National College of Ireland

Configuration Manual

MSc Research Project
Cyber Security

Jordan Enwright
Student ID: X21238103

School of Computing
National College of Ireland

Supervisor: Dr. Imran Khan

National College of Ireland

MSc Project Submission Sheet

School of Computing

Student Name:	Jordan Robert Enwright		
Student ID:	X21238103		
Programme:	MSCCYB1	**Year:**	2023
Module:	MSc Research Project		
Lecturer:	Dr. Imran Khan		
Submission Due Date:	August 14th 2023 2pm		
Project Title:	Research Project Configuration Manual		
Word Count:	1974	**Page Count: 12**	

I hereby certify that the information contained in this (my submission) is information pertaining to research I conducted for this project. All information other than my own contribution will be fully referenced and listed in the relevant bibliography section at the rear of the project.
ALL internet material must be referenced in the bibliography section. Students are required to use the Referencing Standard specified in the report template. To use other author's written or electronic work is illegal (plagiarism) and may result in disciplinary action.

Signature: Jordan R. Enwright

Date: September 18th 2023

PLEASE READ THE FOLLOWING INSTRUCTIONS AND CHECKLIST

Attach a completed copy of this sheet to each project (including multiple copies)	□
Attach a Moodle submission receipt of the online project submission, to each project (including multiple copies).	□
You must ensure that you retain a HARD COPY of the project, both for your own reference and in case a project is lost or mislaid. It is not sufficient to keep a copy on computer.	□

Assignments that are submitted to the Programme Coordinator Office must be placed into the assignment box located outside the office.

Office Use Only	
Signature:	
Date:	
Penalty Applied (if applicable):	

Configuration Manual

Jordan Enwright
X21238103

1 Introduction

This manual provides detailed instructions to replicate the research setup conducted in "Helping non-technical business executives know if they are a target of cybercrime". The goal is to ensure accurate replication by describing the necessary software tools and configurations. The manual assumes that the standard software and tools are already installed on your system.

2 Prerequisites

- A computer system capable of performing local application development.
- Strong understanding of cyber security principles and ability to identify important security factors.
- Access to the necessary datasets and articles used in the research, see references.

3 Software Tools

- Microsoft's Visual Studio Code version 1.81.0
- GitHub Desktop version 3.2.7
- Git version 2.35.1.windows.2
- Node.js version 16.15.0
- Node Package Manager version 8.5.5
- MongoDB Atlas Account
- MongoDB Compass
- Express.js version 4.18.2
- React.js version 18.2.0
- Google Chrome for application testing and reading research
- PuTTY SSH client version 0.78
- Microsoft Azure account
    - Azure VMs
- Azure-CLI version 2.51.0
- Microsoft Word and Excel
- Application dependencies
    - reduxjs version 1.9.5
    - bootstrap version 5.3.0
    - react-bootstrap version 2.8.0
    - react-dom version 18.2.0
    - react-icons version 4.10.1
    - react-redux version 8.1.1
    - react-router-bootstrap version 0.26.2",
    - react-router-dom version 6.14.2",
    - react-toastify version 9.1.3"
    - types/react version 18.2.14",

- types/react-dom version 18.2.6",
- @vitejs/plugin-react version 4.0.1
- eslint version 8.44.0
- eslint-plugin-react version 7.32.2
- eslint-plugin-react-hooks version 4.6.0
- eslint-plugin-react-refresh version 0.4.1
- vite version 4.4.0
- bcryptjs version 2.4.3
- concurrently version 8.2.0
- cookie-parser version 1.4.6
- dotenv version 16.3.1
- express version 4.18.2
- express-async-handler version 1.2.0
- jsonwebtoken version 9.0.0
- mongoose version 7.3.1
- nodemon version 2.0.22

4 Research Setup

The initial step in the research process was to gather as many respected articles as possible and reports on cyber security incident and risk assessment. In fact, risk assessment only became a considered search term after initial searches for cyber security incidents did not yield enough relevant data points. After considering risk assessment more search terms came to mind and were added to the future searches.

After several rounds of searching, I had amassed a respectable amount of research article, industry reports, governmental standards, and other papers. With these resources, I began to read through each of them, identifying key points made and themes that I noticed. This process often led to more questions which would start the search cycle over again until I felt like I had enough information to move to the next phase of the project.

