Multi-Technology Infrastructure for Advanced Training and Testing in Cyber Range Systems

Ionuț LATEȘ[1], Cătălin BOJA[1], Alin ZAMFIROIU[1,2]*

[1] Bucharest University of Economic Studies, 6 Piata Romana, Bucharest, 010374, Romania
ionut.lates@csie.ase.ro, catalin.boja@csie.ase.ro, alin.zamfiroiu@csie.ase.ro

[2] National Institute for Research & Development in Informatics - ICI Bucharest,
8-10 Mareșal Averescu Avenue, Bucharest, 011455, Romania
alin.zamfiroiu@ici.ro (**Corresponding author*)

Abstract: This paper presents the design and deployment of a multi-technology infrastructure which was created for advanced training and testing within cyber range systems. By integrating modern tools such as Terraform for Infrastructure as Code (IaC), Ansible for configuration management, and VMware for virtualization, the proposed architecture becomes scalable, automatable and secure. The proposed infrastructure focuses on automation as in can enhance its deployment speed, reduce errors and ensure consistency across different training environments. Additionally, this paper demonstrates that the proposed infrastructure can adapt to hybrid cloud solutions and that it is capable of supporting complex, isolated network topologies for multi-team exercises. The presented benchmarks related to this infrastructure reveal significant improvements as regards the deployment efficiency and resource utilization. This paper concludes that this multi-technology cyber range infrastructure enhances cybersecurity training and educational services by providing realistic, scalable, and secure environments for hands-on training and testing.

Keywords: Cyber Range, Automation, Capture the Flag, Infrastructure as Code, Terraform, Ansible, Cybersecurity Training.

1. Introduction

Today, it is more important than ever to be able to evaluate the skills of cybersecurity professionals effectively due to the field's rapid evolution. Traditional methods are struggling to keep pace with the increasing complexity and frequency of cyber threats. This need has encouraged the creation of novel strategies, one of which stands out as a crucial remedy: cybersecurity cyber range exercises.

Cybersecurity experts can participate in realistic scenarios that replicate the complexity of actual cyber threats and attacks in a dynamic and immersive environment by using cyber range exercises (Linardos, 2021). These activities provide practitioners with the chance of gaining practical experience while also evaluating their capacity to apply academic information in real-world contexts. Cyber ranges enable a thorough assessment of the abilities which are essential for managing and preventing cyber incidents by simulating cyber-attack situations, from detection to mitigation and reaction (Ukwandu et al., 2020). This paper aims to determine the effectiveness and methodology of employing cyber range exercises as tools for cybersecurity competence assessment. It explores how these tests might be set up and evaluated to offer significant insights into the abilities and preparedness of cybersecurity experts. The integration of cyber ranges in the assessment procedure represents a substantial change in direction toward a more practical, experience-based evaluation methodology. This research contributes to the existing body of knowledge on enhancing cybersecurity competence evaluation and establishes a foundation for future studies and advancements in cyber range exercises. With the increased reliance on digital infrastructure and the accompanying increase in cyber threats, this research is pertinent and important. Through the improvement of cybersecurity competency assessment techniques, stakeholders from many industries can more effectively recognize, nurture, and utilize the talent required to protect digital assets and uphold cyber resilience (Glas et al., 2023).

Țhe remainder of this paper is structured as follows. Section 2 provides information regarding the cyber range infrastructure orchestration and configuration technologies used for different cyber range types. Section 3 describes the proposed methodology related to the integration of Terraform for infrastructure provisioning and to the integration of Ansible for configuration management. Further on, Section 4 sets forth the generic architecture design for a cyber range system, providing detailed information about each component of a cyber range infrastructure. Section 5 outlines the implementation challenges and benchmarks, while Section 6 discusses the obtained results and the related implications. Section 7 provides a comparative analysis of

https://doi.org/10.24846/v34i3y202502

the cyber range types introduced in the previous sections, including the proposed model. Finally, Section 8 concludes this paper and outlines possible future research directions.

2. Infrastructure Orchestration and Configuration

Table 1 presents numerous types of cyber ranges and the various technologies used in order to enable distinct cybersecurity training and simulation scenarios. Each type of cyber range is specifically designed to address distinct business requirements, ranging from general implementations and industrial control systems to specialized areas such as finance, healthcare, and government defense. Technologies such as VMware, Terraform (HashiCorp, 2025), and Ansible (Red Hat, 2025) are essential, providing virtualization, infrastructure automation, and seamless security orchestration. Open-source tools like KVM, as well as container-based solutions like Docker and Kubernetes, are used for creating more flexible and scalable cyber range environments.

One important technology used in cybersecurity to automate the deployment and management of cyber ranges is Terraform (Ong et al., 2023; Thiyagarajan, 2020; Pathak, 2024). For example, cybersecurity training platforms such as RangeForce and cybersecurity training businesses such as CyberBit (Werner, 2021) offer hands-on activities designed for enterprise clientele. Without Terraform, setting up training environments for each customer would require a manual VM, network, and security configuration, making the process time-consuming and labour-intensive. This hampered the efficiency of training delivery while also limiting the scalability of cyber ranges. By introducing Terraform, these companies were able to specify their infrastructure as code (IaC), allowing them to fully automate the deployment process. With Terraform (Ong et al., 2023; Thiyagarajan, 2020; Pathak, 2024), the deployment of preconfigured VMs, networking components, and security tools across several cloud platforms, including AWS, Azure, and Google Cloud Platform (GCP), can be done by a single command. The infrastructure can be quickly torn down and rebuilt after each session, ensuring a clean slate for every exercise. Scalability was greatly enhanced because new training sessions could be turned up automatically without manual intervention. Cost optimization was achieved by ensuring that resources were only available when needed, reducing unnecessary cloud expenses. Multi-cloud flexibility enabled the same infrastructure code to be deployed across various cloud providers and on-premises environments, providing flexibility for different needs. (Virág et al., 2021; Katsantonis et al., 2023).

