**STUDENT – PRODUCT ASSESSMENT TASK**

|  |  |  |  |
| --- | --- | --- | --- |
| Task Number | 2 of 3 . | Task Name | Industry Project Documentation |
| National unit/s code | VU23220  VU23221 | National unit/s title | Develop and carry out a cyber security industry project  Evaluate and test an incident response plan for an enterprise |
| National qualification code | 22603VIC | National qualification title | Certificate IV in Cybersecurity |
| RMIT Program code | C4424 | RMIT Course code | INTE5061 |

Section A – **Assessment Information**

|  |  |
| --- | --- |
| **Assessment duration and/or due date** | You will be advised of the session dates for demonstration on commencement of this unit.  This assessment will be released in week 10 and will be due in week 15. The exact date and time will be made available through Canvas. |
| **Task instructions** | |
| **Type of Product (tick which applies)**  Project  Report  Portfolio  Case study  **Summary and Purpose of Assessment**  This project is one of two assessment tasks you need to complete satisfactorily, in order to be deemed competent for this unit. Completing this project allows you to demonstrate developing and undertaking the implementation of a solution for an industry project.  **Assessment Instructions**  You must work in a team to develop an industry project including identifying the business problem and undertaking implementation and evaluation of a solution.  **What**  You have been nominated as the team organiser for a group of four (5) including yourself. Your team will be designing and implementing a cyber-security management plan for a new client. The details of the client will be provided to you by your assessor, or they will direct you to use the simulation client (included at Appendix 1). For this project your assessor will play the role of the client in confirming project requirements and seeking feedback.  The target of this project is to use introductory red team / blue team methods to achieve a secure system that is protected against common vulnerabilities.  Your manager (also played by the assessor) will be the system designer for this project. You will direct all feedback and questions to the system designer and apply all feedback which they provide to you.  In your teams you will need to carry out a number of different activities in order to plan, implement and evaluate the project. The teamwork will be conducted in class – you will make decision, configure labs, run tests and test your management plan over the five (5) planned sessions.  There are two (2) overall assessments that make up the criteria you will demonstrate for this assessment.   * In Assessment Task 1, you must individually submit a completed set of project documentation that shows that your team has planned, implemented, and evaluated the project and worked successfully as a team. Your version of the documents will demonstrate your role as the organiser / leader, include the communications you carried out and it will contain the decisions, test results and outcomes of work from the group work. Each of the documents has a submission date in line with the planned classroom activities. * In Assessment Task 2, you will be assessed on your practical performance in the five (5) sessions, including both the teamwork and the class-group discussions, aspects of the implementation and a training session for users of the system.   Each student in your group, including you, will play the role of the organiser / leader at least once over the five (5) planned sessions. You will be observed undertaking some aspects of this project during those sessions.  There are seven (7) key milestones for the project broken into five (5) team sessions. NOTE: You will find more detail about what you need to achieve in the criteria in the Marking Guide at Section B of this assessment (Section C in the Assessors Version).   1. Session 1    1. Team establishment    2. Project scope and plan 2. Session 2    1. Solution design and development 3. Session 3    1. Implementation of the solution    2. Revision and finalisation of the implementation plan including design of training, documentation, and support programs 4. Session 4    1. Implementation training, technical documentation, and support 5. Session 5    1. Project finalisation including evaluation   You will need to work with the systems designer (your Assessor) to formalise the design of the solution, but in general you should consider each of the following and demonstrate knowledge and use of each of the following at least once (1) across the project:  Testing concepts and procedures for cybersecurity including virtualisation   1. Installing and using software packages including those for testing 2. Using procedures and systems to identify data traffic anomalies 3. Connecting cyber security equipment and networked devices 4. Using basic Linux commands 5. Interpreting and writing basic scripts   The following options should be considered and discussed but you may then make the decision about how they relate to other aspects of your designed solution:   1. Interconnecting virtual images 2. Virtualisation operation and structure 3. Creating and configuring virtualised images 4. Configuring firewalls 5. Implementing Intrusion Detection Systems (IDS) features to examine data for anomalies for a potential security threat 6. Implement Intrusion Prevention Systems (IPS) to monitor data traffic   You will be working with all computing devices within this organisation including desktop PCs and laptops, networked computers and scanners and the cloud-based storage. You will be able to assess the security of personal devices in simulation through a virtual machine or bring your own device – you will not have access to the staff’s personal devices.  There is a $0 working budget for this project. If a solution requires a paid product or service, you should recommend the in your designed solution and plan for its implementation in the implementation plan. During the lessons learned you will report why it has not been implemented – because budget was not allocated.  You will provide written documentation to support each stage. Templates have been provided for each of the documents to be completed. You must address each section of the template in as much detail as possible.  You will be marked against the criteria in the marking guide at Section B of this assessment, however the following instructions will assist you in completing the documentation accurately:  **Pre-Session 1:**  You will participate in a briefing meeting with the assessor to begin this project. It is during this meeting that you should ask questions to confirm the approach to management and you will then break into teams.  Your team will then use the initial briefing to configure a lab environment that creates a range of different types of vulnerabilities. These are vulnerabilities that you will be required to solve.  You will then be directed to pass on the configuration to another group.  **Session 1**  Your team will carry out team establishment activities to agree to an approach to the project including who will play the role of leader during each session, how you will work as a team to identify and solve problems and complete the required milestones. You must also discuss how you will measure performance.   * You will record your findings from this discussion in the Work Plan at Appendix 2. * You will be observed participating in the discussion to address criteria 3 in Assessment Task 2.   Once you have an approach to work, you must investigate the configured lab using red-teaming methods to identify and exploit vulnerabilities. This will be a red-teaming exercise.   * You will need to individually contribute your findings to the group to be collated into the initial project plan using the template at Appendix 3. * You will be observed participating in the activity to address criteria 4 in Assessment Task 2.   You must individually complete and submit the following documents at the start of Session 2:   * A team plan using the template at Appendix 2. * A project plan using the template at Appendix 3.   **Session 2**  You must complete any remaining testing and vulnerability identification activities and use these to design a solution for workplace cybersecurity.  Each person in the team must contribute to the decision-making processes – this could be through individual research, voting or formal decision-making processes or similar. **NOTE:** You should consider keeping meeting minutes to show the decision-making process – you’ll be able to submit this with your portfolio of documentation after Session 3.  You will be observed familiarising yourself with the proposed resources for the solution to address criteria 5 in Assessment Task 2.  You will then individually create the following document in your own time and submit at the start of Session 3:   * An implementation plan using the template at Appendix 4   **Session 3**  You must now implement your agreed solution within the configured lab checking and verifying that each aspect of the solution works as intended and will reach the project target. You should also make adjustments and refinements to improve the solution as required. This will be a blue-teaming activity.  As a team you must share your findings from the verification activities and make decisions about the changes together. **NOTE:** You should consider keeping meeting minutes to show the decision-making process.   * During the session you must collate your evidence of the verification activities to create an updated and finalised implementation plan. You must show the results from your verification activities against each implemented action and all changes that have been made as a result of the verification activities. Refer to criteria 4 in the Marking Guide. * You will be observed carrying out blue-teaming activities to address criteria 6 of Assessment Task 2.   **IMPORTANT:** You must submit the updated implementation plan inclusive of your verification evidence at the end of Session 3 or as directed by your assessor because you will need the feedback, from this session, to undertake the next session.  You will also individually collate OR complete the following documents in your own time and submit these at the start of Session 4:   * Technical documentation for the implemented and verified solution using the template at Appendix 5. * At least two (2) other pieces of documentation demonstrating the implementation process including team contributions and the discussion of policies, plans and other matters and preparation for training and other end-user support activities. Refer to the list at Criteria 5 in the Marking Guide.   **Session 4**  You must now carry out any remaining implementation activities to secure the clients system and carry out end-user support activities including providing training and other supports. You will receive feedback from your assessor on your implementation plan, and you will gather information about your technical and other support documentation from the end-users to make any final adjustments.  You must find a partner to train in your solution and provide support. You will have 15 minutes for this activity – your assessor will advise you when to begin:   * You must demonstrate at least one (1) skill related to your solution such as how to operate the software or how to carry out monitoring activities. * Your partner will ask you at least one (1) question about the solution which you will answer and/or demonstrate in order to demonstrate providing support. * You must collect feedback from your partner which will help you to improve the way you communicate the solution. You must collate the findings from that feedback into revised technical documentation to address this task. * You will be observed providing the training and support to complete criteria 7 and 8 in Assessment Task 2.   You will then swap roles to receive training and support and give feedback on your partners solution.  You will individually complete the following documents in your own time and submit these at the start of Session 5:   * Revised technical documentation incorporating feedback from the training and support activities   **Session 5**  You must carry out project finalisation activities. This will include:   * Checking that each aspect of your implementation plan has been implemented and is functioning as expected or reporting any aspects of the plan which were not possible or that need to be implemented at a later stage. * Evaluating your team’s performance to determine opportunities to improve your teamwork or individual performance.   You will individually complete the following documents in your own time and submit these by the due date indicated by your assessor:   * A lessons learned report using the template at Appendix 6.   **Where**  You will be provided some class time to work on this assessment in five (5) programmed sessions. Your assessor will give you the dates and times of each session on commencement of this project.  However, it is expected that the majority of the documentation, and some additional communication with your team, outside of class.  **How**  You will be assessed against the criteria listed in the marking guide in Section B of this task. To achieve a satisfactory result, you will need to address all criteria satisfactorily. | |
| **Conditions for assessment** | |
| * You must submit all assessment evidence as instructed. Your assessor will assess the documentation you provide. * You must complete the task within the maximum allowed duration * Please make arrangements with your assessor at least one week prior to the assessment due date if you feel you require special allowance or allowable adjustment to this task * You will have the opportunity to resubmit any product deemed unsatisfactory (one resubmit is allowed per unit). * If the product assessment is a group-based activity each student will be assessed individually against all assessment criteria * You will be assessed as satisfactory or not satisfactory * You can appeal the assessment decision according to the [RMIT Assessment Processes](https://www.rmit.edu.au/content/dam/rmit/documents/about/policy/assessment/assessment-processes.pdf). | |
| **Equipment/resources students must supply (if applicable):** | **Equipment/resources to be provided by RMIT or the workplace (if applicable):** |
| * Computer with internet access and relevant software * USB Storage Device for transporting files * Team members * Copies of Appendix 1 – 5 | * Onsite computer and internet access |

