vulnerabilities. Artificial intelligence from system side is also planned to implement

to the cyber exercises with as hidden software robot which aims for hacking students running virtual lab exercise during training. The development of the Virtual Lab system allows students to come up with new ideas and more varied exercises to strengthen their own skills. Teachers, students, and the administrators of the virtual system enable the continuous development of the system with their own work. The interviews in the study gathered information on how the current virtual system has been built, maintained, and updated. The focus of the interviews was on reviewing partly undocumented features which were meant to measure the existing features of the Virtual Lab system. The teachers and personnel who were interviewed were proud of the current Virtual Lab system and tried to prove that the system is sufficient for cyber range activities such as cyber training. According to interviewed personnel, only the imagination sets limits for Virtual Lab system scenarios. CTF competitions may require different laboratories for offensive and defensive actions. CTF-competitions can use two or more laboratories, and laboratories can be connected together. The Virtual Lab system can be used in cyber exercises so that trainees can be divided into groups in different physical spaces, or even participate in the exercise remotely. Interviews revealed that Xamk's Virtual Lab teacher ID’s can be used to track cyber practice (white/purple team). There are currently no known technical limitations in the amount of signed people in Virtual Lab system for one scenario. The busiest time for usage of Virtual Lab is between autumn and spring, when students use the system and are participating in the actual schoolwork.

In the interviews, it was shown that Virtual Lab system is updated whenever it is necessary. There are also current development processes on going in the system which may see the result of improved user experience in the future. The future brings also more documentation for the use of Virtual Lab system, which also includes documentation of cyber exercises and cyber range full live actions. When the Virtual Lab systems cyber exercises increase the amount of training, it will also bring development of communication tools inside the scenarios blue- and red team battles. For the future, development process also enables possibility to connect another cyber range platform for joining even bigger battles.

At a moment, Xamk does not advertise actively cyber exercises in their webpages, so booking up for cyber training is possible only through the director

of the cybersecurity degree program. There are possibilities in future to provide official cyber exercises and trainings for customers outside the Xamk. Currently, it is possible to book penetration testing and the possibility will remain in the future. Although little cybersecurity training is currently offered to outsiders, the situation is different for school students. Students can choose cybersecurity studies for their elective studies. The cybersecurity training program is one of the most popular programs at Xamk.

3.4 Cyber range and knowledge management

Virtual cyber exercises are required for preparation and maintaining the skills for the requirements of organization. The needs of the participants are based on ICT-infrastructure requirements with selected cyber maturity level, figure 9 describes how in the cyber exercises the participant will learn with different ways during exercise.

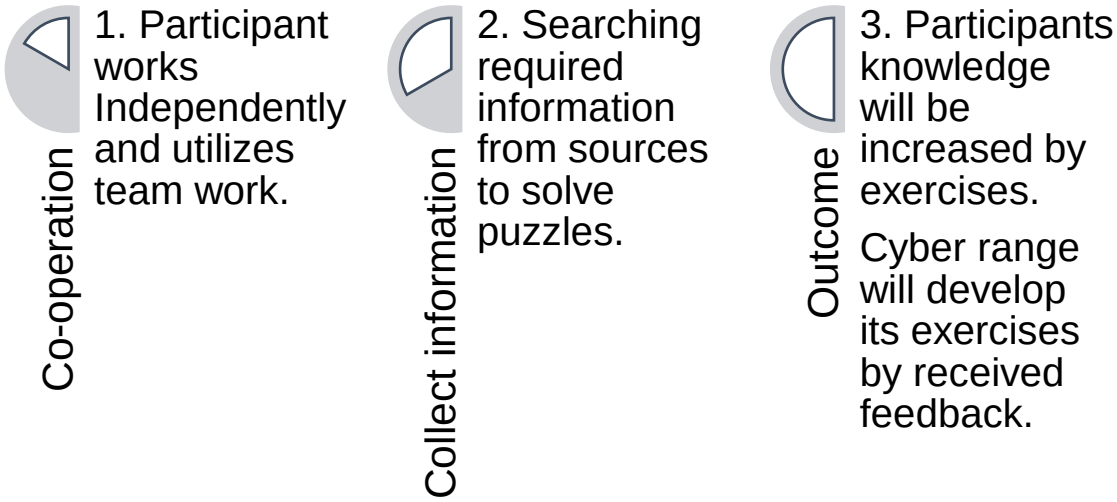


Figure 9. Outcome of cyber range exercises

As presented in figure 9, the reason to participate in cyber exercises is to develop individual and group skills by cyber scenarios. At the same time, cyber range platform will develop its virtual environment by received feedback. During the cyber exercise, the participants have the possibility to work individually or utilize teamwork. Participants can also search required information from cyber

range instructions or from Internet to solve scenarios. As an outcome, the exercises will increase participant's knowledge of how to handle incidents shown in the scenarios.

3.5 Knowledge management for cyber range

Cyber exercises and training provide new information and efficiency for organization level and encourages teams thinking universally "out-of-the-box". Learning to think outside the box provides knowledge as outcome and increase the organization's cyber maturity level and level of knowledge management when from data flow can be identified as the valuable information. Knowledge management (KM) is needed to transform information for training exercises and make transition to the knowledge for participants. KM can be considered as a value formed as a result of the activities of persons participating in cyber exercises. KM can be built in groups by sharing information between individuals. Sharing the information helps individual learning from received information, which aims for creation of knowledge. KM is created by individuals and no organization can create knowledge without people (Jakubik 2007). By gathering information, the received data is needed to process collected information. Collected information forms knowledge, and knowledge shapes itself to wisdom. In the so-called SECI-model, the lifecycle of information is evaluated and described, which can give a more holistic view of how knowledge is created from cyber exercises.

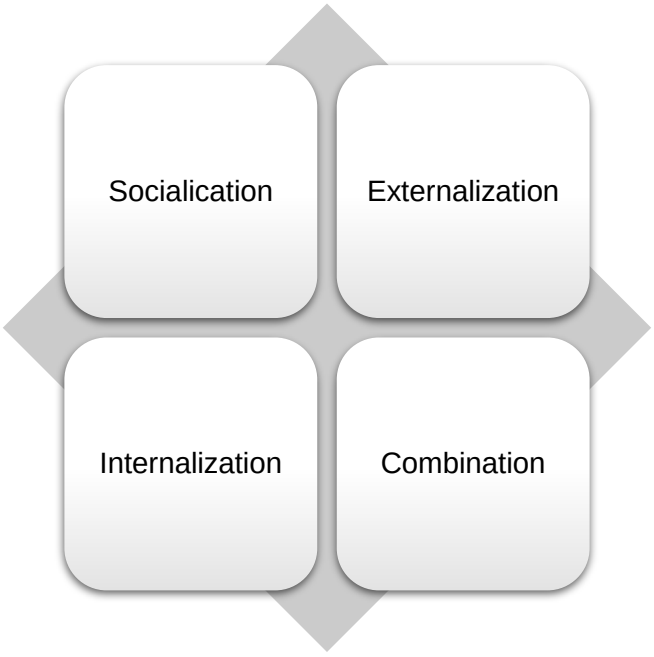


Figure 10. SECI-model (Nonaka and Takeuchi 1995)

figure 10 presents Nonaka-Takeuchi model, which was created in 1990, and it describes layers of knowledge and model explains creation from tacit and explicit knowledge to the organizational knowledge. In the cyber ranges, the knowledge is formed similar ways by the exercises (Nonaka and Takeuchi, 1995). From the Nonaka-Takeuchi created model there has been developed detailed model also for cyber exercise practices, which is described in the figure 11.

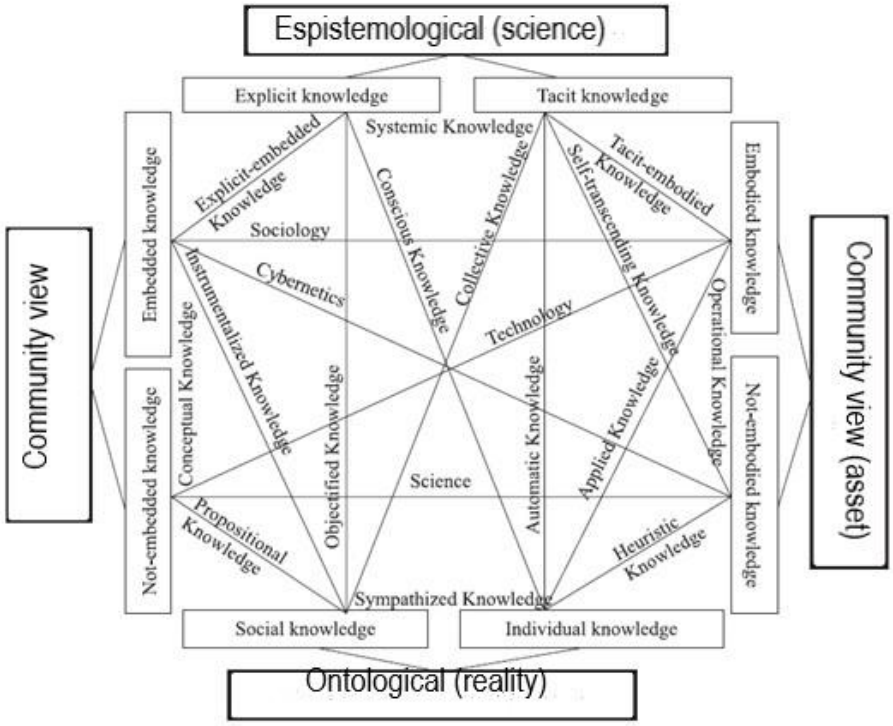


Figure 11. Model for knowledge shaping (Jakubik 2007, 7)

Figure 11 show the model of knowledge creation. The SECI definition published by Nonaka and Takeuchi in 1995 has been interpreted in more detail, clarifying the relationships between segments and the information they contain. Knowledge management explores different kind of knowledge, showing their relationship to each other. For example, when individuals are sharing ideas (tacit knowledge) and stories with others (embedded knowledge), it will help solve conflicts and enable learning in action, which starts creation of knowledge (Jakubik 2007, 7).

3.6 Observations for cyber range

Gathering information is one of the most important ways to gain a holistic view of the best practices of other cyber training centers. Data collection activities improve the targeting of cyber practice and virtual training can improve cyber

performance. The high-quality content of cyber exercises and the services provided by the virtual cyber training platform can provide students and customers with the opportunity to learn cybersecurity.

In addition to cyber training, the Cyber range platform can also be used to test various devices. In the USA, for example, there was a project in 2008 which was funded by the U.S. Department of Defense (DoD), and which was aiming at testing virtual cybersecurity testing capability (VCSTC). The project contained testing of network security devices with using virtualization technology without physical network infrastructure (Pederson et al. 2008). The Virtual Lab system enables testing and training of various network components and software, for example, in terms of configuration.

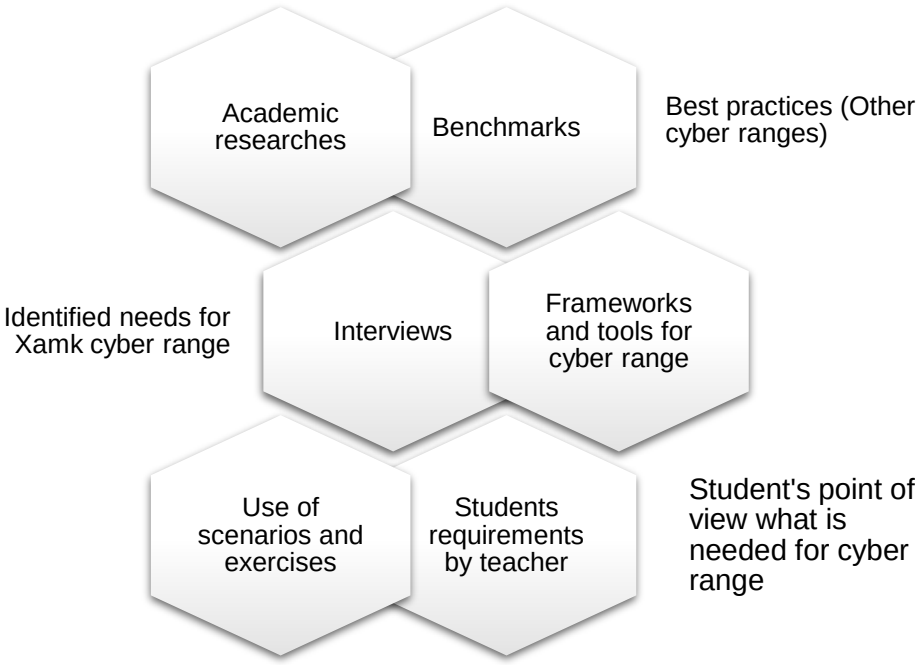


Figure 12. Observations – for the concept of cyber range

As figure 12 illustrates, the observations are focusing identified needs of Xamk cyber range which are found from academic research, benchmarks, interviews, and cyber range related documentation. In the literature review, studies revealed that resources are a key element for developing cyber range platform. The cyber range platform is tested during study writing. Resources might contain human or financial factor in implementation phase. When all elements are in place, it is time for marketing and advertising Xamk cyber range.

3.7 Analysis – summary

As a summary, the current Virtual Lab system technical environment seems to have suitable capacity for running in the cyber range, cyber platform virtual exercises. During the summer of 2021 the Virtual Lab environment contained 92 different laboratories, which contained also test environments. Many of those laboratories has limited lifecycle, so the number of active laboratories will constantly be changing, which is one main functionality in the cyber range platform. In literature review was noticed that recently has published quite many research studies which has examined different cyber range platforms functionalities. Most of the studies highlighted functional cyber ranges basic functionalities which are identified as a key element. A challenge for future in cyber ranges all over the world is that cyber range platforms should have capability to have for example federated network for another cyber range platform, which could enable potentiality to generate crossover cyber exercises between cyber range platforms.

4 BENCHMARKS AND BEST PRACTISES FOR CYBER RANGE ENVIRONMENT

This chapter benchmarks designs of cyber ranges and their frameworks related to training of cybersecurity. Virtual cyber training platforms are used for training due to their flexibility as well as ease of use. Virtual platforms take advantage of a variety of standards, ease-of-use tools, and other innovations that revitalize the virtual training environment cost-effectively. Best practices for this study contain frameworks and tools for setting up cyber range platform and helps in cyber scenarios and exercises.

4.1 Best practices for cyber ranges - frameworks

Researchers have published studies which are evaluated frameworks and tools used in cyber range scenarios and exercises. Cyber ranges use threat modelling, virtualization, and communication in its extensive use, which enable suitable scoping in virtual scenarios and exercises (Jiang et al. 2020, 6). There are published different frameworks, tools, and best practices, which can guide for using threats, tools, resources, scenario types and other cybersecurity related as best practices for cyber range.

For cyber exercises, there is a published literature describing scenarios implemented using a virtual cyber exercise platform. These descriptions constitute best practices for designing virtual exercises. One of the well-known publishers is the National Institute of Standards and Technology (NIST), whose publications contain extensive descriptions of cyber practice. It includes research data where the best practices are possible to find. National Initiative for Cybersecurity Education (NICE) has prepared the cyber range: “A Guidance document for the use cases, features and type of cyber ranges in cybersecurity education”, which was still draft version in 2021 (NIST 2021).

Virtual training platforms can be used to build realistic cyber exercises with the virtualized devices actually used in the organization. To make successful cyber range scenarios, the virtual environment needs to replicate with required activities from the organization’s network (Fieldeffect 2021). In a cyber exercise, the events written in the scenario may be routine repetitive activities (e.g., opening e-mails and attachments or using network resources), or the incident may be a

one-time critical event (Poudel 2021). Scenarios need to include training goals which makes cyber practice interesting from the perspective of the participant. Exercises and drills are focused on improving specific skills, which needs to be measurable for tracking skill development (Fieldeffect 2021). Scenarios' story-line is required to follow current real-world cybersecurity incidents and emerging attack techniques, which helps in creating scenarios and prepares participants of exercise for current issues (Fieldeffect 2021).

Creating cyber exercises should be easy, as the number of devices in one exercise can reach tens and may require activation and configuration or system hardening. Cyber ranges use modular structure (ability to duplicate- and import scenarios and easily create coursework) and content which may be easily modified for different kind of scenarios for changed purposes (courses, assessments, capture-the-flag, full team-based scenarios) so the scenarios can be started quickly on demand (Fieldeffect 2021). Exercises need to be effective, and there need to be visibility of the progress for to gauge effectiveness of the training. Exercises might contain milestones and participants can advance the exercise whenever participants want with detailed track of progress (Fieldeffect 2021). The visibility of exercise means that there need to be insight where the difficulties are during the training and ability to engage with assistance when it is needed. Creating a cyber exercise also has its own challenges. In connection with the creation of a cyber exercise, the training environment must also be secured by hardening the virtual devices used in the exercise against unauthorized use. It is also important to prevent data from leaking out of the training environment during a cyber exercise (Toderick et al. 2021). Exercises require resources from the planning to the post-training, which requires among other instructors and observers who can monitor training and deliver real-time assistance to activate learning experience (Fieldeffect 2021). The scenarios of cyber range are often built from real incidents and with real work environment. Testing the devices is also common as cyber exercise, which are needed to be tested before rollout to the production environment. After the cyber range exercises provides feedback about the current scenario and incident handling.

4.2 Guidelines and frameworks for cyber range actions

European Cybersecurity organization (ECSO) has published document for working group 5 (WG5) which is titled as “understanding cyber ranges: From Hype to Reality”. SWG 5.1, March 2020 (ECSO 2020c). Cyber range environments and technical exercises document describes cyber as a separate military domain and defines cyber range and used technologies (ECSO 2020c). ECSO has described cloud technology as an asset for scalability. All the scenarios and exercises may require roles and responsibilities. National Initiative for Cybersecurity education (NICE) Framework has been published document NIST Special publication 800-181. NICE framework is nationally (USA) concentrated on developing organization’s cybersecurity related work. NICE framework includes cybersecurity functions including areas of specialties with work roles (Stein et al. 2017). NICE framework is a fundamental reference for describing and sharing information and resources about cybersecurity. The framework describes work roles and how they are performing (Stein et al. 2017). Performance workforce was described with roles of work, knowledge, tasks, skills, and abilities (KSA) with 50 work roles which are commonly used and provides capability indicators for each work roles in NICE framework. Continuous learning and development need indicators based on the level of education as well as experience. The indicators to be monitored may include pre-defined indicators (Stein et al. 2017). Capability indicators are 1. Education 2. Training 3. Experiential learning 4. Continuous learning 5. Credentials/Certification 6. Entry to work 7. Intermediate learning 8. Advanced learning. These indicators can be presented according to figure 13 according to four different categories.

Figure 13 shows that capability indications include four different parts: 1. Selection and recruitment, which contains recruitment strategies and plans for resourcing. 2. Development of employee of identifying needed training and cybersecurity skills 3. Succession planning with identifying leadership skill sets including employee retention 4. Workforce planning with benchmarking capabilities and identifying skill gaps (Stein et al. 2017, 10). Cyber ranges may also require specialization for certain types of functionalities, for example industrial control systems (ICS).

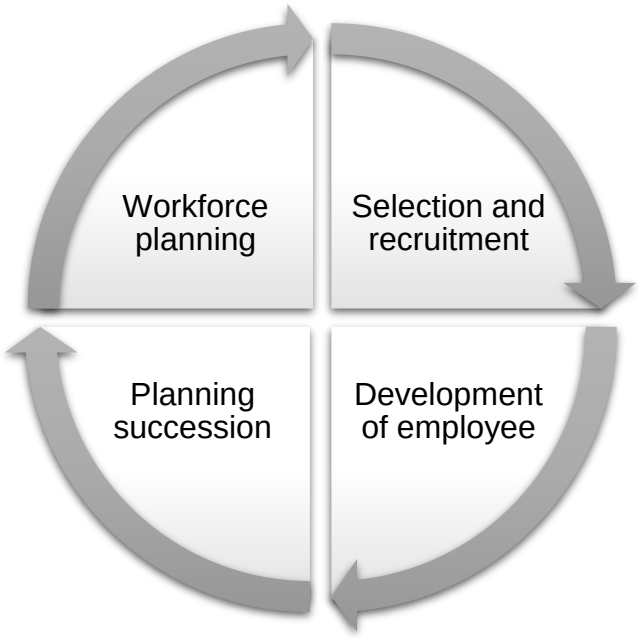


Figure 13. Capability indications (Stein et al. 2017, 10)

NIST has published a guide to industrial control systems (ICS) security. NIST has released public documentation of titled as: “Guide to Industrial Control Systems security” for supervisory control and data acquisition (SCADA) systems in 2015 (Stouffer et al. 2015). ICS are used by different kind of electric-, automotive-, water-, transportation-, chemical-, pulp-, paper- and energy (oil, gas, nuclear) industries. ICS are controlling scattered assets using controlled data flow. Distributed control systems (DCS) are controlling closed network by using supervisory and regulatory control (Stouffer et al. 2015, 10). ICS-systems are built in physically secured areas and are closed environments. Differences between ICT- and ICS systems from information processing systems are in logic execution processes. ICS systems related threats are related to terrorist groups, insiders, intruders, and accidents.

Possible ICS system incidents are listed below (Stouffer et al. 2015, 11):

- ICS network information flow is blocked or delayed (disrupt ICS operation)
- ICS component damage or impact by unauthorized changes (instructions, commands alarm thresholds)
- ICS network operator receiving inaccurate information by disguised unauthorized changes or operator’s initiate inappropriate actions which cause negative effects
- modification of ICS component configuration
- infection of ICS software with malware
- interference with ICS equipment protection system
- interference of operation of safety systems

Security objectives included to ICS (Stouffer et al. 2015, 11):

- ICS network logical access restrictions
- ICS network and device physical access restrictions
- exploitation prevention to ICS-components
- unauthorized data modification restrictions
- event and incident logging activity
- adverse conditions handling by maintenance (defense-in-depth)
- processes for incidents; system recovery

Jason Kick published with Mitre in 2014 a publication titled as “Cyber exercise playbook” which describes cyber exercise as a process model and its contents with terminology. In the cyber scenarios and exercises, the planning phase is most important because the objectives of the training with exercise outcome must be selected carefully (Kick 2014). The cyber exercise playbook describes three different types of exercises: 1. Tabletop 2. Hybrid and 3. Full live (Kick 2014, 9). The tabletop exercise contains a scripted storyline, and it is possible to execute with paper and discussion. Hybrid type exercise include also virtual platform exercises, and it is more realistic. The full live exercise is done completely in virtual platform and typically its planning phase is longer (even 12 months) and large number of participants are involved in the exercise. All exercises include objectives, lesson learned and future (Kick 2014, 9).

Mitre Att&ck (“Adversial Tactics, Techniques and Common Knowledge”) is a knowledge base which is using adversary tactics and techniques based in real-world simulations. The Att&ck- and D3fend knowledge bases are used for development of threat models and methodologies. Mitre Att&ck and D3fend are both knowledge bases which provide more information about methodologies of attacker’s and defender’s side in the network. The knowledge bases will help to focus on certain assets during cyber scenarios and exercises. Mitre frameworks has included kill chains, which makes possible diverse into sequences of attack and defend, which are described figure below. Att&ck provides a tool including methods for attack and counter measures (defense) with tactics for offensive actions in the network. Mitre’s Att&ck matrix contains 14 categories and stages of attack. Att&ck has three levels (tactics, techniques, and procedures) as described in the figure 14 (Mitre 2021).

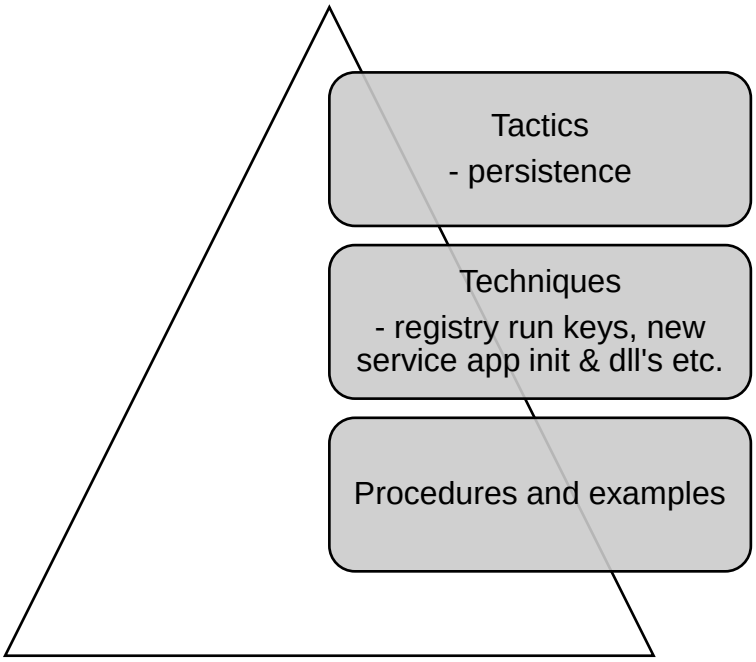
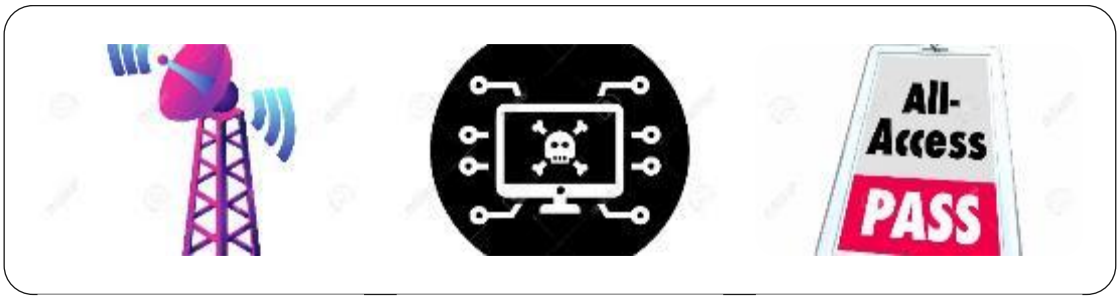


Figure 14. Mitre Att&ck and d3fend overall topology (Exabeam 2020)

As shown in figure 14, developing, and maintaining tactics may require change and perseverance, as cyber-attacks are constantly evolving. Maintaining a variety of offensive and defensive techniques is important to keep the attack area to a minimum. Procedures and various examples must be tested and found to be secure in order to keep the attack options used by a potential attacker limited. Figure 14 is generally suitable for defensive measures.



