information

Article

Securing the Network: A Red and Blue Cybersecurity Competition Case Study

Cristian Chindrus † and Constantin-Florin Caruntu *,†

Department of Automatic Control and Applied Informatics, "Gheorghe Asachi" Technical University of Iasi, 700050 Iasi, Romania; cristian.chindrus@student.tuiasi.ro

* Correspondence: caruntuc@ac.tuiasi.ro

† These authors contributed equally to this work.

Abstract: In today's dynamic and evolving digital landscape, safeguarding network infrastructure against cyber threats has become a paramount concern for organizations worldwide. This paper presents a novel and practical approach to enhancing cybersecurity readiness. The competition, designed as a simulated cyber battleground, involves a Red Team emulating attackers and a Blue Team defending against their orchestrated assaults. Over two days, multiple teams engage in strategic maneuvers to breach and fortify digital defenses. The core objective of this study is to assess the efficacy of the Red and Blue cybersecurity competition in fostering real-world incident response capabilities and honing the skills of cybersecurity practitioners. This paper delves into the competition's structural framework, including the intricate network architecture and the roles of the participating teams. This study gauges the competition's impact on enhancing teamwork and incident response strategies by analyzing participant performance data and outcomes. The findings underscore the significance of immersive training experiences in cultivating proactive cybersecurity mindsets. Participants not only showcase heightened proficiency in countering cyber threats but also develop a profound understanding of attacker methodologies. Furthermore, the competition fosters an environment of continuous learning and knowledge exchange, propelling participants toward heightened cyber resilience.

Keywords: cybersecurity; Red and Blue Team; collaborative training; cybersecuritycompetitions; incident response; attack scenarios

Citation: Chindrus, C.; Caruntu, C.-F. Securing the Network: A Red and Blue Cybersecurity Competition Case Study. *Information* **2023**, *14*, 587. https://doi.org/10.3390/info14110587

Academic Editors: Jose de Vasconcelos, Hugo Barbosa and Carla Cordeiro

Received: 29 September 2023
Revised: 24 October 2023
Accepted: 25 October 2023
Published: 26 October 2023

1. Introduction

In the contemporary digital era, characterized by an increasing reliance on interconnected technology, the safeguarding of network infrastructure against a rapidly evolving spectrum of cyber threats has emerged as a critical imperative. Cybersecurity, once a niche concern, has now become a central pillar in the operations of organizations across industries [1]. The growing sophistication of malicious actors, coupled with the increasing frequency and impact of cyber incidents, has underscored the urgency for organizations to fortify their cyber defenses and equip their workforce with advanced incident response capabilities.

As organizations face these challenges, innovative approaches to cybersecurity training have gained prominence. Traditional methods, though essential, often fall short in providing the real-world, dynamic scenarios necessary to prepare cybersecurity professionals for the intricacies of modern cyber threats. In response, cybersecurity competitions have emerged as a dynamic and immersive training methodology, offering a simulated battleground where defenders and attackers engage in strategic encounters [2].

Cybersecurity encompasses strategies and measures to safeguard digital systems and information from unauthorized access and cyber threats. This field has grown significantly in response to the rising challenges. Key tactics include firewalls, encryption, strong passwords, and threat detection. The authors of [3] outline the top five current cybersecurity

challenges and emphasize the importance of awareness in protecting digital environments from electronic threats. Artificial intelligence (AI) empowers cybersecurity by automating tasks, enhancing threat detection, and bolstering defenses. A systematic review of AI applications in cybersecurity can be found in [4]. It categorizes these AI use cases using a National Institute of Standards and Technology (NIST) cybersecurity framework, providing a comprehensive view of AI's potential to enhance security across various domains. Cybersecurity social networking is an evolving interdisciplinary field that tackles security issues within the realm of social networks. The research in [5] defines risk as the combination of consequences and the likelihood of occurrence, highlighting risk assessment as a critical task in the broader context of IT security. This approach encompasses physical, hardware, software, network, and human resources, integrating multiple protection levels and strategies.

This paper explores the field of cybersecurity competitions, focusing on the intriguing domain of Red and Blue Cybersecurity Competitions. Such competitions simulate adversarial scenarios, pitting Red teams, and emulating attackers, against Blue teams, tasked with defending critical digital assets. This study proposes a thorough examination of the competition's conception, design, execution, and the resulting outcomes. Through a combination of qualitative and quantitative analyses, this research endeavors to provide a holistic understanding of the competition's effectiveness in enhancing participants' defensive and offensive cybersecurity skills. Moreover, this study aspires to contribute to the broader field of cybersecurity education by extrapolating insights and lessons from the competition's structure and outcomes, potentially informing the development of more robust and impactful training paradigms in the realm of cyber defense and offense.

The authors in [6] present a comprehensive framework for competence development and assessment in hybrid cybersecurity exercises. With the rise of security threats, especially in cyber defense exercises (CDX), the framework targets the effective evaluation of diverse participant skills. It optimizes CDX to include all teams, even non-technical trainees, enhancing resource utilization and cybersecurity awareness. Covering formative assessment, team composition, objectives, and exercise flow, the framework enriches cybersecurity training methodologies. Developed through empirical research, it offers insights into diverse trainee-focused hybrid exercises. Yamin et al. [7] explore cybersecurity training by studying cyber ranges and security testbeds, emphasizing their essential role in counteracting cyber threats and crimes. It investigates two training forms: one enhancing security professionals' threat defense skills, and the other raising cybersecurity awareness among non-security professionals and the public. This study examines how specialized infrastructures like cyber ranges enable hands-on learning and scenario execution.

In [8], the authors present a holistic method for combined Red and Blue Team assessments, vital for evaluating network/system security and detecting vulnerabilities. These assessments encompass diverse operational, managerial, and technical tasks, emphasizing key principles. The paper introduces a dedicated Red and Blue Team methodology as a guide for effective security audits and penetration testing. This methodology enhances assessment robustness and cybersecurity readiness. Andreolini et al. [9] describe a novel framework for evaluating trainee performance in modern cybersecurity exercises. It includes a distributed monitoring architecture to capture trainee activity data, a directed graph-based algorithm for modeling actions, and novel scoring algorithms based on graph operations. These algorithms comprehensively assess trainee attributes like speed and precision, enabling precise progress measurement and error identification—overcoming limitations in common cyber ranges.

The primary objective of this study is to assess the efficacy of Red and Blue Cybersecurity Competitions in cultivating robust incident response capabilities and enhancing the overall cybersecurity readiness of participants. By delving into the competition's intricacies, examining participant performance data, and evaluating the impact on technical expertise and strategic thinking, this paper seeks to provide valuable insights into the potential of this innovative training paradigm.

In preceding studies, the core system [10] and system architecture [11] have been presented in individual cases. The outcomes elucidated in those analyses relate to the inaugural instance of the competition. However, in the current paper, we wish to outline the following:

- A comprehensive overview of all elements within each subsystem, providing a holistic view of the competition.
- A comparative analysis based on two editions of the competition.
- In comparison with [12], the findings highlight the continuous improvement in participants' skills and capabilities when addressing real-world incidents and challenges.
- This assessment underscores the competition's effectiveness as a practical learning platform that closely mirrors real-world scenarios and not just a presentation of cybersecurity impact as in [13].

In the following sections, we will delve into the methodology, structure, and outcomes of the Red and Blue Cybersecurity Competition. By exploring the nuances of this immersive training approach, we aim to shed light on its transformative potential in equipping cybersecurity professionals to navigate the complex and ever-evolving landscape of cyber threats.

2. Importance of Competition in Cybersecurity Training

With the evolution of cybersecurity, the concept of competition has garnered substantial recognition as an essential driver for fostering effective training methodologies. This section embarks on a comprehensive exploration of the profound significance that competition holds within the domain of cybersecurity training. By delving into its multifaceted dimensions and discerning the extensive benefits it imparts, we gain insights into how competition propels training strategies to new heights of efficacy.

Competition, when exploited within the context of cybersecurity training, assumes a multifaceted role that extends beyond its conventional connotations. At its core, competition offers an immersive and dynamic environment where individuals and teams engage in strategic maneuvers and tactical confrontations [14]. This interactive setting not only mirrors real-world scenarios but also serves as an incubator for the cultivation of essential skills and attributes.

A primary dimension of competition in cybersecurity training lies in its ability to instill a heightened sense of urgency and resourcefulness. Participants are compelled to navigate intricate challenges and adversaries, often under stringent time constraints. This pressured environment stimulates quick thinking, decision-making agility, and the ability to adapt swiftly to unforeseen circumstances—all indispensable qualities in the cybersecurity landscape, where rapid responses to emerging threats are paramount.

Moreover, competition acts for the refinement of communication, collaboration, and teamwork—attributes that are pivotal in effective cybersecurity operations. As participants engage in tactical endeavors, the interplay of diverse skill sets and perspectives fosters a dynamic exchange of ideas and strategies. This collaborative ethos mirrors the real-world synergy required among cybersecurity professionals to combat multifaceted threats [15].

Beyond its experiential advantages, competition also significantly contributes to the psychological and emotional aspects of cybersecurity training. The inherent drive to excel and outperform peers fuels a culture of continuous improvement and self-motivation. Participants cultivate a resilient mindset, where the pursuit of excellence becomes a cornerstone of their professional ethos.

2.1. The Role of Competition in Cybersecurity

Competition, a formidable force in the realm of cybersecurity training, has the power to inject dynamism and intensity into the learning process. Within this context, competition constructs an immersive arena where participants are not merely passive learners but active contenders. This environment propels individuals to harness their accumulated knowledge,

technical skills, and strategic insight to overcome their opponents, effectively simulating the real-world combat between defenders and threat actors.

At its core, the essence of competition lies in its capacity to stimulate multifaceted cognitive responses. Participants are galvanized by the inherent challenge to prove their worth, fostering a state of heightened engagement and awareness. The spirit of competition serves as a forge that sparks critical thinking, innovative problem-solving, and the cultivation of an agile mindset—qualities inherently demanded by the intricate and ever-evolving cybersecurity landscape [16].

Furthermore, competition introduces an element of urgency that mirrors the time-sensitive nature of cybersecurity incidents. In this pressured environment, participants are compelled to make swift, yet calculated decisions. This experiential facet not only augments the participants' technical proficiency but also nurtures their capacity to analyze complex scenarios under time constraints—an indispensable attribute in the face of emergent cyber threats.

