|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Student Name | Dylan Wondal | Student Number | | 473393445 |
| Unit Code/s & Name/s | VU23217 Recognise the need for cyber security in an organisation | | | |
| Cluster Name  *If applicable* | N/A | | | |
| Assessment Name | Cyber Security Methodology Recommendation Portfolio | Assessment Task No. | | 2 of 2 |
| Assessment Due Date | Week 8 | Date Submitted | | / / |
| Assessor Name | Elankayer Sithirasenan | | | |
| **Student Declaration:** I declare that this assessment is my own work. Any ideas and comments made by other people have been acknowledged as references. I understand that if this statement is found to be false, it will be regarded as misconduct and will be subject to disciplinary action as outlined in the TAFE Queensland Student Rules. I understand that by emailing or submitting this assessment electronically, I agree to this Declaration in lieu of a written signature. | | | | |
| Student Signature |  | | Date | / / |
| **PRIVACY STATEMENT:** TAFE Queensland is collecting your personal information on this form for the purpose of assessment. In accordance with the Information Privacy Act 2009 (Qld), your personal information will only be accessed by staff employed by TAFE Queensland for the purposes of conducting assessment. Your information will not be provided to any other person or agency unless you have provided TAFE Queensland with permission, if authorised under our Privacy Policy (available at <https://tafeqld.edu.au/global/privacy-policy.html>) or disclosure is otherwise permitted or required by law. Your information will be stored securely. If you wish to access or correct any of your information, discuss how it has been managed or have a concern or complaint about the way the information has been collected, used, stored, or disclosed, please contact the TAFE Queensland Privacy Officer at [privacy@tafeqld.edu.au](mailto:privacy@tafeqld.edu.au) | | | | |

