IV. International Conference on Electrical, Computer and Energy Technologies (ICECET 2024)
25-27 July 2024, Sydney-Australia

Optimising IT security research via a low cost, instantly available, cloud based cyber range

1st Patrick Wake
Durham University
Durham, UK
patrick.d.wake@durham.ac.uk

2nd Sue Black
Durham University
Durham, UK
sue.black@durham.ac.uk

3rd Jonathan Young
Durham University
Durham, UK
jonathan.p.young@durham.ac.uk

***Abstract*—For enterprise, companies and institutions, testing the effectiveness of IT security measures can be costly. Time and effort costs are added to the infrastructure fees associated with creating a cyber range. Enterprises' only viable alternative to simulation is to test the IT security measures on a live production environment, where the costs saved in simulation are replaced by the unthinkable potential costs of getting it wrong and being hacked or losing data.**

Similarly, academics researching IT security can spend as much time preparing their test environment as they do on the actual experiment they want to conduct, whilst always running the risk that researcher A's environment is materially different to researcher B's.

Here we present a blueprint for a cyber range which replicates the IT estate of a small and medium sized enterprise (SME) which has been protected with the security provisions stipulated by the Cyber Essentials standard. As many instances of the cyber range as enterprise or a researcher requires can be created at will in seconds in the cloud, freeing them up to concentrate on experimentation in a repeatable environment.

It is our intention that the blue print will be made available and kept updated by the research community.

***Index Terms*—Cyber Range, Security Standards, Cyber Essentials, Hacking**

I. Introduction

There is a serious digital threat to organisations of cyber incidents [2], or "hacking" [20], which cause business disruptions and data loss, leading to trust issues and financial losses [8] [9]. Fines for data breaches can cost up to hundreds of millions of pounds [10].

Besides hacking, organizations also deal with phishing, code exploitation, and ransomware [5] [6] [14]. Globally, cybercriminals steal $600 billion per year from governments, companies and individuals, over the course of five years, from 2019 to 2023, will reach $5.2 trillion [13] [1].

To combat these threats, the cybersecurity industry has grown, reaching £10.5 billion in the UK by 2023 [4]. It was estimated that approximately 2.39 million cases of cyber crimes affected UK businesses between April 2022 and April 2023 [3]. This has led the UK government to lead multiple advisory, government organisations and frameworks such as Cyber Essentials to advise SMEs and other organisations to better protect themselves[11]. Organisations wishing to investigate or test their IT security preparedness or posture, and researchers in IT security benefit greatly from having access to a 'like live' environment or model of an organisation on which to simulate real life threats and IT security provisions

A cyber range is a virtualised platform which provides a dedicated testbed allowing for a comprehensive and unbiased assessment. Typically containing multiple types of infrastructure, networks and computers, this enables security testing to be conducted in a real-world cyber threat scenario

Previous research on cyber ranges has been towards gaining a better understanding in attacking and defensive skills [24] [16]. Whilst there are multiple cyber range designs that are used for cyber exercises worldwide [25] [24], thus far there has been no research in the use of a cyber ranges to review security standards, or one that has been created that aligns to Cyber Essentials.

Cyber ranges have matured over time [24] [16], but there are still improvements that can be made [21]. Previous research has shown that cyber ranges are typically expensive, time-consuming to construct and difficult to deploy and maintain [7]. Urias *et al* wrote that previous cyber ranges used older technologies and suffered from slower networks and from licensing issues. This led to slow deployments which lacked automation [21].

In general, a cyber range should be able to provide [21]:

1) Real-time feedback with high-fidelity simulation.
2) An environment where teams can engage to support the range experiment.
3) An environment where hypotheses may be tested by various teams.
4) Performance-based assessment metrics and data.

In this work, we propose an novel approach to improve on previous designs by modernising credential management and configuration management, as well as create the first cyber range of its kind, hardened and aligned to the Cyber Essentials framework, focusing on improving automation, repeatability and robustness.

II. Design

In this section, we describe the design and the topology used to allow for repeatable results with maximum scalability, ease of maintenance and security within a strict budget. The cyber range has been built using public cloud infrastructure. With minimal administrative overheads managing the infrastructure provides greater ease in ensuring the environment is compliant to Cyber Essentials[23].