In essence, competition transcends the boundaries of a conventional learning paradigm, encapsulating the true spirit of cybersecurity. By creating an environment that mirrors the high-stakes struggle between defenders and adversaries, competition not only imparts technical skills but also forges a resilient and adaptable mindset. As we delve further into this paper, we unravel the various dimensions through which competition intertwines with cybersecurity training, underscoring its role as a transformative force in preparing cybersecurity professionals for the complex challenges that lie ahead.

2.2. Advantages of Competition in Cybersecurity Training

The integration of competition into the cybersecurity training presents a number of advantages that significantly augment the efficacy of the learning experience. Foremost, this approach transcends theoretical comprehension, immersing participants into authentic scenarios that mirror the intricacies of real-world cyber challenges. The act of decision-making takes on tangible consequences, compelling individuals to navigate the intricate maze of cybersecurity with a practical perspective [17]. The pressure inherent in competitive environments acts as a furnace, shaping the development of resilience and composed responses—attributes indispensable for skillful incident management.

Beyond its immersive qualities, competition lays the foundation for a culture of perpetual enhancement. The competitive ethos serves as a powerful motivator, propelling participants to remain attuned to the ever-evolving threat landscape and on top of innovative defensive stratagems. Incentivized by the drive to secure victory, participants are inherently inclined toward dynamic learning, wherein knowledge is not static but constantly refined in response to emerging challenges.

Furthermore, the collaborative fabric intrinsic to competitive frameworks encourages a rich exchange of insights. The pooling of diverse expertise becomes a hallmark of competition, as participants collaboratively decipher complex dilemmas. This knowledge-sharing paradigm not only accelerates problem-solving but also cultivates a collective intelligence that thrives on mutual support and the synergy of minds.

2.3. Examples of Competitions

These exercises emulate real-world attack scenarios, pitting offensive "Red Teams" against defensive "Blue Teams". The Red Teams employ sophisticated tactics to infiltrate systems, while the Blue Teams adeptly counteract these assaults. Such competitions underscore the importance of effective teamwork, strategic thinking, and rapid decision-making in cybersecurity defense. Examples of competitions are Locked Shields and DEFCON, which are described in what follows.

The "Locked Shields" exercise stands as a seminal Red Team (RT) versus Blue Team (BT) cybersecurity exercise, uniting member nations and partners of the Cooperative Cyber Defence Center of Excellence (CCDCOE) [18]. This training paradigm converges

the collective expertise of diverse entities to navigate the intricate labyrinth of modern cyber warfare.

Within the exercise's conceptual framework, the stage is set on a fictional island nation, Berylia, located in the northern reaches of the Atlantic Ocean. Berylia grapples with a burgeoning security crisis, emblematic of contemporary cyberattacks, as orchestrated attacks target both military and civilian IT systems. This wave of cyber attacks is creating a cascading domino effect, disrupting the very fabric of Berylian governance, military operations, communication networks, water treatment facilities, and the electricity grid. Unraveling in the wake of this turmoil is a palpable surge of public unrest and protests, underscoring the tangible ramifications of cyber chaos [19].

In an innovative stride, the exercise's domain encompasses the emulation of a central bank's reserve management and financial messaging systems, marking an unprecedented inclusion. Furthermore, the integration of a 5G standalone mobile communication platform underscores a visionary facet of critical infrastructure. This strategic maneuver serves a dual purpose—it imparts cyber defenders with firsthand experience in grappling with nascent technological shifts while presenting an opportune testing ground for safeguarding forthcoming advancements.

Capture the flag (CTF) competitions constitute a cornerstone of the cybersecurity training paradigm, designed to scrutinize participants' technical prowess through a series of intellectually demanding phases [20]. Regrettably, despite a predominantly tech-savvy audience, these CTF events often fail to captivate, akin to observing diligent students tackling complex homework assignments. The unhurried cadence of these competitions, spanning entire days or even multiple days, further adds to the challenge of sustaining audience engagement [21].

In emblematic instances like DEFCON, the unfolding of competition progress is relayed to the audience in a rudimentary spreadsheet format, succinctly encapsulating each team's journey in safeguarding their networks or probing vulnerabilities [22]. Yet, beneath this seemingly mundane surface, the CTF competition conceals moments of technical ingenuity, punctuated by consequential tactical choices and intricate adversarial maneuvers. These turning points have the power to decide the winner, unraveling the intricate web of how, why, and where success was forged.

3. Red and Blue Team Training

In the rapidly evolving landscape of contemporary cybersecurity, the concept of Red and Blue Team Training has emerged as a strategic imperative in bolstering digital defenses. This section presents a comprehensive investigation into the world of Red and Blue Team Training, delving deeply into its foundational elements, operational distinctions, methodologies, and the substantial benefits it confers in elevating organizational cybersecurity readiness [23].

Red and Blue Team Training represents a dynamic paradigm in cybersecurity education and preparation. Rooted in a simulation-based approach, it mirrors real-world cyber conflict scenarios by pitting offensive "Red Teams" against defensive "Blue Teams". The Red Teams, akin to adversarial entities, orchestrate sophisticated attacks to exploit vulnerabilities, while the Blue Teams ardently safeguard digital assets by detecting, countering, and neutralizing the incursions.

This immersive training methodology transcends theoretical instruction, offering a hands-on platform where participants engage in a high-stakes, adversarial competition. Beyond technical acumen, it nurtures strategic thinking, adaptive problem-solving, and real-time decision-making in the face of dynamic threats.

In the evolving landscape of modern cybersecurity, the paradigm of Red and Blue Team Training stands as a formidable entity, and strengthens the fortifications of digital defenses. This section undertakes an extensive exploration into the far-reaching influence of Red and Blue Team Training, unraveling the complexity of its operational dynamics and showing the key factors that underpin its effectiveness [24].

At its core, Red and Blue Team Training embodies a holistic approach to cybersecurity preparedness. The Red Team, embodying the role of the aggressor, employs an arsenal of tactics mirroring real-world threat actors to infiltrate an organization's digital ecosystem. Counterbalancing this, the Blue Team emerges as the guardian, orchestrating a vigilant defense to counter and neutralize the simulated attacks launched by their adversarial counterpart [23].

Within the complex field of cybersecurity education, the adoption of Red and Blue Team Training stands as a potent avenue for nurturing skilled defenders and adept adversaries. However, this section pivots toward the multifaceted challenges that frequently impact the trajectory of effective training. It further delves into pioneering strategies devised to transcend these impediments, while concurrently scrutinizing methodologies geared toward a comprehensive evaluation of the genuine efficacy of Red and Blue Team Training initiatives [1].

Moreover, Red and Blue Team Training promotes collaboration and synergy among cybersecurity practitioners. The interplay between Red and Blue Teams cultivates a holistic understanding of attack vectors, enabling defenders to proactively fortify their defenses.

3.1. Definition of Red and Blue Teams

In the intricate struggle of cybersecurity, Red and Blue Teams emerge as the embodiment of adversaries and defenders [24]. The Red Team embodies the attacker's persona, utilizing an array of offensive tactics to breach an organization's digital fortifications. In stark contrast, the Blue Team embodies the role of guardians, orchestrating countermeasures to repel and mitigate the simulated assaults orchestrated by the Red Team [25]. This dynamic exchange sets the stage for a controlled arena fostering skill refinement, incident response augmentation, and the revelation of security weak points.

The Red Team's role as aggressors entails the execution of multifaceted attack vectors, mirroring the techniques used by actual threat actors. Their endeavors span from exploiting software vulnerabilities to social engineering, painting a vivid picture of the diverse threat landscape. In parallel, the Blue Team's tenacity is demonstrated through proactive threat detection, rapid incident containment, and the fortification of digital perimeters [26].

The synergy between these teams materializes in the form of invaluable learning opportunities. The adversarial context enables cybersecurity professionals to fine-tune their defensive strategies while evolving to predict and thwart emergent attack patterns. The combination of Red and Blue Teams, underpinned by robust training methodologies, culminates in a virtuous cycle of skill growth and organizational resilience.

In the realm of cybersecurity, a dilemma occurs, defining the distinct tactical trajectories of Red and Blue Teams. These two entities, while unified in the pursuit of bolstering digital security, adopt roles as starkly opposed as they are complementary [13]. The Red Team assumes the mantle of the adversary, venturing into the digital domain with the aim of probing, exploiting, and laying bare vulnerabilities that may otherwise remain concealed. In stark contrast, the Blue Team ascends as the vigilant guardian, entrusted with the pivotal responsibility of identifying, mitigating, and orchestrating countermeasures against the simulated threats propagated by the Red Team [26].

3.2. How Red and Blue Team Training Works

At the forefront of contemporary cybersecurity, the paradigm of Red and Blue Team Training unfolds as a carefully constructed arena, emulating the tumultuous landscapes of actual cyber attack scenarios. In this dynamic enactment, the Red Team, analogous to a framework of virtual attackers, mobilizes an array of intricate hacking techniques. Their objective resonates with that of genuine threat actors—to infiltrate and compromise an organization's digital infrastructure [27].

In a synchronous battle of defense and offense, the Blue Team stands resolute, assuming the mantle of sentinels charged with the safeguarding of the organization's digital domain. Their endeavor encompasses not only the detection of the Red Team's intricate

maneuvers but also the analytical prowess to discern the motives and methodologies that underpin these attacks. Through swift and strategic action, the Blue Team endeavors to thwart the Red Team's advances, neutralizing their impact and fortifying the organization's cyber defenses.

This realm of simulation serves as an priceless pool, forging the skills and resilience of cybersecurity practitioners. The immersive experience granted by Red and Blue Team Training offers a veritable playground for participants to hone their capacities in responding adeptly to the ever-evolving spectrum of cyber threats. By navigating this virtual battlefield, participants cultivate a refined skill set, augmented by practical insights and strategic dexterity [13]. Thus, the synergy between simulated scenarios and real-world challenges engenders a robust cadre of cybersecurity professionals adept in countering the countless permutations of digital intrusion.