5 Data Preparation

After analysing the resources, I had found the next phase was to prepare the data in way that would be more accessible to me for the rest of the research project. Industry reports were stripped of their colourful marketing content and hard numbers and statistics were pulled out, for example the data on cyber breaches and incidents from the Verizon Data Breach and Incident Report 2022, was turned into a bar chart to easily visualize the attack frequency difference across different industries.

Once the data had been separated from the original sources, it was categorized by its ability to support a central cyber security topic. These topics evolved into the questions that would be added to the CCAS tool. This is visualized in Table 2 of the report.

6 Replication Steps

After preparing the data visually and categorizing the data it was time to being the process of deeply analysing the data to see what kind of question could be asked to gauge the organization’s risk factors that were dependent on the given category.

By comparing the data within each category, a key question was developed. These questions would then be tested by asking non-technical individuals to answer them and if the individual felt like they could answer the question honestly and if they felt like their co-workers would likely answer the same way. This latter part is targeting an objective of the research which was that employees of the same company should get similar CCASs as the questions are to be designed at an organizational level not a personal level. A secondary test was conducted by the research, in regard to the answer options. Each question has various answer options, some answer options were binary, “Do you have remote workers?”, other led to more categorical options, “How is the data stored?” Each of these options needed to be able to add to the CCAS, in a way that made sense comparatively to the other options as well as maintaining a balanced ratio to the other questions and their possible scores.

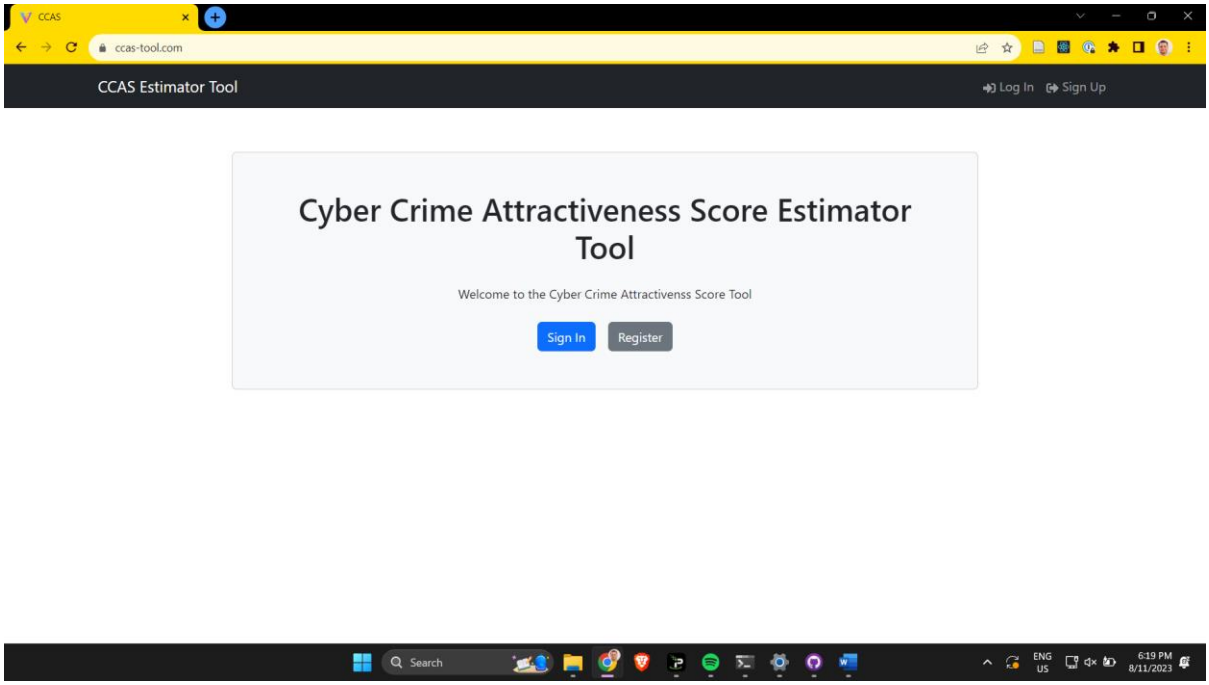
After each round of testing the questions were also reevaluated by the researcher to determine if a logical and realistic score could be given to each of the answer options. The data collection phase included not only categorical data collection but also subject data within each category. For example, when the researcher investigated the categorical data on data types, the original answer options I came up with needed to change as they did not make sense in terms of real-world effect. So initially I had answer options of non-GDPR data, financial data, medical data, religious data, and sexual orientation data. However, after some testing, it turned out that these answer options did not make real-world sense, and instead needed to be changed to anonymised data, publicly available data, and sensitive data. These three categories make more sense in term of data protection as per most governmental standards.

