CASE-STUDY GUIDELINES:

The report should investigate all reasonable threats AND address the following three questions:

- Could an online presence grow the business by up to 50%?
- Could changing to an international supply chain reduce costs by up to 24%?
- Could the business lose up to 33% of its existing customers if the business doesn't provide some online features?

Risk Assessment of The Pampered Pets Business as It Stands Currently

- A selection of a risk assessment methodology with justifications for the selection.
- A risk and threat modelling exercise that enumerates and evaluates the current threats and risks to the business.
- A list of potential mitigations to the identified risks and threats.

Carry out a risk assessment around the potential digitalisation process as applied to the Pampered Pets business

- A selection of a risk assessment methodology with justifications for the selection.
- A list of proposed changes that form the basis of the digitalisation process/ transformation (e.g., e-commerce portal, ERP system, online marketing, blogs, etc. – note you do not have to include ALL these features).
- A risk and threat modelling exercise that enumerates and evaluates the potential threats and risks to the business of the proposed changes.
- A list of potential mitigations to the identified risks and threats.

1000 Word Limit

Development Team Project: Risk Identification Report

Risk Assessment of The Pampered Pets Business as It Stands Currently

1) Octave-S

As from (Lambrinoudakis, et al., 2022), '**O**perationally **C**ritical **T**hreat, **A**sset, and **V**ulnerability **E**valuation' is a self-directed approach that is tailored to be used by small organisations (less than 100 people).

3 to 5 interdisciplinary team-players collect and analyse data, producing a protection strategy and mitigation plans according to the organisation's operational security risks.

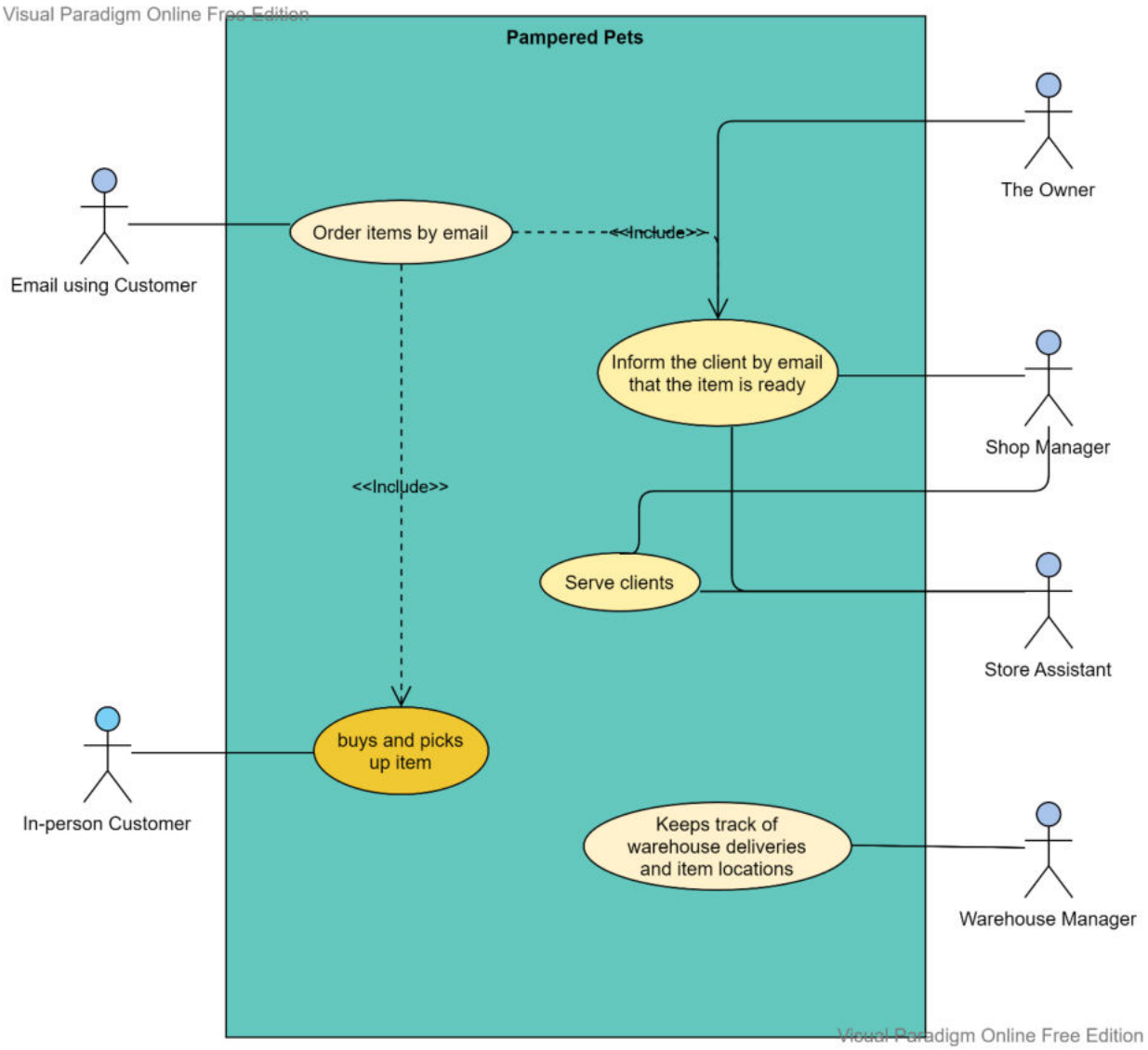
A. **Phase 1: Creation of Asset-Based Threat Profiles:** First it involves gathering enterprise, operational area and staff knowledge about the enterprise so as to create the table below. (Tsukerman, 2020)