With these key considerations the following public clouds were considered:

- Microsoft Azure
- Google Cloud Platform
- Amazon Web Services
- Skytap
- SnapLabs by Immersive Labs

Due to the key requirement of repeatability and ease of use from a maintenance and portal access perspective, Skytap was chosen to host the environment as it simply requires a browser to access and administer the environment allowing all parties to focus on using and testing the cyber range, rather than administering it an the wider cloud environment (an example can be seen in Figure 1).

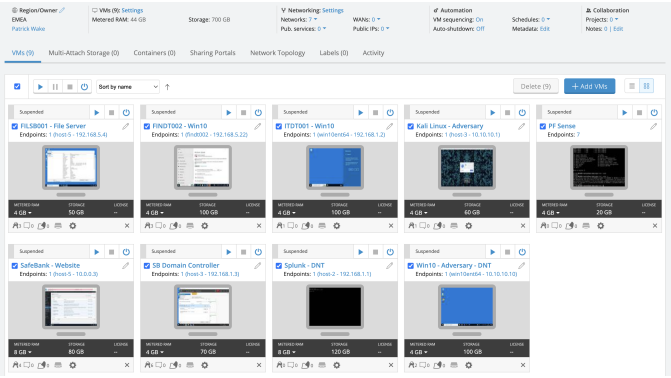


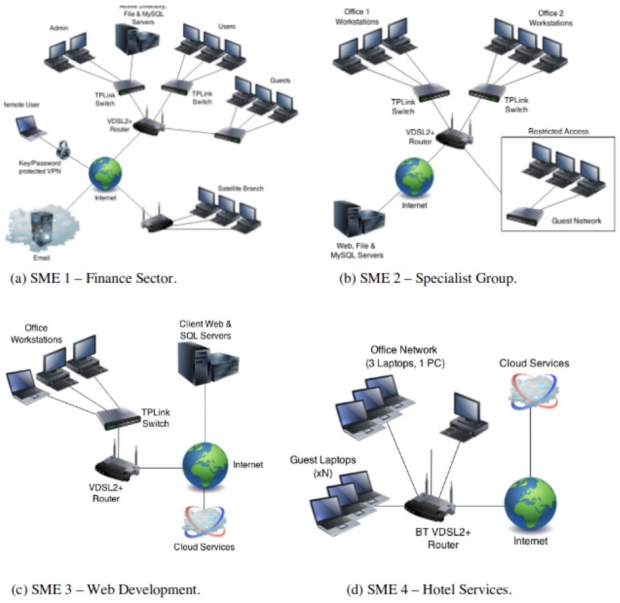
Figure 1: Skytap VMs

Using the following peer reviewed topology designs based on surveys of 20 Small to Medium Enterprises [18] Figure 2, I have selected ”SME1” to base the cyber range environment shown in Figure 3.

This topology was selected as it will prove a comparable study for future research conducted from cyber security Controls effectiveness [19]. Of the four topologies evaluated, ”SME1” was chosen because it provided a more varied technology stack and a more complex design. The network topology provides an interesting opportunity to investigate network design flaws, due to its more varied technology footprint in comparison to the other ”SME” designs from Figure 2.

III. Implementation

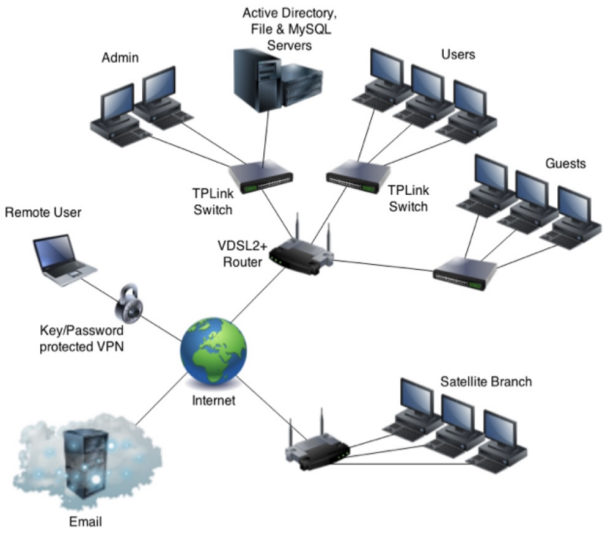
This section describes the implementation and configuration of the virtual machines and network within the cyber range, as well how it aligns to Cyber Essentials and utilises current and fully patched operating systems, such as Windows 10, Server



(a) SME 1 – Finance Sector. (b) SME 2 – Specialist Group.

