Toward Next-Generation Cyber Range: A Comparative Study of Training Platforms

Alexandre Grimaldi, Julien Ribiollet, Pantaleone Nespoli, Joaquin Garcia-Alfaro

Toward Next-Generation Cyber Range: A Comparative Study of Training Platforms

Alexandre Grimaldi[†], Julien Ribiollet[†],
Pantaleone Nespoli[†,‡], Joaquin Garcia-Alfaro[†]

[†]SAMOVAR, Télécom SudParis, Institut Polytechnique de Paris, Palaiseau, France

[‡]Department of Information and Communications Engineering, University of Murcia, Murcia, Spain

Abstract. As cyber incidents increase in number and disruption, cybersecurity competencies represent a need more than ever. In this context, Cyber Range platforms have been proven as an effective tool to train both professional and common users in such competencies. This study presents a comparative analysis of eight Cyber Range platforms, discussing the needed evolution toward next-generation cyber range platforms. The comparative analysis focuses on key aspects such as application domains, methods of experimentation, infrastructure technologies, and topology generation, among others. This study also aims to provide insights into the capabilities and features offered by different Cyber Range platforms and, specifically, network topology generation tools, allowing for informed decision-making when selecting the most suitable solution for specific training and experimentation needs. Additionally, the study considers how the ethical and well-thought use of Artificial Intelligence (AI) could enhance the automation processes of Cyber Ranges, whether it acts in scenario randomization or topology generation.

Keywords: Cyber Range, Cybersecurity, Cyber Defense, Educational Technology, Cybersecurity Education.

1 Introduction

In the rapidly evolving landscape of cyberspace, the need for skilled cybersecurity professionals has become more critical than ever. As organizations and individuals continue to grapple with sophisticated cyber threats, it is imperative to equip future cybersecurity practitioners with practical skills that reflect real-world scenarios [23]. While theoretical knowledge forms the foundation, hands-on experience in tackling complex cybersecurity challenges is crucial to fostering expertise in this field. To bridge this gap between theory and practice, the development of effective cybersecurity training programs is essential [4].

In particular. network topology generation refers to the creation of realistic and dynamic network environments that simulate various cybersecurity scenarios. These environments serve as training grounds for individuals to gain hands-on experience in detecting, preventing, and mitigating cyber threats. By replicating complex network infrastructures, topology generation enables trainees to

develop critical thinking, analytical, and problem-solving skills, while familiarizing themselves with the tools, techniques, and procedures employed by malicious actors in a controlled environment [13].

Nevertheless, traditional methods of topology generation require manual configuration, which can be time-consuming and error-prone. Additionally, once the cyberexercise has finished, users already know how to solve the proposed challenges, forcing the instructor to create another scenario. Autonomous topology generation tools, on the other hand, leverage advanced algorithms or AI techniques to automate the process of creating complex network environments. These tools can automatically generate realistic topologies, incorporating diverse network components, traffic patterns, and potential cyberattack scenarios. While automatic topology generation tools have been widely used in the network ecosystem, very little attention has been given to the use of those tools to create complex and motivating scenarios to train users' cybersecurity capabilities [22].

In light of the above, this paper presents a study on the most prominent Cyber Range platforms nowadays. Concretely, eight Cyber Ranges are compared based on 13 key features (e.g., application domains, methods of experimentation, infrastructure technologies, and topology generation, among others). Such a side-by-side comparison serves as a starting point for an interesting discussion on the actual limitations of the Cyber Range ecosystem, with particular attention on the generation of training scenarios. In particular, two of the most prominent tools for automatic scenario generation are analyzed (i.e., SecGen and CyExec*), highlighting their pros and cons.

Section 2 details the criteria used to contrast the Cyber Range proposals. Next, different Cyber Range are analyzed in Section 3, adding a side-by-side comparison based on the proposed criteria. Section 4 focuses on the generation of network topologies for cybersecurity training, analyzing two existing tools. Section 5 discusses on the limitations of the actual Cyber Ranges ecosystem, highlighting some potential improvements to address the open challenges. Section 6 concludes the paper, presenting some interesting future research lines.

2 Comparison Criteria

To better understand the current landscape of Cyber Ranges solutions and the challenges related to topology generation, it is mandatory to review some of the existing solutions and, consequently, gain essential insights about their core features. In order to have a fair comparison among them, this section provides details of which criteria are used for this classification and why they are pertinent.

2.1 Application Domains

Cyber Ranges can be used for training in a large variety of contexts. From students in cybersecurity schools to military groups, there are multiple application domains. Conducting a study on more than forty platforms, authors in [18] identified the following four categories, that is, (i) military defence and intelligence, (ii) academic purposes, (iii) commercial organisations and enterprises, and (iv) government training.

Military Defence and Intelligence — Training in this domain prioritizes national security and defense, emphasizing the counteraction of complex cyber threats and offensive operations. It frequently involves employing advanced techniques and simulations of real-world scenarios.

Academic Purposes — Training in academic institutions aims to educate and prepare students for careers in cybersecurity. It encompasses a wide range of topics and offers practical experience in network security, penetration testing, forensics, incident response, and much more.

Commercial Organizations and Enterprises — On a broad scale, training in this domain focuses on cybersecurity best practices for employees. It may include topics such as secure coding, data protection, risk management, and security awareness training.

Depending on the specific role and focus of the organization or company, the training for different teams like the red team, blue team, purple team, and others can be tailored to meet their specific objectives. This customization is essential because the goals pursued by these teams can vary significantly.

Government Training — Government training programs focus on preparing personnel within government agencies for various cybersecurity challenges specific to their operations and responsibilities. These agencies often handle sensitive information, critical infrastructure, and national security interests.

2.2 Team Formation

Depending on the type of scenario a Cyber Range is recreating, teams constitute a central part of the training. A Cyber Range can assign a user to a specific team or let the user choose the behavior they wish to have. Among such teams, the Red team acts as offensive operators, while the Blue team is responsible for defending against an adversary attack. Some Cyber Range platforms can even offer a user to act as a member of the Yellow team (i.e., system administration). A team's behavior can also be emulated and automated by the Grey team (i.e., background traffic generation) to add realism to a certain situation. Nevertheless, most platforms take the classic approach of Red-Blue-Grey teams.

2.3 Methods of Experimentation

Generally, Cyber Range platforms offer scenarios to train on cybersecurity competencies. Based on this study, there are two main techniques to deploy such scenarios, i.e., simulation or emulation of the environment.