|  |  |
| --- | --- |
| Instructions to Student | General Instructions:  You are employed by MidTown IT as a cyber security analyst. Your job is to identify threats, risks and vulnerabilities in two different organisations and recommend suitable methodologies to protect the organisations’ data. The organisations are:   * WIDGET Accounting * Local Kindergarten   Your teacher/assessor will take on the role of the project manager assigned to this project by MidTown IT.  Read the project documentation provided and familiarise yourself with the Project Scenario or Case Study before proceeding with portfolio tasks. Confirm anything you are not sure about in the project with your manager (teacher/assessor). It is essential that you have a clear understanding of the scenario and tasks that you need to complete.  This assessment instrument requires the student to complete a project portfolio that is divided into six (6) parts:   * Part 1 – Cyber-security concepts * Part 2 – Identify cyber-security needs of organisations * Task 1: Identify organisations’ data risks, vulnerabilities and cyber-security needs * Task 2 Identify cyber-security measures for the organisation * Part 3 – Methods and tools to safeguard privacy * Task 1: Methods and tools selection * Task 2: Protecting personal data of an internet service user * Task 3: Demonstration – Cyber Kill Chain process and Malware * Part 4 – Internet of Things (IoT) devices * Part 5 – Current cyber-security frameworks * Part 6 – Contingency task   Materials Required:   * Access to PCs and peripherals – these may differ between classrooms * Access to the internet * Access to Connect (LMS) * Access to Word processing software, such as Microsoft Word * Access to special-purpose tools, equipment and materials to complete the assessment   Online Delivery:   * Students to supply their own PC or laptop, peripherals and internet access * Students will require permission to install the required software (e.g. Python) * Students will require access to Microsoft Office or similar application   Documentation:   * MidTown IT Scenario or Case Study * MidTown IT Cyber Security Methodology Recommendation Template   Assessment Criteria:  To achieve a satisfactory result, your assessor will be looking for your ability to demonstrate the following key skills/tasks/knowledge to an acceptable industry standard. Demonstrated ability to:   * Understand cyber-security concepts and terminology * Identify threats, risks and vulnerabilities * Identify current cyber-security threat trends * Identify the need for cyber-security systems in organisations * Determine cyber-security practice needs in organisations * Determine cyber-security attacks and techniques * Understand and differentiate between threat actors, threat vectors and threat goals * Recommend suitable cyber-security methodologies for organisations including infrastructure, equipment and software * Work with policies, procedures and tools for protecting organisational data * Identify the vulnerabilities of IoT devices * Investigate and use mitigation strategies such as Cyber Kill Chain Process and MITRE ATT&CK * Determine behaviour-based cyber-security strategies * Investigate and explain current cyber-security frameworks such as NTIs CSF, ACSC and CIS   Refer to the marking criteria for specific details:  VU23217\_AT2\_MC\_TQM\_v1  Details of location:  TAFE will provide a simulated work environment in the classroom. Research activities may be conducted in the classroom or at home.  If you are unable to attend a scheduled assessment activity, you must notify your teacher before the assessment is due and supply a doctor's certificate and approval from the team manager for an extension.  Time restrictions:  This assignment is designed to take place over eight (8) weeks or approximately 32 hours. The student is expected to attend classes as per timetable details and should be able to commit up to three (3) hours per week of their own time to study or study related activities.  Interactions:  Teamwork skills are essential in the IT industry, therefore you should work in teams to consult and collaborate on practical activities. However, each student must complete the assessment tasks individually (unless indicated).  Level of assistance permitted:  Staff cannot directly show students answers or solutions but can support and guide them to complete tasks individually. Teachers and tutors should be available in class and accessible by email for students working from home.  Reasonable Adjustments:  Reasonable adjustments are available to students for a variety of reasons, including disability, language, literacy and numeracy (LLN) problems or extenuating circumstances. Talk to your teacher, counsellor or disability officer if you require extra support or an extension based on the conditions identified.  Number of Attempts:  You will receive up to two (2) attempts at this assessment task. Should your 1st attempt be unsatisfactory (U), your teacher will provide feedback and discuss the relevant sections / questions with you and will arrange a due date for the submission of your 2nd attempt. If your 2nd submission is unsatisfactory (U), or you fail to submit a 2nd attempt, you will receive an overall unsatisfactory result for this assessment task. Only one re-assessment attempt may be granted for each assessment task.  ***For more information, refer to the Student Rules.***  Work, Health and Safety:  The work environment should be assessed for safety prior to class. Special consideration should be taken regarding potential ICT-related hazards such as tripping hazards, electromagnetic radiation, ergonomics and posture. TAFE Queensland health and safety policies and procedures should be followed at all times. |
| **Submission details** (if relevant) | Evidence Required to be Submitted:  Insert your details on the cover page and sign the Student Declaration. Include this template with your submission.  Submission via Connect:  Upload a single file into Assessment 2 (AT2) Assignment Folder in Connect.  Multiple files can be compressed into a single file.  Name the file:  VU23217\_AT2\_Surname\_Student Number  Accessing Connect:   * TAFE Queensland Learning Management System (Connect): [*https://connect.tafeqld.edu.au/d2l/login*](https://connect.tafeqld.edu.au/d2l/login) * **Username:** 9 digit student number * **For Password:** Reset password go to: [*https://passwordreset.tafeqld.edu.au/default.aspx*](https://passwordreset.tafeqld.edu.au/default.aspx) |
| Instructions to Assessor | Specifications of assessment:  To be judged competent in this assessment item, the student is required to demonstrate competence in all indicators shown in the marking guide.  Gather evidence to demonstrate consistent performance in conditions that are safe and replicate the workplace. Noise levels, production flow, interruptions and time variances must be typical of those experienced in the cyber-security field of work and include access to:   * project requirements.   Ensure that students read and familiarise themselves with the Project Scenario provided and relevant files and/or resources before attempting the assessment.  Storage Devices:   * Students are required to provide their own storage device.   Materials Required:   * Access to PCs and peripherals – these may differ between classrooms * Access to the internet * Access to Connect (LMS) * Access to Word processing software, such as Microsoft Word * Access to special-purpose tools, equipment and materials to complete the assessment   Online Delivery:   * Student to supply their own PC or laptop, peripherals and internet access * Students will require permission to install the required software (e.g. Python) * Students will require access to Microsoft Office or similar application   Documentation:   * MidTown IT Scenario or Case Study * MidTown IT Cyber Security Methodology Recommendation Template   Level of Assistance Permitted:  Teachers and tutors should be available in class and accessible by email for students working from home. Staff cannot directly show students answers but can support and guide them to complete tasks individually. Students with disability will receive reasonable adjustments.  Interactions:  Teamwork skills are essential in the IT industry, therefore you should work in teams to consult and collaborate on practical activities. However, each student must complete the assessment tasks individually (unless indicated).  Contingencies:  Reasonable adjustment is available to students for a variety of reasons, including disability, language, literacy and numeracy (LLN) problems or extenuating circumstances.  Work, Health and Safety:  The work environment should be assessed for safety prior to class. Special consideration should be taken regarding potential ICT-related hazards such as tripping hazards, electromagnetic radiation, ergonomics and posture. TAFE Queensland health and safety policies and procedures should be followed at all times. |
| Note to Student | *An overview of all Assessment Tasks relevant to this unit is located in the Unit Study Guide.*  If you have any questions or need help regarding this assessment item, please contact your teacher/tutor through email or during face-to-face sessions. |

# Project Scenarios

You are employed by MidTown IT as a cyber security analyst. Your job is to identify threats, risks and vulnerabilities in two different organisations and recommend suitable methodologies to protect the organisations’ data.