Pre-attack
- Reconnaissance
- Target selection
- Inform. Gathering
- Weakness identification
- Adversary OPSEC.
- Personal development
- Build capabilities
- Stage capabilities

Att&ck enterprise
- Deliver
- Exploit
- Control
- Execute
- Maintain

Post-attack
- Initial access
- Execution
- Defense evasion
- Credential access
- Discovery
- Lateral movement
- Command & Control

Figure 15. Mitre Att&ck functions (Exabeam 2020)

As shown in figure 15, the attack can be divided into three different phases. Before the attack, information is collected about the target and vulnerabilities and vulnerabilities in the systems are sought. The attack exploits detected vulnerabilities and attempts to remotely gain control over the target systems. After the attack, an attempt is made to gain access to other systems and to maintain contact with the command servers. Mitre Att&ck kill chain is approximate which is containing steps for pre-attack phase (reconnaissance, weaponize) and attack phase steps (deliver, exploit, control, execute, maintain) as described in the figure 15. Mitre Att&ck is based on blue team purpose as protecting internal networks. Mitre Att&ck is concentrating on three phases (Mitre 2021): Pre-attack, attack and post attack which provide together end-to-end adversary attacks. Mitre Att&ck is used for discovering analytic covering and defense gaps in internal networks and an adversary emulation playbook for red teams. Mitre Att&ck is used also to help companies to meet detection requirements for audits and security purposes. This knowledge base is open and available to any person or organization for use (Mitre 2021). Defenders of the blue team need knowledge, which is available from knowledge base d3fend, and it's including the assets. Commonly, the blue team must know also attack knowledge base, as described in figure 16.

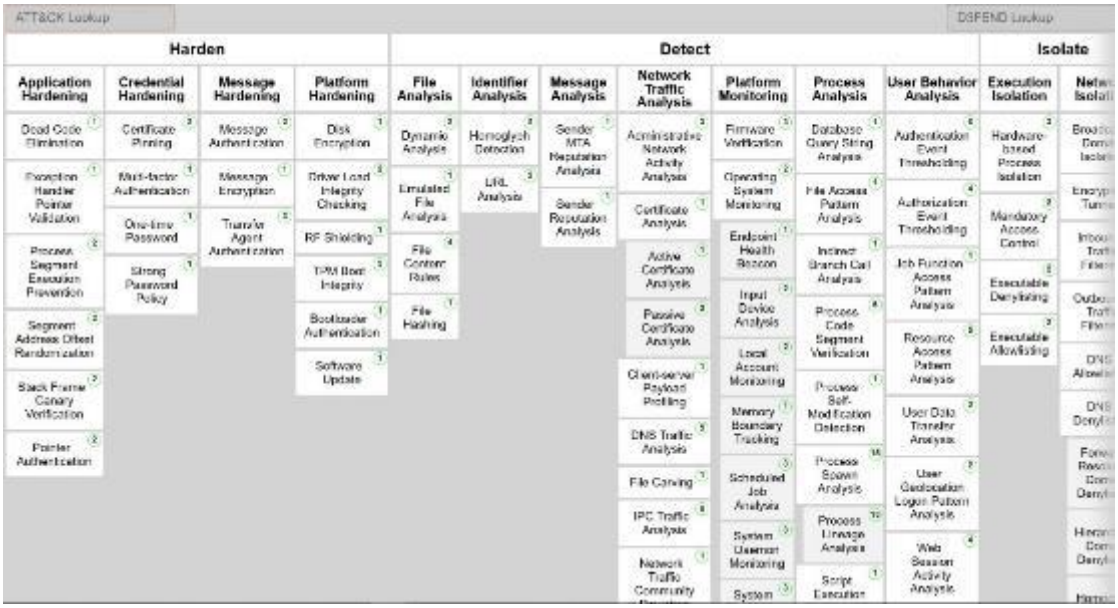


Figure 16. Mitre Att&ck and d3fend Model (Mitre 2021)

As presented in figure 16, the Att&ck and d3fend knowledge bases will show actions and counter measures any known attack methods with defensive actions, which may help defensive actions in exercise. The functions illustrated in

figure 16 are divided into the tasks of the attacker and the defender. The tasks are divided into hardening, detection, and isolation measures. Cyber range exercises may have involved web applications or Internet related actions with objectives, which may need to have information about known vulnerabilities and issues with network devices.

The open web application security project (OWASP) is a foundation which maintain community that is focused on fixing software-based vulnerabilities and is founded in 2001 by Mark Curphey and Dennis Groves (OWASP 2021). OWASP releases annually TOP 10 application security risks, which is based on popularity of globally used vulnerabilities. Web applications are used for collecting information, interactions, e-commerce, and services uses web applications as an interface (Abdullah 2020). Web application can deliver public or non-public information. At the same time, the attack against web applications has been increased to find vulnerabilities and stealing information. OWASP Zed Attack Proxy is one of the OWASP's active projects which provides testing against buggy web application (bWAPP) and "damn vulnerable web application" (DVWA) (Abdullah, 2020).

The knowledge of offensive team tools will help defender to found suitable protection against offensive actions. One of the known tool sets for red team is Cobalt strike, which is threat emulation software. Cobalt strike is created by Raphael Mudge in 2012 and software sends out beacons which can detect network vulnerabilities (Cobalt strike 2012). Cobalt Strike is a tool which includes software for emulation threats. Cobalt Strike includes tools for reconnaissance post exploitation, covert communication, attack packages, spear phishing and browser pivoting. Cobalt strike's community also supports communication, and Cobalt strike's reports provides a timeline and a list of red team indicators. Cobalt strike is included in the categories of Mitre models.

In 2020 Cobalt strike source code leaked, which resulted in the use of Cobalt strike as malware campaigns, for example in ransomware (Osborne 2021). Cobalt strike has become popular and is used in many malware campaigns. Cobalt strike utilizes two methods as avoiding detection: 1. Obfuscates the shell code

2. Leverages a domain-specific language Malleable C&C (Buber 2020). For Cobalt strike campaign identification, the network traffic, and the frequency of the communications to destination/target must be analyzed (Buber 2020).

4.3 Technical tools for cyber range environment

Cyber range platforms are virtual environments which usually have modular structure. Cyber ranges may include support for different technical tools, which could contain commercial products or open source-based software. As for a technical example, the company called Sandia National Laboratories (SNL) has developed an open-source emulation and analysis tool (emulytics) which is targeted to launch and maintain virtual machines in a cyber range (Raybourn et al. 2018). This cyber range environment called “Cyber Scorpion” introduced proof of concept which provided “zero-entry” exercises: network forensics, social engineering, penetration testing and reverse engineering (Raybourn et al. 2018).

RHEA group has introduced “cyber integration, test and evaluation framework” (CITEF) – cyber range platform. CITEF platform is possible to enable emulation of realistic environments for testing, planning, and training purposes. CITEF supports cybersecurity frameworks such as NIST cybersecurity framework, document identifications as NIST SP800-53, NIST SP 800-82 and NERC CIP. CITEF includes critical infrastructure simulation included with SCADA, ICS, and Internet of things (IoT) (Rheagroup 2021). Figure 17 shows a network image of the topology of the CITEF network.

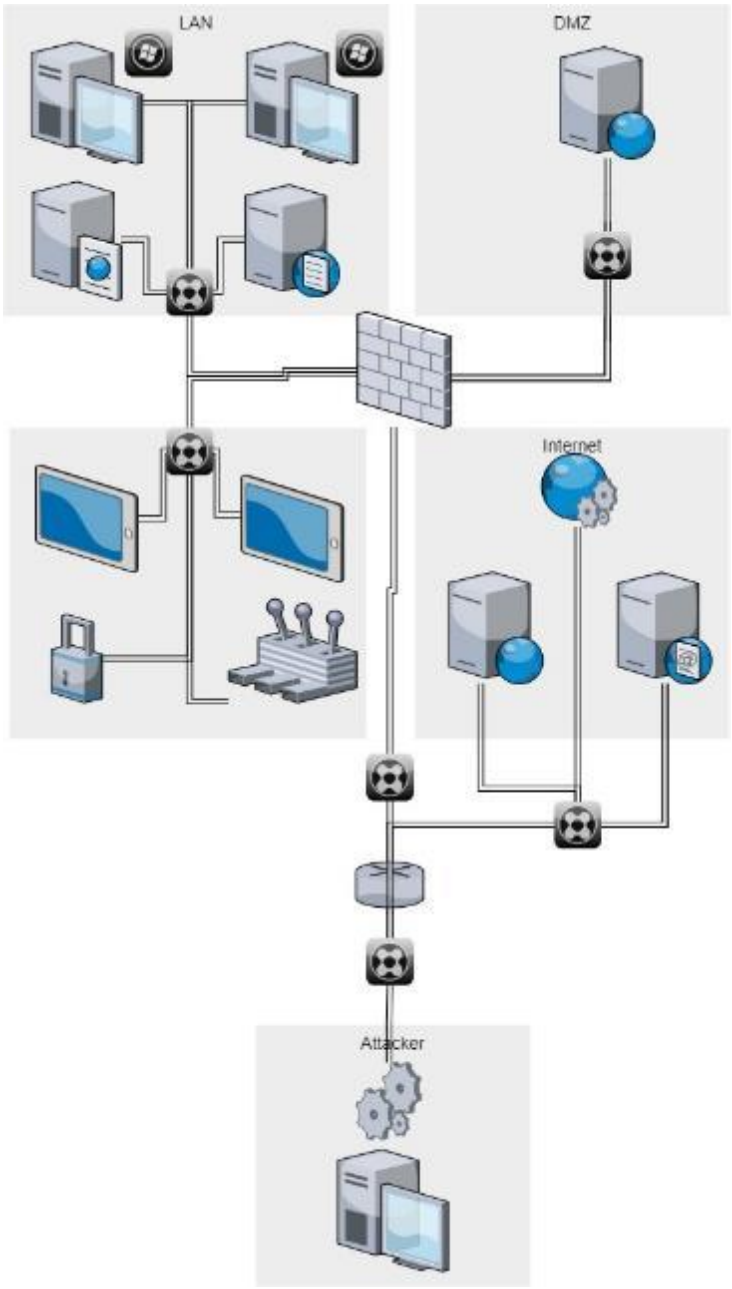


Figure 17. Topology example of CITEF cyber range services (Rheagroup 2021)

Figure 17 shows a CITEF topology model which is adaptable for specific scenarios which may be constructed against a realistic model. There are also systems which uses some automated features. Raytheon is marketing “Cyber reasoning systems” (CRS) which aims for automated searching abilities with discovery of vulnerabilities in binary code. It also contains protection of the system. CRS uses machine learning and other AI technologies, which aims offensive skills of the system. Main components in the CRS are 1. Fuzzing 2. Analyze 3. Update, 4. Patch and 5. Update.

Fuzzing means that the system is overloaded with random data until it goes down. Then the system will analyze the crash and is observing coding errors and vulnerabilities from code. After analyzing system is comparing vulnerabilities against known issues. After check functionality, the system is automatically patching the found vulnerabilities. After patch functionality, the update functionality adds information for its databases for learning (Avgerinos et al. 2018). Cyber range modules might contain also artificial intelligence (AI) for actions when automation is required to reduce need of resources. ECSO working group 6 has been researched AI benefits and challenges in their study (ECSO 2020b).

The Lincoln adaptable real-time information assurance test bed (LARIAT) is an addition for testing environment for evaluation of intrusion detection procedures (Rossey et al. 2002). LARIAT provides methods for cyber range red team offensive actions by generating background user traffic with real network attacks. LARIAT attack scenarios contain individual attack components, which may exploit, scans or deliver payloads (Rossey et al. 2002). As described in the figure 18 below, the attack usually is started with network scanning and then proceeds to the compromising host by exploitation.

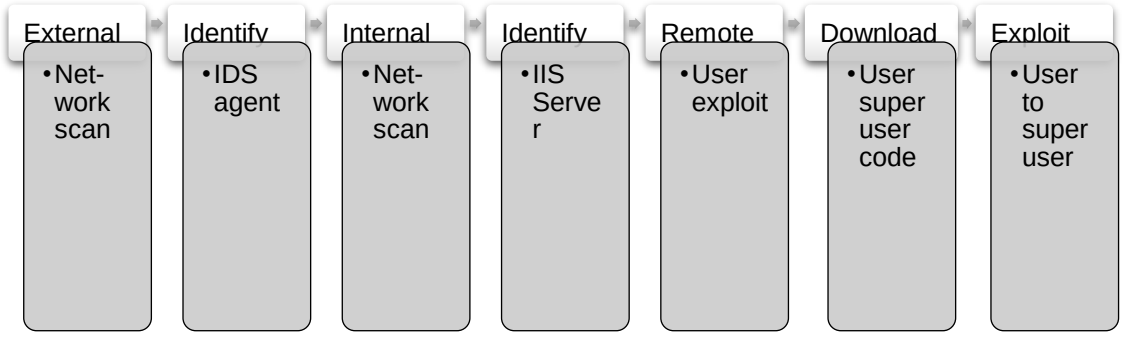


Figure 18. Attack scenario using lariat attack model (Rossey et al. 2002, 5)

LARIAT in the attack pattern as shown in figure 18 storage maintains real-time information in XML based knowledge base, which informs remote attacking hosts to launch attacks and checks that attack was applied successfully (Rossey et al. 2002). Knowledge bases maintain scenario-based information.

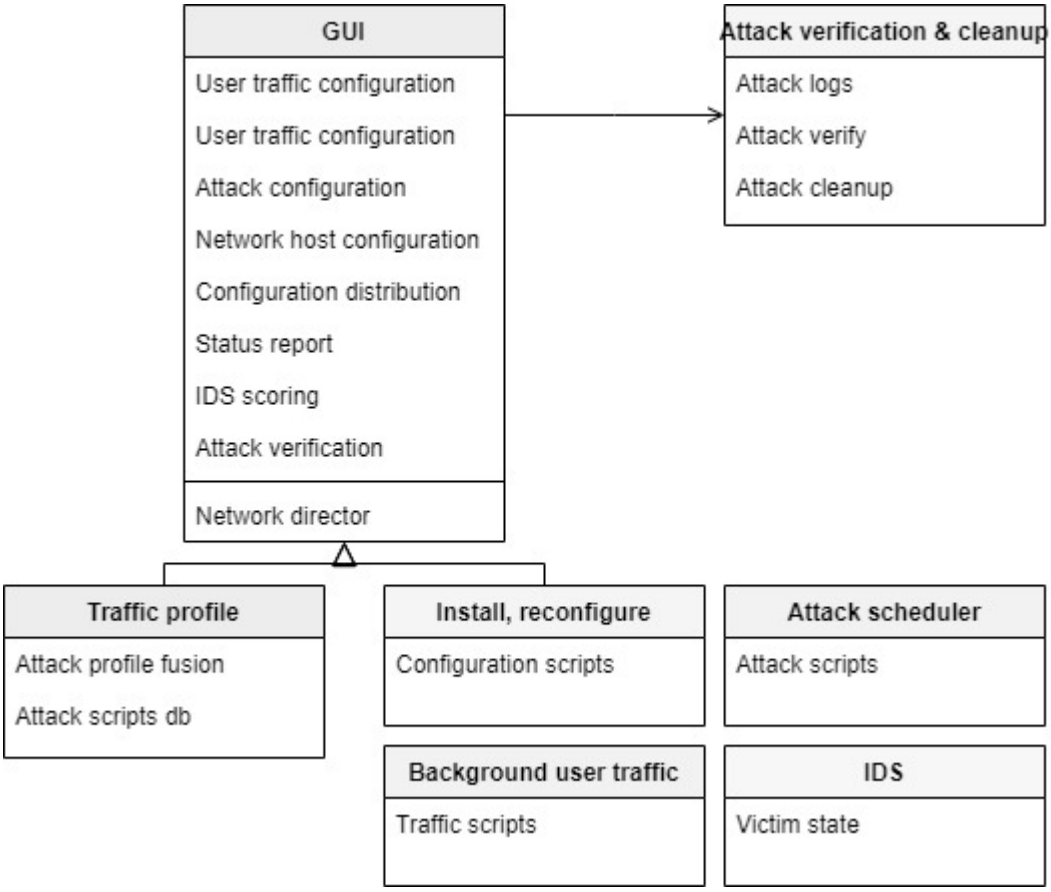


Figure 19. Software components of VulnerVAN (Rossey et al. 2002, 5)

Figure 19 shows the software components of VulnerVAN. VulnerVAN consists of an interface that controls the components associated with the attack. The user interface confirms the attack and returns to the initial state after the exercise. The user interface also controls background traffic, application installations, attack scheduling, and network traffic detection. The name of the tool for creating cyber scenarios for networks is called a vulnerable network generation tool (VulnerVAN). VulnerVAN tool can be used for the understanding the phases of cyber-attack (Venkatesan et al. 2019). In cyber range virtual scenarios, the red team may utilize the tool in offensive action automation. Vulnervan environment contains user input in the scenario description and describes attack sequence which are using attack step library for attack generation. Virtual machines generate attack sequence which may also involve network components. Attack orchestrator coordinates desired attack model and draw sequence diagram as shown in figure 20.

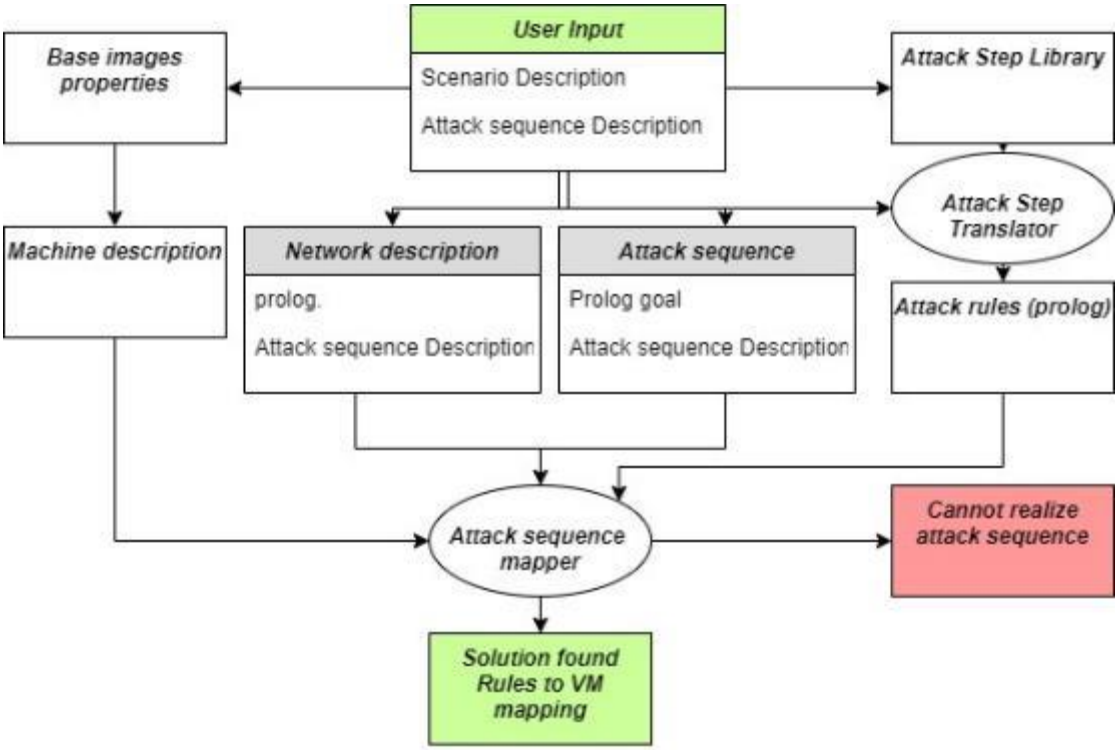


Figure 20. Scenario and Attack sequence translation (Venkatesan et al. 2019, 4)

According to figure 20, the communication network of the training environment and the periodic attacks in it are managed according to the user input. The scenarios are implemented as a pre-installed entity, with things happening in a phased manner. If the rules associated with the attack can be implemented on a scheduled basis, the system will implement it. If the rule cannot be enforced, the attack will not be executed.

Malicious data in IoT devices can be also described in the cyber range environment (Hussain et al. 2021). Software vulnerabilities are scored according to their severity. Vulnerabilities are scored according to the CVSS (Common Vulnerability Scoring System) method. The CVSS method provides useful information about the criticality of the vulnerability (Gatlan 2021). Exploitation of software vulnerabilities has increased every year, with traditional methods of analyzing various software vulnerabilities proving cumbersome. The research has focused on predicting vulnerabilities using in-depth algorithms that can automate the search for vulnerabilities (Jeon et al. 2021). There is also existing a system whose bots, according to their programming, can fix various system vulnerabilities without human intervention as updates are released to the systems. An information system called Mayhem has been developed for several years,

including analyzes of backups and studies of self-healing information systems (Avgerinos et al. 2018).

Table 6. Example of vulnerabilities used in ransomware (Gatlan 2021)

Pulse secure/VPN	CVE-2020-8243 CVE-2020-8260 CVE-2019-11510 CVE-2019-11539 CVE-2021-22893
Citrix	CVE-2020-8195 CVE-2020-8196 CVE-2019-11634 CVE-2019-19781
Microsoft Exchange	CVE-2021-34473 CVE-2021-34523 CVE-2021-26855 CVE-2021-31207
Fortinet	CVE-2020-12812 CVE-2019-5591 CVE-2018-13379
SonicWall	CVE-2021-20016 CVE-2020-5135 CVE-2019-7481
F5	CVE-2021-22986 CVE-2020-5902
Palo Alto	CVE-2020-2021 CVE-2019-1579
QNAP	CVE-2021-28799 CVE-2020-36198
Sophos	CVE-2020-12271
SharePoint	CVE-2019-0604
Microsoft Windows	CVE-2019-0708 CVE-2020-1472 CVE-2021-31166 CVE-2021-36942
Microsoft Office	CVE-2017-0199 CVE-2017-11882 CVE-2021-40444
vCenter	CVE-2021-21985
Accellion	CVE-2021-27101 CVE-2021-27104 CVE-2021-27102 CVE-2021-27103
File Zen	CVE-2021-20655
Atlassian	CVE-2021-26084
Zoho Corp	CVE-2021-40539
Microsoft Azure	CVE-2021-38647

As table 6 above shows, the usual systems which has vulnerabilities are used in offensive actions. The vulnerabilities described in the table may also be present on the training platform, in which case the training environment itself can be attacked. It also reminds how important it is to update the organization infrastructure in regular basis. However, with these vulnerabilities has possibility to demonstrate in exercise actions of the ransomware.

4.4 Exploit kits for use of cyber range

Exploit kits (EK) are developed for compromise sites to manipulate web traffic scanning browser-based vulnerable application and run malware with goal of establish control over device (Arntz 2021). EK's purpose is to exploit automatically found vulnerabilities on infecting target machine and delivering payload during the web-browsing in Internet. EK's are commonly used to distribute malware, such as remote access tool (RAT). Some EK's are sold or rent on black markets for certain an amount of money.

Typical activity of EK starts with compromised website (landing page), which will activate after profiling the visitor's device and found vulnerabilities (Paloalto networks 2021). The vulnerable application will be exploited and run malware on victim's device on commonly used browser in environments (Java, Flash, Silverlight etc.). After exploitation, the exploit kit sent encrypted binary file to the infected device which will decrypted and executed (Paloalto networks 2021). Some Linux distributions have large collection of different kind of tools for malware analyzes and penetration test purposes and usually these tools have implemented as part of cyber range platform tool set.

4.5 Benchmarks of cyber ranges

Cyber range platforms are used globally and most of the training facilities are found in the USA, Europe, and Australia. There are several approaches in the cyber range security awareness training, which aims for better experience for using cyber range even remote locations (Tian et al. 2018). Currently, the market for cyber platform users is open and many cyber companies worldwide offer their services to their customers (Morgan 2021). Organization's possibilities for gaining knowledge and skills for personnel, which has been improved by real-world based virtual scenarios.

There are built globally cyber ranges which are used only by military. In Estonia, The Estonian Center for Defense (NATO Cyber Range) has developed its cyber range with Tallinn-based companies, Guardtime (Guardtime 2021) and Cyber Technologies. Cyber range has developed automated command development platform for the maintenance. With increased automation, the need of resources is decreased with training exercises (Tambur 2020).

Figure 21. Cyber ranges globally (Chouliaras et al. 2021)

As figure 21 shows, most of the cyber ranges are in the USA and in Europe. Two types of cyber ranges have been identified, internal use and commercial use cyber ranges. Internal cyber ranges are mainly used by military or by a separately defined faction, for example universities. Cyber ranges have been built for different purposes (CTF competition, SOC-demonstrations etc.). Some cyber ranges are cloud-based, which can offer their services globally. Some cyber ranges use different branches (for example, Virginia cyber range and U.S. cyber range are in the same platform). Benefits for cloud-based platforms are that they can be used almost everywhere.

4.6 Services offered by cyber range platforms

Cyber range scenarios are categorized as customer-based exercises which can customized, and even services of real-world can be enabled.

Table 2. Services offered by cyber range (Cyberstartupobservatory 2021)

training education, awareness	**network security**	**cloud security**	**IoT**	**cyber threat intelligence**
governance, compliance	web security	endpoint security	mobile security	I am, fraud
data security	application security	detection, prevention	phishing prevention	SOC
e-mail security	user and entity behavior analytics (UEBA)	deception	cyber posture breach, attack simulation	incident, response, forensics
insider threats	blockchain	HW-based attacks rogue device mitigation	automotive aviation/rail, metro/ boat	industrial cybersecurity healthcare

As described in Table 2, the defensive and offensive actions for exercises can be created with need and scoping containing for all or needed services. Cyber ranges provide different kind of services to aid the progress of cyber ranges. Blueteamslab service offers customer detailed information on what is needed to do and required to complete the given tasks and scenarios. Once the customer is logged in, the user interface will show details about the scenarios which has been played through. Blueteamslab is providing scenarios for Incident Response, digital forensics, and threat hunting (Blueteamslab 2021).