Simulation — Simulation involves modeling the state of the target. The goal is to recreate a model as accurately as possible for every detail and every behavior that the target does in reality. Cyber Ranges utilize various tools to facilitate

these simulations, including Vagrant [1], Docker, Terraform [2], GNS3 [3], Ixia [4], and others. A successful simulation should be almost undetectable by the end-user.

Emulation — Sometimes, only imitating a behavior can be enough to recreate a realistic situation. This is where emulation comes into play, as it focuses on imitating externally observable behavior to match an existing real target. Interestingly, the target's internal state does not necessarily have to reflect the real world as long as it appears accurate to the end user.

Emulation finds widespread application in mimicking hardware behavior through software. When combined with virtualization, it enables the imitation of electronic equipment without the need for physical components. This powerful combination allows for the faithful reproduction of hardware functionality in a virtual environment, providing a cost-effective and flexible alternative to physical hardware usage.

2.4 Infrastructure Technologies

Infrastructure technologies are fundamental components of a Cyber Range, providing the underlying framework necessary for its operation and functionality. These technologies encompass a range of systems and resources, including network infrastructure, virtualization platforms, cloud computing services, and storage solutions. Network infrastructure forms the backbone of the Cyber Range, enabling connectivity, data transmission, and communication between simulated environments and users. Virtualization platforms, such as hypervisors, allow for the creation and management of virtual machines and networks, enabling the emulation of diverse systems and scenarios within the Cyber Range. Cloud computing services offer scalability and flexibility, facilitating the provisioning of resources on-demand and enabling the deployment of complex Cyber Range environments. Storage solutions play a crucial role in securely storing and managing the large volumes of data generated during Cyber Range exercises. Examples of these technologies include Kubernetes [5], Argo CD [6], and object storage.

Before choosing infrastructure solutions, it is important to consider the architecture approach. Monolithic architecture involves building an application as a single, self-contained unit, while microservices architectures decompose the application into small, independent services that can be developed, deployed, and scaled individually. Monolithic architecture offers simplicity on a small scale, while microservices architecture provides scalability, flexibility, and fault isolation, but it is more complex to set up initially.

[1] https://www.vagrantup.com
[2] https://www.terraform.io/
[3] https://www.gns3.com/
[4] https://github.com/open-traffic-generator/ixia-c
[5] https://kubernetes.io/
[6] https://argoproj.github.io/cd/

2.5 Front-End Technologies

Front-end technologies are crucial for the presentation of a Cyber Range, too. In this sense, panels and user interfaces should be user-friendly and easy to use to leverage the full capabilities of the tool.

User Interface (UI) — As the primary point of interaction between users and the Cyber Range platform, the UI directly impacts the user experience and the overall success of training exercises. A well-designed and intuitive UI enhances user engagement, simplifies navigation, and promotes efficient access to essential functionalities. It allows users, including instructors and trainees, to easily interact with the Cyber Range environment, configure scenarios, monitor progress, and analyze results. A clear and visually appealing UI improves cognitive load management, reducing user confusion and enhancing the learning experience. Moreover, a customizable UI can adapt to different user roles and preferences, catering to various skill levels and training objectives. The UI serves as a gateway to the Cyber Range, shaping users' interactions and facilitating effective training and skill development.

Instructor Interface — Instructors using a Cyber Range for education and training require several key capabilities. These include evaluating user actions, enabling communication, providing instructor-specific functionalities, and facilitating user evaluation and feedback.

User evaluation is crucial, involving capturing and analyzing data on user interactions, tasks, and system behavior. Recording and reviewing user sessions and analyzing the data helps assess performance and identify areas for improvement.

Communication facilities are also important in a Cyber Range environment. Features like chat functionality and event broadcasting enable instructors to communicate with users, provide guidance, and facilitate collaborative learning experiences.

To enhance the instructional process, an instructor mode functionality can be valuable. This mode allows instructors to demonstrate sample answers, showcase best practices, provide step-by-step guidance to users and control the workflow of the scenario.

Least but not last, user evaluation is a critical aspect of educational and training Cyber Ranges. Instructors require the ability to conduct assessments, analyze user performance, and deliver feedback. This includes generating reports that summarize user evaluation results, progress, and areas of strength or weakness. The delivery of evaluation and feedback reports enables personalized learning, highlights areas for improvement, and encourages continued growth and development among users.

2.6 Scenario

Scenarios are a crucial element of a Cyber Range, as they provide the context and purpose for training exercises and simulations. A scenario in a Cyber Range represents a specific simulated environment or situation designed to

replicate real-world cybersecurity challenges. These scenarios range from isolated incidents to complex multi-stage attacks, encompassing various attack vectors and techniques. The creation of realistic and relevant scenarios is vital to effectively train and assess participants' cybersecurity-related skills and capabilities. Well-designed scenarios should consider different levels of difficulty, align with specific learning objectives, and reflect current cybersecurity threats and trends. They should incorporate various attack and defense techniques, ensuring comprehensive coverage of relevant cybersecurity skills. Additionally, scenarios should offer the flexibility to adapt and evolve, allowing for the integration of new threats, technologies, and learning outcomes. By leveraging crafted scenarios, Cyber Ranges can provide a dynamic and immersive training environment, enabling participants to gain practical experience and enhance their ability to detect, respond to, and mitigate real-world cybersecurity incidents.

2.7 Topology Generation

Topology generation is another critical aspect of a Cyber Range as it involves the creation and configuration of network architectures that accurately simulate real-world environments. The generation of realistic network topologies within a Cyber Range allows for the replication of complex infrastructure, including interconnected systems, devices, and services. This process involves defining the layout, connectivity, and characteristics of virtual machines, routers, switches, firewalls, and other network components. An accurate topology generation is able to create lifelike scenarios for training exercises and simulations, enabling participants to develop practical skills in securing and defending network environments. It involves considering factors such as network segmentation, subnetting, IP addressing, and the configuration of various network protocols and services. With advanced techniques and tools, such as automated network configuration and software-defined networking (SDN) technologies, Cyber Ranges can enhance the process of topology generation, enabling more dynamic and scalable training environments.