3.3. How Red and Blue Team Training Improves Cybersecurity Posture

In dissecting the mechanics of Red and Blue Team Training, emphasis is placed on the pivotal role of experiential learning. Participants are immersed in realistic scenarios, transcending theoretical realms to navigate authentic decision-making processes with real-world implications. This hands-on engagement cultivates resilience and composure, attributes paramount to effective incident response.

In the relentless search of cybersecurity excellence, Red and Blue Team Training emerges as a pivotal pillar. Central to this methodology is a simulated real-world scenario, wherein participants immerse themselves in the intricate dance of adversaries. The Red Team, assuming the role of aggressors, employs sophisticated tactics to breach systems, while the Blue Team, the trusted defenders, adeptly counters these incursions. This dynamic synergy fosters a comprehensive skill set encompassing proactive threat detection, rapid incident response, and strategic vulnerability mitigation [28].

The impact of Red and Blue Team Training resonates across the multidimensional landscape of cybersecurity readiness. By submerging participants in authentic adversarial contexts, the training nurtures an acute grasp of attack vectors, vulnerabilities, and defensive strategies. This experiential mode of learning empowers participants to discern nuanced signs of compromise, facilitating swift and precise countermeasures.

Moreover, Red and Blue Team Training forges enduring resilience and adaptability in cybersecurity practitioners. The competitive and ever-evolving exercises refine the participants' ability to navigate fluid threats, giving them the agility to counter complicated attacks. The collaborative spirit of this training fosters teamwork and efficient communication across diverse skill sets, underscoring the paramount importance of a united defensive front. As this exploration unfolds, subsequent sections delve deeper, unraveling the strategic intricacies of Red and Blue Team Training's orchestration in enhancing cybersecurity prowess.

3.4. Best Practices for Implementing Red and Blue Team Training

The implementation of Red and Blue Team Training necessitates a deliberate and strategic approach to amplify its transformative influence. To ensure its efficacy, a set of best practices takes center stage [8]:

- **Targeted Skill Development:** Tailoring training objectives to the unique needs and proficiency levels of participants emerges as a cornerstone. This customization not only optimizes skill augmentation but also harmonizes training outcomes with organizational cybersecurity aspirations.
- **Realistic Scenario Design:** The crafting of scenarios mirroring real-world challenges assumes paramount importance. This entails encompassing a spectrum of attack vectors, system configurations, and industry-relevant scenarios. Such fidelity to realism lays the foundation for cultivating practical and nuanced problem-solving skills.
- **Continuous Learning Cycle:** Embracing a cyclical training model that champions iterative learning constitutes an essential element. Post-exercise assessments and

structured debriefings serve as conduits for perpetuating knowledge retention and gradual enhancement over time.

- **Interdisciplinary Collaboration:** The promotion of cross-functional collaboration between Red and Blue Teams emerges as a cornerstone. This interplay mirrors the symbiosis requisite for effective cybersecurity defense. By embracing diverse perspectives, participants are fortified with a holistic outlook, nurturing multifaceted cybersecurity strategies.
- **Feedback and Evaluation:** The regular assessment of participant performance accompanied by robust feedback mechanisms assumes pivotal importance. This iterative feedback loop not only informs the fine-tuning of training methodologies but also underpins the continuous evolution of training outcomes.

3.5. Common Challenges Faced during Red and Blue Team Training

While Red and Blue Team Training offers transformative benefits in cybersecurity education as detailed in the previous section, it is imperative to acknowledge and address the potential hurdles that can hinder its optimal execution. This section undertakes a comprehensive analysis of these challenges, encompassing a spectrum of technical intricacies to logistical considerations, each warranting meticulous contemplation [29]:

1. *Resource Limitations:* The successful implementation of Red and Blue Team Training hinges on the availability of essential resources, including time, personnel, and appropriate technology. Acquiring and configuring requisite tools, establishing suitable training environments, and securing proficient trainers can present substantial obstacles.
2. *Realism and Relevance:* A cornerstone of effective training lies in crafting scenarios that authentically emulate contemporary cyber threats. Achieving the delicate equilibrium between realistic simulations and predefined training objectives is paramount to ensure that the acquired skills translate into practical proficiency.
3. *Team Dynamics and Communication:* The collaborative dynamic between Red and Blue Teams hinges upon uninterrupted communication and synchronized strategic maneuvers. Overcoming potential barriers in communication, fostering a harmonious team environment, and aligning tactical approaches require dedicated efforts.
4. *Skill Diversity:* Participants engaged in Red and Blue Team Training invariably possess diverse levels of technical insight and domain expertise. Tailoring training protocols to accommodate this spectrum of skill sets while upholding meaningful engagement and skill enhancement poses a multifaceted challenge.

3.6. Strategies for Overcoming These Challenges

In response to the multifaceted challenges inherent in Red and Blue Team Training, a strategic toolkit of innovative approaches emerges as an imperative. These solutions are designed to transcend obstacles, fostering an environment that leads to optimal training outcomes and cybersecurity readiness [30]:

1. *Adoption of Simulation Technology:* Embracing cutting-edge simulation technologies serves as a potent remedy for resource constraints. These platforms offer a cost-effective and scalable avenue to replicate intricate cyber scenarios, mitigating challenges posed by limited resources and facilitating immersive experiential learning.
2. *Customized Scenario Development:* Tailoring training scenarios to mirror an organization's unique cybersecurity landscape elevates training relevance and participant engagement. By mirroring real-world vulnerabilities and incidents, participants hone skills that directly translate into bolstered defense mechanisms.
3. *Communication Enhancement Workshops:* Integrating specialized communication workshops into training regimens can enhance interpersonal skills, facilitating seamless information exchange and collaboration between Red and Blue Teams. Effective communication is pivotal to coordinated defense maneuvers.
4. *Adoption of Progressive Learning Pathways:* Implementing a tiered training framework accommodates participants with divergent skill levels. This modular approach en-

sures inclusivity, allowing novices and experts alike to engage at their proficiency level, fostering a culture of continuous learning and skill enhancement.

In the journey to optimize the effectiveness of Red and Blue Team Training, proactively addressing challenges and devising adaptable strategies assume a pivotal role. By confronting these challenges head-on and delineating effective strategies and assessment methodologies, this paper takes significant strides in advancing our understanding of the intricate dynamics that encompass cybersecurity training. Moreover, it underscores the compelling need for a perpetually evolving paradigm in response to the ever-changing landscape of cybersecurity, ensuring the training remains at the forefront of educational excellence.

4. Red and Blue Competition for Cybersecurity Training—Case Study

Through the paradigm of a Red Team and Blue Team cybersecurity simulation, the Red Team assumes the role of an ethical hacker, strategically endeavoring to exploit vulnerabilities that have been identified by the Blue Team. This simulation embodies the concept of penetration testing, a process that involves replicating the techniques and methodologies employed by real-world attackers. This pragmatic approach signifies a departure from relying solely on theoretical capabilities and security equipment, instead anchoring the company's defense mechanisms in their actual performance when confronted with genuine threats.

The essence of red teaming lies in its capacity to provide an authentic assessment of an organization's cybersecurity incident response capabilities. By simulating genuine attack scenarios, red teaming serves as a test for an organization's preparedness to counter sophisticated cyber threats. In direct contrast, the Blue Team undertakes the role of network defenders within this simulation. Their pivotal role involves identifying and rectifying vulnerabilities, effectively learning which aspects within the organizational framework require attention and improvement. Furthermore, their engagement enhances their ability to swiftly respond to and mitigate potential breaches.

While prevention is widely acknowledged as a cornerstone of cybersecurity, this simulation underscores the equal significance of detection and remediation. These three facets together fortify an organization's overall defense capability. By fusing the proactive measures of the Blue Team with the probing initiatives of the Red Team, this simulation cultivates a holistic approach to cybersecurity that not only safeguards against potential attacks but also bolsters the organization's capacity to effectively counteract them.

4.1. The Architecture of Red and Blue Competition

The network architecture designed for such a scenario initially appears simplistic, as illustrated in the diagram below (Figure 1). It necessitates the deployment of a router, a core system, and a series of subnets, corresponding in number to the participating teams. These subnets are intended to house vulnerable systems that demand protection through the identification and resolution of security issues. Moreover, these virtual machines (VMs) are employed to launch attacks on opposing teams, aimed at flag identification. In our specific instance, there exist six VMs, each endowed with distinct vulnerabilities.

A notable challenge posed by this architecture pertains to the multitude of rules imperative for the configuration of the router. The initial set of regulations seeks to proscribe direct entry to the VMs owned by rival teams. Access to these systems is exclusively sanctioned within the boundaries of the originating team's designated subnet. With the competition segmented into three distinct phases, each phase presenting two available VMs, new sets of rules are needed. These subsequent regulations function to constrain and obstruct access to the VMs during each competition phase.

In every stage of the competition, a grace period is afforded, granting teams the opportunity to familiarize themselves with their assigned systems. However, during this interval, access to the adversarial teams' VMs is prohibited. Subsequently, another set of three rules is implemented, governing the interaction between any two teams for each given time period.

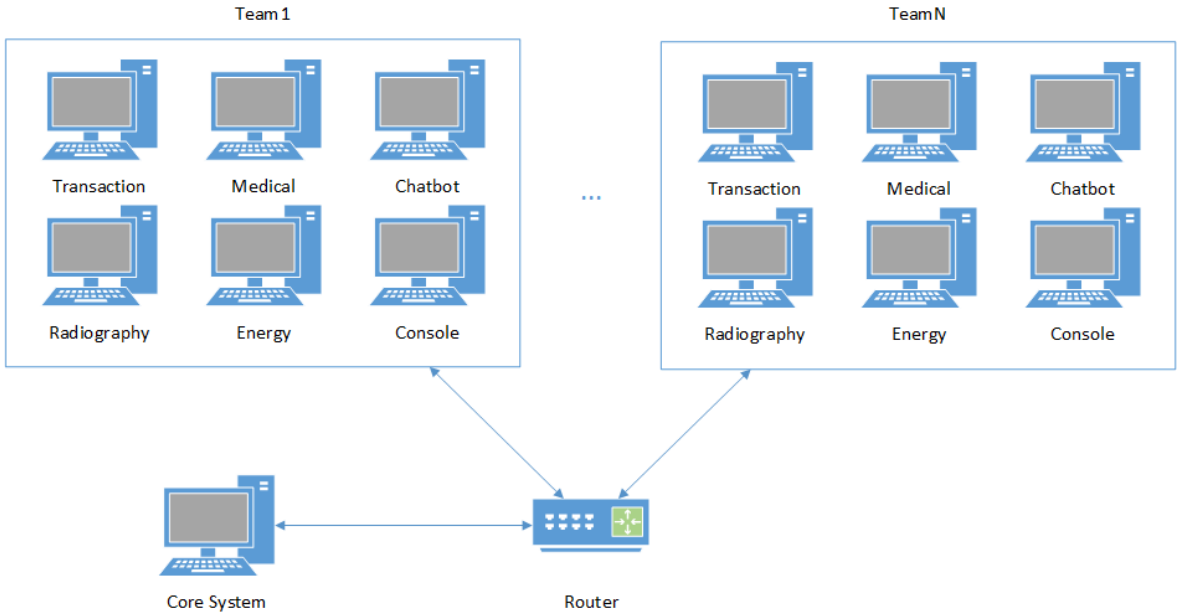

Figure 1. Network's architecture.