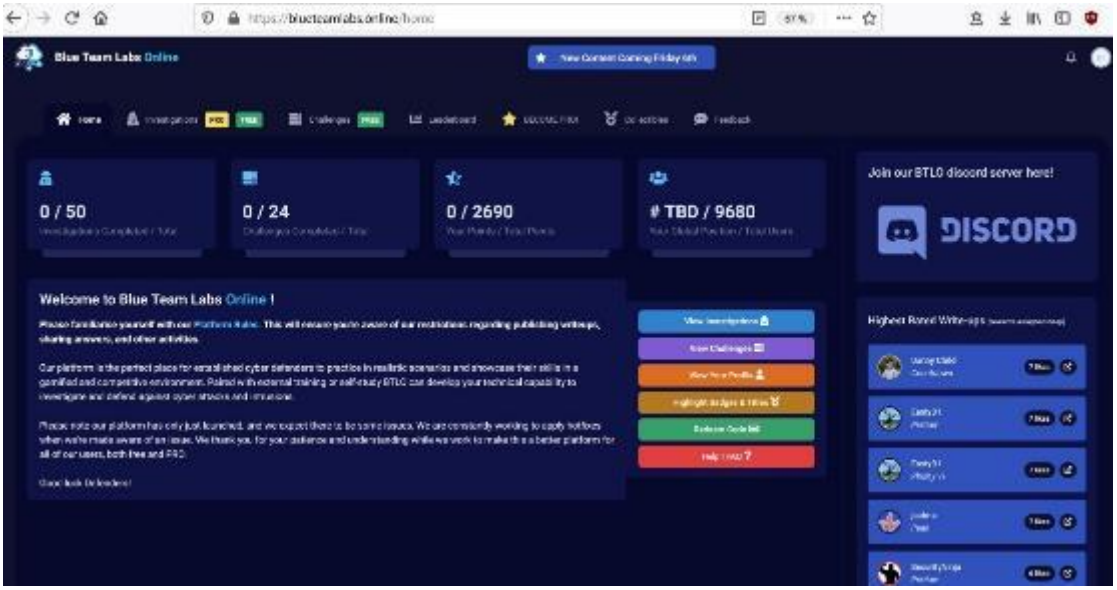


Figure 22. User interface (Blueteamslab 2021)

Figure 22 shows a view of the user's progress and achievements. It is easy for the user to continue performing tasks and get more information to complete tasks through the user interface. The interface also provides access to the Discord forum, where other performers have provided their own tips for the task. The available scenarios are detailed with figure and description which aims for given pre-informative for needed goals and user interface helps by walkthrough with instructions on how the user is progressed in the scenario.

Figure 23. Scenarios (Blueteamslab 2021)

Figure 23 contains descriptions of the different types of cyber scenarios and their severity. The user interface also shows the execution rate of the scenarios and the possibility to open more scenarios if the previous scenarios can be completed. Some service scenarios were chargeable. The scenarios are detailed step-by-step goals which are given detailed instructions for every given step. There is also an interface for other users which has completed current scenarios. There is possibility to interact for maintenance for getting help if required during exercise. Detailed steps for proceeding selecting scenarios will enable learning from given scenarios. Information is given as much it is possible and points are given for correct answers.

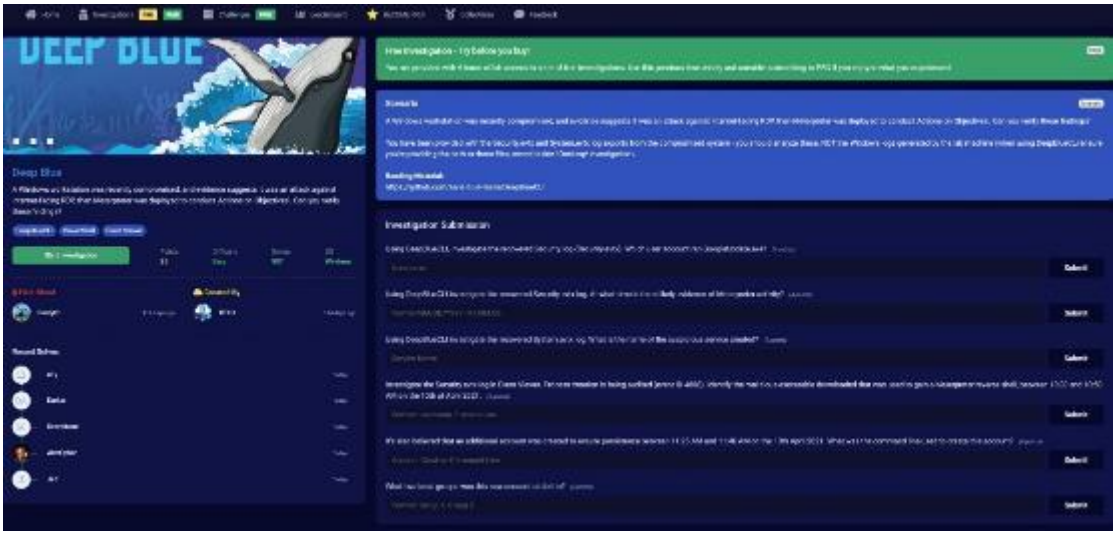


Figure 24. Scenario information and steps to completion (Blueteamslab 2021)

Figure 24 shows the descriptions of the scenarios as well as a to-do list of the scenarios, which are divided into steps. The latest performers of the scenario can also be viewed via the user interface.

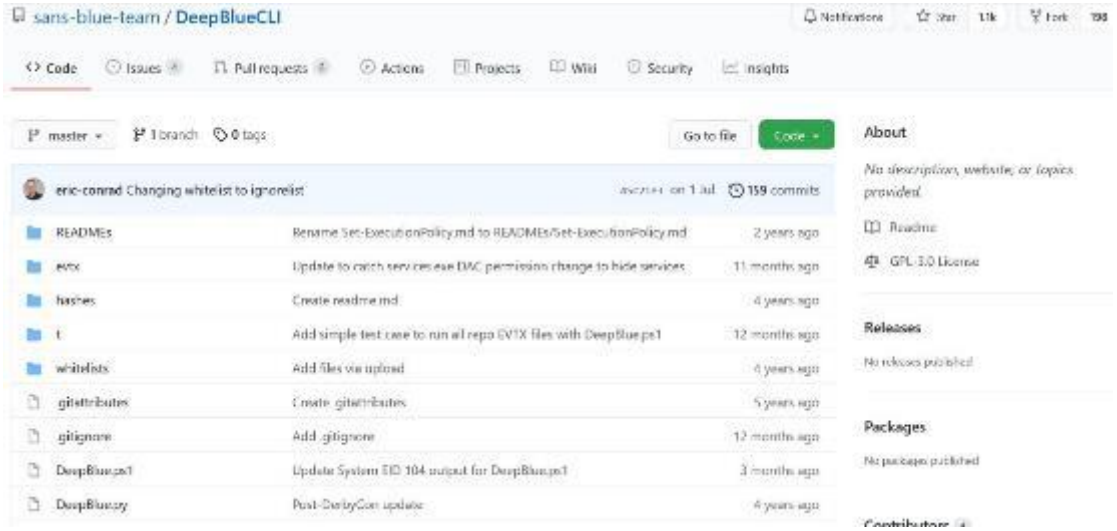


Figure 25. DeepblueCLI scenario (Conrad et al. 2021)

Blueteamslab scenarios are supported by the GitHub portal, which provides instructions, attributes, and scripts to perform the tasks in the scenarios, as shown in figure 25. According to figure 25 The scenarios use DeepblueCLI which is basically a PowerShell module, and it provides commands which can be found on the GitHub. Commands are needed to complete scenarios. The portal is maintained on a voluntary basis, in which case updates to the pages are made as needed.

The Cyber defense exercise platform (CDeX) built on the cloud service platform offers a slightly different approach. CDeX is founded by Vector Synergy and cyber range is a cloud-based platform which offers its services via Internet. CDeX has offices which are in Belgium and Poland. The cloud-based cyber range environment is simple and easy to use (CDEX 2021). CDeX platform offers cybersecurity testing for all users. Free testing period is limited to eight hours.

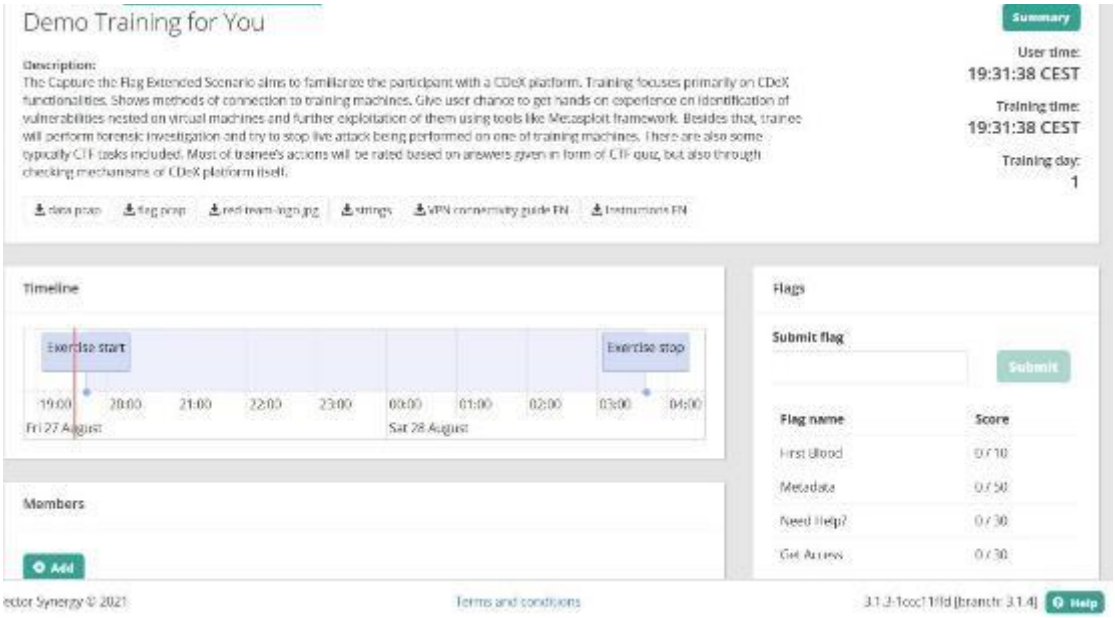


Figure 26. CDeX-cyber range user interface (CDEX 2021)

As shown in figure 26, comprehensive descriptions can be found in the cyber exercise, but also in a timeline that can be used to verify actions and response times to observed deviations. Figure 26 also shows the scores in the exercise-related issues, which can be used to make the task easier by reducing the points, or ready-made solutions. Visual setup also shows users who are logged in the exercise module. All servers which are used in exercise are listed in a table with login credentials.

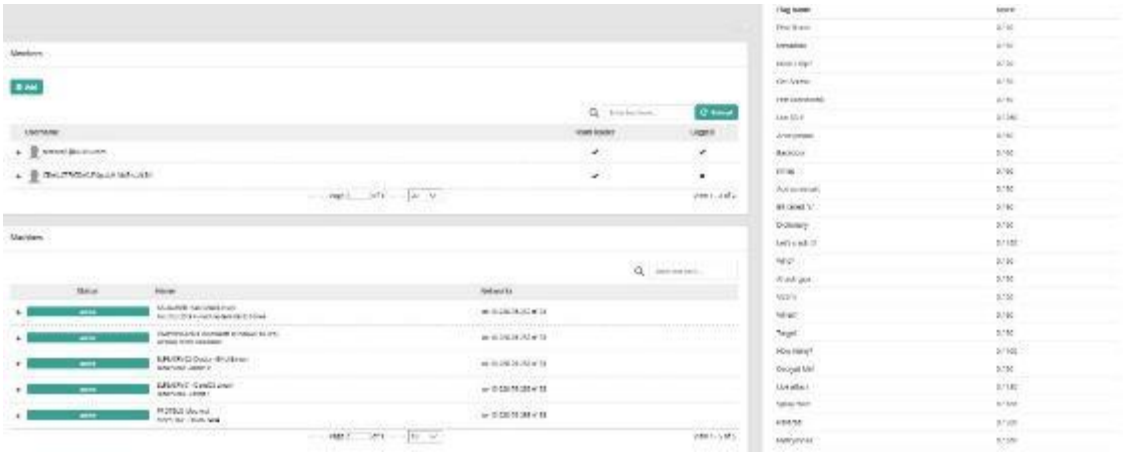


Figure 27. CDeX main screen (CDEX 2021)

Figure 27 also shows people performing the same task. The status of the virtual servers in the task as well as the active network devices is displayed, allowing logging in to the devices. Figure 28 shows a hint bar that makes it possible to ask for help completing a task. Below the hints' menu is a VPN certificate that can be viewed and downloaded as needed.

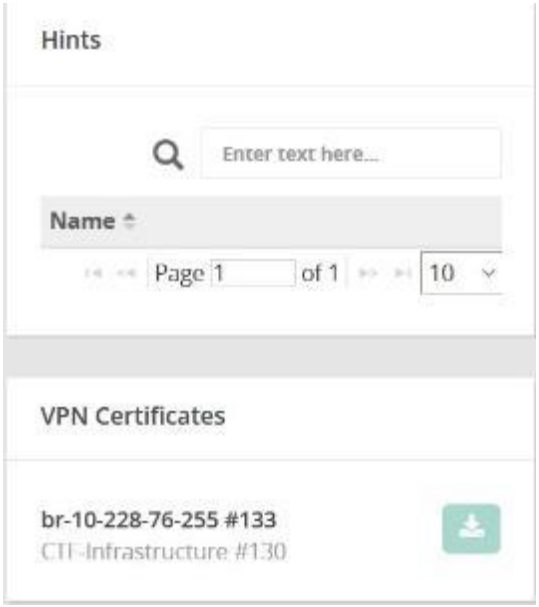


Figure 28. CDeX help – button for exercise (CDEX 2021)

There is also one known cyber training center in Finland. JYVSECTEC maintains a cyber platform located in Jyväskylä, Finland. Finnish cyber range called JYVSECTEC Realistic Global Cyber Environment (RGCE) is focused on implementations and deployments for hardware, equipment, and service investments for cybersecurity research, development, and training Centre (JYCSECTEC 2021).

JYVSECTEC RGCE services: (JYCSECTEC 2021):

- Finnish Cybersecurity Certificate (FINCSC), which is cost-effective nationally recognized certification mechanism for companies which are ensured business continuity and properly handled data protection
- JYVSECTEC provides information- and cyber exercises which focuses increasing personnel's knowledge and skill to adapt to constant change of digitalization and cyber threats
- security testing services includes fuzzing, source code auditing, DDoS stress tests and web application penetration testing possibilities all development lifecycle phases
- consulting services for evaluation of functionality, reliability in various fields of information and cybersecurity area
- JYVSECTEC publications of cybersecurity research literature.

JYVSECTEC has detailed brochures for their services which are found in their website. Cyber range actions are described with detailed information and cyber range capacity seems to be suitable for big cyber exercises (JYVSECTEC 2021).

In Austrian Institute of Technology (AIT) Cyber range is known for its cyber range platform which is in Vienna. AIT Cyber range is focused on critical infrastructure cyber training and research (CyberRange 2021). AIT has several reference projects, for example SIREN, which is commissioned by the International Atomic Energy Agency (IAEA) (CyberRange 2021). AIT Austrian Institute of Technology has developed a special virtual IT training and simulation platform, which simulates extremely sensitive industrial control systems (ICS) (CyberRange 2021). AIT Cyber range offers also realistic environment and has developed in response to the increasing digitalization and networking of industrial control systems for nuclear power plants (NPP) (CyberRange 2021).

AIT services are listed below (CyberRange 2021):

- awareness training for cybersecurity
- IT and OT technologies and vulnerability management learning
- threat and Attack scenario assessments
- certificate of knowledge and processes for IT operations and IT development
- cybersecurity exercises (incident management, contingency and recovery plans, reporting, EU NIS directive and EU GDPR, Risk management)
- development and research (secure system design, validation of security technologies, future threat scenarios)

Cyberbit Cyber range has been built in 2015 to solve critical problems (Cyberbit 2021). Cyberbit has currently offices in the USA, Israel, United Kingdom, Germany, Singapore, and India (Cyberbit 2021). Centralized cybersecurity management, called the SOC function, includes a wide variety of cybersecurity aspect to support operations. Cyberbit cyber training platform supports centralized cybersecurity management functionalities (Cyberbit 2021). Cyberbit cyber ranges are available all over the world. For example, cyber range is used by several universities and institutes which are for example: Miami Dade College, Austria's A1, French ISE, Israeli defense forces, IABG cyber range (Cyberbit 2021).

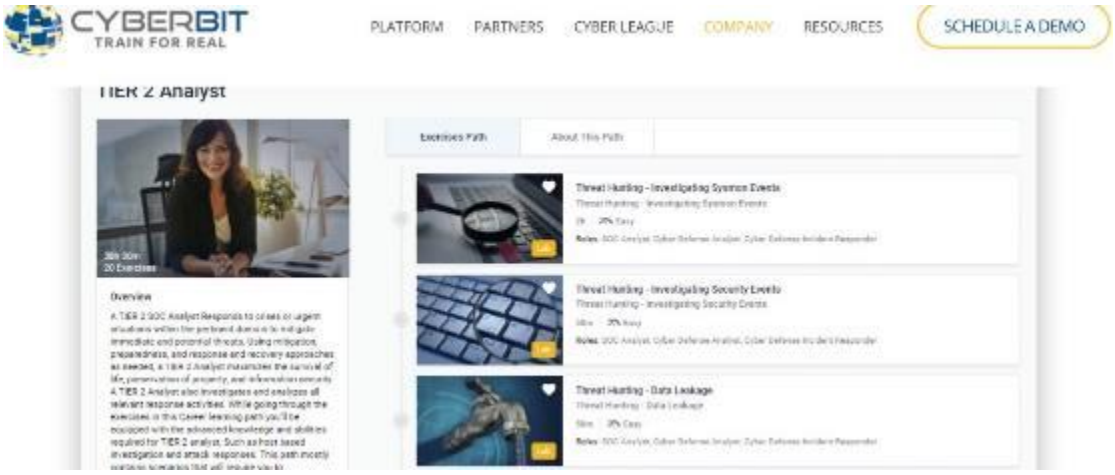


Figure 29. Cyberbit scenario description (Cyberbit 2021)

Figure 29 shows the different cyber exercises with the roles used during the exercise in addition to the description. Exercises can be linked to the favorite menu in the user interface. Cyberbit exercises contains description of contents of selected scenario with selected difficulty level. Exercises may contain similarities with different difficulties.

Cyberbit services (Cyberbit 2021) are listed below:

- cyber labs, which aims for learning paths and building blocks. They validate SOC-team performance and progress. Hands-on virtual environment offers IT, Networking, through live Mitre Att&ck techniques and use of commercial tools during an incident and in threat hunting
- cyber range exercises are built in hands-on environment which aims for training real-world scenarios. Simulated attacks provide virtual SOC experience (massive networks included, reverse engineered attacks, and commercially licensed security tools). With world largest catalog of simulated attacks

- performance based assessment, which aims in validating operational readiness. Integrated with Mitre Att&ck and NICE Framework. Cyber range is cloud-based on-demand platform
- Cyberbit platform provide measurable results to track key performance indicators (KPI) and teams performance both in labs and in cyber range exercises. Cyberbit measurable KPIs are investigation findings, response with containment actions, which are evaluated automatically based on trainee actions during training. Results can be viewed in detailed dashboards where progress can be tracked (Cyberbit 2021)

Users can use the Cyberbit virtual platform as a cloud service from almost anywhere. Cyberbit cyber range platform is used in schools and universities remotely. Cyberbit has the large number of resources which gives cyber range platform large variety of functions in cyber exercises.

KYPO Cyber Range Platform (KYPO CRP) is developed by Masaryk University since 2013, and it represents several years of our experience with cyber ranges in education, cyber defense exercises, and trainings. KYPO CRP is entirely based on selected approaches, which includes containers, infrastructures as code, used microservices. KYPO Cyber range has released its code as an open Source. KYPO homepage contains video instructions of how the cyber range can be configured properly. KYPO provides cost-efficient, scalable and interoperability training which is aimed to minimize human interaction.

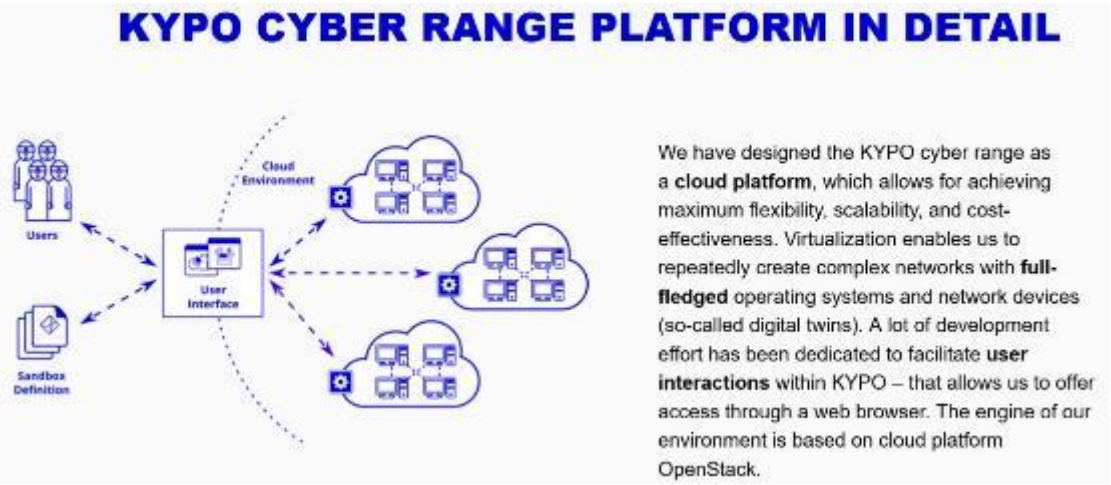


Figure 30. KYPO-Platform (KYPO 2021)

As shown in figure 30, the KYPO virtual training platform can be used as a cloud service and the platform can be customized to suit the needs of the users. Using the KYPO platform enables to create functional cyber range environment and provide even development for source code if necessary. As an open-source

solution, the source code of the KYPO platform is freely downloadable, so it can also be evaluated.

Virginia cyber range / U.S. cyber range is a cloud-based cyber training platform which is focused on realistic, hands-on cybersecurity teaching and labs with exercises for students (high schools, colleges, and universities) for both students and teachers (Virginia cyber range 2021). The platform is using approximately 155 000 virtual machines (Virginia cyber range 2021). Virginia cyber range provides flexible sign-up with different ways relating to where are student and what courses user has going on. Possible methods are for signing up are Google, Facebook or Azure accounts for cyber exercises and use of invitation code is possible. For teachers and students, there are different sign-up pages. Virginia cyber range contain community, which provides support and findings, newsletters and knowledge base related to cyber range and its virtual exercises (Virginia cyber range 2021). Community includes video material from workshops, advisory board, awards for cybersecurity educator and offers annually cybersecurity education conference (Virginia cyber range 2021). The U.S. cyber range hosts weekly cybersecurity workshops.

The U.S. cyber range and the Virginia cyber range differ in that the U.S. cyber range has published a service price list that is missing from the Virginia cyber range. Virginia cyber range offers downloadable learning material which is focused on self-paced learning. Downloadable assignments and software tools enable offline studies for different areas of defensive and offensive security. Overall, the cyber ranges all over the world offers cyber training for closed audiences, groups, students, individuals with written scenarios or team competitions. Some cyber ranges offer facilities for trainings, and some cyber ranges are used virtually all over the world.

4.7 Cyber training exercise websites

Some companies provide learning services instead of cyber range activities. Hack in the box is the internet based virtual platform which aims for penetration testing and exchanging information with other members (Hackthebox 2021). Hack the box provides a virtual environment which contains different vulnerabilities and CTF-challenges.

Figure 31. User interface of Hack the box (Hackthebox 2021)

As shown in figure 31, the service interface provides its own profile as well as a possible team to support training. In addition, with the help of the user interface, it is possible to receive instructions, teaching and exercises with different themes and levels to choose from by theme. The user interface shows your own level of competence, which increases with the help of the completed exercises. Hack the box service provides virtual training for application security, reverse engineering, forensic analysis, incident response, software development, development, and IT operations (DevOps) with possibility for penetration testing. Basic tools which are provided by Kali Linux makes possibility to get started with exercises briefly. Activities from other users can also be viewed and learn by watching them.

Tips for learning in open cyber range platforms (Touhid 2021):

- protect computers and machines from hackers (Hackers may use same trainings)
    - use virtual machine or use hardened physical computer
    - avoid handling personal or organizational information and disconnect the VPN from the organization
- learn Python
    - Python is usable for everywhere
- keep notes from actions
    - by keeping a diary, it is possible to check previous settings and parameterization
- use search engine searches
    - Search different engines for example Google things is needed to proceed in the exercise.

4.8 Websites offering learning experience

“Try hack me” service was founded in 2018. It is a service which provides cybersecurity training with scenarios from the real-world which offers point by answering questions, participating challenges with selected skill level and generated lessons. Try hack me provides a web-based virtual cyber platform that allows you to practice specific cyber topics. Try hack me has also community where is possible to participate in different conversations (Tryhackme 2021).

Hacker101 service provides free lessons for web security which includes capture the flag competition and video lessons (Hacker101 2021). Hacker101 includes learning tracks for beginners, penetration test people, web hacking, mobile phone hacking and cryptography. Hacker101 service regularly publishes capture the flag competitions, the content of which varies by theme. For cyber range exercises, Hacker101 offers a starter’s video guide to penetration testing with OWASP-framework.

Dfirdiva is a web-based service which offers free Digital Forensics and Incident Response (DFIR) & cybersecurity training (Dfirdiva, 2021). DFIR is an area of cybersecurity that identifies and investigates cyber-attacks. Dfirdiva is focused training and website contains over 300 forensics and incident response (DFIR) exercises. Dfirdiva includes four core training categories, which are 1. General IT & cybersecurity 2. Networking 3. Linux and 4. Programming & Scripting (Dfirdiva, 2021). The service includes blogs and offers scholarships to deserving researchers.

LimaCharlie service provides information and support for cybersecurity actions for cloud services, IoT services and endpoint protection with commercial services (LimaCharlie 2021). LimaCharlie service includes its services’ documentation of best practices with quick start guide with education & training services. Users of LimaCharlie has possibility to join community and ask support for personnel of LimaCharlie.

Simplycyber service offers free resources for use of cybersecurity and weekly videos for newsletter subscribers (Simplycyber 2021). Simply cyber contains information about cybersecurity resources including training, conferences,

speakers, labs etc. Some information contains links to other cybersecurity services. The Simplycyber service publishes videos of presentations of current vulnerabilities. The Simply Cyber website also contains links to courses offered by selected universities.