Table 1. Technologies used for Cyber Range infrastructures

Cyber Range	Technologies Used	Source
Cyber Range Revolution (General Implementation)	VMware vSphere, Terraform, Ansible	(Ong et al., 2023)
Industrial Control Cyber Range	VMware for virtualized attack simulation	(Low et al., 2022)
Security Automation Cyber Range	Ansible for automated security scenarios	(Acheampong et al., 2022)
Cloud-based Disaster Recovery Cyber Range	Terraform & Ansible for automated recovery	(Thiyagarajan, 2020)
Cyber Ranges in the Financial & Healthcare Sectors	Terraform & Ansible for IaC deployment	(Pathak, 2024)
Educational Cyber Range	Open-source virtualization tools (KVM, VMware)	(Brunner et al., 2019)
National Cyber Range (Government & Defense)	VMware & Hybrid Cloud Infrastructure	(Yamin et al., 2020)
CyExec* Container-Based Cyber Range	Container-based virtualization (Docker, Kubernetes)	(Nakata & Otsuka, 2021)
USA National Cyber Range (NCR)	Network traffic generator/injector	(Park et al., 2022)
SIEM Tools	Cyber Security Lab - Universiti Teknologi MARA (UiTM), Malaysia	(Mohd Ariffin et al., 2022)
IDS	AIT cyber range	(Mills et al., 2024)

Other important use cases for Terraform in cyber ranges are red teaming and attack simulations. Terraform enables rapid red team deployment, increasing the testing frequency and effectiveness. Consistent configurations ensure standardized environments, while automated cleanup removes any residual infrastructure enhancing the overall system security (Kokkonen et al., 2022).

Another technology with a significant impact on the automation of numerous cyber operations, particularly blue team training and incident response exercises, is Ansible. Government-operated cyber ranges, such as the IBM X-Force Cyber Range or CybExer (GFCE, 2025), are responsible with training Security Operations Centre (SOC) analysts in cyber threat detection, response, and mitigation. Configuring key security tools like SIEM, IDS, and firewalls was time-consuming and labor-intensive, slowing down the training setup and introducing potential inconsistencies. (Georgescu et al., 2020). Ansible automated the deployment of tools like Splunk (SIEM), Suricata (NIDS), and OSSEC (HIDS), enabling a fast infrastructure setup and immediate analyst engagement. This ensured a rapid, realistic training with consistent environments and reduced human error (Park et al., 2022).

Ansible enables the enforcement of compliance automation and security hardening in cyber ranges. For example, a hospital security team can use Ansible to apply and monitor security configurations based on CIS benchmarks and STIGs, ensuring compliance with standards like HIPAA and NIST. Playbooks deploy settings across systems, detect deviations, and auto-correct misconfigurations, thereby reducing vulnerabilities, maintaining compliance, and freeing engineers from repetitive tasks so that they focus on strategic security efforts (Gustafsson & Almroth, 2020; Yamin & Katt, 2022).

Considering the hardware infrastructure and hypervisors, VMware technologies are critical in developing high-fidelity, secure environments for cyber range exercises. For example, the NIST National Cyber Range (NCR) holds large-scale military cyber exercises for training people for nation-state-level cyber warfare. One of the key problems with regard to these exercises was the necessity for a safe, realistic training environment capable of correctly replicating real-world network infrastructure without putting sensitive systems at risk. VMware ESXi (Ong et al, 2023) offers an ideal answer by hosting full-scale enterprise networks. This system enabled red teams (offensive security) and blue teams (defensive security) to participate in realistic cyber warfare simulations that replicated the intricacies of real enterprise networks.

VMware's snapshot capability enabled rapid VM rollbacks, allowing quick resets between exercises for a continuous iterative training. It provided realistic enterprise environments, improved security through isolation, and supported flexible scenarios via instant restoration, eliminating the manual reconfiguration overhead (Sharifi et al., 2021).

VMware offered risk-free testing by isolating training from production systems, ensured accuracy through realistic replicas of the corporate infrastructure, and cut costs by eliminating the need for extra hardware. This blend of realism, security, and efficiency makes VMware essential for modern cyber ranges in both government and commercial settings (Jelo & Helebrandt, 2022; Glas et al., 2023).

Based on this research one can draw the conclusion that modern cyber ranges rely on three core technologies, each of them playing a distinct role. Terraform excels in scalable, cloud-based attack simulations, enabling a fast deployment across platforms like AWS and Azure, which are ideal for flexible, cost-effective red teaming. Ansible supports blue team training, the automation of security setup and compliance enforcement with regard to standards like HIPAA and NIST, reducing human effort while strengthening security. VMware enables high-fidelity enterprise simulations with full-system virtualization, allowing snapshot-based rollbacks and a safe, realistic training.

Together, these technologies form a full toolkit for creating flexible, secure, and realistic cyber ranges that can be adapted to a variety of training and operational requirements (Ukwandu et al., 2020; Ong et al., 2023).

3. Methodology

The proposed methodology focuses on the integration of Terraform for infrastructure provisioning and of Ansible for configuration management. The diagram in Figure 1 illustrates the automated deployment process for CTF exercises, outlining each phase from the initial formulation of exercise specifications to the final validation and readiness of the infrastructure.

The deployment process begins with the specification related to the CTF exercises. This includes deciding what types of challenges to include, the amount of resources needed and whether any specific settings or security measures are required. Once these criteria are established, the following step is to identify the infrastructure requirements. The extraction method identifies the virtual machines, networking components, and storage resources required for the exercises.