A selection of six VMs was chosen to cover a wide range of vulnerabilities and facilitate broad participation in this competition. It was determined that effectively addressing the tasks required between two and four participants for each of the two VMs. Additionally, the infrastructure of the cyber range dictated that there should be between 20 and 25 participating teams, introducing a new constraint regarding the number of vulnerable VMs. To resolve as many vulnerabilities identified by the Blue Team as possible and enable the Red Team to automate attacks, it was decided to progressively unlock challenges over the course of the competition's three phases.

An additional stipulation imposed for the fair conduct of the competition mandates that teams exclusively access the VM corresponding to their assigned mission. For example, a team associated with VM1 can only exploit vulnerabilities intrinsic to VM1, which is linked to the opposing team's objectives. This requirement translates into the establishment of six rules, corresponding to the number of missions, for every connection between two teams.

Virtual machines are configured and deployed through the utilization of Ansible scripts, which offer the flexibility to delineate essential hardware prerequisites and other pertinent parameters. It is advised that VMs adhere to the recommended hardware specifications encompassing two central processing units (CPUs), four gigabytes of random access memory (RAM), and a 40-gigabyte hard disk capacity. Conversely, the core system necessitates a more robust hardware configuration, mandating a minimum of 16 CPUs, 64 gigabytes of RAM, and a hard disk capacity of 100 gigabytes. Notably, the implementation of this framework does not entail the need for specialized hardware equipment. The only requisites involve the employment of servers that align with the stipulated hardware prerequisites, ensuring an optimal and seamless execution of the system.

To further challenge the detection capabilities of both the opposing teams and the core system, a mechanism is implemented whereby all traffic visible within a team's designated subnet emanates from a singular IP address. This IP address corresponds to the default gateway aligned with each network segment. The obscuring of IPs across subnets is realized through the execution of network address translation (NAT) for each source IP.

The culmination of these regulations entails an intricate web of rules, necessitating multiplication to accommodate the number of participating teams. This multiplication concludes in a substantial volume of rules, an extensive collection that mandates real-time management during the competition's runtime.

4.2. Vulnerabilities Description

The cybersecurity competition features a collection of six distinct virtual machines, each engineered to incorporate a diverse range of vulnerabilities. These vulnerabilities have been intentionally incorporated to rigorously evaluate the incident response proficiency of the participating individuals. Throughout the competition's progression, a strategic approach was adopted, revealing sets of two virtual machines during each sequential phase. This methodical revealing of VMs ensured a controlled and incremental escalation of challenge complexity, allowing participants to gradually adapt to evolving scenarios. The distribution of vulnerabilities across these virtual machines enabled the evaluation of participants' adeptness in identifying and mitigating a spectrum of cyber threats. This systematic structure facilitated a comprehensive assessment of the contestants' capabilities, contributing to an enhanced understanding of their preparedness in the dynamic realm of cybersecurity.

4.2.1. First Phase

In the first phase, participants were provided with a set of VMs characterized by a low level of complexity. This strategic approach aimed at facilitating the accommodation of participants to the unique competition format. By providing VMs with relatively manageable challenges, participants were given the opportunity to familiarize themselves with the new competition framework.

The initial virtual machine, referred to as "Transaction", functions to replicate transactional processes within multiple blockchain wallets. This simulation deliberately incorporates a series of vulnerabilities inspired by the intricacies of cryptocurrency wallet operations. Notably, this virtual machine presents a spectrum of at least five distinct methods for exploitation, encompassing a susceptible API and a collection of misconfigurations inherent in the application's developmental phase.

Subsequently, the second virtual machine, denominated as "Medical", emulates the online platform of a medical clinic. Termed "Medical", this virtual environment introduces an array of vulnerabilities, encompassing local file inclusion (LFI), remote code execution (RCE), SQL injection, and JSON web token (JWT) attacks. Additionally, the presence of diverse authentication token issues adds complexity to this virtual realm, effectively challenging participants' capacities for effective incident response.

This comprehensive scenario serves as a rigorous testing ground, probing participants' adeptness in identifying and mitigating intricate cybersecurity threats. The virtual machines, Transaction and Medical, mirror real-world situations, thereby furnishing participants with an opportunity to hone their technical skills, tactical decision-making, and their ability to navigate multifaceted security vulnerabilities. Such experiential learning not only enhances participants' cybersecurity readiness but also reinforces their understanding of the evolving threat landscape.

4.2.2. Second Phase

In the context of the second phase, the augmentation of the scenario involved the preparation of two additional virtual machines to further challenge participants' cybersecurity prowess.

The first of these virtual machines, called "Chatbot", emulates a functional chat service, as suggested by its nomenclature. The VM was meticulously designed with a curated set of predefined questions, accompanied by a series of code development intricacies deliberately introduced into its framework. Within this construct, three pivotal vulnerabilities were strategically embedded: SQL Injection, Command Injection, and Directory Traversal. The successful exploitation of these vulnerabilities demanded the acquisition of unauthorized access to a specific user account, thereby facilitating the retrieval of decryption keys and consequently granting access to concealed information of utmost importance.

Concurrently, the second supplementary virtual machine, emblematic of an X-ray clinic's web page, emerged as a complex challenge. This virtual environment catered

to functions such as appointment scheduling and provision of analysis data. Within its construct, two distinct web vulnerabilities, namely XML External Entity (XXE) and Local File Inclusion, were meticulously incorporated. The LFI vulnerability enabled the manipulation of appointment-related files without undergoing stringent validation, consequently allowing unauthorized access to the database directly through the browser. Furthermore, an inadvertent active FTP server and a designated port-operating server were discovered within this virtual machine, unintentionally expanding its attack surface. This port served as a conduit through which physicians could access their schedules, thus inadvertently introducing an additional layer of vulnerability.

This augmentation in the scenario not only fostered an intensified testing ground for participants but also served as a comprehensive exercise in identifying, exploiting, and mitigating multifaceted vulnerabilities. This experiential learning platform, characterized by intricately engineered virtual machines, served to enhance participants' tactical skills, strategic decision-making, and overall preparedness in the realm of cybersecurity.

4.2.3. Third Phase

In the final phase of the competition, the landscape evolved to encompass a distinct industrial focus, where two virtual machines were introduced to emulate intricate scenarios reflective of the industrial sector's cybersecurity challenges.

The first of these VMs, aptly named "Energy", entailed the simulation of a Supervisory Control and Data Acquisition (SCADA) communication protocol governing interactions among multiple power stations. Each individual VM in this configuration held four distinct pieces of information pertaining to the respective power station. Crucially, one specific piece of data, concerning nuclear fuel—a critical and sensitive component—was intended to remain strictly inaccessible. However, vulnerabilities stemming from the developmental intricacies of the specialized protocol introduced misconfigurations, thereby potentially exposing confidential nuclear fuel data. Notably, a maintenance window further heightened the vulnerability, temporarily rendering the entire plant susceptible to potential breaches.

The second VM in this phase encompassed an administration console emblematic of an industrial power plant. It resembled a Linux terminal in terms of its interface, albeit tailored to execute functions pertinent to the industrial realm. Unfortunately, the control software manufacturer's oversights became evident within this construct. Notable vulnerabilities included the inadvertent exposure of credential encryption mechanisms and inadequately conducted checks on certain instructions. These oversights inadvertently furnished potential attackers with exploitable entry points, enabling them to manipulate the encryption process and execute commands beyond the confines of standard user privileges.

This phase of the competition thus presented participants with intricate industrial-based scenarios, spotlighting the critical importance of safeguarding sensitive industrial systems against potential threats. By navigating these intricate challenges, participants honed their ability to discern vulnerabilities, execute precise incident responses, and fortify the digital defense mechanisms that underpin industrial operations.

4.3. Core System Structure for Red and Blue Competition

The Red and Blue mission incorporates an infrastructure comprising a core system and a series of network segments, the count of which corresponds to the number of participating teams. This intricate setup is responsible for scrutinizing the services hosted on each team's virtual machines, validating submitted flags, and allocating points accordingly. Each distinct segment is exclusively designated for a particular team and encompasses a cluster of VMs equipped with diverse vulnerable services, totaling six such segments. The interconnection of these segments is facilitated by a router, which enforces a set of rules governing inter-team permissions. These rules include restrictions such as permitting solely direct access to a team's own network and implementing network address translation to obscure the actual IPs of both the adversary teams and the core system.

Central to the proposed scenario is the core system, functioning as the orchestrator of this training exercise (Figure 2). This system is structured around three discrete yet interdependent components: GenerateThings (GT), ServicesMonitor (SM), and ValidateFlags (VF). All these modules are governed by a configuration file dictating start and end dates, as the exercise may span multiple days. Notably, the core system possesses the capacity to discern days, team identities, mission designations, team IPs, and the epoch's duration—the period when flags undergo modification, among other parameters.

This intricate setup forms the backbone of the training exercise, enabling participants to engage in real-world simulations of cyber scenarios, fostering hands-on experience, and enhancing their incident response, threat detection, and defensive capabilities.