INE is a site that provides users with computer network training as well as cybersecurity. Computer network training includes IT processes and cybersecurity training penetration testing related entities. INE includes a data science learning path that includes the basics of machine learning. The learning path also includes the Azure cloud service, which can be learned through the INE service (INE 2021).

Vulnerable by design (Vulnhub) offers hands-on experience in digital security, computer software, and network management. Cyber range exercises for use of virtual machines are possible through Vulnhub, Vulnhub offers virtual server platform exercises with different difficulty levels. Vulnhub aims for practical virtual server learning in system and network administration (Vulnhub, 2021). The user can define the learning from exercises individually or in groups.

Sololearn is one of the largest online communities through which to learn programming. Cyber exercises for programmers are possible to learn through cyber range platform. Sololearn offers python core, Java, C#, JavaScript, C++, etc. exercises with step-by-step guidance and there is also possible to earn certificates from exercises. Sololearn provides a platform for testing and discussing your own source code at "Code Playground" (Sololearn 2021).

Cryptography is also part of cybersecurity, and cyber exercises are found on a website called Cryptohack. Cryptohack is providing a series of interactive puzzles and challenges which are evaluated by points and participants can track their progress. Cryptohack also offers courses to help you learn encryption algorithms. Almost all the challenges of the site have been done with Python 3 (Cryptohack 2021).

Web security academy by Portswigger offers free online web security training academy which is created by developers of Burp suite. The training environment includes a variety of instructions to make it easier to do the exercises. The

exercises themselves include laboratories of different levels in different subject areas, such as SQL injections, cross-site scripting, clickjacking, DOM-based vulnerabilities, HTTP request smuggling, and XML external entity injection, as well as many other exercises related to web vulnerabilities. Latest exercises contain authentication, HTTP Host header attacks and business logic vulnerabilities. In addition to cyber education, Portswigger provides research on various software vulnerabilities that researchers publish to the service. Portswigger's news service publishes cybersecurity news through its service (Portswigger 2021).

PicoCTF was founded in 2013. PicoCTF provides training in various areas of cybersecurity. The service contains study material in the form of text and videos. External links have been added to the service to supplement picoCTF's learning materials. PicoCTF provides a community to practice and compete with a variety of CTF challenges. PicoCTF regularly hosts CTF challenges for high school students in the United States (PicoCTF 2021). If cyber range user is needed for community for exchanging thoughts related to cybersecurity, the visit in the security innovation community might be useful. Security innovation (SI) community offers free application security training resources, including access to SI’s Instafriends cyber range (Security innovation, 2021).

4.9 Exercise types for cybersecurity

Different organizations plan exercises with specific priorities. Optimized and ready-made training methods are used to plan cyber exercises. If it is desired to specify which industries and the companies representing them organize cyber exercises, a sketch of potential critical infrastructure actors can be created as shown in figure 32.

Figure 32 illustrates the functions and functions of the state. At the top of the image are top-level descriptions of related matters. The middle line illustrates the different industries, below which are the activities related to cyber exercises, which are separated by industry. Mapping cyber exercises allows us to target the appropriate focus area for the exercises. Cyber exercises should provide their users with the risks and preparations associated with that industry.

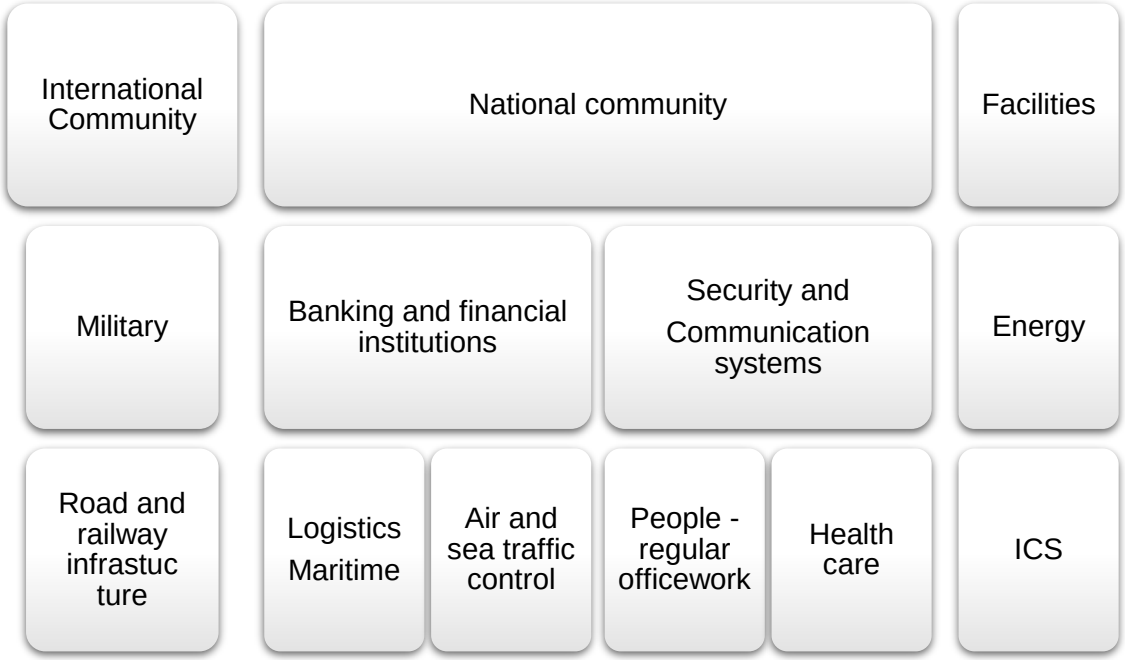


Figure 32. Potential industries for cyber training (Ween, A. et al. 2019, 341)

Organizations want to organize easy and useful cyber exercises, so these exercises can be organized mainly in four different ways: Tabletop exercise, hybrid exercise, cyber range training virtual simulation (full live), and Individual completed exercises. Tabletop exercises are easy and quick to organize. It is a paper-driven exercise where injects and attacks are scripted via paper. Through this, it is possible to evaluate the organization-specific guidelines of organizations. Second, in addition to the exercise on tabletop, hybrid-style exercises also include a virtual element, which makes the exercise type a little harder to organize, but the exercise type brings more realism in terms of attack and defense. 3. Full live exercise is delivered fully with real injects in real like environment. These are the most complex and largest exercises to be held, and it may take a year to plan a full live exercise (Kick 2014). Cyber exercises can also be done alone, allowing to progress at the student's own pace.

Table 3. Typical cyber exercises (NCSC-FI 2020)

scenario type	**scenario event list**
phishing, hoax	business email compromise (BEC)
	unknown USB-device
	unknown device found on network
	infected software
	domain hijack
	data manipulation
	distributed denial of service
data leak	personnel data
	password leak
	database leak
	recycled device
disruption, data breach	parameter changes
	long-term attack
	acquisition
	crypto mining
	unknown network traffic
miscellaneous	hacktivism
	white hat informs about vulnerability
	blackout; electric failure

Table 3 provides examples of different types of cyber exercises. The topics are given at the title level and a story has been added to them, which can be adapted to the purpose of the exercise. Traficom's table of cyber scenarios provides from organization's point of view possibility to enhance interaction between personnel. National Cybersecurity Centre Finland (NCSC-FI) has published cyber training scenarios which contains training examples for the organizer of cyber training exercise. NCSC-Fi supports cybersecurity trainings for Finnish company called KONE in 2020 (NCSC-fi 2020). According to NCSC-FI, the cybersecurity incidents are concentrated about software/device malfunctions, data breaches, data leakages, spam, DDoS attacks, Phishing, IoT-related incidents, hoax, malware, and vulnerabilities of the software (Traficom 2021). Cybersecurity exercises contain planning phases, which contains selection of type of cyber training and preparation for exercise which are described in table 3.

Cyber range scenarios need phases of planning and preparations before the exercise is ready to go live. Planning and preparations phases include:

- preparation for exercises
    - selection of exercise type: Tabletop, paper-driven, hybrid exercise or full live exercise
    - scoping strategic and operating environment selection with sufficient details and resources. Expectations for exercise
- planning of exercise
    - planning phase contains storyline or plot for the exercise
- content of exercise (execution)
    - building required environment for the exercise. Selection for objectives and possible intervals to the exercise. Session timeline expectation. Exercise audience/observers storyline and objectives
- post exercise actions
    - follow-up learning from exercise is feedback which is given by participants. Feedback is part of analysis report which written after exercise After-Action Report (AAR). These reports are used to improve the quality of the training. AAR collect information which can be focused to improve ability to respond to different cyber threats

Cybersecurity management system contains different activities and requires training. Cyber exercises consist of different teams, which all have a purpose of their own. Teams for team-based cybersecurity live exercises are: Blue, Red, green, purple, yellow, orange, and white. Teams are formed based on need and are typically named as colors. The exercise has the possibility to create group called as an exercise controller (ECG) which tasks are to observe exercise with master scenario event list (MSEL), but group is called white team (WT). MSEL contains selected offensive actions and threats to be executed in the scenario. ECG drives the execution by giving selected tasks in exercise to Red Team (RT) and executes selected threats in exercises that are scheduled to run during the events of scenario.

Responsibility of the White Team (WT) is to carry out the exercise, collect information from exercise and monitors scenario and gives feedback to ECG and Red Team (RT) it needed modifies the objectives during the exercise (Savva, 2020). The scenarios with the objectives on it are created by WT. WT work as observers and solve possible conflicts that may arise between the red- and blue teams, as well as answers questions that are arisen during the exercise. WT also evaluates the team progression by assigning scores to teams (Savva 2020). As close to actions of WT, the purple team’s (PT) responsibility is to

collect information between red and blue team with collaborative action (communicative). The team may contain a group of observers, or it can be a mixture of blue and red team members (Savva 2020).

The offensive action group is called Red Team (RT). The group of attackers that are responsible for offensive actions in the information systems by executing planned attacks and try to breach behind blue team (BT) defense line in the exercise. RT has no knowledge about used security controls, but it uses actively reconnaissance. RT's objective is to improve the target company cyber assurance by demonstrating the impacts of cyber-attacks on BT protected enterprise infrastructure (Shea 2020).

Blue Team (BT) is responsible for defensive actions in cyber exercise. BT's role is to be able to keep information systems secure in the enterprise. Exercise can consist of one or multiple blue teams that form together the defense line of the company network. The BT defends the information systems entrusted to it by monitoring its networks and perform data analysis based on risk assessments. On BT protected systems is needed the threat detection ability to detect offensive actions (IDS/IPS, network segmentation). By internal vulnerability scans and DNS audits, some known vulnerabilities can be fixed during exercise (Shea, 2020).

Cyber exercises need administration for actions like systems, virtualization services, scenario etc. Green Team (GT) is used as technical team which responsibility is to solve technical issues which has raised during exercise (Miessler 2020). GT members are responsible for preparing and maintaining the cyber range technical infrastructure. GT may also be used source of automated network traffic generator and generating background noise in a bigger exercise. (Kick 2014; Silokunnas 2016)

As part of a technical support, cyber exercises may contain also orange team (OT) and yellow team (YT) which may give technical support for blue and red team (Miessler, 2020). There may also be different tasks for teams. For example, orange team may organize communication between red and yellow team (builders) if there is a need to engage red team. Builders are learning how to

better build their applications, systems, networks etc. Orange team represents users of the organization (Savva 2020). All teams are illustrated in figure 33.

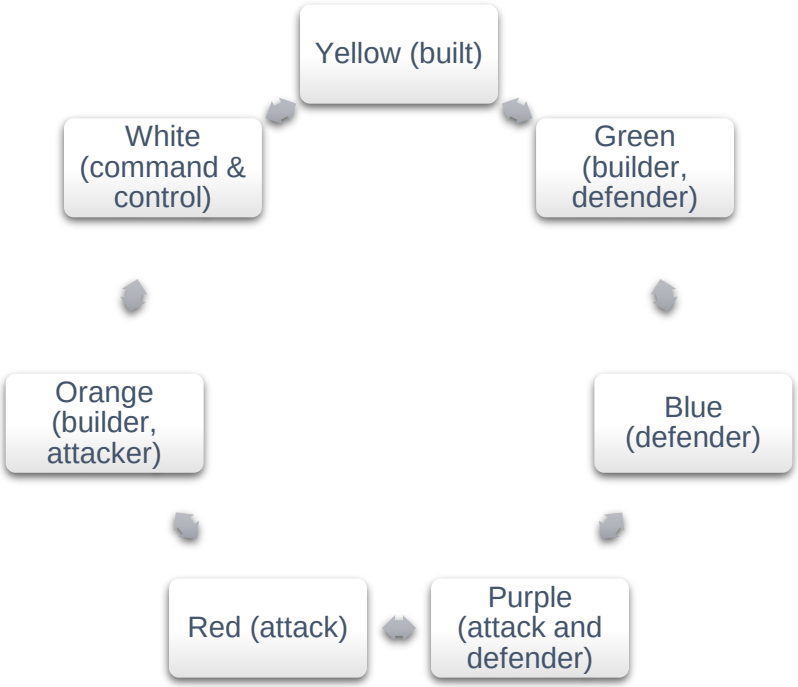


Figure 33. Cyber range teams (Miessler 2020)

All groups are linked to each other as illustrated in the figure 33. However, usually required teams in exercises are red and blue. Other teams are formed whenever it is necessary. When cyber range uses capabilities and functionalities of real ICT infrastructure, participants will collect information from different areas (cybersecurity scenarios, monitoring incidents, constant learning, management, team communication, environment handling). Cyber exercises enhance collaboration and communication, and teams are learning how to react to incidents of the ICT systems in organization network (Chouliaras et al. 2021).

Participants in a cyber exercise are required to take certain measures to get the most out of the exercise. In the exercise, the participant may have to install virtual workstations or servers in the virtual environment. The purpose of these installations may be to run various applications and scripts. For this reason, the participant should know the characteristics of the information systems used in the cyber exercise.

For learning purposes, there are few skills which are needed to learn for understanding cybersecurity (Cyberspatial 2021):

- building a virtual machine with operating systems.
- command line (shell commands and scripting with bash or PowerShell, etc.)
- system administration (configuring systems etc. knowing your system)
- computer networking (device interaction, OSI-layers incl. TCP, etc.)
- personal digital security

Virtual environments are a place to study cybersecurity incidents and makes possible to create knowledge of behaviors and steps for actions of disaster recovery. Most useful tools for training are different command line tools, which some of them might include Kali Linux. Configuring system parameters and evaluation of different features are skills which are strengthened by training. Networks and knowledge of Open Systems Interconnection (OSI)-layers are important for cybersecurity because structure of the networks and logs of the network devices may contain useful data for analysis. Personal digital security means that you need to know security features of your devises. Cyber range training scenarios need documentation to back up the scenario functionalities. The functionalities are useful when the participant takes notes of its own.

4.10 Human-in-the-loop and industrial cyber ranges

Systems which are required to have human element along are called “Human-in-the-loop” concept (Kucek and Leitner 2020, 110). Organizations in different industries are aimed to increase preparedness and cyber incidents’ response time in automated environment which is called Industry 4.0 systems (Kucek and Leitner, 2020, 107-118). Industry 4.0 systems which are called also cyber-physical systems (CPS) can be used for training against malicious users. CPS can be used as well as cyber incidents and practice with on-premises and virtually separated locations. Defense-in-depth is used in military strategy and many industries such as energy sector and is known as universal framework in the field of cybersecurity. Defense-in-depth is obtaining multiple layers of security controls and ability for monitoring intruders progression. In the cybersecurity environment, it can apply after the organization knows the used controls and uses the knowledge of analyzing threats and vulnerabilities for protecting ICS critical assets (Fabro et al. 2016, 11-50).

Key elements for countermeasures ICS (Fabro et al. 2016, 44):

- implementing secured ICS systems and networks best practices with risk assessments by a defense-in-depth approach
- isolate ICS network connections by minimizing attack vectors
- ICS systems Hardening by disabling unnecessary services etc. enable available security features with implementing configuration management
- monitor networks and logs by assessing the security of the ICS, networks, and interconnections

Management of the human element can be done by identifying requirements for ICS systems and with regular training of personnel. All actions need to be traceable, because certain training might be included in the focus of security audits. Table 4 describes the different security controls that can be used to create a defense-in-depth entity. It also describes defensive approach which focus on key elements for decreasing impact of attack. More attention is being paid to the security of ICS systems today. Various measures have been found to protect systems to increase intrusion time and shorten response time. The department of Homeland security (DHS) has identified nine key elements which provide suitable security controls for industrial control systems cyber emergency response team, as described in table 4. As seen in Table 4, the defensive controls of ICS systems have similarities than the defensive controls in the ICT systems. The protection of information systems based on risk assessment can be implemented by utilizing best practices.

Table 4. Defense-in-depth strategy elements (Fabro et al. 2016, 6)

element	description
risk management program	threat identification, risk assessments, asset management
architecture of cybersecurity	frameworks / best practices / audits policies, procedures, and processes
physical security	field electronics locked down, access controls for control center, remote site surveillance, physical restrictions
ICS network architecture	common architecture/Zones, demilitarized zones (DMZ), virtual LANs
ICS network perimeter security	firewalls / one-way data diodes, remote access & authentication, jump servers / Hosts
host security	patch and vulnerability management, field devices, virtual machines
security monitoring	intrusion detection system, security audit logging, security incident and event monitoring
vendor management	supply chain management, managed services /outsourcing, leveraging cloud services
the human element	policies, procedures, training and awareness

4.11 ICT- and ICS based models for incident response

Tabletops for ICS incident response training are for preparing actual cyber exercise. Exercise required capabilities for defense, processes for safety and preparedness for cyber actions (Parsons 2021). Tabletops are training type which is done by paper, and they are based on discussions on a meeting and are guide by organizational instructions and incident response plan. Participant's knowledge and understanding of the existing ICS defenses are required and if weaknesses are found, it makes it possible to update instructions and incident response plan immediately. The question for the exercises is: How the organization will respond to ICS threat when the exercise begins (Parsons 2021).

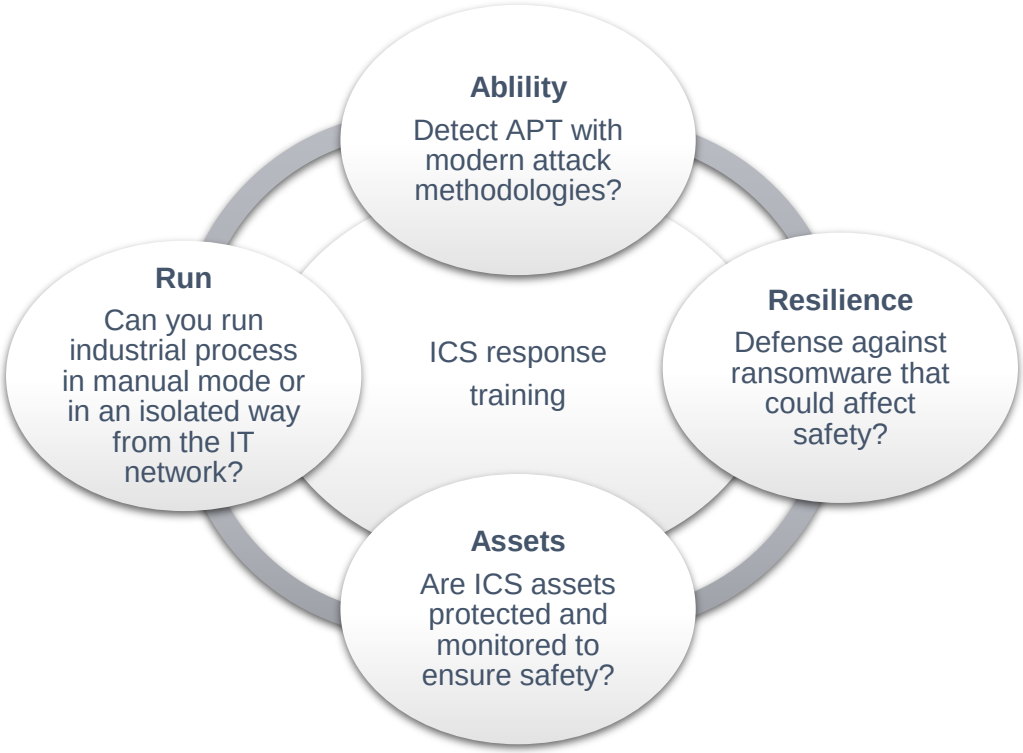


Figure 34. ICS response against threats (Parsons 2021)

As figure 34 presents, the ICS response training may be used in any cyber exercise. Tabletop training can improve ICS incident response if selected exercise is suitable to execute without virtual environment. For example, organizational procedures and guides may be useful to put in objectives of tabletop exercises.

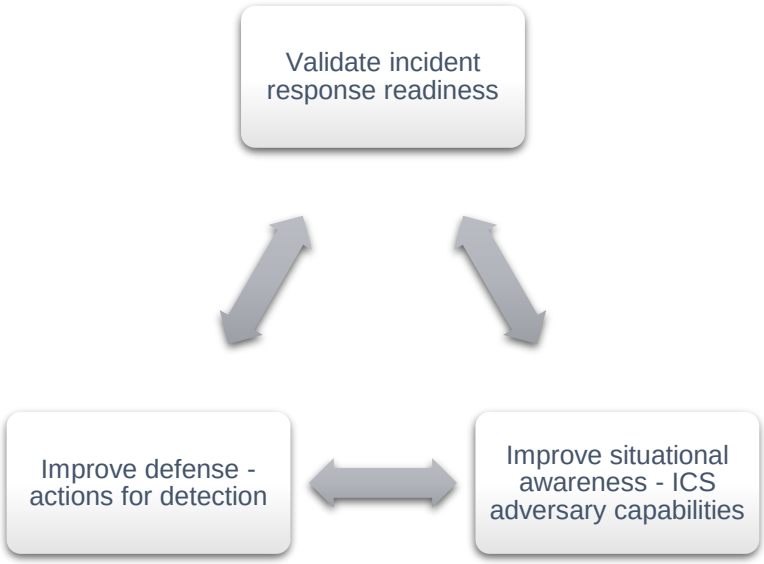


Figure 35. ICS response cycle (Parsons 2021)

Figure 35 shows that ICS response cycle contains three factors which will create value by training incident response. Incident validation and response readiness are objectives are values which need constant improvement. Training will also improve defense and the rehearsed activities to detect things which are presented in scenario documentation. Training also improves situational awareness, which include task evaluation for adversary capabilities. When evaluating instructions and guides, the selecting suitable method for evaluation is recommended tabletops exercise. Improvements can be identified with security and safety playbooks, incident response plans and with organization own guidance. Tabletops can help team members to follow processes and ICS-specific security (Parsons 2021).

ICS response tasks during validation processes are identified detection gaps and improve understanding of engineering operations. As an outcome, the exercises help to validate needed actions for the ICS incident response plan. Teams in exercises are involved and includes adversary capabilities with attack techniques which gives an outcome for reviewing threat intelligence action. Tabletop brings values from cross-departmental relationships, including supply chain providers. ICS response tasks during improving awareness are educated other teams and build cross-team relationships for ICS incident response in facilities.

Tabletop exercises gives possibility to identify issues of critical areas. Critical areas are for example changes of threat detection, data collection, log files, network segmentation, access control updates, security and safety process changes and the communications of roles and responsibilities. If there is a need to improve perception and response, then the roles at the organizational level and the responsibilities between teams must be considered.

4.12 Scoring of cyber exercises and key performance indicators (KPI)

Training in a virtual cyber training environment requires different measurement methods to support the activity. The performance of the tasks in the cyber exercise can be assessed in order of priority by scoring the performance according to the solutions of the tasks. In addition, activities related to cyber exercises can

be measured as needed. In CTF competitions, participants' performance is judged in order of priority. For this reason, CTF competitions usually have time limits, after which the points received by a player or team are added together (Singh, et al. 2022). The winning player/team is the one who solved the most tasks (flags) or completed them earlier and thus got the highest score. Scoring for CTF competitions can be done on a round-by-round or competition-by-competition basis according to the competition plan. In practice, flags are collected on a task-by-task basis, so that the participants' ranking is seen after each round (Singh, et al. 2022). Generally, during a CTF competition, the entrant must submit the collected flags to an online portal that will award individual performance points to the individual or group. If the system in use does not automatically detect the receipt of a flag, competitors will be judged on the basis of the generated timestamp. For virtual exercises in the learning environment, an assessment system suitable for the exercise should be considered, which may differ from the system used in CTF competitions (Singh, et al. 2022).

The management of security requires measurements, which are called key performance indicators (KPI) and key risk indicators (KRI). The effectiveness of cybersecurity relies on past collected data metrics, which also requires interaction between business owners. Cybersecurity statistics and reports tells a tale, and selected KPI’s need to focus on relevant aspects clearly. It may also require that the organization is benchmarking also third-party vendors (Fasulo, 2019). Measurements are needed for evaluation of progress and outcome of the cyber exercise. Measurements can be made cyber range platform, cybersecurity exercises, participants of exercise. A typical measurement is incident response time. However, in real life, only identified assets can be measured. Identified measurements are needed to accept before usage. Cyber exercises may measure participants actions and monitoring network behavior. Typical measurements may include (Pederson 2008):

- **Interval metrics**
    - Interval metrics means the ability to count selected things, but not against any standard. Many decision support systems provide for inputs in the form of counts of different forms, which are used for different things for example voting.

- **Nominal metrics**
    - Most human-oriented decision-support systems may have nominal measurements in the form of ideas, options, or other kind of possibilities. Nominal metrics does not include any formal basis in an underlying scientific model. Nominal metrics may include a list of things with no basis for formal comparison.
- **Ordinal metrics**
    - Ordinal metrics implies a partial ordering. Most decision support systems support comparison between similar things or alternatives, and this produces ordinal metrics.
- **Ratio metrics**
    - Ratio metrics are meant for the ability to add, subtract, compare, and normalize to a common “no value” for measurable objects. Almost all decision support systems use ratio-based calculations, even if the underlying metrics are not ratio-based.

Things measured in cyber exercises can relate to threats, response times, data network, cloud services, malware, access rights, outdated information systems, or the supply chain etc. In cybersecurity illustrated, metrics are ensuring for decision-making process is correct and efficient because every action must be explained (Froehlich 2020).