(c) SME 3 – Web Development. (d) SME 4 – Hotel Services.

Figure 2: Topologies of SME Networks [19]



(a) SME 1 – Finance Sector.

Figure 3: Chosen Topology [19]

2022 and modern Linux operating systems. The configuration and system resources can be found in Table 1.

When building the cyber range, strict compliance was followed to ensure alignment with Cyber Essentials [15], For the cyber range to be as realistic as possible, multiple technology solutions have been implemented such as File servers, MySQL Databases, File Transfer Protocol, security monitoring, Web Application, Domain Server and Job Application Portal were created. To ensure that these technologies follow Cyber Essentials controls multiple controls were implemented from the framework. An example of this is ensuring local firewalls were enabled as well as the implementation of a network

Machine Name:	OS Type:	IP Adress:	RAM:
File Server - FILSB001	Windows Server 2022	192.168.5.4	4GB
FINDT002 – WIN10	Windows 10	192.168.5.22	4GB
ITDT001 - WIN10	Windows 10	192.168.1.2	4GB
Kali Linux	Kali Linux	10.10.10.1	4GB
pfSense	FreeBSD 14.0	10.10.10.200	1GB
SafeBank Website	Windows Server 2022	10.0.0.3	8GB
SB Domain Controller	Windows Server 2022	192.168.1.3	4GB
Splunk	CentOS Linux 7	192.168.1.1	8GB
WIN10 – Adversary	Windows 10	10.10.10.10	4GB

Table I: Virtual Machine Configuration.

firewall. For this research I chose a pfSence firewall. PfSense was selected as the firewall due to being opensource and freely available, but with a record of great reliability and documentation.

Further to this, to ensure strong password management controls are in place, I removed all default passwords within the cyber range, and ensured that all operating systems were hardened by the removal of all software and services that were not in use on the machines. Windows Auto-updates were also enabled on all end point machines leaving only the servers to be manually confirm updates before being ready to test, but due to the template design of the environment this only needs to take place once before being created as many times as needed. Windows Defender was enabled with auto-run/auto-play disabled on all systems, with only user accounts that are actively in use being enabled.

Windows Defender was chosen as it comes built in with the Windows operating systems, ensuring ease of management and updates. Furthermore, Windows Defender is the market leader in endpoint protection platforms [12] as seen in the Gartner's Magic Quadrant, ensuring that any potential malware uploaded to the cyber range is rigorously tested.

Having selected Skytap as the platform to build the cyber range, one of the issues to be overcome was the limitations on controlling network traffic and the ability to conduct monitoring between VlAN'. Whilst building a secure segmented network design (seen in Figure 7) After working closely with Skytap engineers, they confirmed that routing traffic and monitoring between VLAN' nativity within the platform was not possible. To create a novel solution to this problem, the pfSense firewall was utilised to route the traffic between the VLAN', enabling the cyber range to conduct network spanning and promiscuous monitoring, this can be seen in Figure 4, Figure 5 and Figure 6.