Once questions, answer options, and scoring had been finalized, it was time to create the research artifact, CCAS-tool.com.

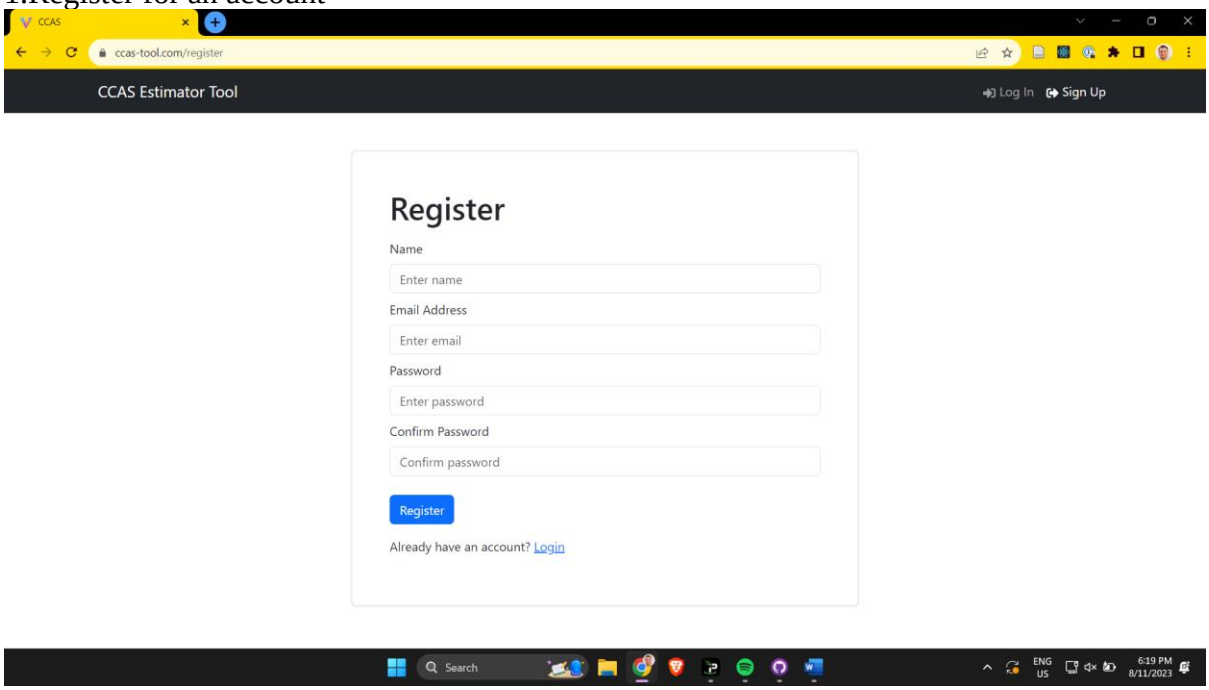
The web application was developed using the MERN stack (MongoDB, Express, React, Node.js) for familiarity and built-in security. The web application needed to facilitate user account creation and secure login. The CCAS web app employs the scoring system to assess an organization's attractiveness to cybercrime. Each question's answer options carry specific scores, informed by real-world data or CGP impact ratings (CISA, 2023). The goal is to prevent underestimating risk by valuing answers too low. The scoring adds up weighted scores from all questions to gauge an organization's cybercrime appeal, where higher scores indicate higher risk.

CCAS draws from sources like the Verizon Data Breach Report and other cybersecurity reports to assign logical values to answer options, ensuring alignment with actual risks. The web application targets simplicity and clarity for non-technical users, reflecting in its user interface and straightforward questions. Given the sensitivity of data, the MERN stack's built-in security features are leveraged, using Json Web Tokens for authorization, immediate hashing and salting of passwords.

