CyberGuard: An Immersive Cybersecurity Simulation Platform

Vasu Tyagi
Student, Department of Computer Science
D.Y Patil University, Ambi
Pune, India
vasutyagi13@gmail.com

Dr. Mahantesh Kodabagi
Associate Professor, Dept. Of CE/IT, SOET
D.Y Patil University, Ambi
Pune, India
mahantesh.kodabagi@dypatiluniversitypune.edu.in

Akash Sundararaju
Student, Department of Computer Science
D.Y Patil University, Ambi
Pune, India
akashsraju@outlook.com

Siddharth Nair
Student, Department of Computer Science
D.Y Patil University, Ambi
Pune, India
nair9siddharth@gmail.com

Aditya Khera
Student, Department of Computer Science
D.Y Patil University, Ambi
Pune, India
adityakhera2002@gmail.com

***Abstract*— In today's digital landscape, cyberattacks pose a growing threat to organizations. To address this, our review informs the introduction of "CyberGuard" – an advanced training simulation software. Unlike traditional tools, it not only lets users defend against simulated threats but also provides hands-on experience in launching attacks, enhancing overall preparedness. Emphasizing real-time threat detection, "CyberGuard" equips users with the skills needed to safeguard against evolving cyber risks. Additionally, our research paper delves into the evolving malware industry, outlining traits, propagation methods, intent, and damage caused, while maintaining a central focus on the significance of "CyberGuard" in today's cybersecurity landscape.**

***Keywords*—cybersecurity, training, simulation, malware, virus, cyber defence, preparedness**

I. INTRODUCTION

With the growing rate of digital transformation, everybody's data is shifting to online platforms that are easier and more convenient to manage. While this process has its advantages, it subjects the data to a variety of risks. In the year 2022, the Indian Computer Emergency Response Team (CERT-In) handled 13,91,457 incidents. A total of 653 security alerts, 38 advisories and 488 Vulnerability Notes were issued during the year 2022 [1]. Within the Indian insurance sector, 11% of all websites faced an attack, as against the global average of 4%. Rather than distributed denial of service (DDoS) attacks like ransomware, 99% of the attacks are vulnerability attacks like probe attacks using botnets [2]. It has been well documented that the recent COVID-19 pandemic has caused several tutors to strongly recommend several virtual reality technologies to be incorporated into teaching and learning as the standard in the future [3]. As a positive response to the COVID-19 pandemic, digital technologies are being deployed such as online Virtual Learning (VL) and Remote Teaching (RT) approaches as appropriate tools [4].

II. REVIEW OF PAST WORK

We conducted a review of previously written research papers relating to simulations and training pertaining to cybersecurity. One such paper split the testing system into three different models: the physical model, the emulated model, and the simulated model. The physical model is a model whose physical features match and resemble the physical features of the modelled system. It is mostly to test the effect of attacks and evaluate protective measures without the real system getting damaged. Their biggest drawback tended to be their cost, as replicating a system can prove to be expensive [5].

The emulated models rely on virtualisation to act in the place of a real device. They provide better flexibility than physical models because they are easier, faster, and cheaper to make changes in and scale. Finally, the simulation models provide a means of examining complex interactions and changes in systems over time. The benefit of these simulation models that stood out to us was the social analysis benefits that can be extracted from the results [5].

One group of researchers from Sakarya University implemented a cyber-attack simulator a DEVS (Discrete Event System Definition) based Suite that was integrated with the BRITE topology generation tool to measure the different metrics for each attack. It is based on the DEVS approach, which is a discrete, event-based, modular, and hierarchical simulation approach. While it is the most prominent approach, it requires a high level of technical knowledge to setup and conduct these tests, making it difficult for the common man to use [6].

To better understand the value of simulating cybersecurity, we referred to Cloudshare's website. The website's glossary outlines some benefits of cybersecurity training simulators like: real-life experiences, safe testing, data insights, and organisation-wide training. It can also help create a cybersecurity culture, that helps people be more aware and prepared in case of cyber-attacks [7].

Two researchers in Korea designed a malware distribution simulator using the Mirai botnet's source code, to understand the weaknesses of IoT devices better. To create this tool, they first outlined the propagation technique of the Mirai malware with its problems. Using this information, they created the malware simulation tool to copy Mirai's effect while attempting to fix some of the problems themselves. The author's concluded the paper by stating that the tool was created only to detect and prevent network threats to IoT infrastructure. They stated that the software can later be improved upon by adding several scenarios, automating it, and further optimising it [8].

Sarah Gordon classified simulators into two categories: Simulators for Education and Tests using Simulators. The Simulators for Education referred to demonstration programs like Virlab and AVP. She implies that they raise awareness, but can mislead by providing the users with false expectations of the virus' behaviours [9].

The tests using simulators referred to Rosenthal's Virus Simulator. This simulator is no longer a live issue, but is still widely regarded as ethically and technically flawed by the research community. This classification helped us understand the differences between the two types and allowed us to realise that we wanted to help improve the educational simulation options that were available [9].

Another paper considers Cyber Ranges and security testbeds as a form of testing and educating people. The authors conducted and reviewed surveys and discovered that the Cyber Range systems are used mainly for research, training, and exercise, with 80% of participants having developed their systems to cover at least two [10].