Measurable threat vectors (Froehlich 2020):

- offensive action detection / intrusion attempts
- rates (incident), levels of severity and response times with time to remediation
- patching reported incidents (upgrading, fixing found incidents and vulnerabilities)
- response times
- threat vectors (number of users erupted from the application/data access levels, insider threat)
- organization total volume of data
- annual peer review /competitor comparison
- avoid complex reports for board members
- common Vulnerability Scoring System (CVSS)

Statistically, daily observations of anomalous activity in computer networks constitute routine daily activities. Different rates and severity levels of found incidents with response times are interested, and improvement of security may require changes for technical efficiency. By collecting incidents with their levels of severity, it can show the resources how the technical environment is protected. Patching the found vulnerabilities is critical, and board members understand

that discovered vulnerabilities must be fixed. CVSS scoring systems helps to measure severity of found vulnerabilities. Researchers have built a list of vulnerabilities which is used by ransomware gangs. These identified vulnerabilities have CVSS score and has possibility to use and measure in cyber range exercises for both teams of red and blue (Gatlan 2021).

Showing the board members, the threat vectors by cybersecurity metrics, showing that insider threats are an issue among other issues. With using metrics of data, including internal data loss metrics, on/off boarding metrics with tracking application access may illustrate organization data handling also with data loss by theft for the board members. A possible way to demonstrate the impact of cybersecurity is to measure and make comparisons between the organization's own metrics and its competitors. Benchmarking can help an organization understand the current need to develop cybersecurity. Some vendors of cybersecurity may generate reports for board members. Offered reports are too technical with result of unread documentation. Important thing is to offer board cybersecurity metrics with customized information (Froehlich 2020).

There is also possible to track KPIs from selected areas (Fasulo 2019):

- organization preparedness level
    - number of devices are in network and upgraded
- internal network unidentified devices
    - devices with source of outside the organization (for example employees own devices etc.)
- cybersecurity awareness training with results
- security ratings
- access management
- compliance of cybersecurity policy
- non-human traffic
- virus infection monitoring
    - phishing attack success
    - cost per incident

Typical examples of common KPIs are easy to track and received metrics are illustrating organization's preparedness level. Metrics may show all devices on the internal network with unidentified devices and intrusion attempts. Statistics may also reveal mean time between failures and meant time to detect, with acknowledged time until the full recovery. Metrics may also show results of cybersecurity awareness training, system patching and incident reports. Security ratings are to score systems with security ratings (for example network security,

DNS health, scrabble score calculator (CUIT) score, endpoint security, IP reputation, web application security, hacker chatter, leaked credentials etc.). With information of access, management could have metrics for number of administrative accounts, removed and unused accounts. Information may be given also with non-human traffic and number of virus infections. The result of metrics would give approximately costs of cybersecurity (Fasulo 2019).

5 CONCEPT OF PROPOSAL FOR XAMK CYBER RANGE

This chapter presents the concept of the proposal for Xamk cyber range environment. The collected information was combined with current state analysis for Xamk Virtual Lab system. Cyber range deliver knowledge for participants of training sessions, and it also provides feedback for Xamk how to improve virtual training procedures in the future.

5.1 Building a concept plan for the cyber range

The planning process started from the request of Xamk. Xamk needed to enhance Virtual Lab system to the purposes of create concept for cyber range virtual training. Concept for the training in cyber range environment required suitable research documentation and interviews with written assignments for fulling requirements set by Xamk. Chapter 4.3 collected information on cyber practice platforms located in different countries. The chapter reviewed the published information on the purpose of cyber training platforms, also considering the technical aspects. Based on the information gathered in Chapter 4, it can be concluded that the use of a virtual cyber training platform should be planned and planned for the long term. Cyber range concept requires several aspects to take into consideration:

- resourcing
- services for use of cyber range
- cyber range platform user interface with scenarios with suitable documentation
- measurements and knowledge gathering and
- marketing & advertisement.

Information is gathered through meetings before, during and after the exercises. The continuous development of the training environment costs money, but at the same time as the technology develops, the competence requirements of the staff also increase. As the activity develops, the exercises in the training environment can be targeted to the desired industry. Measures related to the training environment require careful planning. Table 5 provides a possible example of what is included in the plan.

Table 5. Overall requirements for suitable cyber range environment

requirements	**description**
resources	cyber range resources are function required by maintenance, scenarios, and facility operations during exercises
cyber exercises	virtual cyber exercises are created according to a risk assessment and an agreed level of difficulty. Exercises focus on event detection and response.
cyber scenarios	capabilities to build team based CTF competitions and realistic ICT environments fast and with selected configuration and parameters. With automation, pre-designed environments can be created quickly, saving time
user interface (UI)	customer learning experience starts with user interface (UI). The descriptive user interface saves the time of the teacher/practitioner and allows the participant to learn and retrieve more information for the exercise tasks: with up-to-date documentation, received hints, achieved checkpoints and milestones, timeline (if necessary) and progression in exercise. Possibility to interact with administrator etc. or team member (if necessary)
documentation and scripts	the documentation can be used to describe the environment, what to do in the exercise, and how to proceed. If, after a cyber exercise, you return to a certain point in the exercise, then with the help of documentation it is possible. The walkthrough guide instructs the trainee all the steps needed to go through the administrator's instructions include describing the various exercise-related scripts as well as the program code and contents in such a way that the solutions to the problem situations are also described appropriately
marketing; website information	upcoming exercises can be marketed in school course descriptions as well as on web pages. An email list with reminders adds value to training participants satisfied exercise advertisers promote the exercises to other exercise participants, so well-designed exercises will add participants to the course annual CTF competitions bring visibility to the training environment outside of school, even on a small scale
measurements	with the help of the indicators agreed in connection with the exercises, the agreed values can be measured from the exercise, which can be used to measure the development by comparing the results with, for example, the performance of other years
knowledge gathering	the exercises in the training environment develop according to the outside world and the feedback received, forming the best practices for continuous development

Overall requirements from table 5 contains the main eight areas of identified functional assets. Resources are the most essential part of the foundation of a

virtual cyber training environment that affects all activities. Organizing cyber range exercise requires human resources which are producing contents to the actual exercise, documentation, and virtual training environment, not forgetting marketing, and promoting the exercise. The learning activities carried out during the exercise are measured in the agreed ways. The data collected in Chapter 4 have been used in Table 5. Table 5 summarizes the conclusions drawn from the analysis regarding the design requirements for the cyber training platform. The utilization rate of the cyber training environment should be kept as high as possible. For this reason, it would be important to map out the different functionalities so that the training activities can be targeted at the right industries. Supporting the cyber training environment in a hybrid model, i.e., using it on-site or as a remote exercise, does not exclude any participants. Using a training environment based on the hybrid model also supports the teleworking models introduced during the COVID-19 pandemic. Organizing cyber exercises in on-site cyber exercises allows for more effective communication with other people in the room. The cyber training environment has not currently been audited to match any classified information, but it will be possible in the future if customers so wish. As shown in figure 35, the cyber training environment is suitable as a cyber training environment for almost all industries, provided that the training activities do not involve the use of classified information.

Cyber exercises usually consist of an operating environment with equipment that, based on a risk assessment, has been assessed to be exposed to a certain degree of threat. There may be vulnerabilities in the devices in your operating environment that could be directly or indirectly affected by the threat (figure 36).

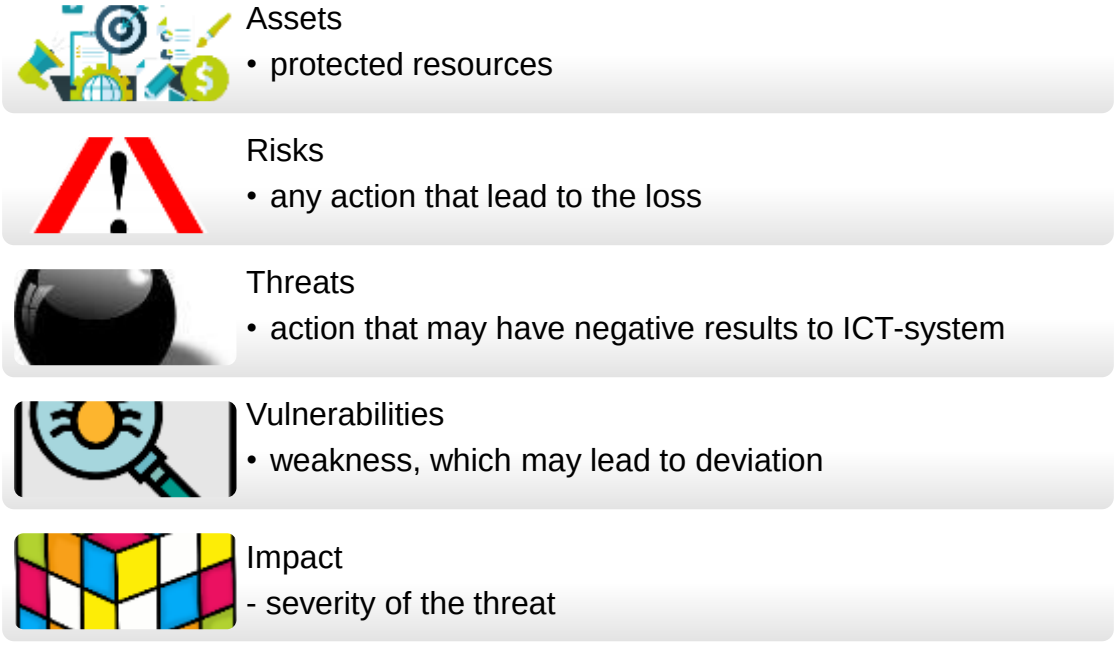


Figure 36. Coverage of the cyber range terms

As illustrated in figure 36, several threats can be associated with cyber practice. These variables, asset, risk, threats, vulnerabilities, and impacts presented above must be clarified before the start of the exercise. These illustrated terms can be found in every operating environment and can be accurately modeled in a cyber training environment. With the help of risk management, various implementation assessments can be formed for threats, as well as threats to the vulnerabilities of the equipment in the operating environment. This terminology can be used to describe all types of exercises, which can include one or more different threats and, if necessary, unexpected events. The equipment in the operating environment is described as an asset, which can be defined for each exercise, if necessary.

From an information security perspective, risk means a combination of the probability and consequences of an accident. In terms of information security, various scams, spam, intelligence and espionage, malware, and affecting the capacity of network connections are considered threats. In addition to the above, security threats include unauthorized access to the information systems, unauthorized use of the information, disclosure of classified information, corruption of the information, and destruction of the information. Equipment in data networks and systems, e.g., firewalls, switches, and processors usually include software that can be upgraded. These software programs may contain features that an attacker may take advantage of to gain access to information. These

vulnerabilities, or vulnerabilities, are addressed as they are identified. Unknown vulnerabilities are called zero-day vulnerabilities, and poorly made fixes, that is, vulnerabilities that can be exploited after an upgrade, are called n-day vulnerabilities. When a risk assessment addresses a vulnerability, it has a certain impact. From an information security perspective, the impact is a loss of availability, integrity, and confidentiality.

After defining the basic structure of the cyber training environment and the basics of the exercises, other issues related to the environment of the cyber training environment can be considered. Concept may also describe the features which maximize the benefits of using cyber range. Proposed concept also handles resources for the cyber range platforms maintaining operations. At the end the evaluation possible measurements are described for continual improvement which is based on continuous learning. Knowledge gathering by learning is an outcome of training in cyber exercises.

5.2 Implementing current state analysis into concept

At a moment, cyber range contains adequate level pre-selected exercises. Documentation of the exercises are found from the learn.xamk.fi -platform. As a possibility to expand cyber range functionalities, the cyber range needs different kind of exercises with new user interface. The platform's user experience would be expanded when documentation and help would aid learning during exercise. At a moment, four different scenario types have been validated, which may be used in top level selections:

- team based scenarios for example capture the flag (CTF), which the exercise goals can be changed or modified during the exercise
- individual assignments and exercises for cyber exercises (blue or red team)
- classroom lectures with details to fulfill given assignment and
- testing activities for selected network products

The purpose of the exercise for the participants' point-of-view is to gain knowledge. Knowledge is created to the exercise information flow by personnel. Participants and maintenance of the exercise focus to keep revealing interesting issues in exercise. Participants in the cyber exercise should be able to filter out the essential parts of the information obtained to complete the exercise and take notes to support learning. Cyber exercises are static state only during the

exercise. As in a real life, the environment and architectures are constantly evolving, and the same is in a cyber range. Cyber range and its exercises are developing further, and the participant may learn more during training if the scenario behaves unexpectedly.

Organization fails commonly to handle correctly its first faced incident of any kind. This happens because the organization has no previous experience of handling new issues. Realistic scenarios are based on currently going on campaigns which could be for example ransomware, DDoS attacks, insider activity or any other relevant incident which is required for training which the organization may not have previous experience. Increasing realistically for scenarios may need to be included “deep” learning. ICT infrastructure with user’s “own” email account may add an element of realistic behavior, which may add “hands-on” experience. As a computer-based platform, cyber range, which need resources for maintenance and updates. Virtual system is running 24/7 and is deliverable for customer by remotely or physically on-site. Maintenance or personnel of organization are evaluating platform and exercises from identifying key elements required for selected exercise. Successful exercise enables usage of measurements which contains values of performance.

As an outcome, cyber range is producing learning and documentation for actions of continuous improvement. Knowledge creates preparedness, which will be activated during actions of exercise. Picking a piece of an information flow and produce data collection of exercise will enable supportive actions for cyber range, and exercise data enable handling incidents in organizations network.

5.3 Cyber range task difficulty and cognitive workload

Exercises in cyber range environment and task generation need to be simple, but the complexity of scenarios is needed to set with the same level of organizations maturity level. If there are constructed complex scenarios with high workload and level difficulty is set too high, it might arouse problems with learning during exercise. There are three variables which may need to notice:

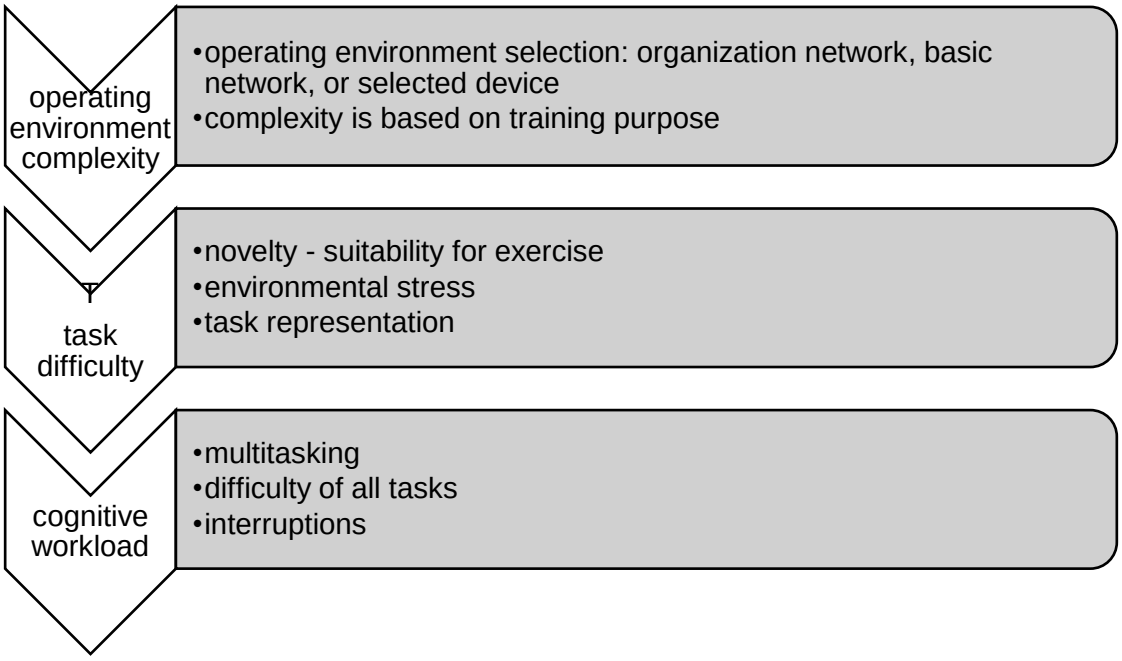


Figure 37. Influence related to operating environment complexity (Roque et al. 2020)

As figure 37 above shows, the level of difficulty of the operating environment should be set to a level that the participant can complete it to the end. If the difficulty level of the exercise is set too high, the participant in the exercise will not benefit from it. Task difficulty is an objective which is needed to set correctly in the planning phase of the exercise. Cognitive workload is based on the level of participants and their own abilities to work with under pressure. Workload must be optimized during exercise if it is not meant to use as measurable value. Cognitive workload means to exercise multitasking activities within the range of “possible to make“ and tasks are relatively easy to accomplish. With the exercise, there may be interruptions which also increase the cognitive workload.

The operating environment of the cyber exercise can also utilize cloud services and their platforms, if necessary, is the cloud service provider provides such a service. Cyber exercises might also use IaaS public cloud services because of ephemeral nature of training, event or testing if no classified information is used during exercise (Ravello Community 2016). Through the cloud service, it is possible to mirror the cyber training environment, for example from the server room to the training environment, thus providing a realistic training environment.

(Ravello Community 2016). The key challenges for using public cloud on cyber range exercises are (Ravello Community 2016):

- different network & security appliances
- no layer two networking on public cloud
- virtual environment (for example VMware) workloads
- port mirroring
- difficulty in creation, deployment & control

5.4 Functionalities for cyber training

The cyber training environment should focus on those industries where there is demand in the province. As there are only a few cyber training environments in Finland, potential users can come from all over Finland. Training may give effective results in places which are active around the clock. Cyber exercises in different industries will be largely focused on the subjects taught in the school. Security operation center (SOC) provides round-the-clock operations, and SOC-focused cyber drills can be implemented for all industries. Cyber drills for IT information systems and OT information systems can be organized in a cyber training environment if the functions can be implemented as virtually. Threats to critical infrastructure will increase in the future as they are more affected by digitalization in the context of equipment modernization. Cyber exercises in health information systems are also becoming more common in the future. Health information systems often contain sensitive personal information that is targeted by attackers (figure 30).

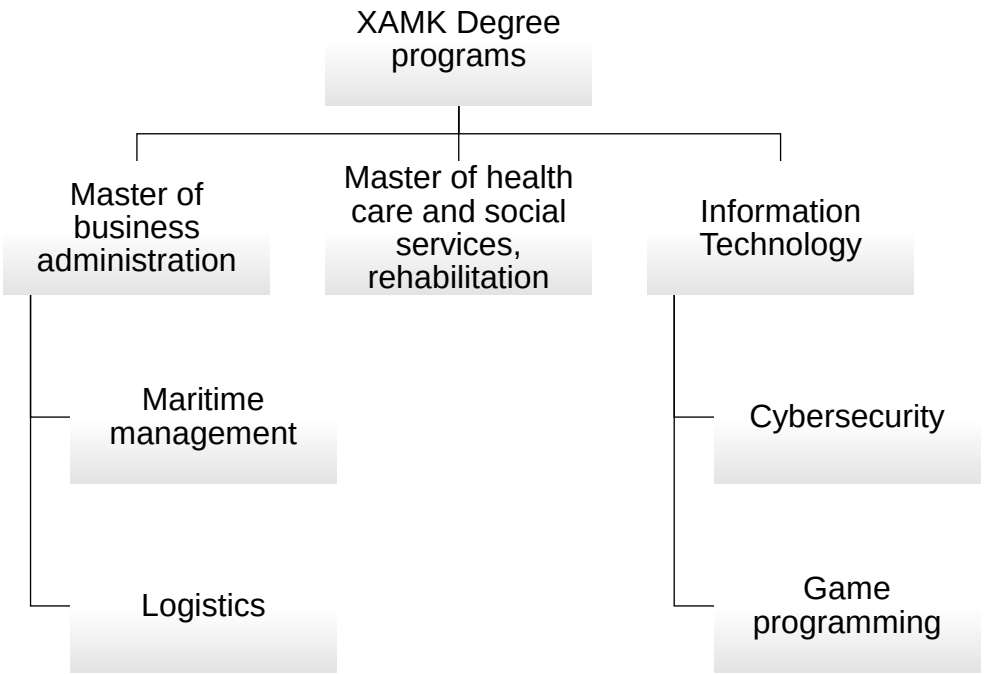


Figure 38. Fields of training identified to Xamk's cyber practice

As shown in figure 38, virtual cyber exercises may also be held for other training programs at Xamk. Through the exercises on the virtual cyber training platform, there are three types of training programs in Xamk (figure 38) that are suitable for students to practice cyber. This figure does not rule out the need for students in other degree programs to conduct cyber exercises.

In addition to training programs, Xamk's virtual cyber training platform is suitable for training in the following functions:

- training in Security operations center (SOC) functionalities
    - centralized control room for threat and incident management
- training of information- and cybersecurity functions
    - ICT/ICS/IoT -infrastructure training
    - IT service-, technical- and application management
- critical Infrastructure protection
    - air, railroad, maritime & land (road), energy etc. where applicable
- healthcare
    - sensitive information protection

The intention would be that all industries could use the cyber training platform in their cyber exercises to carry out their own exercises. The cyber training platform is also suitable for infrastructure design in different industries for testing various network devices and configuration. As technology advances, so does communication, and if necessary, support for Internet of Things (IoT) devices can be added to the cyber training platform. Process automation attacks can be safely practiced in a cyber training environment. The cyber training environment also provides a training environment for exercises related to the defense of maritime information systems and road and rail network information systems.

Security controls on corporate networks are usually classified information, and organizations are reluctant to disclose this to third parties. However, the training is possible in such a way that the cyber training can include different equipment from a specific manufacturer, which can be used to simulate a similar environment or function.

5.5 Technical functional details for cyber range

It is advisable to integrate the functionalities of the cyber training environment into a framework for threat management and event management. The most common knowledge bases of reference used in cyber exercises are Mitre Attack

and defend. Mitre knowledge bases contain a description from the point of view of the attacker as well as the defender, which can be used to protect against unauthorized actions. Cyber exercises can include functionalities that take advantage of vulnerability management frameworks. One of the frameworks developed for vulnerability assessment with web and application security that is called “Open-Source Foundation for Application Security Project” (OWASP) (OWASP, 2021). OWASP top 10 is designed to increase security awareness about serious security vulnerabilities in various web applications. OWASP top 10 is updated regularly. OWASP's top 10 incident response guidance provides users with tools and best practices for managing web applications. Latest OWASP has been updated in 2021.

The Common Vulnerability Scoring System (CVSS) is a known open industry standard for assessing the severity of security vulnerabilities in computer systems. In the CVSS system, vulnerabilities are assessed on a scale of 0 to 10. Severity levels are defined as a score of 0-3.9 low, 4-6.9 moderate, 7-8.9 high, and 9-10 critical. CVSS scores are well-suited to a cyber-training environment, as they can be used to implement combinations of different vulnerabilities and their scores for training. Realistic vulnerabilities can be exploited in a cyber training environment by using out-of-date applications as well as an external threat to exploit the vulnerabilities. Companies are working to update vulnerabilities that currently have a critical (9-10 points) CVSS score quickly, but high- and medium-level vulnerabilities are updated according to the normal update cycle. This could allow an attacker to exploit a combination of middle and high-level vulnerabilities to gain access to information.

For example, in virtual cyber exercises, it may be necessary to include external threats in the exercise. These external factors may include vulnerabilities inherent in the software or may be a threat. An external factor can also cause unnecessary background noise to network traffic, or the author can encrypt communications on the corporate network or add an entry point to the intranet.

Possible channels of influence of the external threat factor:

- TOR-network and its exit points
- peer-to-peer networks, “Torrent” client
- VPN-connections and its management
- stock markets (including bit-, Dogecoins etc.)
- cloud or selected web services,
- network background traffic generation
- threats from bot-networks with software-based artificial intelligence (AI)
- hidden device with sending anomalies in the data flow of network
- other services (NTP, bank, blockchain, bitcoin, stock markets, RSS-feed etc.)
- phishing site

Any external element that can be used in the exercise, which can be virtual, can give the training environment a sense of reality, giving the trainee concrete information about protecting their environment. In addition to external factors, additional functionalities related to these threats can be implemented in the exercise, which are described in the list below.

These features might include following:

- user has in exercise email account in use (ability to send and receive emails) and receive maybe sophisticated attempts
- interactive features such as encrypting/decrypting, chat-box, watering holes which are used for offensive actions against the ICT-environment
- organizational network infrastructure in use (PKI-infrastructure)
  - attacker might use stolen certificates/credentials
- automatic or scripted network behaviors etc. background noise.
  - simulated internet background noise, that can be included for example randomly generated ping requests etc.
- some unexpected incidents (scripted etc.) in the middle of exercise scheduled offensive actions
- story documentation with timeline and provided walkthrough guide.
- teamwork is always increasing customer experience
- multiple solutions as for an exercise

Using only selected functionalities for usage of exercise may help for scoping exercise for suitable requirements. The requirements may use key performance indicators which measure the selected areas of exercise and participants.

5.6 Key performance indicators (KPI) for cyber range

Key performance indicators (KPI) for the cyber range actions are an effective way to measure the success of your cybersecurity program and gives suggestions on future decision-making. According to the study, the pattern for effective

cybersecurity KPI could be: “How much time it takes between threat detection and response. How much is expected recovery time after cyber incident?”

Possible cyber range KPI measurements might include

- intrusion attempts
- meantime to detect threat (MTTD), which means how long it takes to identify threats and potential cyber incidents?
- meantime to acknowledge threat (MTTA) which means average time to begin working on an issue after receiving an alert?
- meantime to contain attack vectors (MMTC) which means how long it does to contain identified attack vectors?
- meantime to resolve threat (MTTR) How long does it take your team to respond to a threat or cyber incident once the team is aware of it?
- number of cybersecurity incidents reported during exercise.
- non-human traffic or lateral movement?
- virus infection monitoring. Phishing attack success rate?

KPIs could also form the question: “how learning can be measured?” The answer to this question may already be partially in place. Measuring learning in virtual exercises can be done through feedback surveys, which also provide information on how the exercise can be developed in the future. The answers to the feedback form can vary and are usually related to the illogicality observed in the exercises. Learning is an ongoing process that aims to develop competence to a higher level.

Cyber range actions are executed in virtual environment. The capabilities for virtual environment automatic measurements and monitoring enables effective automated feedback for cyber range platform administrators. User behavior monitoring service could give feedback directly by platform itself. Directly monitoring users’ actions in virtual platform could give tacit information for maintenance which could improve or comparing scoping next training exercise. At moment the platform is measuring maintenance functions which includes capacity of the processor and memory usage etc. Visual KPI measurements could inform about interaction between team members and teams and may include also time-consuming methods (information searching in platform etc.). Leadership and actions in the team based on communication in the team, which may also be documented for evaluation purposes.