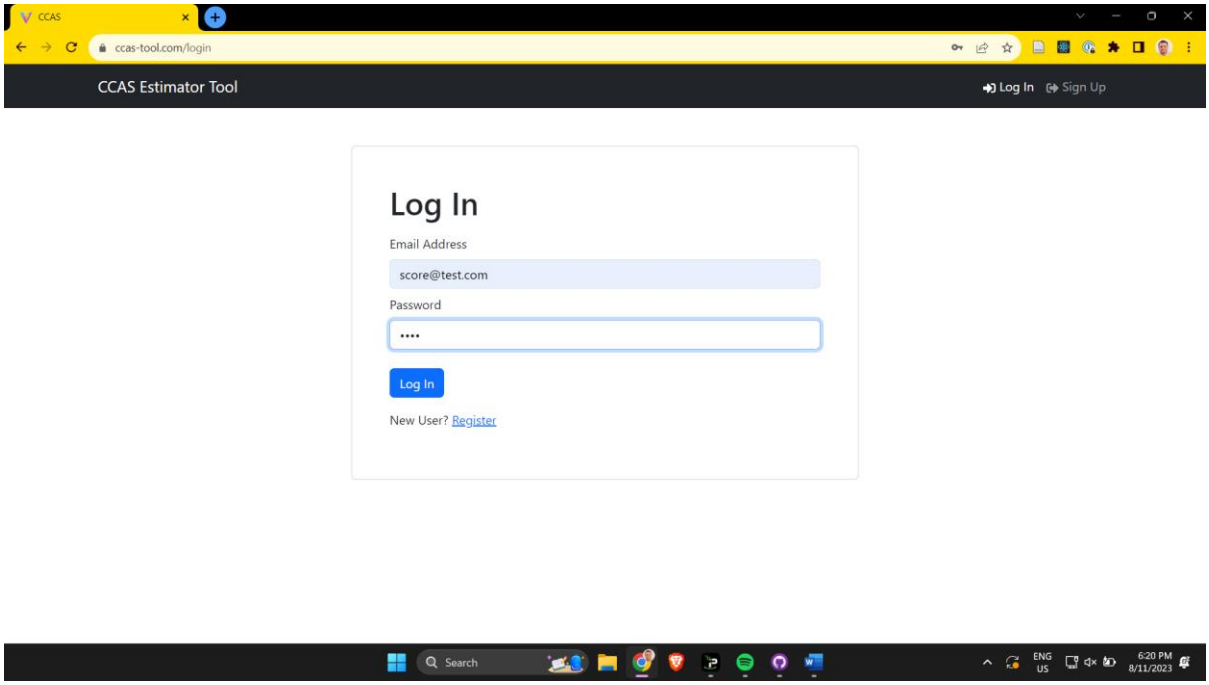
App Walk Through
https://www.ccas-tool.com