Your teacher will take on the role of project manager for the projects.

|  |  |
| --- | --- |
| Scenario-01 | Scenario 1: WIDGET Accounting |
| WIDGET Accounting is a small company located in Belconnen in the ACT. They have 15 employees, including an office manager and the business owner. Ten of the employees work onsite at the office, whilst the remaining five work remotely from home or at a client’s premises.  Responsibility for ICT resides with their office manager, who is working their way through a TAFE ICT course in their spare time.  WIDGET’s ICT infrastructure consists of the following:   * All the staff use laptops with Windows 10 Pro as the SOE. These are all standard licences, are patched and do NOT have security software installed. Staff are free to choose their own passwords for their individual machines. * The business has recently moved to the Office 365 Business subscription service for Microsoft Office applications. * Wireless internet access for office staff is provided via ADSL using a D-Link-2740B wireless router and the Wi-Fi password is publicly available. * Staff are permitted to connect their mobiles, laptops and other electronic devices through this wireless network. They can also form an Internet-of-Things (IoT) structure by connecting these devices at the same time for work purposes. * Wired network and internet access are also provided by a recently installed NETGEAR JGS524 24-Port Gigabit Switch. There are 20 network jacks available, which can be used to connect any physical computing device. A couple of jacks are located in the public area of the office accessible to clients and visitors. * Staff working remotely use either their personal mobile phones as hot spots or their home internet connections to connect to the internet and they do not have any password policy enforced. * Sensitive data is stored on laptops, servers and the NAS without using cryptographic techniques. * Employees share passwords and logins with each other if they are having difficulty logging in or they need to access material on other machines. * The business does not have a website and instead conducts marketing campaigns through a Facebook page and a Twitter account. The username and password for these services are the same as the business owner’s username and password for his work laptop. | |

|  |  |
| --- | --- |
| Scenario-01 | Scenario 2: Local Kindergarten |
| **Employees:** 12  **Remote work:** Some admin employees work from home two to three days a week.  **Online activities:** Enrolments and related activities (e.g. cancellations, attendance changes)  **Max number of children:** 150  **Children’s ages:** 0 to 3-years-old  Organisational data includes:   * Staff details * Payroll details * Equipment details * Children’s details – including medical records * Parents’ and guardians’ details   Networked devices:   * 10 PCs * Peripherals e.g. fax, printers and scanners * 12 laptops * 12 company mobile phones * 15 tablets * Smart TVs * 2 robots (internet connected) – can dance and play nursery songs on demand * 7 intelligent baby monitors – internet connected * A number of voice-activated devices | |

# Instructions:

In order to comply with organisational procedures and standardised documentation, you must use the template provided to complete parts 1 to 6 – MidTown IT Cyber Security Methodology Recommendation Template.

## PART 1 – Cyber-security concepts

Before starting your analysis of the two organisations, a revision of the most common cyber-security concepts is required.

* 1. Define the following concepts:

1. A cyber-security threat

**A cyber-security threat is an unwanted threat to a company’s technological resources and can lead to data being stolen, confidential information stolen and a general disruption to the digital side.**

1. Threat actors

**A threat actor is the person or group behind the cyber-security threat with malicious goals in mind.**

1. Threat vectors

**A threat vector is how the threat actors gain unwanted access to a computer system whether it is through vulnerable software or social engineering.**

1. Threat goals

**The threat goal is what the attackers end goal is once a system is compromised, whether that be installing malware, stealing data or taking the system completely offline.**

* 1. Cyber-security attacks

1. Outline the characteristics of a cyber-security attack.

**The general characteristics of a cyber-security attack are**

1. Identify and explain three (3) sources of cyber-security attacks.

**1.** **Nation/state backed groups – These groups are secretly sponsored by their government and usually target enemy states/countries. An example of the Lazarus group who is backed by North Korea**