After establishing the infrastructure specifications, Terraform provisions the specified resources by initializing the infrastructure setup, which makes up the foundation for the CTF exercises. Next, the system determines if the infrastructure was effectively installed or if it stays unaltered from earlier deployments. If the infrastructure is already in place or if it was successfully deployed, the process continues with the extraction of the configuration specifications. If the infrastructure was not yet installed, Terraform scripts provision the required virtual machines, networks, and storage space, ensuring its consistent and automated deployment. When the infrastructure deployment encounters issues, the system follows the established error management protocols, like re-applying the Terraform scripts and recording any persistent issues. If the issues remain unresolved, a fatal error occurs, terminating the deployment process.

Once the infrastructure is in place, the next step is to extract the configuration specifications. This phase describes the installation of programs, the service configurations, and security settings required for the CTF environment. Ansible is then employed for applying these settings, automating the software installation and service configuration. The implementation of service configurations is then tested to guarantee their accuracy. If the configurations are successfully implemented, the procedure will go on with validation and testing. However, if problems occur, Ansible's error handling and logging tools are enabled and attempts of reimplementing the configurations are made. Persistent mistakes result in a fatal error, which ends the process of CTF infrastructure deployment.

Validation and testing are critical components of this process, which ensure that all CTF services function properly. This step involves comprehensive testing to verify if the CTF environment meets the defined criteria. The results of these tests define the readiness of the CTF infrastructure.

The process ends with a notification on the CTF infrastructure readiness, assuming all validations are successful. If unrecoverable issues are discovered at any step, the deployment is halted, and detailed logs are provided to aid in troubleshooting.

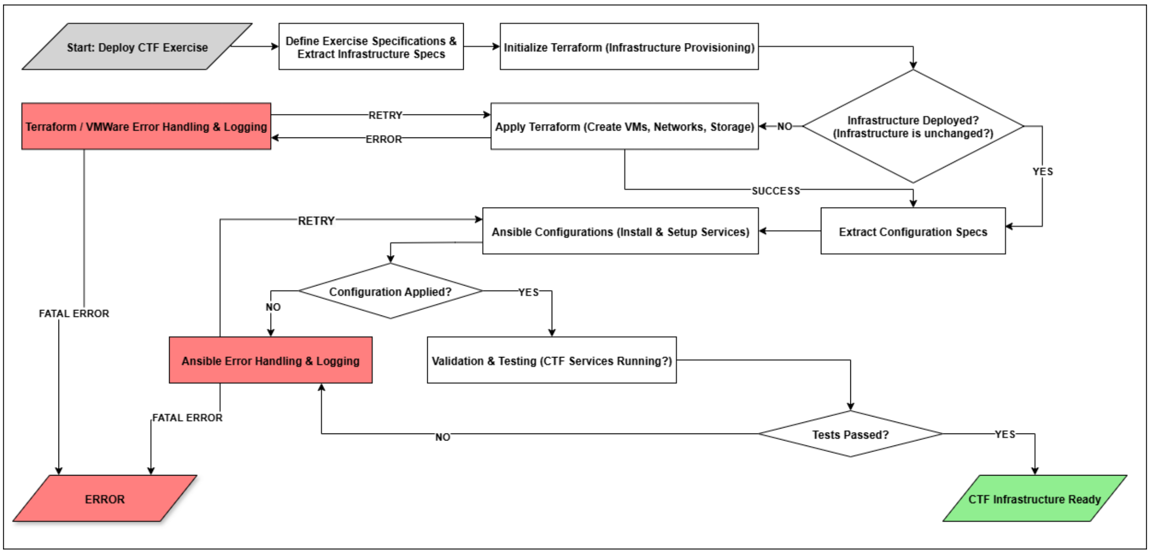
Start: Deploy CTF Exercise
Define Exercise Specifications & Extract Infrastructure Specs
Initialize Terraform (Infrastructure Provisioning)
Terraform / VMWare Error Handling & Logging
RETRY
ERROR
Apply Terraform (Create VMs, Networks, Storage)
NO
Infrastructure Deployed? (Infrastructure is unchanged?)
YES
SUCCESS
RETRY
Ansible Configurations (Install & Setup Services)
Extract Configuration Specs
Configuration Applied?
YES
NO
FATAL ERROR
Ansible Error Handling & Logging
Validation & Testing (CTF Services Running?)
FATAL ERROR
NO
Tests Passed?
YES
ERROR
CTF Infrastructure Ready

Figure 1. CTF infrastructure deployment methodology

To sum up, the automated deployment process, as described, makes use of Terraform and Ansible to deploy and configure an efficient, reproducible, and error-free CTF exercises infrastructure. This methodology not only simplifies the setup procedure, but it also guarantees the consistency and dependability required for an effective cybersecurity training. By adopting this strategy, organizations may improve the scalability of their training programs while also providing robust environments for building cybersecurity capabilities.

4. Generic Architecture

Figure 2 illustrates a strong, multifaceted cyber range architecture that employs cutting-edge technology and tools to deliver a dynamic, scalable, and secure training environment. It emphasizes the seamless integration of automation, virtualization, cloud resources, and collaboration platforms, which are critical to providing successful cybersecurity training and simulations in today's fast-changing cyber threat scenario.

Critical automation and orchestration tools power the Core Infrastructure, streamlining the scenario deployment and management. Terraform and Ansible are vital tools for designing the Infrastructure as code (IaC) and automating the virtual environment configuration, respectively. The Infrastructure Administration System and the Scenario Administration System offer a centralized control over the deployment, monitoring, and deconstruction of training environments, ensuring an efficient management and a rapid scalability. GitLab for version control, OpenVPN Server for secure remote access, and the collaboration platforms like Slack, Jitsi Meet and Moodle all help to facilitate communication, coordination, and e-learning integration inside the cyber range ecosystem.