Critical Assets that are important to the enterprise	**Threat profile**	**Security Requirements**
Hardware (Computers)	• Theft • Virus and malwares • Slow processing	• A secure place, cctvs, guards, etc. • Antivirus • Upgrades and updates • Firewalls • Upgrade to router
Network Devices	• Theft • Hacking • Unauthorised access • Slow dataflow	

	• Denial of Service	• Availability of fast network connection • Authentication • Authorisation • Non-repudiation • Security Architecture and Design • Incident Management • Integrity • Availability • Data Loss Prevention • Confidentiality • Disaster Recovery • Physical Access Control • Monitoring and Auditing Physical Security • System and Network Management • Monitoring and Auditing IT Security • Encryption • Cybersecurity training
Software (Spreadsheet Package)	• Repudiation • Slow dataflow and processing of data • Tampering • Unauthorised access	
Data/Information	• Repudiation • Slow dataflow and processing of data • Information disclosure • Tampering • Data Loss and Theft • Unauthorised access	
Humans	• Social engineering attack • Lack of cybersecurity training	
Reputation	• Information disclosure • Tampering • repudiation • Cyber attacks	

	• Unauthorised access	• Security Strategy and Management • Data privacy and security Policies like GDPR • Cybersecurity insurance
Services	• Information disclosure • Tampering and Unauthorised access	

B. Phase 2: Identification of infrastructure vulnerabilities



C. Phase 3, Identification of risks to the critical assets, creation of a protection strategy and mitigation plans to address the risks to the critical assets

2) **MITRE ATT&CK (Adversarial Tactics, Techniques, and Common Knowledge).** is a globally-accessible knowledge base and model of cyber attackers' behaviour that reflects the various stages of an attacker's attack lifecycle and the platforms they are known to target (Trellix, N.D.). Matrices for Windows, Linux, Mac, and mobile Systems exist and highly helpful in diagnosing attacks. Below is a description as from (Anon, N.D.)

Tactic	Description	Techniques	Solutions
Initial Access	Trying to gain access into the network.	• Phishing • Replicate using removable media • Valid accounts • Hardware Additions	• Antivirus • Upgrades and updates • Firewalls • Upgrade to router for a faster and more secure network connection • Authentication • Authorisation
Execution	Trying to run a malware	• Scheduled task • Shared modules • User execution • System services	