Table 6. Key Performance Indicators (KPI) for virtual cyber exercises

KPI type	description	measure purpose
visual	interaction (individuals, teams), leadership & actions	time between detected activities
platform-based	user behavior monitoring, platform behavior	evaluation and reducing tacit knowledge
learning	learning monitoring	continuous development of operations
KPI measurements	technical monitoring (intrusion attempts, MTTD, MTTA, MMTC, MTTR etc.)	analysis of technical situation information

Table 6 describes the gauges and how they could be used on the exercise platform and in the exercise itself. The functioning of an organization can be developed using the maturity model method. Based on selected organizational exercises, the cybersecurity maturity level determination is possible with four level determination, which might also be recognized as KPI. For example, cybersecurity maturity model exercise: Security Information and event management (SIEM) is observing systems including networks, which forms a base level in the maturity model. Level two maturity model includes analytics and utilization of software called security orchestration, automation, and response (SOAR) to use for collaboration and automation. Maturity model could include for example 24/7 network data monitoring. Increasing the level three might support for incident early detection. Performance will stop the attack at its early stage, which may include incident investigation remotely with automated features of threat hunting. Highest maturity level four might include extended capabilities with automated incident detection with automated playbooks of incident handling. With customized threat intelligence and monitoring systems which provide visibility of keeping network data “clean”.

5.6.1 KPI by cyber team exercise

The virtual training platform offers a variety of cyber exercises that can be performed individually or in a team. Team-based cyber exercises can include a group exercise, or an exercise between groups where the groups are against each other or collaborate. Teams can be modified in the cyber exercises by the need and there might be different teams even for individual tasks (management, maintenance, observation, information gathering etc.).

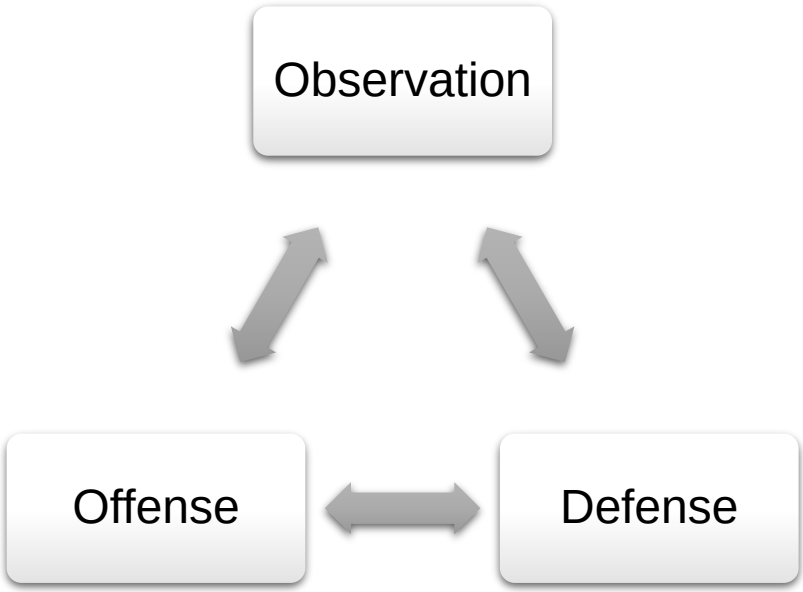


Figure 39. Triangle of team exercise

The figure 39 above illustrates the arrangement of groups in cyber exercises into three different categories that form the functionalities of the exercise. The management of the exercise is in observation, which will also produce maintenance functions and is interactive with both offense and defense. Offense is practically a red team designed to focus on designing different attack scenarios. Defense means a blue team specializing in defense in cyber drills, which can be formed in cyber drills as needed. Blue team's function is defending the virtual network and prevent any offensive actions detected. Collection of KPI's requires observations about the exercise actions, which may need also deep knowledge of behaviors of malicious acts or threats in the current exercise. Supervisors monitor the performance of both teams during the exercise and monitor cyber exercise events, including the use of automated scripts. Automated scripts can also be used to measure cyber exercises that are set to start at a specific stage of the exercise. Typically, different perspectives are used to model the threats used in cyber exercise to focus the exercise on the desired issue. The content of a cyber exercise can thus become a complex entity, which may require the creation of new types of teams.

Exercise might contain management White Team (WT) responsibility is to carry out the exercise, collect information from exercise and monitors scenario and gives feedback for participants. Sometimes purple team (PT) may be suitable for exercise. PT responsibility is to collect information between red and blue team, may include members of both teams. Cyber exercise may also include

use of several blue teams. Cyber exercise situational awareness with WT. Functionalities and infrastructural maintenance may be used as green team.

Measurements of virtual exercises may need to identify and evaluate based on need and purpose. Cyber exercise may contain different kind of virtual exercises which might include aspects of:

- cybersecurity competitions (standalone or federated for other cyber range) including capture the flag (CTF)
- use of selected measurements by the objectives
- security testing
- measurements related to testing objectives
- security research
- research objectives. Security-related research can be lengthy
- information security training
- as part of the lessons, the cyber exercise might contain study related material or virtual tasks
- development of cyber capabilities with competence assessment
- measurement of selected objectives
- development of cyber resilience
- measurement of selected objectives

Pre-agreed indicators can be attached to cyber exercises, which can be used to monitor the long-term development of the organization, the individual and the exercise itself.

5.7 Scenario types for different industries

Virtual cyber exercises can include different levels of industry-specific exercise scenarios that can be practiced in a closed environment.

These industry-based exercises can be set on three level:

- 1st Level: Skills development labs
- 2nd Level: Individual and team exercises
- 3rd Level: Attacks and war gaming

Level one exercises mainly include information security lessons as well as teacher-assigned assignments. Level two exercises may include broader scenarios that can be practiced individually or in a group. Level one and two might contain forensics or time-consuming tasks of reverse-engineering. Level three exercises are offensive exercises that groups (red versus blue) do to each

other. All levels might also include assignments for situational awareness (Network monitoring and reconnaissance).

Table 7. Scenario examples for maritime industry technology

action	system	description
spoofing	AIS	analysts from “Sky Truth and Global Fishing Watch” find out that ships’ locations have been manipulated with a shore-based receiver via the automatic identification system (AIS), which shows location, course, and speed of speed. International law requires commercial ships to have AIS transponders. While military ships are exempt from the requirement, many use AIS transponders under an alias while navigating at sea (BBC 2021)
phishing/ spoofing	email	cyber-attack was implemented through a phishing email including voicemail-themed attachment, spoofing the tug ship’s operator (Macola 2020)
ransomware	malware	ransomware is identified as a potential threat in the industry at 2020 (Macola 2020)
DDOS	routers	ship is unable to reach Internet based connections. Obtain Internet access for ship systems

Table 7 illustrates example exercises that could be organized for the maritime industry. Tabletop exercises and cyber ranges can be good complements, helping organizations understand their larger risk profile. Industry specified examples of cyber range exercise has been identified. These industries specified exercises has target outcome, which may help for resolving occurring incidents in the future. Industries which are focused on activities on sea are requiring functions focused by Maritime Industry technology. Ships are using a system called Automatic Identification System (AIS) system, which is used to identify ships cruising to the international seas. The ICT/ICS-systems used in this industry may require industry specified actions. These systems may be used as “closed systems” at a time when ships are cruising on the ocean. Network connection might be used via satellite or any other suitable method etc.

Automation systems have similarities as regular ICT-systems. ICS-systems are automation systems which carries signals and process information. ICS-systems are usually categorized as critical infrastructure which are built in closed

environment. Indirect influence on these systems is possible, for example with transferrable media, when the system is updated during maintenance.

Table 8. Scenario examples for ICS technology

action	system	description
value change in configuration	ICS	water tank control system (Xamk cyber scenario) has possibility to change values in its system. Protect the water tank control system
insider	ICS	insider has uploaded malicious code in ICS systems. Find the infected system, isolate it, and restore the system to its defaults and run backup
network detection and response (NDR)	ICS	know your network's traffic. Find source for unidentified network traffic, isolate infected devices, and correct source values
credential hopping	ICS	an attacker has compromised an office network by using a hijacked Internet browser cookie. Since then, he has accessed servers on the intranet. Find out what information the attacker may have had access to

Table 8 describes example exercises that could be organized for the energy sector. Other cyber exercise related exercises are team competitions which could include "capture the flag" etc. type of competitions.

Table 9. Scenario examples for cyber range

type	action	description
CTF	team play	red (attacker) vs blue (defender one or more teams) teams exercise for selected scenarios
test	device configuration tests	network devices with their configurations are suitable for testing in virtual environments (for example Secure Network Setup, Web Application Security Analysis etc.)
test	research	research can be done via cyber exercises, which supports testing activities and validations of test results

Table 9 describes example exercises that could be organized as competitions, for example. These basic types of examples are typical cyber exercises, which contains the elements which are typically encountered in real life. With industry-

based knowledge, these exercises are realistic and learning to handle industry-based incidents is getting better.

5.8 Technical platform of cyber range

The features of the technical platform play an important role in terms of cost as well as the features it provides for cyber exercises. One of the key possibilities of a virtual training environment is to separate the training environment from all external data networks. The long-term development of a virtual platform requires modularity and a long-term development plan for the hardware and software used. Third-party hardware added to the technical platform may require some form of collaboration through different equipment manufacturers, allowing students to learn about the latest equipment on the market during cyber exercises. The cyber-training environment also supports OSI-compliant Internet services. These services need also public IP addresses in the closed environment and real geographic locations. Platforms need to include internet service providers Internet core services like DNS, NTP and web-services.

The virtual training environment also requires the possibility to use services familiar from the Internet, which can be created in the training environment as simulated services. Simulated services enable a realistic experience for cyber training, incorporating background noise through a variety of automated functions. In a cyber training environment, resources are usually at minimum level, and it means automated services (software robots, scripts, virtual backups) that are managed centrally.

5.9 Facilities and marketing of virtual training environment

A virtual cyber training environment develops best when used extensively. External user groups provide funding for the maintenance of the training environment, if desired. Advertising the virtual training environment in various publications, on the Internet and on the school's own intranet enables the sharing of information about the existence of the training environment. Commercial and educational cyber learning environments in the United States and Europe are constantly promoting their services. One of the most useful ways to promote a virtual training environment is to develop the facilities of the training environment together with nearby companies. Various cybersecurity competitions also

create a brand and serve as advertisements. Whether the competition is big or small, it may exceed the new threshold, with the news itself serving as an advertisement for a virtual training environment. Satisfied users are the best advertisers of the virtual training environment.

Physical spaces where cyber exercises can be performed can also be considered as an advertisement for a cyber training environment. The exercises in the virtual training environment can be considered remote, but one of the purposes of the exercise is to introduce the trainees to each other and to improve different levels of communication, so the physical facilities for implementing the training environment allow for a better outcome of the exercise itself.

6 RESULTS, CONCLUSIONS AND DISCUSSIONS

This chapter describes the results of the study and presents the concept of cyber range functions at Xamk. The Conclusions' section contains views on the development of cyber-training capabilities in the future.

6.1 Answer for research question

CTF competitions are competitions created for a specific type of group, the topics of which are typically related to cybersecurity, for the purpose of ranking competitors' results. The most popular forms of CTF competition are jeopardy, hack quest and attack-defense, which also contain explanations and analyzes for scoring the game. In the competition, points are earned by collecting flags, which are usually random strings embedded in challenges. After the competition, a report will be created, which may include, for example, information about the background of the exercise and the participant, the methodology used, the results of the competition and related discussions. Xamk's concept for virtual cyber exercises is illustrated in Figure 40.

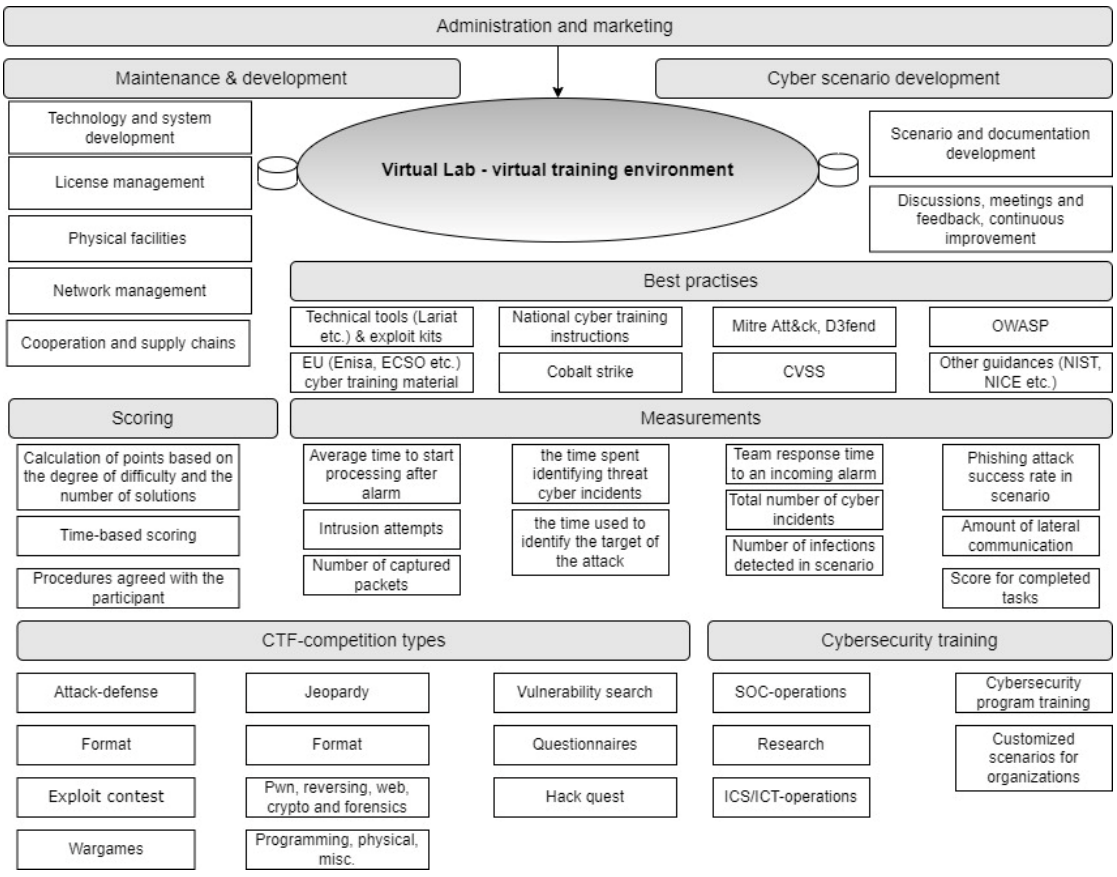


Figure 40. Cyber range concept

The issues related to the concept in Figure 40 are described in the answers to the research questions. *Research question: What functionalities will be most beneficial for the concept of cyber range?*

The concept of virtual cyber training should consider the target group for which the exercises are performed. The ability of Xamk's training programs to take advantage of the cyber training platform is a clear advantage that can help increase cyber awareness. In addition, local businesses can practice on a virtual cyber training platform. Opportunities to increase the use of the cyber training platform are to organize annual events, which can be e.g., CTF competition. In general, every cyber training platform in the world supports SOC activities, which can be used to implement a wide variety of cyber exercises.

Best practices were found in the virtual cyber exercise environment and the exercises held in it through academic research. Academic research contained useful information for this research. However, it was interesting to see how different cyber ranges were implemented the features of their own. According to the approach of scientific research, in order to optimize resources, there should be a lot of automated functions in the use of the virtual training environment, e.g., automated training environment creation, network background traffic, etc. This should be done, for example, with some kind of template that the user could start when starting the training. In order to calculate the points, the functionalities should be ready, which would allow the participants of the exercise to be ranked. These functionalities are:

- in CTF competitions, it is important to create the right kind of event that is suitable for the target group. After that, you have to choose the size of the group and agree on the rules and criteria for scoring
- typical types of CTF competitions are jeopardy, attack-defense, and hack quest, where participants solve problems ahead one at a time. For each solution, the participant receives a point.
- CTF competitions can also use a specific theme or topic suitable for the target group. For example, in the "format" competition, each challenge is a separate entity, downloading a file from the server that participants must find by any means of the flag. In a "Pwn" contest, participants use a command prompt to try to access a remote server that is running the vulnerability. Reverse engineering, crypto, forensics, programming and web challenge are also available forms of competition
- during the exercise, groups that attack and defend should have real-time information available to the white and purple groups so that the exercise follows the cyber exercise script

- scoring of tasks in CTF competitions can be done in different ways and also considers the level of difficulty of the tasks. Time can be used as one of the scoring criteria. The number of solvers in the tasks can also be a factor that decreases the points, in which case the first solver gets the most points
- the most useful functionality of a virtual cyber exercise was the ability to do any kind of cyber exercise quickly and reliably as needed. Fast loading of cyber exercises even with slower internet connections is also considered a useful feature
- documentation added to the virtual cyber exercise and the purpose of the tasks were perceived as a feature that increases customer satisfaction. It would also be useful to have answers to questions raised during virtual cyber exercises, if necessary. Frequently asked questions (FAQ) about cyber exercises and the answers to them add value to the participant
- data collection and continuous development of reporting enable tacit data collection. With the help of reporting, it is possible to develop activities and enable the monitoring of learning
- the user interface should be able to log in by groups (red, blue, white / purple etc.) so that the groups can communicate with each other
- the feedback and the final meeting after the exercise should be a clear and supportive one for the participant's learning
- best practices also include the use of various offensive attack and defense concepts and instructions in a virtual training environment (Mitre best practices, OWASP, CVSS, NIST, NICE, etc.)
- national and EU level cyber training guidelines are also utilized in a virtual training environment if possible

What are the key functions for the cyber range?

Important features of the virtual cyber training platform are a modular operating environment that allows the system to be updated as needed. Automated functionalities in the virtual environment reduce maintenance resources. An important thing is the user's experience of the response time of the training environment, which must remain small even if large training groups are involved in the training. Maintenance should see in real time how much hardware power is being used by the virtual environment and be able to increase capacity as needed. One necessary feature could be to freeze the training environment for a certain period of time, for example, if there are breaks in the training for some reason. Building a virtual training environment in several layers could add value to the training if you want to practice cybersecurity on a large scale. On the first layer, for example, the equipment in the network environment could be hardened. During the configuration of the devices, a connection to the undocumented subnet of the training environment would be detected, which would be

determined. There could be problem areas in this second layer that require reflection and decision that should be resolved during the exercise. Exercise should use logical and perhaps even physical problem-solving, depending on what kind of exercise environment is built. If physical facilities are used, then the existence of physical devices can also be utilized. In this case, it would be possible to use the Insider threat, for example, in the exercise, and one of the tasks in the exercise could be to know which of the people in the group is Insider.

What features are needed to maximize the benefits of the cyber range?
In a cyber exercise, it is important to identify the participant's level of competence and, based on this knowledge, create an exercise that will enhance the participant's learning. It is possible to find out this level of competence in advance from all trainees, in which case different tasks that develop the level of competence can be created for the exercise in groups, or even on a personal level. If the exercise had the opportunity to use alternative approaches according to the level of difficulty (beginner/professional), the participant could potentially speed up their development during the exercise. The training environment should have procedures in place to score the various activities performed by the participants. Observers should see the preparations of the attacking and defending party so that they can implement the learning. The procedures in the training environment should be used to identify things that the participant has done well in the exercise, as well as things that need to be improved.

In practice, this means that training elements must be designed for each CTF competition for a specific group of users. For example, cybersecurity students need general exercises provided by the SOC environment through wide-ranging anomalies. Gaming programmers need hands-on practice to test the security of their applications for vulnerabilities. Forensics researchers can make their own observations about the above and possibly perform reverse engineering if necessary.

A virtual training environment requires sufficient capacity to operate to maintain adequate running of virtual cyber workouts without sacrificing performance. Cyber range and its exercises should focus on realistic simulations and based on real life threats and incidents. The layout and configuration of the devices in

the virtual training environment should be done so that the configuration of several similar devices does not have to be done many times. In addition, shortcuts could be added to the right mouse button to perform certain functions. If the training environment is a large entity, then things that make it easier to use, such as saving the scripts used in the training environment, speed up their use if the same scripts often do not need to be rewritten and the exercise allows scripts to be saved. The virtual training environment should support a feature in which a surprise event occurs during a certain period of time. The trigger for an event could be an event after a certain procedure, or an occasional thing that would get the attention of the group participating in the exercise. If necessary, a surprising event could be used, for example, to get attention to a particular place, or even out of the threat itself, in which case it would be a distraction designed for cyber practice. The benefits can be, for example

- user-friendly training environment
- high-quality exercise scenarios that allow you to perform individual or multiple exercises in different ways
- automated actions to make the cyber learning environment feel like the real world to the user

What are the key resources needed for the cyber range?

Maintaining a virtual training environment requires planning and continuous development. Resource-intensive maintenance functions include software updates, license and vulnerability management, and ongoing documentation maintenance are essential, not forgetting the maintenance and development of components and network equipment. The virtual cyber exercise includes an exercise environment, performance-related documentation, material related to the exercise, estimated schedules of events for the exercise as well as user support. If cyber exercises also include physical elements, then the exercises related to the use of space and possible physical equipment must be considered in larger-scale exercises. The necessary resources are:

- with regard to marketing, consideration should be given to making invitations to CTF competitions and to notifying various stakeholders and potential participants of various cyber events
- developing and maintaining a virtual training environment requires human resources as well as funding for licenses
- in terms of stakeholders, customer relationship management is also part of cyber training
- however, the most important thing is to teach cybersecurity, which enables teachers and students to work together to learn and contribute to the use of the virtual learning environment

What are cyber range training evaluation and measurements of performance?
Metrics related to cyber drills can help with training development issues, such as connection speed, processor response time, and memory usage optimization. Cybersecurity-related metrics can help measure learning as well as assess response times. The metrics used during a workout may be based on timeline utilization and may be defined on a per-workout basis prior to the exercise.
In connection with cyber exercises, it is possible to measure the time spent on observations made by individuals as well as the communication within the group. The number and quality of attacks by the red team is also measurable, so that the defensive actions of the blue team can also be measured in terms of response time. Different metrics can be planned for an exercise planning meeting. Perhaps the most important indicator, however, is the participant's feedback on the training that has been completed, which allows the exercise itself to be further developed into a better whole. The indicators that may be used in the exercise may be, for example:

- number of intrusion attempts
- how long it takes to identify threats and cyber disruptions
- the average time to start processing incident after receiving an alarm
- number of captured packets (if used in the exercise)
- how long does it take to identify the target of an attack (attack vectors)?
- how long does it take for a team to respond to a threat or cyber event when the team is aware of it?
- total number of all cyber incidents and threats
- amount of lateral communication in the training environment (machine-generated data traffic)
- the number of viral infections detected in a cyber training environment during training
- phishing attack success rate
- score for completed tasks

6.2 Roadmap for implementation of proposals

The proposal for a virtual cyber training platform concept requires resources, planning, and possibly financial investment. After the acquisitions, system installations and testing also take time. Figure 41 shows the time it may take for different functions. The roadmap in the figure 41 above depicts the order in which the new virtual cyber training platform concept can be launched. With the help of marketing, the virtual cyber training platform is made known which can be implemented, for example, with the help of the Internet. It would be a good idea to create several cyber exercises for the virtual cyber training platform, the most suitable of which would be available to users at any given time. Once a

year, the timeliness of new cyber training platforms should be assessed, needs to be identified, and future purchases considered. In the future, it will also be important to improve and update new physical cyber training facilities. At the appropriate stage, the organization of annual cyber practice competitions should begin. The competition may be small-scale, sponsored or promoted.

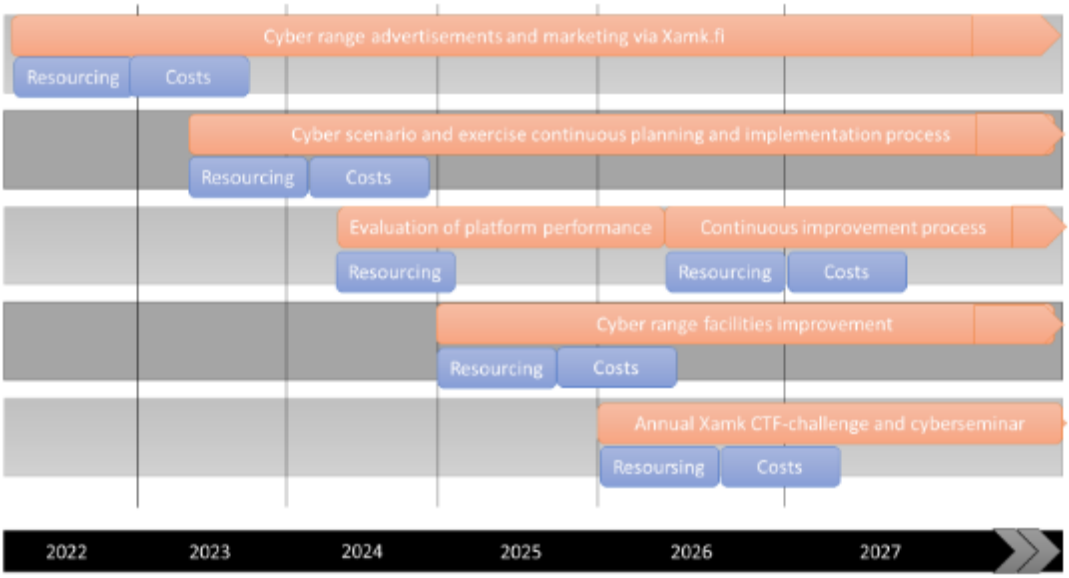


Figure 41. Roadmap proposal for implementation process of cyber range concept

The implementation of the proposals according to Figure 41 can also be utilized in a way that deviates from the proposed schedule. Key features to enable cyber range activities for big audience:

- easy way to enroll and participate in the cyber range exercises (pre-made, customized scenarios of full live/CTF-challenge) via Xamk.fi pages
- advertisements of the cyber range capabilities and references by satisfied customers in commercials
- cybersecurity education may include annual CTF-challenge or red/blue-war, which may include commercial challenge for everyone. CTF-challenges may be included under annual changed theme, but visibility is the key factor if local media is writing about it
- resources are also needed for maintaining the cyber range. For example, some companies have their own, separate staff for cyber-training platform operations.