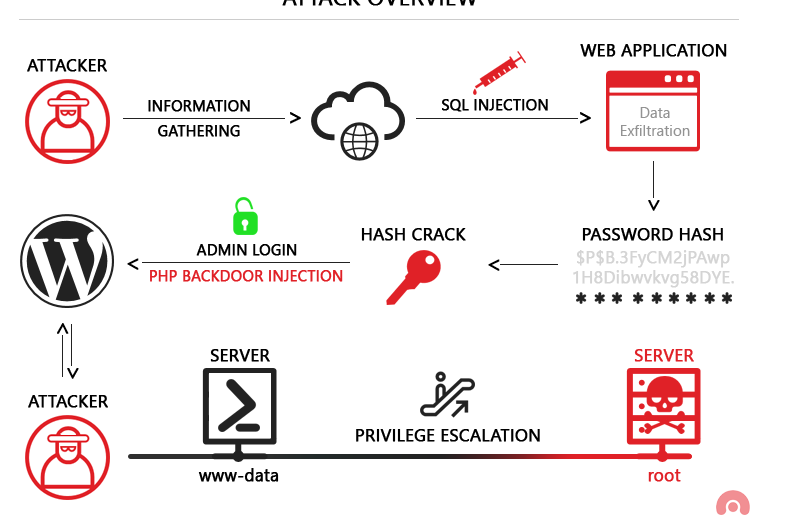
**2. Hacktivists – These groups are made of people from all over the world and have a goal usually for the better of the world. The most known hacktivist group is Anonymous.**

**3. Cybercriminals – These groups are organised and usually aim to gain from hacking a company whether it be financial or confidential database**

1. Explain how an attack operates. Use an example to illustrate your answer.

**An attack starts with reconnaissance to find out as much information about the target as possible. The next step in an attack the exploitation where the vulnerable system is attacked and the attackers gain unauthorised access. From there the attackers can either attempt privilege escalation or begin the malicious tasks.**

**The following diagram shows an attacker using SQL injection:**

**(Image: Agathoklis Prodromou, 2019)**

* 1. Investigate and explain at least three (3) common and emerging cyber-security attacks, and techniques used by threat actors to infiltrate an organisation. Provide references for your sources using a formal referencing style, e.g. APA or Harvard.

**1. Phishing:**

**Phishing is the most common attack used by threat actors to gain access to a system. Phishing involves sending a fake email that appears to come from a known source and tricks the user into downloading/installing malware or revealing personal information. A common technique for threat actors is spear-phishing where the fake message includes information about the target which can help make them believe the message is legitimate (CheckPoint, 2020).**

**2. Ransomware:**

**Ransomware is another common attack used. It is a piece of malware that encrypts everything on the victims computer and can only be decrypted using the key that the threat actors have. To get the key, the victim must pay a certain amount usually in cryptocurrency so it can’t be traced. A common technique is to combine the ransomware with a phishing attempt to get the target to download and run the software (Australian Cyber Security Centre, 2021).**

**3. Supply chain attacks**

**Supply chain attacks are becoming a more common threat in the current day where threat actors will attack their targets suppliers/partners to gain access to their systems and then eventually reach their true target. Techniques used are malware insertion where malware is inserted into a legitimate update package and then run by the target, installing the malware Korolov, 2020).**

* 1. Investigate and outline at least three current cyber-threat trends and outline their potential effect on an organisation’s data.

**1. A current cyber threat to an organisations data is the work from home people. Usually these staff will use their own devices which most likely won’t have the same security as the devices that are in the office. This means they are more likely to be successfully attacked and an organisations private data can be stolen through the remote user.**

**2. Internet of things is another threat that hackers can take advantage of as most IOT devices are not thought of when securing devices. Since most IOT devices are connected to the internet, threat actors can gain access to them then pivot further into the organisations network and steal sensitive data.**

**3. Cloud security is another threat that can be exploited to gain sensitive data. With a lot of companies using cloud providers to host their data, a simple misconfiguration in the access controls can allow any unauthenticated user to access the data from anywhere at any time.**

* 1. Research and explain the following cyber-security terms:

1. Botnets

**A botnet is a network of devices that have been compromised and taken over to be used for malicious activities such as email spam or denial of service attacks (Paloaltonetworks.com, 2019).**

1. Malware

**Malware is software that has malicious intent and can cause damage or harm to a network or system (Malwarebytes, 2020).**