Section B – **Marking Guide**

|  |  |
| --- | --- |
| **TASK:**  Describe the product to be assessed | This product assessment demonstrates the skills and knowledge to work in a team on an industry-based project that leads to a solution.  You must demonstrate participation in the development of an industry project that leads to a solution.  You require access to a safe work environment for assessment in simulation.  You will need access to software and digital equipment to complete the assessment. |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Criteria for assessment | | Satisfactory | Not Satisfactory | Marking Guide  *Minimum requirements to be met:* |
| 1 | Collated your discussion outcomes from Session 1 to individually develop a team plan. |  |  |  |
| 1a | The team members for the project have been selected to carry out specific responsibilities based on their existing skills and knowledge.  It is clear who will play the role of organiser/leader for each of the four (4) remaining sessions. |  |  |  |
| 1b | The team members have established at least three (3) team performance criteria and their related performance measurements.  They have identified and explained a suitable methodology for performance measurement.  An IRT has been formed |  |  |  |
| 1c | The team has identified at least two (2) cybersecurity models used for intrusion in an organisation including the components found in each model.  The team has identified the Business implications to the organisation of cyber incidents.  The team has created an incident management plan based on the IRP (Incident Response plan) | ☐ | ☐ |  |
| 2 | Individually documented a project scope and plan based on the team discussions from Session 1.  By submitting the plan to their assessor, they have demonstrated submitting documentation for substantiation by the relevant persons (the client and the systems designer/manager). |  |  |  |
| 2a | The team has used the simulation background information and an initial investigation of the configured lab environment using red and blue teaming methods to:   * Document the key business / cyber security problems and vulnerabilities * Develop additional questions (at least two) for the systems designer OR client. |  |  |  |
| 2b | The team has agreed to and used at least (1) problem solving methodology to identify:   * Scope of the project * System boundaries (project parameters) of the business problem * Objectives (at least two) of the project and the expected outcomes * Has created a purple management team and defined the activities to combat a cyber-attack. |  |  |  |
| 2c | The team has broken down the key milestones from the project to document work plans / schedules. They have included:   * At least two (2) additional key elements for each of the milestones. NOTE: it is strongly recommended that students use the criteria within this marking guide to guide this breakdown. * A breakdown of the milestones and elements into tasks/activities to be completed * Resources needed to complete the project including any related costs of time, people, places, and things (equipment / tools) * A schedule (timeline) of project tasks that is realistic * Delegation of tasks and responsibilities to team members |  |  |  |
| 2d | The team has identified at least three (3) risks to their project and/or team success and documented related processes for:   * Managing the identified risks * Managing at least one (1) type of unexpected event that may impact on project objectives or timelines.   NOTE: It is strongly suggested that the plan relate to unexpected change in systems design. |  |  |  |
| 3 | Individually documented the agreed solution and its corresponding implementation plan. |  |  |  |
| 3a | The team has identified has each of the following key components and requirements is relevant to the solution and how they are to be implemented:   * Testing concepts and procedures for cyber security * Response plans for a cyber security incident is planed * Using procedures to identify data traffic anomalies * Installing and using software packages * Connecting cyber security equipment and networked devices * Using basic Linux commands * Interpret and writing basic scripts |  |  |  |
| 3b | For each of the relevant aspects of the solution, the team has determined and allocated relevant resources including:   * Discussion of how they familiarised themselves with the operation of the resources * Discussion of the function and operation of the required resources * Discussion of how they confirmed the resources were appropriate |  |  |  |
| 3c | Included an implementation plan for the solution. The plan includes:   * Suitable systematic processes for implementation * Testing and verification methods for each aspect of the solution * Strategies to minimise disruption to the end user * Processes for collecting and protecting evidence |  |  |  |
| 4 | Individually documented the results from soft or trial implementation by updating the implementation plan.  There is evidence of the group completing each of the following at a minimum:   * Testing concepts and procedures for cyber security * Using procedures to identify data traffic anomalies * Installing and using software packages * Connecting cyber security equipment and networked devices * Using basic Linux commands * Interpret and writing basic scripts   By submitting their findings, they have provided feedback to the system designer. |  |  |  |
| Each section of the provided design has been BOTH:   * Implemented * Tested for functionality according to prescribed test procedures |  |  |
| Reported on the teams participating in verification of end-to-end functionality of the design.  There is evidence that each of the team members has provided input into the final verification. |  |  |
| 5 | Individually produced implementation process documentation that:   * Reflects the changes/feedback from the system designer (the assessor) * Indicates implementation of the revised plan has occurred with end-users |  |  |  |
| 5a | Individually documented the implementation process as evidence of planning and implementing changes with minimum end-user disruption. This includes:   1. Technical documents (template at Appendix 5) covering the scope of work (at least one)   AND any two of the following:   1. Reports 2. Meeting minutes from meetings with:  * Team * End-Users  1. Email trails 2. Logbook 3. Presentations   **NOTE: Students in a team may choose different types of documentation to submit as evidence for this section**. |  |  |  |
| 5b | At least one (1) of the types of documents submitted demonstrates that matters affecting policies, plans and other related issues were discussed regularly with the team and acted upon. |  |  |
| 5c | At least one (1) of the documents shows that you sought the input of each team member during the decision-making processes for their week of leadership. |  |  |
| 5d | Submitted documentation for end user training including:   * Details of the training to be provided (time, date, location, people to attend, key outcomes expected) * Any support materials for training.   **NOTE: This could be within another document or as part of a revised implementation plan.** |  |  |  |
| 5e | Each document is accurate in regards to the findings from implementation AND the planned solution. |  |  |  |
| 5f | Completed each section of the technical documentation template (appendix 5).  By accurately completing each section of the template the student has demonstrated skills and knowledge in:   * Business implications of cyber security breaches * Operating systems (Windows or Linux) * Interconnecting virtual images * Virtualisation operation and structure * Creating and configuring virtualised images * Using networking devices * Configuring firewalls * Implementing Intrusion Detection Systems (IDS) features to examine data for anomalies for a potential security threat * Implementing Intrusion Prevention Systems (IPS) to monitor data traffic * Supporting the process of risk assessment |  |  |  |
| 6 | Submitted a PDF copy of their revised technical documentation with the changes identified through consultation and training activities in Session 4.  By submitting the revised technical documents to the system designer (the assessor) they have both submitted the items for approval and printed (to PDF format) and distributed the documentation intended for publication. |  |  |  |
| 7 | Individually prepared a ‘lessons learned’ document that collates the groups findings from review and completion of the project.  By collating the group findings and submitting the lessons learned document using the template at appendix 6 and successfully achieving a satisfactory result against each aspect of the template, you have demonstrated the process of obtaining final sign-off from the client (played by the assessor) and/or key stakeholders (team members). |  |  |  |
| 7a | The team has closed the project undertaking all agreed actions, from their project plan, to report findings and lessons learned. |  |  |
| 7b | Reviewed team performance against the agreed objectives from their work plan from task 1. They have included evidence of achievement to validate all findings.  The following conditions have been demonstrated in the student’s response:   * The majority of objectives were achieved. * Objectives not achieved have an accompanying recommendation for either: * A proposed workplace change * Another improvement * Individual achievements (whether they fully met objectives or otherwise) are recognised * Individual contributions to the generation of changes and improvements are appropriately recognised. * Effectiveness of red teaming and incident response tests |  |  |
| 7c | Reviewed the team objectives against the project/client targets. It is clear from the review that the project deliverables have OR will meet the project expectations given adjustment and more time.   * They have included at least one (1) source of information that validates their findings. * The majority of each of the following were achieved:  1. Timeframes 2. Scope 3. Cost 4. Quality expectations  * Targets and other objectives not achieved have an accompanying recommendation for either:  1. a proposed workplace change 2. another improvement |  |  |
| 7d | Reviewed the projects risk strategy to determine its effectiveness in this project.  Where there is opportunity for adjustment and/or improvement you have specified this including how that adjustment will be implemented. |  |  |

**Appendix 1**

The client is new to cyber-security in general but has begun to sell digital products via a subscriber website. The digital products range from royalty-based music and video clips through to plans and specifications for business products.

* Users download the content in a format of their choice and by entering a contract for its fair use.
* The content is submitted to the site and managed by the content-creator / artist.
* The client receives its money as portion of the sale or lease fee agreed to by the user.

The client is concerned about fraud regarding the originality and uniqueness of content and ensuring that the original content creator is correctly attributed and receives fair compensation.

Likewise, they are concerned about the security of the website ensuring that the content remains secure behind the paywall and cannot be easily mined and distributed by others.

Finally, they are concerned about financial security – they have heard of other organisations where the transaction is made, the content is accessed but then the payment is cancelled, resulting in the distribution of work, essentially, for free.

They run the website in the cloud, with only the physical website files backed up physically to an external hard drive. Each integrated application, software and website is accessed via usernames and passwords issued to staff. One of the two company directors is responsible for enrolling new users and forwarding the details, via email, to the staff member. They keep a spreadsheet of all login details in case someone forgets their access details. They ask that staff who create new accounts with other web resources forward the login details of those accounts to the director for safekeeping and to maintain business interests too.

They wish this to remain as a lifestyle business so infrastructure includes portable devices that can be used on and offsite including laptop computers, printers, normal peripheral devices (wireless keyboards and mice), USBs / external drives. The current office contains an ARLO nanny-style cam connected to the WIFI and accessible by the company directors when they receive a notification of movement in the office outside of business hours.

Staff access the workplace network to run their personal devices included smart phones, tablets, and laptops (as needed). The staff currently use their own networks when offsite. This includes tethering to a mobile phone, using free Wi-Fi hotspots and accessing home networks.

While they do not expect to be able to solve all problems immediately, they do wish to secure the current infrastructure using a range of security tools and software, physical infrastructure, access management and regular monitoring. Additional infrastructure, tools and processes should be recommended for implementation and a plan for implementation established that enables the company directors to budget for the additional costs.

**Appendix 2 – Team Work Plan**

|  |  |
| --- | --- |
| **Date of Plan** | *Sep 19, 2023* |
| **Team Members** | **Role & Responsibilities** |
| *William* | *App 3 questions, plan stage 1 (LAN), App 4 IPS vuln, App 5 IPS/IDS, Demo IPS* |
| *Victor* | *App 3 scope, plan stage 3 (pfsense), App 4 AD vuln, App 5 networking devices & OS* |
| *Josiah* | *App 3 teaming, plan stage 4 (WLAN), App 4 phishing vuln, App 5 firewalls, Demo AD* |
| *Kim* | *App 3 problems, plan stage 2 (website), App 4 backup vuln, App 5 virtualisation, Demo backup* |
| *Jimmy* | *App 3 plan resources, App 4 Wi-Fi vuln, App 5 user support & business implications, Demo wireless* |
| **Leadership Schedule** | |
| **Team Member** | **Session** |
| *Victor* | *19-25th Sep* |
| *Kim* | *26 Sep - 2 Oct* |
| *Jimmy* | *3-9th Oct* |
| *Will* | *10-16th Oct* |
| *Josiah* | *17-23rd Oct* |
| **What strategies will you apply to working effectively as a team?** | *Regular in person communication, Discord, OneDrive* |
| **How will you ensure that each team member contributes to decision making?** | *Group meetings* |
| **How will you solve problems within the team?** | *Discussing issues and topics, being goal oriented* |
| **Team Performance Criteria** | **Methodology for Performance Measurement** |
| *Good attitude* | *Smiles, inclusive* |
| *Output/regular contribution* | *Work* |
| *Engaging in conversations* | *Wpm, each group member giving their own thoughts* |