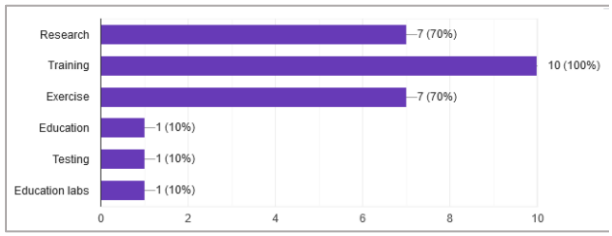

Fig 1. Objectives of Cyber Ranges

The paper also found SCADA/ICS and Read Team/Blue Team Exercises to be the focus of these Cyber Ranges [10].

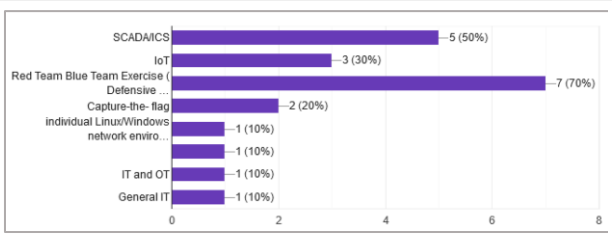

Fig 2. Domains of Cyber Range

Lastly, they also asked the participants to identify their preferred environment to conduct these tests. While the result was mostly mixed, the simulation environment had a small lead [10].

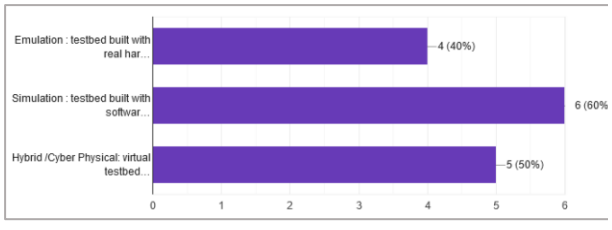

Fig 3. Types of Environment

There were also joint research efforts between maritime and engineering departments in Portugal and Malaysia to compare immersive and non-immersive simulators for education. When the team of researchers used immersive technologies like AR, VR, MR, and gamification tool they found that the participants were more engaged in the training and test scenarios. They were also able to conclude that these digital technologies allow students to include risky emergency scenarios in training, which would be impossible in a regular classroom [11].

This paper attempted to introduce an immersive cyber security platform to businesses in the hospitality sector. Since the hospitality sector can often be more vulnerable to attacks relying on human error, it is an excellent industry to act as a test subject for such an experiment [12].

The authors of this paper also felt that adding gamification elements would help address the engagement problem to maximise the effectiveness of the training. They stated that gamification can be used to play on the addictive tendencies of the human brain to increase enthusiasm and user motivation. The model they designed to combine Cyber Security Awareness and gamification is shown below [12].

Another paper conducted an experiment through a top tier

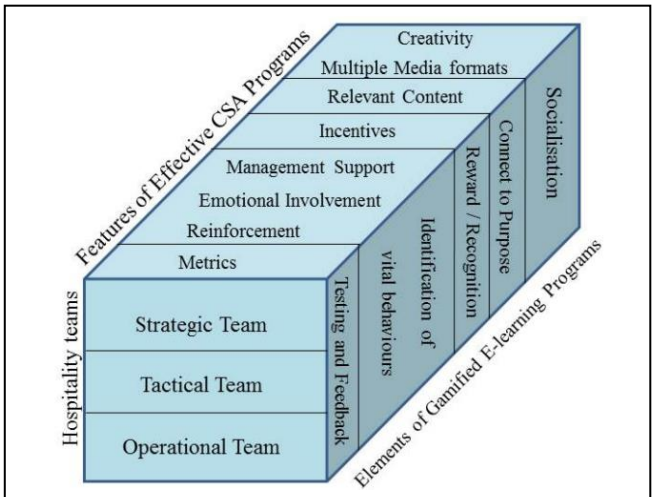

Fig 4. Aligning CSA with immersive gamification

university in the United States. It had two hundred and nine undergraduate students in a computer science program, from interdisciplinary backgrounds partake in the study. The students were assigned to four sections of a cybersecurity course. All sections had a common syllabus, professor, and textbook. The assignments and exams in were also identical.

The sections consisted of different teaching methodologies like: classroom and laboratory work, textbook quizzes, simulation challenges, competitive activities, or a combination of the above. The results of this study clearly showed that simulation noticeably improved the students' applied performances.

III. Designing CyberGuard

Using the information we learnt from the review, it was understood that one of the biggest issues that could arise in an educational software such as ours, is the user's engagement. People are often uninterested in learning topics that may seem complex, and keeping them interested in cybersecurity could prove to be a challenge.

To circumvent the issue, we used the gamification tactic used by other researchers. Adding gamified elements to the software provides a form of "reward" and can make the user

competitive, therefore keeping them engaged with the material.

CyberGuard is a piece of software designed to keep both sides of the cybersecurity equation in mind when dealing with cyberattacks. It helps provide the user with an understanding of both, the red team, and the blue team's side of an attack. This process allows the user to view both sides of the coin and use that to their advantage in a high-pressure scenario, if it ever arose.

CyberGuard is to be designed with six main menus in mind: Blue Team Training, Red Team Training, Malware Simulation/Database, Performance Analysis, an Assistant, and an Administrator Control.