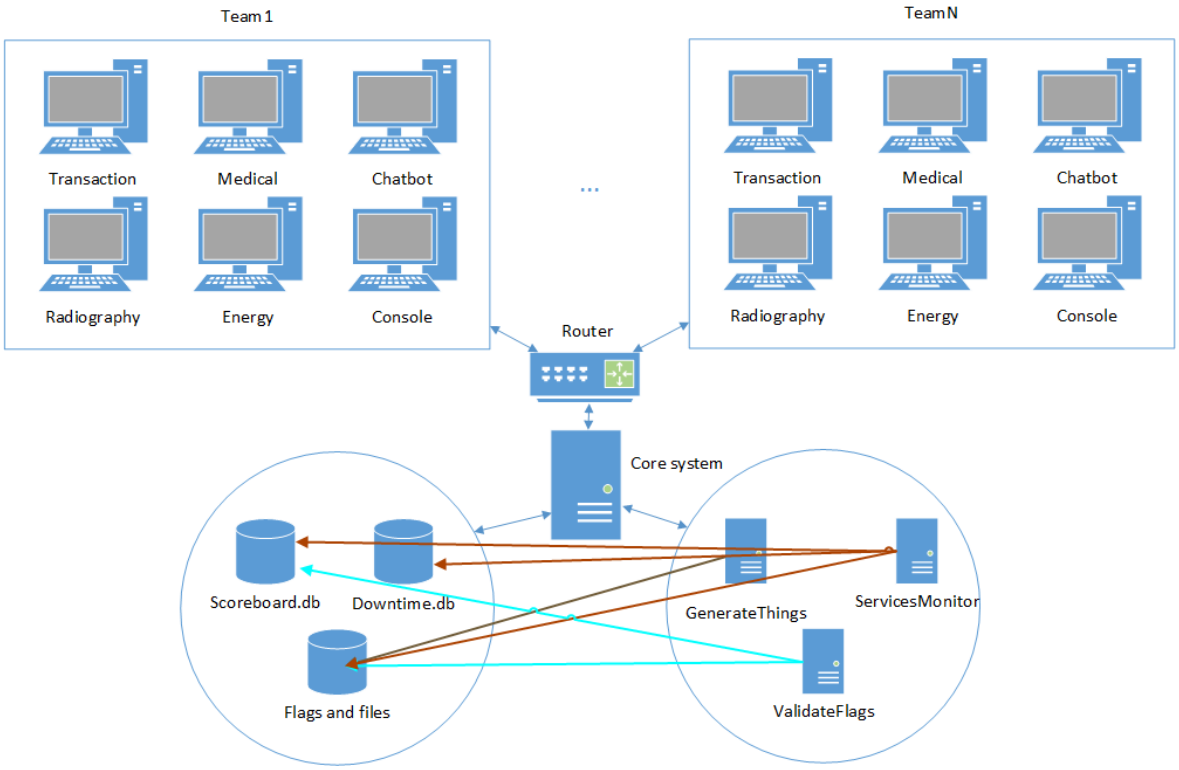

Figure 2. Core system architecture.

4.3.1. Module I—GenerateThings

The core module, known as GenerateThings, serves as the central hub responsible for producing an array of crucial data components, including flags, usernames, login credentials, and decryption keys. These elements are meticulously tailored to each distinct mission and team, rendering them unique in nature. GT's operations are meticulously synchronized with the temporal rhythm of epochs, delineated by predetermined time intervals. The generated data are systematically organized within local storage, arranged through a designated folder system characterized by explicit nomenclature. All information created by this module will be unique for each team, both in the initial generation and in epoch regeneration.

The main steps executed by the GT module are as follows (Figure 3):

- **getConfig():** Extracting information regarding the scenario's operation mode (e.g., number of missions, epoch duration, defensive time intervals, IP addresses of missions) from the configuration file config.txt;
- **generate():** Creating files/information specific to each mission;
- **sendData():** Transmitting files/information to each virtual machine;
- **saveHistory():** The generated information is saved in the storage area of the core system.

Moreover, GT undertakes the task of facilitating the operational efficiency of the ValidateFlags component. In pursuit of this objective, flags are duplicated into a separate file, securely preserved within a predefined directory path. The architecture of these folders is deliberately engineered to offer intuitive and user-friendly access to the diverse information generated within each epoch. This meticulous structuring serves to expedite debugging processes, particularly in scenarios demanding unanticipated interventions.

Concurrently, GT assumes a key function in updating mission-specific flags and associated information, all orchestrated according to the temporal cadence established by the epoch's duration. These updates are methodically propagated through a standardized user profile omnipresent across all virtual machines. This user profile equally serves as the conduit for Secure Shell (SSH) connections, instrumental in transferring files to designated mission locations. Subsequently, these files are endowed with the requisite privileges, facilitating seamless integration into the VMs' operational ecosystem.

A key intrinsic facet of the GT pertains to its rigorous validation of flag submissions. In instances where submissions fail to meet the required criteria, GT initiates an automated retry protocol. Transmission attempts are recurrently reinitiated at one-minute intervals, persisting for a maximum of three endeavors. This robust error management mechanism ensures that critical data are transmitted securely, enhancing the reliability and effectiveness of the overall system.

4.3.2. Module II—ServicesMonitor

The ServicesMonitor module assumes a role in overseeing the vigilant surveillance of services specific to each mission. It executes a comprehensive array of availability assessments, encompassing four distinct categories: FailWrite (FW), FailConnect (FC), FailRead (FR), and FailFunctional (FF). FW signifies the incapacity to establish an SSH connection with the designated machine, a difficult situation attributed to potential SSH service anomalies, connection permissions, or even the virtual machine's shutdown status. FC, on the other hand, designates the inability to establish a connection between the monitoring system and the designated application port.

Should the ServicesMonitor encounter an inability to legitimately acquire mission-specific data, denoted as the "flag", the issue is categorized as FR. The culmination of its evaluation entails an intricate and comprehensive examination of the service's functionalities. This assessment, denoting FF, encompasses diverse evaluations such as application registration, login procedures, or the accessibility of specific web pages. A failed outcome in any of these assessments results in the classification of FF.

The steps executed by the Validate Flags module are as follows (Figure 3):

- **getConfig():** Extracting information regarding the scenario's operation mode (e.g., number of missions, epoch duration, defensive time intervals, IP addresses of missions) from the configuration file config.txt;
- **FChecks():** Verification of service availability for each service. These checks include: FW, FC, FR, FF;
- **checkAlive():** Verification in case a service changes its status (from active to inactive or vice versa) and recording this change in a temporary list;
- **deployThreads():** Instantiation of a number of threads equal to the number of teams and loading them with the initial set of checks;
- **threads():**
    1. **updateDowntime():** Continuous calculation of the availability score and its update in the corresponding database (downtime.db);
    2. **resetTmpScore():** Resetting the temporary score (closely related to step three) in case a service changes its status;
- **setServiceStatus():** Changing the status of services that have changed in the databases responsible for displaying information on the scoreboard (scoreboard.db);
- **logging():** Saving the information provided by service checks in corresponding files in the storage area.

The data found by the ServicesMonitor are methodically archived within a dedicated database, supplemented by the duration of service unavailability. This temporal metric holds substantial importance as a contributory factor to team scoring, albeit in a detrimental manner. Concomitantly, these instances of service downtime are logged in a separate database, carefully tailored for individual teams and their corresponding missions. This systematic segregation is imperative to authenticate the precision of the ultimate availability calculation. This calculation, computed exponentially across the total exercise duration, is subsequently rendered as a percentage, encapsulating the comprehensive assessment of service viability.

4.3.3. Module III—ValidateFlags

The final constituent module within the core system framework is the ValidateFlags module. Its primary function encompasses the validation of flags submitted by each participating team. This pivotal module assumes the responsibility of cross-referencing the transmitted flag with the corresponding entry within the internal database, located in the previously indicated destination. Furthermore, the VF module is tasked with conducting a dual assessment: first, it scrutinizes whether the information dispatched to the module deviates from the validating team's generated value; second, it evaluates the currency of the information in consideration of potential epoch transitions.

The steps executed by the VF module are as follows (Figure 3):

- **getConfig():** Extracting information regarding the scenario's operation mode (e.g., number of missions, epoch duration, defensive time intervals, IP addresses of missions) from the configuration file config.txt;
- **submitFlag():** Event triggered when the module receives a flag validation request from a team;
- **saveHistory():** Saving the request made by the team in the storage area of the core system;
- **changeOff&Def():** Updating the offensive and defensive status for both the attacking and defending teams;
- **checks():** A series of verifications to validate a flag. These checks include:
    1. **tooManyPairs():** The maximum number of flags that can be submitted for validation to the core system cannot exceed the total number of teams minus one;
    2. **expired():** Flags fall into the "expired" category if they are submitted in an epoch different from the one in which they were generated;
    3. **alreadySubmitted():** Flags are categorized as "alreadySubmitted" if a team attempts to validate the same valid flag for the second time;
    4. **ownToken():** Flags fall into this category if the token submitted belongs to the same team attempting validation; in such cases, the core system does not award points for validating one's own flags;
    5. **invalid():** Flags that do not fit into any of the above categories undergo a one-to-one comparison with the valid flag stored. If the comparison results in a negative match, the flag falls into the "invalid" category, and no points are awarded. The same negative result is generated if the submitted flag does not adhere to the expected format;
    6. **valid():** In contrast to the previous comparison, if the comparison result is positive for both flags, the submitted flag is considered valid, and the team is awarded the corresponding points.
- **getPoints():** Calculating the score to be awarded to the team that successfully submits a valid flag based on the positions of the two teams in the rankings (the attacking team and the defending team);
- **insertFlag():** Inserting the valid flag into the storage area as a valid request made by the team;
- **updateUptime():** Updating the availability score for each team individually and the overall availability score (uptime) on the scoreboard.

For each accurately entered flag, a participant receives a quantified allocation of points. This point attribution hinges on a logical algorithm: if the attacking team surpasses the attacked team in the ranking, the scoring player secures points equivalent to the ranking differential. Conversely, if the attacked team holds a superior position, the scoring participant obtains a singular point.