**Appendix 3 – Project Plan**

|  |  |  |
| --- | --- | --- |
| **The Business** | *Key aspects of the business, from the simulation include...*   1. B2C digital goods sales requires public facing infrastructure via a website that can handle user authentication and a secure payment portal. 2. Digital assets must be secured and only accessible by authorised users. 3. A Hybrid cloud and on-prem model is used so both cloud services and physical infrastructure must be secured 4. Lifestyle is a focus of the company so remote access and portable devices are a requirement as well as BYOD access | |
| **The Problem(s)** | 1. Client is concerned about fraud in relation to original content. Due to this issue, content creators request appropriate attribution and compensation 2. Issues regarding security of the website to prevent avoiding the paywall, mining, and unauthorised distribution    1. Prevent the content being accessed followed by cancelled payment 3. Backing up of files are only on a physical external hard drive. The issue with relying on one form of backup is the possibility of it failing during a recovery process. Such risk includes physical deterioration of the device, exposure from fire or natural disasters, and theft. 4. Staff can access every application, software and website via issued usernames and passwords. Incorrect implementation of access controls on staff accounts can negatively impact company files and resources. Company data can be breached if staff has unauthorised access to certain websites, downloading and installing inappropriate software and applications, and manipulating control settings 5. One of the company directors relies on email communication to enrol new users and exchange details with staff members. Staff are required to send to the director (via email) all the new account login details created from external web resources.  The lack of encryption, password-protection, and multi-factor authentication within emails containing sensitive data poses as a security risk. An email phishing attack can compromise sensitive company data 6. All staff login details are stored on a spreadsheet. If company files are subjected to insufficient encryption protocols and incorrect implementation of access controls, sensitive login data may be accessible by unauthorised users. 7. Staff are accessing the workplace network via free public Wi-Fi and home network on personal devices (laptops, tablets, phone). The lack of wireless security, operating systems, firewalls and VPN requirements on personal devices established by the company poses as a security risk to internal data and resources 8. The business uses an ‘ARLO’ nanny cam that is connected to the wireless network. Company directors have 24/7 access to the cam software.  IoT devices, like the ARLO cam, have security vulnerabilities including operating on default configurations, lack of security software and updates, which the device can be at risk of hacking and man-in-the-middle (eavesdropping) attack. 9. Wired network is connected to the wireless network 10. USB/external drives | |
| **Red, Blue and Purple teaming activities** | *Potential issues, attacks and prevention*   * *Syn Flood DoS attack*   + *MAC address filtering* * *Ransomware or system failure*   + *Cloud backup* * *Social Engineering / Phishing (e.g. BeEF; Zphisher)*   + *Fake phishing emails, employee training* * *Port scanning (Nmap)*   + *Firewall, port security* * *DHCP starvation*   + *MAC address filtering* * *ARP Poisoning MITM attack*   + *MAC address filtering* * *Website spidering (ZAP)* * *Website vulnerability scanning (ZAP & Burp)*     Blue teaming   * *Active Directory*   + *Structured hierarchical environment*   + *User accounts within domain controller* * *Firewall*   + Preventing port scans   + Preventing network scans * *Network Segmentation*    + Preventing malware such as ransomware from spreading to the whole network * *Cloud Service Azure*    + A backup in case of a ransomware attack and system failure * *Proxy Server*    + Stopping employees from accessing malicious websites * *IPS & IDS SIEM*   + Preventing Arp/MITM attacks   + Preventing DHCP starvation attacks     **Incident response plan activities = suggest who is responsible and specifics of their duties during response incident** | |
| **Project Scope** | *The project scope, the range of devices, the types of vulnerabilities, the types of solutions*  *Scope:*   * *LAN network –*   + *Build active directory with a structured hierarchy, implement shared files/folders access, and group policies.*     - *Ensure appropriately assigned permissions, login detail storage, and access for AD.*   + *Create 10 Windows 10 clients connected to the domain.*   + *Proxy server and basic router firewall to protect the network perimeter and police internal traffic.*   + *Kali Linux machine for pen testing*   + *Ubuntu assign dedicated device designed for use as a SIEM tool.* * *Web service- azure*   + *Hosting website on Azure (cloud platform), no need for DMZ unless setting up own service as cloud provides all the services traditional web, email, backup, etc., servers would’ve offered.* * *Install Pfsense connected via VPN to Azure, and implement a SIEM tool*   + *Build Ubuntu with Pfsense and SIEM tool (ELK stack with metricbeats)*   + *Create 10 Windows 10 VM on Azure with antivirus pre-installed for employees’ remote use*   + *Create a replica domain controller*   + *Setup site-to-site VPN to the cloud from the LAN and an anywhere VPN to the cloud for remote connections*   + *IPS can also check data when syncing* * *Wireless network*   + *Wireless adapter*   + *Segmenting the wireless router away from the LAN network,*   + *Applying VLAN and ACL to direct traffic*   + *Proxy server for authentication, separate from the LAN*   *Devices:*   * *20x Windows 10 clients* * *2 servers (1 backup on the cloud)* * *Ubuntu device for the SIEM tool running Elastic service* * *Firewall with Pfsense software* * *Routers and switches*   *Vulnerabilities and solutions:*   * *Data mining and fraud through cancelled payments after purchase.* * *Use a cloud service with the appropriate security such as Azure.* * *Reliance on physical backups to external hard drives.* * *Backing up data on the cloud or in a server.* * *Shared usernames and passwords across staff for applications, software and website.* * *Individualised accounts with targeted privilege levels (with AD) for corresponding use case.* * *Single individual manually enrolling new users and emailing details to staff members.*   + *Using AD or another database system to record login details automatically via software.* * *Manual storage of all login details as plain text in a spreadsheet.*   + *Stored in a secure database preferably encrypted* * *Unmanaged use of USBs/external drives.*   + *Prevent use of unknown USBs in company network connected devices, force data transfer through USB where contents are scanned before allowed in.* * *Using ARLO nanny cams hosting footage on an external network*   + *Host security footage on the LAN or on a secure company owned cloud, have encryption/VPN if traffic goes externally, implement security software and appropriate configuration which may require upgrading to other cameras if necessary.*   + *Alternatively configure the ARLO nanny cams off the default settings, upgrade, and update firmware, connect to a separate network dedicated to the ARLO nanny cams with encryption, SSID cloaked, and mac filtering enabled to explicitly permit access via the company directors.* * *Use of BYOD*   + *Require a minimum standard of software, hardware, use of security measures such as anti-malware software and use, updating software. Also implement policies to facilitate this use, and if necessary, force employees to use the cloud VM.* * *Own networks when off-site*   + *Employees must not connect to public Wi-Fi, instead must use a personal or company provided hotspot. Work must be done via a VPN connection to operate a cloud Windows VM client where all company data is to be stored.* * *No security policy/incident response plan* | |
| **System Boundaries / Project Parameters** | Known parameters:   1. Delivery time (expected time of completion at each stage) 2. Client’s budget    1. Due to the client's budget, the recommended solutions are to be completed in 4 stages   Boundaries include:   1. Server room (location and construction) 2. Type and cost of equipment/systems 3. Specialized personnel required to install systems   Necessities for delivering the core service:   1. Secure and functional local environment with necessary equipment.    1. Physical server for AAA authentication    2. Local storage of data    3. IPS and firewall    4. Domain connected client devices configured with appropriate permissions. 2. Functional website on Azure 3. Secure connection to the cloud (VPN). 4. (Optional) Virtual machines on Azure with RDC   Exclusions include:   * Security camera replacement, disconnect if vulnerability is too severe. * Regulation of content and payment system on the website, outside the area of expertise (which is networking). | |
| **Key Questions to Be Answered & Assumptions** | 1. What type of user permissions are required? 2. Do you require group policies? If so, how many groups and what kind of group policies do you require? Who will be responsible for controlling these groups? 3. How many folders, drives etc. Do you require? Do you require a backup server? (Yes, security & load balancing) Is ongoing support required? Do you require training for staff or is there already someone responsible for training? 4. How many users and devices are within the current infrastructure? 5. What is the client’s expected time of delivery in terms of implementing new services, infrastructure, employee training? | |
| **Project Plan**  ***Refer to this spreadsheet for the Project Plan.***  [***https://rmiteduau.sharepoint.com/:x:/r/sites/CertIV-CyberSecurityProject/Shared%20Documents/Project%20Plan.xlsx?d=wa9e405621ef547f49e0661d2627f8f32&csf=1&web=1&e=VBl6aq***](../../../:x:/r/sites/CertIV-CyberSecurityProject/Shared%20Documents/Project%20Plan.xlsx?d=wa9e405621ef547f49e0661d2627f8f32&csf=1&web=1&e=VBl6aq) | | |
| **Risk Plan** | | |
| **Risk** | | **Processes and Controls** |
| Identify the risks and unexpected events that would influence your ability to carry out the agreed actions. | | Identify the processes and controls that can be implemented to manage the risks and respond to unexpected events. |
| Construction and setup of a new server room can be subjected to delays or cost overruns | | * Consider leveraging cloud service (e.g., Microsoft Azure) or virtualisation to temporarily host applications and workload; * Prepare a plan and budget allocation; * Regular monitoring of construction progress; * Identify and address construction or equipment delivery issues promptly to avoid further delays |
| Physical hardware installation may encounter compatibility issues, damage during transport, or delays in procurement | | * Maintain backup systems and redundancy measures to ensure business continuity; * Leverage remote access alternative and cloud service to allow employees to work remotely if on-site hardware is either unavailable or undergoing maintenance * Conduct thorough hardware compatibility testing before deployment; * Implement handling and transport procedures to prevent damage; * Maintain vendor and supplier relationships for efficient procurement and access to backup alternatives |
| Initial implementation of changes in infrastructure and operations may cause interruptions or downtime, affecting customer experience | | * Schedule updates during low-traffic periods; * use load balancing and redundancy for critical services; * Run new and old systems in parallel while carefully implementing data migration; * have backup plan ready |
| Proxy tools (like CCProxy) may conflict with existing configurations or misuse | | * Update or reconfigure the proxy tool to align with existing network configurations and security policies * Implement access control and monitoring to prevent misuse. Ensure that only authorised users have access * Monitor network traffic and usage patterns to determine if proxy tool is being misused for unauthorised activities |
| Lack of comprehensive technical documentation may hinder troubleshooting and knowledge transfer between employees | | * Create and maintain documentation templates, manuals, and guidelines for configurations, procedures and processes to ensure consistency in format, content, and structure. This will make it easier for workers to understand and use the documentation; * Encourage collaboration among workers to ensure that relevant knowledge is shared within the company * Provide training to workers on the importance of documentation |
| Employees may lack the required knowledge and skills to operate, maintain and troubleshoot new systems and infrastructure | | * Invest in employee training and development programs (in-house training and/or external courses or certifications); * Enhance the onboarding process for new employees by providing training on the company’s systems and infrastructure * Create documentation and manuals for new systems and infrastructure. These resources should be easily accessible and serve as reference guide for employees * Seek external consultants or experts who can provide insight, training and guidance on new systems |
| Resistance from employees to adapt to new technologies and processes | | * Communicate to employees on the benefits of changes and consider employee feedback * Offer hands-on experience and practical training sessions where employees can interact with new systems and tools |
| Initial phase of setting up Azure within the business may lead to unauthorised access to Azure resources, data breaches or leaks in the cloud | | * Only Administrator/IT staff is allocated access to Azure resources and controls; * Enable Azure Security Centre for continuous monitoring and threat detection * Regularly review and update security policies and access controls. |
| Running services in Microsoft Azure can lead to unexpected costs if not monitored and managed correctly | | * Use Azure Cost Management and Billing to monitor and control costs. * Set up and implement Azure Policy to enforce cost control measures. |
| Azure services may experience outages or downtime, affecting the replica domain controller’s availability | | * Implement Virtual Machine redundancy to increase availability to business data and resources; * Develop a disaster recovery plan to mitigate downtime. |

**Appendix 4 – Implementation Plan**

* ***Josiah– phishing attack, Will – IPS, Kim – backup, Jimmy – wireless, Victor – AD***

