ISSN: 2321-2152

# IJMECE

## International Journal of modern electronics and communication engineering

E-Mail
editor.ijmece@gmail.com
editor@ijmece.com

www.ijmece.com

# Red team vs blue team simulations in enhancing Soc preparedness

**A.SRUTHI[1], CHILLALE SEEMA [2], BANDA NIHARIKA [3], GANASALA VISHAL [4], PASPULA SATHWIK [5]**

[1] Assistant Professor, Dept. of CS, Sri Indu College of Engineering and Technology, Hyderabad,
[2 3 4] Research Student, Dept. of CS, Sri Indu College of Engineering and Technology, Hyderabad

**Abstract.** Effective measures are required to counteract cybersecurity threats, which are emerging at a fast pace. One effective strategy for dealing with this problem is to train as a red and blue squad. It mimics actual assaults by placing the Red

in the role of attackers and the blue team in the role of defenders. In addition to preparing workers to react appropriately to security crises, this training aids businesses in identifying potential risks. Competition is a great way to keep participants motivated to achieve and keep up with the ever-changing dangers, which enriches this training even more. If we want to see better cross-team communication and understanding, this article suggests merging the Red and Blue teams. Results show that this method improves responsiveness to actual assaults. Members of the team are better able to detect and address weaknesses when they work to improve their mutual understanding.

These findings demonstrate the possible benefits of a joint Red and Blue team strategy to improve cybersecurity preparedness. To thoroughly investigate its advantages and disadvantages, further study is required.

**Keywords:** Cybersecurity, Red and Blue Team, training, attack scenarios, competition, mitigation.

## 1. Introduction

Organizations worldwide are facing a plethora of cybersecurity threats brought forth by the current era's fast changing digital ecosystem.
As technology advances, cybercriminals get more crafty and modify their approaches accordingly.

developments, calling for strong plans to guarantee adequate cybersecurity preparedness. As a result, in light of these growing dangers, the Red vs. Blue team competition has become a viable strategy for strengthening enterprises' cybersecurity defenses via the simulation of real-world assault scenarios.
In order to better identify, react to, and mitigate cyber threats, this scientific research seeks to investigate the possibility of Red and Blue team competition as a means to improve cybersecurity preparedness. Organizations may strengthen their cybersecurity posture via the Red and Blue team competition, which offers a dynamic and realistic training environment that promotes teamwork, skill development, and a culture of continuous growth.
In order to increase cybersecurity preparedness, this research aims to examine the advantages and practical consequences of red team and blue team competition (Cheung et al., 2012). The goal of this research is to clarify

the role of the "Red Team" and the "Blue Team" rivalry in the dynamic field of cyber defense by reviewing relevant literature and case studies. The effectiveness and potential of this training strategy to improve cybersecurity preparedness may be better understood by businesses by looking at the results and lessons learnt from adopting it.

Two crucial responsibilities in cybersecurity are brought together in the Red and Blue team competition: the Red team represents the attackers, while the Blue team represents the defenders. Through this cooperative method, businesses are able to recreate actual assaults, with the Blue team facing the challenge of detecting and responding to threats while the Red team tries to penetrate their defenses. Participating in these simulations allows firms to find security holes, practice responding to incidents, and improve their cybersecurity plans (DeCusatis et al., 2021).

When looking at the Red vs Blue battle, it's easy to see the obvious division of labor between the two sides, with one side taking on the offensive and the other the defensive. This dynamic takes place in a corporate-like network architecture. The fundamental nature of the tournament is the strategic interaction between the two teams, which mimics the adversarial nature of cybersecurity. While one group works to strengthen the network against intrusions, the other group hunts for security holes that may be exploited. Protecting digital assets from bad intent is an ongoing concern for enterprises in the real world, and this structure reflects that difficulty. By making cybersecurity training more of a contest, this method encourages teams to demonstrate their agility, creativity, and competence by finding and exploiting security flaws. The dualistic character of cybersecurity is summed up by the Red vs Blue conflict, which is a high-stakes battle between the dogged search of vulnerabilities and the equally dogged protection against them.

As part of the Red and Blue competition paradigm, two teams work together to train. By simulating real-life situations, this method promotes offensive and defensive roles communicating, understanding, and working together. The focus on collaboration encourages a comprehensive understanding of cybersecurity, enabling participants to devise plans that include both defensive and offensive viewpoints. The preparedness to face evolving threats is enhanced by Red and Blue contests, which include jointly detecting vulnerabilities and refining responses. In contrast, the "Red versus Blue" format pits the Red Team against the Blue Team head-on. Because of the hostile environment, the level of competition is high, and both teams are trying to out-plan one another. This approach encourages planning ahead and making snap decisions when time is of the essence, but it could stifle chances for teamwork and knowledge sharing.

Without a thorough grasp of holistic cybersecurity procedures, the emphasis on competitiveness risks diluting the topic.