The infrastructure is built on a combination of private cloud hardware and public cloud resources from providers such as AWS, Azure, and Google Cloud, allowing for hybrid deployment models that combine on-premises system security and control with cloud service scalability and flexibility. The Hypervisor layer, powered by VMware ESXi and vCenter, ensures an effective virtualization by creating isolated environments for each scenario and optimizing resource consumption throughout the hardware stack.

If the individual scenario infrastructures are zoomed in, it can be seen that each of them is provisioned with a set of critical cybersecurity tools and technologies. This includes Scenario VMs and Containers that simulate real-world IT environments, an OpenVPN Server for secure access, and security monitoring tools such as IDS/IPS (Intrusion Detection/Prevention Systems) and SIEM solutions like Wazuh and Snort. Furthermore, penetration testing and incident response tools are incorporated, allowing the participants to engage in extensive, hands-on cybersecurity exercises that simulate real-world challenges.

At a large scale, the Cyber Range systems architecture consists of three main components:

- the private cloud configured with hardware and a hypervisor, or public cloud;
- the core infrastructure represented by the orchestration and configuration systems, the scenario development and administration tools,

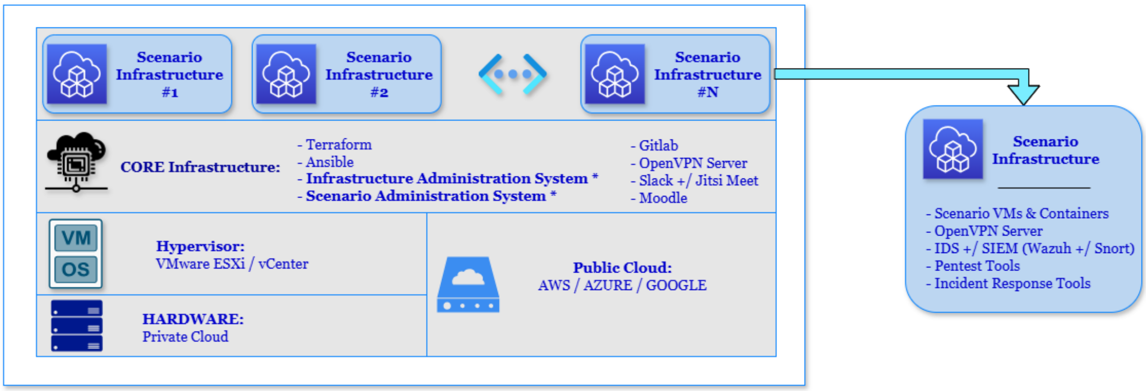

Figure 2. Generic cyber range architecture

version control and communications systems, network configuration, administration and exercise management tools;

- the scenario infrastructure which is the result of the design, implementation, orchestration and configuration of a scenario.

The cyber range architecture can be deployed on a private cloud infrastructure configured with a dedicated hardware and hypervisor technology or on a public cloud platform. In the case of a private cloud, organizations can leverage their own data centers and hardware resources to create a scalable and isolated environment for the cyber range. Alternatively, organizations can opt for a public cloud solution which provides on-demand scalability and infrastructure resources for hosting the cyber range.

The core infrastructure of the cyber range architecture comprises various components and systems that facilitate the orchestration, configuration, and management of that environment. This covers orchestration technologies that automate the provisioning and configuration of infrastructure resources, such as Terraform or Ansible. Cyber defense scenarios are built by using planning tools, with the setups and code tracked via GitLab. The participants and instructors collaborate in real time through chat or video platforms. Network settings are configured with admin tools, while exercise management systems help the instructors plan, monitor, and assess the participant performance.

Each cyber defense scenario is specifically designed to mirror real-world cybersecurity difficulties, giving the participants practical experience and training possibilities. Aside from the actual network environments, services, and applications, the infrastructure also includes virtualized environments that the participants can use in these scenarios. The deployment, configuration, and monitoring of the scenarios are coordinated and managed by the core infrastructure components, assuring the system's consistency. This makes it simple to replicate, scale, and customize the scenarios to match various training goals and learning results.

The cyber range architecture offers a flexible and scalable environment for cybersecurity training, testing, and experimentation by merging the hardware level, core infrastructure, and scenario infrastructure components. Organizations can use it in order to model accurate cyber defense scenarios, allowing the participants to practice their skills in a safe environment.

Creating a highly automated cyber range requires the integration of multiple architectural components to enable scalability, flexibility, security, and realism in cybersecurity training and testing environments. Scalability is a critical requirement, allowing the infrastructure to extend horizontally in order to handle a large number of virtual machines (VMs) or containers running various cybersecurity scenarios simultaneously. This is accomplished via virtualization tools like VMware or container orchestration solutions like Kubernetes, which enable a dynamic resource allocation and an efficient administration of complex workloads.

Virtualization and emulation are critical for building isolated, reproducible, and regulated environments that closely simulate real-world IT systems. Virtualization technologies replicate network topologies, operating systems, and applications, whereas network emulation tools simulate network characteristics such as latency and packet loss, creating realistic situations for hands-on training and testing. An orchestration and configuration management framework supports these technologies by automating the deployment, configuration, and monitoring of cybersecurity scenarios. This platform streamlines scenario generation and resource management, which results in uniform, efficient, and repeatable settings across numerous contexts.

The use of Infrastructure as Code (IaC) concepts with tools such as Terraform and Ansible improves automation by allowing the declarative specification of infrastructure components and configurations. This strategy makes version control, consistent deployment, and rapid replication of environments easier, encouraging collaboration and simplifying infrastructure maintenance. Network security restrictions are similarly important, ensuring that the cyber range is segregated from the production systems and protected from unwanted access. The cyber range environment's integrity and confidentiality are maintained by implementing firewalls, access controls, encryption, and intrusion detection systems, as well as by conducting regular security audits.