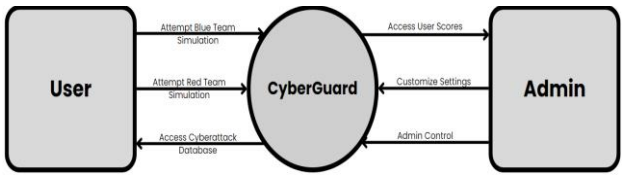

Fig 5. Level 0 DFD Diagram of Cyber Guard

A. Blue Team Training

The Blue Team Training module of the software is designed to provide the user with a hands-on experience of a cyber-attack that they will need to defend against while being guided by the software. The software will be expected to judge them on speed and accuracy.

The software will aim to provide simulation for multiple different types of attacks and will eventually also be able to test the user on identifying an attack based on the symptoms of the attacks.

Once the training/test is conducted, the software will generate the performance report for the user and provide them with feedback based on how they handled the given scenario.

B. Red Team Training

The Red Team Training module will be designed to provide the user with an insight into the mind of the attacker. Here the user will be able to understand how the attack itself takes place and how the attacker would prepare to attack.

Like the Blue Team Training module, the software will generate a performance report and give the user feedback on how they can improve depending on how the user responded to the scenario.

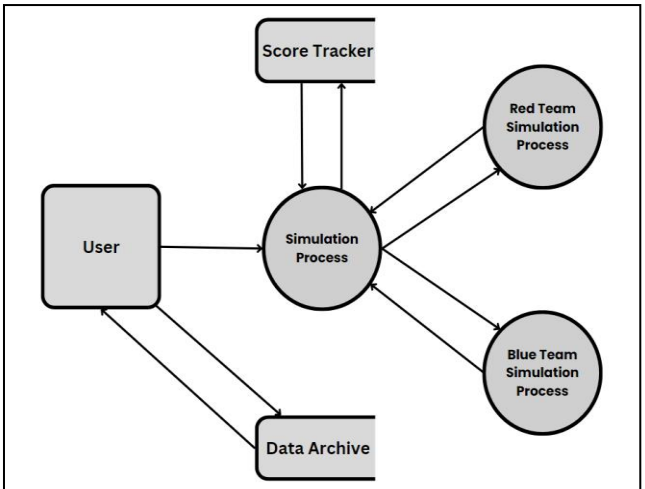

Fig 6. Level 1 DFD Diagram of Cyber Guard

C. Malware Simulation/Database

The Malware Simulation/Database will be an archive of all the different types of malware that have been included or plan to be included into the software.

Here the user will be able to view the symptoms of each malware, as well as read up information on the malware itself. This module of the software act as a library to the users, in case they want to or feel the need to learn about these types of viruses.

To provide this database of malware, we did conducted research into the evolution of malware so that the user can understand how malwares have evolved since the beginning.

Malware refers to malicious software. This usually refers to a type of software that is designed to cause damage to a computer, server, or network. Ever since their appearance, they have evolved to spread through all possible modes of data transfer. Malware is often used to access sensitive information, exploit it for financial gain, slow down the system, or put an end to the system.

While the term malware usually refers to harmful software, the initial forms of malware were not designed to harm systems in any way, shape, or form. These were just created to prove that such programs could exist and spread as quickly as they do. Present-day malware has grown into harmful software like ransomware, and is often used to exploit people financially.

Early malware existed in the form of worms. They were given the name "worm" as their main purpose is to just replicate themselves and "wiggle" their way through systems and access as many systems as possible. Worms are generally used to propagate other malware and gain access to systems.

Another form of malware that appeared in the early stages of evolution was the Trojan. A Trojan is a type of malware that presents itself as a legitimate program while carrying a malicious payload. This is why the term "Trojan" is used as an umbrella term to describe a method of malware delivery. They can be referred to as "the Swiss Army knife of hacking" since they are multi-purpose and can be used in a flexible way to fit our purpose.

Eventually a type of malware called keyloggers were created to steal personal or financial information. These malware are used to record input, often from keyboards, to record information like usernames, passwords, bank account

numbers or credit or debit card numbers. Keyloggers exist in the forms of hardware and software keyloggers, such that they can be installed as a program or plugged in as external hardware.

Keyloggers are a part of a larger type of malware referred to as spyware. Spyware is a category of malware that installs itself onto a system and monitors the behaviour, often online behaviour, of the user of the system. They can give the attacker access to the features that the user's system provides to the user.

Rootkits are a type of more complex but significantly more harmful type of malware. They allow for the attacker to have remote access to the victim's computer. These malware are used to slow down systems and gain administrative access to those infected systems, while hiding the malware's existence. They provide a form of privilege escalation to the attacker.

One of the most well known forms of malware in the present-day era is ransomware. Ransomware is a class of malware that encrypts the data on the victim's system once it is triggered. Once the data is encrypted, the malware prevents use of the system until a sum of money is paid to the attacker. Once the attacker receives the money, they may provide the user with their decryption key to unlock the system or continue to harass the victim.

A less harmful form of malware is adware. Adware exists to cause pop-ups of unwanted ads. These ads slow down the computer system that they infect. These ads usually link to malicious web pages that install malware themselves or act as a form of social engineering to get the victim to install malware onto their system themselves.

We can broadly divide malware into four phases: Early File and Boot Sector Infectors (Pre - 1990), Email-based and Network Worms (1990s - Early 2000s), Advanced Malware and Exploits (Mid 2000s - Late 2000s) and Ransomware and IoT malware (2010s- Present).

The first phase refers to the birth of malware and its discovery. These malwares were primitive and lacked any methods to hide themselves. These malwares could almost exclusively be transferred through infected hardware.