2.8 Accessibility

Among others, accessibility ensures that the training environment is available and usable for a wide range of users, including individuals with diverse abilities and needs. Inclusive design principles are essential to ensure that all participants can access, understand, and use the Cyber Range platform and its associated resources. This includes considerations for users with visual, auditory, physical, and cognitive impairments. To enhance accessibility, Cyber Ranges should provide features such as adjustable font sizes, color contrast options, alternative text for images, keyboard navigation support, and compatibility with assistive technologies. Additionally, providing clear and concise instructions, intuitive user interfaces, and comprehensive documentation contributes to the overall accessibility of the Cyber Range, improving users learning opportunities.

2.9 Traffic

To enhance training realism within the Cyber Range, traffic generation can be depicted as one of the most important functionality. Such a generation varies

based on its main goal, but generally, it can be divided into two categories, i.e., background and adversarial traffic generation.

Background Traffic — Background traffic refers to the normal, seemingly random network activity that one would typically encounter during network inspection. It comprises the everyday operations of sending and receiving emails, interacting with online content, and engaging in conversations with friends and colleagues. Background traffic plays a major part in making a Cyber Range realistic as attackers often hide their activity blending in with other users of a network. For network intrusion-detection scenarios, having no background traffic makes the exercise pointless. Common network intrusion-detection tools have a much more difficult time identifying malicious traffic in a realistic noisy network environment than it does when only the malicious traffic is present.

Adversarial Traffic — Adversarial traffic is essential in Cyber Ranges for realistic testing and red-on-blue exercises. It provides cover for red teams to assess their stealth and tests the effectiveness of defensive tools. Malicious traffic can mimic normal system administrator activity, such as scanning ports, creating accounts, and changing passwords. It also involves more overtly malicious actions like creating botnets and performing network reconnaissance or exploitation.

2.10 User Modeling

During Cyber Range exercises, it is important to simulate the presence and behavior of benign users within the environment. It creates Non-Player Characters (NPCs) that can behave realistically without human intervention to generate context-driven traffic. User activity simulation creates specific scenarios that mimic real-world environments, adding a layer of realism to the training. Examples of user activity simulation include simulating internet browsing, watching YouTube videos, utilizing P2P file sharing applications for downloads, sending emails, and interacting with cloud services like Office 365 and Dropbox. While it shares similarities with the concept of background traffic, user modeling focuses on replicating precise behaviors based on predefined models. Being more than a simple traffic noise, a user model can be instructed to react to triggers, to interact with GUI-only softwares, to mimic seemingly human responses to phishing campaigns...

To facilitate user activity simulation, desirable features include the availability of a simulation library. This library would contain a comprehensive list of pre-defined user simulations that can be easily incorporated into the Cyber Range exercises. Additionally, the ability to import or create custom simulations provides flexibility to tailor the user activity scenarios based on specific training objectives or real-world use cases. The GHOSTS framework [19] specifically aims to provide tools to build such realistic, accurate and autonomous NPCs. Still in the early stages of development, GHOSTS shows promising possibilities for NPCs orchestration. The use of large samples of real-world data and eventually the use of AI could enable NPCs to deliver complex coordination scenarios, such as Distributed Denial Of Service (DDOS) attacks.

2.11 Data Collection and Analysis

The capability of a Cyber Range to gather users' interactions encompasses various aspects such as the traffic generated, memory dumps, tools utilized, and systems targeted. At its simplest level, it involves collecting data provided by the users, such as their responses to tasks or challenges. However, at an advanced level, the Cyber Range can collect all user interactions within the simulated environment and with the platform itself.

The extent of data collection depends on the core technologies employed by the Cyber Range and the methods used to create the simulation environment. Some technologies may offer better native support for data collection, allowing for a more comprehensive and accurate gathering of user interactions.

Additionally, the Cyber Range's ability to facilitate the analysis of collected data plays a crucial role. Data analysis, encompassing both automatically collected data and the output of user activities, forms the foundation for providing meaningful feedback to Cyber Range users. This analysis enables insights into how the Cyber Range is being used and how users perform within the simulated environment, facilitating the educational processes the instructors perform.

In some cases, the inclusion of AI technology, often through third-party solutions, can further enhance the analysis capabilities of the Cyber Range. AI technologies can enable advanced data processing, pattern recognition, and user behavior modeling, leading to more sophisticated and valuable feedback for users.

2.12 Scoring and Reporting

An important feature in a Cyber Range is the ability to score users based on their activities and interactions within the platform. This scoring mechanism can range from simple collection of user input to questions and tasks, to more complex attack and defense systems that involve automated tests for evaluating service availability, system integrity, and other performance indicators. To achieve high scoring capabilities, a strong coupling and integration with the Cyber Range infrastructure is necessary.

To facilitate effective assessment and analysis, Cyber Ranges should provide standard reports, such as individual or team-based performance reports, as well as the flexibility to create custom reports. Reporting capabilities are often an integral part of additional Cyber Range features, enabling the extraction and presentation of valuable insights from user activities and system data. These reports can provide essential feedback for users, instructors, and administrators to evaluate performance, identify areas of improvement, and track progress.

Real-time cyber situational awareness is another critical aspect of Cyber Range capabilities. It allows for clear visualization of the Cyber Range usage, showcasing the impact of tools used, and providing visibility into the actions taken by the users. By displaying real-time information, such as network traffic, system vulnerabilities, and user interactions, cyber situational awareness enhances the understanding of the Cyber Range environment, promotes effective decision-making, and improves overall situational awareness.

2.13 Ownership and License

Ownership and licensing are crucial aspects in the development and operation of Cyber Ranges. Ownership refers to the legal rights and control over the platform and its assets, while licensing governs the terms for use and distribution.

Determining ownership involves identifying the entity or entities with legal rights and control over the Cyber Range. Ownership arrangements may vary, depending on whether it's developed by a single organization, collaboratively, or hosted by a third-party provider. Clear ownership ensures accountability, decision-making authority, and long-term sustainability.

Licensing regulates how the Cyber Range is made available and the permissions granted. It outlines terms, conditions, and restrictions for access, distribution, and usage. Licensing agreements address issues like user rights, content sharing, commercial usage, modifications, and legal liabilities.

Choosing the right licensing model significantly impacts adoption, engagement, and sustainability. Options include open-source licenses for collaboration, proprietary licenses for selective usage, or hybrid models. The chosen model should align with goals, considering factors like community participation, commercialization potential, government involvement, and intellectual property protection.

3 Comparison of Cyber Ranges solutions

The main goal of this study was to provide a comprehensive overview of Cyber Range and network topology generation tools, albeit within a limited scope. Instead of aiming for an exhaustive list, we aimed to present a well-rounded representation of the possibilities available. To achieve this, we considered a combination of open-source and proprietary tools, using different technologies.