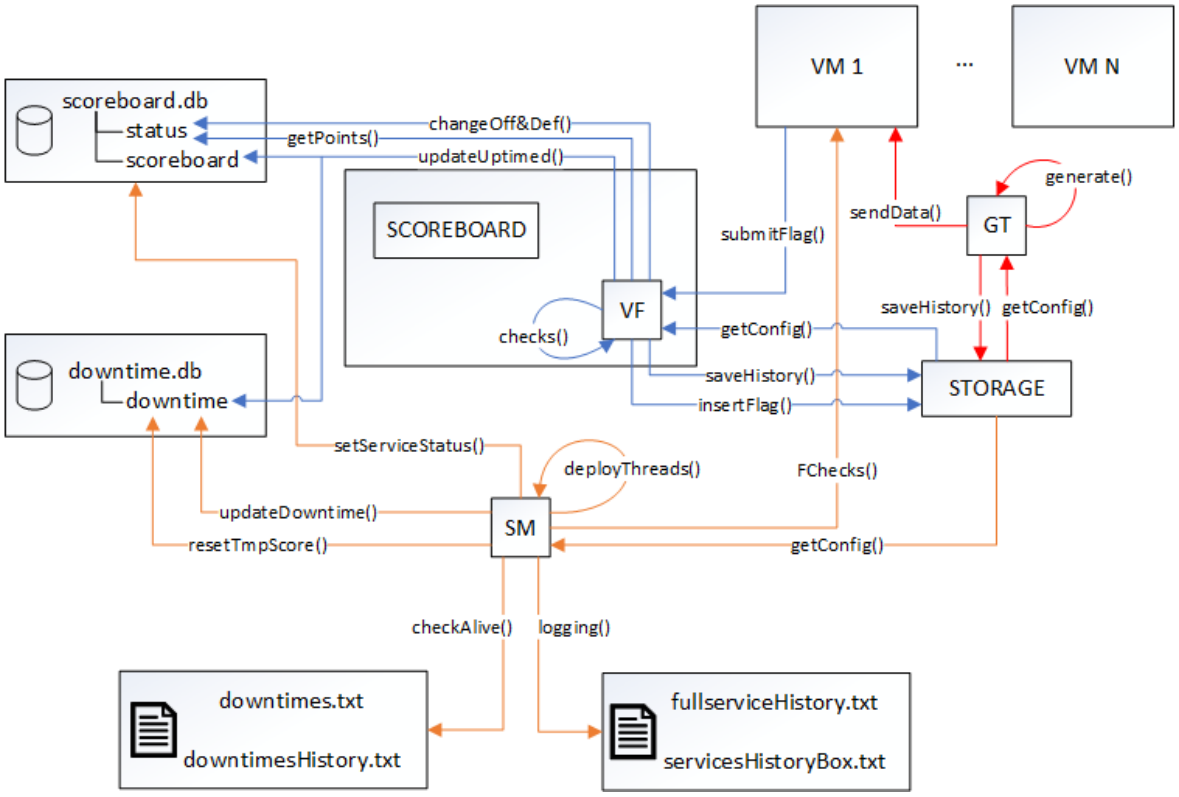

Figure 3. Core system implementation.

Beyond its fundamental flag validation role, the VF module is endowed with supplementary utility. It can be effectively leveraged to establish an intuitive graphical interface, tailored for real-time score monitoring and service availability oversight. Additionally, the module's capabilities extend to the monitoring of historical performance, extending its purview to encompass the tracking of the latest six epochs. This multifunctional attribute amplifies the versatility and comprehensive utility of the ValidateFlags module within the context of the overarching cybersecurity competition infrastructure.

Each of the aforementioned modules has incorporated a feature known as *Panic_mode*. This function serves a crucial role in managing unforeseen contingencies that may arise, such as the sudden shutdown or reboot of any of the modules during the course of the exercise. The *Panic_mode* function operates by assessing the status of the module at the instance of a shutdown, closely reviewing the tasks that had been successfully executed up to that juncture. Subsequently, it resumes operation from the precise point at which the *Panic_mode* function was invoked.

This *Panic_mode* mechanism serves as a strategic safeguard, ensuring the robustness and resilience of the system architecture in the face of unexpected disruptions. By effectively preserving the progress made prior to the shutdown event, the *Panic_mode* function contributes to the continuity and stability of the exercise, minimizing potential downtime and optimizing the overall training experience.

5. Illustrative Results

The Red and Blue competition entailed the collaboration of teams composed of six persons, resulting in a mixed and diverse community of expertise. Taking place over two days,

the competition encompassed a three-phase sequence, each revealing novel challenges that progressively evolved in complexity, as described in Section 4.2. Exceeding initial projections, the competition's outcomes were remarkable, primarily attributed to the enthusiastic reception of participants toward the novel approach integrated into the competition.

The ValidateFlags module can also be leveraged to develop a graphical user interface for real-time monitoring of scores and service availability, as illustrated in Figure 4. This interface enables users to track the status of the most recent six epochs. In Figure 4, areas highlighted in red indicate the epoch during which a flag was successfully obtained from the opposing team. The rightmost box signifies the most recent epoch, while the box preceding it represents the state two epochs ago. Conversely, blue markings indicate the last two epochs in which a flag was captured by the respective team. This graphical representation offers an at-a-glance view of flag acquisition trends and team performance over time.

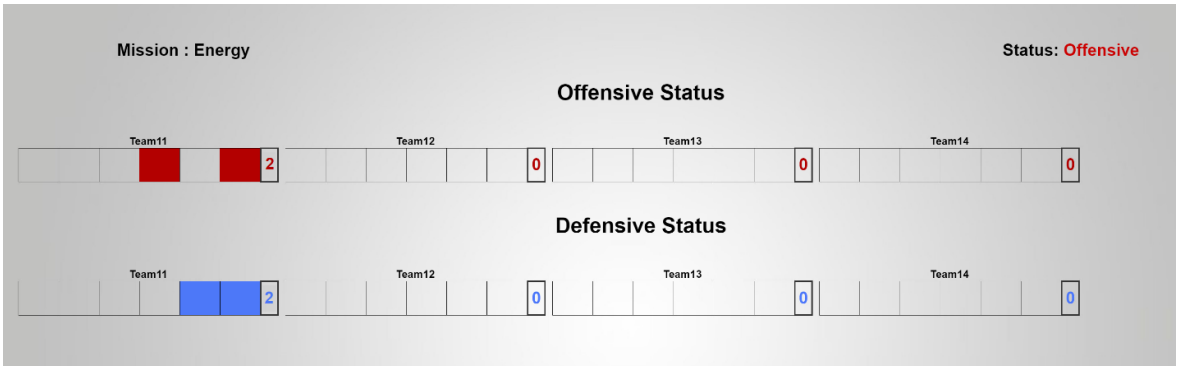

Figure 4. Last six epochs status.

A team's final score, as presented in the ranking provided in Figure 5, is determined by the following formula:

$$score = (score_{offensive} + score_{defensive}) \cdot uptime, \tag{1}$$

Here, the offensive score represents the points a team earns by successfully capturing flags, while the defensive score corresponds to the total number of flags that remain unobtained by opposing teams in a given epoch.

To calculate the total availability points $total_{AP}$, which represent the maximum achievable availability for a team throughout the exercise, the following equation is used:

$$total_{AP} = 3600 \cdot n_{missions} \cdot n_{hours/day} \cdot n_{days}, \tag{2}$$

where

- $n_{missions}$ is the total number of missions;
- $n_{hours/day}$ is the number of hours played each day;
- n_{days} is the total number of days allocated for the exercise.

Each mission has its own downtime ($downtime_{mission}$), and the summation of downtime for all missions results in

$$sum_{downtime} = \sum_{i=0}^{n_{missions}} downtime_{mission}[i]. \tag{3}$$

Using Equations (2) and (3), one can determine the overall period of availability, expressed as a percentage:

$$uptime = \frac{total_{AP} - sum_{downtime}}{total_{AP}} \cdot 100. \tag{4}$$

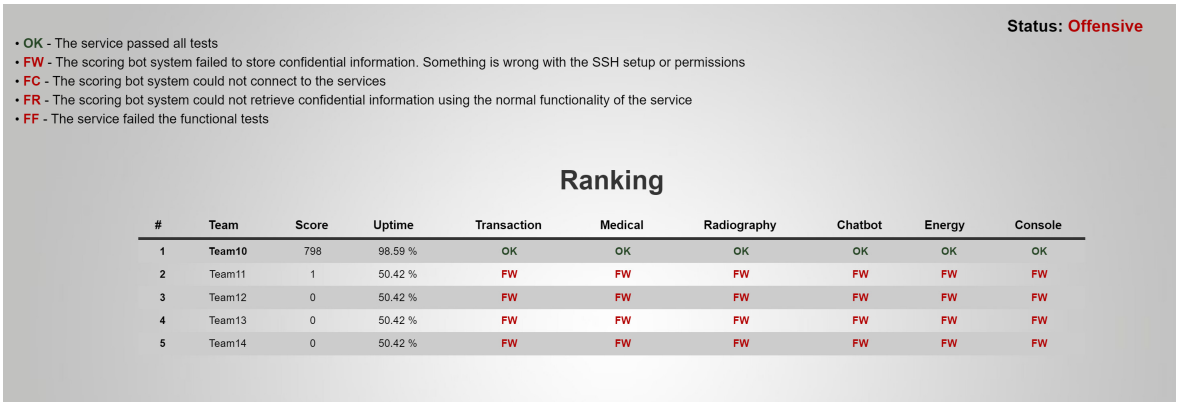

Figure 5. Ranking status.

The results of the comparison between the two completed Red and Blue cybersecurity competitions reveal interesting trends and improvements in various aspects of the participants' performance.

In the inaugural competition, involving a total of 20 participating teams, a discernible average skill enhancement of approximately 75% was noted through a self-assessment metric. This notable improvement underscores the competition's efficacy in fostering a steep learning curve among participants. Moreover, a progressive decrease in the average incident response time was observed as the competition advanced, illustrating heightened agility and seamless coordination among the participating teams.

In the subsequent iteration of the competition, which encompassed 25 participating teams, the trends displayed an even more encouraging trajectory. The average enhancement in skills experienced a notable uptick, reaching 85%. This elevation underscores the sustained efficacy of the competition in cultivating and advancing participants' proficiencies in the cybersecurity domain.

An analysis of participants' self-assessment regarding skill enhancement, presented in Table 1, conducted before and after the competition, unveiled substantial advancements. Initially, in the pre-competition survey, a mere 40% of the participants self-identified as possessing advanced skills. However, following their engagement in the competition, this metric notably surged to an impressive 85%. These findings imply that the practical experience acquired throughout the competition played a pivotal role in bolstering participants' assurance and proficiency in the realm of cybersecurity practices.