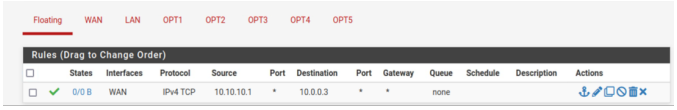


Figure 4: pfSense Inbound/Outbound Floating Rule

To ensure repeatable results for each assessment, the cyber range utilises saved templates of a confirmed complaint version for consistent assessments. The virtual machines (from Table 1) outlined in this chapter are managed by Skytap "VM Sequencing" (Figure 8) to ensure all services and operating

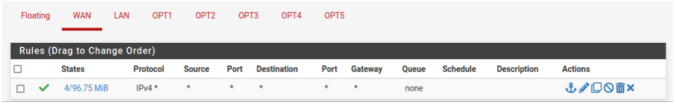


Figure 5: pfSense WAN Rule

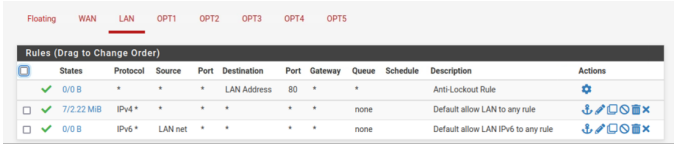


Figure 6: pfSense LAN Rule

systems have been enabled correctly in the same identical way each time the templated is loaded. To ensure the environment is compliant to the standards being tested, vulnerability and compliance scans have been conducted using automated vulnerability management, using Nessus authenticated scans and manually checked and no vulnerabilities were identified.

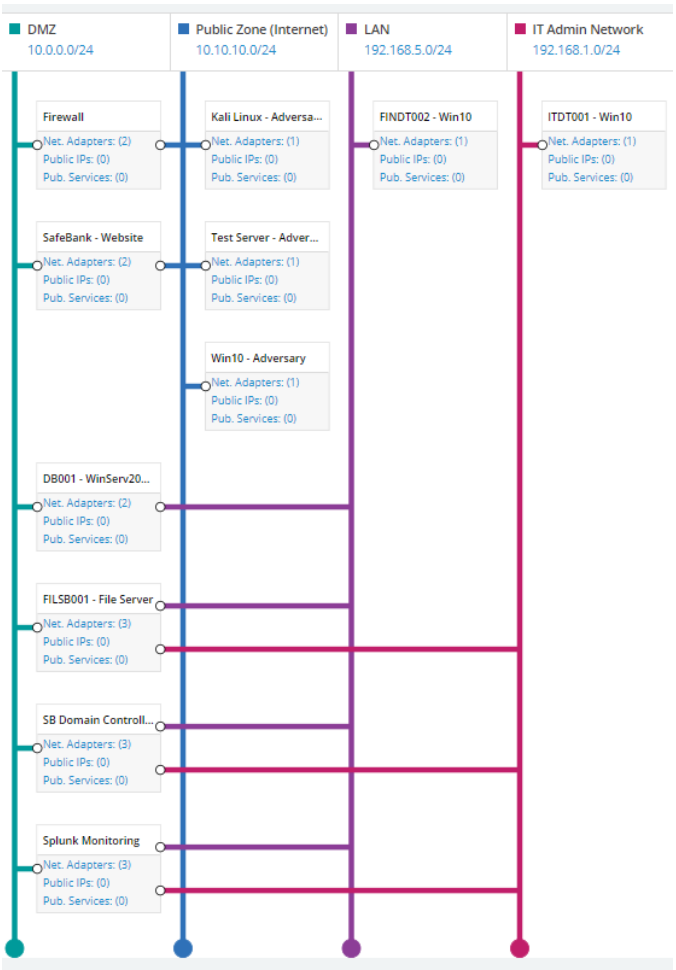


Figure 7: Network Topology

To recreate a realistic representation of an organisation's IT estate, multiple services were needed [23] [18]. The File

VM	Do not run	Stage 1	Delay After stage 1	Stage 2	Delay After stage 2	Stage 3	Delay After stage 3	Final Stage
		All	1 minutes	All	1 minutes	All	0 minutes	All
Firewall	○	○		◉		○		○
Kali Linux - Adversary	○	○		○		○		◉
FILSB001 - File Server	○	○		◉		○		○
FINDT002 - Win10	○	○		○		◉		○
SB Domain Controller	○	◉		○		○		○
ITDT001 - Win10	○	○		○		◉		○
Splunk Monitoring	○	○		◉		○		○
DB001 - WinServ2019 MySQL DB	○	○		○		◉		○
Win10 - Adversary	○	○		○		○		◉
SafeBank - Website	○	○		◉		○		○
Test Server - Adversary	○	○		○		○		◉

Figure 8: Environment Scheduling

Server called FILSB001 in the cyber rage hosted a shared network drive as well as a FTP server. The FTP service and file share utilise Microsoft standard services, these specific versions were selected as part of the server configuration As they form part of the standard Microsoft services and can utilise Microsoft's monthly updates, creating ease of management and implementation.