|  |  |
| --- | --- |
| **DESIGNED SOLUTION** | |
| **Summary** | *The key vulnerability targets mentioned in this section will be...*   1. *Phishing*    1. *Aim to identify phishing attempts and eliminating such threats through training.* 2. *Vulnerable network perimeter without an IPS*    1. *Aim to identify all suspicious traffic, prevent these threats and adapting security measures.* 3. *Lack of backups*    1. *Aim to have some redundancy in case of faults.* 4. *Insecure and not configured WLAN device.*    1. *Aim to configure the current network device and secure it using multiple methods such as SSID configuration changes, SSID cloaking, administrative configuration changes, web-filtering, firmware upgrades and remote access disabling.* 5. *Current insecure user account management and login storage system.*    1. *Aim to replace the current system with AD, preventing the previous threats entirely by storing logins securely and managing access appropriately with a DC.* |
| **Testing Concepts and Procedures** | *Identification would involve:*   1. *Sending fake phishing emails* 2. *Pen testing or audits for the network perimeter, WLAN security, and the user account management*   *Confirm vulnerabilities resolved and verify reliability:*   1. *Identifying vulnerabilities again as mentioned above with follow up pen testing and audits for all vulnerabilities.* 2. *Test functionality of the new setup, such as by attempting to use backup measures to restore data and test its integrity.* |
| **Data Traffic Anomalies** | *The IPS and proxy server can send detected traffic anomalies to a syslog server whilst the SIEM tool can proccess and send alerts as necessary.* |
| **Software Packages** | * *CCProxy: provides logging, filtering and caching services with data. Can apply integration with AD.*   + *Employees accessing the internet will have their traffic linked to their user account.*   + *Suspicious sites will be blocked, which will prevent potential exposure to malware.*   + *Internet traffic will be logged for follow up forensics if a breach occurs.* * *Pfsense with Snort: detects traffic passing through the firewall whilst logging and blocking traffic.*   + *e.g., Sends alerts when a suspicious packet is detected by the firewall*   + *Can block the sender and recipient of suspicious traffic from going through, stopping potential attempts of installing malware or attempts at unauthorised access.* * *ELK stack on Ubuntu: SIEM tool ingesting data from the AD server and displaying notable information.*   + *Plugins with the Windows server can be used to send ELK stack via metricbeats, fundamentally performs like Splunk.* * *Windows Active Directory: Manages user accounts and permissions.*   + *User accounts created in the company domain’s organisational unit*   + *Assign users to groups with specific policies (permissions) corresponding to their position to prevent/limit unauthorised access.*   + *Integrate AD with other applications such as CCProxy so a centralised user directory can be used.*   + *Store login details with AES256 encryption using AD default settings.* * *Kali Linux with zphisher, nmap and ettercap for red teaming. These attacks will help identify vulnerabilities.* |
| **Networked Devices** | * *Server for hosting the Radius AAA, SIEM, and internal DNS shared via virtualisation.*   + *Software:*     - *Windows Server (with AD), CCProxy, winlogbeats/metricbeats*     - *ELK stack*     - *Pfsense with Splunk* * *Firewall device which also acts as a router for VPN tunnelling to the cloud.* * *Switch and (wireless) router.* * *Windows 10 client devices joined to the domain.* |
| **Operating System Commands (Linux)** | Operating systems:   * Windows Server * Windows 10 * PFsense - Firewall * Kali Linux – Security tool for testing * Ubuntu – SIEM tool   Linux Commnds:  **Installing the SIEM tool**   * sudo apt install gedit * wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add - * echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list * sudo apt-get update * sudo apt-get install logstash * sudo apt install openjdk-17-jdk -y * sudo apt-get install elasticsearch * sudo apt-get install kibana * sudo apt install gedit -y * sudo /bin/systemctl enable elasticsearch.service && sudo /bin/systemctl enable kibana.service && sudo /bin/systemctl enable > * gedit -s /etc/kibana/kibana.yml * gedit -s /etc/elasticsearch/elasticsearch.yml   Attacking with Kali  nmap -sT -v -P0 (target ipaddress)  sudo git clone https://github.com/htr-tech/zphisher.git  cd zphisher  sudo bash zphisher.sh  sudo ettercap -G |
| **Scripts** | #!/bin/bash  wget -qO - https://artifacts.elastic.co/GPG-KEY-elasticsearch | sudo apt-key add -  echo "deb https://artifacts.elastic.co/packages/7.x/apt stable main" | sudo tee -a /etc/apt/sources.list.d/elastic-7.x.list  sudo apt-get update  sudo apt-get install logstash  sudo apt install openjdk-17-jdk -y  sudo apt-get install elasticsearch  sudo apt-get install kibana  sudo apt install gedit -y  sudo /bin/systemctl enable elasticsearch.service && sudo /bin/systemctl enable kibana.service && sudo /bin/systemctl enable >  gedit -s /etc/kibana/kibana.yml  echo "update the Kibana Config - the Elastic Config will open automatically when it is closed"  gedit -s /etc/elasticsearch/elasticsearch.yml  echo "Update the Config files then start the programs with the sudo service commands" |
| **Resources** | * Server for virtualization of Windows Server and SIEM tool * Laptops for workers * Physical firewall for PFsense and IPS * Azure – Replica domain controller * Routers |
| **IMPLEMENTATION PLAN** | |
| **NOTE: You must add additional rows and labels to address additional vulnerabilities and/or aspects of the solution. You will need to incorporate the designed solution throughout your implementation plan. You may change the layout of the section below or include additional sections as long as you address the existing labels at a minimum.** | |
| **Vulnerability 1 Phishing Attack** | |
| **Description** | Employees are not trained to identify fraudulent emails and the IPS/IDS is not setup to block suspicious websites |
| **Results from Testing** | From this screenshot you can see that phishing is very versatile and can replicate the look of many different websites  https://cdn.discordapp.com/attachments/1083151053962367027/1156083065987276860/image.png?ex=6513adc1&is=65125c41&hm=dcc797d5e3c9c632da846004be699ba3a0c253441c27ed90cdeca2cf0525fd08&  Usually there will be some urgency paired with the link for example they could send an email saying your account has been logged into and if the victim is panicking and not paying attention, they won't double check the link and as you can see URL 3 is very unsuspecting at a glance    The website that it replicates is very unassuming, but you can see that it is even capable of getting the victims IP (Internet Protocol) address allowing the attacker to do further attacks with it  https://cdn.discordapp.com/attachments/1083151053962367027/1156082618224357416/image.png?ex=6513ad57&is=65125bd7&hm=3d1b674009f0eb926c556fcf73f8f8c705f66389f0b6531c4312b80f30238cac&  If the victim puts in their account details, they are very easily compromised, and they would be none the wiser as all the page does after is refresh them to the real site and the average user would think none the wiser |
| **Improvement Objective** | The objective for improvement is to effectively train employees to identify a phishing attack from scam emails. Less usernames and passwords being stolen and blocking the phishing links with IPS |
| **Actions for Implementation** | Check vulnerability 1 in the spreadsheet [Vulnerability assessment](../../../:x:/r/sites/CertIV-CyberSecurityProject/_layouts/15/Doc.aspx?sourcedoc=%7BA46EF221-FFFC-4F8A-8A93-D18DB44C5EB5%7D&file=Vulnerability%20Assessments.xlsx&action=default&mobileredirect=true) |
| **Strategies and Processes** | Check vulnerability 1 in the spreadsheet [Vulnerability assessment](../../../:x:/r/sites/CertIV-CyberSecurityProject/_layouts/15/Doc.aspx?sourcedoc=%7BA46EF221-FFFC-4F8A-8A93-D18DB44C5EB5%7D&file=Vulnerability%20Assessments.xlsx&action=default&mobileredirect=true) |
| **Timeline** | Check vulnerability 1 in the spreadsheet [Vulnerability assessment](../../../:x:/r/sites/CertIV-CyberSecurityProject/Shared%20Documents/Vulnerability%20Assessments.xlsx?d=wa46ef221fffc4f8a8a93d18db44c5eb5&csf=1&web=1&e=vfRsk9) |
| **Resources** | Check vulnerability 1 in the spreadsheet [Vulnerability assessment](../../../:x:/r/sites/CertIV-CyberSecurityProject/_layouts/15/Doc.aspx?sourcedoc=%7BA46EF221-FFFC-4F8A-8A93-D18DB44C5EB5%7D&file=Vulnerability%20Assessments.xlsx&action=default&mobileredirect=true) |
| **Person(s) Responsible** | Check vulnerability 1 in the spreadsheet [Vulnerability assessment](../../../:x:/r/sites/CertIV-CyberSecurityProject/_layouts/15/Doc.aspx?sourcedoc=%7BA46EF221-FFFC-4F8A-8A93-D18DB44C5EB5%7D&file=Vulnerability%20Assessments.xlsx&action=default&mobileredirect=true) |
| **Verification Method & Procedure** | * Less cases of phishing attacks |
| **Results from Verification and Changes** | Blocking links from cloudflare through CCproxy prevented anyone from being able to access the malicious site |
| **Vulnerability 2** | |
| **Description** | **No IDS/IPS to monitor and block suspicious traffic** |
| **Results from Testing** | Vulnerability testing revealed that there is no threat detection or response which allowed us to execute a Syn Flood attack, port scans, ARP spoofing and confirmed that a wide range of other network attacks would be possible. |
| **Improvement Objective** | Our key objective for improvement is to implement and IDS/IPS that will monitor network traffic to detect potentially malicious activity and when needed, respond by blocking the host involved. |
| **Actions for Implementation** | Refer to vulerability 2 of the spreadsheet  [https://rmiteduau.sharepoint.com/:x:/r/sites/CertIV-CyberSecurityProject/\_layouts/15/Doc.aspx?sourcedoc=%7BA46EF221-FFFC-4F8A-8A93-D18DB44C5EB5%7D&file=Vulnerability%20Assessments.xlsx&action=default&mobileredirect=true](../../../:x:/r/sites/CertIV-CyberSecurityProject/_layouts/15/Doc.aspx?sourcedoc=%7BA46EF221-FFFC-4F8A-8A93-D18DB44C5EB5%7D&file=Vulnerability%20Assessments.xlsx&action=default&mobileredirect=true) |
| **Strategies and Processes** | [*https://rmiteduau.sharepoint.com/:x:/r/sites/CertIV-CyberSecurityProject/Shared%20Documents/Vulnerability%20Assessments.xlsx?d=wa46ef221fffc4f8a8a93d18db44c5eb5&csf=1&web=1&e=eTOZXQ*](../../../:x:/r/sites/CertIV-CyberSecurityProject/Shared%20Documents/Vulnerability%20Assessments.xlsx?d=wa46ef221fffc4f8a8a93d18db44c5eb5&csf=1&web=1&e=eTOZXQ) |
| **Timeline** | [*https://rmiteduau.sharepoint.com/:x:/r/sites/CertIV-CyberSecurityProject/Shared%20Documents/Vulnerability%20Assessments.xlsx?d=wa46ef221fffc4f8a8a93d18db44c5eb5&csf=1&web=1&e=eTOZXQ*](../../../:x:/r/sites/CertIV-CyberSecurityProject/Shared%20Documents/Vulnerability%20Assessments.xlsx?d=wa46ef221fffc4f8a8a93d18db44c5eb5&csf=1&web=1&e=eTOZXQ) |
| **Resources** | [*https://rmiteduau.sharepoint.com/:x:/r/sites/CertIV-CyberSecurityProject/Shared%20Documents/Vulnerability%20Assessments.xlsx?d=wa46ef221fffc4f8a8a93d18db44c5eb5&csf=1&web=1&e=eTOZXQ*](../../../:x:/r/sites/CertIV-CyberSecurityProject/Shared%20Documents/Vulnerability%20Assessments.xlsx?d=wa46ef221fffc4f8a8a93d18db44c5eb5&csf=1&web=1&e=eTOZXQ) |
| **Person(s) Responsible** | [*https://rmiteduau.sharepoint.com/:x:/r/sites/CertIV-CyberSecurityProject/Shared%20Documents/Vulnerability%20Assessments.xlsx?d=wa46ef221fffc4f8a8a93d18db44c5eb5&csf=1&web=1&e=eTOZXQ*](../../../:x:/r/sites/CertIV-CyberSecurityProject/Shared%20Documents/Vulnerability%20Assessments.xlsx?d=wa46ef221fffc4f8a8a93d18db44c5eb5&csf=1&web=1&e=eTOZXQ) |
| **Verification Method & Procedure** | Following implementation, a series of tests including a Syn Flood, Arp poising and port scans will be performed against various critical network devices and Snort will be monitored to ensure it is detecting and blocking the attacks. |
| **Results from Verification and Changes** | * Snort was installed. * Rulesets were downloaded. * Interfaces were configured. * Logging enabled. * Confirmed alerts were triggering. |
| **Vulnerability 3: Wi-Fi Vulnerability + ARLO nanny cam not secured** | |
| **Description** | *Staff networks into the website using personal devices, when off-site the staff uses their own networks which includes mobile phone, tethering, free Wi-fi hotspots and home networks. This network is not configured to hash and encrypt the data during transit, thereby allowing attackers to exploit through multiple methods such as MiTM, Evil Twin Attack, Eavesdropping, Session Hi-jacking.*  *ARLO nanny cam is not configured to be on a secure network within the wifi, there is only one network from the clients information that they have provided.* |
| **Results from Testing** | **They wish this to remain as a lifestyle business so infrastructure includes portable devices that can be used on and offsite including laptop computers, printers, normal peripheral devices (wireless keyboards and mice), USBs / external drives. The current office contains an ARLO nanny-style cam connected to the WIFI and accessible by the company directors when they receive a notification of movement in the office outside of business hours.**  **Staff accesses the workplace network to run their personal devices included smart phones, tablets, and laptops (as needed). The staff currently use their own networks when offsite. This includes tethering to a mobile phone, using free Wi-Fi hotspots and accessing home networks.**   * **Vulnerability identified:**   + **Portable devices can connect to the network without restrictions and no implementation of security policies to prevent external connection.**   + **No mention of Wi-Fi Cloaking/SSID broadcast is enabled.**   + **No set up of a proxy to encrypt data traffic.**   + **No limitation of network access such as after-hours, website filters.**   + **No mention of Wi-Fi security enabled.**   + **No mention of router security or firmware upgrade/patches.**   + **Remote desktop management was not disabled if the Wi-Fi were to be connected to.**   + **Devices that are connected may not be up to date/recently patched for security exploits.**   **The current office contains an ARLO nanny-style cam connected to the WIFI and accessible by the company directors when they receive a notification of movement in the office outside of business hours.**   * Vulnerability found:   + Not put into a separate network within the office.   + Not configured off the default settings.   + No mention of security/firmware upgrade/patches. |
| **Improvement Objective** | *Improvement objective for the Wi-Fi Vulnerability:*   * + *Should not be able to connect to wifi on a guest or random stranger’s device.*   + *Should not be able to see the Wi-Fi broadcasting to snoop around.*   + *Should not be able to configure the device remotely once accessed.*   + *Access to nanny-cam is denied unless coming from company directors device.* |
| **Actions for Implementation** | Refer to vulnerability 3 of the document  [https://rmiteduau.sharepoint.com/:x:/r/sites/CertIV-CyberSecurityProject/\_layouts/15/Doc.aspx?sourcedoc=%7BA46EF221-FFFC-4F8A-8A93-D18DB44C5EB5%7D&file=Vulnerability%20Assessments.xlsx&action=default&mobileredirect=true](../../../:x:/r/sites/CertIV-CyberSecurityProject/_layouts/15/Doc.aspx?sourcedoc=%7BA46EF221-FFFC-4F8A-8A93-D18DB44C5EB5%7D&file=Vulnerability%20Assessments.xlsx&action=default&mobileredirect=true) |
| **Strategies and Processes** | Refer to vulnerability 3 of the document  [https://rmiteduau.sharepoint.com/:x:/r/sites/CertIV-CyberSecurityProject/\_layouts/15/Doc.aspx?sourcedoc=%7BA46EF221-FFFC-4F8A-8A93-D18DB44C5EB5%7D&file=Vulnerability%20Assessments.xlsx&action=default&mobileredirect=true](../../../:x:/r/sites/CertIV-CyberSecurityProject/_layouts/15/Doc.aspx?sourcedoc=%7BA46EF221-FFFC-4F8A-8A93-D18DB44C5EB5%7D&file=Vulnerability%20Assessments.xlsx&action=default&mobileredirect=true) |
| **Timeline** | Refer to vulnerability 3 of the document  [https://rmiteduau.sharepoint.com/:x:/r/sites/CertIV-CyberSecurityProject/\_layouts/15/Doc.aspx?sourcedoc=%7BA46EF221-FFFC-4F8A-8A93-D18DB44C5EB5%7D&file=Vulnerability%20Assessments.xlsx&action=default&mobileredirect=true](../../../:x:/r/sites/CertIV-CyberSecurityProject/_layouts/15/Doc.aspx?sourcedoc=%7BA46EF221-FFFC-4F8A-8A93-D18DB44C5EB5%7D&file=Vulnerability%20Assessments.xlsx&action=default&mobileredirect=true) |
| **Resources** | Refer to vulnerability 3 of the document  [https://rmiteduau.sharepoint.com/:x:/r/sites/CertIV-CyberSecurityProject/\_layouts/15/Doc.aspx?sourcedoc=%7BA46EF221-FFFC-4F8A-8A93-D18DB44C5EB5%7D&file=Vulnerability%20Assessments.xlsx&action=default&mobileredirect=true](../../../:x:/r/sites/CertIV-CyberSecurityProject/_layouts/15/Doc.aspx?sourcedoc=%7BA46EF221-FFFC-4F8A-8A93-D18DB44C5EB5%7D&file=Vulnerability%20Assessments.xlsx&action=default&mobileredirect=true) |
| **Person(s) Responsible** | Refer to vulnerability 3 of the document  [https://rmiteduau.sharepoint.com/:x:/r/sites/CertIV-CyberSecurityProject/\_layouts/15/Doc.aspx?sourcedoc=%7BA46EF221-FFFC-4F8A-8A93-D18DB44C5EB5%7D&file=Vulnerability%20Assessments.xlsx&action=default&mobileredirect=true](../../../:x:/r/sites/CertIV-CyberSecurityProject/_layouts/15/Doc.aspx?sourcedoc=%7BA46EF221-FFFC-4F8A-8A93-D18DB44C5EB5%7D&file=Vulnerability%20Assessments.xlsx&action=default&mobileredirect=true) |
| **Verification Method & Procedure** | * *Check the configurations of the Wi-Fi Router.* * *Check if SSID broadcast was enabled.* * *Check if access required authorization.* * *Check MAC filtering permissions set to only permit company directors mac address devices to be able to connect to ARLO nanny-cam.* |
| **Results from Verification and Changes** | * *Wi-Fi Router was configured correctly*   + *SSID option to broadcast was disabled, requiring manual name input to connect to Wi-Fi Network.*   + *WPA2 Security is used. AES encryption is used.*   + *Firmware is upgraded.*   + *Maximum number of users was reassigned to appropriate amount (5/10/15)*   + *Administrative settings were configured:*     - *Changed default administrative username and password.*     - *Applied web filtering.* * ARLO nanny-cam was fixed   + Separate network, broadcast disabled.   + WPA2 security and AES encryption is being used for the network.   + Firmware and software upgraded and patched.   + MAC addressed filtered to only permit access by company dire |
| **Vulnerability 4:** | |
| **Description** | *Back-up: Only one (physical) form of back-up is utilised by the client.*  *The issue with relying on one form of backup is the possibility of it failing during a recovery process. Such risk includes physical deterioration of the device (external hard drive), exposure from fire or natural disasters, and theft.* |
| **Results from Testing** | *Client runs the website in the cloud, but only have the physical website files backed up to an external hard drive.*  *An alternative back-up source has not been established and implemented I.e. Cloud service like Microsoft Azure* |
| **Improvement Objective** | *Improvement is to facilitate Azure as an additional source of back-up for the client which can be integrated seamlessly into the existing business infrastructure.*  *The proposed solution of establishing a Cloud environment (to help provide an alternative source of back-up) is proved to be effective when configurations are set to backup critical files on a regular basis, as well as encrypting data at rest, activating data recovery service, and implementing appropriate access controls* |
| **Actions for Implementation** | *Step 1: Set up Microsoft Azure Account* *(this will serve as the primary storage location for website files backup)*  *[1.] Create storage account on Azure portal* *[2.] Configure the storage account (Name, Region for data residency, Performance tier e.g. Standard/Premium SSD; Encryption*  *Step 2: Set up Backup configuration using Azure Backup to regularly backup files.*  *[1.] Select Azure Backup service for backups* *[2.] Define frequency of backup (e.g. daily, weekly), how long backups should be retained (e.g. 30 days, 90 days), and which resource should be backed up. Critical files and data should be backed up on a frequent basis, and less important files can be backed up on less often basis.* *[3.] Create & configure a Backup Vault (e.g. backup policy, retention setting)*  *Step 3: Automate the backup process through Azure Functions*  *[1.] Create triggers for scheduled backups (e.g. daily at midnight) or event-based backups triggered by changes in website files*  *Step 4: Enable data encryption at rest and in transit to ensure the security of backup data*  *[1.] Configure encryption during Storage Account creation using appropriate encryption option (e.g. SSE with storage service encryption)* *[2.] Ensure data transmitted between the virtual server and Azure Storage is encrypted*  *Step 5: Provide appropriate access to personnel in relation to company backup process and procedures*  *[1.] Assign appropriate roles to personnel involved in back-up I.e., IT Administrator/s* |
| **Strategies and Processes** | *[Step 1.] Create and set up an Azure Storage Account and configure its security settings*  *[Step 2.] Configure backup policies (I.e., specific files, frequency of backups, scheduling of backups)*  *[Step 3.] Configure Azure backup to automate backup schedule for integral company files*  *[Step 4.] Enable data and file encryption*  *[Step 5.] Train IT Administration on Azure Backup management and policies* |
| **Timeline** | *Step 1 – approx. 1 day* *Step 2 – approx. 3 to 5 days* *Step 3 – approx. 2 to 5 days* *Step 4 – approx. 2 to 5 day* *Step 5 – approx. 3 to 7 days* |
| **Resources** | *People: Cloud Engineer; IT staff*  *Space: Cloud, using Azure Storage (100 GB)*  *Time: approximately up to 7 days to implement cloud backup system. Breakdown of timeline in detail:*  [https://rmiteduau.sharepoint.com/:x:/r/sites/CertIV-CyberSecurityProject/\_layouts/15/Doc.aspx?sourcedoc=%7BA46EF221-FFFC-4F8A-8A93-D18DB44C5EB5%7D&file=Vulnerability%20Assessments.xlsx&action=default&mobileredirect=true](../../../:x:/r/sites/CertIV-CyberSecurityProject/_layouts/15/Doc.aspx?sourcedoc=%7BA46EF221-FFFC-4F8A-8A93-D18DB44C5EB5%7D&file=Vulnerability%20Assessments.xlsx&action=default&mobileredirect=true)  *Cost: $69 AUD/month (Pay-you-go subscription)* |
| **Person(s) Responsible** | *Cloud Engineer (to create and implement cloud infrastructure)* *IT Administrator (to manage access control, data encryption, checking of backup files and scheduling of backups; also responsible in data recovery process)* |
| **Verification Method & Procedure** | * *Check if Azure account was created and configured correctly (Region, Premium SSD, Encryption at rest) to facilitate business infrastructure and current operations* * *Check backup service is defined appropriately. Frequency, type of resources and directories should be set correctly* * *Check if automated backup is activated – either scheduled or event-based (e.g. changing critical website files)* * *Check if data encryption at rest and in transit is configured* * *Ensure staff has correct level of access to resources* |
| **Results from Verification and Changes** | * *Azure File Storage is created* * *Data backup is established and configured with on-going and scheduled backups of files* * *Data Recovery services Vault is created and configured* * *Regular maintenance schedule in checking backup files*   Inserting image... |
| **Vulnerability 5:** | |
| **Description** | *Shared staff logins and accounts, with login details being recorded manually in a spreadsheet.* |
| **Results from Testing** | *Anyone including the janitor has access to shared staff accounts for applications, software and the website. The spreadsheet with all the logins recorded is insecurely stored in plain text so unauthorised access will leave all the employee's accounts compromised.* |
| **Improvement Objective** | *Create a hierarchical, structured environment with separate accounts for each individual and grouping these users into their appropriate permissions. These user details will also be stored in AES-256, which is the encryption for default policy settings. Ref:* [*https://www.ibm.com/docs/en/engineering-lifecycle-management-suite/lifecycle-management/6.0?topic=encryption-enforcing-algorithms-domain-clients*](https://www.ibm.com/docs/en/engineering-lifecycle-management-suite/lifecycle-management/6.0?topic=encryption-enforcing-algorithms-domain-clients)  *Penetration tests and audits can check if the environment is structured appropriately, checking whether people can gain unauthorised access to accounts or permissions outside their responsibilities.* |
| **Actions for Implementation** | *Check vulnerability 5 in the spreadsheet* [*Vulnerability Assessments.xlsx*](../../../:x:/r/sites/CertIV-CyberSecurityProject/Shared%20Documents/Vulnerability%20Assessments.xlsx?d=wa46ef221fffc4f8a8a93d18db44c5eb5&csf=1&web=1&e=vfRsk9) |
| **Strategies and Processes** | *Check vulnerability 5 in the spreadsheet* [*Vulnerability Assessments.xlsx*](../../../:x:/r/sites/CertIV-CyberSecurityProject/Shared%20Documents/Vulnerability%20Assessments.xlsx?d=wa46ef221fffc4f8a8a93d18db44c5eb5&csf=1&web=1&e=vfRsk9) |
| **Timeline** | *Check vulnerability 5 in the spreadsheet* [*Vulnerability Assessments.xlsx*](../../../:x:/r/sites/CertIV-CyberSecurityProject/Shared%20Documents/Vulnerability%20Assessments.xlsx?d=wa46ef221fffc4f8a8a93d18db44c5eb5&csf=1&web=1&e=vfRsk9) |
| **Resources** | *Check vulnerability 5 in the spreadsheet* [*Vulnerability Assessments.xlsx*](../../../:x:/r/sites/CertIV-CyberSecurityProject/Shared%20Documents/Vulnerability%20Assessments.xlsx?d=wa46ef221fffc4f8a8a93d18db44c5eb5&csf=1&web=1&e=vfRsk9) |
| **Person(s) Responsible** | *Check vulnerability 5 in the spreadsheet* [*Vulnerability Assessments.xlsx*](../../../:x:/r/sites/CertIV-CyberSecurityProject/Shared%20Documents/Vulnerability%20Assessments.xlsx?d=wa46ef221fffc4f8a8a93d18db44c5eb5&csf=1&web=1&e=vfRsk9) |
| **Verification Method & Procedure** | 1. *Pen testing by hiring specialists who attempt to gain unauthorised access to accounts* 2. *Regular internal and/or external audits for account security and general cyber security compliance* 3. *Ensure secure logins*    1. *Forced minimum password complexity upon creation*    2. *Password expiration after a regular interval (3 months)*    3. *Compulsory multi-factor authentication* |
| **Results from Verification and Changes** | 1. *AD shows all users (employees) have their own individual account.* 2. *Group policy corresponding to specific permissions are assigned to users with relevant roles/jobs.* 3. *Login details are stored securely and not manually sent and recorded from emails.* 4. *Users are securely logging in with an enforced minimum password policy.* 5. *Proxy server with AD showed internet activity linked with each user account.* |