A strong monitoring and analytics system is essential for tracking infrastructure performance, participant activity, and security events. This system offers insights for optimizing the training performance, identifying performance bottlenecks, and improving the effectiveness of cybersecurity scenarios. Integrating the cyber range with threat intelligence platforms and Security Information and Event Management (SIEM) systems guarantees that scenarios reflect real-world threats, preparing the participants to face various cyber problems.

Finally, integrating text, audio, and video communication systems improves collaboration, coordination, and knowledge exchange among students and teachers. These tools offer a dynamic and interactive learning environment that enhances the training experience.

By embracing these architectural requirements, businesses can create a highly automated cyber range that would provide effective, realistic cybersecurity training, testing, and experimentation.

5. Implementation Challenges and Benchmarks

One of the issues in cyber range deployment is maintaining an effective isolation of groups and scenario instances. In a multi-user, multi-scenario environment, where multiple teams or individuals may be participating in different cybersecurity exercises simultaneously, a strict separation between these instances is critical for avoiding interference, data leakage, and unintended cross-contamination of activities. Isolation ensures that the activities, data, and configurations typical of a scenario do not affect other scenarios, hence maintaining the integrity of each training session is important.

Proper isolation ensures that participants are in realistic, interference-free situations while protecting sensitive data and guaranteeing the smooth execution of several activities. However, deploying and sustaining these isolation techniques can be difficult, as it necessitates a combination of technologies, policies, and ongoing monitoring to assure a consistent and dependable separation of scenario instances.

Ensuring a secure and separated playground network access in a cyber range is critical for controlled training scenarios. VPN tunnelling using OpenVPN provides encrypted access for remote users, while QoS measures optimize bandwidth for high-intensity cybersecurity exercises. Continuous monitoring with IDS (Snort), SIEM (Wazuh), and network analytics detects unwanted access, while automated provisioning and teardown using Terraform, Ansible, and snapshots keep cyber range environments clean and secure. Cyber Ranges may provide realistic cybersecurity training by leveraging VMware port groups for segmentation and OpenVPN for a controlled access.

The CTF infrastructure comprises 90 virtual machines (VMs) distributed among multiple teams, each equipped with an OpenVPN server for a secure access, playground servers exposing various services, and attack VMs running Kali Linux for solving CTF challenges. The deployment stack includes VMware vCenter for VM provisioning, Terraform for an automated VM creation from templates, and Ansible for software configuration and service setup, while pre-configured VM templates optimize the infrastructure provisioning time. The hardware setup consists of two HPE ProLiant DL380 Gen10 servers, each powered by two Intel Xeon Silver 4110 CPUs (16 cores, 32 threads) with 255.65 GB RAM and HDD storage.

Table 2 shows the recorded time required for fully deploying and configuring the entire CTF infrastructure.

Table 2. CTF infrastructure deployment time

Phase	Time per VM	Total time
Terraform VM provisioning (vCenter)	~1.5 min	~135 min (2 hours 15 min)
Ansible configuration & service setup	~3 min	~270 min (4 hours 30 min)
OpenVPN setup & validation	~2 min	~180 min (3 hours)
Total Deployment Time	~6.5 min	~7-8 hours

There are several observations regarding technical details. First, Terraform VM provisioning scales linearly, with small delays owing to the vCenter API. Second, Ansible configuration runs in parallel but it is limited by the CPU/RAM capacity. Third, network setup (the installation and configuration of the VPN server) requires a significant processing time across multiple VMs, especially the generation of the keys for the OpenVPN server and for each client profile.

Table 3 presents the error handling and recovery mechanism implemented during the infrastructure deployment process.

Table 3. Error handling and recovery

Failure Scenario	Detection Method	Recovery Mechanism
VM cloning failure (vCenter overload)	Terraform logs	Auto-retry (1 attempt)
Network misconfiguration (VPN issues)	Ansible validation	Re-run the affected playbooks
Storage bottleneck (delayed I/O)	Monitoring alerts	Staggered deployments

Considering the presented data, there are several optimization recommendations, especially regarding the upgrading of the hardware systems. To enhance deployment speed and reduce the performance bottlenecks for many deployed VMs, several improvement suggestions are proposed:

- switching from HDD to SSD/NVMe storage would cut down the provisioning time by ~50%;
- enhancing the Ansible parallel execution (the number of forks is 20), will reduce the configuration time, but it also requires a careful CPU load balancing;
- using multiple vCenter resource pools – leads to spreading the VM provisioning loads across both servers.

Another important improvement may be obtained by pre-configuring VPN services in VM templates, which may reduce VPN setup time by ~40%. Nevertheless, it is imperative to prioritize access security, as the pre-generation of keys in the VM template results in the duplication of the cryptographic keys, which results in utilizing the same keys for multiple servers and clients.

6. Results

Following the previously presented methodology, the Cyber Range prototype was developed and configured for planning and running a CTF exercise. This section provides information about the analysed challenges, including brief descriptions and statistics for many categories of participants and rankings (individual exercise, teams exercise, statistics for each challenge etc.).

The exercise specifications were developed for a total of 42 unique users, organized in 13 different teams (3 teams with 4 members, and 10 teams with 3 members). The challenges covered the following categories: Network Red Team CTF, Reverse Engineering and Steganography. For the category entitled “Network Red Team CTF”, the exercise specifications provided the images of the target virtual machines (and containers) used by the orchestration module to deploy the necessary instances of target machines.