The web site and CV application portal has been built using WordPress and hosted on an XAMPP webserver. WordPress was chosen as the content management system (CMS) as it makes up the majority of the market share as it is used by 43.0% of all the websites on the internet, which is a CMS market share of 64.3% [22]. Whilst Cyber Essentials has no strict adherence regarding web application secure coding best practices (other than refer its readers to OWASP [17]) it does however require Applications to mitigate *"high-risk or critical updates for applications (including any plugins such as java, Adobe Reader and .Net) installed within 14 days of release."*

As seen in Figure 9 and figure 10 these systems were upgraded and plugins set to auto-update.

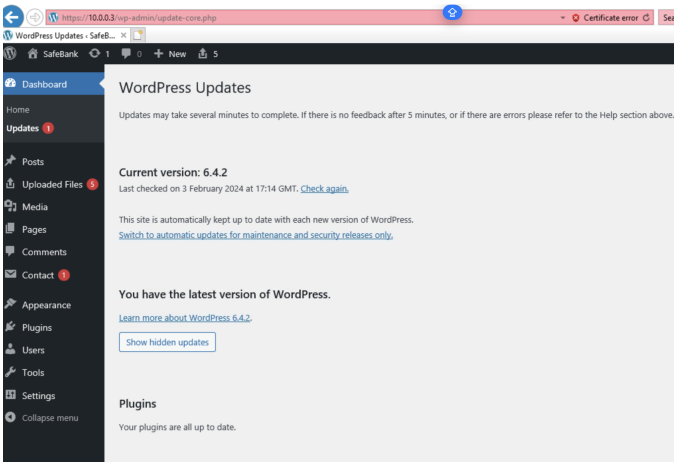


Figure 9: Wordpress Dashboard

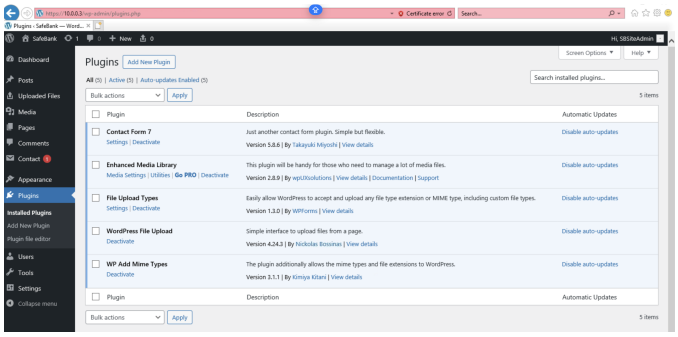


Figure 10: Wordpress Plugins

IV. Imitating Human Behaviour

One of the discussion points in [23] was how to add the human interaction element. As well as how to conduct the simulation in a realistic way for a fair test. This has been implemented in the cyber range by creating an account called "Sam", Sam is an "employee" within the 'finance' team who is reviewing CV's. To do this Sam copy's the CV from the application portal from the website and adds them to the finance group drive. Then every five minutes sam opens up the CV documents to read them. Whilst more human simulations could have been added such as clicking links in documents or allowing for copy, pasting and running of executables, this was reviewed as not a fair test and not a potentially realistic scenario.