+ Add Rows as Required

**Appendix 5 – Technical Documentation**

**Instructions:**

Use each of the headings below to plan and prepare your technical documentation.

You must address each heading and its prompts with knowledge and instructions in plain-English. You should assume that the end-user is a lay person with no experience in cybersecurity. This means you should consider the who, what, when, where how and why of each prompt and use screen shots, images, and diagrams where possible.

**How you the end-user support the process of cyber-risk assessment**

**What is the process of cyber risk assessment?**

The process of cyber risk assessment involves several steps. **Risk identification, risk assessment** and **risk treatment**.

**How is cyber risk assessment carried out?**

The risk assessment is carried out in phases beginning with:

**Risk identification** steps:

**Determine information value.**

**Identify and Prioritize Assets.**

Begin with collection of all devices and information owned or managed by the organization are assets. Gathered assets must be inventoried and assessed for the level of protected needed to thwart potential attacks. Asset management will consist of inventorying all assets, and then develop and implement policies and procedures to protect them.

**Identify the Threats.**

What are the possible vulnerabilities of a system?

Who may want to exploit those vulnerabilities to access specific information assets?

What are the consequences if system vulnerabilities are exploited, and assets are lost?

**Identify Vulnerabilities.**

* Internal system compromise?
* Stolen Customer Data?
* Phony transactions from an external server?
* Data input errors?
* Data centre destruction?

**Calculate the likelihood and impact of various scenarios on a Per-Year Basis, prioritize risks based on the cost of prevention vs information value, Document results in risk report, Implement and monitor security controls.**

**Risk Assessment are categorized into three categories.**

High risk: Negligence means that no actions or controls are taken to lower risk. Threat is very high, and the cost of incident would be catastrophic.

Lower risk: Exercising due care can help lower the level of the risk. Risk still exists but these reasonable steps lower the potential loss.

Acceptable risk: exercising due diligence involves taking reasonable step to eliminate the risk. Some risks still exist, but multiple controls are implemented to prevent potential loss.

**Risks can be internal, external, or even both.**

**Quantitative risk analysis or Qualitive risk analysis difference, following the examples below.**

|  |  |
| --- | --- |
| Quantitative Risk Analysis | Qualitative Risk Analysis |
|  |  |

**Proceed with a Risk Treatment Solution:**

* + **Employ Security Control to mitigate risk.**
    - **Administrative Controls** – Consisting of procedures and policies that organisations put into place when dealing with sensitive information. This determines how people act.
    - **Technical Control –** Consists of hardware/software implemented to manage risk and provide protection.
    - **Physical Control –** Consists of mechanism such as fences, locks, keycard scanners being deployed to protect systems, facilities, personnel, and resources. Physical controls physically separate people or other threats from systems.
  + **Avoid the risk by eliminating corresponding activities.**
  + **Transfer risk to external party i.e., insurance**
  + **Accept the risk.**

**What role and how can end-users play in the process of cyber-risk assessment?**

End-users are the first line of defence against cybersecurity attacks and can help in the prevention of cyber incidents by following the best practices and reporting suspicious activities. They also contribute to the risk assessment process through identifying potential risks and vulnerabilities in their systems and networks, they provide feedback on the effectiveness of security controls and help prioritise risks based on their impact on business operations, and they can be trained to recognize observable phishing cues and lures that appear in websites, emails, and social networks. They need systematic, coordinated, and integrated training to do this.

**What are the business implications of the types of vulnerabilities and cyber security breaches you identified in your initial investigations?**

* + Business implications of being breached by a **Phishing attack**:

Loss of Money: Phishing attacks can lead to financial losses from theft of funds to fraudulent actions, Loss of intellectual property: Theft of intellectual property because of a successful phishing campaign can be the most destructive loss of all. Trade secrets, research, lists of customers, formulas, new development are the vectors that would be impacted. Damage to reputation when announcing the breach, the reputation takes a sudden hit. Loss of business will follow and news about the breach will happen.

Disruption of operational activities: Cyber-attacks causes major damage to business.

* + Business implications **not having an IPS/IDS system to detect and respond to suspicious traffic**:

Increased risk of cyber-attacks: No IDS/IPS implemented, businesses would be more vulnerable to a cyber-attack, which will lead to a data breach, financial loss and damage to reputation, Increased response time: Without an IDS/IPS, businesses will take longer to detect and respond to cyber-attacks, which can lead to considerable damage being done before the attack is stopped and loss of customer trust: a data breach will lead to the loss of customer trust.