Persistence	Any access, action, or configuration change to a system that allows an attacker to have a persistent presence in that system	• Account manipulation • Boot or logon AutoStart execution • Browser Extensions • Create/modify Account or system process • Event triggered execution • Modify authentication process • Valid accounts	• Non-repudiation • Security Architecture and Design • Incident Management • Integrity • Access controls • Data Loss Prevention • Disaster Recovery • Physical Access Control • Monitoring and Auditing Physical Security • System and Network Management • Monitoring and Auditing IT Security • Encryption
Privilege Escalation	attacker gaining a higher privilege level on a system or network e.g.	• DLL Injection • Well shell • Valid accounts • Scheduled tasks • Hijack execution flow	

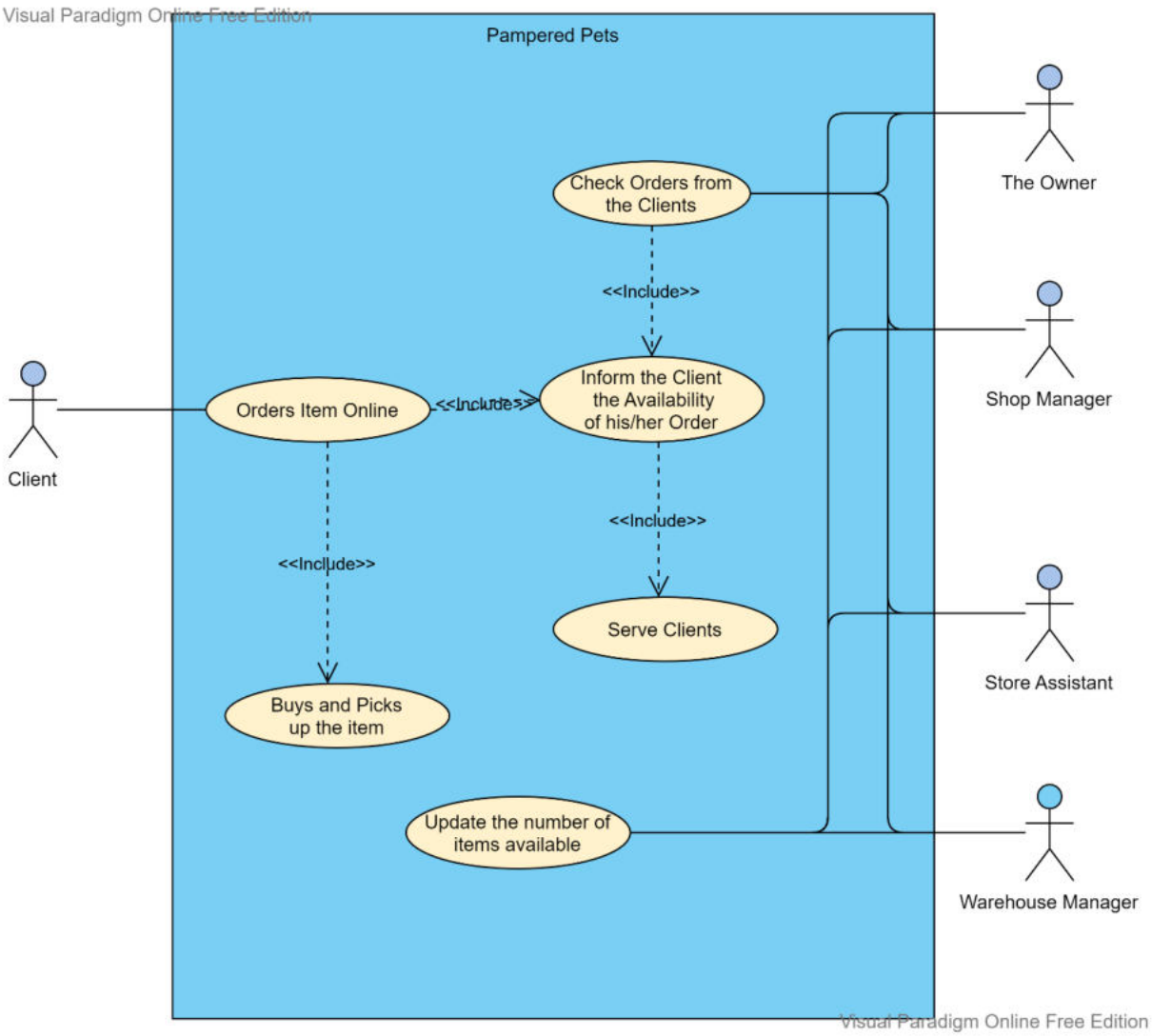
Defence Evasion	Techniques that an attacker can use to avoid detection e.g.,	• file deletion • pre-OS boot • Injection • Weaken encryption • Valid Accounts	• Cybersecurity training • Security Strategy and Management • Data privacy and security Policies like GDPR • Event management
Credential Access	Access to credentials used in an enterprise environment.eg	• Credential dumping, • Key logging, • Input capture • Brute force • Man-in-the-middle • Steal web session cookie • Network sniffing	
Discovery	Allows attacker to gain knowledge of the system and network	• Application Window discovery • Network service discovery	