Competitors in the Red and Blue team event also get the opportunity to hone their cybersecurity expertise. Participants must constantly update their knowledge and skills due to the ever-changing nature of the danger environment they are exposed to. According to Pusey et al. (2016), firms may promote a culture of continuous improvement via cooperation between the Red and Blue teams, which allows for the sharing of insights and best practices.

Organisations may improve their cyber threat detection, response, and mitigation capabilities by studying the efficacy of this training method. To help readers grasp the importance of red and blue team competition in enhancing enterprises' cybersecurity posture in a constantly changing digital ecosystem, this article will explore the many benefits it offers in the following parts.

## 2. Understanding the Red and Blue Team Competition

There has been a lot of buzz about using Red and Blue team competition as a training tool for cybersecurity. In this part, we'll try to explain the idea and its complexities in detail.

Competition between red and blue teams, with an emphasis on the game's essential elements and objectives.

Team Red and Team Blue compete in a simulated exercise whereby two groups, one representing attackers and the other representing defenders, fight strategic combat in a cyber environment. In this scenario, the Blue team functions as guardians of the system or network, while the Red team plays the part of enemies, using aggressive methods to breach the

defenses set up by the Blue team. By comparing the efficacy of defensive measures and discovering any weaknesses, the main goal of the Red and Blue team competition is to improve enterprises' overall cybersecurity posture (Veerasamy, 2009).
Within this framework, members of the Red team use their knowledge to detect and take advantage of system vulnerabilities, mimicking actual assault situations.
On the other side, the Blue team's goal is to protect the system by tracking the Red team's moves and reacting defensively. Students learn effective strategies for both defending against and attacking cyber threats via this dynamic and participatory approach.
There are a number of essential components to the Red and Blue team competition's objectives. To begin with, it lets businesses test how well their security mechanisms withstand mock assaults (Zhang et al., 2018).
By outlining the pros and cons of current cybersecurity techniques, this review helps to enhance them specifically.
Furthermore, the Red and Blue team competition is a great way for cybersecurity experts to hone their technical abilities, develop a proactive attitude, and work together more effectively as a team.
Due to its complexity, the Red and Blue team competition necessitates a multi-faceted strategy. Using sophisticated threat information, implementing realistic scenario designs, and implementing rigorous assessment procedures are all part of it (Thomas et al., 2019).
Furthermore, in order to get the most out of the competition, the Red and Blue teams must work together and coordinate well.

## 2.1. Red Team

When it comes to cyberwarfare tournaments, the Red side is always on the offense. Their main focus is on trying to break cybersecurity systems via simulations of real-world cyber assaults.

shields that businesses use. Members of the Red team are highly skilled cybersecurity experts who use their knowledge to get into the organization's systems illegally by finding and exploiting flaws. Overarchingly, the Red team's goal is to test and analyze the Blue team's protection systems.
In order to mimic the methods used by real cybercriminals, the Red team uses a wide variety of advanced tactics, tools, and strategies. They are able to evaluate the entire resilience of a company's security architecture, find possible weaknesses, and simulate realistic attack scenarios thanks to their extensive knowledge and skills (Bock et al.,

2018 in the year. By putting themselves in the shoes of the bad guys, the Red team is able to show the Blue team where they went wrong with their defenses.
In order to test the boundaries of the Blue team's strengths and vulnerabilities, the Red team works tirelessly throughout the tournament to do just that. The Red and Blue teams are always learning from each other and improving their game via this dynamic interaction.
To test the Blue team's defenses, the Red team launches actual and simulated cyberattacks.

There is more to the Red team's role in the tournament than just testing and evaluation. In general, an organization's cybersecurity posture is much improved by their works. Through a thorough evaluation of the Blue team's defense mechanisms, the Red team helps find weak spots, makes it easier to put in place specific security measures, and makes the organization more resistant to cyber threats in general.

As the leading offensive team in cybersecurity tournaments, the Red team is crucial. By revealing gaps and vulnerabilities, their knowledge, creativity, and simulated cyber-attacks help firms strengthen their defensive capabilities. According to Haney and Paul (2018), firms may improve their cybersecurity plans, incident response skills, and security culture by conducting a thorough evaluation. Organizations are able to keep up with the constantly changing cyber threat environment thanks to the partnership between the Red and Blue teams inside the competition framework, which helps to enhance cybersecurity practices.

### 2.2. Blue Team

When it comes to cyberwarfare tournaments, the Red side is always on the offense. Their main focus is on trying to break cybersecurity systems via simulations of real-world cyber assaults.

shields that businesses use. Members of the Red team are highly skilled cybersecurity experts who use their knowledge to get into the organization's systems illegally by finding and exploiting flaws. Overarchingly, the Red team's goal is to test and analyze the Blue team's protection systems.