The second phase of malware shows a major improvement in malware technology. This new generation of malware can travel through networks and start to show a level of encryption.

In the third phase, we see a few incredibly advanced malwares that gained a large boost in destructive strength. These malwares also showed a level of restraint never seen before.

The fourth and final phase of malware refers to the modern level of malware. These modern malwares show more of a focus on ransomware.

1) Phase One

Before the existence of malware, a man named Bob Thomas wrote a self-replicating computer program in 1971 that was designed to copy itself between systems. This program was termed "Creeper". Creeper was considered to be the first ever computer worm. It was not designed to be a damaging program, but was created to test the possibility of a self-replicating program spread to different computers.

The malware was countered with the "Reaper" antivirus, made a year later in 1972 by Ray Tomlinson. The Reaper also made its way through the ARPANET and was created with the purpose of deleting Creeper.

The first ever fork bomb, Rabbit or Wabbit was created in 1974. This was one of the first intentionally bad malware. It was created to slow down the systems by replicating itself within the system itself, until the system was clogged and overworked.

In 1975, The first ever trojan, ANIMAL, was created. The program would depict itself as one of the then ongoing trends of being an animal guessing game. While the victim would play this guessing game, the program would attempt to spread by infecting uninfected directories.

One of the first malware for the Apple systems was created by Rich Skrenta, a 15-year-old high school student as a prank to annoy his fellow classmates. Elk Cloner would disguise itself as a game, and on the fiftieth time the game was booted, the system would show a blank screen instead, with a short poem about the virus:

ELK CLONER:
THE PROGRAM WITH A PERSONALITY
IT WILL GET ON ALL YOUR DISKS
IT WILL INFILTRATE YOUR CHIPS
YES, IT'S CLONER!
IT WILL STICK TO YOU LIKE GLUE,
IT WILL MODIFY RAM TOO
SEND IN THE CLONER!

Elk Cloner did not cause deliberate harm but Apple DOS tracks without a standard image had their reserved tracks overwritten. The malware infected the Apple II systems and was never patched for the Apple II DOS. The release of Apple III was the only counter to it if the user could not rewrite the DOS onto the infected list.

In January 1986, two Pakistani brothers, Amjad Farooq Alvi and Basit Farooq Alvi, released the Brain virus to the world. This malware was created to protect their heart monitoring program from copyright infringement. Brain was used to infect IBM systems and would replace the boot sector of a floppy with a copy of the virus. Kaspersky was able to release an antivirus for Brain.

Jerusalem was a virus first discovered in October 1987. It was a logic bomb DOS virus set to trigger on Friday 13th except in 1987. Once activated it would delete any executable file run that day and also increase the size of .exe files until they grow too large for the computer. This version of the virus was isolated to Jerusalem but a large number of variants were created after. The malware could be removed with Dr. Solomon's Antivirus Tool.

Another malware well known for its large number of variants is the Vienna virus. The Vienna virus was designed to damage files, and would damage .com files by replacing the first five bytes with the hex character string "EAF0FF00F0", causing the system to warm reboot when the infected file is run. Detection of the malware was easy as all infected files had an impossible value of 62 in the seconds part of the timestamp.

Malware made a jump in technology when the Cascade virus was discovered in 1987, as it was the first well known malware to use an encryption algorithm to hide itself. It would infect .com files and had the effect of making text on the screen fall and form a heap at the bottom. The infected

files would also have an increased size. In response to the malware, IBM developed its own antivirus software.

In November 1987, a malware referred to as the SCA virus was discovered. This malware was designed for Amiga systems. It was a boot sector virus that featured a line of text at every 15th copy after a warm reboot: Something wonderful has happened, Your AMIGA is alive !!! and, even better... Some of your disks are infected by a VIRUS!!! Another masterpiece of The Mega-Mighty SCA!!

The SCA virus will not harm disks per se but did spread to write enabled floppies. If they used custom bootblocks, they were rendered unusable. It would also end up destroying newer file systems if the user did not know how to remove SCA using the install command. The Swiss Cracking Association produced the first Amiga virus checker to combat the virus.

In the end of 1987, a computer worm referred to as Christmas Tree EXEC was discovered. It was the first computer worm to cause large scale disruptions. It drew a crude christmas tree as text graphics and then forwarded itself to each entry on the victim's email contacts file. It managed to spread into the European Academic Research Network, BITNET, and IBM's VNET and caused very powerful disruptions. It was dealt with by shutting down the networks for a short amount of time.

CyberAIDS and Festering Hate are two of the first Apple ProDOS viruses. CyberAIDS affected legitimate users in 1987 and its variants culminated in the form of Festering Hate in 1988. Festering Hate would infect all available files in an attempt to destroy them. The detonation page also had the home number of John Maxfield, a well-known FBI informant specialising in cybersecurity.

The Morris worm was released on November 2, 1988. It was the first computer worm to gain significant mainstream media attention. It also resulted in the first felony conviction in the US under the 1986 Computer Fraud and Abuse Act. It was created by a graduate from Cornell named Robert Tappan Morris. While the worm was meant to be created to highlight the weaknesses in networks at the time, it ended up doing a large, but unintentional amount of damage. The author initially programmed the worm to check for infection status, but thought that system administrators would counter it by reporting false positives. Instead, he programmed the worm to spread 14 percent of the time, regardless of infection status. This ended up in systems being infected multiple times, causing those systems to slow down until they were no longer usable.