* + Business implications of being breached **without Wi-Fi VPN to filter data:**

Increased risk of cyber-attacks: Without VPN, businesses are particularly more vulnerable to attacks which can lead to data breaches, financial losses, and a stain to their reputation/damage to reputation.

Increased cost: The cost of a cyber-attack can be quite significant. Without VPN, businesses may spend a lot more money on remediation efforts and repairing the damage caused by the attacks and a considerable loss of customer trust.

* + Business implications of being breached by an attack while **website files are backed up to a physical external hard drive only:**

Loss of data: Damaged/Stolen physical hard drives can lead to data loss, the business may lose all its website files. This can lead to an incredibly significant downtime and loss of revenue. Increased cost: Just like having no VPN, a business will use a lot more money on remediation efforts and repairing the damage and they can receive damage to their reputation.

* + Business implications of being breached and having staff login details all recorded manually in a spreadsheet:

Loss of Data: Stolen or damage data will lead to significant downtime and loss of revenue.

Increased risk of cyber-attacks: The login details open the window for further attacks which will increase the cost and could cause significant destruction of data. Irrefutable damage to reputation: With this breach announced, the reputation immediately plummets to the bottom, this will tarnish the image and will liquidate the organisation.

**What are the implications to the user if they do not adopt or implement the solution?**

Users will suffer from negligence and be held accountable in court and will be investigated in which they shall be in legal liability which extends to the whole organisation and be exposed to risk of identity theft, financial fraud, financial losses, and other cyber-related crimes.

**Operating systems (Windows or Linux)**

* Give an overview of how the operating system used within the organisation is vulnerable to cybersecurity risks.

*Below are details on the current configuration of the operating system or its application. Any associated risks are also listed.*

1. *Issue: Login details for new users are emailed to them, and separately recorded manually in a spreadsheet.*

*Risk: Accounts will be compromised if unauthorised access to the login spreadsheet or any emails sending account details, given both store the username and password in plain text.*

1. *Issue: Although no details are given, there is no indication of an organised, hierarchical domain structure existing either.*

*Risk: Employees should have different account permissions and access corresponding to their job’s role, otherwise unnecessary/unauthorised access is automatically given to others. Companies have an internal hierarchy organised into an appropriate structure, so network permissions should correspond to this.*

1. *Issue: Currently lacking OS related cyber security policies, such as…* 
   1. *A software updating policy.*

*Risk: Outdated software may have known vulnerabilities that may be taken advantage of. Security updates help patch these vulnerabilities.*

* 1. *A mandatory anti-malware software.*

*Risk: If a device is breached, detection of suspicious activity will be harder to identify without an anti-malware program. Anti-malware can also prevent malware from spreading by quarantining and deleting affected area.*

* 1. *Software firewall must always be on.*

*Risk: A firewall protects against foreign traffic, so having an inactive software is more vulnerable to many attacks such as port scanning, certain DoS flood attacks, and malware is more easily installed.*

* Describe two methods the user can implement to improve security when using the operating system identified.

*Solutions include…*

1. *Using an* ***active directory*** *with group policy to create a hierarchical, organised structure for users. Employee account can be grouped based on which permissions are necessary for their role and responsibilities. This includes having the few but necessary IT/managerial staff with admin privileges to reset passwords in case users forget their password.*

*Users can be forced to change their initial password upon creation in the account in the active directory and may also reset their own password at will. The details will be stored securely in the active directory using AES-256 by default, so the final login details will neither be present in emails nor stored in plain text.*

*Configuration:*

* *2 users with access to admin privileges: Company director in charge of admin and IT staff*
* *Hierarchical AD structure with group policy corresponding to responsibilities in the company.*
* *Shared folders with access given through group permissions.*
* *Limited permissions for employees including limiting control panel and other security changes.*
* *Integration with other essential services such as a proxy server.*

*Training for use:*

* 1. *Add a new user to AD and group policy.*
  2. *Change permissions of user/group.*
  3. *Changing password*

1. *Regular forced software* ***updates*** *and use of* ***anti-malware*** *software.*

* *Anti-malware applications can help detect malware earlier and remove suspicious software. Some anti-malware programs may prevent downloading suspicious material and other cyber security features.*
* *Timely software updates can prevent discovered security vulnerabilities from being taken advantage of by bad actors, help minimise risks.*

*Implementation:*

1. *Mandatory installation and regular scans using the anti-malware software. Regular reminders can be configured.*
2. *Software updates can be logged, checked and the user can be alerted to available updates. Company devices can also be configured to automatically update every night when not in use.*

*Necessary training:*

1. *Teaching how to use an anti-malware software.*
2. *Informing employees potential damages from a breach to the individual and company.*
3. *(Related but not directly related to OS) Prevent viewing or installing data from suspicious sources to avoid the initial breach.*

**Virtualisation operation and structure**

* Explain what virtualisation is and why the end-user needs to use it.

Virtualisation facilitates multi-tasking of operating systems on a hardware computer. It creates a virtual (rather than actual) environment of computer hardware, allowing users to use their computer's resources more efficiently. Virtualisation is a cost-effective and efficient (e.g., time and space) alternative to computing, since users don't need a separate physical computer for each task.

A proposed solution to virtualisation for the user is to migrate over to a cloud platform like Microsoft Azure.

By transferring an existing business infrastructure over to Microsoft Azure, the business can utilise Windows Server to run regular file backup and use the same running database (which can be backed up in cloud). In addition, this method offers portability and savings in costs since it saves time in maintenance and troubleshooting.

Integrating Azure is beneficial for the business for a number of reasons including:

* Hosting a website through a web domain, like GoDaddy.com, can be an expensive and labour-intensive process in hosting multiple servers (i.e. redirecting all files and resources while a website is operating constantly at the same time). This methodology does not allow the anticipation for surges in traffic in the future, and therefore, creating issues around load balancing and expandability of business operations.  
     
  Opting for an Azure-based solution enables the user to:   
  - only pay for resources that are used (with upfront quotation and approximate pricing models catered to changing infrastructure and operational costs),  
   - scale resources up or down based on traffic demands (ensuring a website remains available and responsive). Administrators can create and run additional servers on Azure, enabling hosting of the company website offsite, and therefore, authentication of users can occur closer to site,   
  - access load balancing services to prevent overloading of a single server and improve website performance,  
  - access redundancy and failover options (ensuring the website remains operational even if one server or data centre experiences issues),  
   - streamline deployment and management of web applications, reducing labour-intensive tasks and the need for constant manual intervention,  
   - implement built-in security features and compliance certifications to help protect a website and customer data,  
   - access data centres around the world through cloud provider (Azure), enabling service of content from locations that are geographically closer to certain users, reducing latency and improving user experience
* Open access to internal company files containing sensitive data (e.g., Excel spreadsheet containing staff login details) and openness of user login access within a business can create security vulnerabilities. Without correctly assigned access groups and file protection, unauthorised users are permitted to access the web server, to view, modify, or remove any file that is made available on the company website.  
   By hosting files in the cloud, authorised users can remote in to access files (e.g., via laptop; personal hot spot through mobile device and VPN in). Therefore, it is ideal for the user to create Windows 10 virtual machines in the cloud so authorised users can connect via remote desktop to VPN in to access company data and files using approved company equipment and devices.  
   Through Azure’s Active Directory, authorised users can control and manage access to resources. Additional features like multi-factor authentication (MFA), conditional access and identity protection can enhance the security of user login access. Role-Based Access Control (RBAC) allows a user to assign specific roles and permissions to other users, ensuring that only authorised personnel can access sensitive files.  
   Encryption solutions are also provided through Azure for data at rest and in transit. Files and databases can be encrypted to protect sensitive data against unauthorised access.
* The creation of replica of domain controller via cloud increases reliability and availability of site access and control. If the business expands, administrators can add more replica domain controllers in Azure to accommodate increased demands on Active Directory services. Robust security features including setting correct permissions to specific role-based groups to manage website, files and resources can enhance the overall security of the infrastructure.
* Explain how they access the virtualisation.

Accessing Microsoft Azure as a user can be conducted through Azure Portal. Azure Portal is a user-friendly web-based interface.

First log into the Azure account via the portal, or create an Azure account by:

* Going to the Microsoft Azure website: [https://azure.com](https://azure.com/).
* Select "Start free" or "Create a free account". Click on the relevant option to begin the account creation process
* Sign in with an existing Microsoft account (e.g., Outlook.com, Hotmail, or Xbox Live account) or create a new Microsoft account
* The user will need to provide some basic information, including name, phone number, email address, location for identity verification.
* Microsoft will send a verification code to the provided phone number or email. Enter the code to confirm your identity.
* The user will need to provide billing information to verify user identity. This is to ensure that the user can continue using Azure services if they exceed the free tier limits.
* Review and accept Microsoft's terms and conditions, and complete the account creation process.
* Once the account is created, the user can access the Azure Portal and start using Azure services.

To back up files in Azure, a user can use Azure Backup. An overview of creating Azure Backup:

* In the Azure Portal, search for "Recovery Services Vaults" and create a new vault. This vault will manage backups.
* Set up backup policies for your files, specifying what to back up, how often, and where to store the backups.
* On the machine the user wants to back up, install the Azure Backup Agent. This agent helps Azure communicate with computer/s and servers.
* Use the Azure Backup Agent to configure a backup schedule, including which files or folders to back up.
* The user can monitor the status of backups in the Recovery Services Vault. If the user needs to restore files or systems, the user can do so from the vault.
* Explain the structure of the virtualisation.

Microsoft Azure facilitates various cloud services and structures to support virtualisation, such as:

* Services are segregated by regions. These regions are located globally and provide the physical infrastructure where digital resources are hosted.
* Hosting of data centres within each Azure region. These data centres are secured sites that house the physical servers and networking equipment required to run Azure services. They are designed to be resilient and fault-tolerant.
* Subscription based service for provisioning and management of Azure resources. Multiple subscriptions are applicable across different purposes (i.e., development, testing, production).
* Resource groups are logical depositories that help users organise and manage Azure resources. A user can delete, move, or monitor all the resources within a resource group collectively.
* Azure Virtual Network establishes the infrastructure for communication between resources. A user can allocate IP address ranges, subnets, and security rules to control how resources interact.
* Custom Virtual machine images can be created to capture VM configurations, applications and data. These images can be used to deploy consistent VMs. VMs are integral components in virtualisation where various operating systems host applications and services. Running multiple VMs on a single physical server is possible in Azure through a software layer referred to as ‘hypervisor’.
* Identity and Access Management (IAM) is responsible for managing user access to Azure resources. It includes Azure Active Directory for identity services and Role Based Access Controls
* Tools like Azure Monitor and Azure Security Centre monitor, manage, and secure resources. These tools offer insights into resource health and performance.
* Azure Policy allows a user to define and enforce governance rules for resources. It ensures compliance with organisational standards and regulations.
* Azure Cost Management helps track and optimise expenditure on Azure resources. It provides cost analysis, budgeting, and alerts.
* Give instructions for each of the following as they related to your planned solution:
* Creating and configuring virtualised images

To create and configure virtualised images (e.g., Windows Server; Windows 10):

1. Login to Azure Portal website [https://portal.azure.com](https://portal.azure.com/)
2. In the left menu panel, click ‘Virtual machines’, then ‘Create’.  
    Alternatively, go to the Azure services section and click ‘Virtual machines’ then ‘Create’.
3. Fill out the basic settings of the virtual machine, including:  
    *Subscription*  
    *Resource* *group* (choose an existing group or create a new group by clicking ‘Create New’)  
    *Virtual* *machine* *name* (e.g., SVR2 for Windows Server; Client2 for Windows 10 computer)  
    *Region* (location of where the VM resources will be created e.g., Australia East)  
    *Image* (select Windows Server 2022 Datacentre for server, and Windows 10 Pro for the computer)  
    *Size* (select disk size according to business requirement)
4. Under the ‘Administration account’ section, provide a username and password for VM login
5. Under ‘Inbound port rules’, select ‘allow selected ports’ for Public inbound ports, and select ‘HTTP (80), RDP (3389)’ option under ‘Select inbound port
6. Go to the next menu page by clicking ‘Next: Disk’.   
   Ensure the OS disk type is ‘Premium SSD’ and Encryption type is ‘(Default) Encryption at rest with a platform managed key’
7. Then go to ‘Next: Networking’ button, fill in the details accordingly:  
    *Virtual network* (choose a virtual network or ‘Create New’)  
    *Subnet* (allocated default option is acceptable for this example)  
    *Public IP* (‘Create New’ or choose an existing public IP)  
    *NIC Network security group* (select Basic)  
    *Public inbound ports* (choose ‘Allow selected ports’)  
    *Select inbound ports* (choose ‘HTTP (80), RDP (3389))
8. Proceed with ‘Review + Create’ button. A ‘validation passed’ notification will appear on screen once Azure validates the configured details
9. Click ‘Create’ and a success message of ‘Your deployment is complete’ will appear once the VM is created.
10. Select ‘Go to resource’ to view the newly created VM. Click ‘Connect’ to begin connecting to the VM.
11. Repeat steps 1-10 to create another VM.