Although our comparison only includes a limited sample of the numerous Cyber Ranges available in the market or under development, we are confident that our selection provides a broad representation of the current Cyber Range landscape. The chosen eight Cyber Ranges offer a diverse range of solutions, allowing for a comprehensive overview. They have been carefully selected based on the previously mentioned comparison criteria, ensuring their relevance to our study. Moreover, these selected Cyber Ranges have ample documentation available, which facilitates a thorough analysis.

Our investigation revealed a scarcity of efficient network topology generation tools that emphasize autonomous generation. Consequently, we expanded our analysis to include more conventional Cyber Range solutions to compensate for this deficiency. As a result, our findings and insights are more robust and captivating than they would have been without this inclusion.

3.1 Analysis

As previously stated, we intentionally opted to showcase only a select few examples. Next, we provide a concise overview of each tool.

SecGen — SecGen [15] is a tool designed for learning penetration testing techniques by generating vulnerable virtual machines. It offers a catalog of vulnerabilities that can be randomly selected based on scenario constraints defined in an XML-based configuration language. SecGen utilizes Puppet and Vagrant to create the necessary virtual machines. Although it lacks support for verification, SecGen allows for post-provisioning module tests to be conducted.

CyberVAN and VulnerVAN — CyberVAN [3] is a testbed environment that utilizes host virtualization and network virtualization technologies. It enables the creation of high-fidelity experimentation scenarios and flexible utilization of testbed resources. Scenarios within CyberVAN consist of interconnected virtual machines (VMs) running various operating systems, including Windows, Linux, and Android. These VMs are connected through a simulated network facilitated by network simulators like ns3, OPNET, and QualNET. CyberVAN supports realistic packet forwarding and control, including wireless protocols for mobile networks. Users can create, deploy, and save their own experimentation scenarios on CyberVAN testbeds, making it a versatile environment for cybersecurity training and exercises.

VulnerVAN [20], on the other hand, is used for generating vulnerable scenarios within CyberVAN. Users provide specifications of the target network and attack sequences using Network Input Collector and Attack Sequence Input Collector. The Vulnerable Scenario Generator (VSG) in VulnerVAN takes this input and generates a CyberVAN scenario with exploits and actions necessary for the specified attack steps. It also creates a sequence diagram depicting a realizable attack path. VulnerVAN includes an attacker playbook reference to facilitate Red Team operations during the attack steps.

CyExec* — CyExec* [9] [10] is a Cyber Range system that has been developed to address the challenges associated with the high initial and maintenance costs, as well as the difficulty of developing new scenarios, typically encountered in Cyber Range environments. This system leverages container-type virtualization, which offers a lightweight execution environment for running multiple virtual instances efficiently, thus optimizing hardware utilization and reducing overall costs. CyExec* incorporates a DAG-based scenario randomization technology. This system automatically generates multiple scenarios with the same learning objective, enhancing educational effectiveness, using the power of dockerfiles and docker-compose for topology generation.

Cyberbit Cyber Range — CyberBit Cyber Range [5] offers a robust and flexible infrastructure that allows for scalability and customization of scenarios. It features an automatic scenario emulator, reducing reliance on instructor red teams and enabling the execution of both benign traffic and complex attack sequences. The platform provides an extensive library of off-the-shelf scenarios and courses, facilitating efficient and accelerated training. Additionally, a user-friendly attack scenario builder eliminates the need for coding when creating new scenarios. The Cyber Range is accompanied by clear and comprehensive scenario documentation to support instructor onboarding as operations expand.

It supports both IT and OT environments, enabling simulation of attacks across various network topographies, including IT, SCADA, IoT, and more. CyberBit Cyber Range offers the flexibility of on-premises or cloud deployment, ensuring enhanced accessibility for users.

Airbus Cyber Range — The Airbus Cyber Range platform [2] offers a range of advanced features for modeling real or representative systems. Its graphical interface enables simplified construction through drag-and-drop functionality, allowing for efficient workspace management and the integration of multiple isolated environments. The platform supports collaborative modeling and integration work, facilitating effective teamwork. Integration with equipment and real systems is seamless, while the live traffic generator ensures realistic scenarios. The scenario engine enables the creation and execution of complex scenarios, while the platform also offers the capability to import/export machines or topologies. Access to screen offset and command line is available for each machine, ensuring granular control. Additionally, the platform efficiently manages the virtual machine park for seamless operation and scalability.

CRACK — CRACK [14] is a comprehensive framework that automates the design, model verification, generation, and testing of cyber scenarios. It leverages CRACK SDL, a Scenario Definition Language based on TOSCA, to declaratively specify scenario elements and their interactions. Notably, CRACK supports automatic verification of scenarios against training objectives through formal encoding of SDL properties. Upon successful verification, the framework automatically deploys the scenario in the Cyber Range and conducts tests to ensure consistency between the deployed system's behavior and its specification.

CRATE — CRATE [1] [6] is an emulation-based Cyber Range that employs a combination of virtual machines and hardware devices. Research experiments and training sessions are conducted through the execution of scenarios within emulated environments. To ensure flexibility, independence, and the ability to handle sensitive data, CRATE is hosted on a dedicated hardware platform locally. The Swedish Defence Research Agency operates and oversees CRATE's operations.

KYPO Cyber Range — The KYPO Cyber Range [21] stands out for its utilization of structured JSON files to define various aspects such as goals, network topology, software, and scenario workflows. These specifications are then transformed into Ansible and Puppet scripts, streamlining the deployment process. Additionally, KYPO offers a range of preconfigured templates that encompass diverse cybersecurity scenarios, including Distributed Denial of Service (DDoS) and phishing attacks. However, it is worth noting that KYPO lacks support for scenario verification and testing, which may limit its overall effectiveness in certain use cases.

3.2 Overall comparison

Next, we present a comparative analysis to provide an overall assessment of the features and capabilities of these tools, based on the predefined criteria. This analysis is based on existing results in Refs. [4][18], along with other resources gathered from platform specific papers.

Comparison — Table 1 presents some of our findings about the eight Cyber Ranges reported in our work. Next, we present a short summary about it.

Comparison Analysis — The European Cyber Security Organisation defines a Cyber Range as ''*A Cyber Range is a platform for the development, delivery and use of interactive simulation environments. A simulation environment is a representation of an organisation's ICT, OT, mobile and physical systems, applications and infrastructures, including the simulation of attacks, users and their activities and of any other Internet, public or third-party services which the simulated environment may depend upon. A Cyber Range includes a combination of core technologies for the realisation and use of the simulation environment and of additional components which are, in turn, desirable or required for achieving specific Cyber Range use cases*" [12].