In 1989 the AIDS Trojan was discovered. It replaces the AUTOEXEC.BAT to start the boot count. Once this count reaches 90, the malware hides directories and encrypts the names of all files on C: drive. The victim is then asked to renew their licence and contact PC Cyborg Corporation. It also presented the victim with an end user licence agreement:

> If you install [this] on a microcomputer...
>
> then under terms of this license you agree to pay PC Cyborg Corporation in full for the cost of leasing these programs...
>
> In the case of your breach of this license agreement, PC Cyborg reserves the right to take legal action necessary to recover any outstanding debts payable to PC Cyborg Corporation and to use program mechanisms to ensure termination of your use...
>
> These program mechanisms will adversely affect other program applications...
>
> You are hereby advised of the most serious consequences of your failure to abide by the terms of this license agreement; your conscience may haunt you for the rest of your life...
>
> and your [PC] will stop functioning normally...
>
> You are strictly prohibited from sharing [this product] with others...

It was countered by the program AIDSOUT for removal and CLEARAID for decryption

In February 1991, the Michelangelo virus was discovered. Like all other boot sector viruses, the Michelangelo virus operated at the BIOS level. The virus was activated on March 6th of every year. If the PC in AT or PS/2 the virus overwrites the first 100 sectors of the hard disk with nulls. Even though it was designed to affect DOS systems, it can easily disrupt other operating systems installed on the system, as it infects the master boot record of the hard drive. For many years users were advised not to boot their system on March 6th. The virus became irrelevant as the DOS systems were no longer used.

2) Phase Two

In phase two we see malware grow in complexity. The newer malware also has a greater spread as they use email and networks to propagate themselves more easily.

The CIH virus is the first virus to have such a large impact in the second phase. It was written by a student at Tatung University in Taiwan, named Chen Ing-hau. The author claimed to have written the virus as a challenge against claims of antivirus efficiency by antivirus software developers. The payload overwrote the first megabyte of the hard drive with zeros. This deletes the content of the partition table and causes the machine to hang or cue the blue screen of death. The virus was countered by the author themselves who released an antivirus after a public apology.

In January 1999, a computer worm for Microsoft Windows was discovered. It was called Happy99. It used to spread email and usenet. It installed itselves and ran in the background of the victim machine. It does no damage to the computer, other than modifying Winsock to allow itself to spread. It also stored a list of spammed newsgroups and mail addresses on the infected hard drive.

The Melissa virus was discovered in March 1999. It is a macro virus targeting Microsoft Word and Outlook. It infects computers by email. The email reads "Here's that document you asked for. Don't show anyone else ;)." Alongside the email a word document is attached titled 'list.doc' containing a list of pornographic sites and login for each. It then mass-mails to the first 50 people in the user's contact list. The virus significantly slowed down email systems. The virus was removed by the Computer Emergency Response Team.

The discovery of the ILOVEYOU worm, sometimes referred to as the Love Bug, took place in May 2001. At the time, it was the fastest spreading computer worm, as it infected ten million Windows personal computers after its release. It spread using an email with the attachment "LOVE-LETTER-FOR-YOU.TXT.vbs". At the time windows did not show the.vbs extension, leading the victim to believe that the file is a text file. Opening the files runs the Visual Basic Script and damages files, overwrites random files, and hides MP3

files and then copies itself to all addresses in the Windows Address Book. Microsoft then issued a security patch preventing code from running when opening an email attachment.

The Sadmind and Code Red worms both exploited bugs in the Microsoft IIS web server. They both left backdoors that could be used after the attacks were complete.

These backdoors were exploited by a computer worm known as Nimda. It was able to affect workstations running any version of Windows from 95 to XP. It was incredibly effective since it used 5 different infection vectors, namely: email, open network shares, compromised websites, exploitation of various Internet Information Services directory traversal vulnerabilities, and backdoors left by the "Code Red II" and "sadmind" worms.

In the end of the second phase, we saw the SQL Slammer worm in 2003. The SQL Slammer worm exploited a buffer overflow bug in Microsoft's SQL Server and Desktop Engine database products. There was a patch for the bug released six months prior, but multiple organisations had not yet applied it. It generates random IP addresses and sends itself out to those addresses, and if the host of one of the addresses is running an unpatched copy of the Microsoft SQL Server Resolution Service on UDP port 1434, the host is now infected and spreading more to the internet.

3) Phase Three

On January 26, the computer worm "mydoom" was released on the internet. As of 2023, it is still the fastest spreading computer worm. It uses junk email as its method of propagation, with the text message "[name]; I'm just doing my job, nothing personal, sorry,". It had an attachment that, when executed, sends the worm to email addresses in the victim's address book. It avoided targeting email addresses at universities like Rutgers, MIT, Stanford, and UC Berkeley, as well as companies such as Microsoft and Symantec. The original version had two payloads: the first being a backdoor on port 3127/tcp to allow remote control, and the second being a denial-of-service attack against the website of the SCO group time to go off on 1st February. The second version also targeted Microsoft and blocked access to over 60 antivirus sites.

Although the attack was supposed to begin on 1 February 2004 SCO groups website went offline briefly soon after the worm was released. On 1 February SCO removed www.sco.com from the DNS at 1700 UTC on 31 January. To counter the worm Microsoft released the security patch, major antivirus programs were able to detect it and manual deletion of the infected files was recommended.