In case of an individual exercise, an isolated game subnet will be created for each player. If the exercise is performed in teams, each team will have its isolated game subnet, but the members of a team will have access to the same subnet (and by default to the same data and resources). The diagram shown in Figure 3 illustrates the topology of the ready-to-use exercise network infrastructure (the CTF playground network topology). It is organized into teams, each of them having a dedicated environment, with controlled access and specific services. The mission is structured as a CTF challenge that involves scanning and exploiting a network target (identified by its IP address) by using the previously analysed tools. All the necessary tools are installed on a Kali Linux virtual machine (one instance for each player). Both the target and the Kali Linux VM are configured in an isolated environment, which can be accessed via a VPN connection.

The network is connected to the Internet for global access. It can also be set for Intranet/local access when the players are present on site. The Demilitarized Zone (DMZ) hosts two main components. The former is a customized CTFd web platform used for managing competitions, registering teams, and submitting flags. The latter is the OpenVPN Gateway which manages the remote access to the exercise playground infrastructure.

The next level illustrated in Figure 3 is that of the infrastructure deployed for each team. Each team has its own segregated network, denoted by a subnet (e.g. 10.1.2.0/24 for Team 1). The general organization for each team includes three main components, as follows:

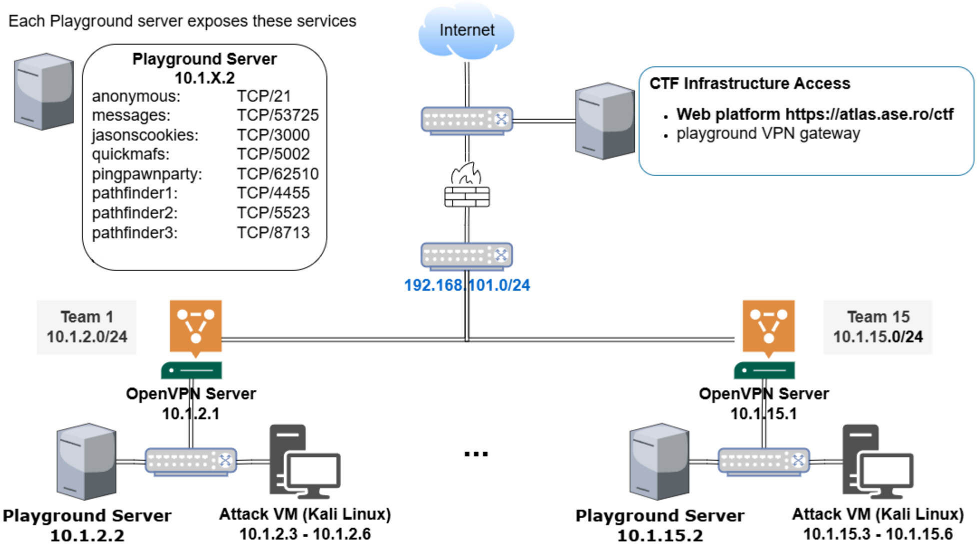

Figure 3. CTF exercise network topology

The first component is represented by an instance of the OpenVPN Server, each team having its own OpenVPN server with a subnet-specific IP address (e.g. 10.1.2.1 for Team 1), used for the team members' access to the playground network resources.

The second component is the playground server namely the exercise target server. On this server are running all the services associated with a certain scenario and it can be accessed via the team's subnet address (e.g. 10.1.2.2 for Team 1). In this exercise, all the challenges are predicated on exploiting the exposed services' vulnerabilities or misconfigurations.

The third component is represented by the attack virtual machines (Kali Linux). Each team has four dedicated Kali Linux virtual machines for launching attacks to the target playground server (e.g. 10.1.2.3 to 10.1.2.6 for Team 1).

Regarding the connections between networks, the teams' subnets are isolated from one another, and communication between them is restricted. The main firewall regulates traffic and separates the DMZ from the teams' internal network, also providing network traffic routing only to specific subnets. Each player received an OpenVPN profile (.ovpn file) required for accessing the game subnet.

The final ranking was determined by using the provided flags from the CTFd platform. To guarantee that there were no teams sharing the acquired flags, the playground server logs were analysed to confirm that each team completed the entire target exploitation and flag collection process.

In the end, all registered data is available for analysis and statistics. Statistics on the time until a challenge was solved, together with the number of teams/players who submitted the right flag for a certain task can show the difficulty level of the respective challenge. Figure 4 illustrates the number of flag submission attempts (success or failure). Another relevant statistic is represented by the percentage of correct submissions (successful attempts) for each challenge. These results prove that the proposed infrastructure achieved its aim, by providing a reliable environment for cyber exercises.

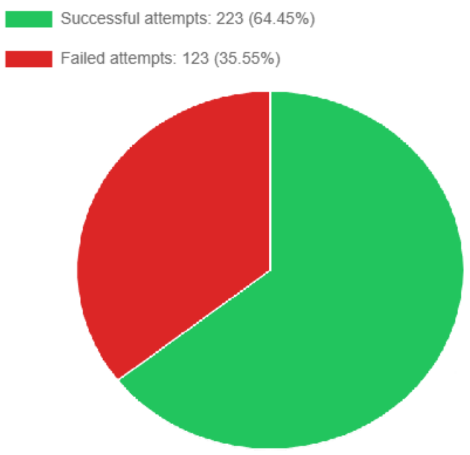

Figure 4. Successful attempts and failed attempts

7. Discussion

Table 4 compares the cyber range types already presented in the current paper – including the proposed model. It groups the main criteria employed in order to distinguish between the analysed models in several categories, including purpose, deployment model, target audience, specialization, scalability, and notable findings. This comparison is intended to present how different cyber range architectures and implementations meet specific training, testing, and operational needs in sectors such as education, industry, government, and cloud infrastructure.