Table 1. Comparison results

	SecGen	CyberVAN / VulnerVAN	CyExec*	Cyberbit CR	Airbus CyberRange	CRACK	CRATE	KYPO
Application Domain	Academic	Military & Defense	Academic	Commercial (as a service)	Commercial & Defense	Academic	Government & Military	Academic & Defense
Team Formation	None	None	None	Courses can be themed specifically for a team.	Yes, strong integration of teaming (Red, Blue, Grey, ...).	None	If needed, teams can get coloured (i.e., to define their role).	If needed, users can be grouped in teams (specific actions & rights).
Experimentation Methods	Simulation	Simulation	Simulation	Simulation	Simulation	Simulation	Emulation	Simulation
Infrastructure Technology	VM Networks powered by Vagrant & Puppet.	Cloud-based, VM Networks.	Container-based (Docker), run remotely or locally.	VM Network (cloud-based or local) as per client request.	VM Network as SaaS. Hybrid with actual IoT devices.	Directives for IaaS provider (supporting TOSCA interfaces).	VM Networks based on virtualbox.	Sandboxes in cloud-based VM networks.
User Interface	Access to powered VMs & web-based dashboard.	None	None	Yes, with skill tree, course catalog, scores, ...	Yes, strong gamification (web-based chat & scoreboard).	None	Hardened (e.g., VPN-based) GUI, reporting scores & exercices.	Web-based portal allowing end-user remote access.
Instructor Interface	Website (if existing) + Vagrant & other module configuration files.	XML files + GUI on Web interface.	Dockerfiles & docker-compose (requires high-level of expertise).	None	Scenario creation & orchestrations using a web interface, for deeper into customization.	None, apart from the scenarios defined with its SDL.	Web-based CRATE Exercise Control, providing management & support tools.	PMP can be used to create UI-based complex scenarios.
Scenario	Catalog of vulnerabilities defined in an XML-based language.	Pre-programmed scenarios, no automation. Import/export features.	DAG-based scenario randomization, customizable using docker-compose.	Large catalog of pre-made scenarios.	Large catalog of pre-made scenarios & on-demand scenarios.	No automation per se, but connection to a Scenario Definition Language based on TOSCA.	Graphical tool to create scenarios, without automation features.	No automation, but can get scenarios from other compatible platforms.
Scoring & Reporting	None	None	No	Yes, alongside with courses & MCQ	Yes	No	Yes	Yes
Topology Generation	Outputs Vagrant & Puppet files for each scenario.	Based on NS-3 networks & EMANE models.	Based on docker-compose.	Unspecified.	Drag & drop engine from instructor interface to setup VMs.	Based on the tested scenario.	NodeAgent service from API, to deploy VMs, set configurations, etc.	Visualization tools & easy-to-use creation tools.
Accessibility	Easily extendable and possible integration with CTFd.	Nothing specifiied	Container allows for more versatility.	Easy-to-use on demand service.	Easy-to-use.	Easy to use, once the scenario is created. Extensible & modular.	Roles are clearly defined. Usage of GUI make it user friendly.	Easy-to-use, well documents & highly UI-based tool.
Traffic	Nothing specified	Adversarial & background traffic generate on scenario basis.	Nothing specified	Nothing specified	On-demand	Not directly implemented in CRACK.	SVED (Scanning, Vulnerabilities, Exploits & Detection) able to mimic attack patterns.	Nothing specified
User Modeling	No	Yes	No	No	Yes	No	Yes (using SVED & Autolt, providing interactions with GUI tools).	Yes
Data Analysis	No	Yes	No	Yes	Yes	No	Yes, automated	Yes
License	GNU GPLv3 (or later)	Military & Defense	Academic	Commercial (as a service)	Commercial & Defense	Academic	Government & Military	Academic & Defense

In order to analyse our comparison tables, we need to ask ourselves *what makes a specific Cyber Range stand out?*, in regard to the previously quoted definition. Some responses are listed next:

- **Performance** is a crucial factor that Cyber Range creators must consider, particularly as the number of users and the complexity of network topologies increase. Emulation-based tools like CRATE allow for hardware attacks in Cyber Ranges but suffer from significant performance costs. In contrast, CyExec* utilizes container-based virtualization, reducing memory consumption by half and storage consumption to 1/60 compared to VM-based Cyber Ranges.
- **Usability** is an important consideration when aiming to reach a wide audience beyond specific companies or organizations. Graphical User Interfaces (GUIs) play a key role in providing easy access to the Cyber Range for end-users and enabling scenarists to create exercises on the spot. Platforms like Airbus CyberRange offer a comprehensive "in a box" solution, allowing any paying company to use it without additional requirements. KYPO and CRATE feature useful instructor interfaces that facilitate scenario creation within the Cyber Range itself. User-centric platforms such as CyberBit draw inspiration from existing Capture the Flag (CTF) platforms, incorporating dashboards, scoreboards, and progression curves. Currently, CRACK, CyberVAN, and CyExec have different development goals and may not prioritize extensive GUI features.
- **Scenario creation** is pivotal to the success of Cyber Ranges in any application domain. The inclusion of a wide variety of exercises is highly desirable. The presented Cyber Ranges employ different approaches to achieve this. SecGen, CyExec, and CRACK utilize declarative programming languages (such as XML, YAML, or CRACK SDL) to empower scenarists to create their own exercises. Other proprietary platforms may choose not to provide scenario editors but instead offer a large catalog of pre-made exercises. However, catalogs often come with additional costs or subscription-based business models, potentially limiting accessibility.
- **Automation** is one of the most advanced features a Cyber Range can incorporate. A comparison of multiple Cyber Ranges' automation levels is presented in this paper [6], with a focus on scenario and topology generation. Two dominant automation features stand out: scenario generation and topology generation. SecGen and CyExec* provide innovative methods to randomize and automate scenario creation based on templates, which is discussed further. Regarding topology generation, SecGen and CyExec must adapt the topology to the generated scenario. CRATE and CyberVAN offer solutions to automate parts of network topology generation, while Airbus developed a drag-and-drop interface that automates the background work of connecting components together, although it still relies heavily on human interaction.
- **Realism** is a challenging aspect to quantify or precisely define. Several features contribute to creating a realistic exercise, such as the presence of synthetic (bogus) traffic to emulate activity within the Cyber Range, user modeling to define patterns in the behavior of simulated users in the network, and team formation to assign specific and realistic tasks to groups of par-

ticipants. Realism appears to be inherent in platforms used for military or defense purposes. CyberVAN, CRATE, and KYPO all present solutions for creating realistic training contexts for response teams (blue, white, and green teams). CRATE and Airbus CyberRange go even further when deployed locally, enabling physical interaction with the network.