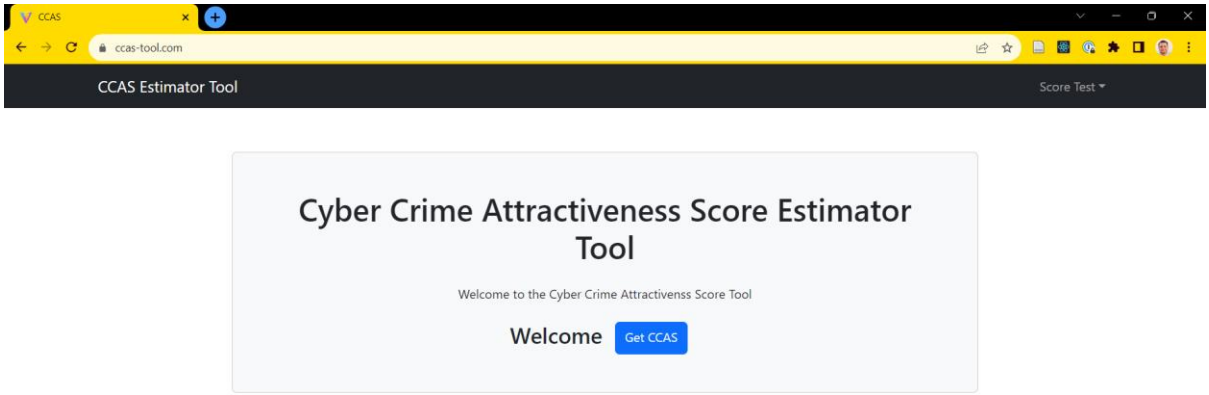


1.Register for an account

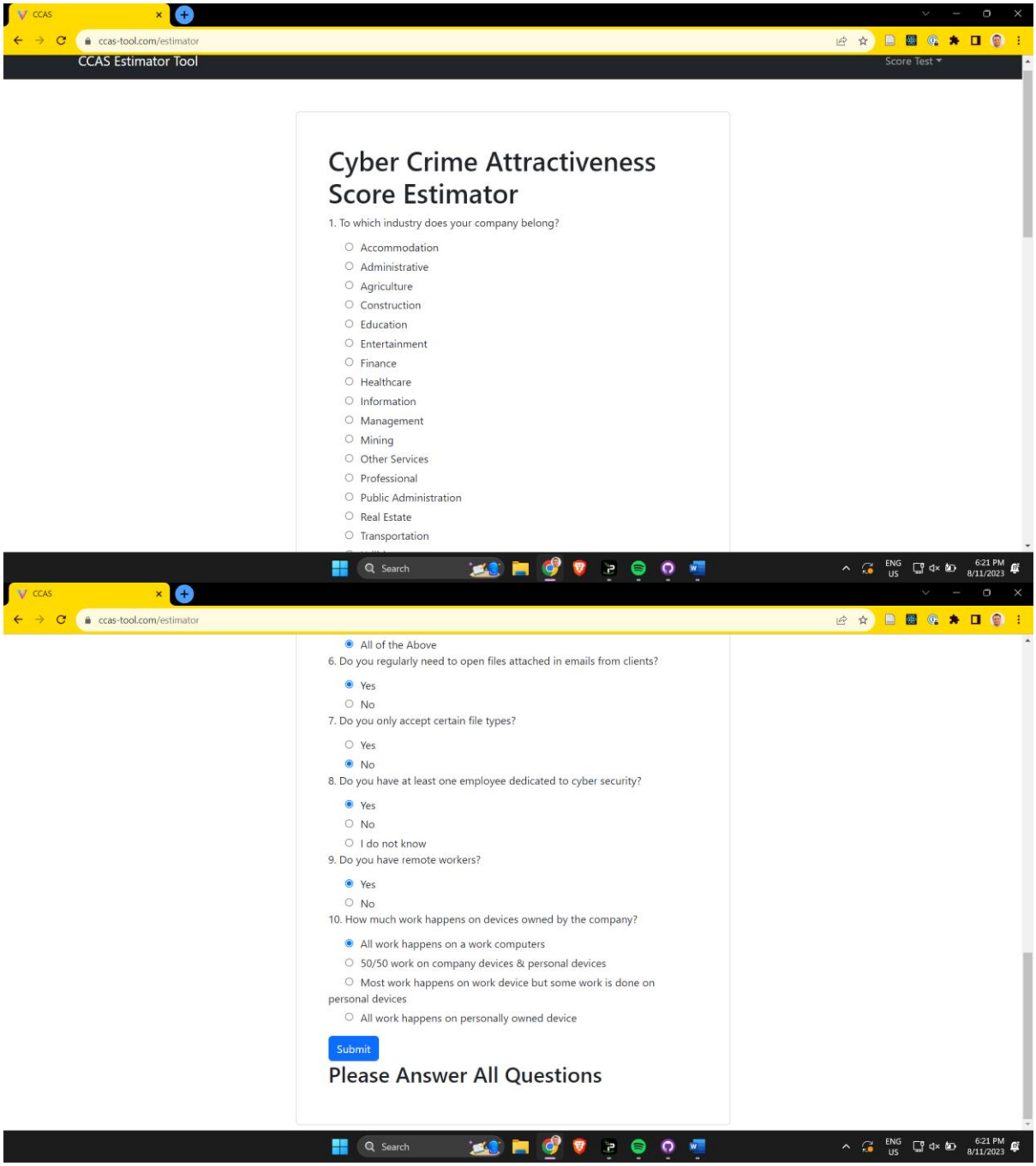


2. Or log into your account. For testing purposes there is a tester account. Email: score@test.com and password: 1234

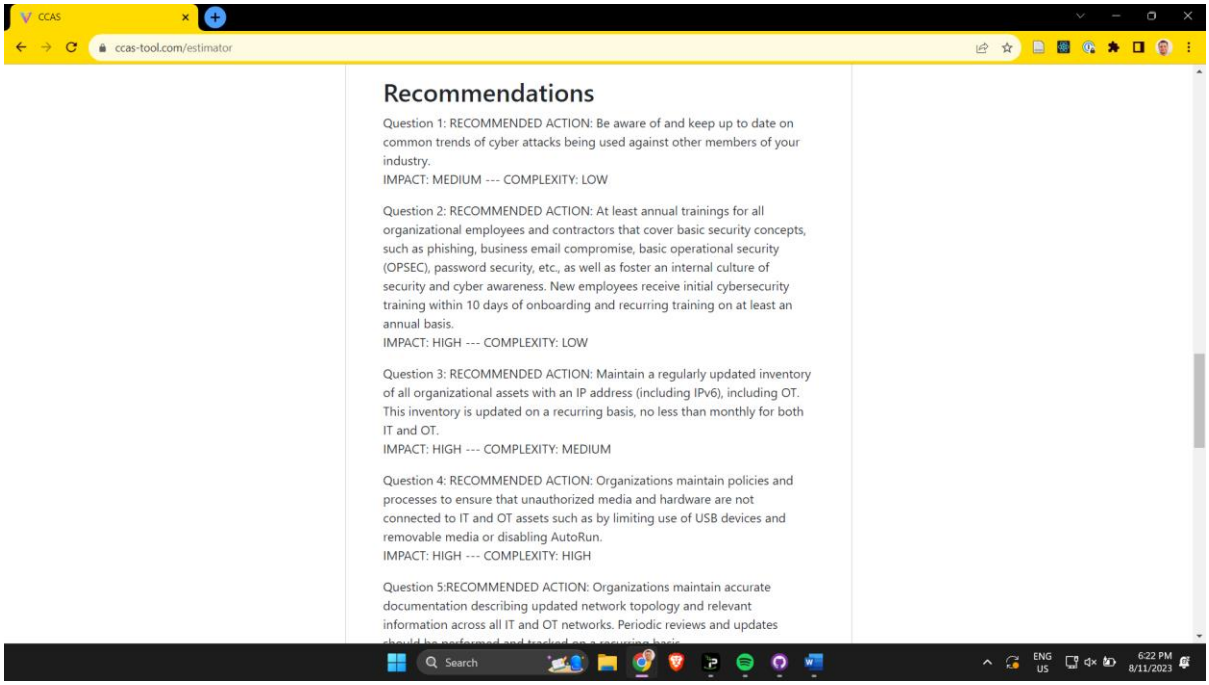




3. Click “Get CCAS” button.



4. Answer all the questions, and then click “submit”.
5. The score will be shown, along with recommendations that align with CISA CGP.



7 Troubleshooting

Troubleshooting the development and deployment of a MERN application to Azure virtual machines (VMs) can involve several challenges and considerations. The process of deploying a MERN app to Azure VMs involves multiple components, including the operating system, web server, database, and application code, which can all contribute to potential issues. Most development troubleshooting was handled by rereading documentation on the various components used for development, as well as referring to the MERN tutorial (Traversy, 2023)

One common challenge is ensuring the proper configuration of the virtual machines. Issues might arise if the VMs have insufficient resources, such as CPU, memory, or disk space, leading to poor app performance or even crashes. Properly scaling the VMs to match the application's requirements is crucial. Initially, I deployed the web app to the lowest tier VM Azure offered and it took so long to install the dependencies that the VM would often become unresponsive. The same thing would happen when I would try to build the app on the VM, the build process would make it most of the way through and then just freeze. It was able to build the app and install the dependencies but not consistently, and therefore I had to upgrade to a VM with more resources, to improve stability and consistency.

Networking and security configurations can also cause deployment hiccups. If the VMs are not configured with the appropriate inbound and outbound rules, firewalls, or network settings, it might result in connectivity problems between different components of the MERN stack. Ensuring that ports are open and network traffic is allowed is essential for the app to function as expected. Azure has default security settings on the VMs that I was unaware of, so I was able to SSH into the VM and confirm the VM was up and running but the VM would not server the web app on the correct port, because the port was blocked by default.