For the simulation of "Sam" opening the CV's in the Finance Group drive, the automation utilises Windows Task Scheduler which runs a Powershell command, which in turn runs a command from a file on Sam's Desktop, as seen in code example 1 in the Appendix. The Task Scheduler is set to run upon initial login and then every five minutes thereafter, the script that is ran can be seen in Code 1 (within the Appendix):

The full process can be seen in Figure 11, Figure 12 and Figure 13

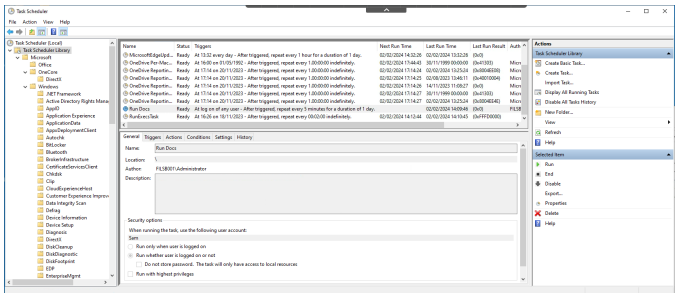


Figure 11: Task Scheduler Summary

The code in the script file as seen in code example 2 (within the Appendix), reviews the documents in the file server called Filsb001 and specifically looks for the extensions for .doc, .docx and .docm. This was done as different text editors will save the files differently, dependent on the version of the text editor they are running. The script will then attempt to open each word document that meets these extension types.

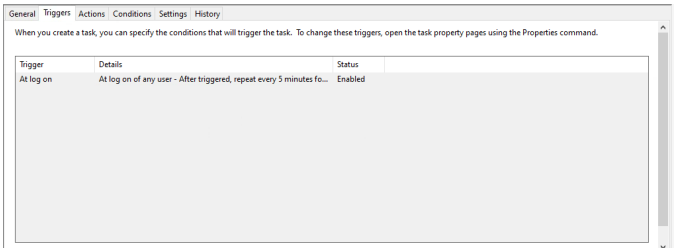


Figure 12: Task Scheduler Trigger

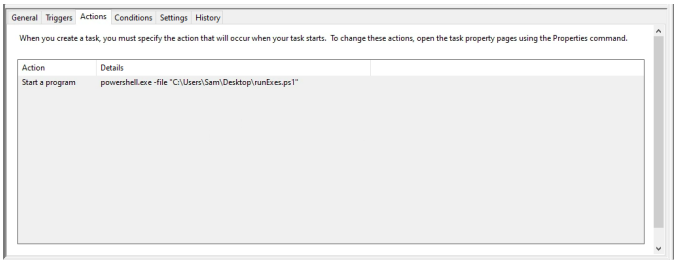


Figure 13: Task Scheduler Actions

For the simulation of "Sam" copying the CV's into the Finance Group drive (as seen in code example 3), the automation again uses Windows Task Scheduler and Powershell to run an initial command from a script file on Sam's Desktop, with a slight difference in the command that it will open copy.ps1 rather than runExesc.ps1 from the desktop. This process can be seen in Figure 14, Figure 15 and Figure 16.

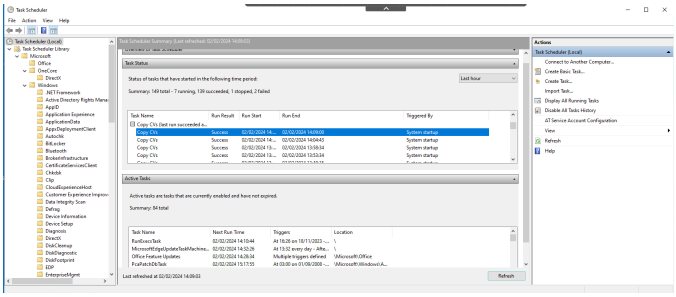


Figure 14: Task Scheduler Summary of Copy to Group Drive

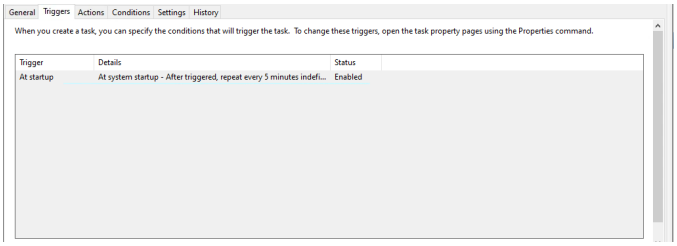


Figure 15: Task Scheduler Copy Trigger

V. Discussion

To the best of our knowledge, no works address the automation and creation of a cloud based cyber range compliant