In order to mimic the methods used by real cybercriminals, the Red team uses a wide variety of advanced tactics, tools, and strategies. They are able to evaluate the entire resilience of a company's security architecture, find possible weaknesses, and simulate realistic attack scenarios thanks to their extensive knowledge and skills (Bock et al.,

2018 in the year. By putting themselves in the shoes of the bad guys, the Red team is able to show the Blue team where they went wrong with their defenses.

In order to test the boundaries of the Blue team's strengths and vulnerabilities, the Red team works tirelessly throughout the tournament to do just that. The Red and Blue teams are always learning from each other and improving their game via this dynamic interaction. To test the Blue team's defenses, the Red team launches actual and simulated cyberattacks.

There is more to the Red team's role in the tournament than just testing and evaluation. In general, an organization's cybersecurity posture is much improved by their works. Through a thorough evaluation of the Blue team's defense mechanisms, the Red team helps find weak spots, makes it easier to put in place specific security measures, and makes the organization more resistant to cyber threats in general.

As the leading offensive team in cybersecurity tournaments, the Red team is crucial. By revealing gaps and vulnerabilities, their knowledge, creativity, and simulated cyber-attacks help firms strengthen their defensive capabilities. According to Haney and Paul (2018), firms may improve their cybersecurity plans, incident response skills, and security culture by conducting a thorough evaluation. Organizations are able to keep up with the constantly changing cyber threat environment thanks to the partnership between the Red and Blue teams inside the competition framework, which helps to enhance cybersecurity practices.

## 2.3. Objectives of Red and Blue Team Competition

The main objective of the Red and Blue team competition is to improve cybersecurity readiness by creating a virtual setting that closely resembles actual cyber-attack situations. It has

technique allows businesses to assess their defensive capabilities, pinpoint weaknesses, and improve their tactics for responding to incidents.
Companies may learn a lot about their cybersecurity strengths and shortcomings in the simulated setting of the Red Team and Blue Team contests. Security controls, incident response procedures, and vulnerability management are among the areas that need improvement. Attiah et al. (2018) found that enterprises may learn a lot about where their cybersecurity defenses are lacking and how to strengthen them by comparing the attack vectors used by the Red team with the response efficacy of the Blue team.
In addition, cybersecurity experts cultivate an environment of cooperation and collaboration via Red and Blue team contests. Learning and progress are made possible by the Red and Blue teams exchanging information, skills, and best practices. It fosters a culture of resilience, promotes the adoption of proactive security measures, and promotes innovation in defensive techniques.

Incorporating lessons learnt from Red Team and Blue Team contests into cybersecurity processes may help businesses realize the advantages of these exercises. Improving threat intelligence capabilities, bolstering security standards, and giving continual training to workers are all part of this. Furthermore, in order to maintain a strong and adaptable cybersecurity preparedness, firms should regularly upgrade their defenses in response to new threats and industry best practices.
According to Katsantonis et al. (2021), the main objectives of the competition are:
• Find Open Security Hole(s): Organizations may find out where their cybersecurity defenses are weakest via red team competition and blue team competition. By simulating assaults, the Red team finds vulnerabilities that could otherwise go undetected. In order to proactively manage and mitigate possible threats, companies must first assess their vulnerabilities.
Organizations may test the efficacy of their incident response systems via red team vs. blue team competition. Organizations may improve their cyber-defense capabilities and incident response strategies by evaluating the Blue team's performance in detecting and responding to the Red team's assaults.
Cybersecurity professionals may benefit greatly from participating in red and blue team competitions, which provide excellent chances for skill development.
By taking part in the competition, they improve their technical knowledge, analytical thinking, and capacity to solve problems. Competitors get the knowledge and experience to face real-world cyber threats in this difficult and ever-changing battle, which also helps them advance professionally.

Competing as a Red or Blue team encourages members of both sides to work together and share what they know. Professionals in the field of cybersecurity may network with one another, discuss ideas, and learn from the experiences of others via the competition. By working together, we create an atmosphere of cooperation, which is perfect for exchanging cybersecurity best practices and brainstorming new ideas.

## 3. Benefits of Red and Blue Team Competition

There are several ways in which a company's cybersecurity preparedness may be improved via the use of red and blue team competition, which has recently become a popular technique in cybersecurity training. Through the practice of assault simulations