* Interconnecting virtual images

To connect Virtual Machines (VM) in Azure via Domain Controller:

* Create a Virtual Network

Sign in to the Azure Portal at <https://portal.azure.com>.

Click "Create a resource," then search for and select "Virtual Network."

Follow the steps to create a virtual network, specifying address ranges, DNS settings, and resource groups. Ensure that the IP address and subnet settings are appropriate for the network design.

* Create a Domain Controller Virtual Machine

In the Azure Portal, click "Create a resource," then search for and select "Windows Server" to create a new virtual machine.

During setup, choose the virtual network as created in the first step.

Configure the VM with a static private IP address and choose the Windows Server operating system.

Install the Active Directory Domain Services (AD DS) on this VM and promote the server to the domain controller.

* Create Additional Virtual Machines

Create Window 10 virtual machines as required to connect in the same virtual network as the domain controller.  
 On each VM, join them to the domain controlled by the domain controller. This integrates them into the same Active Directory (AD) environment.

* In addition to the process of interconnecting virtual images, establish VPN connectivity by creating a Virtual Network Gateway.

In the Azure Portal, create a Virtual Network Gateway. This gateway connects your virtual network to your on-premises network.

Configure the gateway settings, including the VPN type (Site-to-Site), IP address, and shared key.

* Configure an On-Premises VPN Device

Configure the on-premises VPN device to connect to the Azure Virtual Network Gateway.

Ensure that the VPN device and Azure's Virtual Network Gateway settings match, including IP addresses and shared keys.

* Connect to Azure via VPN

Configure the on-premises VPN device to connect to Azure using the established VPN settings.

* Connect to Windows Server via RDP  
   Once the VMs are promoted to a domain controller and VPN connection is established, the user can RDP to the Windows Server  
   To RDP:

1. Configure Network Security Group (NSG) Rules to allow RDP traffic.

In the Azure Portal, go to the VM's "Networking" section.

Click "Add inbound port rule" and create a rule allowing RDP traffic on port 3389.

1. Obtain the Public IP Address:

Get the public IP address associated with the Azure VM. This information is located in the Azure Portal by navigating to the VM and checking the "Overview" section.

1. Use Remote Desktop Client:

On the local computer, open the Remote Desktop Client application.

4. Connect to the Azure VM:

In the Remote Desktop Client, enter the public IP address of the Azure VM.

5. Enter Credentials:

When prompted, enter the username and password for the Azure VM. This should be the same as the credentials as provided when creating the VM.

8. Connect:

Click "Connect" to establish the RDP session to the Azure VM.

8. Authenticate:

Authenticate with the Azure VM using the provided username and password.

9. Access the VM:

Once authenticated, the user will have full control over the Azure VM

* Removing Public IP Address:

Removing the public IP address can help reduce costs in utilising Azure resources. The user can still RDP to the Windows Server without a public IP address since VPN connectivity allows secure access to VMs over a private network.

To do this:

* In the Azure Portal, navigate to the Windows Server VM for which you want to remove the public IP address.
* In the VM settings, go to the "Networking" section.
* Disassociate the public IP configuration from the VM's network interface.
* Connect to the network by using Remote Desktop Protocol (RDP) to connect to the Windows Server using its private IP address.
* Make sure to have an alternate way to access the VM before removing the public IP address, as the user will no longer be able to access it over the public internet.

**Using networking devices**

* Explain what networking devices the end-user may need to interact with.

*End users will need to interact with:*

1. *AAA server (AD) when connected to the company’s network requires computers or other end devices used to access the network and connects to the AAA server.*
2. *Physical data storage servers where files and shared folders are stored use end device such as company computers to access this resource, connected through the company’s network to the storage server and/or cloud storage.*
3. *Company owned computers on the LAN used for internal network access and authenticating through the AAA server.*
4. *Wi-Fi router connected through an end device such as computers, phones, and IOT that require a wireless connection.*
5. *The email server use a computer or phone ultimately connected to the server in the cloud.*
6. *Web server access for staff responsible for running the website use end devices such as company computers. This is used to access the resource located virtually in the cloud.*
7. *Anywhere VPN when working remotely use devices such as a company laptop or BYOD. This will require downloading and using the company’s designated VPN application such as Cisco AnyConnect.*
8. *Windows 10 VM on the Azure cloud when working remotely connected to remote devices such as a company laptop or BYOD with remote desktop downloaded with the anywhere VPN active.*

* Give instructions for using networking devices post-implementation of your planned solution. i.e. how to gain access, how to maintain access, how to control access, how to secure etc.

1. *AAA server (AD) when connected to the company’s network.*

*Access gained: by having a user account within the active directory created by the administrator. Subsequent access requires logging in.*

*Access maintained, controlled: by managing user accounts in an organised manner within the AD and assigning user accounts to the appropriate groups with corresponding policy/permissions.*

*Access secured: by limiting access of administrator privileges to necessary individuals only.*

1. *Physical data storage servers where files and shared folders are stored.*

*Access gained: by adding relevant users to a domain group with access to specific storage resources such as shared folders.*

*Access maintained, controlled, and secured: by managing and limiting permissions through a group policy on a need-only basis.*

1. *Company devices on the LAN.*

*Access gained: by adding users to the AD and logging in to the company device with the same login credentials.*

*Access maintained, controlled, and secured: through general AD management mentioned above.*

1. *Wi-Fi router*

*Access gained, maintained, controlled, and secured: mirroring what was mentioned above with AD for logins. Users can access the internet through the AD connected to a proxy server, although not necessary for the guest Wi-Fi network.*

1. *Email server*

*Access gained, maintained, controlled, and secured through: the AD given email service integration and since every employee would have a company email DC management would centralise this process. Therefore, access controls will again mirror those given for AD above.*

1. *Web server access for staff responsible for running the website.*

*Access gained, maintained, and controlled: again, through the AD with account logins and the same management methods mentioned above. The centralised system will allow easier control and logging for records.*

*Access secured: by giving specific access to required staff only which can be controlled via the RDC given it is in the cloud and can sync with the local AD.*

1. *Anywhere VPN when working remotely.*

*Instruction: For each session, users will need to launch the VPN application, connect to the company’s portal, then login with their account details to connect to the company’s network remotely.*

*Access gained, maintained, controlled, and secured: through the AD given integration with the VPN program is possible. Access management and security will also repeat what was mentioned above.*

1. *Windows 10 VM on the Azure cloud when working remotely.*

*Access gained, maintained, controlled, and secured: through AD where the user logs in to their account within the company’s domain to access their designated VM. Access management is again repeating above but company files and data is to stay on the VM or at least have a copy saved on the VM to ensure there is a cloud backup in case there are issues with the physical device.*

**Configuring firewalls**

* Explain how firewalls are to be used in the client workplace as identified in your planned solution.

We will be installing pfSense on a dedicated physical firewall to act as a barrier between the internal and external networl then we will be installing Snort with the pfSense package manager from there we will be configuring Snort to be an IPS meaning that it will monitor network traffic for malicious activity and take action to prevent it by blocking said traffic you will also have an Oinkcode provided to you via email, this will be necessary later for Snort. This implementation in the worksplace will enhace network security

* Give instructions for configuring or maintaining the firewall as it applies post-implementation of your planned solution.

PFsense Configuration:

* You will access the firewalls GUI by entering its IP in a web browser
* Login to to PFsense through credentials provided via email
* Install Snort through the Pfsense package manager
* Copy and paste the oinkcode provided through the same email into snort

Firewall Rules:

* Configure rules that will block certain kinds of suspicious or malicious traffic based on the IP that it’s coming from
* Some suspicious traffic could be an incoming nmap scan or an attempted synflood attack

Monitoring:

* Regularly update rules to align with current emerging threats

Post-implementation you will be making sure to:

* Keep pfSense and Snort up to date
* Regularly review and update Snort rule sets
* Monitor logs
* Tune Snort to minimize false positives

**Implementing Intrusion Detection Systems (IDS)**

* Identify and explain the purpose of the intrusion detection systems (IDS) implemented by your team. Include examples of the key features to support your answer.

Intrusion detection systems are a key component of a network security perimeter that contributes to the depth of defense by acting as a second line behind the firewall. The IDS is limited to just monitoring traffic and triggering alerts based on the configured rules and as a result we are using a detection system where a prevention system cannot function.

We have used Snort to implement our IDS as a feature of our PFsense firewall however the IDS capability is only configured on the LAN side. We are using promiscuous mode to allow the IDS to monitor all traffic on the network, including traffic not flowing directly through the IDS.

The IDS implementation allows internal activity to be monitored without it needing to pass through the firewall and facilitates faster detection of threats that have compromised internal end devices such as malware or insider threats. These threats often try to stay silent by not contacting external servers and will carry out reconnaissance by scanning the network or may attempt to move laterally or escalate privileges entirely within the internal network.

By improving detection speeds of these threats a response can be initiated faster to mitigate potential damages.

* Explain how your end-user can use the IDS to examine data for and respond to anomalies in line with your planned solution.

The IDS in use, Snort, can be accessed by navigating to the web interface at 192.168.1.1. Within Snort, the end user can navigate to the 'Services tab' and select Snort from the dropdown menu.

Within the Snort user interface, the 'Alerts' menu can be opened which will allow the user to view the Alerts for each interface. Each alert will contain vital information such as the date & time, priority level, Reason for the alert as well as the source and destination IP addresses involved.

As an IDS cannot respond to threats by dropping packets or blocking hosts, it is vital to monitor these alert logs so that an appropriate response can be initiated in the event of malicious traffic.

**Implementing Intrusion Prevention Systems (IPS)**

* Identify and explain the purpose of the intrusion prevention systems (IPS) implemented by your team.

The Intrusion prevention system expands on the concept of the IDS by including automatic threat response by dropping packets and blocking hosts that are found to violate the security rules. The IPS sits behind the firewall to monitor traffic on the WAN interface which allows it work in tandem with the firewall to ensure that traffic allowed through firewall is still screened and malicious traffic is blocked.

Some protocols cannot viably be blocked completely by the firewall as they have legitimate use cases but can also be leveraged by adversaries. The IPS fills this gap by performing more thorough analysis of packets to identify signatures of known vulnerabilities, unusual traffic patterns or activity such as port scans.

The automated actions of the IPS serves to both prevent attacks as well as speed up both detection of incidents and initiate a response immediately. This mitigates the potential damages caused by threats not detected sooner and reinforces the depth of our defense.

* Explain how your end-user can use the IPS to monitor traffic and respond to anomalies in line with your planned solution.

As the IPS is an additional component of Snort which also our IDS, Alerts can be viewed manually in the same manner. The IPS is distinct however by taking an automated approach to responding. The end user can access the Snort user interface and configure a particular interface to enable blocking.

When blocking is enabled there are two primary methods, Legacy or inline, that can be used, Legacy or inline. Legacy mode will make copies of packets to analyse while still passing the original packets through until it detects a rule violation and then block any further offending packets. Inline mode analyses the original packets and does not pass them on until they have been confirmed to not violate any rules.

Legacy mode will typically have a lower impact on network performance but can result in some packets being sent on before a rule violation is triggered while Inline prevents any packets leaking but may degrade network performance further. The user should consider their priorities and desired balance between network performance and total security when selecting the one to use.

Another commonality between the IDS and IPS functions of Snort is the configuration of rulesets. These are critical to determine what triggers alerts and can be configured per interface. The same rulesets can be applied to both detection and response functions with the only difference being that Snort will block packets when in prevention mode rather than just trigger alerts.

**Appendix 6 – Lessons Learned**

**Instructions:**

* Replace the grey italic prompt text/questions with your own response. You should try to address each of the key points in the prompt text.
* You must show how you met the majority of the objectives for both the project and your team using evidence i.e. results, screen shots, meeting minutes, quotes, digital timestamps etc.
* You must identify at least one (1) improvement for each objective not achieved OR where you met all objectives, one (1) improvement for each of the possible improvement prompts in the table.