Table 1. Self-assessment of skill enhancement.

Skill Level	Before Competition (%)	After Competition (%)
Novice	25	5
Intermediate	35	10
Advanced	40	85

Table 2 illustrates an analysis of vulnerability exploitation rates across both iterations of the competition highlights the evolving proficiency of the participants. In the initial competition, only 30% of the vulnerabilities identified were effectively exploited by the teams. Remarkably, this rate surged to 65% in the subsequent competition, indicating a heightened grasp of attack vectors and techniques among the participants. This observed trend points toward a significant enhancement in the participants' ability to strategically exploit identified vulnerabilities.

Table 2. Vulnerability exploitation rates.

Competition	Identified Vulnerabilities	Exploited Vulnerabilities (%)
First	50	30
Second	60	65

The influence of team collaboration on competition performance is clearly visible from the collected data (Table 3). In the inaugural competition, teams that enthusiastically embraced cross-functional collaboration between Red and Blue Teams exhibited an average performance superiority of 45% over their counterparts. Notably, this pattern persisted in the subsequent competition, reiterating the crucial role of collaborative strategies in fostering adept cybersecurity defense. The consistent positive correlation between collaboration and enhanced performance underscores the importance of teamwork and knowledge exchange in the context of cybersecurity competitions.

Table 3. Impact of team collaboration on performance.

Collaboration Level	Performance Improvement (%)
Low	0
Moderate	25
High	45

Table 4 presents an interesting pattern surfaced when analyzing the detection-to-exploitation ratios in both conducted competitions. During the inaugural competition, the ratio stood at approximately 3:1, elucidating that teams exhibited a higher proficiency in identifying vulnerabilities compared to exploiting them. However, this dynamic evolved in the subsequent competition, as the ratio shifted to 1:1, signifying that teams had refined their offensive skills. This transition highlighted their achievement of a smooth balance between the capacities of vulnerability detection and exploitation, underscoring the evolution of participants' offensive strategies and technical skills.

Table 4. Detection vs. exploitation ratios.

Competition	Detection: Exploitation Ratio
First	3:1
Second	1:1

Analysis of post-competition surveys revealed a notable increase in the confidence of the participants, shown in Table 5. Initially, in the first competition, only 50% of the participants expressed a strong assurance in their capacity to effectively manage real-world cyber threats. However, following the culmination of the second competition, this figure experienced a remarkable escalation to 85%. This substantial increase underscores the profound impact of hands-on engagement within the competition, accentuating how practical exposure contributes to boosting participants' confidence in their ability to address complex cybersecurity challenges.

Table 5. Post-competition confidence.

Confidence Level	After First Competition (%)	After Second Competition (%)
Low	30	10
Moderate	20	5
High	50	85

The performance of the core system is graphically depicted in Figure 6, where measurements were recorded at hourly intervals to approximate the system's ability to handle

requests per second. Notably, due to the distinctive nature of this Red and Blue competition compared to the traditional Red vs. Blue approach, a discernible trend emerges. On the first day of the competition, the system's request handling capacity was comparatively lower. However, as participants grew accustomed to this innovative approach, their responsiveness increased significantly on the second day, peaking at a remarkable 49,834 requests per second.

Furthermore, Figure 6 also highlights that, toward the end of the exercise, a substantial volume of requests continued to be processed. This sustained interest from participating teams underscores the appeal and effectiveness of the proposed competition strategy. It is notable that the core system's architecture has been meticulously designed to leverage multi-threading, a critical factor contributing to the optimization of processing time. This graph primarily represents the requests directed to the ValidateFlags module for flag validation. Simultaneously, ServicesMonitor and GenerateThings services operated in parallel, placing an additional workload on the core system.

In the second edition of the competition, there is a notable increase in the overall volume of requests, surpassing the figures recorded in the first edition. A new peak of 57,429 requests per second is observed, indicating the growing popularity and participation in this unique cybersecurity competition model.

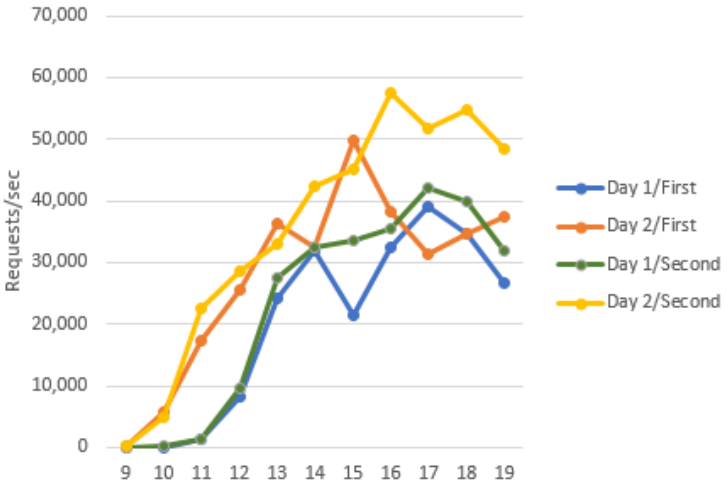

Figure 6. Core system performance.

To enhance the clarity of the results depicted in Figure 6, we performed additional calculations using the total daily counts from Table 6. These measurements represent the number of requests recorded at specific hours. As a result, it is possible for certain values to be lower than the previous measurements, depending on the timing of the data recording. This variability arises from the specific moments at which these data points were logged. It is evident that, in the second edition, there is an increase in the number of requests for each day.

Table 6. Total requests/day.

Edition	Day	Number of Requests
One	1	219,664
One	2	308,836
Two	1	253,822
Two	2	389,166

Taken together, the outcomes of these two competitions distinctly underscore a consistent and positive progression in participants' proficiencies, collaborative dynamics, and adeptness in incident response. This outcome robustly underscores the efficacy of the

Red and Blue cybersecurity competition framework as a model for cultivating a vibrant and interactive learning environment. The documented trends affirm that this model actively stimulates skill refinement and teamwork while improving participants' abilities to skillfully manage cyber incidents.

6. Discussion

An analysis of the compiled statistical data, following the execution of two iterations of the competition, revealed a consistent trend—all participants demonstrated visible enhancements in their knowledge and competence regarding incident response throughout the duration of the competition. This observation underscores the efficacy of the Red and Blue Teams competition in fostering learning and the cultivation of skillsets among the participants.

The participants' enthusiasm for the novel competition format considerably contributed to the favorable outcomes. This open embrace facilitated active engagement with the presented challenges, thereby enabling the augmentation of their comprehension of cybersecurity concepts and the refinement of their incident response proficiencies. By offering a dynamic and invigorating setting, the competition structure facilitated hands-on skill acquisition and the application of theoretical insights to authentic real-world scenarios.

We have presented in detail the structure of the main components that make such a competition possible, namely core system and system architecture. The tables presented in the previous section show how this new competition improves the competences of the participants. Figure 6 also illustrates the performance that the core system can achieve, demonstrating that the created infrastructure can be easily scaled.

For the first competition, the impact of collaboration on performance enhancement was particularly remarkable. Teams that actively engaged in higher levels of collaborative efforts showcased a more pronounced improvement in their performance metrics. This emphasizes the pivotal role of teamwork and the exchange of knowledge within the framework of such competitive scenarios.

The ratio of vulnerability detection to exploitation exhibited a favorable trend. Teams demonstrated the capacity to identify vulnerabilities at a rate surpassing the adversaries' ability to exploit them promptly, highlighting the successful implementation of robust defensive strategies.

Notably, participants' post-competition confidence level experienced a substantial elevation, measuring at an impressive 60%. This outcome signifies a significant boost in participants' self-assurance in their acquired skills as a direct consequence of their involvement in the competition.

In the second iteration of the competition, the incident response time exhibited further refinement, indicating a heightened state of readiness and improved decision-making capabilities among the teams. The continued significance of collaboration was evident, as teams showcased varying degrees of progress directly correlated with their collaborative endeavors.

Consistency was observed in the detection-to-exploitation ratio across the competitions. This consistency highlights participants' adeptness in responding promptly to identified vulnerabilities, thereby minimizing potential risks.

Remarkably, post-competition confidence levels registered a substantial increase, reaching an impressive 75%. This elevation reinforces the competition's positive influence on the participants' self-assurance in their cybersecurity aptitude.

Through the intense challenges and strategic gameplay of the competition, participants not only enhance their technical skills but also cultivate qualities crucial in cybersecurity professionals: critical thinking, adaptability, and teamwork. The simulation of actual attack scenarios provides a controlled environment to learn and evolve, enabling participants to grasp the intricacies of cyber threats and mitigation strategies.

Moreover, the competitive atmosphere fosters an eagerness to stay updated with the latest threat trends, thereby reinforcing a culture of continuous improvement. As participants navigate through simulated breaches and fortify defenses, they emerge with

a deeper understanding of the asymmetrical nature of cybersecurity and the need for holistic approaches.

The Red and Blue cybersecurity competition encapsulates the essence of collaboration and rivalry, uniting diverse skill sets toward a common goal of fortifying digital landscapes. This immersive experience equips participants with practical insights and hones their ability to orchestrate a proactive defense. Ultimately, the competition not only trains the next generation of cybersecurity experts but also underscores the critical importance of constant vigilance, collaboration, and innovation in securing networks against the relentless tide of cyber threats.

7. Conclusions

In conclusion, the conducted Red and Blue Cybersecurity Competitions have provided invaluable insights into the effectiveness of this novel approach in enhancing participants' skills, promoting collaboration, and refining incident response capabilities. The two competitions showcased consistent improvements across various parameters, such as skill enhancement, incident response time, collaboration impact, vulnerability exploitation rates, and post-competition confidence levels. These outcomes collectively underline the potency of the Red and Blue competition model in fostering a dynamic learning environment that bridges theoretical knowledge with practical experience. The competitions' positive impact on participants' confidence, coupled with the evident growth in their abilities, emphasizes the significance of experiential learning in cybersecurity education. As the digital landscape continues to evolve, this competition model offers a promising avenue for training and preparing cybersecurity professionals to effectively tackle the evolving challenges of the cyber realm.