1. Viruses

**A virus is a piece of software that can replicate itself to other devices and continue to spread and possibly delete files (Nieles, Dempsey and Pillitteri, 2017).**

1. Worms

**A worm is similar to a virus in that it replicates and spreads but a worm does it through networks to reach other systems (Nieles, Dempsey and Pillitteri, 2017).**

1. Root Kits

**A root kit is software that allows hackers to have administrator level privileges. This is achieved with the root kit operating at kernel level which has the most access to the host system(Kaspersky, 2021).**

## PART 2 – Identify cyber-security needs of organisations

### Task 1: Identify organisations’ data risks, vulnerabilities and cyber-security needs

For **each** scenario presented, provide the following information:

* 1. Describe the organisation’s data types and associated data risks for each type of data identified.
  2. Identify the different ways data is accessed in the organisation.
  3. Consider the risk that a security breach poses for the organisation and describe the reason the organisation has to protect:

1. Organisation’s data
2. Online identity of users and their private data
   1. Based on each organisation’s data, identify the potential vulnerabilities of the organisation. Identify and explain at least three (3) vulnerabilities.
   2. For each vulnerability identified, explain the techniques that attackers could use to infiltrate the data.
   3. For each organisation, list and explain the cyber-attack methods that could be utilised to bring their infrastructure defences down.

### Task 2: Identify cyber-security measures for the organisation

Task 1 identified the organisations’ data, risks and vulnerabilities. This section concentrates on outlining the security measures required to protect the organisations against potential cyber attacks.

For **each** scenario presented, complete the following tasks:

* 1. Based on the information obtained in Task 1, outline a strategy to defend the organisation’s data from threat actors. The strategy must include:

1. Cyber-defence methods
2. Cyber-defence techniques
3. Organisational policies and procedures
   1. Recommend four (4) essential cyber-security awareness practices for the scenarios presented.

## PART 3 – Methods and tools to safeguard personal privacy

### Task 1: Methods and tools selection

For **each** scenario, complete the following tasks:

3.1 Examine the scenario presented and identify the security methods and tools that could be used to protect the organisation’s data. For each method and tool, provide a brief description.

3.2 Outline the setup required to protect the organisation from cyber-security attacks. The setup includes:

1. Common infrastructure
2. Equipment
3. Software

3.3 Investigate and propose measures to protect the organisation from cyber attacks. The measures must include:

1. Relevant cyber-security policies and procedures
2. Cyber-security tools and systems

3.4 Explain the following mitigation strategies and identify how they could be utilised in the scenario presented.

a) Cyber Kill Chain process

b) MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK)

3.5 Investigate and explain why *behaviour-based security* is different from a traditional firewall. Which methods should be used in the scenario? And why?

### TASK 2: Protecting personal data of an internet service user (not part of the scenarios)

3.6 Select one of the following online services:

* Facebook
* Twitter
* Instagram
* LinkedIn

Find the terms of service and any privacy/security policies for the selected online service. Read these documents.

A friend of yours suffers a breach of privacy on the selected service, so you decide to improve your own security on this service. In your own opinion, what processes could you take to keep the information on this service secure and private? In your answer, include not only the mechanisms and configurations of the service you can use, but also what actions you can take (as a user) to protect yourself, e.g. don’t upload certain sorts of information or don’t upload certain photos.

### Task 3: Demonstration: Malware simulation

3.7 **Attacking a system with malware**

Part of the Cyber Kill Chain process (used by attackers to infiltrate a system) is to deliver malware into the system which exploits a vulnerability in the system. In this task, you will simulate these steps in the Cyber Kill Chain process.

For this activity, you need to select a malware simulation tool. Identify and briefly describe the tool.

Run the selected tool within your virtual environment.

Launch the simulated malware attack. Take screenshots that show the delivery of the malware to the user, the user launching the malware and any results (successful or otherwise) of the malware. Submit screenshots as evidence.

3.8 After completing 3.7, answer the following questions:

a) Was the malware attack successful or not?

b) If successful, how do you know that it was successful?

c) If not, what defence mechanism on your PC prevented the attack?

## PART 4 – Internet of Things (IoT) devices

**For this part of the portfolio, you can concentrate on the scenario that is more likely to use IoT devices.**

4.1 Provide examples of IoT devices that could be implemented in the scenario selected. Identify at least three (3) devices.

4.2 For each IoT device identified in 4.1, research and explain manufacturers’ details on:

a) The methods that the device uses to protect data privacy

b) The techniques used to protect devices from cyber threats

c) User authentication techniques

d) Devices vulnerabilities

Provide references for your sources as evidence using a formal referencing style, e.g. APA or Harvard.