The current Virtual Lab system is suitable for cyber range activities such as cyber scenarios and exercises which are need for planned and implemented. Planning phase which is including storylines needs resources and may need financial impact. Key features for the Virtual Lab system and its improvements:

- virtual lab system needs constant attention and a roadmap for ten years. The roadmap includes all project manager's activities, such a milestone. All implementations for the cyber range scenario automation and software artificial intelligence should include in the roadmap
- virtual lab environment might be included also tabletop exercises, hybrid exercises which could use for example laptop computers (external storage) and maybe even co-operation between another cyber range environment (native or abroad)
- The purpose of the roadmap is to show long-term plans for cyber range and roadmap attracts potential investors or sponsors. Roadmap is also key factor for marketing cyber range different industries

Communication and exchange of information between participants in the virtual exercise is part of the training procedure during the exercise. Cyber scenarios and exercises planning may be scheduled periodically, and post exercise actions evaluated by participants and administrators. With received feedback, it is possible to upgrade virtual contents of the cyber exercises for the next training if necessary. Using a physical building as part of a virtual cyber exercise may be part of a cyber training plan. Suitable facilities and sophisticated upgrades for rooms may help participants to achieve set goals for exercise. Key principles to receive information for continuous improvement: after cyber exercise "hot wash" – meetings and minutes of meeting, feedback is needed from observers and measurement metrics from exercises.

As a summary, the cyber range and its activities are all related to each segment in the training plan. Participants in a virtual cyber exercise can represent many industries, but the exercises are aimed at students and those working in the field of cybersecurity. Cyber exercises need a modern platform which is constantly evolving and improving its services (long-term planning). The platform requires resources for generating scenarios and exercises. At the same time, the virtual platform itself and cyber range environment requires focus and requires realistic background noise (Basically from other internet services). Continuous improvement needs information from participants of the cyber exercises and from environment, the people of cyber range maintenance.

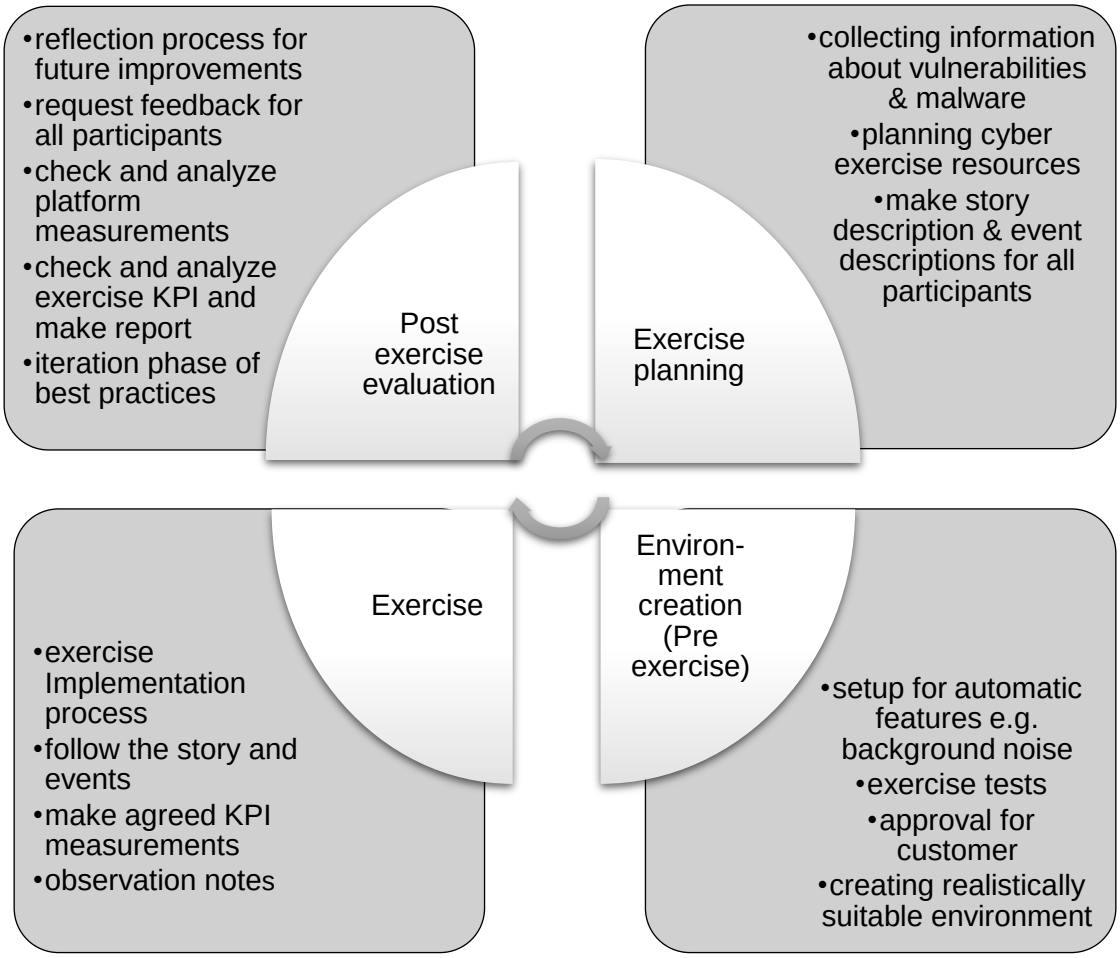


Figure 42. Four phases for cyber exercise planning

As illustrated in the figure 42 above, virtual cyber training involves four different steps that are exercise planning, environment creation (pre-exercise), exercise and post exercise evaluation. Exercise planning is an important phase of the cybersecurity because without objectives the training does not provide learning as an outcome and results cannot be measured properly. Planning phase contains resource allocation for entire cyber exercise because organizations differences about guiding principles, tools, processes, and environment must be similar stage in the training. Exercise needs also suitable story (Master scenario event list), including participants, injects, execution order of incidents and normal working day routines which may also include background noise. Post-exercise evaluation includes going through the exercise, receiving feedback from participants, and extracting the data collected in the measurements. Finally, a report is compiled on the information collected.

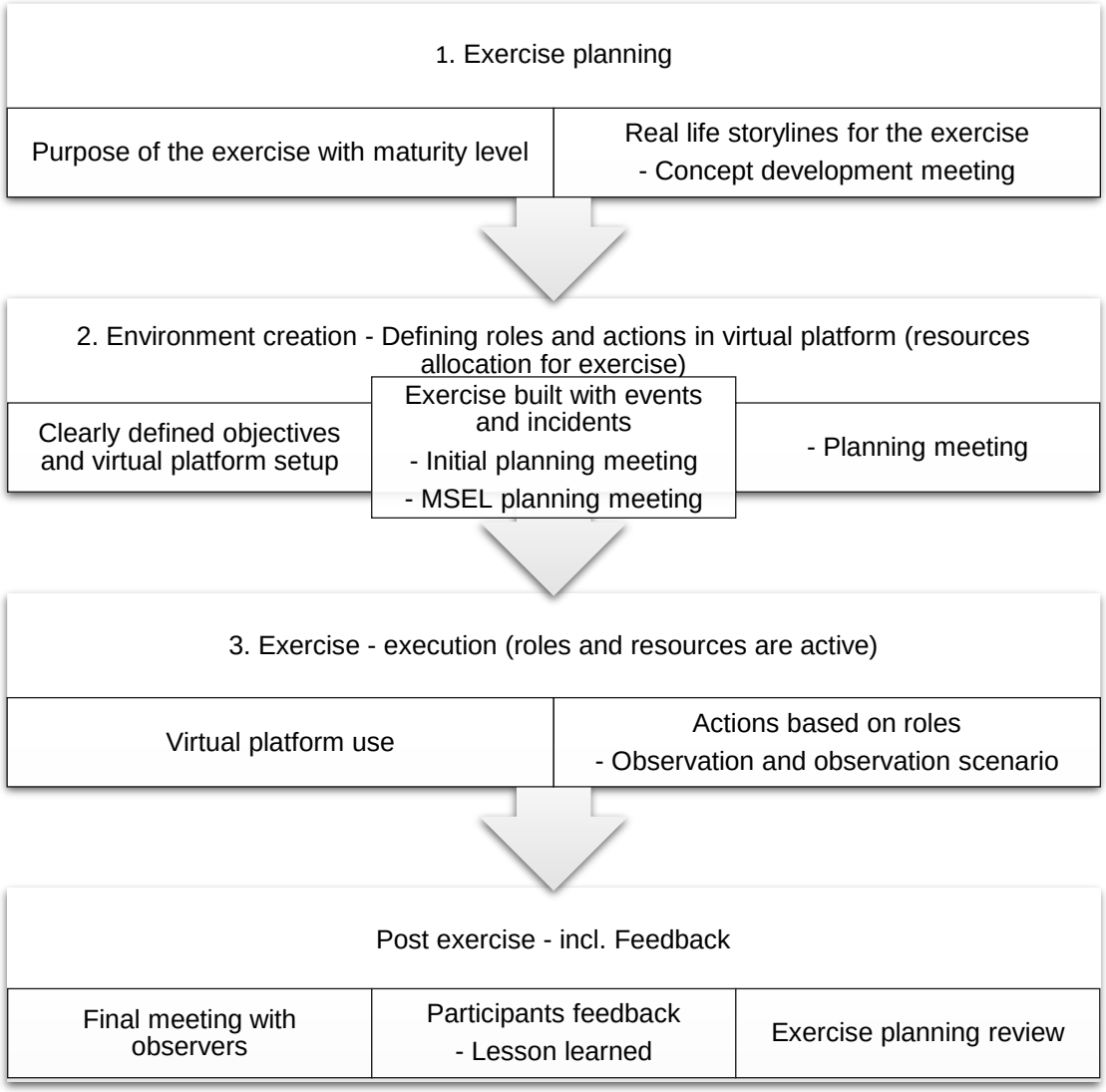


Figure 43. Process for planning cyber scenarios and exercises

As illustrated in figure 43, the objectives of the cyber exercise planning are clearly defined cyber scenario objectives and outcomes. In the cyber exercise there must be rules of defined engagement for red team which will enable planned impacts. The outcome of the exercise can be for example a defensive checklist of required actions against the offensive actions in the organization's network.

6.3 Roadmap for improvement path of Virtual Lab infrastructure

Realistic environment with current security incidents with some recognized vulnerabilities aid cyber exercise to reach goals for learning from exercise. The created documentation includes story, incidents, exercise approval tests, observation guidance and walkthrough paper (estimated). Also, feedback forms need for to be ready during exercise, the same as war diary/journal.

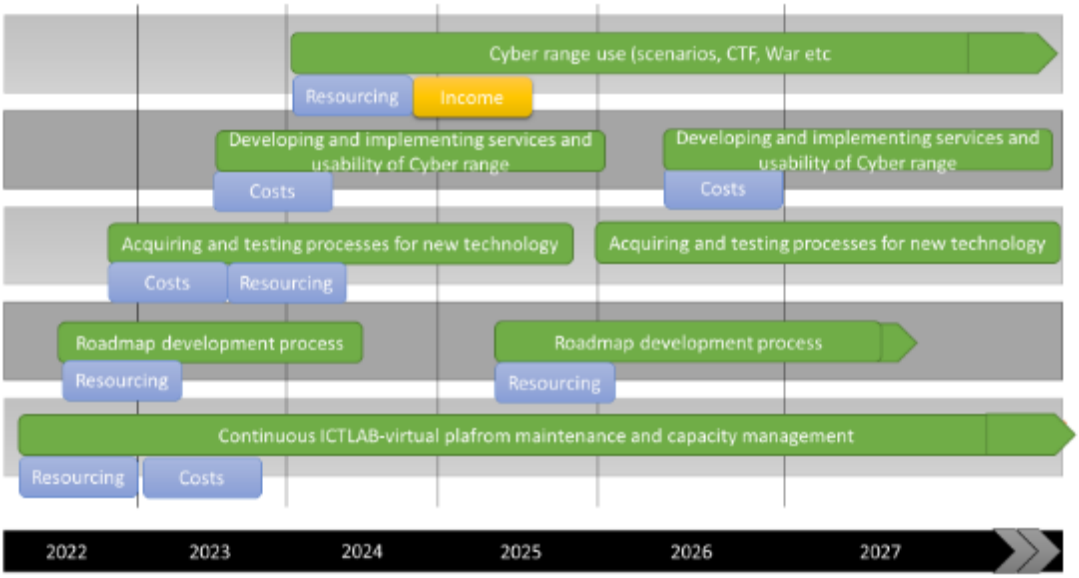


Figure 44. Roadmap for planning process for virtual platform development

Figure 44 illustrates a roadmap for using the cyber training platform by time window. The design and use of the cyber-training platform are described in the top line, and the other lines describe the estimated development times related to the development. Selecting suitable objectives for cyber training:

- Start discussion with organization requested objectives: Usually related to awareness, preparedness, and coordination
- Select suitable objective(s) with selected effectiveness relating to cyber education
- Prepare for evaluation of organization's incident reporting and analysis guides with guidance for improvements
- Prepare for reaction and detection of offensive actions in the training. Also, with purpose of impact of continuity management
- Select what functionalities are needed for protective methods and possibility to find and fix vulnerabilities

These roadmap actions are indicative only. In practice, planning is affected by the number of staff available, the availability of different software licenses, and the complexity of the scenarios created.

6.4 Cyber range platform – building process for scenarios

Environment creation (pre-exercise) contains work which is done in virtual platform and created the environment where exercise is executed. The environment is created from scratch, and it follows the written story with selected incidents and occurrences. The usability is an important variable in the created scene, which means that after the environment is ready to exercise, functionalities will

be tested against storyline with background noise and artificial intelligence features. Environment administrators and observers should have visibility in the actions of cyber range.

Exercise actions contain the documented exercise steps. Before the exercise, the participants are informed about the features of the exercise and need for documentation of actions. During the exercise, the people involved in observation take notes and administrators keeps the environment alive. Changing circumstances in environment (e.g., generated virtual power failure in device or power pike) with changing behaviors may increase the intensity of the training, which may add extra value for training. The exercise may have limited amount of time, or the exercise might contain aspects of infinite amount of time when the defender does not know when the actual attack is over. After the exercise, meetings (hot wash) are important because of knowledge transfer.

Cyber range needs resources in maintenance and building different environments and functionalities. If scenario is complex, the building of environment requires more efforts and time. The consumed time is needed to be as small as possible. If there is need to decide how the time is saved, then there needed to make decision of what kind of assistance would be replaced human resources. There are currently three options which are possible to use, which are software robotics, traditional or virtualized software with scripting activities and backups/snapshots from previous machines.

Human resources can be replaced by software robotics for processing/building scenario environments if the environment is using only known software with known configurations and there is made interface for applying software and there is no need for human’s interaction. If the scenario which is needed to build uses different or not-yet-known software, then software robotics cannot help in the building process because software robot must have proper learning before it can work properly. If software robotics are not suitable, then there must be used regular software and scripting methods. Scripting is one possible tool for saving time which will enable automated installation processes, when building the scenario for cyber range. Backups and snapshots are one possibility to save time in scenario building process, and it can be used if previously done and saved scenario is suitable for the use of upcoming exercise.

Software robots are suitable for actions where work is repeatable, and software and parameters remain the same. Scripting and backups do the similar activities but requires human interaction. Using software, robot might need occasionally input for decision-making by human, which can be for example captcha recognition activity. If in-depth learning algorithms are utilized in software robots or information systems that control bots, these can also be used in cyber exercises to act as offensive or defensive parties. When utilizing software-based robots, scripts, etc., one must start with a simple and easy implementation. With the help of software robotics, the virtual training environment could be managed, for example, with its own user interface.

Table 10. Software robotics and automated features for cyber range

functionality	**description**
email sender	a software robot may send email and act like a user in the virtual machine and create background noise. Received e-mails can be sent back to the sender automatically and action can be taken based on the reply message received
door knock service	software robot may be used for knocking doors by selected software and the purposes of the scenario. Ping and other queries can be recorded, and various measurements can be made, which can be utilized in different ways later
scripted events	scripted events may occur during the exercises. These pre-written events may start by some actions in the network, etc.
bot network	automated functionality for software robot for maintains and use of scenario purposes scripted events. Supported for offensive or defensive actions with deep learning algorithms
use of exploit kits	attackers are selling/renting exploit kits for payload delivery in web services, for example distribution platform in Chrome browser and component of chromium (Magnitude Ex)

The things described in table 10 can be incorporated into a virtual environment, which may include use cases for relating to use of automation. The examples could be automated findings of threats, malware analysis, VPN software checks, registry setting change surveillance, vulnerability management and automated information control orchestration tool for workflows etc.

Post exercise actions contains feedback and learning from exercise for knowledge transfer. Feedback is required from participants and environment administrators because it will give more information about success factors and

what things are needed to develop further. All information is needed to collect and transfer into knowledge which will aid for planning process in the next cyber exercise. The analysis of war diary will help for analyzing time consumption and actions performed by participants which will give result as in timeline. Observer notes will be fulfilling the war diary's information and makes possible to write end report (After action review, AAR) of the cyber exercise.

As outcome, the four phases form a cycle of cyber training is different for every exercise but collected information will remain the same. Participants will learn from realistic cyber training and used to meet their exercise objectives. Training assesses the organization's capability to determine operational impacts of cyber-attacks and implement proper recovery procedures for the exercise. There are numerous questions to ask at the final meeting. It is advisable to select only the questions related to the exercise in question at the meeting, so that the length of the meeting is not prolonged, and the answers received are of the highest possible quality.

Example questions for the final meeting (hot wash):

- CSIRT: how the team was formed? correct specialist involved training? did team learn as much as expected, what did team learn? how was the training acceptable? did training contain enough exercises?
- guidance: was the channels of communication and interaction defined suitable? are the guidance procedures of guidance suitable for training? covers the guidance all aspects of response procedures.
- detection: how the incident was detected? what procedures etc. can be automated? did the security controls be adequate?
- analysis: did analysis procedures be adequate? how role was logs in the training? what evidence collected during training?
- recovery: how backups were used and were they available? were there any procedures for testing backups? was the restore of the systems required in training?

There are many options for the outcome of the exercise, from which it is worth choosing the essential things through which the objectives of the exercise can be stated. Possible outcomes for cyber training:

- checklist for required (defensive) actions
- completion of selected cyber training at the appropriate level
- training for use of cyber tool for network/system security
- training for offensive actions with selected tools
- information gathering for unknown incident or upcoming cyber training
- raising the level of maturity of an organization
- knowledge to protecting personal information

In practice, the goal of cyber practice is to increase competence, but it is also possible to practice various practical close-knit activities. In virtual cyber exercises, it is also worth remembering to keep the level of documentation and software at a general level to avoid possible abuses. A detailed description of a training diary with its attributes in the wrong hands may serve as a handbook for a potential attacker. However, other documentation relevant to the exercise should be kept available so that it is possible to complete the exercise.

6.5 Summary

The popularity of cyber exercises has grown in Finland in the last two years, and cyber exercises have been actively discussed in the field of information security. Cyber exercises need suitable environment and facilities for proper real-time training. South-Eastern Finland University of Applied Sciences (Xamk) has identified this need and is developing its current environment for the future. Some online hardware vendors may have to work with educational institutions that maintain a cyber-learning environment at some level. Co-operation will aid students' knowledge about the products and familiarizes the products features.

This study focus was aimed for developing cyber range concept for Xamk which would increase the amount of exercise and improve the learning experience of students and teachers. The study was implementing best practices of knowledge management and available knowledge on current operative cyber ranges. This thesis used action research model as an approach of this research. During the concept process of the interviews, benchmarks, and observations, the main findings were added to the concept of Xamk cyber range. Information, which was collected in interviews from Xamk, observations with benchmarks, eight main categories were identified for concept of Xamk cyber range. There are also subcategories for cyber exercises for different industries. After the identification, the development of cyber range has been started to improve cyber exercises in Xamk.

The identified features are related to the improvement of advertisement outside of Xamk to get cyber range introduced to everyone. Other identified improvements related to the customer experience of cyber exercises. The user interface needs face lifting by descriptions and hints for exercise. Exercise may contain

several outcomes, so they also require walkthrough guide, so user has possibility to make exercise of his own. There is also need for some automation or artificial intelligence put in exercises which might require new tools for example network traffic or threat modeling. Authentic user environment might also improve exercise experience If users have e-mails on their own during exercise. There would be significant improvement on cybersecurity on all industries if all Xamk students would have to participate in lecture which is focused on “regular user cybersecurity-oriented behavior” as needed. There would also be possible to use a chat box for teacher, resources, or other team members.

Overall, the cyber exercises are learning to handle threats and incident management and response time is part of it. In exercises, all user actions would be measurable in the view of virtual platform, exercise planners and participants. If measurement of actions were possible, the continuous learning would also be possible because there would be comparison information. The concept of cyber training and exercise system gives an opportunity to enhance individuals or teams cyber skills. Participants will be gaining knowledge during training and exercises. Cyber range platforms purpose is industry-based and uses customer segmentation-based content. As a technology related training, the cyber range need resources for maintaining the infrastructure. Cyber range need constant attention for capacity, modules including software, and networks.

The scenarios of cyber range need scenario-based software, which may be commercial or open-source software. Also, the malware might have significant role in the scenario, so cyber range should also have required malware for obtaining the scenario outcome. Advertising is important, so people with intention of participate in cyber training would find the cyber range and sign-up for the training. Xamk website requires information on possibility to execute cyber exercises. There would be possibility to make external cybersecurity trainings for industries. Basic cybersecurity awareness skills are required for all Xamk students.

6.6 Conclusions and discussion

The purpose of this research was to create concept of Xamk cyber range for the cybersecurity training. The European Union and Finland are introducing virtual cyber exercises in various industries, and increased cyber-attacks provide a basis for cyber exercises, enabling them to be better combated. The study required a research method to map Xamk's needs for future implementations. During the study, it was even possible to identify a few training programs where virtual exercises might be helpful. The selected perspective aims for development of concept for students and personnel of Xamk which may have expanded the use also for external users and organizations. The research has been created in such a way that the research results can be utilized in other similar research, or, for example, in the further development research of the cyber training environment.

6.7 Reliability and validity of this study

The approach of this study was action research which focused on concepting the Xamk cyber range. The current Xamk ICT laboratory environment is used for cyber exercises but is also suitable for cyber range training, and the focus of the study was made concept for cyber range. Interviews of this study were made remotely in the Finnish language with teachers, but translation is made in English in the study. Some interviews contained tacit information about the Xamk ICT laboratory environment, which included suitable information to the study. This study evaluations are possible to reproduce by using similar methodologies, which means that study is then reliable. However, technologies and cyber training are both evolving constantly, so there might appear more specific solutions in the future, but currently all analysis are valid.

Validity of this study contains current information about current ICT laboratory system and concepting procedures which were based on planning, researching, and receiving information from interviews and benchmarks. During conception phase, the reflection was made against other cyber ranges and best practices of academic research for the use of Xamk. The outcome of the study was a result of research objective which aided to keep focus to find a concept for Xamk cyber range.

REFERENCES

Abdullah, H. 2020. Evaluation of Open-Source Web Application Vulnerability Scanners. Academic Journal of Nawroz University. 9. Research Article. Available at: https://doi.org/10.25007/ajnu.v9n1a532 [Accessed 1 August 2021].

Airbus, 2021. Cyber Range. WWW document. Available at: https://airbus-cybersecurity.com/products-and-services/prevent/cyberrange/ [Accessed 27 June 2021].

Arntz, P. 2021. Chrome targeted by magnitude exploit kit. Malwarebytes labs. WWW document. Available at: https://blog.malwarebytes.com/exploits-and-vulnerabilities/2021/10/magnitude-ek-has-been-spotted-targeting-the-chrome-browser/ [Accessed 2 November 2021].

Avgerinos, T., Brumley, D., Davis, J., Goulden, R., Nighswander, T., Rebert, A, & Williamson, N. 2018. The Mayhem Cyber Reasoning System. *IEEE Security & Privacy*. 16 (2), 52-60, Research Article. Available at: https://ieeexplore.ieee.org/abstract/document/8328972 [Accessed 11 August 2021].

Blueteamslab, 2021. Blue team labs online. WWW document. Available at: https://blueteamlabs.online/ [Accessed 4 August 2021].

BBC, 2021. Warship positions faked including UK aircraft carrier. *BBC news*. WWW document. Available at: https://www.bbc.com/news/technology-58027363 [Accessed 3 August 2021].

Buber, Z. 2020. How to Identify Cobalt Strike on Your Network. *Dark Reading*. Research Article. Available at: https://www.darkreading.com/threat-intelligence/how-to-identify-cobalt-strike-on-your-network/a/d-id/1339357 [Accessed 4 June 2021].

Budning, K., Wilner, A. & Cote, G. 2021. Connecting the dots on Canada's connected battlespace, *International Journal*, 76 (1),154–162. Research Article. Available at: https://journals.sagepub.com/doi/full/10.1177/0020702021992855 [Accessed 4 June 2021].

CDEX, 2021. Cyber range platform & training. Vector synergy. WWW Document Available at: https://cdex.cloud/ [Accessed 27 August 2021].

Chouliaras, N., Kittes, G, Kantzavelou, I, Maglaras, L, Pantziou, G, & Ferrag, A, 2021. Cyber Ranges and Testbeds for Education, Training, and Research. *ResearchGate*. Research Article. Available at: https://www.researchgate.net/publication/349396111_Cyber_Ranges_and_TestBeds_for_Education_Training_and_Research [Accessed 11 June 2021].

Cyberstartupobservatory, 2021. Brazil Cybersecurity Companies – Brazil Cyberslide. WWW Document Available at: https://cyberstartupobservatory.com/brazil-cyber-security-companies/ [Accessed 29 July 2021].

Conrad, E, Wright, J., Masek, P., and Burnham, Z. 2021. sans-blue-team / DeepblueCLI. WWW Document. Available at: https://github.com/sans-blue-team/DeepBlueCLI, [Accessed 3 August 2021].

Cyberbit, 2021. Hyper-Realistic Cyber Range Attack Simulation. Cyberbit.com. WWW Document. Available at: https://www.cyberbit.com/platform/cyber-range/ [Accessed 25 May 2021].

Cyber Ranges, 2021. Cyber Space, Engaged. WWW Document. Available at: https://cyberranges.com/ [Accessed 25 May 2021].

CyberRange, 2021. AIT Cyber Range, *Austrian institute of technology*. WWW Document Available at: https://cyberrange.at/ [Accessed 25 May 2021].

Cyberspatial, 2021.Getting into Cybersecurity: 5 Skills You NEED to Learn. WWW Document. Available at: https://www.youtube.com/watch?v=Kx4y9c7w2JQ [Accessed 3 August 2021].

Cobalt strike, 2012. Software for Adversary Simulations and Red Team Operations. WWW Document Available at: https://www.cobaltstrike.com/ [Accessed 4 June 2021].