situations, this kind of training allows businesses to detect weaknesses ahead of time, strengthen defensive capabilities, and fine-tune crisis response plans. The capacity to create an immersive and realistic training environment is one of the main benefits of the Red and Blue team competition. Participants get hands-on experience in countering sophisticated attackers by simulating real-life cyber assaults (Yamin et al., 2020). Competitions like this help students hone abilities that are crucial in actual cybersecurity incidents: the capacity to think critically, solve problems quickly, and make snap judgments. The Red and Blue team competition also encourages players to work together as a unit. Collaboration, dialogue, and the exchange of information are fostered by the ever-changing dynamic between the Blue and Red teams. This team effort fosters an environment of collaboration and information sharing, which improves cybersecurity operations as a whole. The function of Red and Blue team competition in revealing weaknesses in an organization's infrastructure and processes is another advantage (Brilingaitė et al., 2020). The extensive testing of the organization's defenses by the Red team's assaults uncovers possible holes that may have been overlooked. With this knowledge, businesses may fortify their security measures, increase the resilience of their digital assets, and proactively fix vulnerabilities. In addition, competing on the Red and Blue teams is a great way to hone your abilities and discover new things. Attendees will get the chance to learn about cutting-edge assault methods, defensive tactics, and best practices in the field. Professionals in the field of cybersecurity are able to improve their defenses against cyberattacks by continuously learning about new threats and using what they've learned to real-world situations (Shen et al., 2021). operate together in their network setting. They learn about the ever-changing techniques, tactics, and procedures (TTPs) used by threat actors via this practical experience, which improves their ability to foresee and counteract actual threats. Organizations may find their defensive strategy's weak spots via the repetitive nature of blue and red team contests. The Blue team is able to improve its incident response plans, defense measures, and detecting skills thanks to the lessons learned and experiences gained from these events. According to Karjalainen and Kokkonen (2020), businesses may adjust their security posture to new threats by continuously improving their systems.

### 3.3. Skill Development and Knowledge Sharing

One of the most important ways that cybersecurity experts can learn from one another and improve their skills is via red and blue team competitions. This one-of-a-kind platform fosters an atmosphere of healthy competition, which in turn inspires users to take part.

so that they might become more technically proficient, think more critically, and solve problems more effectively. Pros show their mettle in cybersecurity by taking part in simulated attack and defensive situations, which test their analytical thinking, strategy, and execution.

Teams from the opposite color often work together, which is a major perk of the Red and Blue rivalry. By working together, experts in the field of cybersecurity are able to share their knowledge, insights, and experiences, creating an environment where everyone is always trying to become better. By taking part in these contests, experts may broaden their technical understanding via exposure to various attack scenarios and vectors (Katsantonis et al., 2017). Team contests, whether they are red or blue, are great for developing analytical and problem-solving abilities. Complex scenario analysis, rapid decision-making, and real-time strategy adaptation are the participants' challenges. By mimicking the fast-paced, high-stakes setting of real cybersecurity crises, these contests help participants hone their ability to remain calm and collected under pressure.
Competitors from both the Red and Blue teams may learn from one another. By interacting with other professionals in the field, cybersecurity experts may pick up new skills, understand other points of view, and come up with creative solutions to old problems (Vigna, 2003). By working together, members of this community are driven to improve their abilities over time, keep up with developments in their field, and pioneer new approaches to cybersecurity.

## 4. Implementing Red and Blue Team Competition

A router, a central system, and several network segments (subnets) representing the competing teams make up the Red and Blue competition's architecture (Fig. 1). An overview of the network design

Participation in this kind of competition is intended to provide a realistic setting that mimics cyber-attack situations. Every subnet has defenseless systems that need fixing; players must find these holes and fix them while simultaneously attacking other teams to find certain warning signs.
In order to encourage cooperation and collaboration across teams, this architecture primarily aims to test the participants' capacities to respond to incidents. But setting up the router rules might be tricky since there are a lot of regulations that limit access to different parts of the competition. You are not allowed to access the virtual machines (VMs) of the other team in any way. Furthermore, the virtual machine (VM) that corresponds to each team's task is the only one that they are allowed to access. In order to hide the real IP addresses of the other team and the main system, Network Address Translation (NAT) is used. By masking IP addresses, this NAT feature keeps users anonymous and stops hackers in their tracks.