Santy was discovered in December 2004 and was the first ever webworm. It was created in Perl and exploited a vulnerability in phpBB. It attacked about 40000 websites within the first 24 hours. It caused .php and .html files on infected servers to display the message "This site is defaced!!! This site is defaced!!! NeverEverNoSanity WebWorm generation X". To combat the malware Google Blocked its search queries and anti-Santy anti-worm was released to try patch vulnerabilities.

In January 2007 private computers in Europe and the United State received an email with a subject stating "230 dead as storm batters Europe". Once the attachment is opened the malware installs wincom32 and injects the payload passing packets to destination encoded within the malware. It may also try to download and install a trojan. Machines running Windows 2000, XP and Vista were affected. The infected machine becomes part of a botnet with a peer-to-peer control setup. It also installs the rootkit Win32.agent.dh. This worm has no counter for infected machines but an antivirus can prevent its attack.

Conficker is a worm discovered in November 2008. It exploited a vulnerability in a network service on Windows 2000, XP and Vista, and Windows Server 2003, 2008 and 2008 R2 Beta. It later was able to propagate over LANs through removable media and network shares. Conficker also blocked some popular antivirus websites.

4) Phase Four

In the fourth phase we see malware become significantly more powerful as they start to use IoT devices to propagate themselves further. There is also a sudden increase in the use of ransomware.

January 2009 sees the discovery of the computer worm psyb0t. Psyb0t is a computer worm that infects even routers and high-speed modems. It targeted modems and routers with processors running Mipsel Linux firmware. Once infected, the routers could no longer access ports 22, 23 and 80. Psyb0t was able to use about 100000 devices to perform a distributed denial-of-service attack against DroneBL, a service to blacklist IPs. It used brute force attacks to gain access. The recommended countermeasures were to update credentials and firmware. In case of infection, it was recommended to perform a hard reset.

Stuxnet is a very complex and advanced computer worm discovered in 2010. It was made up of 3 components: the main payload, a link file to execute the propagated copies in sync, and a rootkit to hide the files, to prevent detection. It was used to perform an attack on the SCADA systems in Iran's nuclear facilities. Iran lost almost one-fifth of their nuclear centrifuges due to the attack.

ZeroAccess is a combination of a trojan, botnet and rootkit. The malware propagates itself through forms of social engineering, advertising networks and third-party people installing the rootkit. It performed 2 main functions: bitcoin mining or click fraud. It was estimated to have made 2.7 million USD per year in September 2012. ZeroAccess also removed Tidserv malware if it was present. TDSS killer and other antivirus applications received updates to counter it.

Flame is a type of malware that is used for targeted cyber espionage in Middle Eastern countries. It was discovered in 2012. It can spread over LAN, record audio, screenshot, keyboard activity, network traffic, Skype conversations and can convert infected systems into Bluetooth beacons to download contact information from nearby devices. It has an inbuilt kill switch to delete itself.

Cryptolocker in one of the first major ransomware attacks made. It affected Windows machines. It was discovered in 2012 and ran rampant till mid-2014. It spread using email attachments, using the Gameover ZeuS botnet. It was finally isolated in May2014 and the botnet used to spread it was taken down by Operation Tovar, an international joint venture. The list of keys used by CryptoLocker was used to build a tool to retrieve the encrypted data for free.

As security improved, malware got increasingly powerful, resulting in Regin. Regin is a hacking toolkit used by the US National Security Agency (NSA) and its British counterpart, the GCHQ. While it was first discovered in 2012, there are samples that date from 2003.

BashLite is a malware written in C, so that it can be cross-compiled easily. It infects Linux systems to launch distributed denial-of-service attacks. It holds open TCP connections, and uses a client-server model for command and control. It propagated via brute forcing, and used a built-in dictionary of common usernames and passwords.

Pegasus spyware was first developed in 2011 by the NSO group to assist government combat terror and crime. In 2016 an iOS exploitation was discovered by the Citizen Lab in the University of Toronto. As of 2022 Pegasus can read texts, track calls, collect passwords, track location, access the mobile microphone and camera.

WannaCry is a massive ransomware attack that took place in May 2017. It used the EternalBlue exploit developed by the US National Security Agency. The initial attack was stopped within 8 hours of its release by Marcus Hutchins. He discovered a kill switch domain hardcoded in the malware. Once the domain name was registered, the attack stopped spreading but did not affect the infected systems. Eventually a PayBreak system was developed that could defeat WannaCry and several similar families.

Since the development of WannaCry there have been few ransomwares like Petya and Ryuk but no major jumps in terms of strength of malware.

D. Performance Analysis

The performance analysis module will be expected to provide the user with their performance reports from all the training simulations and tests they have undergone.

This module will calculate a score based on given metrics like speed, accuracy, and ability to identify the virus. Using these metrics, the software will grade the user's performance and provide them with the result, as well as overall feedback for them to work on and practice.

E. Assisstant

The assistant designed for CyberGuard will be a Large Language Model (LLM) trained using a detailed documentation of the working of CyberGuard. It will be able to answer any queries the user may have about using the software.

In the case of it being unable to answer, it will save the question and forward it to technical support so that they may deal with the issue, and mark that question as a gap in the LLM's knowledge.

F. Administrator Control

The Administrator Control panel will be designed to provide the management and service providers access to the working of the software. It will allow them to review the performance records of various users as well as change the difficulty of the various exercises.

It will also allow for modification of the malware database to allow the managers to decide what tests the employees can give or to add more tests if they feel the need to do so.