4 Scenario and Topology Generation

The ability to efficiently and realistically create a wide variety of exercises is a major challenge for Cyber Ranges. Our previous comparison revealed that currently, no platform successfully meets all three requirements simultaneously.

Topology generation poses significant difficulties when implementing Cyber Ranges, as it introduces various constraints. Depending on the infrastructure, scenario implementation, and desired level of user freedom, achieving effective topology generation may be extremely challenging or even unattainable.

The comparison presented in Table 1 highlights two standout Cyber Range platforms: SecGen and CyExec*. While there are other Cyber Ranges that could have been examined, it should be noted that some of them are privately owned solutions, which limits access to the resources necessary for understanding their methods of generating topology, thereby limiting our ability to comprehensively analyze them.

In the sequel, we conduct an in-depth analysis of how SecGen and CyExec* successfully automate scenario and topology generation while maintaining an efficient and user-friendly platform.

4.1 SecGen

SecGen [15], a Ruby application with an XML configuration language, is designed to facilitate the creation of realistic cybersecurity scenarios. It operates by reading and processing a comprehensive configuration that encompasses vulnerabilities, services, networks, users, and content. By incorporating scenario-specific logic, SecGen efficiently randomizes the generated scenarios. Leveraging the power of Puppet and Vagrant, the application effectively provisions the necessary virtual machines (VMs) for the scenario. An appealing aspect of SecGen is its open-source nature, with the code readily accessible on GitHub[7] under the GNU General Public License version 3 or later.

Architecture Overview — SecGen employs a structured architecture consisting of *system* objects that represent Virtual Machines (VMs) and *module* objects. VMs are based on selected Vagrant baseboxes determined by specified attributes. Each VM is associated with a list of SecGen modules, primarily chosen based on specified attributes.

Modules have various types (base, vulnerability, service, utility, network, generator, encoder) and include a module path and an associative array of attributes (such as CVE number [8], difficulty level, CVSS [9], etc.) defined in a

[7] https://github.com/cliffe/SecGen
[8] https://cve.mitre.org/
[9] https://nvd.nist.gov/vuln-metrics/cvss

secgen_metadata.xml file located at the root of a module's directory. Modules can receive data through named parameters from the output of other modules or from data stored in a datastore. Modules may incorporate Puppet code to be deployed and executed on the VMs (e.g., vulnerability, service, and utility modules) or local code for data randomization or transformation (e.g., encoder and generator modules). Modules can have default inputs, as well as dependencies or conflicts with other modules.

SecGen's operation comprises two stages: Stage 1 involves building the project output, while Stage 2 focuses on building VMs based on the generated project output.

During Stage 1, all available modules are read, along with the scenario definition. The scenario definition determines the selection of modules for each system. Some modules automatically include additional modules in the scenario, either as dependencies or default inputs for parameters. Randomization occurs in this stage. Modules with local code are executed to produce output, which is then used as input for other module parameters.

Librarian-puppet is utilized to deploy the corresponding puppet modules for the selected SecGen modules into the project output directory. A Vagrantfile is created, referencing the generated data and puppet modules. Additionally, output files describing the generated scenario, including an XML file listing flags with associated hints, are produced.

In Stage 2, the process simply involves invoking *vagrant up*, leveraging Vagrant to generate and provision the VMs based on the defined configuration.

Scenario Specification — SecGen utilizes a flexible module selection logic that considers various attributes defined in each module's secgen_metadata.xml file. These attributes, such as difficulty level and CVE, serve as constraints for module selection. If there is ambiguity in the selection process, SecGen employs randomization to choose from the remaining matching options. For instance, when filtering vulnerabilities based on a specified difficulty level, SecGen randomly selects from the vulnerabilities that meet the criteria. The filters specified for module selection are regular expression (regexp) matches, allowing for versatile and precise filtering capabilities.

4.2 CyExec*

While SecGen uses VMs to support its network topology generation, there are alternative approaches for recreating pseudo-realistic attack environments. The in-development platform called "CyExec*" aims to surpass SecGen and other VM-based Cyber Ranges by leveraging container-based virtualization. This paper [9] from 2021 presents a comprehensive experiment comparing the performance and reproducibility of container-based virtualization with other types of virtualization. The results demonstrate significant advantages, leading to the development of CyExec*, a Cyber Range that reduces memory consumption by half and storage consumption to 1/60 compared to other VM-based Cyber Ranges, while maintaining similar CPU usage.

CyExec* introduces an efficient approach for creating randomized scenarios and topology, enabling the generation of numerous exercises from a single template.

DAG-based Scenario — To generate multiple scenarios, the authors of this paper [10] aimed to understand the structure of a generic Cyber Range scenario. They concluded that a typical scenario consists of several milestones separated by operations and actions related to individual attack methods, similar to a Capture the Flag (CTF) challenge. Between two milestones, multiple subscenarios are possible. Based on this observation, the authors adopted the following approach: for a set of fixed milestones, randomization is incorporated into the selection of the means the attacker must employ to reach the next milestone.

Essentially, this randomized Cyber Range scenario takes the form of a Directed Acyclic Graph (DAG), where milestones are represented as vertices and subscenarios (randomly selected from a predefined pool) are represented as edges. This method allows the generation of multiple random scenarios with different paths but identical objectives from a single template. It enables users to experience similar security incidents in a wide variety of situations.

Implementation — In CyExec*, each component of the scenario topology is defined using a simple Dockerfile. To build a network environment using multiple Dockerfiles, the authors utilize docker-compose. Initially, the scenario creator provides a default scenario with a base system configuration (a docker-compose.yml file). Complex programs are unnecessary to build new scenarios—adding or modifying Dockerfiles and the docker-compose.yml file is sufficient.

To create the aforementioned DAG-based scenario, each distinct possibility for connecting two milestones requires its own Dockerfile. A function randomly selects a subscenario and adds the corresponding Dockerfile to the docker-compose.yml file, thereby generating the random scenario. Additionally, a Dockerfile for the end-user interface in the network is included, which can be a Kali Linux image running in the network, accessible through a web interface or via *docker exec*.