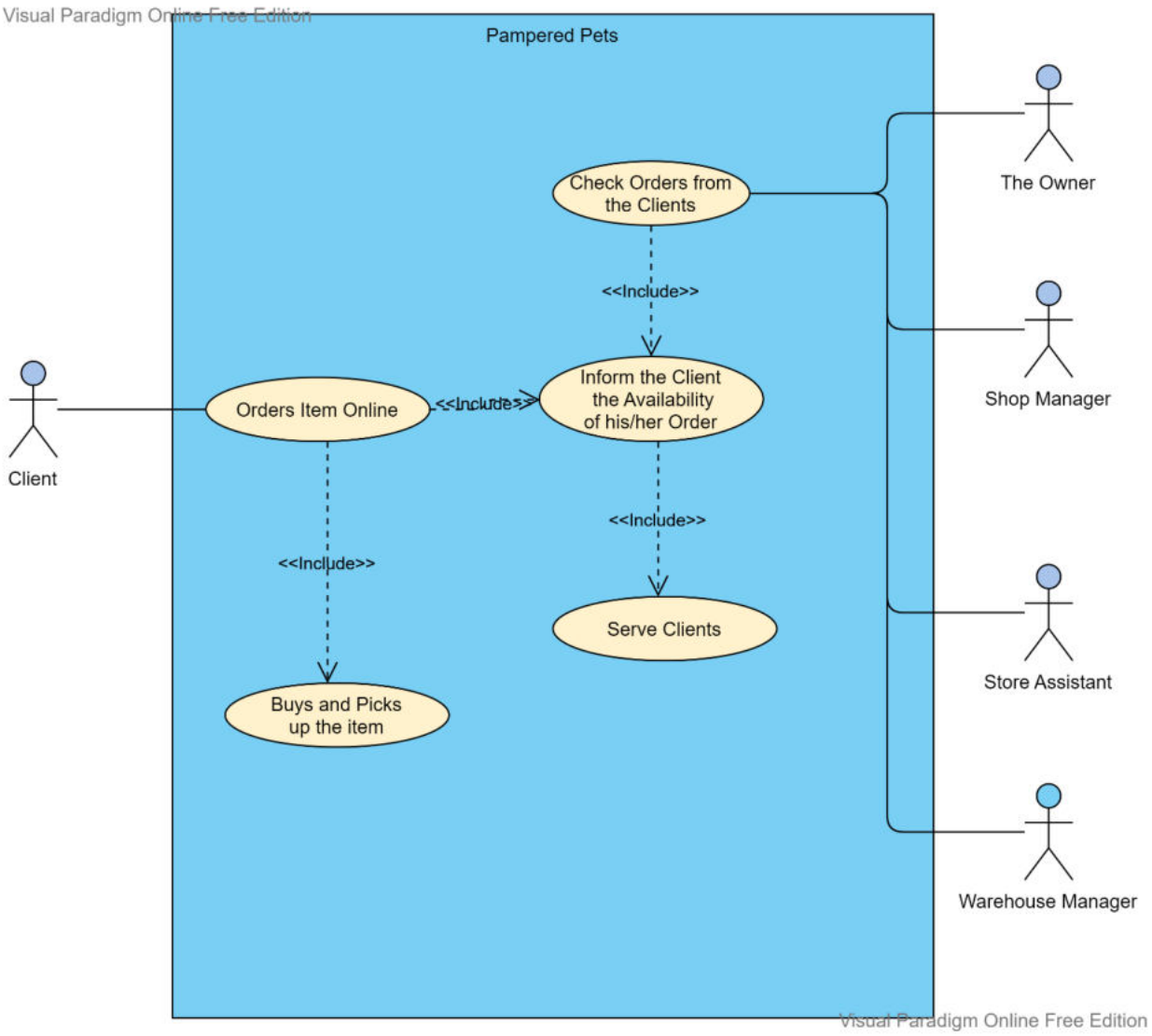
		• File and directory discovery • Sniffing • Password policy discovery • Permission group discovery	
Lateral Movement	Gaining access and control remote systems on a network	• Replication through removable media • Software deployment tools • Sharing tainted data	
Collection	Attacker collecting data for their own benefits	• Browser session hijackin • Data from local system	
Exfiltration	Stealing data	• Scheduled transfer	
Impact	Trying to manipulate, interrupt or destroy data	• Network Denial of Service	