Cryptohack, 2021. Cryptohack, a fun, free platform for learning modern cryptography. WWW Document. Available at: https://cryptohack.org/ [Accessed 5 October 2021].

Deter-project, 2021. DETER: research project. WWW Document. Available at: https://deter-project.org/ [Accessed 5 August 2021].

Debatty, T., & Mees, W. 2019. Building a Cyber Range for training Cyber Defense Situation Awareness. 2019 International Conference on Military Communications and Information Systems (ICMCIS), 1-6. Research Article. Available at: https://www.semanticscholar.org/paper/Building-a-Cyber-Range-for-training-CyberDefense-Debatty-Mees/c92a13fd8d613de765f2d542cdfce7b1898f3d81 [Accessed 11 August 2021].

DVV, 2021.Testaa organisaatiosi digiturvallisuus taistoharjoituksessa. Digital population data services. WWW Document. Available at: https://dvv.fi/taisto# [Accessed 11 August 2021].

Dfirdiva, 2021. Ddfirdiva. WWW Document. Available at: https://freetraining.dfirdiva.com/ [Accessed 4 October 2021].

ECSO (European Cybersecurity Organization), 2020a. WG5: Education, Training Awareness, Cyber Ranges. *European Cybersecurity organization*. E-journal. Available at: https://ecs-org.eu/working-groups/wg5-education-training-awareness-cyber-ranges [Accessed 28 May 2021].

ECSO (European Cybersecurity Organization), 2020b. WG6: SRIA and cybersecurity technologies. *European Cybersecurity organization*. E-journal. Available at: https://ecs-org.eu/working-groups/wg6-sria-and-cyber-security-technologies [Accessed 22 August 2021].

ECSO (European Cybersecurity Organization), 2020c. WG5 paper: Understanding cyber ranges: From Hype to Reality. SWG 5.1. E-journal. Available at: https://www.ecs-org.eu [Accessed 11 June 2021].

Ekami, 2021. Ekami Vocational education. The joint Authority of Education of Kotka-Hamina Region Group (EKAMI). WWW Document. Available at: https://ekami.fi/in-english [Accessed 29 May 2021].

Exabeam, 2020. What is Mitre Att&ck part – basic terminology and matrices. WWW Document. Available at: https://www.youtube.com/watch?v=bK5eFF-HgC4 [Accessed 9 August 2021].

Fabro, M., Gorski, E., Spiers, N., Diedrich, J.,& Kuipers, D. 2016. Recommended practice: improving industrial control system cybersecurity with defense-in-depth strategies. Department of Homeland Security's NCCIS and ICS-CERT. Research Article. Available at: https://us-cert.cisa.gov [Accessed 11 November 2021].

Fasulo, P. 2019. TOP 20 Cybersecurity KPIs to track in 2021. Security Scorecard. WWW Document. Available at: https://securityscorecard.com/blog/9-cybersecurity-metrics-kpis-to-track [Accessed 5 August 2021].

Fieldeffect. 2021. Field Effect Cyber Range. WWW Document. Available at: https://fieldeffect.com/ [Accessed 27 June 2021].

Froehlich, A. 2020. 7 key cybersecurity metrics for the board and how to present them, Search Security. WWW Document. Available at: https://searchsecurity.techtarget.com/tip/7-key-cybersecurity-metrics-for-the-board-and-how-to-present-them [Accessed 5 September 2021].

Gatlan, S. 2021. Researchers compile list of vulnerabilities abused by ransomware gangs. Bleeping computer. WWW Document. Available at: https://www.bleepingcomputer.com/news/security/researchers-compile-list-of-vulnerabilities-abused-by-ransomware-gangs/ [Accessed 22 September 2021].

Guardtime, 2021. Guardtime. WWW Document. Available at: https://guardtime.com/technology [Accessed 27 June 2021].

Graziano, A. 2021. Cyber Range – What it is, what it is Not and What it Will be! *Cybersecurity Observatory*. WWW Document. Available at: https://cyber-startupobservatory.com/cyber-range-what-it-is-what-it-is-not-and-what-it-will-be/ [Accessed 11 June 2021].

Hacker101, 2021. Learn to Hack. WWW Document. Available at: https://www.hacker101.com/ [Accessed 4 September 2021].

Hack the box. 2021. A Massive Hacking Playground. WWW Document. Available at: https://app.hackthebox.eu/home [Accessed 18 August 2021].

Harris, M. 2021. They Told Their Therapists Everything. Hackers Leaked It All. Wired.com. WWW Document. Available at: https://www.wired.com/story/vastaamo-psychotherapy-patients-hack-data-breach/ [Accessed 30 October 2021].

Hennink, M. Hutter, I. & Bailey, A. 2020. Qualitative research methods. Los Angeles, *Sage publications ltd*. 4-65. Research Article. Available at: https://kaakkuri.finna.fi [Accessed 30 October 2021].

Hussain, F. Abbas, S. Shah, G. Pires, I. Fayyaz, U. Shahzad, F. Garcia, N. & Zdravevski. 2021. A Framework for Malicious Traffic Detection in IoT Healthcare Environment. *Sensors*, no 21. Research Article. Available at: https://www.mdpi.com/1424-8220/21/9/3025 [Accessed 18 August 2021].

IBM, 2021. IBM Security Command Center. WWW Document. Available at: https://www.ibm.com/security/services/managed-security-services/security-operations-centers [Accessed 27 June 2021].

IAEA, 2011. Computer Security at Nuclear Facilities. International Atomic Energy Agency (IAEA). E-Journal. Available at: https://www.iaea.org/publications/8691/computer-security-at-nuclear-facilities [Accessed 18 June 2021].

Virtual Lab 2021. Stats. WWW Document. Available at: https://virtual.ictlab.fi/stats/stats.html [Accessed 26 June 2021].

INE, 2021. Train for your future in Cybersecurity. WWW Document. Available at: https://ine.com/pages/cybersecurity [Accessed 26 June 2021].

Jakubik, M. 2007. Exploring the knowledge landscape: Four emerging views of knowledge. *Journal of Knowledge Management, no 11*, 6-19. Research Article. Available at: https://www.emerald.com/insight/content/doi/10.1108/13673270710762675/ full/html. 1367-3270. [Accessed 18 June 2021].

Jeon, S. & Kim, H. K. 2021. AutoVAS: An automated vulnerability analysis system with a deep learning approach. *Computers & security*, no. 106, 102308. Research Article. Available at: https://www-sciencedirect-com.ezproxy.xamk.fi/science/article/pii/S0167404821001322?via%3Di-hub#fig0020 [Accessed 31 November 2021].

Jiang, H., Choi, T., & Ko, K. 2020. Pandora: A Cyber Range Environment for the Safe Testing and Deployment of Autonomous Cyber Attack Tools. Research Article. Available at: https://arxiv.org/abs/2009.11484v1 [Accessed 11 August 2021].

JYVSECTEC, 2021. Jyvsectec Center RGCE, JAMK. WWW Document. Available at: https://jyvsectec.fi/2015/02/jyvsectec-center-rgce/ [Accessed 30 May 2021].

Kan, M. 2022. Malware That Can Survive OS Reinstalls Strikes Again, Likely for Cyberespionage. *PC Mag.com*, WWW Document. Available at: https://uk.pcmag.com/security/138262/malware-that-can-survive-os-reinstalls-strikes-again-likely-for-cyberespionage [Accessed 28 January 2022].

Kaspersky, 2021. What is Cybersecurity? WWW Document. Available at: https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security [Accessed 1 June 2021].

Kick, J. 2014. Cyber Exercise Play Book. Mitre. WWW Document Available at: https://www.mitre.org/publications/technical-papers/cyber-exercise-playbook [Accessed 27 October 2021].

Kucek, S. and Leitner, M. 2020. Training the Human-in-the-Loop in Industrial Cyber Ranges. Research Article. Available at: https://link.springer.com/chapter/10.1007%2F978-3-030-48602-0_10 [Accessed 11 November 2021].

KYPO, 2021. KYPO Cyber Range plattform. Masaryk University. WWW Document. Available at: https://crp.kypo.muni.cz/ [Accessed 27 June 2021].

Macola, I. 2020. US Tugboat cyber-attack: the experts respond. Ship technology. WWW Document. Available at: https://www.ship-technology.com/features/cyber-attacks-in-the-maritime-sector-the-experts-respond/ [Accessed 4 August 2021].

Limacharlie, 2021. Focus on Cybersecurity, Not IT. WWW Document. Available at: https://www.limacharlie.io/ [Accessed 4 September 2021].

Love, J. 2018. A Brief History of Malware – Its Evolution and Impact. *Last line*. Available at: https://www.lastline.com/blog/history-of-malware-its-evolution-and-impact/ [Accessed 27 January 2022].

Miessler, D. 2020. The difference between red, blue, and purple teams. WWW document. Available at: https://danielmiessler.com/study/red-blue-purple-teams/ [Accessed 11 June 2021].

Miller, R. 2016. IBM opens new Cambridge, MA security headquarters with massive cyber range. WWW Document. Available at: http://tcrn.ch/2ghoBlv [Accessed 27 June 2021].

Mirkovic, J., Benzel, T. V., Faber, T., Braden, R., Wroclawski, J. T. & Schwab, S. 2010. The DETER project: Advancing the science of cybersecurity experimentation and test. *IEEE International Conference on Technologies for Homeland Security (HST)*, 1-7. Research Article. Available at: https://ieeexplore.ieee.org/document/5655108 [Accessed 27 June 2021].

Mitre, 2021. ATT&CK. WWW Document. Available at: https://attack.mitre.org/ [Accessed 3 June 2021].

Morgan, S. 2021. 15 Hot Cyber Range Companies to Watch in 2021. *Cybercrime Magazine*. E-journal. Available at: https://cybersecurityventures.com/10-hot-cyber-range-companies-to-watch-in-2020/ [Accessed 3 June 2021].

NCSC-fi, 2020. At KONE, cyber exercises help in developing the information security measures of the future. Traficom. WWW Document. Available at: https://www.kyberturvallisuuskeskus.fi/en/news/kone-cyber-exercises-help-developing-information-security-measures-future [Accessed 17 June 2021].

Neuvonen-Rauhala, M-L. 2020. Xamk beyond 2020. South-Eastern Finland University of Applied Sciences. E-journal. Available at: https://www.theseus.fi/handle/10024/354911 [Accessed 21 August 2021].

NIST, 2021. The Cyber Range: A Guide. the National Initiative for Cybersecurity Education (NICE). WWW Document. Available at: https://nist.gov [Accessed 25 May 2021].

Nonaka, I. & Takeuchi, H. 1996. The knowledge-creating company: How Japanese companies create the dynamics of innovation. *Long range planning*, 29 (4), 592. Research Article. Available at: https://www.infona.pl/resource/bwmeta1.element.elsevier-4a1fa796-da72-3abf-96c8-63beda57d3c8 [Accessed 25 May 2021].

Osborne, C. 2021. This is how the Cobalt Strike penetration testing tool is being used by cyber criminals. Zdnet.com. E-journal. Available at: https://www.zdnet.com/article/this-is-how-the-cobalt-strike-penetration-testing-tool-is-being-abused-by-cybercriminals/ [Accessed 4 June 2021].

OWASP, 2021. Who is the OWASP Foundation? WWW Document. Available at: https://owasp.org/ [Accessed 3 June 2021].

Paloalto networks, 2021.What is an exploit kit? WWW Document. Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-an-exploit-kit [Accessed 5 November 2021].

Parsons, D. 2021. Top 5 ICS Incident Response Tabletops and How to Run Them. SANS institute. WWW Document. Available at: https://www.sans.org [Accessed 21 June 2021].

Patten, D. 2017 The evolution to fileless malware. I*nfosecwriters.com.* WWW Document. Available at: www.infosecwriters.com/Papers/DPatten_Fileless.pdf [Accessed 27 January 2022].

Pederson, P., Lee, D., Shu, G., Chen, D., Liu, Z., Li, N., & Sang, L. 2008. Virtual Cyber-Security Testing Capability for Large Scale Distributed Information Infrastructure Protection. *IEEE Conference on Technologies for Homeland Security*, 2008, 372-377. WWW Document. Available at: https://ieeexplore.ieee.org/document/4534480 [Accessed 16 August 2021].

PicoCTF, 2021. PicoCTF, let learning happen through exploration. *Carnegie Mellon University*. WWW Document. Available at: https://picoctf.org/index#picogym [Accessed 5 September 2021].

Poudel, D. 2021. The Basic Services of Internet You Must Know it. Ourtechroom.com. WWW Document. Available at: https://ourtechroom.com/tech/basic-services-of-internet-that-you-must-know-it/ [Accessed 8 June 2021].

Poremba, S. 2017. Study Shows the Complexity of Malware Attacks. *IT Business Edge*. WWW Document. Available at: https://www.itbusinessedge.com/security/study-shows-the-complexity-of-malware-attacks/ [27 January 2022].

Portswigger, 2021. Web security Academy. WWW Document. Available at: https://portswigger.net/web-security [Accessed 5 September 2021].

Raybourn E.M., Kunz M., Fritz D., & Urias V. 2018. A Zero-Entry Cyber Range Environment for Future Learning Ecosystems. *Springer*. Research Article. Available at: https://link.springer.com/chapter/10.1007%2F978-3-319-98935-8_5 [Accessed 27 June 2021].

Ravello Community. 2016. Five challenges with cyber range training on AWS. Oracle.com, 26.5.2016. WWW Document Available at: https://blogs.oracle.com/ravello/cyber-range-training-environment [Accessed 2 July 2021].

Roque, A., Stetson, D., & Hannon, D. 2020. Assessing the cognitive complexity of cyber range environments. *Journal of Defense modeling and simulation: Applications Methodology*, 17, 39-46. Research Article. Available at: https://journals.sagepub.com/doi/10.1177/1548512918820654 [Accessed 29 June 2021].

Rheagroup, 2021. Next generation cyber-range services. WWW Document. Available at: https://www.rheagroup.com/services-solutions/security/cybersecurity/cyber-range/ [Accessed 4 August 2021].

Rossey, L., Cunningham, R, Fried, D, Rabek, J.C., Lippmann, R., Haines, J., & Zissman, M, 2002. LARIAT: Lincoln adaptable real-time information assurance testbed. 6. 6-2671. Research Article. Available at: https://ieeexplore.ieee.org/document/1036158 [Accessed 14 August 2021].

Savva, S. 2020. Red, Blue, and other color teams. WWW Document. Available at: https://cyberranges.com/cr-glossary/red-blue-and-other-colour-teams/ [Accessed 11 June 2021].

Secretariat of the Security Committee, 2019. Finland's Cybersecurity Strategy, *Forssa print*. WWW Document. Available at: https://turvallisuuskomitea.fi/en/finlands-cyber-security-strategy-2019/ [Accessed 14 June 2021].

Security Innovation, 2021. Experience the power of cyber ranges and community to make security approachable. WWW Document. Available at: https://community.securityinnovation.com/ [Accessed 5 September 2021].

Silverman, D. 2020. London, *Sage Publications Ltd*. *4-60.* Available at: https://kaakkuri.finna.fi [Accessed 20 January 2022]

Simplycyber, 2021. Simply Cyber. WWW Document. Available at: https://www.simplycyber.io/ [Accessed 4 September 2021].

Sololearn, 2021. The best way to learn to code. WWW Document. Available at: https://www.sololearn.com/home [Accessed 5 September 2021].

Stein, D, Scribner, B, Kyle, N, Newhouse, W, Williams, C, & Yakin, B, 2017. National Initiative for Cybersecurity Education (NICE) Framework Work Role Capability Indicators: Indicators for Performing Work Roles. NIST, CSRC, NISTIR 8292 (Draft). WWW Document. Available at: https://csrc.nist.gov/publications/detail/nistir/8193/draft [Accessed 15 June 2021].

Stouffer, K. Pellitory, V, Lightman, S, Abrams, M., & Hahn, A. 2015. Guide to Industrial Control Systems (ICS) Security. NIST Special publication 800-82, rev.2. WWW Document. Available at: https://csrc.nist.gov/ [Accessed 8 August 2021].

Shea, S. 2021. Red team vs. blue team vs. purple team: What's the difference? WWW Document. Available at: https://searchsecurity.techtarget.com/tip/Red-team-vs-blue-team-vs-purple-team-Whats-the-difference [Accessed 11 June 2021].

Singh M., Negi R., & Shukla S.K. 2022. Automated Flag Detection and Participant Performance Evaluation for Pwnable CTF. *Communications in Computer and Information Science*, vol 1536. Available at: https://link.springer.com/chapter/10.1007/978-3-030-96057-5_9 [Accessed 22 February 2022].

Tambur, S. 2020. Estonian companies to develop a NATO cyber platform. Estonian World. WWW Document. Available at: https://estonianworld.com/security/estonian-companies-to-develop-a-nato-cyber-platform/ [Accessed 27 June 2021].

Tian, Z., Cui, Y., An L., Su, S., Yin, X., Yin, X., & Cui, X. 2018. A Real-Time Correlation of Host-Level Events in Cyber Range Service for Smart Campus. *IEEE Access*, 6, 35355-35364. Research Article. Available at: https://ieeexplore.ieee.org/document/8382167 [Accessed 27 June 2021].

Toderick, L., Yang, B., Chou, T-S. & Hempenius, N. 2021. A Secure Environment to Measure and Manage Cybersecurity Lab Activities. *CIEC*. Research Article. Available at: https://peer.asee.org/38704 [Accessed 28 January 2022].

Touhid, 2019. Six key elements of cybersecurity. Cyber threat & security portal. WWW Document, Available at: https://cyberthreatportal.com/elements-of-cybersecurity/ [*Accessed* 17 August 2021].

Turčaník, M. 2020. A cyber range for armed forces education. *Information & security,* 46.3, 304-310. WWW Document. Available at: https://procon.bg/system/files/4622_cyber_range.pdf [Accessed 5 July 2021].

Turton, W. & Mehrotra, K. 2021. Hackers Breached Colonial Pipeline Using Compromised Password. Bloomberg.com. WWW Document. Available at: https://www.bloomberg.com/news/articles/2021-06-04/hackers-breached-colonial-pipeline-using-compromised-password [Accessed 30 October 2021].

Turvallisuuskomitea.fi, 2021. The security Committee. WWW Document. Available at: https://turvallisuuskomitea.fi/en/frontpage/ [Accessed 29 May 2021].

Turvallisuuskomitea, 2019. Tiedote: Turvallisuusviranomaiset kehittävät osaamistaan kansallisessa kyberturvallisuusharjoituksessa (KYHA19) JAMKissa – jatkossa myös terveydenhuollon toimijat mukaan harjoituksiin. Turvallisuuskomitea. WWW Document. Available at: https://turvallisuuskomitea.fi/tiedote-turvallisuusviranomaiset-kehittavat-osaamistaan-kansallisessa-kyberturvallisuusharjoituksessa-kyha19-jamkissa-jatkossa-myos-terveydenhuollon-toimijat-mukaan-harjoituksiin/ [Accessed 9 May 2021].

Traficom, 2021. Monitoring and incident response. National Cybersecurity Centre. WWW Document. Available at: https://www.kyberturvallisuuskeskus.fi/en/our-services/monitoring-and-incident-response [Accessed 3 June 2021].

Tryhackme, 2021. Cybersecurity training. WWW Document. Available at: https://tryhackme.com/ [Accessed 22 August 2021].

Virginia Cyber Range, 2021. Virginia Cyber Range. WWW Document. Available at: https://www.virginiacyberrange.org/ [Accessed 3 June 2021].

Venkatesan, S., Youzwak, J., Sugrim, S., & Chiang, C-Y., Poylisher, A., Witkowski, M., Walther, G., Wolberg, M., Chadha, R., Newcomb, A., Hoffman, B., & Buchler, N. 2019. VulnerVAN: A Vulnerable Network Generation Tool. WWW Document. Available at: https://www.researchgate.net/publication/339696707_VulnerVAN_A_Vulnerable_Network_Generation_Tool [Accessed 16 August 2021].

Ween, A. Dortmans, P, Thakur, N., & Rowe, C. 2019. Framing cyber warfare: an analyst's perspective. *The Journal of Defense Modeling and Simulation*, 16(3),335–345. Research Document. Available at: https://journals.sagepub.com/doi/full/10.1177/1548512917725620. [Accessed 10 August 2021].

Xamk, 2021. South-Eastern Finland University of Applied Sciences. WWW Document. Available at: https://www.Xamk.fi/en/frontpage/ [Accessed 29 May 2021].

Zuber-Skerritt, O, & Wood, L, 2019, Action Learning and Action Research : Genres and Approaches, Bingley, *Emerald Publishing Limited*. Research Article. Available at: https://www.emerald.com/insight/publication/doi/10.1108/9781787695375 [Accessed 6 June 2021].

Vulnhub, 2021. Virtual machines. WWW Document. Available at: https://www.vulnhub.com/ [Accessed 1 January 2022].

Watson, M.K. Pelkey J., Noyes, C., and Rodgers, M.O. 2019. Using Kolb's Learning Cycle to Improve Student Sustainability Knowledge. *Sustainability*, 11,4602. Research Article. Available at: https://www.mdpi.com/2071-1050/11/17/4602. [Accessed 6 June 2021].

List of figures

List of tables

Appendix 1: Cyber ranges/platforms/institutes (Chouliaras et al. 2021)

The virtual cyber-training environments below were operational at the time of writing the study.

cyber range / institute	physical location	reference
A3C Cyber Test Range	Adelaide, Australia	https://www.cybercollaboration.org.au/about
APAC, Palo Alto	Sydney, Australia, Amsterdam, Netherland, Washington DC, Santa Clara (USA)	https://www.paloaltonetworks.com/events/cyber-range-apac-20
Accenture Cyber Range	Houston, Texas	https://www.infosecurity-magazine.com/news/accenture-opens-cyber-ranges/f
Airbus Cyber Range	France/Germany/UK	https://airbus-cyber-security.com/products-and-services/prevent/cyberrange/
Arkansas Cyber Range	Arkansas, USA	https://uca.edu/cse/cyber-range/
AIT Austrian Institute of Technology	Vienna, Austria	https://cyberrange.at/
Baltimore Cyber Range	Baltimore, Maryland, USA	https://baltimorecyber-range.com/
Canada Cyber range	Canada	https://cyberrange.ca/
Catalyst Cyber Range	Canada	https://www.cybersecurecatalyst.ca/cyber-range-overview
CDeX (cyber defense exercise platform)	Poland	https://cdex.cloud/cyber-range/
Cisco Cyber Range Lab	India	https://newsroom.cisco.com/press-release-content?articleId=1839017
Cloud Range	Nashville, Tennessee, USA	https://www.cloudrangecyber.com/
Cyberbit Cyber Range	Ra'anana, Israel	https://www.cyberbit.com/
Cyber Ranges	Limassol, Cyprus	https://www.cyber-ranges.com/
CYRAN, De Montfort University	Leicester, Great Britain	https://www.dmu.ac.uk/research/centres-institutes/cti/consultancy-commercial-services.aspx
CYRIN	Minneapolis, USA	https://cyrin.atcorp.com/
CYLAB, Royal Military Academy	Belgium	https://cylab.be/resources/cyberrange
CYBERIUM (fujitsu)	Japan	https://www.fujitsu.com/fi/services/security/offerings/soc/index.html
Cybexer Cyber Range	Tallinn, Estonia	https://www.cybexer.com/
CWR Cyber Warfare Range	Gilbert, Arizona, USA	https://www.azcwr.org/
DECIDE platform (NUARI)	Northfield, Vermont, USA	https://nuari.net/decide/

Elbit systems	Brisbane, Australia	https://www.elbit-systems.com.au/cyber-training/
Florida Cyber Range Uni.west Florida	Pensacola, Florida, USA	https://uwf.edu/centers/center-for-cybersecurity/florida-cyber-range/
Field Effect	Ottawa, Canada	https://fieldeffect.com/
Fifth Domain	Canberra, Australia	https://www.cybersecurityintelligence.com/fifthdomain-6312.html
Georgia Cyber Range	Augusta, Georgia, USA	https://www.gacyber-center.org/
HNS-platform	Brest, France	https://www.diateam.net/ https://tracxn.com/d/companies/hns-platform.com
IBM X-Force Command C-TOC	Cambridge, Maryland, USA	https://www.ibm.com/security/services/managed-security-services/security-operations-centers
JAMK University of Applied Sciences (JYVSECTEC)	Jyväskylä, Finland	https://jyvsectec.fi/
Kleared4 Persistent Cyber Training Environment (PCTE)	Puerto Rico	https://kleared4.com
Masaryk University (KYPO)	Czech Republic	https://crp.kypo.muni.cz/
National Cyber Range (NCR)	Orlando, USA	https://www.peostri.army.mil/national-cyber-range-ncr
Naval Postgraduate School dc	Monterey, California, USA	https://nps.edu/web/cmis
NATO Cyber Range	CCDCOE, Estonia	https://ccdcoe.org/
NMU Cyber hub, Michigan Cyber Range	Michigan, USA	https://www.michiganbusiness.org/press-releases/2019/05/newest-cyber-range-hub-located-nmu-university/
Norwegian Cyber Range. Norwegian University of Science and Technology (NCR)	Trondheim, Norway	https://www.ntnu.edu/ https://www.ntnu.no/ncr
Range force	Manassas, USA	https://www.rangeforce.com/
Raytheon Cyber Range	Waltham, Massachusetts, USA	https://www.raytheon.com/cyber/capabilities/range
Sandia National Laboratories (Cyber Scorpion)	USA	https://www.sandia.gov/missions/national_security_programs/cybersecurity.html
Silensec Cyber Range	New York, USA	https://cs.hofstra.edu/docs/pages/resources/silensec.html https://www.silensec.com/about-us/cyber-ranges

SIMOC Cyber Range platform	Rio De Janeiro, Brazil	https://www.rustcon.com.br/
Swedish Defense Research Agency (CRATE)	Stockholm, Sweden	https://www.foi.se/en/foi/resources/crate---cyber-range-and-training-environment.html
Università degli Studi di Milano	Milan, italy	https://www.unimi.it/it
UNSW Institute for Cyber Security	Canberra, Australia	https://unsw.adfa.edu.au/our-research/facilities/cyber-security-labs
Wayne Range Hub	part of Michigan Cyber Range	https://wayne.edu/educationaloutreach/cyber-range
Virginia Tech	Blacksburg, Virginia, USA	https://it.vt.edu/administration/units/virginiacyber-range.html https://www.virginiacyber-range.org/