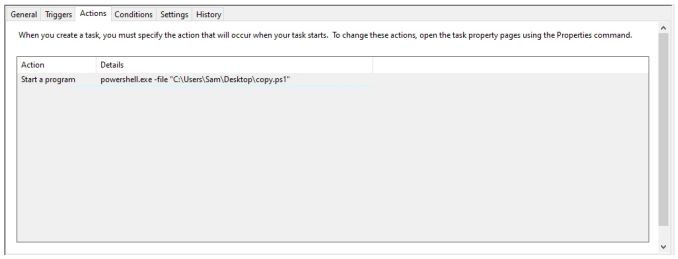


Figure 16: Task Scheduler Copy Actions

to cyber essentials. Whilst other cyber ranges have used a hybrid approach in their design using physical assets as well as digital, this led to multiple complications

When building the cyber range there were a number of challenges and processes that needed to be overcome and applied [23], whilst some of these were technical in nature when building the cyber range, some were design choices and process-related such as the imitation of human behaviour. It was very important to have an imitation of human behaviour in the cyber range as controls such as malware protection needed to be assessed to evaluate cyber essentials, whilst highlighted in [23]. However, whilst incorrectly suggesting that 100% of employees would enable macros to review CV's, the assessment was able to provide a fair test of malware protection controls. One concern that arose when testing malware was inconsistent pop-up notifications from Microsoft Word. This would randomly appear, be it in the form of a sign-in request or licence reminder. The consequence of this would mean that any automation scripts would fail, this is due to the human imitation scripts not being able to close any pop-ups. The workaround to this was to manually open Word each time the template was run, as this was the only manual element to the entire environment this was an accepted risk.

Another key area was removing all ambiguity on the compliant nature of the cyber range to the Cyber Essentials standard[23]. To do this I recruited ten industry experts, of which six were penetration testers, two 3rd line engineers and two security analysts to conduct a manual review as well as a vulnerability assessment using Tenable. This came with its own challenges on how specific defensive controls such as antivirus and Firewalls are selected. We could implement best of breed security solutions based on Forrester and Gartner's magic quadrant

VI. Conclusion

In this work, we have presented a cloud based environment that automates the creation of a Cyber Essentials compliant cyber range, which is able to be completely managed from a web browser from any device. The cyber range has been created in a robust, repeatable, safe and effective manner for the testing of an SME organisation which is aligned to the Cyber Essentials framework.

We have also shown the capability of imitating human behavior to actively interact with defensive controls such as malware protection and network security.

Using this platform enables the user to create multiple environments which are completely identical and secure, with the use of VM scheduling and templates. Implementing only the security controls outlined in guidance from the Cyber Essentials framework. This will allow for future work outlined in [23] in which the Cyber Essentials framework can be evaluated for its effectiveness, or used to test modern hacking methodologies such as malware evasion techniques or 'living off the land' in a hardened environment.

References

[1] Omar Abbosh and Kelly Bissell. Securing the digital economy: Reinventing the internet for trust", accenture. 2019. accessed 05 January 23.

[2] Robert Ernest George Bloomfield. Bullets to bytes: Defending the united kingdom in cyberspace. 2019.

[3] Innovation Technology Department for Science. Cyber security breaches survey 2023. https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2023/cyber-security-breaches-survey-2023, April 2023. (Accessed on 05/01/2024).

[4] Innovation Technology Department for Science. Uk cyber security sectoral analysis 2023. 2023. accessed 05 January 23.

[5] Rachna Dhamija, J. D. Tygar, and Marti Hearst. Why phishing works. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*. ACM, 2006.

[6] Jon Erickson. *Hacking: the art of exploitation*. No starch press, 2008.

[7] Richard Fujimoto, Conrad Bock, Wei Chen, Ernest Page, and Jitesh H Panchal. *Research challenges in modeling and simulation for engineering complex systems*. Springer, 2017.

[8] Gordon, Loeb, and Sohail. Market value of voluntary disclosures concerning information security. *MIS Quarterly*, 34(3):567, 2010.