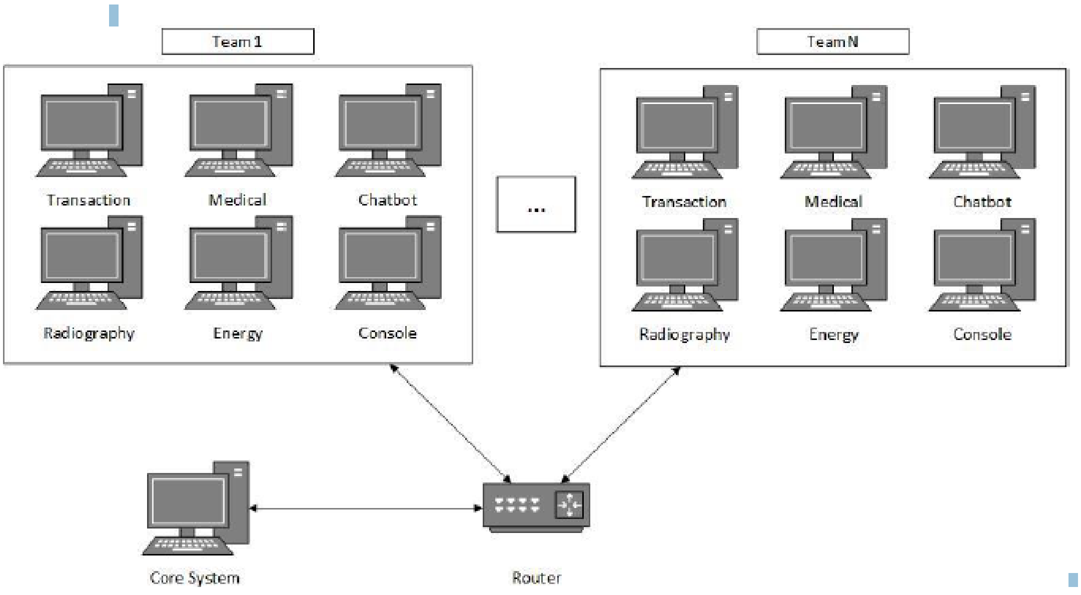


Fig. 1 – Red and Blue team competition network.

### 4.1. Network Architecture and Vulnerable Machines

In order to evaluate players' capacities to respond to incidents and encourage them to cooperate together, the network architecture in a cybersecurity competition scenario is essential. A router, central system, and several subnets representing the competing teams make up the standard components. Every subnet contains

susceptible systems that teams use to initiate assaults and detect warning signs. Six virtual machines (VMs) with different vulnerabilities are part of the design, thus regulations are needed to make sure everyone plays by the rules. One set of regulations limits access to the current team's subnet and forbids direct access to the virtual machines (VMs) of the other team. Additional rule sets are necessary to govern access to the virtual machines (VMs) that are particular to each phase, since there are three phases with two accessible VMs each. Teams get to know their own computers during the grace periods of each phase, but they can't access the virtual machines (VMs) of the other teams. By designating a single IP address as the default gateway in each subnet, three distinct sets of rules are applied at regular intervals throughout the connection between any two teams, making detection more difficult. Between different subnets, NAT is used to hide IP addresses. Virtual machines (VMs) allocated to different missions cannot be accessed by the same team. For example, if one team is linked to VM1, they are limited to exploiting vulnerabilities in the other team's VM1. Six rules, one for each task, are needed for each team-to-team link. The administration of these regulations grows in importance as the number of competing teams

increases. In a cybersecurity competition, the network architecture is crucial because it simulates the actual world, puts competitors' technical skills, collaboration, and knowledge of attacker techniques and tactics to the test, and rewards exceptional performance.
In order to test how well competitors can handle incidents, the cybersecurity competition uses six virtual PCs, each with its own set of vulnerabilities. 'Transaction' is the name of the first virtual machine (VM), and it mimics the behavior of a bitcoin wallet, which introduces security holes in that area.
'Medical' is the second virtual machine, and it stands for a medical clinic's website that is susceptible to vulnerabilities like SQL Injection, Local File Inclusion (LFI), and Remote Code Execution (RCE).
Two more virtual machines are added in the second stage. The first, named "Chatbot," acts like a chatbot but uses vulnerabilities such as SQL Injection, Command Injection, and Directory Traversal to pose as a chat service with pre-set queries.
The X-ray clinic's website is mimicked by the second virtual machine (VM), 'Radiography,' which contains vulnerabilities like XML External Entity (XXE) and LFI.
Two VMs with an emphasis on industry are introduced in the last stage. The first, titled "Energy," showcases a communication protocol for Supervisory Control and Data Acquisition (SCADA) across various power plants, with a focus on safeguarding vital information such as nuclear fuel. The second virtual machine (VM), named "Console," looks like an industrial power plant's control panel and shows how flaws in the control software may be exploited.
Careful consideration is given to the design of each virtual machine (VM) inside the system, ensuring that it aligns with the specific features of each machine. Alongside this, security holes have been purposefully created to match the specific characteristics of every virtual machine. By using this strategic approach, we can make sure that the system vulnerabilities are tailored to each machine's unique peculiarities, making the training environment more realistic and relevant. This technique allows for a more realistic and hands-on learning experience by tailoring the vulnerabilities to the unique characteristics of each virtual machine.
Ansible scripts may describe hardware requirements and other factors that are needed for VM configuration and deployment. Virtual Machines often need a minimum of two processors, four gigabytes of RAM, and forty gigabytes of hard drive space.
Your Core System will not run without at least 16 CPU, 64 GB of RAM, and 100 GB of hard drive space. Specialized hardware is not necessary; all that is needed are servers capable of meeting all hardware specifications.
The virtual machines (VMs) and network architecture used in this competition provide a realistic and difficult environment for participants to test their abilities in detecting and preventing cybersecurity risks. Using a wide variety of vulnerability types and scenarios, the competition provides a thorough way to assess competitors' skills and make sure they are prepared to face real-world cybersecurity threats.