The comparison indicates that cyber ranges differ greatly in terms of design and use, each of them being adapted to the specific requirements of its target customers. General-purpose and container-based cyber ranges provide adaptable, scalable environments for varied industries. Educational cyber ranges aim at low-cost, easily accessible configurations for academic teaching, whereas sector-specific ranges focus on compliance and privacy-critical industries such as finance and healthcare. Cloud-based and security automation cyber ranges support dynamic, remote training environments, allowing for a rapid scenario deployment and integration with enterprise

Table 4. Comparison of the proposed platform with other platforms

Cyber Range Type	Purpose	Deployment Model	Target Users	Specialization	Scalability	Notable Insights	Source
Cyber Range Revolution (General)	General cybersecurity training & testing	Cloud-based	Public & private sector	Broad threat simulation & orchestration	High	Emphasizes adaptable frameworks in order to suit different training needs	Ong et al. (2023)
Industrial Control Cyber Range	Securing industrial systems (ICS/SCADA)	Hardware-in-the-loop or virtual	Engineers, OT/IT staff	ICS protocols, real-time constraints	Medium	The realistic emulation of industrial environments is critical	Low et al. (2022)
Security Automation Cyber Range	SOC analyst training & red/blue teaming	Virtualized/cloud-based	Security professionals	Automation, incident response	High	Focuses on tool integration (e.g. SIEM, SOAR) and threat detection	Acheampong et al. (2022)
Cloud-based Disaster Recovery Cyber Range	Cloud resilience & disaster recovery	Cloud-native (AWS, Azure)	IT managers, DevOps	Failover, backup testing	Very High	Highlights orchestration and remote scenario implementation	Thiyagarajan (2020)
Financial & Healthcare Sector Cyber Ranges	Compliance and sector-specific threats	Hybrid or private cloud	Sector specialists	HIPAA, PCI-DSS scenarios	Medium	Emphasizes privacy, data integrity, and regulatory compliance	Pathak (2024)
Educational Cyber Range	Cybersecurity education & student training	Open-source virtual environments	Students, academic staff	Pen-testing, forensics	Medium	Low-cost, rapid deployment, suitable for classrooms	Brunner et al. (2019)
National Cyber Range (Gov. & Defense)	National cyber defense & wargaming	High-security on-premise	Military, intelligence agencies	Nation-state attacks, malware, DDoS	Very High	Enables full-scale simulation of cyberwarfare	Yamin et al. (2020)
CyExec*	Developer security training (DevSecOps)	Containerized (Docker, Kubernetes)	Developers, security teams	Agile, modular exercises	High	Supports scalable, rapid deployments and testing	Nakata & Otsuka (2021)
USA National Cyber Range (NCR)	Strategic national-level cyber operations	Secure, federated infrastructure	DoD, federal agencies	Cyber-kinetic integration, protocol fuzzing	Very High	Integrates real-life and cybersecurity scenarios for a more realistic perspective	Park et al. (2022)
The proposed Cyber Range	Cybersecurity training / Academic hands-on support / CTF events	Virtualized / Private Cloud – Private hardware infrastructure	Students / Cybersecurity trainees	Cybersecurity training / CTF events	High	Full infrastructure control, privacy, customizable, high scalability	-

resources. Meanwhile, industrial control and national-level cyber ranges offer high-fidelity simulations needed for critical infrastructure security and national defense, but they frequently require large resources (Dumitrache et al., 2025). This diversity emphasizes the need of selecting the cyber ranges in accordance with a company`s goals, user needs, and operational circumstances.

8. Conclusions and Future Work

This paper analysed the design and deployment of a multi-technology infrastructure for advanced training and testing in cyber range systems. The use of technologies such as Ansible, Terraform, VMware, IDS, SIEM and others illustrates the ability to create realistic, scalable, and secure systems for simulated cybersecurity scenarios. Terraform for Infrastructure as Code (IaC) allows for a rapid and repeatable virtualized environment provisioning, while Ansible's configuration management capabilities make it easier to install and maintain software and security solutions across multiple platforms. Further on, VMware serves as the foundation for virtualization, allowing the implementation of separated network environments for a variety of training and testing scenarios. Intrusion Detection Systems (IDS) play an important role in monitoring network traffic for detecting signals of hostile activity, hence improving the defensive posture of simulation environments. Furthermore, the use of SIEM systems ensures a thorough log collection, correlation, and analysis, which makes it possible to have useful insights into security incidents and contributes to taking effective action. By utilizing these tools and technologies, cyber range environments can closely mirror real-world network situations, allowing trainees to practice and enhance their skills in a secure and controlled environment. The use of automated traffic generation and attack simulation tools make the training process more realistic and improve its effectiveness.

Future research and development in cyber range systems should focus on improving user/player profiling in order to better understand individual performance and learning patterns. Advanced analytics and machine learning algorithms can be used for evaluating user interactions, identifying strengths and weaknesses, and providing personalized skill improvement suggestions.

REFERENCES

Acheampong, R., Bălan, T., Popovici, D.-M. et al. (2022) Security Scenarios Automation and Deployment in Virtual Environment using Ansible. In: *2022 14th International Conference on Communications (COMM), 16-18 June 2022, Bucharest, Romania*. New York, USA, IEEE. pp. 1-7.

Brunner, R., Oh, S. K., Ramirez, J. et al. (2019) Design for an educational cyber range. In: *Proceedings of the 6th Annual Symposium on Hot Topics in the Science of Security*, *1-3 April 2019, Nashville, USA*. Maryland, USA, National Security Agency. https://doi.org/10.1145/3314058.3317727.

Dumitrache, M., Sacala, I. S., Rotuna, C. I., Gheorghita, A., Sandu, I., & Smada, D. (2025). Developing an Intelligent Security Monitoring Platform for Internet Domains. A Practical Implementation Approach. *Studies in Informatics and Control*, 34(1), 75-84. doi: 10.24846/v34i1y202506

Georgescu, A., Vevera, A. V. & Cîrnu, C. E. (2020) Cyber as a Transformative Element in the Critical Infrastructure Protection Framework. *Romanian Cyber Security Journal*. 2(1), 37-44.