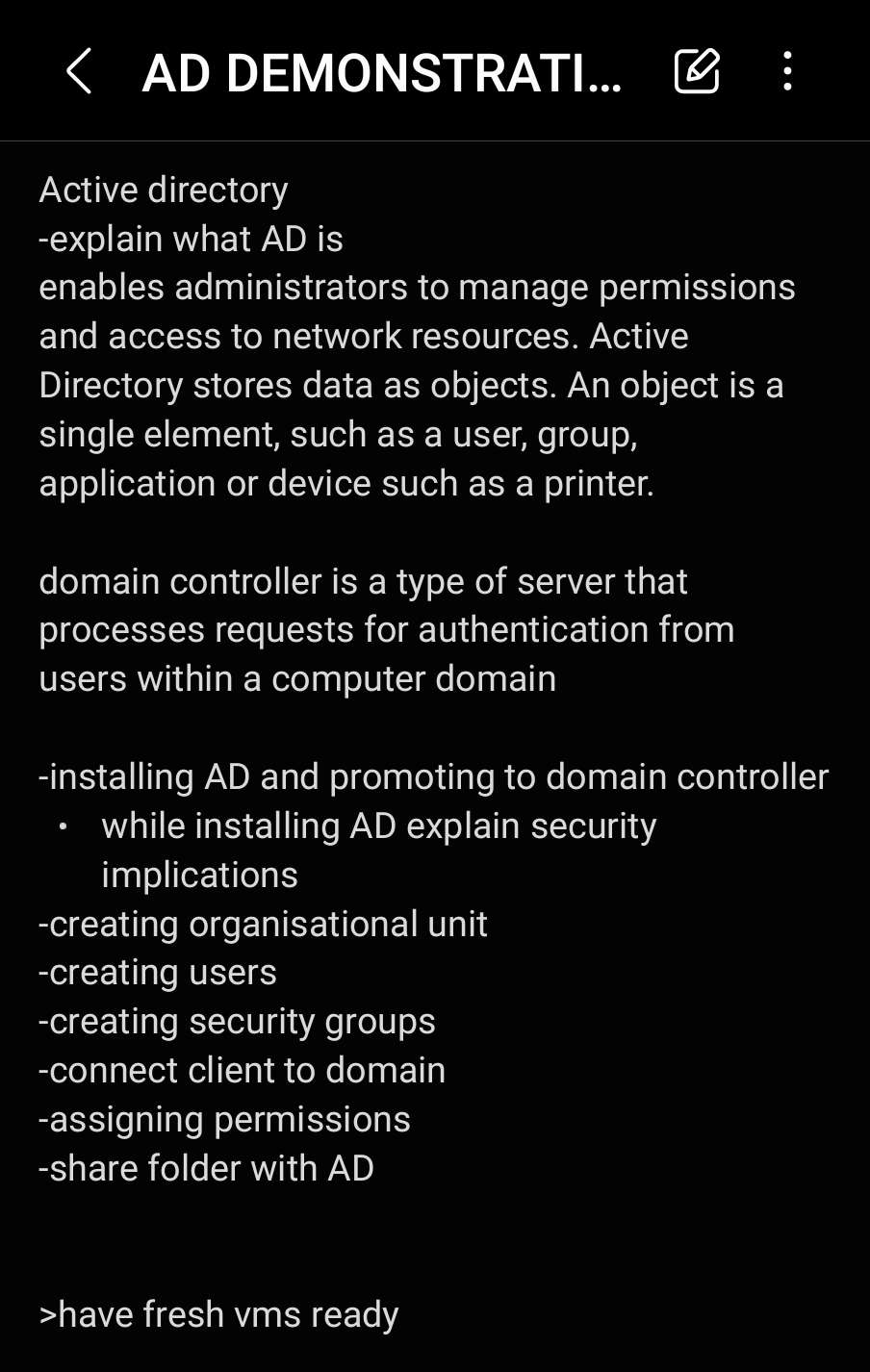
|  |  |
| --- | --- |
| **Summary** | *Teamwork: successful because…*   * *Everyone contributed and was actively involved as both member and leader.* * *Regular communication and milestones were completed on time.* * *Positive and supportive attitude from everyone.* * *Members were helpful and left no one behind. Collaborated as a team*   *Solution implementation: successful because…*   * *Backups created for preparation against faults.* * *Individualised accounts for all employees, with integration with applications, software, and websites.* * *Hierarchical, structured domain environment created to control user permissions.* * *Logins stored securely with AD.* * *Segmented network to protect against guest clients from interfering with the LAN.* * *Employee training and policy to prevent poor cyber practices.* |
| **Project Review** | *Most of the project objectives, scope, timelines, costs, quality, and other parameters mentioned above. This was the case given the current documentation are living documents, so expectations are adjusted.*  *Areas that were not addressed include:*   1. *Website issues including preventing fraud, proving ownership of content, protecting against unauthorised distribution and content mining would require specialists to rectify. Only the networking configuration was fixed.* |
| **Project Achievements** | *We all contributed effectively and managed to complete the demonstration section by supporting each other. Every section was a group effort, but individual contributions include:*   * *Will: App 3 questions, plan stage 1 (LAN), App 4 IPS vuln, App 5 IPS/IDS, Demo IPS* * *Kim: App 3 problems, plan stage 2 (website), App 4 backup vuln, App 5 virtualisation, Demo backup* * *Victor: App 3 scope, plan stage 3 (pfsense), App 4 AD vuln, App 5 networking devices & OS* * *Josiah: App 3 teaming, plan stage 4 (WLAN), App 4 phishing vuln, App 5 firewalls, Demo AD* * *Jimmy: App 3 plan resources, App 4 Wi-Fi vuln, App 5 user support & business implications, Demo wireless, Resolved Arlo-cam IoT* |
| **Possible Improvements** | *Overall, the team worked very effectively by…*   * *Delivering milestones* * *Regular meetings to support each other to meet deadlines.* * *Delegating tasks appropriately in line with proposed schedule* * *Being organised by using spreadsheets for appropriate content.*  *File sharing and resources on OneDrive made it easy to for everyone to contribute equally and ensured cohesion and relevancy in responses* * *Setting a timeline of necessary objectives.*     *Future optimisation…*   * *Highlighting overlap between sections where content can be copied.* |
| **Team Review** | *Yes, our team worked effectively on a consistent basis by meeting weekly timelines and cooperating to solve any issues. This is evident from our living timeline document and our discussion both in real life and through messages which can be seen on our chat logs (shown in the below table).*    *Our original strategies include…*   * *Having a timeline with objectives so we know where our progress should be and what to do next.* * *Being organised and communicating openly and actively.* * *Supporting and helping each other and having a positive attitude.* * *Focusing on getting a framework and content filled instead of being distracted with details, since future corrections aren’t difficult.* * *Changing the format of documents to excel files when appropriate for larger tables.* * *Having a dedicated OneDrive for easily accessible, shared access to files.*   *Since everyone in the group is a good individual contributor and willing to support others, it was a pleasant experience collaborating with each other. The results should speak for itself.* |
| **Possible Improvements** | *No major improvements aside from identifying overlapping sections in this report so repeated information could be copied to save time. This team performed very well and was organised so there are not any other noticeable improvements. Performance metrics would not be necessary for this specific group since we all did our part but would be applicable for other groups where some do not carry their weight.* |
| **Risk Review** | *Our team made an emphasis on identifying all the risks early on and systematically addressing everything within our current skillset. We did have to adapt some of our topics whilst working on them to prevent overlap and cover all major risk areas such as with appendix 4 and the lesson plan.* |
| **Possible Improvements** | *Although we identified all the risks early on and had a living document to adapt to any changes, we could have better communicated major risks outside our area of expertise that would require outsourcing to the company. This would include implementing cyber security policies (legal), and website mining and payment protection (web developer).* |

Lesson plans

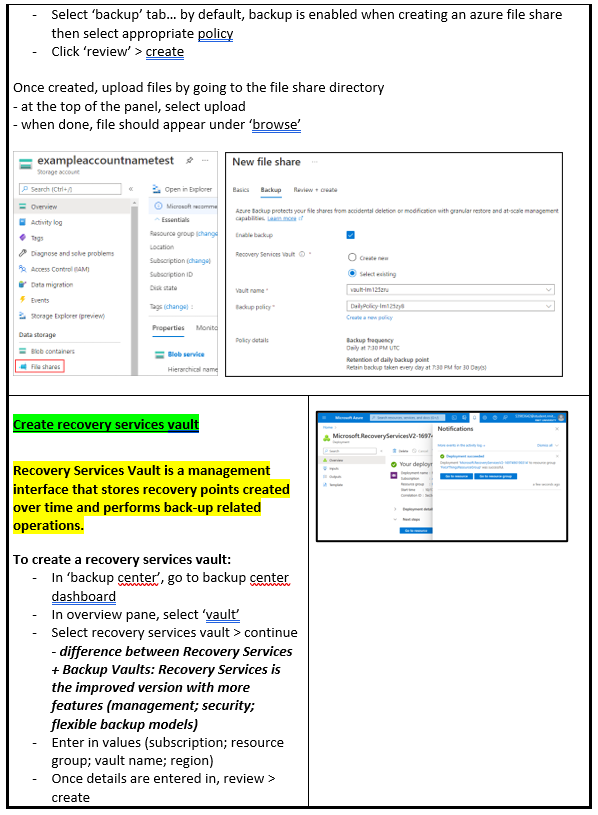
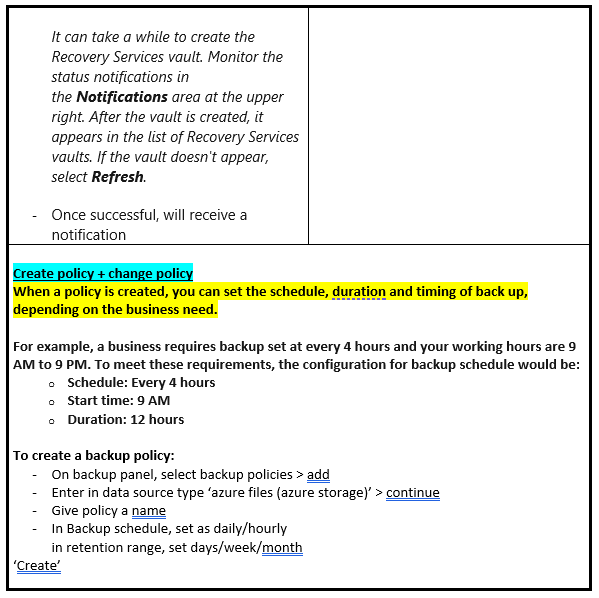
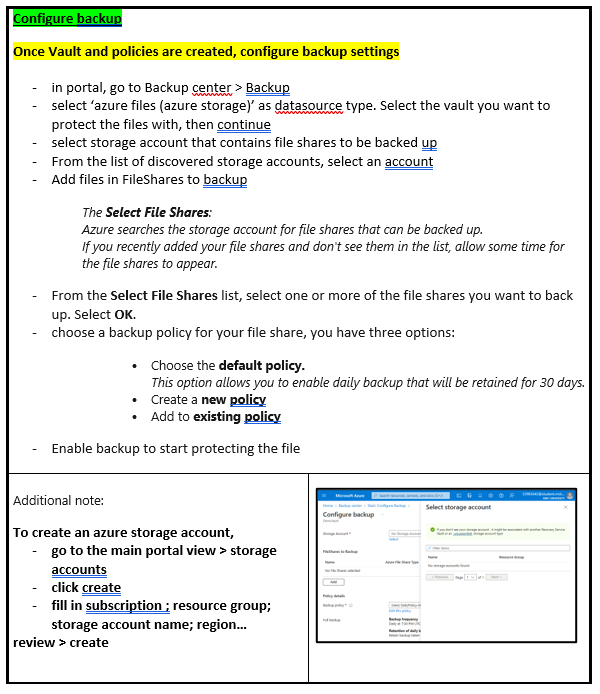
Jimmy

|  |
| --- |
| Inserting image... |
|  |
| Jimmy (continued) |
|  |

Josiah



Kim

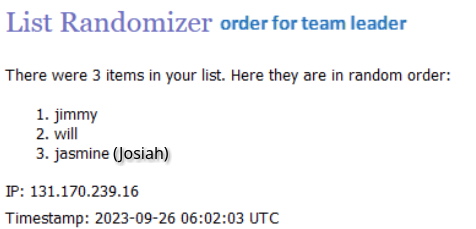
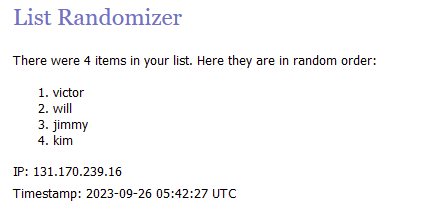
Victor – will be presenting for department on Nov 20th instead.

Will



|  |  |
| --- | --- |
| A screenshot of a computer  Description automatically generated | A screenshot of a computer  Description automatically generated |
| A screenshot of a computer  Description automatically generated | A screenshot of a computer  Description automatically generated |
| A screenshot of a computer  Description automatically generated | A screenshot of a computer  Description automatically generated |

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Screenshots and evidence**  *of activity in chat & list contributions* | **Proof of being a good leader** | **Proof of being a good member** |
| Jimmy Nguyen |  | * Delegating tasks * Actively engaging with members | 1. Contribution to the document 2. Active communication of completed tasks that were assigned 3. *Jimmy: App 3 plan resources, App 4 Wi-Fi vuln, App 5 user support & business implications, Demo wireless, Resolved Arlo-cam IoT* |
| Josiah Rulloda | Inserting image... | Delegating tasks  Actively engaging with members | 1. Contribution to the document 2. Active communication of completed tasks that were assigned |
| Kim Ho |  | Delegating tasks  Actively engaging with members | 1. Contribution to the document 2. Active communication of completed tasks that were assigned |
| Victor Lee | Leader above, member below | Delegating tasks  Actively engaging with members | 1. Contribution to the document   *App 3 scope, plan stage 3 (pfsense), App 4 AD vuln, App 5 networking devices & OS, App 6*   1. Active communication of completed tasks that were assigned |
| William Spiller | Inserting image... | Delegating tasks  Actively engaging with members | 1. Contribution to the document 2. Active communication of completed tasks that were assigned |



Section C **– Feedback to Student**

|  |  |  |  |
| --- | --- | --- | --- |
| **Has the student successfully completed the task?** | | Yes No | |
|  | |  |  |
| **Feedback to student:** | | | |
|  | | | |
| **Assessor Name** | **Date** | | |