### 4.2. Core System Architecture

As the "brain" of the training exercise, the core system is the primary component of the suggested scenario. It is made up of three separate modules: Things (GT), Services (SM), and

verify flags (VF). Despite their autonomy, these modules do share certain resources. Because the exercise might last for many days, a configuration file is essential for specifying when it will begin and when it will conclude.
Day determination, team names, mission names, team IP addresses, and epoch duration (the time it takes for the flags to change) are all accessible parts of the core system.
The cybersecurity training exercise may be carried out efficiently since the main system also includes other operations and features.
Unique flags and other mission-specific information, such as login credentials, decryption keys, and usernames, are generated by the GenerateThings (GT) module. The epoch period determines when these randomly produced things—strings based on mission-specific Python functions—are formed. Each team's items are unique. GT uses a well-organized system of local folders to store all of its created data. A separate file additionally stores the flags to make the ValidateFlags (VF) module's actions easier.
Each player earns one point according to the folder arrangement. Plus, you may access the ValidateFlags module. In situations when debugging is needed, this structure is useful since it provides simple access to the relevant information.
Additionally, the epoch period determines how often the GT component must update the flags and mission-related data.
A generic user account is used on every virtual machine (VM) to transmit these files. This user account is used to create Secure Shell (SSH) connections, which are used to transfer data to the specific locations for each mission. In order for the programs running on the virtual machines to make good use of these files, the proper permissions are provided.
The GT module also checks if flags have been sent successfully, which is a crucial step. To make sure the flags are received successfully, the transmission procedure is automatically resumed every minute if a submission is failed. A maximum of three tries are attempted.
Ensuring mission-specific service availability is the responsibility of the ServicesMonitor (SM) component. It tests for availability in four different ways: write, connect, read, and fail functionally. Failure to establish an SSH connection with the relevant machine is indicated by FW. This might be due to problems with the SSH service, permissions for connections, or a virtual machine shutdown. When the monitoring system and the application's port cannot be connected, it will be indicated by the FC. The SM is set to FR if it is unable to receive the mission-specific data (the flag) via authorized means. In its most thorough version, the FailFunctional (FF) test checks for all of the features that a service should have. Activities such as application registration or login, or the accessibility of certain web sites, might be part of this test. An FF occurs if even one of these tests returns negative results.
Along with the amount of time that service was down, SM stores all of the data it collects in a database. A team's score is negatively affected by the duration of their absence. Each team and mission has its own database to ensure precise tracking of this information. This is essential for getting the percentage of ultimate availability, which is an exponential function of total exercise time, right.
The last part of the main system is the ValidateFlags module, which checks the flags that each team has supplied. Its principal function is to verify that the value of the communicated flag matches that which is kept in the internal database, which is located at the previously indicated location. It also checks that the given data is not expired because of an epoch change

and that it varies from the value produced by the validation team. The player earns points for each flag that is input properly. These points may be used to construct a graphical interface that shows the state of the past six epochs, as well as real-time scores and service availability. An other publication by the same writers (Chindruș and Căruntu, 2022) provides a more comprehensive explanation of the Core System design.

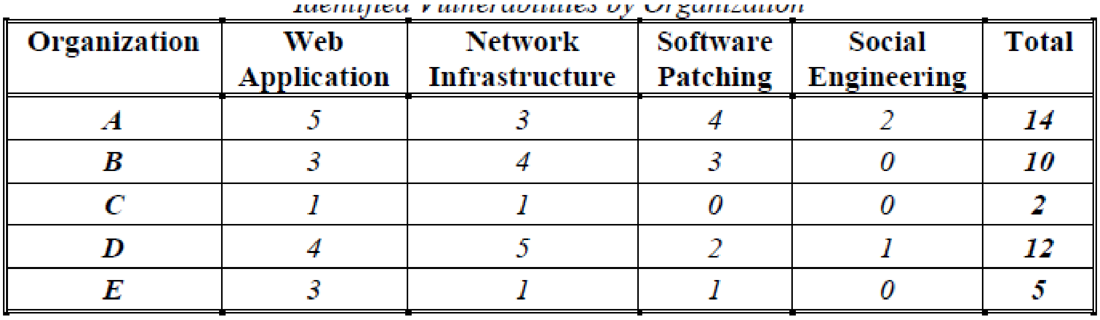
### 4.3. Results

Twenty teams, with six members each, competed in the Red and Blue team competition, making for a varied and interesting field of competitors. The tournament had three separate events and took place over the course of two days.

levels, which, as the tournament went on, revealed more difficult obstacles. Thanks in large part to the competitors' openness to the competition's fresh approach, the results were better than originally anticipated. By the end of the competition, all competitors had significantly improved their knowledge and incident reaction abilities, according to the statistical data that was gathered. The strength of the Red and Blue team competition in promoting learning and skill development among the participants is highlighted by this remark. A big element of the success was the competitors' willingness to try out the new structure of the tournament. They were able to improve their knowledge of cybersecurity principles and their ability to respond to incidents because they were open to the challenges that were given to them. A dynamic and engaging atmosphere was created by the competition structure, which allowed participants to use their academic knowledge in real-world circumstances and acquire practical skills. Table 1 provides an in-depth analysis of the vulnerabilities discovered by various firms in the Red and Blue team competition, organized in a top-five relevant findings. Web applications, network infrastructure, software patching, and social engineering are the four main categories into which vulnerabilities are classified in the table.