[9] Oliver Hinz, Michael Nofer, Dirk Schiereck, and Julian Trillig. The influence of data theft on the share prices and systematic risk of consumer electronics companies. *Information Management*, 52(3):337–347, 2015.

[10] ICO. Ico fines british airways £20m for data breach affecting more than 400,000 customers, 2020.

[11] Kenneth J Knapp, Christopher Maurer, and Miloslava Plachkinova. Maintaining a cybersecurity curriculum: Professional certifications as valuable guidance. *Journal of Information Systems Education*, 28(2):101, 2017.

[12] Rob Lefferts. Microsoft is named a leader in the 2022 gartner® magic quadrant™ for endpoint protection platforms. 2023. accessed 06 January 23.

[13] James Andrew Lewis. "economic impact of cybercrime", center for strategic international studies (csis). 2018. accessed 21 October 20.

[14] Savita Mohurle and Manisha Patil. A brief study of wannacry threat: Ransomware attack 2017. *International journal of advanced research in computer science*, 8(5):1938–1940, 2017.

[15] NCSC. Cyber essentials: Requirements for it infrastructure v3.1. https://www.ncsc.gov.uk/files/Cyber-Essentials-Requirements-for-Infrastructure-v3-1-April-2023.pdf, April 2023. (Accessed on 04/02/2024).

[16] NICE. Cyber ranges, 2018.

[17] OWASP. Owasp application security verification standard. https://owasp.org/www-project-application-security-verification-standard/, Feb 2024. (Accessed on 03/02/2024).

[18] J. M. Such, P. Ciholas, A. Rashid, J. Vidler, and T. Seabrook. Basic cyber hygiene: Does it work? *Computer*, 52, 2019.

[19] Jose M Such, John Vidler, Timothy Seabrook, and Awais Rashid. Cyber security controls effectiveness: a qualitative assessment of cyber essentials. 2015. read best paper yet.

[20] Leonie Maria Tanczer. 50 shades of hacking: how it and cybersecurity industry actors perceive good, bad, and former hackers. *Contemporary Security Policy*, 41(1):108–128, 2020.

[21] Vincent E Urias, William MS Stout, Brian Van Leeuwen, and Han Lin. 2018 international carnahan conference on security technology iccst. *Cyber range infrastructure limitations and needs of tomorrow: A position paper*, pages 1–5, 2018.

[22] W3Techs. Usage statistics of content management systems. https://w3techs.com/technologies/overview/content_management, 2022.

[23] Patrick Wake, Sue Black, and Jonathan Young. Work in progress: Evaluation of security standards through a cyber range using hackers' tactics, techniques and procedures. In *2023 IEEE European Symposium on Security and Privacy Workshops (EuroSPW)*, pages 653–658, 2023.

[24] Muhammad Mudassar Yamin, Basel Katt, and Vasileios Gkioulos. Cyber ranges and security testbeds: Scenarios, functions, tools and architecture. *Computers Security*, 88:101636, 2020.

[25] Pavel ÄŒeleda, Jakub ÄŒegan, Jan Vykopal, and Daniel TovarÅˆÃ¡k. Kypoâ€“a platform for cyber defence exercises. *MS Support to Operational Tasks Including War Gaming, Logistics, Cyber Defence. NATO Science and Technology Organization*, 2015.

VII. Appendix

```
InfoSecTest$pwsh_folder = Get-ChildItem -Path \\Filsb001\g
$extensions = @(".doc", ".docx", ".docm")

foreach ($file in $pwsh_folder) {
    Write-Host "Processing file: $($file.Name)"

    foreach ($extension in $extensions) {
        if ($file.Extension -eq $extension) {
            Start-Process winword.exe -ArgumentList $file.FullName -PassThru |
            Wait-Process
        }
    }
}
```

Code 1: Simulate Human Interaction by Automation of Opening Word

```
Copy "\\HTTP-01\uploads\*.doc*" "G:\"
```

Code 2: Simulate Human Interaction by Automation of Copying all Documents to Group Drive

```
powershell.exe -file "C:\Users\Sam\Desktop\runExecs.ps1"
```

Code 3: Initiate Script