Moreover, compatibility between the MERN components and the Azure environment is paramount. Issues can arise if the Node.js version, MongoDB version, or other dependencies

used in the app are not compatible with the environment provided by Azure. These incompatibilities can lead to runtime errors or unexpected behaviour. Verifying the compatibility of each component and ensuring that they are up to date is a critical troubleshooting step. This is mostly mitigated upon VM creation by selecting a VM that has comparable specification to the development environment and ensuring both environments are running the same versions, ideally both running the most up to date versions of all the requirements.

Deployment logs and monitoring tools can be invaluable when diagnosing issues. Azure provides various tools to monitor VMs, application performance, and resource utilization. Analysing logs and performance metrics can help identify bottlenecks, errors, or other anomalies that might be affecting the deployment. These tools are when I ended up using to diagnose the connection issues I mentioned earlier. Azure does do a good job of offering tools and documentation to assist their users to be able to complete most tasks.

Troubleshooting the development and deployment of a MERN app to Azure VMs involves addressing challenges related to resource allocation, networking, security, compatibility, and monitoring. Paying careful attention to these aspects and leveraging Azure's monitoring and diagnostic tools can greatly aid in resolving issues and ensuring a successful deployment.

8 Conclusion

In conclusion, this manual serves as a comprehensive guide to replicate the research setup presented in "Helping non-technical business executives know if they are a target of cybercrime." Its objective is to facilitate accurate replication by providing detailed instructions on software tools and configurations required for the setup. Before delving into the replication steps, certain prerequisites are essential, including a capable computer system for local application development, a strong grasp of cyber security principles, and access to the necessary datasets and research articles as outlined in the references.

The manual encompasses various phases, starting with the gathering of relevant articles and reports on cyber security incidents and risk assessment, followed by data preparation involving categorization and transformation of resources into usable data. The replication steps involve analysing categorized data to formulate questions that gauge an organization's risk factors. The questions underwent rigorous testing to ensure consistency across employees within an organization, ultimately leading to the creation of the research artifact, CCAS-tool.com.

Troubleshooting is crucial in the development and deployment process, particularly while migrating the MERN application to Azure VMs. Challenges ranging from resource allocation and networking to security, compatibility, and monitoring need to be addressed meticulously. The manual provides insights into tackling these challenges, with an emphasis on proper VM configuration, network and security settings, compatibility checks, and the utilization of Azure's monitoring and diagnostic tools.

This manual equips readers with the knowledge and guidance needed to replicate the research setup effectively while providing a comprehensive understanding of the considerations and challenges associated with the deployment of a MERN app on Azure VMs.

References

Azumah, F.D., Nachinaab, J.O., Krampah, S. and Ayim, P.N. (2020). Determinants of Target Victim Selection: A Case Study of Criminals from Gambaga Prisons. *Journal of Victimology and Victim Justice*, 3(1), pp.93–112. doi:https://doi.org/10.1177/2516606920927258.

Benz, M. and Chatterjee, D. (2020). Calculated risk? A cybersecurity evaluation tool for SMEs. *Business Horizons*, [online] 63(4), pp.531–540. doi:https://doi.org/10.1016/j.bushor.2020.03.010..

Böhme, R., Laube, S. and Riek, M. (2021). *A Fundamental Approach to Cyber Risk Analysis*. [online] Available at: https://www.casact.org/sites/default/files/2021-07/Approach-Cyber-Risk-Bohme-Laube-Riek.pdf [Accessed 15 Apr. 2023].

Center for Internet Security (2023). *CIS Control 3: Data Protection*. [online] CIS. Available at: https://www.cisecurity.org/controls/data-protection.

CISA (2022). *YEAR IN REVIEW CISA 2 0 2 2*. [online] Available at: https://www.cisa.gov/sites/default/files/publications/CISA-YearInReview_v1_508.pdf.

CISA (2023). *PERFORMANCE GOALS*. [online] Available at: https://www.cisa.gov/sites/default/files/2023-03/CISA_CPG_REPORT_v1.0.1_FINAL.pdf.

Department for Digital, Culture, Media, & Sport (2021). Cyber Security Breaches Survey 2021. (Cited by 20)

ENISA (2022). *Incident reporting*. [online] CIRAS. Available at: https://ciras.enisa.europa.eu/ [Accessed 10 Aug. 2023].