**Table 1**

*Identified Vulnerabilities by Organization*



Identified Vulnerabilities by Organization

| Organization | Web Application | Network Infrastructure | Software Patching | Social Engineering | Total |
|---|---|---|---|---|---|
| *A* | *5* | *3* | *4* | *2* | ***14*** |
| *B* | *3* | *4* | *3* | *0* | ***10*** |
| *C* | *1* | *1* | *0* | *0* | ***2*** |
| *D* | *4* | *5* | *2* | *1* | ***12*** |
| *E* | *3* | *1* | *1* | *0* | ***5*** |

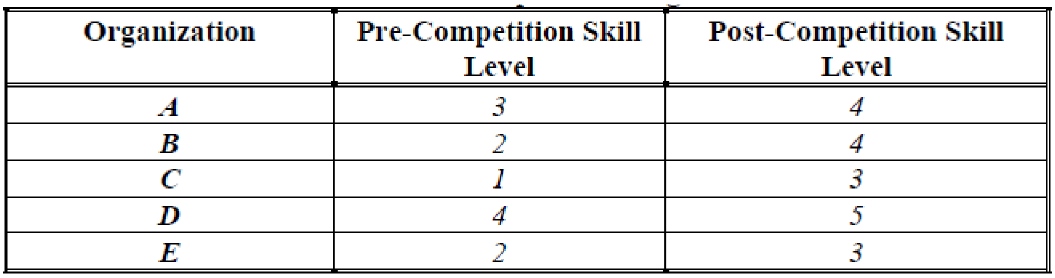
The results show that companies A and D found the most vulnerabilities overall, which might mean that their online apps and network infrastructure aren't as secure as they could be. Organization

With a focus on software patching and network infrastructure, B showed a fairly even distribution of vulnerabilities across the different categories. Companies C and E, on the other

hand, had fewer vulnerabilities overall, which may indicate that their cybersecurity protections were better in those areas.
To get a complete picture of an organization's cybersecurity posture, it is crucial to do a thorough evaluation of vulnerabilities across all dimensions, as shown in the table. Organizations may then use this information to prioritize areas that need improvement according to the vulnerabilities that have been discovered. This helps with budget allocation and implementing focused mitigation techniques. With these facts in hand, firms may fortify their cybersecurity preparedness and safeguard themselves from any dangers.
Table 2 shows how the Red and Blue team members were rated for their skill growth. More improvement in one's abilities is indicated by higher ratings, which may be anywhere from 1 to 5.

**Table 2**

*Skill Development Rating*



| Organization | Pre-Competition Skill Level | Post-Competition Skill Level |
|---|---|---|
| *A* | *3* | *4* |
| *B* | *2* | *4* |
| *C* | *1* | *3* |
| *D* | *4* | *5* |
| *E* | *2* | *3* |

## 5. Conclusion

Organizations must prioritize strengthening their cybersecurity preparedness in today's fast-paced digital ecosystem. A captivating strategy to strengthen cybersecurity has arisen: red team vs. blue team rivalry.

defenses and get businesses ready to deal with cyber attacks. Red and blue team rivalry has been discussed in this study, along with its advantages, dynamics, and potential to improve cybersecurity preparedness.
Teams participating in Red and Blue team competitions learn a great deal about their own strengths and areas for improvement via participating in realistic assault simulations. Organizations may quickly identify and mitigate cyber threats with the help of comprehensive detection and response capabilities that it allows. Additionally, the Red and Blue team competition encourages the development of skills, exchange of information, and a proactive approach when it comes to cybersecurity via its collaborative nature.
Companies may lessen the likelihood of successful cyberattacks by participating in Red and Blue team competitions, which encourage the discovery and correction of cybersecurity weaknesses. By encouraging a mindset of constant development and learning, this training approach keeps cybersecurity solutions current despite the ever-changing nature of cyber threats.
An exciting and productive way to improve cybersecurity preparedness is via red and blue

team competition. Stronger defenses, better responses to cyber disasters, and less total risk exposure may be achieved by businesses via skill development, collaborative learning, and realistic simulations. Embracing competition between Red and Blue teams is becoming more and more vital in sustaining a resilient and secure digital environment as the cybersecurity landscape keeps changing. Organizations may protect their precious assets and information from cyber attacks by using this training model.

## REFERENCES

*[1].* Andreolini M., Colacino V.G., Colajanni M., Marchetti M., *A framework for the evaluation of trainee performance in cyber range exercises*, Mobile Networks and Applications, vol. 25, pp. 236–247, 2020.