		• Data manipulation, destruction, encryption • Defacement • Account access removal • System shutdown/reboot	

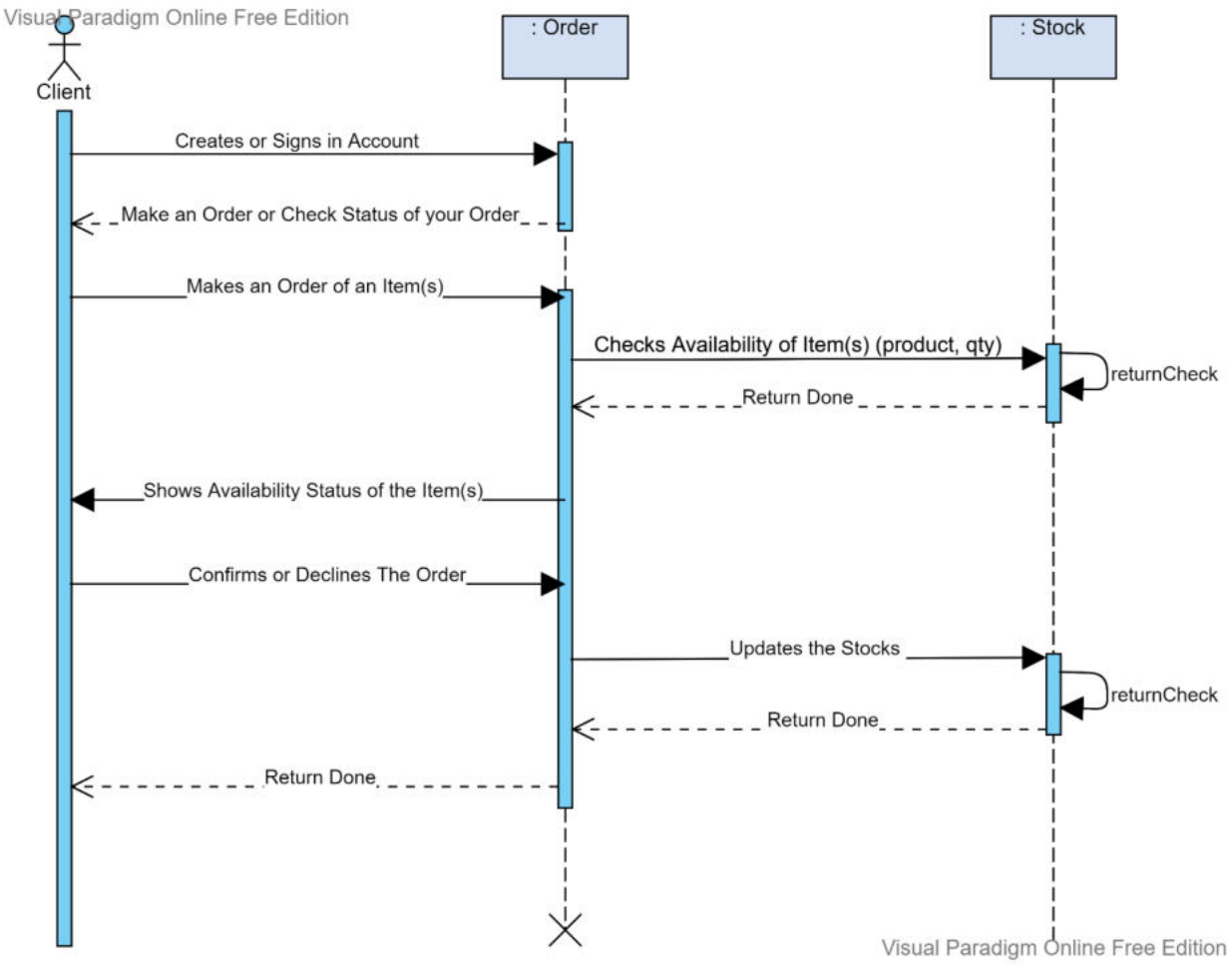
1) Diagrams after Digitalisation

I have created a few diagrams (2 use case diagrams and a sequence diagram); you can choose the most suitable one. Else let me know if any modification is needed.


Visual Paradigm Online Free Edition
Pampered Pets
Check Orders from the Clients
<<Include>>
Inform the Client the Availability of his/her Order
<<Include>>
Serve Clients
Orders Item Online
<<Include>>
<<Include>>
Buys and Picks up the item
Update the number of items available
Client
The Owner
Shop Manager
Store Assistant
Warehouse Manager
Visual Paradigm Online Free Edition


Visual Paradigm Online Free Edition
Pampered Pets
Check Orders from the Clients
The Owner
<<Include>>
Shop Manager
Client
Orders Item Online
<<Include>>
Inform the Client the Availability of his/her Order
<<Include>>
<<Include>>
Serve Clients
Store Assistant
Buys and Picks up the item
Warehouse Manager
Visual Paradigm Online Free Edition

2)



3) List Of Proposed Changes That Form the Basis of The Digitalisation Process

a. **Upgrade to a more secure spreadsheet application, ERP**

b. **Network upgrade:** firewalls, switch or router application preferably a router because it can link wired and wireless network and also it is more secure and gives faster connection than hub (Orenda, 2017), Wi-Fi access passwords, for

c. **data loss prevention,** like Cloud data storage, External hard disk backup, data backup to servers
d. **can create a domain server so as to have a centralised management of the network, user accounts, data, emails etc**