To summarize, the scenario creator starts by designing a template docker-compose.yml file that defines the milestones for the default scenario. For each consecutive pair of milestones, they create multiple Dockerfiles, each representing an independent vulnerable service or machine that leads to the same milestone. Once all the components are prepared, the scenario creator informs CyExec* about the desired number of environments to generate, the number of users, and other relevant parameters. The software then generates docker-compose files based on the default template, while randomly selecting the different Dockerfiles that allow the end-users to progress from one milestone to the next.

5 Discussion and Open Challenges

In addition to performance, scalability, and diversity considerations, future research should focus on addressing key challenges within Cyber Range platforms.

As we delve into the evaluation of existing Cyber Range platforms, it becomes evident that each solution has its unique strengths and limitations. For example, while CyExec* stands out as a lightweight platform, its reliance on labor-intensive preparations limits the extent of result randomization. On the other hand, SecGen offers simplicity and adequate variety, but its resource-intensive nature poses constraints. However, to drive the field forward, it is essential to explore ways to reconcile the positive aspects found across multiple platforms and push the boundaries of what is currently available. By harnessing the best features and functionalities from different solutions, we can propel the development of more advanced and comprehensive Cyber Range platforms. To encourage collaboration and advancement in the field, authors are encouraged to release their code on accessible platforms such as GitHub or GitLab, accompanied by an extensive README.md documentation. By providing open access to their codebase, researchers enable others to experiment, learn, and build upon existing foundations, fostering innovation and collaboration within the Cyber Range community.

The integration of AI within Cyber Range platforms and network topology generation tools holds great potential for enhancing their capabilities. As mentioned in [7], *there are relatively few literatures on the development trend of AI in the field of cyber range*. In particular, machine learning (ML) algorithms could automate scenario design by analyzing historical data and generating dynamic and diverse scenarios, saving time for instructors while maintaining challenging training environments. Additionally, ML techniques could enable adaptive user modeling, tailoring the training experience to individual needs and skill levels. This personalization enhances learning outcomes and allows for more effective skill development. Furthermore, ML algorithms can simulate realistic network traffic patterns, mimicking real-world threats and facilitating immersive training experiences.

It is of utmost importance to prioritize ethical considerations when researching new methods for automation within Cyber Range platforms with the use of AI. As the field advances and AI technologies become more integrated into cybersecurity training and experimentation, it is crucial to ensure responsible and ethical practices. By proactively addressing ethical concerns, researchers can mitigate potential risks and promote the development of AI-driven automation that aligns with societal values. This involves safeguarding user privacy and data security, addressing biases and fairness issues, and establishing clear guidelines for responsible use. By integrating ethical considerations into the research process, we can ensure that the benefits of automation and AI within Cyber Range platforms are harnessed in a manner that respects individual rights, upholds accountability, and promotes the responsible application of these technologies in the field of cybersecurity.

Apart from the previously-mentioned difficulty that refers to the automatic generation of scenarios, some challenges still exist in the Cyber Range ecosystem. For example, the users' motivation should be considered during the trainings. In this sense, the use of gamification elements would help as it has been proven a powerful approach to improving student motivation [8]. Still, its application in the context of cybersecurity has mainly been limited to serious games [17]. Furthermore, the cyberexercises proposed in the Cyber Ranges are static, be-

ing unable to adapt to the users' capabilities. One could easily argue that a system capable of dynamically adapting the cyberexercises based on the users' performance would be greatly appreciated.

Another notable shortcoming of the analyzed Cyber Ranges is the absence of powerful learning analytics. Those tools are fundamental for educators since, by using them, they would be granted comprehensive access to the complete dataset encompassing their students, thereby facilitating the provision of tailored assistance and diligent oversight. On the other side, students could access their individual performance metrics, thus promoting self-awareness and self-assessment.

By amalgamating these attributes within a unified platform, the Cyber Range encompasses the components commonly referred to as the Learning Content Management System (LCMS) utilized by instructors for content creation, and the Learning Management System (LMS), which serves as the arena for students' learning experiences [11]. Consequently, the application of the Learning Tools Interoperability (LTI) IMS standard presents an opportunity for Cyber Range platforms to function as external providers of cybersecurity exercises [16]. This, in turn, allows for the seamless integration of Cyber Range with other LMSs such as Sakai, Moodle, or Open edX, thereby facilitating the effective delivery of comprehensive cybersecurity courses encompassing both theoretical and practical components.

6 Conclusion

In this research paper, an analysis of eight Cyber Range platforms has been conducted, focusing on their features and capabilities. The principal objective was to comprehensively understand the significance involved in developing such powerful tools for cybersecurity education. Cyber Ranges offer a necessary and innovative approach to teaching cybersecurity to both students and professionals across various fields. With this mindset, a side-by-side comparison has been presented, leveraging detailed criteria and, thus, reaching a fair analysis of the selected tools.

Particularly, the study focuses on the generation of cybersecurity training scenarios since they represent one of the main limitations of the current Cyber Range ecosystem. Indeed, the simulation of large-scale networks for cyber-attack scenarios can be highly resource-intensive and demanding in terms of performance. Additionally, generating a diverse set of exercises can be a time-consuming and challenging task. Some platforms, such as CyberBit CR and Airbus CyberRange, have opted to refrain from automating their scenario and topology generation processes. Instead, they rely on extensive exercise catalogs provided to their clients. Nonetheless, emerging tools like SecGen, CyExec*, and CRATE aim to address this issue by introducing new features for scenario randomization and automatic topology generation.

To foster the performed research, two existing approaches and platforms for topology generation have been reviewed, highlighting their strengths and limitations. Through the analysis, it is evident that a successful cybersecurity training environment requires scalable, diverse, and performance-oriented topology generation techniques.

Additionally, we have also discussed the trade-offs between container-based comprehensive platforms, such as CyExec*, and simpler yet resource-intensive VM-based platforms like SecGen. While CyExec* offers extensive capabilities, its labor-intensive preparations limit result randomization. On the other hand, SecGen provides simplicity but poses constraints due to its resource-intensive nature.