*[2].* Attiah A., Chatterjee M., Zou C.C., *A game theoretic approach to model cyber attack and defense strategies*, in International Conference on Communications, Kansas City, MO, USA, 2018, pp. 1–7.

*[3].* Bock K., Hughey G., Levin D., *King of the hill: A novel cybersecurity competition for teaching penetration testing*, in USENIX Workshop on Advances in Security Education, Baltimore, MD, 2018.

*[4].* Brilingaitė A., Bukauskas L., Juozapavičius A., *A framework for competence development and assessment in hybrid cybersecurity exercises*, Computers Security, vol. 88, p. 101607, 2020.

*[5].* Chindruș C., Căruntu C.F., *Development and Testing of a Core System for Red and Blue Scenario in Cyber Security Incidents*, 2022 15th International Conference on Security of Information and Networks (SIN), Sousse, Tunisia, 2022, pp. 1-7.

*[6].* Cheung R.S., Cohen J.P., Lo H.Z., Elia F., Carrillo-Marquez V., *Effectiveness of cybersecurity competitions*, in International Conference on Security and Management. Las Vegas, USA: The Steering Committee of The World Congress in Computer Science, 2012, p. 1.

*[7].* DeCusatis C., Bavaro J., Cannistraci T., Griffin B., Jenkins J., Ronan M., *Red-Blue team exercises for cybersecurity training during a pandemic*, in IEEE 11th Annual Computing and Communication Workshop and Conference, NV, USA, 2021, pp. 1055–1060.

*[8].* Haney J.M., Paul C.L., *Toward integrated tactical operations for Red/Blue cyber defense teams*, in Workshop on Security Information Workers at Symposium on Usable Privacy and Security, Baltimore, MD, USA, 2018.

*[9].* Karjalainen M., Kokkonen T., *Comprehensive cyber arena; the next generation cyber range*, in IEEE European Symposium on Security and Privacy Workshops, Genoa, Italy, 2020, pp. 11–16.

*[10].* Katsantonis M.N., Fouliras P., Mavridis I., *Conceptual analysis of cyber security education based on live competitions*, in IEEE Global Engineering Education Conference, Athens, Greece, 2017, pp. 771–779.

*[11].* Katsantonis M.N., Mavridis I., Gritzalis D., *Design and evaluation of cofelet-based approaches for cyber security learning and training*, Computers & Security, vol. 105, p. 102263, 2021.

*[12].* Khan M.A., Merabet A., Alkaabi S., Sayed H.E., *Game-based learning platform to enhance cybersecurity education*, Education and Information Technologies, pp. 1–25, 2022.

*[13].* 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. Cham: Springer, 2018, pp. 277–288.

*[14].* Pusey P., Gondree M., Peterson Z., *The outcomes of cybersecurity competitions and implications for underrepresented populations*, IEEE Security & Privacy, vol. 14, no. 6, pp. 90–95, 2016.

*[15].* Seker E., Ozbenli H.H., *The concept of cyber defence exercises (cdx): Planning, execution, evaluation*, in International Conference on Cyber Security and Protection of Digital Services. Glasgow, UK: IEEE, 2018, pp. 1–9.

*[16].* Shen C.C., Chiou Y.-M., Mouza C., Rutherford T., *Work-inprogress-design and evaluation of mixed reality programs for cybersecurity education*, in 7th International Conference of the Immersive Learning Research Network. Eureka, CA, USA: IEEE, 2021, pp. 1–3.

*[17].* Thomas L.J., Balders M., Countney Z., Zhong C., Yao J., Xu C., *Cybersecurity education: From beginners to advanced players in cybersecurity competitions*, in International Conference on Intelligence and Security Informatics. Shenzhen, China: IEEE, 2019, pp. 149–151.

[18]. Veerasamy N., *High-level methodology for carrying out combined Red and Blue teams*, in 2nd International Conference on Computer and Electrical Engineering, Dubai, United Arab Emirates, 2009, pp. 416–420.

[19]. Vigna G., *Teaching network security through live exercises*, in Security Education and Critical Infrastructures, C. Irvine and H. Armstrong, Eds. New York, NY: Springer US, 2003, pp. 3–18.

*[20].* Yamin M.M., Katt B., Gkioulos V., *Cyber ranges and security testbeds: Scenarios, functions, tools and architecture*, Computers Security, vol. 88, p. 101636, 2020.

*[21].* Yang P., Gao F., Zhang H., *Multi-player evolutionary game of network attack and*
[22]. *defense based on system dynamics*, Mathematics, vol. 9, no. 23, p. 3014, 2021.
*[23].* Zhang H., Jiang L., Huang S., Wang J., Zhang Y., *Attack-defense differential game*
[24]. *model for network defense strategy selection*, IEEE Access, vol. 7, pp. 50 618–
[25]. 50 629, 2018