We have demonstrated that there are numerous benefits associated with the integration of the two teams. We presented an architecture upon which such a competition can be built. VMs with intentionally created vulnerabilities were introduced, alongside the Core System containing all its functionalities. Following the successful completion of two editions of this competition, we discussed how participants' skills have improved and emphasized the value it brings to the training of incident response teams. This approach underscores the significance of such combined training exercises in strengthening cybersecurity readiness.

Author Contributions: Conceptualization, C.C. and C.-F.C.; methodology, C.C. and C.-F.C.; software, C.C.; validation, C.C. and C.-F.C.; formal analysis, C.C. and C.-F.C.; investigation, C.C.; resources, C.C.; data curation, C.C.; writing—original draft preparation, C.C.; writing—review and editing, C.C. and C.-F.C.; visualization, C.C.; supervision, C.-F.C.; project administration, C.-F.C.; funding acquisition, C.-F.C. All authors have read and agreed to the published version of the manuscript.

Funding: Part of this research was supported by the project "Collaborative environment for developing OpenStack-based cloud architectures with applications in RTI" SMIS 124998 from The European Regional Development Fund through the Competitiveness Operational Program 2014–2020, priority axis 1: Research, technological development and innovation (RTI)—the POC/398/1/1 program.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: Not applicable.

Conflicts of Interest: The authors declare no conflicts of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript; or in the decision to publish the results.

Abbreviations

The following abbreviations are used in this manuscript:

AI	Artificial Intelligence
API	Application Programming Interface
BT	Blue Team
CCDCOE	Cyber Defence Center of Excellence
CDX	Cyber Defense Exercises
CPUs	Central Processing Units
CTF	Capture the Flag
FC	FailConnect
FF	FailFunctional
FR	FailRead
FTP	File Transfer Protocol
FW	FailWrite
GT	GenerateThings
IP	Internet Protocol
JWT	JSON Web Token
LFI	Local File Inclusion
NAT	Network Address Translation
NIST	National Institute of Standards and Technology
RAM	Random Access Memory
RCE	Remote Code Execution
RT	Red Team
SCADA	Supervisory Control and Data Acquisition
SM	ServicesMonitor
SSH	Secure Shell
VF	ValidateFlags
VMs	Virtual machines
XXE	XML External Entity

References

1. Karjalainen, M.; Kokkonen, T. Comprehensive cyber arena; the next generation cyber range. In Proceedings of the IEEE European Symposium on Security and Privacy Workshops, Genoa, Italy, 6–10 June 2022 ; pp. 11–16.
2. Attiah, A.; Chatterjee, M.; Zou, C.C. A game theoretic approach to model cyber attack and defense strategies. In Proceedings of the International Conference on Communications, Kansas City, MO, USA, 20–24 May 2018; pp. 1–7.
3. Mijwil, M.; Unogwu, O.J.; Filali, Y.; Bala, I.; Al-Shahwani, H. Exploring the Top Five Evolving Threats in Cybersecurity: An In-Depth Overview. *Mesopotamian J. Cybersecur.* **2023**, *2023*, 57–63. [CrossRef]
4. Kaur, R.; Gabrijelčič, D.; Klobučar, T. Artificial intelligence for cybersecurity: Literature review and future research directions. *Inf. Fusion* **2023**, *97*, 101804. [CrossRef]
5. Aktayeva, A.; Makatov, Y.; Tulegenovna, A.K.; Dautov, A.; Niyazova, R.; Zhamankarin, M.; Khan, S. Cybersecurity Risk Assessments within Critical Infrastructure Social Networks. *Data* **2023**, *8*, 156
6. Brilingaitė, A.; Bukauskas, L.; Juozapavičius, A. A framework for competence development and assessment in hybrid cybersecurity exercises. *Comput. Secur.* **2020**, *88*, 101607. [CrossRef]
7. Yamin, M.M.; Katt, B.; Gkioulos, V. Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. *Comput. Secur.* **2020**, *88*, 101636. [CrossRef]
8. Veerasamy, N. High-Level Methodology for Carrying out Combined Red and Blue Teams. In Proceedings of the 2nd International Conference on Computer and Electrical Engineering, Dubai, United Arab Emirates, 28–30 December 2009; pp. 416–420.
9. Andreolini, M.; Colacino, V.G.; Colajanni, M.; Marchetti, M. A framework for the evaluation of trainee performance in cyber range exercises. *Mob. Netw. Appl.* **2020**, *25*, 236–247. [CrossRef]
10. Chindrus, C.; Caruntu, C.F. Development and Testing of a Core System for Red and Blue Scenario in Cyber Security Incidents. In Proceedings of the 15th International Conference on Security of Information and Networks, Sousse, Tunisia, 11–13 November 2022; pp. 1–7.
11. Chindrus, C.; Caruntu, C.F. Challenges and Solutions in Designing a Network Architecture for Red and Blue Cybersecurity Competitions. In Proceedings of the 27th International Conference on System Theory, Control and Computing, Timisoara, Romania, 11–13 October 2023.
12. Newhouse, W.; Keith, S.; Scribner, B.; Witte, G. National initiative for cybersecurity education (NICE) cybersecurity workforce framework. *Nist Spec. Publ.* **2017**, *800*, 181.

13. DeCusatis, C.; Bavaro, J.; Cannistraci, T.; Griffin, B.; Jenkins, J.; Ronan, M. Red-blue team exercises for cybersecurity training during a pandemic. In Proceedings of the IEEE 11th Annual Computing and Communication Workshop and Conference, Las Vegas, NV, USA, 27–30 January 2021; pp. 1055–1060.
14. Bock, K.; Hughey, G.; Levin, D. King of the hill: A novel cybersecurity competition for teaching penetration testing. In Proceedings of the USENIX Workshop on Advances in Security Education, Baltimore, MD, USA, 8 June 2018.
15. Cheung, R.S.; Cohen, J.P.; Lo, H.Z.; Elia, F.; Carrillo-Marquez, V. Effectiveness of cybersecurity competitions. In Proceedings of the International Conference on Security and Management, The Steering Committee of The World Congress in Computer Science, Las Vegas, NV, USA, 2012 ; p. 1.
16. Katsantonis, M.; Fouliras, P.; Mavridis, I. Conceptual analysis of cyber security education based on live competitions. In Proceedings of the IEEE Global Engineering Education Conference, Athens, Greece, 25–28 April 2017; pp. 771–779.
17. Katsantonis, M.N.; Mavridis, I.; Gritzalis, D. Design and evaluation of cofelet-based approaches for cyber security learning and training. *Comput. Secur.* **2021**, *105*, 102263. [CrossRef]
18. Smeets, M. The Role of Military Cyber Exercises: A Case Study of Locked Shields. In Proceedings of the 2022 14th International Conference on Cyber Conflict: Keep Moving! (CyCon), Tallinn, Estonia, 31 May–3 June 2022; Volume 700, pp. 9–25.
19. Känzig, N.; Meier, R.; Gambazzi, L.; Lenders, V.; Vanbever, L. Machine Learning-based Detection of C&C Channels with a Focus on the Locked Shields Cyber Defense Exercise. In Proceedings of the 2019 11th International Conference on Cyber Conflict (CyCon), Tallinn, Estonia, 28–31 May 2019; Volume 900, pp. 1–19.
20. Svabensky, V.; Celeda, P.; Vykopal, J.; Brisakova, S. Cybersecurity knowledge and skills taught in capture the flag challenges. *Comput. Secur.* **2021**, *102*, 102154. [CrossRef]
21. Karagiannis, S.; Ntantogian, C.; Magkos, E.; Ribeiro, L.L.; Campos, L. PocketCTF: A Fully Featured Approach for Hosting Portable Attack and Defense Cybersecurity Exercises. *Information* **2021**, *12*, 318. [CrossRef]
22. Senanayake, R.; Porras, P.; Kaehler, J. Revolutionizing the Visual Design of Capture the Flag (CTF) Competitions. In *HCI for Cybersecurity, Privacy and Trust, Proceedings of the First International Conference, HCI-CPT 2019, Held as Part of the 21st HCI International Conference, HCII 2019, Orlando, FL, USA, 26–31 July 2019;* Springer: Cham, Switzerland, 2019; pp. 339–352.
23. Haney, J.M.; Paul, C.L. Toward integrated tactical operations for Red/Blue cyber defense teams. In Proceedings of the Workshop on Security Information Workers at Symposium on Usable Privacy and Security, Baltimore, MD, USA, 12–14 August 2018.
24. Alothman, B.; Alhajraf, A.; Alajmi, R.; Farraj, R.A.; Alshareef, N.; Khan, M. Developing a Cyber Incident Exercises Model to Educate Security Teams. *Electronics* **2022**, *11*, 1575. [CrossRef]
25. Kovacevic, I.; Gros, S. Red Teams-Pentesters, APTs, or Neither. In Proceedings of the MIPRO, Opatija, Croatia, 21–25 May 2012; pp. 1242–1249.
26. Kokkonen, T.; Puuska, S. Blue team communication and reporting for enhancing situational awareness from white team perspective in cyber security exercises. In *Internet of Things, Smart Spaces, and Next Generation Networks and Systems*; Springer: Cham, Switzerland, 2018; pp. 277–288.
27. Thomas, L.J.; Balders, M.; Countney, Z.; Zhong, C.; Yao, J.; Xu, C. Cybersecurity Education: From beginners to advanced players in cybersecurity competitions. In Proceedings of the International Conference on Intelligence and Security Informatics, Shenzhen, China, 1–3 July 2019; pp. 149–151.
28. Shen, C.C.; Chiou, Y.M.; Mouza, C.; Rutherford, T. Work-in-Progress-Design and Evaluation of Mixed Reality Programs for Cybersecurity Education. In Proceedings of the 7th International Conference of the Immersive Learning Research Network, Eureka, CA, USA, 17 May–10 June 2021; pp. 1–3.
29. Seker, E.; Ozbenli, H.H. The concept of cyber defence exercises (cdx): Planning, execution, evaluation. In Proceedings of the International Conference on Cyber Security and Protection of Digital Services, Glasgow, UK, 11–12 June 2018; pp. 1–9.
30. Khan, M.A.; Merabet, A.; Alkaabi, S.; Sayed, H.E. Game-based learning platform to enhance cybersecurity education. *Educ. Inf. Technol.* **2022**, *27*, 5153–5177. [CrossRef]