IV. Conclusion and Future Work

To conclude, we can say that since COVID-19 educating people using technology and immersive methods has become much more prominent and effective. Using the reviews of past works, we were able to determine that simulation is often the easier and cheaper option when trying to replicate a scenario.

While simulation may be the more successful way to educate and engage people with the study material, it may result in the gamified elements overtaking the actual educational material in the software. We can also state that the simulation software needs to be correct and constantly updated as the world of cybersecurity keeps changing, and an outdated software can result in the users' being led astray.

V. Acknowledgement

We would like to express our sincere gratitude to Dr. Mahantesh Kodabagi, Dr. Moresh Mukhedkar, and Prof. Malayaj Kumar for their invaluable guidance and support throughout the development of the project and research paper on "CyberGuard: An Immersive Cybersecurity Simulation Platform." Their collective expertise, mentorship, and insights have been instrumental in shaping the direction, scope, and quality of this endeavor.

Their unwavering commitment to fostering innovation and academic excellence has created a conducive environment for exploration, critical thinking, and growth in the realm of cybersecurity simulation. Their constructive feedback, profound knowledge, and encouragement have enriched the project, ensuring its relevance, impact, and contribution to the field.

In conclusion, we extend our heartfelt appreciation to Dr. Mahantesh Kodabagi, Dr. Moresh Mukhedkar, and Prof. Malayaj Kumar for their exceptional mentorship, guidance, and support. Their contributions have been pivotal in the successful execution and completion of this project, and we are profoundly grateful for the opportunity to learn and collaborate with such esteemed professionals in the cybersecurity domain.

VI. References

[1] Hamdi Kavak, Jose J. Padilla, Daniele Vernon-Bido, Saikou Y. Diallo, Ross Gore, Sachin Shetty, "Simulation for cybersecurity: state of the art and future directions," Journal of Cybersecurity, Volume 7, Issue 1, 2021.

[2] S. Kara, S. Hizal, and A. Zengin, "Design and Implementation of a Devs-Based Cyber-Attack Simulator for Cyber Security," International Journal of Simulation Modelling, Volume 21, Number 1, March 2022.

[3] "Cyber Security Simulation Training." Cloudshare. Accessed: Sep. 3, 2023.

[4] Song-Yi Hwang and Jeong-Nyeo Kim, "A Malware Distribution Simulator for the Verification of Network Threat Prevention Tools," Sensors 2021, 21(21), 6983.

[5] David Harley, Lysa Myers, Eddy Willems, "Test Files and Product Evaluation: the Case for and against Malware Simulation," AVAR (Association of Anti-Virus Asia Researchers 13th Conference, November 2010.

[6] Holdsworth, J., & Apeh, E. (2017). "An Effective Immersive Cyber Security Awareness Learning Platform for Businesses in the Hospitality Sector." In 2017 IEEE 25th International Requirements Engineering Conference Workshops (REW) (pp. 111-117). IEEE. doi: 10.1109/REW.2017.47

[7] Chouliaras, N., Kittes, G., Kantzavelou, I., Maglaras, L., Pantziou, G., & Ferrag, M. A. (2021). "Cyber Ranges and TestBeds for Education, Training, and Research." Applied Sciences, 11(4), 1809. https://doi.org/10.3390/app11041809

[8] Dewan, M. H., Godina, R., Chowdhury, M. R. K., Noor, C. W. M., Wan Nik, W. M. N., & Man, M. (2023). "Immersive and Non-Immersive Simulators for the Education and Training in Maritime Domain—A Review." Journal of Marine Science and Engineering, 11(1), 147. https://doi.org/10.3390/jmse11010147

[9] Workman, M. D. (2021). "An Exploratory Study of Mode Efficacy in Cybersecurity Training." Journal of Cybersecurity Education, Research and Practice, Volume 2021, Number 1, Article 2, July 2021. Available at: https://digitalcommons.kennesaw.edu/jcerp/vol2021/iss1/2

[10] Jaber, A., & Fritsch, L. (2023). "Towards AI-powered Cybersecurity Attack Modeling with Simulation Tools: Review of Attack Simulators." In L. Barolli (Ed.), Advances on P2P, Parallel, Grid, Cloud and Internet Computing. 3PGCIC 2022. Lecture Notes in Networks and Systems (Vol. 571). Springer, Cham. https://doi.org/10.1007/978-3-031-19945-5_25

[11] Veksler Vladislav D., Buchler Norbou, Hoffman Blaine E., Cassenti Daniel N., Sample Char, Sugrim Shridat. "Simulations in Cyber-Security: A Review of Cognitive Modeling of Network Attackers, Defenders, and Users." Frontiers in Psychology, vol. 9, 2018. ISSN: 1664-1078. DOI: 10.3389/fpsyg.2018.00691. URL: https://www.frontiersin.org/articles/10.3389/fpsyg.2018.00691.

[12] Indian Computer Emergency Response Team (CERT-In), Ministry of Electronics & Information Technology (MeitY), Government of India, "Annual Report 2022."

[13] The Economic Times, May 09, 2023, "India sees sharp increase in cyberattacks in Q1 2023: report," [Online]. Available: https://economictimes.indiatimes.com/tech/technology/sharp-increase-in-cyberattacks-in-india-in-q1-2023-report/articleshow/100096450.cms

[14] B. Shambare and C. Simuja, "A Critical Review of Teaching with Virtual Lab: A Panacea to Challenges of Conducting Practical Experiments in Science Subjects Beyond the COVID-19 Pandemic in Rural Schools in South Africa," J. Educ. Technol. Syst., vol. 50, pp. 393–408, 2022.