GFCE (2025) *CybExer Technologies* https://cybilportal.org/actors/cybexer-technologies/# [Accessed 23rd February 2025].

Glas, M., Vielberth, M. & Pernul, G.. (2023) Train as you Fight: Evaluating Authentic Cybersecurity Training in Cyber Ranges. In: *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems*, *23 - 28 April 2023, Hamburg, Germany*. https://doi.org/10.1145/3544548.3581046.

Gustafsson, T. & Almroth, J. (2020) Cyber Range Automation Overview with a Case Study of CRATE. In: *Proceedings of the 25th Nordic Conference on Secure IT Systems, 23-24 November 2020, Virtual Event.* Berlin, Heidelberg, Germany, Springer-Verlag. pp. 192-209.

HashiCorp. (2025) *Automate Infrastructure on Any Cloud*. https://www.terraform.io [Accessed 28th February 2025].

Jelo, M. & Helebrandt, P. (2022) Gamification of cyber ranges in cybersecurity education. In: *2022 20th International Conference on Emerging eLearning Technologies and Applications (ICETA)*, *20-21*

October 2022, Stary Smokovec, Slovakia. New York, USA, IEEE. pp. 280-285.

Katsantonis, M. N., Manikas, A., Mavridis, I. et al. (2023) Cyber range design framework for cyber security education and training. *International Journal of Information Security*. 22(4), 1005-1027. doi:10.1007/s10207-023-00680-4.

Kokkonen, T., Paijanen, J. & Sipola, T. (2022) Multi-National Cyber Security Exercise, Case Flagship 2. In: *Proceedings of the 14th International Conference on Education Technology and Computers, 28-30 October 2022, Barcelona, Spain.* New York, USA, Association for Computing Machinery. pp. 292 - 298.

Linardos, V. (2021) *Development of a cyber range platform*. Master's thesis, University of Piraeus.

Low, X., Yang, D. & Yang, D. (2022) Design and Implementation of Industrial Control Cyber Range System. In: *2022 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), 14-16 October 2022, Suzhou, China*. New York, USA, IEEE. pp. 166-170.

Mills, A., White, J. & Legg, P. (2024) GoibhniUWE: A Lightweight and Modular Container-Based Cyber Range. *Journal of Cybersecurity and Privacy*. 4(3), 615-628. doi:10.3390/jcp4030029.

Mohd Ariffin, M. A., Darus, M. Y., Haron, H. et al. (2022) Deployment of Honeypot and SIEM Tools for Cyber Security Education Model In UITM. *International Journal of Emerging Technologies in Learning (iJET)*. 17(20), 149-172. doi: 10.3991/ijet.v17i20.32901.

Nakata, R. & Otsuka, A. (2021) CyExec*: A High-Performance Container-Based Cyber Range With Scenario Randomization. *IEEE Access*. 9, 109095-109114. https://doi.org/10.1109/ACCESS.2021.3101245.

Ong, T. C., Premkumar, B. & Guo, H. (2023) Cyber Range Revolution: Transforming the Future of Cybersecurity Training. In: *2023 IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)*, *11-13 December 2023, Singapore*. New York, USA, IEEE. https://doi.org/10.1109/SOLI60636.2023.10425741.

Park, M., Lee, H., Kim, Y. et al. (2022) Design and Implementation of Multi-Cyber Range for Cyber Training and Testing. *Applied Sciences*. 12(24), art. no. 12546. doi: 10.3390/app122412546.

Pathak, A. (2024) Automating Infrastructure Management: Benefits and Challenges of Ansible and Terraform Implementation Across Sectors. *International Journal of Scientific Research in Computer Science, Engineering and Information Technology*. 10(5), 381-394.

Red Hat, Inc. (2025) *Ansible (Version 2.15.0)*. https://www.redhat.com/en/ansible-collaborative?intcmp=7015Y000003t7aWQAQ [Accessed 28th February 2025]

Sharifi, A. Z., Vanijja, V., Pal, D. et al. (2021) CyberIoT: An Initial Conceptualization of a Web-based Cyber Range for IoT. In: *2021 International Conference on Computational Performance Evaluation (ComPE), 1-3 December 2021, Shillong, India.* New York, USA, IEEE. pp. 091-096.

Thiyagarajan, R. (2020) *Single and Multi-Cloud Disaster Recovery Management using Terraform and Ansible*. MSc Research Project, National College of Ireland.

Ukwandu, E., Farah, M. A. B., Hindy, H. et al. (2020) A Review of Cyber-Ranges and Test-Beds: Current and Future Trends. *Sensors*. 20(24), art. no. 7148. https://doi.org/10.3390/s20247148.

Virág, C., Čegan, J., Lieskovan, T. et al. (2021) The Current State of The Art and Future of European Cyber Range Ecosystem. In: *2021 IEEE International Conference on Cyber Security and Resilience (CSR)*, *26-28 July 2021*, *Rhodes, Greece*. New York, USA, IEEE. pp. 390-395.

Werner, K. (2021) *RangeForce Named Market Leader in Cybersecurity Training by Global InfoSec Awards.* https://www.rangeforce.com/news-center/press-releases/2021-market-leader-global-infosec-awards [Accessed 23rd February 2025].

Yamin, M. M., Katt, B. & Gkioulos, V. (2020) Cyber Ranges and Security Testbeds: Scenarios, Functions, Tools and Architecture. *Computers & Security*. 88, art. no. 101636. https://doi.org/10.1016/j.cose.2019.101636.

Yamin, M. M. & Katt, B. (2022) Use of cyber attack and defense agents in cyber ranges: A case study. *Computers & Security*. 122, art. no. 102892. https://doi.org/10.1016/j.cose.2022.102892.