e. **Antivirus** installation in the computers
f. **Upgrade/buy computers to latest technology since harry is using an old computer.**
g. **Computers to have better set-ups.** E.g. automatic updates, Authentication and Authorisation,
h. **A secure Online application or website for the clients to purchase products from**
i. **Cybersecurity Insurance**
j.

Text in orange do not use since we won't be using OCTAVE.

The use case diagram was just for my notes.

References

Lambrinoudakis, C. et al., 2022. *COMPENDIUM OF RISK MANAGEMENT FRAMEWORKS WITH POTENTIAL INTEROPERABILITY,* Attiki, Greece: European Union Agency for Cybersecurity (ENISA).

Tsukerman, E., 2020. *Cybersecurity Threat Modeling with OCTAVE.* [Online]
Available at: https://www.pluralsight.com/guides/cybersecurity-threat-modeling-with-octave
[Accessed 9 September 2022].

Anon, N.D.. *Mitre Att&ck.* [Online]
Available at: https://attack.mitre.org/
[Accessed 10 Seeptember 2022].

Carnegie Mellon Institute, N.D. *Octave Forte.* [Online]
Available at: https://resources.sei.cmu.edu/asset_files/FactSheet/2020_010_001_643960.pdf
[Accessed 9 September 2022].

Orenda, 2017. *Do You Know the Difference Between Hub, Switch & Router.* [Online]
Available at: https://medium.com/@fiberstoreorenda/do-you-know-the-difference-between-hub-switch-router-b74c2e8a8143
[Accessed 9 September 2022].

Trellix, N.D.. *What Is the MITRE ATT&CK Framework?.* [Online]
Available at: https://www.trellix.com/en-us/security-awareness/cybersecurity/what-is-mitre-attack-framework.html
[Accessed 9 September 2022].