ENISA (2023a). *Cybersecurity Maturity Assessment for Small and Medium Enterprises*. [online] ENISA. Available at: https://www.enisa.europa.eu/cybersecurity-maturity-assessment-for-small-and-medium-enterprises/ [Accessed 10 Aug. 2023].

ENISA (2023b). *ECSM 2022 Campaign Report*. [online] *https://www.enisa.europa.eu*. Available at: https://www.enisa.europa.eu/publications/european-cybersecurity-month-2022-campaign-report [Accessed 10 Aug. 2023].

European Union Agency for Cybersecurity (2022). ENISA Threat Landscape 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022: European Union Agency for Cybersecurity.

Garcia Perez, A., Lopez Martinez, A. and Gil Perez, M. (2023). Adaptive vulnerability-based risk identification software with virtualization functions for dynamic management. *SSRN*, [online] pp.1–30. Available at: https://ssrn.com/abstract=4469646 [Accessed 10 Aug. 2023].

IBM (2022). *Cost of a Data Breach Report 2022*. [online] Available at: https://www.ibm.com/downloads/cas/3R8N1DZJ.

Malaivongs, S., Kiattisin, S. and Chatjuthamard, P. (2022). Cyber Trust Index: A Framework for Rating and Improving Cybersecurity Performance. *Applied Sciences*, 12(21), p.11174. doi:https://doi.org/10.3390/app122111174.

Simoiu, C. (2020). Who Is Targeted by email-based Phishing and malware? Measuring Factors That Differentiate Risk. In: A. Zand and E. Bursztein, eds., ACM Internet Measurement Conference.

NIST (2019). *Cybersecurity Framework*. [online] National Institute of Standards and Technology. Available at: https://www.nist.gov/cyberframework.

Ojoawo, E. (2023). *Phishing attacks: The phisherman, the phish, the bait and the hook | Tripwire*. [online] www.tripwire.com. Available at: https://www.tripwire.com/state-of-security/phishing-attacks-phisherman-phish-bait-and-hook.

Rai, M. (2019). A STUDY ON CYBER CRIMES, CYBER CRIMINALS AND MAJOR SECURITY BREACHES. International Research Journal of Engineering and Technology, [online] 6(7). Available at: https://www.irjet.net/archives/V6/i7/IRJET-V6I740.pdf.

Sweeney, B. (2016). *Cybersecurity Is Every Executive's Job*. [online] Harvard Business Review. Available at: https://enterprisersproject.com/sites/default/files/cybersecurity_is_every_executives_job.pdf [Accessed 10 Aug. 2023].

Tenable (2023). *CIS Control 13: Data Protection (CIS Controls Assessment Specification)*. [online] docs.tenable.com. Available at: https://docs.tenable.com/security-center/CIS-CAS/Content/PDF/CIS_CAS_Controls.pdf [Accessed 10 Aug. 2023].

Traversy, B. (2023). *MERN Crash Course (Part 1) - Backend API, Middleware, Database, JWT*. [online] www.traversymedia.com. Available at: https://www.traversymedia.com/blog/mern-crash-course-part-1 [Accessed 10 Aug. 2023].

Tripwire (2017). *Small Companies Overconfident about Their Security Posture, Finds Survey | Tripwire*. [online] www.tripwire.com. Available at: https://www.tripwire.com/state-of-security/small-companies-overconfident-security-posture-finds-survey [Accessed 10 Aug. 2023].

Tripwire (2023a). *Reviewing Remote Work Security: Best Practices | Tripwire*. [online] www.tripwire.com. Available at: https://www.tripwire.com/state-of-security/reviewing-remote-work-security-best-practices [Accessed 10 Aug. 2023].

Tripwire (2023b). *Three Reasons Why Business Security Starts with Employee Education | Tripwire*. [online] www.tripwire.com. Available at: https://www.tripwire.com/state-of-security/reasons-why-business-security-starts-employee-education [Accessed 10 Aug. 2023].

Verizon (2022). *Data Breach Investigation Report*. [online] *www.verizon.com*. Available at: https://www.verizon.com/business/resources/T11a/reports/dbir/2022-data-breach-investigations-reportdbir.pdf [Accessed 10 Aug. 2023].