[15] B. Anthony Jr. and S. Noel, "Examining the adoption of emergency remote teaching and virtual learning during and after COVID-19 pandemic," Int. J. Educ. Manag., vol. 35, pp. 1136–1150, 2021.

[16] H. Kavak et al., "Simulation for cybersecurity: state of the art and future directions," Journal of Cybersecurity, vol. 7, no. 1, pp. tyab005, 2021.

[17] S. Kara, S. Hizal, and A. Zengin, "Design and Implementation of a Devs-Based Cyber-Attack Simulator for Cyber Security," Int. J. Simulation Modelling, vol. 21, no. 1, March 2022.

[18] "Cyber Security Simulation Training." Cloudshare. [Online]. Available: https://www.cloudshare.com/ virtual-it-labs-glossary/cyber-security-simulation-training/ Accessed: Sep. 3, 2023.

[19] S.-Y. Hwang and J.-N. Kim, "A Malware Distribution Simulator for the Verification of Network Threat Prevention Tools," Sensors, vol. 21, no. 21, pp. 6983, 2021.

[20] S. Gordon, "Are Good Virus Simulators Still a Bad Idea?," Elsevier Advanced Technology, 1995.

[21] N. Chouliaras et al., "Cyber Ranges and TestBeds for Education, Training, and Research," Appl. Sci., vol. 11, no. 4, p. 1809, 2021.

[22] M. H. Dewan et al., "Immersive and Non-Immersive Simulators for the Education and Training in Maritime Domain—A Review," J. Marine Sci. Eng., vol. 11, no. 1, p. 147, 2023.

[23] J. Holdsworth and E. Apeh, "An Effective Immersive Cyber Security Awareness Learning Platform for Businesses in the Hospitality Sector," 2017 IEEE 25th International Requirements Engineering Conference Workshops (REW), Lisbon, Portugal, 2017, pp. 111-117, doi: 10.1109/REW.2017.47.

[24] M. D. Workman, "An exploratory study of mode efficacy in cybersecurity training," Journal of Cybersecurity Education, Research and Practice, vol. 2021, no. 1, Article 2. [Online]. Available: https://digitalcommons.kennesaw.edu/jcerp/vol2021/iss1/2

[25] J. Metcalf, "Core War: Creeper & Reaper."

[26] T. Chen and J.-M. Robert, "The Evolution of Viruses and Worms," 2004.

[27] E. S. Raymond, "wabbit," October 1, 2004.

[28] "Prank starts 25 years of computer security woes," CTV, Associated Press.

[29] "First virus hatched as a practical joke," The Sydney Morning Herald.

[30] "Brain - the first PC virus in the wild," [Online]. Available: https://www.f-secure.com/v-descs/brain.shtml

[31] "Virus Distribution Strategies," IBM, [Online]. Available: https://web.archive.org/web/20010211122852/http://www.research.ibm.com/antivirus/SciPapers/White/VB95/vb95.distrib-node10.html

[32] J. Maher, "The Scene," The Future Was Here: The Commodore Amiga, MIT Press.

[33] T. Scott, "A Christmas Computer Bug, and the Future of Files" (video).

[34] "Cascade," [Online]. Available: https://www.f-secure.com/v-descs/cascade.shtml

[35] D. A. Lyons, "CyberAIDS warning--a real virus (Weishaar)," July 24, 1988.

[36] "The Morris Worm Turns 30," Global Knowledge Blog.

[37] E. Spafford, "An analysis of the worm," December 8, 1988.

[38] "The Computer Virus That Haunted Early AIDS Researchers," The Atlantic.

[39] J. Bates, "High Level-Programs & the AIDS Trojan," In: Wilding E, Skulason F (eds) Virus Bulletin.

[40] "CERT Advisory CA-1992-02," [Online]. Available: http://www.cert.org/advisories/CA-1992-02.html

[41] "Virus: W32/Melissa Description | F-Secure Labs," [Online]. Available: https://www.f-secure.com/v-descs/melissa.shtml

[42] "Melissa Virus," Federal Bureau of Investigation.

[43] "What is the ILOVEYOU worm, what does it do, and how do I detect and remove it?," University Information Technology Services.

[44] "Information about the Network Worm "Nimda"," Kaspersky Lab, Kaspersky.com.

[45] "SQLExp SQL Server Worm Analysis," DeepSight™ Threat Management System Threat Analysis.

[46] "Psyb0t Evolves, Targets Unprotected Linux Mipsel Routers," OStatic.

[47] "The ZeroAccess Botnet: Mining and Fraud for Massive Financial Gain," Sophos.

[48] "Flamer: Highly Sophisticated and Discreet Threat Targets the Middle East," Symantec.

[49] "sKyWIper: A Complex Malware for Targeted Attacks," Budapest University of Technology and Economics.

[50] "'Operation Tovar' Targets 'Gameover' ZeuS Botnet, CryptoLocker Scourge," Krebs on Security.

[51] "Regin White Paper," Symantec.

[52] "Experts Unmask 'Regin' Trojan as NSA Tool," Spiegel.de.

[53] "First attacks using shellshock Bash bug discovered," ZDNet.

[54] "BASHLITE Malware Uses ShellShock to Hijack Devices Running BusyBox," SecurityWeek.com.

[55] "Technical Analysis of Pegasus Spyware," Lookou