The future development of Cyber Range platforms should aim to address these challenges and strike a balance between comprehensiveness, resource efficiency, and diversity. Moreover, we have emphasized the potential of AI in enhancing Cyber Range platforms. Machine learning algorithms can automate scenario design, analyzing historical data to generate dynamic and diverse training scenarios. ML techniques can also enable adaptive user modeling, tailoring the training experience to individual needs and skill levels. Moreover, AI can simulate realistic network traffic patterns, providing immersive training experiences. However, it is crucial to prioritize ethical considerations when integrating AI into Cyber Range platforms. Responsible and ethical practices should be followed to safeguard user privacy, address biases, and ensure the responsible use of AI technologies. Finally, we have discussed the educational viewpoint of Cyber Range platforms, suggesting the use of tools to motivate the students and powerful learning analytics, while the integration with other LMS would be really appreciated.

Acknowledgements — This work has been supported by the Spanish Ministry of Universities linked to the European Union through the NextGenerationEU program, under Margarita Salas postdoctoral fellowship (172/MSJD/22). The work represents as well a contribution to the International Alliance for Strengthening Cybersecurity and Privacy in Healthcare (CybAlliance, Project no. 337316).

References

1. Jonas Almroth and Tommy Gustafsson. Crate exercise control–a cyber defense exercise management and support tool. In *2020 IEEE European Symposium on Security and Privacy (EuroS&P) Workshops*, pages 37–45. IEEE, 2020.
2. Adrien Bécue, Eva Maia, Linda Feeken, Philipp Borchers, and Isabel Praça. A new concept of digital twin supporting optimization and resilience of factories of the future. *Applied Sciences*, 10(13), 2020.
3. Ritu Chadha, Thomas Bowen, Cho-Yu Chiang, Yitzchak Gottlieb, Alex Poylisher, Angello Sapello, Constantin Serban, Shridatt Sugrim, Gary Walther, Lisa Marvel, Allison Newcomb, and Jonathan Santos. Cybervan: A cyber security virtual assured network testbed. pages 1125–1130, 11 2016.
4. Nestoras Chouliaras, George Kittes, Ioanna Kantzavelou, Leandros Maglaras, Grammati Pantziou, and Mohamed Amine Ferrag. Cyber ranges and testbeds for education, training, and research. *Applied Sciences*, 11:1809, 02 2021.
5. Cyberbit. Cyber security training platform. `https://www.cyberbit.com/blog/security-training/cyber-security-training-platform/`, 2023. Accessed on Jun 21, 2023.
6. Tommy Gustafsson and Jonas Almroth. Cyber range automation overview with a case study of crate. 11 2020.
7. Jiujiang Han, Ming Xian, Jian Liu, and Huimei Wang. Research on the application of artificial intelligence in cyber range. *Journal of Physics: Conference Series*, 2030:012084, 09 2021.

8. Elisa D Mekler, Florian Brühlmann, Klaus Opwis, and Alexandre N Tuch. Do points, levels and leaderboards harm intrinsic motivation? an empirical analysis of common gamification elements. In *Proceedings of the First International Conference on gameful design, research, and applications*, pages 66–73, 2013.
9. Ryotaro Nakata and Akira Otsuka. Cyexec*: A high-performance container-based cyber range with scenario randomization. *IEEE Access*, 9:109095–109114, 01 2021.
10. Ryotaro Nakata and Akira Otsuka. Cyexec*: Automatic generation of randomized cyber range scenarios. In *International Conference on Information Systems Security and Privacy*, 2021.
11. Suman Ninoriya, PM Chawan, and BB Meshram. Cms, lms and lcms for elearning. *International Journal of Computer Science Issues (IJCSI)*, 8(2):644, 2011.
12. European Cyber Security Organisation. Understanding cyber ranges: From hype to reality. 2020.
13. Enrico Russo, Gabriele Costa, and Alessandro Armando. Scenario design and validation for next generation cyber ranges. In *2018 IEEE 17th International Symposium on Network Computing and Applications (NCA)*, pages 1–4, 2018.
14. Enrico Russo, Gabriele Costa, and Alessandro Armando. Building next generation cyber ranges with crack. *Computers & Security*, 95:101837, 2020.
15. Z. Cliffe Schreuders, Thomas Shaw, Mohammad Shan-A-Khuda, Gajendra Ravichandran, Jason Keighley, and Mihai Ordean. Security scenario generator (SecGen): A framework for generating randomly vulnerable rich-scenario VMs for learning computer security and hosting CTF events. In *2017 USENIX Workshop on Advances in Security Education (ASE 17)*, Vancouver, BC, August 2017. USENIX Association.
16. Antonio J Sierra, Álvaro Martín-Rodríguez, Teresa Ariza, Javier Muñoz-Calle, and Francisco J Fernández-Jiménez. Lti for interoperating e-assessment tools with lms. In *Methodologies and Intelligent Systems for Technology Enhanced Learning: 6th International Conference*, pages 173–181. Springer, 2016.
17. Jin-Ning Tioh, Mani Mina, and Douglas W Jacobson. Cyber security training a survey of serious games in cyber security. In *2017 IEEE Frontiers in Education Conference (FIE)*, pages 1–5. IEEE, 2017.
18. Elochukwu Ukwandu, Mohamed Amine Farah, Hanan Hindy, David Brosset, Dimitris Kavallieros, Robert Atkinson, Christos Tachtatzis, Miroslav Bures, Ivan Andonovic, and Xavier Bellekens. A review of cyber-ranges and test-beds: Current and future trends. *Sensors*, 20(24):7148, 2020.
19. Dustin Updyke, Geoff Dobson, Thomas Podnar, Luke Osterritter, Benjamin Earl, and Adam Cerini. Ghosts in the machine: A framework for cyber-warfare exercise npc simulation. 12 2018.
20. Sridhar Venkatesan, Jason Youzwak, Shridatt Sugrim, Cho-Yu Chiang, Alexander Poylisher, Matthew Witkowski, Gary Walther, Michelle Wolberg, Ritu Chadha, Allison Newcomb, Blaine Hoffman, and Norbou Buchler. Vulnervan: A vulnerable network generation tool. 11 2019.
21. Jan Vykopal, Radek Ošlejšek, Pavel Celeda, Martin Vizváry, and Daniel Tovarňák. Kypo cyber range: Design and use cases. pages 310–321, 01 2017.
22. Muhammad Mudassar Yamin and Basel Katt. Modeling and executing cyber security exercise scenarios in cyber ranges. *Computers & Security*, 116:102635, 2022.
23. Muhammad Mudassar Yamin, Basel Katt, and Vasileios Gkioulos. Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. *Computers & Security*, 88:101636, 2020.