4.3 **IoT Demonstration** (not part of the scenarios)

**NOTE:** Your teacher/assessor may direct you to use a different network simulator program if Cisco Packet Tracer is not available.

Create a small local area network using the Cisco Packet Tracer network simulator with the following devices and cabling:

Diagram

Description automatically generated

Screenshot of CISCO Packet Tracer used with permission from CISCO.

Open a new packet tracer file and add in the required devices as per the diagram.

* Configure the Home Router with the IP address of 192.168.0.1/24.
* DHCP enabled and starting IP address of 192.168.0.50
* 2.4ghz and 5 ghz SSID of HomeNetwork
* WiFi Security Mode WPA2 Personal
* WiFi Encryption AES
* WiFi Password HomeNetworkPass
* Configure the Server with a static IP address of 192.168.0.2/24
* Configure the Server to be an IoT Server
* Create the IoT User admin with password admin through the Server desktop app ‘IoT Monitor’
* Configure all other devices to connect to the Home Router WiFi network and get their IP address via DHCP.
* Register the IoT devices to the Server 192.168.0.2 using the username/password of admin/admin
* Use the Smartphone to login to the desktop app ‘IoT Monitor’ using the admin credentials.
* Paste a screenshot below of all the devices connected and their current status set as follows:
* Door – Locked
* Fan – Low
* Light – On

## PART 5 – Current cyber-security frameworks

Investigate the following current cyber-security frameworks and provide the information requested.

5.1 National Institute of Standards and Technology Cyber Security Framework (NIST CSF)

|  |  |
| --- | --- |
| NIST CSF | |
| Definition: |  |
| **Fundamentals:** |  |
| Purpose: |  |
| Objectives: |  |

5.2 Australian Cyber Security Centre (ACSC)

|  |  |
| --- | --- |
| ACSC | |
| Definition: |  |
| **Essential Eight Strategies:** |  |
| Purpose: |  |
| Objectives: |  |

5.3 Centre for Internet Security (CIS)

|  |  |
| --- | --- |
| CIS | |
| Definition: |  |
| **CIS controls:** |  |
| Purpose: |  |
| Objectives: |  |

## PART 6 – Contingency task

6.1 Assume that, as a cyber security analyst, you have analysed the cyber-security needs of an organisation and presented a recommendation that includes the methodology, tools, policies, cyber-awareness training requirements and cyber best practices. Communication with the client has been very positive and you are confident that management will go ahead and implement the cyber-security recommendation. However, you have just received an email communicating to you that a new director has been appointed and she considers your recommendation excessive for the type of data that they manage. How would you proceed from this point?

References:

Agathoklis Prodromou (2019). *Exploiting SQL Injection: a Hands-on Example | Acunetix*. [online] Acunetix. Available at: https://www.acunetix.com/blog/articles/exploiting-sql-injection-example/.

CheckPoint (2020). What Is Phishing? *Check Point Software*. [online] 3 Nov. Available at: <https://www.checkpoint.com/cyber-hub/threat-prevention/what-is-phishing/>.

Australian Cyber Security Centre (2021). *Ransomware | Cyber.gov.au*. [online] Cyber.gov.au. Available at: <https://www.cyber.gov.au/ransomware>.

‌

Korolov, M. (2020). *What is a supply chain attack? Why to be wary of third-party providers*. [online] CSO Online. Available at: https://www.csoonline.com/article/3191947/supply-chain-attacks-show-why-you-should-be-wary-of-third-party-providers.html.

‌

Paloaltonetworks.com. (2019). *What is a Botnet? - Palo Alto Networks*. [online] Available at: https://www.paloaltonetworks.com/cyberpedia/what-is-botnet.

‌

Malwarebytes (2020). *What is malware? Definition and how to tell if you’re infected*. [online] Malwarebytes. Available at: <https://www.malwarebytes.com/malware>.

‌Nieles, M., Dempsey, K. and Pillitteri, V.Y. (2017). An introduction to information security. *An Introduction to Information Security*. [online] doi:https://doi.org/10.6028/nist.sp.800-12r1.

‌

Kaspersky (2021). *What is Rootkit – Definition and Explanation*. [online] www.kaspersky.com. Available at: https://www.kaspersky.com/resource-center/definitions/what-is-rootkit.

‌

**End of Assessment**